Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2017/2018

Obsah

I. prednáška

O logike a tomto kurze
Syntax výrokovej logiky

19. februára 2018

1. Úvod

1.1. O logike

I.1 Čo je logika

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

Jazyk zápis pozorovaní, definície pojmov, formulovanie teórií

Syntax pravidlá zápisu tvrdení

Sémantika význam tvrdení

Usudzovanie (inferencia) odvodenie nových dôsledkov z doterajších poznatkov

Dôkaz presvedčenie ostatných o správnosti záverov usudzovania

I.2 Poznatky a teórie

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

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

P1: Sarah nepôjde na párty, ak pôjde Kim.

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

P3: Sarah nepôjde bez Jima.

I.3 Možné svety a logické dôsledky

- Tvrdenie rozdeľuje množinu **možných stavov sveta** na tie stavy, v ktorých je pravdivé (**modely**), a tie stavy, v ktorých je nepravdivé
- Teória môže mať viacero modelov (ale aj žiaden)

  Príklad 1.2. Vymenujme možné stavy prítomnosti Kim, Jima a Sarah na párty a zistime, v ktorých sú pravdivé jednotlivé tvrdenia našej teórie a celá teória.
- **Logickými dôsledkami** teórie sú tvrdenia, ktoré sú pravdivé vo *všetkých* modeloch teórie (svetoch, v ktorých je pravdivá)

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

I.4 Logické usudzovanie

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

Príklad 1.4. Vieme, že ak na párty pôjde Kim, tak nepôjde Sarah (P1), a že ak pôjde Jim, tak pôjde Kim (P2).
Predpokladajme, že na párty pôjde Jim.
Potom podľa (P2) pôjde aj Kim.
Potom podľa (P1) nepôjde Sarah.
Teda: Ak na párty pôjde Jim, nepôjde Sarah.

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

I.5 Usudzovacie pravidlá, korektnosť, dedukcia

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

Ak pôjde Jim, tak pôjde Kim.	Ak je dilítium dekryštalizované, tak antihmota neprúdi.
Pôjde Jim.	Dilítium je dekryštalizované.
Pôjde Kim.	Antihmota neprúdi.

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

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

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

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

- **Dedukcia** — usudzovanie iba pomocou korektných pravidiel

I.6 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 červené Fabie?

Abdukcia — odvodzovanie možných príčin z následkov:

Ak je batéria vybitá, auto nenaštartuje.
Ak je nádrž prázdna, auto nenaštartuje.
Nádrž nie je prázdna.
Auto nenaštartovalo.
___
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.7 Nededuktívne pravidlá

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

- **Prirodzený jazyk** je problematický — tvrdenia môžu byť viacznačné, ťažko zrozumiteľné, používať obraty a ustálené výrazy so špeciálnym významom
  - Mišo *je* myš.
  - Videl som dievča v sále *s ďalekohľadom*.
  - Vlastníci bytov a nebytových priestorov v dome prijímajú rozhodnutia na schôdzi vlastníkov dvojtretinovou väčšinou hlasov všetkých vlastníkov bytov a nebytových priestorov v dome, ak hlasujú o zmluve o úvere a o každom dodatku k nej, o zmluve o zabezpečení úveru a o každom dodatku k nej, o zmluve o nájme a kúpe veci, ktorú vlastníci bytov a nebytových priestorov v dome užívajú s právom jej kúpy po uplynutí dojednaného času užívania a o každom dodatku k nej, o zmluve o vstavbe alebo nadstavbe a o každom dodatku k nim, o zmene účelu užívania spoločných častí domu a spoločných zariadení domu a o zmene formy výkonu správy; ak sa rozhoduje o nadstavbe alebo o vstavbe v podkroví alebo povale, vyžaduje sa zároveň súhlas všetkých vlastníkov bytov a nebytových priestorov v dome na najvyššom poschodí. *— Zákon č. 182/1993 Z. z. SR v znení neskorších predpisov*
  - Nikto nie je dokonalý.
- Tieto ťažkosti sa obchádzajú použitím **formálneho** jazyka
  - Presne definovaná, zjednodušená syntax (pravidlá zápisu tvrdení)
    a sémantika (význam) — podobne ako programovací jazyk
- Problémy z reálneho sveta opísané v prirodzenom jazyku musíme najprv **formalizovať**, a potom naň môžeme použiť logický aparát

I.9 Formalizácia poznatkov

- S formalizáciou ste sa už stretli pri riešení slovných úloh

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

- Stretli ste sa už aj s formálnym jazykom výrokovej logiky

  Príklad 1.5. Sformalizujme náš párty príklad:

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

  P1: Sarah nepôjde na párty, ak pôjde Kim.

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

  P3: Sarah nepôjde bez Jima.

I.10 Kalkuly — formalizácia usudzovania

- Pre mnohé logiky sú známe **kalkuly** —
  množiny usudzovacích pravidiel, ktoré sú

  korektné — odvodzujú iba logické dôsledky

  úplné — umožňujú odvodiť všetky logické dôsledky

- Kalkuly existujú aj v iných častiach matematiky
  - na počítanie s číslami, zlomkami (aritmetický kalkul),
  - riešenie lineárnych rovníc (kalkul lineárnej algebry),
  - derivovanie, integrovanie, riešenie diferenciálnych rovníc (kalkul matematickej analýzy)

  ...

  Nie vždy sú úplné

I.11 Výpočtová logika — automatizácia usudzovania

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

I.12 Výpočtová logika — aplikácie

- Overovanie, dopĺňanie, hľadanie dôkazov matematických viet
- Špecifikácia a verifikácia hardvérových obvodov, programov, komunikačných protokolov

    - Špecifikácia a verifikácia programov (3. ročník)
    - Formálne metódy tvorby softvéru (magisterský)
- Logické programovanie
    - Programovacie paradigmy (3. ročník)
    - Výpočtová logika (magisterský)
    - Logické programovanie ASP (magisterský)
- Databázy — pohľady, integritné obmedzenia, optimalizácia dopytov
    - Deduktívne databázy (3. ročník)
- Sémantický web a integrácia dát z rôznych zdrojov
    - Reprezentácia znalostí a inferencia (magisterský)
    - Ontológie a znalostné inžinierstvo (magisterský)
- Analýza zákonov, regulácií, zmlúv

I.13

Spomeňte si I.1
Tvrdenie, ktoré je pravdivé vo všetkých svetoch, v ktorých je pravdivá teória, je jej

A. premisou,

B. logickým dôsledkom,

C. záverom,

D. implikáciou.

Spomeňte si I.2
Účelom dôkazu je presvedčiť ostatných o správnosti nášho úsudku. Preto musí pozostávať z ....

Spomeňte si I.3
Usudzovanie, pri ktorom používame iba také pravidlá, ktoré z pravdivých premís vždy odvodia pravdivé závery, sa nazýva:

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

1.2. O tomto kurze

I.14 Čím sa budeme zaoberať v tomto kurze

Teoreticky
- Jazykmi výrokovej a predikátovej logiky, ich syntaxou a sémantikou
- Korektnosťou usudzovacích pravidiel
- Korektnosťou a úplnosťou logických kalkulov
- Automatizovateľnými kalkulmi

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

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

I.15 Organizácia kurzu — rozvrh, kontakty, pravidlá

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

2. Výroková logika

2.1. Opakovanie: Výroková logika v prirodzenom jazyku

I.16 Opakovanie: Výroková logika v prirodzenom jazyku

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

Príklady 2.1.

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

Negatívne príklady

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

Výrokom priraďujeme *pravdivostné hodnoty*

I.17 Opakovanie: Výroková logika v prirodzenom jazyku

Operácie s výrokmi – *logické spojky*

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

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

Negatívny príklad
Spojku „pretože“ nepovažujeme za *logickú* spojku.

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

I.18 (Meta) matematika výrokovej logiky

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

2.2. Syntax výrokovej logiky

I.19 Syntax výrokovej logiky

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

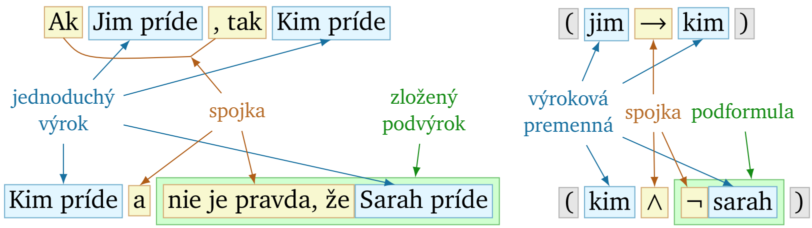
I.20 Syntax výrokovej logiky

Aké tvrdenia chceme zapisovať vo výrokovej logike?

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

  Ich formálnu verziu nazveme **výrokové premenné**

- Zložené výroky, tvorené podvýrokmi a spojkou:



  Ich formálnu verziu nazveme **formuly**

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

  Tieto základné prvky nazveme **symboly**

I.21 Symboly jazyka výrokovej logiky

Definícia 2.3. *Symbolmi jazyka výrokovej logiky* sú:

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

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

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

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

I.22 Symboly, výrokové premenné

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

Je o čosi všeobecnejší ako pojem znak.

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

Dohoda

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

Výrokové premenné formalizujú jednoduché výroky.

I.23 Výrokové formuly

- Povedzme, že máme množinu výrokových premenných $\mathcal{V} = \{\text{kim}, \text{jim}, \text{sarah}\}$
- Ako môžu vyzerať 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.
2. Opíšeme, ako sa z jednoduchších formúl skladajú zložitejšie.

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

i. každá výroková premenná $p \in \mathcal{V}$ je výrokovou formulou z $\mathcal{E}$ (hovoríme jej *atomická formula* alebo iba *atóm*);

ii. ak A je výroková formula z $\mathcal{E}$, tak aj postupnosť symbolov $\neg A$ je výrokovou formulou z $\mathcal{E}$ (*negácia* formuly A);

iii. ak A a B sú výrokové formuly z $\mathcal{E}$, tak aj $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$ sú výrokovými formulami z $\mathcal{E}$ (*konjunkcia*, *disjunkcia*, *implikácia* formúl A a B).

Dohoda

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

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

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

$$
\begin{aligned}
\mathcal{E} = \{&\text{kim}, \text{jim}, \text{sarah}, && \text{podľa (i)}\\
&\neg\text{kim}, \neg\text{jim}, \neg\text{sarah}, && \text{podľa (ii)}\\
&(\text{kim} \land \text{kim}), (\text{kim} \land \text{jim}), (\text{kim} \land \text{sarah}), && \text{podľa (iii) pre } \land\\
&(\text{kim} \land \neg\text{kim}), (\text{kim} \land \neg\text{jim}), (\text{kim} \land \neg\text{sarah}), &&\\
&(\text{jim} \land \text{kim}), (\text{jim} \land \text{jim}), (\text{jim} \land \text{sarah}), &&\\
&(\text{jim} \land \neg\text{kim}), (\text{jim} \land \neg\text{jim}), (\text{jim} \land \neg\text{sarah}), &&\\
&(\neg\text{kim} \land \text{kim}), (\neg\text{kim} \land \text{jim}), (\neg\text{kim} \land \text{sarah}), \dots, &&\\
&(\neg\text{jim} \land \neg\text{sarah}), \dots, && \text{podľa (iii) pre } \to\\
&(\text{sarah} \lor (\text{kim} \to \text{jim})), \dots, && \text{a potom pre } \lor\\
&(\neg(\text{kim} \land \text{sarah}) \lor (\neg\text{jim} \to \neg\text{sarah})), \dots\} && \text{podľa (iii) pre } \land, \to, \lor
\end{aligned}
$$

I.26 Vytvárajúca postupnosť

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

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

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

I.27 Vytvárajúca postupnosť

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

II. prednáška

Sémantika výrokovej logiky

26. februára 2018

II.1

Spomeňte si II.1

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

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

B. $(p \land \neg(q \to r))$,

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

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 $((A \to B) \land (B \to A))$.

II.3 Jednoznačnosť rozkladu formúl výrokovej logiky

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

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

  i. každá výroková premenná $p \in \mathcal{V}$ je „formulou" z $\mathcal{E}$;

  ii. ak A je „formula" z $\mathcal{E}$, tak aj postupnosť symbolov $\neg A$ je „formulou" z $\mathcal{E}$;

  iii. ak A a B sú „formuly" z $\mathcal{E}$, tak aj $A \land B$, $A \lor B$ a $A \to B$ 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 $(jim \to kim \to \neg sarah)$ „formulou“?
- Aký by bol jej význam?

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

  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 $b \in \{\land, \lor, \to\}$ také, že $X = (A\ b\ B)$.*

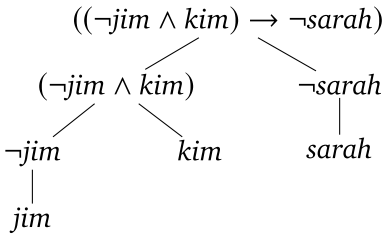
II.5 Vytvárajúca postupnosť a vytvárajúci strom

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

  $jim, sarah, \neg jim, kim, \neg sarah, (\neg jim \land kim), ((\neg jim \land kim) \to \neg sarah)$

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

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



- Takéto stromy voláme vytvárajúce.

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

II.6 Vytvárajúci strom formuly

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

- v koreni T je formula X,

- ak vrchol obsahuje formulu $\neg A$, tak má práve jedno dieťa, ktoré obsahuje formulu A,

- ak vrchol obsahuje formulu $(A \; b \; B)$, kde b je jedna z binárnych spojok, tak má dve deti, pričom ľavé dieťa obsahuje formulu A a pravé formulu B,

- vrcholy obsahujúce výrokové premenné sú listami.

II.7 Podformuly

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

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

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

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

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

- Ako tieto pojmy presne zadefinujeme?

II.8 Podformuly

Definícia 2.13 (Priama podformula)**.**

- Priamou podformulou $\neg A$ je formula A.
- Priamymi podformulami $(A \land B)$, $(A \lor B)$ 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.9 Meranie zložitosti formúl

- Zložitosť formúl by sa mohla merať napríklad jej dĺžkou (počtom symbolov)
- Prirodzenejšie je ale merať zložitosť počtom netriviálnych krokov potrebných na konštrukciu formuly:

- pridanie negácie pred formulu,
- spojenie formúl spojkou

- Tejto miere hovoríme *stupeň formuly*

  Príklad 2.15. Aký je stupeň formuly $((p \lor \neg q) \land \neg(q \to p))$?

- Ako stupeň zadefinujeme?

  Induktívne, podobne ako sme zadefinovali formuly:

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

II.10 Stupeň formuly

Definícia 2.16 (Stupeň formuly)**.**

- Výroková premenná je stupňa 0.
- Ak A je formula stupňa n, tak $\neg A$ je stupňa $n + 1$.
- Ak A je formula stupňa n_1 a B je formula stupňa n_2, tak $(A \land B)$, $(A \lor B)$ a $(A \to B)$ 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:

- $\deg(p) = 0$,
- $\deg(\neg A) = \deg(A) + 1$,
- $\deg((A \land B)) = \deg((A \lor B)) = \deg((A \to B)) = \deg(A) + \deg(B) + 1$.

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

báza indukcie: *každá formula stupňa* 0 *má vlastnosť P,*

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

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

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

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

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

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

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 $((p \lor \neg q) \land \neg(q \to p))$ jej:

i. priame podformuly,

ii. podformuly,

iii. vytvárajúci strom.

Spomeňte si II.4
Stupeň formuly $((\neg p \leftrightarrow q) \land q)$ je ....
$\mathrm{vars}(((\neg p \leftrightarrow q) \land q)) =$ ....

2.3. Sémantika výrokovej logiky

II.14 Sémantika výrokovej logiky

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

II.15 Ohodnotenie výrokových premenných

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

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

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

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

II.16 Ohodnotenie výrokových premenných

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

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

$$v_1(\text{svieti\_slnko}) = t \qquad v_1(\text{zobral\_som\_si\_čiapku}) = f$$

Pondelkové ráno pred týždňom opisuje ohodnotenie v_2, kde okrem iného

$$v_2(\text{svieti\_slnko}) = f \qquad v_2(\text{zobral\_som\_si\_čiapku}) = f$$

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

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

Prečo „okrem iného“?

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

II.17 Spĺňanie výrokových formúl

- Na formulu sa dá pozerať ako na **podmienku**,
  ktorú stav sveta buď **spĺňa** (je v tomto stave pravdivá)
  alebo **nespĺňa** (je v ňom nepravdivá).

- Z pravdivostného ohodnotenia výrokových premenných v nejakom stave sveta, vieme *jednoznačne* povedať,
  ktoré formuly sú v tomto stave splnené.

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

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

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

Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

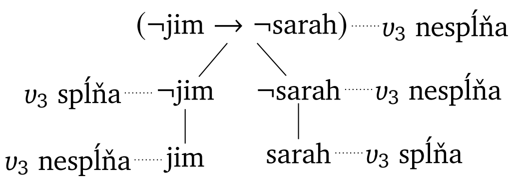
Formulu	jim	sarah	¬jim	¬sarah	(¬jim → ¬sarah)
ohodnotenie v_3	nespĺňa	spĺňa	spĺňa	nespĺňa	nespĺňa

II.18 Spĺňanie výrokových formúl — vytvárajúci strom

Príklad 2.21 (pokračovanie).

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

Iná možnosť je použiť vytvárajúci strom:



II.19 Spĺňanie výrokových formúl — program

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

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

- Veľmi podobne vieme zadefinovať 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 $(A \land B)$ vtt v spĺňa A a v spĺňa B;
- v spĺňa formulu $(A \lor B)$ vtt v spĺňa A alebo v spĺňa B;
- v spĺňa formulu $(A \to B)$ vtt v nespĺňa A alebo v spĺňa B.

Dohoda

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

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

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

Zistime, ktoré z formúl

$$((\mathrm{kim} \lor \mathrm{jim}) \lor \mathrm{sarah})$$
$$(\mathrm{kim} \to \neg\mathrm{sarah}) \qquad (\mathrm{jim} \to \mathrm{kim}) \qquad (\neg\mathrm{jim} \to \neg\mathrm{sarah})$$

ohodnotenie v_3 spĺňa a ktoré nespĺňa.

$\deg(X)$	v_3 spĺňa X	v_3 nespĺňa X
0	kim, sarah	jim
1	¬jim, (kim ∨ jim), (jim → kim)	¬sarah
2	((kim ∨ jim) ∨ sarah)	(kim → ¬sarah)
3		(¬jim → ¬sarah)

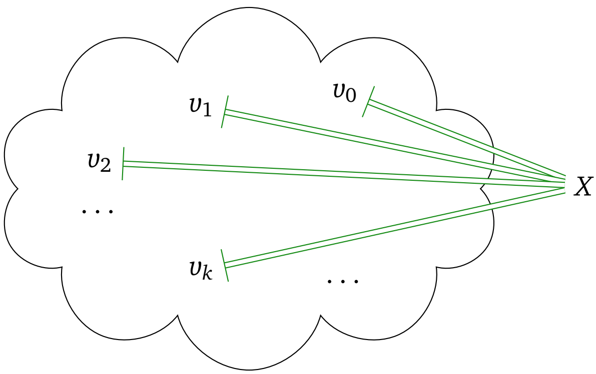
2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť

II.22 Spĺňanie z hľadiska formuly

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

Dohoda
V ďalších definíciách a tvrdeniach predpokladáme, že sme si *pevne zvolili* nejakú množinu výrokových premenných $\mathcal{V}$ a hodnoty t, f.
Formulou rozumieme formulu nad množinou výrok. prem. $\mathcal{V}$.
Ohodnotením rozumieme ohodnotenie množiny výrok. prem. $\mathcal{V}$.

II.23 Tautológia



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

II.24 Tautológia — testovanie

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

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

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

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

II.25 Tautológia — testovanie

Príklad 2.26. Zistime, či je $X = (\neg(p \land q) \to (\neg p \lor \neg q))$ tautológiou.

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

v							
p	q	$(p \land q)$	$\neg(p \land q)$	$\neg p$	$\neg q$	$(\neg p \lor \neg q)$	$(\neg(p \land q) \to (\neg p \lor \neg q))$
f	f	$\not\models$	$\models$	$\models$	$\models$	$\models$	$\models$
t	f	$\not\models$	$\models$	$\not\models$	$\models$	$\models$	$\models$
f	t	$\not\models$	$\models$	$\models$	$\not\models$	$\models$	$\models$
t	t	$\models$	$\not\models$	$\not\models$	$\not\models$	$\not\models$	$\models$

Pretože všetky skúmané ohodnotenia spĺňajú X, je X tautológiou.

II.26 Ohodnotenia zhodujúce sa na premenných formuly

Dôkaz. Indukciou na stupeň formuly X.

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

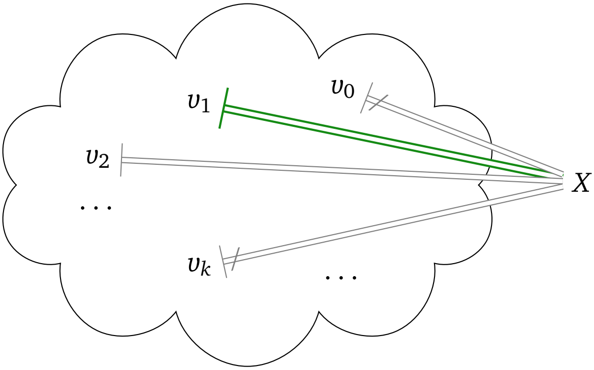
Krok: Nech X je stupňa $n > 0$ a tvrdenie platí pre všetky formuly stupňa nižšieho ako n (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na premenných v X. Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

- $X = \neg A$ pre práve jednu formulu A. Pretože $\deg(X) = \deg(A) + 1 > \deg(A)$, podľa ind. predpokladu tvrdenie platí pre A. Ohodnotenia v_1 a v_2 sa zhodujú na premenných v A (rovnaké ako v X). Preto $v_1 \models A$ vtt $v_2 \models A$, a teda $v_1 \models \neg A$ vtt $v_1 \not\models A$ vtt $v_2 \not\models A$ vtt $v_2 \models \neg A$.

- $X = (A \land B)$ pre práve jednu dvojicu formúl A, B. Pretože $\deg(X) = \deg(A) + \deg(B) + 1 > \deg(A)$ aj $\deg(B)$, podľa ind. predpokladu pre A aj B tvrdenie platí. Podobne pre ďalšie binárne spojky.

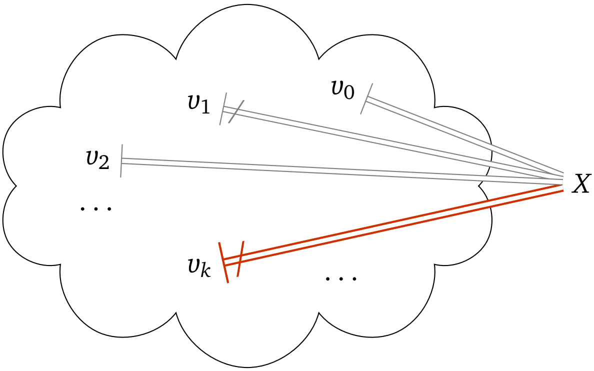
□

II.27 Splniteľnosť



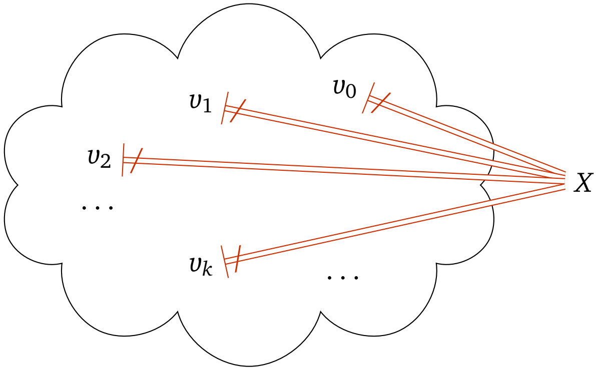
Definícia 2.27. Formulu X nazveme *splniteľnou*
vtt **nejaké** ohodnotenie výrokových premenných **spĺňa** X
(teda **existuje** také ohodnotenie výrokových premenných v, že $v \models X$).

II.28 Falzifikovateľnosť



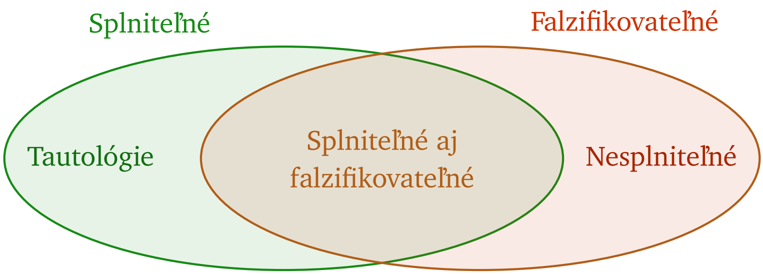
Definícia 2.28. Formulu X nazveme *falzifikovateľnou*
vtt **nejaké** ohodnotenie výrokových premenných **nespĺňa** X
(teda **existuje** také ohodnotenie výrokových premenných v, že $v \not\models X$).

II.29 Nesplniteľnosť



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

II.30 „Geografia" výrokových formúl podľa spĺňania



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

Obrázok podľa [Papadimitriou, 1994]

Zamyslite sa II.5
Ak formula *nie* je falzifikovateľná, je:

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

III. prednáška

Vyplývanie, ekvivalentné úpravy

5. marca 2018

III.1 Tautológie a (ne)splniteľnosť

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

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

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

III.2 Teórie

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

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

Dohoda

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

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

$$\begin{aligned} T_{\text{party}} = \{\, &((\text{kim} \lor \text{jim}) \lor \text{sara}), && (\text{kim} \to \neg\text{sara}), \\ &(\text{jim} \to \text{kim}), && (\neg\text{jim} \to \neg\text{sara}) \,\} \end{aligned}$$

III.3 Splnenie teórie, model

Pojem spĺňania sa jednoducho rozšíri na teórie.

Definícia 2.33. Nech T je teória. Ohodnotenie v *spĺňa teóriu* T (skrátene $v \models T$) vtt v spĺňa každú formulu X z množiny T.

Spĺňajúce ohodnotenie nazývame *modelom* teórie T.

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

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

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

2.5. Výrokovologické vyplývanie

III.4 Splniteľnosť teórie

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

Definícia 2.36. 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.

III.5 Logické dôsledky a vyplývanie

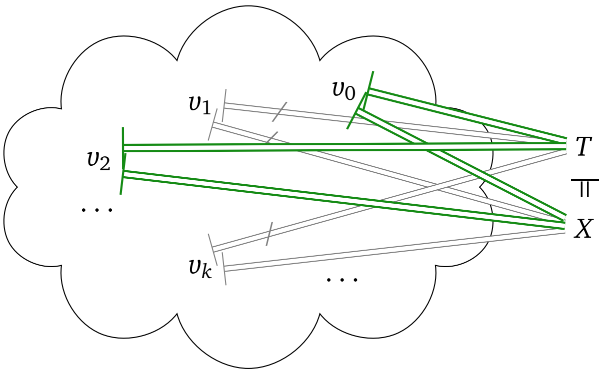
- Aký je *účel* teórií? Kedy je teória užitočná?
  - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) *doteraz neznáme skutočnosti* (teda nezapísané v teórii),
    ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

- 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*.

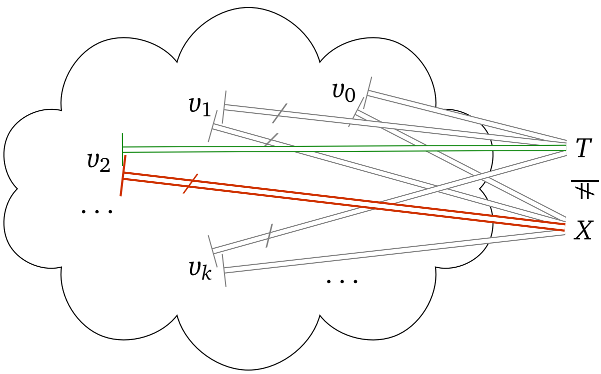
Ktorá ďalšia formula vyplýva z T_{party}?

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 Nevyplývanie



Príklad 2.40. Ktoré atomické formuly a ich negácie nevyplývajú z T_{party}?
Vyplýva z T_{party} formula $(kim \longrightarrow jim)$?

III.8 Vyplývanie a (ne)splniteľnosť

Použitie SAT solvera na rozhodovanie vyplývania je založené na:

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

Dôkaz. Nech $T = \{X_1, X_2, \ldots, X_n, \ldots\}$.
($\Rightarrow$) Predpokladajme, že X vyplýva z množiny T. Nech v je nejaké ohodnotenie $\mathcal{V}$. Potrebujeme ukázať, že v nespĺňa T_1. Máme dve možnosti:

- Ak v nespĺňa T, tak nespĺňa ani T_1.
- Ak v spĺňa T, tak v musí spĺňať aj X (definícia vyplývania). To znamená, že $\neg X$ je nesplnená pri v, a teda v nespĺňa T_1.

($\Leftarrow$) Opačne, nech T_1 je nesplniteľná a nech v je nejaké ohodnotenie $\mathcal{V}$. v teda nespĺňa T_1. Potrebujeme ukázať, že ak v spĺňa T, tak potom v spĺňa aj X. Ak v spĺňa T, potom spĺňa každé X_i. Keďže ale v nespĺňa T_1, v musí nespĺňať $\neg X$ (jediná zostávajúca formula z T_1), čo znamená, že v spĺňa X. □

III.9 Nezávislosť

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

Príklad 2.43. Ktorá atomická formula je nezávislá od T_{party}?
Je aj jej negácia nezávislá od T_{party}?

III.10 Vzťahy vyplývania, implikácií a tautológií

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

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

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

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

c) Nasledujúce tvrdenia sú ekvivalentné:

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

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

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

iv. $\models (((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n) \to B)$

III.11 Hlasujte

Spomeňte si III.1
Formula X vyplýva z teórie T vtt každý model T spĺňa X.
Pravda alebo nepravda?

2.6. Ekvivalencia formúl

III.12 Ekvivalencia formúl

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

Definícia 2.46. Dve formuly X a Y sú *(výrokovologicky) ekvivalentné* ($X \Leftrightarrow Y$) vtt
pre každé ohodnotenie v výrokových premenných platí,
že v spĺňa X vtt v spĺňa Y.

Ako súvisí takto sémanticky zadefinovaná ekvivalencia formúl so skratkou $\leftrightarrow$?

Podľa dohody z 2. prednášky je $(X \leftrightarrow Y)$ je skráteným zápisom $((X \to Y) \wedge (Y \to X))$.

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

III.13 Ekvivalencia a vyplývanie

Ako súvisí ekvivalencia formúl s vyplývaním?

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

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

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

Dôkaz $\{Y\} \models X$ je podobný.

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

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

III.14 Tranzitivita ekvivalencie

Tvrdenie 2.49 (Tranzitivita ekvivalencie)**.** *Nech X, Y a Z sú formuly.*
Ak X je ekvivalentná s Y a Y je ekvivalentná so Z,
tak X je ekvivalentná so Z.

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

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

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

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

2.6.1. Ekvivalentné úpravy

III.15 Ekvivalentné úpravy

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

Príklad 2.50.

$$A = \neg\neg(r \land q) \qquad B = (r \land q) \qquad X = (p \to \neg\, \neg\neg(r \land q)\,)$$

$$\rightsquigarrow$$

$$Y = (p \to \neg\,(r \land q)\,)$$

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

III.16 Pravidlá ekvivalentných úprav

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

Príklad 2.51. $C = \neg\neg\, p \qquad D = p$

$$\rightsquigarrow \qquad \rightsquigarrow$$

$$A = \neg\neg\,(r \land q) \qquad B = (r \land q)$$

III.17 Korektnosť ekvivalentných úprav

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

III.18 Substitúcia a ekvivalentné úpravy

Oba druhy dosadení pri ekvivalentných úpravách sú *substitúcie*

Definícia 2.52 (Substitúcia)**.** Nech X, A, B sú formuly. *Substitúciou* B za A v X (skrátene $X[A|B]$)) nazývame formulu, ktorá vznikne nahradením každého výskytu A v X formulou B.

Substitúciu si vieme predstaviť ako cyklus prechádzajúci cez X

nech ℓ je dĺžka A
kým nie si na konci X:
  ak sa nasledujúcich ℓ symbolov zhoduje s A:
    nahraď ich za B
    pokračuj za posledným nahradeným symbolom
  inak:
    pokračuj ďalším symbolom

alebo ako rekurzívne definovanú operáciu: (cv02)

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

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

III.19 Korektnosť ekvivalentných úprav

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.

III.20 Sémantické vlastnosti substitúcie

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.

III.21 Ekvivalencie pre ekvivalentné úpravy

Veta 2.56. *Nech A, B a C sú ľubovoľné formuly, $\top$ je ľubovoľná tautológia a $\bot$ je ľubovoľná nesplniteľná formula.*
Nasledujúce dvojice formúl sú ekvivalentné:

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

III.22 Ekvivalencie pre ekvivalentné úpravy

Veta 2.56 (Pokračovanie)**.**

$(A \land A)$ a A $(A \lor A)$ a A	idempotencia
$(A \land \top)$ a A $(A \lor \bot)$ a A	identita
$(A \lor (A \land B))$ a A $(A \land (A \lor B))$ a A	absorpcia
$(A \lor \neg A)$ a $\top$ $(A \land \neg A)$ a $\bot$	vylúčenie tretieho spor
$(A \to B)$ a $(\neg A \lor B)$	nahradenie $\to$

2.6.2. Konjunktívna a disjunktívna normálna forma

III.23 Konjunkcia a disjunkcia postupnosti formúl

Dohoda

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

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

III.24 Konjunktívny a disjunktívny normálny tvar

Definícia 2.57.

Literál je výroková premenná
alebo negácia výrokovej premennej.

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

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

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

III.25 Konjunktívny a disjunktívny normálny tvar

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

$$\begin{aligned}
A_1 &= p & A_6 &= ((p \land \neg q) \lor (\neg p \land r) \lor (\neg p \land q \land \neg r)) \\
A_2 &= \neg q & A_7 &= ((\neg p \lor q \lor \neg r) \land (q \to r)) \\
A_3 &= \square & A_8 &= ((\neg p \lor \neg q) \land (p \lor r) \land (p \lor q \lor \neg r)) \\
A_4 &= (p \lor \neg q) & A_9 &= ((\neg p \lor (p \land r)) \land (p \lor q \lor \neg r)) \\
A_5 &= (p \land \neg q) & A_{10} &= ((\neg p \lor p \lor r) \land (\neg(p \lor q) \lor \neg r))
\end{aligned}$$

IV. prednáška

CNF

Tablový kalkul

12. marca 2018

IV.1 Existencia DNF a CNF

Veta 2.59.

1. *Ku každej formule X existuje ekvivalentná formula D v disjunktívnom normálnom tvare.*
2. *Ku každej formule X existuje ekvivalentná formula C v konjunktívnom normálnom tvare.*

Dôkaz.

1. Zoberme všetky ohodnotenia $v_1, \dots, v_n$ také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné $q \notin \mathrm{vars}(X)$. 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 $p \in \mathrm{vars}(X)$. Očividne formula $D = \bigvee_{1 \leq i \leq n} C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).
2. K $\neg X$ teda existuje ekvivalentná formula D v DNF. Znegovaním D a aplikáciou de Morganových pravidiel dostaneme formulu C v CNF, ktorá je ekvivalentná s X. □

IV.2 CNF — trochu lepší prístup

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

- Všimnime si:

  CNF je konjunkcia disjunkcií literálov — výrokových premenných alebo ich negácií

  Teda:

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

IV.3 CNF — trochu lepší prístup

Algoritmus CNF$_1$

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

Tvrdenie 2.60. *Výsledná formula alg. CNF$_1$ je ekvivalentná s pôvodnou a je v CNF.*

Príklad 2.61.

1. $((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$
2. $(\neg(a \lor \neg b) \lor \neg(c \lor (d \land \neg e)))$ [1 — nahradenie implikácie]
3. $((\neg a \land \neg\neg b) \lor \neg(c \lor (d \land \neg e)))$ [2 — deMorganovo pravidlo]
4. $((\neg a \land b) \lor \neg(c \lor (d \land \neg e)))$ [2 — dvojitá implikácia]
5. $((\neg a \land b) \lor (\neg c \land \neg(d \land \neg e)))$ [2 — deMorganovo pravidlo]
6. $((\neg a \land b) \lor (\neg c \land (\neg d \lor \neg\neg e)))$ [2 — deMorganovo pravidlo]
7. $((\neg a \land b) \lor (\neg c \land (\neg d \lor e)))$ [2 — dvojitá implikácia]
8. $(((\neg a \land b) \lor \neg c) \land ((\neg a \land b) \lor (\neg d \lor e)))$ [3 — distributívnosť]
9. $(((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e))))$ [3]
10. $((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e)))$ [4]
11. $((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$ [4 — asoc.]

Distribúcia $\lor$ cez $\land$ spôsobuje nárast formuly:

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

IV.6 CNF — obmedzenie exponenciálneho rastu

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

1. Zoberme *nové* výrokové premenné $r_1, \ldots, r_n, s$
2. Vyjadrime, že r_i je ekvivalentným zástupcom konjunkcie $(p_i \land q_i)$: $(r_i \leftrightarrow (p_i \land q_i))$
3. Použime r_i na vyjadrenie, že s je ekvivalentným zástupcom disjunkcie A_n: $(s \leftrightarrow (r_1 \lor \cdots \lor r_n))$
4. A_n teda môžeme nahradiť formulou $((s \leftrightarrow (r_1 \lor \cdots \lor r_n)) \land (r_1 \leftrightarrow (p_1 \land q_1)) \land \cdots \land (r_n \leftrightarrow (p_n \land q_n)) \land s)$

Ekvivalentnými úpravami

- prvý konjunkt upravíme na $n + 1$ klauzúl,
- ďalších n na 3 klauzuly každý

spolu iba $4 \cdot n + 2$ klauzúl!

IV.7 CNF — Cejtinova transformácia

Cejtinova transformácia (angl. Tseytin transformation)

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

2.7. Kalkuly

IV.8 Dokazovanie ekvivalencie syntakticky vs. sémanticky

- Pomocou substitúcie ekvivalentných formúl vieme dokázať, že dve formuly sú ekvivalentné bez toho, aby sme vyšetrovali všetky ohodnotenia ich výrokových premenných.
- Výhodné pri formulách s veľkým počtom premenných.

- Formulu $X = ((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$ sme upravili do CNF $Y = ((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$ pomocou 12 substitúcií ekvivalentných podformúl.
- Zároveň sme dokázali, že X a Y sú ekvivalentné.
- Na dôkaz ich ekvivalencie tabuľkovou metódou by sme potrebovali vyšetriť 32 prípadov.

IV.9 Ekvivalencia syntakticky vs. sémanticky

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

IV.10 Kalkuly — dokazovanie vyplývania syntakticky

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

- Ukážeme si dva kalkuly:

  tablový — stromový, prirodzenejší

  rezolvenciu — lineárny, strojový

2.8. Tablový kalkul

IV.11 Dôkaz vyplývania sporom v slovenčine

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

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

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

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

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

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

IV.12 Tablová notácia pre dôkazy

Dôkaz stručne zapíšeme v tablovej notácii:

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

- Ak z niektorého faktu o formule X **vyplýva** o jej *priamych podformulách* fakt F_1 **alebo** fakt F_2, **rozdelíme** úvahu na dve nezávislé vetvy, pričom prvá začne faktom F_1 a druhá faktom F_2. K obom si poznačíme písmeno β a číslo zdrojového faktu.

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

IV.13 Dôkaz vyplývania sporom v tablovej notácii

Príklad 2.63.

<table>
<tr><td>(1)</td><td colspan="8">$\mathbf{T}(kim \to (jim \land \neg sarah))$</td><td>z T'_{party}</td></tr>
<tr><td>(2)</td><td colspan="8">$\mathbf{T}(eva \to kim)$</td><td>z T'_{party}</td></tr>
<tr><td>(3)</td><td colspan="8">$\mathbf{F}(sarah \to \neg eva)$</td><td>dôkaz sporom</td></tr>
<tr><td>(4)</td><td colspan="8">$\mathbf{T}\, sarah$</td><td>$\alpha(3)$</td></tr>
<tr><td>(5)</td><td colspan="8">$\mathbf{F}\, \neg eva$</td><td>$\alpha(3)$</td></tr>
<tr><td>(6)</td><td colspan="8">$\mathbf{T}\, eva$</td><td>$\alpha(5)$</td></tr>
<tr><td>(7)</td><td>$\mathbf{F}\, eva$</td><td>$\beta(2)$</td><td>(8)</td><td colspan="5">$\mathbf{T}\, kim$</td><td>$\beta(2)$</td></tr>
<tr><td></td><td>$*$</td><td>(6) a (7)</td><td>(9)</td><td>$\mathbf{F}\, kim$</td><td>$\beta(1)$</td><td>(10)</td><td colspan="2">$\mathbf{T}(jim \land \neg sarah)$</td><td>$\beta(1)$</td></tr>
<tr><td></td><td></td><td></td><td></td><td>$*$</td><td>(8) a (9)</td><td>(11)</td><td colspan="2">$\mathbf{T}\, jim$</td><td>$\alpha(10)$</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>(12)</td><td colspan="2">$\mathbf{T}\, \neg sarah$</td><td>$\alpha(10)$</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>(13)</td><td colspan="2">$\mathbf{F}\, sarah$</td><td>$\alpha(12)$</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">$*$</td><td>(4) a (13)</td></tr>
</table>

IV.14 Spĺňanie a priame podformuly

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

1. *T) Ak v spĺňa $\neg X$, tak v nespĺňa X.*

   F) Ak v nespĺňa $\neg X$, tak v spĺňa X.

2. *T) Ak v spĺňa $(X \land Y)$, tak v spĺňa X a v spĺňa Y.*

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

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

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

4. *T) Ak v splĺňa $(X \to Y)$, tak v nesplĺňa X alebo v splĺňa Y.*

   F) Ak v nesplĺňa $(X \to Y)$, tak v splĺňa X a v nesplĺňa Y.

IV.15 Označené formuly a ich sémantika

Definícia 2.65. Nech X je formula výrokovej logiky.
Postupnosti symbolov $\mathbf{T}X$ a $\mathbf{F}X$ nazývame *označené formuly*.

Definícia 2.66. Nech v je ohodnotenie výrokových premenných a X je formula. Potom

- *v splĺňa* $\mathbf{T}X$ vtt v splĺňa X;
- *v splĺňa* $\mathbf{F}X$ vtt v nesplĺňa X.

Dohoda

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

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

IV.16 Tablové pravidlá

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

$$
\begin{array}{c}
\alpha \\ \hline
\alpha_1 \\
\alpha_2
\end{array}
\qquad\qquad
\begin{array}{c|c}
\multicolumn{2}{c}{\beta} \\ \hline
\beta_1 & \beta_2
\end{array}
$$

$$
\begin{array}{c}
\mathbf{T}(X \land Y) \\ \hline
\mathbf{T}\,X \\
\mathbf{T}\,Y
\end{array}
\qquad\qquad
\begin{array}{c|c}
\multicolumn{2}{c}{\mathbf{F}(X \land Y)} \\ \hline
\mathbf{F}\,X & \mathbf{F}\,Y
\end{array}
\qquad\qquad
\begin{array}{c}
\mathbf{T}\,\neg X \\ \hline
\mathbf{F}\,X
\end{array}
$$

$$
\begin{array}{c}
\mathbf{F}(X \lor Y) \\ \hline
\mathbf{F}\,X \\
\mathbf{F}\,Y
\end{array}
\qquad\qquad
\begin{array}{c|c}
\multicolumn{2}{c}{\mathbf{T}(X \lor Y)} \\ \hline
\mathbf{T}\,X & \mathbf{T}\,Y
\end{array}
\qquad\qquad
\begin{array}{c}
\mathbf{F}\,\neg X \\ \hline
\mathbf{T}\,X
\end{array}
$$

$$
\begin{array}{c}
\mathbf{F}(X \to Y) \\ \hline
\mathbf{T}\,X \\
\mathbf{F}\,Y
\end{array}
\qquad\qquad
\begin{array}{c|c}
\multicolumn{2}{c}{\mathbf{T}(X \to Y)} \\ \hline
\mathbf{F}\,X & \mathbf{T}\,Y
\end{array}
$$

IV.17 Jednotný zápis označených formúl typu α

Definícia 2.67 (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
$\mathbf{T}(X \land Y)$	$\mathbf{T}\,X$	$\mathbf{T}\,Y$
$\mathbf{F}(X \lor Y)$	$\mathbf{F}\,X$	$\mathbf{F}\,Y$
$\mathbf{F}(X \to Y)$	$\mathbf{T}\,X$	$\mathbf{F}\,Y$
$\mathbf{T}\,\neg X$	$\mathbf{F}\,X$	$\mathbf{F}\,X$
$\mathbf{F}\,\neg X$	$\mathbf{T}\,X$	$\mathbf{T}\,X$

Pozorovanie 2.68 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie výrokových premenných.*
Potom v spĺňa α vtt v spĺňa α_1 a v spĺňa α_2.

IV.18 Jednotný zápis označených formúl typu β

Definícia 2.69 (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
$\mathbf{F}(X \land Y)$	$\mathbf{F}X$	$\mathbf{F}Y$
$\mathbf{T}(X \lor Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
$\mathbf{T}(X \to Y)$	$\mathbf{F}X$	$\mathbf{T}Y$

Pozorovanie 2.70 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie výrokových premenných.*
Potom v splĺňa β vtt v splĺňa β_1 alebo v splĺňa β_2.

IV.19 Tablo pre množinu označených formúl

Definícia 2.71. *Analytické tablo pre množinu označených formúl S^+* (skrátene *tablo pre S^+*) je binárny strom, ktorého vrcholy obsahujú označené formuly
a ktorý je skonštruovaný podľa nasledovných rekurzívnych pravidiel:

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

  A: Ak sa na vetve π_y (ceste z koreňa do y) vyskytuje nejaká označená formula α, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci α_1 alebo α_2.

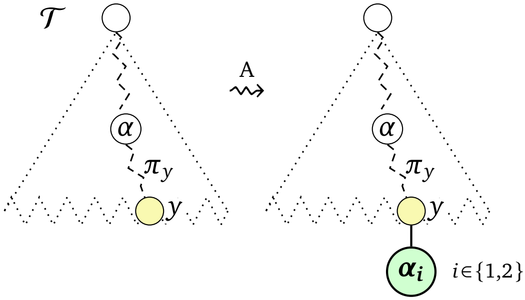
  B: Ak sa na vetve π_y vyskytuje nejaká označená formula β, tak ako deti y pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2.

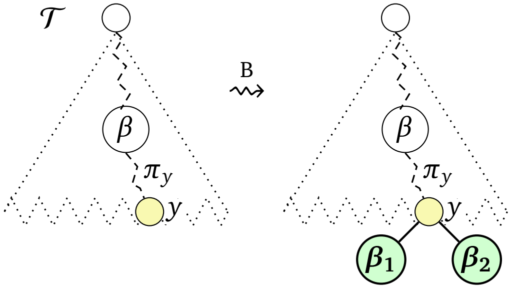
  S^+: Ako jediné dieťa y pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

Nič iné nie je tablom pre S^+.

IV.20 Tablá, tablové pravidlá, operácie rozšírenia

Operácia priameho rozšírenia





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

Pravidlá a označené formuly v nich

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\alpha_2}$$

α	α_1	α_2
$\mathbf{T}(X \land Y)$	$\mathbf{T}\,X$	$\mathbf{T}\,Y$
$\mathbf{F}(X \lor Y)$	$\mathbf{F}\,X$	$\mathbf{F}\,Y$
$\mathbf{F}(X \to Y)$	$\mathbf{T}\,X$	$\mathbf{F}\,Y$
$\mathbf{T}\,\neg X$	$\mathbf{F}\,X$	$\mathbf{F}\,X$
$\mathbf{F}\,\neg X$	$\mathbf{T}\,X$	$\mathbf{T}\,X$

$$\frac{\beta}{\beta_1 \mid \beta_2}$$

β	β_1	β_2
$\mathbf{F}(X \land Y)$	$\mathbf{F}\,X$	$\mathbf{F}\,Y$
$\mathbf{T}(X \lor Y)$	$\mathbf{T}\,X$	$\mathbf{T}\,Y$
$\mathbf{T}(X \to Y)$	$\mathbf{F}\,X$	$\mathbf{T}\,Y$

IV.21 Uzavretosť a otvorenosť vetvy a tabla

Definícia 2.72. *Vetvou* tabla $\mathcal{T}$ je každá cesta od koreňa $\mathcal{T}$ k niektorému listu $\mathcal{T}$.

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

Definícia 2.73. *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.

2.8.1. Korektnosť

IV.22 Korektnosť tablového kalkulu

Korektnosť (angl. *soundness*) kalkulu neformálne:
Ak v kalkule dokážeme nejaké tvrdenie, tak to tvrdenie je naozaj pravdivé.

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

Dôsledok 2.75. *Nech S je množina formúl a X je formula.*
Ak existuje uzavreté tablo pre $\{\mathbf{T}\, A \mid A \in S\} \cup \{\mathbf{F}\, X\}$ (skr. $S \vdash X$),
tak z S vyplýva X ($S \vDash X$).

Dôsledok 2.76. *Nech X je formula.*
Ak existuje uzavreté tablo pre $\{\mathbf{F}\, X\}$ (skr. $\vdash X$), tak X je tautológia ($\vDash X$).

V. prednáška

Korektnosť a úplnosť tablového kalkulu

19. marca 2018

V.1 Korektnosť — splnenie priameho rozšírenia tabla

Na dôkaz korektnosti potrebujeme pomocnú definíciu a dve lemy.

Definícia 2.77. Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a nech v je ohodnotenie množiny výrokových premenných. Potom:

- *v spĺňa vetvu 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 2.78 (K1)**.** *Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+*
a nech v je ohodnotenie množiny výrokových premenných.
Ak v spĺňa S^+ a v spĺňa $\mathcal{T}$, tak v spĺňa aj každé priame rozšírenie $\mathcal{T}$.

V.2 Korektnosť — splnenie priameho rozšírenia tabla

Dôkaz lemy K1. Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie množiny výrokových premenných. Nech $v \models S^+$. Nech v spĺňa $\mathcal{T}$ a v ňom vetvu π. Nech $\mathcal{T}_1$ je rozšírenie $\mathcal{T}$. Nastáva jeden z prípadov:

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ operáciou A, pridaním nového dieťaťa z nejakému listu y v $\mathcal{T}$, pričom 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 $\mathcal{T}$ operáciou B, 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 $\mathcal{T}$ operáciou Ax, pridaním nového dieťaťa z nejakému listu y v $\mathcal{T}$, pričom z obsahuje formulu $X^+ \in S^+$. Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π a teda je splnené.
  Ak $\pi = \pi_y$, tak v spĺňa vetvu π_z v table $\mathcal{T}_1$, pretože je rozšírením splnenej vetvy π o vrchol z obsahujúci splnenú formulu X (pretože $v \models S^+$). Preto v spĺňa tablo $\mathcal{T}_1$. □

V.3 Korektnosť — splnenie množiny a tabla pre ňu

Lema 2.79 (K2)**.** *Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+*
a nech v je ohodnotenie.
Ak v spĺňa S^+, tak v spĺňa $\mathcal{T}$.

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

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

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

V.4 Korektnosť — dôkaz

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

Sporom: Predpokladajme, že existuje ohodnotenie, ktoré spĺňa S^+. Označme ho v.
Potom podľa lemy K2 v spĺňa tablo $\mathcal{T}$, teda v spĺňa niektorú vetvu π v $\mathcal{T}$.
Pretože $\mathcal{T}$ je uzavreté, aj vetva π je uzavretá,
teda π obsahuje označené formuly $\mathbf{T}\,X$ a $\mathbf{F}\,X$ pre nejakú formulu X.
Ale $v \models \mathbf{T}\,X$ vtt $v \models X$ a $v \models \mathbf{F}\,X$ vtt $v \not\models X$, čo je spor. □

2.8.2. Tablový dôkaz splniteľnosti

V.5 Úplná vetva a tablo

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

Definícia 2.80 (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 2.81. Vybudujme úplné tablo pre $\mathbf{F}\,X$, kde $X = (((p \lor q) \land (r \lor p)) \to (p \land (q \lor r)))$.

V.6 Otvorené tablo a splniteľnosť

Nech tablové pravidlá v príklade použijeme v akomkoľvek,

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

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

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

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

Otázka. • Dá sa vždy nájsť úplné tablo?

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

V.7 Existencia úplného tabla

Lema 2.82 (o existencii úplného tabla)**.** *Nech S^+ je konečná množina označených formúl.*
Potom existuje úplné tablo pre S^+.

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

- Na π_y sa nachádza nejaká formula α, ale nenachádza sa niektorá z formúl 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 operáciu A. Ak platí druhá možnosť, aplikujeme operáciu B. Získame tablo $\mathcal{T}_{i+1}$, s ktorým proces opakujeme.

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

2.8.3. Hintikkova lema

V.8 Nadol nasýtené množiny a Hintikkova lemma

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

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

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

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

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

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

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

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

v je korektne definované vďaka H_0.

Indukciou na stupeň formuly dokážeme, že v 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 2.68).
  - Ak X^+ je β, potom aspoň jedna z β_1, β_2 je v S^+ (H_2). Nech je to ktorákoľvek, je nižšieho stupňa ako X^+, teda podľa IP ju v spĺňa, a preto v spĺňa β (podľa pozorovania 2.70). □

2.8.4. Úplnosť

V.10 Úplnosť

Úplnosť kalkulu neformálne:
Ak je nejaké tvrdenie pravdivé, tak existuje jeho dôkaz v kalkule.

Veta 2.86 (o úplnosti)**.** *Nech S^+ je konečná nesplniteľná množina označených formúl.*
Potom existuje uzavreté tablo pre S^+.

Dôsledok 2.87. *Nech S je konečná teória a X je formula.*
Ak $S \vDash X$, tak $S \vdash X$.

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

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

V.11 Úplnosť — dôkaz

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

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

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

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

VI. prednáška
Korektné pravidlá
Rezolvencia

26. marca 2018

2.8.5. Nové korektné pravidlá

VI.1 Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

- Na dokázanie *korektnosti* tablového kalkulu stačilo, aby mali pravidlá vlastnosť:

  Nech v je ohodnotenie. Ak v spĺňa premisu (a množinu S^+), tak spĺňa oba (α) závery/aspoň jeden (β) záver.

  – Vďaka tejto vlastnosti zo splniteľnej množiny S^+ skonštruujeme iba splniteľné tablá.
  – Netreba opačnú implikáciu (ak v spĺňa oba/jeden záver, tak spĺňa premisu).
- Na dôkaz *úplnosti* stačili pravidlá (S^+), α, β, pretože stačia na vybudovanie úplného tabla.

VI.2 Nové pravidlo

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

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

Upravíme definíciu priameho rozšírenia:

Úprava definície 2.71
(...) Nech $\mathcal{T}$ je tablo pre S^+ a y je nejaký jeho list. Potom tablom pre S^+ je aj každé *priame rozšírenie* $\mathcal{T}$ ktoroukoľvek z operácií:

A $\cdots$

$\vdots$

DS$_1$: Ak sa na vetve π_y nachádzajú *obe* formuly $\mathbf{T}(A \lor B)$ a $\mathbf{F}\,A$, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci $\mathbf{T}\,B$.

VI.3 Nové pravidlo vs. korektnosť a úplnosť

- Pravidlo (DS$_1$) je *korektné*:

  Nech v je ľubovoľné ohodnotenie.
  Ak v spĺňa $\mathbf{T}(A \lor B)$ a $\mathbf{F}\,A$, tak v spĺňa $\mathbf{T}\,B$.

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

- Preto stále dokážeme lemu K1 (2.78):

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

  Z nej dokážeme lemu K2 a vetu o korektnosti

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

VI.4 Nové pravidlá vo všeobecnosti

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

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

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

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 $C_1^+, \dots, C_k^+$.

VI.5 Nové pravidlá vo všeobecnosti

Úprava definície 2.71

(...)

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

  $\vdots$

  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 $C_1^+, \dots, C_k^+$.

2.9. Rezolvencia vo výrokovej logike

VI.6 Tranzitivita implikácie

Vráťme sa k neoznačeným formulám.

Je nasledujúce pravidlo korektné?

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

Nahraďme implikácie disjunkciami:

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

VI.7 Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

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

$$\frac{(k_1 \lor \cdots \lor p \lor \cdots \lor k_m) \qquad (\ell_1 \lor \cdots \lor \neg p \lor \cdots \lor \ell_n)}{(k_1 \lor \cdots \lor k_m \lor \ell_1 \lor \cdots \lor \ell_n)}$$

pre ľubovoľnú výrokovú premennú p
a ľubovoľné literály $k_1, \ldots, k_m, \ell_1, \ldots, \ell_n$.

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

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

VI.8 Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

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

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

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

VI.9 Pozorovania o rezolvencii

- Rezolvencia s jednotkovou klauzulou skráti druhú klauzulu:

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

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

VI.10 Pozorovania o rezolvencii

- Ak rezolvencia odvodí **prázdnu klauzulu**

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

premisy **nie sú súčasne splniteľné**

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

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

Prečo?

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

VI.11 Problematické prípady

- Opakovaným aplikovaním rezolvencie môžeme odvodzovať ďalšie dôsledky

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

(1) $(\neg p \lor r)$ predpoklad z S

(2) $(\neg q \lor r)$ predpoklad z S

(3) $(p \lor q)$ predpoklad z S

(4) $(r \lor q)$ rezolventa (1) a (3)

(5) $(r \lor r)$ rezolventa (2) a (4)

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

- Preto potrebujeme ešte *pravidlo idempotencie*:

$$\frac{(k_1 \lor \cdots \lor \ell \lor \cdots \lor \ell \lor \cdots \lor k_n)}{(k_1 \lor \ell \lor \cdots \lor k_n)}$$

VI.12 Rezolvenčné odvodenie a zamietnutie

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

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

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

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

VI.13 Korektnosť a úplnosť rezolvencie

Veta 2.95 (Korektnosť rezolvencie). *Nech S je množina klauzúl. Ak existuje zamietnutie S, tak S je nesplniteľná.*

Veta 2.96 (Úplnosť rezolvencie). *Nech S je množina klauzúl. Ak S je nesplniteľná, tak existuje zamietnutie S.*

2.10. Späť k dôkazom o vyplývaní

VI.14 Konzultácie a termín pre 6. sadu úloh

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

  využívajte **konzultačné hodiny**:

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

- Riešenie **6. sady úloh** odovzdajte

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

VI.15 Uvažovanie o vyplývaní

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

Dokážte alebo vyvráťte:

c) Ak $T \models \neg X$, tak $T \not\models X$.

d) Ak $T \not\models X$, tak $T \models \neg X$.

e) $T \models (X \to Y)$ vtt $T \cup \{X\} \models Y$.

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

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

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

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

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

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

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

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

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

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

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

Riešenie 2.97 (e, smer $\Rightarrow$). Zoberme ľubovoľnú teóriu T a formuly X a Y také, že $T \models (X \to Y)$, teda
pre každé ohodnotenie v platí, že ak $v \models T$, tak $v \models (X \to Y)$.
Aby tvrdenie (e$\Rightarrow$) platilo, musí $T \cup \{X\} \models Y$, teda
pre každé ohodnotenie v musí platiť, že $(*)$ ak $v \models T \cup \{X\}$, tak $v \models Y$.
Zoberme teda ľubovoľné ohodnotenie v.

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

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

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

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

Riešenie 2.97 (e, smer $\Leftarrow$). Zoberme ľubovoľnú teóriu T a formuly X a Y také, že $T \cup \{X\} \models Y$, teda
pre každé ohodnotenie v platí, že ak $v \models T$, tak $v \models (X \to Y)$.
Aby tvrdenie (e$\Leftarrow$) platilo, musí $T \models (X \to Y)$, teda
pre každé ohodnotenie v musí platiť, že $(*)$ ak $v \models T$, tak $v \models (X \to Y)$.
Zoberme teda ľubovoľné ohodnotenie v.

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

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

VI.20 Problémy v dôkazoch (1)

Používanie pojmov *splnenie* a *vyplývanie*

- ✅ ohodnotenie v spĺňa formulu X
- ✅ formula X je splnená v ohodnotení v
- ✅ $v \models X$
- ⛔ formula X spĺňa ohodnotenie v
- ✅ ohodnotenie v spĺňa teóriu T
- ✅ teória T je splnená v ohodnotení v
- ✅ $v \models T$
- ⛔ teória T spĺňa ohodnotenie v

- ✅ z teórie T vyplýva formula X
- ✅ formula X vyplýva z teórie T
- ✅ formula X je (logickým) dôsledkom teórie T
- ✅ teória T má (logický) dôsledok X
- ✅ $T \models X$
- ⛔ z ohodnotenia v vyplýva...
- ⛔ z formuly X vyplýva teória T

Ignorovanie pojmov a ich definícií

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

Definície pojmov a ich negovanie

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

Skríženie pojmov splnenia a vyplývania

⚠ **Vyplývanie z teórie ($T \models X$) sa správa *inak* ako splnenie formuly ohodnotením ($v \models X$)**

- ✅ $v \models \neg X$ vtt $v \not\models X$
  priamo z definície splnenia formuly ohodnotením
- ⛔ $T \models \neg X$ vtt $T \not\models X$
  neplatí ani v jednom smere (videli sme pred chvíľou)

⚠ Symbol $\models$ sa (žiaľ) používa pre oba pojmy

Skoky v uvažovaní veľké a nezdôvodnené

- Ak $T \models (X \to Y)$, tak $T \not\models X$ alebo $T \models Y$.
- Ak $T \not\models X$ alebo $T \models Y$, tak $T \models (X \to Y)$.
- Ak $v \not\models T$, tak T je nesplniteľná.

VI.23 Problémy v dôkazoch (4)

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

VI.24 Problémy v dôkazoch (5)

Uvažovanie o formulách a teóriách, akoby to boli výrokové premenné

- Ohodnotenie v priraďuje t alebo f iba výrokovej premennej
  ($v(p) = t$, $v(p) = f$, $\cancel{v(X) = t}$, $\cancel{v(X \land Y) = t}$, $\cancel{v(T) = t}$)

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

VII. prednáška
SAT solver a algoritmus DPLL
Syntax relačnej logiky prvého rádu

9. apríla 2018

2.11. Problém výrokovologickej splniteľnosti (SAT)

VII.1 Problém SAT

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

  Príklad 2.98. Je množina klauzúl S splniteľná?

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

VII.2 Tabuľková metóda

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

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

2.11.1. Naivný backtracking

VII.3 Naivný backtracking v Pythone

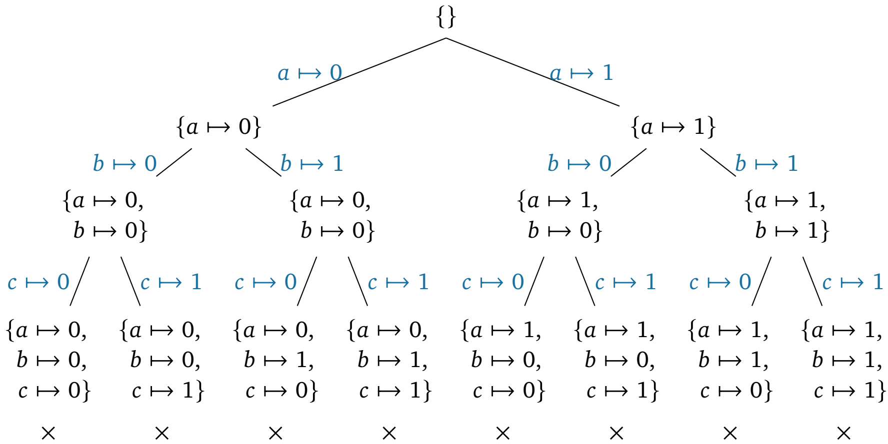
```python
#!/usr/bin/env python3
class Sat(object):
    def __init__(self, n, clauses):
        self.n, self.clauses, self.solution = n, clauses, None
    def checkClause(self, e, c):
        return any( ( e[abs(lit)] if lit > 0 else not e[abs(lit)] )
                      for lit in c )
    def check(self, e):
        return all( self.checkClause(e, cl) for cl in self.clauses )
    def solve(self, i, e):
        if i >= self.n:
            if self.check(e):
                self.solution = e
                return True
            return False
        for v in [True, False]:
            e[i] = v
            if self.solve(i+1, e):
                return True
        return False
Sat(20, [[]]).solve(0, {})
```

Čas: $O(s2^N)$, priestor: $O(s+N)$;
N — počet premenných,
s — súčet veľkostí klauzúl

VII.4 Strom prehľadávania ohodnotení

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

$\times$: $v \not\models S$ $\qquad f := 0, t := 1$



VII.5 Naivné C++

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

VII.6 Trochu lepšie C++

```
#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;
}
```

VII.7 Čas

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

VII.8 Priebežné vyhodnocovanie klauzúl

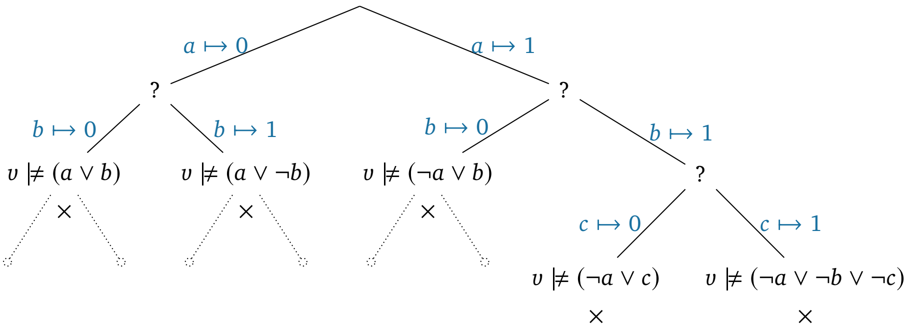
- Každý uzol prehľadávaného stromu ohodnotení je *čiastočné ohodnotenie*
- Ohodnotenie v uzle je *rozšírením* ohodnotenia v rodičovi

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

VII.9 Prehľadávanie s priebežným vyhodnocovaním

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

$\times$: $v \not\models S$



VII.10 Zjednodušenie množiny klauzúl podľa literálu

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

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

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

  Tieto klauzuly sú pre zistenie splniteľnosti vo všetkých v' *nepodstatné*, môžeme ich vynechať
- v' splní klauzulu $(\ell_1 \vee \cdots \vee \neg a \vee \cdots \vee \ell_n)$ obsahujúcu $\neg a$ vtt v' splní *zjednodušenú* klauzulu $(\ell_1 \vee \cdots \vee \cdots \vee \ell_n)$

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

Stačia nám zjednodušené klauzuly

VII.11 Zjednodušenie množiny klauzúl podľa literálu

Množinu klauzúl

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

teda môžeme *zjednodušiť podľa* a na

$$S|_a = \{ \qquad b, \quad (\neg b \lor \neg c), \quad c \}.$$

Analogicky môžeme S zjednodušiť podľa $\neg a$ na

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

VII.12 Zjednodušenie množiny klauzúl podľa literálu

Definícia 2.99. Nech p je výroková premenná.
Komplementom literálu p je $\neg p$. *Komplementom literálu* $\neg p$ je p.
Komplement literálu ℓ označujeme $\bar{\ell}$.

Definícia 2.100. Nech ℓ je literál a S je množina klauzúl. Potom definujeme

$$\begin{aligned} S|_\ell = {} & \{ (\ell_1 \lor \cdots \lor \cdots \lor \ell_n) \mid (\ell_1 \lor \cdots \lor \bar{\ell} \lor \cdots \lor \ell_n) \in S \} \cup \\ & \{ C \mid C \in S, \text{ v } C \text{ sa nevyskytuje } \ell \text{ ani } \bar{\ell} \}. \end{aligned}$$

Tvrdenie 2.101. *Nech ℓ je literál a S je množina klauzúl.*
Potom $S \cup \{\ell\}$ je splniteľná vtt $S|_\ell$ je splniteľná.

VII.13 Propagácia jednotkových klauzúl

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

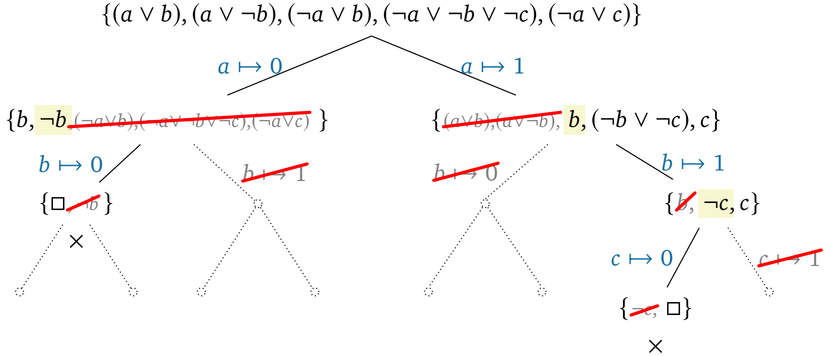
- Preto T' spĺňajú *iba* ohodnotenia v, v ktorých $v(b) = 0$
- Pre také ohodnotenia môžeme T' ďalej zjednodušiť podľa $\neg b$: $T'' := T'|_{\neg b} = \{c\}$
- T'' môžu splniť iba ohodnotenia v, v ktorých $v(c) = 1$
- Pre také ohodnotenia môžeme T'' ďalej zjednodušiť podľa c: $T''' := T''|_c = \{\}$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

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

VII.14 Propagácia jednotkových klauzúl

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

VII.15 Prehľadávanie so zjednodušovaním klauzúla unit propagation



VII.16 Eliminácia nezmiešaných literálov

- Všimnime si literál u v množine klauzúl:

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

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

- Vynechajme z T všetky klauzuly obsahujúce u:

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

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

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

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

VII.17 Eliminácia nezmiešaných literálov

Definícia 2.103. 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 2.104. *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 2.105 (Davis and Putnam [1960], Davis et al. [1962]).

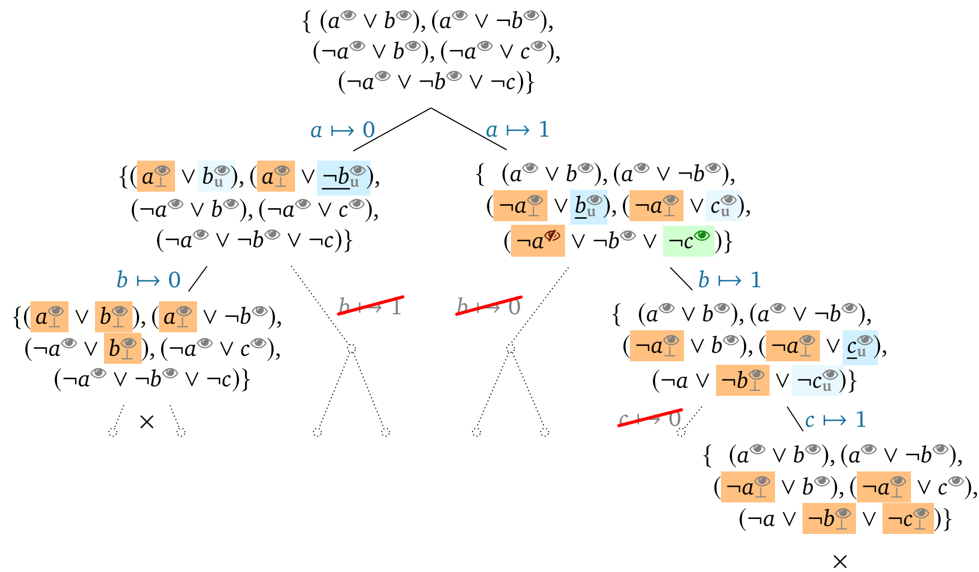
```
function DPLL(Φ, e)
    if Φ obsahuje prázdnu klauzulu then
        return False
    end if
    if e ohodnocuje všetky premenné then
        return True
    end if
    while existuje jednotková (unit) klauzula ℓ vo Φ do
        Φ, e ← UNIT-PROPAGATE(ℓ, Φ, e)
    end while
    while existuje nezmiešaný (pure) literál ℓ vo Φ do
        Φ, e ← PURE-LITERAL-ASSIGN(ℓ, Φ, e)
    end while
    x ← CHOOSE-BRANCH-LITERAL(Φ, e)
    return DPLL(Φ|x, e(x ↦ T)) or DPLL(Φ|¬x, e(x ↦ F))
end function
```

VII.19 Technika sledovaných literálov (watched literals)

Aby sme nemuseli zjednodušovať množinu klauzúl:

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

VII.20 Prehľadávanie s unit propagation a sledovaním



3. Logika prvého rádu

3.1. Syntax relačnej logiky prvého rádu

VII.21 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.

VII.22 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

VII.23 Štruktúra jednoduchých viet

- 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

VII.24 Predikátové symboly a ich argumenty

- *Atomické formuly* (jednoduché výroky) *v logike prvého rádu*:
  $\mathit{predikátový\_symbol}\,(\mathit{argument}_1,\ \mathit{argument}_2,\ \ldots,\ \mathit{argument}_n)$

  Predikátový symbol zodpovedá prísudku
  alebo celej prísudkovej časti:
  (je) minister, (je) starší (ako), prijal, <, …

  Jeho *argumenty* zodpovedajú podmetu, predmetu, …
  Úloha argumentu je daná *pozíciou*
  (ako v programovacích jazykoch).

- Predikátový symbol má jednoznačne určenú *aritu* —
  očakávaný počet argumentov

- *Vždy* musí mať práve toľko argumentov, aká je jeho arita

Dohoda 3.1. Aritu budeme niekedy písať ako horný index symbolu (minister^1, starší^2, prijal^4, <^{2}).

VII.25 Význam predikátových symbolov

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

minister$^1(arg_1)$	arg_1 je minister
myš_domová$^1(arg_1)$	arg_1 je myš domová
ľahká$^1(arg_1)$	arg_1 je ľahká

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

starší$^2(arg_1, arg_2)$	arg_1 je starší ako arg_2
medzi$^3(arg_1, arg_2, arg_3)$	arg_1 sa nachádza medzi arg_2 a arg_3
prijal$^4(arg_1, arg_2, arg_3, arg_4)$	arg_1 prijal arg_2 od arg_3 v čase arg_4

VII.26 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, ...: starší^2(arg_1, arg_2) — arg_1 je starší/staršia/staršie ako arg_2

VII.27 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 konštánt*.
  - Dorothy, Hlohovský, Jerry, 0, 1, 2, ..., rok2013
- Môžu byť *argumentmi predikátových symbolov* v atomických formulách
  - minister(Hlohovský), starší(Dorothy, George), prijal(Hlohovský, úplatok250000€, Veselič, rok2013)
- 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

VII.28 Výrokové spojky a atomické formuly

- V logike prvého rádu môžeme atomické formuly *spájať výrokovými spojkami* rovnako ako vo výrokovej logike:
  - ((matka(Dorothy)∧syn(George)) → starší(Dorothy, George))
  - (zomrel(Stephen_Hawking) → ¬ najznámejší_žijúci_fyzik ≐ Stephen_Hawking)
  - (prijal(Hlohovský, úplatok250000€, Veselič, rok2013) → ¬dôveryhodný(Hlohovský))
- Máme ale aj zaujímavejšie možnosti…

VII.29 Premenné a otvorené atomické formuly

- Atomické formuly nemusia vyjadrovať iba vlastnosti *konkrétnych* objektov označených konštantami
- Argumentami predikátových symbolov môžu byť aj *symboly indivíduových 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*
  - starší(x,Dorothy), minister(z_5)

  Nepredstavujú plnohodnotné výroky, ale *výrokové formy*
- Premenné a formuly s nimi nadobúdajú význam pomocou *kvantifikátorov*

VII.30 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*
  - $\forall x\ \mathtt{star\check{s}\acute{i}}(x, \mathtt{Dorothy})$ — každý je starší ako Dorothy
- Kvantifikovaná formula nemusí byť atomická:
  - $\forall x (\mathtt{star\check{s}\acute{i}}(x, \mathtt{Dorothy}) \lor \neg\mathtt{star\check{s}\acute{i}}(\mathtt{George}, x))$

VII.31 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*
  - $\exists x\ \mathtt{star\check{s}\acute{i}}(x, \mathtt{George})$ — niekto je starší ako George
- Kvantifikovaná formula nemusí byť atomická:
  - $\exists x (\mathtt{star\check{s}\acute{i}}(x, \mathtt{George}) \land \mathtt{star\check{s}\acute{i}}(\mathtt{Virginia}, x))$
- Kvantifikovaná formula môže obsahovať ďalšie kvantifikátory:
  - $\exists x\ \forall y\ \mathtt{star\check{s}\acute{i}}(x, \mathtt{y})$
  - $\forall x \big(\exists y\ \exists u\ \exists z (\mathtt{prijal}(x, u, \mathtt{y}, \mathtt{z}) \land \mathtt{\acute{u}platok}(u)) \to \neg\mathtt{d\hat{o}veryhodn\acute{y}}(x)\big)$

VII.32 Symboly jazyka relačnej logiky prvého rádu

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

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

mimologické symboly, ktorými sú

symboly konštánt z nejakej spočítateľnej množiny $\mathcal{C}_\mathcal{L}$ (označované a, $b, \ldots$);

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

logické symboly, ktorými sú

logické spojky: unárna $\neg$, binárne $\land$, $\lor$, $\to$,

symbol rovnosti $\doteq$,

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

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

Množiny $\mathcal{V}_\mathcal{L}, \mathcal{C}_\mathcal{L}, \mathcal{P}_\mathcal{L}$ sú vzájomne disjunktné.
Logické a pomocné symboly sa nevyskytujú v symboloch z $\mathcal{V}_\mathcal{L}, \mathcal{C}_\mathcal{L}, \mathcal{P}_\mathcal{L}$.
Každému symbolu $P \in \mathcal{P}_\mathcal{L}$ je priradená *arita* $\mathrm{ar}(P) \in \mathbb{N}^+$.

VII.33 Symboly jazyka relačnej logiky prvého rádu

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

VII.34 Atomické formuly relačnej logiky prvého rádu

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 $P(t_1, \ldots, t_n)$, kde
P je predikátový symbol s aritou n a $t_1, \ldots, t_n$ sú termy.

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

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

VII.35 Formuly jazyka relačnej logiky prvého rádu

Definícia 3.7. Množina $\mathcal{E}_{\mathcal{L}}$ všetkých *formúl* jazyka relačnej logiky prvého rádu $\mathcal{L}$
je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, pre ktorú platí:

- Všetky atomické formuly z $\mathcal{A}_{\mathcal{L}}$ sú formulami z $\mathcal{E}_{\mathcal{L}}$ (teda $\mathcal{A}_{\mathcal{L}} \subseteq \mathcal{E}_{\mathcal{L}}$).
- Ak A je formula z $\mathcal{E}_{\mathcal{L}}$, tak aj $\neg A$ je formula z $\mathcal{E}_{\mathcal{L}}$ (*negácia* A).
- Ak A a B sú formuly z $\mathcal{E}_{\mathcal{L}}$, tak aj $(A \land B)$, $(A \lor B)$, $(A \to B)$ sú formuly z $\mathcal{E}_{\mathcal{L}}$ (*konjunkcia*, *disjunkcia*, *implikácia* A a B).
- Ak x je indivíduová 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 $A, B, C, \ldots$ s prípadnými indexmi.
$(A \leftrightarrow B)$ je skratka postupnosti symbolov $((A \to B) \land (B \to A))$.

3.2. Formalizácia v logike prvého rádu

3.2.1. Jednoduchá formalizácia

VII.36 Jednoduchá formalizácia

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

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

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

3.2.2. Základné idiómy

VII.37 Základné idiómy: Obmedzená kvantifikácia

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

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

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

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

Jednoduchá vlastnosť „Nikto nie je dokonalý“:

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

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

- S dôrazom na zámeno:
  - $\neg\exists x\, (\mathtt{vegán}(x) \land \mathtt{obézny}(x))$
- S dôrazom na negatívne tvrdenie:
  - $\forall x\, \neg(\mathtt{vegán}(x) \land \mathtt{obézny}(x))$
  - $\forall x\, (\neg\mathtt{vegán}(x) \lor \neg\mathtt{obézny}(x))$
  - $\forall x\, (\mathtt{vegán}(x) \to \neg\mathtt{obézny}(x))$

Zamlčaná existencia

- každý vegán si kúpil tekvicu:
  - $\forall x(\mathtt{vegán}(x) \to \exists y(\mathtt{kúpil}(x, y) \land \mathtt{tekvica}(y)))$
- žiadny vegán si nekúpil syr:
  - $\neg\exists x(\mathtt{vegán}(x) \land \exists y(\mathtt{kúpil}(x, y) \land \mathtt{syr}(y))$
  - $\forall x(\mathtt{vegán}(x) \to \neg\exists y(\mathtt{kúpil}(x, y) \land \mathtt{syr}(y))$
  - $\forall x(\mathtt{vegán}(x) \to \forall y(\neg\mathtt{kúpil}(x, y) \lor \neg\mathtt{syr}(y))$
  - $\forall x(\mathtt{vegán}(x) \to \forall y(\mathtt{kúpil}(x, y) \to \neg\mathtt{syr}(y))$

Existencia v antecedente s odkazom v konzekvente

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

3.2.3. Nutné a postačujúce podmienky

VII.40 Nutné a postačujúce podmienky

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

VII.41 Postačujúca podmienka

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

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

VII.42 Nutná podmienka

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

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

- Ekvivalentne:
  „Pre každého platí, že je vegán, *iba* ak si kúpil tekvicu.“
  „Pre každého platí, že ak si *ne*kúpil tekvicu, tak *nie* je vegán.“
  „Pre každého platí, že ak je vegán, tak si kúpil tekvicu.“
- Formalizácia je teda $\forall x \big(\texttt{vegán}(x) \to \exists y(\texttt{kúpil}(x, y) \land \texttt{syr}(y))\big)$

3.2.4. Idiómy s rovnosťou

VII.43 Idiómy s rovnosťou: Enumerácia

Vymenovanie objektov s vlastnosťou

- V byte č. 14 bývajú Aďa, Biba, Ciri, Dada.
  - $\big(\texttt{býva\_v}(\texttt{Aďa}, \texttt{byt14}) \land \cdots \land \texttt{býva\_v}(\texttt{Dada}, \texttt{byt14})\big)$

  Ekvivalentne:
  Každá z Aďa, Biba, Ciri, Dada býva v byte č. 14.
  - $\forall x \big((x \doteq \texttt{Aďa} \lor \cdots \lor x \doteq \texttt{Dada}) \to \texttt{býva\_v}(x, \texttt{byt14})\big)$
- V byte č. 14 bývajú *iba* Aďa, Biba, Ciri, Dada.
  Každý, kto býva v byte č. 14, je jedna z Aďa, Biba, Ciri, Dada.
  - $\forall x \big(\texttt{býva\_v}(x, \texttt{byt14}) \to (x \doteq \texttt{Aďa} \lor \cdots \lor x \doteq \texttt{Dada})\big)$

VII.44 Idiómy s rovnosťou: Obmedzenia počtu

Aspoň k:

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

Najviac jeden:

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

- $\neg\exists t_1\, \exists t_2 \big(\neg\, t_1 \doteq t_2 \land \mathtt{tekvica}(t_1) \land \mathtt{tekvica}(t_2) \land \mathtt{kúpil}(\mathtt{Anka}, t_1) \land \mathtt{kúpil}(\mathtt{Anka}, t_2)\big)$
- $\forall t_1\, \forall t_2\, \neg \big(\neg\, t_1 \doteq t_2 \land \mathtt{tekvica}(t_1) \land \mathtt{tekvica}(t_2) \land \mathtt{kúpil}(\mathtt{Anka}, t_1) \land \mathtt{kúpil}(\mathtt{Anka}, t_2)\big)$
- $\forall t_1\, \forall t_2 \big(t_1 \doteq t_2 \lor \neg\mathtt{tekvica}(t_1) \lor \neg\mathtt{tekvica}(t_2) \lor \neg\mathtt{kúpil}(\mathtt{Anka}, t_1) \lor \neg\mathtt{kúpil}(\mathtt{Anka}, t_2)\big)$
- $\forall t_1\, \forall t_2 \big((\mathtt{tekvica}(t_1) \land \mathtt{tekvica}(t_2) \land \mathtt{kúpil}(\mathtt{Anka}, t_1) \land \mathtt{kúpil}(\mathtt{Anka}, t_2)) \to t_1 \doteq t_2\big)$

• Teda ekvivalentne: Všetky tekvice, ktoré si Anka kúpila, sú rovnaké.

VIII. prednáška

Definície predikátov. Sémantika relačnej logiky prvého rádu

16. apríla 2018

VIII.1 Formuly jazyka relačnej logiky prvého rádu

Otestujte sa VIII.1

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

a) $\forall x\ \mathtt{človek}(x) \land \mathtt{žena}(\mathtt{Eva})$

b) $\mathtt{chytá}(\mathtt{mačka}(\mathtt{Muro}), \mathtt{myš}(y))$

c) $(\neg \mathtt{prší} \lor \exists x(\mathtt{zmoknutý}(x)))$

d) $(\forall x \neg x \doteq \mathtt{Eva} \to \neg \exists x\, x \doteq x)$

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

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

b) **Nie** je formula, význam pravdepodobne správne vyjadruje formula: $\big(\mathtt{mačka}((\mathtt{Muro}) \land \mathtt{myš}(y)) \land \mathtt{chytá}(\mathtt{Muro}, y)\big)$.

c) **Nie** je formula — ak by prší bol predikát, musel by mať argument; prší nemôže byť indivíduová konštanta, pretože tie nie sú formulami. Navyše priama podformula kvantifikácie je atomická, ktorá sa nezátvorkuje. Význam pravdepodobne správne vyjadruje formula: $(\neg \mathtt{prší}(\mathtt{počasie}) \lor \exists x\ \mathtt{zmoknutý}(x))$

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

3.2.5. Definície predikátov

VIII.2 Pojmy

- V mnohých doménach sú zaujímavé komplikovanejšie *kombinácie* vlastností alebo vzťahov:
  - x má spoločného rodiča s y: $\exists z(\mathtt{rodič}(z, x) \land \mathtt{rodič}(z, y))$
  - x je živočích, ktorý konzumuje iba rastliny: $\big(\mathtt{živočích}(x) \land \forall y(\mathtt{konzumuje}(x, y) \to \mathtt{rastlina}(y))\big)$
- Často sa vyskytujúce kombinácie vzťahov a vlastností je výhodné:
  - *pomenovať*
  - a jasne *vyjadriť význam* nového mena pomocou doteraz známych vlastností a vzťahov,

  teda *zadefinovať pojem*

VIII.3 Definície pojmov

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

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

Príklad 3.11.
- x je *súrodencom* y práve vtedy, keď x má spoločného rodiča s y
  $\forall x \forall y \big(\mathtt{súrodenec}(x, y) \leftrightarrow \exists z(\mathtt{rodič}(z, x) \land \mathtt{rodič}(z, y))\big)$

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

VIII.4 Explicitná def. a nutná a postačujúca podmienka

Poznámka 3.12. 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

VIII.5 Použitie pojmov

Využitím definovaného pojmu

- skracujeme tvrdenia:
  - králiky sú bylinožravce:
    $\forall x(\texttt{králik}(x) \rightarrow \texttt{bylinožravec}(x))$

- jednoduchšie definujeme ďalšie pojmy:
  - x je *sestrou* y práve vtedy, keď x je žena, ktorá je súrodencom y:
    $\forall x \forall y\big(\texttt{sestra}(x,y) \leftrightarrow (\texttt{žena}(x) \land \texttt{súrodenec}(x,y))\big)$

Vyskúšajte si VIII.2
Zadefinujte pojem *teta* (chápaný ako vzťah dvoch ľudí)
neformálne (v slovenčine) aj formálne (formulou logiky prvého rádu).

Riešenie. Osoba x je *tetou* y vtedy a len vtedy, keď x je sestrou rodiča y.
$\forall x \forall y\big(\texttt{teta}(x,y) \leftrightarrow \exists z(\texttt{sestra}(x,z) \land \texttt{rodič}(z,y))\big)$

3.3. Sémantika relačnej logiky prvého rádu

VIII.6 Význam atomických formúl — výroková logika

Významom atomických formúl je pravdivostná hodnota

Vo výrokovej logike:

- Atomické formuly sú výrokové premenné — nemajú *žiadnu štruktúru*

$$\mathtt{starší\_Howard\_Virginia}, \quad \mathtt{otec\_George}$$

- Význam im *priamo* priraďuje *ohodnotenie*

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

- Rôzne ohodnotenia — rôzne stavy sveta

VIII.7 Význam atomických formúl — logika prvého rádu

Významom atomických formúl je pravdivostná hodnota

Logika prvého rádu:

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

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

- *Termy* (symboly konštánt a *indivíduových* premenných)

$$\mathtt{Dorothy}, \quad \mathtt{George}, \quad \mathtt{Hlohovský}, \quad \mathtt{úplatok250000€}, \quad \ldots\ u, \quad x, \quad \ldots$$

  označujú objekty

- *Predikátové symboly*

$$\mathtt{minister}^1, \quad \mathtt{starší}^1, \quad \mathtt{prijal}^4$$

  označujú vlastnosti alebo vzťahy objektov

❓ Aký matematický objekt predstavuje *vlastnosť* objektov?

- Množina, napríklad pre vlastnosť byť ministrom môžeme vytvoriť množinu všetkých objektov s touto vlastnosťou:
  { 🚺$_{\text{Pšenová}}$, 🚹$_{\text{Hlohovský}}$, 🚺$_{\text{Zubáková}}$, 🚹$_{\text{Žinčica}}$, $\ldots$ }

❓ Aký matematický objekt predstavuje *vzťah* niekoľkých objektov?

- Usporiadaná n-tica: (🚺$_{\text{Dorothy}}$, 🚹$_{\text{George}}$)

❓ Aký matematický objekt predstavuje
mnoho vzťahov rovnakého druhu?

- Množina usporiadaných n-tíc, napríklad pre vzťah byť starší
  {(🚺$_{\text{Dorothy}}$, 🚺$_{\text{Virginia}}$), (🚹$_{\text{Howard}}$, 🚺$_{\text{Virginia}}$), (🚺$_{\text{Dorothy}}$, 🚹$_{\text{Howard}}$),
  (🚺$_{\text{Dorothy}}$, 🚹$_{\text{George}}$), (🚹$_{\text{George}}$, 🚺$_{\text{Virginia}}$)}

❓ Odkiaľ vyberáme objekty do týchto množín?

- Z množiny objektov existujúcich v časti sveta, ktorá nás zaujíma

VIII.9 Význam mimologických symbolov

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

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

  M = {🚺$_{\text{Pšenová}}$, 🚹$_{\text{Hlohovský}}$, 🚺$_{\text{Zubáková}}$, 🚹$_{\text{Žinčica}}$, $\ldots$, 🚹$_{\text{Veselič}}$, 🚹$_{\text{Petržlen}}$, $\ldots$,
  💵$_{50000}$, 💵$_{250000}$, $\ldots$, 🏍$_{\text{HD}}$, $\ldots$, 📅$_{2012}$, 📅$_{2013}$, $\ldots$ }

- *Interpretujeme* mimologické symboly v tejto doméne:

  Symboly konštánt interpretujeme ako *objekty z domény*

  $i(\texttt{Hlohovský})$ = 🚹$_{\text{Hlohovský}}$, $i(\texttt{rok2013})$ = 📅$_{2013}$,
  $i(\texttt{minister\_vnútra})$ = 🚹$_{\text{Hlohovský}}$, $\ldots$

  Predikátové symboly interpretujeme ako množiny prvkov domény

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

alebo ich n-tíc

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

v závislosti od arity symbolu

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

VIII.10 Štruktúra

Definícia 3.13. Nech $\mathcal{L}$ je jazyk relačnej logiky prvého rádu.
Štruktúrou pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (M, i)$, kde

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

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

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

Dohoda 3.14. Štruktúry označujeme veľkými *písanými* písmenami $\mathcal{M}$, $\mathcal{N}$, ...
Doménu označujeme *rovnakým*, ale *tlačeným* písmenom ako štruktúru.

VIII.11 Štruktúry

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

VIII.12 Ohodnotenie premenných

Definícia 3.15. Nech $\mathcal{M} = (M, i)$ je štruktúra pre jazyk $\mathcal{L}$.
Ohodnotenie (indivíduových) premenných je ľubovoľná funkcia $e\colon \mathcal{V}_{\mathcal{L}} \to M$ (priraďuje premenným prvky domény).

Zápisom $e(x/v)$ označíme ohodnotenie indivíduových premenných, ktoré priraďuje premennej x hodnotu v z domény M
a všetkým ostatným premenným rovnakú hodnotu ako im priraďuje e.

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

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

Ohodnotením (indivíduových) premenných je napríklad

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

Potom

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

VIII.13 Hodnota termov

Definícia 3.16. Nech $\mathcal{M} = (M, i)$ je štruktúra, e je ohodnotenie premenných.
Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e je prvok $t^{\mathcal{M}}[e]$ z M určený nasledovne:

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

VIII.14 Splnenie atomickej formuly v štruktúre

Konečne môžeme určiť význam atomickej formuly

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

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

  $$i(\texttt{Aďa}) = 🚺_{\text{Andrea K.}}, \quad i(\texttt{Biba}) = 🚺_{\text{Bibiána V.}},$$
  $$i(\texttt{Ciri}) = 🚺_{\text{Alena G.}}, \quad i(\texttt{Dada}) = 🚺_{\text{Daniela L.}}$$

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

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

- Pre formulu $\texttt{má\_rada}(\texttt{Biba}, x)$
  1. vyhodnotíme termy vo formule:
     $\texttt{Biba}^{\mathcal{M}}[e] = i(\texttt{Biba}) = 🚺_{\text{Bibiána V.}}, \qquad x^{\mathcal{M}}[e] = e(x) = 🚹_{\text{Fero Z.}}$
  2. zistíme, či $(🚺_{\text{Bibiána V.}}, 🚹_{\text{Fero Z.}}) \in i(\texttt{má\_rada})$ —
     v tomto prípade nie

- Takže štruktúra $\mathcal{M}$ ne*spĺňa* formulu $\texttt{má\_rada}(\texttt{Biba}, x)$
  pri ohodnotení e

VIII.15 Splnenie existenčne kvantifikovanej formuly

- Vyhodnotenie splnenia formuly s *výrokovými spojkami* v štruktúre pri ohodnotení si vieme ľahko predstaviť

- Ako vyhodnotíme splnenie formuly s *kvantifikátormi*?

- $\exists x\, \texttt{má\_rada}(\texttt{Biba}, x)$
  1. Vyskúšame všetky ohodnotenia, ktoré postupne priraďujú kvantifikovanej premennej jednotlivé prvky domény:

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

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

VIII.16 Splnenie všeobecne kvantifikovanej formuly

- Nech $e = \{x \mapsto$ Andrea K.$, y \mapsto$ Daniela V.$\}$
- $\forall x\, \neg\texttt{má\_rada}(y, x)$
  1. Vyskúšame všetky ohodnotenia, ktoré postupne priraďujú kvantifikovanej premennej jednotlivé prvky domény:

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

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

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

VIII.17 Splnenie formuly v štruktúre

Definícia 3.17. Nech $\mathcal{M} = (M, i)$ je štruktúra, e je ohodnotenie premenných.
Relácia *štruktúra $\mathcal{M}$ spĺňa formulu A pri ohodnotení e* (skrátene $\mathcal{M} \models A[e]$) má nasledovnú induktívnu definíciu:

- ▶ $\mathcal{M} \models t_1 \doteq t_2[e]$ vtt $t_1^{\mathcal{M}}[e] = t_2^{\mathcal{M}}[e]$,
- ▶ $\mathcal{M} \models P(t_1, \ldots, t_n)[e]$ vtt $\left(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e]\right) \in i(P)$,
- • $\mathcal{M} \models \neg A[e]$ vtt $\mathcal{M} \not\models A[e]$,
- • $\mathcal{M} \models (A \land B)[e]$ vtt $\mathcal{M} \models A[e]$ a zároveň $\mathcal{M} \models B[e]$,
- • $\mathcal{M} \models (A \lor B)[e]$ vtt $\mathcal{M} \models A[e]$ alebo $\mathcal{M} \models B[e]$,
- • $\mathcal{M} \models (A \to B)[e]$ 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 $t_1, t_2, \ldots, t_n$, všetky premenné x a všetky formuly A, B.

VIII.18 Splnenie množiny formúl

Definícia 3.18. Nech S je množina formúl jazyka $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$,
nech e je ohodnotenie výrokových premenných.
Štruktúra $\mathcal{M}$ spĺňa množinu S pri ohodnotení e (skrátene $\mathcal{M} \models S[e]$) vtt pre všetky formuly X z S platí $\mathcal{M} \models X[e]$.

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

$$\begin{aligned}
A_1 &= (\text{má_rada}(\text{Biba}, \text{Ciri}) \lor \text{má_rada}(\text{Biba}, \text{Dada})),\\
A_2 &= \forall x(\text{má_rada}(\text{Biba}, x) \to \text{má_rada}(\text{Aďa}, x)),\\
A_3 &= \forall x(\text{má_rada}(x, \text{Ciri}) \to \text{má_rada}(\text{Ciri}, x)),\\
A_4 &= \exists x(\text{má_rada}(x, \text{Biba}) \land \text{má_rada}(\text{Biba}, x)),\\
A_5 &= \forall x\, \neg\text{má_rada}(x, x), \quad A_6 = \forall x\, \exists y\, \text{má_rada}(x, y)
\end{aligned}$$

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

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

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

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

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

Definícia 3.22. Nech X je formula v jazyku $\mathcal{L}$.
Formula X je *platná* (skrátene $\models X$) vtt
každá štruktúra $\mathcal{M}$ pre $\mathcal{L}$ spĺňa X pri každom ohodnotení e.

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

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

Definícia 3.23. Nech X je formula v jazyku $\mathcal{L}$, nech S je množina formúl v jazyku $\mathcal{L}$.
Formula X *(prvorádovo) vyplýva z S* (skrátene $S \models X$) vtt
pre každú štruktúru $\mathcal{M}$ pre $\mathcal{L}$ a každé ohodnotenie e platí, že
ak $\mathcal{M}$ spĺňa S pri e, tak $\mathcal{M}$ spĺňa X pri e.

Tvrdenie 3.24. *Nech X je formula v jazyku $\mathcal{L}$.*
Potom X je platná ($\models X$) vtt
X prvorádovo vyplýva z prázdnej množiny formúl ($\{\} \models X$).

Tvrdenie 3.25. *Nech X je formula a S je množina formúl v spoločnom jazyku $\mathcal{L}$.*
Potom z S vyplýva X vtt $S \cup \{\neg X\}$ je nesplniteľná.

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

a) Nech T je ľubovoľná výroková teória,
nech X a Y sú ľubovoľné výrokové formuly.
Ak $T \models (X \to Y)$, tak $T \not\models X$ alebo $T \models Y$.

b) Nech T je ľubovoľná výroková teória,
nech X a Y sú ľubovoľné výrokové formuly.
Ak $T \not\models X$ alebo $T \models Y$, tak $T \models (X \to Y)$.

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

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

b) Tvrdenie neplatí. Háčik je v tom, že $T \models (X \to Y)$ musí podľa tvrdenia platiť aj keď iba $T \not\models X$, aj keď iba $T \models Y$. Práve v prvom prípade je problém.

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

IX. prednáška

Logika prvého rádu s funkčnými symbolmi

Tablá pre logiku prvého rádu

23. apríla 2018

3.4. Logika prvého rádu (s funkčnými symbolmi)

3.4.1. Syntax logiky prvého rádu (s funkčnými symbolmi)

IX.1 Mimologické symboly v relačnej logike

V doterajšej — *relačnej* logike prvého rádu
boli dva druhy mimologických symbolov:

symboly konštánt: mená *konkrétnych význačných objektov alebo hodnôt*

- Adelka, Hlohovský, úplatok250000, 0, 1, π;

predikátové symboly: mená *vlastností* a *vzťahov* objektov/hodnôt

- žena^1, profesor^1, starší^2, prijal^4, $<^2$;

Okrem nich používame

symboly premenných: *dočasné* mená objektov/hodnôt,
ktorých vlastnosti popisuje kvantifikovaná formula
(ako riadiaca premenná cyklu)

- x, t, kto, $čo$, $komu$

IX.2 Vzťahy s jednoznačne určenými objektmi

V niektorých vzťahoch jeden z účastníkov

- pre každú kombináciu ostatných účastníkov *existuje*
- a je *jednoznačne určený*

Napríklad:

- Každý človek má *práve jednu* biologickú matku
  $\forall x\big(\texttt{človek}(x) \rightarrow \exists y(\texttt{rodič}(y,x) \land \texttt{žena}(y))\big)$
  $\forall x\, \forall y_1\, \forall y_2\big((\texttt{človek}(x) \land \texttt{rodič}(y_1,x) \land \texttt{žena}(y_1) \land$
  $\qquad \texttt{rodič}(y_2,x) \land \texttt{žena}(y_2)) \rightarrow$
  $\qquad y_1 \doteq y_2\big)$

- Každý študent dostane z každej úlohy *práve jedno* hodnotenie
  $\forall x\, \forall u((\texttt{študent}(x) \land \texttt{úloha}(u)) \rightarrow \exists z\, \texttt{hodnotenie}(x,u,z))$
  $\forall x\, \forall u\, \forall y\, \forall z_1\, \forall z_2\big((\texttt{študent}(x) \land \texttt{úloha}(u) \land$
  $\qquad \texttt{hodnotenie}(x,u,z_1) \land \texttt{hodnotenie}(x,u,z_2)) \rightarrow$
  $\qquad z_1 \doteq z_2\big)$

- Podobne: otec, cena tovaru so zľavou podľa množstva, prvorodené dieťa rodičov, súčet čísel, prienik množín, ...

IX.3 Funkčné symboly

- Relácii, v ktorej posledná zložka n-tíc je jednoznačne určená, hovoríme ...

- V logike prvého rádu sa funkcie označujú *funkčnými symbolmi*
  - Tretí druh mimologických symbolov

- Funkčný symbol má význam, iba keď dostane argumenty:
  $\texttt{matka}(\texttt{Adelka})$, $\texttt{hodnotenie}(\texttt{Igor}, \texttt{su08})$, ...

- *Čo označujú* tieto postupnosti symbolov? *Aký význam* majú?

  $\texttt{matka}(\texttt{Adelka})$: Adelkina mama

  $\texttt{hodnotenie}(\texttt{Igor}, \texttt{su08})$: číslo, počet Igorovych bodov z 8. s. ú.

► Významom je teda *objekt*

⚠ Významom $(\texttt{rodič}(\texttt{Magda}, \texttt{Adelka}) \land \texttt{žena}(\texttt{Magda}))$ je pravdivostná hodnota

IX.4 Termy s funkčnými symbolmi

- Doteraz sme mali dva druhy výrazov:

  termy (konštanty, premenné) — významom je *objekt*

  formuly — významom je *pravdivostná hodnota*

- Výrazy s funkčnými symbolmi sú *nový druh termov*

- Termy s funkčnými symbolmi môžu byť argumentmi
  - predikátových symbolov:

    $\mathtt{teta}(\mathtt{matka}(\mathtt{Adelka}), \mathtt{Hugo})$:
    Adelkina mama je Hugovou tetou,

    $\mathtt{dostatočné}(\mathtt{hodnotenie}(\mathtt{Igor}, \mathtt{su08}))$:
    Igorovo hodnotenie z 8. s. ú. je dostatočné,
  - ale aj argumentmi funkčných symbolov:

    $\mathtt{matka}(\mathtt{matka}(\mathtt{Adelka}))$:
    Adelkina stará mama z matkinej strany

IX.5 Definičný obor a obor hodnôt

- Vnorené termy nedávajú vždy zmysel:
  $\mathtt{hodnotenie}(\mathtt{hodnotenie}(\mathtt{Igor}, \mathtt{su08}), \mathtt{su03})$

- Hodnota funkčného symbolu je *definované pre všetky argumenty*

- Akou formulou môžeme vyjadiť, že hodnota funkčného symbolu
  - nás zaujíma iba pre nejaký druh argumentov — definičný obor
  - je nejakého druhu — obor hodnôt?
  - ▶ $\forall x \big(\mathtt{človek}(x) \to \mathtt{človek}(\mathtt{matka}(x))\big)$
  - ▶ $\forall x \big(\mathtt{človek}(x) \to \mathtt{žena}(\mathtt{matka}(x))\big)$
  - ▶ $\forall x\, \forall u \big(\mathtt{študent}(x) \land \mathtt{úloha}(u) \to \mathbb{Q}(\mathtt{hodnotenie}(x, u))\big)$

- Definície syntaxe logiky prvého rádu sa *mierne líšia* od doterajších definícií syntaxe *relačnej* logiky prvého rádu
- Musíme:
  - pridať *funkčné symboly* medzi symboly jazyka,
  - rozšíriť termy o *aplikácie funkčných symbolov* a ich *vnáranie*
- Atomické formuly a formuly zadefinujeme *zdanlivo* rovnako ako doteraz, ale *využitím nových termov*

Definícia 3.27. *Symbolmi jazyka logiky prvého rádu* $\mathcal{L}$ sú:

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

mimologické symboly:

symboly konštánt z nejakej spočítateľnej množiny $\mathcal{C}_\mathcal{L}$ $(a, b, \ldots)$,

funkčné symboly z nejakej spočítateľnej množiny $\mathcal{F}_\mathcal{L}$ $(f, g, \ldots)$,

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

logické symboly:

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

symbol rovnosti $\doteq$,

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

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

Množiny $\mathcal{V}_\mathcal{L}, \mathcal{C}_\mathcal{L}, \mathcal{F}_\mathcal{L}, \mathcal{P}_\mathcal{L}$ sú vzájomne disjunktné.
Logické a pomocné symboly sa nevyskytujú v symboloch z $\mathcal{V}_\mathcal{L}$, $\mathcal{C}_\mathcal{L}$, $\mathcal{F}_\mathcal{L}$, $\mathcal{P}_\mathcal{L}$.

Každému symbolu $s \in \mathcal{P}_\mathcal{L} \cup \mathcal{F}_\mathcal{L}$ je priradená *arita* $\mathrm{ar}(s) \in \mathbb{N}^+$.

Príklad 3.28. **Symboly konštánt** označujú *konkrétne význačné objekty alebo hodnoty*

- Adelka, Igor, su08, 0, 1, $\emptyset$, π;

Predikátové symboly označujú *vlastnosti* a *vzťahy* objektov/hodnôt

- $\mathtt{žena}^1$, $\mathtt{profesor}^1$, $\mathtt{starší}^2$, $\mathtt{prijal}^4$, $<^2$;

Funkčné symboly označujú *vzťahy*, v ktorých je
jeden účastník jednoznačne určený ostatnými účastníkmi:

- $\mathtt{matka}^1$, $\mathtt{hodnotenie}^2$, $+^2$, $*^2$, $\cap^2$

Symboly premenných *dočasne* označujú objekty/hodnoty, ktorých vlastnosti popisuje kvantifikovaná formula (ako riadiaca premenná cyklu)

- x, t, *kto*, *čo*, *komu*

IX.9 Označovanie symbolov jazyka logiky prvého rádu

Dohoda 3.29.

- Sadzba **konkrétnych** symbolov:
  - *symboly premenných* — neproporčná italika: x, u_7, …;
  - *ostatné* (konštánt, funkčné, predikátové) — zvislá egyptienka: Adelka, súrodenec, cena, ….
- Zvyčajné *označovanie nekonkrétnych symbolov* (*meta premenné*):

  premenných: malé písmená z konca abecedy x, y, z;

  konštánt: malé písmená zo začiatku abecedy a, b, c;

  funkčných: f, g, h;

  predikátových: P, Q, R

  všetky podľa potreby s prípadnými dolnými indexmi.
- Aritu budeme niekedy písať ako horný index symbolov, konkrétnych aj nekonkrétnych: $\mathtt{matka}^1$, $<^2$, P^5.

Definícia 3.30. Množina $\mathcal{T}_\mathcal{L}$ *termov* jazyka logiky prvého rádu $\mathcal{L}$ je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, pre ktorú platí:

- každý symbol premennej $x \in \mathcal{V}_\mathcal{L}$ je termom;
- každý symbol konštanty $c \in \mathcal{C}_\mathcal{L}$ je termom;
- ak f je funkčný symbol s aritou n a $t_1, \ldots, t_n$ sú termy, tak aj $f(t_1, \ldots, t_n)$ je termom.

Inak povedané:

- $\mathcal{V}_\mathcal{L} \cup \mathcal{C}_\mathcal{L} \subseteq \mathcal{T}_\mathcal{L}$;
- ak $f \in \mathcal{F}_\mathcal{L}$, $\mathrm{ar}(f) = n$ a $t_1, \ldots, t_n \in \mathcal{T}_\mathcal{L}$, tak aj $f(t_1, \ldots, t_n) \in \mathcal{T}_\mathcal{L}$.

Dohoda 3.31. Termy označujeme písmenami t, s, r s prípadnými dolnými indexmi.

Príklad 3.32. *Termy označujú objekty — konkrétne*, pomenované symbolmi *konštánt*:

- Adelka, Igor, su08, 0, 1, $\emptyset$

nekonkrétne, označené *premennými*:

- x, u_3, *niekto*, *čo*, ...

alebo *nepriamo* pomenované pomocou *funkčných* vzťahov:

- matka(Adelka), matka(x), hodnotenie(Igor, x), $+(k, 1)$, $\cap(X, Y)$.

Termy možno *ľubovoľne vnárať*:

- matka(matka(matka(Adelka))), $*(*(x, 1), +(1, 1))$, $\cap(\cup(X, \emptyset), Y)$.

IX.12 Atomické formuly jazyka logiky prvého rádu

Definícia 3.33 (Atomické formuly)**.** Nech $\mathcal{L}$ je jazyk 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 $P(t_1, \ldots, t_n)$, kde
P je predikátový symbol s aritou n a t_1, …, 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 $\mathcal{A}_{\mathcal{L}}$.

IX.13 Príklady atomických formúl

Príklad 3.34. *Predikátové atomické* formuly formalizujú *jednoduché výroky* o *vlastnostiach* objektov označených termami:

- úloha(su08), žena(matka(x)), párne(+(1, x))

a o *vzťahoch* objektov:

- starší(Howard, x), rodič(matka(Adelka), Oliverko),
  <(+(1, 1), 0), disjunktné(Z, ∩(X, Y)), prijal(štátny_tajomník(Ministerstvo_

Rovnostné atómy vyjadrujú, že dva termy označujú *ten istý* objekt:

- Butler $\doteq$ x,   matka(Adelka) $\doteq$ matka(Oliverko),
  +(1, 0) $\doteq$ 1,   ∩(X, Y) $\doteq$ $\emptyset$.

IX.14 Formuly jazyka logiky prvého rádu

Definícia 3.35. Množina $\mathcal{E}_{\mathcal{L}}$ *formúl* jazyka 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 $\mathcal{E}_{\mathcal{L}}$.

- 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 $(A \land B)$, $(A \lor B)$, $(A \to B)$ sú formuly z $\mathcal{E}_{\mathcal{L}}$
  (*konjunkcia*, *disjunkcia*, *implikácia* A a B).
- Ak x je indivíduová 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).

IX.15 Skracovanie zápisu formúl

Dohoda 3.36. Zápis formúl môžeme skracovať nasledujúcim spôsobom:

1. Negáciu rovnostného atómu $\neg\, s \doteq t$ skrátene zapisujeme $s \not\doteq t$.
2. Ak $\circ \in \{\land, \lor\}$, tak $((A \circ B) \circ C)$ môžeme skrátiť na $(A \circ B \circ C)$.
3. Binárnym spojkám priradíme *prioritu*:
   najvyššiu prioritu má $\land$, *strednú* $\lor$, *najnižšiu* $\to$.
4. Ak spojka $\circ$ má *vyššiu* prioritu ako $\diamond$, tak v každej formule môžeme podformulu $((A \circ B) \diamond X)$ skrátiť na $(A \circ B \diamond X)$
   a symetricky $(X \diamond (A \circ B))$ skrátiť na $(X \diamond A \circ B)$.
5. Vonkajší pár zátvoriek okolo celej formuly môžeme vždy vynechať, napr. $(\forall x(a \doteq x \lor P(x)) \to P(b))$ skrátime na $\forall x(a \doteq x \lor P(x)) \to P(b)$.

Neodstraňujeme (ale ani nepridávame) zátvorky
okolo priamych podformúl negácie a kvantifikátorov,
implikácie vnorenej v implikácii

IX.16 Skracovanie zápisu formúl

Príklad 3.37. Formulu

$$\Big(\exists x\, \forall y \big(S(x) \land \big(P(y) \to (\neg Z(x,y) \lor S(x,y))\big)\big) \to \forall x \big((U(x) \land R(x)) \to Q(x)\big)\Big)$$

môžeme maximálne skrátiť na

$$\exists x\, \forall y \big(S(x) \land \big(P(y) \to \neg Z(x,y) \lor S(x,y)\big)\big) \to \forall x \big(U(x) \land R(x) \to Q(x)\big).$$

Skrátený zápis

$$P(a,x) \land (x \doteq b \lor P(x,b) \lor R(x)) \to P(f(a),x) \lor b \doteq f(x) \land P(a,b)$$

vznikol z formuly

$$\big(\big(P(a,x) \land ((x \doteq b \lor P(x,b)) \lor R(x))\big) \to \big(P(f(a),x) \lor (b \doteq f(x) \land P(a,b))\big)\big).$$

3.4.2. Sémantika logiky prvého rádu s funkčnými symbolmi

IX.17 **Štruktúry**

Rozšírme štruktúru tak, aby dávala význam aj funkčným symbolom:

Definícia 3.38. Nech $\mathcal{L}$ je jazyk 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 $\mathcal{L}$ priraďuje prvok $i(c) \in M$;
- *každému funkčnému symbolu f jazyka $\mathcal{L}$ s aritou n priraďuje funkciu $i(f)\colon M^n \to M$;*
- každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $i(P) \subseteq M^n$.

Príklad 3.39. Nájdime štruktúru pre jazyk $\mathcal{L}$, v ktorom

- $\mathcal{V}_{\mathcal{L}} = \{x, y, z, x_1, y_1, z_1, \ldots\}$,
- $\mathcal{C}_{\mathcal{L}} = \{\texttt{Adelka}, \texttt{Oliverko}\}$,
- $\mathcal{F}_{\mathcal{L}} = \{\texttt{matka}^1\}$,
- $\mathcal{P}_{\mathcal{L}} = \{\texttt{rodič}^2, \texttt{žena}^1\}$.

Riešenie. Štruktúrou pre tento jazyk môže byť napríklad $\mathcal{M} = (M, i)$, kde

$$\begin{aligned}
M &= \{\faFemale_{\text{Magdaléna U.}}, \faFemale_{\text{Iveta T.}}, \faFemale_{\text{Adela U.}}, \faMale_{\text{Oliver U.}}, \faGlobe\},\\
i(\texttt{Adelka}) &= \faFemale_{\text{Adela U.}}, \qquad i(\texttt{Oliverko}) = \faMale_{\text{Oliver U.}}\\
i(\texttt{matka}) &= \{(\faFemale_{\text{Adela U.}}, \faFemale_{\text{Magdaléna U.}}), (\faMale_{\text{Oliver U.}}, \faFemale_{\text{Magdaléna U.}}),\\
&\qquad (\faFemale_{\text{Magdaléna U.}}, \faFemale_{\text{Iveta T.}}), (\faFemale_{\text{Iveta T.}}, \faGlobe), (\faGlobe, \faGlobe)\}\\
i(\texttt{žena}) &= \{\faFemale_{\text{Magdaléna U.}}, \faFemale_{\text{Iveta T.}}, \faFemale_{\text{Adela U.}}, \faGlobe\}\\
i(\texttt{rodič}) &= \{(\faFemale_{\text{Magdaléna U.}}, \faFemale_{\text{Adela U.}}), (\faFemale_{\text{Magdaléna U.}}, \faMale_{\text{Oliver U.}}),\\
&\qquad (\faFemale_{\text{Iveta T.}}, \faFemale_{\text{Magdaléna U.}}), (\faGlobe, \faFemale_{\text{Iveta T.}}), (\faGlobe, \faGlobe)\}
\end{aligned}$$

Zmena definície štruktúry neovplyvňuje ohodnotenia premenných

Definícia 3.40. Nech $\mathcal{M} = (M, i)$ je štruktúra pre jazyk logiky prvého rádu $\mathcal{L}$.
Ohodnotenie (indivíduových) premenných je ľubovoľná funkcia $e\colon \mathcal{V}_{\mathcal{L}} \to M$ (priraďuje premenným prvky domény).

Zápisom $e(x/v)$ označíme ohodnotenie indivíduových premenných, ktoré priraďuje premennej x hodnotu v z domény M [teda $e(x/v)(x) = v$] a všetkým ostatným premenným rovnakú hodnotu ako e [teda $e(x/v)(y) = e(y)$].

Príklad 3.41. Nech $\mathcal{V}_{\mathcal{L}} = \{x, y\}$ a nech $\mathcal{M} = (\{\faFemale_{\text{Magdaléna U.}}, \faFemale_{\text{Adela U.}}, \faMale_{\text{Oliver U.}}\}, i)$.
Potom ohodnotením indivíduových premenných je napríklad

$$e = \{x \mapsto \faFemale_{\text{Magdaléna U.}}, y \mapsto \faFemale_{\text{Adela U.}}\}$$

$$\text{a } e(y/\faMale_{\text{Oliver U.}}) = \{x \mapsto \faFemale_{\text{Magdaléna U.}}, y \mapsto \faMale_{\text{Oliver U.}}\}$$

IX.20 Hodnota termu

Termy s funkčnými symbolmi môžu byť vnorené,
vyhodnocujeme ich rekurzívne

Definícia 3.42. Nech $\mathcal{M} = (M, i)$ je štruktúra pre jazyk logiky prvého rádu $\mathcal{L}$,
nech e je ohodnotenie premenných.
Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e
je prvok z M označovaný $t^{\mathcal{M}}[e]$ a zadefinovaný induktívne nasledovne:

$$x^{\mathcal{M}}[e] = e(x), \text{ ak } x \text{ je premenná,}$$

$$a^{\mathcal{M}}[e] = i(a), \text{ ak } a \text{ je konštanta,}$$

$$\big(f(t_1, \dots, t_n)\big)^{\mathcal{M}}[e] = i(f)(t_1^{\mathcal{M}}[e], \dots, t_n^{\mathcal{M}}[e]), \textit{ ak } t_1, \dots, t_n \textit{ sú termy.}$$

IX.21 Hodnota termov

Príklad 3.43. Vyhodnoťme termy

$$\begin{aligned} t_1 &= \mathsf{Adelka}, & t_3 &= \mathsf{matka}(\mathsf{Adelka}),\\ t_2 &= x, & t_4 &= \mathsf{matka}(y),\\ & & t_5 &= \mathsf{matka}(\mathsf{matka}(\mathsf{Oliverko})) \end{aligned}$$

v štruktúre z príkladu 3.39 pri ohodnotení
$e = \{x \mapsto \text{Oliver U.}, y \mapsto \text{Magdaléna U.}, \dots\}$.

Riešenie.

$$t_1^{\mathcal{M}}[e] = \mathsf{Adelka}^{\mathcal{M}}[e] = i(\mathsf{Adelka}) = \text{Adela U.}$$
$$t_2^{\mathcal{M}}[e] = x^{\mathcal{M}}[e] = e(x) = \text{Oliver U.}$$
$$t_3^{\mathcal{M}}[e] = \big(\mathsf{matka}(\mathsf{Adelka})\big)^{\mathcal{M}}[e] = i(\mathsf{matka})(i(\mathsf{Adelka})) = \text{Magdaléna U.}$$
$$t_4^{\mathcal{M}}[e] = \big(\mathsf{matka}(y)\big)^{\mathcal{M}}[e] = i(\mathsf{matka})(e(y)) = \text{Iveta T.}$$
$$\begin{aligned} t_5^{\mathcal{M}}[e] &= \big(\mathsf{matka}(\mathsf{matka}(\mathsf{Oliverko}))\big)^{\mathcal{M}}[e]\\ &= i(\mathsf{matka})(i(\mathsf{matka})(i(\mathsf{Oliverko}))) = \text{Iveta T.} \end{aligned}$$

IX.22 Splnenie formuly v štruktúre

Definícia 3.44. 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 induktívnu definíciu:

- $\mathcal{M} \models t_1 \doteq t_2[e]$ vtt $t_1^{\mathcal{M}}[e] = t_2^{\mathcal{M}}[e]$,
- $\mathcal{M} \models P(t_1, \ldots, t_n)[e]$ vtt $\big(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e]\big) \in i(P)$,
- $\mathcal{M} \models \neg A[e]$ vtt $\mathcal{M} \not\models A[e]$,
- $\mathcal{M} \models (A \land B)[e]$ vtt $\mathcal{M} \models A[e]$ a zároveň $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \lor B)[e]$ 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 $t_1, t_2, \ldots, t_n$, všetky premenné x a všetky formuly A, B.

IX.23 Splnenie formuly v štruktúre

Príklad 3.45. Zistime, či sú v štruktúre z príkladu 3.39 splnené formuly:

- $\mathtt{rodič}(\mathtt{matka}(\mathtt{Adelka}), \mathtt{Oliverko})$,
- $\neg(\mathtt{matka}(\mathtt{Oliverko}) \doteq y)$,
- $\big(\mathtt{rodič}(x, y) \rightarrow \mathtt{žena}(y)\big)$.
- $\forall x\, \forall y\, (\mathtt{rodič}(x, y) \land \mathtt{žena}(x) \leftrightarrow \mathtt{matka}(y) \doteq x)$.

pri ohodnotení $e_1 = \{x \mapsto {}_{\text{Magdaléna U.}}, y \mapsto {}_{\text{Iveta T.}}, \ldots\}$.

IX.24 Splnenie množiny formúl

Definícia 3.46. 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 $\mathcal{M} \models X[e]$.

IX.25 Splniteľnosť, nesplniteľnosť, platnosť

Definícia 3.47. 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.

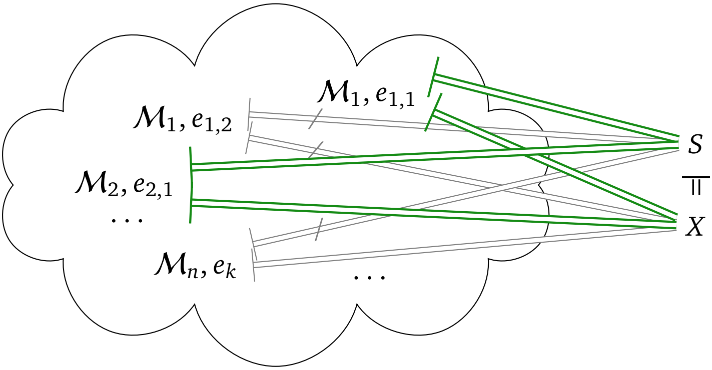
Množina formúl S je *splniteľná* vtt aspoň jedna štruktúra $\mathcal{M}$ pre $\mathcal{L}$ spĺňa S pri aspoň jednom ohodnotení e.

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

Definícia 3.48. 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.

IX.26 Prvorádové vyplývanie

Definícia 3.49. Nech X je formula v jazyku $\mathcal{L}$, nech S je množina formúl v jazyku $\mathcal{L}$.
Formula X *(prvorádovo) vyplýva* z S
(tiež X je *logickým dôsledkom* 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.



3.5. Voľné a viazané premenné

IX.27 Oblasť platnosti kvantifikátora

Dohoda 3.50. Nech $\mathcal{L}$ je ľubovoľný jazyk logiky prvého rádu. Všetky symboly, termy a formuly v nasledujúcich definíciách a tvrdeniach sú v jazyku $\mathcal{L}$.

Definícia 3.51 (Oblasť platnosti kvantifikátora)**.** Nech A je postupnosť symbolov, nech B je formula, nech $Q \in \{\forall, \exists\}$, nech x je premenná.
V postupnosti $A = \dots Q x\, B \dots$ sa výskyt formuly $Q x\, B$
nazýva *oblasť platnosti kvantifikátora* Qx *v* A.

Príklad 3.52. Vyznačme všetky oblasti platnosti kvantifikátora $\forall x$ vo formule

$$\forall x\, P(x) \land R(x, x) \to \forall x(R(x, y) \land \exists y\, P(y)) \lor \forall y\, P(y).$$

Riešenie. $\forall x\, P(x) \land R(x, x) \to \forall x(R(x, y) \land \exists y\, P(y)) \lor \forall y\, P(y)$

IX.28 Voľné a viazané výskyty premenných

Definícia 3.53 (Voľné a viazané výskyty premenných)**.** Nech A je postupnosť symbolov, nech x je premenná.

Výskyt premennej x v A je *viazaný* vtt sa *nachádza v niektorej* oblasti platnosti kvantifikátora $\forall x$ alebo $\exists x$ v A.

Výskyt premennej x A je *voľný* vtt sa *nenachádza v žiadnej* oblasti platnosti kvantifikátora $\forall x$ ani $\exists x$ v A.

Príklad 3.54.

$$
\begin{aligned}
&\neg\mathtt{richer}(x, y) \land \mathtt{hates}(x, y)\\
&\neg\mathtt{richer}(x, y) \land \exists \underline{y}\,\mathtt{hates}(x, \underline{y})\\
&\exists \underline{y}(\neg\mathtt{richer}(x, \underline{y}) \land \mathtt{hates}(x, \underline{y}))\\
&\forall \underline{x} \exists \underline{y}(\neg\mathtt{richer}(\underline{x}, \underline{y}) \land \mathtt{hates}(\underline{x}, \underline{y}))\\
&\forall \underline{x}(\neg\mathtt{richer}(\underline{x}, y) \land \exists \underline{y}\,\mathtt{hates}(\underline{x}, \underline{y}))
\end{aligned}
$$

IX.29 Voľné a viazané premenné

Definícia 3.55 (Voľné a viazané premenné)**.** Nech A je formula alebo term, nech x je premenná.

Premenná x je *viazaná* v A vtt x sa vyskytuje v A a *všetky* výskyty x v A sú viazané.

Premenná x je *voľná* v A vtt x má v A *aspoň jeden voľný výskyt*.

Množinu voľných premenných formuly A označíme $\mathrm{free}(A)$.

Príklad 3.56.

$$
\begin{aligned}
&\mathrm{free}(\neg\mathtt{richer}(x, y) \land \mathtt{hates}(z, y)) = \{x, y, z\}\\
&\mathrm{free}(\neg\mathtt{richer}(x, y) \land \exists \underline{y}\,\mathtt{hates}(z, \underline{y})) = \{x, y, z\}\\
&\mathrm{free}(\exists \underline{y}(\neg\mathtt{richer}(x, \underline{y}) \land \mathtt{hates}(z, \underline{y}))) = \{x, z\}\\
&\mathrm{free}(\exists \underline{y}(\neg\mathtt{richer}(x, \underline{y}) \land \forall \underline{z}\,\mathtt{hates}(\underline{z}, \underline{y}))) = \{x\}\\
&\mathrm{free}(\exists \underline{y} \exists \underline{z}(\forall \underline{x} \neg\mathtt{richer}(\underline{x}, \underline{y}) \land \mathtt{hates}(\underline{z}, \underline{y}))) = \{\}
\end{aligned}
$$

IX.30 Voľné a viazané premenné

Tvrdenie 3.57. *Pre každú indivíduovú premennú x, každý symbol konštanty a, každú aritu $n > 0$, každý funkčný symbol f s aritou n, každý predikátový symbol P s aritou n, všetky termy $t_1, t_2, \ldots, t_n$ a všetky formuly A, B platí:*

$$
\begin{aligned}
\mathrm{free}\big(\, x \,\big) &= \{x\} \\
\mathrm{free}\big(\, a \,\big) &= \{\} \\
\mathrm{free}\big(\, f(t_1, \ldots, t_n) \,\big) &= \mathrm{free}(t_1) \cup \cdots \cup \mathrm{free}(t_n) \\
\mathrm{free}\big(\, t_1 \doteq t_2 \,\big) &= \mathrm{free}(t_1) \cup \mathrm{free}(t_2) \\
\mathrm{free}\big(\, P(t_1, \ldots, t_n) \,\big) &= \mathrm{free}(t_1) \cup \cdots \cup \mathrm{free}(t_n) \\
\mathrm{free}\big(\, \neg A \,\big) &= \mathrm{free}(A) \\
\mathrm{free}\big(\, A \land B \,\big) &= \mathrm{free}\big(\, A \lor B \,\big) = \mathrm{free}\big(\, A \to B \,\big) = \mathrm{free}(A) \cup \mathrm{free}(B) \\
\mathrm{free}\big(\, \forall x\, A \,\big) &= \mathrm{free}\big(\, \exists x\, A \,\big) = \mathrm{free}(A) \setminus \{x\}
\end{aligned}
$$

IX.31 Voľné premenné a splnenie formuly

Tvrdenie 3.58. *Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech e_1 a e_2 sú ohodnotenia, nech X je formula jazyka $\mathcal{L}$, nech S je množina formúl jazyka $\mathcal{L}$.*

- *Ak sa ohodnotenia e_1 a e_2 zhodujú na voľných premenných formuly X (teda $e_1(x) = e_2(x)$ pre každú $x \in \mathrm{free}(X)$), tak $\mathcal{M} \models X[e_1]$ vtt $\mathcal{M} \models X[e_2]$.*
- *Ak sa ohodnotenia e_1 a e_2 zhodujú na voľných premenných všetkých formúl z S, tak $\mathcal{M} \models S[e_1]$ vtt $\mathcal{M} \models S[e_2]$.*

Inými slovami: Splnenie formuly (množiny formúl) v štruktúre závisí iba od ohodnotenia jej voľných premenných.

IX.32 Uzavreté formuly a teórie

Definícia 3.59 (Uzavretá formula, teória)**.** Formula A jazyka $\mathcal{L}$ je *uzavretá* vtt neobsahuje žiadne voľné výskyty premenných (teda $\mathrm{free}(x) = \emptyset$).

Teóriou v jazyku $\mathcal{L}$ je každá spočítateľná množinu uzavretých formúl jazyka $\mathcal{L}$.

Tvrdenie 3.60. *Nech X je* uzavretá *formula jazyka $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech e_1 a e_2 sú ohodnotenia. Potom $\mathcal{M} \models X[e_1]$ vtt $\mathcal{M} \models X[e_2]$.*

Neformálnejšie:
Splnenie uzavretej formuly v štruktúre nezávisí od ohodnotenia.

IX.33 Splnenie formuly a množiny formúl v štruktúre

Definícia 3.61 (Splnenie v štruktúre)**.** Nech X je formula jazyka $\mathcal{L}$, nech S je množina formúl jazyka $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.

Štruktúra $\mathcal{M}$ spĺňa formulu X (skrátene $\mathcal{M} \models X$) vtt štruktúra $\mathcal{M}$ spĺňa X pri *každom ohodnotení e*.

Štruktúra $\mathcal{M}$ spĺňa množinu S (skrátene $\mathcal{M} \models S$) vtt pre každú formulu A z S platí $\mathcal{M} \models A$.

IX.34 Nezávislosť od ohodnotení

Dôsledok 3.62. *Nech X je uzavretá formula jazyka $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.*
Potom sú nasledujúce tvrdenia ekvivalentné:

a) $\mathcal{M} \models X$ (teda $\mathcal{M} \models X[e]$ pre každé e),

b) $\mathcal{M} \models X[e]$ pri aspoň jednom ohodnotení e.

Dôsledok 3.63. *Nech T je teória v jazyku $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.*
Potom sú nasledujúce tvrdenia ekvivalentné:

a) $\mathcal{M} \models T$,

b) $\mathcal{M} \models T[e]$ pre všetky ohodnotenia e,

c) $\mathcal{M} \models T[e]$ pre aspoň jedno ohodnotenie e.

3.6. Substitúcia

IX.35 Substitúcia

Definícia 3.64 (Substitúcia). *Substitúciou* (v jazyku $\mathcal{L}$) nazývame každé zobrazenie $\sigma\colon V \to \mathcal{T}_{\mathcal{L}}$ z nejakej množiny indivíduových premenných $V \subseteq \mathcal{V}_{\mathcal{L}}$ do termov jazyka $\mathcal{L}$.

Príklad 3.65. Keď $\mathcal{V}_{\mathcal{L}} = \{u, v, \dots, z\}$, $\mathcal{C}_{\mathcal{L}} = \{\mathtt{Adelka}, \mathtt{Oliverko}\}$, $\mathcal{F}_{\mathcal{L}} = \{\mathtt{matka}^1\}$,
napríklad $\sigma_1 = \{x \mapsto \mathtt{Adelka}, y \mapsto \mathtt{matka}(u)\}$ je substitúcia.

IX.36 Problémy s dosadzovaním

Substitúcie chceme použiť na dosádzanie za premenné v termoch a formulách.

Musíme si však dať pozor na niektoré špeciálne prípady:

Príklad 3.66. Nech $A = \exists y\,(\mathtt{rodič}(y, x) \land x \neq y)$ a nech $B = \forall x\, A$.

- B hovorí, že každý má rodiča, ktorým nie je ona sama/on sám
- B je splniteľná
- Ak $\mathcal{M} \models B$, tak $\mathcal{M} \models A\,[e(x/m)]$ pre každé $m \in \mathcal{M}$
- Keby sme dosadili podľa $\sigma_2 = \{x \mapsto y\}$ do A,
  dostaneme $A' = \exists y(\mathtt{rodič}(y, y) \land y \neq y)$
- $\mathcal{M} \not\models A'\,[e]$ pre všetky e (dokonca je A' je nesplniteľná)
- A' **významovo nezodpovedá** A **pri žiadnom ohodnotení** e
- σ nezodpovedá žiadnemu ohodnoteniu e

IX.37 Substituovateľnosť a aplikovateľnosť substitúcie

Definícia 3.67 (Substituovateľnosť, aplikovateľnosť substitúcie)**.** Nech A postupnosť symbolov (term alebo formula), nech t je term, x je premenná, nech $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia.

Term t je *substituovateľný* za premennú x v A vtt pre žiadnu premennú y vyskytujúcu sa v t žiaden voľný výskyt premennej x v A sa nenachádza v oblasti platnosti kvantifikátora $\exists y$ ani $\forall y$ v A.

Substitúcia σ je *aplikovateľná* na A vtt term t_i je substituovateľný za x_i v A pre každé $i \in \{1, \ldots, n\}$.

IX.38 Substituovateľnosť a aplikovateľnosť substitúcie

Príklad 3.68. Nech $A = \exists \underline{y}\,(\mathtt{rodič}(x, \underline{y}) \land x \not\doteq \underline{y})$.

- Za premennú x *nie je substituovateľný* v A žiaden term, v ktorom sa vyskytuje y, napr. y, $\mathtt{matka}(y)$, …
- Substitúcie $\{x \mapsto y\}$, $\{x \mapsto \mathtt{matka}(y)\}$, … *nie sú aplikovateľné* na A

IX.39 Substitúcia do postupnosti symbolov

Definícia 3.69 (Substitúcia do postupnosti symbolov)**.** Nech A je postupnosť symbolov, nech $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia.
Ak σ je aplikovateľná na A, tak $A\sigma$ je postupnosť symbolov, ktorá vznikne *súčasným* dosadením t_i za každý *voľný* výskyt premennej x_i v A.

Príklad 3.70. Nech $A = \exists \underline{y}\,(\mathtt{rodič}(x, \underline{y}) \land x \not\doteq \underline{y})$,

$$\sigma = \{x \mapsto \mathtt{matka}(\mathtt{Oliverko}), \underline{y} \mapsto z\}.$$

Substitúcia σ *je aplikovateľná* na A. V A je voľná iba premenná x, dosadíme za ňu term $\mathtt{matka}(\mathtt{Oliverko})$, ktorý neobsahuje premenné. Všetky výskyty y sú viazané, za ne sa nedosádza.

$$A\sigma = \exists \underline{y}\,(\mathtt{rodič}(\mathtt{matka}(\mathtt{Oliverko}), \underline{y}) \land \mathtt{matka}(\mathtt{Oliverko}) \not\doteq \underline{y})$$

IX.40 Substitúcia do termov a formúl rekurzívne

Tvrdenie 3.71. *Pre každú substitúciu* $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$, *každú premennú* $y \in \mathcal{V}_\mathcal{L} \setminus \{x_1, \dots, x_n\}$, *každý symbol konštanty* $a \in \mathcal{C}_\mathcal{L}$, *každý funkčný symbol* $f^k \in \mathcal{P}_\mathcal{L}$, *každý predikátový symbol* $P^k \in \mathcal{P}_\mathcal{L}$, *každé* $i \in \{1, \dots, n\}$, *každú spojku* $\diamond \in \{\land, \lor, \to\}$, *všetky formuly* A *a* B *a všetky termy* $s_1, s_2, \dots, s_k \in \mathcal{T}_\mathcal{L}$ *platí:*

$$
\begin{aligned}
&x_i\sigma = t_i \qquad y\sigma = y \qquad a\sigma = a & (f(s_1, \dots, s_k))\sigma &= f(s_1\sigma, \dots, s_k\sigma) \\
&(s_1 \doteq s_2)\sigma = (s_1\sigma \doteq s_2\sigma) & (P(s_1, \dots, s_k))\sigma &= P(s_1\sigma, \dots, s_k\sigma) \\
&(\neg A)\sigma = \neg(A\sigma) & ((A \diamond B))\sigma &= (A\sigma \diamond B\sigma) \\
&(\forall y\, A)\sigma = \forall y\, (A\sigma) & (\exists y\, A)\sigma &= \exists y\, (A\sigma) \\
&(\forall x_i\, A)\sigma = \forall x_i\, (A\sigma_i) & (\exists x_i\, A)\sigma &= \exists x_i\, (A\sigma_i),
\end{aligned}
$$

kde $\sigma_i = \sigma \setminus \{x_i \mapsto t_i\}$.

IX.41 Substituovateľnosť a substitúcia

Príklad 3.72. Nech $\sigma_1 = \{x \mapsto a, y \mapsto f(a, x, y)\}$.
Potom $\big(g\big(g(a, x), f(z, y, b)\big)\big)\sigma_1 = g\big(g(a, a), f(z, f(a, x, y), b)\big)$.

Príklad 3.73. Nech $\sigma_2 = \{x \mapsto \mathtt{matka}(y), y \mapsto \mathtt{Adelka}\}$. Potom

- $(\mathtt{rodič}(x, y) \to \mathtt{má\_rád}(y, x))\sigma_2 =$
  $\mathtt{rodič}(\mathtt{matka}(y), \mathtt{Adelka}) \to \mathtt{má\_rád}(\mathtt{Adelka}, \mathtt{matka}(y))$;
- $(\exists x\, \mathtt{rodič}(x, y))\sigma_2 = \exists x\, \mathtt{rodič}(x, \mathtt{Adelka})$;
- σ_2 nie je aplikovateľná na $\exists y\, \mathtt{rodič}(y, x)$;
  všimnite si zmenu významu, keby sme za x dosadili $\mathtt{matka}(y)$:
  $\exists y\, \mathtt{rodič}(y, \mathtt{matka}(y))$.

IX.42 Substitúcia a hodnota termu

Príklad 3.74. Zoberme štruktúru $\mathcal{M} = (M, i)$, kde

$$\begin{aligned}
M &= \{\text{♀}_{\text{Magdaléna U.}}, \text{♀}_{\text{Iveta T.}}, \text{♀}_{\text{Adela U.}}, \text{♂}_{\text{Oliver U.}}, \text{🌍}\}, \\
i(\mathtt{Adelka}) &= \text{♀}_{\text{Adela U.}}, \qquad i(\mathtt{Oliverko}) = \text{♂}_{\text{Oliver U.}} \\
i(\mathtt{matka}) &= \{(\text{♀}_{\text{Adela U.}}, \text{♀}_{\text{Magdaléna U.}}), (\text{♂}_{\text{Oliver U.}}, \text{♀}_{\text{Magdaléna U.}}), \\
&\qquad (\text{♀}_{\text{Magdaléna U.}}, \text{♀}_{\text{Iveta T.}}), (\text{♀}_{\text{Iveta T.}}, \text{🌍}), (\text{🌍}, \text{🌍})\}
\end{aligned}$$

Nech $e = \{x \mapsto \text{♀}_{\text{Adela U.}}, y \mapsto \text{♂}_{\text{Oliver U.}}\}$, $\quad \sigma_1 = \{x \mapsto \mathtt{matka}(y)\}$.
Ako mení substitúcia **hodnotu** termu?

$$\begin{aligned}
((\mathtt{matka}(x))\sigma_1)^{\mathcal{M}}[e] &= (\mathtt{matka}(\mathtt{matka}(y)))^{\mathcal{M}}[e] \\
&= i(\mathtt{matka})(i(\mathtt{matka})(\text{♂}_{\text{Oliver U.}})) = i(\mathtt{matka})(\text{♂}_{\text{Magdaléna U.}}) = \text{♀}_{\text{Iveta T.}} \\
&= (\mathtt{matka}(x))^{\mathcal{M}}[e(x/\text{♀}_{\text{Magdaléna U.}})] \\
&= (\mathtt{matka}(x))^{\mathcal{M}}[e(x/(\mathtt{matka}(y))^{\mathcal{M}}[e])]
\end{aligned}$$

IX.43 Substitúcia a hodnota termu

Hodnota termu $t\sigma$ po substitúcii $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ pri ohodnotení e
sa rovná hodnote pôvodného termu t pri takom ohodnotení e', ktoré

- každej substituovanej premennej x_i
  priradí hodnotu za ňu substituovaného termu t_i pri ohodnotení e,
- ostatným premenným priraďuje rovnaké hodnoty ako e.

Tvrdenie 3.75. *Nech $\mathcal{M}$ je štruktúra pre jazyk $\mathcal{L}$, e je ohodnotenie premenných, t je term a $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia.
Potom $(t\sigma)^{\mathcal{M}}[e] = t^{\mathcal{M}}[e(x_1/t_1^{\mathcal{M}}[e]) \cdots (x_n/t_n^{\mathcal{M}}[e])]$.*

IX.44 Substitúcia a splnenie formuly

Tvrdenie 3.76. *Nech A je formula jazyka $\mathcal{L}$ a nech $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia aplikovateľná na A. Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a nech e je ohodnotenie indivíduových premenných.
Potom $\mathcal{M} \models A\sigma[e]$ vtt $\mathcal{M} \models A[e(x_1/t_1^{\mathcal{M}}[e]) \cdots (x_n/t_n^{\mathcal{M}}[e])]$.*

Inak povedané: Štruktúra spĺňa formulu $A\sigma$ po substitúcii pri ohodnotení e vtt spĺňa pôvodnú formulu A pri takom ohodnotení e', ktoré každej substituovanej premennej x_i priradí hodnotu za ňu substituovaného termu t_i pri ohodnotení e a ostatným premenným priraďuje rovnaké hodnoty ako e.

3.7. Tablá pre logiku prvého rádu

IX.45 Dokazovanie vyplývania a platnosti

- Nájdením štruktúry a ohodnotenia vieme ukázať splniteľnosť, neplatnosť, nevyplývanie
- Ako ale ukážeme vyplývanie, platnosť, nesplniteľnosť?
- Podľa definícií vyžadujú skúmanie *všetkých štruktúr a ohodnotení* — nekonečne veľa možností
- Pokúsme sa ale o dôkaz

IX.46 Dokazovanie vyplývania

Príklad 3.77. Dokážme, že $\{\exists x\,\text{muž}(x) \land \exists x\,\text{žena}(x)\} \models \exists x(\text{muž}(x) \lor \text{žena}(x))$,
teda že pre každú štruktúru $\mathcal{M}$ a každé ohodnotenie e:
Ak $\mathcal{M} \models \{\exists x\,\text{muž}(x) \land \exists x\,\text{žena}(x)\}\,[e]$, tak $\mathcal{M} \models \exists x(\text{muž}(x) \lor \text{žena}(x))\,[e]$.

Sporom: Predpokladajme, že tvrdenie neplatí,
teda v *nejakej* štruktúre $\mathcal{M} = (M, i)$ a pri *nejakom* ohodnotení e,
(1) $\mathcal{M} \models \{\exists x\,\text{muž}(x) \land \exists x\,\text{žena}(x)\}\,[e]$, ale (2) $\mathcal{M} \not\models \exists x(\text{muž}(x) \lor \text{žena}(x))\,[e]$.

Podľa (1) máme (3) $\mathcal{M} \models \exists x\,\text{muž}(x)\,[e]$ a (4) $\mathcal{M} \models \exists x\,\text{žena}(x)\,[e]$.
Podľa (3) $\mathcal{M} \models \text{muž}(x)\,[e(x/m_1)]$ pre nejaké $m_1 \in M$,
teda (5) $\mathcal{M} \models \text{muž}(y)\,[e']$, kde y je nová premenná a $e' = e(y/m_1)$.
Podľa (4) podobne $\mathcal{M} \models \text{žena}(x)\,[e(x/m_2)]$ pre nejaké $m_2 \in M$
(m_2 je pravdepodobne *iné* ako m_1!),
teda (6) $\mathcal{M} \models \text{žena}(z)\,[e'']$, kde z je nová premenná a $e'' = e(z/m_2)$.

Podľa (2) ale $\mathcal{M} \not\models \text{muž}(x) \vee \text{žena}(x)\,[e(x/m)]$ pre všetky $m \in M$, teda aj $\mathcal{M} \not\models \text{muž}(x) \vee \text{žena}(x)\,[e(x/m_2)]$, čiže (7) $\mathcal{M} \not\models \text{muž}(z) \vee \text{žena}(z)\,[e'']$. Potom ale (8) $\mathcal{M} \not\models \text{muž}(z)\,[e'']$ a (9) $\mathcal{M} \not\models \text{žena}(z)\,[e'']$, čo je však v spore s (6).

X. prednáška

Korektnosť tabiel pre logiku prvého rádu

30. apríla 2018

X.1 Splnenie označených formúl, vyplývanie

Podobne ako vo výrokovej logike môžeme zaviesť označovanie formúl logiky prvého rádu znamienkami **T** a **F**.

Definícia 3.78. Nech $\mathcal{M}$ je štruktúra pre jazyk $\mathcal{L}$, nech e je ohodnotenie indivíduových premenných, nech X je formula jazyka $\mathcal{L}$. Potom:

- $\mathcal{M} \models \mathbf{T}\, X[e]$ vtt $\mathcal{M} \models X[e]$;
- $\mathcal{M} \models \mathbf{F}\, X[e]$ vtt $\mathcal{M} \not\models X[e]$.

Splnenie množiny označených formúl a *splniteľnosť* ozn. formuly/množiny ozn. formúl definujeme analogicky ako pre neoznačené formuly.

Tvrdenie 3.79. *Nech X je formula a S je množina formúl v jazyku $\mathcal{L}$. Formula X prvorádovo vyplýva z S vtt množina $\{\, \mathbf{T}\, Y \mid Y \in S \,\} \cup \{\mathbf{F}\, X\}$ je prvorádovo súčasne nesplniteľná.*

X.2 Jednotný zápis označených formúl — α a β

Pre všetky definície odteraz zvoľme pevne ľubovoľný jazyk logiky prvého rádu $\mathcal{L}$.

Definícia 3.80 (Jednotný zápis označených formúl typu α)**.** Označená formula je *typu* α vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly A a B. Takéto formuly označujeme písmenom α; α_1 označuje príslušnú formulu zo stredného stĺpca a α_2 príslušnú formulu z pravého stĺpca.

α	α_1	α_2
$\mathbf{T}(A \land B)$	$\mathbf{T}A$	$\mathbf{T}B$
$\mathbf{F}(A \lor B)$	$\mathbf{F}A$	$\mathbf{F}B$
$\mathbf{F}(A \to B)$	$\mathbf{T}A$	$\mathbf{F}B$
$\mathbf{T}\,\neg A$	$\mathbf{F}A$	$\mathbf{F}A$
$\mathbf{F}\,\neg A$	$\mathbf{T}A$	$\mathbf{T}A$

Definícia 3.81 (Jednotný zápis označených formúl typu β).
Označená formula je *typu* β vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly A a B. Takéto formuly označujeme písmenom β; β_1 označuje príslušnú formulu zo stredného stĺpca a β_2 príslušnú formulu z pravého stĺpca.

β	β_1	β_2
$\mathbf{F}(A \land B)$	$\mathbf{F}A$	$\mathbf{F}B$
$\mathbf{T}(A \lor B)$	$\mathbf{T}A$	$\mathbf{T}B$
$\mathbf{T}(A \to B)$	$\mathbf{F}A$	$\mathbf{T}B$

X.3 Jednotný zápis označených formúl — γ a δ

Definícia 3.82 (Jednotný zápis označených formúl typu γ).
Označená formula je *typu* γ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejakú formulu A a indivíduovú premennú x. Takéto formuly označujeme $\gamma(x)$ a pre ľubovoľný term t substituovateľný za x v A príslušnú formulu z pravého stĺpca označujeme $\gamma_1(t)$.

$\gamma(x)$	$\gamma_1(t)$
$\mathbf{F}\,\exists x\, A$	$\mathbf{F}A\{x \mapsto t\}$
$\mathbf{T}\,\forall x\, A$	$\mathbf{T}A\{x \mapsto t\}$

Definícia 3.83 (Jednotný zápis označených formúl typu δ).
Označená formula je *typu* δ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejakú formulu A a indivíduovú premennú x. Takéto formuly označujeme $\delta(x)$ a pre ľubovoľnú premennú y substituovateľnú za x v A príslušnú formulu z pravého stĺpca označujeme $\delta_1(y)$.

$\delta(x)$	$\delta_1(y)$
$\mathbf{T}\,\exists x\, A$	$\mathbf{T}A\{x \mapsto y\}$
$\mathbf{F}\,\forall x\, A$	$\mathbf{F}A\{x \mapsto y\}$

X.4 Rovnosť

- Pravidlá pre α a β formuly umožňujú pracovať s logickými spojkami
- Pravidlá pre γ a δ formuly umožňujú pracovať s kvantifikátormi.
- V jazyku je ešte jeden logický symbol — rovnosť ($\doteq$)
- Žiadne pravidlo s ňou zatiaľ nepracuje
- Čo potrebujeme, aby rovnosť mala očakávané vlastnosti?

X.5 Axiomatizácia rovnosti

- Rovnosť by sme mohli popísať teóriou — *axiomatizovať* ju
- Je reflexívna, symetrická a tranzitívna:

$$\forall x\, x \doteq x$$
$$\forall x\, \forall y (x \doteq y \to y \doteq x)$$
$$\forall x\, \forall y\, \forall z (x \doteq y \land y \doteq z \to x \doteq z)$$

- Navyše má vlastnosť substitúcie alebo *kongruencie*:

  Pre každý pár rovnajúcich sa k-tic argumentov:

  - hodnota každého funkčného symbolu f^k je rovnaká,
  - každý predikátový symbol P^k je
    na oboch k-tiach splnený alebo na oboch nesplnený.

$$\begin{aligned}\forall x_1\, \forall y_1 \ldots \forall x_k\, \forall y_k \big(x_1 \doteq y_1 \land \cdots \land x_k \doteq y_k \to{} \\ f(x_1, \ldots, x_k) \doteq f(y_1, \ldots, y_k)\big)\end{aligned}$$
$$\begin{aligned}\forall x_1\, \forall y_1 \ldots \forall x_k\, \forall y_k \big(x_1 \doteq y_1 \land \cdots \land x_k \doteq y_k \to{} \\ (P(x_1, \ldots, x_k) \leftrightarrow P(y_1, \ldots, y_k))\big)\end{aligned}$$

X.6 Dôkazy s axiomatizovanou rovnosťou

- Skúsme niečo dokázať:

1. $\mathbf{T}\, \mathtt{matka}(\mathtt{Oliverko}) \doteq \mathtt{Magda}$ $\quad S^+$
2. $\mathbf{T}\, \exists x\, \mathtt{prvé\_dieťa}(\mathtt{matka}(\mathtt{Oliverko}), x) \doteq \mathtt{Adelka}$ $\quad S^+$
3. $\mathbf{F}\, \exists x\, \mathtt{prvé\_dieťa}(\mathtt{Magda}, x) \doteq \mathtt{Adelka}$ $\quad S^+$

$\ldots$

X.7 Eulerovo pravidlo

- Dôkazy s axiómami rovnosti sú prácne aj v jednoduchých prípadoch
- Vlastnosť kongruencie sa však dá induktívne zovšeobecniť na ľubovoľné formuly
- *Eulerovo pravidlo*: V každej formule môžeme nahradiť rovné rovným

1.	$\mathbf{T}\,\mathtt{matka}(\mathtt{Oliverko}) \doteq \mathtt{Magda}$	S^+
2.	$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(\mathtt{matka}(\mathtt{Oliverko}), x) \doteq \mathtt{Adelka}$	S^+
3.	$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(\mathtt{Magda}, x) \doteq \mathtt{Adelka}$	Euler 1, 2

- Ale *naozaj*?

$$\mathbf{T}\,\mathtt{matka}(\mathtt{Oliverko}) \doteq x$$
$$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(\mathtt{matka}(\mathtt{Oliverko}), x) \doteq \mathtt{Adelka}$$
$$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(x, x) \doteq \mathtt{Adelka}$$ ***partenogenéza?!?***

X.8 Eulerovo pravidlo presne

- *Eulerovo pravidlo*: V každej formule môžeme nahradiť rovné rovným
- Čo znamená „nahradiť“? A kedy to môžeme urobiť *bez zmeny významu* formuly?
- Substitúcia $\{x \mapsto t\}$ nahrádza premennú termom
- Eulerovo pravidlo potrebuje nahradiť jeden term t_1 druhým t_2
- Dá sa to popísať substitúciami? Áno:

- Chceme nahradiť term $t_1 = \texttt{matka(Oliverko)}$ termom $t_2 = \texttt{Magda}$ vo formule:

$$\begin{aligned} A_1^+ &= \mathbf{T}\,\exists x\, \texttt{prvé\_dieťa}(\texttt{matka(Oliverko)}, x) \doteq \texttt{Adelka} \\ &= A^+\{q \mapsto \texttt{matka(Oliverko)}\} \\ A^+ &= \mathbf{T}\,\exists x\, \texttt{prvé\_dieťa}(q, x) \doteq \texttt{Adelka} \\ A_2^+ &= A^+\{q \mapsto \texttt{Magda}\} \\ &= \mathbf{T}\,\exists x\, \texttt{prvé\_dieťa}(\texttt{Magda}, x) \doteq \texttt{Adelka} \end{aligned}$$

X.9 Eulerovo pravidlo — obmedzenia

- Vyjadrenie Eulerovho pravidla pomocou substitúcií:

$$\frac{\mathbf{T}\, t_1 \doteq t_2 \qquad A^+\{q \mapsto t_1\}}{A^+\{q \mapsto t_2\}}$$

- Automaticky dostávame aj *rozumné obmedzenia*

- **Nemôžeme** nahradiť term $t_1 = \texttt{matka(Oliverko)}$ termom $t_2 = \underline{x}$ vo formule:

$$\begin{aligned} A_1^+ &= \mathbf{T}\,\exists \underline{x}\, \texttt{prvé\_dieťa}(\texttt{matka(Oliverko)}, \underline{x}) \doteq \texttt{Adelka} \\ &= A^+\{q \mapsto \texttt{matka(Oliverko)}\} \\ A^+ &= \mathbf{T}\,\exists \underline{x}\, \texttt{prvé\_dieťa}(q, \underline{x}) \doteq \texttt{Adelka} \end{aligned}$$

lebo substitúcia $\{q \mapsto \underline{x}\}$ **nie je aplikovateľná** na A^+
($\underline{x}$ je viazané v mieste voľného výskytu q)

X.10 Vlastnosti rovnosti

- Eulerovo pravidlo odvodí symetriu, tranzitivitu aj kongruenciu

- Ale potrebuje pomocníčku — reflexivitu:

$$\frac{}{\mathbf{T}\, t_0 \doteq t_0}$$

- Symetriu potom odvodíme v table postupnosťou krokov:

1. $\mathbf{T}\, t_1 \doteq t_2$		
2. $\mathbf{T}\, t_1 \doteq t_1$	reflexivita	$A^+\{q \mapsto t_1\}$ pre $A^+ = \mathbf{T}\, q \doteq t_1$
3. $\mathbf{T}\, t_2 \doteq t_1$	Euler 1 a 2	$A^+\{q \mapsto t_2\}$

- Tranzitivitu odvodíme:

1. $\mathbf{T}\, t_1 \doteq t_2$		$A^+\{q \mapsto t_2\}$ pre $A^+ = \mathbf{T}\, t_1 \doteq q$
2. $\mathbf{T}\, t_2 \doteq t_3$		
3. $\mathbf{T}\, t_2 \doteq t_1$	Euler 2 a 1	$A^+\{q \mapsto t_3\}$

X.11 Tablové pravidlá pre logiku prvého rádu

Definícia 3.84. Tablovými pravidlami pre logiku prvého rádu sú:

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\alpha_2} \qquad\qquad \frac{\beta}{\beta_1 \mid \beta_2}$$

$$\frac{\gamma(x)}{\gamma_1(t)} \qquad\qquad \frac{\delta(x)}{\delta_1(y)}$$

$$\frac{}{\mathbf{T}\, t_0 \doteq t_0} \qquad\qquad \frac{\mathbf{T}\, t_1 \doteq t_2 \quad A^+\{x \mapsto t_1\}}{A^+\{x \mapsto t_2\}}$$

pre všetky ozn. formuly α, β, $\gamma(x)$, $\delta(x)$ príslušných typov a všetky im zodpovedajúce α_1, α_2, β_1, β_2, $\gamma_1(t)$ a $\delta_1(y)$, všetky termy t_0, všetky ozn. formuly A^+, všetky termy t_1 a t_2 substituovateľné za x do príslušnej A^+.

X.12 Tablo pre množinu označených formúl

Definícia 3.85. *Analytické tablo pre množinu* označených *formúl* S^+ (skrátene *tablo pre* S^+) je binárny strom, ktorého vrcholy obsahujú označené formuly
a ktorý je skonštruovaný induktívne podľa nasledovných pravidiel:

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

  A: Ak sa na vetve π_ℓ (ceste z koreňa do ℓ) vyskytuje nejaká označená formula α, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci α_1 alebo α_2.

  B: Ak sa na vetve π_ℓ vyskytuje nejaká označená formula β, tak ako deti ℓ pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2.

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

X.13 Tablo pre množinu označených formúl

Definícia 3.85 (pokračovanie)**.**

  C: Ak sa na vetve π_ℓ vyskytuje nejaká označená formula $\gamma(x)$, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $\gamma_1(t)$ pre ľubovoľný term t substituovateľný za x v $\gamma_1(x)$.

  D: Ak sa na vetve π_ℓ vyskytuje nejaká označená formula $\delta(x)$, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $\delta_1(y)$ pre ľubovoľnú premennú y, ktorá je substitovateľná za x v $\delta_1(x)$ a **nemá voľný výskyt** v žiadnej formule na vetve π_ℓ.

  E: Ak sa na vetve π_ℓ vyskytuje $\mathbf{T}\, t_1 \doteq t_2$ pre nejaké termy t_1 a t_2 a označená formula $A^+\{x \mapsto t_1\}$ pre nejakú A^+,
  v ktorej sú t_1 a t_2 substituovateľné za x,

tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $A^+\{x \mapsto t_2\}$.

Ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci označenú formulu $\mathbf{T}\, t \doteq t$ pre ľubovoľný term t.

3.8. Korektnosť tablového kalkulu pre logiku prvého rádu

X.14 Korektnosť tablových pravidiel

Tvrdenie 3.86. *Nech S je množina označených formúl v jazyku $\mathcal{L}$, nech x a y sú premenné, nech s, t sú termy, nech α, β, γ, δ sú ozn. formuly príslušného typu, A je ozn. formula.*

- *Ak $\alpha \in S$, tak S je splniteľná vtt $S \cup \{\alpha_1, \alpha_2\}$ je splniteľná.*
- *Ak $\beta \in S$,
tak S je splniteľná vtt $S \cup \{\beta_1\}$ je splniteľná alebo $S \cup \{\beta_2\}$ je splniteľná.*
- *Ak $\gamma(x) \in S$ a τ je term substituovateľný za x v $\gamma_1(x)$,
tak S je splniteľná vtt $S \cup \{\gamma_1(\tau)\}$ je splniteľná.*
- *Ak $\delta(x) \in S$, y je substituovateľná za x v $\delta_1(x)$
a y sa nemá voľný výskyt v S,
tak S je splniteľná vtt $S \cup \{\delta_1(y)\}$ je splniteľná.*
- *S je splniteľná vtt $S \cup \{\mathbf{T}\, t \doteq t\}$ je splniteľná.*
- *Ak $\{\mathbf{T}\, t_1 \doteq t_2, A^+\{x \mapsto t_1\}\} \subseteq S$, tak $S \cup \{A^+\{x \mapsto t_2\}\}$ je splniteľná.*

X.15 Korektnosť tablových pravidiel — dôkaz

Dôkaz (čiastočný, pre pravidlo δ v smere $\Rightarrow$). Zoberme ľubovoľné S, x, y, t a $\delta(x)$ spĺňajúce predpoklady tvrdenia. Nech S je splniteľná, teda existuje štruktúra $\mathcal{M}$ a ohodnotenie e také, že $\mathcal{M} \models S[e]$. Preto aj $\mathcal{M} \models \delta(x)[e]$. Podľa tvaru $\delta(x)$ môžu nastať nasledujúce dva prípady.

- Ak $\delta(x) = \mathbf{T}\,\exists x A$ pre nejakú formulu A, tak podľa def. 3.78 $\mathcal{M} \models \exists x A[e]$ a podľa def. 3.44 máme nejakého *svedka* $m \in M$ takého, že $\mathcal{M} \models A[e(x/m)]$. Podľa tvr. 3.76 potom $\mathcal{M} \models A\{x \mapsto y\}[e(x/m)(y/m)]$. Prem. x nie je voľná v $A\{x \mapsto y\}$, preto podľa tvr. 3.58 $\mathcal{M} \models A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \mathbf{T}\,A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \delta_1(y)[e(y/m)]$.

- Ak $\delta(x) = \mathbf{F}\,\forall y A$ pre nejakú formulu A, tak podľa def. 3.78 $\mathcal{M} \not\models \forall x A[e]$ a podľa def. 3.44 neplatí, že $\mathcal{M} \models A[e(x/m)]$ pre každé $m \in M$. Preto máme nejaký *kontrapríklad* $m \in M$ taký, že $\mathcal{M} \not\models A[e(x/m)]$. Podľa tvr. 3.76 potom $\mathcal{M} \not\models A\{x \mapsto y\}[e(x/m)(y/m)]$. Prem. x nie je voľná v $A\{x \mapsto y\}$, preto podľa tvr. 3.58 $\mathcal{M} \not\models A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \mathbf{F}\,A\{x \mapsto y\}[e(y/m)]$, čiže $\mathcal{M} \models \delta_1(y)[e(y/m)]$.

Navyše y nie je voľná v žiadnej formule z S, preto $\mathcal{M} \models S[e(y/m)]$. Teda $\mathcal{M} \models (S \cup \{\delta_1(y)\})[e(y/m)]$. Preto je $S \cup \{\delta_1(y)\}$ splniteľná. □

X.16 Korektnosť prvorádových tabiel

Otvorené a uzavreté vetvy a tablá sú definované rovnako ako pri tablách pre výrokovú logiku.

Veta 3.87 (Korektnosť tablového kalkulu). *Nech S^+ je množina označených formúl.*
Ak existuje uzavreté tablo $\mathcal{T}$ pre S^+, tak je množina S^+ nesplniteľná.

Dôkaz (nepriamy). Nech S^+ je množina označených formúl.
Nech S^+ je splniteľná. Dokážeme, že každé tablo $\mathcal{T}$ pre S^+ je otvorené, úplnou indukciou na počet vrcholov tabla $\mathcal{T}$.
... □

3.8.1. Ďalšie korektné pravidlá

X.17 Pohodlnejšie verzie pravidiel γ a δ

Tvrdenie 3.88. *Nasledujúce pravidlá sú korektné:*

$$\gamma^* \qquad \frac{\mathbf{T}\,\forall x_1 \dots \forall x_n\, A}{\mathbf{T}\, A\{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}} \qquad \frac{\mathbf{F}\,\exists x_1 \dots \exists x_n\, A}{\mathbf{F}\, A\{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}}$$

$$\delta^* \qquad \frac{\mathbf{F}\,\forall x_1 \dots \forall x_n\, A}{\mathbf{F}\, A\{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}} \qquad \frac{\mathbf{T}\,\exists x_1 \dots \exists x_n\, A}{\mathbf{T}\, A\{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}}$$

kde A je formula, $x_1, \dots, x_n$ sú premenné,
$t_1, \dots, t_n$ sú termy substituovateľné za príslušné $x_1, \dots, x_n$ v A
a $y_1, \dots, y_n$ sú premenné substituovateľné za príslušné $x_1, \dots, x_n$ v A
pričom $y_1, \dots, y_n$ sa ***nevyskytujú voľné*** *vo vetve, v liste ktorej je pravidlo použité.*

X.18 Pravidlá pre ekvivalenciu

Tvrdenie 3.89. *Nasledujúce pravidlá sú korektné:*

$$\mathit{ESTT} \quad \frac{\mathbf{T}(A_1 \leftrightarrow A_2) \quad \mathbf{T}\, A_i}{\mathbf{T}\, A_{3-i}} \qquad \mathit{ESTF} \quad \frac{\mathbf{T}(A_1 \leftrightarrow A_2) \quad \mathbf{F}\, A_i}{\mathbf{F}\, A_{3-i}}$$

$$\mathit{ESFT} \quad \frac{\mathbf{F}(A_1 \leftrightarrow A_2) \quad \mathbf{T}\, A_i}{\mathbf{F}\, A_{3-i}} \qquad \mathit{ESFF} \quad \frac{\mathbf{F}(A_1 \leftrightarrow A_2) \quad \mathbf{F}\, A_i}{\mathbf{T}\, A_{3-i}}$$

kde A_1 a A_2 sú formuly, $i \in \{1, 2\}$.

X.19 Dokazovanie s rovnosťou a explicitnými definíciami

- Využime nové pravidlá na dôkaz vlastnosti množín.
- Zoberme jazyk $\mathcal{L}$, kde $\mathcal{C}_\mathcal{L} = \{\emptyset\}$, $\mathcal{P}_\mathcal{L} = \{\in^2, \subseteq^2\}$ a $\mathcal{F}_\mathcal{L} = \{\cup^2, \cap^2, \setminus^2, \complement^1\}$.
- Binárne symboly budeme zapisovať infixovo,
  napr. namiesto $\in(t_1, t_2)$ napíšeme $t_1 \in t_2$,
  namiesto $\cup(t_1, t_2)$ napíšeme $(t_1 \cup t_2)$, ….

Príklad 3.90. Dokážme tablom, že $T \models X$ pre

$$T = \left\{ \begin{array}{c} \forall x\, \forall y (x \subseteq y \leftrightarrow \forall z (z \in x \rightarrow z \in y)) \\ \forall x\, \forall y\, \forall z (z \in (x \cup y) \leftrightarrow (z \in x \lor z \in y)) \end{array} \right\}$$

$$X = \forall x\, \forall y ((x \cup y) \doteq x \rightarrow y \subseteq x)$$

XI. prednáška

Rezolvencia v logike prvého rádu

7. mája 2018

3.9. Rezolvencia

XI.1 Výrokové pravidlo rezolvencie (opakovanie)

Výroková rezolvencia — odvodzovacie pravidlo pre výrokové klauzuly:

$$\frac{k_1 \lor \cdots \lor p \lor \cdots \lor k_m \qquad \ell_1 \lor \cdots \lor \neg p \lor \cdots \lor \ell_n}{k_1 \lor \cdots \lor k_m \lor \ell_1 \lor \cdots \lor \ell_n}$$

Rezolvenčné *odvodenie* z množiny klauzúl S je postupnosť klauzúl, z ktorých každá:

- je prvkom S, alebo
- vznikla pravidlom rezolvencie
  z niektorých dvoch predchádzajúcich klauzúl v postupnosti, alebo
- vznikla pravidlom idempotencie
  z niektorej z predchádzajúcej klauzuly v postupnosti.

Rezolvenčné *zamietnutie* množiny klauzúl S je rezolvenčné odvodenie z S, ktorého posledným prvkom je prázdna klauzula $\square$ (klauzula s 0 literálmi).

XI.2 Prvorádové klauzuly a klauzálne teórie

Definícia 3.91. Nech $\mathcal{L}$ je jazyk logiky prvého rádu.

Literál je atomická formula $P(t_1, \dots, t_m)$ jazyka $\mathcal{L}$
alebo jej negácia $\neg P(t_1, \dots, t_m)$.

Klauzula je všeobecný uzáver disjunkcie literálov, teda uzavretá formula jazyka $\mathcal{L}$ v tvare $\forall x_1 \cdots \forall x_k (L_1 \lor \cdots \lor L_n)$ (skrátene $\forall \vec{x} \bigvee_{i=1}^{n} L_i$),
kde $L_1, \ldots, L_n$ sú literály
a $x_1, \ldots, x_k$ sú *všetky* voľné premenné formuly $L_1 \lor \cdots \lor L_n$.
Klauzula môže byť aj *jednotková* ($\forall \vec{x}\, L_1$) alebo *prázdna* ($\square$).

Klauzálna teória je množina klauzúl $\{C_1, \ldots, C_n\}$.
Môže byť tvorená aj jedinou klauzulou alebo byť prázdna.

Dohoda 3.92. Všeobecné kvantifikátory v zápise klauzúl budeme zanedbávať.

Teda namiesto $\forall x_1 \cdots \forall x_n (L_1 \lor \cdots \lor L_m)$ píšeme iba $L_1 \lor \cdots \lor L_m$.

XI.3 Formalizácia do klauzálnych teórií

Príklad 3.93. Klauzálnymi teóriami sa dajú formalizovať mnohé tvrdenia:

- Implikácie vieme vyjadriť disjunkciami a negáciami, konjunkciu v konzekvente viacerými klauzulami,
  - Každý, kto má rád Ciri, má rád Bibu a Edo ho tiež má rád:
    $\forall x(\neg \texttt{má\_rád}(x, \texttt{Ciri}) \lor \texttt{má\_rád}(x, \texttt{Biba}))$, $\forall x(\neg \texttt{má\_rád}(x, \texttt{Ciri}) \lor \texttt{má\_rád}(\texttt{Edo}, x))$

  konjunkciu v antecedente viacerými literálmi v klauzule
  - Každý, kto má rád Bibu a Dadu, má rád aj Aďu:
    $\forall x(\neg \texttt{má\_rád}(x, \texttt{Biba}) \lor \neg \texttt{má\_rád}(x, \texttt{Dada}) \lor \texttt{má\_rád}(x, \texttt{Aďa}))$
- Namiesto existenčného kvantifikátora
  môžeme *pomenovať* objekt konštantou
  - Niekto má rád všetkých: $\forall y\, \texttt{má\_rád}(\textbf{filantrop}, y)$

  alebo funkciou, ktorej dáme ako argumenty súvisiace objekty
  - Každého má niekto rád: $\forall y\, \texttt{má\_rád}(\texttt{obdivovateľ}(y), y)$

Príklad 3.94.

- Každého má niekto rád: $\forall y\, \text{má\_rád}(\text{obdivovateľ}(y), y)$,
  teda aj Ciri má niekto rád: $\text{má\_rád}(\text{obdivovateľ}(\text{Ciri}), \text{Ciri})$
- Kto má rád Ciri, toho má rád Edo:

  $$\forall x(\neg\text{má\_rád}(x, \text{Ciri}) \lor \text{má\_rád}(\text{Edo}, x)),$$

  ak Cirin obdivovateľ má rád Ciri, tak ho Edo má rád:

  $$\neg\text{má\_rád}(\text{obdivovateľ}(\text{Ciri}), \text{Ciri}) \lor \\ \text{má\_rád}(\text{Edo}, \text{obdivovateľ}(\text{Ciri})).$$

- Preto (výrokovou rezolvenciou):

  $$\frac{\begin{array}{c}\text{má\_rád}(\text{obdivovateľ}(\text{Ciri}), \text{Ciri}) \\ \neg\,\text{má\_rád}(\text{obdivovateľ}(\text{Ciri}), \text{Ciri}) \lor \text{má\_rád}(\text{Edo}, \text{obdivovateľ}(\text{Ciri}))\end{array}}{\text{má\_rád}(\text{Edo}, \text{obdivovateľ}(\text{Ciri}))}$$

- Celý úsudok z príkladu aj s dosadeniami:

  $$\frac{\begin{array}{c}\forall y\, \text{má\_rád}(\text{obdivovateľ}(y), y) \\ \forall x(\neg\text{má\_rád}(x, \text{Ciri}) \lor \text{má\_rád}(\text{Edo}, x))\end{array}}{\text{má\_rád}(\text{Edo}, \text{obdivovateľ}(\text{Ciri}))}$$

- Aby sme klauzuly mohli rezolvovať, potrebovali sme substitúciu:

  $$\sigma = \{x \mapsto \text{obdivovateľ}(\text{Ciri}), y \mapsto \text{Ciri}\}$$

- Po substitúcii σ majú komplementárne literály
  rovnaké argumenty predikátu:

  $$\begin{aligned} \text{má\_rád}(\text{obdivovateľ}(y), y)\sigma &= \text{má\_rád}(\text{obdivovateľ}(\text{Ciri}), \text{Ciri}) \\ \neg\text{má\_rád}(x, \text{Ciri})\sigma &= \neg\text{má\_rád}(\text{obdivovateľ}(\text{Ciri}), \text{Ciri}) \end{aligned}$$

Definícia 3.95. Nech A, B sú postupnosti symbolov, σ je substitúcia. Substitúcia σ je *unifikátorom* A a B vtt $A\sigma = B\sigma$.

Príklad 3.96.

- $A_1 = \mathtt{má\_rád}(\mathtt{filantrop}, y)$, $B_1 = \mathtt{má\_rád}(x, \mathtt{Ciri})$,
  $\sigma_1 = \{x \mapsto \mathtt{filantrop}, y \mapsto \mathtt{Ciri}\}$
- $A_2 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_2 = \mathtt{má\_rád}(x, \mathtt{Ciri})$,
  $\sigma_2 = \{x \mapsto \mathtt{obdivovateľ}(\mathtt{Ciri}), y \mapsto \mathtt{Ciri}\}$
- $A_3 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_3 = \mathtt{má\_rád}(\mathtt{Edo}, x)$,
  $\sigma_3 =$??? **neexistuje!**
- $A_4 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_4 = \mathtt{má\_rád}(x, x)$,
  $\sigma_4 =$??? **neexistuje!**

Definícia 3.97. Nech $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ a $\theta = \{y_1 \mapsto s_1, \dots, y_m \mapsto s_m\}$ sú substitúcie.
Zložením (kompozíciou) substitúcií σ a θ
je substitúcia $\sigma\theta = \{x_1 \mapsto t_1\theta, \dots, x_n \mapsto t_n\theta, y_{i_1} \mapsto s_{i_1}, \dots, y_{i_k} \mapsto s_{i_k}\}$,
kde $\{y_{i_1}, \dots, y_{i_k}\} = \{y_1, \dots, y_m\} \setminus \{x_1, \dots, x_n\}$.

Príklad 3.98.

$$\sigma = \{x \mapsto \mathtt{obdivovateľ}(y), z \mapsto y\}$$

$$\theta = \{y \mapsto \mathtt{filantrop}\}$$

$$\sigma\theta = \{x \mapsto \mathtt{obdivovateľ}(\mathtt{filantrop}), z \mapsto \mathtt{filantrop}, y \mapsto \mathtt{filantrop}\}$$

Definícia 3.99. Nech A, B sú postupnosti symbolov, σ a θ sú substitúcie.

σ je *všeobecnejšia* ako θ vtt existuje subst. γ taká, že $\theta = \sigma\gamma$.

σ je *najvšeobecnejším unifikátorom* A a B vtt

- σ je unifikátorom A a B a zároveň
- pre každý unifikátor θ A a B je σ všeobecnejšia ako θ.

Príklad 3.100. $A_5 = \texttt{má\_rád}(\texttt{obdivovateľ}(x), y)$, $B_5 = \texttt{má\_rád}(u, v)$

- $\sigma_{51} = \{u \mapsto \texttt{obdivovateľ}(\texttt{Ciri}), v \mapsto y, x \mapsto \texttt{Ciri}\}$
  $\theta_{51} = \{u \mapsto \texttt{obdivovateľ}(\texttt{Ciri}), v \mapsto \texttt{Biba}, x \mapsto \texttt{Ciri}, y \mapsto \texttt{Biba}\}$
  $\gamma_{51} = \{y \mapsto \texttt{Biba}\}$
- $\sigma_{52} = \{u \mapsto \texttt{obdivovateľ}(x), v \mapsto y\}$
  $\theta_{52} = \{u \mapsto \texttt{obdivovateľ}(\texttt{Ciri}), v \mapsto y, x \mapsto \texttt{Ciri}\}$
  $\gamma_{52} = \{x \mapsto \texttt{Ciri}\}$

XI.9 Unifikátory a rezolvencia

Príklad 3.101.

$$\frac{\begin{array}{c}\texttt{má\_rád}(\texttt{obdivovateľ}(y), y)\sigma \\ (\neg\texttt{má\_rád}(x, \texttt{Ciri}) \lor \texttt{má\_rád}(\texttt{Edo}, x))\sigma\end{array}}{\texttt{má\_rád}(\texttt{Edo}, x)\sigma}$$

$$\sigma = \{x \mapsto \texttt{obdivovateľ}(\texttt{Ciri}), y \mapsto \texttt{Ciri}\}$$

$$\frac{\begin{array}{c}\texttt{má\_rád}(\texttt{obdivovateľ}(\texttt{Ciri}), \texttt{Ciri}) \\ \neg\,\texttt{má\_rád}(\texttt{obdivovateľ}(\texttt{Ciri}), \texttt{Ciri}) \lor \texttt{má\_rád}(\texttt{Edo}, \texttt{obdivovateľ}(\texttt{Ciri}))\end{array}}{\texttt{má\_rád}(\texttt{Edo}, \texttt{obdivovateľ}(\texttt{Ciri}))}$$

XI.10 Unifikátory a rezolvencia

Príklad 3.102. Rovnaké premenné v klauzulách môžu zabrániť unifikácii literálov:

$$\texttt{má\_rád}(\texttt{obdivovateľ}(x), x) \qquad \neg\texttt{má\_rád}(x, \texttt{Ciri}) \lor \texttt{má\_rád}(\texttt{Edo}, x)$$

Klauzuly sú však všeobecne kvantifikované *nezávisle* od seba.
Premenovanie premenných v jednej z nich nezmení jej význam,
ale umožní unifikáciu (viď predchádzajúci príklad).

$$\texttt{má\_rád}(\texttt{obdivovateľ}(y), y) \qquad \neg\texttt{má\_rád}(x, \texttt{Ciri}) \lor \texttt{má\_rád}(\texttt{Edo}, x)$$

Definícia 3.103. *Premenovaním premenných* je každá substitúcia $\sigma = \{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}$, kde $y_1, \ldots, y_n$ sú premenné.

XI.11 Prvorádová rezolvencia — pravidlá

Definícia 3.104. Nech C a D sú prvorádové klauzuly, nech A a B sú atómy, nech L a K sú literály.

Rezolvencia (angl. resolution) je odvodzovacie pravidlo

$$\frac{A \lor C \quad \neg B \lor D}{(C\theta \lor D)\sigma} \quad \begin{array}{l}\sigma \text{ je unifikátor } A\theta \text{ a } B,\\ \theta \text{ je premenovanie premenných.}\end{array}$$

Faktorizácia (angl. factoring) je odvodzovacie pravidlo

$$\frac{L \lor K \lor C}{(L \lor C)\sigma} \quad \sigma \text{ je unifikátor } L \text{ a } K.$$

Faktorizácia je zovšeobecnenie idempotencie pri výrokovej rezolvencii.

XI.12 Rezolvenčné odvodenie a zamietnutie

Definícia 3.105. Nech T je klauzálna teória.

Rezolvenčným odvodením z T je každá konečná postupnosť klauzúl
$\mathcal{Z} = (C_1, C_2, \ldots, C_n)$, kde každá klauzula C_i, $1 \leq i \leq n$, je:

- prvkom T, alebo
- odvodená pravidlom rezolvencie z klauzúl C_j a C_k, ktoré sa v $\mathcal{Z}$ nachádzajú pred C_i (teda $j, k < i$), alebo
- odvodená pravidlom faktorizácie z klauzuly C_j, ktorá sa v $\mathcal{Z}$ nachádza pred C_i (teda $j < i$).

Zamietnutím T (angl. refutation) je každé rezolvenčné odvodenie
$\mathcal{Z} = (C_1, C_2, \ldots, C_n)$, kde $C_n = \square$.

XI.13 Refutačná korektnosť a úplnosť rezolvencie

Veta 3.106 (Refutačná korektnosť a úplnosť rezolvencie)**.** *Nech T je klauzálna teória. Potom existuje zamietnutie $\{C_1, \ldots, C_n\}$ vtt T je nesplniteľná.*

Príklad 3.107. Dokážme nesplniteľnosť:

$$\left\{\begin{array}{c} \forall x\, \mathtt{má\_rád}(\mathtt{obdivovateľ}(x), x), \\ \forall x\, \forall y\, \neg\mathtt{má\_rád}(x, \mathtt{obdivovateľ}(y)), \\ \forall x(\neg\mathtt{má\_rád}(x, \mathrm{Ciri}) \lor \mathtt{má\_rád}(\mathtt{Edo}, x)) \end{array}\right\}$$

3.10. Prevod do klauzálnej teórie a skolemizácia

XI.14 Rezolvencia vs. prvorádové teórie

- Rezolvencia je teda refutačne korektná a úplná
- Pracuje však iba s klauzálnymi teóriami
- Vo výrokovej logike sa dala ľubovoľná teória *upraviť na ekvisplniteľnú* klauzálnu teóriu (resp. formulu v CNF)
- Na zistenie jej (ne)splniteľnosti sme potom mohli použiť výrokovú rezolvenciu (alebo výrokový SAT solver)
- Je podobná úprava možná aj v logike prvého rádu?

XI.15 Prvorádová ekvivalencia a ekvisplniteľnosť

Definícia 3.108 (Prvorádová ekvi*valencia*)**.** Množiny formúl S a T sú *(prvorádovo) ekvivalentné* ($S \Leftrightarrow T$) vtt pre každú štruktúru $\mathcal{M}$ a každé ohodnotenie e platí $\mathcal{M} \models S[e]$ vtt $\mathcal{M} \models T[e]$.

Definícia 3.109 (Prvorádová ekvi*splniteľnosť*)**.** Množiny formúl S a T sú *(prvorádovo) rovnako splniteľné* (*ekvisplniteľné*, equisatisfiable) vtt S má model vtt T má model.

Tvrdenie 3.110 (Ekvivalentná úprava)**.** *Nech X, A, B sú formuly a nech* $\mathrm{free}(A) = \mathrm{free}(B)$. *Ak $A \Leftrightarrow B$, tak $X \Leftrightarrow X[\,A \mid B\,]$.*

XI.16 Nahradenie implikácií

Rovnako ako vo výrokovej logike môžeme každú formulu $(A \to B)$ ekvivalentne nahradiť formulou $(\neg A \lor B)$.

Príklad 3.111.

$$\begin{aligned} &\forall x(\texttt{dobré}(x) \land \texttt{dieťa}(x) \to \exists y(\texttt{dostane}(x,y) \land \texttt{darček}(y))) \\ \Leftrightarrow\ &\forall x(\neg(\texttt{dobré}(x) \land \texttt{dieťa}(x)) \lor \exists y(\texttt{dostane}(x,y) \land \texttt{darček}(y))) \end{aligned}$$

$$\begin{aligned} &\forall x(\neg\texttt{dobré}(x) \to \neg\exists y\, \texttt{dostane}(x,y)) \\ \Leftrightarrow\ &\forall x(\neg\neg\texttt{dobré}(x) \lor \neg\exists y\, \texttt{dostane}(x,y)) \end{aligned}$$

XI.17 Konverzia do negačného normálneho tvaru (NNF)

Definícia 3.112. Formula X je v *negačnom normálnom tvare* (NNF) vtt neobsahuje implikáciu
a pre každú jej podformulu $\neg A$ platí, že A je atomická formula.

Formulu bez implikácií do NNF upravíme pomocou

- de Morganovych zákonov:

$$\neg(A \land B) \Leftrightarrow \neg A \lor \neg B \qquad\qquad \neg(A \lor B) \Leftrightarrow \neg A \land \neg B$$

- pravidla dvojitej negácie:

$$\neg\neg A \Leftrightarrow A$$

- pravidiel pre negáciu kvantifikátorov:

$$\neg\, \exists x\, A \Leftrightarrow \forall x\, \neg A \qquad\qquad \neg\, \forall x\, A \Leftrightarrow \exists x\, \neg A$$

Tvrdenie 3.113. *Pre každú formulu X existuje formula Y v NNF taká, že $X \Leftrightarrow Y$.*

Príklad 3.114.

$$\begin{aligned} &\forall x(\neg(\mathtt{dobré}(x) \land \mathtt{dieťa}(x)) \lor \exists y(\mathtt{dostane}(x,y) \land \mathtt{darček}(y))) \\ \Leftrightarrow\ &\forall x((\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x)) \lor \exists y(\mathtt{dostane}(x,y) \land \mathtt{darček}(y))) \end{aligned}$$

$$\begin{aligned} &\forall x(\neg\neg\mathtt{dobré}(x) \lor \neg\exists y\, \mathtt{dostane}(x,y)) \\ \Leftrightarrow\ &\forall x(\mathtt{dobré}(x) \lor \forall y\, \neg\mathtt{dostane}(x,y)) \end{aligned}$$

XI.19 Skolemizácia

Skolemizácia je úprava formuly X v NNF, pri ktorej:

- každý výskyt podformuly $\exists y\, A$, ktorý sa nachádza v X *mimo* všetkých oblastí platnosti všeobecných kvantifikátorov nahradíme formulou

  $$A\{y \mapsto c\}$$

  pre *nový* symbol konštanty c, nazývaný *Skolemova konštanta*;
- každý výskyt podformuly $\exists y\, A$, ktorý sa nachádza v X v oblasti platnosti všeobecných kvantifikátorov premenných $x_1, \ldots, x_n$

  $$X = \cdots \forall x_1(\cdots \forall x_2(\cdots \forall x_n(\cdots \exists y\, A \cdots) \cdots) \cdots) \cdots$$

  nahradíme formulou

  $$A\{y \mapsto f(x_1, x_2, \ldots, x_n)\}$$

  pre *nový* funkčný symbol f, nazývaný *Skolemova funkcia*.

Skolemove konštanty a funkcie *pomenúvajú* objekty, ktorých existenciu formula postuluje.

XI.20 Skolemizácia

Tvrdenie 3.115. *Pre každú formulu X v jazyku $\mathcal{L}$ existuje formula Y vo vhodnom rozšírení $\mathcal{L}'$ jazyka $\mathcal{L}$ taká, že Y neobsahuje existenčné kvantifikátory a X a Y sú* ekvisplniteľné.

Príklad 3.116.

$$\exists x\,(\mathtt{dobr\acute{e}}(x) \land \mathtt{die\check{t}a}(x))$$

$$\rightsquigarrow \mathtt{dobr\acute{e}}(\,\mathtt{nejak\acute{e}\_dobr\acute{e}\_die\check{t}a}\,) \land \mathtt{die\check{t}a}(\,\mathtt{nejak\acute{e}\_dobr\acute{e}\_die\check{t}a}\,)$$

$$\forall x(\,\neg\mathtt{dobr\acute{e}}(x) \lor \neg\mathtt{die\check{t}a}(x) \lor \exists y(\mathtt{dostane}(x,y) \land \mathtt{dar\check{c}ek}(y))\,)$$

$$\begin{aligned}\rightsquigarrow \forall x(\,&\neg\mathtt{dobr\acute{e}}(x) \lor \neg\mathtt{die\check{t}a}(x) \lor \\ &(\mathtt{dostane}(x, \mathtt{dar\check{c}ek\_pre}(x)\,) \land \mathtt{dar\check{c}ek}(\,\mathtt{dar\check{c}ek\_pre}(x)\,))\,)\end{aligned}$$

XI.21 Skolemizácia

Príklad 3.117.

$$\begin{aligned}&\exists z\Big(R(z,z) \land \forall x\big(\neg R(x,z) \lor \exists u(R(x,u) \land R(u,z)) \\ &\qquad\qquad\qquad \lor \forall y\exists v(\neg R(y,v) \land R(x,v))\big)\Big)\end{aligned}$$

$$\begin{aligned}\rightsquigarrow\ &R(c,c) \land \forall x\big(\neg R(x,c) \lor (R(x,f_1(x)) \land R(f_1(x),c)) \\ &\qquad\qquad \lor \forall y(\neg R(y,f_2(x,y)) \land R(x,f_2(x,y)))\big)\end{aligned}$$

XI.22 Konverzia do PNF

Definícia 3.118. Formula X je v *prenexnom normálnom tvare* (PNF) vtt má tvar $Q_1x_1\,Q_2x_2 \cdots Q_nx_n\,A$, kde $Q_i \in \{\forall, \exists\}$, x_i je premenná a A je formula bez kvantifikátorov (*matica* formuly X).

Skolemizovanú formulu v NNF upravíme do PNF opakovanou aplikáciou nasledujúcich transformácií:

- ak x **nemá voľný výskyt** v B,

$$\forall x\,A \land B \Leftrightarrow \forall x\,(A \land B) \qquad B \land \forall x\,A \Leftrightarrow \forall x\,(B \land A)$$
$$\forall x\,A \lor B \Leftrightarrow \forall x\,(A \lor B) \qquad B \lor \forall x\,A \Leftrightarrow \forall x\,(B \lor A)$$

- ak sa x má voľný výskyt v B a y je **nová** premenná,

$$\begin{array}{ll} \forall x\, A \land B \Leftrightarrow \forall y\, A\{x \mapsto y\} \land B & B \land \forall x\, A \Leftrightarrow B \land \forall y\, A\{x \mapsto y\} \\ \forall x\, A \lor B \Leftrightarrow \forall y\, A\{x \mapsto y\} \lor B & B \lor \forall x\, A \Leftrightarrow B \lor \forall y\, A\{x \mapsto y\} \end{array}$$

XI.23 Konverzia do PNF

Tvrdenie 3.119. *Pre každú formulu X v NNF existuje ekvivalentná formula Y v PNF a NNF.*

Príklad 3.120.

$$\begin{aligned} &\forall x(\,\mathtt{dobré}(x) \lor \forall y\, \neg\mathtt{dostane}(x,y)\,) \\ \Leftrightarrow\ &\forall x\, \forall y\,(\,\mathtt{dobré}(x) \lor \neg\mathtt{dostane}(x,y)\,) \end{aligned}$$

Pozor! Pre ekvivalentnosť prenexovania je nutné, aby boli premenné viazané rôznymi kvantifikátormi rôzne:

$$(\forall x\, A(x) \lor \forall x\, B(x)) \not\Leftrightarrow \forall x\, (A(x) \lor B(x)) \quad \textbf{!!!}$$
$$(\forall x\, A(x) \lor \forall x\, B(x)) \Leftrightarrow \forall x\, \forall y\, (A(x) \lor B(y))$$

Premenné je lepšie premenovať ešte pred skolemizáciou.

XI.24 Konverzia do CNF

Maticu (najväčšiu podformulu bez kvantifikátorov) formuly v PNF upravíme do CNF pomocou distributívnosti a komutatívnosti disjunkcie:

$$(A \lor (X \land Y)) \Leftrightarrow ((A \lor X) \land (A \lor Y))$$
$$((X \land Y) \lor A) \Leftrightarrow ((X \lor A) \land (Y \lor A))$$

Príklad 3.121.

$$\begin{aligned} &\forall x(\,\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \\ &\qquad (\mathtt{dostane}(x, \mathtt{darček\_pre}(x)) \land \mathtt{darček}(\mathtt{darček\_pre}(x)))\,) \\ \Leftrightarrow\ &\forall x(\,(\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{dostane}(x, \mathtt{darček\_pre}(x))) \land \\ &\qquad (\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{darček}(\mathtt{darček\_pre}(x)))\,) \end{aligned}$$

Formula, ktorej matica je v CNF, je ekvivalentná s konjunkciou klauzúl:

$$\forall x(A \land B) \Leftrightarrow (\forall x\, A \land \forall x\, B)$$

a konjunkcia klauzúl je ekvivalentná s ich množinou:

$$\{(\forall x\, A \land \forall x\, B)\} \Leftrightarrow \{\forall x\, A, \forall x\, B\}$$

Príklad 3.122.

$$\begin{aligned}
&\{\forall x(\,(\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x) \lor \mathrm{dostane}(x, \mathrm{dar\check{c}ek_pre}(x))) \land \\
&\qquad (\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x) \lor \mathrm{dar\check{c}ek}(\mathrm{dar\check{c}ek_pre}(x)))\,)\} \\
\Leftrightarrow\ &\{(\,\forall x(\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x) \lor \mathrm{dostane}(x, \mathrm{dar\check{c}ek_pre}(x))) \land \\
&\quad \forall x(\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x) \lor \mathrm{dar\check{c}ek}(\mathrm{dar\check{c}ek_pre}(x)))\,)\} \\
\Leftrightarrow\ &\{\forall x(\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x) \lor \mathrm{dostane}(x, \mathrm{dar\check{c}ek_pre}(x))), \\
&\ \forall x(\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x) \lor \mathrm{dar\check{c}ek}(\mathrm{dar\check{c}ek_pre}(x)))\}
\end{aligned}$$

Veta 3.123. *Ku každej teórii T v jazyku logiky prvého rádu $\mathcal{L}$ existuje ekvisplniteľná klauzálna teória v nejakom rozšírení $\mathcal{L}'$ jazyka $\mathcal{L}$ o Skolemove konštanty a funkcie.*

Príklad 3.124.

$$\left\{\begin{array}{l}
\forall x\,(\mathrm{dobr\acute{e}}(x) \land \mathrm{die\check{t}a}(x) \to \exists y(\mathrm{dostane}(x, y) \land \mathrm{dar\check{c}ek}(y))), \\
\exists x\,(\mathrm{dobr\acute{e}}(x) \land \mathrm{die\check{t}a}(x)), \\
\forall x\,(\neg\mathrm{dobr\acute{e}}(x) \to \neg\exists y\,\mathrm{dostane}(x, y))
\end{array}\right\} \rightsquigarrow$$

$$\left\{\begin{array}{l}
\forall x_1(\neg\mathrm{dobr\acute{e}}(x_1) \lor \neg\mathrm{die\check{t}a}(x_1) \lor \mathrm{dostane}(x_1, \mathrm{dar\check{c}ek_pre}(x_1))), \\
\forall x_2(\neg\mathrm{dobr\acute{e}}(x_2) \lor \neg\mathrm{die\check{t}a}(x_2) \lor \mathrm{dar\check{c}ek}(\mathrm{dar\check{c}ek_pre}(x_2))), \\
\mathrm{dobr\acute{e}}(\mathrm{nejak\acute{e}_dobr\acute{e}_die\check{t}a}), \mathrm{die\check{t}a}(\mathrm{nejak\acute{e}_dobr\acute{e}_die\check{t}a}), \\
\forall x_3\, \forall y\,(\mathrm{dobr\acute{e}}(x_3) \lor \neg\mathrm{dostane}(x_3, y))
\end{array}\right\}$$

Dôkaz/algoritmus

T_{I}: Implikácie nahradíme disjunkciami.

T_{N}: *Negačný normálny tvar* (NNF): Presunieme negácie k atómom.

T_{V}: Premenujeme premenné tak,
aby každý kvantifikátor viazal inú premennú ako ostatné kvantifikátory.

T_{S}: *Skolemizácia*: Existenčné kvantifikátory nahradíme substitúciou nimi viazaných premenných za Skolemove konštanty/aplikácie Skolemovych funkcií na všeobecne príslušné kvantifikované premenné.

T_{P}: *Prenexný normálny tvar* (PNF):
presunieme všeobecné kvantifikátory na začiatok formuly.

T_{D}: *Konjunktívny normálny tvar* (CNF): distribuujeme disjunkcie do konjunkcií.

T_{K}: Odstránime konjunkcie rozdelením konjunktov do samostatne kvantifikovaných klauzúl.

Skolemizácia vytvorí ekvisplniteľnú teóriu, ostatné úpravy sú ekvivalentné.

Dôsledok 3.125 (Úplnosť rezolvencie)**.** *Nech T je konečná teória, nech X je uzavretá formula.*
Nech $T'_X = \{C_1, \dots, C_n\}$ je klauzálna teória ekvisplniteľná s $T \cup \{\neg X\}$.
Potom z T vyplýva X vtt existuje zamietnutie T'_X.

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