Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2018/2019

Obsah

I. prednáška

O logike a tomto kurze
Syntax výrokovej logiky

18. februára 2019

1. Úvod

1.1. O logike

I.1 Čo je logika

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

  Jazyk zápis pozorovaní, definície pojmov, formulovanie teórií

  Syntax pravidlá zápisu tvrdení

  Sémantika význam tvrdení

  Usudzovanie (inferencia) odvodenie nových dôsledkov z doterajších poznatkov

  Dôkaz presvedčenie ostatných o správnosti záverov usudzovania

I.2 Poznatky a teórie

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

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

P1: Sarah nepôjde na párty, ak pôjde Kim.

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

P3: Sarah nepôjde bez Jima.

I.3 Možné stavy sveta a modely

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

- $\models$ stavy, v ktorých je pravdivé — **modely** tvrdenia (teórie),
- $\not\models$ stavy, v ktorých je nepravdivé.

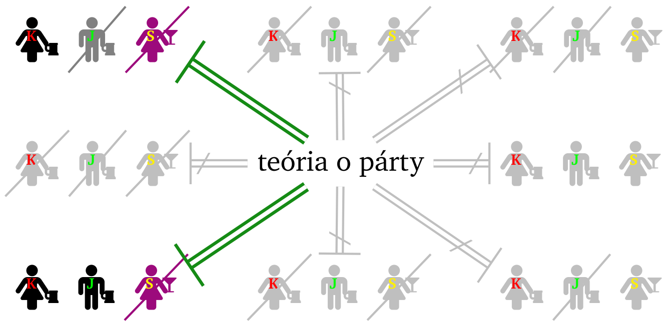
Tvrdenie aj teória môžu mať viacero modelov, ale aj žiaden.

Príklad 1.2. Vymenujme možné stavy prítomnosti Kim, Jima a Sarah na párty.
Zistime, v ktorých sú pravdivé jednotlivé tvrdenia našej teórie a celá teória.

I.4 Logické dôsledky

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

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



I.5 Logické usudzovanie

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

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

  > Predpokladajme, že na párty pôjde Jim.
  >
  > Teda podľa (P2) pôjde aj Kim.
  >
  > Teda podľa (P1) nepôjde Sarah.

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

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

I.6 Usudzovacie pravidlá

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

Ak pôjde Jim, tak pôjde Kim.	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

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

I.7 Korektné usudzovacie pravidlá a dedukcia

Korektné pravidlo odvodí z pravdivých premís pravdivý záver

Príklad 1.5. Pravidlo *modus ponens*

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

je korektné.

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

Dedukcia je usudzovanie, pri ktorom sa používajú iba korektné pravidlá

I.8 Nededuktívne pravidlá

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

Indukcia — zovšeobecnenie:

Videl som tisíc havranov.
Žiaden nebol inej farby ako čiernej.
———
Všetky havrany sú čierne.

Platí aj pre biele bicykle?

Abdukcia — odvodzovanie možných príčin z následkov:

Ak je batéria vybitá, auto 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.9 Nededuktívne pravidlá

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

I.10 Ťažkosti s prirodzeným jazykom

Prirodzený jazyk je problematický:

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

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

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

I.11 Formálne jazyky

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

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

I.12 Formalizácia poznatkov

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

Karol je trikrát starší ako Mária.
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 1.6. 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.13 Kalkuly — formalizácia usudzovania

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

  korektné — odvodzujú iba logické dôsledky

  úplné — umožňujú odvodiť všetky logické dôsledky

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

  ...

  Poznáte už aj jeden logický kalkul — ekvivalentné úpravy

  Sú korektné, ale nie vždy úplné

I.14 Výpočtová logika — automatizácia usudzovania

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

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

I.15 Výpočtová logika — aplikácie

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

I.16

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

A. premisou,

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.17 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.18 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.19 Opakovanie: Výroková logika v prirodzenom jazyku

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

Príklady 2.1.

- Miro je v poslucharni 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.20 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.21 (Meta) matematika výrokovej logiky

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

2.2. Syntax výrokovej logiky

I.22 Syntax výrokovej logiky

- Syntax sú pravidlá budovania viet v jazyku

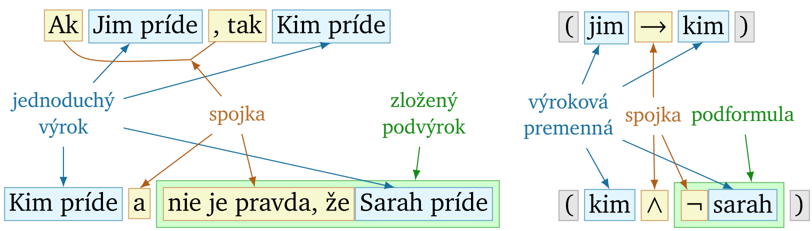
- Pri formálnych jazykoch sú popísané matematicky
- Nedajte sa tým odradiť, nie je to oveľa iné ako programovanie
- Viac sa budete formálnymi jazykmi zaoberať na Úvode do teoretickej informatiky
- Naše definície vychádzajú prevažne z kníh [Smullyan, 1979] a [Švejdar, 2002]

I.23 Syntax výrokovej logiky

Aké tvrdenia chceme zapisovať vo výrokovej logike?

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

  Ich formálnu verziu nazveme **výrokové premenné**
- Zložené výroky, tvorené podvýrokmi a spojkou:



  Ich formálnu verziu nazveme **formuly**
- Čo sú *základné* stavebné kamene týchto výrokov?
  - jednoduché výroky a spojky

  Tieto základné prvky nazveme **symboly**

I.24 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 $\neg$, $\land$, $\lor$, $\rightarrow$, (a), ani jej prvky tieto symboly neobsahujú;
- *logické* symboly (*logické spojky*): $\neg$, $\land$, $\lor$, $\rightarrow$
  (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 $\land$, $\lor$, $\rightarrow$ sú *binárne* (spájajú dve formuly).

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

I.25 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.26 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. ¬sarah.
  - Premenné alebo aj ich negácie spojené spojkou, napr. (¬kim ∨ sarah).
  - Ale negovať a spájať spojkami môžeme aj zložitejšie formuly, napr. (¬(kim ∧ sarah) → (¬kim ∨ ¬sarah)).

- Ako presne popíšeme, čo je formula?

  Induktívnou definíciou:

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

I.27 Výrokové formuly

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

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

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

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

Dohoda

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

I.28 Výrokové formuly

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

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

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

I.29 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 niektorý predchádzajúci člen postupnosti, alebo
- má jeden z tvarov $(A \land B)$, $(A \lor B)$, $(A \to B)$, kde A a B sú niektoré predchádzajúce členy postupnosti.

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

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

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

II. prednáška
Sémantika výrokovej logiky

25. februára 2019

II.1

Spomeňte si II.1

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

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

Čo keby sme zadefinovali „formuly“ takto?

Definícia „formúl“ ⚠

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

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

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

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

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

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

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

II.4 Jednoznačnosť rozkladu formúl výrokovej logiky

Pre našu definíciu formúl platí:

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

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

II.5 Problémy s vytvárajúcou postupnosťou

Vytvárajúca postupnosť popisuje konštrukciu formuly podľa definície formúl:

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

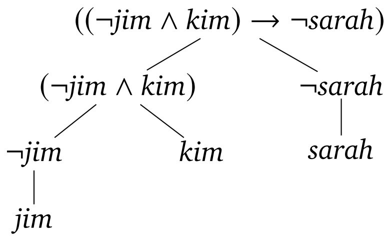
ale

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

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

II.6 Vytvárajúci strom

Konštrukciu si ale vieme predstaviť ako *strom*:



Takéto stromy voláme *vytvárajúce*.

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

II.7 Vytvárajúci strom formuly

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

- v koreni T je formula X,
- ak vrchol obsahuje formulu $\neg A$, tak má práve jedno dieťa, ktoré obsahuje formulu A,
- ak vrchol obsahuje formulu $(A\ b\ B)$, 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.8 Syntaktické vzťahy formúl

Uvažujme formulu:

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

- Ako nazveme formuly, z ktorých vznikla?

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

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

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

- Ako tieto pojmy presne zadefinujeme?

II.9 Podformuly

Definícia 2.13 (Priama podformula)**.**

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

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

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

II.10 Meranie syntaktickej zložitosti formúl

Miera zložitosti/veľkosti formuly:

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

Lepšiu mieru nazývame *stupeň formuly*

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

II.11 Meranie syntaktickej zložitosti formúl

Ako stupeň zadefinujeme?

Podobne ako sme zadefinovali formuly — induktívne:

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

II.12 Stupeň formuly

Definícia 2.16 (Stupeň formuly)**.**

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

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

II.13 Indukcia na stupeň formuly

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

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

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

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

II.14 Množina výrokových premenných formuly

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

- 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 výrokových premenných formúl $(A \land B)$, $(A \lor B)$ a $(A \to B)$.

II.15 Množina výrokových premenných formuly

Definícia 2.18 (Množina výrok. prem. formuly [vars(X)]).

- 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 $\mathrm{vars}((A \land B)) = \mathrm{vars}((A \lor B)) = \mathrm{vars}((A \to B)) = \mathrm{vars}(A) \cup \mathrm{vars}(B)$.

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:

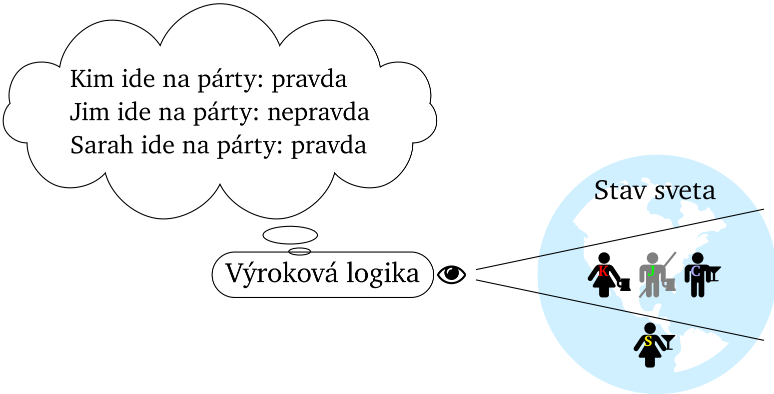
i. priame podformuly,
ii. podformuly,
iii. vytvárajúci strom.

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.17 Sémantika výrokovej logiky

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



II.18 Predstava výrokovej logiky o svete

Výroková logika vníma svet *veľmi zjednodušene*.

Zaujíma ju iba

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

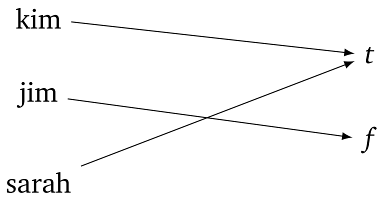
II.19 Formalizácia výrokového pohľadu na svet

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

II.20 Ohodnotenie výrokových premenných

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

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



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.21 Ohodnotenie výrokových premenných

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

II.23 Spĺňanie výrokových formúl

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

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

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

Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

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

II.24 Spĺňanie výrokových formúl — vytvárajúci strom

Príklad 2.21 (pokračovanie).

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

Iná možnosť je použiť vytvárajúci strom:

- $(\neg\mathrm{jim} \to \neg\mathrm{sarah})$ ⋯ v_3 nespĺňa
  - $\neg\mathrm{jim}$ ⋯ v_3 spĺňa
    - jim ⋯ v_3 nespĺňa
  - $\neg\mathrm{sarah}$ ⋯ v_3 nespĺňa
    - sarah ⋯ v_3 spĺňa

II.25 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 $(A \wedge B)$ vtt v spĺňa A a v spĺňa B;
- v spĺňa formulu $(A \vee B)$ vtt v spĺňa A alebo v spĺňa B;
- v spĺňa formulu $(A \rightarrow B)$ vtt v nespĺňa A alebo v spĺňa B.

Dohoda

- Skratka *vtt* znamená *vtedy a len vtedy, keď.*
- Vzťah *ohodnotenie v spĺňa formulu X* 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.*

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

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

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

II.28 Spĺňanie výrokových formúl — príklad

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

$\deg(X)$	$v_3 \models X$	$v_3 \not\models X$
0	kim, sarah	jim
1	$\neg$jim, (kim $\lor$ jim), (jim $\to$ kim)	$\neg$sarah
2	((kim $\lor$ jim) $\lor$ sarah)	(kim $\to$ $\neg$sarah)
3		($\neg$jim $\to$ $\neg$sarah)

2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť

II.29 Spĺňanie z hľadiska formuly

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

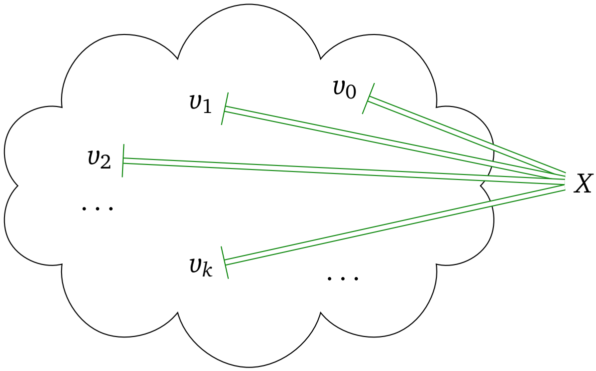
Dohoda

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

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

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

II.30 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.31 Tautológia — testovanie

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

II.32 Tautológia — testovanie

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

Presnejšie:
Pre každú formulu X a všetky ohodnotenia v_1 a v_2, ktoré zhodujú na množine $\mathrm{vars}(X)$ *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.33 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.34 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 $v_2 \models p$.

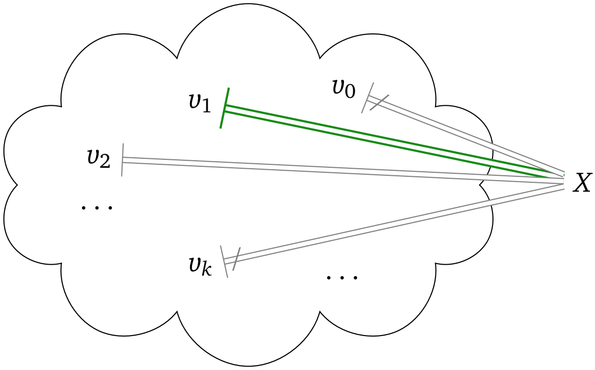
Krok: Nech X je stupňa $n > 0$ a tvrdenie platí pre všetky formuly stupňa nižšieho ako n (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na premenných v X. Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

- $X = \neg A$ 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.

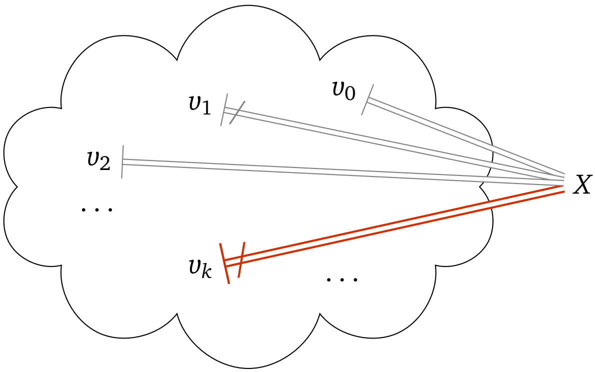
□

II.35 Splniteľnosť



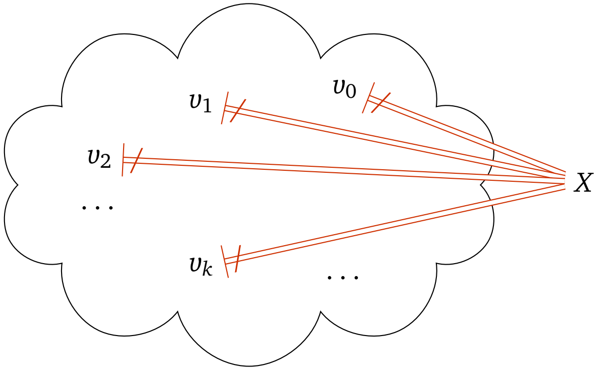
Definícia 2.27. Formulu X nazveme *splniteľnou*
vtt **nejaké** ohodnotenie výrokových premenných **spĺňa** X
(teda **existuje** také ohodnotenie výrokových premenných v, že $v \models X$).

II.36 Falzifikovateľnosť



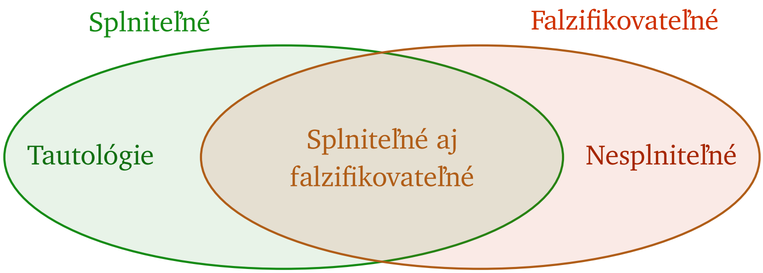
Definícia 2.28. Formulu X nazveme *falzifikovateľnou*
vtt **nejaké** ohodnotenie výrokových premenných **nespĺňa** X
(teda **existuje** také ohodnotenie výrokových premenných v, že $v \not\models X$).

II.37 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.38 „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 a ekvivalencia

4. marca 2019

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 výrokových 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 splĺňania sa jednoducho rozšíri na teórie.

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

Príklad 2.34. Aké ohodnotenie splĺňa (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 splĺňaní 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

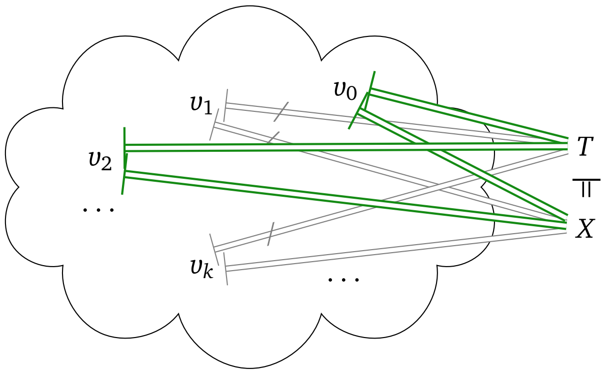
- Aký je *účel* teórií? Kedy je teória užitočná?
  - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) *doteraz neznáme skutočnosti* (teda nezapísané v teórii), ktoré platia vo všetkých stavoch sveta splĺňajúcich teóriu.

- 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*.

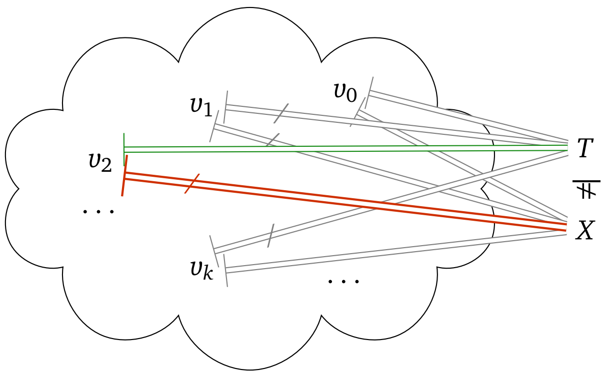
Ktorá ďalšia formula vyplýva z T_{party}?

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 ($kim \rightarrow jim$)?

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* $T \cup \{\neg X\}$ *je nesplniteľná.*

Prečo je to tak?

III.9 Vyplývanie a (ne)splniteľnosť — dôkaz

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

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

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

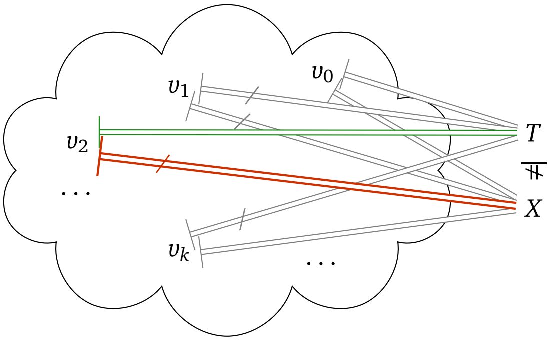
V oboch prípadoch v nespĺňa $T \cup \{\neg X\}$. Pretože v bolo ľubovoľné, môžeme zovšeobecniť, že žiadne v nespĺňa $T \cup \{\neg X\}$, teda $T \cup \{\neg X\}$ je nesplniteľná.

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

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

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

III.11 Nevyplývanie a negácia formuly



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

Nie! Na to, aby z T nevyplývala formula X, stačí, keď *existuje jediné* ohodnotenie, ktoré spĺňa T, ale nespĺňa X.
Na to, aby z T vyplývala formula $\neg X$, je nutné, aby všetky ohodnotenia, ktoré spĺňajú T, nespĺňali X (a teda spĺňali $\neg X$).

III.12 Vzťahy vyplývania, implikácií a tautológií

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

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

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

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

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

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

III.13 Hlasujte

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

2.6. Ekvivalencia formúl

III.14 Ekvivalencia formúl

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

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

III.15 Ekvivalencia formúl a skratka ↔

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

Tvrdenie 2.47. *Formuly X a Y sú výrokovologicky ekvivalentné vtt formula $(X \leftrightarrow Y)$ je tautológia.*
Skrátene: Pre všetky formuly X a Y platí, že $X \Leftrightarrow Y$ *vtt* $\models (X \leftrightarrow Y)$.

III.16 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.17 Tranzitivita ekvivalencie

„je tautológia“

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

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

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

syntaktická ekvivalencia (postup. symbolov $((X \to Y) \land (Y \to X))$)

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

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

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

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

2.6.1. Ekvivalentné úpravy

III.18 Ekvivalentné úpravy

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

Príklad 2.50 (Nahradenie podformuly ekvivalentnou).

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

$$\rightsquigarrow$$

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

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

III.19 Pravidlá ekvivalentných úprav

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

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

$$\rightsquigarrow \qquad \rightsquigarrow$$

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

III.20 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.21 Substitúcia

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.

III.22 Substitúcia ako cyklus

Substitúciu si vieme predstaviť ako cyklus prechádzajúci cez X:

Substitúcia ako cyklus

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

III.23 Substitúcia rekurzívne

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

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

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

III.24 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.25 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.26 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* $((A \land B) \land C)$	asociatívnosť
$(A \lor (B \lor C))$ *a* $((A \lor B) \lor C)$	
$(A \land B)$ *a* $(B \land A)$	komutatívnosť
$(A \lor B)$ *a* $(B \lor A)$	
$(A \land (B \lor C))$ *a* $((A \land B) \lor (A \land C))$	distributívnosť
$(A \lor (B \land C))$ *a* $((A \lor B) \land (A \lor C))$	
$\neg(A \land B)$ *a* $(\neg A \lor \neg B)$	de Morganove
$\neg(A \lor B)$ *a* $(\neg A \land \neg B)$	pravidlá
$\neg\neg A$ *a* A	dvojitá negácia

III.27 Ekvivalencie pre ekvivalentné úpravy

Veta 2.56 (Pokračovanie)**.**

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

2.6.2. Konjunktívna a disjunktívna normálna forma

III.28 Konjunkcia a disjunkcia postupnosti formúl

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

- *Konjunkciu postupnosti formúl* $A_1, \dots, A_n$,
  teda $(((A_1 \land A_2) \land A_3) \land \cdots \land A_n)$,
  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.29 Konjunktívny a disjunktívny normálny tvar

Definícia 2.57.

Literál je výroková premenná
alebo negácia výrokovej premennej.

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

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

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

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

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

Literatúra

Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994. ISBN 978-0-201-53082-7.

Raymond M. Smullyan. *Logika prvého rádu*. Alfa, 1979. Z angl. orig. *First-Order Logic*, Berlin-Heidelberg: Springer-Verlag, 1968 preložil Svätoslav Mathé.

Vítězslav Švejdar. *Logika: neúplnost, složitost, nutnost*. Academia, 2002. Prístupné aj na http://www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf.