Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2017/2018

Obsah

I. O logike a tomto kurze Syntax výrokovej logiky **3**

1. Úvod **3**
1.1. O logike . . . 3
1.2. O kurze . . . 9

2. Výroková logika **10**
2.1. Opakovanie: Výroková logika v prirodzenom jazyku . . . 10
2.2. Syntax . . . 12

II. Sémantika výrokovej logiky **16**
2.3. Sémantika . . . 17
2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť . . . 20

III. Vyplývanie, ekvivalentné úpravy **26**
2.5. Vyplývanie . . . 27
2.6. Ekvivalencia . . . 30
2.6.1. Ekvivalentné úpravy . . . 32

2.6.2. Konjunktívna a disjunktívna normálna forma 35

IV. CNF. Tablový kalkul **37**
2.7. Kalkuly 40
2.8. Tablový kalkul 42
2.8.1. Korektnosť 47

V. Korektnosť a úplnosť tablového kalkulu **48**
2.8.2. Tablový dôkaz splniteľnosti 50
2.8.3. Hintikkova lema 51
2.8.4. Úplnosť 52

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

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

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

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

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

- **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**

I.8 Formálny jazyk

- **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]

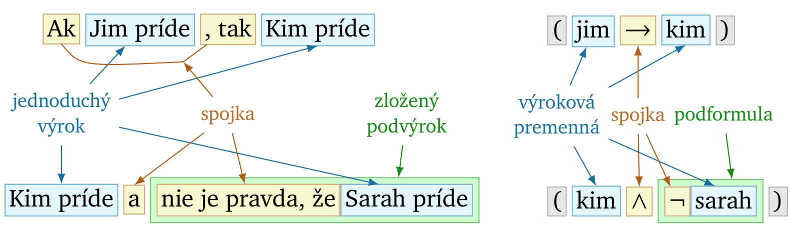
I.20 Syntax výrokovej logiky

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 $\neg$, $\wedge$, $\vee$, $\rightarrow$, (a), ani jej prvky tieto symboly neobsahujú;
- *logické* symboly (*logické spojky*): $\neg$, $\wedge$, $\vee$, $\rightarrow$
  (nazývané, v uvedenom poradí, *symbol negácie*, *symbol konjunkcie*, *symbol disjunkcie*, *symbol implikácie* a čítané „*nie*“, „*a*“, „*alebo*“, „*ak* . . . , *tak* . . . “);
- *pomocné* symboly: (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.

- 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. $(\neg(\text{kim} \land \text{sarah}) \to (\neg\text{kim} \lor \neg\text{sarah}))$.
- 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 $(A \land B)$, $(A \lor B)$ a $(A \to B)$ 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 $\mathcal{V}$?

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

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.*

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

2.3. Sémantika výrokovej logiky

II.1 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.2 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 2.11. 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.3 Ohodnotenie výrokových premenných

Príklad 2.12. Zoberme $t \neq f$ (napr. $t = 1, f = 0$), $\mathcal{V} = \{\text{a}, \text{á}, \text{ä}, \dots, \text{ž}, 0, \dots, 9, \_\}^+$.

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.4 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 2.13. 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:

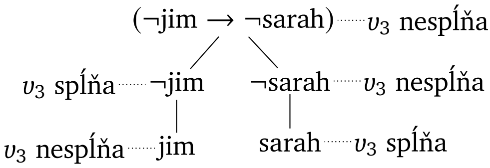
Formulu	jim	sarah	¬jim	¬sarah	(¬jim → ¬sarah)
ohodnotenie v_3	nespĺňa	spĺňa	spĺňa	nespĺňa	nespĺňa

II.5 Spĺňanie výrokových formúl — vytvárajúci strom

Príklad 2.13 (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.6 Spĺňanie výrokových formúl — program

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

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

- Veľmi podobne vieme zadefinovať splnenie matematicky.

II.7 Spĺňanie výrokových formúl — definícia

Definícia 2.14. 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 2.15. 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

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

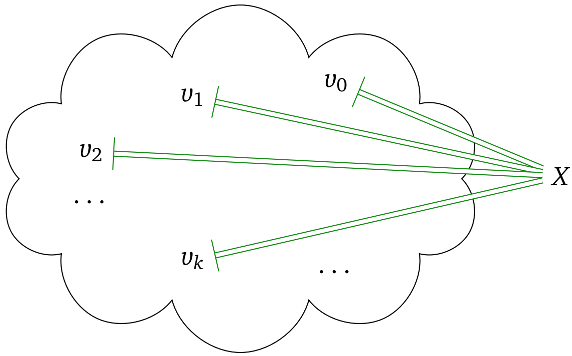
ohodnotenie v_3 spĺňa a ktoré nespĺňa.

deg(X)	v_3 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

- 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. $\mathcal{V}$.



Definícia 2.16. 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.11 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 2.17. *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.12 Tautológia — testovanie

Príklad 2.18. Zistime, či je $X = (\neg(p \wedge q) \rightarrow (\neg p \vee \neg q))$ tautológiou.

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

v							
p	q	$(p \wedge q)$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p \vee \neg q)$	$(\neg(p \wedge q) \rightarrow (\neg p \vee \neg q))$
f	f	$\not\models$	$\models$	$\models$	$\models$	$\models$	$\models$
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.13 Ohodnotenia zhodujúce sa na premenných formuly

Dôkaz. Indukciou na stupeň formuly X.

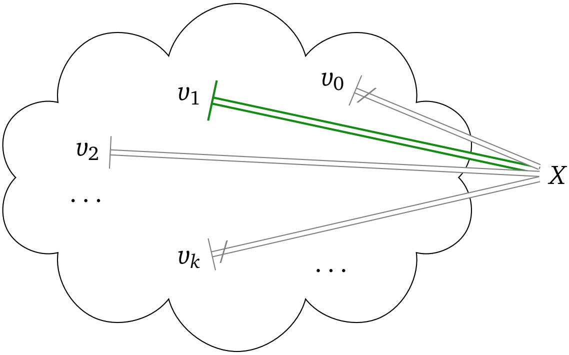
Báza: Nech X je stupňa 0. Podľa vety o jednoznačnosti rozkladu a definície stupňa musí byť $X = p$ pre nejakú výrokovú premennú. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na premenných v X, teda aj na p. Podľa definície spĺňania $v_1 \models p$ vtt $v_1(p) = t$ vtt $v_2(p) = t$ vtt $v_2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

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

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

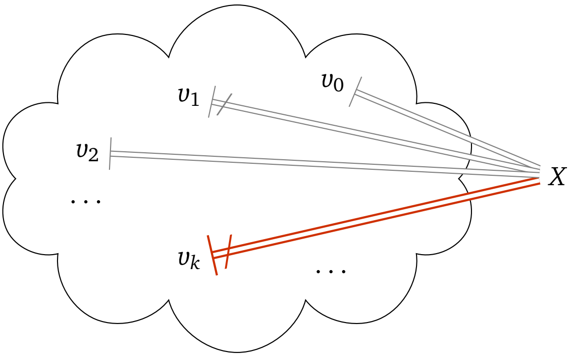
- $X = (A \wedge B)$ pre práve jednu dvojicu formúl A, B. Pretože $\deg(X) = \deg(A) + \deg(B) + 1 > \deg(A)$ aj $\deg(B)$, podľa ind. predpokladu pre A aj B tvrdenie platí. Podobne pre ďalšie binárne spojky.

□

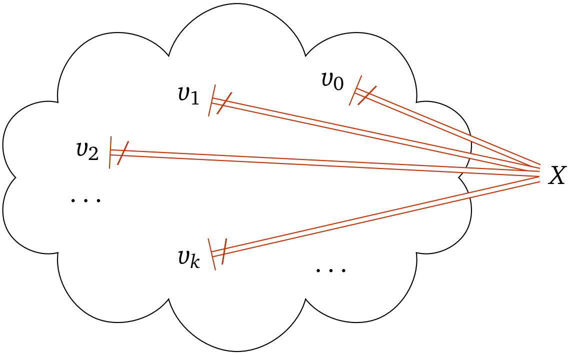


Definícia 2.19. Formulu X nazveme *splniteľnou*
vtt **nejaké** ohodnotenie výrokových premenných **spĺňa** X
(teda **existuje** také ohodnotenie výrokových premenných v, že $v \models X$).

II.15 Falzifikovateľnosť

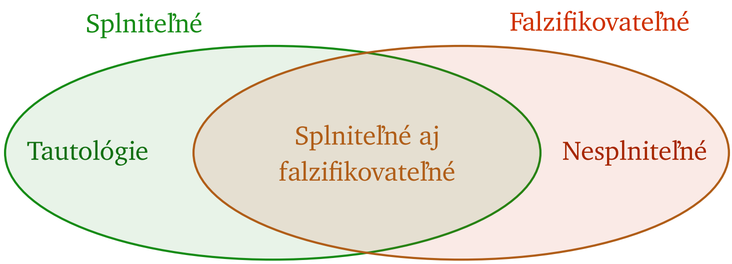


Definícia 2.20. Formulu X nazveme *falzifikovateľnou*
vtt **nejaké** ohodnotenie výrokových premenných **nespĺňa** X
(teda **existuje** také ohodnotenie výrokových premenných v, že $v \not\models X$).



Definícia 2.21. Formulu X nazveme *nesplniteľnou*
vtt **každé** ohodnotenie výrokových premenných **nespĺňa** X
(teda **pre každé** ohodnotenie výrokových premenných v platí $v \not\models X$).

II.17 „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.1
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 2.22. *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 2.23. *(Výrokovologickou) teóriou* nazývame každú množinu formúl.

Dohoda

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

Príklad 2.24. 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 2.25. 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 2.26. Aké ohodnotenie spĺňa (teda je modelom) T_{party}?

Tvrdenie 2.27. *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 2.28. Teória T je *súčasne výrokovologicky splniteľná* (skrátene *splniteľná*) vtt existuje aspoň jeden model T.

Teória je *nesplniteľná* vtt nie je splniteľná.

Príklad 2.29. T_{party} je súčasne splniteľná množina formúl.

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

III.5 Logické dôsledky a vyplývanie

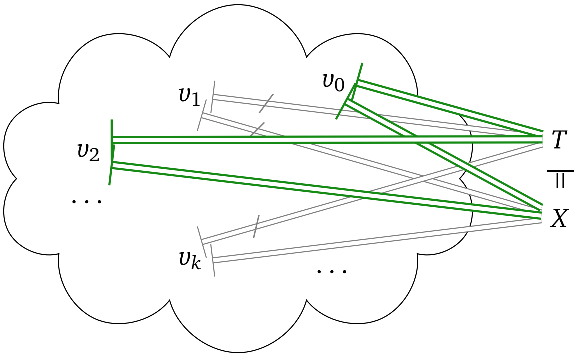
- Aký je *účel* teórií? Kedy je teória užitočná?
  – Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) <presentation> *doteraz neznáme skutočnosti* (teda nezapísané v teórii),
    ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

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

Príklad 2.30. Všimnime si, že v *každom* ohodnotení, ktoré spĺňa T_{party}, je splnená aj premenná *kim*.

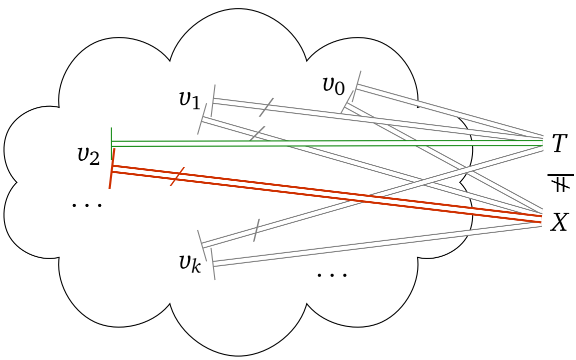
Ktorá ďalšia formula vyplýva z T_{party}?

III.6 Výrokovologické vyplývanie



Definícia 2.31 (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 2.32. Ktoré atomické formuly a ich negácie nevyplývajú z T_{party}?
Vyplýva z T_{party} formula $(kim \to jim)$?

III.8 Vyplývanie a (ne)splniteľnosť

Použitie SAT solvera na rozhodovanie vyplývania je založené na:

Tvrdenie 2.33. *Formula X výrokovologicky vyplýva z teórie T vtt množina $T_1 = T \cup \{\neg X\}$ je nesplniteľná.*

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

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

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

III.9 Nezávislosť

Definícia 2.34. 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 2.35. Ktorá atomická formula je nezávislá od T_{party}?
Je aj jej negácia nezávislá od T_{party}?

III.10 Vzťahy vyplývania, implikácií a tautológií

Tvrdenie 2.36. *Nech S a T sú teórie, $S \subseteq T$, A je formula. Ak $S \models A$, tak $T \models A$.*

Tvrdenie 2.37. *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.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 2.38. 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 $((X \to Y) \land (Y \to X))$.

Tvrdenie 2.39. *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 2.40. *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 2.41 (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 2.42. $A = \neg\neg(r \wedge q)$ $\quad B = (r \wedge q)$ $\quad X = (p \rightarrow \neg \boxed{\neg\neg(r \wedge q)})$

  $$\Downarrow$$

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

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

III.16 Pravidlá ekvivalentných úprav

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

    Príklad 2.43. $C = \neg\neg \boxed{p}$ $\qquad D = \boxed{p}$

    $$\Downarrow \qquad \Downarrow$$

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

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 2.44 (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 2.45 (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 2.46 (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 2.47. *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 2.48. *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.22 Ekvivalencie pre ekvivalentné úpravy

Veta 2.48 (Pokračovanie)**.**

$$
\begin{array}{rl}
(A \wedge A) \Leftrightarrow A & \textit{idempotencia} \\
(A \vee A) \Leftrightarrow A & \\[1em]
(A \wedge \top) \Leftrightarrow A & \textit{identita} \\
(A \vee \bot) \Leftrightarrow A & \\[1em]
(A \vee (A \wedge B)) \Leftrightarrow A & \textit{absorpcia} \\
(A \wedge (A \vee B)) \Leftrightarrow A & \\[1em]
(A \vee \neg A) \Leftrightarrow \top & \textit{vylúčenie tretieho} \\
(A \wedge \neg A) \Leftrightarrow \bot & \textit{spor} \\[1em]
(A \rightarrow B) \Leftrightarrow (\neg A \vee B) & \textit{nahradenie} \rightarrow
\end{array}
$$

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

Definícia 2.49.
- Výrokovú premennú alebo negáciou premennej nazývame *literál*.
- Disjunkciu literálov nazývame *klauzula* (tiež „klauza“).
- Hovoríme, že formula X je v *konjunktívnom normálnom tvare* (CNF), ak X je *konjunkciou* klauzúl.
- Hovoríme, že formula X je v *disjunktívnom normálnom tvare* (DNF), ak X je *disjunkciou* formúl, z ktorých každá je konjunkciou literálov.

Príklad 2.50. Ktoré z nasledujúcich formúl sú literálmi, klauzulami, sú v CNF, v DNF:

$$\begin{aligned}
A_1 &= p & A_6 &= ((p \wedge \neg q) \vee (\neg p \wedge r) \vee (\neg p \wedge q \wedge \neg r)) \\
A_2 &= \neg q & A_7 &= ((\neg p \vee q \vee \neg r) \wedge (q \rightarrow r)) \\
A_3 &= \Box & A_8 &= ((\neg p \vee \neg q) \wedge (p \vee r) \wedge (p \vee q \vee \neg r)) \\
A_4 &= (p \vee \neg q) & A_9 &= ((\neg p \vee (p \wedge r)) \wedge (p \vee q \vee \neg r)) \\
A_5 &= (p \wedge \neg q) & A_{10} &= ((\neg p \vee p \vee r) \wedge (\neg(p \vee q) \vee \neg r))
\end{aligned}$$

IV. prednáška

CNF. Tablový kalkul

12. marca 2018

IV.1 Existencia DNF a CNF

Veta 2.51. *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 $v_1, \ldots, v_n$ 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 $D = \bigvee_{1 \le i \le n} C_i$ 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:
   - $(A \to B) \quad \Leftrightarrow \quad (\neg A \lor B)$.
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 2.52. *Výsledná formula alg. CNF$_1$ je ekvivalentná s pôvodnou a je v CNF.*

IV.4 CNF — trochu lepší prístup

Príklad 2.53. 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. $((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee \neg\neg e)))$ [2 — deMorganovo pravidlo]

7. $((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee e)))$ [2 — dvojitá implikácia]

8. $(((\neg a \wedge b) \vee \neg c) \wedge ((\neg a \wedge b) \vee (\neg d \vee e)))$ [3 — distributívnosť]

9. $(((\neg a \vee \neg c) \wedge (b \vee \neg c)) \wedge ((\neg a \vee (\neg d \vee e)) \wedge (b \vee (\neg d \vee e))))$ [3]

10. $((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee (\neg d \vee e)) \wedge (b \vee (\neg d \vee e)))$ [4]

11. $((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee \neg d \vee e) \wedge (b \vee \neg d \vee e))$ [4 — asoc.]

IV.5 CNF — prečo iba *trochu* lepší prístup

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

- $A_2 = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2))$
  $C_2 = ((p_1 \vee p_2) \wedge (p_1 \vee q_2) \wedge (q_1 \vee p_2) \wedge (q_1 \vee p_2))$
  $A_2 \Leftrightarrow C_2, \quad \deg(A_2) = 3, \quad \deg(B_2) = 7$

- $A_3 = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee (p_3 \wedge q_3))$
  $C_3 = ((p_1 \vee p_2 \vee p_3) \wedge (p_1 \vee q_2 \vee p_3) \wedge (q_1 \vee p_2 \vee p_3) \wedge (q_1 \vee p_2 \vee p_3) \wedge (p_1 \vee p_2 \vee q_3) \wedge (p_1 \vee q_2 \vee q_3) \wedge (q_1 \vee p_2 \vee q_3) \wedge (q_1 \vee p_2 \vee q_3))$ $A_3 \Leftrightarrow C_3$,
  $\deg(A_3) = 5, \qquad \deg(C_3) = 23$

- $A_n = ((p_1 \wedge q_1) \vee \cdots \vee (p_n \wedge q_n))$
  Koľko klauzúl bude obsahovať C_n?
  Akého bude stupňa?

IV.6 CNF — obmedzenie exponenciálneho rastu

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

1. Zoberme *nové* výrokové premenné $r_1, \ldots, r_n, s$

2. Vyjadrime, že r_i je ekvivalentným zástupcom konjunkcie $(p_i \wedge q_i)$: $(r_i \leftrightarrow (p_i \wedge q_i))$

3. Použime r_i na vyjadrenie, že s je ekvivalentným zástupcom disjunkcie A_n: $(s \leftrightarrow (r_1 \vee \cdots \vee r_n))$

4. A_n teda môžeme nahradiť formulou $((s \leftrightarrow (r_1 \vee \cdots \vee r_n)) \wedge (r_1 \leftrightarrow (p_1 \wedge q_1)) \wedge \cdots \wedge (r_n \leftrightarrow (p_n \wedge q_n)) \wedge s)$

Ekvivalentnými úpravami

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

spolu iba $4 \cdot n$

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

IV.9 Ekvivalencia syntakticky vs. sémanticky

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

IV.10 Kalkuly — dokazovanie vyplývania syntakticky

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

  tablový — stromový, prirodzenejší

  rezolvenciu — lineárny, strojový

2.8. Tablový kalkul

IV.11 Dôkaz vyplývania sporom v slovenčine

Príklad 2.54. Dokážme, že z $T'_{\text{party}} = \{ (kim \rightarrow (jim \land \neg sarah)), (eva \rightarrow kim) \}$ vyplýva $(sarah \rightarrow \neg eva)$. Poďme na to sporom:

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

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

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

Platí teda (8) a podľa (1) ďalej môžu nastať dva prípady: (9) $v \not\models kim$, ktorý je však v spore s (8), alebo (10) $v \models (jim \land \neg sarah)$. 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 $(sarah \rightarrow \neg eva)$. □

IV.12 Tablová notácia pre dôkazy

Dôkaz stručne zapíšeme v tablovej notácii:

- **T** X označuje fakt, že v spĺňa X.
- **F** X označuje fakt, že v nespĺňa X.
- Ak z niektorého predchádzajúceho faktu o formule X priamo *z definície 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 2.55.

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

IV.14 Spĺňanie a priame podformuly

Pozorovanie 2.56. *Nech v je ľubovoľné ohodnotenie výrokových premenných. Nech X a Y sú ľubovoľné formuly.*

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

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

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

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

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

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

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

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

Definícia 2.57. Nech X je formula výrokovej logiky.
Postupnosti symbolov $\mathbf{T}\,X$ a $\mathbf{F}\,X$ nazývame *označené formuly*.

Definícia 2.58. Nech v je ohodnotenie výrokových premenných a X je formula. Potom

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

Dohoda

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

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

IV.16 Tablové pravidlá

Podľa pozorovania 2.56 a definície 2.58 môžeme sformulovať pravidlá pre označené formuly:

$$\frac{\alpha}{\begin{array}{c}\alpha_1\\ \alpha_2\end{array}} \qquad \frac{\beta}{\beta_1 \mid \beta_2}$$

$$\frac{\mathbf{T}(X \wedge Y)}{\begin{array}{c}\mathbf{T}\,X\\ \mathbf{T}\,Y\end{array}} \qquad \frac{\mathbf{F}(X \wedge Y)}{\mathbf{F}\,X \mid \mathbf{F}\,Y} \qquad \frac{\mathbf{T}\,\neg X}{\mathbf{F}\,X}$$

$$\frac{\mathbf{F}(X \vee Y)}{\begin{array}{c}\mathbf{F}\,X\\ \mathbf{F}\,Y\end{array}} \qquad \frac{\mathbf{T}(X \vee Y)}{\mathbf{T}\,X \mid \mathbf{T}\,Y} \qquad \frac{\mathbf{F}\,\neg X}{\mathbf{T}\,X}$$

$$\frac{\mathbf{F}(X \to Y)}{\begin{array}{c}\mathbf{T}\,X\\ \mathbf{F}\,Y\end{array}} \qquad \frac{\mathbf{T}(X \to Y)}{\mathbf{F}\,X \mid \mathbf{T}\,Y}$$

IV.17 Jednotný zápis označených formúl typu α

Definícia 2.59 (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
$\mathbf{T}(X \land Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
$\mathbf{F}(X \lor Y)$	$\mathbf{F}X$	$\mathbf{F}Y$
$\mathbf{F}(X \to Y)$	$\mathbf{T}X$	$\mathbf{F}Y$
$\mathbf{T}\lnot X$	$\mathbf{F}X$	$\mathbf{F}X$
$\mathbf{F}\lnot X$	$\mathbf{T}X$	$\mathbf{T}X$

Pozorovanie 2.60 (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 2.61 (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 2.62 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie výrokových premenných.*
Potom v spĺňa β vtt v spĺňa β_1 alebo v spĺňa β_2.

IV.19 Tablo pre množinu označených formúl

Definícia 2.63. *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:

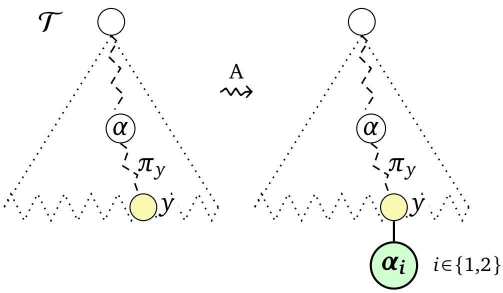
- Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu A^+ z S^+ je tablom pre S^+.

- 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^+.

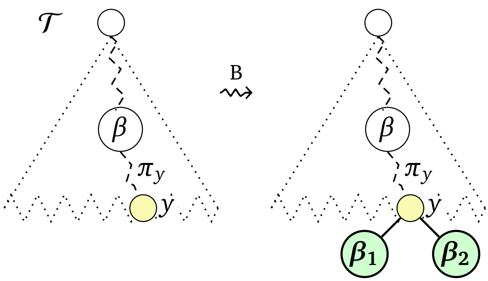
IV.20 Tablá, tablové pravidlá, operácie rozšírenia

Operácia priameho rozšírenia | **Pravidlá a označené formuly v nich**



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

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



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

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

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

IV.21 Uzavretosť a otvorenosť vetvy a tabla

Definícia 2.64. *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 $X^+ \in \mathrm{formulas}(\pi)$.

Definícia 2.65. *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 2.66 (Korektnosť tablového kalkulu)**.** *Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+.*
Potom je množina S^+ nesplniteľná.

Dôsledok 2.67. *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 2.69. *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 2.70. 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 2.71 (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 2.72 (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. $\square$

2.8.2. Tablový dôkaz splniteľnosti

V.5 Úplná vetva a tablo

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

Definícia 2.73 (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 2.74. 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 2.75 (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 2.76. 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 2.77. *Nech π je úplná otvorená vetva nejakého tabla $\mathcal{T}$. Potom množina všetkých formúl na π je nadol nasýtená.*

Lema 2.78 (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 2.60).
  - 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 2.62). □

2.8.4. Úplnosť

V.10 Úplnosť

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

Veta 2.79 (o úplnosti)**.** *Nech S^+ je konečná nesplniteľná množina označených formúl.*
Potom existuje uzavreté tablo pre S^+.

Dôsledok 2.80. *Nech S je konečná teória a X je formula.*
Ak $S \vDash X$, tak $S \vdash X$.

Dôsledok 2.81. *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. □

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.