Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2016/2017

Obsah

I. prednáška

O logike a tomto kurze
Syntax výrokovej logiky

20. februára 2017

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*
- Z teórie môžeme odvodiť *logické dôsledky*, ktoré nie sú priamo jej súčasťou, ale logicky z nej *vyplývajú*

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

(P1) Sára nepôjde na párty, ak pôjde Kim.

(P2) Jim pôjde na párty, len ak pôjde Kim.

(P3) Sára nepôjde bez Jima.

I.3 Možné svety a logické dôsledky

- Tvrdenie rozdeľuje množinu **možných stavov sveta/svetov** na tie, v ktorých je pravdivé (**modely**), a tie, v ktorých je nepravdivé

- Teória môže mať viacero modelov (ale aj žiaden)

  Príklad 1.2. Vymenujme možné stavy prítomnosti Kim, Jima a Sáry 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:
Sára 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 Sára (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 Sára.
Teda: Ak na párty pôjde Jim, nepôjde Sára.

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

I.5 Usudzovacie pravidlá, korektnosť, dedukcia

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

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

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

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

- *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)
- Na tomto predmete sa budeme zaoberať iba dedukciou

I.8 Formalizácia

- 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 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

- 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?

  $$k = 3 \cdot m$$
  $$k + m = 12$$

- Stretli ste sa už aj s formálnym jazykom výrokovej logiky

  Príklad 1.5. Sformalizujme náš párty príklad:

  (P0) Niekto z trojice Kim, Jim, Sára pôjde na párty.

  (P1) Sára nepôjde na párty, ak pôjde Kim.

  (P2) Jim pôjde na párty, len ak pôjde Kim.

  (P3) Sára nepôjde bez Jima.

I.10 Výpočtová logika — automatizácia usudzovania

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

  korektné — odvodzujú iba logické dôsledky

  úplné — umožňujú odvodiť všetky logické dôsledky

- 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.11 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.12

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

A: premisou, C: záverom,

B: logickým dôsledkom, D: implikáciou.

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

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

A: abdukcia, C: formalizácia, E: indukcia,

B: interpretácia, D: dedukcia, F: inferencia.

2. O tomto kurze

2.1. Sylabus

I.13 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

2.2. Organizácia kurzu

I.14 Organizácia kurzu — rozvrh, kontakty, pravidlá

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

3. Výroková logika

3.1. Opakovanie: Výroková logika v prirodzenom jazyku

I.15 Opakovanie: Výroková logika v prirodzenom jazyku

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

Príklady 3.1.

- 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.16 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 3.2. 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.17 (Meta) matematika výrokovej logiky

- Stredoškolský prístup príliš neoddeľuje samotný jazyk výrokovej logiky od jeho významu a vlastne ani jednu stránku jasne nedefinuje
- V tomto kurze sa budeme snažiť byť presní
- Pojmy z výrokovej logiky budeme *definovať matematicky* — ako množiny, postupnosti, funkcie, atď.
- Na praktických cvičeniach veľa pojmov zadefinujete programátorsky: ako reťazce, slovníky, triedy a ich metódy

- 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)

3.2. Syntax výrokovej logiky

I.18 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

I.19 Symboly jazyka výrokovej logiky

Definícia 3.3 (podľa [Smullyan, 1979, I.1.1], rovnako ďalšie). *Symbolmi jazyka výrokovej logiky* sú:

- *výrokové premenné* z nejakej nekonečnej spočítateľnej množiny $\mathcal{V} = \{p_1, p_2, \ldots, p_n, \ldots\}$, ktorej prvkami nie sú symboly $\neg$, $\land$, $\lor$, $\to$, (a), ani jej prvky tieto symboly neobsahujú;
- *logické* symboly (*logické spojky*): $\neg$, $\land$, $\lor$, $\to$ (nazývané, v uvedenom poradí, „*nie*“, „*a*“, „*alebo*“, „*ak* . . . , *tak* . . . “);
- *pomocné* symboly: (a) (*ľavá zátvorka* a *pravá zátvorka*).

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

Spojky $\land$, $\lor$, $\to$ sú *binárne* (majú dva argumenty).

I.20 Symboly, výrokové premenné

Symbol je základný pojem, ktorý matematicky nedefinujeme.

Je o čosi všeobecnejší ako pojem znak.

Príklad 3.4. 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, Sára.

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

Výrokové premenné formalizujú jednoduché výroky.

I.21 Formuly výrokovej logiky

Definícia 3.5. *Formulou výrokovej logiky* (skrátene *formulou*) nad množinou výrokových premenných $\mathcal{V}$ je postupnosť symbolov vytvorená nasledovnými pravidlami:

- Každá výroková premenná je formulou (voláme ju *atomická f.*).
- Ak A je formulou, tak aj $\neg A$ je formulou (*negácia* formuly A).
- Ak A a B sú formulami, tak aj $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$ sú formulami (*konjunkcia*, *disjunkcia*, *implikácia* formúl A a B).

Nič iné nie je formulou.

Dohoda
Formuly označujeme veľkými písmenami A, B, C, X, Y, Z, podľa potreby aj s dolnými indexmi. Množinu všetkých formúl označíme $\mathcal{E}$.

Formula je matematickou formalizáciou zloženého výroku.

II. prednáška
Sémantika výrokovej logiky

27. februára 2017

II.1 Alternatívna definícia formuly

Definícia 3.6. *Vytvárajúcou postupnosťou* je ľubovoľná konečná postupnosť, ktorej každý člen je výroková premenná, alebo má tvar $\neg A$, pričom A je nejaký predchádzajúci člen postupnosti, alebo má jeden z tvarov $(A \land B)$, $(A \lor B)$, $(A \rightarrow B)$, kde A a B sú nejaké predchádzajúce členy postupnosti.

Definícia 3.7. Postupnosť symbolov A je *formula*, ak existuje vytvárajúca postupnosť, ktorej posledným prvkom je A. Túto postupnosť voláme tiež vytvárajúca postupnosť pre A.

Príklad 3.8. Nájdime vytvárajúcu postupnosť pre formulu $(\neg p \rightarrow (p \lor q))$.

II.2

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: $(p \land \neg(q \rightarrow r))$, C: $\neg(\neg(\neg p))$.

II.3 Jednoznačnosť rozkladu formúl výrokovej logiky

Tvrdenie 3.9 (o jednoznačnosti rozkladu)**.** *Pre každú formulu X platí práve jedna z nasledujúcich možností:*

- *X je výroková premenná.*
- *Existuje práve jedna formula A taká, že $X = \neg A$.*

- *Existujú práve jedna dvojica formúl A, B a jedna spojka $b \in \{\wedge, \vee, \rightarrow\}$ také, že $X = (A\, b\, B)$.*

Príklad 3.10. Jednoznačnosť rozkladu by pri neopatrnej definícii formuly *nemusela platiť*. Nájdime takú definíciu „formuly“ a „formulu“, ktorá sa nedá jednoznačne rozložiť:

> *„Formulou“ výrokovej logiky* nad mn. výrok. prem. $\mathcal{V}$ je postupnosť symbolov vytvorená podľa nasledovných pravidiel: …

II.4 Vytvárajúci strom formuly

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

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

Príklad 3.12. Nájdime vytvárajúci strom pre formulu $((p \wedge q) \rightarrow ((\neg p \vee \neg\neg q) \vee (q \rightarrow \neg p)))$.

II.5 Podformuly

Definícia 3.13 (Priama podformula)**.**

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

Definícia 3.14 (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.

Príklad 3.15. Vymenujme priame podformuly a podformuly $((p \lor \neg q) \land \neg(q \to p))$.

Spomeňte si II.2
Sú nasledujúce tvrdenia pravdivé? Odpovedzte áno/nie.

a) Vďaka jednoznačnosti rozkladu má každá formula práve jednu priamu podformulu.

b) Postorderový výpis vytvárajúceho stromu formuly X je vytvárajúcou postupnosťou tejto formuly.

II.7 Stupeň formuly

Definícia 3.16 (Stupeň formuly [deg(X)]).

- 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 3.16 (Stupeň formuly [deg(X)] stručne, symbolicky).

- $\deg(p) = 0$ pre každú $p \in \mathcal{V}$,
- $\deg(\neg A) = \deg(A) + 1$ pre každú $A \in \mathcal{E}$,
- $\deg((A \land B)) = \deg((A \lor B)) = \deg((A \to B)) = \deg(A) + \deg(B) + 1$ pre všetky $A, B \in \mathcal{E}$.

Príklad 3.17. Aký je stupeň formuly $((p \lor \neg q) \land \neg(q \to p))$?

Veta 3.18 (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 ($P = \mathcal{E}$).

Príklad 3.19. Dokážme:

> Množina všetkých formúl vo vytvárajúcom strome formuly X
> je rovná zjednoteniu množiny všetkých podformúl X s $\{X\}$.

Vyskúšajte si II.3
Stupeň formuly $((\neg p \to q) \land q)$ je ....

II.10 Množina výrokových premenných formuly

Definícia 3.20 (Množina výrok. prem. formuly $[\mathrm{vars}(X)]$)**.**

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

Definícia 3.20 ($\mathrm{vars}(X)$ stručnejšie)**.**

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

3.3. Sémantika výrokovej logiky

II.11 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.12 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 dáždnik, $\ldots$).
- Ako vieme *programátorsky* popísať pravdivosť výrokových premenných v nejakom stave sveta? A *matematicky*?

Definícia 3.21. 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.13 Ohodnotenie výrokových premenných

Príklad 3.22. Zoberme $t \neq f$ (napr. $t = 1, f = 0$), $\mathcal{V} = \{$a, á, ä, ..., ž, 0, ..., 9, _$\}^+$

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

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

Minulotýždňové ráno opisuje ohodnotenie v_2, kde okrem iného

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

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

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

Prečo „okrem iného“?

II.14 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 3.23. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{$a, ..., z$\}^+$, také že

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

Spĺňa svet s týmto ohodnotením formulu (¬jim → ¬sara)?

Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

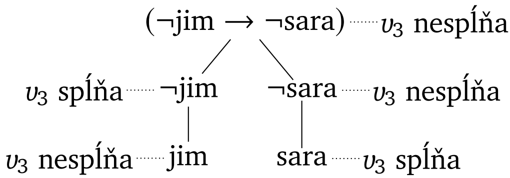
Formulu	jim	sara	¬jim	¬sara	(¬jim → ¬sara)
ohodn. v_3	nespĺňa	spĺňa	spĺňa	nespĺňa	nespĺňa

II.15 Spĺňanie výrokových formúl — vytvárajúci strom

Príklad 3.23 (pokračovanie).

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

Iná možnosť je použiť vytvárajúci strom:



II.16 Spĺňanie výrokových formúl — program

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

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

- Veľmi podobne vieme zadefinovať splnenie matematicky.

II.17 Spĺňanie výrokových formúl — definícia

Definícia 3.24. 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*.

II.18 Spĺňanie výrokových formúl — príklad

Príklad 3.25. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{\mathrm{a}, \ldots, \mathrm{z}\}^+$, také že

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

Zistime, ktoré z formúl

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

ohodnotenie v_3 spĺňa a ktoré nespĺňa.

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

II.19 Spĺňanie výrokových formúl

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. $\mathcal{V}$.

Tvrdenie 3.26. *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 výrokových premenných vyskytujúcich sa v X, platí $v_1 \models X$ vtt $v_2 \models X$.*

II.20 Spĺňanie výrokových formúl

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 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.

□

3.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť

II.21 Tautológia, (ne)splniteľnosť, falzifikovateľnosť

Definícia 3.27. Formulu X nazveme *tautológiou* (skrátene $\models X$) vtt je splnená pri každom ohodnotení výrokových premenných.

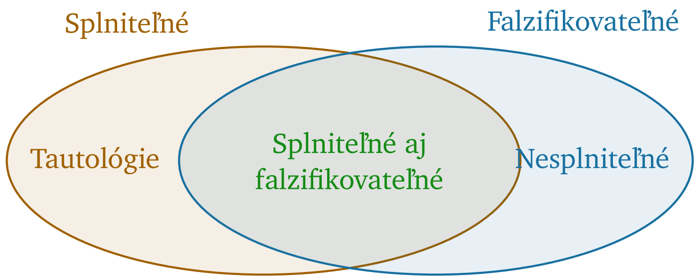
Príklad 3.28. $(p \vee \neg p)$, $\neg(p \wedge \neg p)$, $(\neg\neg p \to p)$, $(p \to \neg\neg p)$, $(p \to (q \to p))$, $((p \to (q \to r)) \to ((p \to q) \to (p \to r)))$, $((\neg q \to \neg p) \to (p \to q))$

Definícia 3.29. Formulu X nazveme *splniteľnou* vtt je splnená pri aspoň jednom ohodnotení výrokových premenných.

Formulu X nazveme *nesplniteľnou* vtt nie je splniteľná.

Formulu X nazveme *falzifikovateľnou* vtt je nesplnená pri aspoň jednom ohodnotení výrokových premenných.

II.22 „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.4

Ak formula *nie* je falzifikovateľná, je:

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

III. prednáška
Vyplývanie, ekvivalentné úpravy

6. marca 2017

III.1 Tautológie a (ne)splniteľnosť

Tvrdenie 3.30. *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 boolovskom ohodnotení (podľa definície spĺňania pri ohodnotení), a teda neexistuje žiadne ohodnotenie, pri ktorom by $\neg X$ bola splnená, teda $\neg X$ nie je splniteľná.

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

III.2 Teórie

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

Definícia 3.31. *(Výrokovologickou) teóriou* nazývame každú množinu formúl.

Dohoda

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

Príklad 3.32. Formalizácia problému pozývania známych na párty je teóriou:

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

III.3 Splnenie teórie, model

Pojem spĺňania sa jednoducho rozšíri na teórie.

Definícia 3.33. Nech T je teória. Ohodnotenie v *spĺňa teóriu* T (skrátene $v \models T$) vtt v spĺňa každú formulu X z množiny T.

Spĺňajúce ohodnotenie nazývame *modelom* teórie T.

Príklad 3.34. Aké ohodnotenie spĺňa (teda je modelom) T_{party}?

Tvrdenie 3.35. *Splnenie teórie T pri ohodnotení výrokových premenných závisí iba od ohodnotenia výrokových premenných, ktoré sa vyskytujú vo formulách v T.*

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

3.5. 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 3.36. Teória T je *súčasne (výrokovologicky) splniteľná* vtt existuje aspoň jeden model T, (t.j. ohodnotenie výrokových premenných, ktoré spĺňa všetky formuly z T).

Teória je *nesplniteľná* vtt nie je splniteľná.

Príklad 3.37. T_{party} je súčasne splniteľná množina formúl.

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

III.5 Výrokovologické vyplývanie

- Aký je účel teórií? Kedy je teória užitočná?
- Keď pomocou z nej dokážeme odvodiť doteraz neznáme skutočnosti, zistiť *uvažovaním* (alebo počítaním), čo vo svete platí, aj keď to priamo v teórii nie je zapísané.

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

Príklad 3.38. Všimnime si, že v *každom* ohodnotení, ktoré spĺňa T_{party}, je premenná kim pravdivá.

Definícia 3.39 (Výrokovologické vyplývanie)**.** Z teórie T *výrokovologicky vyplýva* formula X (X je *výrokovologickým dôsledkom* T, skrátene $T \models X$) vtt každé ohodnotenie výrokových premenných, ktoré spĺňa T, spĺňa aj X.

III.6 Vyplývanie a (ne)splniteľnosť

Tvrdenie 3.40. *Formula X výrokovologicky vyplýva z teórie T vtt množina $T_1 = T \cup \{\neg X\}$ je nesplniteľná.*

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

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

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

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

III.7 Nezávislosť

Definícia 3.41. 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 3.42. Atomická formula jim je nezávislá od T_{party}.

III.8 Vzťahy vyplývania, implikácií a tautológií

Tvrdenia

- $T \cup \{A\} \models B$ vtt $T \models A \to B$
- $\{\} \models A$ vtt $\models A$ (A je tautológia)
- Nasledujúce tvrdenia sú ekvivalentné:
  - $\{A_1, A_2, \ldots, A_n\} \models B$
  - $\{((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n)\} \models B$
  - $\{\} \models ((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n) \to B)$
  - $\models (((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n) \to B)$

III.9 Hlasujte

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

3.6. Ekvivalencia formúl

III.10 Ekvivalencia formúl

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

Definícia 3.43. Dve formuly X a Y sú *(výrokovologicky) ekvivalentné* vtt pre každé ohodnotenie v výrokových premenných platí,
že v spĺňa X vtt v spĺňa Y.

Ako súvisí ekvivalencia formúl so „spojkou" *práve vtedy, keď* ($\leftrightarrow$)?

Dohoda
Formulu $((X \to Y) \wedge (Y \to X))$ skrátene zapíšeme $(X \leftrightarrow Y)$.

Tvrdenie 3.44. *Formuly X a Y sú výrokovologicky ekvivalentné vtt formula $(X \leftrightarrow Y)$ je tautológia.*

III.11 **Asociativita a komutativita konjunkcie a disjunkcie**

Tvrdenie 3.45 (Asociativita a komutativita $\land$ a $\lor$). *Nech A_1, A_2, A_3 sú formuly.*
Nasledujúce dvojice formúl sú ekvivalentné:

- $((A_1 \land A_2) \land A_3)$ *a* $(A_1 \land (A_2 \land A_3))$,
- $((A_1 \lor A_2) \lor A_3)$ *a* $(A_1 \lor (A_2 \lor A_3))$.
- $(A_1 \land A_2)$ *a* $(A_2 \land A_1)$,
- $(A_1 \lor A_2)$ *a* $(A_2 \lor A_1)$,

3.7. Ekvivalentné úpravy

III.12 **Ekvivalentné úpravy**

Na Matematike (1) ste ekvivalente upravovali formuly.

Cieľom je zvyčajne formulu zjednodušiť alebo upraviť do požadovaného tvaru (napr. vstup pre SAT solver), prípadne ukázať, že je tautológia upravením na známu tautológiu.

Čo to ale vlastne je ekvivalentná úprava?

Definícia 3.46. Zobrazenie $u\colon \mathcal{E} \to \mathcal{E}$ nazveme *ekvivalentnou úpravou* vtt pre každú formulu A platí, že formuly A a $u(A)$ sú ekvivalentné.

Príklad *syntaktickej manipulácie* formúl s predvídateľným sémantickým výsledkom.

III.13 **Substitúcia a ekvivalentné úpravy**

Oba druhy ekvivalentných úprav sú založené na *substitúcii*.

Definícia 3.47 (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.

Veta 3.48 (Ekvivalentné úpravy). *Nech X je formula, A a B sú ekvivalentné formuly.*
Potom X a $X[A|B]$ sú tiež ekvivalentné.

Tvrdenie 3.49. *Nech X je tautológia, a výroková premenná a Y ľubovoľná formula.*
Potom $X[a|Y]$ je tiež tautológia.

III.14 Ekvivalentné úpravy

Ekvivalentné úpravy zvyčajne pozostávajú z kombinácie:

- nahradenia podformuly A vo formule X formulou B, ktorá je ekvivalentná s A;

  Príklad 3.50. $A = \neg\neg p \qquad B = p \qquad (q \to \neg \neg\neg p) \rightsquigarrow (q \to \neg p)$

- nahradenia formuly, ktorá vznikne dosadením formuly A za nejakú výrokovú premennú p vo formule X,
  formulou, ktorá vznikne dosadením A za rovnakú premennú vo formule Y ekvivalentnej s X.

  Príklad 3.51. $(\neg(r \to s) \wedge \neg q) \quad \rightsquigarrow \quad \neg((r \to s) \vee q)$

  $X = (\neg p \wedge \neg q) \qquad Y = \neg(p \vee q)$

  $A = (r \to s)$

III.15 Ekvivalencie pre ekvivalentné úpravy

Veta 3.52. *Nech A, B a C sú ľubovoľné formuly, $\top$ je ľubovoľná tautológia a $\bot$ je ľubovoľná nesplniteľná formula.*
Nasledujúce dvojice formúl sú ekvivalentné:

$(A \wedge (B \wedge C))$ *a* $((A \wedge B) \wedge C)$	*asociatívnosť*
$(A \vee (B \vee C))$ *a* $((A \vee B) \vee C)$	
$(A \wedge (B \vee C))$ *a* $((A \wedge B) \vee (A \wedge C))$	*distributívnosť*
$(A \vee (B \wedge C))$ *a* $((A \vee B) \wedge (A \vee C))$	
$(A \wedge B)$ *a* $(B \wedge A)$	*komutatívnosť*
$(A \vee B)$ *a* $(B \vee A)$	
$\neg(A \wedge B)$ *a* $(\neg A \vee \neg B)$	*de Morganove*
$\neg(A \vee B)$ *a* $(\neg A \wedge \neg B)$	*pravidlá*
$\neg\neg A$ *a* A	*dvojitá negácia*

Veta 3.52 (Pokračovanie)**.**

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

3.8. Konjunktívna a disjunktívna normálna forma

Dohoda

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

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

Definícia 3.53.
- Výrokovú premennú alebo negáciou premennej nazývame *literál*. Disjunkciu literálov nazývame *klauzula* (tiež „klauza“).
- Hovoríme, že formula X je v *disjunktívnom normálnom tvare* (DNF), ak X je disjunkciou formúl, z ktorých každá je konjunkciou literálov.
- Hovoríme, že formula X je v *konjunktívnom normálnom tvare* (CNF), ak X je konjunkciou klauz (formúl, z ktorých každá je disjunkciou literálov).

Príklad 3.54.
- Literály: p, $\neg q$, ...
- Klauzuly: $(p \lor \neg q)$, ale aj p, $\bot$
- DNF: $((p \land \neg q) \lor (\neg p \land r) \lor (\neg p \land q \land \neg r))$, ale aj $(p \land \neg q)$, $(p \lor \neg q)$, q, $\neg p$
- CNF: $((\neg p \lor \neg q) \land (p \lor r) \land (p \lor q \lor \neg r))$, ale aj $(p \lor \neg q)$, $(p \land \neg q)$, q, $\neg p$

IV. prednáška
CNF, kalkuly
13. marca 2017

IV.1 Zápis ekvivalentnosti formúl

Definícia 3.55. Formuly A a B sú v relácii $\Leftrightarrow$ vtt
pre každé ohodnotenie v platí $v \models A$ vtt $v \models B$,
teda keď formuly A a B sú ekvivalentné.

Veta 3.56. *Relácia $\Leftrightarrow$ na formulách je reláciou ekvivalencie, teda je reflexívna, symetrická a tranzitívna.*

IV.2 Zápis ekvivalentnosti formúl

Dohoda

- Ak formuly A a B sú ekvivalentné a B vznikne substitúciou podľa viet 3.48 a 3.52, názov/skratku substituovaného páru ekvivalentných podformúl zapíšeme nad symbol $\Leftrightarrow$, napríklad:

$$(A \land \neg\neg B) \overset{\text{dvoj.neg.}}{\Leftrightarrow} (A \land B)$$

- Zápisom $A_1 \Leftrightarrow A_2 \Leftrightarrow \cdots \Leftrightarrow A_n$ vyjadrujeme, že $A_i \Leftrightarrow A_{i+1}$ pre každé $1 \leq i < n$.

IV.3 Existencia DNF, CNF

Veta 3.57.
1. *Ku každej formule X existuje ekvivalentná formula A v disjunktívnom normálnom tvare.*
2. *Ku každej formule X existuje ekvivalentná formula B v konjunktívnom normálnom tvare.*

Dôkaz. 1. Zoberme všetky ohodnotenia v_i také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné q nevyskytujúce sa v 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 premennú p z X. Očividne formula $A = \bigvee_i C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).

2. K $\neg X$ teda existuje ekvivalentná formula A_1 v DNF. Znegovaním A_1 a aplikáciou de Morganových pravidiel dostaneme formulu B v CNF, ktorá je ekvivalentná s X. □

IV.4 CNF – trochu lepší prístup

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

  CNF je konjunkcia disjunkcií literálov — výrokových premenných alebo ich negácií

  Teda:

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

IV.5 CNF – trochu lepší prístup

Algoritmus CNF$_1$

1. Prepíšeme implikácie:

- $(A \rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$.

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

3. „Roznásobíme“ $\wedge$ s $\vee$ podľa distributívnosti a komutatívnosti:
   - $(A \vee (B \wedge C)) \quad \Leftrightarrow \quad ((A \vee B) \wedge (A \vee C))$
   - $((B \wedge C) \vee A) \quad \Leftrightarrow (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C)) \Leftrightarrow ((B \vee A) \wedge (A \vee C)) \Leftrightarrow \quad ((B \vee A) \wedge (C \vee A))$

4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

Tvrdenie 3.58. *Výsledná formula alg. CNF$_1$ je ekvivalentná s pôvodnou a je v CNF.*

IV.6 CNF – trochu lepší prístup

Príklad 3.59. $((a \vee \neg b) \rightarrow \neg(c \vee (d \wedge \neg e)))$

<all> $\overset{1}{\Leftrightarrow} (\neg(a \vee \neg b) \vee \neg(c \vee (d \wedge \neg e)))$

<all> $\overset{2}{\Leftrightarrow} ((\neg a \wedge \neg\neg b) \vee \neg(c \vee (d \wedge \neg e)))$

<all> $\overset{2}{\Leftrightarrow} ((\neg a \wedge b) \vee \neg(c \vee (d \wedge \neg e)))$

<all> $\overset{2}{\Leftrightarrow} ((\neg a \wedge b) \vee (\neg c \wedge \neg(d \wedge \neg e)))$

<all> $\overset{2}{\Leftrightarrow} ((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee \neg\neg e)))$

<all> $\overset{2}{\Leftrightarrow} ((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee e)))$

<all> $\overset{3}{\Leftrightarrow} (((\neg a \wedge b) \vee \neg c) \wedge ((\neg a \wedge b) \vee (\neg d \vee e)))$

<all> $\overset{2\times 3}{\Leftrightarrow} (((\neg a \vee \neg c) \wedge (b \vee \neg c)) \wedge ((\neg a \vee (\neg d \vee e)) \wedge (b \vee (\neg d \vee e))))$

<all> $\overset{4}{\Leftrightarrow} ((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee (\neg d \vee e)) \wedge (b \vee (\neg d \vee e)))$

<all> $\overset{2\times 4}{\Leftrightarrow} ((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee \neg d \vee e) \wedge (b \vee \neg d \vee e))$

IV.7 CNF – trochu lepší prístup

- Algoritmus CNF_1 je jednoduchý, ale nie vždy výhodný
- Všimnite si:
  - Z formuly $((p_1 \land q_1) \lor (p_2 \land q_2))$ s 2 konjunkciami dostaneme $((p_1 \lor p_2) \land (p_1 \lor q_2) \land (q_1 \lor p_1) \land (q_1 \lor q_2))$ so 4 klauzulami
  - Z formuly $((p_1 \land q_1) \lor (p_2 \land q_2) \lor (p_3 \land q_3))$ s 3 konjunkciami dostaneme $((p_1 \lor p_2 \lor p_3) \land (p_1 \lor p_2 \lor q_3) \land (p_1 \lor q_2 \lor p_3) \land (p_1 \lor q_2 \lor q_3) \land (q_1 \lor p_2 \lor p_3) \land (q_1 \lor p_2 \lor q_3) \land (q_1 \lor q_2 \lor p_3) \land (q_1 \lor q_2 \lor q_3))$ s 8 klauzulami
  - Z $((p_1 \land q_1) \lor (p_2 \land q_2) \lor \cdots \lor (p_n \land q_n))$ s n konjunkciami dostaneme $\bigwedge_{x_1 \in \{p_1, q_1\}} \cdots \bigwedge_{x_n \in \{p_n, q_n\}} \bigvee_{i=1}^{n} x_i$ s 2^n klauzulami
- Distribuovanie disjunkcií dovnútra konjunkcií teda môže formulu zväčšiť exponenciálne

IV.8 CNF – iný prístup

- Pri úprave formuly do CNF pre SAT solver *nepotrebujeme*, aby bola výsledná formula s pôvodnou *ekvivalentná*
- Stačí nám oveľa slabšia vlastnosť:

Definícia 3.60. Formuly X a Y sú *rovnako splniteľné* (ekvisplniteľné, equisatisfiable) práve vtedy, keď X je splniteľná vtt Y je splniteľná.

Tvrdenie 3.61. *Ak X a Y sú ekvivalentné, sú aj rovnako splniteľné.*

Príklad 3.62 (Ekvivalentnosť vs. ekvisplniteľnosť). Sú $(p \to q)$ a $(p \land r)$ rovnako splniteľné? Sú ekvivalentné?

- Ako by sa dá vyhnúť exponenciálnemu nárastu $X = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee \cdots \vee (p_n \wedge q_n))$,
  keď nám stačí nájsť rovnako splniteľnú formulu?

- Označme $X_i = (p_i \wedge q_i)$.
  - Aký je vzťah medzi X a X_i?

    X je splnená vtt jedna z X_i je splnená.
  - Akými klauzulami to vieme vyjadriť?

    $(X_i \to X)$ pre každé $i \in \{1, \ldots, n\}$ $\quad (\neg X_i \vee X)$
    $(X \to (X_1 \vee \cdots \vee X_n))$ $\quad (\neg X \vee X_1 \vee \cdots \vee X_n)$
  - Aký je vzťah medzi X_i, p_i a q_i?

    X_i je splnená vtt p_i je splnená a q_i je splnená.
  - Akými klauzulami to vieme vyjadriť?

    Pre každé $i \in \{1, \ldots, n\}$:
    $(X_i \to p_i)$ $\quad (\neg X_i \vee p_i)$
    $(X_i \to q_i)$ $\quad (\neg X_i \vee q_i)$
    $((p \wedge q) \to X_i)$ $\quad (\neg p \vee \neg q \vee X_i)$
  - Koľko klauzúl potrebujeme? $4n+1$, celkový stupeň CNF $11n+1$

Algoritmus CNF$_2$

1. Zostrojíme vytvárajúci strom pre formulu X a označíme formuly v ňom $X_0, X_1, X_2, \ldots$ tak, aby $X_0 = X$.

2. Pre každú formulu X_i, ak $X_i = p$ pre nejakú $p \in \mathcal{V}$, označíme $x_i = p$, inak označíme ako x_i novú výrokovú premennú,
   ktorá bude „reprezentovať“ formulu X_i.

3. Vytvoríme formuly, ktoré popisujú vzťah medzi X_i a jej priamymi podformulami prostredníctvom „reprezentačných“ premenných:

- ak X_i je tvaru $\neg X_j$ pre nejaké X_j, pridáme $(x_i \leftrightarrow \neg x_j)$,
- ak X_i je tvaru $(X_j \wedge X_k)$, pridáme $(x_i \leftrightarrow (x_j \wedge x_k))$,
- ak X_i je tvaru $(X_j \vee X_k)$, pridáme $(x_i \leftrightarrow (x_j \vee x_k))$,
- ak X_i je tvaru $(X_j \rightarrow X_k)$ pridáme $(x_i \leftrightarrow (x_j \rightarrow x_k))$,

4. Pridáme formulu x_0 (chceme aby formula X bola pravdivá).

5. Všetky nové formuly z krokov 3 a 4 prevedieme do CNF (je to jednoduché) a spojíme konjunkciou.

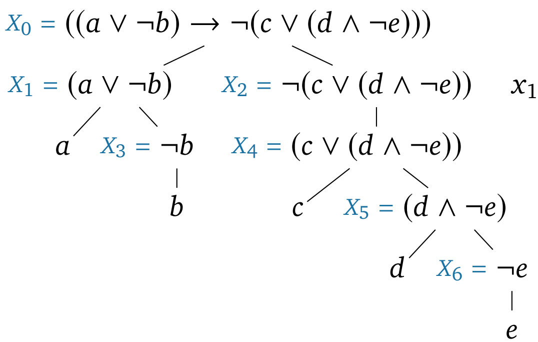
IV.11 CNF – iný prístup

Tvrdenie 3.63. *Výsledná formula Y algoritmu CNF$_2$ je v CNF, jej dĺžka je lineárna voči veľkosti X a Y je ekvisplniteľná s X.*

Lema 3.64. *Ak $X = (A \; c \; B)$ je formula a $p, q, r \in \mathcal{V}$ sa nevyskytujú v X, tak X a $Y = (p \wedge (p \leftrightarrow (q \; c \; r)) \wedge (q \leftrightarrow A) \wedge (r \leftrightarrow B))$ sú ekvisplniteľné.*

IV.12 CNF – iný prístup

Príklad 3.65.



x_0

$(x_0 \leftrightarrow (x_1 \rightarrow x_2))$

$x_1 \leftrightarrow (a \vee x_3)$ $\quad x_2 \leftrightarrow \neg x_4$

$x_3 \leftrightarrow \neg b$ $\quad x_4 \leftrightarrow (c \vee x_5)$

$x_5 \leftrightarrow (d \wedge x_6)$

$x_6 \leftrightarrow \neg e$

3.9. Kalkuly

IV.13 Dokazovanie ekvivalencie syntakticky vs. sémanticky

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

IV.14 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* ekvivalentné formuly
- Má dve pomerne samozrejmé pravidlá:
  Eulerovské *pravidlo* nahradenia ekvivalentnej formuly ekvivalentnou a tranzitivita ekvivalencie
  $$\frac{A \Leftrightarrow B}{X \Leftrightarrow X[A|B]} \qquad \frac{A \Leftrightarrow B \quad B \Leftrightarrow C}{A \Leftrightarrow C}$$
- Veľa (nevýhoda) *schém axióm* — distributívnosť, de Morgan, …

  - vytvoríme z nich nekonečne veľa axióm, základných ekvival.

- Postupnosť substitúcií slúži ako **dôkaz**:
  Každý (aj program), kto pozná pravidlo a axiómy
  ľahko mechanicky overí, že postupnosť je správna

IV.15 Dokazovanie vyplývania a tautológií syntakticky vs. sémanticky — kalkuly

- 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.

- Tautológie a vyplývanie formúl z množín sme doteraz dokazovali sémanticky — vyšetrovaním všetkých ohodnotení.

- Na tento účel ale existujú aj syntaktické metódy — *kalkuly*.

- Ukážeme si tri kalkuly:

  hilbertovský — klasický, lineárny, pomerne ťažkopádny

  tablový — modernejší, stromový, prirodzenejší

  rezolvenciu — strojový

V. prednáška
Hilbertovský a tablový kalkul

20. marca 2017

V.1 Organizačné poznámky

Konzultačné hodiny

streda 13:10–14:30
na I-16 (Kľuka) a I-7 (Šiška k praktickým cvičeniam)

Midterm
- piatok 7. apríla o 12:30 v A
- (pondelok 10. apríla o 18:10 v A)

Vysvetľovanie riešení

Vysvetľujte svoj postup, odvolávajte sa na definície,
dajte najavo, že chápete súvislosť medzi definovanými pojmami, ktoré sa nachádzajú v zadaní a technikou, ktorú používate na vyriešenie úlohy

Domáce úlohy

Ohodnotené a okomentované riešenia na cvičeniach

Konzultácie po cvičeniach alebo počas konzult. hodín

V.2 Usudzovacie pravidlá

- Na úvodnej prednáške sme *usudzovacie pravidlo* neformálne zadefinovali ako *vzor (šablóna) úsudkov*, napríklad:

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

- Úsudok získame dosadením výrokov (alebo výrokových foriem) na príslušné miesta v pravidle
- Teraz sa pokúsime:
  - formálne zadefinovať pravidlá,
  - ukázať, ako pravidlami budujeme *dôkazy* vyplývania,
  - diskutovať, či sú správne a či môžeme dokázať všetky vyplývania

V.3 Kalkul

Neformálne definície:

- *Odvodzovacie pravidlo* je množina $(n+1)$-tíc formúl, zapisovaných
$$\text{(R)}\quad \frac{A_1 \quad \cdots \quad A_n}{A},$$
vytvorená substitúciou do jednej vzorovej $(n+1)$-tice.
Formuly $A_1, \ldots, A_n$ nazývame *premisami* pravidla (R).
Formulu A nazývame *záver* pravidla (R).
- Pravidlo bez premís ($n = 0$) nazývame *schéma axióm* a namiesto
$$\frac{}{A}$$
ho zapisujeme iba A.
- *Kalkul* je systém odvodzovacích pravidiel.

3.10. Hilbertovský kalkul

V.4 Hilbertovský kalkul — axiómy a pravidlo

Definícia 3.66. *Hilbertovský kalkul* sa skladá z axióm vytvorených podľa nasledujúcich schém axióm pre všetky formuly A, B, C:

(A1) $(A \to (B \to A))$

(A2) $((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$

(A3) $((\neg A \to \neg B) \to (B \to A))$

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

(A5) $(A \to (B \to (A \wedge B)))$

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

(A7) $((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$

a pravidla *modus ponens*:

(MP) $\dfrac{A \quad (A \to B)}{B}$

pre všetky formuly A a B.

[Švejdar, 2002, §1.3]

V.5 Hilbertovský kalkul — dôkaz

Definícia 3.67. *(Formálnym) dôkazom* z množiny predpokladov S je postupnosť formúl $Y_1, Y_2, \ldots, Y_n$, v ktorej každá formula Y_i je

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

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

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

[Švejdar, 2002, §1.3]

Príklad 3.68. Nájdime dôkaz formuly $Z = (X \to X)$ z množiny predpokladov $\{\}$
(pre ľubovoľnú formulu X):

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

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

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

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

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

V.7 Veta o dedukcii

Veta 3.69 (o dedukcii). *$S \cup \{X\} \vdash Y$ vtt $S \vdash (X \to Y)$*

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

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

Báza: Nech $k = 1$. Y_1 nemohla byť odvodená pravidlom (MP), takže je buď axióma, alebo patrí do S, alebo je X. V treťom prípade použijeme dôkaz $(X \to X)$ z predchádzajúceho príkladu 3.68. V prvých dvoch prípadoch je postupnosť $Y_1, (Y_1 \to (X \to Y_1)), (X \to Y_1)$ dôkazom $(X \to Y_1)$.

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

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

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

Príklad 3.70. Ukážme $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$ (pre ľubovoľné formuly A, B a C).

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

Posledný dôkaz nájdeme veľmi ľahko:

$Y_1 = A$ — predpoklad

$Y_2 = (A \to B)$ — predpoklad

$Y_3 = B$ — (MP) pre Y_1 a Y_2

$Y_4 = (B \to C)$ — predpoklad

$Y_5 = C$ — (MP) pre Y_3, Y_4

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

Príklad 3.71. Ukážme $\{\} \vdash (\neg X \to (X \to Y))$ (pre ľubovoľné formuly X a Y).

$Y_1 = (\neg X \to (\neg Y \to \neg X))$ — (A1) pre $A = \neg X$, $B = \neg Y$

$Y_2 = ((\neg Y \to \neg X) \to (X \to Y))$ — (A3) pre $A = Y$, $B = X$

$\vdots$ — dôkaz z príkladu 3.70

$Y_n = ((\neg X \to (\neg Y \to \neg X)) \to (((\neg Y \to \neg X) \to (X \to Y)) \to (\neg X \to (X \to Y))))$

$Y_{n+1} = (((\neg Y \to \neg X) \to (X \to Y)) \to (\neg X \to (X \to Y)))$ — (MP) pre Y_1 a Y_n

$Y_{n+2} = (\neg X \to (X \to Y))$ — (MP) pre Y_2 a Y_{n+1}

Veta 3.72. *Pre každú množinu formúl S a každú formulu X platí:*

(korektnosť) *ak je X dokázateľná z S ($S \vdash X$),*
tak X výrokovologicky vyplýva z S ($S \vDash X$);

(úplnosť) *ak X výrokovologicky vyplýva z S ($S \vDash X$),*
tak X je dokázateľná z S ($S \vdash X$).

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

Ak S je množina výrokových formúl a

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

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

Úplnosť (angl. completeness) je komplikovanejšia.

V.11

Vyskúšajte si V.1
Ukážte $\{\} \vdash (\neg\neg X \to X)$.

3.11. Tablový kalkul

V.12 Dôkaz tautológie sporom

Príklad 3.73. Je formula $X = (p \to (q \to (p \land q)))$ tautológia?

Dokážme tvrdenie sporom: Zoberme ľubovoľné ohodnotenie v a predpokladajme (1) $v \not\models (p \to (q \to (p \land q)))$.
<all> Potom podľa definície spĺňania (2) $v \models p$ a (3) $v \not\models (q \to (p \land q))$, teda opäť podľa definície spĺňania (4) $v \models q$ a (5) $v \not\models (p \land q)$.
<all> Z faktu (5) dostávame, že (6) $v \not\models p$ alebo (7) $v \not\models q$. Nevieme, ktorá z týchto možností platí pre v, ale môžeme ich predpokladať *nezávisle od seba*:

- Nech platí (6), teda $v \not\models p$. To je však v spore s faktom (2).
- Nech platí (7). To je v spore s faktom (4).

V oboch prípadoch sme dospeli k sporu a ďalšie možnosti nie sú.
<all> Preto $v \models X$.

V.13 Dôkaz tautológie sporom

Príklad 3.74. Predchádzajúcu úvahu môžeme stručne zapísať, ak sa dohodneme, že:

- $\mathbf{F}X$ označuje, že v nespĺňa X;
- $\mathbf{T}X$ označuje, že v spĺňa X;
- ak z niektorého z predchádzajúcich faktov vyplýva priamo z definície spĺňania nový fakt, zapíšeme ho do ďalšieho riadka;
- ak z niektorého faktu vyplýva, že platí fakt F_1 alebo fakt F_2, rozdelíme úvahu na dve nezávislé *vetvy*, pričom prvá začne faktom F_1 a druhá faktom F_2;
- ak nastane spor, pridáme riadok so symbolom $*$.

V.14 Dôkaz tautológie sporom

Príklad 3.75.

$$
\begin{array}{lcccl|cccl}
(1) & & & & \multicolumn{4}{c}{\mathbf{F}(p \to (q \to (p \land q)))} & \\
(2) & & & & \multicolumn{4}{c}{\mathbf{T}p} & \text{z } (1) \\
(3) & & & & \multicolumn{4}{c}{\mathbf{F}(q \to (p \land q))} & \text{z } (1) \\
(4) & & & & \multicolumn{4}{c}{\mathbf{T}q} & \text{z } (3) \\
(5) & & & & \multicolumn{4}{c}{\mathbf{F}(p \land q)} & \text{z } (3) \\
(6) & \mathbf{F}p & \text{z } (5) & & & (7) & \mathbf{F}q & & \text{z } (5) \\
 & * & \text{medzi } (2) \text{ a } (6) & & & & * & & \text{medzi } (4) \text{ a } (7)
\end{array}
$$

V.15 Spĺňanie a priame podformuly

Pozorovanie 3.76. *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.

V.16 Označené formuly a ich sémantika

Definícia 3.77. Nech X je formula výrokovej logiky.
Postupnosti symbolov $\mathbf{T}X$ a $\mathbf{F}X$ nazývame *označenými formulami*.

Definícia 3.78. Nech v je ohodnotenie výrokových premenných a X je formula. Potom

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

Dohoda

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

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

V.17 Tablové pravidlá

Podľa pozorovania 3.76 a definície 3.78 môžeme sformulovať pravidlá pre označené formuly:

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

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

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

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

V.18 Jednotný zápis označených formúl — α

Definícia 3.79 (Jednotný zápis označených formúl typu α).
<all>Označená formula A^+ je typu α, ak 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 a α_2 príslušnú formulu z pravého stĺpca.

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

Pozorovanie 3.80 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie výrokových premenných.*
Ak v spĺňa α, tak v spĺňa α_1 a v spĺňa α_2.

V.19 Jednotný zápis označených formúl — β

Definícia 3.81 (Jednotný zápis označených formúl typu β).
<all>Označená formula B^+ je typu β, ak 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 a 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 3.82 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie výrokových premenných.*
Ak v spĺňa β, tak v spĺňa β_1 alebo v spĺňa β_2.

V.20 Tablo pre množinu označených formúl

Definícia 3.83. *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.

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

Nič iné nie je tablom pre S^+.

V.21 Vetvy a uzavretosť

Definícia 3.84. *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.

Definícia 3.85. Vetva π tabla $\mathcal{T}$ je *uzavretá* vtt obsahuje 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.

3.11.1. Korektnosť

V.22 Korektnosť tablového kalkulu

Veta 3.86 (Korektnosť tablového kalkulu)**.** *Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+. Potom je množina S^+ nesplniteľná.*

Dôsledok 3.87. *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 X vyplýva z S ($S \vDash X$).

Pozorovanie 3.88. *Formula X je tautológia vtt $\mathbf{F}X$ je nesplniteľná.*

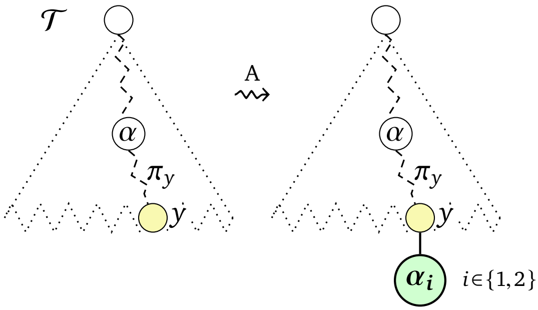
Dôsledok 3.89. *Nech X je formula a existuje uzavreté tablo pre $\{\mathbf{F}X\}$ (skr. $\vdash X$). Potom X je tautológia ($\vDash X$).*

VI. prednáška

Korektnosť a úplnosť tablového kalkulu

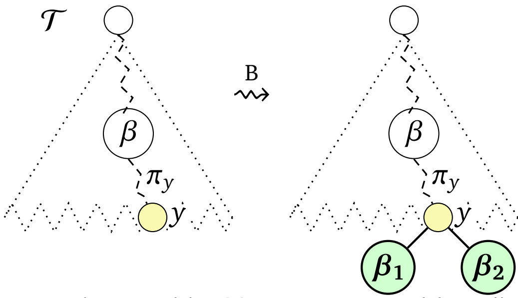
27. marca 2017

VI.1 Tablá, tablové pravidlá, operácie rozšírenia



$$\frac{\alpha}{\begin{array}{c}\alpha_1\\ \alpha_2\end{array}}$$

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



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

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

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

VI.2 Korektnosť — dôkaz

Definícia 3.90. Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie množiny výrokových premenných.

Hovoríme, že *v spĺňa vetvu π* v table $\mathcal{T}$ vtt v spĺňa všetky označené formuly obsiahnuté vo vrcholoch na vetve π.

Hovoríme, že *v spĺňa tablo $\mathcal{T}$*, ak spĺňa niektorú jeho vetvu.

Lema 3.91 (K1)**.** *Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie množiny výrokových premenných.*
Ak v spĺňa S^+ a v spĺňa $\mathcal{T}$, tak v spĺňa aj každé priame rozšírenie $\mathcal{T}$.

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 $\mathcal{T}_1$. □

Lema 3.92 (K2)**.** *Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie. Ak v spĺňa S^+, tak v spĺňa $\mathcal{T}$.*

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

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

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

VII. prednáška
Úplnosť tabiel, korektné pravidlá Výroková rezolvencia

3. apríla 2017

VII.1 Korektnosť — dôkaz

Dôkaz vety o korektnosti. Sporom: Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+. Nech v je ohodnotenie, ktoré spĺňa S^+. 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. □

3.11.2. Tablový dôkaz splniteľnosti

VII.2 Otvorené tablo a splniteľnosť

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

Definícia 3.93 (Úplná vetva a úplné tablo)**.** Nech S^+ je množina označených formúl a $\mathcal{T}$ je tablo pre S^+.

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

- pre každú ozn. formulu α, ktorá sa vyskytuje na π, sa aj obidve α_1 a α_2 vyskytujú na π,
- pre každú ozn. formulu β, ktorá sa vyskytuje na π, sa aspoň jedna z ozn. formúl β_1 alebo β_2 vyskytuje na π.
- každá $X^+ \in S^+$ sa vyskytuje na π.

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

Príklad 3.94. Vybudujme úplné tablo pre $\mathbf{F}X$, kde $X = (((p \vee q) \wedge (r \vee p)) \rightarrow (p \wedge (q \vee r)))$.

Nech tablové pravidlá použijeme v akomkoľvek poradí, nepodarí sa nám nájsť uzavreté tablo.

Navyše z tabla, v ktorom sme v každej vetve aplikovali všetky aplikovateľné pravidlá, vieme vytvoriť ohodnotenie v tak, že zoberieme niektorú otvorenú vetvu π a 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.

Lema 3.95 (o existencii úplného tabla). *Nech S^+ je konečná množina označených formúl.*
Potom existuje úplné tablo pre S^+.

Dôkaz. Vybudujme tablo $\mathcal{T}_0$ pre S^+ tak, že do koreňa vložíme niektorú formulu z S^+ a opakovaním 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. □

3.11.3. Hintikkova lema

Definícia 3.96. Množina označených formúl S^+ sa nazýva *nadol nasýtená* vtt platí:

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

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

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

Pozorovanie 3.97. *Nech π je úplná otvorená vetva nejakého tabla $\mathcal{T}$. Potom množina všetkých formúl na π je nadol nasýtená.*

Lema 3.98 (Hintikkova)**.** *Každá nadol nasýtená množina S^+ je splniteľná.*

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

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

v je 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 3.80).
  - 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 3.82). □

3.11.4. Úplnosť

VII.6 Úplnosť

Úplnosť kalkulu neformálne znamená, že je dostatočne silný, aby sa v ňom dali dokázať všetky dôsledky teórií.

Veta 3.99 (o úplnosti)**.** *Nech S^+ je konečná nesplniteľná množina označených formúl.*
Potom existuje uzavreté tablo pre S^+.

Dôsledok 3.100. *Nech S je konečná teória a X je formula.*
Ak $S \vDash X$, tak $S \vdash X$.

Dôsledok 3.101. *Nech X je formula. Ak $\vDash X$, tak $\vdash X$.*

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

VII.7 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. □

3.11.5. Nové korektné pravidlá

VII.8 Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

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

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

- Vďaka tejto vlastnosti zo splniteľnej množiny S^+ skonštruujeme iba splniteľné tablá.
- Netreba opačnú implikáciu (ak v splĺňa oba/jeden záver, tak splĺňa premisu).

• Na dôkaz *úplnosti* stačili pravidlá (Ax), α, β,
pretože stačia na vybudovanie úplného tabla.

VII.9 Nové pravidlo

Čo sa stane, ak pridáme nové pravidlo, napr.

$$\frac{\mathbf{T}(A \lor B) \quad \mathbf{F}A}{\mathbf{T}B} \quad (\lor_1) \quad ?$$

Upravíme definíciu priameho rozšírenia:

Úprava definície 3.83
(...) 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: ...

⋮

$\lor_1$: Ak sa na vetve π_y nachádzajú *obe* formuly $\mathbf{T}(A \lor B)$ a $\mathbf{F}A$, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci $\mathbf{T}B$.

VII.10 Nové pravidlo vs. korektnosť a úplnosť

• Pravidlo ($\lor_1$) je *korektné*:

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

Keďže v splĺňa $\mathbf{T}(A \lor B)$, v splĺňa A alebo v splĺňa B.
Pretože ale v splĺňa $\mathbf{F}A$, nesplĺňa A. Takže v musí splĺňať B.

- Preto stále dokážeme lemu K1 (3.91):

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

  Z nej dokážeme K2 a vetu o korektnosti

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

VII.11 Nové pravidlá vo všeobecnosti

Definícia 3.102 (Tablové pravidlo a jeho korektnosť)**.** *Tablové pravidlo* je množina dvojíc zapisovaných:

$$\begin{array}{c|c|c} P_1^+ & \dots & P_n^+ \\ \hline C_1^+ & \dots & C_k^+ \end{array} \qquad (R)$$

tvorených n-ticou (označených) formúl, ktoré nazývame *premisy*, a k-ticou (označených) formúl, ktoré nazývame *závery*,
pričom $n \geq 0$ a $k > 0$.

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

VII.12 Nové pravidlá vo všeobecnosti

Úprava definície 3.83
(...)

- ...

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

$$\vdots$$

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

3.12. Rezolvencia vo výrokovej logike

VII.13 Tranzitivita implikácie

Vráťme sa k neoznačeným formulám.

Je nasledujúce pravidlo korektné?

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

Nahraďme implikácie disjunkciami:

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

VII.14 Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

Definícia 3.103. *Rezolvenčný princíp* (*rezolvencia*, angl. *resolution principle*) je pravidlo

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

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

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

VII.15 Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

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

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

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

Rezolventa je logickým dôsledkom množiny obsahujúcej obe premisy.

VII.16 Pozorovania o rezolvencii

- Rezolvencia s jednotkovou klauzulou skráti druhú klauzulu:

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

- Ak rezolvencia odvodí **prázdnu klauzulu**

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

  premisy **nie sú súčasne splniteľné**

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

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

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

VII.17 Problematické prípady

- Opakovaným aplikovaním rezolvencie môžeme odvodzovať ďalšie dôsledky

  Príklad 3.104. Z množiny $S = \{(\neg p \vee r), (\neg q \vee r), (p \vee q)\}$ odvodíme $(r \vee r)$:

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

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

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

  (4) $(r \vee q)$ rezolventa (1) a (2)

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

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

- Preto potrebujeme ešte *pravidlo idempotencie*:

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

VII.18 Rezolvenčné odvodenie a zamietnutie

Definícia 3.105. *Rezolvenčné odvodenie* z množiny klauzúl S je každá (aj nekonečná) postupnosť klauzúl $C_1, C_2, \ldots, C_n, \ldots$, ktorej každý člen C_i je:

- prvkom S,

- rezolventou dvoch predchádzajúcich klauzúl C_j a C_k, t.j., $j < i$ a $k < i$,

- záverom pravidla idempotencie pre nejakú predchádzajúcu klauzulu C_j, $j < i$.

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

Veta 3.106 (Korektnosť rezolvencie)**.** *Nech S je množina klauzúl. Ak existuje zamietnutie S, tak S je nesplniteľná.*

Veta 3.107 (Úplnosť rezolvencie)**.** *Nech S je množina klauzúl. Ak S je nesplniteľná, tak existuje zamietnutie S.*

VIII. prednáška

SAT solver a algoritmus DPLL
Štruktúry

10. apríla 2017

3.13. Problém výrokovologickej splniteľnosti (SAT)

VIII.1 Problém SAT

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

  Príklad 3.108. Je množina klauzúl S splniteľná?

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

VIII.2 Tabuľková metóda

- Tabuľkovou metódou skúmame *všetky* ohodnotenia výrokových premenných
- Preskúmanie ohodnotení trvá $\mathrm{O}(s2^N)$ krokov,
  kde N je počet premenných a s je súčet veľkostí klauzúl
  - 2^N ohodnotení, pre každé treba zistiť, či sú všetky klauzuly splnené
- Celú tabuľku si pamätáme (píšeme na papier)
- Tabuľka zaberá priestor $\mathrm{O}(k2^N)$, kde k je počet klauzúl
- Tabuľka slúži aj ako dôkaz nesplniteľnosti

3.13.1. Naivný backtracking

VIII.3 Naivný backtracking v Pythone

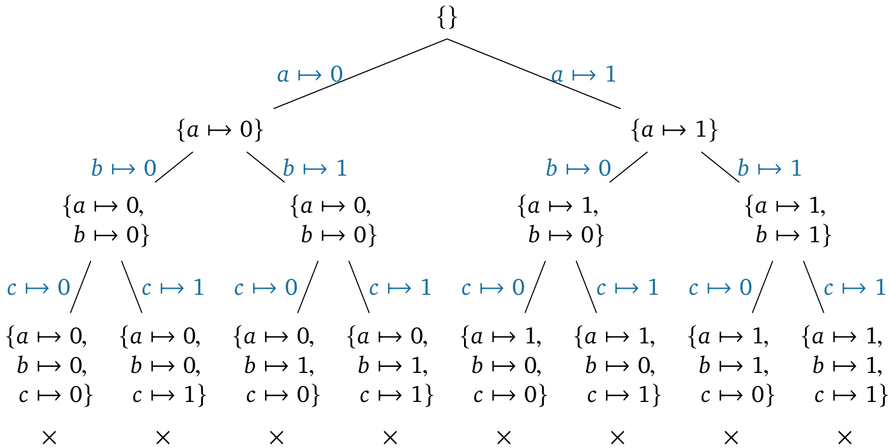
```
#!/usr/bin/env python3
class Sat(object):
    def __init__(self, n, clauses):
        self.n, self.clauses, self.solution = n, clauses, None
    def checkClause(self, e, c):
        return any( ( e[abs(lit)] if lit > 0 else not e[abs(lit)] )
                        for lit in c )
    def check(self,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

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

VIII.4 Strom prehľadávania ohodnotení

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

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



VIII.5 Naivné C++

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

VIII.6 Trochu lepšie C++

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

VIII.7 Čas

Čas prehľadávania stromu ohodnotení v závislosti od počtu literálov

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

3.13.2. Optimalizácia backtrackingu

VIII.8 Priebežné vyhodnocovanie klauzúl

- Každý uzol prehľadávaného stromu ohodnotení je *čiastočné ohodnotenie*
- Ohodnotenie v uzle je *rozšírením* ohodnotenia v rodičovi
- Niektoré klauzuly sa dajú vyhodnotiť aj v čiastočnom ohodnotení

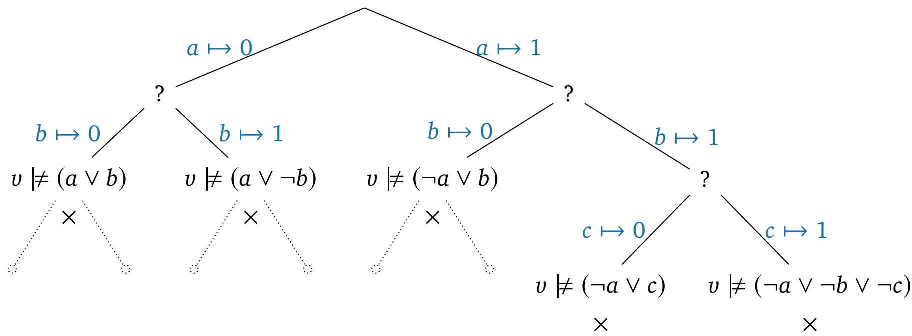
    - Napríklad v čiastočnom ohodnotení $v = \{a \mapsto 0, b \mapsto 1\}$ vieme určiť splnenie $(a \lor b)$, $(a \lor \neg b)$, $(\neg a \lor b)$ z našej S

- Ak je niektorá nesplnená, môžeme „backtracknúť“ — zastaviť prehľadávanie vetvy a vrátiť sa o úroveň vyššie

VIII.9 Prehľadávanie s priebežným vyhodnocovaním

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

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



VIII.10 Zjednodušenie množiny klauzúl podľa literálu

Nech v je čiastočné ohodnotenie, v ktorom $v(a) = 1$.
Čo vieme o splnení klauzúl z S každým rozšírením v' ohodnotenia v?

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

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

- v' splní klauzulu $(\ell_1 \lor \cdots \lor \neg a \lor \cdots \lor \ell_n)$ obsahujúcu $\neg a$ vtt v' splní *zjednodušenú* klauzulu $(\ell_1 \lor \cdots \lor \cdots \lor \ell_n)$
    - $\{a \mapsto 1, \ldots\} \models (\neg a \lor \neg b \lor \neg c)$ vtt $\{a \mapsto 1, \ldots\} \models (\neg b \lor \neg c)$

- Mimochodom, $(\neg b \vee \neg c)$ je rezolventa a a $(\neg a \vee \neg b \vee \neg c)$

Stačia nám zjednodušené klauzuly

VIII.11 Zjednodušenie množiny klauzúl podľa literálu

Množinu klauzúl

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

teda môžeme *zjednodušiť podľa* a na

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

Analogicky môžeme S zjednodušiť podľa $\neg a$ na

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

VIII.12 Zjednodušenie množiny klauzúl podľa literálu

Definícia 3.109. Nech p je výroková premenná.
Komplementom literálu p je $\neg p$. *Komplementom literálu $\neg p$* je p.
Komplement literálu ℓ označujeme $\bar{\ell}$.

Definícia 3.110. Nech ℓ je literál a S je množina klauzúl. Potom definujeme

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

Tvrdenie 3.111. *Nech ℓ je literál a S je množina klauzúl. Potom $S \cup \{\ell\}$ je splniteľná vtt $S|_\ell$ je splniteľná.*

VIII.13 Propagácia jednotkových klauzúl

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

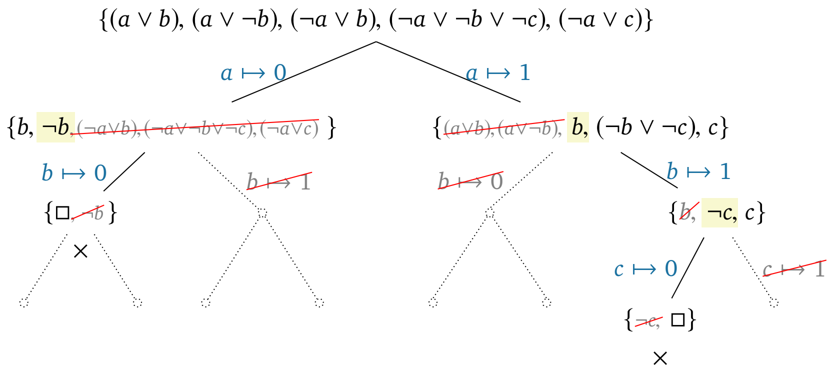
- Preto T' spĺňajú *iba* ohodnotenia v, v ktorých $v(b) = 0$
- Pre také ohodnotenia môžeme T' ďalej zjednodušiť podľa $\neg b$: $T'' := T'|_{\neg b} = \{c\}$
- T'' môžu splniť iba ohodnotenia v, v ktorých $v(c) = 1$
- Pre také ohodnotenia môžeme T'' ďalej zjednodušiť podľa c: $T''' := T''|_c = \{\}$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

Proces opakovaného rozširovania ohodnotení podľa jednotkových klauzúl a zjednodušovania sa nazýva *propagácia jednotkových klauzúl* (*unit propagation*)

VIII.14 Propagácia jednotkových klauzúl

Dôsledok 3.112. *Nech ℓ je literál a S je množina klauzúl obsahujúca jednotkovú klauzulu ℓ ($\ell \in S$). Potom S je splniteľná vtt $S|_\ell$ je splniteľná.*

VIII.15 Prehľadávanie so zjednodušovaním klauzúla unit propagation



- Všimnime si literál u v množine klauzúl:

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

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

- Vynechajme z T všetky klauzuly obsahujúce u:

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

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

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

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

Definícia 3.113. Nech ℓ je literál a S je množina klauzúl.
Literál ℓ je *nezmiešaný* (*pure*) v S vtt ℓ sa vyskytuje v niektorej klauzule z S, ale jeho komplement $\bar{\ell}$ sa nevyskytuje v žiadnej klauzule z S.

Tvrdenie 3.114. *Nech ℓ je literál a S je množina klauzúl.*
Ak ℓ je nezmiešaný v S, tak S je splniteľná vtt $S|_\ell$ je splniteľná.

3.13.3. DPLL

Algoritmus 3.115 (Davis and Putnam [1960], Davis et al. [1962]).

```
1: function DPLL(Φ, e)
2:     if Φ obsahuje prázdnu klauzulu then
```

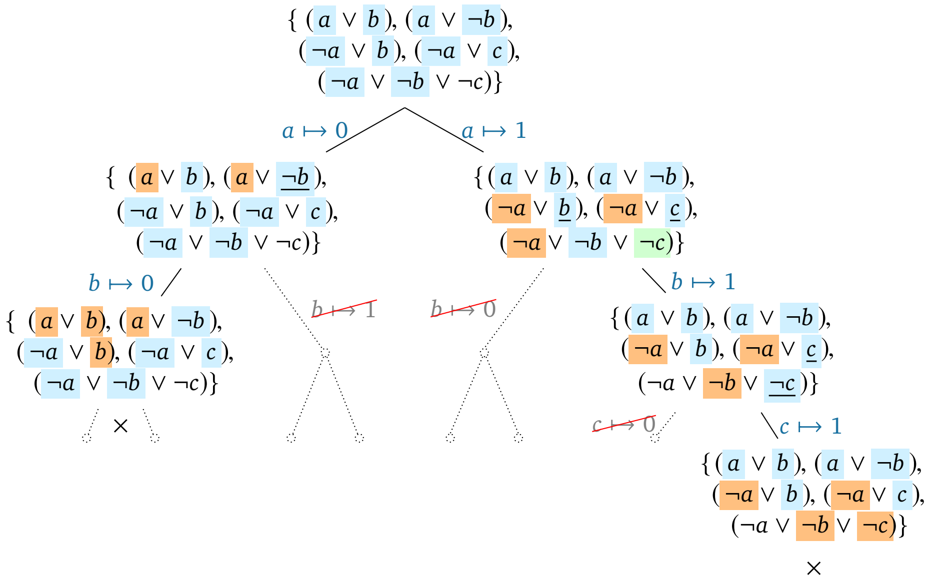
    return False
  end if
  if e ohodnocuje všetky premenné **then**
    return True
  end if
  while existuje jednotková (unit) klauzula ℓ vo Φ **do**
    $\Phi, e \leftarrow$ UNIT-PROPAGATE(ℓ, Φ, e)
  end while
  while existuje nezmiešaný (pure) literál ℓ vo Φ **do**
    $\Phi, e \leftarrow$ PURE-LITERAL-ASSIGN(ℓ, Φ, e)
  end while
  $x \leftarrow$ CHOOSE-BRANCH-LITERAL(Φ, e)
  return DPLL$(\Phi|_x, e(x \mapsto T))$ **or** DPLL$(\Phi|_{\neg x}, e(x \mapsto F))$
end function

VIII.19 Technika sledovaných literálov (watched literals)

Aby sme nemuseli zjednodušovať množinu klauzúl:

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

VIII.20 Prehľadávanie s unit propagation a sledovaním



4. Výroková logika s rovnosťou

4.1. Syntax výrokovej logiky s rovnosťou

VIII.21 Štruktúra výrokov — objekty a vzťahy

Jazyk výrokovej logiky nie je najpohodlnejší na zápis problémov, v ktorých sa opakujú *vlastnosti* alebo *vzťahy*, ktoré sa dajú aplikovať na viacero *objektov*:

- V probléme typickej americkej rodiny sme mali napríklad vlastnosť „x je dcéra" alebo vzťah „x je staršia/-í ako y".
  Objektmi vlastností a vzťahov boli Dorothy, George, Howard a Virginia

- V probléme vraždy v dreadburskom panstve sme mali napríklad vzťahy „x je bohatší/-ia ako y", „x nenávidí y".
  Objektmi boli Agáta, komorník (Butler) a Karol (Charles)

- V online bazári vzniká vzťah „x kupuje od y tovar z“.
  Objektmi sú rôzni konkrétni predávajúci a kupujúci, rôzne konkrétne tovary

VIII.22 Štruktúra výrokov — jednoznačne určené objekty

V niektorých vzťahoch je ku každému objektu *práve jeden* objekt (alebo hodnota) — teda súvisiaci objekt vždy existuje a je jednoznačne určený:

- každý človek má práve jednu biologickú matku,
- každý kus tovaru v bazári má práve jednu aktuálnu cenu,
- každý študent dostane za každú úlohu práve jedno hodnotenie,
- súčet každej dvojice čísel je práve jeden.

Takýto jednoznačne určený objekt (hodnotu) vieme pomenovať, aj keď nemá vlastné meno, pomocou zdrojového objektu a vzťahu:

- Emina mama,
- cena tovaru č. 531246,
- Jarkino hodnotenie z midtermu,
- súčet 1 a 1.

VIII.23 Krok k štruktúrovanejším výrokom

Výroková logika veľmi zjednodušuje prirodzený jazyk:

- skúma iba štruktúru tvrdení tvorenú spojkami,
- atomické výroky *nemajú štruktúru*

Spravme teraz **malý** krok k logike, ktorá vyjadrí zložitejšie tvrdenia. Zachyťme:

- **konkrétne objekty**,

- **vlastnosti** a **vzťahy**,
- nepriamo pomenované **jednoznačne určené objekty**

ale **nepokúšajme** sa zatiaľ o zámená (niekto), či číslovky (všetci, práve dve)

VIII.24 Symboly jazyka výrokovej logiky s rovnosťou

Definícia 4.1. *Symbolmi jazyka výrokovej logiky s rovnosťou $\mathcal{L}$ sú:*

- *mimologické* symboly:
  - *symboly konštánt* z nejakej spočítateľnej množiny $\mathcal{C}_{\mathcal{L}}$ $(a, b, \dots)$;
  - *funkčné symboly* z nejakej spočítateľnej množiny $\mathcal{F}_{\mathcal{L}}$ $(f, g, \dots)$;
  - *predikátové symboly* z nejakej spočít. množiny $\mathcal{P}_{\mathcal{L}}$ $(P, R, \dots)$;
- *logické symboly*:
  - *logické spojky*: unárna $\neg$, binárne $\land$, $\lor$, $\to$;
  - *symbol rovnosti* $\doteq$ (niekedy zapisovaný priamo ako $=$);
- *pomocné symboly* (,) a , (ľavá, pravá zátvorka a čiarka);

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

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

VIII.25 Symboly jazyka logiky s rovnosťou

Poznámka 4.2. Symboly (konštánt, funkčné, predikátové) môžu byť nealfabetické (1, $<$, $+$), či tvorené viacerými znakmi (`Virginia`, `dcéra`, `cena`).

Dohoda 4.3. Aritu budeme niekedy písať ako horný index symbolov ($\texttt{matka}^1$, $<^2$).

VIII.26 Príklady a účel symbolov

Príklad 4.4. Symboly konštánt predstavujú *konkrétne* objekty alebo hodnoty,
podobne ako *vlastné mená* v prirodzenom jazyku
alebo konštanty v programovacom jazyku:

- `Agatha`, `Ema`, `Tovar531246`, `0`, `1`

Predikátové symboly predstavujú *vlastnosti* a *vzťahy*:

- $\texttt{kolobežka}^1$, $\texttt{syn}^1$, $\texttt{nenávidí}^2$, $\texttt{kupuje}^3$, $<^2$

Funkčné symboly predstavujú *vzťahy s jednoznačne určenými objektmi*:

- $\texttt{cena}^1$, $\texttt{hodnotenie}^2$, $+^2$

VIII.27 Termy jazyka logiky s rovnosťou

Definícia 4.5. Množina $\mathcal{T}_\mathcal{L}$ *termov* jazyka logiky s rovnosťou $\mathcal{L}$ je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, pre ktorú platí:

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

Inak povedané:

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

Dohoda 4.6. Termy označujeme písmenami t, s, r s prípadnými dolnými indexmi.

VIII.28 Termy jazyka logiky s rovnosťou

Príklad 4.7. Termy predstavujú konkrétne objekty — buď priamo pomenované symbolmi konštánt:

- `Agatha`, `Ema`, `Tovar531246`, `0`, `1`

alebo nepriamo pomenované pomocou jednoznačných vzťahov:

- `matka(Ema)`, `cena(Tovar531246)`, `predávajúci(Tovar531246)`, `+(0, 1)`.

Termy možno ľubovoľne vnárať:

- `matka(matka(matka(Ema)))`, `+(+(1, 0), +(1, 1))`, `cena(predávajúci(Tovar531246))`.

Vidíme, že používanie funkčných symbolov na označenie vzťahov má úskalia. :)

VIII.29 Atomické formuly jazyka logiky s rovnosťou

Definícia 4.8 (Atomické formuly)**.** Nech $\mathcal{L}$ je jazyk logiky s rovnosťou.

- Ak t_1 a t_2 sú termy, tak postupnosť symbolov $t_1 \doteq t_2$ nazývame *rovnostný atóm* jazyka $\mathcal{L}$.
- Ak P je predikátový symbol s aritou n a $t_1, \ldots, t_n$ sú termy, tak postupnosť symbolov $P(t_1, \ldots, t_n)$ nazývame *predikátový atóm* jazyka $\mathcal{L}$.
- Rovnostné a predikátové atómy jazyka $\mathcal{L}$ spoločne nazývame *atomickými formulami* (skrátene *atómami*) jazyka $\mathcal{L}$.
- Množinu všetkých atómov jazyka $\mathcal{L}$ označujeme $\mathcal{A}_{\mathcal{L}}$.

VIII.30 Príklady atomických formúl

Príklad 4.9. Predikátové atomické formuly predstavujú výroky o vlastnostiach objektov označených termami:

- `bicykel(Tovar531246)`, `žena(matka(Miro))`, `párne(+(1, 1))`, a o vzťahoch objektov:

- $\mathtt{starší(Howard, Virginia)}$, $\mathtt{dieťa(Miro, matka(Ema))}$, $\mathtt{<(+(1, 1), 0)}$, $\mathtt{kupuje(Jofi22, Katulienka, Tovar531246)}$.

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

- $\mathtt{Butler} \doteq \mathtt{Charles}$, $\mathtt{matka(Miro)} \doteq \mathtt{matka(Ema)}$, $\mathtt{+(1, 0)} \doteq \mathtt{1}$.

VIII.31 Formuly jazyka logiky s rovnosťou

Definícia 4.10. Množina $\mathcal{E}_{\mathcal{L}}$ *formúl* jazyka logiky s rovnosťou $\mathcal{L}$ je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, pre ktorú platí:

- Všetky atomické formuly z $\mathcal{A}_{\mathcal{L}}$ sú formulami.
- Ak A je formula, tak aj $\neg A$ je formula (*negácia* A).
- Ak A a B sú formuly, tak aj $(A \land B)$, $(A \lor B)$, $(A \to B)$ sú formuly (*konjunkcia*, *disjunkcia*, *implikácia* A a B).

Dohoda
Formuly označujeme písmenami $A, B, C, \ldots$ s prípadnými indexmi.

VIII.32 Formuly jazyka logiky s rovnosťou

Príklad 4.11. Formuly tvoríme z atómov tak, ako doteraz:

$$(\mathtt{dieťa(Miro, matka(Ema))} \to \mathtt{matka(Miro)} \doteq \mathtt{Ivana})$$

$$\big(\mathtt{killed(Charles, Agatha)} \to \\ (\mathtt{hates(Charles, Agatha)} \land \neg\mathtt{richer(Charles, Agatha)})\big)$$

$$\big(\neg\, \mathtt{Charles} \doteq \mathtt{Butler} \to \mathtt{hates(Agatha, Charles)}\big)$$

VIII.33 Zjednodušenie zápisu formúl

Dohoda 4.12. Zápis formúl môžeme zjednodušovať nasledujúcim spôsobom:

- Negáciu rovnostného atómu $\neg\, s \doteq t$ skrátene zapisujeme $s \neq t$.
- Vonkajší pár zátvoriek môžeme vždy vynechať, teda napr. namiesto $(a \doteq b \to b \doteq a)$ môžeme písať $a \doteq b \to b \doteq a$.
- Binárnym spojkám priradíme prioritu:
  najvyššiu má $\wedge$, nižšiu $\vee$, najnižšiu $\to$.
- Ak $Z = (A\, b_1\, B)$ je priamou podformulou $(X\, b_2\, Y)$ (teda $Z = X$ alebo $Z = Y$) a b_1 má vyššiu prioritu ako b_2, môžeme vynechať zátvorky okolo Z.

Príklad 4.13. Namiesto $((P(a, b) \wedge (P(c, a) \vee P(b, c))) \to (P(a, c) \vee P(c, a)))$ môžeme písať $P(a, b) \wedge (P(a, c) \vee P(b, c)) \to P(a, c) \vee P(c, a)$.

4.2. Sématika logiky s rovnosťou

VIII.34 Štruktúry

Definícia 4.14. Nech $\mathcal{L}$ je jazyk logiky s rovnosťou.
Štruktúrou pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (M, i)$, kde

- M je neprázdna množina, nazývaná *doména* štruktúry $\mathcal{M}$;
- i je zobrazenie, nazývané *interpretačná funkcia* štruktúry $\mathcal{M}$, ktoré
  - každému symbolu konštanty c jazyka $\mathcal{L}$ priraďuje prvok $i(c) \in M$;
  - každému funkčnému symbolu f jazyka $\mathcal{L}$ s aritou n priraďuje funkciu $i(f)\colon M^n \to M$;
  - každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $i(P) \subseteq M^n$.

Dohoda 4.15. Štruktúry označujeme veľkými *písanými* písmenami $\mathcal{M}$, $\mathcal{N}$, ….
Doménu označujeme rovnakým, ale *tlačeným* písmenom ako štruktúru.

VIII.35 Štruktúry

Príklad 4.16. Nájdime štruktúru pre jazyk $\mathcal{L}_{\text{Rodina}}$ pre zjednodušené rodinné vzťahy so symbolmi konštánt $\mathtt{Ema}$, $\mathtt{Miro}$, $\mathtt{Ivana}$,
predikátovými symbolmi $\mathtt{žena}^1$ a $\mathtt{dieťa}^2$,
a funkčným symbolom $\mathtt{matka}^2$.

VIII.36 Hodnota termov

Definícia 4.17. Nech $\mathcal{M} = (M, i)$ je štruktúra pre jazyk $\mathcal{L}$.
Hodnotou termu t jazyka $\mathcal{L}$ v štruktúre $\mathcal{M}$ je prvok z M označovaný $t^{\mathcal{M}}$, ktorý je určený nasledovne:

- $a^{\mathcal{M}} = i(a)$, ak a je konštanta,
- $\big(f(t_1, \dots, t_n)\big)^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}})$, ak f je funkčný symbol a t_1, …, t_n sú termy.

Príklad 4.18. Vyhodnoťme termy $\mathtt{Ivana}$, $\mathtt{matka}(\mathtt{Miro})$, $\mathtt{matka}(\mathtt{matka}(\mathtt{Ema}))$ v štruktúre z predchádzajúceho príkladu.

VIII.37 Splnenie formuly v štruktúre

Definícia 4.19. Nech $\mathcal{L}$ je jazyk výrokovej logiky s rovnosťou.
Relácia *štruktúra $\mathcal{M}$ spĺňa formulu A* (skrátene $\mathcal{M} \models A$) medzi formulami $\mathcal{L}$ a štruktúrami pre $\mathcal{L}$ je definovaná pre každú štruktúru $\mathcal{M} = (M, i)$ induktívne vzhľadom na stupeň formuly nasledovne:

- $\mathcal{M} \models t_1 \doteq t_2$ vtt $t_1^{\mathcal{M}} = t_2^{\mathcal{M}}$,
- $\mathcal{M} \models P(t_1, \dots, t_n)$ vtt $\big(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}\big) \in i(P)$,
- $\mathcal{M} \models \neg A$ vtt $\mathcal{M} \not\models A$,
- $\mathcal{M} \models (A \land B)$ vtt $\mathcal{M} \models A$ a zároveň $\mathcal{M} \models B$,
- $\mathcal{M} \models (A \lor B)$ vtt $\mathcal{M} \models A$ alebo $\mathcal{M} \models B$,
- $\mathcal{M} \models (A \to B)$ vtt $\mathcal{M} \not\models A$ alebo $\mathcal{M} \models B$,

pre každú aritu $n > 0$, každý predikátový symbol P s aritou n, všetky termy $t_1, t_2, \dots, t_n$, a všetky formuly A, B.

Príklad 4.20. Zistime, či sú v štruktúre z príkladu 4.16 splnené formuly:

- $\mathtt{dieťa}(\mathtt{Ema}, \mathtt{Ivana})$,
- $\mathtt{matka}(\mathtt{Ema}) \not\doteq \mathtt{Ema}$,
- $\mathtt{dieťa}(\mathtt{Miro}, \mathtt{matka}(\mathtt{Ema})) \rightarrow \mathtt{matka}(\mathtt{Miro}) \doteq \mathtt{Ivana}$.

Literatúra

Martin Davis and Hillary Putnam. A computing procedure for quantification theory. *J. Assoc. Comput. Mach.*, 7:201–215, 1960.

Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, 1962.

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.