Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra aplikovanej informatiky

Matematika (4): Logika pre informatikov

Poznámky z prednášok

Ján Kľuka, Ján Mazák

Letný semester 2021/2022

Posledná aktualizácia: 9. mája 2022

Obsah

1. prednáška

Úvod
Atomické formuly

0 Úvod

0.1 O logike

Čo je logika

Logika je vedná disciplína, ktorá študuje usudzovanie.

Správne, racionálne usudzovanie je základom vedy a inžinierstva.

Vyžaduje rozoznať správne úsudky z predpokladaných princípov a pozorovania od chybných úvah a špekulácií.

Správnosť úsudkov, zdá sa, nie je iba vec konvencie a dohody.

Logika skúma, *aké* sú zákonitosti správneho usudzovania a *prečo* sú zákonitosťami.

Ako logika študuje usudzovanie

Logika má dva hlavné predmety záujmu:

Jazyk zápis pozorovaní, definície pojmov, formulovanie teórií

Syntax pravidlá zápisu tvrdení

Sémantika význam tvrdení

Usudzovanie (inferencia) odvodzovanie nových *logických dôsledkov* z doterajších poznatkov. Aký má vzťah s jazykom, štruktúrou tvrdení?

Jazyk, poznatky a teórie

Jazyk slúži na formulovanie tvrdení, ktoré vyjadrujú poznatky o svete (princípy jeho fungovania aj pozorované fakty).

Súboru poznatkov, ktoré považujeme za pravdivé, hovoríme *teória*.

Príklad 0.1 (Party time!). Máme troch nových známych — Kim, Jima a Sarah. Organizujeme párty a P0: chceme na ňu pozvať niekoho z nich. Od spoločných kamarátov sme sa ale dozvedeli o ich požiadavkách:

P1: Sarah nepôjde na párty, ak pôjde Kim.

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

P3: Sarah nepôjde bez Jima.

Možné stavy sveta a modely

Jedna z otázok, ktoré si o teórii o party môžeme položiť, je: „V akých zostavách môžu noví známi prísť na párty tak, aby boli všetky podmienky splnené?"

Priamočiaro (aj keď prácne) to zistíme tak, že:

1. vymenujeme *všetky možné stavy sveta* (účasti nových známych),
2. zistíme, v ktorých sú všetky podmienky splnené.

K	J	S	P0	P1	P2	P3
n	n	n	n			
n	n	p	p	p	p	n
n	p	n	p	p	n	
n	p	p	p	p	n	
p	n	n	*p*	*p*	*p*	*p*
p	n	p	p	n		
p	p	n	*p*	*p*	*p*	*p*
p	p	p	p	n		

P0: Niekto z Kim, Jima, Sarah príde na párty.

P1: Sarah nepôjde na párty, ak pôjde Kim.

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

P3: Sarah nepôjde bez Jima.

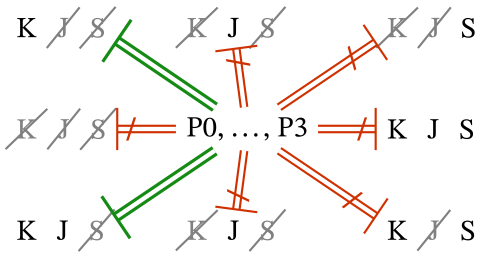
Možné stavy sveta a modely

Teória rozdeľuje *možné stavy sveta* (interpretácie) na:

- $\models$ stavy, v ktorých je pravdivá — *modely* teórie,
- $\not\models$ stavy, v ktorých je nepravdivá.

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

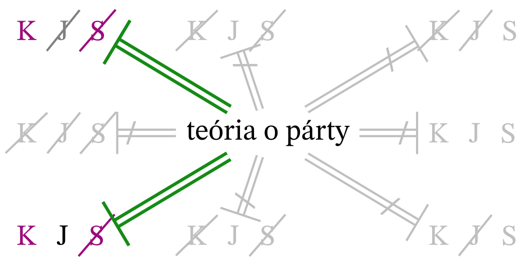
Príklad 0.2. Modelmi teórie P0, P1, P2, P3 sú dve situácie: keď Kim príde na párty a ostatní noví známi nie, a keď Kim a Jim prídu na párty a Sarah nie.



Logické dôsledky

Často je zaujímavá iná otázka o teórii — musí byť nejaké tvrdenie pravdivé *vždy, keď* je pravdivá teória?

V našom príklade: Kto *musí* a kto *nesmie* prísť na párty, aby boli podmienky P0, …, P3 splnené?



Logické dôsledky

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

Príklad 0.3. Logickými dôsledkami teórie P0, P1, P2, P3 sú napríklad:

- *Kim príde na párty.*
- *Sarah nepríde na párty.*

Logických dôsledkov je nekonečne veľa, môžu nimi byť ľubovoľne zložité tvrdenia:

- Na party príde Kim alebo Jim.

- Ak príde Sarah, tak príde aj Jim.
- Ak príde Jim, tak nepríde Sarah.

⋮

Logické usudzovanie

Preskúmať všetky stavy sveta je často nepraktické až nemožné.

Logické dôsledky ale môžeme *odvodzovať usudzovaním* (*inferovať*).

Pri odvodení vychádzame z *premís* (predpokladov) a postupnosťou *správnych úsudkov* dospievame k *záverom*.

Príklad 0.4. Vieme, že ak na párty pôjde Kim, tak nepôjde Sarah (P1), a že ak pôjde Jim, tak pôjde Kim (P2).

1. Predpokladajme, že na párty pôjde Jim.
2. Podľa 1. a P2 pôjde aj Kim.
3. Podľa 2. a P1 nepôjde Sarah.

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

Dedukcia

Úsudok je správny (*korektný*) vtedy, keď *vždy*, keď sú pravdivé jeho premisy, je pravdivý aj jeho záver.

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

Dedukcia je usudzovanie, pri ktorom sa používajú iba správne úsudky.

Logika študuje dedukciu, ale aj niektoré nededuktívne úsudky, ktoré sú *vo všeobecnosti* nesprávne, ale sú správne v *špeciálnych* prípadoch alebo sú *užitočné*:

- indukcia — zovšeobecnenie;
- abdukcia — odvodzovanie možných príčin z následkov;
- usudzovanie na základe analógie (podobnosti).

Kontrapríklady

Ak úsudok nie je správny, vieme nájsť *kontrapríklad* — stav sveta, v ktorom sú *predpoklady pravdivé*, ale *záver je nepravdivý*.

Príklad 0.5. Nesprávny úsudok: Ak platia tvrdenia teórie o party, na party príde Jim.

Kontrapríklad: Stav, kedy príde Kim, nepríde Jim, nepríde Sarah.

Teória je pravdivá, výrok „na party príde Jim" nie je pravdivý.

Matematická logika

Matematická logika

- modeluje jazyk, jeho sémantiku a usudzovanie ako matematické objekty (množiny, postuposti, zobrazenia, stromy);
- rieši logické problémy matematickými metódami.

Rozvinula sa koncom 19. a v prvej polovici 20. storočia vďaka snahám vybudovať základy matematiky bez sporov a paradoxov, mechanizovať overovanie dôkazov alebo priamo matematických viet.

Matematická logika a informatika

Informatika sa vyvinula z matematickej logiky (von Neumann, Turing, Church, …)

Väčšina *programovacích jazykov* obsahuje logické prvky:

- `all(x > m for x in arr)`,

fragmenty niektorých sú priamo preložiteľné na logické formuly:

- `select T1.x, T2.y from T1 inner join T2 on T1.z = T2.z where T1.z > 25`,

niektoré (Prolog) sú podmnožinou logických jazykov.

Metódami logiky sa dá *presne špecifikovať*, čo má program robiť, *popísať*, čo robí, a *dokázať*, že robí to, čo bolo špecifikované.

Vo *výpočtovej logike* a umelej inteligencii sa metódy logiky používajú na riešenie rôznych ťažkých problémov (plánovanie, rozvrh, hľadanie a overovanie dôkazov matematických tvrdení, hľadanie vysvetlení, …).

Formálne jazyky a formalizácia

Matematická logika nepracuje s prirodzeným jazykom, ale s jeho zjednodušenými modelmi — *formálnymi jazykmi*.

- Presne definovaná, zjednodušená syntax a sémantika.
- Obchádzajú problémy prirodzeného jazyka:

  viacznačnosť slov, nejednoznačné syntaktické vzťahy, zložitá syntaktickú analýzu, výminky, obraty s ustáleným významom, …

- Niekoľko formálnych jazykov už poznáte: aritmetika, jazyky fyzikálnych a chemických vzorcov, programovacie jazyky, …

Problémy z reálneho sveta opísané v prirodzenom jazyku musíme najprv *sformalizovať*, a potom naň môžeme použiť aparát matematickej logiky.

Formalizácia vyžaduje cvik — trocha veda, trocha umenie.

Ťažkosti s prirodzeným jazykom

Prirodzený jazyk je problematický:

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

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

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

Formalizácia poznatkov

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

Karol je trikrát starší ako Mária.
Súčet Karolovho a Máriinho veku je 12 rokov.
Koľko rokov majú Karol a Mária?

$$\rightsquigarrow \quad \begin{aligned} k &= 3 \cdot m \\ k + m &= 12 \end{aligned}$$

Stretli ste sa už aj s formálnym jazykom výrokovej logiky.

Príklad 0.6. Sformalizujme náš párty príklad:

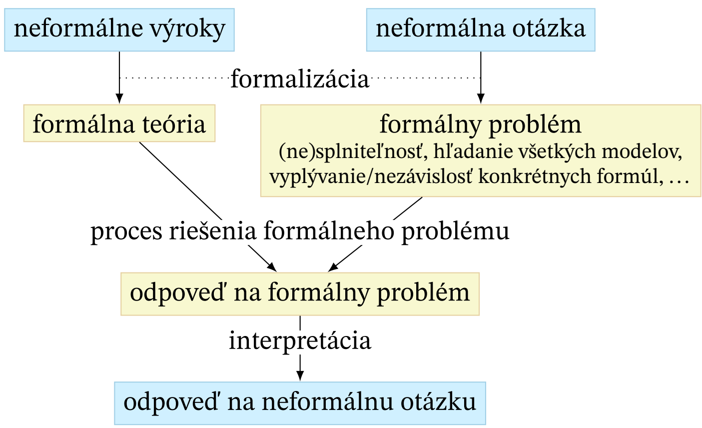
P0: Niekto z trojice Kim, Jim, Sarah pôjde na párty.

P1: Sarah nepôjde na párty, ak pôjde Kim.

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

P3: Sarah nepôjde bez Jima.

Schéma riešenia problémov pomocou logiky



Logika prvého rádu

Jazyk logiky prvého rádu (FOL) je jeden zo základných formálnych jazykov, ktorým sa logika zaoberá.

Do dnešnej podoby sa vyvinul koncom 19. a v prvej polovici 20. storočia — G. Frege, G. Peano, C. S. Peirce.

Výrokové spojky + *kvantifikátory* $\forall$ a $\exists$.

Dá sa v ňom vyjadriť veľa zaujímavých tvrdení, bežne sa používa v matematike.

$$\forall\varepsilon > 0\ \exists\delta > 0 \ldots$$

Kalkuly — formalizácia usudzovania

Pre mnohé logické jazyky sú známe *kalkuly* — množiny usudzovacích pravidiel, ktoré sú

korektné — odvodzujú iba logické dôsledky,

úplné — umožňujú odvodiť všetky logické dôsledky.

Kalkuly sú bežné v matematike

- na počítanie s číslami, zlomkami (kalkul elementárnej aritmetiky),
- riešenie lineárnych rovníc (kalkul lineárnej algebry),
- derivovanie, integrovanie, riešenie diferenciálnych rovníc (kalkul matematickej analýzy)

$\vdots$

Sú korektné, ale nie vždy úplné.

Poznáte už aj jeden logický kalkul — ekvivalentné úpravy.

0.2 O tomto kurze

Prístup k logike na tomto predmete

Stredoškolský prístup príliš *neoddeľuje jazyk* výrokov od jeho *významu* a vlastne ani jednu stránku *nedefinuje jasne*.

Prevedieme vás základmi matematickej a výpočtovej logiky pre (postupne čoraz zložitejšie) fragmenty jazykov logiky prvého rádu.

Pojmy z logiky (výrok, model, logický dôsledok, dôkaz, ...) budeme *definovať matematicky* (ako množiny, postupnosti, funkcie, ...) *zdanlivo* budeme o jednoduchých veciach hovoriť zložito, na praktických cvičeniach ako *dátové štruktúry*.

Budeme *dokazovať* ich vlastnosti a *programovať* algoritmy podľa konštruktívnych dôkazov.

Budeme vyjadrovať výpočtové problémy v logických jazykoch a hľadať ich riešenia pomocou hotových nástrojov na riešenie logických problémov.

Organizácia kurzu — rozvrh, kontakty, pravidlá

Organizácia predmetu — rozvrh, kontakty a pravidlá absolvovania — sú popísané na oficiálnej webovej stránke predmetu:

1-AIN-412 https://dai.fmph.uniba.sk/w/Course:Mathematics_4

1-INF-210 http://www.dcs.fmph.uniba.sk/~mazak/vyucba/udml/

1 Atomické formuly

Jazyky logiky prvého rádu

Logika prvého rádu je trieda (rodina) formálnych jazykov.
Zdieľajú:

- časti abecedy — *logické symboly* (spojky, kvantifikátory)
- pravidlá tvorby *formúl* (slov)

Líšia sa v *mimologických symboloch* — časť abecedy, pomocou ktorej sa tvoria najjednoduchšie — *atomické formuly* (*atómy*).

Atomické formuly a výroky v prirodzenom jazyku

Atomické formuly logiky prvého rádu zodpovedajú *pozitívnym jednoduchým vetám* o vlastnostiach, stavoch, vzťahoch a rovnosti *jednotlivých pomenovaných* objektov.

Príklady 1.1.

- ✓ Milo beží.
- ✓ Jarka vidí Mila.
- ✗ Milo beží, ale Jarka ho nevidí.

- ✗ Jarka vidí všetkých.
- ✓ Jarka dala Milovi Bobíka v sobotu.
- ✗ Jarka nie je doma.
- ✗ Niekto je doma.
- ✓ Súčet 2 a 2 je 3.
- ✓ Prezidentkou SR je Zuzana Čaputová.

Indivíduové konštanty

Indivíduové konštanty sú symboly jazyka logiky prvého rádu, ktoré pomenúvajú jednotlivé, pevne zvolené objekty.

Zodpovedajú *približne* vlastným menám, jednoznačným pomenovaniam, niekedy zámenám; konštantám v matematike a programovacích jazykoch.

Príklady 1.2. Jarka, 2, Zuzana_Čaputová, sobota, π, …

Indivíduové konštanty a objekty

Indivíduová konštanta

- vždy pomenúva skutočný, existujúci objekt (na rozdiel od vlastného mena *Zeus*);
- nikdy nepomenúva viac objektov (na rozdiel od vlastného mena *Jarka*).

Objekt

- *môže* byť pomenovaný aj *viacerými* indivíduovými konštantami (napr. Prezidentka_SR a Zuzana_Čaputová);
- *nemusí* mať žiadne meno.

Predikátové symboly

Predikátové symboly sú symboly jazyka logiky prvého rádu, ktoré vyjadrujú vlastnosti alebo vzťahy.

Jednoduché vety v slovenčine majú *podmetovú* (*subjekt*) a *prísudkovú* časť (*predikát*):

Jarka	vidí	Mila.
podmet	prísudok	predmet
podmetová časť	prísudková časť	

Do logiky prvého rádu prekladáme takéto tvrdenie pomocou predikátového symbolu vidí, ktorý má dva *argumenty* („podmety“): indivíduové konštanty Jarka a Milo.

Úloha argumentu v predikáte je daná jeho poradím (podobne ako pozičné argumenty funkcií/metód v prog. jazykoch).

Arita predikátového symbolu

Predikátový symbol má pevne určený počet argumentov — *aritu*.

Vždy musí mať práve toľko argumentov, aká je jeho arita.

Dohoda 1.3. Aritu budeme *niekedy* písať ako horný index symbolu. Napríklad beží^1, vidí^2, dal^4, $<^2$.

Zamýšľaný význam predikátových symbolov

Unárny predikátový symbol (teda s aritou 1) zvyčajne označuje *vlastnosť*, druh, rolu, stav.

Príklady 1.4.

$\text{pes}(x)$	x je pes
$\text{čierne}(x)$	x je čierne
$\text{beží}(x)$	x beží

Binárny, *ternárny*, … predikátový symbol (s aritou 2, 3, …) zvyčajne označuje *vzťah* svojich argumentov.

Príklady 1.5.

$\text{vidí}(x, y)$	x vidí y
$\text{dal}(x, y, z, t)$	x dal(a/o) objektu y objekt z v čase t

Kategorickosť významu predikátových symbolov

V bežnom jazyku často nie je celkom jasné, či objekt má alebo nemá nejakú vlastnosť — kedy je niekto *mladý*?

Predikátové symboly predstavujú *kategorické* vlastnosti/vzťahy — pre každý objekt sa dá *jednoznačne rozhodnúť*, či má alebo nemá túto vlastnosť/vzťah s iným objektom či inými objektmi.

Význam predikátového symbolu preto často zodpovedá rovnakému slovenskému predikátu iba približne.

Príklad 1.6. Predikát mladší^2 môže označovať vzťah „x je mladší ako y“ presne.

Predikát mladý^1 zodpovedá vlastnosti „x je mladý“ iba približne.

Nekategorickými vlastnosťami sa zaoberajú *fuzzy* logiky. Predikáty v nich zachytávajú význam týchto vlastností presnejšie.

Atomické formuly

Atomické formuly majú tvar

$$predikát(argument_1, argument_2, \dots, argument_k),$$

alebo

$$argument_1 \doteq argument_2,$$

pričom k je arita *predikát*u, a $argument_1, \dots, argument_k$ sú (nateraz) indivíduové konštanty.

Atomická formula zodpovedá (jednoduchému) *výroku* v slovenčine, t.j. tvrdeniu, ktorého *pravdivostná hodnota* (pravda alebo nepravda) sa dá jednoznačne určiť, lebo predikát označuje kategorickú vlastnosť/vzťah a indivíduové konštanty jednoznačne označujú objekty.

Formalizácia jednoduchých výrokov

Formalizácia je preklad výrokov z prirodzeného jazyka do formálneho logického jazyka.

Nie je to jednoznačný proces.

Vopred daný prvorádový jazyk (konštanty a predikáty) sa snažíme využiť čo najlepšie.

Príklad 1.7. Sformalizujme v jazyku s konštantami Evka, Jarka a Milo a predikátom vyšší^2 výroky:

A_1: Jarka je vyššia ako Milo. $\rightsquigarrow$ vyšší(Jarka, Milo)

A_2: Evka je nižšia ako Milo. $\rightsquigarrow$ vyšší(Milo, Evka)

Zanedbávame nepodstatné detaily — pomocné slovesá, predložky, skloňovanie, rod, …: x je vyšší/vyššia/vyššie ako $y \rightsquigarrow$ vyšší(x, y).

Návrh jazyka pri formalizácii

Formalizácia spojená s *návrhom vlastného jazyka* je *iteratívna*: Postupne zisťujeme, aké predikáty a konštanty potrebujeme, upravujeme predchádzajúce formalizácie.

Príklady 1.8. A_1: Jarka dala Milovi Bobíka.

⇝ ~~d(Jarka)~~ ~~dalBobíka(Jarka, Milo)~~ dal(Jarka, Milo, Bobík)

A_2: Evka dostala Bobíka od Mila.

⇝ ~~dalBobíka(Milo, Evka)~~ dal(Milo, Evka, Bobík)

A_3: Evka dala Jarke Cilku.

⇝ ~~dalCilku(Evka, Jarka)~~ dal(Evka, Jarka, Cilka)

A_4: Bobík je pes.

⇝ pes(Bobík)

Návrh jazyka pri formalizácii

Minimalizujeme počet predikátov, uprednostňujeme flexibilnejšie, viacúčelovejšie (dal^3 pred $\mathsf{dalBobíka}^2$ a $\mathsf{dalCilku}^2$).

Dosiahneme

- expresívnejší jazyk (vyjadrí viac menším počtom prostriedkov),
- zrejmejšie logické vzťahy výrokov.

Podobné normalizácii databázových schém.

1.1 Syntax atomických formúl

Presné definície

Cieľom logiky je uvažovať o jazyku, výrokoch, vyplývaní, dôkazoch.

Výpočtová logika sa snaží automaticky riešiť konkrétne problémy vyjadrené v logických jazykoch.

Spoľahlivé a overiteľné úvahy a výpočty vyžadujú *presnú* dohodu na tom, o čom hovoríme — *definíciu* logických pojmov (jazyk, výrok, pravdivosť, …).

Pojmy (napr. *atomická formula*) môžeme zadefinovať napríklad

- *matematicky* ako množiny, n-tice, relácie, funkcie, postupnosti, …;
- *informaticky* tým, že ich *naprogramujeme*, napr. zadefinujeme triedu `AtomickaFormula` v Pythone.

Matematický jazyk je univerzálnejší ako programovací — abstraktnejší, menej nie až tak podstatných detailov.

Syntax atomických formúl logiky prvého rádu

Najprv sa musíme dohodnúť na tom, aká je *syntax* atomických formúl logiky prvého rádu:

- z čoho sa skladajú,
- čím vlastne sú,
- akú majú štruktúru.

Symboly jazyka atomických formúl logiky prvého rádu

Z čoho sa skladajú atomické formuly?

Definícia 1.9. *Symbolmi jazyka $\mathcal{L}$ atomických formúl logiky prvého rádu* sú mimologické, logické a pomocné symboly, pričom:

Mimologickými symbolmi sú

- *indivíduové konštanty* z nejakej neprázdnej spočítateľnej množiny $\mathcal{C}_\mathcal{L}$
- a *predikátové symboly* z nejakej spočítateľnej množiny $\mathcal{P}_\mathcal{L}$.

Jediným *logickým symbolom* je $\doteq$ (symbol rovnosti).

Pomocnými symbolmi sú **(**, **)** a **,** (ľavá, pravá zátvorka a čiarka).

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

Abeceda jazyka atomických formúl logiky prvého rádu

Na Úvode do teoretickej informatiky/Formálnych jazykoch a automatoch by ste povedali, že *abecedou* jazyka $\mathcal{L}$ atomických formúl logiky prvého rádu je $\Sigma_{\mathcal{L}} = \mathcal{C}_{\mathcal{L}} \cup \mathcal{P}_{\mathcal{L}} \cup \{\doteq, (,), ,\}$.

V logike sa väčšinou pojem *abeceda* nepoužíva, pretože potrebujeme rozlišovať *rôzne druhy* symbolov.

Namiesto *abeceda jazyka* $\mathcal{L}$ hovoríme *množina všetkých symbolov jazyka* $\mathcal{L}$ alebo len *symboly jazyka* $\mathcal{L}$.

Na zápise množiny $\Sigma_{\mathcal{L}}$ však ľahko vidíme, čím sa rôzne jazyky atomických formúl logiky prvého rádu od seba líšia a čo majú spoločné.

Príklady symbolov jazykov atomických formúl logiky prvého rádu

Príklad 1.10. Príklad o deťoch a zvieratkách sme sformalizovali v jazyku $\mathcal{L}_{\mathrm{dz}}$, v ktorom

$$\begin{aligned}
\mathcal{C}_{\mathcal{L}_{\mathrm{dz}}} &= \{\mathsf{Bobík}, \mathsf{Cilka}, \mathsf{Evka}, \mathsf{Jarka}, \mathsf{Milo}\},\\
\mathcal{P}_{\mathcal{L}_{\mathrm{dz}}} &= \{\mathsf{dal}, \mathsf{pes}\}, \quad \mathrm{ar}_{\mathcal{L}_{\mathrm{dz}}}(\mathsf{dal}) = 3, \quad \mathrm{ar}_{\mathcal{L}_{\mathrm{dz}}}(\mathsf{pes}) = 1.
\end{aligned}$$

Príklad 1.11. Príklad o návštevníkoch party by sme mohli sformalizovať v jazyku $\mathcal{L}_{\mathrm{party}}$, kde

$$\begin{aligned}
\mathcal{C}_{\mathcal{L}_{\mathrm{party}}} &= \{\mathsf{Kim}, \mathsf{Jim}, \mathsf{Sarah}\},\\
\mathcal{P}_{\mathcal{L}_{\mathrm{party}}} &= \{\mathsf{príde}\}, \quad \mathrm{ar}_{\mathcal{L}_{\mathrm{party}}}(\mathsf{príde}) = 1.
\end{aligned}$$

Označenia symbolov

Keď budeme hovoriť o *ľubovoľnom* jazyku $\mathcal{L}$, často budeme potrebovať nejak označiť niektoré jeho konštanty alebo predikáty, aj keď nebudeme vedieť, aké konkrétne symboly to sú.

Na označenie symbolov použijeme *meta premenné*: premenné v (matematickej) slovenčine, pomocou ktorých budeme hovoriť *o* (po grécky *meta*) týchto symboloch.

Dohoda 1.12. Indivíduové konštanty budeme spravidla označovať meta premennými a, b, c, d s prípadnými dolnými indexmi.

Predikátové symboly budeme spravidla označovať meta premennými P, Q, R s prípadnými dolnými indexmi.

Atomické formuly jazyka

Čo sú atomické formuly?

Definícia 1.13. Nech $\mathcal{L}$ je jazyk atomických formúl logiky prvého rádu.

Rovnostný atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $c_1 \doteq c_2$, kde c_1 a c_2 sú indivíduové konštanty z $\mathcal{C}_{\mathcal{L}}$.

Predikátový atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $P(c_1, \dots, c_n)$, kde P je predikátový symbol z $\mathcal{P}_{\mathcal{L}}$ s aritou n a $c_1, \dots, c_n$ sú indivíduové konštanty z $\mathcal{C}_{\mathcal{L}}$.

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

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

Slová jazyka atomických formúl logiky prvého rádu

Na Úvode do teoretickej informatiky by ste povedali, že jazyk $\mathcal{L}$ atomických formúl logiky prvého rádu nad abecedou $\Sigma_{\mathcal{L}} = \mathcal{C}_{\mathcal{L}} \cup \mathcal{P}_{\mathcal{L}} \cup \{\doteq, (,), ,\}$ je množina slov

$$\{\, c_1 \doteq c_2 \mid c_1 \in \mathcal{C}_{\mathcal{L}}, c_2 \in \mathcal{C}_{\mathcal{L}} \,\} \cup \{\, P(c_1, \dots, c_n) \mid P \in \mathcal{P}_{\mathcal{L}}, \mathrm{ar}_{\mathcal{L}}(P) = n, c_1 \in \mathcal{C}_{\mathcal{L}}, \dots, c_n \in \mathcal{C}_{\mathcal{L}} \,\}.$$

V logike sa jazyk takto nedefinuje, pretože potrebujeme rozlišovať *rôzne druhy slov*.

Príklady atómov jazyka

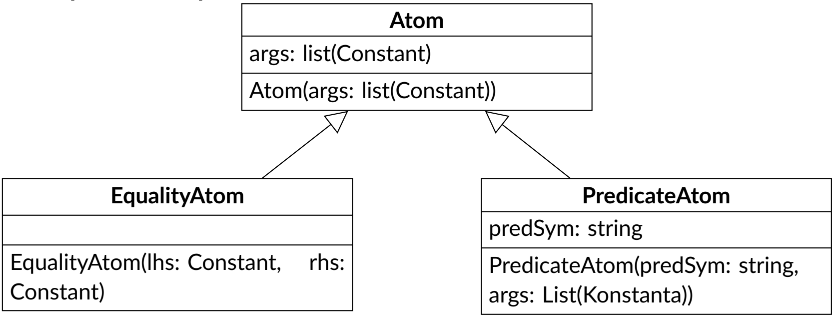
Príklad 1.14. V jazyku $\mathcal{L}_{\mathrm{dz}}$, kde $\mathcal{C}_{\mathcal{L}_{\mathrm{dz}}} = \{\mathsf{Bobík}, \mathsf{Cilka}, \mathsf{Evka}, \mathsf{Jarka}, \mathsf{Milo}\}$, $\mathcal{P}_{\mathcal{L}_{\mathrm{dz}}} = \{\mathsf{dal}, \mathsf{pes}\}$, $\mathrm{ar}_{\mathcal{L}_{\mathrm{dz}}}(\mathsf{dal}) = 3$, $\mathrm{ar}_{\mathcal{L}_{\mathrm{dz}}}(\mathsf{pes}) = 1$, sú *okrem iných* rovnostné atómy:

$$\begin{array}{cc} \mathsf{Bobík} \doteq \mathsf{Bobík} & \mathsf{Cilka} \doteq \mathsf{Bobík} \\ \mathsf{Evka} \doteq \mathsf{Jarka} & \mathsf{Bobík} \doteq \mathsf{Cilka} \end{array}$$

a predikátové atómy:

$$\mathsf{pes}(\mathsf{Cilka}) \qquad \mathsf{dal}(\mathsf{Cilka}, \mathsf{Milo}, \mathsf{Bobík}) \qquad \mathsf{dal}(\mathsf{Jarka}, \mathsf{Evka}, \mathsf{Milo}).$$

Atómy ako triedy



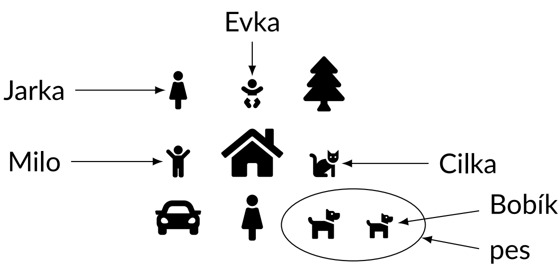
1.2 Sémantika atomických formúl

Vyhodnotenie atomickej formuly

Ako zistíme, či je atomická formula pes(Bobík) pravdivá v nejakej situácii (napríklad u babky Evky, Jarky a Mila na dedine)?

Pozrieme sa na túto situáciu a zistíme:

1. aký objekt b pomenúva konštanta Bobík;
2. akú vlastnosť p označuje predikát pes;
3. či objekt b má vlastnosť p.



Vyhodnotenie atomickej formuly

Ako môžeme tento postup matematicky alebo informaticky modelovať?
Potrebujeme:

- matematický/informatický model situácie (stavu vybranej časti sveta),

- postup na jeho použitie pri vyhodnocovaní pravdivosti formúl.

Matematický model stavu sveta

Ako môžeme matematicky popísať nejakú situáciu tak, aby sme pomocou tohto popisu mohli vyhodnocovať atomické formuly v nejakom jazyku logiky prvého rádu $\mathcal{L}$?

Matematický model stavu sveta

Potrebujeme vedieť:

- ktoré objekty sú v popisovanej situácii prítomné,
- ▶ množina všetkých týchto objektov — *doména*;
- jednoznačné priradenie významu všetkým indivíduovým konštantám a predikátom z jazyka $\mathcal{L}$
- ▶ *interpretačná funkcia*;
- pre každú indivíduovú konštantu c z jazyka $\mathcal{L}$, ktorý *objekt* z domény konštanta c pomenúva,
- pre každý unárny predikát P z jazyka $\mathcal{L}$, ktoré objekty z domény majú vlastnosť označenú predikátom P,
- ▶ tvoria *podmnožinu* domény;
- pre každý n-árny predikát R z jazyka $\mathcal{L}$, $n > 1$, ktoré n-tice objektov z domény sú vo vzťahu ozn. pred. R,
- ▶ tvoria *n-árnu reláciu* na doméne.

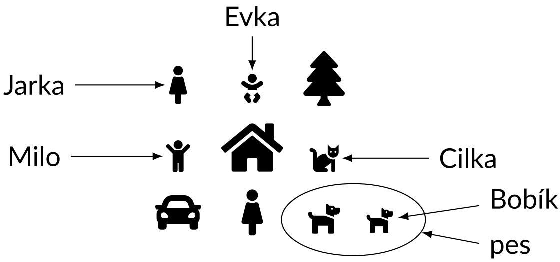
Štruktúra pre jazyk

Definícia 1.15. Nech $\mathcal{L}$ je jazyk atomických formúl logiky prvého rádu. *Štruktúrou* pre jazyk $\mathcal{L}$ (niekedy *interpretáciou* jazyka $\mathcal{L}$) nazývame dvojicu $\mathcal{M} = (D, i)$, kde D je ľubovoľná *neprázdna* množina nazývaná *doména* štruktúry $\mathcal{M}$; i je zobrazenie, nazývané *interpretačná funkcia* štruktúry $\mathcal{M}$, ktoré

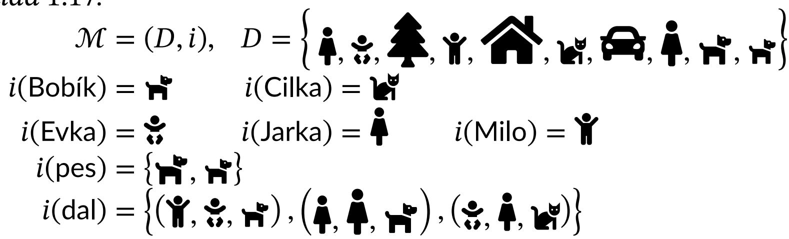
- každej indivíduovej konštante c jazyka $\mathcal{L}$ priraďuje prvok $i(c) \in D$;
- každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $i(P) \subseteq D^n$.

Dohoda 1.16. Štruktúry označujeme veľkými *písanými* písmenami $\mathcal{M}$, $\mathcal{N}$, ...

Príklad štruktúry



Príklad 1.17.



Štruktúra ako informatický objekt

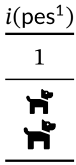
Štruktúru sme definovali pomocou *matematických* objektov.

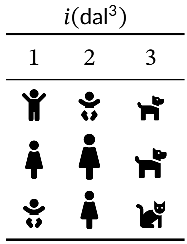
Aký *informatický* objekt sa podobá na štruktúru?

Databáza:

Predikátové symboly jazyka ~ veľmi zjednodušená schéma DB (arita ~ počet stĺpcov)

Interpretácia predikátových symbolov ~ konkrétne tabuľky s dátami





Štruktúry — upozornenia

Štruktúr pre daný jazyk je *nekonečne veľa*.
Doména štruktúry

- môže mať ľubovoľné prvky;
- nijak *nesúvisí* s intuitívnym významom interpretovaného jazyka;
- môže byť *nekonečná*.

Interpretácia symbolov konštánt:

- každej konštante je priradený objekt domény;
- nie každý objekt domény musí byť priradený nejakej konštante;
- rôznym konštantám môže byť priradený rovnaký objekt.

Interpretácie predikátových symbolov môžu byť *nekonečné*.

Príklad 1.18 (Štruktúra s nekonečnou doménou). $\mathcal{M} = (\mathbb{N}, i)$ $\quad i(\mathsf{pes}) = \{ 2n \mid n \in \mathbb{N} \}$ $\quad i(\mathsf{dal}) = \{ (n, m, n+m) \mid n, m \in \mathbb{N} \}$ $\quad i(\mathsf{Bobík}) = 0$ $\quad i(\mathsf{Cilka}) = 1$ $\quad i(\mathsf{Evka}) = 3$ $\quad i(\mathsf{Jarka}) = 5$ $\quad i(\mathsf{Milo}) = 0$

Pravdivosť atomickej formuly v štruktúre

Ako zistíme, či je atomická formula pravdivá v štruktúre?

Definícia 1.19. Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk $\mathcal{L}$ atomických formúl jazyka logiky prvého rádu.

Rovnostný atóm $c_1 \doteq c_2$ jazyka $\mathcal{L}$ je *pravdivý v štruktúre $\mathcal{M}$* vtedy a len vtedy, keď $i(c_1) = i(c_2)$.

Predikátový atóm $P(c_1, \dots, c_n)$ jazyka $\mathcal{L}$ je *pravdivý v štruktúre* $\mathcal{M}$ vtedy a len vtedy, keď $(i(c_1), \dots, i(c_n)) \in i(P)$.

Vzťah *atóm A je pravdivý v štruktúre $\mathcal{M}$* skrátene zapisujeme $\mathcal{M} \models A$. Hovoríme aj, že $\mathcal{M}$ je *modelom A*.

Vzťah *atóm A nie je pravdivý v štruktúre $\mathcal{M}$* zapisujeme $\mathcal{M} \not\models A$. Hovoríme aj, že *$A$ je nepravdivý* v $\mathcal{M}$ a *$\mathcal{M}$ nie je modelom A*.

Príklad 1.20 (Určenie pravdivosti atómov v štruktúre).

$\mathcal{M} = (D, i)$, $D = \{$👩, 👶, 🌲, 🧒, 🏠, 🐈, 🚗, 👩, 🐕, 🐕$\}$

$i(\mathsf{Bobík}) =$ 🐕 $\quad i(\mathsf{Cilka}) =$ 🐈

$i(\mathsf{Evka}) =$ 👶 $\quad i(\mathsf{Jarka}) =$ 👩 $\quad i(\mathsf{Milo}) =$ 🧒

$i(\mathsf{pes}) = \{$🐕, 🐕$\}$

$i(\mathsf{dal}) = \{($🧒, 👶, 🐕$), ($👩, 👩, 🐕$), ($👶, 👩, 🐈$)\}$

Atóm $\mathsf{pes}(\mathsf{Bobík})$ *je pravdivý* v štruktúre $\mathcal{M}$, t.j., $\mathcal{M} \models \mathsf{pes}(\mathsf{Bobík})$, lebo objekt $i(\mathsf{Bobík}) =$ 🐕 je prvkom množiny $\{$🐕, 🐕$\} = i(\mathsf{pes})$.

Atóm $\mathsf{dal}(\mathsf{Evka}, \mathsf{Jarka}, \mathsf{Cilka})$ *je pravdivý* v $\mathcal{M}$, t.j., $\mathcal{M} \models \mathsf{dal}(\mathsf{Evka}, \mathsf{Jarka}, \mathsf{Cilka})$, lebo $(i(\mathsf{Evka}), i(\mathsf{Jarka}), i(\mathsf{Cilka})) = ($👶, 👩, 🐈$) \in i(\mathsf{dal})$.

Atóm $\mathsf{Cilka} \doteq \mathsf{Bobík}$ *nie je pravdivý* v $\mathcal{M}$, t.j., $\mathcal{M} \not\models \mathsf{Cilka} \doteq \mathsf{Bobík}$, lebo $i(\mathsf{Cilka}) =$ 🐈 $\neq$ 🐕 $= i(\mathsf{Bobík})$.

1.3 Zhrnutie

Zhrnutie

- Logika prvého rádu je rodina formálnych jazykov.
- Každý jazyk logiky prvého rádu je daný neprázdnou množinou indivíduových konštánt a množinou predikátových symbolov.
- Atomické formuly sú základnými výrazmi prvorádového jazyka.
  - Postupnosti symbolov $P(c_1, \dots, c_n)$ (predikátové) a $c_1 \doteq c_2$ (rovnostné).
  - Zodpovedajú pozitívnym jednoduchým výrokom o vlastnostiach, stavoch, vzťahoch, rovnosti jednotlivých pomenovaných objektov.

- Význam jazyku dáva štruktúra — matematický opis stavu sveta
  - Skladá sa z neprázdnej domény a z interpretačnej funkcie.
  - Konštanty interpretuje ako prvky domény.
  - Predikáty interpretuje ako podmnožiny domény/relácie na doméne.
- Pravdivosť atómu určíme interpretovaním argumentov a zistením, či je výsledná n-tica objektov prvkom interpretácie predikátu, resp. pri rovnostnom atóme, či sa objekty rovnajú.

2. prednáška

Výrokovologické spojky

Rekapitulácia

Minulý týždeň sme si povedali:

- čo sú symboly jazyka *atomických formúl* logiky prvého rádu;
- čo sú atomické formuly;
- čo sú štruktúry:
  - modely stavu sveta,
  - neprázdna doména + interpretačná funkcia,
  - konštanty označujú objekty,
  - predikáty označujú vzťahy a vlastnosti;
- kedy sú atomické formuly pravdivé v danej štruktúre.
- Jazyk atomických formúl je oproti slovenčine veľmi slabý.
- Môžu byť pravdivé vo veľmi čudných štruktúrach.

2 Výrokovologické spojky

Výrokovologické spojky

Atomické formuly logiky prvého rádu môžeme spájať do zložitejších tvrdení *výrokovologickými spojkami*.

- Zodpovedajú spojkám v slovenčine, ktorými vytvárame súvetia.
- Významom spojky je vždy *boolovská funkcia*, teda funkcia na pravdivostných hodnotách spájaných výrokov. Pravdivostná hodnota zloženého výroku závisí *iba* od pravdivostných hodnôt podvýrokov.

Príklad 2.1. Negácia, konjunkcia, disjunkcia, implikácia, ekvivalencia, …

Nevýrokovologické spojky

Negatívny príklad

Spojka *pretože* nie je výrokovologická.

Dôkaz. Uvažujme o výroku „*Karol je doma, pretože Jarka je v škole*“.

Je pravdivý v situácii: Je 18:00 a Karol je doma, aby nakŕmil psíka. Ten by inak musel čakať na Jarku, ktorá šla dopoludnia do školy a vráti až o 19:30.

Nie je pravdivý v situácii: Jarka išla ráno do školy, ale Karol ostal doma, lebo je chorý. S Jarkinou prítomnosťou v škole to nesúvisí.

V oboch situáciách sú výroky „*Karol je doma*“ aj „*Jarka je v škole*“ pravdivé, ale pravdivostná hodnota zloženého výroku je rôzna. *Nezávisí* iba od pravdivostných hodnôt podvýrokov (ale od existencie vzťahu *príčina-následok* medzi nimi).

Spojka *pretože* teda nie je *funkciou* na pravdivostných hodnotách. □

2.1 Boolovské spojky

Negácia

Negácia ¬ je *unárna* spojka — má jeden argument, formulu.

Zodpovedá výrazom *nie*, „*nie je pravda, že* … “, predpone *ne*-.

Ľubovoľne vnárateľná.

Formula *vytvorená* negáciou sa *nezátvorkuje*.

Okolo argumentu negácie *nepridávame* zátvorky, ale môže ich mať on sám, ak to jeho štruktúra vyžaduje.

Príklad 2.2.

$\neg\mathsf{doma}(\mathsf{Karol})$	Karol *nie* je doma.
$\neg\mathsf{Jarka} \doteq \mathsf{Karol}$	Jarka *nie* je Karol.
$\neg\neg\neg\mathsf{poslúcha}(\mathsf{Cilka})$	*Nie* je pravda, že *nie* je pravda, že Cilka *ne*poslúcha.
$\cancel{(\neg\mathsf{doma}(\mathsf{Karol}))}$	nesprávna
$\cancel{\neg(\mathsf{doma}(\mathsf{Karol}))}$	syntax

Konjunkcia

Konjunkcia ∧ je *binárna* spojka.

Zodpovedá spojkám *a*, *aj*, *i*, *tiež*, *ale*, *avšak*, *no*, *hoci*, *ani*, *ba (aj/ani)*, …

Formalizujeme ňou zlučovacie, stupňovacie a odporovacie súvetia:

- Jarka je doma *aj* Karol je doma.
  $(\text{doma}(\text{Jarka}) \wedge \text{doma}(\text{Karol}))$

- Jarka je v škole, *no* Karol je doma.
  $(\text{v\_škole}(\text{Jarka}) \wedge \text{doma}(\text{Karol}))$

- *Ani* Jarka nie je doma, *ani* Karol tam nie je.
  $(\neg\text{doma}(\text{Jarka}) \wedge \neg\text{doma}(\text{Karol}))$

- *Nielen* Jarka je chorá, *ale aj* Karol je chorý.
  $(\text{chorý}(\text{Jarka}) \wedge \text{chorý}(\text{Karol}))$

Zloženú formulu vždy *zátvorkujeme*.

Formalizácia viacnásobných vetných členov konjunkciou

Zlučovacie viacnásobné vetné členy tiež formalizujeme ako konjunkcie:

- *Jarka aj Karol* sú doma.
  $(\text{doma}(\text{Jarka}) \wedge \text{doma}(\text{Karol}))$

- Karol *sa potkol a spadol*.
  $(\text{potkol\_sa}(\text{Karol}) \wedge \text{spadol}(\text{Karol}))$

- Jarka dostala Bobíka *od mamy a otca*.
  $(\text{dostal}(\text{Jarka}, \text{Bobík}, \text{mama}) \wedge \text{dostal}(\text{Jarka}, \text{Bobík}, \text{otec}))$

Podobne (jednoduché a viacnásobné zlučovacie) prívlastky vlastností:

- Eismann je *ruský špión*.
  $(\text{Rus}(\text{Eismann}) \wedge \text{špión}(\text{Eismann}))$

- Bobík je *malý čierny psík*.
  $\big((\text{malý}(\text{Bobík}) \wedge \text{čierny}(\text{Bobík})) \wedge \text{pes}(\text{Bobík})\big)$

Stratené v preklade

Zlučovacie súvetia niekedy vyjadrujú časovú následnosť, ktorá sa pri priamočiarom preklade do logiky prvého rádu *stráca*:

- Jarka a Karol sa stretli *a* išli do kina. $\big(\text{stretli\_sa}(\text{Jarka}, \text{Karol}) \wedge \big(\text{do\_kina}(\text{Jarka}) \wedge \text{do\_kina}(\text{Karol})\big)\big)$

- Jarka a Karol išli do kina *a* stretli sa. $\big($(do_kina(Jarka)$\wedge$do_kina(Karol))$\wedge$ stretli_sa(Jarka, Karol)$\big)$

Disjunkcia

Disjunkcia $\vee$ je binárna spojka, ktorá zodpovedá spojkám *alebo*, *či* v *inkluzívnom* význame (môžu nastať aj obe možnosti). Inkluzívnu disjunkciu vyjadruje tiež *„alebo aj/i"* a častice *respektíve*, *eventuálne*, *poprípade*, *prípadne*.

Disjunkciou formalizujeme vylučovacie súvetia s inkluzívnym významom:

- Jarka je doma *alebo* Karol je doma.
  (doma(Jarka) $\vee$ doma(Karol))

- Bobíka kúpe Jarka, prípadne ho kúpe Karol. (kúpe(Jarka, Bobík) $\vee$ kúpe(Karol, Bobík))

Zloženú formulu vždy *zátvorkujeme*.

Formalizácia viacnásobných vetných členov disjunkciou

Viacnásobné vetné členy s vylučovacou spojkou (v inkluzívnom význame) tiež prekladáme ako disjunkcie:

- Doma je Jarka alebo Karol. (doma(Jarka) $\vee$ doma(Karol))

- Jarka je doma alebo v škole. (doma(Jarka) $\vee$ v_škole(Jarka))

- Jarka dostala Bobíka od mamy alebo otca. (dostal(Jarka, Bobík, mama)$\vee$ dostal(Jarka, Bobík, otec))

- Bobík je čierny či tmavohnedý psík. $\big($(čierny(Bobík)$\vee$tmavohnedý(Bobík))$\wedge$ pes(Bobík)$\big)$

Exkluzívna disjunkcia

Konštrukcie *„buď …, alebo …"*, *„buď …, buď …"*, *„alebo …, alebo …"* *spravidla* (v matematike vždy) vyjadrujú *exkluzívnu* disjunkciu.

- Buď je batéria vybitá alebo svieti kontrolka.

Exkluzívnu disjunkciu môžeme vyjadriť zložitejšou formulou:

$$\big((\text{vybitá}(\text{batéria}) \lor \text{svieti}(\text{kontrolka})) \land \neg(\text{vybitá}(\text{batéria}) \land \text{svieti}(\text{kontrolka}))\big).$$

Niekedy aj samotné *alebo* spája možnosti, o ktorých vieme, že sú vzájomne výlučné (na základe znalostí o fungovaní domény alebo z kontextu):

- Jarka sa nachádza doma alebo v škole. (Nemôže byť súčasne na dvoch miestach.)

Viď *Znalosti na pozadí* ďalej.

Jednoznačnosť rozkladu

Formuly s binárnymi spojkami sú vždy uzátvorkované. Dajú sa jednoznačne rozložiť na podformuly a interpretovať.

Slovenské tvrdenia so spojkami nie sú vždy jednoznačné:

- Karol je doma a Jarka je doma alebo je Bobík šťastný.
  - ? $\big((\text{doma}(\text{Karol}) \land \text{doma}(\text{Jarka})) \lor \text{šťastný}(\text{Bobík})\big)$
  - ? $\big(\text{doma}(\text{Karol}) \land (\text{doma}(\text{Jarka}) \lor \text{šťastný}(\text{Bobík}))\big)$
- Karol je doma alebo Jarka je doma a Bobík je šťastný.
  - ? $\big((\text{doma}(\text{Karol}) \lor \text{doma}(\text{Jarka})) \land \text{šťastný}(\text{Bobík})\big)$
  - ? $\big(\text{doma}(\text{Karol}) \lor (\text{doma}(\text{Jarka}) \land \text{šťastný}(\text{Bobík}))\big)$

Jednoznačnosť rozkladu v slovenčine

Slovenčina má prostriedky podobné zátvorkám:

- Viacnásobný vetný člen (+*obaja*, *niekto z*):
  - Karol aj Jarka sú (obaja) doma alebo je Bobík šťastný.
    $\big((\text{doma}(\text{Karol}) \land \text{doma}(\text{Jarka})) \lor \text{šťastný}(\text{Bobík})\big)$
  - Doma je Karol alebo Jarka a Bobík je šťastný.
    Niekto z dvojice Karol a Jarka je doma a Bobík je šťastný.
    $\big((\text{doma}(\text{Karol}) \lor \text{doma}(\text{Jarka})) \land \text{šťastný}(\text{Bobík})\big)$

- Kombinácie spojok *buď …, alebo …, alebo …*; *aj …, aj …*; *ani …, ani …*; a pod.
  - Karol je doma a buď je doma Jarka, alebo je Bobík šťastný, alebo jedno aj druhé. Aj Karol je doma, aj je doma Jarka alebo je Bobík šťastný.
    $(\text{doma}(\text{Karol}) \land (\text{doma}(\text{Jarka}) \lor \text{šťastný}(\text{Bobík})))$
  - Buď je doma Karol, alebo je doma Jarka a Bobík je šťastný, alebo aj aj. $(\text{doma}(\text{Karol}) \lor (\text{doma}(\text{Jarka}) \land \text{šťastný}(\text{Bobík})))$

Oblasť platnosti negácie

Výskyt negácie sa vzťahuje na *najkratšiu nasledujúcu formulu* — *oblasť platnosti* tohto výskytu.

- $((\neg\,\text{doma}(\text{Karol}) \land \text{doma}(\text{Jarka})) \lor \text{šťastný}(\text{Bobík}))$
- $(\neg\,(\text{doma}(\text{Karol}) \land \text{doma}(\text{Jarka})) \lor \text{šťastný}(\text{Bobík}))$

Argument negácie je *uzátvorkovaný práve vtedy*, keď je *priamo* vytvorený binárnou spojkou:

✔ $\neg\neg(\text{doma}(\text{Karol}) \land \text{doma}(\text{Jarka}))$

✖ $\neg(\neg(\text{doma}(\text{Karol}) \land \text{doma}(\text{Jarka})))$

Negácia rovnostného atómu

Rovnosť nie je spojka, preto:

✔ $\neg\,\text{Jarka} \doteq \text{Karol}$ — Jarka *nie* je Karol.

✖ $\neg(\text{Jarka} \doteq \text{Karol})$

Zátvorky sú zbytočné, lebo čítanie „*«Nie je pravda, že Jarka» sa rovná Karol*“ je nezmyselné:

1. Syntakticky: Negácia sa vzťahuje na formulu. Konštanta nie je formula, rovnosť s oboma argumentmi je.

2. Sémanticky: Negácia je funkcia na pravdivostných hodnotách. Konštanty označujú objekty domény. Objekty nie sú pravdivé ani nepravdivé.

Dohoda 2.3. Formulu $\neg \tau \doteq \sigma$ budeme skrátene zapisovať $\tau \not\doteq \sigma$.

2.2 Implikácia

Implikácia

Implikácia $\rightarrow$ je binárna spojka približne zodpovedajúca podmienkovému podraďovaciemu súvetiu *ak …, tak …*.

Vo formule $(A \rightarrow B)$ hovoríme podformule A *antecedent* a podformule B *konzekvent*.

Formula vytvorená implikáciou je *nepravdivá* v *jedinom* prípade: antecedent je pravdivý a konzekvent nepravdivý.

Tomuto významu nezodpovedajú všetky súvetia *ak …, tak …*:

Napr. veta „*Ak* by *Sarah prišla, Jim* by *prišiel tiež.*“ je nepravdivá, keď ňou chceme povedať, že si myslíme, že išli rovnakým autobusom, ale v skutočnosti Jim išiel iným a zmeškal ho.

Implikácia plne nevystihuje prípady, keď *ak …, tak …* vyjadruje (neboolovský) vzťah príčina-následok (ako *pretože*).

Keď …, potom … má často význam časovej následnosti, ktorý implikácia tiež nepostihuje.

Nutná a postačujúca podmienka

Implikáciu vyjadrujú aj súvetia:

Jim príde, *ak* príde Kim.	Jim príde, *iba ak* príde Kim.

Vedľajšie vety (*príde Kim*) sú *podmienkami* hlavnej vety (*Jim príde*).

Ale je medzi nimi *podstatný rozdiel*:

$$\text{Jim príde, } \underbrace{\textit{ak}\text{ príde Kim.}}_{\substack{\textit{postačujúca}\\ \text{podmienka}}} \qquad \text{Jim príde, } \underbrace{\textit{iba ak}\text{ príde Kim.}}_{\substack{\textit{nutná}\\ \text{podmienka}}}$$

Postačujúca podmienka

Jim príde, *ak* príde Kim.

- Na to, aby prišiel Jim, *stačí*, aby prišla Kim.

- Teda, ak príde Kim, tak príde aj Jim.
- Nepravdivé, keď Kim príde, ale Jim *ne*príde.
- Zodpovedá teda (príde(Kim) → príde(Jim)).

Vo všeobecnosti:

$$A\text{, ak } B. \qquad \rightsquigarrow \qquad (B \to A)$$

Iné vyjadrenia:

- Jim príde, *pokiaľ* príde Kim.

Nutná podmienka

Jim príde, *iba ak* príde Kim.

- Na to, aby prišiel Jim, *je nevyhnutné*, aby prišla Kim, ale nemusí to stačiť.
- Teda, ak Jim príde, tak príde aj Kim.
- Nepravdivé, keď Jim príde, ale Kim *ne*príde.
- Zodpovedá teda (príde(Jim) → príde(Kim)).

Vo všeobecnosti:

$$A\text{, iba ak } B. \qquad \rightsquigarrow \qquad (A \to B)$$

Iné vyjadrenia:

- Jim príde, *iba pokiaľ* s Kim.
- Jim príde *iba* spolu s Kim.
- Jim *ne*príde *bez* Kim.

Nutná a postačujúca podmienka rukolapne

Určite by sa vám páčilo, keby z pravidiel predmetu vyplývalo:

> Z logiky prejdete, *ak* odovzdáte všetky domáce úlohy.

Stačilo by odovzdať úlohy a *nebolo by nutné* urobiť nič iné.

Žiaľ, z našich pravidiel vyplýva:

> Z logiky prejdete, *iba ak* odovzdáte všetky domáce úlohy.

Odovzdať úlohy *je nutné*, ale na prejdenie to *nestačí*.

Súvetia formalizované implikáciou

$(A \to B)$ formalizuje (okrem iných) zložené výroky:

- Ak A, tak B.
- Ak A, tak aj B.
- Ak A, B.
- Pokiaľ A, [tak (aj)] B.
- A, iba/len/jedine ak/pokiaľ(/keď) B.
- A nastane iba spolu s B.
- A nenastane bez B.
- B, ak/pokiaľ(/keď) A.

2.3 Ekvivalencia

Ekvivalencia

Ekvivalencia $\leftrightarrow$ vyjadruje, že ňou spojené výroky majú rovnakú pravdivostnú hodnotu.

Zodpovedá slovenským výrazom *ak a iba ak*; *vtedy a len vtedy, keď*; *práve vtedy, keď*; *rovnaký … ako …*; *taký … ako …*.

- Jim príde, ak a iba ak príde Kim. (príde(Jim) $\leftrightarrow$ príde(Kim))
- Číslo n je párne práve vtedy, keď n^2 je párne. (párne(n) $\leftrightarrow$ párne(n^2))
- Müller je taký Nemec, ako je Stirlitz Rus. (Nemec(Müller) $\leftrightarrow$ Rus(Stirlitz))

Ekvivalencia

Ekvivalencia ($A \leftrightarrow B$) zodpovedá tvrdeniu, že A je nutnou *aj* postačujúcou podmienkou B.

Budeme ju preto považovať za *skratku* za formulu

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

Ďalšie spojky a vetné konštrukcie

V slovenčine a iných prirodzených aj umelých jazykoch sa dajú tvoriť aj oveľa komplikovanejšie podmienené tvrdenia:

- Karol je doma, *ak* je Jarka v škole, *inak* má Jarka obavy.
- Karol je doma, *ak* je Jarka v škole, *inak* má Jarka obavy, *okrem* prípadov, keď je Bobík s ním.

Výrokovologické spojky sa dajú vytvoriť aj pre takéto konštrukcie, ale väčšinou sa to nerobí.

Na ich vyjadrenie stačia aj základné spojky. Mohli by sme pre ne vymyslieť označenie a považovať aj ako skratky, podobne ako ekvivalenciu.

2.4 Syntax výrokovologických formúl

Syntax a sémantika formúl s výrokovologickými spojkami

Podobne ako pri atomických formulách, aj pri formulách s výrokovologickými spojkami potrebujeme *zadefinovať* — presne a záväzne — ich *syntax* (skladbu) a *sémantiku* (význam).

Niektoré definície preberieme, iné rozšírime alebo modifikujeme, ďalšie pridáme.

Syntax výrokovologických formúl logiky prvého rádu špecifikuje:

- z čoho sa skladajú,
- čím sú a akú majú štruktúru.

Symboly výrokovologickej časti logiky prvého rádu

Definícia 2.4. *Symbolmi jazyka $\mathcal{L}$ výrokovologickej časti logiky prvého rádu* sú:

mimologické symboly, ktorými sú

- *indivíduové konštanty* z nejakej neprázdnej spočítateľnej množiny $\mathcal{C}_{\mathcal{L}}$
- a *predikátové symboly* z nejakej spočítateľnej množiny $\mathcal{P}_{\mathcal{L}}$;

logické symboly, ktorými sú

- *výrokovologické spojky* $\neg$, $\land$, $\lor$, $\to$ (nazývané, v uvedenom poradí, *symbol negácie*, *symbol konjunkcie*, *symbol disjunkcie*, *symbol implikácie*);
- a *symbol rovnosti* $\doteq$;

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

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

Atomické formuly

Definícia atomických formúl je takmer rovnaká ako doteraz:

Definícia 2.5. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.

Rovnostný atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $c_1 \doteq c_2$, kde c_1 a c_2 sú indivíduové konštanty z $\mathcal{C}_{\mathcal{L}}$.

Predikátový atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $P(c_1, \dots, c_n)$, kde P je predikátový symbol z $\mathcal{P}_{\mathcal{L}}$ s aritou n a c_1, …, c_n sú indivíduové konštanty z $\mathcal{C}_{\mathcal{L}}$.

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

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

Čo sú výrokovologické formuly?

Majme jazyk $\mathcal{L}$, kde $\mathcal{C}_\mathcal{L} = \{\mathsf{Kim}, \mathsf{Jim}, \mathsf{Sarah}\}$ a $\mathcal{P}_\mathcal{L} = \{\mathsf{príde}^1\}$.
Čo sú formuly tohto jazyka?

- Samotné atómy, napr. $\mathsf{príde}(\mathsf{Sarah})$.
- Negácie atómov, napr. $\neg\mathsf{príde}(\mathsf{Sarah})$.
- Atómy alebo aj ich negácie spojené spojkou, napr. $(\neg\mathsf{príde}(\mathsf{Kim})\lor\mathsf{príde}(\mathsf{Sarah}))$.
- Ale negovať a spájať spojkami môžeme aj zložitejšie formuly, napr. $\big(\neg(\mathsf{príde}(\mathsf{Kim}) \land \mathsf{príde}(\mathsf{Sarah})) \to (\neg\mathsf{príde}(\mathsf{Kim}) \lor \neg\mathsf{príde}(\mathsf{Sarah}))\big)$.

Ako to presne a úplne popíšeme?

Čo sú výrokovologické formuly?

Ako presne a úplne popíšeme, čo je formula?
Induktívnou definíciou:

1. Povieme, čo sú základné formuly, ktoré sa nedajú rozdeliť na menšie formuly.
   - ▶ Podobne ako báza pri matematickej indukcii.
2. Opíšeme, ako sa z jednoduchších formúl skladajú zložitejšie.
   - ▶ Podobne ako indukčný krok pri matematickej indukcii.
3. Zabezpečíme, že nič iné nie je formulou.

Formuly jazyka výrokovologickej časti logiky prvého rádu

Definícia 2.6. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. *Množina $\mathcal{E}_\mathcal{L}$ formúl jazyka $\mathcal{L}$* je (3.) *najmenšia* množina postupností symbolov, ktorá spĺňa všetky nasledujúce podmienky:

1. Každý atóm z $\mathcal{A}_\mathcal{L}$ je formulou z $\mathcal{E}_\mathcal{L}$.

2.1. Ak A patrí do $\mathcal{E}_\mathcal{L}$, tak aj postupnosť symbolov $\neg A$ patrí do $\mathcal{E}_\mathcal{L}$ a nazývame ju *negácia* formuly A.

2.2. Ak A a B sú v $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosti symbolov $(A \wedge B)$, $(A \vee B)$ a $(A \to B)$ patria do $\mathcal{E}_{\mathcal{L}}$ a nazývame ich postupne *konjunkcia*, *disjunkcia* a *implikácia* formúl A a B.

Každý prvok A množiny $\mathcal{E}_{\mathcal{L}}$ nazývame *formulou* jazyka $\mathcal{L}$.

Dohody · Vytvorenie formuly

Dohoda 2.7. Formuly označujeme meta premennými A, B, C, X, Y, Z, podľa potreby aj s dolnými indexmi.

Dohoda 2.8. Pre každú dvojicu formúl $A, B \in \mathcal{E}_{\mathcal{L}}$ je zápis $(A \leftrightarrow B)$ *skratka* za formulu $((A \to B) \wedge (B \to A))$.

Technicky $(\cdot \leftrightarrow \cdot) : \mathcal{E}_{\mathcal{L}} \to \mathcal{E}_{\mathcal{L}}$ funkcia na formulách definovaná ako $(A \leftrightarrow B) = \big((A \to B) \wedge (B \to A)\big)$ pre každé dve formuly A a B.

Príklad 2.9. Ako by sme podľa definície 2.6 mohli dokázať, že $\big(\neg \mathsf{príde}(\mathsf{Kim}) \to (\mathsf{príde}(\mathsf{Jim}) \vee \mathsf{príde}(\mathsf{Sarah}))\big)$ je formula? Teda, ako by sme ju podľa definície 2.6 mohli *vytvoriť*?

Indukcia na konštrukciu formuly

Veta 2.10 (Princíp indukcie na konštrukciu formuly). *Nech P je ľubovoľná vlastnosť formúl ($P \subseteq \mathcal{E}_{\mathcal{L}}$). Ak platí súčasne*

1. *každý atóm z $\mathcal{A}_{\mathcal{L}}$ má vlastnosť P,*

2.1. *ak formula A má vlastnosť P, tak aj $\neg A$ má vlastnosť P,*

2.2. *ak formuly A a B majú vlastnosť P, tak aj každá z formúl $(A \wedge B)$, $(A \vee B)$ a $(A \to B)$ má vlastnosť P,*

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

Vytvárajúca postupnosť

Definícia 2.11. *Vytvárajúcou postupnosťou* nad jazykom $\mathcal{L}$ výrokovologickej časti logiky prvého rádu je ľubovoľná konečná postupnosť $A_0, \ldots, A_n$ postupností symbolov, ktorej každý člen

- je atóm z $\mathcal{A}_{\mathcal{L}}$, alebo
- má tvar $\neg A$, pričom A je niektorý predchádzajúci člen postupnosti, alebo
- má jeden z tvarov $(A \land B)$, $(A \lor B)$, $(A \to B)$, kde A a B sú niektoré predchádzajúce členy postupnosti.

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

Formula a existencia vytvárajúcej postupnosti

Tvrdenie 2.12. *Postupnosť symbolov A je výrokovologickou formulou vtt existuje vytvárajúca postupnosť pre A.*

Osnova dôkazu. ($\Rightarrow$) *Indukciou na konštrukciu formuly*
($\Leftarrow$) *Indukciou na dĺžku vytvárajúcej postupnosti* □

vtt skracuje „*vtedy a len vtedy, keď*“.
Vytvárajúcu postupnosť by sme mohli použiť na alternatívnu definíciu formúl.

(Ne)jednoznačnosť rozkladu formúl výrokovej logiky

Čo keby sme zadefinovali „formuly“ takto?

Definícia „formúl“ ⚠

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Množina $\mathcal{E}_{\mathcal{L}}$ „formúl“ jazyka $\mathcal{L}$ je (3.) *najmenšia* množina postupností symbolov, ktorá spĺňa všetky nasledujúce podmienky:

1. Každý atóm z $\mathcal{A}_{\mathcal{L}}$ je „formulou“ z $\mathcal{E}_{\mathcal{L}}$.

2.1. Ak A patrí do $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosť symbolov $\neg A$ patrí do $\mathcal{E}_{\mathcal{L}}$.

2.2. Ak A a B sú v $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosti symbolov $A \land B$, $A \lor B$ a $A \to B$ patria do $\mathcal{E}_{\mathcal{L}}$.

2.3. ak A patrí do $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosť symbolov (A) je v $\mathcal{E}_{\mathcal{L}}$.

Každý prvok A množiny $\mathcal{E}_{\mathcal{L}}$ nazývame „formulou“ jazyka $\mathcal{L}$.

Čo znamená „formula“ (príde(Jim) → príde(Kim) → ¬príde(Sarah))?

Formulu by sme mohli čítať ako A = (príde(Jim) → (príde(Kim) → ¬príde(Sarah))) alebo ako B = ((príde(Jim) → príde(Kim)) → ¬príde(Sarah)).

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

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

Jednoznačnosť rozkladu formúl výrokovej logiky

Pre našu definíciu formúl platí:

Tvrdenie 2.13 (o jednoznačnosti rozkladu). *Pre každú formulu $X \in \mathcal{E}_{\mathcal{L}}$ v jazyku $\mathcal{L}$ platí práve jedna z nasledujúcich možností:*

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

Problémy s vytvárajúcou postupnosťou

Vytvárajúca postupnosť popisuje konštrukciu formuly podľa definície formúl:

$$\begin{gathered}\text{príde(Jim)},\ \text{príde(Sarah)},\ \neg\text{príde(Jim)},\ \text{príde(Kim)},\\ \neg\text{príde(Sarah)},\ (\neg\text{príde(Jim)} \land \text{príde(Kim)}),\\ ((\neg\text{príde(Jim)} \land \text{príde(Kim)}) \to \neg\text{príde(Sarah)})\end{gathered}$$

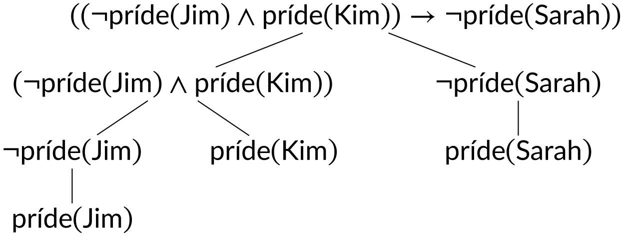
ale

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

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

Vytvárajúci strom

Konštrukciu si vieme predstaviť ako *strom*:



Takéto stromy voláme *vytvárajúce*.

Ako ich *presne* a *všeobecne* popíšeme — zadefinujeme?
Podobne ako sa definuje napr. binárny vyhľadávací strom.

Vytvárajúci strom formuly

Definícia 2.14. *Vytvárajúci strom T* pre formulu X je binárny strom obsahujúci v každom vrchole formulu, pričom platí:

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

Syntaktické vzťahy formúl

Uvažujme formulu:

((¬príde(Jim) ∧ príde(Kim)) → ¬príde(Sarah))

Ako nazveme formuly, z ktorých vznikla?

príde(Sarah), ¬príde(Jim), (¬príde(Jim) ∧ príde(Kim)), …

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

$$(\neg\text{príde}(\text{Jim}) \land \text{príde}(\text{Kim})) \quad \text{a} \quad \neg\text{príde}(\text{Sarah})$$

Ako tieto pojmy presne zadefinujeme?

Podformuly

Definícia 2.15 (Priama podformula)**.** Pre všetky formuly A a B:

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

Definícia 2.16 (Podformula)**.** Vzťah *byť podformulou* je najmenšia relácia na formulách spĺňajúca pre všetky formuly X, Y a Z:

- X je podformulou X.
- 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.

Formula X je *vlastnou podformulou* formuly Y práve vtedy, keď X je podformulou Y a $X \neq Y$.

Meranie syntaktickej zložitosti formúl

Miera zložitosti/veľkosti formuly:

- Jednoduchá: dĺžka, teda počet symbolov
  - Počíta aj pomocné symboly.
  - Nič nemá mieru 0, ani atómy.
- Lepšia: počet netriviálnych krokov pri konštrukcii formuly
  - pridanie negácie,
  - spojenie formúl spojkou.

Túto lepšiu mieru nazývame *stupeň formuly*.

Príklad 2.17. Aký je stupeň formuly $\big((\text{príde}(\text{Jim}) \lor \neg\text{príde}(\text{Kim})) \land \neg(\text{príde}(\text{Sarah}) \to \text{pr}$

Meranie syntaktickej zložitosti formúl

Ako stupeň zadefinujeme?

Podobne ako sme zadefinovali formuly — induktívne:

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

Stupeň formuly

Definícia 2.18 (Stupeň formuly)**.** Pre všetky formuly A a B a všetky n, $n_1, n_2 \in \mathbb{N}$:

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

Definícia 2.18 (Stupeň formuly presnejšie a symbolicky)**.** *Stupeň* $\deg(X)$ formuly $X \in \mathcal{E}_{\mathcal{L}}$ definujeme pre všetky formuly $A, B \in \mathcal{E}_{\mathcal{L}}$ nasledovne:

- $\deg(A) = 0$, ak $A \in \mathcal{A}_{\mathcal{L}}$,
- $\deg(\neg A) = \deg(A) + 1$,
- $\deg((A \wedge B)) = \deg((A \vee B)) = \deg((A \to B)) = \deg(A) + \deg(B) + 1$.

Indukcia na stupeň formuly

Pomocou stupňa vieme indukciu na konštrukciu formuly zredukovať na špeciálny prípad matematickej indukcie:

Veta 2.19 (Princíp indukcie na stupeň formuly)**.** *Nech P je ľubovoľná vlastnosť formúl ($P \subseteq \mathcal{E}_{\mathcal{L}}$). Ak platí súčasne*

1. báza indukcie: *každá formula stupňa* 0 *má vlastnosť P,*
2. 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 ($P = \mathcal{E}_{\mathcal{L}}$).

2.5 Sémantika výrokovologických formúl

Sémantika výrokovej logiky

Význam formúl výrokovologickej časti logiky prvého rádu popíšeme podobne ako význam atomických formúl pomocou *štruktúr*.

Štruktúra pre jazyk

Definícia štruktúry takmer nemení:

Definícia 2.20. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. *Štruktúrou* pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (D, i)$, kde D je ľubovoľná *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 $i(c) \in D$;
- každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $i(P) \subseteq D^n$.

Pravdivosť formuly v štruktúre

Definícia 2.21. Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk $\mathcal{L}$ výrokovologickej časti logiky prvého rádu. Reláciu *formula A je pravdivá v štruktúre $\mathcal{M}$* ($\mathcal{M} \models A$) definujeme *induktívne* pre všetky arity $n > 0$, všetky predikátové symboly P s aritou n všetky konštanty $c_1, c_2, \dots, c_n$, a všetky formuly A, B jazyka $\mathcal{L}$ nasledovne:

- $\mathcal{M} \models c_1 \doteq c_2$ vtt $i(c_1) = i(c_2)$,
- $\mathcal{M} \models P(c_1, \dots, c_n)$ vtt $\big(i(c_1), \dots, i(c_n)\big) \in i(P)$,
- $\mathcal{M} \models \neg A$ 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 $\mathcal{M} \models B$,

kde $\mathcal{M} \not\models A$ skracuje *A nie je pravdivá v $\mathcal{M}$*.

Vyhodnotenie pravdivosti formuly

Príklad 2.22 (Vyhodnotenie pravdivosti formuly v štruktúre). Majme štruktúru $\mathcal{M} = (D, i)$ pre jazyk o party, kde $D = \{0, 1, 2, 3\}$, $i(\mathsf{Kim}) = 1$, $i(\mathsf{Jim}) = 2$, $i(\mathsf{Sarah}) = 3$, $i(\mathsf{príde}) = \{1, 3\}$.

Formuly vyhodnocujeme podľa definície postupom zdola nahor (od atómov cez zložitejšie podformuly k cieľovej formule):

- $\mathcal{M} \not\models (\neg(\mathsf{príde}(\mathsf{Jim}) \lor \neg\mathsf{príde}(\mathsf{Kim})) \to \neg\mathsf{príde}(\mathsf{Sarah}))$
  - $\mathcal{M} \models \neg(\mathsf{príde}(\mathsf{Jim}) \lor \neg\mathsf{príde}(\mathsf{Kim}))$
    - $\mathcal{M} \not\models (\mathsf{príde}(\mathsf{Jim}) \lor \neg\mathsf{príde}(\mathsf{Kim}))$
      - $\mathcal{M} \not\models \mathsf{príde}(\mathsf{Jim})$
        - $i(\mathsf{Jim}) \notin i(\mathsf{príde})$
          - $2 \notin \{1, 3\}$
      - $\mathcal{M} \not\models \neg\mathsf{príde}(\mathsf{Kim})$
        - $\mathcal{M} \models \mathsf{príde}(\mathsf{Kim})$
          - $i(\mathsf{Kim}) \in i(\mathsf{príde})$
            - $1 \in \{1, 3\}$
  - $\mathcal{M} \not\models \neg\mathsf{príde}(\mathsf{Sarah})$
    - $\mathcal{M} \models \mathsf{príde}(\mathsf{Sarah})$
      - $i(\mathsf{Sarah}) \in i(\mathsf{príde})$
        - $3 \in \{1, 3\}$

Vyhodnotenie pravdivosti formuly

Príklad 2.23 (Vyhodnotenie pravdivosti formuly v štruktúre). Majme štruktúru $\mathcal{M} = (D, i)$ pre jazyk o party, kde $D = \{0, 1, 2, 3\}$, $i(\mathsf{Kim}) = 1$, $i(\mathsf{Jim}) = 2$, $i(\mathsf{Sarah}) = 3$, $i(\mathsf{príde}) = \{1, 3\}$.

Vyhodnotenie pravdivosti môžeme zapísať aj tabuľkou:

	$p(J)$	$p(K)$	$\neg p(K)$	$(p(J) \lor \neg p(K))$	$\neg(p(J) \lor \neg p(K))$	$p(S)$	$\neg p(S)$	$(\neg(p(J) \lor \neg p(K)) \to \neg p(S))$
$\mathcal{M}$	$\not\models$	$\models$	$\not\models$	$\not\models$	$\models$	$\models$	$\not\models$	$\not\models$

kde $p = \mathsf{príde}$, $K = \mathsf{Kim}$, $J = \mathsf{Jim}$ a $S = \mathsf{Sarah}$.

Všimnite si, že v záhlaví tabuľky je vytvárajúca postupnosť vyhodnocovanej formuly.

Hľadanie štruktúry

Príklad 2.24 (Nájdenie štruktúry, v ktorej je formula pravdivá). *V akej štruktúre* $\mathcal{M} = (D, i)$ je pravdivá formula $\mathcal{M} \models \big(\neg(\text{príde}(\text{Jim}) \lor \neg\text{príde}(\text{Kim})) \to \neg\text{príde}(\text{Sarah})\big)$?

Na zodpovedanie je dobré postupovať podľa definície pravdivosti zhora nadol (od cieľovej formuly cez podformuly k atómom):

$\mathcal{M} \models \big(\neg(\text{príde}(\text{Jim}) \lor \neg\text{príde}(\text{Kim})) \to \neg\text{príde}(\text{Sarah})\big)$ vtt $\mathcal{M} \not\models \neg(\text{príde}(\text{Jim}) \lor \neg\text{príde}(\text{Kim}))$ alebo $\mathcal{M} \models \neg\text{príde}(\text{Sarah})$ vtt $\mathcal{M} \models (\text{príde}(\text{Jim}) \lor \neg\text{príde}(\text{Kim}))$ alebo $\mathcal{M} \not\models \text{príde}(\text{Sarah})$ vtt $\mathcal{M} \models \text{príde}(\text{Jim})$ alebo $\mathcal{M} \models \neg\text{príde}(\text{Kim})$ alebo $\mathcal{M} \not\models \text{príde}(\text{Sarah})$ vtt $i(\text{Jim}) \in i(\text{príde})$ alebo $i(\text{Kim}) \notin i(\text{príde})$ alebo $i(\text{Sarah}) \notin i(\text{príde})$.

2.6 Teórie a ich modely

Teórie v neformálnej logike

Medzi základnými logickými pojmami z úvodnej prednášky boli teória a model.

Neformálne je *teória* súbor tvrdení, ktoré pokladáme za pravdivé.

Zvyčajne popisujú našu predstavu o zákonitostiach platných v nejakej časti sveta a pozorovania o jej stave.

Príklad 2.25. Máme troch nových známych — Kim, Jima a Sarah. Organizujeme párty a P0: chceme, aby na ňu prišiel niekto z nich. Od spoločných kamarátov sme sa ale dozvedeli o ich požiadavkách:

P1: Sarah nepríde na párty, ak príde Kim.

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

P3: Sarah nepríde bez Jima.

Výrokovologické teórie

V logike prvého rádu tvrdenia zapisujeme formulami. Teóriu preto budeme chápať ako súbor (čiže množinu) formúl.

Definícia 2.26. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Každú množinu formúl jazyka $\mathcal{L}$ budeme nazývať *teóriou* v jazyku $\mathcal{L}$.

Príklad 2.27.

$$\begin{aligned} T_{\text{party}} = \{&((\text{príde}(\text{Kim}) \lor \text{príde}(\text{Jim})) \lor \text{príde}(\text{Sarah})),\\ &(\text{príde}(\text{Kim}) \to \neg\text{príde}(\text{Sarah})),\\ &(\text{príde}(\text{Jim}) \to \text{príde}(\text{Kim})),\\ &(\text{príde}(\text{Sarah}) \to \text{príde}(\text{Jim}))\} \end{aligned}$$

Modely teórií

Neformálne je *modelom* teórie stav vybranej časti sveta, v ktorom sú všetky tvrdenia v teórii pravdivé.

Pre logiku prvého rádu stavy sveta vyjadrujú štruktúry.

Príklad 2.28 (Model teórie o party).

$$\begin{aligned} &\mathcal{M} = (\{\text{k}, \text{j}, \text{s}, \text{e}, \text{h}\}, i),\\ &i(\text{Kim}) = \text{k}, \qquad i(\text{Jim}) = \text{j}, \qquad i(\text{Sarah}) = \text{s},\\ &i(\text{príde}) = \{\text{k}, \text{j}, \text{e}\}; \end{aligned}$$

$$\left.\begin{aligned} &\mathcal{M} \models ((\text{príde}(\text{Kim}) \lor \text{príde}(\text{Jim})) \lor \text{príde}(\text{Sarah}))\\ &\mathcal{M} \models (\text{príde}(\text{Kim}) \to \neg\text{príde}(\text{Sarah}))\\ &\mathcal{M} \models (\text{príde}(\text{Jim}) \to \text{príde}(\text{Kim}))\\ &\mathcal{M} \models (\text{príde}(\text{Sarah}) \to \text{príde}(\text{Jim})) \end{aligned}\right\} \mathcal{M} \models T_{\text{party}}$$

Model teórie

Definícia 2.29 (Model)**.** Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je teória v jazyku $\mathcal{L}$ a $\mathcal{M}$ je štruktúra pre jazyk $\mathcal{L}$.

Teória T je *pravdivá* v $\mathcal{M}$, skrátene $\mathcal{M} \models T$, vtt *každá* formula X z T je pravdivá v $\mathcal{M}$ (teda $\mathcal{M} \models X$).

Hovoríme tiež, že $\mathcal{M}$ je *modelom* T.

Teória T je *nepravdivá* v $\mathcal{M}$, skrátene $\mathcal{M} \not\models T$, vtt T nie je pravdivá v $\mathcal{M}$.

2.7 Správnosť a vernosť formalizácie

Skúška správnosti formalizácie

Správnou formalizáciou výroku je taká formula, ktorá je pravdivá *za tých istých okolností* ako formalizovaný výrok.

Formuly dokážeme vyhodnocovať iba v štruktúrach.

Preto *za tých istých okolností* znamená *v tých istých štruktúrach*.

Vernosť formalizácie

Výrok „*Nie je pravda, že Jarka a Karol sú doma*" sa dá *správne* formalizovať ako

$$\neg(\mathsf{doma}(\mathsf{Jarka}) \wedge \mathsf{doma}(\mathsf{Karol})),$$

ale rovnako *správna* je aj formalizácia

$$(\neg\mathsf{doma}(\mathsf{Jarka}) \vee \neg\mathsf{doma}(\mathsf{Karol})),$$

lebo je pravdivá v rovnakých štruktúrach.

Pri formalizácii sa snažíme o správnosť, ale zároveň *uprednostňujeme* formalizácie, ktoré *vernejšie* zachytávajú štruktúru výroku.

Zvyšuje to pravdepodobnosť, že sme neurobili chybu, a uľahčuje hľadanie chýb.

Prvá formalizácia je vernejšia ako druhá, a preto ju uprednostníme.

Znalosti na pozadí

Na praktických cvičeniach ste sa stretli so *znalosťami na pozadí* (background knowledge): vzájomná výlučnosť vlastností *je Nemec* a *je Rus*, ktorá v úlohe nebola explicitne uvedená.

Uprednostňujeme ich vyjadrovanie *samostatnými formulami*.

Rovnaké dôvody ako pre vernosť.

Skutočné súčasti významu a konverzačné implikatúry

Niektoré tvrdenia *vyznievajú* silnejšie, ako naozaj sú:

- „*Prílohou sú zemiaky* alebo *šalát*" môže niekomu znieť ako exkluzívna disjunkcia.
- „*Prejdete, ak všetky úlohy vyriešite na 100 %*" znie mnohým ako ekvivalencia.

Skutočnú časť významu tvrdenia *nemôžeme poprieť* v dodatku k pôvodnému tvrdeniu bez sporu s ním.

- Keď k tvrdeniu *„Karol a Jarka sú doma“* dodáme *„Ale Karol nie je doma,“* dostaneme sa do sporu.

  Takže *„Karol je doma“* je skutočne časťou významu pôvodného výroku.

Skutočné súčasti významu a konverzačné implikatúry

Časť významu tvrdenia, ktorú *môžeme poprieť* dodatkami bez sporu s pôvodným tvrdením, sa nazýva *konverzačná implikatúra* (H. P. Grice). *Nie je skutočnou časťou významu* pôvodného tvrdenia.

- Prílohou sú zemiaky alebo šalát. *Ale môžete si (pol na pol alebo za príplatok) dať aj oboje.*

  Dodatok popiera exkluzívnosť, ale nie je v spore s tvrdením. Takže exkluzívnosť nie je súčasťou významu základného tvrdenia, je to iba konverzačná implikatúra.

- Prejdete, ak všetky úlohy vyriešite na 100 %. *Ale nemusíte mať všetko na 100 %, aby ste prešli.*

  Dodatok popiera implikáciu *„Prejdete,* iba ak *všetky úlohy vyriešite na 100 %,“* ale nie je v spore s pôvodným tvrdením. Táto implikácia teda nie je skutočne časťou významu základného tvrdenia, je to len konverzačná implikatúra.

3. prednáška

Výrokovologické vyplývanie

Rekapitulácia

Minulý týždeň sme hovorili o tom,

- čo sú výrokovologické spojky,
- ako zodpovedajú slovenským spojkám,
- čo sú symboly jazyka výrokovologickej časti logiky prvého rádu,
- čo sú formuly tohto jazyka,
- kedy sú formuly pravdivé v danej štruktúre.
- čo je výrokovologická teória a jej model.

3 Výrokovologické vyplývanie

Logické dôsledky

Na 1. prednáške:

- Hovorili sme o tom, že logiku zaujíma, čo a prečo sú zákonitosti správneho usudzovania.
- Správne úsudky odvodzujú z predpokladov (teórií) závery, ktoré sú ich logickými dôsledkami.
- *Logickými dôsledkami* teórie sú tvrdenia, ktoré sú pravdivé vo *všetkých modeloch* teórie.

Minulý týždeň sme začali pracovať s *výrokovologickou* časťou logiky prvého rádu.

Už vieme, čo sú v nej teórie a modely.

Čo sú logické dôsledky?

3.1 Výrokovologické ohodnotenia

Nekonečne veľa štruktúr

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

$$\begin{aligned} T_{\text{party}} = \{&((\text{príde}(\text{Kim}) \lor \text{príde}(\text{Jim})) \lor \text{príde}(\text{Sarah})),\\ &(\text{príde}(\text{Kim}) \to \neg\text{príde}(\text{Sarah})),\\ &(\text{príde}(\text{Jim}) \to \text{príde}(\text{Kim})),\\ &(\text{príde}(\text{Sarah}) \to \text{príde}(\text{Jim}))\} \end{aligned}$$

Ale štruktúr je nekonečne veľa a ak má teória jeden model, má aj nekonečne veľa ďalších:

$$\begin{array}{llll} \mathcal{M}_1 = (\{\text{k}, \text{j}, \text{s}\}, i_1) & \mathcal{M}_1' = (\{\text{k}, \text{j}, \text{s}, 0, 1\}, i_1') & \mathcal{M}_1'' = (\{2, 4, 6\}, i_1'') & \cdots \\ i_1(\text{Kim}) = \text{k} & i_1'(\text{Kim}) = \text{k} & i_1''(\text{Kim}) = 2 & \\ i_1(\text{Jim}) = \text{j} & i_1'(\text{Jim}) = \text{j} & i_1''(\text{Jim}) = 4 & \\ i_1(\text{Sarah}) = \text{s} & i_1'(\text{Sarah}) = \text{s} & i_1''(\text{Sarah}) = 6 & \\ i_1(\text{príde}) = \{\text{k}, \text{j}\} & i_1'(\text{príde}) = \{\text{k}, \text{j}, 1\} & i_1''(\text{príde}) = \{2, 4\} & \end{array}$$

Rozdiely modelov

V čom sa líšia a čo majú spoločné nasledujúce modely T_{party}?

$$\begin{array}{lll} \mathcal{M}_1 = (\{\text{k}, \text{j}, \text{s}, \text{e}, \text{h}\}, i_1) & \mathcal{M}_2 = (\{1, 2, 3\}, i_2) & \mathcal{M}_3 = (\{\text{kj}, \text{s}\}, i_3) \\ i_1(\text{Kim}) = \text{k} & i_2(\text{Kim}) = 1 & i_3(\text{Kim}) = \text{kj} \\ i_1(\text{Jim}) = \text{j} & i_2(\text{Jim}) = 2 & i_3(\text{Jim}) = \text{kj} \\ i_1(\text{Sarah}) = \text{s} & i_2(\text{Sarah}) = 3 & i_3(\text{Sarah}) = \text{s} \\ i_1(\text{príde}) = \{\text{k}, \text{j}, \text{e}\} & i_2(\text{príde}) = \{1, 2\} & i_3(\text{príde}) = \{\text{kj}\} \end{array}$$

Líšia sa doménami aj v interpretáciách.

Líšia sa v pravdivosti rovnostných atómov, napr. Kim $\doteq$ Jim.

Zhodujú sa na pravdivosti *všetkých predikátových* atómov príde(Kim), príde(Jim), príde(Sarah).

V T_{party} *na ničom inom nezáleží.*

Ohodnotenie atómov

Z každej zo štruktúr

$\mathcal{M}_1 = (\{\mathsf{k}, \mathsf{j}, \mathsf{s}, \mathsf{e}, \mathsf{h}\}, i_1)$	$\mathcal{M}_2 = (\{1, 2, 3\}, i_2)$	$\mathcal{M}_3 = (\{\mathsf{kj}, \mathsf{s}\}, i_3)$
$i_1(\mathsf{Kim}) = \mathsf{k}$	$i_2(\mathsf{Kim}) = 1$	$i_3(\mathsf{Kim}) = \mathsf{kj}$
$i_1(\mathsf{Jim}) = \mathsf{j}$	$i_2(\mathsf{Jim}) = 2$	$i_3(\mathsf{Jim}) = \mathsf{kj}$
$i_1(\mathsf{Sarah}) = \mathsf{s}$	$i_2(\mathsf{Sarah}) = 3$	$i_3(\mathsf{Sarah}) = \mathsf{s}$
$i_1(\mathsf{príde}) = \{\mathsf{k}, \mathsf{j}, \mathsf{e}\}$	$i_2(\mathsf{príde}) = \{1, 2\}$	$i_3(\mathsf{príde}) = \{\mathsf{kj}\}$

môžeme skonštruovať to isté *ohodnotenie predikátových atómov*:

$$
\begin{aligned}
v(\mathsf{príde}(\mathsf{Kim})) &= t && \text{lebo } \mathcal{M}_j \models \mathsf{príde}(\mathsf{Kim}),\\
v(\mathsf{príde}(\mathsf{Jim})) &= t && \text{lebo } \mathcal{M}_j \models \mathsf{príde}(\mathsf{Jim}),\\
v(\mathsf{príde}(\mathsf{Sarah})) &= f && \text{lebo } \mathcal{M}_j \not\models \mathsf{príde}(\mathsf{Sarah}).
\end{aligned}
$$

Všetky tieto štruktúry (a nekonečne veľa ďalších) vieme pri vyhodnocovaní formúl jazyka $\mathcal{L}_{\text{party}}$ nahradiť týmto ohodnotením.

Výrokovologické formuly, teórie a ohodnotenia

Definícia 3.1. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.

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

Výrokovologickými formulami jazyka $\mathcal{L}$ nazveme všetky formuly jazyka $\mathcal{L}$, ktoré *neobsahujú symbol rovnosti*. Množinu všetkých výrokovologických formúl jazyka $\mathcal{L}$ označujeme $\mathcal{PE}_{\mathcal{L}}$.

Definícia 3.2. Nech (f, t) je usporiadaná dvojica *pravdivostných hodnôt*, $f \neq t$, kde f predstavuje *nepravdu* a t predstavuje *pravdu*. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.

Výrokovologickým ohodnotením pre $\mathcal{L}$, skrátene *ohodnotením*, nazveme každé zobrazenie $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$.

Pravdivé formuly v ohodnotení

Ako vyhodnotíme, či je formula pravdivá v nejakom ohodnotení?

Definícia 3.3. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech (f, t) sú pravdivostné hodnoty a nech $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ je výrokovologické ohodnotenie pre $\mathcal{L}$. Reláciu *výrokovologická formula A je pravdivá v ohodnotení v* ($v \models_{\mathrm{p}} A$) definujeme *induktívne* pre všetky predikátové atómy a a všetky výrokovologické formuly A, B jazyka $\mathcal{L}$ nasledovne:

- $v \models_{\mathrm{p}} a$ vtt $v(a) = t$,
- $v \models_{\mathrm{p}} \neg A$ vtt $v \not\models_{\mathrm{p}} A$,
- $v \models_{\mathrm{p}} (A \land B)$ vtt $v \models_{\mathrm{p}} A$ a zároveň $v \models_{\mathrm{p}} B$,
- $v \models_{\mathrm{p}} (A \lor B)$ vtt $v \models_{\mathrm{p}} A$ alebo $v \models_{\mathrm{p}} B$,
- $v \models_{\mathrm{p}} (A \to B)$ vtt $v \not\models_{\mathrm{p}} A$ alebo $v \models_{\mathrm{p}} B$,

kde *vtt* skracuje *vtedy a len vtedy* a $v \not\models_{\mathrm{p}} A$ skracuje *A nie je pravdivá vo v*.

Vyhodnotenie formuly v ohodnotení

Príklad 3.4. Vyhodnoťme formulu

$$X = ((\text{príde(Jim)} \lor \neg\text{príde(Kim)}) \to \text{príde(Sarah)})$$

vo výrokovologickom ohodnotení

$$v = \{\text{príde(Kim)} \mapsto t,\ \text{príde(Jim)} \mapsto t,\ \text{príde(Sarah)} \mapsto f\}$$

zdola nahor:

	p(Kim)	p(Jim)	p(Sarah)	¬p(Kim)	(p(Jim) ∨ ¬p(Kim))	X
v	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$

príde sme skrátili na p.

Ohodnotenie zhodné so štruktúrou

Definícia 3.5. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech (f, t) sú pravdivostné hodnoty, $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ je výrokovologické ohodnotenie pre $\mathcal{L}$ a $S \subseteq \mathcal{PA}_{\mathcal{L}}$ je množina predikátových atómov.

Ohodnotenie v a štruktúra $\mathcal{M}$ sú navzájom *zhodné na S* vtt pre každý predikátový atóm $A \in S$ platí

$$v(A) = t \text{ vtt } \mathcal{M} \models A.$$

Ohodnotenie v a štruktúra $\mathcal{M}$ sú navzájom *zhodné* vtt sú zhodné na $\mathcal{PA}_{\mathcal{L}}$.

Konštrukcia ohodnotenia zhodného so štruktúrou

Ohodnotenie zhodné so štruktúrou zostrojíme ľahko:

Tvrdenie 3.6. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a (f, t) sú pravdivostné hodnoty. Zobrazenie $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ definované pre každý atóm $A \in \mathcal{PA}_{\mathcal{L}}$ nasledovne:*

$$v(A) = \begin{cases} t, & \text{ak } \mathcal{M} \models A, \\ f, & \text{ak } \mathcal{M} \not\models A \end{cases}$$

je výrokovologické ohodnotenie zhodné s $\mathcal{M}$.

Dôkaz. Pre každý atóm $A \in \mathcal{PA}_{\mathcal{L}}$ musíme dokázať, že $v(A) = t$ vtt $\mathcal{M} \models A$:

($\Leftarrow$) Priamo: Ak $\mathcal{M} \models A$, tak $v(A) = t$ podľa jeho definície v leme.

($\Rightarrow$) Nepriamo: Ak $\mathcal{M} \not\models A$, tak $v(A) = f$ podľa jeho definície v leme, a pretože $t \neq f$, tak $v(A) \neq t$. □

Dokážeme zostrojiť aj štruktúru z ohodnotenia, aby boli zhodné?

Príklad 3.7 (Konštrukcia štruktúry zhodnej s ohodnotením). Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, kde $\mathcal{C}_{\mathcal{L}} = \{\mathsf{Kim}, \mathsf{Jim}, \mathsf{Sarah}\}$ a $\mathcal{P}_{\mathcal{L}} = \{\mathsf{príde}\}$.

Nech v je výrokovologické ohodnotenie pre $\mathcal{L}$, kde

$$v(\mathsf{príde}(\mathsf{Kim})) = t \qquad v(\mathsf{príde}(\mathsf{Jim})) = t \qquad v(\mathsf{príde}(\mathsf{Sarah})) = f$$

Zostrojme štruktúru pre $\mathcal{L}$ zhodnú s v.

Možnosťou, ktorú ľahko zovšeobecníme na všetky jazyky, je použiť ako doménu množinu konštánt:

$$\mathcal{M} = (\underbrace{\{\mathsf{Kim}, \mathsf{Jim}, \mathsf{Sarah}\}}_{\mathcal{C}_{\mathcal{L}}}, i)$$

Každú konštantu interpretujeme ňou samou:

$$i(\text{Kim}) = \text{Kim} \qquad i(\text{Jim}) = \text{Jim} \qquad i(\text{Sarah}) = \text{Sarah}$$

predikát príde ako množinu tých c, pre ktoré $v(\text{príde}(c)) = t$:

$$i(\text{príde}) = \{\text{Kim}, \text{Jim}\}$$

Konštrukcia štruktúry zhodnej s ohodnotením

Ako zostrojíme štruktúru zhodnú s ohodnotením pre hocijaký jazyk?

Tvrdenie 3.8. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech (f, t) sú pravdivostné hodnoty a $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ je výrokovologické ohodnotenie pre $\mathcal{L}$.*

Nech $\mathcal{M} = (D, i)$ je štruktúra pre $\mathcal{L}$ s doménou $D = \mathcal{C}_{\mathcal{L}}$ a interpretačnou funkciou definovanou pre všetky $n > 0$, všetky konštanty c a všetky predikátové symboly $P \in \mathcal{P}_{\mathcal{L}}$ s aritou n takto:

$$\begin{aligned} i(c) &= c \\ i(P) &= \{\, (c_1, \dots, c_n) \in \mathcal{C}_{\mathcal{L}}^n \mid v(P(c_1, \dots, c_n)) = t \,\} \end{aligned}$$

Potom $\mathcal{M}$ je zhodná s v.

Štruktúram zo syntaktického materiálu sa hovorí *herbrandovské*.
Zhoda ohodnotenia a štruktúry je definované iba na *atómoch*.
Ako sa správajú na *zložitejších* formulách?

Zhoda na *všetkých* výrokovologických formulách

Tvrdenie 3.9. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a v je výrokovologické ohodnotenie pre $\mathcal{L}$ zhodné s $\mathcal{M}$. Potom pre každú výrokovologickú formulu $X \in \mathcal{PE}_{\mathcal{L}}$ platí, že $v \models_{\mathrm{p}} X$ vtt $\mathcal{M} \models X$.*

Dôkaz indukciou na konštrukciu formuly. 1.1: Nech X je rovnostný atóm. Potom nie je výrokovologickou formulou a tvrdenie preň triviálne platí.

1.2: Nech X je predikátový atóm. Potom $v \models_{\mathrm{p}} X$ vtt $v(X) = t$ vtt $\mathcal{M} \models X$.

2.1: Indukčný predpoklad: Nech tvrdenie platí pre formulu X. Dokážme tvrdenie pre $\neg X$. Ak X neobsahuje symbol rovnosti $\doteq$, potom $v \models_{\mathrm{p}} \neg X$ vtt $v \not\models_{\mathrm{p}} X$ vtt (podľa IP) $\mathcal{M} \not\models X$ vtt $\mathcal{M} \models \neg X$. Ak X obsahuje $\doteq$, $\neg X$ ho obsahuje tiež, teda nie je výrokovologická a tvrdenie pre ňu platí triviálne.

2.2: IP: Nech tvrdenie platí pre formuly X a Y. Dokážme ho pre $(X \land Y)$, $(X \lor Y)$, $(X \to Y)$. Ak X alebo Y obsahuje $\doteq$, tvrdenie platí pre $(X \land Y)$, $(X \lor Y)$, $(X \to Y)$ triviálne, lebo nie sú výrokovologické.

Nech teda X ani Y neobsahuje $\doteq$. Potom platí $v \models_{\mathrm{p}} (X \to Y)$ vtt $v \not\models_{\mathrm{p}} X$ alebo $v \models_{\mathrm{p}} Y$ vtt (podľa IP) vtt $\mathcal{M} \not\models X$ alebo $\mathcal{M} \models Y$ vtt $\mathcal{M} \models (X \to Y)$.

Ďalej $v \models_{\mathrm{p}} (X \land Y)$ vtt $v \models_{\mathrm{p}} X$ a $v \models_{\mathrm{p}} Y$ vtt (podľa IP) vtt $\mathcal{M} \models X$ a $\mathcal{M} \models Y$ vtt $\mathcal{M} \models (X \land Y)$.

Nakoniec $v \models_{\mathrm{p}} (X \lor Y)$ vtt $v \models_{\mathrm{p}} X$ alebo $v \models_{\mathrm{p}} Y$ vtt (podľa IP) vtt $\mathcal{M} \models X$ alebo $\mathcal{M} \models Y$ vtt $\mathcal{M} \models (X \lor Y)$. □

3.2 Výrokovologické teórie a modely

Výrokovologické teórie

Vráťme sa naspäť k teóriám, modelom a vyplývaniu.

Definícia 3.10. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Každú množinu výrokovologických formúl jazyka $\mathcal{L}$ budeme nazývať *výrokovologickou teóriou* v jazyku $\mathcal{L}$.

Príklad 3.11. Výrokovologickou teóriou je

$$\begin{aligned} T_{\text{party}} = \{&((\mathsf{príde}(\mathsf{Kim}) \lor \mathsf{príde}(\mathsf{Jim})) \lor \mathsf{príde}(\mathsf{Sarah})),\\ &(\mathsf{príde}(\mathsf{Kim}) \to \neg\mathsf{príde}(\mathsf{Sarah})),\\ &(\mathsf{príde}(\mathsf{Jim}) \to \mathsf{príde}(\mathsf{Kim})),\\ &(\mathsf{príde}(\mathsf{Sarah}) \to \mathsf{príde}(\mathsf{Jim}))\}, \end{aligned}$$

ale nie

$$T_{\text{party}} \cup \{\mathsf{Kim} \doteq \mathsf{Sarah}\}.$$

Príklad výrokovologického modelu

Príklad 3.12 (Výrokovologický model teórie o party).

$$v = \{\text{príde}(\text{Kim}) \mapsto t, \text{príde}(\text{Jim}) \mapsto t, \text{príde}(\text{Sarah}) \mapsto f\}$$

$$\left.\begin{aligned} v &\models_{\mathrm{p}} ((\text{príde}(\text{Kim}) \lor \text{príde}(\text{Jim})) \lor \text{príde}(\text{Sarah})) \\ v &\models_{\mathrm{p}} (\text{príde}(\text{Kim}) \to \neg\text{príde}(\text{Sarah})) \\ v &\models_{\mathrm{p}} (\text{príde}(\text{Jim}) \to \text{príde}(\text{Kim})) \\ v &\models_{\mathrm{p}} (\text{príde}(\text{Sarah}) \to \text{príde}(\text{Jim})) \end{aligned}\right\} v \models_{\mathrm{p}} T_{\text{party}}$$

Výrokovologický model

Definícia 3.13 (Výrokovologický model)**.** Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je teória v jazyku $\mathcal{L}$ a v je výrokovologické ohodnotenie pre jazyk $\mathcal{L}$.

Teória T je *pravdivá* v ohodnotení v, skrátene $v \models_{\mathrm{p}} T$, vtt *každá* formula X z T je pravdivá vo v (teda $v \models_{\mathrm{p}} X$ pre každú $X \in T$).

Hovoríme tiež, že v je *výrokovologickým modelom* T.

Teória T je *nepravdivá* vo v, skrátene $v \not\models_{\mathrm{p}} T$, vtt T nie je pravdivá vo v.

Zrejme $v \not\models_{\mathrm{p}} T$ vtt $v \not\models_{\mathrm{p}} X$ pre *nejakú* $X \in T$.

Model teórie, splniteľnosť a nesplniteľnosť

Definícia 3.14 (Splniteľnosť a nesplniteľnosť)**.** Teória je *výrokovologicky splniteľná* vtt má aspoň jeden výrokovologický model.

Teória je *výrokovologicky nesplniteľná* vtt nemá žiaden výrokovologický model.

Zrejme teória nie je splniteľná vtt keď je nesplniteľná.

Príklad 3.15. T_{party} je evidentne splniteľná.

3.3 Vyplývanie, nezávislosť a nesplniteľnosť

Výrokovologické vyplývanie

Ak sú množiny konštánt a predikátových symbolov jazyka konečné, jazyk má konečne veľa predikátových atómov a teda aj *konečne veľa* ohodnotení.

Uvažovať o všetkých ohodnoteniach a modeloch teórie nie je také odstrašujúce. Napríklad si ľahšie predstavíme logický dôsledok:

Definícia 3.16. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X je *výrokovologickým dôsledkom* teórie T vtt pre každé ohodnotenie v pre jazyk $\mathcal{L}$ platí, že ak $v \models_p T$, tak $v \models_p X$.

Hovoríme tiež, že X *vyplýva* z T a píšeme $T \models_p X$.

Ak X *ne*vyplýva z T, píšeme $T \not\models_p X$.

Príklad výrokovologického vyplývania

Príklad 3.17. Vyplýva príde(Kim) výrokovologicky z T_{party}? Pretože vieme vymenovať všetky ohodnotenia pre $\mathcal{L}_{\text{party}}$, zistíme to ľahko:

	v_i			((p(K) ∨ p(J)) ∨ p(S))	(p(K) → ¬p(S))	(p(J) → p(K))	(p(S) → p(J))	T_{party}	p(K)
	p(K)	p(J)	p(S)						
v_0	f	f	f	$\not\models_p$				$\not\models_p$	
v_1	f	f	t	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	
v_2	f	t	f	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
v_3	f	t	t	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
v_4	t	f	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$
v_5	t	f	t	$\models_p$	$\not\models_p$			$\not\models_p$	
v_6	t	t	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$
v_7	t	t	t	$\models_p$	$\not\models_p$			$\not\models_p$	

Skrátili sme príde na p, Kim na K, Jim na J, Sarah na S.

Logický záver: Formula príde(Kim) výrokovologicky vyplýva z T_{party}.

Praktický záver: Aby boli všetky požiadavky splnené, Kim *musí* prísť na párty.

Príklad nezávislosti

Príklad 3.18. Vyplýva príde(Jim) výrokovologicky z T_{party}?

	v_i			((p(K) ∨ p(J)) ∨ p(S))	(p(K) → ¬p(S))	(p(J) → p(K))	(p(S) → p(J))	T_{party}	p(J)
	p(K)	p(J)	p(S)						
v_0	f	f	f	$\not\models_{\text{p}}$				$\not\models_{\text{p}}$	
v_1	f	f	t	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\not\models_{\text{p}}$	$\not\models_{\text{p}}$	
v_2	f	t	f	$\models_{\text{p}}$	$\models_{\text{p}}$	$\not\models_{\text{p}}$		$\not\models_{\text{p}}$	
v_3	f	t	t	$\models_{\text{p}}$	$\models_{\text{p}}$	$\not\models_{\text{p}}$		$\not\models_{\text{p}}$	
v_4	t	f	f	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\not\models_{\text{p}}$
v_5	t	f	t	$\models_{\text{p}}$	$\not\models_{\text{p}}$			$\not\models_{\text{p}}$	
v_6	t	t	f	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$	$\models_{\text{p}}$
v_7	t	t	t	$\models_{\text{p}}$	$\not\models_{\text{p}}$			$\not\models_{\text{p}}$	

Logický záver: Formula príde(Jim) *nevyplýva* z T_{party}.

Výrokovologická nezávislosť

Vzťahu medzi príde(Jim) a T_{party} hovoríme *nezávislosť*.

Definícia 3.19. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X je *výrokovologicky nezávislá* od teórie T vtt existujú také ohodnotenia v_0 a v_1 pre jazyk $\mathcal{L}$, že $v_0 \models_{\text{p}} T$ aj $v_1 \models_{\text{p}} T$, ale $v_0 \not\models_{\text{p}} X$ a $v_1 \models_{\text{p}} X$.

Príklad 3.20 (pokračovanie príkladu 3.18). *Logický záver:* Formula príde(Jim) je *nezávislá* od T_{party}.

Praktický záver: Všetky požiadavky budú naplnené *bez ohľadu na to*, či Jim príde alebo nepríde na párty. *Nie je nutné*, aby bol prítomý ani aby bol neprítomý. *Môže, ale nemusí* prísť. Jeho prítomnosť od požiadaviek *nezávisí*.

Príklad vyplývania negácie

Príklad 3.21. Je príde(Sarah) výrokovologickým dôsledkom T_{party} alebo nezávislá od T_{party}?

	v_i			$((\mathsf{p}(\mathsf{K}) \lor \mathsf{p}(\mathsf{J}))$	$(\mathsf{p}(\mathsf{K}) \to$	$(\mathsf{p}(\mathsf{J}) \to$	$(\mathsf{p}(\mathsf{S}) \to$		
	p(K)	p(J)	p(S)	$\lor\, \mathsf{p}(\mathsf{S}))$	$\neg \mathsf{p}(\mathsf{S}))$	$\mathsf{p}(\mathsf{K}))$	$\mathsf{p}(\mathsf{J}))$	T_{party}	p(S)
v_0	f	f	f	$\not\models_{\mathrm{p}}$				$\not\models_{\mathrm{p}}$	
v_1	f	f	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	
v_2	f	t	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$		$\not\models_{\mathrm{p}}$	
v_3	f	t	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$		$\not\models_{\mathrm{p}}$	
v_4	t	f	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_5	t	f	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$	
v_6	t	t	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_7	t	t	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$	

Logický záver: Formula príde(Sarah) *nevyplýva* z T_{party}, ale ani *nie je nezávislá* od T_{party}.

Vyplývanie negácie

Tvrdenie 3.22. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je splniteľná výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.*

Formula X nevyplýva z teórie T a nie je výrokovologicky nezávislá od T vtt $\neg X$ vyplýva z T.

Príklad 3.23 (pokračovanie príkladu 3.21). *Logický záver:* Z T_{party} vyplýva ¬príde(Sarah).

Praktický záver: Aby boli všetky požiadavky naplnené, Sarah *nesmie* prísť na party.

Vzťahy teórií a formúl

Medzi *ohodnotením a formulou* sú iba *dva vzájomne výlučné* vzťahy:

$$\text{Buď } v \models_{\mathrm{p}} X, \text{ alebo } v \not\models_{\mathrm{p}} X.$$

Medzi *teóriou a formulou* je *viac* možných vzťahov:

	existuje v také, že $v \models_{\mathrm{p}} T$ a $v \models_{\mathrm{p}} X$	pre všetky v, ak $v \models_{\mathrm{p}} T$, tak $v \not\models_{\mathrm{p}} X$
existuje v také, že $v \models_{\mathrm{p}} T$ a $v \not\models_{\mathrm{p}} X$	X je nezávislá od T $T \not\models_{\mathrm{p}} X$ a $T \not\models_{\mathrm{p}} \neg X$	$T \models_{\mathrm{p}} \neg X$ a $T \not\models_{\mathrm{p}} X$
pre všetky v, ak $v \models_{\mathrm{p}} T$, tak $v \models_{\mathrm{p}} X$	$T \models_{\mathrm{p}} X$ a $T \not\models_{\mathrm{p}} \neg X$	T je *nesplniteľná* $T \models_{\mathrm{p}} X$ aj $T \models_{\mathrm{p}} \neg X$

Nesplniteľná teória

Príklad 3.24. Je teória $T'_{\text{party}} = T_{\text{party}} \cup \{(\neg\text{príde(Sarah)} \to \neg\text{príde(Kim)})\}$ splniteľná?

	v_i			((p(K) ∨ p(J)) ∨ p(S))	(p(K) → ¬p(S))	(p(J) → p(K))	(p(S) → p(J))	(¬p(S) → ¬p(K))	
	p(K)	p(J)	p(S)						T'_{party}
v_0	*f*	*f*	*f*	$\not\models_{\mathrm{p}}$					$\not\models_{\mathrm{p}}$
v_1	*f*	*f*	*t*	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$		$\not\models_{\mathrm{p}}$
v_2	*f*	*t*	*f*	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$
v_3	*f*	*t*	*t*	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$
v_4	*t*	*f*	*f*	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_5	*t*	*f*	*t*	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$				$\not\models_{\mathrm{p}}$
v_6	*t*	*t*	*f*	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_7	*t*	*t*	*t*	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$				$\not\models_{\mathrm{p}}$

Logický záver: T'_{party} je nesplniteľná, vyplýva z nej každá formula.

Praktický záver: T'_{party} *nemá* praktické dôsledky, lebo *nevypovedá o žiadnom stave sveta*. Na jej základe *nevieme rozhodnúť*, kto musí alebo nesmie prísť na párty.

Vyplývanie a nesplniteľnosť

Nesplniteľnosť ale nie neužitočná vlastnosť.

Tvrdenie 3.25. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je splniteľná výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.*

Formula X výrokovologicky vyplýva z teórie T vtt $T \cup \{\neg X\}$ je výrokovologicky nesplniteľná.

Podľa tohto tvrdenia sa rozhodnutie vyplývania dá *zredukovať* na rozhodnutie splniteľnosti.

Výrokovologickú splniteľnosť rozhoduje SAT solver.

Množina atómov formuly a teórie

Definícia 3.26. *Množinu atómov* $\mathrm{atoms}(X)$ formuly $X \in \mathcal{E}_{\mathcal{L}}$ definujeme pre všetky formuly $A, B \in \mathcal{E}_{\mathcal{L}}$ nasledovne:

- $\mathrm{atoms}(A) = \{A\}$, ak A je atóm,
- $\mathrm{atoms}(\neg A) = \mathrm{atoms}(A)$,
- $\mathrm{atoms}((A \wedge B)) = \mathrm{atoms}((A \vee B)) = \mathrm{atoms}((A \to B)) = \mathrm{atoms}(A) \cup \mathrm{atoms}(B)$.

Množinou atómov teórie T je

$$\mathrm{atoms}(T) = \bigcup_{X \in T} \mathrm{atoms}(X).$$

Ohodnotenia zhodné na atómoch teórie

Definícia 3.27. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $M \subseteq \mathcal{PA}_{\mathcal{L}}$. Ohodnotenia v_1 a v_2 sa *zhodujú* na množine M vtt $v_1(A) = v_2(A)$ pre každý atóm $A \in M$.

Tvrdenie 3.28. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Pre každú výrokovologickú teóriu T a formulu X jazyka $\mathcal{L}$ a všetky ohodnotenia v_1 a v_2, ktoré zhodujú na množine* $\mathrm{atoms}(T) \cup \mathrm{atoms}(X)$ *platí*

- $v_1 \models_{\mathrm{p}} T$ *vtt* $v_2 \models_{\mathrm{p}} T$,
- $v_1 \models_{\mathrm{p}} X$ *vtt* $v_2 \models_{\mathrm{p}} X$.

Ohodnotenia postačujúce na skúmanie teórií

Inak povedané: Pravdivosť formuly/teórie v ohodnotení závisí *iba* od pravdivostných hodnôt tých atómov, ktoré sa v nej vyskytujú.

Takže na zistenie vyplývania, nezávislosti, splniteľnosti stačí preskúmať všetky ohodnotenia, ktoré sa *líšia* na atómoch *vyskytujúcich* sa vo formule a teórii.

Pokiaľ je teória je konečná, stačí skúmať konečne veľa ohodnotení, aj keby bol jazyk nekonečný.

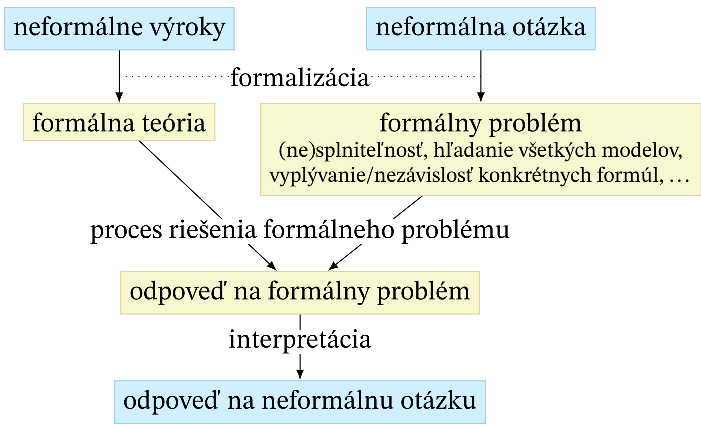
Rekapitulácia

Rekapitulácia

Dnes sme sa naučili:

- ako zjednodušiť štruktúry na výrokovologické ohodnotenia,
- čo je logické vyplývanie z teórie a logický dôsledok teórie,
- čo je nezávislosť formuly od teórie,
- štyri situácie vo vzťahoch teórií a formúl a ich praktické dôsledky,
- čo sú splniteľné a nesplniteľné teórie,
- ako súvisí nesplniteľnosť a vyplývanie.

Schéma riešenia problémov pomocou logiky



4. prednáška

Vlastnosti a vzťahy výrokovologických formúl

Rekapitulácia

Minulý týždeň sme:

- *zjednodušili* pohľad na možné stavy sveta zo štruktúr na *výrokovologické* ohodnotenia,
- zistili sme, že na zistenie vyplývania/logických dôsledkov stačí pre konečné teórie skúmať konečne veľa ohodnotení, ktoré zastúpia nekonečne veľa štruktúr,
- presne sme zadefinovali vzťahy medzi teóriou a formulou z hľadiska ohodnotení:
  - výrokovologické vyplývanie,
  - výrokovologickú nezávislosť.

4 Vlastnosti a vzťahy výrokovologických formúl

4.1 Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly

Logické dôsledky prázdnej teórie

Tvrdenie vyplýva z nejakej teórie (je jej logickým dôsledkom), keď je pravdivé v každom modeli teórie, teda v každom stave sveta, v ktorom sú pravdivé všetky tvrdenia teórie.

Čo keď je teória *prázdna*?

- Je pravdivá v *každom* stave sveta.
- Jej logické dôsledky sú teda *tiež* pravdivé v každom stave sveta.

Navyše:

- Každý model hocijakej neprázdnej teórie T je aj modelom prázdnej teórie.
- Logické dôsledky prázdnej teórie sú v ňom pravdivé.
- Preto sú aj logickými dôsledkami T.

Logické dôsledky prázdnej teórie sú teda dôsledkami *všetkých* teórií.

Príklady logických dôsledkov prázdnej teórie

Existujú vôbec logické dôsledky prázdnej teórie?
Áno, napríklad:

- pre každú konštantu c je pravdivé tvrdenie $c \doteq c$;
- pre každý atóm A je pravdivé $(A \lor \neg A)$.

Pretože sú pravdivé bez ohľadu na teóriu a sú pravdivé v každom stave sveta, sú *logickými pravdami* a sú *nutne* pravdivé.

Rozpoznateľné logické pravdy

Jazyk a spôsob pohľadu na stavy sveta ovplyvňuje, ktoré logické pravdy dokážeme rozpoznať:

- $c \doteq c$ aj $(A \lor \neg A)$ sú pravdivé v každej štruktúre.
- Výrokovologické ohodnotenia sa nezaoberajú rovnostnými atómami. Pomocou nich nezistíme, že $c \doteq c$ je nutne pravda. Ale zistíme, že $(A \lor \neg A)$ pre každý *predikátový* atóm A je pravdivé v každom ohodnotení, a teda je nutne pravdou.

Logickým pravdám, ktorých nutnú pravdivosť dokážeme určiť rozborom všetkých výrokovologických ohodnotení, hovoríme *tautológie*.

Príklad tautológie

Príklad 4.1 (Peirceov zákon). Majme jazyk $\mathcal{L}$ s $\mathcal{C}_{\mathcal{L}} = \{\mathsf{a}, \mathsf{b}\}$, $\mathcal{P}_{\mathcal{L}} = \{\mathsf{p}^1\}$. Je formula $X = \big(\big((\mathsf{p}(\mathsf{a}) \to \mathsf{p}(\mathsf{b})) \to \mathsf{p}(\mathsf{a})\big) \to \mathsf{p}(\mathsf{a})\big)$ tautológiou?

Označme $A = \mathsf{p}(\mathsf{a})$ a $B = \mathsf{p}(\mathsf{b})$, teda $X = \big(\big((A \to B) \to A\big) \to A\big)$ a preskúmajme všetky výrokovologické ohodnotenia týchto atómov:

	v_i				X
	A	B	$(A \to B)$	$\big((A \to B) \to A\big)$	$\big(\big((A \to B) \to A\big) \to A\big)$
v_0	f	f	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_1	f	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_2	t	f	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_3	t	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$

Pretože X je pravdivá vo všetkých ohodnoteniach pre $\mathcal{L}$, X je tautológiou.

Tautológia

Definícia 4.2. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X je výrokovologická formula. Formulu X nazveme *tautológiou* (skrátene $\models_{\mathrm{p}} X$) vtt X je *pravdivá* v *každom* výrokovologickom ohodnotení v pre $\mathcal{L}$ (teda *pre každé* výrokovologické ohodnotenie v pre $\mathcal{L}$ platí $v \models_{\mathrm{p}} X$).

Definícia vyžaduje preveriť všetky možné ohodnotenia pre $\mathcal{L}$, teda ohodnotenia *všetkých predikátových atómov jazyka $\mathcal{L}$*. Ale…

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\models_{\mathrm{p}}$
v_1	f	f	$\cdots$	$\models_{\mathrm{p}}$
		$\cdots$		
v_k	t	f	$\cdots$	$\models_{\mathrm{p}}$
		$\cdots$		

Postačujúca podmienka pre tautológiu

Na konci minulej prednášky sme spomenuli, že platí:

Tvrdenie 4.3. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X je výrokovologická formula jazyka $\mathcal{L}$. Pre všetky ohodnotenia v_1 a v_2, ktoré zhodujú na množine* $\mathrm{atoms}(X)$*, platí $v_1 \models_{\mathrm{p}} X$ vtt $v_2 \models_{\mathrm{p}} X$.*

Na zistenie, či formula je tautológia, teda stačí teda preverovať ohodnotenia atómov *vyskytujúcich* sa vo formule:

Dôsledok 4.4. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X je výrokovologická formula jazyka $\mathcal{L}$. Formula X je tautológiou vtt X je pravdivá v každom výrokovologickom ohodnotení $v : \operatorname{atoms}(X) \to \{f, t\}$.*

Dôkaz tvrdenia 4.3. Tvrdenie dokážeme indukciou na konštrukciu formuly:

1.1. Ak X je rovnostný atóm, nie je výrokovologickou formulou a tvrdenie preň platí triviálne.

1.2. Nech X je predikátový atóm. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na $\operatorname{atoms}(X)$, teda na samotnom X. Podľa definície pravdivosti platí $v_1 \models_p X$ vtt $v_1(X) = t$ vtt $v_2(X) = t$ vtt $v_2 \models_p X$.

2.1 Indukčný predpoklad (IP): Predpokladajme, že tvrdenie platí pre formulu X. Dokážme ho pre $\neg X$. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na $\operatorname{atoms}(\neg X)$. Pretože $\operatorname{atoms}(\neg X) = \operatorname{atoms}(X)$, v_1 a v_2 sa zhodujú na $\operatorname{atoms}(X)$, a teda podľa IP $v_1 \models_p X$ vtt $v_2 \models_p X$. Preto $v_1 \models_p \neg X$ vtt (def. $\models_p$) $v_1 \not\models_p X$ vtt (IP) $v_2 \not\models_p X$ vtt (def. $\models_p$) $v_2 \models_p \neg X$.

2.2 Indukčný predpoklad (IP): Predpokladajme, že tvrdenie platí pre formuly X a Y. Dokážme ho pre $(X \land Y)$. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na $\operatorname{atoms}((X \land Y))$. Pretože $\operatorname{atoms}((X \land Y)) = \operatorname{atoms}(X) \cup \operatorname{atoms}(Y)$, v_1 a v_2 sa zhodujú na $\operatorname{atoms}(X)$, a teda podľa IP $v_1 \models_p X$ vtt $v_2 \models_p X$; tiež sa zhodujú na $\operatorname{atoms}(Y)$, a teda podľa IP $v_1 \models_p Y$ vtt $v_2 \models_p Y$. Preto $v_1 \models_p (X \land Y)$ vtt (def. $\models_p$) $v_1 \models_p X$ a $v_1 \models_p Y$ vtt (IP) $v_2 \models_p X$ a $v_2 \models_p Y$ vtt (def. $\models_p$) $v_2 \models_p (X \land Y)$.

Podobne postupujeme pre ďalšie binárne spojky. □

Tautológie a vyplývanie

Tvrdenie 4.5 (Tautológie, vyplývanie a jeho monotónnosť)**.** *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech A je výrokovologická formula v $\mathcal{L}$. Nech T_1 a T_2 sú výrokovologické teórie v $\mathcal{L}$. Potom:*

a) $\models_p A$ (A je tautológia) vtt $\emptyset \models_p A$ (A vyplýva z prázdnej teórie).

b) $T_1 \models_p A$ a $T_1 \subseteq T_2$, tak $T_2 \models_p A$.

c) $\models_p A$ vtt pre každú teóriu T v $\mathcal{L}$, $T \models_p A$.

Splniteľnosť

Kým tautológie sú *nutne* pravdivé, teda pravdivé vo *všetkých* ohodnoteniach, mnohé formuly iba *môžu* byť pravdivé, teda sú pravdivé v *niektorých* ohodnoteniach.

Nazývame ich *splniteľné*.

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\nvDash_{\mathrm{p}}$
v_1	f	f	$\cdots$	$\nvDash_{\mathrm{p}}$
		$\cdots$		
v_k	t	f	$\cdots$	$\vDash_{\mathrm{p}}$
		$\cdots$		

Definícia 4.6. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X je výrokovologická formula. Formulu X nazveme *splniteľnou* vtt X je *pravdivá* v *nejakom* výrokovologickom ohodnotení pre $\mathcal{L}$ (teda *existuje* také výrokovologické ohodnotenie v pre $\mathcal{L}$, že $v \vDash_{\mathrm{p}} X$).

Falzifikovateľnosť

Na rozdiel od tautológií, ktoré sú *nutne* pravdivé, a teda *nemôžu* byť *ne*pravdivé, mnohé formuly *môžu* byť *ne*pravdivé, teda sú *ne*pravdivé v *niektorých* ohodnoteniach.

Nazývame ich *falzifikovateľné*.

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\vDash_{\mathrm{p}}$
v_1	f	f	$\cdots$	$\vDash_{\mathrm{p}}$
		$\cdots$		
v_k	t	f	$\cdots$	$\nvDash_{\mathrm{p}}$
		$\cdots$		

Definícia 4.7. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X je výrokovologická formula. Formulu X nazveme *falzifikovateľnou* vtt X je *nepravdivá* v *nejakom* výrokovologickom ohodnotení pre $\mathcal{L}$ (teda *existuje* také výrokovologické ohodnotenie v pre $\mathcal{L}$, že $v \nvDash_{\mathrm{p}} X$).

Nesplniteľnosť

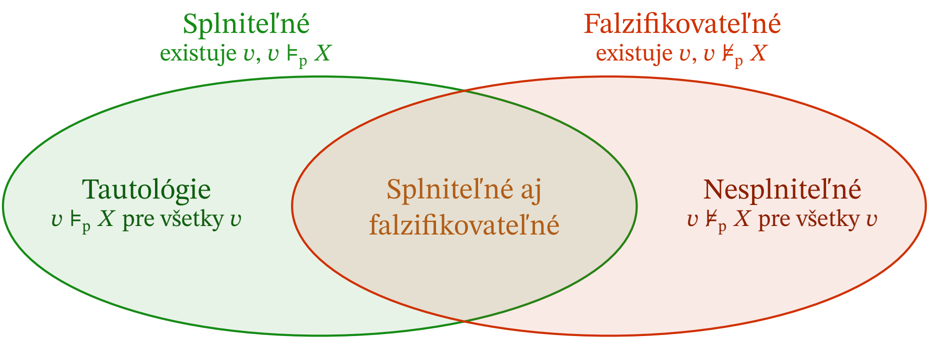
Nakoniec, mnohé formuly sú *nutne ne*pravdivé, teda sú *ne*pravdivé vo *všetkých* ohodnoteniach.

Nazývame ich *nesplniteľné*.

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\not\models_{\mathrm{p}}$
v_1	f	f	$\cdots$	$\not\models_{\mathrm{p}}$
		$\cdots$		
v_k	t	f	$\cdots$	$\not\models_{\mathrm{p}}$
		$\cdots$		

Definícia 4.8. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X je výrokovologická formula. Formulu X nazveme *nesplniteľnou* vtt X je *nepravdivá* v *každom* výrokovologickom ohodnotení pre $\mathcal{L}$ (teda pre *každé* výrokovologické ohodnotenie v pre $\mathcal{L}$, platí $v \not\models_{\mathrm{p}} X$).

„Geografia" formúl podľa pravdivosti vo všetkých ohodnoteniach



Obrázok podľa Papadimitriou [1994]

4.2 Ekvivalencia

Logická ekvivalencia

Dve tvrdenia sú *ekvivalentné*, ak sú v každom stave sveta buď obe pravdivé alebo obe nepravdivé.

Ekvivalentné tvrdenia sú navzájom nahraditeľné. To je výhodné vtedy, keď potrebujeme, aby tvrdenie malo nejaký požadovaný tvar, alebo používalo iba niektoré spojky. Napríklad vstupom pre SAT solver je teória zložená iba z disjunkcií literálov.

Podobne ako pri tautológiách môžeme pomocou skúmania všetkých ohodnotení rozpoznať *niektoré* ekvivalentné tvrdenia zapísané formulami (ale nie všetky, pretože ohodnotenia napríklad nedávajú význam rovnostným atómom).

Príklad výrokovologicky ekvivalentných formúl

Príklad 4.9. V jazyku $\mathcal{L}$ z príkladu 4.1 označme $A = \mathrm{p(a)}$ a $B = \mathrm{p(b)}$. Sú formuly $X = \neg(A \to \neg B)$ a $Y = (A \land B)$ výrokovologicky ekvivalentné?

Preskúmajme všetky výrokovologické ohodnotenia atómov A a B:

	v_i				X	Y
	A	B	$\neg B$	$(A \to \neg B)$	$\neg(A \to \neg B)$	$(A \land B)$
v_0	f	f	$\models_\mathrm{p}$	$\models_\mathrm{p}$	$\not\models_\mathrm{p}$	$\not\models_\mathrm{p}$
v_1	f	t	$\not\models_\mathrm{p}$	$\models_\mathrm{p}$	$\not\models_\mathrm{p}$	$\not\models_\mathrm{p}$
v_2	t	f	$\models_\mathrm{p}$	$\models_\mathrm{p}$	$\not\models_\mathrm{p}$	$\not\models_\mathrm{p}$
v_3	t	t	$\not\models_\mathrm{p}$	$\not\models_\mathrm{p}$	$\models_\mathrm{p}$	$\models_\mathrm{p}$

X je pravdivá *v práve tých* ohodnoteniach pre $\mathcal{L}$, v ktorých je pravdivá Y, preto X a Y sú výrokovologicky ekvivalentné.

Výrokovogická ekvivalencia

Definícia 4.10. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X a Y sú výrokovologické formuly jazyka $\mathcal{L}$. Formuly X a Y sú *výrokovologicky ekvivalentné*, skrátene $X \Leftrightarrow_\mathrm{p} Y$ vtt pre *každé* výrokovologické ohodnotenie v pre jazyk $\mathcal{L}$ platí, že X je pravdivá vo v vtt Y je pravdivá vo v.

$\Leftrightarrow_\mathrm{p}$ verzus $\leftrightarrow$

⚠ ***Pozor!*** Nemýľte si zápis $X \Leftrightarrow_\mathrm{p} Y$ s formulou $(X \leftrightarrow Y)$.

- $X \Leftrightarrow_\mathrm{p} Y$ je skrátené vyjadrenie vzťahu dvoch formúl podľa práve uvedenej definície. Keď napíšeme $X \Leftrightarrow_\mathrm{p} Y$, tvrdíme tým, že X a Y sú výrokovologicky ekvivalentné formuly (alebo sa pýtame, či to tak je).

- $(X \leftrightarrow Y)$ je formula, postupnosť symbolov, ktorá môže byť pravdivá v nejakom ohodnotení a nepravdivá v inom, môže byť splniteľná, tautológia, falzifikovateľná, nesplniteľná, môže vyplývať, či byť nezávislá od nejakej teórie, alebo môže byť výrokovologicky ekvivalentná s inou formulou.

Medzi $X \Leftrightarrow_{\mathrm{p}} Y$ a $(X \leftrightarrow Y)$ je vzťah, ktorý si ozrejmíme neskôr.

Známe ekvivalencie

O mnohých dvojiciach formúl už viete, že sú vzájomne ekvivalentné. Zhrnuli sme ich do nasledujúcej vety.

Známe ekvivalencie

Veta 4.11. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech A, B a C sú ľubovoľné výrokovologické formuly jazyka $\mathcal{L}$. Potom:*

$$(A \to B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor B) \qquad \text{nahradenie } \to$$

$$(A \land (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \land B) \land C) \qquad \text{asociatívnosť } \land$$
$$(A \lor (B \lor C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \lor C) \qquad \text{asociatívnosť } \lor$$

$$(A \land B) \Leftrightarrow_{\mathrm{p}} (B \land A) \qquad \text{komutatívnosť } \land$$
$$(A \lor B) \Leftrightarrow_{\mathrm{p}} (B \lor A) \qquad \text{komutatívnosť } \lor$$

$$(A \land (B \lor C)) \Leftrightarrow_{\mathrm{p}} ((A \land B) \lor (A \land C)) \qquad \text{distributívnosť } \land \text{ cez } \lor$$
$$(A \lor (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C)) \qquad \text{distributívnosť } \lor \text{ cez } \land$$

Veta 4.11 (pokračovanie)**.**

$$\neg(A \land B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor \neg B) \qquad \text{de Morganove}$$
$$\neg(A \lor B) \Leftrightarrow_{\mathrm{p}} (\neg A \land \neg B) \qquad \text{zákony}$$

$$\neg\neg A \Leftrightarrow_{\mathrm{p}} A \qquad \text{zákon dvojitej negácie}$$

$$(A \land A) \Leftrightarrow_{\mathrm{p}} A \qquad \text{idempotencia pre } \land$$
$$(A \lor A) \Leftrightarrow_{\mathrm{p}} A \qquad \text{idempotencia pre } \lor$$

$$
\begin{aligned}
(A \wedge \top) &\Leftrightarrow_{\mathrm{p}} A && \text{identita pre } \wedge \\
(A \vee \bot) &\Leftrightarrow_{\mathrm{p}} A && \text{identita pre } \vee \\[1ex]
(A \vee (A \wedge B)) &\Leftrightarrow_{\mathrm{p}} A && \text{absorpcia} \\
(A \wedge (A \vee B)) &\Leftrightarrow_{\mathrm{p}} A && \\[1ex]
(A \vee \neg A) &\Leftrightarrow_{\mathrm{p}} \top && \text{vylúčenie tretieho } \textit{(tertium non datur)} \\
(A \wedge \neg A) &\Leftrightarrow_{\mathrm{p}} \bot && \text{spor,}
\end{aligned}
$$

kde $\top$ *je ľubovoľná tautológia a* $\bot$ *je ľubovoľná nesplniteľná formula.*

Všeobecné dôkazy známych ekvivalencií

Pre *konkrétne* dvojice formúl v konkrétnom jazyku sa ekvivalencia dá dokázať rozborom všetkých ohodnotení ako v príklade 4.9.

Dôkaz ekvivalencie $(A \to B)$ a $(\neg A \vee B)$ pre *ľubovoľné* formuly A a B vyžaduje *opatrnejší* postup.

Nemôžeme predpokladať, že A a B sú atomické a ohodnotenia im *priamo* priraďujú pravdivostné hodnoty f a t (ak napr. $A = (\mathrm{p}(\mathrm{a}) \wedge \neg\mathrm{p}(\mathrm{a}))$, tak $v(A)$ nie je definované, definované sú iba $v(\mathrm{p}(\mathrm{a}))$ a $v(\mathrm{p}(\mathrm{b}))$).

Môžeme však:

1. zobrať *ľubovoľné* ohodnotenie v,
2. rozobrať všetky prípady, akými môžu byť A a B pravdivé alebo nepravdivé v tomto ohodnotení (teda $v \models_{\mathrm{p}} A$ a $v \models_{\mathrm{p}} B$, $v \models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$, $v \not\models_{\mathrm{p}} A$ a $v \models_{\mathrm{p}} B$, $v \not\models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$)
3. a ukázať, že v každom prípade je $(A \to B)$ pravdivá vo v vtt je $(\neg A \vee B)$ pravdivá vo v.

Príklad 4.12 (Dôkaz prvej ekvivalentnej dvojice z vety 4.11). Nech A a B sú ľubovoľné výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

Nech v je ľubovoľné ohodnotenie pre $\mathcal{L}$. V tomto ohodnotení môže byť každá z formúl A a B buď pravdivá alebo nepravdivá, a teda môžu nastať nasledovné prípady:

- $v \not\models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$, vtedy $v \models_{\mathrm{p}} (A \to B)$ a $v \models_{\mathrm{p}} (\neg A \vee B)$;

- $v \not\models_p A$ a $v \models_p B$, vtedy $v \models_p (A \to B)$ a $v \models_p (\neg A \lor B)$;
- $v \models_p A$ a $v \not\models_p B$, vtedy $v \not\models_p (A \to B)$ a $v \not\models_p (\neg A \lor B)$;
- $v \models_p A$ a $v \models_p B$, vtedy $v \models_p (A \to B)$ a $v \models_p (\neg A \lor B)$.

Rozobrali sme *všetky prípady* pravdivosti A a B v ohodnotení v a aj keď sa prípady od seba líšia pravdivosťou $(A \to B)$ a $(\neg A \lor B)$, v *každom prípade* platí, že $v \models_p (A \to B)$ *vtt* $v \models_p (\neg A \lor B)$. Preto môžeme konštatovať, že bez ohľadu na to, ktorý prípad nastáva, v ohodnotení v platí, že $v \models_p (A \to B)$ vtt $v \models_p (\neg A \lor B)$.

Pretože ohodnotenie v bolo *ľubovoľné*, môžeme toto konštatovanie *zovšeobecniť* na všetky ohodnotenia pre $\mathcal{L}$ a podľa definície 4.10 sú $(A \to B)$ a $(\neg A \lor B)$ výrokovologicky ekvivalentné.

Dôkazy rozborom prípadov

Rozbor prípadov z odrážkového zoznamu v predchádzajúcom dôkaze môžeme zapísať do *podobnej* tabuľky ako v príklade 4.9:

	A	B	$(A \to B)$	$(\neg A \lor B)$
v	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$
v	$\not\models_p$	$\models_p$	$\models_p$	$\models_p$
v	$\models_p$	$\not\models_p$	$\not\models_p$	$\not\models_p$
v	$\models_p$	$\models_p$	$\models_p$	$\models_p$

Vždy ju však treba doplniť

1. úvodom o ľubovoľnom ohodnotení,
2. úvodom k rozboru prípadov,
3. záverom o všetkých prípadoch,
4. záverom o všetkých ohodnoteniach.

Podobne môžeme uvažovať o tautológiách, nesplniteľnosti, aj vyplývaní.

4.3 Vzťah tautológií, vyplývania a ekvivalencie

Tautológie a vyplývanie

Tautológie nie sú zaujímavé iba preto, že sú logickými pravdami.

Kedy je formula $((A_1 \land A_2) \to B)$ tautológia?

Vtedy, keď je pravdivá v každom ohodnotení, teda keď v každom ohodnotení v máme $v \nvDash_{\mathrm{p}} (A_1 \land A_2)$ alebo $v \vDash_{\mathrm{p}} B$, čiže keď v každom ohodnotení v, v ktorom $v \vDash_{\mathrm{p}} (A_1 \land A_2)$, máme aj $v \vDash_{\mathrm{p}} B$ teda keď v každom ohodnotení v, v ktorom $v \vDash_{\mathrm{p}} A_1$ a $v \vDash_{\mathrm{p}} A_2$, máme aj $v \vDash_{\mathrm{p}} B$, teda keď z $\{A_1, A_2\}$ výrokovologicky *vyplýva* B.

Vzťahy výrokovologického vyplývania a tautológií

Pripomeňme, že podľa tvrdenia 4.5: $\emptyset \vDash_{\mathrm{p}} A$ vtt $\vDash_{\mathrm{p}} A$.

Tvrdenie 4.13 (Sémantická verzia vety od dedukcii). *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech T je výrokovologická teória, nech A, B, C sú výrokovologické formuly v $\mathcal{L}$. Potom:*

a) $T \cup \{A\} \vDash_{\mathrm{p}} C$ *vtt* $T \vDash_{\mathrm{p}} (A \to C)$.

b) $T \cup \{A, B\} \vDash_{\mathrm{p}} C$ *vtt* $T \cup \{(A \land B)\} \vDash_{\mathrm{p}} C$.

Dôsledok 4.14 (Redukcia vyplývania na tautológiu). *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech A_1, A_2, …, A_n a C sú výrokovologické formuly v jazyku $\mathcal{L}$. Potom* $\{A_1, \dots, A_n\} \vDash_{\mathrm{p}} C$ *vtt* $\vDash_{\mathrm{p}} \big(((\cdots(A_1 \land A_2) \land \cdots) \land A_n\big) \to C\big)$.

Dôkaz tvrdenia 4.13. a) Nech T je teória a A a C sú výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

($\Leftarrow$) Predpokladajme, že z T vyplýva $(A \to C)$ a dokážme *priamo*, že z $T \cup \{A\}$ vyplýva C.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$, ktoré je modelom $T \cup \{A\}$. Vo v sú teda pravdivé všetky formuly z $T \cup \{A\}$. Preto $v \vDash_{\mathrm{p}} T$ a tiež $v \vDash_{\mathrm{p}} A$.

Z $v \vDash_{\mathrm{p}} T$ na základe predpokladu $T \vDash_{\mathrm{p}} (A \to C)$ dostávame, že vo v je pravdivá implikácia $(A \to C)$, teda podľa definície pravdivosti $v \nvDash_{\mathrm{p}} A$ alebo $v \vDash_{\mathrm{p}} C$. Pretože ale vieme, že $v \vDash_{\mathrm{p}} A$, musí $v \vDash_{\mathrm{p}} C$.

Keďže v bolo ľubovoľné, môžeme toto zistenie zovšebecniť na všetky ohodnotenia a podľa definície vyplývania potom $T \cup \{A\} \vDash_p C$.

($\Rightarrow$) Predpokladajme, že z $T \cup \{A\}$ vyplýva C a dokážme *sporom*, že z T vyplýva $(A \to C)$.

Nech by existovalo ohodnotenie v, ktoré je modelom T, ale nie formuly $(A \to C)$, teda podľa definície pravdivosti $v \vDash_p A$ a $v \nvDash_p C$. Potom $v \vDash_p T \cup \{A\}$ a z predpokladu $T \cup \{A\} \vDash_p C$ dostávame $v \vDash_p C$, čo je spor.

b) Dôkaz je podobný ako v časti a). $\square$

Dôkaz dôsledku 4.14. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech $A_1, A_2, \dots, A_n$ a C sú výrokovologické formuly v jazyku $\mathcal{L}$.

Opakovaným použitím tvrdenia 4.13 a pomocou 4.5 dostávame:

$$\begin{aligned}
\{A_1, A_2, \dots, A_n\} \vDash_p C \quad & \text{vtt} \quad \{(A_1 \land A_2), \dots, A_n\} \vDash_p C \\
& \text{vtt} \quad \cdots \\
& \text{vtt} \quad \emptyset \cup \{((\cdots(A_1 \land A_2) \land \cdots) \land A_n)\} \vDash_p C \\
& \text{vtt} \quad \emptyset \vDash_p \big(((\cdots(A_1 \land A_2) \land \cdots) \land A_n\big) \to C\big) \\
& \text{vtt} \quad \vDash_p \big(((\cdots(A_1 \land A_2) \land \cdots) \land A_n\big) \to C\big) \qquad \square
\end{aligned}$$

Tautológie a ekvivalencia

Kedy je formula $(X \leftrightarrow Y)$, teda $((X \to Y) \land (Y \to X))$ tautológia?

Vtedy a len vtedy, keď je pravdivá v každom ohodnotení, teda vtt v každom ohodnotení v máme $v \vDash_p (X \to Y)$ a $v \vDash_p (Y \to X)$, vtt v každom ohodnotení v máme buď $v \nvDash_p X$ alebo $v \vDash Y$ a zároveň buď $v \nvDash_p Y$ alebo $v \vDash X$, vtt v každom ohodnotení v platí, že ak $v \vDash_p X$, tak $v \vDash_p Y$, a ak $v \vDash_p Y$, tak $v \vDash_p X$, vtt v každom ohodnotení v máme $v \vDash_p X$ vtt $v \vDash_p Y$, vtt X je výrokovologicky *ekvivalentná* s Y.

Tvrdenie 4.15. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X a Y sú výrokovologické formuly v $\mathcal{L}$. Potom $(X \leftrightarrow Y)$ je tautológia vtt X a Y sú výrokologicky ekvivalentné. (Skrátene: $\vDash_p (X \leftrightarrow Y)$ vtt $X \Leftrightarrow_p Y$.)*

4.4 Ekvivalentné úpravy a CNF

Reťazenie ekvivalentných úprav

Určite ste už robili ekvivalentné úpravy formúl, pri ktorých ste *reťazili dvojice* vzájomne ekvivalentných formúl:

$$\neg(A \to \neg B) \Leftrightarrow_{\mathrm{p}} \neg(\neg A \vee \neg B) \Leftrightarrow_{\mathrm{p}} (\neg\neg A \wedge \neg\neg B) \Leftrightarrow_{\mathrm{p}} (A \wedge B)$$

a nakoniec ste prehlásili, že prvá $\neg(A \to \neg B)$ a posledná formula $(A \wedge B)$ sú ekvivalentné.

Mohli ste to urobiť, lebo $\Leftrightarrow_{\mathrm{p}}$ je *tranzitívna* relácia na formulách, dokonca viac než iba tranzitívna.

Výrokovologická ekvivalencia ako relácia ekvivalencie

Tvrdenie 4.16. *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.*

Vzťah výrokovologickej ekvivalencie $\Leftrightarrow_{\mathrm{p}}$ je reláciou ekvivalencie na výrokovologických formulách jazyka $\mathcal{L}$, teda pre všetky výrokovologické formuly X, Y, Z jazyka $\mathcal{L}$ platí:

- *Reflexivita: $X \Leftrightarrow_{\mathrm{p}} X$.*
- *Symetria: Ak $X \Leftrightarrow_{\mathrm{p}} Y$, tak $Y \Leftrightarrow_{\mathrm{p}} X$.*
- *Tranzitivita: Ak $X \Leftrightarrow_{\mathrm{p}} Y$ a $Y \Leftrightarrow_{\mathrm{p}} Z$, tak $X \Leftrightarrow_{\mathrm{p}} Z$.*

Dôkaz. Priamym dôkazom dokážeme tranzitivitu. Ostatné vlastnosti sa dajú dokázať podobne.

Nech X, Y a Z sú výrokovologické formuly jazyka $\mathcal{L}$. Nech (1) X je výrokovologicky ekvivalentná s Y a (2) Y je ekvivalentná so Z.

Aby sme dokázali, že X je výrokovologicky ekvivalentná so Z, musíme ukázať, že pre každé ohodnotenie pre jazyk $\mathcal{L}$ platí, že $v \models_{\mathrm{p}} X$ vtt $v \models_{\mathrm{p}} Y$.

Nech teda v je ľubovoľné ohodnotenie pre $\mathcal{L}$.

- Ak $v \models_{\mathrm{p}} X$, tak podľa predpokladu (1) a definície výrokovologickej ekvivalencie 4.10 musí platiť $v \models_{\mathrm{p}} Y$, a teda podľa predpokladu (2) a definície ekvivalencie máme $v \models_{\mathrm{p}} Z$.
- Nezávisle od toho, ak $v \models_{\mathrm{p}} Z$, tak $v \models_{\mathrm{p}} Y$ podľa (2) a def. 4.10, a teda $v \models_{\mathrm{p}} X$ podľa (1) a def. 4.10.

Preto $v \models_{\mathrm{p}} X$ vtt $v \models_{\mathrm{p}} Z$.

Pretože v bolo ľubovoľné, môžeme náš záver zovšeobecniť na všetky ohodnotenia, a teda podľa definície ekvivalencie 4.10 sú X a Z výrokovologicky ekvivalentné. □

Substitúcia pri ekvivalentných úpravách

V reťazci ekvivalentných úprav

$$\neg(A \to \neg B) \Leftrightarrow_{\mathrm{p}} \neg(\neg A \lor \neg B) \Leftrightarrow_{\mathrm{p}} (\neg\neg A \land \neg\neg B)$$
$$\Leftrightarrow_{\mathrm{p}} (A \land \neg\neg B) \Leftrightarrow_{\mathrm{p}} (A \land B)$$

v prvom, treťom a štvrtom kroku *nezodpovedá celá* formula niektorej zo známych ekvivalencií z vety 4.11.

Podľa známej ekvivalencie sme *nahrádzali podformuly — substituovali* sme ich.

Definícia 4.17 (Substitúcia)**.** Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X, A, B sú formuly jazyka $\mathcal{L}$. *Substitúciou B za A v X* (skrátene $X[A|B]$) nazývame formulu, ktorá vznikne nahradením každého výskytu A v X formulou B.

Substitúcia rekurzívne

Substitúciu si vieme predstaviť aj ako induktívne definovanú (rekurzívnu) operáciu:

Substitúcia rekurzívne

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Pre všetky formuly A, B, X, Y jazyka $\mathcal{L}$ a všetky binárne spojky $b \in \{\land, \lor, \to\}$:

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

Korektnosť substitúcie ekvivalentnej formuly

Substitúciou ekvivalentnej podformuly, napríklad

$$(\neg\neg O \land \neg\neg C)[\neg\neg O|O] = (O \land \neg\neg C),$$

skutočne dostávame formulu ekvivalentnú s pôvodnou:

Veta 4.18 (Ekvivalentné úpravy substitúciou). *Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X je formula, A a B sú výrokovologicky ekvivalentné formuly jazyka $\mathcal{L}$. Potom formuly X a $X[A|B]$ sú tiež výrokovologicky ekvivalentné.*

Toto tvrdenie môžeme dokázať indukciou na konštrukciu formuly.

Ekvivalentné úpravy a vstup pre SAT solver

Častým použitím ekvivalentných úprav je transformácia teórie (napríklad o nejakom Sudoku) do tvaru vhodného pre SAT solver.

Aby sme tento tvar mohli popísať, potrebujeme pomenovať viacnásobne vnorené konjunkcie a viacnásobne vnorené disjunkcie a dohodneme sa na skracovaní ich zápisu vynechaním vnútorných zátvoriek.

Konjunkcia a disjunkcia postupnosti formúl

Definícia 4.19. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech $A_1, A_2, \dots, A_n$ je konečná postupnosť formúl jazyka $\mathcal{L}$.

- *Konjunkciou postupnosti* $A_1, \dots, A_n$ je formula $(((A_1 \land A_2) \land A_3) \land \dots \land A_n)$, skrátene $(A_1 \land A_2 \land A_3 \land \dots \land A_n)$.
    - Konjunkciu *prázdnej* postupnosti formúl ($n = 0$) označujeme $\top$. Chápeme ju ako ľubovoľnú *tautológiu*, napríklad $(P(c) \lor \neg P(c))$ pre nejaký unárny predikát P a nejakú konštantu c jazyka $\mathcal{L}$.
- *Disjunkciou postupnosti* $A_1, \dots, A_n$ je formula $(((A_1 \lor A_2) \lor A_3) \lor \dots \lor A_n)$, skrátene $(A_1 \lor A_2 \lor A_3 \lor \dots \lor A_n)$.
    - Disjunkciu *prázdnej* postupnosti formúl označujeme $\bot$ alebo $\Box$. Chápeme ju ako ľubovoľnú *nesplniteľnú* formulu, napríklad $(P(c) \land \neg P(c))$.
- Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1.

Literál, klauzula, konjunktívny normálny tvar

Vstup do SAT solvera je formula v konjunktívnom normálnom tvare.

Definícia 4.20.

Literál je atóm alebo negácia atómu.

Klauzula (tiež „klauza“, angl. *clause*) je *disjunkcia* postupnosti literálov.

Formula v konjunktívnom normálnom tvare (angl. conjunctive normal form, *CNF*) je *konjunkcia* postupnosti klauzúl.

Príklad 4.21. **Literály:** $P, C, \neg C, \neg O$

Klauzuly: $P, \neg O, \square, (\neg P \lor O \lor \neg C)$

CNF: $P, \neg O, \top, (P \lor \neg O)\ (P \land \neg O \land C), \square, ((P \lor O) \land \square), ((\neg P \lor O) \land (O \lor C))$
ak $P = \text{pacient(Edo)}$, $O = \text{očkovaný(Edo)}$, $C = \text{chorý(Edo)}$.

Existencia ekvivalentnej formuly v CNF

Veta 4.22. *Ku každej výrokovologickej formule X existuje ekvivalentná formula C v konjunktívnom normálnom tvare.*

Dôkaz. Zoberme všetky ohodnotenia $v_1, \dots, v_n$ také, že $v_i \models_p \neg X$ a $v_i(A) = f$ pre všetky atómy $A \notin \text{atoms}(\neg X)$. Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu A, ak $v_i(A) = t$, alebo $\neg A$, ak $v_i(A) = f$, pre každý atóm $A \in \text{atoms}(\neg X)$. Očividne formula $D = (C_1 \lor \dots \lor C_n)$ je ekvivalentná s $\neg X$ (vymenúva všetky možnosti, kedy je $\neg X$ pravdivá).

Znegovaním D a aplikáciou de Morganových pravidiel dostaneme formulu C v CNF, ktorá je ekvivalentná s X. □

Konverzia formuly do ekvivalentnej v CNF

Skúmanie všetkých ohodnotení podľa dôkazu vety 4.22 nie je ideálny spôsob ako upraviť formulu do CNF — najmä keď má veľa premenných a jej splniteľnosť chceme rozhodnúť SAT solverom.

Jednoduchý algoritmus na konverziu formuly do ekvivalentnej formuly v CNF založený na ekvivalentných úpravách si naprogramujete ako **4. praktické cvičenie**.

Konverzia formuly do ekvivalentnej v CNF

Základný algoritmus konverzie do CNF má dve fázy:

1. Upravíme formulu na *negačný normálny tvar* (NNF) — nevyskytuje sa v ňom implikácia a negované sú iba atómy:
   - Nahradíme implikácie disjunkciami: $(A \to B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor B)$
   - Presunieme $\neg$ k atómom opakovaným použitím de Morganových zákonov a zákona dvojitej negácie.
2. Odstránime konjunkcie vnorené v disjunkciách „roznásobením" podľa distributívnosti a komutatívnosti:

$$\begin{aligned}
(A \lor (B \land C)) &\Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C)) \\
((B \land C) \lor A) &\Leftrightarrow_{\mathrm{p}} (A \lor (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C)) \\
&\Leftrightarrow_{\mathrm{p}} ((B \lor A) \land (A \lor C)) \\
&\Leftrightarrow_{\mathrm{p}} ((B \lor A) \land (C \lor A))
\end{aligned}$$

Konverzia formuly do ekvivalentnej v CNF

Príklad 4.23. Úprava formuly do NNF:

$$\begin{aligned}
((\neg S \land P) \to \neg(Z \lor \neg O)) &\Leftrightarrow_{\mathrm{p}} (\neg(\neg S \land P) \lor \neg(Z \lor \neg O)) \quad \text{(nahr. } \to\text{)} \\
&\Leftrightarrow_{\mathrm{p}} ((\neg\neg S \lor \neg P) \lor (\neg Z \land \neg\neg O)) \quad (2 \times \text{de Morgan}) \\
&\Leftrightarrow_{\mathrm{p}} ((S \lor \neg P) \lor (\neg Z \land O)) \quad (2 \times \text{dvoj. neg.})
\end{aligned}$$

Úprava formuly v NNF do CNF:

$$\begin{aligned}
&((S \lor \neg P) \lor (\neg Z \land O)) \\
&\qquad \Leftrightarrow_{\mathrm{p}} (((S \lor \neg P) \lor \neg Z) \land ((S \lor \neg P) \lor O)) \quad \text{(distr. } \land \text{ cez } \lor\text{)}
\end{aligned}$$

Podľa dohody v def. 4.19 výslednú formulu v CNF skrátene zapíšeme:

$$((S \lor \neg P \lor \neg Z) \land (S \lor \neg P \lor O))$$

Zhrnutie

- Význačné sémantické vlastnosti formúl: tautologickosť, splniteľnosť, nesplniteľnosť, falzifikovateľnosť
- Ekvivalencia — sémantický vzťah formúl
- Vzťah tautológií s vyplývaním a ekvivalenciou
- Syntaktické odvodenie ekvivalencie pomocou substitúcií podľa známych ekvivalencií
- NNF a CNF

5. prednáška
Dôkazy a výrokovologické tablá

Rekapitulácia

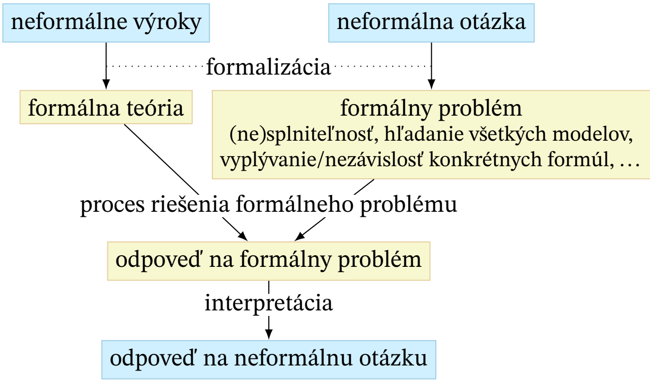
Minulý týždeň sme sa zaoberali:

- vlastnosťami formúl vzhľadom na všetky ohodnotenia:
  - tautológia,
  - splniteľnosť,
  - falzifikovateľnosť,
  - nesplniteľnosť;
- vzťahmi formúl:
  - ekvivalencia;
- vzťahom vyplývania a ekvivalencie s tautológiami;
- transformáciou formúl medzi jazykmi so zachovaním splniteľnosti.

5 Dôkazy a výrokovologické tablá

Riešenie slovných úloh pomocou formálnej logiky

V 3. sade teoretických úloh (AIN) sme riešili neformálne zadané problémy pomocou ich formálnej verzie:



Formálny problém sme riešili hrubou silou a sémanticky — rozborom všetkých ohodnotení. Žiadne naozajstné usudzovanie. Výsledok zodpovedal výsledku neformálneho úsudku o probléme.

Dôkazy neformálnych meta tvrdení

V 4. sade teoretických úloh sme dokazovali tvrdenia o vyplývaní, splniteľnosti a tautológiách:

- matematické tvrdenia v slovenčine;
- dôkazy tiež v slovenčine.

Usudzovanie, ale neformálne.

Formalizácia dôkazov

Logiku zaujíma *jazyk* a *usudzovanie*.

Výroky v slovenčine (jazyk) sme *sformalizovali* ako *formuly* v jazyku logiky prvého rádu

- matematická „dátová štruktúra“: postupnosti symbolov s induktívnymi pravidlami konštrukcie;
- javovská dátová štruktúra: stromy objektov podtried triedy `Formula`.

Dôkazy (usudzovanie) začneme *formalizovať* tento týždeň.

Čo sú dôkazy a prečo sa dokazuje

Dôkaz je úvaha, ktorá zdôvodňuje, prečo je nejaký záver logickým dôsledkom predpokladov.

Načo sú vlastne dobré *dôkazy*?

- Môžeme nimi *presvedčiť* iných o pravdivosti svojich záverov.
- Zvyčajne sú menej prácne a *pochopiteľnejšie* ako rozbor všetkých možností.

  Už 16 možností v 3. sade úloh bolo prácne rozobrať.

  Ak je možností nekonečne veľa, rozbor všetkých možností ani nie je možný.
- Odvodzovaním podľa pravidiel dôkazov môžeme skúmať, aké dôsledky má naša teória aj bez konkrétneho cieľa.

Prečo formalizovať dôkazy

Načo je dobré *formalizovať* dôkazy?

- Aby sme si ujasnili, *čo* sú dôkazy a kedy sú *správne*. Správna argumentácia nie je dôležitá iba v matematike:
  - uvažovanie o správnosti našich programov či dopytov,
  - základ kritického/vedeckého myslenia v bežnom živote.
- Aby sme vedeli naprogramovať *dátové štruktúry* na ich reprezentáciu v počítači.
- Aby sme mohli dokazovanie *automatizovať*.
  - Automatické dokazovanie je jeden z cieľov umelej inteligencie.
- Aby sme zistili, čo sa dá a čo sa *nedá* dokázať.
  - Prakticky: Čo sa nedá dokázať, toho dôkaz sa nedá automatizovať.
  - Filozoficky: Hranice poznania a chápania.

5.1 Druhy dôkazov

Druhy dôkazov

V matematike sa na to používa viac typov dôkazov:

- priamy,
- sporom,
- nepriamy,
- analýzou prípadov,

ktoré sa často kombinujú.

Priamy dôkaz a analýza prípadov

Priamy dôkaz Z predpokladov postupným odvodzovaním jednoduchých logických dôsledkov dospejeme k požadovanému záveru.

Dôkaz analýzou (rozborom) prípadov Keď predpoklady obsahujú *disjunkciu*, dokážeme požadovaný záver *z každého disjunktu* a ostatných predpokladov *nezávisle* od ostatných disjunktov.

Ak aj predpoklady disjunkciu neobsahujú, môžeme rozoberať prípady, že je nejaké pomocné tvrdenie pravdivé alebo nepravdivé.

Príklad priameho dôkazu s analýzou prípadov

Príklad 5.1 (Párty po covide · priamy dôkaz s analýzou prípadov). (A_1) Anka príde, iba ak príde Betka a Cyril. (A_2) Ak príde Betka alebo Dávid, príde aj Evka. (A_3) Evka nepríde, ak príde Fero.

Teda: (X) Ak príde Anka, tak nepríde Fero.

Dôkaz (priamo). Predpokladajme, že tvrdenia A_1 až A_3 sú pravdivé. Dokážme X.

Ak nepríde Anka, X je pravdivé (X je implikácia a jej antecedent je nepravdivý).

Preto predpokladajme, že Anka príde. Podľa A_1 potom musia prísť aj Betka a Cyril. Preto príde Betka, a teda príde Betka alebo Dávid. Podľa A_2 potom príde aj Evka. Pretože podľa A_3 by Evka neprišla, ak by prišiel Fero, ale Evka príde, musí byť pravda, že Fero nepríde. Preto je tvrdenie X opäť pravdivé (X je implikácia a jej konzekvent je pravdivý).

Dôkaz sporom a nepriamy dôkaz

Dôkaz sporom Príjmeme predpoklady, ale *spochybníme záver* — predpokladáme, že je nepravdivý. Postupným odvodzovaním jednoduchých logických dôsledkov dospejeme k *sporu* s predpokladom alebo iným dôsledkom.

Záver teda nemôže byť nepravdivý, preto ak sú pravdivé predpoklady, je nutne pravdivý, vyplýva z nich.

Nepriamy dôkaz — variácia dôkazu sporom Predpokladáme, že záver je nepravdivý. Postupným odvodzovaním jednoduchých logických dôsledkov dospejeme k nepravdivosti niektorého z predpokladov.

Tým dokážeme: Ak je nepravdivý záver, tak sú nepravdivé predpoklady. Obmena: Ak sú pravdivé predpoklady, je pravdivý záver.

Príklad dôkazu sporom

Príklad 5.2 (Párty po covide · dôkaz sporom).
(A_1) Anka príde, iba ak príde Betka a Cyril. (A_2) Ak príde Betka alebo Dávid, príde aj Evka. (A_3) Evka nepríde, ak príde Fero.

Teda: (X) Ak príde Anka, tak nepríde Fero.

Dôkaz (sporom). Predpokladajme, že tvrdenia A_1 až A_3 sú pravdivé, ale X je nepravdivé.

Predpokladáme teda, že príde Anka a príde aj Fero. Preto príde Fero, a teda podľa predpokladu A_3 Evka nepríde. Zároveň vieme, že príde Anka, a podľa A_1 teda prídu aj Betka a Cyril. Preto príde Betka, a teda príde Betka alebo Dávid. Podľa A_2 potom príde aj Evka. To je však spor z predchádzajúcim dôsledkom A_3, že Evka nepríde.

Predpoklad, že X je nepravdivé viedol k sporu, preto X je pravdivé.

Výhody dôkazu sporom

Dôkaz sporom je veľmi konkrétna ukážka kritického, vedeckého myslenia:

1. Pochybujeme o pravdivosti tvrdenia.

2. Vyvrátením tejto pochybnosti sa presvedčíme o pravdivosti.

Má ale aj „technickú“ výhodu: Nemusíme pri ňom až tak tápať, ako dospejeme k cieľu, pretože

- dostaneme viac predpokladov;
- máme jednoduchý cieľ: nájsť spor;
- väčšinou stačí tvrdenia iba zjednodušovať.

Odvodzovanie jednoduchých dôsledkov

Kroky dôkazu by mali odvodzovať *jednoduché dôsledky*.

Tie potom používame na odvodenie ďalších dôsledkov.

Aký dôsledok je jednoduchý?

Závisí od čitateľa dôkazu — musí byť schopný ho overiť.

Matematici (a učitelia) radi robia väčšie skoky a nechajú čitateľa (študenta) domýšľať si, prečo ich mohli urobiť.

Vyučujúci chcú od študentov malé kroky — aby si overili, že študent skutočne uvažuje správne.

5.2 Výrokovologické tablá

Jednoduché dôsledky podľa definície pravdivosti formúl

Pozrime sa znova na príklad dôkazu sporom:

1. Sformalizujme ho.
2. Uvedomme si, čo vlastne dokazujeme.
3. Všímajme si, aké kroky robíme.

Príklad dôkazu sporom s formulami

Príklad 5.3 (Párty po covide · formalizovaný dôkaz sporom). Dokážme, že z teórie $T = \{A_1, A_2, A_3\}$, kde

$A_1 = (\mathsf{p(A)} \to (\mathsf{p(B)} \land \mathsf{p(C)}))$ Anka príde, iba ak príde Betka a Cyril.
$A_2 = ((\mathsf{p(B)} \lor \mathsf{p(D)}) \to \mathsf{p(E)})$ Ak príde Betka alebo Dávid, príde aj Evka.
$A_3 = (\mathsf{p(F)} \to \neg\mathsf{p(E)})$, Evka nepríde, ak príde Fero.

vyplýva formula X, pričom

$X = (\mathsf{p(A)} \to \neg\mathsf{p(F)})$ Ak príde Anka, tak nepríde Fero.

Príklad 5.3 (Párty po covide · formal. dôkaz sporom, pokrač.).
Dôkaz (sporom). Predpokladajme, pre nejaké ohodnotenie v platí, že
(1) $v \models_p (\mathsf{p(A)} \to (\mathsf{p(B)} \land \mathsf{p(C)}))$,
(2) $v \models_p ((\mathsf{p(B)} \lor \mathsf{p(D)}) \to \mathsf{p(E)})$,
(3) $v \models_p (\mathsf{p(F)} \to \neg\mathsf{p(E)})$, ale
(4) $v \not\models_p (\mathsf{p(A)} \to \neg\mathsf{p(F)})$.
Podľa definície pravdivosti v ohodnotení, potom máme:
(5) $v \models_p \mathsf{p(A)}$ zo (4) a súčasne
(6) $v \not\models_p \neg\mathsf{p(F)}$ zo (4), teda
(7) $v \models_p \mathsf{p(F)}$ z (6). Ďalej
(8) $v \not\models_p \mathsf{p(F)}$, alebo (9) $v \models_p \neg\mathsf{p(E)}$ podľa (3).

čo je v spore so (7),	(10) $v \not\models_p \mathsf{p(E)}$ z (9). Zároveň		
	(11) $v \not\models_p \mathsf{p(A)}$, alebo (12) $v \models_p (\mathsf{p(B)} \land \mathsf{p(C)})$ podľa (1).		
	čo je v spore s (5),	(13) $v \models_p \mathsf{p(B)}$ z (12). Potom podľa (2):	
		(14) $v \not\models_p (\mathsf{p(B)} \lor \mathsf{p(D)})$, alebo	(15) $v \models_p \mathsf{p(E)}$, spor s (10).
		(16) $v \not\models_p \mathsf{p(B)}$ zo (14), spor s (13);	

Tablový kalkul

Z takýchto dôkazov sporom vychádza *tablový kalkul* — jeden z *formálnych deduktívnych systémov* pre výrokovologickú časť logiky prvého rádu

Formálny deduktívny systém je systém odvodzovacích pravidiel na konštrukciu dôkazov vyplývania formúl z teórií.

Nami používaná verzia tablového kalkulu pochádza od Raymonda M. Smullyana [Smullyan, 1979].

Postupne si ukážeme, ako predchádzajúci dôkaz premeníme na *tablo* — formálny dôkaz v tablovom kalkule.

Označené formuly a ich sémantika

Zbavme sa najprv opakovania $v \models_p \cdots$ a $v \not\models_p \cdots$.

Definícia 5.4. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech X je výrokovologická formula jazyka $\mathcal{L}$. Postupnosti symbolov $\mathbf{T}X$ a $\mathbf{F}X$ nazývame *označené formuly*.

Definícia 5.5. Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, v je ohodnotenie pre $\mathcal{L}$ a X je výrokovologická formula v $\mathcal{L}$. Potom

- *vo v je pravdivá* $\mathbf{T}X$ (skrátene $v \models_p \mathbf{T}X$) vtt vo v je pravdivá X;

- *vo v je pravdivá* $\mathbf{F}X$ (skr. $v \models_p \mathbf{F}X$) vtt vo v nie je pravdivá X.

Znamienko $\mathbf{F}$ sa teda správa ako negácia a $\mathbf{T}$ nemení význam formuly. Znamienka $\mathbf{F}$ a $\mathbf{T}$ sa *nesmú* objaviť v podformulách. Vďaka znamienkam stačí hovoriť iba o pravdivých ozn. formulách.

Príklad 5.5 (Párty po covide · dôkaz s označenými formulami). Predpokladajme, pre nejakom ohodnotení v sú pravdivé označené formuly
(1) $\mathbf{T}(p(A) \to (p(B) \land p(C)))$,
(2) $\mathbf{T}((p(B) \lor p(D)) \to p(E))$,
(3) $\mathbf{T}(p(F) \to \neg p(E))$, ale
(4) $\mathbf{F}(p(A) \to \neg p(F))$.
Podľa definície pravdivosti, sú vo v pravdivé:
(5) $\mathbf{T}\, p(A)$ zo (4) a súčasne
(6) $\mathbf{F}\, \neg p(F)$ zo (4), teda
(7) $\mathbf{T}\, p(F)$ z (6). Ďalej
(8) $\mathbf{F}\, p(F)$, alebo (9) $\mathbf{T}\, \neg p(E)$ podľa (3).
čo je v spore so (7), (10) $\mathbf{F}\, p(E)$ z (9). Zároveň
(11) $\mathbf{F}\, p(A)$, alebo (12) $\mathbf{T}(p(B) \land p(C))$ z (1).
čo je v spore s (5), (13) $\mathbf{T}\, p(B)$ z (12). Potom podľa (2)
(14) $\mathbf{F}(p(B) \lor p(D))$, alebo (15) $\mathbf{T}\, p(E)$,
(16) $\mathbf{F}\, p(B)$ zo (14), spor s (13); spor s (10).

Kroky odvodenia

Všimnime si teraz kroky, ktoré sme v dôkaze robili:

- Niektoré z pravdivosti formuly *priamo odvodili* pravdivosť niektorej priamej podformuly, napr.:
  - z (4) $\mathbf{F}(p(A) \to \neg p(F))$ sme odvodili (5) $\mathbf{T}\, p(A)$;
  - z (4) $\mathbf{F}(p(A) \to \neg p(F))$ sme odvodili (6) $\mathbf{F}\, \neg p(F)$;
  - z (9) $\mathbf{T}\, \neg p(E)$ sme odvodili (10) $\mathbf{F}\, p(E)$.
- Iné viedli k *analýze prípadov* pravdivosti *oboch* priamych podformúl:
  - (2) $\mathbf{T}((p(B) \lor p(D)) \to p(E))$ viedla k analýze prípadov: (14) $\mathbf{F}(p(B) \lor p(D))$ *alebo* (15) $\mathbf{T}\, p(E)$.

Priame odvodenie pravdivosti priamych podformúl

Z definície pravdivosti formúl ľahko dostaneme:

Pozorovanie 5.6. *Nech v je ľubovoľné ohodnotenie pre jazyk $\mathcal{L}$ výrokovologickej časti logiky prvého rádu. Nech X a Y sú ľubovoľné formuly $\mathcal{L}$:*

Ak $v \models_p \neg X$, *tak* $v \not\models_p X$.	*Ak* $v \models_p \mathbf{T}\,\neg X$, *tak* $v \models_p \mathbf{F}\,X$.
Ak $v \not\models_p \neg X$, *tak* $v \models_p X$.	*Ak* $v \models_p \mathbf{F}\,\neg X$, *tak* $v \models_p \mathbf{T}\,X$.
Ak $v \models_p (X \land Y)$, *tak* $v \models_p X$.	*Ak* $v \models_p \mathbf{T}(X \land Y)$, *tak* $v \models_p \mathbf{T}\,X$.
Ak $v \models_p (X \land Y)$, *tak* $v \models_p Y$.	*Ak* $v \models_p \mathbf{T}(X \land Y)$, *tak* $v \models_p \mathbf{T}\,Y$.
Ak $v \not\models_p (X \lor Y)$, *tak* $v \not\models_p X$.	*Ak* $v \models_p \mathbf{F}(X \lor Y)$, *tak* $v \models_p \mathbf{F}\,X$.
Ak $v \not\models_p (X \lor Y)$, *tak* $v \not\models_p Y$.	*Ak* $v \models_p \mathbf{F}(X \lor Y)$, *tak* $v \models_p \mathbf{F}\,Y$.
Ak $v \not\models_p (X \to Y)$, *tak* $v \models_p X$.	*Ak* $v \models_p \mathbf{F}(X \to Y)$, *tak* $v \models_p \mathbf{T}\,X$.
Ak $v \not\models_p (X \to Y)$, *tak* $v \not\models_p Y$.	*Ak* $v \models_p \mathbf{F}(X \to Y)$, *tak* $v \models_p \mathbf{F}\,Y$.

Zjednodušujúce tablové pravidlá

Z pozorovania 5.6 môžeme sformulovať pravidlá, ktoré priamo odvodzujú z označených formúl ich označené podformuly:

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

$$\frac{\mathbf{T}(X \land Y)}{\mathbf{T}\,Y} \qquad \frac{\mathbf{F}(X \lor Y)}{\mathbf{F}\,Y} \qquad \frac{\mathbf{F}(X \to Y)}{\mathbf{F}\,Y}$$

Na tieto pravdidlá sa dá pozerať ako na *špeciálne prípady jedného pravidla*, ktorému sa hovorí α, *zjednodušenie* alebo *sploštenie* (angl. *flatten*), pre rôzne spojky.

Jednotný zápis označených formúl typu α

Definícia 5.7 (Jednotný zápis označených formúl typu α)**.**
Označená formula A^+ je *typu α* vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly X a Y. Takéto formuly budeme označovať písmenom α; α_1 bude označovať príslušnú označenú formulu zo stredného stĺpca, α_2 príslušnú formulu z pravého stĺpca.

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

Pozorovanie 5.8 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie pre jazyk $\mathcal{L}$ výrokovologickej časti logiky prvého rádu. Potom $v \models_{\mathrm{p}} \alpha$ vtt $v \models_{\mathrm{p}} \alpha_1$ a $v \models_{\mathrm{p}} \alpha_2$.*

Analýza prípadov pravdivosti priamych podformúl

Z definície pravdivosti formúl ľahko dostaneme:

Pozorovanie 5.9. *Nech v je ľubovoľné ohodnotenie pre jazyk $\mathcal{L}$ výrokovologickej časti logiky prvého rádu. Nech X a Y sú ľubovoľné formuly $\mathcal{L}$:*

- *Ak $v \not\models_{\mathrm{p}} (X \land Y)$, tak $v \not\models_{\mathrm{p}} X$ alebo $v \not\models_{\mathrm{p}} Y$. Ak $v \models_{\mathrm{p}} \mathbf{F}(X \land Y)$, tak $v \models_{\mathrm{p}} \mathbf{F}X$ alebo $v \models_{\mathrm{p}} \mathbf{F}Y$.*
- *Ak $v \models_{\mathrm{p}} (X \lor Y)$, tak $v \models_{\mathrm{p}} X$ alebo $v \models_{\mathrm{p}} Y$. Ak $v \models_{\mathrm{p}} \mathbf{T}(X \lor Y)$, tak $v \models_{\mathrm{p}} \mathbf{T}X$ alebo $v \models_{\mathrm{p}} \mathbf{T}Y$.*
- *Ak $v \models_{\mathrm{p}} (X \to Y)$, tak $v \not\models_{\mathrm{p}} X$ alebo $v \models_{\mathrm{p}} Y$. Ak $v \models_{\mathrm{p}} \mathbf{T}(X \to Y)$, tak $v \models_{\mathrm{p}} \mathbf{F}X$ alebo $v \models_{\mathrm{p}} \mathbf{T}Y$.*

Rozvetvujúce tablové pravidlá

Z pozorovania 5.9 môžeme sformulovať pravidlá, ktoré vedú k analýze prípadov pravdivosti priamych podformúl:

$$\frac{\mathbf{F}(X \land Y)}{\mathbf{F}X \mid \mathbf{F}Y} \qquad \frac{\mathbf{T}(X \lor Y)}{\mathbf{T}X \mid \mathbf{T}Y} \qquad \frac{\mathbf{T}(X \to Y)}{\mathbf{F}X \mid \mathbf{T}Y}$$

Aj na tieto pravdidlá sa dá pozerať ako na špeciálne prípady jedného pravidla, ktorému sa hovorí β, *vetvenie* alebo *rozdelenie* (angl. *split*), pre rôzne spojky.

Jednotný zápis označených formúl typu β

Definícia 5.10 (Jednotný zápis označených formúl typu β). Označená formula B^+ je *typu β* vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly X a Y. Takéto formuly budeme označovať písmenom β; β_1 bude označovať príslušnú označenú formulu zo stredného stĺpca, β_2 príslušnú formulu z pravého stĺpca.

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

Pozorovanie 5.11 (Stručne vďaka jednotnému zápisu)**.** *Nech v je ľubovoľné ohodnotenie pre jazyk $\mathcal{L}$ výrokovologickej časti logiky prvého rádu. Potom $v \models_{\mathrm{p}} \beta$ vtt $v \models_{\mathrm{p}} \beta_1$ alebo $v \models_{\mathrm{p}} \beta_2$.*

Označovanie označených formúl a ich množín

Čo vlastne dokazujeme v našom príklade? To, že predpoklad existencie ohodnotenia v, v ktorom sú pravdivé všetky prvky množiny označených formúl

$$\begin{aligned} S^+ = \{\ & \mathbf{T}\mathsf{(p(A) \to (p(B) \land p(C)))}, \\ & \mathbf{T}\mathsf{((p(B) \lor p(D)) \to p(E))}, \\ & \mathbf{T}\mathsf{(p(F) \to \neg p(E))}, \\ & \mathbf{F}\mathsf{(p(A) \to \neg p(F))}\ \} \end{aligned}$$

vedie k sporu, teda že S^+ je *nesplniteľná*.

Dohoda 5.12. 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.

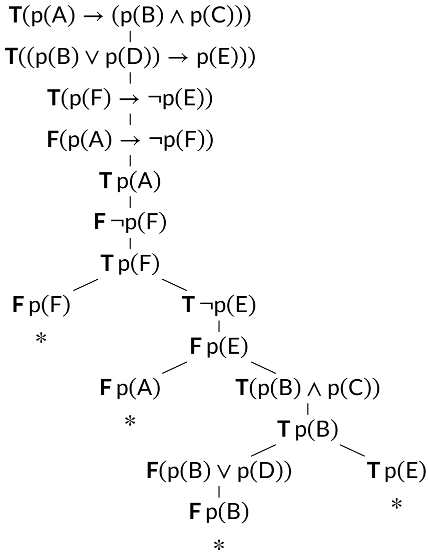
Príklad 5.12 (Párty po covide · tablo).

1.	$\mathbf{T}\mathsf{(p(A) \to (p(B) \land p(C)))}$	S^+
2.	$\mathbf{T}\mathsf{((p(B) \lor p(D)) \to p(E))}$	S^+
3.	$\mathbf{T}\mathsf{(p(F) \to \neg p(E))}$	S^+
4.	$\mathbf{F}\mathsf{(p(A) \to \neg p(F))}$	S^+
5.	$\mathbf{T}\,\mathsf{p(A)}$	$\alpha 4$
6.	$\mathbf{F}\,\mathsf{\neg p(F)}$	$\alpha 4$
7.	$\mathbf{T}\,\mathsf{p(F)}$	$\alpha 6$

<table>
<tr><td rowspan="3">8. $\mathbf{F}\,\mathsf{p(F)}$ $\beta 3$
$*7, 8$</td><td colspan="3">9. $\mathbf{T}\,\mathsf{\neg p(E)}$ $\beta 3$
10. $\mathbf{F}\,\mathsf{p(E)}$ $\alpha 9$</td></tr>
<tr><td rowspan="2">11. $\mathbf{F}\,\mathsf{p(A)}$ $\beta 1$
$*5, 11$</td><td colspan="2">12. $\mathbf{T}\mathsf{(p(B) \land p(C))}$ $\beta 1$
13. $\mathbf{T}\,\mathsf{p(B)}$ $\alpha 12$</td></tr>
<tr><td>14. $\mathbf{F}\mathsf{(p(B) \lor p(D))}$ $\beta 2$
16. $\mathbf{F}\,\mathsf{p(B)}$ $\alpha 14$
$*13, 16$</td><td>15. $\mathbf{T}\,\mathsf{p(E)}$ $\beta 2$
$*10,15$</td></tr>
</table>

Štruktúra tabla

Čo je teda tablo? Aká „dátová štruktúra“? Čo v nej musí platiť?



Definícia 5.13 (Tablo pre množinu označených formúl)**.** *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 induktívnych 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* $\mathcal{T}$ ktorýmkoľvek z pravidiel:

  α: 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.

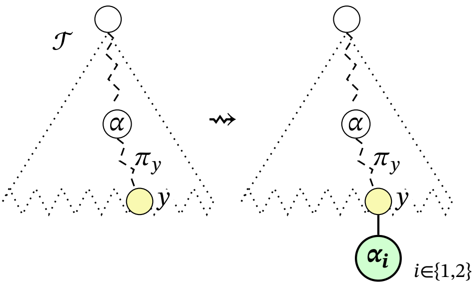
  β: Ak sa na vetve π_y (ceste z koreňa do y) vyskytuje nejaká označená formula β, tak ako deti y pripojíme *dva* nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2.

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

Nič iné nie je tablom pre S^+.

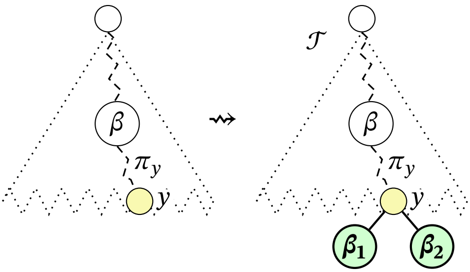
Tablá a tablové pravidlá

Pôvodné tablo Možné priame rozšírenie Pravidlá a označené formuly v nich



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

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



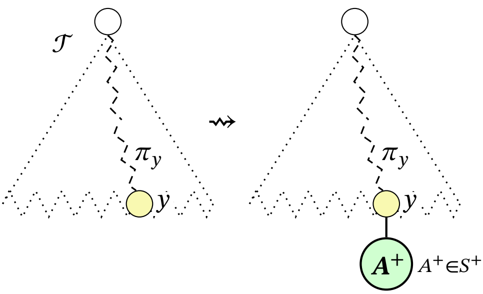
$$\frac{\beta}{\beta_1 \mid \beta_2}$$

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

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

Tablá a tablové pravidlá (pokračovanie)

Pôvodné tablo Možné priame rozšírenie Pravidlá a označené formuly v nich



$$\frac{}{A^+} \qquad A^+ \in S^+$$

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

Uzavretosť a otvorenosť vetvy a tabla

Definícia 5.14. *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 X^+ sa nachádza v niektorom vrchole na π. Skrátene to budeme zapisovať $X^+ \in formulas(\pi)$.

Tablo ~ dôkaz sporom. Vetvenie ~ rozbor možných prípadov. $\Longrightarrow$ Spor musí nastať vo všetkých vetvách.

Definícia 5.15. *Vetva* π tabla $\mathcal{T}$ je *uzavretá* vtt na π sa súčasne vyskytujú označené formuly $\mathbf{F}X$ a $\mathbf{T}X$ pre nejakú formulu X. Inak je π *otvorená*.

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

Príklad — vetvy a uzavretosť

Príklad 5.16 (Vetvy a uzavretosť). Určme vetvy v table a zistime, či sú uzavreté a či je uzavreté tablo:

1.	$\mathbf{T}(p(A) \to (p(B) \land p(C)))$	S^+
2.	$\mathbf{T}((p(B) \lor p(D)) \to p(E))$	S^+
3.	$\mathbf{T}(p(F) \to \neg p(E))$	S^+
4.	$\mathbf{F}(p(A) \to \neg p(F))$	S^+
5.	$\mathbf{T}\,p(A)$	$\alpha 4$
6.	$\mathbf{F}\,\neg p(F)$	$\alpha 4$
7.	$\mathbf{T}\,p(F)$	$\alpha 6$

<table>
<tr>
<td>8. $\mathbf{F}\,p(F)$ $\beta 3$
$*7, 8$</td>
<td>
9. $\mathbf{T}\,\neg p(E)$ $\beta 3$
10. $\mathbf{F}\,p(E)$ $\alpha 9$
<table>
<tr>
<td>11. $\mathbf{F}\,p(A)$ $\beta 1$
$*5, 11$</td>
<td>
12. $\mathbf{T}(p(B) \land p(C))$ $\beta 1$
13. $\mathbf{T}\,p(B)$ $\alpha 12$
<table>
<tr>
<td>14. $\mathbf{F}(p(B) \lor p(D))$ $\beta 2$</td>
<td>15. $\mathbf{T}\,p(E)$ $\beta 2$
$*10,15$</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>

Korektnosť tablového kalkulu

Veta 5.17 (Korektnosť tablového kalkulu). *Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+. Potom je množina S^+ nesplniteľná.*

Dôsledok 5.18. *Nech S je výrokovologická teória a X je výrokovologická formula. Ak existuje uzavreté tablo pre $\{\mathsf{T}\,A \mid A \in S\} \cup \{\mathsf{F}\,X\}$ (skrát. $S \vdash_{\mathrm{p}} X$), tak z S výrokovologicky vyplýva X ($S \models_{\mathrm{p}} X$).*

Dôsledok 5.19. *Nech X je výrokovologická formula. Ak existuje uzavreté tablo pre $\{\mathsf{F}\,X\}$ (skrátene $\vdash_{\mathrm{p}} X$), tak X je tautológia ($\models_{\mathrm{p}} X$).*

Spomeňte si 5.1

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

6. prednáška

Korektnosť a úplnosť výrokovologických tabiel

Rekapitulácia a plán

Minulý týždeň:

- Sformalizovali sme dôkazy sporom pomocou tabiel.
- Vyslovili, ale nedokázali tvrdenie o *korektnosti tabiel*: *uzavreté tablo* dokazuje výrokovologickú *nesplniteľnosť*
- a dôsledky pre dokazovanie vyplývania a tautológií.

Dnes:

- *Dokážeme* korektnosť tabiel.
- Preskúmame, čo vedia tablá povedať o *splniteľnosti*.
- *Dokážeme* úplnosť tabiel.

5.3 Korektnosť tabiel

Korektnosť — idea dôkazu

Aby sme dokázali korektnosť tabiel, teda vetu 5.17, dokážeme postupne dve lemy:

K1: Ak máme tablo pre splniteľnú množinu S^+ s aspoň jednou splniteľnou vetvou, tak každé jeho *priame rozšírenie* má tiež splniteľnú vetvu.

K2: Každé tablo pre splniteľnú množinu S^+ má aspoň jednu splniteľnú vetvu.

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

Korektnosť — pravdivosť priameho rozšírenia tabla

Všimnime si:

Vetva sa správa ako konjunkcia svojich označených formúl — všetky musia byť naraz pravdivé.

Tablo sa správa ako disjunkcia vetiev — niektorá musí byť pravdivá.

Definícia 5.20. Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+, nech π je vetva tabla $\mathcal{T}$ a nech v je výrokovologické ohodnotenie pre $\mathcal{L}$. Potom:

- *vetva π je pravdivá vo v* ($v \models_p \pi$) vtt vo v sú pravdivé *všetky* označené formuly vyskytujúce sa na vetve π.
- *tablo $\mathcal{T}$ je pravdivé vo v* ($v \models_p \mathcal{T}$) vtt *niektorá* vetva v table $\mathcal{T}$ je pravdivá.

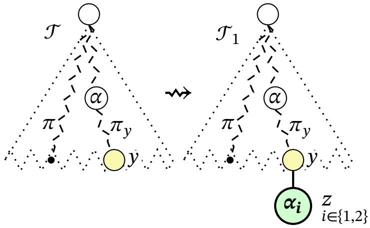
Korektnosť — pravdivosť priameho rozšírenia tabla

Pomocou predchádzajúcej definície sformulujeme lemu K1 takto:

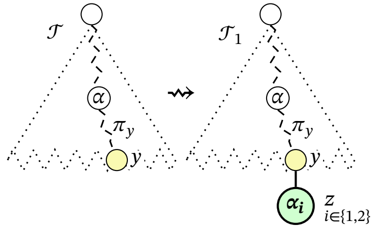
Lema 5.21 (K1). *Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+ a nech v je výrokovologické ohodnotenie pre $\mathcal{L}$. Ak S^+ a $\mathcal{T}$ sú pravdivé vo v, tak aj každé priame rozšírenie $\mathcal{T}$ je pravdivé vo v.*

Dôkaz lemy K1. Nech S^+ je množina označených formúl, $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie.Nech $v \models_p S^+$ a nech $\mathcal{T}$ je pravdivé vo v. Potom je pravdivá niektorá vetva v $\mathcal{T}$. Zoberme jednu takú vetvu a označme ju π. Nech $\mathcal{T}_1$ je priame rozšírenie $\mathcal{T}$. Nastáva jeden z prípadov:

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ pravidlom α, pridaním nového dieťaťa z nejakému listu y v $\mathcal{T}$, pričom z obsahuje α_1 alebo α_2 pre nejakú formulu α na vetve π_y.

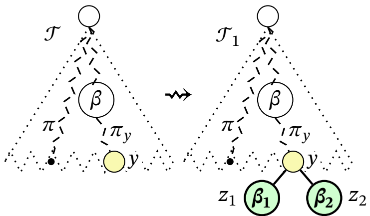


Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π, a teda aj $\mathcal{T}_1$ je pravdivé vo v.

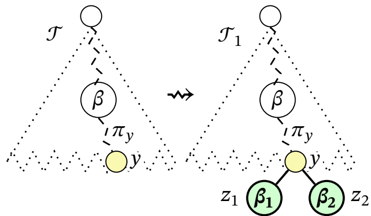


Ak $\pi = \pi_y$, tak α je pravdivá vo v, pretože α je na π. Potom aj α_1 a α_2 sú pravdivé vo v (pozorovanie 5.8). Vetva π_z v table $\mathcal{T}_1$ rozširuje vetvu π pravdivú vo v o vrchol z obsahujúci ozn. formulu α_1 alebo α_2 pravdivú vo v. Preto π_z je pravdivá vo v, a teda aj tablo $\mathcal{T}_1$ je pravdivé vo v.

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ pravidlom β, pridaním detí z_1 a z_2 nejakému listu y v $\mathcal{T}$, pričom z_1 obsahuje β_1 a z_2 obsahuje β_2 pre nejakú formulu β na vetve π_y.

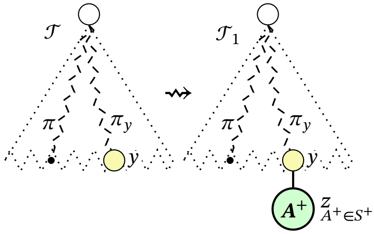


Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π, a teda aj $\mathcal{T}_1$ je pravdivé vo v.

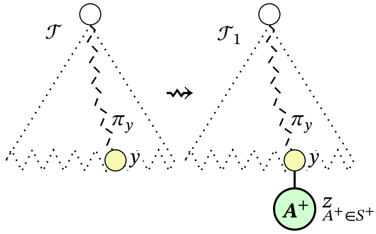


Ak $\pi = \pi_y$, tak $v \models_p \beta$, pretože β je na π. Potom $v \models_p \beta_1$ *alebo* $v \models_p \beta_2$ (poz. 5.11). Ak $v \models_p \beta_1$, tak $v \models_p \pi_{z_1}$, a teda $v \models_p \mathcal{T}_1$. Ak $v \models_p \beta_2$, tak $v \models_p \pi_{z_2}$, a teda $v \models_p \mathcal{T}_1$.

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ pravidlom S^+, pridaním nového dieťaťa z nejakému listu y v $\mathcal{T}$, pričom z obsahuje formulu $A^+ \in S^+$.



Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π, a teda aj $\mathcal{T}_1$ je pravdivé vo v.



Ak $\pi = \pi_y$, tak π_z v table $\mathcal{T}_1$ je pravdivá vo v, pretože je rozšírením vetvy π pravdivej vo v o vrchol z obsahujúci formulu A^+ pravdivú vo v (pretože $v \models_p S^+$ a $A^+ \in S^+$). Preto tablo $\mathcal{T}_1$ je pravdivé vo v. □

Korektnosť — pravdivosť množiny a tabla pre ňu

Lema 5.22 (K2)**.** *Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+ a nech v je ohodnotenie pre $\mathcal{L}$. Ak S^+ je pravdivá vo v, tak aj $\mathcal{T}$ je pravdivé vo v.*

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

Ak má $\mathcal{T}$ jediný vrchol, tento vrchol obsahuje formulu $A^+ \in S^+$, ktorá je pravdivá vo v. Preto je pravdivá 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 je $\mathcal{T}_0$ pravdivé vo v. Podľa lemy K1 je potom vo v pravdivé aj $\mathcal{T}$. □

Korektnosť — dôkaz

Dôkaz vety o korektnosti 5.17. Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+. Sporom: Predpokladajme, že existuje ohodnotenie, v ktorom je S^+ pravdivá. Označme ho v. Potom podľa lemy K2 je vo v pravdivé tablo $\mathcal{T}$, teda vo v je pravdivá niektorá vetva π v $\mathcal{T}$. Pretože $\mathcal{T}$ je uzavreté, aj vetva π je uzavretá. Na π sa teda nachádzajú označené formuly $\mathbf{T}\, X$

a $\mathbf{F}X$ pre nejakú formulu X. Pretože π je pravdivá vo v, musia byť vo v pravdivé všetky formuly na nej. Ale $v \models_p \mathbf{T}X$ vtt $v \models_p X$ a $v \models_p \mathbf{F}X$ vtt $v \not\models_p X$. Teda $\mathbf{T}X$ a $\mathbf{F}X$ nemôžu byť obe pravdivé, čo je spor. □

5.4 Testovanie nesplniteľnosti, splniteľnosti a falzifikovateľnosti

Úplná vetva a tablo

Príklad 5.23. Zistime tablom, či

$$\{((\mathsf{rychly(p)} \lor \mathsf{spravny(p)}) \land (\mathsf{citatelny(p)} \lor \mathsf{rychly(p)}))\} \models_p (\mathsf{rychly(p)} \land (\mathsf{spravny(p)} \lor \mathsf{citatelny(p)})).$$

Vybudujeme tablo pre množinu označených formúl:

$$S^+ = \{\mathbf{T}((\mathsf{rychly(p)} \lor \mathsf{spravny(p)}) \land (\mathsf{citatelny(p)} \lor \mathsf{rychly(p)})), \mathbf{F}(\mathsf{rychly(p)} \land (\mathsf{spravny(p)} \lor \mathsf{citatelny(p)}))\}$$

Podarí sa nám ho uzavrieť?

Úplná vetva a tablo

Nech v príklade tablové pravidlá používame akokoľvek,

- *nenájdeme uzavreté* tablo, ale
- ak pravidlá nepoužívame opakovane na rovnakú formulu v rovnakej vetve, po čase *vybudujeme úplné* a *otvorené* tablo.

Definícia 5.24 (Úplná vetva a úplné tablo). Nech S^+ je množina označených formúl a $\mathcal{T}$ je tablo pre S^+.

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

- pre každú označenú formulu α, ktorá sa vyskytuje na π, sa *obidve* označené formuly α_1 a α_2 vyskytujú na π;
- pre každú označenú formulu β, ktorá sa vyskytuje na π, sa *aspoň jedna* z označených formúl β_1, β_2 vyskytuje na π;
- *každá* $X^+ \in S^+$ sa vyskytuje na π.

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

Otvorené tablo a splniteľnosť

Z *otvoreného* a *úplného* tabla pre S^+ môžeme vytvoriť ohodnotenie v:

1. nájdeme otvorenú vetvu π,
2. pre každý atóm A
   - ak sa na π nachádza $\mathbf{T}\,A$, definujeme $v(A) = t$;
   - ak sa na π nachádza $\mathbf{F}\,A$, definujeme $v(A) = f$;
   - inak definujeme $v(A)$ ľubovoľne.

V tomto v je pravdivá π, a preto je v ňom *pravdivá aj* S^+ (všetky formuly z S^+ sa vyskytujú na π, lebo π je úplná).

Otázka.

- Dá sa vždy nájsť úplné tablo pre S^+?
- Naozaj sa z úplného otvoreného tabla dá vytvoriť model S^+?

Existencia úplného tabla

Lema 5.25 (o existencii úplného tabla)**.** *Nech S^+ je konečná množina označených formúl. Potom existuje úplné tablo pre S^+.*

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

Potom tablo postupne rozširujeme tak, že vyberieme ľubovoľný list y tabla $\mathcal{T}_i$, ktorého vetva π_y je otvorená a nie je úplná. Potom nastane aspoň jedna z možností:

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

Ak platí prvá alebo obe možnosti, aplikujeme pravidlo α. Ak platí druhá možnosť, aplikujeme pravidlo β. Získame tablo $\mathcal{T}_{i+1}$, s ktorým proces opakujeme.

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

5.5 Úplnosť

Nadol nasýtené množiny a Hintikkova lemma

Definícia 5.26. Množina označených formúl S^+ sa nazýva *nadol nasýtená* vtt platí:

H_0: v S^+ sa nevyskytujú naraz $\mathbf{T}\,A$ a $\mathbf{F}\,A$pre žiaden predikátový atóm A;

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

Lema 5.28 (Hintikkova)**.** *Každá nadol nasýtená množina S^+ je splniteľná.*

Dôkaz Hintikkovej lemy. Chceme dokázať, že existuje ohodnotenie v, v ktorom sú pravdivé všetky označené formuly z S^+. Definujme v pre každý predikátový atóm A takto:

$$v(A) = \begin{cases} t, & \text{ak } \mathbf{T}\,A \in S^+; \\ f, & \text{ak } \mathbf{F}\,A \in S^+; \\ t, & \text{ak ani } \mathbf{T}\,A \text{ ani } \mathbf{F}\,A \text{ nie sú v } S^+. \end{cases}$$

v je korektne definované vďaka H_0 (každému atómu priradí t alebo f, žiadnemu nepriradí obe).

Indukciou na stupeň formuly dokážeme, že vo v sú pravdivé všetky formuly z S^+:

1° Všetky označené predikátové atómy (formuly stupňa 0) z S^+ sú pravdivé vo v.

2° Nech $X^+ \in S^+$ a nech platí IP: Vo v sú pravdivé všetky formuly z S^+ nižšieho stupňa ako X^+. X^+ je buď α alebo β:

Ak X^+ je α, potom obidve $\alpha_1, \alpha_2 \in S^+$ (H_1), sú nižšieho stupňa ako X^+, a teda podľa indukčného predpokladu sú pravdivé vo v, preto (podľa poz. 5.8) je v ňom pravdivá aj α.

Ak X^+ je β, potom aspoň jedna z β_1, β_2 je v S^+ (H_2). Nech je to ktorákoľvek, má nižší stupeň ako X^+, teda podľa IP je pravdivá vo v, a preto (podľa poz. 5.11) je vo v pravdivá aj β. □

Úplnosť

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

Veta 5.29 (o úplnosti tablového kalkulu)**.** *Nech S^+ je konečná nesplniteľná množina označených formúl. Potom existuje uzavreté tablo pre S^+.*

Dôsledok 5.30. *Nech S je konečná teória a X je formula. Ak $S \models_{\mathrm{p}} X$, tak $S \vdash_{\mathrm{p}} X$.*

Dôsledok 5.31. *Nech X je formula. Ak $\models_{\mathrm{p}} X$, tak $\vdash_{\mathrm{p}} X$.*

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

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 u*zavretá* alebo ú*plná*.

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

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

7. prednáška
Korektné tablové pravidlá. DPLL

Rekapitulácia

Minulý týždeň:

- Dokázali sme korektnosť tabiel.
- Preskúmali sme, čo vedia tablá povedať o *splniteľnosti*.
- Dokázali sme úplnosť tabiel.

Tento týždeň:

- Pohodlnejšie a intuitívnejšie tablá pomocou ďalších korektných pravidiel.
- SAT solver a algoritmus DPLL.

5.6 Nové korektné pravidlá

Problémy so základnými pravidlami

Základné tablové pravidlá sú jednoduché, ľahko overiteľné a analytické — z (ne)pravdivosti zloženej formuly odvodzujú (ne)pravdivosť jej priamych podformúl.

Nie sú ale úplne pohodlné ani prirodzené, hlavne β.

Príklad 5.32. Dokážme, že pre všetky formuly A, B, C, X, Y, Z:

$$\{(A \to C), (B \to C), (C \to X), (C \to Y), ((X \land Y) \to Z)\} \vdash_{\mathrm{p}} ((A \lor B) \to Z)$$

Všimnime si:

- časté použitia pravidla β na implikáciu, kde sa jedna vetva ihneď uzavrie;
- opakovanie jedného podstromu dôkazu.

Riešenie príkladu 5.32

Tablo pre

$$S^+ = \{\mathbf{T}(A \to C), \mathbf{T}(B \to C), \mathbf{T}(C \to X), \mathbf{T}(C \to Y), \mathbf{T}((X \land Y) \to Z),$$
$$\mathbf{F}((A \lor B) \to Z)\}$$

1. $\mathbf{T}(A \to C)$ S^+
2. $\mathbf{T}(B \to C)$ S^+
3. $\mathbf{T}(C \to X)$ S^+
4. $\mathbf{T}(C \to Y)$ S^+
5. $\mathbf{T}((X \land Y) \to Z)$ S^+
6. $\mathbf{F}((A \lor B) \to Z)$ S^+
7. $\mathbf{T}(A \lor B)$ $\alpha 6$
8. $\mathbf{F}\,Z$ $\alpha 6$

- 9. $\mathbf{F}(X \land Y)\ \beta 5$
  - 10. $\mathbf{T}\,A\ \beta 7$
    - 11. $\mathbf{F}\,A\ \beta 1$ $*$ 10, 11
    - 12. $\mathbf{T}\,C\ \beta 1$
      - 13. $\mathbf{F}\,C\ \beta 3$ $*$ 12, 13
      - 14. $\mathbf{T}\,X\ \beta 3$
        - 15. $\mathbf{F}\,C\ \beta 4$ $*$ 12, 15
        - 16. $\mathbf{T}\,Y\ \beta 4$
          - 17. $\mathbf{F}\,X\ \beta 9$ $*$ 14, 17
          - 18. $\mathbf{F}\,Y\ \beta 9$ $*$ 16, 18
  - 19. $\mathbf{T}\,B\ \beta 7$
    - 20. $\mathbf{F}\,B\ \beta 2$ $*$ 19, 20
    - 21. $\mathbf{T}\,C\ \beta 2$
      - 22. $\mathbf{F}\,C\ \beta 3$ $*$ 21, 22
      - 23. $\mathbf{T}\,X\ \beta 3$
        - 24. $\mathbf{F}\,C\ \beta 4$ $*$ 21, 24
        - 25. $\mathbf{T}\,Y\ \beta 4$
          - 26. $\mathbf{F}\,X\ \beta 9$ $*$ 23, 26
          - 27. $\mathbf{F}\,Y\ \beta 9$ $*$ 25, 27
- 28. $\mathbf{T}\,Z\ \beta 5$ $*$ 8, 28

Odstránenie problémov — nové pravidlá

Keby tablový kalkul obsahoval napríklad veľmi prirodzené pravidlá *modus ponens*, *modus tolens* a *rez*:

$$\frac{\mathbf{T}(X \to Y) \quad \mathbf{T}\,X}{\mathbf{T}\,Y} \tag{MP}$$

$$\frac{\mathbf{T}(X \to Y) \quad \mathbf{F}\,Y}{\mathbf{F}\,X} \tag{MT}$$

$$\frac{}{\mathbf{T}\,X \mid \mathbf{F}\,X} \tag{cut}$$

dôkaz v príklade by sa dal sprehľadniť a odstránila by sa duplicita.

Riešenie príkladu 5.32 s modus ponens a modus tolens

1.	$\mathbf{T}(A \to C)$	S^+
2.	$\mathbf{T}(B \to C)$	S^+
3.	$\mathbf{T}(C \to X)$	S^+
4.	$\mathbf{T}(C \to Y)$	S^+
5.	$\mathbf{T}((X \land Y) \to Z)$	S^+
6.	$\mathbf{F}((A \lor B) \to Z)$	S^+
7.	$\mathbf{T}(A \lor B)$	$\alpha 6$
8.	$\mathbf{F}Z$	$\alpha 6$
9.	$\mathbf{F}(X \land Y)$	MT 5, 8

<table>
<tr><td colspan="2">10. $\mathbf{T}A$ $\beta 7$
11. $\mathbf{T}C$ MP 1, 10
12. $\mathbf{T}X$ MP 3, 11
13. $\mathbf{T}Y$ MP 4, 11</td><td colspan="2">16. $\mathbf{T}B$ $\beta 7$
17. $\mathbf{T}C$ MP 2, 16
18. $\mathbf{T}X$ MP 3, 17
19. $\mathbf{T}Y$ MP 4, 17</td></tr>
<tr><td>14. $\mathbf{F}X$ $\beta 9$
$*$ 12, 14</td><td>15. $\mathbf{F}Y$ $\beta 9$
$*$ 13, 15</td><td>20. $\mathbf{F}X$ $\beta 9$
$*$ 18, 20</td><td>21. $\mathbf{F}Y$ $\beta 9$
$*$ 19, 21</td></tr>
</table>

Riešenie príkladu 5.32 s rezom, modus ponens a modus tolens

1.	$\mathbf{T}(A \to C)$	S^+
2.	$\mathbf{T}(B \to C)$	S^+
3.	$\mathbf{T}(C \to X)$	S^+
4.	$\mathbf{T}(C \to Y)$	S^+
5.	$\mathbf{T}((X \land Y) \to Z)$	S^+
6.	$\mathbf{F}((A \lor B) \to Z)$	S^+
7.	$\mathbf{T}(A \lor B)$	$\alpha 6$
8.	$\mathbf{F}Z$	$\alpha 6$
9.	$\mathbf{F}(X \land Y)$	MT 5, 8

<table>
<tr><td colspan="2">10. $\mathbf{T}C$ cut
11. $\mathbf{T}X$ MP 3, 10
12. $\mathbf{T}Y$ MP 4, 10</td><td colspan="2">15. $\mathbf{F}C$ cut</td></tr>
<tr><td>13. $\mathbf{F}X$ $\beta 9$
$*$ 11, 13</td><td>14. $\mathbf{F}Y$ $\beta 9$
$*$ 12, 14</td><td>16. $\mathbf{T}A$ $\beta 7$
17. $\mathbf{T}C$ MP 1, 16
$*$ 15, 17</td><td>18. $\mathbf{T}B$ $\beta 7$
19. $\mathbf{F}B$ MT 2, 15
$*$ 18, 19</td></tr>
</table>

Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

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

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\alpha_2} \qquad \frac{\beta}{\beta_1 \mid \beta_2} \qquad \frac{}{A^+}\ A^+ \in S^+$$

Nech v je ľubovoľné ohodnotenie, v ktorom je pravdivá S^+. Ak je vo v pravdivá premisa, tak je vo v pravdivý aspoň jeden záver.

- Vďaka tejto vlastnosti zo splniteľnej množiny S^+ skonštruujeme iba splniteľné tablá.
- Netreba opačnú implikáciu (ak je vo v pravdivý aspoň jeden záver, tak je vo v pravdivá premisa).

Na dôkaz *úplnosti* stačili pravidlá (S^+), α, β, pretože stačia na vybudovanie úplného tabla.

Nové pravidlo

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

$$\frac{\mathbf{T}(X \to Y) \quad \mathbf{T}\,X}{\mathbf{T}\,Y} \qquad ? \tag{MP}$$

Upravíme definíciu priameho rozšírenia:

Úprava definície 5.13

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

α: $\cdots$

$\vdots$

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

Nové pravidlo vs. korektnosť a úplnosť

Korektnosť tabiel s MP:

Pri dôkaze lemy K1 (5.21)

> Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie pre $\mathcal{L}$. Ak sú S^+ a $\mathcal{T}$ pravdivé vo v, tak je vo v pravdivé aj každé priame rozšírenie tabla $\mathcal{T}$.

využijeme

Tvrdenie 5.33 (Korektnosť pravidla MP)**.** *Nech X a Y sú ľubovoľné formuly a v je ľubovoľné ohodnotenie. Ak sú vo v pravdivé* $\mathsf{T}(X \to Y)$ *a* $\mathsf{T}\,X$*, tak je vo v pravdivá* $\mathsf{T}\,Y$.

Dôkaz. Keďže $v \models_{\mathrm{p}} \mathsf{T}(X \to Y)$, tak $v \models_{\mathrm{p}} (X \to Y)$, teda $v \not\models_{\mathrm{p}} X$ alebo $v \models_{\mathrm{p}} Y$. Pretože ale $v \models_{\mathrm{p}} \mathsf{T}\,X$, tak $v \models_{\mathrm{p}} X$. Takže $v \models_{\mathrm{p}} Y$, a teda $v \models_{\mathrm{p}} \mathsf{T}\,Y$. □

Dôkaz lemy K2 (5.22) a samotnej vety o korektnosti (5.17) — bez zmeny.
Úplnosť — bez zmeny, úplné tablo vybudujú základné pravidlá.

Tablové pravidlá vo všeobecnosti — problém

Zadefinovať vo všeobecnosti, čo je pravidlo a kedy je korektné, nie je také jednoduché.

Potrebujeme zachytiť, že pravidlo:

- má premisy, ktoré *nejaký tvar* a *zdieľajú nejaké podformuly*, napr. modus tolens (MT) má premisy $\mathsf{T}(X \to Y)$ a $\mathsf{F}\,Y$;
- odvodzuje z nich závery, ktoré tiež zdieľajú podformuly s premisami, napr. $\mathsf{F}\,X$ (alebo medzi sebou v prípade rezu).

pre všetky možné zdieľané podformuly, v našom príklade X a Y.

Tablové pravidlá vo všeobecnosti — vzor

Pravidlo sa dá predstaviť nasledovne:

Pravidlo má *vzor* — dvojicu tvorenú vzormi premís a záverov, kde spoločné podformuly predstavujú *konkrétne atómy*, napr. vzor pravidla MT:

$$\frac{\mathsf{T}(\mathsf{p}(\mathsf{c}) \to \mathsf{q}(\mathsf{c})) \qquad \mathsf{F}\,\mathsf{q}(\mathsf{c})}{\mathsf{F}\,\mathsf{p}(\mathsf{c})}$$

Tablové pravidlá vo všeobecnosti — inštancia

Každý konkrétny prípad — *inštancia* pravidla vznikne *substitúciou* ľubovoľných formúl za atómy vo vzore:

$$\frac{\begin{array}{c}\mathbf{T}(\mathsf{p(c)} \to \mathsf{q(c)})_{[\mathsf{p(c)}|(\mathsf{sedan(a)} \land \mathsf{biely(a)}),\ \mathsf{q(c)}|\mathsf{kupi(B,a)}]}\\ \mathbf{F}\,\mathsf{q(c)}_{[\mathsf{p(c)}|(\mathsf{sedan(a)} \land \mathsf{biely(a)}),\ \mathsf{q(c)}|\mathsf{kupi(B,a)}]}\end{array}}{\mathbf{F}\,\mathsf{p(c)}_{[\mathsf{p(c)}|(\mathsf{sedan(a)} \land \mathsf{biely(a)}),\ \mathsf{q(c)}|\mathsf{kupi(B,a)}]}}$$

$$= \frac{\begin{array}{c}\mathbf{T}((\mathsf{sedan(a)} \land \mathsf{biely(a)}) \to \mathsf{kupi(B,a)})\\ \mathbf{F}\,\mathsf{kupi(B,a)}\end{array}}{\mathbf{F}(\mathsf{sedan(a)} \land \mathsf{biely(a)})}$$

Tablové pravidlá vo všeobecnosti — pravidlo

Samotné pravidlo je množina všetkých inštancií vzoru:

$$\mathrm{MT} = \left\{ \frac{\begin{array}{c}\mathbf{T}(\mathsf{p(c)} \to \mathsf{q(c)})_{[\mathsf{p(c)}|X,\ \mathsf{q(c)}|Y]}\\ \mathbf{F}\,\mathsf{q(c)}_{[\mathsf{p(c)}|X,\ \mathsf{q(c)}|Y]}\end{array}}{\mathbf{F}\,\mathsf{p(c)}_{[\mathsf{p(c)}|X,\ \mathsf{q(c)}|Y]}} \;\middle|\; X, Y \in \mathcal{E}_{\mathcal{L}} \right\}$$

Samozrejme, *konkrétne* pravidlo vieme zapísať aj bez substitúcie:

$$\mathrm{MT} = \left\{ \frac{\mathbf{T}(X \to Y) \quad \mathbf{F}\,Y}{\mathbf{F}\,X} \;\middle|\; X, Y \in \mathcal{E}_{\mathcal{L}} \right\}$$

Tablové pravidlá vo všeobecnosti

Definícia 5.34 (Vzor tablového pravidla)**.** Nech $n \geq 0$ a $k > 0$ sú prirodzené čísla, nech $P_1^+, \dots, P_n^+, C_1^+, \dots, C_k^+$ sú označené formuly.

Dvojicu tvorenú n-ticou $(P_1^+, \dots, P_n^+)$ a k-ticou $(C_1^+, \dots, C_k^+)$ a zapisovanú

$$\frac{P_1^+ \quad \cdots \quad P_n^+}{C_1^+ \;\big|\; \cdots \;\big|\; C_k^+}$$

nazývame *vzorom tablového pravidla*.

Označené formuly $P_1^+, \dots, P_n^+$ nazývame *vzory premís*, označené formuly $C_1^+, \dots, C_k^+$ nazývame *vzory záverov*.

Tablové pravidlá vo všeobecnosti

Definícia 5.35 (Tablové pravidlo a jeho inštancia)**.** Nech

$$\begin{array}{ccc} P_1^+ & \cdots & P_n^+ \\ \hline C_1^+ & \multicolumn{1}{|c|}{\cdots} & C_k^+ \end{array}$$

je vzor tablového pravidla a $a_1, \ldots, a_m$ sú všetky atómy, ktoré sa vyskytujú v označených formulách $P_1^+, \ldots, P_n^+, C_1^+, \ldots, C_k^+$.

Tablové pravidlo R je množina

$$R = \left\{ \begin{array}{ccc} P_1^+{}_{[a_1|X_1,\ldots,a_m|X_m]} & \cdots & P_n^+{}_{[a_1|X_1,\ldots,a_m|X_m]} \\ \hline C_1^+{}_{[a_1|X_1,\ldots,a_m|X_m]} & \multicolumn{1}{|c|}{\cdots} & C_k^+{}_{[a_1|X_1,\ldots,a_m|X_m]} \end{array} \;\middle|\; X_1,\ldots,X_m \in \mathcal{E}_{\mathcal{L}} \right\},$$

Každý prvok množiny R nazývame *inštanciou* pravidla R.

Nové pravidlá vo všeobecnosti

Keď už vieme, čo je pravidlo, môžeme povedať, kedy je korektné:

Definícia 5.36 (Tablové pravidlo a jeho korektnosť)**.** Tablové pravidlo R je *korektné* vtt pre každú inštanciu pravidla R

$$\begin{array}{ccc} P_1^+ & \cdots & P_n^+ \\ \hline C_1^+ & \multicolumn{1}{|c|}{\cdots} & C_k^+ \end{array}$$

a pre každé ohodnotenie v platí, že ak sú vo v pravdivé *všetky* premisy P_1^+, $\ldots$, P_n^+, tak je vo v pravdivý *niektorý* záver $C_1^+, \ldots, C_k^+$.

Nové pravidlá vo všeobecnosti

Úprava definície 5.13

$\ldots$

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

$\vdots$

***R*:** Ak sa pre nejakú inštanciu pravidla R

$$\frac{P_1^+ \quad \cdots \quad P_n^+}{C_1^+ \mid \cdots \mid C_k^+}$$

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

Príklad: Korektnosť rezu

To, že rez

$$\frac{}{\mathsf{T}X \mid \mathsf{F}X}$$

je korektné pravidlo, dokážeme veľmi ľahko:

Tvrdenie 5.37 (Korektnosť pravidla rezu)**.** *Nech X je ľubovoľná formula a v je ľubovoľné ohodnotenie. Potom je vo v pravdivý niektorý zo záverov pravidla rezu $\mathsf{T}X$ alebo $\mathsf{F}X$.*

Dôkaz. Formula X je vo v buď pravdivá alebo nepravdivá. V prvom prípade $v \models_p \mathsf{T}X$. V druhom prípade $v \models_p \mathsf{F}X$. Teda v oboch prípadoch platí, že vo v je pravdivý niektorý zo záverov $\mathsf{T}X$ alebo $\mathsf{F}X$ pravidla rezu. □

6 SAT a DPLL

6.1 Problém výrokovologickej splniteľnosti (SAT)

Problém SAT

Definícia 6.1 (Problém SAT)**.** *Problémom výrokovologickej splniteľnosti* (*SAT*) je problém určenia toho, či je daná množina výrokovologických formúl splniteľná.

- Zvyčajne sa redukuje na problém splniteľnosti *klauzálnej* teórie (teda formuly v CNF).

- *SAT solver* je program, ktorý rieši problém SAT.

Príklad 6.2. Nech a, b, c sú predikátové atómy. Nech $S = \{(a \lor b), (a \lor \neg b), (\neg a \lor b), (\neg a \lor \neg b \lor \neg c), (\neg a \lor c)\}$. Je množina klauzúl S splniteľná?

Tabuľková metóda

Tabuľková metóda:

- Skúma *všetky* ohodnotenia predikátových atómov
- Trvá $O(s{\cdot}2^N)$ krokov,
  - N je počet atómov a s je súčet veľkostí klauzúl
  - 2^N ohodnotení, pre každé treba zistiť, či sú všetky klauzuly pravdivé
- Zaberá priestor $O(k{\cdot}2^N)$
  - k je počet klauzúl
  - Pamätáme si (píšeme na papier) celú tabuľku
- Tabuľka slúži *aj* ako dôkaz prípadnej *ne*splniteľnosti

6.2 Naivný backtracking

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, v, c):
        return any( ( v[abs(lit)] if lit > 0 else not v[abs(lit)] )
                    for lit in c )
    def check(self, v):
        return all( self.checkClause(v, cl) for cl in self.clauses )
    def solve(self, i, v):
        if i >= self.n: # ohodnotili sme vsetky atomy
            if self.check(v):
                self.solution = v
                return True
            return False
        for b in [True, False]:
            v[i] = b
```

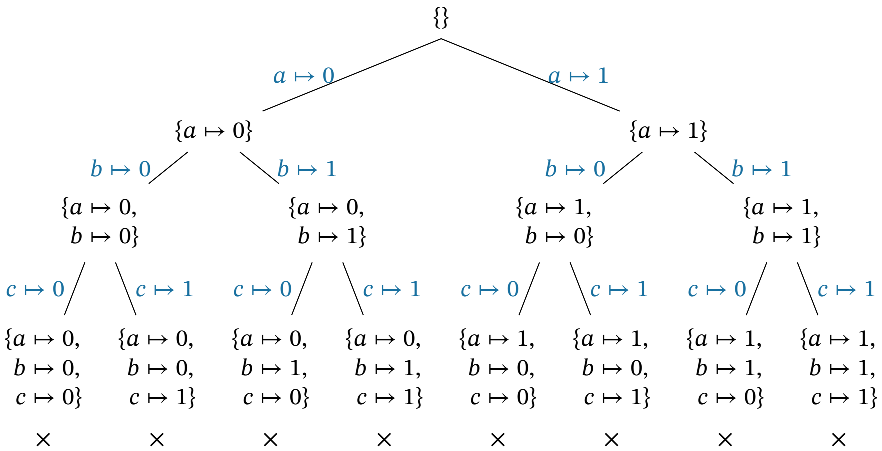
```
            if self.solve(i+1, v):
                return True
        return False
Sat(20, [[]]).solve(0, {})
```

Čas: $O(s \cdot 2^N)$, priestor: $O(s+N)$;
N — počet atómov,
s — súčet veľkostí klauzúl

Strom prehľadávania ohodnotení

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

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



6.3 Optimalizácia backtrackingu

Priebežné vyhodnocovanie klauzúl

Strom ohodnotení:

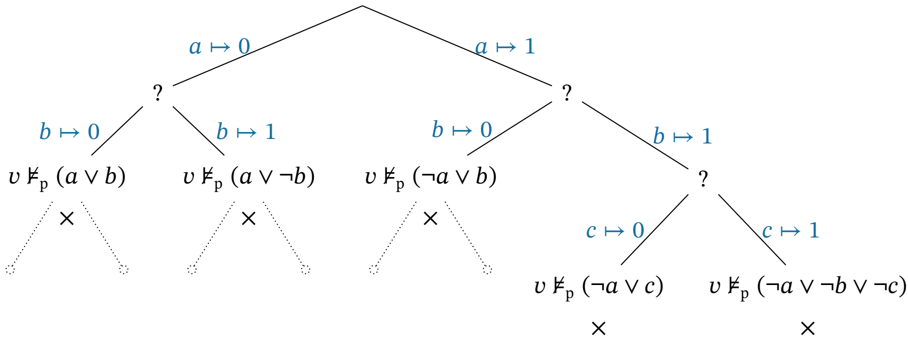
- List — ohodnotenie všetkých premenných
- Každý uzol — *čiastočné ohodnotenie*
- Ohodnotenie v uzle je *rozšírením* ohodnotenia v rodičovi
- Niektoré klauzuly sa dajú vyhodnotiť aj v čiastočnom ohodnotení
  - V čiastočnom ohodnotení $v = \{a \mapsto 0, b \mapsto 1\}$ sa dá určiť pravdivosť $(a \lor b)$, $(a \lor \neg b)$, $(\neg a \lor b)$ z našej S

- Ak nájdeme nepravdivú, môžeme hneď „backtracknúť“ — zastaviť prehľadávanie vetvy a vrátiť sa o úroveň vyššie
  - V čiastočnom ohodnotení $v = \{a \mapsto 0, b \mapsto 0\}$ je nepravdivá $(a \lor b)$ z S

Prehľadávanie s priebežným vyhodnocovaním

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

$\times$ znamená $v \nvDash_p S$? znamená zatiaľ žiadna nepravdivá klauzula



Zjednodušenie množiny klauzúl podľa literálu

Nech v je čiastočné ohodnotenie, v ktorom $v(a) = 1$.
V každom rozšírení ohodnotenia v:

- sú pravdivé klauzuly obsahujúce a
  - $\{a \mapsto 1, ...\} \vDash_p (a \lor b)$
  - $\{a \mapsto 1, ...\} \vDash_p (a \lor \neg b)$
- je pravdivá klauzula $(\ell_1 \lor \cdots \lor \neg a \lor \cdots \lor \ell_n)$ obsahujúca $\neg a$ *vtt* je pravdivá *zjednodušená* klauzulu $(\ell_1 \lor \cdots \lor \cdots \lor \ell_n)$
  - $\{a \mapsto 1, ...\} \vDash_p (\neg a \lor \neg b \lor \neg c)$ vtt $\{a \mapsto 1, ...\} \vDash_p (\neg b \lor \neg c)$

Takže množinu S môžeme *zjednodušiť*:

- klauzuly s a môžeme *vynechať*;
- klauzuly s $\neg a$ môžeme *zjednodušiť*.

Zjednodušenie množiny klauzúl podľa literálu

Množinu klauzúl

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

môžeme *zjednodušiť podľa* $a \mapsto 1$ na

$$S|_{a \mapsto 1} = \{ \quad b, \quad (\neg b \lor \neg c), \quad c \quad \}.$$

Analogicky môžeme S zjednodušiť podľa $a \mapsto 0$ na

$$S|_{a \mapsto 0} = \{ \quad b, \quad \neg b \quad \}.$$

Zjednodušenie množiny klauzúl podľa literálu

Definícia 6.3. Nech P je predikátový atóm, S je množina klauzúl, (t, f) je dvojica pravdivostných hodnôt. Potom definujeme

$$\begin{aligned} S|_{P \mapsto f} &= \{(\ell_1 \lor \cdots \lor \cdots \lor \ell_n) \mid (\ell_1 \lor \cdots \lor P \lor \cdots \lor \ell_n) \in S\} \\ &\quad \cup \{C \mid C \in S, \text{v } C \text{ sa nevyskytuje } P \text{ ani } \neg P\} \\ S|_{P \mapsto t} &= \{(\ell_1 \lor \cdots \lor \cdots \lor \ell_n) \mid (\ell_1 \lor \cdots \lor \neg P \lor \cdots \lor \ell_n) \in S\} \\ &\quad \cup \{C \mid C \in S, \text{v } C \text{ sa nevyskytuje } P \text{ ani } \neg P\} \\ S|_{\neg P \mapsto t} &= S|_{P \mapsto f} \\ S|_{\neg P \mapsto f} &= S|_{P \mapsto t} \end{aligned}$$

Tvrdenie 6.4. *Nech P je predikátový atóm, S je množina klauzúl, (t, f) dvojica pravdivostných hodnôt. Nech $b \in \{t, f\}$ a v je ohodnotenie také, že $v(P) = b$. Potom $v \models_{\mathrm{p}} S$ vtt $v \models_{\mathrm{p}} S|_{P \mapsto b}$.*

Propagácia jednotkových klauzúl

Nech $T = \{(a \lor \neg b), (a \lor b \lor c)\}$. Začnime zjednodušením podľa $a \mapsto 0$:

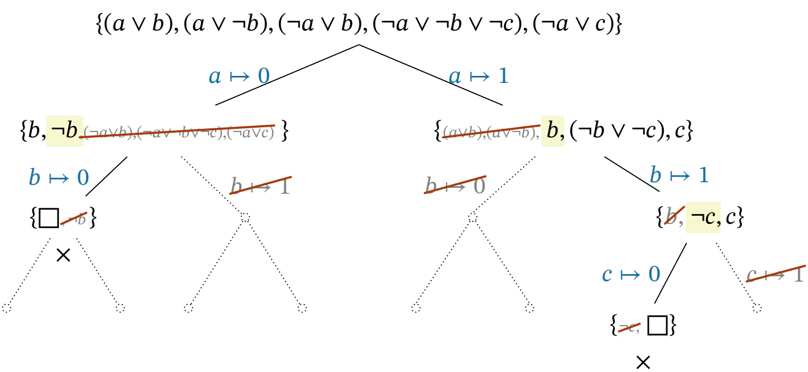
- $T' := T|_{a \mapsto 0} = \{\neg b, (b \lor c)\}$
  - $\neg b$ — *jednotková klauzula* (*unit clause* alebo iba *unit*)
  - T' spĺňajú *iba* ohodnotenia v, kde $v(b) = 0$
  - Takže T' zjednodušíme podľa $b \mapsto 0$
- $T'' := T'|_{b \mapsto 0} = \{c\}$
  - c — jednotková klauzula

  - T'' spĺňajú iba ohodnotenia v, kde $v(c) = 1$
  - Takže T'' zjednodušíme podľa c

- $T''' := T''|_{c \mapsto 1} = \{\}$ prázdna, pravdivá v hocijakom ohodnotení. Podľa tvrdenia 6.4:
  - T'' je pravdivá v každom ohodnotení, kde $v(c) = 1$.
  - T' je pravdivá v každom ohodnotení, kde $v(b) = 0$, $v(c) = 1$.
  - T je pravdivá v ohodnotení $v = \{a \mapsto 0, b \mapsto 0, c \mapsto 1\}$.

Prehľadávanie so zjednodušovaním klauzúla unit propagation

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



Eliminácia nezmiešaných literálov

Všimnime si literál u v množine klauzúl:

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

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

Nech $T' := T|_{P \mapsto 1} = \{(\neg a \vee \neg b \vee c), a, b, \neg c\}$

- Ak nájdeme ohodnotenie $v \models_p T'$, tak $v_0 := v[P \mapsto 0]$ aj $v_1 := v[P \mapsto 1]$ sú modelmi T' a v_1 je navyše modelom T, teda T je splniteľná.

- Ak je T' nesplniteľná, tak je nesplniteľná každá jej nadmnožina, teda aj T.

Z hľadiska splniteľnosti sú klauzuly obsahujúce P nepodstatné. Stačí uvažovať $T|_{P \mapsto 1}$.

Eliminácia nezmiešaných literálov

Definícia 6.5. Nech P je predikátový atóm premenná. *Komplementom literálu* P je $\neg P$. *Komplementom literálu* $\neg P$ je P.
Komplement literálu ℓ označujeme $\bar{\ell}$.

Definícia 6.6. 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 6.7. *Nech ℓ je literál a S je množina klauzúl. Ak ℓ je nezmiešaný v S, tak S je splniteľná vtt $S|_{\ell \mapsto 1}$ je splniteľná.*

6.4 DPLL a sledované literály

DPLL

Algoritmus 6.8 (Davis and Putnam [1960], Davis et al. [1962]).

def DPLL(Φ, v)**:**
    if Φ obsahuje prázdnu klauzulu**:**
        return False
    if v ohodnocuje všetky atómy**:**
        return True
    while existuje jednotková (unit) klauzula ℓ vo Φ**:**
        $\Phi, v = \text{UNIT-PROPAGATE}(\ell, \Phi, v)$
    while existuje nezmiešaný (pure) literál ℓ vo Φ**:**
        $\Phi, v = \text{PURE-LITERAL-ASSIGN}(\ell, \Phi, v)$
    $x = \text{CHOOSE-BRANCH-ATOM}(\Phi, v)$
    return DPLL($\Phi|_{x \mapsto t}, v(x \mapsto t)$) **or** DPLL($\Phi|_{x \mapsto f}, v(x \mapsto f)$)

Technika sledovaných literálov (watched literals)

Aby sme nemuseli zjednodušovať množinu klauzúl:

- Pre každú klauzulu vyberieme 2 *sledované literály*.

  $(\neg a \lor \neg b \lor \neg c)$

- Sledovaný literál musí byť *nenastavený* alebo *true*, ak sa to dá.

- Ak sa sledovaný literál stane *true*: nič nemusíme robiť.

  $\{a \mapsto 0\} \qquad (\neg a \lor \neg b \lor \neg c)$

- Ak sa sledovaný literál stane *false*: musíme nájsť iný.

  $\{a \mapsto 1\} \qquad (\neg a \lor \neg b \lor \neg c)$

  Ak iný nie je, práve sme vyrobili jednotkovú klauzulu (všetky literály okrem druhého sledovaného sú *false*),

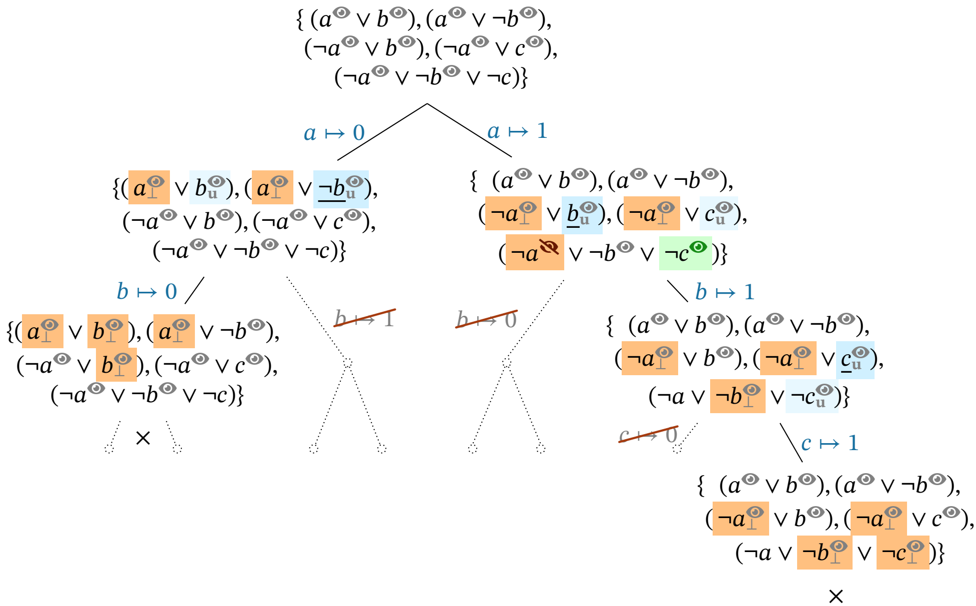
  $\{a \mapsto 1, b \mapsto 1\} \qquad (\neg a \lor \neg b_{\perp} \lor \underline{\neg c}_{\mathrm{u}})$

  alebo spor (aj druhý sledovaný je už *false*).

  $\{a \mapsto 1, b \mapsto 1, c \mapsto 0\} \qquad (\neg a_{\perp} \lor c_{\perp})$

- Keď backtrackujeme: nič nemusíme robiť (možno sa niektoré sledované literály stanú *nenastavenými*).

Prehľadávanie s unit propagation a sledovaním



SAT solver

Moderné SAT solvery:

- algoritmus DPLL: backtracking + propagácia jednotkových klauzúl;
- sledovanie literálov

\+ ďalšie techniky

Tento týždeň na praktických cvičeniach: reprezentácia klauzúl, ohodnotení, sledovanie literálov

Budúci týždeň: DPLL — propagácia jednotkových klauzúl, backtracking

Súťaž o najrýchlejší SAT solver — do konca výučby. Bonus až 6 bodov (podľa umiestnenia)

8. prednáška

Kvantifikátory

7 Kvantifikátory

7.1 Kvantifikácia

Prívlastky

Doteraz sme sa stretávali s prívlastkami, ktoré vyjadrovali vlastnosti alebo vzťahy *konkrétnych jednotlivých* objektov.

- Jurko kŕmi *veľkú Vierkinu myš* Ňufka.
  (kŕmi(Jurko, Ňufko)∧veľký(Ňufko)∧patrí(Ňufko, Vierka)∧myš(Ňufko))

Kvantifikované tvrdenia

V slovenských vetách sa ale používajú aj prívlastky ako *každý*, *nejaká*, *tri*, *tí*, *všetky*, *žiadny*, *nijaké* (gramaticky sú to zámená a číslovky).

- všetky veľké Vierkine myši; nejaké dieťa; traja muži v člne; žiadny Bratislavčan; väčšina škrečkov; tá skriňa v kúte; …

Nevyjadrujú vlastnosť konkrétnych objektov.

Vyjadrujú počet (kvantitu) objektov, ktoré majú nejaké vlastnosti alebo sú v nejakých vzťahoch.

Tvrdeniam, ktoré obsahujú tieto prívlastky, sa preto v logike *kvantifikované tvrdenia*.

Kvantifikácia a logické dôsledky

Kvantifikujúci prívlastok výrazne mení logické vlastnosti tvrdenia:

Všetky myši sú sivé. Ňufko je myš.	*Väčšina* myší je sivá. Ňufko je myš.	*Žiadne* myši nie sú sivé. Ňufko je myš.
Ňufko je sivý.	Ňufko je sivý.	Ňufko je sivý.
Je logický dôsledok.	Nie je log. dôsledkom, ale je prijateľné.	Nie je log. dôsledkom, ani prijateľné. Opak je pravdou.

Kvantifikácia sa nespráva ako funkcia na pravdivostných hodnotách — na rozdiel od logických spojok.

Vyjadruje vzťah súborov objektov (tých, ktoré sú myšami, a tých, ktoré sú sivé).

Skrytá kvantifikácia

Niektoré spojky a vzťahy implicitne vyjadrujú kvantifikáciu:

- Jurko kŕmi Ňufka, iba *keď* je noc.

  Jurko kŕmi Ňufka *vždy* v noci.

  V *každej* chvíli, v ktorej Jurko kŕmi Ňufka, je noc.
- V pondelok cvičí Klárka hru na flautu.

  V *každý* deň, ktorý je pondelkom, cvičí Klárka hru na flautu.
- Z *P logicky vyplýva Q*.

  V *každom* stave sveta, v ktorom je pravdivé P, je pravdivé aj Q.

7.2 Kvantifikátory a premenné

Kvantifikátory logiky prvého rádu

Logika prvého rádu má iba dva symboly kvantifikátorov: $\forall$ a $\exists$.

Zodpovedajú zámenám *všetko* a *niečo*.

S pomocou predikátov, výrokovologických spojok a rovnosti ale dokážu vyjadriť napr. kvantifikácie:

- všetky veľké Vierkine myši; nejaké dieťa; traja muži v člne; žiadny Bratislavčan; zakaždým, keď.

Nedokážeme však nimi vyjadriť:

- väčšina škrečkov; málo študentov; nekonečne veľa prvočísel.

Premenné

Na vyjadrenie toho, na ktoré argumenty predikátov sa vzťahuje kvantifikátor, sa používajú indivíduové premenné.

Indivíduová premenná

- môže byť argumentom predikátu, *podobne* ako indivíduová konštanta;
- neoznačuje konkrétny objekt, *na rozdiel* od indivíduovej konštanty, ale prepája argumenty predikátov, na ktoré sa vzťahuje ten istý kvantifikátor.

V každom prvorádovom jazyku s kvantifikátormi je *nekonečne veľa* premenných — väčšinou malé písmená z konca abecedy, podľa potreby s dolnými indexmi: u, v_4, w, x, y_{37}, z_{123}.

Termy a atómy

Možné argumenty predikátov a rovnosti, teda premenné a konštanty, súhrnne nazývame *termy*.

Atomickými formulami logiky prvého rádu s kvantifikátormi sú potom

- predikátové atómy $\mathit{predikát}(\mathit{term}_1, \dots, \mathit{term}_k)$, kde k je arita predikátu;
- rovnostné atómy $\mathit{term}_1 = \mathit{term}_2$.

Termy a atómy

Možné argumenty predikátov a rovnosti, teda premenné a konštanty, súhrnne nazývame *termy*.

Atomickými formulami logiky prvého rádu s kvantifikátormi sú potom

- predikátové atómy $\mathit{predikát}(\mathit{term}_1, \dots, \mathit{term}_k)$, kde k je arita predikátu;
- rovnostné atómy $\mathit{term}_1 \doteq \mathit{term}_2$.

Všeobecný kvantifikátor

Všeobecný kvantifikátor $\forall$ zodpovedá obratom *všetko*, *každý/ktorýkoľvek/akýkoľvek/hociktorý/ľubovoľný objekt*, *všetky objekty*.

Vždy *viaže* premennú uvedenú bezprostredne za ním.

Postupnosť $\forall x$ čítame *„pre každý objekt x“* (alebo trocha nepresne „pre každé x“).

Oblasť platnosti všeobecného kvantifikátora — *najkratšia ucelená* formula nasledujúca bezprostredne za viazanou premennou — vyjadruje vlastnosť, ktorú prisudzujeme všetkým objektom, napr.:

- $\forall x\,\mathrm{doma}(x)$ — Pre každý objekt x je pravda, že x je doma. (Všetko je doma.) Veta „x je doma“ je *výroková forma*, nie výrok. Jej pravdivosť sa dá jednoznačne určiť, iba keď poznáme hodnotu x.
- $\forall x(\mathrm{človek}(x) \to \mathrm{doma}(x))$ — Pre každý objekt x je pravda, že ak x je človek, tak x je doma. (Každý človek je doma.)

Existenčný kvantifikátor

Existenčný kvantifikátor $\exists$ zodpovedá obratom *niečo*, *nejaký/niektorý/akýsi/ aspoň jeden objekt*, *je/existuje taký objekt*.

Vždy *viaže* premennú uvedenú bezprostredne za ním.

Postupnosť $\exists x$ čítame *„pre nejaký objekt x“* (alebo trocha nepresne „pre nejaké x“).

Oblasť platnosti existenčného kvantifikátora — je *najkratšia ucelená* formula nasledujúca bezprostredne za viazanou premennou — vyjadruje vlastnosť, o ktorej tvrdíme, že ju má aspoň jeden objekt:

- $\exists x\,\mathrm{doma}(x)$ — Pre nejaký objekt x je pravda, že x je doma. (Niečo je doma.)
- $\exists x(\mathrm{človek}(x) \land \mathrm{doma}(x))$ — Pre nejaký objekt x je pravda, že x je človek a x je doma. (Nejaký človek je doma.)

Neexistencia

Neexistenciu v slovenčine zvyčajne vyjadruje *dvojitý zápor*: negatívne zámeno (nikto/nič/žiadne) a negatívne tvrdenie.

„Nikto nie je dokonalý“ môžeme sformalizovať

- s dôrazom na zámeno: $\neg\exists x\,\mathrm{dokonalý}(x)$;
- s dôrazom na negatívne tvrdenie: $\forall x\,\neg\mathrm{dokonalý}(x)$.

⚠ V oboch prípadoch použijeme iba jednu negáciu!

7.3 Syntax relačnej logiky prvého rádu

Symboly jazyka relačnej logiky prvého rádu

Definícia 7.1. *Symbolmi jazyka $\mathcal{L}$ relačnej logiky prvého rádu* sú:

indivíduové premenné z nejakej nekonečnej spočítateľnej množiny $\mathcal{V}_{\mathcal{L}}$;

mimologické symboly, ktorými sú

indivíduové konštanty z nejakej spočítateľnej množiny $\mathcal{C}_{\mathcal{L}}$;

predikátové symboly z nejakej spočítateľnej množiny $\mathcal{P}_{\mathcal{L}}$;

logické symboly, ktorými sú

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

symbol rovnosti $\doteq$,

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

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

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

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

Označovanie symbolov rôznych druhov

Keď budeme hovoriť o *ľubovoľnom* jazyku $\mathcal{L}$, často budeme potrebovať nejak označiť niektoré jeho konštanty alebo predikáty, aj keď nebudeme vedieť, aké konkrétne symboly to sú.

Na označenie symbolov použijeme *meta premenné*: premenné v (matematickej) slovenčine, pomocou ktorých budeme hovoriť *o* (po grécky *meta*) týchto symboloch.

Dohoda 7.2. Indivíduové premenné budeme spravidla označovať meta premennými $u, v, w, x, \ldots, z$ s prípadnými dolnými indexmi.

Indivíduové konštanty budeme spravidla označovať meta premennými a, b, c, d s prípadnými dolnými indexmi.

Predikátové symboly budeme spravidla označovať meta premennými P, Q, R s prípadnými dolnými indexmi.

Atomické formuly relačnej logiky prvého rádu

Definícia 7.3 (Term)**.** Nech $\mathcal{L}$ je jazyk relačnej logiky prvého rádu. Indivíduové premenné z $\mathcal{V}_{\mathcal{L}}$ a konštanty z $\mathcal{C}_{\mathcal{L}}$ súhrnne nazývame *termy* jazyka $\mathcal{L}$.

Definícia 7.4 (Atomické formuly)**.** Nech $\mathcal{L}$ je jazyk relačnej logiky prvého rádu.

Rovnostný atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $t_1 \doteq t_2$, kde t_1 a t_2 sú termy jazyka $\mathcal{L}$.

Predikátový atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $P(t_1, \dots, t_n)$, kde P je predikátový symbol s aritou n a $t_1, \dots, t_n$ sú termy jazyka $\mathcal{L}$.

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

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

Formuly jazyka relačnej logiky prvého rádu

Definícia 7.5. Množina $\mathcal{E}_{\mathcal{L}}$ všetkých *formúl* jazyka relačnej logiky prvého rádu $\mathcal{L}$ je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, ktorá spĺňa všetky nasledujúce podmienky:

1. Každý atóm z $\mathcal{A}_{\mathcal{L}}$ je formulou z $\mathcal{E}_{\mathcal{L}}$. Inak povedané, $\mathcal{A}_{\mathcal{L}} \subseteq \mathcal{E}_{\mathcal{L}}$.
2. Ak A patrí do $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosť symbolov $\neg A$ patrí do $\mathcal{E}_{\mathcal{L}}$ a nazývame ju *negácia* formuly A.
3. Ak A a B sú v $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosti symbolov $(A \land B)$, $(A \lor B)$ a $(A \to B)$ patria do $\mathcal{E}_{\mathcal{L}}$ a nazývame ich postupne *konjunkcia*, *disjunkcia* a *implikácia* formúl A a B.
4. Ak x je indivíduová premenná a A patrí do $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosti symbolov $\exists x\, A$ a $\forall x\, A$ patria do $\mathcal{E}_{\mathcal{L}}$ a nazývame ich postupne *existenčná* a *všeobecná kvantifikácia* formuly A vzhľadom na x.

Každý prvok A množiny $\mathcal{E}_{\mathcal{L}}$ nazývame *formulou* jazyka $\mathcal{L}$.

Príklady formúl

Príklad 7.6. Nech $\mathcal{L}$ je prvorádový jazyk, v ktorom $\mathcal{V}_{\mathcal{L}} = \{x, y, x_1, y_1, x_2, y_2, \ldots\}$, $\mathcal{C}_{\mathcal{L}} = \{\mathsf{Jurko}, \mathsf{Vierka}, \mathsf{Ňufko}\}$ $\mathcal{P}_{\mathcal{L}} = \{\mathsf{myš}^1, \mathsf{škrečok}^1, \mathsf{biely}^1, \mathsf{patrí}^2\}$.

Formulami v jazyku $\mathcal{L}$ sú napríklad: $\mathsf{myš}(\mathsf{Jurko})$, $\mathsf{myš}(x)$, $\mathsf{patrí}(y_2, \mathsf{Vierka})$, $\mathsf{patrí}(x, y)$, $(\mathsf{myš}(x) \land \mathsf{biely}(x))$,
$\exists y\, \mathsf{patrí}(x, y)$,
$\big((\mathsf{myš}(x) \land \mathsf{biely}(x)) \to \exists y\, \mathsf{patrí}(x, y)\big)$,
$\forall x\big((\mathsf{myš}(x) \land \mathsf{biely}(x)) \to \exists y\, \mathsf{patrí}(x, y)\big)$

Označovanie formúl a skratka ekvivalencie

Stále platia doterajšie dohody:

Dohoda 7.7. Formuly označujeme meta premennými A, B, C, X, Y, Z, s prípadnými dolnými indexmi.

Dohoda 7.8. Pre každú dvojicu formúl $A, B \in \mathcal{E}_{\mathcal{L}}$ je zápis $(A \leftrightarrow B)$ *skratka* za formulu $((A \to B) \land (B \to A))$.

Oblasť platnosti kvantifikátora

Dohoda 7.9. Nech $\mathcal{L}$ je ľubovoľný jazyk logiky prvého rádu. Všetky symboly, termy a formuly v nasledujúcich definíciách a tvrdeniach sú v jazyku $\mathcal{L}$.

Definícia 7.10 (Oblasť platnosti kvantifikátora)**.** Nech A je postupnosť symbolov, nech B je formula, nech $Q \in \{\forall, \exists\}$, nech x je premenná. V postupnosti $A = \ldots Q\,x\,B \ldots$ sa výskyt formuly $Q\,x\,B$ nazýva *oblasť platnosti kvantifikátora* $Q\,x$ *v* A.

Príklad 7.11. Vyznačme všetky oblasti platnosti kvantifikátora $\forall x$ vo formule

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

Riešenie. $\big((\underline{\forall x\, M(x)} \land P(x, x)) \to (\underline{\forall x(P(x, y) \land \exists y\, M(y))} \lor \forall y\, M(y))\big)$

Voľné a viazané výskyty premenných

Definícia 7.12 (Voľné a viazané výskyty premenných)**.** Nech A je postupnosť symbolov, nech x je premenná.

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

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

Príklad 7.13.

$$\begin{aligned}
\neg P(x, y) \land K(y, x)\\
\neg P(x, y) \land \exists y K(y, x)\\
\exists y(\neg P(x, y) \land K(y, x))\\
\forall \underline{x} \exists y(\neg P(\underline{x}, y) \land K(y, \underline{x}))\\
\forall \underline{x}(\neg P(\underline{x}, y) \land \exists \underline{y} K(\underline{y}, \underline{x}))
\end{aligned}$$

Voľné a viazané premenné

Definícia 7.14 (Voľné a viazané premenné)**.** Nech A je formula alebo term, nech x je premenná.

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

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

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

Príklad 7.15.

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

Voľné a viazané premenné

Tvrdenie 7.16. *Pre každú indivíduovú premennú x, každý symbol konštanty a, každú aritu $n > 0$, každý predikátový symbol P s aritou n, všetky termy t_1, t_2, …, t_n a všetky formuly A, B platí:*

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

Uzavreté formuly a teórie

Definícia 7.17 (Uzavretá formula, teória). Formula A jazyka $\mathcal{L}$ je *uzavretá* vtt žiadna premenná nie je voľná v A (teda $\mathrm{free}(A) = \emptyset$).

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

Príklad 7.18. Ktoré z týchto formúl sú uzavreté?

- $\exists x\, P(x, x)$ uzavretá,
- $\exists y\, P(x, y)$ otvorená, x je voľná,
- $\big((M(x) \land B(x)) \to \exists y\, P(x, y)\big)$ otvorená, x je voľná,
- $\forall x\big((M(x) \land B(x)) \to \exists y\, P(x, y)\big)$ uzavretá.

7.4 Sémantika relačnej logiky prvého rádu

Štruktúra

Definícia 7.19. Nech $\mathcal{L}$ je jazyk relačnej logiky prvého rádu. *Štruktúrou* pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (D, i)$, kde D je ľubovoľná *neprázdna* množina nazývaná *doména* štruktúry $\mathcal{M}$; i je zobrazenie, nazývané *interpretačná funkcia* štruktúry $\mathcal{M}$, ktoré

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

Dohoda 7.20. Štruktúry označujeme veľkými *písanými* písmenami $\mathcal{M}$, $\mathcal{N}$, ….

Ohodnotenie indivíduových premenných

Definícia 7.21. Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk $\mathcal{L}$. *Ohodnotenie indivíduových premenných* je ľubovoľná funkcia $e : \mathcal{V}_{\mathcal{L}} \to D$ (priraďuje premenným prvky domény).

Nech ďalej x je indivíduová premenná z $\mathcal{L}$ a d je prvok D. Zápisom $e(x/d)$ označíme ohodnotenie indivíduových premenných, ktoré premennej x priraďuje hodnotu d a všetkým ostatným premenným rovnakú hodnotu ako im priraďuje e, čiže $e(x/d) = e'$, kde

$$e'(y) = \begin{cases} d, & \text{ak } y = x, \\ e(y), & \text{ak } y \neq x, \end{cases}$$

alebo množinovo zapísané $e(x/d) = e \setminus \{x \mapsto e(x)\} \cup \{x \mapsto d\}$.

Príklad ohodnotenia indivíduových premenných

Nech

$$\mathcal{V}_{\mathcal{L}} = \{x_1, y_1, x_2, y_2, \ldots\}$$
$$D = \{\text{🚺}_{\text{Alica}}, \text{🚹}_{\text{Bonifác}}, \text{🚹}_{\text{Cyril}}, \text{🚺}_{\text{Eva}}, \text{🚹}_{\text{František}}\}.$$

Ohodnotením (indivíduových) premenných je napríklad

$$\begin{aligned} e = \{&x_1 \mapsto \text{🚺}_{\text{Eva}}, y_1 \mapsto \text{🚹}_{\text{Bonifác}}, x_2 \mapsto \text{🚺}_{\text{Alica}}, y_2 \mapsto \text{🚹}_{\text{Bonifác}}, \\ &x_3 \mapsto \text{🚺}_{\text{Eva}}, y_3 \mapsto \text{🚹}_{\text{Cyril}}, \ldots\} \end{aligned}$$

Potom

$$\begin{aligned} e(y_2/\text{🚺}_{\text{Alica}}) = \{&x_1 \mapsto \text{🚺}_{\text{Eva}}, y_1 \mapsto \text{🚹}_{\text{Bonifác}}, x_2 \mapsto \text{🚺}_{\text{Alica}}, y_2 \mapsto \text{🚺}_{\text{Alica}}, \\ &x_3 \mapsto \text{🚺}_{\text{Eva}}, y_3 \mapsto \text{🚹}_{\text{Cyril}}, \ldots\} \end{aligned}$$

Hodnota termov

Definícia 7.22. Nech $\mathcal{M} = (D, i)$ je štruktúra, e je ohodnotenie premenných. *Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e* je prvok $t^{\mathcal{M}}[e]$ z D určený nasledovne:

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

Splnenie atomickej formuly v štruktúre

Určenie významu *atomickej* formuly, napr. patrí(x, Vierka), v danej štruktúre, napr. $\mathcal{M} = (D, i)$, kde

$$D = \{\text{🚺}_{\text{Viera}}, \text{🚹}_{\text{Juraj}}, \text{🚺}_{\text{Eva}}, \text{🐕}, \text{🐈}, \text{🐉}, \text{🐎}, \text{🐦}, \text{🐟}, \text{🕷}\}$$

$i(\text{Vierka}) = \text{🚺}_{\text{Viera}}$, $\quad i(\text{biely}) = \{\text{🐉}, \text{🐎}, \text{🐦}\}$, $\quad i(\text{patrí}) = \{(\text{🐎}, \text{🚺}_{\text{Viera}}), (\text{🐟}, \text{🚹}_{\text{Juraj}}), (\text{🕷}, \text{🚹}_{\text{Juraj}}), (\text{🐉}, \text{🚺}_{\text{Eva}})\}$

$i(\text{Jurko}) = \text{🚹}_{\text{Juraj}}$,

$i(\text{Ňufko}) = \text{🐉}$

pri ohodnotení premenných, napr. $e = \{x \mapsto \text{🐉}, y \mapsto \text{🚺}_{\text{Eva}}, x_1 \mapsto \text{🐟}, y_1 \mapsto \text{🚺}_{\text{Viera}}, x_2 \mapsto \text{🐎}, \ldots\}$:

1. vyhodnotíme termy, ktoré sa vyskytujú vo formule:
   $x^{\mathcal{M}}[e] = e(x) = \text{🐉}$ $\qquad$ $\text{Vierka}^{\mathcal{M}}[e] = i(\text{Vierka}) = \text{🚺}_{\text{Viera}}$,
2. zistíme, či $(\text{🐉}, \text{🚺}_{\text{Viera}}) \in i(\text{patrí})$: *nie*

Štruktúra $\mathcal{M}$ ***nespĺňa*** formulu patrí(x, Vierka) **pri ohodnotení** e $\mathcal{M} \not\models \text{patrí}(x, \text{Vierka})$

Splnenie existenčne kvantifikovanej formuly

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

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

d	$e(y/d)$	$\mathcal{M} \models^{?} \text{patrí}(y, \text{Vierka})\,[e(y/d)]$
🚺$_{\text{Viera}}$	$\{x \mapsto$ 🐉, $y \mapsto$ 🚺$_{\text{Viera}}$, $x_1 \mapsto \ldots\}$	$\not\models$
$\vdots$	$\vdots$	$\vdots$
🐉	$\{x \mapsto$ 🐉, $y \mapsto$ 🐉, $x_1 \mapsto \ldots\}$	$\not\models$
🐎	$\{x \mapsto$ 🐉, $y \mapsto$ 🐎, $x_1 \mapsto \ldots\}$	$\models$
🕊	$\{x \mapsto$ 🐉, $y \mapsto$ 🕊, $x_1 \mapsto \ldots\}$	$\not\models$
$\vdots$	$\vdots$	$\vdots$
🕷	$\{x \mapsto$ 🐉, $y \mapsto$ 🕷, $x_1 \mapsto \ldots\}$	$\not\models$

2. $\mathcal{M} \models \exists y\, \text{patrí}(y, \text{Vierka})\,[e]$ vtt
   pre aspoň jedno $d \in D$ máme $\mathcal{M} \models \text{patrí}(y, \text{Vierka})\,[e(y/d)]$.
   Pravá strana je pravdivá pre $d =$ 🐎 — *svedok*.
   Takže $\mathcal{M} \models \exists y\, \text{patrí}(y, \text{Vierka})\,[e]$.

Splnenie všeobecne kvantifikovanej formuly

$\mathcal{M} \models \forall x(\text{biely}(x) \to \text{patrí}(x, y))\,[e]$ $\quad B = \text{biely}$, $P = \text{patrí}$

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

d	$\mathcal{M} \models^{?} (B(x) \to P(x, y))\,[e(x/d)]$	
🚺$_{\text{Viera}}$	$\models$	lebo $\mathcal{M} \not\models B(x)\,[e(x/d)]$
$\vdots$	$\vdots$	$\vdots$
🐈	$\models$	lebo $\mathcal{M} \not\models B(x)\,[e(x/d)]$
🐉	$\models$	lebo $\mathcal{M} \models B(x)\,[e(x/d)]$ a $\mathcal{M} \models P(x, y)\,[e(x/d)]$
🐎	$\not\models$	lebo $\mathcal{M} \models B(x)\,[e(x/d)]$ a $\mathcal{M} \not\models P(x, y)\,[e(x/d)]$
🕊	$\not\models$	lebo $\mathcal{M} \models B(x)\,[e(x/d)]$ a $\mathcal{M} \not\models P(x, y)\,[e(x/d)]$
🐟	$\models$	lebo $\mathcal{M} \not\models B(x)\,[e(x/d)]$
🕷	$\models$	lebo $\mathcal{M} \not\models B(x)\,[e(x/d)]$

2. $\mathcal{M} \models \forall x\, (\text{biely}(x) \to \text{patrí}(x, y))\, [e]$ vtt
   pre všetky $d \in D$ máme $\mathcal{M} \models (\text{biely}(x) \to \text{patrí}(x, y))\, [e(x/d)]$.
   pravá strana je nepravdivá pre $d =$ 🐎 a $d =$ 🕊 — *kontrapríklady*.
   Takže $\mathcal{M} \not\models \forall x\, (\text{biely}(x) \to \text{patrí}(x, y))\, [e]$.

Splnenie všeobecne kvantifikovanej implikácie

⚠ Naša $\mathcal{M}$ spĺňa implikáciu $(\text{biely}(x) \to \text{patrí}(x, y))$ pri $e(x/d)$ pre väčšinu $d \in D$ preto, že jej antecedent $\text{biely}(x)$ je nesplnený.

To zodpovedá čítaniu formuly $\forall x(\text{biely}(x) \to \text{patrí}(x, y))$ ako výroku „všetko biele patrí y“:

- Objekty, ktoré *nie sú biele, neovplyvňujú* pravdivosť tohto výroku ani pravdivosť implikácie $(\text{biely}(x) \to \text{patrí}(x, y))$.
- Výrok aj implikácia sú nepravdivé *iba* vtedy, keď nejaký biely objekt nepatrí y.

Ak by nič nebolo biele, teda by $\mathcal{M} \not\models \text{biely}(x)[e(x/d)]$ *pre všetky* $d \in D$, tak by aj formula $\forall x(\text{biely}(x) \to \text{patrí}(x, y))$ aj tvrdenie „všetko biele patrí y“ boli *triviálne* splnené.

Nezávislosť od ohodnotenia viazanej premennej

Pri vyhodnocovaní splnenia kvantifikovanej formuly štruktúrou pri danom ohodnotení e

$$\mathcal{M} \models \exists y\, \text{patrí}(y, \text{Vierka})\, [e]$$
$$\mathcal{M} \models \forall x (\text{biely}(x) \to \text{patrí}(x, y))\, [e]$$

nezáleží na tom, akú hodnotu priraďuje pôvodné ohodnotenie e viazanej premennej.

Priamu podformulu kvantifikovanej formuly vyhodnocujeme pri *nových* ohodnoteniach $e(y/d)$ (resp. $e(x/d)$) postupne pre všetky $d \in D$.

Splnenie formuly v štruktúre

Definícia 7.23. Nech $\mathcal{M} = (D, i)$ je štruktúra, e je ohodnotenie premenných. Relácia *štruktúra $\mathcal{M}$ spĺňa formulu A pri ohodnotení e* (skrátene $\mathcal{M} \models A[e]$) má nasledovnú induktívnu definíciu:

- $\mathcal{M} \models t_1 \doteq t_2[e]$ vtt $t_1^{\mathcal{M}}[e] = t_2^{\mathcal{M}}[e]$,
- $\mathcal{M} \models P(t_1, \dots, t_n)[e]$ vtt $\left(t_1^{\mathcal{M}}[e], \dots, t_n^{\mathcal{M}}[e]\right) \in i(P)$,
- $\mathcal{M} \models \neg A[e]$ vtt $\mathcal{M} \not\models A[e]$,
- $\mathcal{M} \models (A \land B)[e]$ vtt $\mathcal{M} \models A[e]$ a zároveň $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \lor B)[e]$ vtt $\mathcal{M} \models A[e]$ alebo $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \to B)[e]$ vtt $\mathcal{M} \not\models A[e]$ alebo $\mathcal{M} \models B[e]$,
- ▶ $\mathcal{M} \models \exists x A[e]$ vtt pre nejaký prvok $d \in D$ máme $\mathcal{M} \models A[e(x/d)]$,
- ▶ $\mathcal{M} \models \forall x A[e]$ vtt pre každý prvok $d \in D$ máme $\mathcal{M} \models A[e(x/d)]$,

pre všetky arity $n > 0$, všetky predikátové symboly P s aritou n, všetky termy $t_1, t_2, \ldots, t_n$, všetky premenné x a všetky formuly A, B.

Splnenie formuly v štruktúre pri ohodnotení · príklad

Príklad 7.24. Nech $\mathcal{M} = (D, i)$, kde
$D = \{1, 2, 3, 4, 5\}$

$i(\text{Jurko}) = 1$	$i(\text{myš}) = \{3, 4\}$	$i(\text{patrí}) = \{(3, 2),$
$i(\text{Vierka}) = 2$	$i(\text{škrečok}) = \{5\}$	$(4, 2),$
$i(\text{Ňufko}) = 4$	$i(\text{biely}) = \{4, 5\}$	$(5, 1)\}.$

Nech $e = \{x \mapsto 3, y \mapsto 5, \dots\}$.

Zistime, či

- $\mathcal{M} \models ((\text{myš}(x) \land \text{biely}(x)) \to \exists y\, \text{patrí}(x, y))\,[e]$
- $\mathcal{M} \models \forall x((\text{myš}(x) \land \text{biely}(x)) \to \exists y\, \text{patrí}(x, y))\,[e]$

Pravdivosť uzavretej formuly

Neuzavreté formuly zodpovedajú výrokovým formám. Ich splnenie v štruktúre závisí od ohodnotenia voľných premenných.

Uzavreté formuly zodpovedajú výrokom. Ich splnenie v štruktúre nezávisí od ohodnotenia. Preto pri nich môžeme hovoriť o *pravdivosti v štruktúre*.

Definícia 7.25. Nech X je *uzavretá* formula jazyka $\mathcal{L}$, nech T je teória v jazyku $\mathcal{L}$ a nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.

Formula X je *pravdivá* v štruktúre $\mathcal{M}$ (skrátene $\mathcal{M} \models X$) vtt $\mathcal{M}$ spĺňa formulu X pri každom ohodnotení e. Vtedy tiež hovoríme, že $\mathcal{M}$ je *modelom* formuly X.

Teória T je *pravdivá* v štruktúre $\mathcal{M}$ (skrátene $\mathcal{M} \models T$) vtt každá formula X z T je pravdivá v $\mathcal{M}$. Vtedy tiež hovoríme, že $\mathcal{M}$ je *modelom* teórie T.

7.5 Aristotelovské formy

Štyri aristotelovské formy

Dávno pred kodifikáciou logiky prvého rádu sa kvantifikovanými tvrdeniami zaoberal staroveký grécky filozof Aristoteles.

Študoval najmä tvrdenia v tvaroch:

- Všetky P sú Q.
- Niektoré P sú Q.
- Žiadne P nie sú Q.
- Niektoré P nie sú Q.

ktorým dnes hovoríme *obmedzená kvantifikácia*.

Všetky P sú Q

Formu „Všetky P sú Q“ (napr. „Všetky myši sú sivé“) formalizujeme

$$\forall x\,(P(x) \to Q(x))$$

teda „Pre každý objekt x je pravda, že ak x má vlastnosť P, tak x má vlastnosť Q.“, ekvivalentne „Pre každý objekt x je pravda, že x *ne*má vlastnosť P *alebo* x má vlastnosť Q.“

Študenti túto formu niekedy *nesprávne* sformalizujú ako

$$\forall x(P(x) \land Q(x))$$

Pritom táto formalizácia neprejde jednoduchou skúškou — *stačí si ju prečítať*: „*Každý* objekt x má *súčasne* vlastnosť P *aj* vlastnosť Q,“ prirodzenejšie „*Všetko* je P aj Q“ (napr. „Všetko je myš a je to sivé“).

Všetky P sú Q — varianty

Forma „Všetky P sú Q“ sa v prirodzených vetách niekedy rozpoznáva ťažšie, napríklad keď je P alebo Q vzťah:

- Všetky myši kŕmi Jurko.
  Všetky myši sú také, že ich kŕmi Jurko.
  $\forall x(\text{myš}(x) \to \text{kŕmi}(\text{Jurko}, x))$

- Jurko kŕmi *iba* myši.
  Všetko, čo Jurko kŕmi, sú myši.
  $\forall x(\text{kŕmi}(\text{Jurko}, x) \to \text{myš}(x))$.

Niektoré P sú Q

Formu „Niektoré P sú Q“ (napr. „Niektoré myši sú biele“) formalizujeme

$$\exists x\, (P(x) \land Q(x))$$

teda „Existuje aspoň taký jeden objekt x, že x má vlastnosť P a x má vlastnosť Q.“

Študenti túto formu niekedy *nesprávne* sformalizujú ako

$$\exists x(P(x) \to Q(x))$$

Ani táto formalizácia neprejde čítacou skúškou: „Existuje objekt x, ktorý nemá vlastnosť P alebo má vlastnosť Q.“ prirodzenejšie „Niečo nie je P alebo je Q“ (napr. „Niečo nie je myš alebo je to biele“ — je pravdivé vo svete, kde sú všetky myši sivé a je tam jeden človek).

Niektoré P sú Q — varianty

Forma „Niektoré P sú Q“ sa v prirodzených vetách niekedy rozpoznáva ťažšie, napríklad keď je P alebo Q vzťah.

- Jurko kŕmi nejaké myši.
  Jurko kŕmi (nejakú) myš.
  Niečo z toho, čo Jurko kŕmi, sú myši.
  $\exists x(\text{kŕmi}(\text{Jurko}, x) \land \text{myš}(x))$

Niektorých študentov prekvapuje, že pri tejto forme nezáleží na poradí P a Q.

- Nejaké myši kŕmi Jurko.
  Niektoré myši sú také, že ich kŕmi Jurko.
  $\exists x(\text{kŕmi}(\text{Jurko}, x) \land \text{myš}(x))$

Je ale *vernejšie* poradie pri formalizácii zachovať:
$\exists x(\text{myš}(x) \land \text{kŕmi}(\text{Jurko}, x))$

Žiadne P nie sú Q

Formu „Žiadne P nie sú Q“ (napr. „Žiadne myši nie sú červené“) formalizujeme (s dôrazom na „nie sú Q“)

$$\forall x\,(P(x) \to \neg Q(x))$$

teda „Pre každý objekt x je pravda, že ak x má vlastnosť P, tak x nemá vlastnosť Q,“ „Každé P nie je Q,“
alebo rovnako správne (s dôrazom na „žiadne“)

$$\neg\,\exists x\,(P(x) \land Q(x))$$

teda „Nie je pravda, že existuje taký objekt x, že x má vlastnosť P a x má vlastnosť Q.“

Ani pri tejto forme nezáleží na poradí P a Q, ale je *vernejšie* ho pri formalizácii zachovať.

Niektoré P nie sú Q

Formu „Niektoré P nie sú Q“ (napr. „Niektoré myši nie sú sivé“) formalizujeme

$$\exists x(P(x) \land \neg Q(x))$$

teda „Pre nejaký objekt x je pravda, že x má vlastnosť P a x nemá vlastnosť Q.“

7.6 Zamlčané a zdanlivo opačné kvantifikátory

Zamlčaný všeobecný kvantifikátor

Niekedy kvantifikátor nie je explicitne vyjadrený príslušným zámenom.

Použitie všeobecného podstatného mena (zvyčajne, ale nie nutne v množnom čísle) v úlohe *podmetu* zvyčajne chápeme ako *všeobecnú* kvantifikáciu:

- Myši sú sivé.
  $\forall x(\text{myš}(x) \to \text{sivý}(x))$
- Myš je hlodavec.
  $\forall x(\text{myš}(x) \to \text{hlodavec}(x))$
- Kto je zodpovedný, ten je doma.
  $\forall x(\text{zodpovedný}(x) \to \text{doma}(x))$

Zamlčaný existenčný kvantifikátor

Použitie všeobecného podstatného mena v úlohe *predmetu pozitívneho* prísudku zvyčajne chápeme ako *existenčnú* kvantifikáciu:

- Jurko kŕmi myš. $\exists x(\text{kŕmi}(\text{Jurko}, x) \land \text{myš}(x))$
- Bonifác si kúpil syr. $\exists x(\text{kúpil}(\text{Bonifác}, x) \land \text{syr}(x))$

Zamlčaná neexistencia

Použitie všeobecného podstatného mena v úlohe *predmetu negatívneho* prísudku zvyčajne chápeme ako vyjadrenie *neexistencie*:

- Bonifác si nekúpil syr.
  $\neg\exists x(\text{kúpil}(\text{Bonifác}, x) \land \text{syr}(x))$
  $\forall x(\text{kúpil}(\text{Bonifác}, x) \to \neg\text{syr}(x))$

- Jurko nekŕmi myši.
  $\forall x(\mathrm{myš}(x) \to \neg\mathrm{kŕmi}(\mathrm{Jurko}, x))$
  $\forall x(\mathrm{kŕmi}(\mathrm{Jurko}, x) \to \neg\mathrm{myš}(x))$
  $\neg \exists x(\mathrm{kŕmi}(\mathrm{Jurko}, x) \land \mathrm{myš}(x))$

Zdanlivá existencia

V podmienkach sa občas vyskytujú neurčité zámená (niekto/niečo/niektorý/ …), na ktoré sa ale odkazujeme v podmienenej vete:

- Ak je *niekto* doma, tak (on) je zodpovedný.
- Ak Jurko *niečo* kŕmi, má *to* rád.

Také tvrdenie nezodpovedá implikácii s existenčným kvantifikátorom:

✖ $(\exists x\, \mathrm{doma}(x) \to \mathrm{zodpovedný}(x))$

✖ $\exists x(\mathrm{doma}(x) \to \mathrm{zodpovedný}(x))$

ale zodpovedá *všeobecne kvantifikovanej implikácii*:

✔ $\forall x(\mathrm{doma}(x) \to \mathrm{zodpovedný}(x))$

✔ $\forall x(\mathrm{kŕmi}(\mathrm{Jurko}, x) \to \mathrm{má\_rád}(\mathrm{Jurko}, x))$

7.7 Nutné a postačujúce podmienky

Nutné a postačujúce podmienky

Tvrdenia so (zamlčanou) všeobecnou kvantifikáciou majú často formu podraďovacích súvetí:

1. Zodpovedný je *každý, kto* je doma.
2. Zodpovedný je *iba ten, kto* je doma.

pričom

- hlavná veta („Zodpovedný je … “) vyjadruje nejakú *vlastnosť*,
- vedľajšia veta („kto je doma“) vyjadruje *podmienku*, ktorá súvisí s touto vlastnosťou.

Aký je rozdiel medzi týmito podmienkami?

Postačujúca podmienka

Prvé tvrdenie „Zodpovedný je *každý, kto* je doma.“:

- Hovorí, že na to, aby niekto bol zodpovedný, *stačí*, aby platila podmienka, že je doma.
- Inak povedané: Nie je možné, aby bol niekto doma, ale považovali sme ho za nezodpovedného.
- Byť doma je teda *postačujúcou* podmienkou zodpovednosti.
- Ekvivalentne: „Pre každého platí, že je zodpovedný, ak je doma.“ „Pre každého platí, že ak je doma, tak je zodpovedný.“
- Formalizácia je teda $\forall x(\mathsf{doma}(x) \to \mathsf{zodpovedný}(x))$

Nutná podmienka

Druhé tvrdenie „Zodpovedný je *iba ten, kto* je doma.“:

- Hovorí, že na to, aby niekto bol zodpovedný, je *nevyhnutné* aby bol doma.
- Inak povedané: Keby niekto nebol doma, nebol by zodpovedný. Nie je možné, aby bol niekto zodpovedný, ale nebol doma.
- Byť doma je teda *nutnou* podmienkou zodpovednosti.
- Ekvivalentne: „Pre každého platí, že je zodpovedný, *iba* ak je doma.“ „Pre každého platí, že ak *nie* je doma, tak *nie* je zodpovedný.“ „Pre každého platí, že ak je zodpovedný, tak je doma.“
- Formalizácia je teda $\forall x(\mathsf{zodpovedný}(x) \to \mathsf{doma}(x))$

7.8 Zložené kvantifikované vlastnosti

Zložené kvantifikované vlastnosti

Často potrebujeme kvantifikovať objekty, ktoré majú zložité vlastnosti:

1. nejaká Jankina biela myš,

2. každý biely potkan, ktorého kŕmi Jurko.

Prvý druh kvantifikácií je zrejme existenčný a už vieme, že sa spravidla spája s konjunkciou.

Druhý druh kvantifikácií je zrejme všeobecný a vieme, že sa spravidla spája s implikáciou.

Použitie spojok ale závisí od pozície kvantifikácie vo vete.

Zložené existenčne kvantifikované vlastnosti ako podmet

(Nejaká) Jankina biela myš je sýta.

- Veta má formu „Niektoré P sú Q," teda prekladáme ju ako $\exists x(P(x) \land Q(x))$. Pričom ale *$P$ je zložená* vlastnosť.
- Vlastnosť P opisuje objekt, ktorý má zrejme byť súčasne Jankin, biely a má to byť myš. Preto P vytvoríme z jednotlivých predikátov konjunkciou.

$$\exists x\big((\text{patrí}(x, \text{Janka}) \land \text{biely}(x) \land \text{myš}(x)) \land \text{sýty}(x)\big)$$

Zložené všeobecne kvantifikované vlastnosti ako podmet

(Všetky) Jankine biele myši sú sýte.

- Veta má formu „Všetky P sú Q," teda prekladáme ju ako $\forall x(P(x) \to Q(x))$, pričom *P je zložená* vlastnosť.
- Vlastnosť P opäť opisuje objekty, ktoré majú byť súčasne Jankine, biele a myši. Preto aj teraz P vytvoríme konjunkciou.

$$\forall x\big((\text{patrí}(x, \text{Janka}) \land \text{biely}(x) \land \text{myš}(x)) \to \text{sýty}(x)\big)$$

Zložené existenčne kvantifikované vlastnosti ako predmet

Jurko má (nejakú) sýtu bielu myš.

- Aby sme zistili, ktorú aristotelovskú formu má veta, musíme ju preformulovať:
  (Nejaká) sýta biela myš je Jurkova.

- Veta má formu „Niektoré P sú Q," teda prekladáme ju ako $\exists x(P(x) \land Q(x))$, pričom P je zložená vlastnosť.

$$\exists x\big((\text{sýty}(x) \land \text{myš}(x) \land \text{biely}(x)) \land \text{patrí}(x, \text{Jurko})\big)$$

Zložené všeobecne kvantifikované vlastnosti ako predmet

Jurko má všetky sýte biele myši.

- Aj túto vetu musíme preformulovať:
  Všetky sýte biele myši sú Jurkove.
- Veta má formu „Všetky P sú Q," teda prekladáme ju ako $\forall x(P(x) \to Q(x))$. pričom P je zložená vlastnosť.

$$\forall x\big((\text{sýty}(x) \land \text{biely}(x) \land \text{myš}(x)) \to \text{patrí}(x, \text{Jurko})\big)$$

Viacnásobné všeobecne kvantifikované prívlastky

Jurko má všetky myši a škrečky.

- Preformulujeme: Všetky myši a škrečky sú Jurkove.
- Veta má formu „Všetky P sú Q," teda prekladáme ju ako $\forall x(P(x) \to Q(x))$.
- P je zložená vlastnosť. *Ale ako* je zložená?

✗ Keď „myši a škrečky" sformalizujeme $(\text{myš}(x) \land \text{škrečok}(x))$, $\forall x(P(x) \to Q(x))$ bude znamenať „Pre každé x, ak x je myš a zároveň x je škrečok, tak x patrí Jurkovi."

- Vieme ale, že nič nie je naraz myš aj škrečok, takže podmienke (v našom svete) nevyhovuje žiaden objekt, takže Jurkovi nemusí nič patriť.

✓ Intuitívny význam zachováme, keď „myši a škrečky" sformalizujeme $(\text{myš}(x) \lor \text{škrečok}(x))$.

$$\forall x\big((\text{myš}(x) \lor \text{škrečok}(x)) \to \text{patrí}(x, \text{Jurko})\big)$$

7.9 Konverzačné implikatúry

Triviálne pravdivé všeobecne kvantifikované implikácie

Nie všetkým sa zdá intuitívne, že formula

$$\forall x(\text{myš}(x) \to \text{biela}(x))$$

je *pravdivá* vo svetoch, kde *nie sú žiadne myši*.

Dobrý spôsob, ako to pochopiť je, že uvedomiť si, že vo svete, kde nie sú myši, *neexistuje kontrapríklad* pre túto formulu — myš, ktorá by nebola biela.

Hovoríme, že v takom svete je táto formula *triviálne pravdivá*.

Podobne je vo svetoch bez myší triviálne pravdivá ešte prekvapujúcejšia formula:

$$\forall x(\text{myš}(x) \to \text{človek}(x))$$

Triviálne pravdivé všeobecne kvantifikované implikácie

Tvrdenie „Každý prvák, ktorý si zapísal logiku, z nej dostal A," v sebe nesie implikatúru (domnelý dôsledok), že takí prváci existujú.

Ak je takéto tvrdenie nutne triviálne pravdivé, lebo objekty z predpokladu neexistujú (napr. prváci si logiku nemôžu zapisovať), intuitívne ho považujeme zavádzajúce.

Nič to ale nemení na fakte, že je pravdivé.

Existencia prváka, ktorý si zapísal logiku je skutočne iba implikatúra.

Dodatok „Ale žiadny prvák si ju nikdy nezapísal" (negácia implikatúry), nie je s tvrdením v spore, ale objasňuje, že je triviálne pravdivé.

„Niektoré" neimplikuje „nie všetky"

Ďalšia implikatúra sa spája s tvrdeniami: „Niektoré *P* sú *Q*."

Niekomu sa môže „Niektoré *P* sú *Q*" zdať sporné s „Všetky *P* sú *Q*." — Prečo by sme hovorili „niektoré *P*", keď to platí pre všetky *P*? Takýto človek považuje tvrdenie „Nie všetky *P* sú *Q*" za dôsledok tvrdenia „Niektoré *P* sú *Q*". Aj to je však iba implikatúra.

Keď ale na otázku „Dostal niekto Áčko?" odpovieme „Áno, niektorí študenti Áčko dostali. *Vlastne ho dostali všetci,*" druhá veta prvú dopĺňa, ale neprotirečí jej, hoci je negáciou implikatúry.

Ak chceme jasne vyjadriť domnelý význam, povieme „Niektorí študenti Ačko dostali*, ale nie všetci*," čo formalizujeme formulou v tvare $(\exists x(P(x) \land Q(x)) \land \neg \forall x(P(x) \rightarrow Q(x)))$.

9. prednáška

Tablá pre kvantifikátory. Viackvantifikátorové tvrdenia

8 Tablá s kvantifikátormi

8.1 Logické vlastnosti a vzťahy v logike prvého rádu

Logické vlastnosti a vzťahy v logike prvého rádu

Minulý týždeň sme zadefinovali, kedy je *uzavretá* formula a teória (množina uzavretých formúl) *pravdivá* v danej štruktúre ($\mathcal{M} \models A$, $\mathcal{M} \models T$).

Použili sme pomocný induktívne definovaný vzťah *štruktúra spĺňa formulu pri ohodnotení* ($\mathcal{M} \models X[e]$). Je definovaný pre *všetky* formuly (otvorené aj uzavreté).

Pomocou štruktúr a pravdivosti môžeme pre relačnú logiku prvého rádu skonkretizovať *logické vlastnosti a vzťahy*, ktoré už poznáme z výrokovologickej časti logiky prvého rádu:

- splniteľnosť a nesplniteľnosť,
- „vždy pravdivé“ formuly (vo výrokovom prípade sa volali tautológie),
- vyplývanie/logický dôsledok.

Splniteľnosť a nesplniteľnosť

Ako sme sa dohodli minule, predpokladáme, že sme si pevne zvolili ľubovoľný jazyk relačnej logiky prvého rádu $\mathcal{L}$. Všetky definície platia pre symboly, termy, atómy, formuly, teórie, atď. v tomto jazyku a štruktúry a ohodnotenia indivíduových premenných pre tento jazyk. Pretože $\mathcal{L}$ je ľubovoľný, dajú sa definície aplikovať na všetky jazyky relačnej logiky prvého rádu.

Definícia 8.1. Nech X je uzavretá formula a T je teória. Formula X je *prvorádovo splniteľná* vtt X je pravdivá v *nejakej* štruktúre (ekvivalentne: *existuje* štruktúra $\mathcal{M}$ taká, že $\mathcal{M} \models X$). Teória T je *prvorádovo splniteľná* vtt T má model (ekvivalentne: T je pravdivá v *nejakej* štruktúre; *existuje* štruktúra $\mathcal{M}$ taká, že $\mathcal{M} \models T$).

Formula resp. teória je *prvorádovo nesplniteľná* vtt nie je prvorádovo splniteľná.

Splniteľnosť — príklad

Príklad 8.2. Teória $\{\forall x(\text{človek}(x) \lor \text{myš}(x)), \forall x(\text{človek}(x) \to \neg\text{myš}(x))\}$ je prvorádovo *splniteľná*.

Je to tak preto, že je *pravdivá v štruktúre* (teda jej modelom je) $\mathcal{M} = (D, i)$, kde $D = \{1, 2\}$, $i(\text{človek}) = \{1\}$ a $i(\text{myš}) = \{2\}$.

Samozrejme je pravdivá v mnohých iných štruktúrach.

Platné formuly

Formulám, ktoré sú výrokovologicky pravdivé (pravdivé v každom výrokovologickom ohodnotení atómov), sme hovorili tautológie.

Pre formuly, ktoré sú prvorádovo pravdivé (pravdivé v každej štruktúre), sa používa iný pojem:

Definícia 8.3. Nech X je uzavretá formula. Formula X je *platná* (skrátene $\models X$) vtt X je pravdivá v *každej* štruktúre (teda pre *každú* štruktúru $\mathcal{M}$ máme $\mathcal{M} \models X$).

Samozrejme, formula *nie je platná* vtt je nepravdivá *v aspoň jednej* štruktúre.

Platnosť sa ale *nedá overiť vymenovaním* všetkých štruktúr, lebo tých je nekonečne veľa.

Platné formuly — príklad

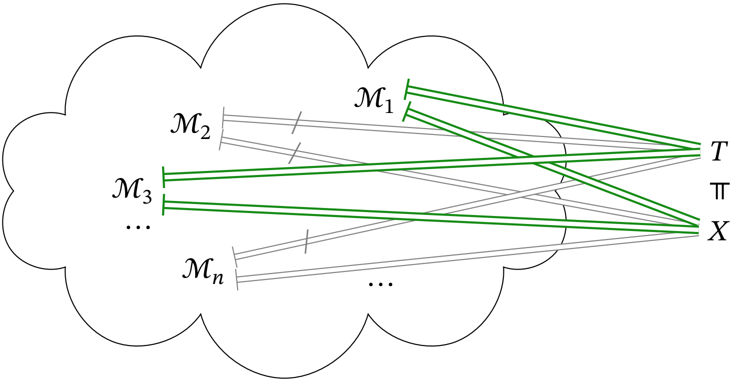
Príklad 8.4. Formula $X = (\forall x\, \text{doma}(x) \to \text{doma}(\text{Jurko}))$ je platná.

Predpokladajme, že by X nebola platná, teda by bola nepravdivá v nejakej štruktúre $\mathcal{M} = (D, i)$. Potom by v $\mathcal{M}$ bol pravdivý antecedent $\forall x\, \text{doma}(x)$, ale nepravdivý konzekvent doma(Jurko), teda $i(\text{Jurko}) \notin i(\text{doma})$. Ak je ale pravdivé $\forall x\, \text{doma}(x)$, tak pre každé $m \in D$ máme $m \in i(\text{doma})$. Preto aj $i(\text{Jurko}) \in i(\text{doma})$, čo je spor.

Preto X je platná.

Prvorádové vyplývanie, prvorádový logický dôsledok

Definícia 8.5. Z teórie T *prvorádovo logicky vyplýva* uzavretá formula X (tiež X je *prvorádovým logickým dôsledkom* T, skrátene $T \vDash X$) vtt X je pravdivá v každom modeli T (ekvivalentne podrobnejšie: pre každú štruktúru $\mathcal{M}$ platí, že ak je v $\mathcal{M}$ pravdivá T, tak je v $\mathcal{M}$ pravdivá X).



Prvorádové vyplývanie — príklad

Prvorádové vyplývanie sa *nedá overiť vymenovaním* všetkých štruktúr, rovnako ako platnosť.

Príklad 8.6. Z teórie $T = \{\forall x(\text{kŕmi}(\text{Jurko}, x) \to \text{škrečok}(x)),$
$\neg\text{škrečok}(\text{Ňufko})\}$
prvorádovo vyplýva $X = \neg\text{kŕmi}(\text{Jurko}, \text{Ňufko})$.

Presvedčíme sa o tom podobnou úvahou ako v príklade platnej formuly.

Prvorádové nevyplývanie a príklad

Samozrejme, formula X *nevyplýva* z teórie T vtt X nie je pravdivá v *aspoň jednom* modeli T. Tento model je *kontrapríkladom* vyplývania.

Príklad 8.7. Z teórie $T = \{\neg \exists x\, \text{väčší}(\text{Chrumko}, x),$
$\neg \exists x\, \text{väčší}(x, \text{Ňufko}),$
$\text{väčší}(\text{Belka}, \text{Fúzik})\}$
prvorádovo nevyplýva $X = \text{väčší}(\text{Ňufko}, \text{Chrumko})$.

Napríklad štruktúra $\mathcal{M} = (D, i)$, kde $D = \{1, 2, 3, 4\}$, $i(\text{Chrumko}) = 1$, $i(\text{Ňufko}) = 2$, $i(\text{Belka}) = 3$, $i(\text{Fúzik}) = 4$, $i(\text{väčší}) = \{(3, 4), (4, 3)\}$, je kontrapríkladom toho, že $T \vDash X$, pretože $\mathcal{M} \vDash T$, ale $\mathcal{M} \nvDash X$.

Výrokovologické, prvorádové a logické vyplývanie

Podobne ako výrokovologické vyplývanie, aj prvorádové vyplývanie je *špeciálny prípad* logického vyplývania v prirodzenom jazyku.

Logické vyplývanie v prirodzenom jazyku je *bohatšie* ako prvorádové vyplývanie. Tvrdenie zodpovedajúce formule X logicky vyplýva z tvrdení v T — keď rozumieme vzťahu „väčší“.

Logika prvého rádu ale „nevidí“ význam predikátov. Pozerá sa na ne len pomocou formúl, v ktorých vystupujú.

Dohoda 8.8. Nateraz budeme *stručne ale nepresne* hovoriť „logický dôsledok“ a „vyplývanie“ namiesto „prvorádový logický dôsledok“ a „prvorádové logické vyplývanie“.

Viac o vzťahu výrokovologického, prvorádového a logického vyplývania neskôr.

Platnosť a vyplývanie

Medzi platnými formulami a prvorádovým vyplývaním je podobný vzťah ako medzi tautológiami a výrokovologickým vyplývaním.

Tvrdenie 8.9. *Nech X je uzavretá formula. Nasledujúce tvrdenia sú vzájomne ekvivalentné:*

- *X je platná ($\models X$);*
- *X vyplýva z prázdnej teórie ($\emptyset \models X$);*
- *X vyplýva z každej teórie (pre každú teóriu T máme $T \models X$).*

Tvrdenie 8.10. *Nech $T = \{A_1, \ldots, A_n\}$ je konečná teória a nech X je uzavretá formula. Nasledujúce tvrdenia sú vzájomne ekvivalentné:*

- *formula $(\bigwedge_{i=1}^{n} A_i \to X)$ je platná (t.j., $\models (\bigwedge_{i=1}^{n} A_i \to X)$);*
- *X vyplýva z teórie T (t.j., $T \models X$).*

8.2 Dokazovanie s kvantifikátormi

Dôkazy a tablá pre logiku prvého rádu

Dôkazy s kvantifikovanými formulami sformalizujeme pomocou rozšírenia tabiel na logiku prvého rádu.

Tablá budú obsahovať označené formuly prvého rádu.

V tablách dovolíme aj *otvorené* formuly.

Tablové pravidlá budú zachovávať splniteľnosť tabla.

Označené formuly logiky prvého rádu

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

Definícia 8.11. Nech $\mathcal{M}$ je štruktúra, e je ohodnotenie indivíduových premenných a X je formula. Potom

- *$\mathcal{M}$ spĺňa označenú formulu* $\mathbf{T}\,X$ pri ohodnotení e vtt $\mathcal{M}$ spĺňa formulu X pri ohodnotení e, skrátene: $\mathcal{M} \models \mathbf{T}\,X[e]$ vtt $\mathcal{M} \models X[e]$;
- *$\mathcal{M}$ spĺňa označenú formulu* $\mathbf{F}\,X$ pri ohodnotení e vtt $\mathcal{M}$ *ne*spĺňa formulu X pri ohodnotení e, skrátene: $\mathcal{M} \models \mathbf{F}\,X[e]$ vtt $\mathcal{M} \not\models X[e]$.

$\mathcal{M}$ spĺňa množinu označených formúl S^+ pri ohodnotení e vtt $\mathcal{M}$ spĺňa *každú* označenú formulu A^+ z S^+ pri ohodnotení e, skrátene: $\mathcal{M} \models S^+[e]$ vtt pre každú $A^+ \in S^+$ máme $\mathcal{M} \models A^+[e]$.

Splniteľnosť označených formúl a ich množín

Definícia 8.12 (Splniteľnosť označených formúl a ich množín)**.** Ozn. formula X^+ je *splniteľná* vtt pre nejakú štruktúru $\mathcal{M}$ a nejaké ohodnotenie indivíduových premenných e máme $\mathcal{M} \models X^+[e]$.

Množina ozn. formúl S^+ je *splniteľná* vtt pre nejakú štruktúru $\mathcal{M}$ a nejaké ohodnotenie indivíduových premenných e máme $\mathcal{M} \models S^+[e]$.

Dôkaz s pozitívnou všeobecnou kvantifikáciou

Príklad 8.13. Dokážme neformálne, že z teórie $T = \{\forall x(\text{kŕmi}(\text{Jurko}, x) \to \text{škrečok}(x)), \neg\text{škrečok}(\text{Ňufko})\}$ prvorádovo vyplýva $X = \neg\text{kŕmi}(\text{Jurko}, \text{Ňufko})$.

Sporom: Nech sú formuly (1) $\forall x(\text{kŕmi}(\text{Jurko}, x) \to \text{škrečok}(x))$ a (2) $\neg\text{škrečok}(\text{Ňufko})$ pravdivé v nejakej štruktúre. Predpokladajme, že (3) $\neg\text{kŕmi}(\text{Jurko}, \text{Ňufko})$ by v nej bola nepravdivá.

Potom (4) kŕmi(Jurko, Ňufko) je pravdivá. Navyše (5) škrečok(Ňufko) je nepravdivá. Pretože podľa prvého predpokladu (1) je formula $(\text{kŕmi}(\text{Jurko}, x) \to \text{škrečok}(x))$ splnená pre každý objekt x, musí byť splnená aj pre objekt označený konštantou Ňufko. Teda *(6)* $(\text{kŕmi}(\text{Jurko}, \text{Ňufko}) \to \text{škrečok}(\text{Ňufko}))$ *je pravdivá*. Pretože už vieme (4), že ľavá strana je pravdivá, musí byť pravá strana (7) škrečok(Ňufko) tiež pravdivá. To je ale v spore so skorším zistením (5), že táto formula je nepravdivá. □

Tablo pre dôkaz

Na väčšinu krokov v predchádzajúcom dôkaze stačia doterajšie tablové pravidlá.

1.	**T** $\forall x(\text{kŕmi}(\text{Jurko}, x) \to \text{škrečok}(x))$	S^+
2.	**T** $\neg\text{škrečok}(\text{Ňufko})$	S^+
3.	**F** $\neg\text{kŕmi}(\text{Jurko}, \text{Ňufko})$	S^+
4.	**T** kŕmi(Jurko, Ňufko)	$\alpha 3$
5.	**F** škrečok(Ňufko)	$\alpha 2$
6.	**T** $(\text{kŕmi}(\text{Jurko}, \text{Ňufko}) \to \text{škrečok}(\text{Ňufko}))$	?1
7.	**T** škrečok(Ňufko)	MP4, 6
	$*$ 5, 7	

Špeciálny prípad pravdivej všeobecne kvantifikovanej formuly

Doterajšie pravidlá ale nestačia na kľúčový krok, v ktorom sme z *pravdivej všeobecne kvantifikovanej* formuly (1)

$$\forall x(\text{kŕmi}(\text{Jurko}, x) \to \text{škrečok}(x))$$

odvodili jej špeciálny prípad (*inštanciu*) (6) pre konštantu Ňufko:

$$(\text{kŕmi}(\text{Jurko}, \text{Ňufko}) \to \text{škrečok}(\text{Ňufko}))$$

Táto formula, ale aj každá iná, ktorá vznikne analogicky dosadením hocijakého termu za premennú x, je logickým dôsledkom formuly (1).

Pravidlo pre pravdivé všeobecne kvantifikované formuly

Na tento krok potrebujeme nové pravidlo:

$$\frac{\mathbf{T}\,\forall x\, A}{\mathbf{T}\, A\{x \mapsto t\}}\ \gamma$$

pre každú formulu A, každú premennú x a každý *term* t, *ak* spĺňajú dôležitú dodatočnú podmienku — viac o nej neskôr.

Zápis $\{x \mapsto t\}$ označuje *substitúciu* — zobrazenie premenných na termy (v tomto prípade je toto zobrazenie iba jednoprvkové).

Zápis $A\{x \mapsto t\}$ označuje *aplikáciu* substitúcie $\{x \mapsto t\}$ na formulu A — je to formula, ktorá vznikne z formuly A nahradením *všetkých voľných výskytov* premennej x termom t.

Špeciálny prípad nepravdivej existenčne kvantifikovanej formuly

Veľmi podobná situácia nastáva pre *nepravdivú existenčne kvantifikovanú formulu*, napr.

$$\mathbf{F}\ \exists x(\mathsf{kŕmi}(\mathsf{Jurko}, x) \land \mathsf{myš}(x)).$$

Inštancia

$$\mathbf{F}(\mathsf{kŕmi}(\mathsf{Jurko}, \mathsf{Chrumko}) \land \mathsf{myš}(\mathsf{Chrumko}))$$

je logickým dôsledkom pôvodnej označenej formuly.

Rovnako je jej logickým dôsledkom každá iná inštancia a môžeme sformulovať pravidlo:

$$\frac{\mathbf{F}\,\exists x\, A}{\mathbf{F}\, A\{x \mapsto t\}}\ \gamma$$

pre každú formulu A, každú premennú x a každý *term* t, *ak* (opäť) spĺňajú dôležitú dodatočnú podmienku.

Dôkaz s $\mathbf{T}\,\forall x\, A$ a $\mathbf{F}\,\exists x\, A$

Pomocou nových pravidiel môžeme dokázať napr. $\{\forall x(\mathsf{kŕmi}(\mathsf{Jurko}, x) \to \mathsf{škrečok}(x)), \forall x(\mathsf{myš}(x) \to \neg\mathsf{škrečok}(x)), \mathsf{myš}(\mathsf{Ňufko})\} \vDash \exists x(\mathsf{myš}(x) \land \neg\mathsf{kŕmi}(\mathsf{Jurko}, x))$:

1.	$\mathbf{T}\, \forall x(\mathrm{kŕmi}(\mathrm{Jurko}, x) \to \mathrm{škrečok}(x))$	S^+
2.	$\mathbf{T}\, \forall x(\mathrm{myš}(x) \to \neg\mathrm{škrečok}(x))$	S^+
3.	$\mathbf{T}\, \mathrm{myš}(\mathrm{Ňufko})$	S^+
4.	$\mathbf{F}\, \exists x(\mathrm{myš}(x) \land \neg\mathrm{kŕmi}(\mathrm{Jurko}, x))$	S^+
5.	$\mathbf{T}\, (\mathrm{myš}(\mathrm{Ňufko}) \to \neg\mathrm{škrečok}(\mathrm{Ňufko}))$	$\gamma 2\{x \mapsto \mathrm{Ňufko}\}$
6.	$\mathbf{T}\, \neg\mathrm{škrečok}(\mathrm{Ňufko})$	MP5, 3
7.	$\mathbf{F}\, \mathrm{škrečok}(\mathrm{Ňufko})$	$\alpha 6$
8.	$\mathbf{T}\, (\mathrm{kŕmi}(\mathrm{Jurko}, \mathrm{Ňufko}) \to \mathrm{škrečok}(\mathrm{Ňufko}))$	$\gamma 1\{x \mapsto \mathrm{Ňufko}\}$
9.	$\mathbf{F}\, \mathrm{kŕmi}(\mathrm{Jurko}, \mathrm{Ňufko})$	MT8, 7
10.	$\mathbf{F}\, (\mathrm{myš}(\mathrm{Ňufko}) \land \neg\mathrm{kŕmi}(\mathrm{Jurko}, \mathrm{Ňufko}))$	$\gamma 4\{x \mapsto \mathrm{Ňufko}\}$

11. $\mathbf{F}\, \mathrm{myš}(\mathrm{Ňufko})$ $\beta 10$	12. $\mathbf{F}\, \neg\mathrm{kŕmi}(\mathrm{Jurko}, \mathrm{Ňufko})$ $\beta 10$
$*$ 3, 11	13. $\mathbf{T}\, \mathrm{kŕmi}(\mathrm{Jurko}, \mathrm{Ňufko})$ $\alpha 12$
	$*$ 9, 13

Dôkaz s pozitívnou existenčnou kvantifikáciou

Príklad 8.14. Dokážme neformálne, že z teórie $T = \{\forall x(\mathrm{kŕmi}(\mathrm{Jurko}, x) \to \mathrm{škrečok}(x)), \exists x\, \neg\mathrm{škrečok}(x)\}$ prvorádovo vyplýva $X = \exists x\, \neg\mathrm{kŕmi}(\mathrm{Jurko}, x)$.

Sporom: Nech sú formuly (1) $\forall x(\mathrm{kŕmi}(\mathrm{Jurko}, x) \to \mathrm{škrečok}(x))$ a (2) $\exists x\, \neg\mathrm{škrečok}(x)$ pravdivé v nejakej štruktúre. Predpokladajme, že (3) $\exists x\, \neg\mathrm{kŕmi}(\mathrm{Jurko}, x)$ by v nej bola nepravdivá.

Podľa druhého predpokladu existuje objekt x, pre ktorý je $\neg\mathrm{škrečok}(x)$ splnená. *Zoberme si teda takýto objekt a označme ho napríklad premennou z.* Potom je (4) $\neg\mathrm{škrečok}(z)$ je splnená, a teda (5) $\mathrm{škrečok}(z)$ je nesplnená. Podľa prvého predpokladu (1) je formula (6) $(\mathrm{kŕmi}(\mathrm{Jurko}, z) \to \mathrm{škrečok}(z))$ splnená. Pretože už vieme (5), že pravá strana je splnená, musí byť aj ľavá strana (7) $\mathrm{kŕmi}(\mathrm{Jurko}, z)$ nesplnená. Podľa predpokladu dôkazu sporom (3) je však aj jeho inštancia (8) $\neg\mathrm{kŕmi}(\mathrm{Jurko}, z)$ nesplnená, teda (9) je splnená $\mathrm{kŕmi}(\mathrm{Jurko}, z)$, čo je v spore so skorším zistením (7), že táto formula je nesplnená. □

Pozitívna existenčná kvantifikácia a jej vlastná premenná

Kľúčovým krokom v predchádzajúcom dôkaze je označenie objektu (*svedka*), ktorý existuje podľa *pozitívnej existenčne* kvantifikovanej formuly

$$\mathbf{T}\, \exists x\, \neg\mathrm{škrečok}(x),$$

dočasným menom — voľnou premennou z a odvodenie:

$$\mathbf{T}\,\neg\text{škrečok}(z).$$

Táto premenná sa *predtým na vetve nesmie vyskytovať voľná*.

Musí to byť *nová*, *vlastná* premenná pre formulu $\mathbf{T}\,\exists x\,\neg\text{škrečok}(x)$.

Vo všeobecnosti:

$$\frac{\mathbf{T}\,\exists x\,A}{\mathbf{T}\,A\{x \mapsto y\}}\;\delta$$

pre každú formulu A, každú premennú x a každú *novú premennú* y, *ak* (opäť) spĺňajú dôležitú dodatočnú podmienku.

Prečo vlastná premenná?

Prečo potrebuje každá pozitívna existenčná formula vlastnú premennú?

Pravidlá *musia zachovávať splniteľnosť* vetiev v table. Konštanty a iné voľné premenné v table môžu označovať objekty s konfliktnými vlastnosťami. Ich dosadením za existenčne kvantifikovanú premennú by sme dospieť k *falošnému* sporu.

Prečo vlastná premenná? — príklad

Vetva

n+1. $\mathbf{T}\,\text{škrečok}(x)$

n+2. $\mathbf{T}\,\exists x\,\neg\text{škrečok}(x)$

je *splniteľná* (napr. je splnená štruktúrou $\mathcal{M} = (\{1,2\}, i)$, $i(\text{škrečok}) = \{1\}$ pri ohodnotení $e = \{x \mapsto 1, \ldots\}$).

Vetva

n+1. $\mathbf{T}\,\text{škrečok}(x)$

n+2. $\mathbf{T}\,\exists x\,\neg\text{škrečok}(x)$

n+3. $\mathbf{T}\,\neg\text{škrečok}(z)$ ✓ $\delta 2\{x \mapsto z\}$

je *splniteľná* (napr. je splnená štruktúrou $\mathcal{M} = (\{1,2\}, i)$, $i(\text{škrečok}) = \{1\}$ pri ohodnotení $e = \{x \mapsto 1, z \mapsto 2, \ldots\}$).

Chybná vetva

n+1. $\mathbf{T}\,\text{škrečok}(x)$

n+2. $\mathbf{T}\,\exists x\,\neg\text{škrečok}(x)$

n+3. $\mathbf{T}\,\neg\text{škrečok}(x)$ ✗ „δ“$2\{x \mapsto x\}$

by bola *nesplniteľná*.

Negatívna všeobecná kvantifikácia a jej vlastná premenná

Negatívna všeobecne kvantifikovaná formula

$$\mathbf{F}\,\forall x\,\text{škrečok}(x),$$

znamená, že pre niektorý objekt x (*kontrapríklad*) je jej priama podformula škrečok(x) nepravdivá.

Tento objekt teda môžeme opäť označiť novou *vlastnou premennou* formuly $\mathbf{F}\,\forall x\,\text{škrečok}(x)$, napríklad u, a môžeme odvodiť:

$$\mathbf{F}\,\text{škrečok}(u).$$

⚠ Táto premenná sa *predtým na vetve nesmie vyskytovať voľná*. ⚠

Vo všeobecnosti:

$$\frac{\mathbf{F}\,\forall x\,A}{\mathbf{F}\,A\{x \mapsto y\}}\ \delta$$

pre každú formulu A, každú premennú x a každú *novú premennú* y, *ak* (opäť) spĺňajú dôležitú dodatočnú podmienku.

Dôkaz s pravidlami pre kvantifikátory

$\{\exists x\,\forall y(\text{kŕmi}(x,y) \to \text{škrečok}(y)), \forall x(\text{myš}(x) \to \neg\text{škrečok}(x))\} \models \forall x(\text{myš}(x) \to \exists y\,\neg\text{kŕmi}(y,x))$:

1.	$\mathbf{T}\,\exists x\,\forall y(\text{kŕmi}(x,y) \to \text{škrečok}(y))$	S^+
2.	$\mathbf{T}\,\forall x(\text{myš}(x) \to \neg\text{škrečok}(x))$	S^+
3.	$\mathbf{F}\,\forall x(\text{myš}(x) \to \exists y\,\neg\text{kŕmi}(y,x))$	S^+
4.	$\mathbf{F}\,(\text{myš}(u) \to \exists y\,\neg\text{kŕmi}(y,u))$	$\delta 3\{x \mapsto u\}$
5.	$\mathbf{T}\,\text{myš}(u)$	$\alpha 4$
6.	$\mathbf{F}\,\exists y\,\neg\text{kŕmi}(y,u)$	$\alpha 4$
7.	$\mathbf{T}\,\forall y(\text{kŕmi}(z,y) \to \text{škrečok}(y))$	$\delta 1\{x \mapsto z\}$
8.	$\mathbf{T}\,(\text{myš}(u) \to \neg\text{škrečok}(u))$	$\gamma 2\{x \mapsto u\}$
9.	$\mathbf{T}\,\neg\text{škrečok}(u)$	MP8, 5
10.	$\mathbf{F}\,\text{škrečok}(u)$	$\alpha 9$
11.	$\mathbf{T}\,(\text{kŕmi}(z,u) \to \text{škrečok}(u))$	$\gamma 7\{y \mapsto u\}$
12.	$\mathbf{F}\,\text{kŕmi}(z,u)$	MT11, 10
13.	$\mathbf{F}\,\neg\text{kŕmi}(z,u)$	$\gamma 6\{y \mapsto z\}$
14.	$\mathbf{T}\,\text{kŕmi}(z,u)$	$\alpha 13$
	$*$ 12, 14	

Tablové pravidlá pre logiku prvého rádu

Definícia 8.15. *Pravidlami tablového kalkulu pre logiku prvého rádu* sú pravidlá typu α a β pre výrokovú logiku a pravidlá:

$$\gamma \qquad \frac{\mathbf{T}\,\forall x\, A}{\mathbf{T}\,A\{x \mapsto t\}} \qquad \frac{\mathbf{F}\,\exists x\, A}{\mathbf{F}\,A\{x \mapsto t\}} \qquad \text{jednotne: } \frac{\gamma(x)}{\gamma_1(t)}$$

$$\delta \qquad \frac{\mathbf{F}\,\forall x\, A}{\mathbf{F}\,A\{x \mapsto y\}} \qquad \frac{\mathbf{T}\,\exists x\, A}{\mathbf{T}\,A\{x \mapsto y\}} \qquad \text{jednotne: } \frac{\delta(x)}{\delta_1(y)}$$

kde A je formula, x je premenná, t je term *substituovateľný* za x v A a y je premenná *substituovateľná* za x v A.

Pri operácii rozšírenia vetvy tabla π o dôsledok niektorého z pravidiel typu δ navyše musí platiť, že ***premenná y nemá voľný výskyt v žiadnej formule na vetve π***.

Substituovateľnosť vysvetlíme nižšie.

Korektnosť pravidiel γ a δ

Tvrdenie 8.16 (Korektnosť pravidiel γ a δ). *Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech x a y sú premenné, nech t je term.*

- *Ak $\gamma(x) \in S^+$ a t je substituovateľný za x v $\gamma_1(x)$, tak S^+ je splniteľná vtt $S^+ \cup \{\gamma_1(t)\}$ je splniteľná.*
- *Ak $\delta(x) \in S^+$, y je substituovateľná za x v $\delta_1(x)$ a y sa nemá voľný výskyt v S^+, tak S^+ je splniteľná vtt $S^+ \cup \{\delta_1(y)\}$ je splniteľná.*

Tablový kalkul pre logiku prvého rádu

Princíp tablových dôkazov ostáva nezmenený:

- Ak chceme dokázať, že formula X je platná, hľadáme uzavreté tablo pre $S^+ = \{\mathbf{F}\,X\}$. Predpokladáme teda, že v nejakej štruktúre a nejakom ohodnotení je X nesplnená a ukážeme spor.
- Podobne pre prvorádové vyplývanie $T \models X$ predpokladáme, že v nejakej štruktúre a nejakom ohodnotení sú splnené všetky formuly z T ($\mathbf{T}\,A$ pre $A \in T$), ale X je nesplnená ($\mathbf{F}\,X$) a ukážeme spor, teda hľadáme uzavreté tablo pre $S^+ = \{\,\mathbf{T}\,A \mid A \in T\,\} \cup \{\mathbf{F}\,X\}$.

Častá chyba pri pravidlách γ a δ

Vetva:

1. **F** myš(u)
2. **T** pes(u)
3. **T** ($\forall x$ pes(x) $\to$ $\forall y$ myš(y))

je *splniteľná* (napr. je splnená štruktúrou $\mathcal{M} = (\{1, 2\}, i)$, kde i(myš) $= \{1\}$, i(pes) $= \{2\}$ pri ohodnotení $e = \{u \mapsto 2, ...\}$).

V table:

1. **F** myš(u)
2. **T** pes(u)
3. **T** ($\forall x$ pes(x) $\to$ $\forall y$ myš(y))

4. **F** $\forall x$ pes(x) $\beta 3$	5. **T** $\forall y$ myš(y) $\beta 3$
6. **F** pes(v) $\delta 4$	7. **T** myš(u) $\gamma 3$
	$*\, 7, 1$

je ľavá vetva *splniteľná* (napr. je splnená tou istou štruktúrou $\mathcal{M}$ ako pôvodná vetva pri ohodnotení $e = \{u \mapsto 2, v \mapsto 1 ...\}$).

Chybná vetva:

1. **F** myš(u)
2. **T** pes(u)
3. **T** ($\forall x$ pes(x) $\to$ $\forall y$ myš(y))
4. **T** (pes(u) $\to$ $\forall y$ myš(y)) „$\gamma 3$“
5. **T** $\forall y$ myš(y) MP4, 2
6. **T** myš(u) $\gamma 5$

je *nesplniteľná*.

8.3 Substitúcia a substituovateľnosť

Substitúcia

Definícia 8.17 (Substitúcia). *Substitúciou* (v jazyku $\mathcal{L}$) nazývame každé zobrazenie $\sigma : V \to \mathcal{T}_{\mathcal{L}}$ z nejakej množiny indivíduových premenných $V \subseteq \mathcal{V}_{\mathcal{L}}$ do termov jazyka $\mathcal{L}$.

Príklad 8.18. Keď $\mathcal{V}_{\mathcal{L}} = \{u, v, \dots, z, u_1, \dots\}$, $\mathcal{C}_{\mathcal{L}} = \{\text{Klárka}, \text{Jurko}\}$, napríklad $\sigma_1 = \{x \mapsto \text{Klárka}, y \mapsto u, z \mapsto x\}$ je substitúcia.

Problém so substitúciou

Vetva

n+1. $\mathbf{T}\,\forall x\,\neg\text{pozná}(x,x)$
n+2. $\mathbf{T}\,\neg\text{pozná}(y,y)$ $\gamma 1\{x \mapsto y\}$
n+3. $\mathbf{T}\,\forall x\,\exists y\,\text{pozná}(x,y)$

je *splniteľná* (napr. je splnená štruktúrou $\mathcal{M} = (\{1,2\}, i)$, $i(\text{pozná}) = \{(1,2),(2,1)\}$ pri ohodnotení $e = \{y \mapsto 1, \ldots\}$).

Ale vetva

n+1. $\mathbf{T}\,\forall x\,\neg\text{pozná}(x,x)$
n+2. $\mathbf{T}\,\neg\text{pozná}(y,y)$ $\gamma 1\{x \mapsto y\}$
n+3. $\mathbf{T}\,\forall x\,\exists y\,\text{pozná}(x,y)$
n+4. $\mathbf{T}\,\exists y\,\text{pozná}(y,y)$ „γ“$3\{x \mapsto y\}$

je *nesplniteľná*. Oprava: Vetva

n+1. $\mathbf{T}\,\forall x\,\neg\text{pozná}(x,x)$
n+2. $\mathbf{T}\,\neg\text{pozná}(z,z)$ $\gamma 1\{x \mapsto z\}$
n+3. $\mathbf{T}\,\forall x\,\exists y\,\text{pozná}(x,y)$
n+4. $\mathbf{T}\,\exists y\,\text{pozná}(z,y)$ $\gamma 3\{x \mapsto z\}$

je *splniteľná*.

Definícia 8.19 (Substituovateľnosť, aplikovateľnosť substitúcie)**.** Nech A postupnosť symbolov (term alebo formula), nech t, t_1, …, t_n sú termy a x, x_1, …, x_n sú premenné.

Term t je *substituovateľný* za premennú x v A vtt *nie je pravda*, že pre niektorú premennú y vyskytujúcu sa v t platí, že v nejakej oblasti platnosti kvantifikátora $\exists y$ alebo $\forall y$ vo formule A sa premenná x vyskytuje voľná.

Substitúcia $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je *aplikovateľná* na A vtt term t_i je substituovateľný za x_i v A pre každé $i \in \{1, \ldots, n\}$.

Príklad 8.20. Nech $A = \exists \underline{y}\,\text{pozná}(x, y)$.

- Substitúcia $\{x \mapsto \underline{y}, z \mapsto \text{Jurko}\}$ *nie je aplikovateľná* na A, lebo term y *nie je substituovateľný* za premennú x v A.
- Substitúcia $\{x \mapsto z, y \mapsto \text{Jurko}, z \mapsto \underline{y}\}$ *je aplikovateľná* na A.

Substitúcia do postupnosti symbolov

Definícia 8.21 (Substitúcia do postupnosti symbolov)**.** Nech A je postupnosť symbolov, nech $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ je substitúcia. Ak σ je aplikovateľná na A, tak $A\sigma$ je postupnosť symbolov, ktorá vznikne *súčasným* nahradením každého *voľného* výskytu premennej x_i v A termom t_i.

Príklad 8.22. Nech $A = \exists y$ pozná(x, y) a $\sigma = \{x \mapsto z, y \mapsto u, z \mapsto y\}$.

Substitúcia σ *je aplikovateľná* na A. V A je voľná iba premenná x, dosadíme za ňu term z, ktorý neobsahuje viazanú premennú y. Všetky výskyty y sú viazané, za ne sa nedosádza. Premenná z sa v A nevyskytuje, nie je za čo dosadzovať.

$A\sigma = \exists y$ pozná(z, y)

Substitúcia do termov a formúl rekurzívne

Tvrdenie 8.23. *Pre každú substitúciu $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$, každú premennú $y \in \mathcal{V}_\mathcal{L} \setminus \{x_1, \dots, x_n\}$, každý symbol konštanty $a \in \mathcal{C}_\mathcal{L}$, každý predikátový symbol $P^k \in \mathcal{P}_\mathcal{L}$, každé $i \in \{1, \dots, n\}$, každú spojku $\diamond \in \{\land, \lor, \to\}$, všetky formuly A a B a všetky termy $s_1, s_2, \dots, s_k \in \mathcal{T}_\mathcal{L}$ platí:*

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

kde $\sigma_i = \sigma \setminus \{x_i \mapsto t_i\}$, za predpokladu, že σ je v danom prípade aplikovateľná.

9 Formalizácia s viacerými kvantifikátormi

Viacnásobné použitie rovnakého kvantifikátora

Použitím jedného kvantifikátora vo formule sme minulý týždeň dokázali vyjadriť pomerne komplikované tvrdenia.

Ale už v príklade tabiel sme videli, že niektoré tvrdenia zodpovedajú viacerým kvantifikátorom vo formule.

Rozoberme si niekoľko typických prípadov.

9.1 Rovnaký kvantifikátor

Viacnásobné použitie rovnakého kvantifikátora

Najjednoduchšie sú opakované použitia rovnakého kvantifikátora na začiatku formuly:

- $\exists x\, \exists y((\mathsf{človek}(x) \land \mathsf{škrečok}(y)) \land \mathsf{kŕmi}(x, y))$
- $\forall x\, \forall y((\mathsf{človek}(x) \land \mathsf{škrečok}(y)) \to \mathsf{kŕmi}(x, y))$

Význam je ľahké uhádnuť, aj keď je možno zrejmejší v alternatívnej forme, ktorá priamo zodpovedá aristotelovským formám obmedzenej kvantifikácie:

- $\exists x(\mathsf{človek}(x) \land \exists y(\mathsf{škrečok}(y) \land \mathsf{kŕmi}(x, y)))$ Nejaký človek (má vlastnosť, že) kŕmi nejakého škrečka.
- $\forall x(\mathsf{človek}(x) \to \forall y(\mathsf{škrečok}(y) \to \mathsf{kŕmi}(x, y))$ Každý človek kŕmi každého škrečka.

Prenexové vs. hlbšie vnorené formy

Dve uvedené formy každého typu tvrdenia sú vzájomne ekvivalentné, majú rovnaký význam.

Prvé formy sú *prenexové* — kvantifikátory sú na začiatku formuly.

Nie je vždy dobré snažiť sa o prenexovú formu, v zložitejších prípadoch môže byť zavádzajúca.

Rôznosť objektov označených premennými — všeobecný prípad

Tento typ tvrdení je väčšinou bezproblémový až na jeden prípad:

$$\forall x\, \forall y((\mathsf{zvieratko}(x) \land \mathsf{zvieratko}(y)) \to (\mathsf{väčší}(x, y) \lor \mathsf{menší}(x, y)))$$

nezodpovedá tvrdeniu: *Pre každé zvieratká x a y platí, že x je väčšie od y alebo x je menšie od y.*

Slovenské *každé zvieratká x a y* znamená, že x a y označujú naozaj viacero zvieratiek. Ale v logike prvého rádu je každá premenná kvantifikovaná samostatne a *rôzne premenné môžu označovať ten istý objekt*. Rôznosť musíme zapísať explicitne:

$$\forall x\,\forall y((\mathrm{zvieratko}(x) \land \mathrm{zvieratko}(y) \land x \not\doteq y) \to (\mathrm{väčší}(x,y) \lor \mathrm{menší}(x,y)))$$

Pre ľubovoľné termy s, t je $s \not\doteq t$ je skratka za $\neg\, s \doteq t$.

Rôznosť objektov označených premennými — existenčný prípad

Podobne formula

$$\exists x\,\exists y(\mathrm{zvieratko}(x) \land \mathrm{zvieratko}(y))$$

neznamená, že existujú aspoň dve zvieratká (je ekvivalentná s $\exists x\, \mathrm{zvieratko}(x)$).

Existenciu aspoň dvoch zvieratiek zabezpečí formula:

$$\exists x\,\exists y(\mathrm{zvieratko}(x) \land \mathrm{zvieratko}(y) \land x \not\doteq y)$$

Podľa dohody zo 4. prednášky do seba vnorené vľavo uzátvorkované konjunkcie skrátene zapisujeme bez vnútorných zátvoriek. Teda $(\mathrm{zvieratko}(x) \land \mathrm{zvieratko}(y) \land x \not\doteq y)$ je skrátený zápis $((\mathrm{zvieratko}(x) \land \mathrm{zvieratko}(y)) \land x \not\doteq y)$. Podobne skracujeme do seba vnorené disjunkcie.

9.2 Alternácia kvantifikátorov

Existencia pre všetky

Časté formuly, v ktorých sa vyskytujú oba kvantifikátory, sú ako

$$\forall x(\mathrm{zvieratko}(x) \to \exists y(\mathrm{človek}(y) \land \mathrm{kŕmi}(y,x)))$$

Hovorí, že *každé zvieratko má vlastnosť, že nejaký človek ho kŕmi*, teda *každé zvieratko niekto kŕmi*.

Ekvivalentne sa to dá vyjadriť aj (v menej vernej) prenexovej forme:

$$\forall x\,\exists y(\mathrm{zvieratko}(x) \to (\mathrm{človek}(y) \land \mathrm{kŕmi}(y,x)))$$

Poradie kvantifikátorov

Pri rovnakých kvantifikátoroch v prenexovej forme na ich poradí nezáleží:

- $\forall x\,\forall y\, \mathrm{má\_rád}(x,y)$ je ekvivalentné $\forall y\,\forall x\, \mathrm{má\_rád}(x,y)$;

- $\exists x\, \exists y\, \text{má\_rád}(x, y)$ je ekvivalentné $\exists y\, \exists x\, \text{má\_rád}(x, y)$.

Pri rôznych kvantifikátoroch zmena poradia vážne mení význam:

- $\forall x\, \exists y\, \text{má\_rád}(x, y)$ — *Každý má rád niekoho.*
- $\exists x\, \forall y\, \text{má\_rád}(x, y)$ — *Niekto má rád všetkých*

Poradie kvantifikovaných premenných

Záleží aj na tom, ako sa kvantifikované premenné použijú vo formule, ktorá je kvantifikovaná.

Porovnajme:

- $\underline{\forall x}\, \exists y\, \text{má\_rád}(\underline{x}, y)$ — *<u>Každý</u> má rád niekoho.*
- $\underline{\forall x}\, \exists y\, \text{má\_rád}(y, \underline{x})$ — *<u>Každého</u> má niekto rád.*

a

- $\underline{\exists x}\, \forall y\, \text{má\_rád}(\underline{x}, y)$ — *<u>Niekto</u> má rád všetkých.*
- $\underline{\exists x}\, \forall y\, \text{má\_rád}(y, \underline{x})$ — *<u>Niekoho</u> majú radi všetci.*

O neekvivalentnosti týchto formúl sa dá ľahko presvedčiť pomocou štruktúr.

Unikátna existencia

Kombináciou oboch kvantifikátorov s rovnosťou môžeme vyjadriť existenciu *práve jedného* (unikátneho) objektu s danou vlastnosťou:

$$\exists x(\text{škrečok}(x) \wedge \forall y(\text{škrečok}(y) \rightarrow x \doteq y))$$

Neformálne: *Nejaký škrečok je jediným škrečkom*.

Podobne sa dá vyjadriť existencia práve k objektov pre každé prirodzené číslo k.

9.3 Postupná formalizácia a parafrázovanie

Postupná formalizácia

Na formalizáciu zložitých tvrdení je najlepšie ísť postupne.
Sformalizujme: *Každého škrečka kŕmi nejaké dieťa.*

1. Rozpoznáme, že tvrdenie má tvar *Všetky P sú Q*, pričom *P* je atomická vlastnosť. Môžeme ho teda čiastočne sformalizovať na:

$$\forall x(\text{škrečok}(x) \rightarrow \textit{nejaké dieťa kŕmi } x)$$

2. Sformalizujeme *nejaké dieťa kŕmi* x: Má formu: *Nejaké P je Q*:

$$\exists y(\text{dieťa}(y) \wedge \text{kŕmi}(y, x))$$

3. Dosadíme:

$$\forall x(\text{škrečok}(x) \rightarrow \exists y(\text{dieťa}(y) \wedge \text{kŕmi}(y, x)))$$

Systematickým prístupom sa dajú správne sformalizovať aj veľmi zložité tvrdenia.

Viacnásobná negácia — nesprávne možnosti

Opatrnosť je potrebná pri formalizácii tvrdení s viacnásobnou negáciou, napríklad: *Nijaké dieťa nechová žiadnu vretenicu.*

Tu sa ľahko stane, že pri *neopatrnej* postupnej formalizácii skončíme s chybnou formulou:

- $\neg \exists x(\text{dieťa}(x) \wedge \neg \exists y(\text{vretenicu}(y) \wedge \text{chová}(x, y)))$ — *Nie je pravda, že nejaké dieťa nemá vlastnosť, že chová nejakú vretenicu,* teda *Každé dieťa má vlastnosť, že chová nejakú vretenicu,* teda *Každé dieťa chová nejakú vretenicu.*

- $\neg \exists x(\text{dieťa}(x) \wedge \neg \exists y(\text{vretenicu}(y) \wedge \neg\text{chová}(x, y)))$ — *Nie je pravda, že nejaké dieťa nemá vlastnosť, že nechová nejakú vretenicu,* teda *Každé dieťa nechová nejakú vretenicu* (ale môže chovať iné).

Viacnásobná negácia — parafráza a správna formalizácia

Na správne sformalizovanie *Žiadne dieťa nechová žiadnu vretenicu.* je lepšie toto tvrdenie *parafrázovať*:

- *Nie je pravda, že nejaké dieťa chová nejakú vretenicu.*

✓ $\neg \exists x(\text{dieťa}(x) \land \exists y(\text{vretenicu}(y) \land \text{chová}(x, y)))$

- *Pre každé dieťa je pravda, že nechová žiadnu vretenicu.*

✓ $\forall x(\text{dieťa}(x) \to \neg \exists y(\text{vretenicu}(y) \land \text{chová}(x, y)))$

- *Pre každé dieťa x je pravda, že pre každú vretenicu y je pravda, že x nechová y.*

✓ $\forall x(\text{dieťa}(x) \to \forall y(\text{vretenicu}(y) \to \neg\text{chová}(x, y)))$

Odkaz z konzekventu — o sedliakoch a osloch

Už minule sme rozoberali zdanlivo existenčné tvrdenia typu:

Ak <u>nejaký</u> prvák navštevuje LPI, tak <u>(on)</u> je bystrý.

Postupnou formalizáciou by sme mohli dospieť k nesprávnej otvorenej formule:

✗ $\big(\exists x(\text{prvák}(x) \land \text{navštevuje}(x, \text{LPI})) \to \text{bystrý}(x)\big).$

✓ $\forall x\big((\text{prvák}(x) \land \text{navštevuje}(x, \text{LPI})) \to \text{bystrý}(x)\big).$

Vyskytujú sa aj v zložitejších kombináciách. Úderným príkladom je:

Každý sedliak, ktorý vlastní <u>nejakého</u> osla, <u>ho</u> bije.

Na existenčné tvrdenie *vlastní nejakého osla* v antecedente odkazuje zámeno *ho* v konzekvente.

Odkaz z konzekventu — nesprávne možnosti

Postupnou formalizáciou by sme mohli dostať nesprávnu formulu:

❌ $\forall x\big((\mathrm{sedliak}(x) \land \exists y(\mathrm{osol}(y) \land \mathrm{vlastní}(x, y))\big) \to \mathrm{bije}(x, y)\big)$

Keby sme sa ju pokúsili „zachrániť" tým, že zaviažeme premennú y, mohlo by to dopadnúť rôzne, ale stále neprávne:

❌ $\forall x\big(\mathrm{sedliak}(x) \land \exists y\big(\mathrm{osol}(y) \land \mathrm{vlastní}(x, y) \land \mathrm{bije}(x, y)\big)\big)$
— *Všetko je sedliak, ktorý vlastní osla, ktorého bije.*

❌ $\forall x\big(\mathrm{sedliak}(x) \to \exists y\big(\mathrm{osol}(y) \land \mathrm{vlastní}(x, y) \land \mathrm{bije}(x, y)\big)\big)$
— *Každý sedliak určite vlastní osla, ktorého bije.*

Existenčný kvantifikátor teda nefunguje.

Odkaz z konzekventu — parafráza a správna formalizácia

Na správne sformalizovanie je tvrdenie *Každý sedliak, ktorý vlastní nejakého osla, ho bije,* potrebné *parafrázovať* na

- *Každý sedliak bije každého osla, ktorého vlastní.*
- *Pre každého osla je pravda, že každý sedliak, ktorý ho vlastní, ho bije.*

Z parafráz už ľahko dostaneme správne formalizácie:

✅ $$\forall x\big(\mathrm{sedliak}(x) \to \forall y\big((\mathrm{osol}(y) \land \mathrm{vlastní}(x, y)) \to \mathrm{bije}(x, y)\big)\big)$$

✅ $$\forall x\big(\mathrm{osol}(x) \to \forall y\big((\mathrm{sedliak}(y) \land \mathrm{vlastní}(y, x)) \to \mathrm{bije}(y, x)\big)\big)$$

9.4 Závislosť od kontextu

Nejednoznačné tvrdenia

> Každú minútu v New Yorku prepadnú jedného človeka. Dnes nám poskytne rozhovor. — *SNL*

Vtip spočíva v potenciálnej nejednoznačnosti prvej vety. Pravdepodobne ste ju pochopili („slabé“ čítanie)

$$\forall x\big(\mathrm{minúta}(x) \to \exists y\big(\mathrm{človek}(y) \land \mathrm{prepadnutýPočas}(x, y)\big)\big)$$

Ale druhá veta vyzdvihla menej pravdepodobný alternatívny význam („silné“ čítanie):

$$\exists y\big(\mathrm{človek}(y) \land \forall x\big(\mathrm{minúta}(x) \to \mathrm{prepadnutýPočas}(x, y)\big)\big)$$

Závisí od situácie, ktoré z čítaní je správne. Formalizácia je teda *kontextovo závislá*.

9.5 Dodatky k formalizácii s jedným kvantifikátorom

Enumerácia — vymenovanie objektov s vlastnosťou

Niekedy potrebujeme vymenovať objekty s nejakou vlastnosťou:

- *Na bunke č. 14 bývajú Aďa, Biba, Ciri, Dada.*

  $\big(\mathrm{býva\_v}(\mathrm{Aďa}, \mathrm{bunka14}) \land \cdots \land \mathrm{býva\_v}(\mathrm{Dada}, \mathrm{bunka14})\big)$

  Ekvivalentne: *Každá z Aďa, Biba, Ciri, Dada býva v bunke č. 14.*

  $\forall x\big((x \doteq \mathrm{Aďa} \lor \cdots \lor x \doteq \mathrm{Dada}) \to \mathrm{býva\_v}(x, \mathrm{bunka14})\big)$

- *Na bunke č. 14 bývajú* iba *Aďa, Biba, Ciri, Dada.*

  Každý, kto býva v bunke č. 14, je jedna z Aďa, Biba, Ciri, Dada.

  $\forall x\big(\mathrm{býva\_v}(x, \mathrm{bunka14}) \to (x \doteq \mathrm{Aďa} \lor \cdots \lor x \doteq \mathrm{Dada})\big)$

Výnimky a implikatúra

Tvrdenia s výnimkami niekedy vyznievajú silnejšie, ako naozaj sú.

Mám rád všetko ovocie, okrem jabĺk.

Toto tvrdenie zodpovedá aristotelovskej forme: *Každé P je Q,* kde P = *ovocie a nie jablko* a Q = *také, že ho mám rád*, teda formálne:

$$\forall x((\mathrm{ovocie}(x) \land \lnot\mathrm{jablko}(x)) \to \mathrm{mám\_rád}(x))$$

Je *veľmi* lákavé z tohto tvrdenia usúdiť, že navyše znamená: *Jablká nemám rád,* ale je to iba implikatúra (zdanlivý dôsledok).

K *Mám rád všetko ovocie, okrem jabĺk* môžeme síce prekvapivo, ale *bez sporu* dodať:

- *Jablká milujem.*
- *Z jabĺk mám rád iba červené.*

V spore s pôvodným tvrdením by bol dodatok: *Ale slivky nemám rád,* pretože slivky sú ovocie a nie sú jablká, takže podľa pôvodného tvrdenia ich mám rád.

10. prednáška

Funkčné symboly. Tablá s rovnosťou

10 Logika prvého rádu

10.1 Funkčné symboly

Vzťahy s jednoznačne určenými objektmi

V niektorých vzťahoch ich predmet vždy *existuje* a je *jednoznačne* určený/-á:

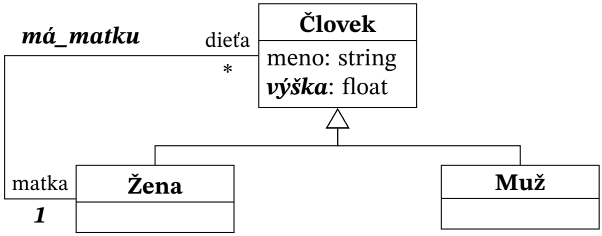
- Každý človek má *práve jednu* biologickú matku.
- Každý človek má (v danej chvíli) *práve jednu* výšku.
- Každé dve čísla majú *práve jeden* súčet (súčin, najväčší spoločný deliteľ, …).
- Každá neprázdna konečná množina čísel má *práve jeden* maximálny prvok.

Takýto predmet potom jednoznačne pomenúvajú menné frázy ako:

- Bonifácova mama; mama Bonifácovej mamy;
- Klárkina výška; výška Jurkovej mamy;
- súčet čísel 2 a 3; súčet čísla 4 a súčinu čísel 2 a 5;
- maximálny prvok množiny $\{2, 7, 19\}$.

Vzťahy s jednoznačne určenými cieľmi v UML

UML má na modelovanie takýchto vzťahov dve možnosti:



Vzťah k jednoznačne určenému *objektu* reprezentuje v UML vzťah s kardinalitou N:1 (*má_matku*).

Vzťah k jednoznačne určenej *hodnote* reprezentuje v UML atribút (*výška*).

Vzťahy s jednoznačne určenými objektmi — predikát a axiómy

Takéto vzťahy môžeme popísať predikátom a formulou pre existenciu a jednoznačnosť:

- Vzťah medzi dieťaťom a matkou môžeme vyjadriť napríklad predikátom má_matku s vlastnosťami existencie a jednoznačnosti:

  $\forall x\, \exists y\, \text{má\_matku}(x, y)$
  $\forall x\, \forall y_1\, \forall y_2\big((\text{má\_matku}(x, y_1) \land \text{má\_matku}(x, y_2)) \to y_1 \doteq y_2\big)$

  alebo stručnejšie:

  $\forall x\, \exists y\big(\text{má\_matku}(x, y) \land \forall y_1(\text{má\_matku}(x, y_1) \to y_1 \doteq y)\big)$

- Podobne súčet dvoch čísel (ak všetko v doméne sú čísla):

  $\forall x\, \forall y\, \exists z\big(\text{súčet}(x, y, z) \land \forall z_1(\text{súčet}(x, y, z_1) \to z_1 \doteq z)\big)$

Vzťahy s jednoznačne určenými objektmi — použitie

Použitie v zložitejších formulách nie je veľmi pohodlné:

- *Bonifácova mama je vedkyňa.*

  $\forall x(\text{má\_matku}(\text{Bonifác}, x) \to \text{vedec}(x))$

  alebo

  $\exists x(\text{má\_matku}(\text{Bonifác}, x) \land \text{vedec}(x))$

  Výrok hovorí o konkrétnych objektoch (Bonifác a jeho mama), ale vo formule musíme použiť kvantifikátory.

- *Mama Klárkinej mamy má Bobíka.*

  $\forall y\, \forall z\big((\text{má\_matku}(\text{Klárka}, y) \land \text{má\_matku}(y, z)) \to \text{má}(z, \text{Bobík})\big)$

- *Ak x delí y a z, delí aj ich súčet.*

  $\forall x\, \forall y\, \forall z\, \forall u\big((\text{delí}(x, y) \land \text{delí}(x, z) \land \text{súčet}(y, z, u)) \to \text{delí}(x, u)\big)$

Funkcie a funkčné symboly

Binárne relácie, ktoré sú všade definované a jednoznačné sa nazývajú… zobrazenia alebo *funkcie*.

Keď f je funkcia a $(x, y) \in f$, y sa nazýva *hodnota funkcie* f pre x a *namiesto y píšeme* $f(x)$.

Reláciám zodpovedajú v logike prvého rádu predikátové symboly. Dalo by sa zadefinovať, ako sa predikáty môžu používať ako funkcie, ale bolo by to komplikované.

Namiesto toho jazyky logiky prvého rádu môžu obsahovať mimologické symboly určené špeciálne na označovanie funkcií — *funkčné symboly*.

Termy s funkčnými symbolmi

Vo formulách sa ani predikátové ani funkčné symboly nedajú použiť samé o sebe — potrebujú argumenty.

Funkčný symbol v jazyku má pevne daný počet argumentov — *aritu* (rovnako ako predikátové symboly).

Postupnosť symbolov

$$\textit{funkčný\_symbol}(\textit{term}_1, \dots, \textit{term}_n)$$

označuje *objekt* — hodnotu funkcie, ktorú označuje *funkčný_symbol*, pre *n*-ticu objektov, ktoré označujú $\textit{term}_1, \dots, \textit{term}_n$. Je to teda *term*, *nie formula*.

Funkčné symboly sa teda líšia od predikátových, pretože $\textit{predikátový\_symbol}(\textit{term}_1, \dots, \textit{term}_n)$ je formula a jej významom je pravdivostná hodnota, nie objekt.

Funkčný symbol namiesto predikátového v atómoch

Napríklad predikát má_matku^2 môžeme nahradiť funkčným symbolom matka^1.

Term matka(Klárka) potom označuje objekt — Klárkinu mamu.

Výrok *Klárkina mama je Magda* namiesto predikátového atómu $\text{má\_matku}(\text{Klárka}, \text{Magda})$ vyjadríme rovnostným atómom $\text{matka}(\text{Klárka}) \doteq \text{Magda}$.

Výrok *Bonifácova mama je vedkyňa* namiesto $\forall x(\text{má\_matku}(\text{Bonifác}, x) \rightarrow \text{vedec}(x))$ vyjadríme atómom $\text{vedec}(\text{matka}(\text{Bonifác}))$.

Podobne, keď súčet^3 nahradíme funkčným symbolom $+^2$:

$$\begin{array}{rcl} \text{súčet}(2, 3, 5) & \rightsquigarrow & +(2, 3) \doteq 5 \\ \forall x(\text{súčet}(7, 3, x) \rightarrow \text{delí}(5, x)) & \rightsquigarrow & \text{delí}(5, +(7, 3)) \end{array}$$

Použitie termov s funkčnými symbolmi

Term s funkčným symbolom môžeme použiť všade, kde sme používali doterajšie termy (indivíduové konštanty a premenné):

- ako argument predikátu alebo rovnosti vo formule:
  - $\forall x\ \text{rodič}(\text{matka}(x), x)$ — *Každého mama je jeho rodičom*;
  - $\forall x \neg\, \text{matka}(x) \doteq x$ — *Nikto nie je sám sebe mamou*;
- ako argument funkčného symbolu:
  - $\text{matka}(\text{matka}(\text{Bonifác}))$ — term označujúci *mamu Bonifácovej mamy* (Bonifácovu starú mamu z maminej strany);
  - $\text{má}(\text{matka}(\text{matka}(\text{Klárka})), \text{Bobík})$ — atóm formalizujúci výrok *Klárkina stará mama z maminej strany má Bobíka*;
  - $\exists x \neg >(\text{výška}(\text{matka}(x)), \text{výška}(x))$ — *Niečia mama nie je vyššia ako on/ona*;
  - $\forall x\, \forall y\, \forall z\big((\text{delí}(x, y) \land \text{delí}(x, z)) \rightarrow \text{delí}(x, +(y, z))\big)$ — *Deliteľ sčítancov delí aj ich súčet*.

Infixová notácia

Dohoda 10.1. *Atómy s binárnymi predikátovými* symbolmi a *termy s binárnymi funkčnými* symbolmi, ktoré sa skladajú z *neabecedných* znakov, môžeme skrátene zapisovať *infixovo*. Teda

- Pre každý neabecedný binárny *predikátový symbol* $\diamond^2$ môžeme *atóm* $\diamond(t_1, t_2)$ skrátiť na $t_1 \diamond t_2$ (bez zátvoriek).

- Pre každý neabecedný *funkčný symbol* $\circ^2$ môžeme *term* $\circ(t_1, t_2)$ skrátiť na $(t_1 \circ t_2)$ (so zátvorkami).

Posledné dva príklady sa sprehľadnia:

- $\exists x \neg\, \mathsf{výška}(\mathsf{matka}(x)) > \mathsf{výška}(x)$ — *Niečia mama nie je vyššia ako on/ona.*
- $\forall x \forall y \forall z \big((x \mid y \land x \mid z) \to x \mid (y + z)\big)$ — *Deliteľ sčítancov delí aj ich súčet.*

Zamýšľaný definičný obor a obor hodnôt funkčných symbolov

Niektoré termy s funkčnými symbolmi môžeme vytvoriť:

$$\mathsf{výška}(\mathsf{výška}(\mathsf{Jurko})), \qquad \mathsf{matka}(\mathsf{výška}(\mathsf{Klárka})),$$

ale nemusia dávať intuitívny zmysel.

Zamýšľaný definičný obor a obor hodnôt funkcie označenej funkčným symbolom môžeme vyjadriť formulami:

$$\forall x\big(\mathsf{človek}(x) \to \big(\mathsf{človek}(\mathsf{matka}(x)) \land \mathsf{žena}(\mathsf{matka}(x))\big)\big)$$
$$\forall x\big(\mathsf{človek}(x) \to \mathsf{dĺžka}(\mathsf{výška}(x))\big)$$

Nič to ale nezmení na tom, že funkcia je *definovaná na celej doméne*.

Funkčné symboly — zhrnutie

	Funkčný symbol	Predikátový symbol
aplikácia na argumenty	$\mathsf{matka}(t)$	$\mathsf{rodič}(t_1, t_2)$
syntaktický typ aplikácie	term	atóm
význam aplikácie	objekt (*matka* t)	pravdivostná hodnota (výroku t_1 *je rodičom* t_2)
podmienky použitia	$\mathsf{matka}(t)$ existuje a je jednoznačne určená pre každé t	t_2 nemusí existovať ani byť jednoznačne určená pre každé t_1
reťazenie aplikácií	$\mathsf{matka}(\mathsf{matka}(t))$	$\cancel{\mathsf{rodič}(t_1, \mathsf{rodič}(t_2, t_3))}$ $(\mathsf{rodič}(t_1, t_2) \land \mathsf{rodič}(t_2, t_3))$

10.2 Syntax logiky prvého rádu

Definícia syntaxe logiky prvého rádu

Keď do definícií doterajšej *relačnej* logiky prvého rádu zahrnieme funkčné symboly, dostaneme konečne (úplnú) *logiku prvého rádu*.

Musíme:

- pridať funkčné symboly medzi symboly jazyka,
- rozšíriť termy o aplikácie funkčných symbolov a vnáranie.

Atomické formuly a formuly zadefinujeme *zdanlivo* rovnako ako doteraz, ale *využitím nových termov*.

Symboly jazyka logiky prvého rádu

Definícia 10.2. *Symbolmi jazyka logiky prvého rádu* $\mathcal{L}$ sú:

indivíduové premenné z nejakej nekonečnej spočítateľnej množiny $\mathcal{V}_{\mathcal{L}}$;

mimologické symboly:

indivíduové konštanty z nejakej spočítateľnej množiny $\mathcal{C}_{\mathcal{L}}$,

funkčné symboly z nejakej spočítateľnej množiny $\mathcal{F}_{\mathcal{L}}$,

predikátové symboly z nejakej spočít. množiny $\mathcal{P}_{\mathcal{L}}$;

logické symboly: logické spojky — unárna $\neg$ a binárne $\land$, $\lor$ a $\rightarrow$, *symbol rovnosti* $\doteq$ a *kvantifikátory* — *existenčný* $\exists$ a *všeobecný* $\forall$;

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

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

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

Označovanie symbolov jazyka logiky prvého rádu

Dohoda 10.3. Keď budeme hovoriť o *ľubovoľných* symboloch jazyka $\mathcal{L}$, budeme ich zvyčajne označovať nasledovnými meta premennými podľa potreby s dolnými indexmi: indivíduové premenné budeme označovať malými písmenami z konca abecedy (x, y, z); indivíduové konštanty malými písmenami zo začiatku abecedy (a, b, c, d, e); funkčné symboly písmenami f, g, h; predikátové symboly písmenami P, Q, R.

Aritu budeme niekedy písať ako horný index symbolov, konkrétnych aj označených meta premennými: pes^1, $<^2$, P^5, matka^1, f^2.

Termy jazyka logiky prvého rádu

Keďže argumentmi funkčných symbolov sú termy, ktoré môžu tiež obsahovať funkčné symboly, musíme termy zadefinovať *induktívne*.

Definícia 10.4. Množina $\mathcal{T}_\mathcal{L}$ *termov* jazyka logiky prvého rádu $\mathcal{L}$ je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, pre ktorú platí:

i. každá indivíduová premenná $x \in \mathcal{V}_\mathcal{L}$ patrí do $\mathcal{T}_\mathcal{L}$ (teda $\mathcal{V}_\mathcal{L} \subseteq \mathcal{T}_\mathcal{L}$);

ii. každá indivíduová konštanta $c \in \mathcal{C}_\mathcal{L}$ patrí do $\mathcal{T}_\mathcal{L}$ (teda $\mathcal{C}_\mathcal{L} \subseteq \mathcal{T}_\mathcal{L}$);

iii. ak f je funkčný symbol s aritou n a $t_1, \dots, t_n$ patria do $\mathcal{T}_\mathcal{L}$, tak aj postupnosť symbolov $f(t_1, \dots, t_n)$ patrí do $\mathcal{T}_\mathcal{L}$.

Každý prvok $\mathcal{T}_\mathcal{L}$ je *term* jazyka $\mathcal{L}$ a nič iné nie je termom jazyka $\mathcal{L}$.

Dohoda 10.5. Termy označujeme písmenami t, s, r s prípadnými dolnými indexmi.

Termy jazyka logiky prvého rádu — príklad

Príklad 10.6. Nech $\mathcal{C}_\mathcal{L} = \{\text{Jurko}, \text{Iveta}\}$, $\mathcal{V}_\mathcal{L} = \{u, v, x, y, z, u_1, v_1, x_1, y_1, \dots\}$, $\mathcal{F}_\mathcal{L} = \{\text{matka}^1, \text{výška}^1\}$.

Podľa i. a ii. bodu definície sú termami: Jurko, Iveta, u, v, x, …

Podľa iii. bodu definície sú termami:
matka(Jurko), matka(Iveta), matka(u), matka(v), …
výška(Jurko), výška(Iveta), výška(u), výška(v), …
matka(matka(Jurko)), matka(výška(Jurko)),
výška(matka(Jurko)), výška(výška(Jurko)), …,
matka(matka(matka(matka(x)))), …

Atomické formuly jazyka logiky prvého rádu

Definícia 10.7 (Atomické formuly)**.** Nech $\mathcal{L}$ je jazyk logiky prvého rádu.

Rovnostný atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $t_1 \doteq t_2$, kde t_1 a t_2 sú termy jazyka $\mathcal{L}$.

Predikátový atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $P(t_1, \dots, t_n)$, kde P je predikátový symbol s aritou n a $t_1, \dots, t_n$ sú termy jazyka $\mathcal{L}$.

Atomickými formulami (skrátene *atómami*) jazyka $\mathcal{L}$ súhrnne nazývame všetky rovnostné a predikátové atómy jazyka $\mathcal{L}$. Množinu všetkých atómov jazyka $\mathcal{L}$ označujeme $\mathcal{A}_{\mathcal{L}}$.

Znenie tejto definície sa takmer nezmenilo, ale zmenili sa pojmy *term* a *jazyk*, ktoré sa v nej používajú. Definuje preto iné postupnosti symbolov ako doteraz.

Formuly jazyka logiky prvého rádu

Definícia 10.8. Množina $\mathcal{E}_{\mathcal{L}}$ všetkých *formúl* jazyka logiky prvého rádu $\mathcal{L}$ je *najmenšia* množina postupností symbolov jazyka $\mathcal{L}$, ktorá spĺňa všetky nasledujúce podmienky:

i. Každý atóm z $\mathcal{A}_{\mathcal{L}}$ patrí do $\mathcal{E}_{\mathcal{L}}$. Inak povedané, $\mathcal{A}_{\mathcal{L}} \subseteq \mathcal{E}_{\mathcal{L}}$.

ii. Ak A patrí do $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosť symbolov $\neg A$ patrí do $\mathcal{E}_{\mathcal{L}}$ a nazývame ju *negácia* formuly A.

iii. Ak A a B sú v $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosti symbolov $(A \land B)$, $(A \lor B)$ a $(A \to B)$ patria do $\mathcal{E}_{\mathcal{L}}$ a nazývame ich postupne *konjunkcia*, *disjunkcia* a *implikácia* formúl A a B.

iv. Ak x je indivíduová premenná a A patrí do $\mathcal{E}_{\mathcal{L}}$, tak aj postupnosti symbolov $\exists x\, A$ a $\forall x\, A$ patria do $\mathcal{E}_{\mathcal{L}}$ a nazývame ich postupne *existenčná* a *všeobecná kvantifikácia* formuly A vzhľadom na x.

Každý prvok A množiny $\mathcal{E}_{\mathcal{L}}$ nazývame *formulou* jazyka $\mathcal{L}$.

Skracovanie zápisu formúl

Dohoda 10.9. Zápis formúl môžeme skracovať nasledujúcim spôsobom:

- Negáciu rovnostného atómu $\neg\, s \doteq t$ skrátene zapisujeme $s \not\doteq t$.
- Ak $\circ \in \{\land, \lor\}$, tak $((A \circ B) \circ C)$ môžeme skrátiť na $(A \circ B \circ C)$.
- Binárnym spojkám priradíme *prioritu*: *najvyššiu* prioritu má $\land$, *strednú* $\lor$, *najnižšiu* $\to$.

  Ak spojka $\circ$ má *vyššiu* prioritu ako $\diamond$, tak v každej formule môžeme podformulu $((A \circ B) \diamond X)$ skrátiť na $(A \circ B \diamond X)$ a podformulu $(X \diamond (A \circ B))$ skrátiť na $(X \diamond A \circ B)$.
- Vonkajší pár zátvoriek okolo celej formuly môžeme vždy vynechať, napr. $(\forall x(a \doteq x \lor P(x)) \to P(b))$ skrátime na $\forall x(a \doteq x \lor P(x)) \to P(b)$.

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

Skracovanie zápisu formúl

Príklad 10.10. Formulu

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

môžeme maximálne skrátiť na

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

Skracovanie zápisu formúl

Príklad 10.11. Skrátený zápis

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

vznikol z formuly

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

10.3 Sémantika logiky prvého rádu

Štruktúry

Rozšírme štruktúru tak, aby dávala význam aj funkčným symbolom:

Definícia 10.12. Nech $\mathcal{L}$ je jazyk logiky prvého rádu. *Štruktúrou* pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (D, i)$, kde

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

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

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

Štruktúry — príklad

Príklad 10.13. Nájdime štruktúru pre jazyk $\mathcal{L}$, v ktorom $\mathcal{V}_{\mathcal{L}} = \{x, y, z, x_1, y_1, \ldots\}$, $\mathcal{C}_{\mathcal{L}} = \{\text{Klárka}, \text{Jurko}\}$, $\mathcal{F}_{\mathcal{L}} = \{\text{matka}^1\}$, $\mathcal{P}_{\mathcal{L}} = \{\text{rodič}^2, \text{žena}^1\}$.

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

$$\begin{aligned}
D &= \{🚺_{\mathrm{M}}, 🚺_{\mathrm{I}}, 🚺_{\mathrm{K}}, 🧒_{\mathrm{J}}, 🚹_{\mathrm{T}}, 🌍\},\\
i(\mathsf{Klárka}) &= 🚺_{\mathrm{K}}, \quad i(\mathsf{Jurko}) = 🧒_{\mathrm{J}}\\
i(\mathsf{matka}) &= \{(🚺_{\mathrm{K}}, 🚺_{\mathrm{M}}), (🧒_{\mathrm{J}}, 🚺_{\mathrm{M}}), (🚺_{\mathrm{M}}, 🚺_{\mathrm{I}}), (🚺_{\mathrm{I}}, 🌍), (🚹_{\mathrm{T}}, 🌍), (🌍, 🌍)\}\\
i(\mathsf{žena}) &= \{🚺_{\mathrm{M}}, 🚺_{\mathrm{I}}, 🚺_{\mathrm{K}}, 🌍\}\\
i(\mathsf{rodič}) &= \{(🚺_{\mathrm{M}}, 🚺_{\mathrm{K}}), (🚺_{\mathrm{M}}, 🧒_{\mathrm{J}}), (🚹_{\mathrm{T}}, 🧒_{\mathrm{J}}), (🚺_{\mathrm{I}}, 🚺_{\mathrm{M}})\}
\end{aligned}$$

Všimnite si, že $i(\mathsf{matka})$ je skutočne funkcia na celej doméne.

Ohodnotenie premenných

Zmena definície štruktúry neovplyvňuje ohodnotenia premenných.

Definícia 10.14. Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk $\mathcal{L}$. *Ohodnotenie indivíduových premenných* je ľubovoľná funkcia $e : \mathcal{V}_{\mathcal{L}} \to D$ (priraďuje premenným prvky domény).

Nech ďalej v je indivíduová premenná z $\mathcal{L}$ a v je prvok D. Zápis $e(x/v)$ označuje ohodnotenie e' indivíduových premenných, pre ktoré platí:

- $e'(x) = v$;
- $e'(y) = e(y)$, ak y je iná premenná ako x.

Hodnota termu

Termy s funkčnými symbolmi môžu byť vnorené, vyhodnocujeme ich rekurzívne:

Definícia 10.15. Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk logiky prvého rádu $\mathcal{L}$, nech e je ohodnotenie premenných. *Hodnotou termu t* v štruktúre $\mathcal{M}$ pri ohodnotení premenných e je prvok z D označovaný $t^{\mathcal{M}}[e]$ a zadefinovaný induktívne pre všetky premenné x, konštanty a, každú aritu n, všetky funkčné symboly f s aritou n, a všetky termy $t_1, \dots, t_n$ nasledovne:

$$\begin{aligned}
x^{\mathcal{M}}[e] &= e(x),\\
a^{\mathcal{M}}[e] &= i(a),\\
\big(f(t_1, \dots, t_n)\big)^{\mathcal{M}}[e] &= i(f)\big(t_1^{\mathcal{M}}[e], \dots, t_n^{\mathcal{M}}[e]\big).
\end{aligned}$$

Hodnoty termov

Príklad 10.16. V štruktúre $\mathcal{M} = (\{🚺_{\mathrm{K}}, 🧒_{\mathrm{J}}, 🚺_{\mathrm{M}}, 🚺_{\mathrm{I}}, 🚹_{\mathrm{T}}, 🌍\}, i)$, $i(\text{Klárka}) = 🚺_{\mathrm{K}}$, $i(\text{Jurko}) = 🧒_{\mathrm{J}}$, $i(\text{matka}) = \{(🚺_{\mathrm{K}}, 🚺_{\mathrm{M}}), (🧒_{\mathrm{J}}, 🚺_{\mathrm{M}}), (🚺_{\mathrm{M}}, 🚺_{\mathrm{I}}), (🚺_{\mathrm{I}}, 🌍), (🚹_{\mathrm{T}}, 🌍), (🌍, 🌍)\}$ pri ohodnotení $e = \{\mathsf{x} \mapsto 🧒_{\mathrm{J}}, \mathsf{y} \mapsto 🚺_{\mathrm{M}}, \ldots\}$ tieto termy: Klárka, x, matka(Klárka), matka(y), matka(matka(Jurko)).

Riešenie. Pripomeňme si podstatné časti štruktúry z príkladu 10.13:

$$\begin{aligned}
\text{Klárka}^{\mathcal{M}}[e] &= i(\text{Klárka}) = 🚺_{\mathrm{K}} \\
\mathsf{x}^{\mathcal{M}}[e] &= e(\mathsf{x}) = 🧒_{\mathrm{J}} \\
\big(\text{matka(Klárka)}\big)^{\mathcal{M}}[e] &= i(\text{matka})\big(\text{Klárka}^{\mathcal{M}}[e]\big) \\
&= i(\text{matka})(🚺_{\mathrm{K}}) = 🚺_{\mathrm{M}} \\
\big(\text{matka}(\mathsf{y})\big)^{\mathcal{M}}[e] &= i(\text{matka})\big(\mathsf{y}^{\mathcal{M}}[e]\big) = i(\text{matka})\big(e(\mathsf{y})\big) \\
&= i(\text{matka})(🚺_{\mathrm{M}}) = 🚺_{\mathrm{I}} \\
\big(\text{matka(matka(Jurko))}\big)^{\mathcal{M}}[e] &= i(\text{matka})\big(i(\text{matka})\big(i(\text{Jurko})\big)\big) = 🚺_{\mathrm{I}}
\end{aligned}$$

Splnenie formuly v štruktúre

Definícia 10.17. Nech $\mathcal{M} = (D, i)$ je štruktúra pre $\mathcal{L}$, e je ohodnotenie premenných. Relácia *štruktúra $\mathcal{M}$ spĺňa formulu X pri ohodnotení e* (skrátene $\mathcal{M} \models X[e]$) má nasledovnú induktívnu definíciu:

- $\mathcal{M} \models t_1 \doteq t_2[e]$ vtt $t_1^{\mathcal{M}}[e] = t_2^{\mathcal{M}}[e]$,
- $\mathcal{M} \models P(t_1, \ldots, t_n)[e]$ vtt $\big(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e]\big) \in i(P)$,
- $\mathcal{M} \models \neg A[e]$ vtt $\mathcal{M} \not\models A[e]$,
- $\mathcal{M} \models (A \land B)[e]$ vtt $\mathcal{M} \models A[e]$ a zároveň $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \lor B)[e]$ vtt $\mathcal{M} \models A[e]$ alebo $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \to B)[e]$ vtt $\mathcal{M} \not\models A[e]$ alebo $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models \exists x\, A[e]$ vtt pre nejaký prvok $m \in D$ máme $\mathcal{M} \models A[e(x/m)]$,
- $\mathcal{M} \models \forall x\, A[e]$ vtt pre každý prvok $m \in D$ máme $\mathcal{M} \models A[e(x/m)]$,

pre všetky arity $n > 0$, všetky predikátové symboly P s aritou n, všetky termy $t_1, t_2, \ldots, t_n$, všetky premenné x a všetky formuly A, B jazyka $\mathcal{L}$.

Ďalšie pojmy

Pojmy:

- pravdivosť uzavretej formuly v štruktúre,
- pravdivosť teórie v štruktúre,
- splniteľnosť,
- nesplniteľnosť,
- platná formula,
- prvorádové vyplývanie

definujeme analogicky ako v relačnej logike prvého rádu.

Pravdivosť formúl v štruktúre

Príklad 10.18 (Pravdivosť formúl v štruktúre). V štruktúre $\mathcal{M} = (\{\text{👩}_{\mathrm{M}}, \text{👩}_{\mathrm{I}}, \text{👧}_{\mathrm{K}}, \text{🧒}_{\mathrm{J}}, \text{👨}_{\mathrm{T}}, \text{🌍}$
kde

$$
\begin{aligned}
i(\text{Klárka}) &= \text{👧}_{\mathrm{K}}, \quad i(\text{Jurko}) = \text{🧒}_{\mathrm{J}}\\
i(\text{matka}) &= \{(\text{👧}_{\mathrm{K}}, \text{👩}_{\mathrm{M}}), (\text{🧒}_{\mathrm{J}}, \text{👩}_{\mathrm{M}}), (\text{👩}_{\mathrm{M}}, \text{👩}_{\mathrm{I}}), (\text{👩}_{\mathrm{I}}, \text{🌍}), (\text{👨}_{\mathrm{T}}, \text{🌍}), (\text{🌍}, \text{🌍})\}\\
i(\text{žena}) &= \{\text{👩}_{\mathrm{M}}, \text{👩}_{\mathrm{I}}, \text{👧}_{\mathrm{K}}, \text{🌍}\}\\
i(\text{rodič}) &= \{(\text{👩}_{\mathrm{M}}, \text{👧}_{\mathrm{K}}), (\text{👩}_{\mathrm{M}}, \text{🧒}_{\mathrm{J}}), (\text{👨}_{\mathrm{T}}, \text{🧒}_{\mathrm{J}}), (\text{👩}_{\mathrm{I}}, \text{👩}_{\mathrm{M}})\}
\end{aligned}
$$

máme napríklad

$$
\begin{aligned}
&\mathcal{M} \models \forall x\, \text{žena}(\text{matka}(x))\\
&\mathcal{M} \models \forall x\, \forall y(\text{žena}(x) \land \text{rodič}(x, y) \to \text{matka}(y) \doteq x)
\end{aligned}
$$

ale

$$
\mathcal{M} \not\models \forall x\, \text{rodič}(\text{matka}(x), x)
$$

11 Tablá pre logiku prvého rádu

Jednotný zápis označených formúl — α a β

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

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

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

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

Jednotný zápis označených formúl — γ a δ

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

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

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

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

11.1 Vlastnosti rovnosti

Rovnosť

Pravidlá pre α a β formuly

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

umožňujú pracovať s logickými spojkami.

Pravidlá pre γ a δ formuly

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

umožňujú pracovať s kvantifikátormi.

V jazyku je ešte jeden logický symbol — rovnosť ($\doteq$).

Žiadne pravidlo s ňou zatiaľ nepracuje.

Čo potrebujeme, aby rovnosť mala očakávané vlastnosti?

Axiomatizácia rovnosti

Rovnosť by sme mohli popísať teóriou — *axiomatizovať* ju.

Rovnosť je reflexívna, symetrická a tranzitívna:

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

Navyše má vlastnosť *kongruencie*: Pre každý pár rovnajúcich sa k-tic argumentov je hodnota každého funkčného symbolu f^k je rovnaká:

$$\forall x_1\, \forall y_1 \dots \forall x_k\, \forall y_k\big(x_1 \doteq y_1 \land \cdots \land x_k \doteq y_k \to f(x_1, \dots, x_k) \doteq f(y_1, \dots, y_k)\big)$$

a každý predikátový symbol P^k je na oboch k-ticiach splnený alebo na oboch nesplnený:

$$\forall x_1\, \forall y_1 \dots \forall x_k\, \forall y_k\big(x_1 \doteq y_1 \land \cdots \land x_k \doteq y_k \to (P(x_1, \dots, x_k) \leftrightarrow P(y_1, \dots, y_k))\big).$$

Dôkazy s axiomatizovanou rovnosťou

Skúsme niečo dokázať:

1.	$\mathbf{T}\, \mathsf{m}(\mathsf{J}) \doteq \mathsf{M}$	S^+
2.	$\mathbf{T}\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), \mathsf{O}) \doteq \mathsf{K}$	S^+
3.	$\mathbf{F}\, \mathsf{pd}(\mathsf{M}, \mathsf{O}) \doteq \mathsf{K}$	S^+
4.	$\mathbf{T}\, \forall x_1\, \forall y_1\, \forall x_2\, \forall y_2 \big(x_1 \doteq y_1 \land x_2 \doteq y_2 \to \mathsf{pd}(x_1, x_2) \doteq \mathsf{pd}(y_1, y_2)\big)$	Kong
5.	$\mathbf{T}\, \forall y_1\, \forall x_2\, \forall y_2 \big(\mathsf{m}(\mathsf{J}) \doteq y_1 \land x_2 \doteq y_2 \to \mathsf{pd}(\mathsf{m}(\mathsf{J}), x_2) \doteq \mathsf{pd}(y_1, y_2)\big)$	$\gamma 4\{x_1 \mapsto \mathsf{m}(\mathsf{J})\}$
	$\vdots$	
8.	$\mathbf{T}\, \mathsf{m}(\mathsf{J}) \doteq \mathsf{M} \land o \doteq o \to \mathsf{pd}(\mathsf{m}(\mathsf{J}), o) \doteq \mathsf{pd}(\mathsf{M}, \mathsf{O})$	$\gamma 8\{y_2 \mapsto \mathsf{O}\}$

9.	$\mathbf{F}\, \mathsf{m}(\mathsf{J}) \doteq \mathsf{M} \land \mathsf{O} \doteq \mathsf{O}$	$\beta 8$	13.	$\mathbf{T}\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), \mathsf{O}) \doteq \mathsf{pd}(\mathsf{M}, \mathsf{O})$	$\beta 8$
10.	$\mathbf{F}\, \mathsf{O} \doteq \mathsf{O}$	NCS9, 1		$\vdots$	
11.	$\mathbf{T}\, \forall x\, x \doteq x$	Refl			
12.	$\mathbf{T}\, \mathsf{O} \doteq \mathsf{O}$	$\gamma 11\{x \mapsto \mathsf{O}\}$			
	$*$ 10, 12				

11.2 Tablové pravidlá pre rovnosť

Leibnitzovo pravidlo

Dôkazy s axiómami rovnosti sú prácne aj v jednoduchých prípadoch.

Kongruencia sa však dá induktívne zovšeobecniť na ľubovoľné formuly — *Leibnitzovo pravidlo*: V každej formule môžeme nahradiť rovné rovným.

1.	$\mathbf{T}\, \mathsf{m}(\mathsf{J}) \doteq \mathsf{M}$	S^+
2.	$\mathbf{T}\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), \mathsf{O}) \doteq \mathsf{K}$	S^+
3.	$\mathbf{F}\, \mathsf{pd}(\mathsf{M}, \mathsf{O}) \doteq \mathsf{K}$	S^+
4.	$\mathbf{T}\, \mathsf{pd}(\mathsf{M}, \mathsf{O}) \doteq \mathsf{K}$	Leibnitz1, 2
	$*$ 3, 4	

Ale *naozaj*?

1.	$\mathbf{T}\, \mathsf{m}(\mathsf{J}) \doteq x$	S^+
2.	$\mathbf{T}\, \exists x\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), x) \doteq \mathsf{K}$	S^+
3.	$\mathbf{T}\, \exists x\, \mathsf{pd}(x, x) \doteq \mathsf{K}$	Leibnitz?1, 2
		partenogenéza?!?

Leibnitzovo pravidlo presne

Leibnitzovo pravidlo: V každej formule môžeme nahradiť rovné rovným.

- Čo znamená „nahradiť“?
- Kedy môžeme nahrádzať bez ohrozenia vyplývania?

Substitúcia $\{x \mapsto t\}$ nahrádza premennú termom.

Pomocou *substituovateľnosti* sme vylúčili prípady, keď by substitúcia odvodila nesprávne „dôsledky“.

Leibnitzovo pravidlo potrebuje nahradiť jeden term t_1 druhým t_2. Dá sa to popísať substitúciami? Potom by sme možno nepotrebovali špeciálne podmienky pre korektnosť Leibnitzovho pravidla.

Leibnitzovo pravidlo presne

Podľa rovnosti $\mathsf{m}(\mathsf{J}) \doteq \mathsf{M}$ chceme nahradiť term $t_1 = \mathsf{m}(\mathsf{J})$ termom $t_2 = \mathsf{M}$ v označenej formule:

$$A_1^+ = \mathbf{T}\, \exists x\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), x) \doteq \mathsf{K}$$

1. Predstavíme si, že na mieste nahrádzaného termu je nová premenná q:

   $A^+ = \mathbf{T}\, \exists x\, \mathsf{pd}(q, x) \doteq \mathsf{K}$

2. Pôvodná formula A_1^+ vznikne z A^+ substitúciou t_1 za q:

   $$\begin{aligned} A_1^+ &= \mathbf{T}\, \exists x\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), x) \doteq \mathsf{K} \\ &= A^+\{q \mapsto \mathsf{m}(\mathsf{J})\} \end{aligned}$$

3. Nová formula A_2^+ vznikne z A^+ substitúciou t_2 za q:

   $$\begin{aligned} A_2^+ &= A^+\{q \mapsto \mathsf{M}\} \\ &= \mathbf{T}\, \exists x\, \mathsf{pd}(\mathsf{M}, x) \doteq \mathsf{K} \end{aligned}$$

Leibnitzovo pravidlo pomocou substitúcií

Vyjadrenie Leibnitzovho pravidla pomocou substitúcií:

$$\frac{\begin{array}{c}\mathbf{T}\, t_1 \doteq t_2 \\ A^+\{q \mapsto t_1\}\end{array}}{A^+\{q \mapsto t_2\}}$$

pre všetky termy t_1 a t_2, označené formuly A^+ a premenné q také, že t_1 a t_2 sú *substituovateľné* za q v A^+.

Leibnitzovo pravidlo — obmedzenia

Automaticky dostávame *rozumné obmedzenia*:
Nemôžeme nahradiť term $t_1 = \mathsf{m}(\mathsf{J})$ termom $t_2 = \underline{\mathsf{x}}$ vo formule:

$$\begin{aligned} A_1^+ &= \mathbf{T}\,\exists \underline{\mathsf{x}}\, \mathsf{pd}(\mathsf{m}(\mathsf{J}), \underline{\mathsf{x}}) \doteq \mathsf{K} \\ &= A^+\{q \mapsto \mathsf{m}(\mathsf{J})\} \\ A^+ &= \mathbf{T}\,\exists \underline{\mathsf{x}}\, \mathsf{pd}(q, \underline{\mathsf{x}}) \doteq \mathsf{K} \end{aligned}$$

lebo $\underline{\mathsf{x}}$ *nie je substituovateľná* za q v A^+ ($\underline{\mathsf{x}}$ je viazaná v mieste voľného výskytu q).

Vlastnosti rovnosti a Leibnitzovo pravidlo

Leibnitzovo pravidlo odvodí symetriu, tranzitivitu aj kongruenciu. Ale potrebuje pomocníčku — reflexivitu:

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

Symetriu potom odvodíme postupnosťou krokov:

1.	$\mathbf{T}\, t_1 \doteq t_2$		
2.	$\mathbf{T}\, t_1 \doteq t_1$	reflexivita	$\mathbf{T}\, q \doteq t_1 \{q \mapsto t_1\}$
3.	$\mathbf{T}\, t_2 \doteq t_1$	Leibnitz 1 a 2	$\mathbf{T}\, q \doteq t_1 \{q \mapsto t_2\}$

Tranzitivitu odvodíme:

1.	$\mathbf{T}\, t_1 \doteq t_2$		$\mathbf{T}\, t_1 \doteq q \{q \mapsto t_2\}$
2.	$\mathbf{T}\, t_2 \doteq t_3$		
3.	$\mathbf{T}\, t_1 \doteq t_3$	Leibnitz 2 a 1	$\mathbf{T}\, t_1 \doteq q \{q \mapsto t_3\}$

11.3 Tablá pre logiku prvého rádu

Tablové pravidlá pre logiku prvého rádu

Definícia 11.1. Tablovými pravidlami pre logiku prvého rádu sú:

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

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

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

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

Tablo pre množinu označených formúl

Definícia 11.2. *Analytické tablo pre množinu* označených *formúl* S^+ (skrátene *tablo pre* S^+) je binárny strom, ktorého vrcholy obsahujú označené formuly a je skonštruovaný induktívne podľa nasledovných pravidiel:

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

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

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

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

Definícia 11.2 (pokračovanie)**.**

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

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

L: Ak sa na vetve π_ℓ vyskytuje $\mathbf{T}\, t_1 \doteq t_2$ pre nejaké termy t_1 a t_2 a označená formula $A^+\{x \mapsto t_1\}$ pre nejakú A^+, v ktorej sú t_1 a t_2 *substituovateľné* za x, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $A^+\{x \mapsto t_2\}$.

R: Ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci označenú formulu $\mathbf{T}\, t \doteq t$ pre ľubovoľný term t.

Korektnosť prvorádových tabiel

Veta 11.3 (Korektnosť tablového kalkulu)**.** *Nech S^+ je množina označených formúl. Ak existuje uzavreté tablo $\mathcal{T}$ pre S^+, tak je množina S^+ nesplniteľná.*

12 Vlastnosti kvantifikátorov

Zoslabenie všeobecného kvantifikátora a premenovanie premenných

Tvrdenie 12.1. *Pre každú formulu A a všetky premenné x a y také, že y je substituovateľná za x v A máme:*

i. $\forall x\, A \models \exists x\, A$

ii. $\forall x\, A \models \forall y\, A\{x \mapsto y\}$

iii. $\exists x\, A \models \exists y\, A\{x \mapsto y\}$

iv. $\forall x\, A \models \exists y\, A\{x \mapsto y\}$

v. $\models \forall y(\forall x\, A \to A\{x \mapsto y\})$

vi. $\models \exists y(A\{x \mapsto y\} \to \forall x\, A)$

vii. $\neg \exists y\, A\{x \mapsto y\} \models \forall y(\exists x\, A \to A\{x \mapsto y\})$

Prvorádovo ekvivalentné formuly

Definícia 12.2. Formuly X a Y sú *prvorádovo ekvivalentné*, skrátene $X \Leftrightarrow Y$, vtt pre každú štruktúru $\mathcal{M}$ a každé ohodnotenie e máme $\mathcal{M} \models X[e]$ vtt $\mathcal{M} \models Y[e]$.

Tvrdenie 12.3. *Nech X a Y sú formuly a nech* $\mathrm{free}(X) \cup \mathrm{free}(Y) = \{x_1, \ldots, x_n\}$. *Nasledujúce tvrdenia sú ekvivalentné:*

a) $X \Leftrightarrow Y$*;*

b) formula $\forall x_1 \cdots \forall x_n (X \leftrightarrow Y)$ *je platná;*

c) existuje uzavreté tablo pre $\{\mathbf{F}(X \leftrightarrow Y)\}$.

De Moganove a distributívne zákony pre kvantifikátory

Tvrdenie 12.4. *Pre každú formulu A a každú premennú x máme:*

i. $\neg \forall x\, A \Leftrightarrow \exists x\, \neg A$*,*

ii. $\neg \exists x\, A \Leftrightarrow \forall x\, \neg A$*.*

Tvrdenie 12.5. *Pre všetky formuly A a B a každú premennú x máme:*

i. $\exists x(A \lor B) \Leftrightarrow (\exists x\, A \lor \exists x\, B)$

ii. $\forall x(A \land B) \Leftrightarrow (\forall x\, A \land \forall x\, B)$

iii. $\exists x(A \land B) \models (\exists x\, A \land \exists x\, B)$

iv. $(\forall x\, A \lor \forall x\, B) \models \forall x(A \lor B)$

Obrátené vyplývania k iii. a iv. neplatia!

Špeciálne distributívne zákony

Tvrdenie 12.6. *Pre každú formulu A, každú premennú x a pre každú formulu C, v ktorej sa x nevyskytuje voľná:*

i. $\exists x(A \lor C) \Leftrightarrow \exists x\, A \lor C$

ii. $\forall x(A \lor C) \Leftrightarrow \forall x\, A \lor C$

iii. $\forall x(A \land C) \Leftrightarrow \forall x\, A \land C$

iv. $\exists x(A \land C) \Leftrightarrow \exists x\, A \land C$

v. $\exists x\, C \Leftrightarrow C$

vi. $\exists x(A \to C) \Leftrightarrow (\forall x\, A \to C)$

vii. $\forall x(A \to C) \Leftrightarrow (\exists x\, A \to C)$

viii. $\forall x(C \to A) \Leftrightarrow (C \to \forall x\, A)$

ix. $\exists x(C \to A) \Leftrightarrow (C \to \exists x\, A)$

x. $\forall x\, C \Leftrightarrow C$

11. prednáška

Korektnosť prvorádových tabiel. Explicitné definície

---

13 Korektnosť tablového kalkulu pre logiku prvého rádu

13.1 Vlastnosti ohodnotení a substitúcie

Voľné premenné a hodnota termu, splnenie formuly, teórie

Tvrdenie 13.1. *Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech e_1 a e_2 sú ohodnotenia, nech t je term, A je formula a S je množina formúl jazyka $\mathcal{L}$.*

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

Substitúcia a hodnota termu

Ako súvisí *hodnota* termu po substitúcii s *hodnotou* termu, do ktorého sa substituuje?

Príklad 13.2. Zoberme štruktúru $\mathcal{M} = (D, i)$, kde

$$\begin{aligned} D &= \{1, 2, 3, 4, 5\}, \\ i(\mathrm{c}) &= 3, \qquad i(\mathrm{d}) = 4 \\ i(\mathrm{f}) &= \{1 \mapsto 2,\ 2 \mapsto 5,\ 3 \mapsto 1,\ 4 \mapsto 1,\ 5 \mapsto 5\} \end{aligned}$$

Nech $e = \{x \mapsto 3,\ y \mapsto 4\}$.

$$\begin{aligned}((\mathsf{f}(\mathsf{x}))\{\mathsf{x} \mapsto \mathsf{f}(\mathsf{y})\})^{\mathcal{M}}[e] &= (\mathsf{f}(\mathsf{f}(\mathsf{y})))^{\mathcal{M}}[e] \\ &= i(\mathsf{f})(\,i(\mathsf{f})(4)\,) = i(\mathsf{f})(1) = 2 \\ &= (\mathsf{f}(\mathsf{x}))^{\mathcal{M}}[e(\mathsf{x}/1)] \\ &= (\mathsf{f}(\mathsf{x}))^{\mathcal{M}}[e(\mathsf{x}/(\mathsf{f}(\mathsf{y}))^{\mathcal{M}}[e])]\end{aligned}$$

Substitúcia vs. hodnota termu a splnenie formuly

Hodnota termu $t\sigma$/splnenie formuly $A\sigma$ po substitúcii $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ pri ohodnotení e sa rovná hodnote termu t/splneniu formuly A pri ohodnotení e', ktoré

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

Tvrdenie 13.3. *Nech $\mathcal{M}$ je štruktúra pre jazyk $\mathcal{L}$ e je ohodnotenie ind. premenných a nech $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ je substitúcia.*

- *Nech t je term jazyka $\mathcal{L}$. Potom $(t\sigma)^{\mathcal{M}}[e] = t^{\mathcal{M}}[e(x_1/t_1^{\mathcal{M}}[e]) \cdots (x_n/t_n^{\mathcal{M}}[e])]$.*
- *Nech A je formula jazyka $\mathcal{L}$ a σ je aplikovateľná na A. Potom $\mathcal{M} \models A\sigma[e]$ vtt $\mathcal{M} \models A[e(x_1/t_1^{\mathcal{M}}[e]) \cdots (x_n/t_n^{\mathcal{M}}[e])]$.*

13.2 Korektnosť tabiel

Korektnosť tablových pravidiel

Tvrdenie 13.4. *Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech x a y sú premenné, nech s, t sú termy, nech $\alpha, \beta, \gamma, \delta$ sú ozn. formuly príslušného typu, A je ozn. formula.*

- *Ak $\alpha \in S^+$, tak S^+ je splniteľná vtt $S^+ \cup \{\alpha_1, \alpha_2\}$ je splniteľná.*
- *Ak $\beta \in S^+$, tak S^+ je splniteľná vtt $S^+ \cup \{\beta_1\}$ je splniteľná alebo $S^+ \cup \{\beta_2\}$ je splniteľná.*

- *Ak $\gamma(x) \in S^+$ a t je term substituovateľný za x v $\gamma_1(x)$, tak S^+ je splniteľná vtt $S^+ \cup \{\gamma_1(t)\}$ je splniteľná.*
- *Ak $\delta(x) \in S^+$, y je substituovateľná za x v $\delta_1(x)$ a y nemá voľný výskyt v S^+, tak S^+ je splniteľná vtt $S^+ \cup \{\delta_1(y)\}$ je splniteľná.*
- *S^+ je splniteľná vtt $S^+ \cup \{\mathbf{T}\, t \doteq t\}$ je splniteľná.*
- *Ak $\{\mathbf{T}\, s \doteq t, A^+\{x \mapsto s\}\} \subseteq S^+$, s a t sú substituovateľné za x v A^+, tak S^+ je splniteľná vtt $S^+ \cup \{A^+\{x \mapsto t\}\}$ je splniteľná.*

Korektnosť tablových pravidiel — dôkaz

Dôkaz (čiastočný, pre pravidlo δ v smere $\Rightarrow$). Zoberme ľubovoľné S^+, x, y a $\delta(x)$ spĺňajúce predpoklady tvrdenia. Nech S^+ je splniteľná, teda existuje štruktúra $\mathcal{M} = (D, i)$ a ohodnotenie e také, že $\mathcal{M} \models S^+[e]$. Preto aj $\mathcal{M} \models \delta(x)[e]$. Podľa tvaru $\delta(x)$ môžu nastať nasledujúce dva prípady:

- Ak $\delta(x) = \mathbf{T}\, \exists x\, A$ pre nejakú formulu A, tak podľa def. 8.11 $\mathcal{M} \models \exists x\, A[e]$ a podľa def. 10.17 máme nejakého *svedka* $m \in D$ takého, že $\mathcal{M} \models A[e(x/m)]$. Podľa tvr. 13.3 potom $\mathcal{M} \models A\{x \mapsto y\}[e(x/m)(y/m)]$. Prem. x nie je voľná v $A\{x \mapsto y\}$, preto podľa tvr. 13.1 $\mathcal{M} \models A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \mathbf{T}\, A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \delta_1(y)[e(y/m)]$.

Korektnosť tablových pravidiel — dôkaz

Dôkaz (čiastočný, pre pravidlo δ v smere $\Rightarrow$, pokračovanie).

- Ak $\delta(x) = \mathbf{F}\, \forall x\, A$ pre nejakú formulu A, tak podľa def. 8.11 $\mathcal{M} \not\models \forall x\, A[e]$ a podľa def. 10.17 neplatí, že $\mathcal{M} \models A[e(x/m)]$ pre každé $m \in D$. Preto máme nejaký *kontrapríklad* $m \in D$ taký, že $\mathcal{M} \not\models A[e(x/m)]$. Podľa tvr. 13.3 potom $\mathcal{M} \not\models A\{x \mapsto y\}[e(x/m)(y/m)]$. Prem. x nie je voľná v $A\{x \mapsto y\}$, preto podľa tvr. 13.1 $\mathcal{M} \not\models A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \mathbf{F}\, A\{x \mapsto y\}[e(y/m)]$, čiže $\mathcal{M} \models \delta_1(y)[e(y/m)]$.

Navyše y nie je voľná v žiadnej formule z S^+, preto $\mathcal{M} \models S^+[e(y/m)]$. Teda $\mathcal{M} \models (S^+ \cup \{\delta_1(y)\})[e(y/m)]$. Preto je $S^+ \cup \{\delta_1(y)\}$ splniteľná. □

Korektnosť — pravdivosť priameho rozšírenia tabla

Vetva sa správa ako konjunkcia svojich označených formúl — všetky musia byť naraz splnené.

Tablo sa správa ako disjunkcia vetiev — niektorá musí byť splnená.

Definícia 13.5. Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+, nech π je vetva tabla $\mathcal{T}$. Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a e je ohodnotenie indivíduových premenných. Potom:

- *štruktúra $\mathcal{M}$ spĺňa vetvu π pri e* vtt $\mathcal{M}$ spĺňa *všetky* označené formuly vyskytujúce sa na vetve π pri e.
- *štruktúra $\mathcal{M}$ spĺňa tablo $\mathcal{T}$ pri e* vtt $\mathcal{M}$ spĺňa *niektorú* vetvu v table $\mathcal{T}$ pri e.

Pomocné tvrdenia pre korektnosť prvorádových tabiel

Lema 13.6 (K1). *Nech S^+ je množina ozn. formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+. Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a e je ohodnotenie ind. premenných. Ak $\mathcal{T}$ a S^+ sú splnené štruktúrou $\mathcal{M}$ pri e, tak aj každé priame rozšírenie $\mathcal{T}$ a S^+ sú splnené štruktúrou $\mathcal{M}$ pri nejakom ohodnotení e'.*

Definícia 13.7. Nech $\mathcal{T}$ je tablo pre nejakú množinu označených formúl. Tablo $\mathcal{T}$ je *splniteľné* vtt existuje štruktúra, ktorá spĺňa $\mathcal{T}$ pri nejakom ohodnotení indivíduových premenných.

Lema 13.8 (K2). *Nech S^+ je množina ozn. formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+. Ak S^+ je splniteľná, tak aj $\mathcal{T}$ je splniteľné.*

Korektnosť prvorádových tabiel

Otvorené a uzavreté vetvy a tablá sú definované rovnako ako pri tablách pre výrokovú logiku.

Veta 13.9 (Korektnosť tablového kalkulu). *Nech S^+ je množina označených formúl. Ak existuje uzavreté tablo $\mathcal{T}$ pre S^+, tak je množina S^+ nesplniteľná.*

Dôkaz (sporom). Nech S^+ je množina označených formúl. Nech existuje uzavreté tablo $\mathcal{T}$ pre S^+, ale S^+ je splniteľná. Pretože $\mathcal{T}$ je uzavreté, pre každú jeho vetva π existuje formula X taká, že $\mathbf{T}\,X$ a $\mathbf{F}\,X$ sa vyskytuje na π, a teda π je nesplniteľná. Preto $\mathcal{T}$ je nesplniteľné. To je v spore s lemou K2, podľa ktorej je $\mathcal{T}$ splniteľné, pretože S^+ je splniteľná. □

13.3 Ďalšie korektné pravidlá

Pohodlnejšie verzie pravidiel γ a δ

Tvrdenie 13.10. *Nasledujúce pravidlá sú korektné:*

$$\gamma^* \qquad \frac{\mathbf{T}\,\forall x_1 \dots \forall x_n\, A}{\mathbf{T}\,A\{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}} \qquad \frac{\mathbf{F}\,\exists x_1 \dots \exists x_n\, A}{\mathbf{F}\,A\{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}}$$

$$\delta^* \qquad \frac{\mathbf{F}\,\forall x_1 \dots \forall x_n\, A}{\mathbf{F}\,A\{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}} \qquad \frac{\mathbf{T}\,\exists x_1 \dots \exists x_n\, A}{\mathbf{T}\,A\{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}}$$

kde A je formula, $x_1, \dots, x_n$ sú premenné, $t_1, \dots, t_n$ sú termy, $y_1, \dots, y_n$ sú navzájom rôzne premenné, ktoré sa nevyskytujú voľné vo vetve, v liste ktorej je pravidlo použité, pričom pre každé $i \in \{1, \dots, n\}$ je term t_i substituovateľný za x_i v A a premenná y_i je substituovateľná za x_i v A.

Pravidlá pre ekvivalenciu

Tvrdenie 13.11. *Nasledujúce pravidlá sú korektné:*

$$ESTT \qquad \frac{\mathbf{T}(A_1 \leftrightarrow A_2) \quad \mathbf{T}\,A_i}{\mathbf{T}\,A_{3-i}} \qquad ESTF \qquad \frac{\mathbf{T}(A_1 \leftrightarrow A_2) \quad \mathbf{F}\,A_i}{\mathbf{F}\,A_{3-i}}$$

$$ESFT \qquad \frac{\mathbf{F}(A_1 \leftrightarrow A_2) \quad \mathbf{T}\,A_i}{\mathbf{F}\,A_{3-i}} \qquad ESFF \qquad \frac{\mathbf{F}(A_1 \leftrightarrow A_2) \quad \mathbf{F}\,A_i}{\mathbf{T}\,A_{3-i}}$$

kde A_1 a A_2 sú formuly, $i \in \{1, 2\}$.

Všimnite si: $3 - 1 = 2$ a $3 - 2 = 1$.

14 Definície

Pojmy

V mnohých doménach sú zaujímavé komplikovanejšie *kombinácie* základných vlastností alebo vzťahov:

- *x má spoločného rodiča s y, ale x je rôzne od y*
  $\exists z(\mathrm{rodič}(z, x) \land \mathrm{rodič}(z, y)) \land \neg x \doteq y$

- *x je živočích, ktorý konzumuje iba rastliny*
  $\mathrm{živočích}(x) \land \forall y(\mathrm{konzumuje}(x, y) \to \mathrm{rastlina}(y))$

Často sa vyskytujúce kombinácie vzťahov a vlastností je výhodné:

- *pomenovať*
- a jasne *vyjadriť význam* nového mena pomocou doteraz známych vlastností a vzťahov,

teda *zadefinovať pojem*.

Definície pojmov

Definícia je tvrdenie, ktoré vyjadruje význam pojmu.

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

Príklad 14.1.
- *Objekt x je* súrodencom *objektu y práve vtedy, keď x nie je y a x má spoločného rodiča s y.*
  $$\forall x\, \forall y\big(\mathrm{súrodenec}(x, y) \leftrightarrow \big(x \not\approx y \land \exists z(\mathrm{rodič}(z, x) \land \mathrm{rodič}(z, y))\big)\big)$$
- *Objekt x je* bylinožravec *vtedy a len vtedy, keď x je živočích, ktorý konzumuje iba rastliny.*
  $$\forall x\big(\mathrm{bylinožravec}(x) \leftrightarrow \big(\mathrm{živočích}(x) \land \forall y(\mathrm{konzumuje}(x, y) \to \mathrm{rastlina}(y))\big)\big)$$

Explicitná def. a nutná a postačujúca podmienka

Všimnite si:

Definícia pojmu *súrodenec* vyjadruje *nutnú aj postačujúcu* podmienku toho, aby medzi dvoma objektmi bol súrodenecký vzťah.

→ Pre každú dvojicu objektov x a y, ktoré označíme za súrodencov, *musí* existovať ich spoločný rodič a musia byť navzájom rôzne.

← Každé dva navzájom rôzne objekty x a y, ktoré majú spoločného rodiča, *musia* byť súrodenci.

Podobne pre iné definície.

Použitie pojmov

Využitím definovaného pojmu

- skracujeme tvrdenia: *Škrečky sú bylinožravce.*
  $\forall x(\text{škrečok}(x) \to \text{bylinožravec}(x))$
- jednoduchšie definujeme ďalšie pojmy:
  Objekt x je sestrou *objektu y práve vtedy,*
  keď x je žena, ktorá je súrodencom y.
  $\forall x\, \forall y\big(\text{sestra}(x, y) \leftrightarrow (\text{žena}(x) \land \text{súrodenec}(x, y))\big)$

Vyskúšajte si 14.1

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

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

Podmienené definície

Niekedy má pojem význam iba pre niektoré druhy objektov, alebo má ten istý pojem rôzne významy pre rôzne druhy objektov.

Vtedy môžeme definície *podmieniť* druhmi:

- *Študent absolvuje predmet vtt je z neho hodnotený inou známkou ako Fx.*
  $$\forall x\, \forall y\big(\text{študent}(x) \land \text{predmet}(y) \to \\ \quad \big(\text{absolvuje}(x, y) \leftrightarrow \\ \quad\quad \exists z(\text{hodnotený}(x, y) \doteq z \land \text{známka}(z) \land z \not\doteq \text{Fx})\big)\big)$$
- *Študent absolvuje študijný program vtt*
  absolvuje každý jeho povinný predmet.
  $$\forall x\, \forall y\big(\text{študent}(x) \land \text{št\_prog}(y) \to \\ \quad \big(\text{absolvuje}(x, y) \leftrightarrow \\ \quad\quad \forall z(\text{pov\_predmet\_prog}(z, y) \to \text{absolvuje}(x, z))\big)\big)$$

Explicitná definícia presne

Definícia 14.2. Nech $\mathcal{L}$ a $\mathcal{L}_1$ sú jazyky logiky prvého rádu. Jazyk $\mathcal{L}_1$ je *rozšírením* jazyka $\mathcal{L}$ vtt $\mathcal{V}_{\mathcal{L}_1} = \mathcal{V}_{\mathcal{L}}$, $\mathcal{C}_{\mathcal{L}} \subseteq \mathcal{C}_{\mathcal{L}_1}$, $\mathcal{P}_{\mathcal{L}} \subseteq \mathcal{P}_{\mathcal{L}_1}$, $\mathcal{F}_{\mathcal{L}} \subseteq \mathcal{F}_{\mathcal{L}_1}$.

Definícia 14.3. Nech $\mathcal{L}$ je jazyk logiky prvého rádu, T je teória v jazyku $\mathcal{L}$, a $\mathcal{L}_P$ je rozšírenie jazyka o predikátový symbol P je s aritou n, ktorý sa nevyskytuje v $\mathcal{L}$. Teóriu v jazyku $\mathcal{L}_P$

$$T \cup \{\forall x_1 \dots \forall x_n (P(x_1, \dots, x_n) \leftrightarrow A)\},$$

kde A je formula, v ktorej sa nevyskytuje P, nazývame *rozšírením teórie T explicitnou definíciou* $\forall x_1 \dots \forall x_n (P(x_1, \dots, x_n) \leftrightarrow A)$ predikátového symbolu P.

Jednoznačnosť interpretácie definovaného predikátu

Význam explicitne definovaného predikátu je jednoznačne určený.

Príklad 14.4. Majme nejakú teóriu T v jazyku $\mathcal{L}$ s $\mathcal{P}_{\mathcal{L}} = \{\mathsf{rodič}^2\}$. Rozšírme T o $X = \forall x\, \forall y \big(\mathsf{súrodenec}(x, y) \leftrightarrow \big(x \not\doteq y \land \exists z(\mathsf{rodič}(z, x) \land \mathsf{rodič}(z, y))\big)\big)$.

Nech $\mathcal{M} = (\{\text{🚺}_{\mathrm{I}}, \text{🚼}_{\mathrm{J}}, \text{🚺}_{\mathrm{K}}, \text{🚹}_{\mathrm{L}}, \text{🚺}_{\mathrm{M}}, \text{🚹}_{\mathrm{N}}, \text{🚹}_{\mathrm{O}}\}, i)$ je model T, kde

$$i(\mathsf{rodič}) = \{(\text{🚺}_{\mathrm{I}}, \text{🚺}_{\mathrm{M}}), (\text{🚹}_{\mathrm{L}}, \text{🚺}_{\mathrm{M}}), (\text{🚺}_{\mathrm{I}}, \text{🚹}_{\mathrm{N}}), (\text{🚹}_{\mathrm{O}}, \text{🚹}_{\mathrm{N}}), (\text{🚺}_{\mathrm{M}}, \text{🚺}_{\mathrm{K}}), (\text{🚺}_{\mathrm{M}}, \text{🚼}_{\mathrm{J}})\}$$

Potom sa $\mathcal{M}$ dá *jednoznačne* rozšíriť na model $T \cup \{X\}$:
$\mathcal{M}_1 = (\{\text{🚺}_{\mathrm{I}}, \text{🚼}_{\mathrm{J}}, \text{🚺}_{\mathrm{K}}, \text{🚹}_{\mathrm{L}}, \text{🚺}_{\mathrm{M}}, \text{🚹}_{\mathrm{N}}, \text{🚹}_{\mathrm{O}}\}, i_1)$, $i_1(\mathsf{rodič}) = i(\mathsf{rodič})$,

$$i(\mathsf{súrodenec}) = \{(\text{🚺}_{\mathrm{M}}, \text{🚹}_{\mathrm{N}}), (\text{🚹}_{\mathrm{N}}, \text{🚺}_{\mathrm{M}}), (\text{🚺}_{\mathrm{K}}, \text{🚼}_{\mathrm{J}}), (\text{🚼}_{\mathrm{J}}, \text{🚺}_{\mathrm{K}})\}$$

Definícia ako dopyt

Explicitne definovaný predikát sa správa ako *dopyt* alebo *pohľad* nad ostatnými predikátmi.

Príklad 14.5.

rodič	
r	d
I	M
L	M
I	N
O	N
M	K
M	J

```
CREATE VIEW súrodenec AS
SELECT r1.d AS d1, r2.d AS d2
FROM rodič AS r1
JOIN rodič AS r2 ON r1.r = r2.r
WHERE r1.d <> r2.d
```

$$\forall x\, \forall y \, \big(\text{súrodenec}(x, y) \leftrightarrow \big(x \not\doteq y \land \exists z(\text{rodič}(z, x) \land \text{rodič}(z, y))\big)\big)$$

súrodenec	
d1	d2
M	N
N	M
K	J
J	K

Jednoznačnosť definičného rozšírenia

Definícia 14.6. Nech $\mathcal{L}_2$ je rozšírenie jazyka $\mathcal{L}_1$. Nech $\mathcal{M}_1 = (D_1, i_1)$ je štruktúra pre $\mathcal{L}_1$ a $\mathcal{M}_2 = (D_2, i_2)$ je štruktúra pre $\mathcal{L}_2$. Potom $\mathcal{M}_2$ je *rozšírením* $\mathcal{M}_1$ vtt $D_2 = D_1$ a $i_2(s) = i_1(s)$ pre každý mimologický symbol s jazyka $\mathcal{L}_1$.

Tvrdenie 14.7. *Nech T je teória v jazyku $\mathcal{L}$ a T' je rozšírenie T explicitnou definíciou nejakého predikátového symbolu. Potom pre každý model teórie T existuje práve jedno jeho rozšírenie, ktoré je modelom teórie T' a každý model teórie T' je rozšírením práve jedného modelu teórie T.*

Konzervativita definičného rozšírenia

Tvrdenie 14.8. *Nech T je teória v jazyku $\mathcal{L}$ a T' je rozšírenie T explicitnou definíciou nejakého predikátového symbolu. Nech X je uzavretá formula jazyka $\mathcal{L}$. Potom $T \vDash X$ vtt $T' \vDash X$.*

Dokazovanie s explicitnými definíciami a rovnosťou

Využime nové pravidlá na dôkaz vyplývania z teórie s definíciou:

Príklad 14.9. Dokážme tablom, že $T \models X$ pre

$$\begin{aligned}
T = \bigl\{&\forall x\,\forall y\bigl(\mathsf{študent}(x) \land \mathsf{predmet}(y) \to \\
&\qquad\quad \bigl(\mathsf{absolvuje}(x, y) \leftrightarrow \\
&\qquad\quad\;\; \exists z(\mathsf{známka}(z) \land \mathsf{hodnotený}(x, y) \doteq z \land z \not\doteq \mathsf{Fx})\bigr)\bigr), \\
&\forall x\,\forall y\bigl(\mathsf{študent}(x) \land \mathsf{št_prog}(y) \to \\
&\qquad\quad \bigl(\mathsf{absolvuje}(x, y) \leftrightarrow \\
&\qquad\quad\;\; \forall z(\mathsf{pov_predmet_prog}(z, y) \to \mathsf{absolvuje}(x, z))\bigr)\bigr), \\
&\forall x\bigl(\mathsf{št_prog}(x) \to \exists y\, \mathsf{pov_predmet_prog}(z, x)\bigr), \\
&\forall x\bigl(\exists y\, \mathsf{pov_predmet_prog}(x, y) \to \mathsf{predmet}(x)\bigr)\bigr\} \\
X = {}&\forall x\,\forall y\bigl(\mathsf{študent}(x) \land \mathsf{št_prog}(y) \land \mathsf{absolvuje}(x, y) \to \\
&\qquad\quad \exists y\, \mathsf{hodnotený}(x, y) \not\doteq \mathsf{Fx}\bigr)
\end{aligned}$$

1. $\mathbf{T}\ \forall x\, \forall y\big(\text{študent}(x) \land \text{predmet}(y) \to (\text{absolvuje}(x,y) \leftrightarrow \exists z(\text{hodnotený}(x,y) \doteq z \land \text{známka}(z) \land z \not\doteq \text{Fx}))\big)$ — S^+

2. $\mathbf{T}\ \forall x\, \forall y\big(\text{študent}(x) \land \text{št\_prog}(y) \to (\text{absolvuje}(x,y) \leftrightarrow \forall z(\text{pov\_predmet\_prog}(z,y) \to \text{absolvuje}(x,z)))\big)$ — S^+

3. $\mathbf{T}\ \forall x\big(\text{št\_prog}(x) \to \exists y\, \text{pov\_predmet\_prog}(z,x)\big)$ — S^+

4. $\mathbf{T}\ \forall x\big(\exists y\, \text{pov\_predmet\_prog}(x,y) \to \text{predmet}(x)\big)$ — S^+

5. $\mathbf{F}\ \forall x\, \forall y\big(\text{študent}(x) \land \text{št\_prog}(y) \land \text{absolvuje}(x,y) \to \exists y\, \text{hodnotený}(x,y) \not\doteq \text{Fx}\big)$ — S^+

6. $\mathbf{F}\ \text{študent}(u) \land \text{št\_prog}(v) \land \text{absolvuje}(u,v) \to \exists y\, \text{hodnotený}(u,y) \not\doteq \text{Fx}$ — $\delta^* 5\{x \mapsto u, y \mapsto v\}$

7. $\mathbf{T}\ \text{študent}(u) \land \text{št\_prog}(v) \land \text{absolvuje}(u,v)$ — $\alpha 6$

8. $\mathbf{F}\ \exists y\, \text{hodnotený}(u,y) \not\doteq \text{Fx}$ — $\alpha 6$

9. $\mathbf{T}\ \text{študent}(u) \land \text{št\_prog}(v)$ — $\alpha 7$

10. $\mathbf{T}\ \text{absolvuje}(u,v)$ — $\alpha 7$

11. $\mathbf{T}\ \text{študent}(u) \land \text{št\_prog}(v) \to \big(\text{absolvuje}(u,v) \leftrightarrow \forall z(\text{pov\_predmet\_prog}(z,v) \to \text{absolvuje}(u,z))\big)$ — $\gamma^* 2\{x \mapsto u, y \mapsto v\}$

12. $\mathbf{T}\ \text{absolvuje}(u,v) \leftrightarrow \forall z(\text{pov\_predmet\_prog}(z,v) \to \text{absolvuje}(u,z))$ — $MP\,11, 9$

13. $\mathbf{T}\ \forall z(\text{pov\_predmet\_prog}(z,v) \to \text{absolvuje}(u,z))$ — $ESTT\,12, 10$

14. $\mathbf{T}\ \text{št\_prog}(v) \to \exists y\, \text{pov\_predmet\_prog}(y,v)$ — $\gamma 3\{x \mapsto v\}$

15. $\mathbf{T}\ \text{št\_prog}(v)$ — $\alpha 9$

16. $\mathbf{T}\ \exists y\, \text{pov\_predmet\_prog}(y,v)$ — $MP\,14, 15$

17. $\mathbf{T}\ \text{pov\_predmet\_prog}(w,v)$ — $\delta^* 16\{y \mapsto w\}$

18. $\mathbf{T}\ \text{pov\_predmet\_prog}(w,v) \to \text{absolvuje}(u,w)$ — $\gamma 13\{z \mapsto w\}$

19. $\mathbf{T}\ \text{absolvuje}(u,w)$ — $MP\,19, 17$

20. $\mathbf{T}\ \exists y\, \text{pov\_predmet\_prog}(w,y) \to \text{predmet}(w)$ — $\gamma 4\{x \mapsto w\}$

---

21. $\mathbf{F}\ \exists y\, \text{pov\_predmet\_prog}(w,y)$ — $\beta 20$

22. $\mathbf{F}\ \text{pov\_predmet\_prog}(w,v)$ — $\gamma 21\{y \mapsto v\}$

$*$ 17, 22

---

23. $\mathbf{T}\ \text{predmet}(w)$ — $\beta 20$

24. $\mathbf{T}\ \text{študent}(u) \land \text{predmet}(w) \to \big(\text{absolvuje}(u,w) \leftrightarrow \exists z(\text{hodnotený}(u,w) \doteq z \land \text{známka}(z) \land z \not\doteq \text{Fx})\big)$ — $\gamma^* 1\{x \mapsto u, y \mapsto w\}$

---

25. $\mathbf{F}\ \text{študent}(u) \land \text{predmet}(w)$ — $\beta 24$

26. $\mathbf{F}\ \text{študent}(u)$ — $NCS\,25, 23$

27. $\mathbf{T}\ \text{študent}(u)$ — $\alpha 9$

$*$ 26, 27

---

28. $\mathbf{T}\ \text{absolvuje}(u,w) \leftrightarrow \exists z(\text{hodnotený}(u,w) \doteq z \land \text{známka}(z) \land z \not\doteq \text{Fx})$ — $\beta 24$

29. $\mathbf{T}\ \exists z(\text{hodnotený}(u,w) \doteq z \land \text{známka}(z) \land z \not\doteq \text{Fx})$ — $ESTT\,28, 19$

30. $\mathbf{T}\ \text{hodnotený}(u,w) \doteq z \land \text{známka}(z) \land z \not\doteq \text{Fx}$ — $\delta 29\{z \mapsto z\}$

31. $\mathbf{T}\ \text{hodnotený}(u,w) \doteq z \land \text{známka}(z)$ — $\alpha 30$

32. $\mathbf{T}\ \text{hodnotený}(u,w) \doteq z$ — $\alpha 31$

33. $\mathbf{T}\ z \not\doteq \text{Fx}$ — $\alpha 30$

34. $\mathbf{T}\ \text{hodnotený}(u,w) \doteq \text{hodnotený}(u,w)$ — Refl

35. $\mathbf{T}\ z \doteq \text{hodnotený}(u,w)$ — Leib 32, 34

36. $\mathbf{T}\ \text{hodnotený}(u,w) \not\doteq \text{Fx}$ — Leib 35, 33

37. $\mathbf{F}\ \text{hodnotený}(u,w) \not\doteq \text{Fx}$ — $\gamma^* 8\{y \mapsto w\}$

$*$ 36, 37

12. prednáška

Rezolvencia

15 Rezolvencia

Automatické dokazovanie v logike prvého rádu

Vyplývanie vo výrokovej logike je rozhodnuteľné.

SAT solver vždy skončí a rozhodne splniteľnosť, v najhoršom prípade v čase $O(2^n)$ pre n atómov.

Logika prvého rádu *nie je* rozhodnuteľná.

- Prvorádovými formulami sa dá opísať fungovanie Turingovho stroja.
- Dá sa nájsť formula, ktorá opisuje, že TS zastaví na každom vstupe.

Existujú však prvorádové automatické dokazovače (Prover9, Vampire).

Nemusia zastaviť, ale ak existuje dôkaz vyplývania, teoreticky ho nájdu.

Ako fungujú automatické dokazovače v logike prvého rádu

Prvé automatické dokazovače využívali prvorádovú verziu DPLL.

Niektoré automatické dokazovače využívajú modifikované tablá.

Väčšina automatických dokazovačov (aj Prover9 a Vampire) je ale založená na *rezolvencii*:

- špeciálne pravidlo na klauzulách,
- kombinuje výrokové a kvantifikátorové odvodzovanie.

Rezolvenčný dôkaz je lineárny, nevetví sa.

15.1 Rezolvencia vo výrokovej logike

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:

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

Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

Definícia 15.1. *Rezolvenčný princíp* (*rezolvencia*, angl. *resolution principle*) je pravidlo

$$\frac{(K_1 \lor \cdots \lor A \lor \cdots \lor K_m) \qquad (L_1 \lor \cdots \lor \neg A \lor \cdots \lor L_n)}{(K_1 \lor \cdots \lor K_m \lor L_1 \lor \cdots \lor L_n)}$$

pre ľubovoľný atóm A a ľubovoľné literály $K_1, \ldots, K_m, L_1, \ldots, L_n$.

Klauzulu $(K_1 \lor \cdots \lor K_m \lor L_1 \lor \cdots \lor L_n)$ nazývame *rezolventou* klauzúl $(K_1 \lor \cdots \lor A \lor \cdots \lor K_m)$ a $(L_1 \lor \cdots \lor \neg A \lor \cdots \lor L_n)$.

Tvrdenie 15.2. *Rezolvencia je korektné pravidlo.*

Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

$$\frac{(\neg A \lor B) \quad (\neg B \lor C)}{(\neg A \lor C)} \qquad \frac{(A \to B) \quad (B \to C)}{(A \to C)} \qquad \text{(HS)}$$

$$\frac{(\neg A \lor B) \quad A}{B} \qquad \frac{(A \to B) \quad A}{B} \qquad \text{(MP)}$$

$$\frac{(\neg A \lor B) \quad \neg B}{\neg A} \qquad \frac{(A \to B) \quad \neg B}{\neg A} \qquad \text{(MT)}$$

Pozorovania o rezolvencii

- Rezolvencia s *jednotkovou* klauzulou skráti druhú klauzulu:

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

- Rezolvencia môže odvodiť *prázdnu klauzulu*:

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

  vtedy premisy *nie sú súčasne splniteľné*

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

Častá chyba pri rezolvencii

Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch:

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

ale *je chyba urobiť to naraz*:

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

Toto *nie je* inštancia rezolvencie ani korektný úsudok.

Prečo?

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

Rezolvenčné odvodenie a problém

Opakovaním rezolvencie môžeme odvodzovať ďalšie dôsledky:

Príklad 15.3. Z množiny $S = \{(A \lor B), (\neg A \lor C), (\neg B \lor A), (\neg A \lor \neg C)\}$ odvodíme:

(1) $(A \lor B)$ predpoklad z S

(2) $(\neg A \lor C)$ predpoklad z S

(3) $(\neg B \lor A)$ predpoklad z S

(4) $(\neg A \lor \neg C)$ predpoklad z S

(5) $(A \lor A)$ rezolventa (3) a (1)

(6) $(B \lor C)$ rezolventa (1) a (2)

(7) $(B \lor \neg C)$ rezolventa (1) a (4)

(8) $(B \lor B)$ rezolventa (6) a (7)

$\vdots$

Problematické prípady

Odvodeniami v príklade dostaneme iba existujúce alebo nové *dvojprvkové* klauzuly ($(A \lor A)$, $(B \lor C)$, $(B \lor B)$, $\dots$) ale žiadnu jednotkovú, lebo rezolventa má $m + n - 2$ literálov.

$S = \{(A \lor B), (\neg A \lor C), (\neg B \lor A), (\neg A \lor \neg C)\}$ je ale nesplniteľná, mali by sme nejak odvodiť prázdnu klauzulu.

To sa nedá bez odvodenia nejakej jednotkovej klauzuly (napr. A).

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

Potrebujeme ešte *pravidlo idempotencie*:

$$\frac{(K_1 \lor \cdots \lor L \lor \cdots \lor L \lor \cdots \lor K_n)}{(K_1 \lor L \lor \cdots \lor K_n)}$$

Rezolvenčné odvodenie a zamietnutie

Definícia 15.4. *Výrokovologické rezolvenčné odvodenie* z množiny klauzúl S je každá (aj nekonečná) postupnosť klauzúl $C_1, C_2, \dots, C_n, \dots$, ktorej každý člen C_i je:

- prvkom S alebo

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

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

Rezolvenčné zamientnutie

Príklad 15.5. Nech $S = \{(A \vee B), (\neg A \vee C), (\neg B \vee A), (\neg A \vee \neg C)\}$.

Kombináciou rezolvencie a idempotencie nájdeme zamietnutie S:

(1) $(A \vee B)$ predpoklad z S

(2) $(\neg A \vee C)$ predpoklad z S

(3) $(\neg B \vee A)$ predpoklad z S

(4) $(\neg A \vee \neg C)$ predpoklad z S

(5) $(A \vee A)$ rezolventa (3) a (1)

(6) A idempotencia (5)

(7) C rezolvencia (6) a (2)

(8) $\neg C$ rezolvencia (6) a (4)

(9) $\square$ rezolvencia (7) a (8)

Korektnosť a úplnosť rezolvencie

Množinu klauzúl nazývame aj *klauzálna teória*.

Veta 15.6 (Korektnosť a úplnosť rezolvencie)**.** *Nech S je množina klauzálna teória. S je výrokovologicky nesplniteľná vtt existuje zamietnutie S.*

Už vieme, že ku každej formule (a teórii) existuje ekvivalentná klauzálna teória (formula v CNF). Výrokovologická splniteľnosť a vyplývanie sa teda dajú rozhodnúť pomocou rezolvencie.

Vyskúšajte si 15.1
Dokážte nesplniteľnosť $S = \{(A \lor B \lor \neg C), (\neg A \lor \neg C), (A \lor \neg B), (\neg A \lor C), (A \lor B \lor C)\}$.

15.2 Prevod do klauzálnej teórie a skolemizácia

Rezolvencia vs. prvorádové teórie

Výrokovologická rezolvencia pracuje s klauzálnymi teóriami.

Výrokovologickú teóriu ľahko upravíme na klauzálnu — ekvivalentnými úpravami do CNF.

Ale čo s formulami v logike prvého rádu, kde sú spojky zložito skombinované s kvantifikátormi?

Prvorádové klauzuly a klauzálne teórie

Ujasnime si najprv, aký tvar chceme dosiahnuť.

Definícia 15.7. Nech $\mathcal{L}$ je jazyk logiky prvého rádu.

Literál je atomická formula $P(t_1, \dots, t_m)$ jazyka $\mathcal{L}$ alebo jej negácia $\neg P(t_1, \dots, t_m)$.

Klauzula je všeobecný uzáver disjunkcie literálov, teda uzavretá formula jazyka $\mathcal{L}$ v tvare $\forall x_1 \cdots \forall x_k (L_1 \lor \cdots \lor L_n)$ kde $L_1, \dots, L_n$ sú literály a $x_1, \dots, x_k$ sú *všetky* voľné premenné formuly $L_1 \lor \cdots \lor L_n$. Klauzula môže byť aj *jednotková* ($\forall \vec{x}\, L_1$) alebo *prázdna* ($\square$).

Klauzálna teória je množina klauzúl $\{C_1, \dots, C_n\}$. Môže byť tvorená aj jedinou klauzulou alebo byť prázdna.

Prvorádová ekvivalencia

Postupovať budeme podobne ako vo výrokovologickom prípade: Postupne odstránime z teórie implikácie, negácie zložených formúl, *existenčné kvantifikátory*, disjunkcie konjunkcií, vnorené všeobecné kvantifikátory.

Podľa možnosti budeme používať ekvivalentné úpravy v prvorádovom zmysle:

Definícia 15.8 (Prvorádová ekvivalencia). Množiny formúl S a T sú *(prvorádovo) ekvivalentné* ($S \Leftrightarrow T$) vtt pre každú štruktúru $\mathcal{M}$ a každé ohodnotenie e platí $\mathcal{M} \models S[e]$ vtt $\mathcal{M} \models T[e]$.

Tvrdenie 15.9 (Ekvivalentná úprava). *Nech X, A, B sú formuly a nech* $\mathrm{free}(A) = \mathrm{free}(B)$. *Ak $A \Leftrightarrow B$, tak $X \Leftrightarrow X[A \mid B]$.*

Nahradenie implikácií

Rovnako ako vo výrokovej logike môžeme každú formulu $(A \to B)$ ekvivalentne nahradiť formulou $(\neg A \lor B)$.

Príklad 15.10.

$$\begin{aligned} &\forall x(\mathsf{dobré}(x) \land \mathsf{dieťa}(x) \to \exists y(\mathsf{dostane}(x,y) \land \mathsf{darček}(y))) \\ \Leftrightarrow\ &\forall x(\neg(\mathsf{dobré}(x) \land \mathsf{dieťa}(x)) \lor \exists y(\mathsf{dostane}(x,y) \land \mathsf{darček}(y))) \end{aligned}$$

$$\begin{aligned} &\forall x(\neg \mathsf{dobré}(x) \to \neg\exists y\, \mathsf{dostane}(x,y)) \\ \Leftrightarrow\ &\forall x(\neg\neg \mathsf{dobré}(x) \lor \neg\exists y\, \mathsf{dostane}(x,y)) \end{aligned}$$

Konverzia do negačného normálneho tvaru (NNF)

Definícia 15.11. Formula X je v *negačnom normálnom tvare* (NNF) vtt neobsahuje implikáciu a pre každú jej podformulu $\neg A$ platí, že A je atomická formula.

Formulu bez implikácií do NNF upravíme pomocou

- de Morganovych zákonov pre spojky:

$$\neg(A \land B) \Leftrightarrow \neg A \lor \neg B \qquad\qquad \neg(A \lor B) \Leftrightarrow \neg A \land \neg B$$

- pravidla dvojitej negácie:

$$\neg\neg A \Leftrightarrow A$$

- zovšeobecnení de Morganovych zákonov pre kvantifikátory:

$$\neg\, \exists x\, A \Leftrightarrow \forall x\, \neg A \qquad\qquad \neg\, \forall x\, A \Leftrightarrow \exists x\, \neg A$$

Konverzia do NNF

Tvrdenie 15.12. *Pre každú formulu X existuje formula Y v NNF taká, že $X \Leftrightarrow Y$.*

Príklad 15.13.

$$\begin{aligned} &\forall x(\,\neg(\mathrm{dobr\acute{e}}(x) \land \mathrm{die\check{t}a}(x)) \lor \exists y(\mathrm{dostane}(x,y) \land \mathrm{dar\check{c}ek}(y))\,) \\ \Leftrightarrow\ &\forall x(\,(\,\neg\mathrm{dobr\acute{e}}(x) \lor \neg\mathrm{die\check{t}a}(x)\,) \lor \exists y(\mathrm{dostane}(x,y) \land \mathrm{dar\check{c}ek}(y))\,) \end{aligned}$$

$$\begin{aligned} &\forall x(\,\neg\neg\mathrm{dobr\acute{e}}(x) \lor \neg\exists y\, \mathrm{dostane}(x,y)\,) \\ \Leftrightarrow\ &\forall x(\,\mathrm{dobr\acute{e}}(x) \lor \forall y\, \neg\mathrm{dostane}(x,y)\,) \end{aligned}$$

Skolemizácia

Skolemizácia (podľa nórskeho logika Thoralfa Skolema) je úprava formuly X v NNF, ktorou nahradíme existenčné kvantifikátory *novými* konštantami alebo funkčnými symbolmi.

Podobá sa pravidlu δ v tablách, ale aplikuje sa naraz na všetky existenčné kvantifikátory.

Výsledná formula je v novom, *rozšírenom jazyku*.

Nie je ekvivalentná s pôvodnou, ale je *ekvisplniteľná*.

Definícia 15.14 (Prvorádová ekvi*splniteľnosť*)**.** Množiny formúl S a T sú *(prvorádovo) rovnako splniteľné* (*ekvisplniteľné*, equisatisfiable) vtt S má model vtt T má model.

Skolemizácia — skolemovská konštanta

Ľahký prípad (v podstate pravidlo δ):

Vo formule X sa vyskytuje $\exists y\, A$ *mimo* všetkých oblastí platnosti všeobecných kvantifikátorov.

1. Pridáme do jazyka novú, *skolemovskú konštantu c* (nebola doteraz v jazyku v žiadnej úlohe).

2. Každý výskyt podformuly $\exists y\, A$ v X *mimo* všetkých oblastí platnosti všeobecných kvantifikátorov nahradíme formulou

$$A\{y \mapsto c\}$$

Konštanta c *pomenúva objekt*, ktorý existuje podľa $\exists y\, A$.

Príklad 15.15.

$$\begin{aligned}&\exists x\,(\text{dobré}(x) \land \text{dieťa}(x))\\ &\rightsquigarrow \text{dobré}(\,\text{nejaké\_dobré\_dieťa}\,) \land \text{dieťa}(\,\text{nejaké\_dobré\_dieťa}\,)\end{aligned}$$

Skolemizácia — skolemovská funkcia

Vo formule X sa vyskytuje $\exists y\, A$ *v oblasti platnosti* všeobecných kvantifikátorov premenných $x_1, \ldots, x_n$:

$$X = \cdots \forall x_1(\cdots \forall x_2(\cdots \forall x_n(\cdots \exists y\, A \cdots) \cdots) \cdots) \cdots$$

1. Pridáme do jazyka nový funkčný symbol, *skolemovskú funkciu* f.
2. Každý výskyt $\exists y\, A$ v X v oblasti platnosti kvantifikátorov $\forall x_1, \ldots, \forall x_n$ nahradíme formulou

$$A\{y \mapsto f(x_1, x_2, \ldots, x_n)\}$$

Funkcia f *pomenúva priradenie* objektu y objektom $x_1, \ldots, x_n$.

Príklad 15.16.

$$\begin{aligned}&\forall x(\,\neg\text{dobré}(x) \lor \neg\text{dieťa}(x) \lor \exists y(\text{dostane}(x, y) \land \text{darček}(y))\,)\\ \rightsquigarrow\ &\forall x(\,\neg\text{dobré}(x) \lor \neg\text{dieťa}(x) \lor\\ &\quad(\text{dostane}(x, \text{darček\_pre}(x)\,) \land \text{darček}(\,\text{darček\_pre}(x)\,))\,)\end{aligned}$$

Skolemizácia

Tvrdenie 15.17. *Pre každú uzavretú formulu X v jazyku $\mathcal{L}$ existuje formula Y vo vhodnom rozšírení $\mathcal{L}'$ jazyka $\mathcal{L}$ taká, že Y neobsahuje existenčné kvantifikátory a X a Y sú ekvisplniteľné.*

Príklad 15.18.

$$\begin{aligned}
\exists z\Big(R(z,z) \land \forall x\big(\neg R(x,z) \lor \exists u(R(x,u) \land R(u,z))\\
\lor \forall y\, \exists v(\neg R(y,v) \land R(x,v))\\
\lor \exists v\, \forall w(R(x,v) \land R(v,w))\big)\Big)
\end{aligned}$$

$$\begin{aligned}
\rightsquigarrow R(c,c) \land \forall x\big(\neg R(x,c) \lor (R(x,f_1(x)) \land R(f_1(x),c))\\
\lor \forall y\big(\neg R(y,f_2(x,y)) \land R(x,f_2(x,y))\big)\\
\lor \forall w\big(\neg R(x,f_3(x)) \land R(f_3(x),w)\big)\big)
\end{aligned}$$

Konverzia do PNF

Definícia 15.19. Formula X je v *prenexnom normálnom tvare* (PNF) vtt má tvar $Q_1 x_1\, Q_2 x_2 \cdots Q_n x_n\, A$, kde $Q_i \in \{\forall, \exists\}$, x_i je premenná a A je formula bez kvantifikátorov (*matica* formuly X).

Skolemizovanú formulu v NNF upravíme do PNF opakovanou aplikáciou nasledujúcich transformácií:

- ak x *nemá voľný výskyt* v B,

$$(\forall x\, A \land B) \Leftrightarrow \forall x\, (A \land B) \qquad (B \land \forall x\, A) \Leftrightarrow \forall x\, (B \land A)$$
$$(\forall x\, A \lor B) \Leftrightarrow \forall x\, (A \lor B) \qquad (B \lor \forall x\, A) \Leftrightarrow \forall x\, (B \lor A)$$

- ak sa x má voľný výskyt v B a y je *nová* premenná,

$$(\forall x\, A \land B) \Leftrightarrow (\forall y\, A\{x \mapsto y\} \land B) \quad (B \land \forall x\, A) \Leftrightarrow (B \land \forall y\, A\{x \mapsto y\})$$
$$(\forall x\, A \lor B) \Leftrightarrow (\forall y\, A\{x \mapsto y\} \lor B) \quad (B \lor \forall x\, A) \Leftrightarrow (B \lor \forall y\, A\{x \mapsto y\})$$

Konverzia do PNF

Tvrdenie 15.20. *Pre každú formulu X v NNF bez existenčných kvantifikátorov existuje ekvivalentná formula Y v PNF a NNF.*

Príklad 15.21.

$$\begin{aligned}
\forall x(\,\mathsf{dobr\acute{e}}(x) \lor \forall y\, \neg\mathsf{dostane}(x,y)\,)\\
\Leftrightarrow \forall x\, \forall y\,(\,\mathsf{dobr\acute{e}}(x) \lor \neg\mathsf{dostane}(x,y)\,)
\end{aligned}$$

Pozor! Pre ekvivalentnosť prenexovania je nutné, aby boli premenné viazané rôznymi kvantifikátormi rôzne:

$$(\forall x\, A(x) \lor \forall x\, B(x)) \not\Leftrightarrow \forall x\, (A(x) \lor B(x))$$

$$\begin{aligned}(\forall x\, A(x) \lor \forall x\, B(x)) &\Leftrightarrow \forall x(A(x) \lor \forall x\, B(x)) \\ &\Leftrightarrow \forall x\, \forall y\, (A(x) \lor B(y))\end{aligned}$$

Prenexujte *po jednom* alebo premenujte premenné (ešte pred skolemizáciou)

Konverzia do CNF

Maticu (najväčšiu podformulu bez kvantifikátorov) formuly v PNF upravíme do CNF pomocou distributívnosti a komutatívnosti disjunkcie:

$$\begin{aligned}(A \lor (X \land Y)) &\Leftrightarrow ((A \lor X) \land (A \lor Y)) \\ ((X \land Y) \lor A) &\Leftrightarrow ((X \lor A) \land (Y \lor A))\end{aligned}$$

Príklad 15.22.

$$\begin{aligned}&\forall x(\neg\mathsf{dobré}(x) \lor \neg\mathsf{dieťa}(x) \lor \\ &\qquad (\mathsf{dostane}(x, \mathsf{darček\_pre}(x)) \land \mathsf{darček}(\mathsf{darček\_pre}(x)))) \\ \Leftrightarrow\ &\forall x((\neg\mathsf{dobré}(x) \lor \neg\mathsf{dieťa}(x) \lor \mathsf{dostane}(x, \mathsf{darček\_pre}(x))) \land \\ &\qquad (\neg\mathsf{dobré}(x) \lor \neg\mathsf{dieťa}(x) \lor \mathsf{darček}(\mathsf{darček\_pre}(x))))\end{aligned}$$

Konverzia do klauzálnej teórie

Formula, ktorej matica je v CNF, je ekvivalentná s konjunkciou klauzúl:

$$\forall x(A \land B) \Leftrightarrow (\forall x\, A \land \forall x\, B)$$

a konjunkcia klauzúl je ekvivalentná s ich množinou:

$$\{(\forall x\, A \land \forall x\, B)\} \Leftrightarrow \{\forall x\, A, \forall x\, B\}$$

Príklad 15.23.

$$
\begin{aligned}
&\{\forall x(\, (\neg \text{dobré}(x) \lor \neg \text{dieťa}(x) \lor \text{dostane}(x, \text{darček\_pre}(x))) \land \\
&\qquad (\neg \text{dobré}(x) \lor \neg \text{dieťa}(x) \lor \text{darček}(\text{darček\_pre}(x)))\,)\} \\
\Leftrightarrow\ &\{(\, \forall x(\neg \text{dobré}(x) \lor \neg \text{dieťa}(x) \lor \text{dostane}(x, \text{darček\_pre}(x))) \land \\
&\quad \forall x(\neg \text{dobré}(x) \lor \neg \text{dieťa}(x) \lor \text{darček}(\text{darček\_pre}(x)))\,)\} \\
\Leftrightarrow\ &\{\forall x(\neg \text{dobré}(x) \lor \neg \text{dieťa}(x) \lor \text{dostane}(x, \text{darček\_pre}(x))), \\
&\quad \forall x(\neg \text{dobré}(x) \lor \neg \text{dieťa}(x) \lor \text{darček}(\text{darček\_pre}(x)))\}
\end{aligned}
$$

Konverzia do klauzálnej teórie

Veta 15.24. *Ku každej teórii T v jazyku logiky prvého rádu $\mathcal{L}$ existuje ekvisplniteľná klauzálna teória v nejakom rozšírení $\mathcal{L}'$ jazyka $\mathcal{L}$ o skolemovské konštanty a funkcie.*

Príklad 15.25.

$$
\left\{
\begin{aligned}
&\forall x\, (\text{dobré}(x) \land \text{dieťa}(x) \to \exists y(\text{dostane}(x, y) \land \text{darček}(y))), \\
&\exists x\, (\text{dobré}(x) \land \text{dieťa}(x)), \\
&\forall x\, (\neg \text{dobré}(x) \to \neg \exists y\, \text{dostane}(x, y))
\end{aligned}
\right\} \rightsquigarrow
$$

$$
\left\{
\begin{aligned}
&\forall x_1(\neg \text{dobré}(x_1) \lor \neg \text{dieťa}(x_1) \lor \text{dostane}(x_1, \text{darček\_pre}(x_1))), \\
&\forall x_2(\neg \text{dobré}(x_2) \lor \neg \text{dieťa}(x_2) \lor \text{darček}(\text{darček\_pre}(x_2))), \\
&\text{dobré}(\text{nejaké\_dobré\_dieťa}), \text{dieťa}(\text{nejaké\_dobré\_dieťa}), \\
&\forall x_3\, \forall y\, (\text{dobré}(x_3) \lor \neg \text{dostane}(x_3, y))
\end{aligned}
\right\}
$$

Konverzia do prvorádovej CNF

Dôkaz/algoritmus

T_{I}: Implikácie nahradíme disjunkciami.

T_{N}: *Negačný normálny tvar* (NNF): Presunieme negácie k atómom.

T_{V}: Premenujeme premenné tak, aby každý kvantifikátor viazal inú premennú ako ostatné kvantifikátory.

T_S: *Skolemizácia*: Existenčné kvantifikátory nahradíme substitúciou nimi viazaných premenných za skolemovské konštanty/aplikácie skolemovských funkcií na príslušné všeobecne kvantifikované premenné.

T_P: *Prenexný normálny tvar* (PNF): presunieme všeobecné kvantifikátory na začiatok formuly.

T_D: *Konjunktívny normálny tvar* (CNF): distribuujeme disjunkcie do konjunkcií.

T_K: Odstránime konjunkcie rozdelením konjunktov do samostatne kvantifikovaných klauzúl.

Skolemizácia vytvorí ekvisplniteľnú teóriu, ostatné úpravy sú ekvivalentné.

15.3 Rezolvencia v logike prvého rádu

Rezolvencia a skrátenie zápisu

Prvorádovou rezolvenciou budeme odvodzovať dôsledky klauzálnych teórií.

Dohoda 15.26. Všeobecné kvantifikátory v zápise klauzúl budeme zanedbávať.

Teda namiesto $\forall x_1 \cdots \forall x_n(L_1 \vee \cdots \vee L_m)$ píšeme iba $L_1 \vee \cdots \vee L_m$.

Úsudky s klauzulami

Príklad 15.27. Každého má niekto rád jeho najlepší kamarát/najlepšia kamarátka (NK):

$$\forall y\, \mathsf{r}(\mathsf{nk}(y), y)$$

Kto má rád Dadu, toho Edo nemá rád:

$$\forall x(\neg\mathsf{r}(x, \mathsf{D}) \vee \neg\mathsf{r}(\mathsf{E}, x)),$$

Teda aj Dadu má niekto rád:

$$\mathsf{r}(\mathsf{nk}(\mathsf{D}), \mathsf{D})$$

Ak Dadin NK má rád Dadu, tak ho Edo nemá rád:

$$\neg \mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \vee \neg \mathrm{r}(\mathrm{E}, \mathrm{nk}(\mathrm{D})).$$

Preto (výrokovou rezolvenciou):

$$\frac{\begin{array}{c}\mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \\ (\neg\, \mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \vee \neg \mathrm{r}(\mathrm{E}, \mathrm{nk}(\mathrm{D})))\end{array}}{\neg \mathrm{r}(\mathrm{E}, \mathrm{nk}(\mathrm{D}))}$$

Úsudky s klauzulami

Celý úsudok z príkladu aj s dosadeniami:

$$\frac{\begin{array}{c}\forall y\, \mathrm{r}(\mathrm{nk}(y), y) \\ \forall x(\neg \mathrm{r}(x, \mathrm{D}) \vee \neg \mathrm{r}(\mathrm{E}, x))\end{array}}{\neg \mathrm{r}(\mathrm{E}, \mathrm{nk}(\mathrm{D}))}$$

Aby sme klauzuly mohli rezolvovať, potrebovali sme substitúciu:

$$\sigma = \{x \mapsto \mathrm{nk}(\mathrm{D}), y \mapsto \mathrm{D}\}$$

Po substitúcii σ majú komplementárne literály rovnaké argumenty predikátu:

$$\begin{aligned} \mathrm{r}(\mathrm{nk}(y), y)\sigma &= \mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \\ \neg \mathrm{r}(x, \mathrm{D})\sigma &= \neg \mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \end{aligned}$$

Unifikátory

Definícia 15.28. Nech A, B sú postupnosti symbolov, σ je substitúcia. Substitúcia σ je *unifikátorom* A a B vtt $A\sigma = B\sigma$.

Príklad 15.29.

- $A_1 = \mathrm{r}(\mathrm{filantrop}, y)$, $B_1 = \mathrm{r}(x, \mathrm{D})$,
  $\sigma_1 = \{x \mapsto \mathrm{filantrop}, y \mapsto \mathrm{D}\}$
- $A_2 = \mathrm{r}(\mathrm{nk}(y), y)$, $B_2 = \mathrm{r}(x, \mathrm{D})$,
  $\sigma_2 = \{x \mapsto \mathrm{nk}(\mathrm{D}), y \mapsto \mathrm{D}\}$

- $A_3 = \mathsf{r}(\mathsf{nk}(y), y)$, $B_3 = \mathsf{r}(\mathsf{E}, x)$,
  $\sigma_3 =$??? *neexistuje!*
- $A_4 = \mathsf{r}(\mathsf{nk}(y), y)$, $B_4 = \mathsf{r}(x, x)$,
  $\sigma_4 =$??? *neexistuje!*

Skladanie substitúcií, premenovanie premenných

Definícia 15.30. Nech $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ a $\theta = \{y_1 \mapsto s_1, \dots, y_m \mapsto s_m\}$ sú substitúcie. *Zložením (kompozíciou) substitúcií* σ a θ je substitúcia $\sigma\theta = \{x_1 \mapsto t_1\theta, \dots, x_n \mapsto t_n\theta, y_{i_1} \mapsto s_{i_1}, \dots, y_{i_k} \mapsto s_{i_k}\}$, kde $\{y_{i_1}, \dots, y_{i_k}\} = \{y_1, \dots, y_m\} \setminus \{x_1, \dots, x_n\}$.

Príklad 15.31.
$$\begin{aligned}
\sigma &= \{x \mapsto \mathsf{nk}(y),\ z \mapsto y\} \\
\theta &= \{y \mapsto \mathsf{filantrop}\} \\
\sigma\theta &= \{x \mapsto \mathsf{nk}(\mathsf{filantrop}), \\
&\qquad z \mapsto \mathsf{filantrop},\ y \mapsto \mathsf{filantrop}\}
\end{aligned}$$

Unifikátory

Definícia 15.32. Nech A, B sú postupnosti symbolov, σ a θ sú substitúcie.

σ je *všeobecnejšia* ako θ vtt existuje subst. γ taká, že $\theta = \sigma\gamma$.

σ je *najvšeobecnejším unifikátorom* A a B vtt

- σ je unifikátorom A a B a zároveň
- pre každý unifikátor θ A a B je σ všeobecnejšia ako θ.

Príklad 15.33. $A_5 = \mathsf{r}(\mathsf{nk}(x), y)$, $B_5 = \mathsf{r}(u, v)$

- $\sigma_{51} = \{u \mapsto \mathsf{nk}(\mathsf{D}), v \mapsto y, x \mapsto \mathsf{D}\}$ $\theta_{51} = \{u \mapsto \mathsf{nk}(\mathsf{D}), v \mapsto \mathsf{Biba}, x \mapsto \mathsf{D}, y \mapsto \mathsf{Biba}\}$ $\gamma_{51} = \{y \mapsto \mathsf{Biba}\}$
- $\sigma_{52} = \{u \mapsto \mathsf{nk}(x), v \mapsto y\}$ $\theta_{52} = \{u \mapsto \mathsf{nk}(\mathsf{D}), v \mapsto y, x \mapsto \mathsf{D}\}$ $\gamma_{52} = \{x \mapsto \mathsf{D}\}$

Unifikátory a rezolvencia

Príklad 15.34.

$$\frac{\mathsf{r}(\mathsf{nk}(y), y)\sigma \qquad (\neg\mathsf{r}(x, \mathsf{D}) \lor \neg\mathsf{r}(\mathsf{E}, x))\sigma}{\neg\mathsf{r}(\mathsf{E}, x)\sigma}$$

$$\sigma = \{x \mapsto \mathsf{nk}(\mathsf{D}), y \mapsto \mathsf{D}\}$$

$$\frac{\mathsf{r}(\mathsf{nk}(\mathsf{D}), \mathsf{D}) \qquad \neg\,\mathsf{r}(\mathsf{nk}(\mathsf{D}), \mathsf{D}) \lor \neg\mathsf{r}(\mathsf{E}, \mathsf{nk}(\mathsf{D}))}{\neg\mathsf{r}(\mathsf{E}, \mathsf{nk}(\mathsf{D}))}$$

Unifikátory a rezolvencia

Príklad 15.35. Rovnaké premenné v klauzulách môžu zabrániť unifikácii literálov:

$$\mathsf{r}(\mathsf{nk}(x), x) \qquad\qquad \neg\mathsf{r}(x, \mathsf{D}) \lor \neg\mathsf{r}(\mathsf{E}, x)$$

Klauzuly sú však všeobecne kvantifikované *nezávisle* od seba. Premenovanie premenných v jednej z nich nezmení jej význam, ale umožní unifikáciu (viď predchádzajúci príklad).

$$\mathsf{r}(\mathsf{nk}(y), y) \qquad\qquad \neg\mathsf{r}(x, \mathsf{D}) \lor \neg\mathsf{r}(\mathsf{E}, x)$$

Definícia 15.36. *Premenovaním premenných* je každá substitúcia $\sigma = \{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}$, kde $y_1, \dots, y_n$ sú premenné.

Prvorádová rezolvencia — pravidlá

Definícia 15.37. Nech C a D sú prvorádové klauzuly, nech A a B sú atómy, nech L a K sú literály.

Rezolvencia (angl. resolution) je odvodzovacie pravidlo

$$\frac{A \lor C \qquad \neg B \lor D}{(C\theta \lor D)\sigma} \qquad \begin{array}{l}\sigma \text{ je unifikátor } A\theta \text{ a } B,\\ \theta \text{ je premenovanie premenných.}\end{array}$$

Faktorizácia (angl. factoring) je odvodzovacie pravidlo

$$\frac{L \lor K \lor C}{(L \lor C)\sigma} \quad \sigma \text{ je unifikátor } L \text{ a } K.$$

Faktorizácia je zovšeobecnenie idempotencie pri výrokovej rezolvencii.

Rezolvencia postupne

Rezolvenciu

$$\frac{\neg \mathsf{P}(x) \lor \neg \mathsf{Q}(y, x) \lor \mathsf{R}(\mathsf{f}(x, y), y) \qquad \neg \mathsf{R}(x, \mathsf{c})}{\neg \mathsf{P}(x) \lor \neg \mathsf{Q}(\mathsf{c}, x)}$$

si môžeme predstaviť ako postupný proces:

$$\begin{array}{lcc}
 & & \neg \mathsf{R}(x, \mathsf{c}) \\
\text{premenovanie:} & & \downarrow \{x \mapsto z\} \\
 & \neg \mathsf{P}(x) \lor \neg \mathsf{Q}(y, x) \lor \mathsf{R}(\mathsf{f}(x, y), y) & \neg \mathsf{R}(z, \mathsf{c}) \\
\text{unifikácia:} & \downarrow \quad \{y \mapsto \mathsf{c}, z \mapsto \mathsf{f}(x, \mathsf{c})\} & \downarrow \\
 & \neg \mathsf{P}(x) \lor \neg \mathsf{Q}(\mathsf{c}, x) \lor \mathsf{R}(\mathsf{f}(x, \mathsf{c}), \mathsf{c}) & \neg \mathsf{R}(\mathsf{f}(x, \mathsf{c}), \mathsf{c}) \\
\hline
 & & \neg \mathsf{P}(x) \lor \neg \mathsf{Q}(\mathsf{c}, x)
\end{array}$$

Rezolvenčné odvodenie a zamietnutie

Definícia 15.38. Nech T je klauzálna teória.

Rezolvenčným odvodením z T je každá (aj nekonečná) postupnosť klauzúl $\mathcal{Z} = (C_1, C_2, \dots, C_n, \dots)$, kde každá klauzula C_i, $1 \le i \le n$, je:

- prvkom T, alebo
- odvodená pravidlom rezolvencie z klauzúl C_j a C_k, ktoré sa v $\mathcal{Z}$ nachádzajú pred C_i (teda $j, k < i$), alebo
- odvodená pravidlom faktorizácie z klauzuly C_j, ktorá sa v $\mathcal{Z}$ nachádza pred C_i (teda $j < i$).

Zamietnutím T (angl. *refutation*) je každé konečné rezolvenčné odvodenie $\mathcal{Z} = (C_1, C_2, \dots, C_n)$, kde $C_n = \square$.

Refutačná korektnosť a úplnosť rezolvencie

Veta 15.39 (Refutačná korektnosť a úplnosť rezolvencie)**.** *Nech T je klauzálna teória. Potom existuje zamietnutie T vtt T je nesplniteľná.*

Príklad 15.40. Dokážme nesplniteľnosť:

$$\left\{\begin{array}{c} \forall x\, \mathrm{r}(\mathrm{nk}(x), x), \\ \forall x\, \forall y\, \mathrm{r}(x, \mathrm{nk}(y)), \\ \forall x(\neg\mathrm{r}(x, \mathrm{D}) \lor \neg\mathrm{r}(\mathrm{E}, x)) \end{array}\right\}$$

Rezolvencia a vyplývanie

Pretože každú teóriu môžeme transformovať na ekvisplniteľnú klauzálnu teóriu, dostávame:

Dôsledok 15.41 (Úplnosť rezolvencie)**.** *Nech T je teória, nech X je uzavretá formula. Nech $T'_X = \{C_1, \dots, C_n\}$ je klauzálna teória ekvisplniteľná s $T \cup \{\neg X\}$. Potom z T vyplýva X vtt existuje zamietnutie T'_X.*

Literatúra

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

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

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.