

Logika pre informatikov a Úvod do matematickej logiky

Poznámky z prednášok

Ján Kl'uka, Ján Mazák, Jozef Šiška

Letný semester 2024/2025

Posledná aktualizácia: 2. marca 2025

Obsah

P1	Úvod. Atomické formuly a štruktúry	3
0	Úvod	3
0.1	O logike	3
0.2	O kurzoch LPI a UdML	12
1	Atomické formuly a štruktúry	13
1.1	Syntax atomických formúl	19
1.2	Štruktúry	23
1.3	Sémantika atomických formúl	26
1.4	Zhrnutie	27

P2	Výrokovologické spojky a ohodnotenia	29
2	Výrokovologické spojky a ohodnotenia	29
2.1	Boolovské spojky	30
2.2	Implikácia	36
2.3	Ekvivalencia	38
2.4	Správnosť a vernosť formalizácie	39
2.5	Syntax výrokovologických formúl	42
2.6	Sémantika výrokovologických formúl	51
2.7	Teórie a ich modely	53
2.8	Výrokovologické ohodnotenia	54
P3	Výrokovologické vyplývanie, sémantické vlastnosti formúl a ekvivalencia	61
3	Výrokovologické vyplývanie	61
3.1	Výrokovologické teórie a modely	62
3.2	Vyplývanie, nezávislosť a nesplniteľnosť	63
4	Sémantické vlastnosti a vzťahy formúl	70
4.1	Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly	70
4.2	Hľadanie ohodnotení	75
4.3	Ekvivalencia	77
4.4	Vzťah tautológií, vyplývania a ekvivalencie	81
4.5	Ekvivalentné úpravy a CNF	83
4.6	CNF vs. XOR	89

1. prednáška

Úvod

Atomické formuly a štruktúry

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.

Historicky sa logika venovala najmä filozofickým hľadiskám, dnes kladieme väčší dôraz na výpočtové aspekty.

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. (Úzko súvisí s jazykom: čím viac možno v jazyku vyjadriť, tým ťažšie je definovať či algoritmicke rozhodovať logické vyplývanie.)

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: „*Môžu noví známi prísť na párty tak, aby boli všetky podmienky splnené? Ak áno, v akých zostavách?*“

Priamočiaro (aj keď práce) 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		

Možné stavy sveta a modely

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

⊢ stavy, v ktorých je pravdivá — *modely* teórie,

⊣ 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.

K	J	S	P0	P1	P2	P3	
n	n	n	n				≠ P0, P1, P2, P3
n	n	p	p	p	p	n	≠ P0, P1, P2, P3
n	p	n	p	p	n		≠ P0, P1, P2, P3
n	p	p	p	p	n		≠ P0, P1, P2, P3
p	n	n	p	p	p	p	≠ P0, P1, P2, P3
p	n	p	p	n			≠ P0, P1, P2, P3
p	p	n	p	p	p	p	≠ P0, P1, P2, P3
p	p	p	p	n			≠ P0, P1, P2, P3

Logické dôsledky

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

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

K	J	S	P0	P1	P2	P3	
n	n	n	n				≠ P0, P1, P2, P3
n	n	p	p	p	p	n	≠ P0, P1, P2, P3
n	p	n	p	p	n		≠ P0, P1, P2, P3
n	p	p	p	p	n		≠ P0, P1, P2, P3
p	n	n	p	p	p	p	≠ P0, P1, P2, P3
p	n	p	p	n			≠ P0, P1, P2, P3
p	p	n	p	p	p	p	≠ P0, P1, P2, P3
p	p	p	p	n			≠ P0, P1, P2, P3

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, existuje *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.

K	J	S	
n	n	n	⊭ P0, P1, P2, P3
n	n	p	⊭ P0, P1, P2, P3
n	p	n	⊭ P0, P1, P2, P3
n	p	p	⊭ P0, P1, P2, P3
p	n	n	⊭ P0, P1, P2, P3
p	n	p	⊭ P0, P1, P2, P3
p	p	n	⊭ P0, P1, P2, P3
p	p	p	⊭ P0, P1, P2, P3

Matematická logika

Matematická logika

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

Rozvinula sa koncom 19. a v prvej polovici 20. storočia hlavne vďaka *Hilbertovmu programu* — snahe vybudovať základy matematiky bez sporov a paradoxov, mechanizovať overovanie dôkazov alebo priamo hľadanie matematických viet.

Matematická logika a informatika

Informatika sa vyvinula z matematickej logiky (J. von Neumann, A. Turing, A. Church, ...)

Väčšina *programovacích jazykov* obsahuje logické prvky:

- $\text{all}(x > m \text{ for } x \text{ in } \text{arr}),$

fragmenty niektorých sú priamo preložiteľné na logické formuly:

- `SELECT t1.x FROM t1 JOIN t2 ON t1.y = t2.y WHERE t1.y > 25,`

niektoré (Prolog, Datalog) 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.

Matematická logika a informatika

Veľa otázok v logike je *algoritmických*:

- Možno usudzovanie pre danú triedu jazykov automatizovať?
- Dá sa nájsť dôkaz pre tvrdenia s takouto štruktúrou dostatočne rýchlym algoritmom?

Výpočtová logika hľadá algoritmické riešenia problémov pre rôzne triedy logických jazykov. Aplikovateľné na iné ťažké problémy (grafové, plánovacie, vysvetľovanie, ...) vyjadriteľné v príslušnej triede.

Logika umožňuje hľadať všeobecné odpovede.

- Ak možno vlastnosť grafu popísať *prvorádovou formulou s najviac dvomi kvantifikátormi* a zároveň ..., existuje pomerne rýchly algoritmus, ktorý rozhodne, či daný graf túto vlastnosť má.

Matematická logika a informatika

Automatizované dokazovače: napr. v r. 1996 počítač dokázal Robbins Conjecture, ktorá odolávala ľudskej snahe 60 rokov.

Donedávna malo automatizované dokazovanie nepresvedčivé výsledky a niektoré oblasti výskumu boli relatívne mŕtve, napr. expertné systémy.

S novými modelmi umelej inteligencie však oživa, napr. AlphaProof rieši 84% úloh z IMO.

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 syntaktická analýza, výnimky, obraty s ustáleným významom, ...

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

Problémy z iných oblastí opísané v prirodzenom jazyku musíme najprv *sformalizovať*, a potom naň môžeme použiť aparát mat. 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: Chlieb sa predáva v potravinách. Videl som dievča v sále *s ďalekohľadom*.
- Ťažko syntakticky analyzovateľné tvrdenia:

Vlastníci bytov a nebytových priestorov v dome prijímajú rozhodnutia na schôdzi vlastníkov dvojtreťinovou 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: *Nikto 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?

$$k = 3 \cdot m$$

$$k + m = 12$$

Stretli ste sa už aj s formálnym jazykom výrokovej logiky.

Príklad 0.6. Sformalizujme náš pártý príklad:

P0: Nieкто z trojice Kim, Jim, Sarah pôjde na pártý. $p(K) \vee p(J) \vee p(S)$

P1: Sarah nepôjde na pártý, ak pôjde Kim. $p(K) \rightarrow \neg p(S)$

P2: Jim pôjde na pártý, len ak pôjde Kim. $p(J) \rightarrow p(K)$

P3: Sarah nepôjde bez Jima. $\neg p(J) \rightarrow \neg p(S)$

Všimnite si, koľko vetných konštrukcií v slovenčine zodpovedá jednej formálnej spojke \rightarrow .

Logika prvého rádu

Jazyk logiky prvého rádu (FOL) je jeden zo základných formálnych jazykov, ktorými 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.

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

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

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

⋮

Sú korektné, ale nie vždy úplné.

Poznáte už aj jeden logický kalkul – ekvivalentné úpravy.

Symbolické vs. aproximačné výpočty

Symbolický výpočet:

$$\begin{aligned}x^2 &= 2 \\(x + \sqrt{2})(x - \sqrt{2}) &= 0 \\x &= \pm\sqrt{2}\end{aligned}$$

Symbols majú jasný význam, výpočet pozostáva z overiteľných krokov, ktoré samé osebe „dávajú zmysel“.

Aproximačný výpočet:

$$\begin{aligned}x^2 &= 2 \\x &\in (1, 2) \\x &\in (1.4, 1.5) \\&\dots \\x &\approx 1.4142\end{aligned}$$

Kroky výpočtu nenesú samé osebe zmysel, sú to len aritmetické operácie, výsledok je nespoľahlivý.

Symbolické vs. aproximačné výpočty

Symbolické:

- úprava výrazov
- derivovanie elem. f.
- matematické dôkazy
- expertné systémy (kľúč na určovanie druhu húb)

Aproximačné / data-driven:

- numerická optimalizácia
- strojové učenie
- neurónové siete
- LLM (ChatGPT)

Symbolické vs. aproximačné výpočty

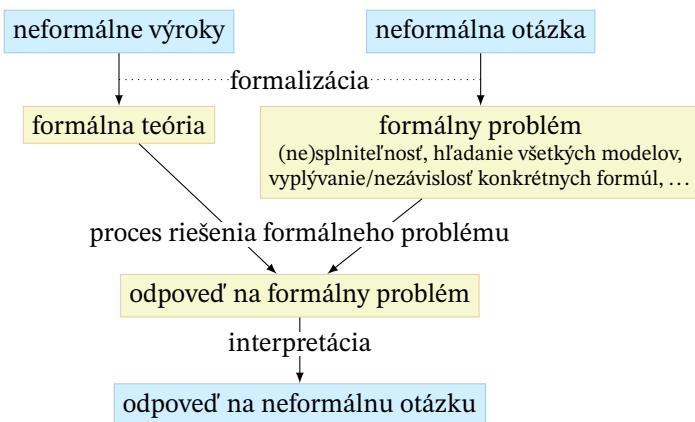
Nevýhodou výpočtov založených na dátach je chýbajúca kontrola nad smerovaním výpočtu a nemožnosť pochopenia/overenia.

Napr. ChatGPT generuje text, ktorý je „pravdepodobný“ (vzhľadom na texty v tréningových vstupoch). Nevie merať ani overovať správnosť. Na začiatku nezvládal ani sčítanie jednociferných čísel; užitočnosť a spoľahlivosť

LLM výrazne stúpne, ak majú prístup ku kalkulačke, ktorá vie robiť symbolickú aritmetiku.

V kontraste s tým symbolické kalkuly garantujú správnosť. Ukážeme si dva (tablá a rezolvenciu), existuje mnoho ďalších (napr. AlphaProof používa Lean).

Schéma riešenia problémov pomocou logiky



0.2 O kurzoch LPI a UdML

Prístup k logike na tomto predmete

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

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

Teoretická časť:

- Matematické definície logických pojmov (výrok, model, logický dôsledok, dôkaz, ...)
- Dôkazy ich vlastností

Praktická časť

- *Dátové štruktúry* na reprezentáciu logických objektov

- *Algoritmické riešenie logických problémov*
- *Formalizácia rôznych problémov v logických jazykoch a ich riešenie nástrojmi na riešenie logických problémov*

Organizácia kurzu — rozvrh, kontakty, pravidlá

Organizácia — rozvrh, kontakty a pravidlá absolvovania — je popísaná na oficiálnych webových stránkach predmetov:

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



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



1 Atomické formuly a štruktúry

Problémy s výrokmi

Ukážeme si, prečo je formalizácia pomocou výrokov nedostatočná.

Čo je *výrok*? Oznamovacia veta,

- ktorej sa dá priradiť pravdivostná hodnota.
- pre ktorú má zmysel otázka na jej platnosť, správnosť, pravdivosť.

Problémy s výrokmi

Nech x je kladné reálne číslo. Potom $x^2 > 0$. [5mm]

Počet hviezd je nepárny. [5mm]

Zajtra vznikne jadro hélia. [5mm]

Odteraz až navždy každú sekundu vznikne jadro hélia.

Problémy s výrokmi

Postupnosť 0, 1, 2, 3, 4, 5, 6, ... je rastúca.[4mm]

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?
- Aký je význam troch bodiek ako symbolu? Môže byť súčasťou výroku popis algoritmu?
- Môže byť výrok nekonečne dlhý?

Problémy s výrokmi

Bu bayonot emas.[4mm]

- Znamená „toto nie je výrok“ v uzbečtine. Aký jazyk je prípustný?
- Čo ak má v rôznych jazykoch ten istý reťazec rôzny význam?
- Môže výrok hovoriť o sebe?

Môže viesť k paradoxom: Zoberme množinu X všetkých množín, ktoré neobsahujú samé seba. Je veta „ X patrí do X “ výrok? Nemôže to byť ani pravda, ani nepravda, pritom to vyzerá ako neškodné matematické tvrdenie.

Problémy s výrokmi

Ako navrhnúť jazyk logiky?

- Bez akýchkoľvek odkazov na pravdivosť (ale zároveň aby pravdivosť bolo možné bez paradoxov neskôr definovať).
- Presný a jednoznačný: vieme pomocou jednoduchých pravidiel rozhodnúť, či reťazec je tvrdením v jazyku alebo nie.
- Logická štruktúra (spojky, kvantifikátory) musí byť oddelená od popisovaného sveta.

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*).

Jazyk logiky: príklad

Každý človek umrie.	$\forall x(C(x) \rightarrow U(x))$
Sokrates je človek.	$C(s)$
Sokrates umrie.	$U(s)$

Konštanty: s Predikáty: C, U

Jazyk logiky: príklad

$\forall x \in \mathbb{R} : x > 0 \rightarrow x \text{ je celé číslo}$

$\forall x(\in(x, \mathbb{R}) \rightarrow (>(x, 0) \rightarrow \in(x, \mathbb{Z})))$

Konštanty: 0, \mathbb{R} , \mathbb{Z} Predikáty: $>$, \in

Konštanty aj predikáty sú úplne iné, ale logické spojky, kvantifikátory a zátvorkovanie majú uvedené dva jazyky spoločné.

Atómy

Atómy zodpovedajú jednoduchým výrokom — nemajú žiadnu vnútornú logickú štruktúru.

Sokrates je človek.	$C(s)$
$7 > 0$	$>(7, 0)$
Juraj má psa Rexa.	$ma_psa(Juraj, Rexo)$

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 nie je doma. |
| ✓ Jarka vidí Mila. | ✗ Nieкто je doma. |
| ✗ Milo beží, ale Jarka ho nevidí. | ✓ Súčet 2 a 2 je 3. |
| ✗ Jarka vidí všetkých. | ✓ Prezidentkou SR je Zuzana Čaputová. |
| ✓ Jarka dala Milovi Bobyho v piatok. | |

Atomické formuly sa skladajú z *individuových konštánt* a *predikátových symbolov*.

Individuové konštanty

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

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

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

Individuová konštanta:

- vždy pomenúva skutočný, existujúci objekt (na rozdiel od vlastného mena *Yeti*);

- nikdy nepomenúva viac objektov (na rozdiel od vlastného mena *Jarka*).
- Objekt z domény, ktorú chceme prvorádovým jazykom opísať,
- *môže byť* pomenovaný aj *viacerými* individuovými konštantami (napr. Prezidentka SR a Zuzana Čaputová);
 - *nemusí* mať žiadne meno.

Predikátové symboly a arita

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

Zodpovedajú

- prísudkom v slovenských vetách,
- množinám alebo reláciám v matematike,
- identifikátorom funkcií s boolovskou návratovou hodnotou.

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

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

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

Dohoda 1.3. Aritu budeme *niekedy* písať ako horný index symbolu. Napríklad beží¹, vidí², dal⁴, <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 mladší² môže označovať vzťah „*x* je mladší ako *y*“ presne.

Predikát mladý¹ 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

$$\text{predikát}(\text{argument}_1, \text{argument}_2, \dots, \text{argument}_k),$$

alebo

$$\text{argument}_1 \doteq \text{argument}_2,$$

pričom *k* je arita predikátu, a $\text{argument}_1, \dots, \text{argument}_k$ sú (nateraz) individuové 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 individuové konštanty jednoznačne označujú objekty.

Formalizácia jednoduchých výrokov

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

Nie je to jednoznačný proces.

V spojení s *návrhom vlastného jazyka* (konštánt a predikátov) je typicky *iteratívna*.

- Postupne zisťujeme, aké predikáty a konštanty potrebujeme, upravujeme predchádzajúce formalizácie.
- Zanedbávame nepodstatné detaily.
- Doterajší jazyk sa snažíme využiť čo najlepšie.

Návrh jazyka popri formalizácii

Príklad 1.7. A_1 : Jarka dala Milovi Bobbyho.

↪ ~~d(Jarka)~~ ~~dalBobyho(Jarka, Milo)~~ dal(Jarka, Milo, Boby)

A_2 : Evka dostala Bobbyho od Mila.

↪ ~~dalBobyho(Milo, Evka)~~ dal(Milo, Evka, Boby)

A_3 : Evka dala Jarke Čilku.

↪ ~~dalČilku(Evka, Jarka)~~ dal(Evka, Jarka, Čilka)

A_4 : Bobby je pes.

↪ pes(Boby)

Návrh jazyka pri formalizácii

Minimalizujeme počet predikátov, uprednostňujeme flexibilnejšie, viacúčelovejšie (dal^3 pred dalBobyho^2 a dalČilku^2).

Dosiahneme

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

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.

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

Pojmy (napr. *atomická formula*) môžeme zadať 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.

Symbols jazyka atomických formúl logiky prvého rádu

Z čoho sa skladajú atomické formuly?

Definícia 1.8. *Symbolmi jazyka \mathcal{L} atomických formúl logiky prvého rádu sú mimologické, logické a pomocné symboly, pričom:*

Mimologickými symbolmi sú

- *individuové 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* $\text{ar}_{\mathcal{L}}(P) \in \mathbb{N}^+$.

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 $\Sigma_{\mathcal{L}} = \mathcal{C}_{\mathcal{L}} \cup \mathcal{P}_{\mathcal{L}} \cup \{=, (,), ,\}$.

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

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

Príklad 1.10. Príklad o návštevníkoch party by sme mohli sformalizovať v jazyku \mathcal{L}_{party} , kde

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

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 1.11. Individuové 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 1.12. 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 individuové 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 individuové 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 UTI/FoJa 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

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

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

Príklady atómov jazyka

Príklad 1.13. V jazyku \mathcal{L}_{dz} , kde $\mathcal{C}_{\mathcal{L}_{\text{dz}}} = \{\text{Boby, Cilka, Evka, Jarka, Milo}\}$, $\mathcal{P}_{\mathcal{L}_{\text{dz}}} = \{\text{dal, pes}\}$, $\text{ar}_{\mathcal{L}_{\text{dz}}}(\text{dal}) = 3$, $\text{ar}_{\mathcal{L}_{\text{dz}}}(\text{pes}) = 1$, sú *okrem iných* rovnostné atómy:

Boby \doteq Boby

Cilka \doteq Boby

Evka \doteq Jarka

Boby \doteq Cilka

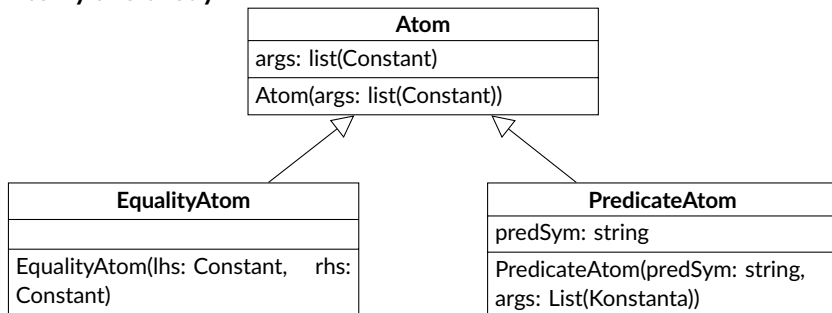
a predikátové atómy:

pes(Cilka)

dal(Cilka, Milo, Boby)

dal(Jarka, Evka, Milo).

Atómy ako triedy



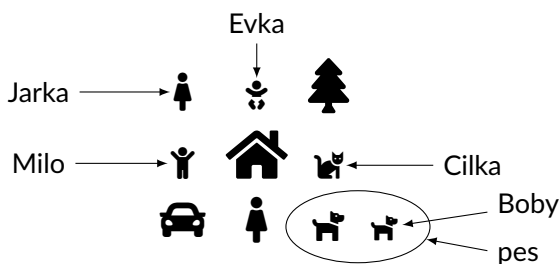
1.2 Štruktúry

Vyhodnotenie atomickej formuly

Ako zistíme, či je atomická formula `pes(Boby)` *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 *Boby*;
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

Potrebujeme vedieť:

- ktoré objekty sú v popisovanej situácii prítomné,
- množina všetkých týchto objektov — *doména*;
- jednoznačné priradenie významu všetkým individuovým konštantám a predikátom z jazyka \mathcal{L}
- *interpretačná funkcia*;
- pre každú individuovú konštantu c z jazyka \mathcal{L} , ktorý *objekt* z domény konštanty 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

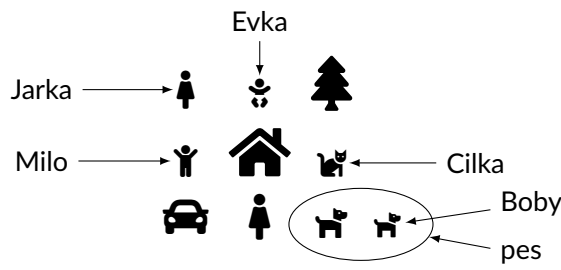
Definícia 1.14. Nech \mathcal{L} je jazyk atomických formúl logiky prvého rádu. *Štruktúrou* pre jazyk \mathcal{L} (niekedy *interpretáciou* jazyka \mathcal{L}) nazývame dvojicu $\mathcal{M} = (D, i)$, kde D je ľubovoľná neprázdna množina nazývaná *doména* štruktúry \mathcal{M} ; i je zobrazenie, nazývané *interpretačná funkcia* štruktúry \mathcal{M} , ktoré

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

Dohoda 1.15. Štruktúry označujeme veľkými písanými písmenami \mathcal{M}, \mathcal{N} ,

....

Príklad štruktúry



Príklad 1.16.

$$\begin{aligned} \mathcal{M} &= (D, i), \quad D = \left\{ \text{person}, \text{person}, \text{tree}, \text{person}, \text{house}, \text{cat}, \text{car}, \text{person}, \text{dog}, \text{dog} \right\} \\ i(\text{Boby}) &= \text{dog} & i(\text{Cilka}) &= \text{cat} \\ i(\text{Evka}) &= \text{person} & i(\text{Jarka}) &= \text{person} & i(\text{Milo}) &= \text{person} \\ i(\text{pes}) &= \{ \text{dog}, \text{dog} \} \\ i(\text{dal}) &= \left\{ (\text{person}, \text{person}, \text{dog}), (\text{person}, \text{person}, \text{dog}), (\text{person}, \text{person}, \text{cat}) \right\} \end{aligned}$$

Štruktúra ako informatický objekt

Štruktúru sme definovali pomocou *matematických* objektov.

Aký *informatický* objekt sa podobá na štruktúru? *Databáza*.

Predikátové symboly jazyka ~ zjednodušená databázová schéma (arita ~ počet stĺpcov)

Interpretácia predikátových symbolov ~ konkrétne tabuľky s dátami (doména ~ dátový typ)

$i(\text{pes}^1)$	$i(\text{dal}^3)$			$i(\text{clovek}^2)$	
1	1	2	3	Meno	Rodné číslo
dog	person	person	dog	Petra	1234
dog	person	person	dog	Michal	5678
	person	person	cat		

Štruktúra ako informatický objekt

Dopytom zodpovedajú logické formuly:

„rodné čísla ľudí, ktorí sa volajú Michal“ $= \{rc \mid \text{clovek}(\text{Michal}, rc)\}$
„rodné čísla všetkých ľudí“ $= \{rc \mid \exists m \text{ clovek}(m, rc)\}$

Štruktúry — upozornenia

Štruktúr pre daný jazyk je *nekonečne veľa*.

Doména štruktúry

- *nesúvisí so zamýšľaným významom* interpretovaného jazyka;
- môže mať ľubovoľné prvky;
- 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 1.17 (Štruktúra s nekonečnou doménou). $\mathcal{M} = (\mathbb{N}, i)$ $i(\text{pes}) = \{2n \mid n \in \mathbb{N}\}$ $i(\text{dal}) = \{(n, m, n + m) \mid n, m \in \mathbb{N}\}$
 $i(\text{Boby}) = 0$ $i(\text{Cilka}) = 1$ $i(\text{Evka}) = 3$ $i(\text{Jarka}) = 5$ $i(\text{Milo}) = 0$

1.3 Sémantika atomických formúl

Pravdivosť atomickej formuly v štruktúre

Ako zistíme, či je atomická formula pravdivá v štruktúre?

Definícia 1.18. 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} skráteno 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 1.19 (Určenie pravdivosti atómov v štruktúre).

$$\begin{aligned} \mathcal{M} &= (D, i), \quad D = \left\{ \text{ľudia, strom, dieťa, dom, mačka, auto, žena, pes, pes} \right\} \\ i(\text{Boby}) &= \text{ľudia} \quad i(\text{Cilka}) = \text{mačka} \\ i(\text{Evka}) &= \text{ľudia} \quad i(\text{Jarka}) = \text{ľudia} \quad i(\text{Milo}) = \text{dieťa} \\ i(\text{pes}) &= \{ \text{ľudia}, \text{ľudia} \} \\ i(\text{dal}) &= \left\{ (\text{dieťa}, \text{ľudia}, \text{ľudia}), (\text{ľudia}, \text{ľudia}, \text{ľudia}), (\text{ľudia}, \text{ľudia}, \text{mačka}) \right\} \end{aligned}$$

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

Atóm $\text{dal}(\text{Evka}, \text{Jarka}, \text{Cilka})$ je *pravdivý* v \mathcal{M} , t.j., $\mathcal{M} \models \text{dal}(\text{Evka}, \text{Jarka}, \text{Cilka})$, lebo $(i(\text{Evka}), i(\text{Jarka}), i(\text{Cilka})) = (\text{ľudia}, \text{ľudia}, \text{mačka}) \in i(\text{dal})$.

Atóm $\text{Cilka} \doteq \text{Boby}$ *nie je pravdivý* v \mathcal{M} , t.j., $\mathcal{M} \not\models \text{Cilka} \doteq \text{Boby}$, lebo $i(\text{Cilka}) = \text{mačka} \neq \text{ľudia} = i(\text{Boby})$.

1.4 Zhrnutie

Zhrnutie

- Logika prvého rádu je rodina formálnych jazykov.
- Každý jazyk logiky prvého rádu je daný neprázdnu množinou individuových 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 a ohodnotenia

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 a ohodnotenia

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 šiel na prechádzku s ich psom. Ten by inak musel čakať na Jarku, ktorá sa zo školy 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 \neg je *unárna* spojka — má jeden argument, formulu.

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

Lubovoľne 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.

$\neg \text{doma}(\text{Karol})$	Karol <i>nie</i> je doma.
$\neg \text{Jarka} \doteq \text{Karol}$	Jarka <i>nie</i> je Karol.
$\neg \neg \neg \text{poslúcha}(\text{Cilka})$	<i>Nie</i> je pravda, že <i>nie</i> je pravda, že Cilka <i>neposlúcha</i> .
$(\neg \text{doma}(\text{Karol}))$	nesprávna
$\neg(\text{doma}(\text{Karol}))$	syntax

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 $\tau \neq \sigma$.

Konjunkcia

Konjunkcia \wedge 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 chorý, *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.*
(doma(Jarka) \wedge doma(Karol))
- *Karol sa potkol a spadol.*
(potkol_sa(Karol) \wedge spadol(Karol))
- *Jarka dostala Bobyho od mamy a otca.*
(dostal(Jarka, Boby, mama) \wedge dostal(Jarka, Boby, otec))

Podobne (jednoduché a viacnásobné zlučovacie) prívlastky vlastností:

- *Eismann je ruský špión.*
(Rus(Eismann) \wedge špión(Eismann))
- *Boby je malý čierny pes.*
((malý(Boby) \wedge čierny(Boby)) \wedge pes(Boby))

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

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*, *popripade*, *pripadne*.

Disjunkciou formalizujeme vylučovacie súvetia s inkluzívnym významom:

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

- Bobyho kúpe Jarka, prípadne ho kúpe Karol. ($\text{kúpe}(\text{Jarka}, \text{Boby}) \vee \text{kúpe}(\text{Karol}, \text{Boby})$)

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. ($\text{doma}(\text{Jarka}) \vee \text{doma}(\text{Karol})$)
- Jarka je doma alebo v škole. ($\text{doma}(\text{Jarka}) \vee \text{v_škole}(\text{Jarka})$)
- Jarka dostala Bobyho od mamy alebo otca. ($\text{dostal}(\text{Jarka}, \text{Boby}, \text{mama}) \vee \text{dostal}(\text{Jarka}, \text{Boby}, \text{otec})$)
- Boby je čierny či tmavohnedý psík. ($((\text{čierny}(\text{Boby}) \vee \text{tmavohnedý}(\text{Boby})) \wedge \text{pes}(\text{Boby}))$)

Exkluzívna disjunkcia

Konštrukcie „*bud' ... , alebo ...*“, „*bud' ... , bud' ...*“, „*alebo ... , alebo ...*“ *spravidla* (v matematike vždy) vyjadrujú *exkluzívnu* disjunkciu.

- Bud' je batéria vybitá alebo svieti kontrolka.

Exkluzívnu disjunkciu môžeme vyjadriť zložitejšou formulou:

$$((\text{vybitá}(\text{batéria}) \vee \text{svieti}(\text{kontrolka})) \wedge \neg(\text{vybitá}(\text{batéria}) \wedge \text{svieti}(\text{kontrolka})))$$

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

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

Vid' *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 Boby šťastný.

❓ $((\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka})) \vee \text{šťastný}(\text{Boby}))$

❓ $(\text{doma}(\text{Karol}) \wedge (\text{doma}(\text{Jarka}) \vee \text{šťastný}(\text{Boby})))$

- Karol je doma alebo Jarka je doma a Boby je šťastný.

❓ $((\text{doma}(\text{Karol}) \vee \text{doma}(\text{Jarka})) \wedge \text{šťastný}(\text{Boby}))$

❓ $(\text{doma}(\text{Karol}) \vee (\text{doma}(\text{Jarka}) \wedge \text{šťastný}(\text{Boby})))$

Jednoznačnosť rozkladu v slovenčine

Slovenčina má prostriedky podobné zátvorkám:

- Viacnásobný vetný člen (+*obaja*, *niekto* z):

- Karol aj Jarka sú (obaja) doma alebo je Boby šťastný.

$((\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka})) \vee \text{šťastný}(\text{Boby}))$

- Doma je Karol alebo Jarka a Boby je šťastný.

Niekoľko z dvojice Karol a Jarka je doma a Boby je šťastný.

$((\text{doma}(\text{Karol}) \vee \text{doma}(\text{Jarka})) \wedge \text{šťastný}(\text{Boby}))$

- Kombinácie spojok *bud'* ..., *alebo* ...; *alebo* ..., *alebo* ...; *aj* ..., *aj* ...; *ani* ..., *ani* ...; a pod.

- Karol je doma a *bud'* je doma Jarka, alebo je Boby šťastný, alebo jedno aj druhé.

$(\text{doma}(\text{Karol}) \wedge (\text{doma}(\text{Jarka}) \vee \text{šťastný}(\text{Boby})))$

- Alebo je doma Karol, alebo je doma Jarka a Boby je šťastný, alebo aj aj. $(\text{doma}(\text{Karol}) \vee (\text{doma}(\text{Jarka}) \wedge \text{šťastný}(\text{Boby})))$

Jednoznačnosť rozkladu

Aj Karol je doma, aj Jarka je doma alebo je Bobby šťastný. Aj Karol je doma, aj Jarka je doma, alebo je Bobby šťastný.

- Má čiarka vplyv na význam tvrdenia?
- Chybovosť pri čiarkach je vysoká, pravidlá nie sú jednoznačné a v čase sa menia.
- Pri formalizácii pomáhajú dodatočné znalosti (napr. o spoločnom fungovaní Karola, Jarky, Bobbyho).

Oblasť platnosti negácie

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

- $((\neg \text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka})) \vee \text{šťastný}(\text{Boby}))$
- $(\neg (\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka}))) \vee \text{šťastný}(\text{Boby})$

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

✓ $\neg \neg (\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka}))$

✗ $\neg (\neg (\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka})))$

Interakcia negácie s alebo v slovenčine

Zamyslite sa 2.1

Ako by ste sformalizovali: „Doma nie je Jarka alebo Karol“?

A. $(\neg \text{doma}(\text{Jarka}) \vee \neg \text{doma}(\text{Karol}))$

B. $\neg (\text{doma}(\text{Jarka}) \vee \text{doma}(\text{Karol}))$

Zvyčajné chápanie v slovenčine je A.

Formalizácii B zodpovedá „Nie je pravda, že je doma Jarka alebo Karol.“

2.2 Implikácia

Implikácia

Implikácia \rightarrow je binárna spojka približne zodpovedajúca podmienkovému podrad'ovaciemu 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*:

Jim príde, *ak* príde Kim.
postačujúca
podmienka

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

- Zodpovedá teda ($\text{príde}(\text{Kim}) \rightarrow \text{príde}(\text{Jim})$).

Vo všeobecnosti:

$$A, \text{ ak } B. \quad \rightsquigarrow \quad (B \rightarrow A)$$

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 *nepríde*.
- Zodpovedá teda ($\text{príde}(\text{Jim}) \rightarrow \text{príde}(\text{Kim})$).

Vo všeobecnosti:

$$A, \text{ iba ak } B. \quad \rightsquigarrow \quad (A \rightarrow B)$$

Iné vyjadrenia:

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

Nutná a postačujúca podmienka rukolapne

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

Z logiky prejdete, *ak* pridete na písomnú aj ústnu skúšku.

Stačilo by prísť na obe časti skúšky a *nebolo by nutné* urobiť nič iné.

Žiaľ, z našich pravidiel vyplýva:

Z logiky prejdete, *iba ak* pridete na písomnú aj ústnu skúšku.

Prísť na obe časti skúšky *je nutné*, ale na prejsenie to *nestačí*.

Súvetia formalizované implikáciou

$(A \rightarrow B)$ 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. ($\text{príde}(\text{Jim}) \leftrightarrow \text{príde}(\text{Kim})$)
- Číslo n je párne práve vtedy, keď n^2 je párne. ($\text{párne}(n) \leftrightarrow \text{párne}(n^2)$)
- Müller je taký Nemec, ako je Stirlitz Rus. ($\text{Nemec}(\text{Müller}) \leftrightarrow \text{Rus}(\text{Stirlitz})$)

Ekvivalencia

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

Budeme ju preto považovať za skratku za formulu

$$((A \rightarrow B) \wedge (B \rightarrow A)).$$

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 s ním Boby.

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 označenia a považovať ich za skratky, podobne ako ekvivalenciu.

2.4 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

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

ale rovnako *správna* je aj formalizácia

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

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 implikatury

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 implikatury

Časť významu tvrdenia, ktorú *môžeme poprieť* dodatkami bez sporu s pôvodným tvrdením, sa nazýva *konverzačná implikatura* (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 implikatura.

- 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.

Formalizácia je ťažká

- Jedna formula môže byť rozdelená do viac viet. Nech x je kladné reálne. Potom $x^2 > 0$.
- Niektoré tvrdenia sú vnútorne veľmi zložené. Postupnosť prvočísel usporiadaných podľa veľkosti je rastúca.
- Existujú jazyky, kde pre niektoré logické spojky neexistuje slovo, využívajú sa iné prvky gramatiky.
- Logickú spojku občas treba hádať z kontextu. It's raining. The game is cancelled. It's raining *and therefore* the game is cancelled.
- Aj intonácia môže ovplyvniť formalizáciu. I said I *might* go. I did not say I am surely going, I only suggested the possibility.

Formalizácia je ťažká

- Mnohé tvrdenia z praxe majú veľmi ďaleko od ideálnych jazykových schém (či už z hľadiska aplikácie gramatických pravidiel alebo formalizácie do presného jazyka).

„Na druhej strane si myslím, že Slovensko, niekedy žiaľ-bohu a niekedy je to aj chvalabohu, že žiaľ-bohu, na Slovensku predsa len tá pracovná sila je ešte stále lacnejšia a teraz, chvalabohu, že je lacnejšia.“

- Jednotlivci majú svoje vnímanie jazykových konštruktov založené na ich osobnej histórii a niekedy sa nezhodnú. Trénovacie množiny pre AI modely tak sú nekonzistentné a výsledok tréningu nemôže byť dokonalý.

Formalizácia je ťažká

Aj najlepšie súčasné AI systémy potrebujú s formalizáciou ľudskú pomoc. Z článku o [AlphaGeometry](#) (2025, parafrázované):

A major weakness is the need to manually transform input problems from natural language into a domain-specific language. Automating this process is an active area of research. It is significantly more complicated than translation between human languages.

Formalization frequently requires re-formulating the original problem into an alternative *equivalent* form, and disambiguating the nuances in the original problem statement. *Automated formalization thus demands significant background knowledge and problem-solving skills* on its own. Using Gemini prompts containing examples obtained manually, we are able to formalize 30 out of 39 formalizable IMO geometry problems.

2.5 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.

Symbole výrokovologickej časti logiky prvého rádu

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

mimologické symboly, ktorými sú

- *individuové 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* $\neg, \wedge, \vee, \rightarrow$ (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* $\text{ar}_{\mathcal{L}}(P) \in \mathbb{N}^+$.

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 individuové 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 individuové 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 $\mathcal{C}_{\mathcal{L}} = \{\text{Kim}, \text{Jim}, \text{Sarah}\}$ a $\mathcal{P}_{\mathcal{L}} = \{\text{príde}^1\}$.

Čo sú formuly tohto jazyka?

- Samotné atómy, napr. $\text{príde}(\text{Sarah})$.
- Negácie atómov, napr. $\neg \text{príde}(\text{Sarah})$.

- Atómy alebo aj ich negácie spojené spojkou, napr. $(\neg \text{príde}(\text{Kim}) \vee \text{príde}(\text{Sarah}))$.
- Ale negovať a spájať spojkami môžeme aj zložitejšie formuly, napr. $(\neg(\text{príde}(\text{Kim}) \wedge \text{príde}(\text{Sarah})) \rightarrow (\neg \text{príde}(\text{Kim}) \vee \neg \text{príde}(\text{Sarah})))$.

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 $(A \rightarrow B)$ 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 $((A \rightarrow B) \wedge (B \rightarrow A))$.

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

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

Vytvárajúca postupnosť

Definícia 2.10. *Vytvárajúcou postupnosťou* nad jazykom \mathcal{L} výrokovologickej časti logiky prvého rádu je ľubovoľná konečná postupnosť A_0, \dots, 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 $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, kde A a B sú niektoré predchádzajúce členy postupnosti.

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

Indukcia (vzhľadom) na konštrukciu formuly

Veta 2.11 (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 $(A \rightarrow B)$ má vlastnosť P ,*

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

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“.

Výrokovologické formuly by sa dali alternatívne zdefinovať ako postupnosti symbolov jazyka \mathcal{L} , pre ktoré existuje vytvárajúca postupnosť nad \mathcal{L} .

Výhoda: Dĺžka vytvárajúcej postupnosti je číslo, tvrdenia o všetkých formulách sa potom dajú dokazovať matematickou alebo úplnou indukciou.

(Ne)jednoznačnosť rozkladu formúl výrokovej logiky

Čo keby sme zdefinovali „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 $A \wedge B$, $A \vee B$ a $A \rightarrow B$ 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) \rightarrow príde(Kim) \rightarrow \neg príde(Sarah))?

Formulu by sme mohli čítať ako $A = (\text{príde}(\text{Jim}) \rightarrow (\text{príde}(\text{Kim}) \rightarrow \neg \text{príde}(\text{Sarah})))$ alebo ako $B = ((\text{príde}(\text{Jim}) \rightarrow \text{príde}(\text{Kim})) \rightarrow \neg \text{príde}(\text{Sarah}))$.

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 binárna spojka $b \in \{\wedge, \vee, \rightarrow\}$ také, že $X = (A \ b \ B)$.

Problémy s vytvárajúcou postupnosťou

Vytvárajúca postupnosť popisuje konštrukciu formuly podľa definície formúl:

príde(Jim), príde(Sarah), \neg príde(Jim), príde(Kim),
 \neg príde(Sarah), $(\neg$ príde(Jim) \wedge príde(Kim)),
 $((\neg$ príde(Jim) \wedge príde(Kim)) \rightarrow \neg príde(Sarah))

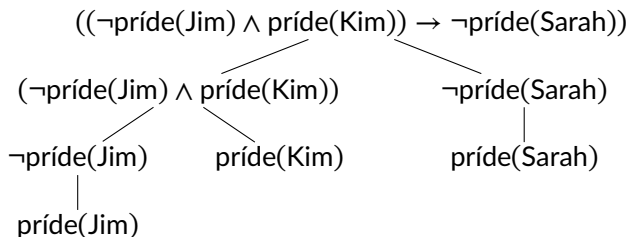
ale

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

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

Vytvárajúci strom

Konštrukciu si vieme predstaviť ako *strom*:



Takéto stromy voláme *vytvárajúce*.

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

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:

$$((\neg \text{príde}(\text{Jim}) \wedge \text{príde}(\text{Kim})) \rightarrow \neg \text{príde}(\text{Sarah}))$$

Ako nazveme formuly, z ktorých vznikla?

$$\text{príde}(\text{Sarah}), \neg \text{príde}(\text{Jim}), (\neg \text{príde}(\text{Jim}) \wedge \text{príde}(\text{Kim})), \dots$$

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

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

Ako tieto pojmy presne zdefinujeme?

Podformuly

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

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

Definícia 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 $((\text{príde}(\text{Jim}) \vee \neg \text{príde}(\text{Kim})) \wedge \neg (\text{príde}(\text{Sarah}) \rightarrow \text{príde}(\text{Kim})))$?

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

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 ($P = \mathcal{E}_{\mathcal{L}}$).

2.6 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 sa 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} priraduje prvok $i(c) \in D$;
- každému predikátovému symbolu P jazyka \mathcal{L} s aritou n priraduje 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:

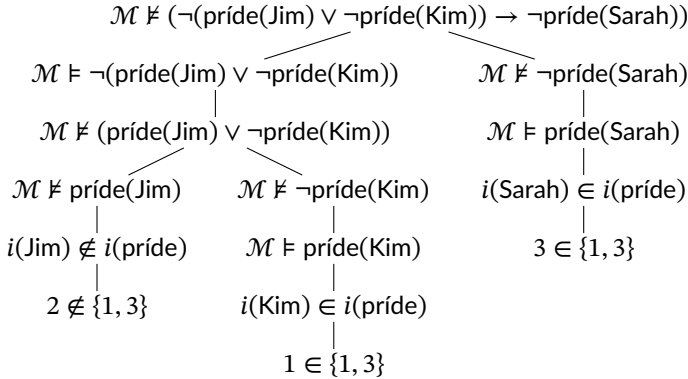
- $\mathcal{M} \models c_1 \doteq c_2$ vtt $i(c_1) = i(c_2)$,
- $\mathcal{M} \models P(c_1, \dots, c_n)$ vtt $(i(c_1), \dots, i(c_n)) \in i(P)$,
- $\mathcal{M} \models \neg A$ vtt $\mathcal{M} \not\models A$,
- $\mathcal{M} \models (A \wedge B)$ vtt $\mathcal{M} \models A$ a zároveň $\mathcal{M} \models B$,
- $\mathcal{M} \models (A \vee B)$ vtt $\mathcal{M} \models A$ alebo $\mathcal{M} \models B$,
- $\mathcal{M} \models (A \rightarrow B)$ vtt $\mathcal{M} \not\models A$ alebo $\mathcal{M} \models B$,

kde $\mathcal{M} \not\models A$ skrakuje *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 $D = \{0, 1, 2, 3\}$, $i(\text{Kim}) = 1$, $i(\text{Jim}) = 2$, $i(\text{Sarah}) = 3$, $i(\text{príde}) = \{1, 3\}$.

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



Vyhodnotenie pravdivosti formuly

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

Vyhodnotenie pravdivosti môžeme zapísať aj tabuľkou:

	$p(J)$	$p(K)$	$\neg p(K)$	$(p(J) \vee \neg p(K))$	$\neg(p(J) \vee \neg p(K))$...
\mathcal{M}	$\not\models$	\models	$\not\models$	$\not\models$	\models	

	$p(S)$	$\neg p(S)$	$(\neg(p(J) \vee \neg p(K)) \rightarrow \neg p(S))$
...	\models	$\not\models$	$\not\models$

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

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 $\mathcal{M} \models (\neg(\text{príde}(\text{Jim}) \vee \neg \text{príde}(\text{Kim})) \rightarrow \neg \text{príde}(\text{Sarah}))$?

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

$\mathcal{M} \models (\neg(\text{príde}(\text{Jim}) \vee \neg \text{príde}(\text{Kim})) \rightarrow \neg \text{príde}(\text{Sarah}))$ vtt $\mathcal{M} \not\models \neg(\text{príde}(\text{Jim}) \vee \neg \text{príde}(\text{Kim}))$ alebo $\mathcal{M} \models \neg \text{príde}(\text{Sarah})$ vtt $\mathcal{M} \models (\text{príde}(\text{Jim}) \vee \neg \text{príde}(\text{Kim}))$ 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 $i(\text{Sarah}) \notin i(\text{príde})$.

2.7 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.

$$T_{\text{party}} = \{((\text{príde}(\text{Kim}) \vee \text{príde}(\text{Jim})) \vee \text{príde}(\text{Sarah})), \\ (\text{príde}(\text{Kim}) \rightarrow \neg \text{príde}(\text{Sarah})), \\ (\text{príde}(\text{Jim}) \rightarrow \text{príde}(\text{Kim})), \\ (\text{príde}(\text{Sarah}) \rightarrow \text{príde}(\text{Jim}))\}$$

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).

$$\begin{aligned} \mathcal{M} &= (\{k, j, s, e, h\}, i), \\ i(\text{Kim}) &= k, \quad i(\text{Jim}) = j, \quad i(\text{Sarah}) = s, \\ i(\text{príde}) &= \{k, j, e\}; \\ \left. \begin{aligned} \mathcal{M} &\models ((\text{príde}(\text{Kim}) \vee \text{príde}(\text{Jim})) \vee \text{príde}(\text{Sarah})) \\ \mathcal{M} &\models (\text{príde}(\text{Kim}) \rightarrow \neg \text{príde}(\text{Sarah})) \\ \mathcal{M} &\models (\text{príde}(\text{Jim}) \rightarrow \text{príde}(\text{Kim})) \\ \mathcal{M} &\models (\text{príde}(\text{Sarah}) \rightarrow \text{príde}(\text{Jim})) \end{aligned} \right\} \mathcal{M} \models T_{\text{party}} \end{aligned}$$

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} .

2.8 Výrokovologické ohodnotenia

Nekonečne veľa štruktúr

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

$$T_{\text{party}} = \{((\text{príde}(\text{Kim}) \vee \text{príde}(\text{Jim})) \vee \text{príde}(\text{Sarah})), \\ (\text{príde}(\text{Kim}) \rightarrow \neg \text{príde}(\text{Sarah})), \\ (\text{príde}(\text{Jim}) \rightarrow \text{príde}(\text{Kim})), \\ (\text{príde}(\text{Sarah}) \rightarrow \text{príde}(\text{Jim}))\}$$

Ale štruktúra je nekonečne veľá a ak má teória jeden model, má aj nekonečne veľá ďalších:

$\mathcal{M}_1 = (\{k, j, s\}, i_1)$	$\mathcal{M}'_1 = (\{k, j, s, 0, 1\}, i'_1)$	$\mathcal{M}''_1 = (\{2, 4, 6\}, i''_1) \quad \dots$
$i_1(\text{Kim}) = k$	$i'_1(\text{Kim}) = k$	$i''_1(\text{Kim}) = 2$
$i_1(\text{Jim}) = j$	$i'_1(\text{Jim}) = j$	$i''_1(\text{Jim}) = 4$
$i_1(\text{Sarah}) = s$	$i'_1(\text{Sarah}) = s$	$i''_1(\text{Sarah}) = 6$
$i_1(\text{príde}) = \{k, j\}$	$i'_1(\text{príde}) = \{k, j, 1\}$	$i''_1(\text{príde}) = \{2, 4\}$

Rozdiely modelov

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

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

Líšia sa doménami aj v interpretáciách.

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

Zhodujú sa na pravdivosti všetkých predikátových atómov $\text{príde}(\text{Kim})$, $\text{príde}(\text{Jim})$, $\text{príde}(\text{Sarah})$.

💡 V T_{party} na ničom inom nezáleží.

Ohodnotenie atómov

Z každej zo štruktúr

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

môžeme skonštruovať to isté *ohodnotenie predikátových atómov*:

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

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 2.30. 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 2.31. 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 $v : \mathcal{PA}_{\mathcal{L}} \rightarrow \{f, t\}$.

Pravdivé formuly v ohodnotení

Ako vyhodnotíme, či je formula pravdivá v nejakom ohodnotení?

Definícia 2.32. Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu, nech (f, t) sú pravdivostné hodnoty a nech $v : \mathcal{PA}_{\mathcal{L}} \rightarrow \{f, t\}$ je výrokovologické ohodnotenie pre \mathcal{L} . Reláciu *výrokovologická formula A je pravdivá v ohodnotení v* ($v \models_p A$) definujeme *induktívne* pre všetky predikátové atómy a a všetky výrokovologické formuly A, B jazyka \mathcal{L} nasledovne:

- $v \models_p a$ vtt $v(a) = t$,
- $v \models_p \neg A$ vtt $v \not\models_p A$,
- $v \models_p (A \wedge B)$ vtt $v \models_p A$ a zároveň $v \models_p B$,
- $v \models_p (A \vee B)$ vtt $v \models_p A$ alebo $v \models_p B$,
- $v \models_p (A \rightarrow B)$ vtt $v \not\models_p A$ alebo $v \models_p B$,

kde vtt skrakuje *vtedy a len vtedy* a $v \not\models_p A$ skrakuje *A nie je pravdivá vo v* .

Vyhodnotenie formuly v ohodnotení

Príklad 2.33. Vyhodnoťme formulu

$$X = ((\text{príde}(\text{Jim}) \vee \neg \text{príde}(\text{Kim})) \rightarrow \text{príde}(\text{Sarah}))$$

vo výrokovologickom ohodnotení

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

zdola nahor:

	p(Kim)	p(Jim)	p(Sarah)	$\neg p(\text{Kim})$	$(p(\text{Jim}) \vee \neg p(\text{Kim}))$	X
v	\models_p	\models_p	$\not\models_p$	$\not\models_p$	\models_p	$\not\models_p$

príde sme skrátili na p.

Ohodnotenie zhodné so štruktúrou

Definícia 2.34. Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu, nech \mathcal{M} je štruktúra pre \mathcal{L} , nech (f, t) sú pravdivostné hodnoty, $v : \mathcal{PA}_{\mathcal{L}} \rightarrow \{f, t\}$ 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 2.35. *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 $v : \mathcal{PA}_{\mathcal{L}} \rightarrow \{f, t\}$ 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 2.36 (Konštrukcia štruktúry zhodnej s ohodnotením). Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu, kde $\mathcal{C}_{\mathcal{L}} = \{\text{Kim, Jim, Sarah}\}$ a $\mathcal{P}_{\mathcal{L}} = \{\text{príde}\}$.

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

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

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

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

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

Každú konštantu interpretujeme ňou samou:

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

predikát prídá 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 hocikajký jazyk?

Tvrdenie 2.37. *Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu, nech (f, t) sú pravdivostné hodnoty a $v : \mathcal{PA}_{\mathcal{L}} \rightarrow \{f, t\}$ 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:

$$i(c) = c$$

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

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 2.38. *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 $v \models_p X$ 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 $v \models_p X$ vtt $v(X) = t$ vtt $\mathcal{M} \models X$ podľa def. zhodnosti v a \mathcal{M} .

2.1: Indukčný predpoklad: Nech tvrdenie platí pre formulu X . Dokážme tvrdenie pre $\neg X$. Ak X neobsahuje symbol rovnosti \doteq , potom $v \models_p \neg X$ vtt (podľa def. \models_p) $v \not\models_p X$ vtt (podľa IP) $\mathcal{M} \not\models X$ vtt (podľa def. \models) $\mathcal{M} \models \neg X$. 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 $(X \wedge Y)$, $(X \vee Y)$, $(X \rightarrow Y)$. Ak X alebo Y obsahuje \doteq , tvrdenie platí pre $(X \wedge Y)$, $(X \vee Y)$, $(X \rightarrow Y)$ triviálne, lebo nie sú výrokovologické.

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

Ďalej $v \models_p (X \wedge Y)$ vtt $v \models_p X$ a $v \models_p Y$ vtt (podľa IP) vtt $\mathcal{M} \models X$ a $\mathcal{M} \models Y$ vtt $\mathcal{M} \models (X \wedge Y)$.

Nakoniec $v \models_p (X \vee Y)$ vtt $v \models_p X$ alebo $v \models_p Y$ vtt (podľa IP) vtt $\mathcal{M} \models X$ alebo $\mathcal{M} \models Y$ vtt $\mathcal{M} \models (X \vee Y)$. □

3. prednáška

Výrokovologické vyplývanie, sémantické vlastnosti formúl a ekvivalencia

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,
- ako zjednodušíme štruktúry na výrokovologické ohodnotenia.

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 teórie a modely

Výrokovologické teórie

Vráťme sa naspäť k teóriám, modelom a vyplývaniu.

Definícia 3.1. 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 3.2. Výrokovologickou teóriou je

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

ale nie

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

Príklad výrokovologického modelu

Príklad 3.3 (Výrokovologický model teórie o party).

$$\left. \begin{aligned} v &= \{\text{príde}(\text{Kim}) \mapsto t, \text{príde}(\text{Jim}) \mapsto t, \text{príde}(\text{Sarah}) \mapsto f\} \\ v &\models_p ((\text{príde}(\text{Kim}) \vee \text{príde}(\text{Jim})) \vee \text{príde}(\text{Sarah})) \\ v &\models_p (\text{príde}(\text{Kim}) \rightarrow \neg \text{príde}(\text{Sarah})) \\ v &\models_p (\text{príde}(\text{Jim}) \rightarrow \text{príde}(\text{Kim})) \\ v &\models_p (\text{príde}(\text{Sarah}) \rightarrow \text{príde}(\text{Jim})) \end{aligned} \right\} v \models_p T_{\text{party}}$$

Výrokovologický model

Definícia 3.4 (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 , skráteno $v \models_p T$, vtt každá formula X z T je pravdivá vo v (teda $v \models_p X$ pre každú $X \in T$).

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

Teória T je *nepravdivá* vo v , skráteno $v \not\models_p T$, vtt T nie je pravdivá vo v .

Zrejme $v \models_p T$ vtt $v \not\models_p X$ pre *nejakú* $X \in T$.

Model teórie, splniteľnosť a nespľniteľnosť

Definícia 3.5 (Splniteľnosť a nespľniteľnosť). Teória je *výrokovologicky splniteľná* vtt má aspoň jeden výrokovologický model.

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

Zrejme teória nie je splniteľná vtt keď je nespľniteľná.

Príklad 3.6. T_{party} je evidentne splniteľná.

3.2 Vyplývanie, nezávislosť a nespľniteľnosť

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 3.7. 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 *nevyplýva* z T , píšeme $T \not\models_p X$.

Príklad výrokovologickeho vyplývania

Príklad 3.8. Vyplýva príde(Kim) výrokovologicky z T_{party} ? Pretože vieme vymenovať všetky ohodnotenia pre $\mathcal{L}_{\text{party}}$, zistíme to ľahko:

	v_i			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	T_{party}	$p(K)$
	$p(K)$	$p(J)$	$p(S)$						
v_0	<i>f</i>	<i>f</i>	<i>f</i>	$\not\vdash_p$				$\not\vdash_p$	
v_1	<i>f</i>	<i>f</i>	<i>t</i>	\vdash_p	\vdash_p	\vdash_p	$\not\vdash_p$	$\not\vdash_p$	
v_2	<i>f</i>	<i>t</i>	<i>f</i>	\vdash_p	\vdash_p	$\not\vdash_p$		$\not\vdash_p$	
v_3	<i>f</i>	<i>t</i>	<i>t</i>	\vdash_p	\vdash_p	$\not\vdash_p$		$\not\vdash_p$	
v_4	<i>t</i>	<i>f</i>	<i>f</i>	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p
v_5	<i>t</i>	<i>f</i>	<i>t</i>	\vdash_p	$\not\vdash_p$			$\not\vdash_p$	
v_6	<i>t</i>	<i>t</i>	<i>f</i>	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p
v_7	<i>t</i>	<i>t</i>	<i>t</i>	\vdash_p	$\not\vdash_p$			$\not\vdash_p$	

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

	v_i			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	T_{party}	$p(J)$
	$p(K)$	$p(J)$	$p(S)$						
v_0	<i>f</i>	<i>f</i>	<i>f</i>	$\not\vdash_p$				$\not\vdash_p$	
v_1	<i>f</i>	<i>f</i>	<i>t</i>	\vdash_p	\vdash_p	\vdash_p	$\not\vdash_p$	$\not\vdash_p$	
v_2	<i>f</i>	<i>t</i>	<i>f</i>	\vdash_p	\vdash_p	$\not\vdash_p$		$\not\vdash_p$	
v_3	<i>f</i>	<i>t</i>	<i>t</i>	\vdash_p	\vdash_p	$\not\vdash_p$		$\not\vdash_p$	
v_4	<i>t</i>	<i>f</i>	<i>f</i>	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p	$\not\vdash_p$
v_5	<i>t</i>	<i>f</i>	<i>t</i>	\vdash_p	$\not\vdash_p$			$\not\vdash_p$	
v_6	<i>t</i>	<i>t</i>	<i>f</i>	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p	\vdash_p
v_7	<i>t</i>	<i>t</i>	<i>t</i>	\vdash_p	$\not\vdash_p$			$\not\vdash_p$	

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

Výrokovologická nezávislosť

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

Definícia 3.10. 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 $v_0 \models_p T$ aj $v_1 \models_p T$, ale $v_0 \not\models_p X$ a $v_1 \models_p X$.

Príklad 3.11 (pokračovanie príkladu 3.9). *Logický záver*: Formula $\text{príde}(\text{Jim})$ 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 prítomný ani aby bol neprítomný. *Môže, ale nemusí* prísť. Jeho prítomnosť od požiadaviek *nezávisí*.

Príklad vyplývania negácie

Príklad 3.12. Je $\text{príde}(\text{Sarah})$ výrokovologickým dôsledkom T_{party} alebo nezávislá od T_{party} ?

	v_i			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	T_{party}	$p(S)$
	$p(K)$	$p(J)$	$p(S)$						
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	$\not\models_p$
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	$\not\models_p$
v_7	t	t	t	\models_p	$\not\models_p$			$\not\models_p$	

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

Vyplývanie negácie

Tvrdenie 3.13. 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 výrokologicky nezávislá od T vtt $\neg X$ vyplýva z T .

Príklad 3.14 (pokračovanie príkladu 3.12). *Logický záver:* Z T_{party} vyplýva $\neg \text{príde}(\text{Sarah})$.

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:

Buď $v \models_p X$, alebo $v \not\models_p X$.

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

	existuje v také, že $v \models_p T$ a $v \models_p X$	pre všetky v , ak $v \models_p T$, tak $v \models_p X$
existuje v také, že $v \models_p T$ a $v \not\models_p X$	X je nezávislá od T $T \not\models_p X$ a $T \not\models_p \neg X$	$T \models_p \neg X$ a $T \not\models_p X$
pre všetky v , ak $v \models_p T$, tak $v \models_p X$	$T \models_p X$ a $T \not\models_p \neg X$	T je <i>nesplniteľná</i> $T \models_p X$ aj $T \models_p \neg X$

Nesplniteľná teória

Príklad 3.15. Je teória $T'_{\text{party}} = T_{\text{party}} \cup \{(\neg \text{príde}(\text{Sarah}) \rightarrow \neg \text{príde}(\text{Kim}))\}$ splniteľná?

	v_i			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	$(\neg p(S) \rightarrow \neg p(K))$	T'_{party}
	$p(K)$	$p(J)$	$p(S)$						
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	$\not\models_p$	$\not\models_p$
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	$\not\models_p$	$\not\models_p$
v_7	t	t	t	\models_p	$\not\models_p$				$\not\models_p$

Logický záver: T'_{party} je nesplnitelná, 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 je neužitočná vlastnosť.

Tvrdenie 3.16. *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 $T \cup \{X\}$ 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 3.17. *Množinu atómov $\text{atoms}(X)$ formuly $X \in \mathcal{E}_{\mathcal{L}}$ definujeme pre všetky formuly $A, B \in \mathcal{E}_{\mathcal{L}}$ nasledovne:*

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

Množinou atómov teórie T je

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

Ohodnotenia zhodné na atónoch teórie

Definícia 3.18. 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 3.19. 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 $\text{atoms}(T) \cup \text{atoms}(X)$ platí

- $v_1 \models_p T$ vtt $v_2 \models_p T$,
- $v_1 \models_p X$ vtt $v_2 \models_p X$.

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 *lišia* na atónoch *vyskytujúcich* sa vo formule a teórii.

Pokiaľ je teória je konečná, stačí skúmať konečne veľa ohodnotení, aj keby bol jazyk nekonečný. (A podľa vety o kompaktnosti ak máme nejaký spor v nekonečnej teórii, nájde sa sporná konečná podmnožina.)

Dôkaz indukciou na konštrukciu formuly

- (1) X je výrokovologická formula jazyka \mathcal{L}
(2) v_1 a v_2 sú ohodnotenia zhodné na $\text{atoms}(X)$ $\Downarrow v_1 \models_p X$ vtt $v_2 \models_p X$

Báza: X je atóm.

- (3) X predikátový atóm podľa 1
(4) $v_1 \models_p X$ vtt $v_1(X) = t$ def. pravdivosti
(5) $v_2 \models_p X$ vtt $v_2(X) = t$ def. pravdivosti
(6) $v_1(X) = v_2(X)$ podľa 2
 $v_1 \models_p X$ vtt $v_2 \models_p X$ podľa 4, 5, 6

Dôkaz indukciou na konštrukciu formuly

- (1) Z je výrokovologická formula jazyka \mathcal{L}
 - (2) v_1 a v_2 sú ohodnotenia zhodné na $\text{atoms}(Z)$ $\Downarrow v_1 \models_p Z \text{ vtt } v_2 \models_p Z$
-

Ind. krok pre \neg : Formula v tvare $Z = \neg X$.

- | | | |
|------|--|---|
| (IP) | Tvrdenie platí pre X | |
| (3) | v_1, v_2 sa zhodujú na $\text{atoms}(X)$ | 2, $\text{atoms}(\neg X) = \text{atoms}(X)$ |
| (4) | $v_1 \models_p X \text{ vtt } v_2 \models_p X$ | 3, IP pre $Z = X$ |
| (5) | $v_1 \models_p \neg X \text{ vtt } v_1 \not\models_p X$ | def. \models_p |
| (6) | $v_2 \models_p \neg X \text{ vtt } v_2 \not\models_p X$ | def. \models_p |
| (7) | $v_1 \not\models_p X \text{ vtt } v_2 \not\models_p X$ | 4, def. $\not\models_p$ |
| | $v_1 \models_p \neg X \text{ vtt } v_2 \models_p \neg X$ | 5, 6, 7 |

Dôkaz indukciou na konštrukciu formuly

- (1) Z je výrokovologická formula jazyka \mathcal{L}
 - (2) v_1 a v_2 sú ohodnotenia zhodné na $\text{atoms}(Z)$ $\Downarrow v_1 \models_p Z \text{ vtt } v_2 \models_p Z$
-

Ind. krok pre \wedge : Formula v tvare $Z = (X \wedge Y)$.

- | | | |
|------|--|---------------------|
| (IP) | Tvrdenie platí pre X aj pre Y | |
| (3) | $\text{atoms}((X \wedge Y)) = \text{atoms}(X) \cup \text{atoms}(Y)$ | def. atoms |
| (4) | v_1, v_2 sa zhodujú na $\text{atoms}(X)$ | 2, 3 |
| (5) | $v_1 \models_p X \text{ vtt } v_2 \models_p X$ | 4, IP pre $Z = X$ |
| (6) | v_1, v_2 sa zhodujú na $\text{atoms}(Y)$ | 2, 3 |
| (7) | $v_1 \models_p Y \text{ vtt } v_2 \models_p Y$ | 6, IP pre $Z = Y$ |
| (8) | $v_1 \models_p (X \wedge Y) \text{ vtt } v_1 \models_p X \text{ a } v_1 \models_p Y$ | def. \models_p |
| (9) | $v_2 \models_p (X \wedge Y) \text{ vtt } v_2 \models_p X \text{ a } v_2 \models_p Y$ | def. \models_p |
| | $v_1 \models_p (X \wedge Y) \text{ vtt } v_2 \models_p (X \wedge Y)$ | 5, 7, 8, 9 |

Dôkaz tvrdenia 3.19 (ešte raz, vo vetách). 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 $\text{atoms}(X)$, teda na samotnom X . Podľa definície pravdivosti platí $v_1 \models_p X \text{ vtt } v_1(X) = t \text{ vtt } v_2(X) = t \text{ vtt } v_2 \models_p X$.

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 $\text{atoms}(\neg X)$. Pretože $\text{atoms}(\neg X) = \text{atoms}(X)$, v_1 a v_2 sa zhodujú na $\text{atoms}(X)$, 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 formulu X a Y . Dokážme ho pre $(X \wedge Y)$. Zoberme ľubovoľné ohodnotenia v_1 a v_2 , ktoré sa zhodujú na $\text{atoms}((X \wedge Y))$. Pretože $\text{atoms}((X \wedge Y)) = \text{atoms}(X) \cup \text{atoms}(Y)$, v_1 a v_2 sa zhodujú na $\text{atoms}(X)$, a teda podľa IP $v_1 \models_p X$ vtt $v_2 \models_p X$; tiež sa zhodujú na $\text{atoms}(Y)$, a teda podľa IP $v_1 \models_p Y$ vtt $v_2 \models_p Y$. Preto $v_1 \models_p (X \wedge Y)$ 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) $v_2 \models_p (X \wedge Y)$.

Podobne postupujeme pre ďalšie binárne spojky. □

4 Sémantické vlastnosti a vzťahy 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 $(A \vee \neg A)$.

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 $(A \vee \neg A)$ sú pravdivé v každej štruktúre.
- Výrokovologické ohodnotenia sa nezaoberajú rovnostnými atómami. Pomocou nich nezistíme, že $c \doteq c$ je nutne pravda. Ale zistíme, že $(A \vee \neg A)$ 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 $\mathcal{C}_{\mathcal{L}} = \{a, b\}$, $\mathcal{P}_{\mathcal{L}} = \{p^1\}$. Je formula $X = (((p(a) \rightarrow p(b)) \rightarrow p(a)) \rightarrow p(a))$ tautológiou?

Označme $A = p(a)$ a $B = p(b)$, teda $X = (((A \rightarrow B) \rightarrow A) \rightarrow A)$ a preskúmame všetky výrokovologické ohodnotenia týchto atómov:

v_i		X			
A	B	$(A \rightarrow B)$	$((A \rightarrow B) \rightarrow A)$	$((((A \rightarrow B) \rightarrow A) \rightarrow A)$	
v_0	f	f	\models_p	$\not\models_p$	\models_p
v_1	f	t	\models_p	$\not\models_p$	\models_p
v_2	t	f	$\not\models_p$	\models_p	\models_p
v_3	t	t	\models_p	\models_p	\models_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 $\models_{\mathcal{L}} X$) vtt X je *pravdivá v každom* výrokovologickom ohodnotení v pre \mathcal{L} (teda *pre každé* výrokovologické ohodnotenie v pre \mathcal{L} platí $v \models_{\mathcal{L}} X$).

v_i				
	A_1	A_2	\dots	X
v_0	f	f	\dots	$\models_{\mathcal{L}} X$
v_1	f	f	\dots	$\models_{\mathcal{L}} X$
		\dots		
v_k	t	f	\dots	$\models_{\mathcal{L}} X$
		\dots		

Definícia vyžaduje preveriť *všetky možné* ohodno-

tenia, ale podľa 3.19 stačí preverovať *ohodnotenia atómov vyskytujúcich sa vo formule*:

Dôsledok 4.3. 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 $v : \text{atoms}(X) \rightarrow \{f, t\}$.

Tautológia a vyplývanie

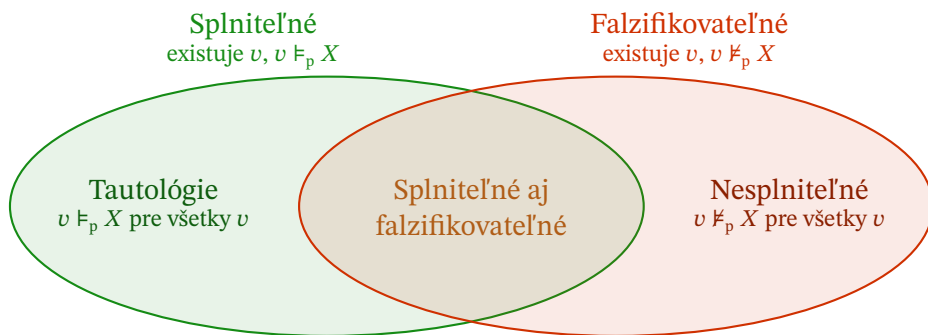
Tvrdenie 4.4 (Tautológia, vyplývanie a jeho monotónnosť). Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu. Nech A je výrokovologická formula v \mathcal{L} . Nech T_1 a T_2 sú výrokovologické teórie v \mathcal{L} . Potom:

- a) $\models_{\mathcal{L}} A$ (A je tautológia) vtt $\emptyset \models_{\mathcal{L}} A$ (A vyplýva z prázdnej teórie).
- b) $T_1 \models_{\mathcal{L}} A$ a $T_1 \subseteq T_2$, tak $T_2 \models_{\mathcal{L}} A$.
- c) $\models_{\mathcal{L}} A$ vtt pre každú teóriu T v \mathcal{L} , $T \models_{\mathcal{L}} A$.

Vlastnosti b) hovoríme *monotónnosť*: pridávaním ďalších formúl do teórie nemožno zrušiť platnosť jej dôsledkov.

„Geografia“ formúl podľa pravdivosti vo všetkých ohodnoteniach

Tautológie (vždy pravdivé) a kontradikcie (vždy nepravdivé) sú „výnimočné“ formuly. Väčšina formúl je kdesi medzi týmito extrémami.



Obrázok podľa [Papadimitriou \[1994\]](#)

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*.

Definícia 4.5. 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 $v \models_p X$).

	v_i			
	A_1	A_2	\dots	X
v_0	f	f	\dots	$\not\models_p$
v_1	f	f	\dots	$\not\models_p$
		\dots		
v_k	t	f	\dots	\models_p
		\dots		

Falzifikovateľnosť

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

Nazývame ich *falzifikovateľné*.

Definícia 4.6. 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 $v \not\models_p X$).

	v_i			
	A_1	A_2	\dots	X
v_0	f	f	\dots	\models_p
v_1	f	f	\dots	\models_p
		\dots		
v_k	t	f	\dots	$\not\models_p$
		\dots		

Nesplniteľnosť

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

Nazývame ich *nesplniteľné*.

Definícia 4.7. 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 $v \not\models_p X$).

	v_i			
	A_1	A_2	\dots	X
v_0	f	f	\dots	$\not\models_p$
v_1	f	f	\dots	$\not\models_p$
		\dots		
v_k	t	f	\dots	$\not\models_p$
		\dots		

4.2 Hľadanie ohodnotení

Ohodnotenia pre danú formulu

Ak máme dané ohodnotenie atómov, pravdivosť formuly zistíme indukciou podľa jej štruktúry. Čo však spraviť, ak naopak máme danú formulu a hľadáme ohodnotenia, v ktorých je pravdivá či nepravdivá?

- Ak by sme hľadali všetky štruktúry, nemáme šancu, je ich nekonečne veľa.
- Všetkých vyhovujúcich ohodnotení môže byť exponenciálne veľa (nemôže teda existovať rýchly všeobecný algoritmus).
- Ohodnotenia možno hľadať rozborom všetkých možností pomocou tabuľky, ktorá má v záhlaví vytvárajúcu postupnosť danej formuly a v riadkoch jednotlivé ohodnotenia.
- Mohli by sme lepšie využiť znalosť štruktúry formuly na urýchlenie postupu? Azda áno: $A \wedge \neg A \wedge B_1 \wedge B_2 \wedge \dots \wedge B_{100}$.

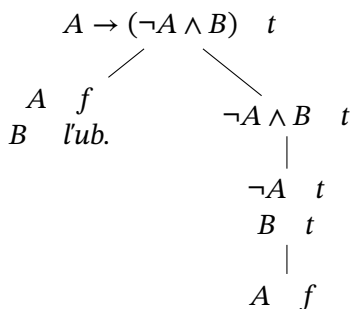
Ohodnotenia pre danú formulu

Pre formulu so známou pravdivostnou hodnotou vieme určiť pravdivosť priamych podformúl. Napr. ak $A \vee B$ je nepravda, tak A aj B musia byť nepravdivé.

Možností môže byť viac, čo zodpovedá vetveniu. Napr. pre pravdivú implikáciu $A \rightarrow B$ osobitne skúmame situácie, kde A je nepravdivá, a kde B je pravdivá.

Pri takejto postupnej analýze dostávame čoraz jednoduchšie formuly. Končíme, keď sa dostaneme k atómom: ich ohodnotenie presne popisuje, ako má model vyzeráť.

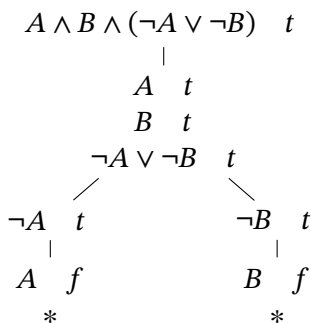
Hľadanie ohodnotení



Ľavá vetva zodpovedá dvom ohodnoteniam, pravá jednému (avšak už obsiahnutému v ľavej vetve).

Hľadanie ohodnotení

Môže sa stať, že v niektorej vetve vznikne *spor* (atóm A má byť zároveň pravdivý aj nepravdivý). Taká vetva neobsahuje žiadne vyhovujúce ohodnotenie a netreba sa ňou ďalej zapodievať.



Spor v každej vetve: formula nie je pravdivá v žiadnom ohodnotení.

Hľadanie ohodnotení

$$\begin{array}{c}
 A \wedge \neg A \wedge B_1 \wedge B_2 \wedge \cdots \wedge B_n \quad t \\
 | \\
 \begin{array}{cc}
 A & t \\
 \neg A & t \\
 B_1 & t \\
 \cdots & \\
 B_n & t
 \end{array} \\
 | \\
 \begin{array}{cc}
 A & f
 \end{array} \\
 *
 \end{array}$$

Tabuľka všetkých možných ohodnotení by mala 2^{n+1} riadkov, pritom táto úvaha je $O(n)$.

4.3 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 výrokovologicke ekvivalentných forém

Príklad 4.8. V jazyku \mathcal{L} z príkladu 4.1 označme $A = p(a)$ a $B = p(b)$. Sú formuly $X = \neg(A \rightarrow \neg B)$ a $Y = (A \wedge B)$ výrokovologicke ekvivalentné?

Preskúmajme všetky výrokovologické ohodnotenia atómov A a B :


v_i				X	Y
A	B	$\neg B$	$(A \rightarrow \neg B)$	$\neg(A \rightarrow \neg B)$	$(A \wedge B)$
v_0	f	f	\models_p	\models_p	\models_p
v_1	f	t	\models_p	\models_p	\models_p
v_2	t	f	\models_p	\models_p	\models_p
v_3	t	t	\models_p	\models_p	\models_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 4.9. 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*, skrátené $X \Leftrightarrow_p Y$ vtt pre *každé* výrokovologické ohodnotenie v pre jazyk \mathcal{L} platí, že X je pravdivá vo v vtt Y je pravdivá vo v .

\Leftrightarrow_p **verzus** \leftrightarrow

 **Pozor!** Nemýľte si zápis $X \Leftrightarrow_p Y$ s formulou $(X \leftrightarrow Y)$.

- $X \Leftrightarrow_p Y$ je skrátené vyjadrenie vzťahu dvoch formúl podľa definície 4.9. Keď napíšeme $X \Leftrightarrow_p Y$, 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, nespĺniteľná, môže vyplývať, či byť nezávislá od nejakej teórie, alebo môže byť výrokovologicky ekvivalentná s inou formulou.

Medzi $X \Leftrightarrow_p Y$ a $(X \leftrightarrow Y)$ je vzťah, ktorý si ozrejníme neskôr.

Známe ekvivalencie

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

Veta 4.10. *Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu. Nech A , B a C sú ľubovoľné výrokovologické formuly jazyka \mathcal{L} . Potom:*

$(A \rightarrow B) \Leftrightarrow_p (\neg A \vee B)$	nahradenie \rightarrow
$(A \wedge (B \wedge C)) \Leftrightarrow_p ((A \wedge B) \wedge C)$	asociatívnosť \wedge
$(A \vee (B \vee C)) \Leftrightarrow_p ((A \vee B) \vee C)$	asociatívnosť \vee
$(A \wedge B) \Leftrightarrow_p (B \wedge A)$	komutatívnosť \wedge
$(A \vee B) \Leftrightarrow_p (B \vee A)$	komutatívnosť \vee
$(A \wedge (B \vee C)) \Leftrightarrow_p ((A \wedge B) \vee (A \wedge C))$	distributívnosť \wedge cez \vee
$(A \vee (B \wedge C)) \Leftrightarrow_p ((A \vee B) \wedge (A \vee C))$	distributívnosť \vee cez \wedge

Veta 4.10 (pokračovanie).

$\neg(A \wedge B) \Leftrightarrow_p (\neg A \vee \neg B)$	de Morganove
$\neg(A \vee B) \Leftrightarrow_p (\neg A \wedge \neg B)$	zákony
$\neg\neg A \Leftrightarrow_p A$	zákon dvojitej negácie
$(A \wedge A) \Leftrightarrow_p A$	idempotencia pre \wedge
$(A \vee A) \Leftrightarrow_p A$	idempotencia pre \vee
$(A \wedge \top) \Leftrightarrow_p A$	identita pre \wedge
$(A \vee \perp) \Leftrightarrow_p A$	identita pre \vee
$(A \vee (A \wedge B)) \Leftrightarrow_p A$	absorpcia
$(A \wedge (A \vee B)) \Leftrightarrow_p A$	
$(A \vee \neg A) \Leftrightarrow_p \top$	vylúčenie tretieho (<i>tertium non datur</i>)
$(A \wedge \neg A) \Leftrightarrow_p \perp$	spor,

kde \top je ľubovoľná tautológia a \perp 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 4.8.

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

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

Môžeme však:

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

Príklad 4.11 (Dôkaz prvej ekvivalentnej dvojice z vety 4.10). 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:

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

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

Pretože ohodnotenie v bolo ľubovoľné, môžeme toto konštatovanie *zovšeobecniť* na všetky ohodnotenia pre \mathcal{L} a podľa definície 4.9 sú $(A \rightarrow B)$ a $(\neg A \vee B)$ výrokovologicky ekvivalentné.

Dôkazy rozborom prípadov

Rozbor prípadov z odrážkového zoznamu v predchádzajúcom dôkaze môžeme zapísať do *podobnej* tabuľky ako v príklade 4.8:

	A	B	$(A \rightarrow B)$	$(\neg A \vee B)$
v	$\not\models_p$	$\not\models_p$	$\not\models_p$	$\not\models_p$
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.

4.4 Vzťah tautológií, vyplývania a ekvivalencie

Tautológie a vyplývanie

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

Kedy je formula $((A_1 \wedge A_2) \rightarrow B)$ tautológia?

Vtedy, keď je pravdivá v každom ohodnotení, teda keď v každom ohodnotení v máme $v \models_p (A_1 \wedge A_2)$ alebo $v \models_p B$, čiže keď v každom ohodnotení v , v ktorom $v \models_p (A_1 \wedge A_2)$, máme aj $v \models_p B$ teda keď v každom ohodnotení v , v ktorom $v \models_p A_1$ a $v \models_p A_2$, máme aj $v \models_p B$, teda keď z $\{A_1, A_2\}$ výrokovologicky vyplýva B .

Vzťahy výrokovologického vyplývania a tautológií

Pripomeňme, že podľa tvrdenia 4.4: $\emptyset \models_p A$ vtt $\models_p A$.

Tvrdenie 4.12 (Sémantická verzia vety o 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) $T \cup \{A\} \models_p C$ vtt $T \models_p (A \rightarrow C)$.

b) $T \cup \{A, B\} \models_p C$ vtt $T \cup \{(A \wedge B)\} \models_p C$.

Dôsledok 4.13 (Redukcia vyplývania na tautológiu). *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} . Potom $\{A_1, \dots, A_n\} \models_p C$ vtt $\models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow C)$.*

Dôkaz tvrdenia 4.12. a) Nech T je teória a A a C sú výrokovologické formuly v ľubovoľnom jazyku \mathcal{L} .

(\Leftarrow) Predpokladajme, že $T \models_p (A \rightarrow C)$ 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 $v \models_p T$ a tiež $v \models_p A$.

Z $v \models_p T$ na základe predpokladu $T \models_p (A \rightarrow C)$ dostávame, že vo v je pravdivá implikácia $(A \rightarrow C)$, teda podľa definície pravdivosti $v \models_p A$ alebo $v \models_p C$. Pretože ale vieme, že $v \models_p A$, musí $v \models_p C$.

Keďže v bol ľubovoľný model $T \cup \{A\}$, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície vyplývania potom $T \cup \{A\} \models_p C$.

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

Nech by existovalo ohodnotenie v , ktoré je modelom T , ale nie formuly $(A \rightarrow C)$, teda podľa definície pravdivosti $v \models_p A$ a $v \not\models_p C$. Z $v \models_p T$ a $v \models_p A$ máme $v \models_p T \cup \{A\}$ a z predpokladu $T \cup \{A\} \models_p C$ dostávame $v \models_p C$, čo je spor.

b) Dôkaz je podobný ako v časti a). □

Dôkaz dôsledku 4.13. 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 4.12 a pomocou 4.4 dostávame:

$$\begin{aligned}
 \{A_1, A_2, \dots, A_n\} \models_p C & \quad \text{vtt} \quad \{(A_1 \wedge A_2), \dots, A_n\} \models_p C \\
 & \quad \text{vtt} \quad \dots \\
 & \quad \text{vtt} \quad \emptyset \cup \{((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n)\} \models_p C \\
 & \quad \text{vtt} \quad \emptyset \models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow C) \\
 & \quad \text{vtt} \quad \models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow C) \quad \square
 \end{aligned}$$

Tautológie a ekvivalencia

Kedy je formula $(X \leftrightarrow Y)$, teda $((X \rightarrow Y) \wedge (Y \rightarrow X))$ tautológia?

Vtedy a len vtedy, keď je pravdivá v každom ohodnotení, teda vtt v každom ohodnotení v máme $v \models_p (X \rightarrow Y)$ a $v \models_p (Y \rightarrow X)$, vtt v každom ohodnotení v máme buď $v \models_p X$ alebo $v \models_p Y$ a zároveň buď $v \models_p Y$ alebo $v \models_p X$, vtt v každom ohodnotení v platí, že ak $v \models_p X$, tak $v \models_p Y$, a ak $v \models_p Y$, tak $v \models_p X$, vtt v každom ohodnotení v máme $v \models_p X$ vtt $v \models_p Y$, vtt X je výrokologicky ekvivalentná s Y .

Tvrdenie 4.14. *Nech \mathcal{L} je jazyk výrokologickej časti logiky prvého rádu. Nech X a Y sú výrokologické formuly v \mathcal{L} . Potom $(X \leftrightarrow Y)$ je tautológia vtt X a Y sú výrokologicky ekvivalentné. (Skrátene: $\models_p (X \leftrightarrow Y)$ vtt $X \Leftrightarrow_p Y$.)*

4.5 Ekvivalentné úpravy a CNF

Reťazenie ekvivalentných úprav

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

$$\neg(A \rightarrow \neg B) \Leftrightarrow_p \neg(\neg A \vee \neg B) \Leftrightarrow_p (\neg\neg A \wedge \neg\neg B) \Leftrightarrow_p (A \wedge B)$$

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

Mohli ste to urobiť, lebo \Leftrightarrow_p je *tranzitívna* relácia na formulách, dokonca viac než iba tranzitívna.

Výrokovologická ekvivalencia ako relácia ekvivalencie

Tvrdenie 4.15. *Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu.*

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

- *Reflexivita: $X \Leftrightarrow_p X$.*
- *Symetria: Ak $X \Leftrightarrow_p Y$, tak $Y \Leftrightarrow_p X$.*
- *Tranzitivita: Ak $X \Leftrightarrow_p Y$ a $Y \Leftrightarrow_p Z$, tak $X \Leftrightarrow_p Z$.*

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 $v \models_p X$ vtt $v \models_p Z$.

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

- Ak $v \models_p X$, tak podľa predpokladu (1) a definície výrokovologickej ekvivalencie 4.9 musí platiť $v \models_p Y$, a teda podľa predpokladu (2) a definície ekvivalencie máme $v \models_p Z$.
- Nezávisle od toho, ak $v \models_p Z$, tak $v \models_p Y$ podľa (2) a def. 4.9, a teda $v \models_p X$ podľa (1) a def. 4.9.

Preto $v \models_p X$ vtt $v \models_p Z$.

Pretože v bolo ľubovoľné, môžeme náš záver zovšeobecniť na všetky ohodnotenia, a teda podľa definície ekvivalencie 4.9 sú X a Z výrokovologicky ekvivalentné. \square

Substitúcia pri ekvivalentných úpravách

V reťazci ekvivalentných úprav

$$\begin{aligned}\neg(A \rightarrow \neg B) &\Leftrightarrow_p \neg(\neg A \vee \neg B) \Leftrightarrow_p (\neg\neg A \wedge \neg\neg B) \\ &\Leftrightarrow_p (A \wedge \neg\neg B) \Leftrightarrow_p (A \wedge B)\end{aligned}$$

v prvom, treťom a štvrtom kroku *nezodpovedá celá* formula niektorej zo známych ekvivalencií z vety 4.10.

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

Definícia 4.16 (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 indukzívne 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 $b \in \{\wedge, \vee, \rightarrow\}$:

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

Korektnosť substitúcie ekvivalentnej formuly

Substitúciou ekvivalentnej podformuly, napríklad

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

skutočne dostávame formulu ekvivalentnú s pôvodnou:

Veta 4.17 (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

Mnoho teoretických i praktických problémov možno formulovať ako otázku splniteľnosti výrokovologickej formuly – SAT (napr. riešiteľnosť sudoku, existenciu cesty či farbenia v grafe, ekvivalenciu logických hardvérových obvodov).

Na riešenie SAT existujú dlhoročne vyvíjané solvery. Ukázalo sa, že najvýhodnejšie je mať vstup v špecifickom tvare: v konjunktívnej normálnej forme (CNF). Transformácia formuly do tejto formy je tak jedným z najčastejších využití ekvivalentných úprav.

Aby sme CNF 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 4.18. 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 $((A_1 \wedge A_2) \wedge A_3) \wedge \dots \wedge A_n$, skrátene $(A_1 \wedge A_2 \wedge A_3 \wedge \dots \wedge A_n)$.
 - Konjunkciu *prázdnej* postupnosti formúl ($n = 0$) označujeme \top . Chápeme ju ako ľubovoľnú *tautológiu*, napríklad $(P(c) \vee \neg P(c))$ pre nejaký unárny predikát P a nejakú konštantu c jazyka \mathcal{L} .
- *Disjunkciou postupnosti* A_1, \dots, A_n je formula $((A_1 \vee A_2) \vee A_3) \vee \dots \vee A_n$, skrátene $(A_1 \vee A_2 \vee A_3 \vee \dots \vee A_n)$.
 - Disjunkciu *prázdnej* postupnosti formúl označujeme \perp alebo \square . Chápeme ju ako ľubovoľnú *nesplniteľnú* formulu, napríklad $(P(c) \wedge \neg P(c))$.
- 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 4.19.

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 4.20. Literály: $P, C, \neg C, \neg O$

Klauzuly: $(\neg P \vee O \vee \neg C)$, ale aj $P, \neg O, \square$,

CNF: $((P \vee O) \wedge \square), ((\neg P \vee O) \wedge (O \vee C))$, ale aj $P, \neg O, \top, (P \vee \neg O) (P \wedge \neg O \wedge C)$,
 \square ,

kde P, O, C sú ľubovoľné atómy.

Existencia ekvivalentnej formuly v CNF

Veta 4.21. *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 $D = (C_1 \vee \dots \vee C_n)$ 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 . \square

Konverzia formuly do ekvivalentnej v CNF

Skúmanie všetkých ohodnotení podľa dôkazu vety 4.21 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: $(A \rightarrow B) \Leftrightarrow_p (\neg A \vee B)$
 - Presunieme \neg k atómom opakovaným použitím de Morganových zákonov a zákona dvojitej negácie.
2. Odstránime konjunkcie vnorené v disjunkciách „roznásobením“ podľa distributívnosti a komutatívnosti:

$$\begin{aligned}(A \vee (B \wedge C)) &\Leftrightarrow_p ((A \vee B) \wedge (A \vee C)) \\ ((B \wedge C) \vee A) &\Leftrightarrow_p (A \vee (B \wedge C)) \Leftrightarrow_p ((A \vee B) \wedge (A \vee C)) \\ &\Leftrightarrow_p ((B \vee A) \wedge (A \vee C)) \\ &\Leftrightarrow_p ((B \vee A) \wedge (C \vee A))\end{aligned}$$

Konverzia formuly do ekvivalentnej v CNF

Príklad 4.22. Úprava formuly do NNF:

$$\begin{aligned}((\neg S \wedge P) \rightarrow \neg(Z \vee \neg O)) &\Leftrightarrow_p (\neg(\neg S \wedge P) \vee \neg(Z \vee \neg O)) \quad (\text{nahr. } \rightarrow) \\ &\Leftrightarrow_p ((\neg\neg S \vee \neg P) \vee (\neg Z \wedge \neg\neg O)) \quad (2 \times \text{de Morgan}) \\ &\Leftrightarrow_p ((S \vee \neg P) \vee (\neg Z \wedge O)) \quad (2 \times \text{dvoj. neg.})\end{aligned}$$

Úprava formuly v NNF do CNF:

$$\begin{aligned}((S \vee \neg P) \vee (\neg Z \wedge O)) \\ &\Leftrightarrow_p (((S \vee \neg P) \vee \neg Z) \wedge ((S \vee \neg P) \vee O)) \quad (\text{distr. } \wedge \text{ cez } \vee)\end{aligned}$$

Podľa dohody v def. 4.18 výslednú formulu v CNF skráteno zapíšeme:

$$((S \vee \neg P \vee \neg Z) \wedge (S \vee \neg P \vee O))$$

4.6 CNF vs. XOR

XOR

Logická spojka exclusive or (XOR):

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- zodpovedá sčítaniu v poli \mathbb{Z}_2
- komutatívna a asociatívna
- rýchlo vypočítateľná, aj na úrovni hardvéru
- dôležitá v kryptológii

XOR

Ideálna šifra: všetky zašifrované texty sú rovnako pravdepodobné. Napr. vezmeme náhodný reťazec (kľúč) rovnako dlhý ako správa a spravíme XOR bit po bite. Použitý kľúč zahodíme a nikdy viac nepoužijeme.

Reálne šifry: kľúč je krátky (napr. 1024 B). Ak by sme ho nakopírovali veľakrát za sebou, bity správy šifrované tým istým bitom kľúča vytvoria slabinu (možno dešifrovať aj bez znalosti kľúča, stačí uhádnuť jeho dĺžku). Preto napr. použijeme kľúč ako seed do pseudonáhodného generátora a vygenerujeme reťazec potrebnej dĺžky.

Útoky na šifry: o.i. pomocou SAT solvera, ktorý vie pracovať s XOR (aktívna oblasť výskumu).

XOR

Ku XOR existuje prepis do CNF, napr. z $a \oplus b \oplus c$ sa stane $(a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (b \vee \neg a \vee \neg c) \wedge (c \vee \neg a \vee \neg b)$

Ale s počtom premenných rastie dĺžka ekvivalentnej CNF formuly exponenciálne. Preto sa oplatí predspracovanie: XOR formuly vnímame ako súčty nad \mathbb{Z}_2 a použijeme Gaussovu elimináciu.

$$a_1 \oplus a_2 \oplus a_3 = 0$$

$$a_1 \oplus a_3 \oplus a_4 = 0$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & | & 0 \\ 1 & 0 & 1 & 1 & | & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & | & 0 \\ 0 & 1 & 0 & 1 & | & 0 \end{pmatrix}$$

Rekapitulácia

Rekapitulácia

Dnes sme prebrali:

- Logické vyplývanie z teórie a logický dôsledok teórie
- Nezávislosť formuly od teórie
- Štyri situácie vo vzťahoch teórií a formúl a ich praktické dôsledky
- Splniteľné a nespĺniteľné teórie
- Vzťah nespĺniteľnosti a vyplývania
- Význačné sémantické vlastnosti formúl: tautologickosť, splniteľnosť, nespĺniteľnosť, falzifikovateľnosť
- Ekvivalencia — sémantický vzťah formúl
- Syntaktické odvodenie ekvivalencie pomocou substitúcií podľa známych ekvivalencií
- NNF a CNF
- Vzťah tautológií s vyplývaním a ekvivalenciou

Literatúra

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