

# Matematika (4): Logika pre informatikov

Poznámky z prednášok

Ján Kl'uka, Jozef Šiška

Letný semester 2019/2020

Posledná aktualizácia: 17. marca 2020

## Obsah

<b>1. Úvod. Atomické formuly</b>	<b>3</b>
<b>0. Úvod</b>	<b>3</b>
0.1. O logike . . . . .	3
0.2. O kurze . . . . .	9
<b>1. Atomické formuly</b>	<b>11</b>
1.1. Syntax atomických formúl . . . . .	15
1.2. Sémantika atomických formúl . . . . .	18
<b>2. Výrokovologické spojky</b>	<b>23</b>
<b>2. Výrokovologické spojky</b>	<b>23</b>
2.1. Boolovské spojky . . . . .	24
2.2. Implikácia . . . . .	29
2.3. Ekvivalencia . . . . .	31

2.4.	Syntax výrokovologických formúl . . . . .	32
2.5.	Sémantika výrokovologických formúl . . . . .	41
2.6.	Správnosť a vernosť formalizácie . . . . .	43
<b>3.</b>	<b>Výrokovologické vyplývanie</b>	<b>45</b>
<b>3.</b>	<b>Výrokovologické vyplývanie</b>	<b>45</b>
3.1.	Teórie a ich modely . . . . .	46
3.2.	Výrokovologické teórie a ohodnotenia . . . . .	47
3.3.	Vyplývanie, nezávislosť a nesplniteľnosť . . . . .	52
<b>4.</b>	<b>Vlastnosti a vzťahy výrokovologických formúl</b>	<b>59</b>
<b>4.</b>	<b>Vlastnosti a vzťahy výrokovologických formúl</b>	<b>59</b>
4.1.	Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly	59
4.2.	Ekvivalencia . . . . .	64
4.3.	Vzťah tautológií, vyplývania a ekvivalencie . . . . .	68
4.4.	Ekvivalentné úpravy a CNF . . . . .	71
<b>5.</b>	<b>Dôkazy a výrokovologické tablá</b>	<b>76</b>
<b>5.</b>	<b>Dôkazy a výrokovologické tablá</b>	<b>76</b>
5.1.	Druhy dôkazov . . . . .	78
5.2.	Výrokovologické tablá . . . . .	80

## 1. prednáška

# Úvod

## Atomické formuly

---

### 0. Úvod

#### 0.1. O logike

##### Čo je logika

Logika je vedná disciplína, ktorá študuje usudzovanie.

Správne, racionálne usudzovanie je základom vedy a inžinierstva.

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

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

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

##### Ako sa v 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 Ako vyplýva z jazyka?

##### Jazyk, poznatky a teórie

*Jazyk* slúži na vyjadrenie tvrdení, ktoré popisujú informácie — poznatky o svete.

Súbor poznatkov, ktoré považujeme za pravdivé, tvorí *teóriu*.

*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

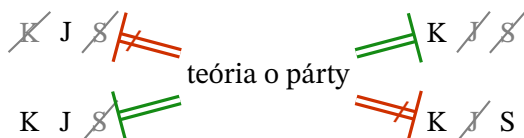
Teória rozdeľuje *možné stavy sveta* (interpretácie) na:

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

⊭ stavy, v ktorých je nepravdivá.

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

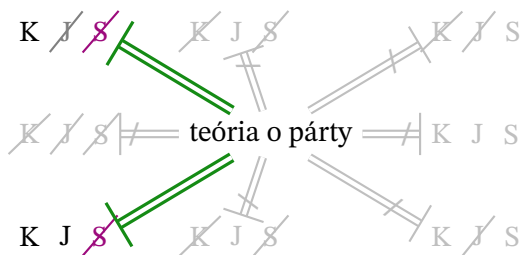
*Príklad 0.2.* Vymenujme možné stavy prítomnosti Kim, Jima a Sarah na párty. Zistíme, v ktorých sú pravdivé jednotlivé tvrdenia našej teórie a celá teória.



### Logické dôsledky

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

*Príklad 0.3.* Logickým dôsledkom teórie P0, P1, P2, P3 je napríklad: *Sarah nepôjde na párty.*



## Logické usudzovanie

Vymenovanie všetkých svetov 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).

### Kontrapríklad

Ak úsudok nie je správny, vieme nájsť *kontrapríklad*.

Stav sveta, v ktorom sú predpoklady pravdivé, ale záver je nepravdivý.

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

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

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

### Ťažkosti s prirodzeným jazykom

*Prirodzený jazyk* je problematický:

- Viacznačné slová: Milo *je* v posluchárni A.
- Viacznačné tvrdenia: Videl som dievča v sále *s ďalekohl'adom*.
- 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.

### Formálne jazyky

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

- Presne definovaná, zjednodušená syntax (pravidlá zápisu tvrdení) a sémantika (význam).

- Niekoľko formálnych jazykov už poznáte: aritmetika, jazyky fyzikálnych a chemických vzorcov, programovacie jazyky, ...
- Problémy z reálneho sveta opísané v prirodzenom jazyku musíme najprv *formalizovať*, a potom naň môžeme použiť logický aparát.
- Formalizácia vyžaduje cvik, trocha veda, trocha umenie.

### Formalizácia poznatkov

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

Karol je trikrát starší ako Mária.		$k = 3 \cdot m$
Súčet Karolovho a Máriinho veku je 12 rokov.	$\rightsquigarrow$	$k + m = 12$
Koľko rokov majú Karol a Mária?		

Stretli ste sa už aj s formálnym jazykom výrokovej logiky.

*Príklad 0.6.* Sformalizujme náš párty príklad:

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

P1: Sarah nepôjde na párty, ak pôjde Kim.

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

P3: Sarah nepôjde bez Jima.

### Logika prvého rádu

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

Do dnešnej podoby sa vyvinul na koncom 19. a v prvej polovici 20. storočia — Gottlob Frege, Giuseppe Peano, Charles Sanders Peirce.

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

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

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

## Logika prvého rádu a informatika

Informatika sa vyvinula z logiky (John von Neumann, Alan Turing, Alonzo Church, ...)

Prvky logiky prvého rádu obsahuje väčšina *programovacích jazykov*:

- `all(x > m for x in arr),`
- `select T1.x, T2.y from T1 inner join T2 on T1.z = T2.z where T1.z > 25,`

niektoré (Prolog) sú priamo podmnožinou FOL.

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

Vo *výpočtovej logike* a umelej inteligencii sa FOL používa na riešenie rôznych ťažkých problémov (plánovanie, rozvrh, hľadanie a overovanie dôkazov matematických tvrdení, ...) simulovaním usudzovania.

## Kalkuly — formalizácia usudzovania

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

**korektné** — odvodzujú iba logické dôsledky

**úplné** — umožňujú odvodiť všetky logické dôsledky

Kalkuly sú bežné v matematike

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

...

Sú korektné, ale nie vždy úplné.

Poznáte už aj jeden logický kalkul — ekvivalentné úpravy.



## 0.2. O tomto kurze

### Čím sa budeme zaoberať v tomto kurze

**Teoreticky** • Jazykmi logiky prvého rádu (FOL), jeho syntaxou a sémantikou

- Správnymi úsudkami v ňom a dôvodmi, prečo sú správne
- Korektnosťou a úplnosťou logických kalkulov
- Automatizáciou usudzovania

**Prakticky** • Vyjadrovaním problémov vo FOL

- Automatizovaním riešenia problémov
- Manipuláciou symbolických stromových štruktúr (výrazov — formúl a termov)
- Programovaním vlastných jednoduchých automatických dokazovačov

**Filozoficky** • Zamýšľanými a nezamýšľanými významami tvrdení

- Obmedzeniami vyjadrovania a usudzovania

### Prístup k logike na tomto predmete

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

V tomto kurze sa budeme snažiť byť *presní*.

- *Zdanlivo* budeme o jednoduchých veciach hovoriť zložito

Pojmy z logiky budeme *definovať matematicky*

- ako množiny, postupnosti, funkcie, atď., ← Matematika (1), (3)

na praktických cvičeniach aj *programami*

- ako reťazce, slovníky, triedy a metódy. ← Programovanie (1), (2)

Budeme sa pokúšať *dokazovať* ich vlastnosti.

Budeme teda hovoriť o *formálnej logike* pomocou matematiky, ktorá je ale sama postavená na *logike v prirodzenom jazyku* — *meta* matematika logiky, matematika **o** logike.

## Organizácia kurzu — rozvrh, kontakty, pravidlá

[https://dai.fmph.uniba.sk/w/Course:Mathematics\\_4](https://dai.fmph.uniba.sk/w/Course:Mathematics_4)

### Aktívne učenie

Na cvičeniach budeme používať techniku nazývanú *aktívne učenie*:

- Riešenie zadaných problémov v skupinkách.
- Cvičiaci budú s vami *konzultovať* postup a riešenia.
- Na tabuľu sa budú úlohy riešiť len výnimočne.
- Budete mať k dispozícii materiály z prednášok a zbierku s ukážkovými riešeniami a ďalšími úlohami.

### Prečo?

- Samostatnou snahou o riešenie sa *naučíte viac a hlbšie* než pozorovaním, ako riešia iní.
- V praxi vám nik neukáže vzorové riešenie problémov.

### Aktívne učenie

Problémy:

- Bude to mierne frustrujúce, budete neistí.
- Preto budete mať *pocit*, že ste sa nenaučili veľa.
- Je to *normálne*, ale *nebude to pravda*!

### Čo s tým?

- Pýtajte sa!
- Prídite na konzultácie (termín oznámime na prvých cvičeniach).

# 1. Atomické formuly

## Jazyky logiky prvého rádu

Logika prvého rádu je trieda (rodina) formálnych jazykov.

Zdieľajú:

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

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

## Atomické formuly a výroky v prirodzenom jazyku

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

*Príklady 1.1.*

- ✓ Milo beží.
- ✓ Jarka vidí Mila.
- ✗ Milo beží, ale Jarka ho nevidí.
- ✗ Jarka vidí všetkých.
- ✓ Jarka dala Milovi Bobíka v sobotu.
- ✗ Jarka nie je doma.
- ✗ Niekoľko je doma.
- ✓ Súčet 2 a 2 je 3.
- ✓ Prezidentkou SR je Zuzana Čaputová.

## Individuové konštanty

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

Zodpovedajú vlastným menám, jednoznačným pomenovaniám, niekedy zámenám.

*Príklady 1.2.* Jarka, 2, Zuzana\_Čaputová, sobota,  $\pi$ , ...

## Individuové konštanty a objekty

### Individuová konštantá

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

### Objekt

- môže byť pomenovaný aj viacerými individuovými konštantami (napr. *Prezidentka\_SR* a *Zuzana\_Čaputová*);
- nemusí mať žiadne meno.

## Predikátové symboly

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

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

Jarka	vidí	Mila.
podmet	prísudok	predmet
podmetová časť	prísudková časť	

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

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

## Arita predikátového symbolu

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

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

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

## Zamýšľaný význam predikátových symbolov

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

Príklady 1.4.     $\text{pes}^1(x)$      $x$  je pes  
                     $\text{čierne}^1(x)$      $x$  je čierne  
                     $\text{beží}^1(x)$      $x$  beží

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

Príklady 1.5.     $\text{vidí}^2(x, y)$              $x$  vidí  $y$   
                     $\text{dal}^4(x, y, z, t)$      $x$  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: predikát mladší<sup>2</sup> môže označovať vzťah „ $x$  je mladší ako  $y$ “ presne; predikát mladý<sup>1</sup> 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

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

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.*

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

*Príklad 1.6.* Sformalizujme v jazyku s konštantami Evka, Jarka a Milo a predikátom vyšší<sup>2</sup> výroky:

$A_1$ : Jarka je vyššia ako Milo.  $\rightsquigarrow$  vyšší<sup>2</sup>(Jarka, Milo)

$A_2$ : Evka je nižšia ako Milo.  $\rightsquigarrow$  vyšší<sup>2</sup>(Milo, Evka)

Zanedbávame nepodstatné detaily — pomocné slovesá, predložky, skloňovanie, rod, ...: vyšší<sup>2</sup>( $x, y$ ) —  $x$  je vyšší/vyššia/vyššie ako  $y$ .

### Návrh jazyka pri formalizácii

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

*Príklady 1.7.*  $A_1$ : Jarka dala Milovi Bobíka.

$\rightsquigarrow$  ~~dalaMiloviBobíka<sup>1</sup>(Jarka)~~ ~~dalBobíka<sup>2</sup>(Jarka, Milo)~~ dal<sup>3</sup>(Jarka, Milo, Bobík)

$A_2$ : Evka dostala Bobíka od Mila.

$\rightsquigarrow$  ~~dalBobíka<sup>2</sup>(Milo, Evka)~~ dal<sup>3</sup>(Milo, Evka, Bobík)

$A_3$ : Evka dala Jarke Cilku.

$\rightsquigarrow$  ~~dalCilku<sup>2</sup>(Evka, Jarka)~~ dal<sup>3</sup>(Evka, Jarka, Cilka)

$A_4$ : Bobík je pes.

$\rightsquigarrow$  pes<sup>1</sup>(Bobík)

## Návrh jazyka pri formalizácii

Minimalizujeme počet predikátov, uprednostňujeme flexibilnejšie, viacúčelovejšie (dal<sup>3</sup> pred dalBobíka<sup>2</sup> a dalCilku<sup>2</sup>).

- Expresívnejší jazyk (vyjadrí viac).
- Zrejmejšie logické vzťahy výrokov.

Podobné normalizácii databázových schém.

### 1.1. Syntax atomických formúl

#### Presné definície

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

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

Spôľahlivé 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. zdefinujeme triedu `AtomickaFormula` v Pythone.

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

#### Syntax atomických formúl logiky prvého rádu

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

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

## Symboly jazyka atomických formúl logiky prvého rádu

Z čoho sa skladajú atomické formuly?

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

Mimologickými symbolmi sú

- *individuové konštanty* z nejakej 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 by ste povedali, že *abecedou* jazyka  $\mathcal{L}$  atomických formúl logiky prvého rádu je  $\Sigma_{\mathcal{L}} = \mathcal{C}_{\mathcal{L}} \cup \mathcal{P}_{\mathcal{L}} \cup \{\doteq, (, ), ,\}$ .

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

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

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

## Príklady symbolov jazykov atomických formúl logiky prvého rádu

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

- $\mathcal{C}_{\mathcal{L}_{\text{dz}}} = \{\text{Bobík, Cilka, Evka, Jarka, Milo}\},$
- $\mathcal{P}_{\mathcal{L}_{\text{dz}}} = \{\text{dal, pes}\},$
- $\text{ar}_{\mathcal{L}_{\text{dz}}}(\text{dal}) = 3, \text{ar}_{\mathcal{L}_{\text{dz}}}(\text{pes}) = 1.$

*Príklad 1.10.* Príklad o návštevníkoch party by sme mohli sformalizovať v jazyku  $\mathcal{L}_{\text{party}}$ , kde  $\mathcal{C}_{\mathcal{L}_{\text{party}}} = \{\text{Kim, Jim, Sarah}\}, \mathcal{P}_{\mathcal{L}_{\text{party}}} = \{\text{príde}\}$  a  $\text{ar}_{\mathcal{L}_{\text{party}}}(\text{príde}) = 1.$



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

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

V logike sa jazyk takto nedefinuje, pretože potrebujeme rozlišovať *rôzne druhy slov*. Navyše tieto slová zodpovedajú slovenským *vetám*.

## Príklady atómov jazyka

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

Bobík  $\doteq$  Bobík

Cilka  $\doteq$  Bobík

Evka  $\doteq$  Jarka

Bobík  $\doteq$  Cilka

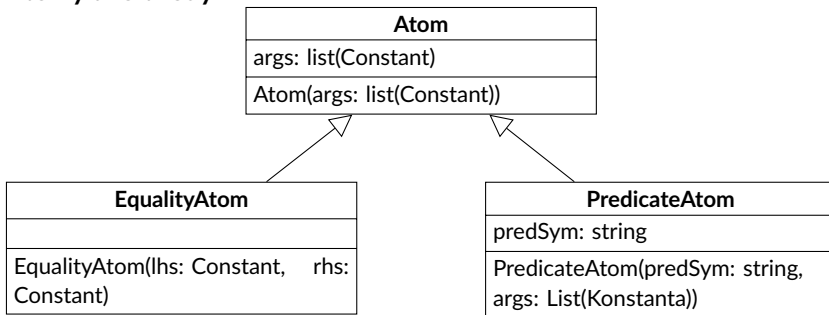
a predikátové atómy:

pes(Cilka)

dal(Cilka, Milo, Bobík)

dal(Jarka, Evka, Milo).

## Atómy ako triedy



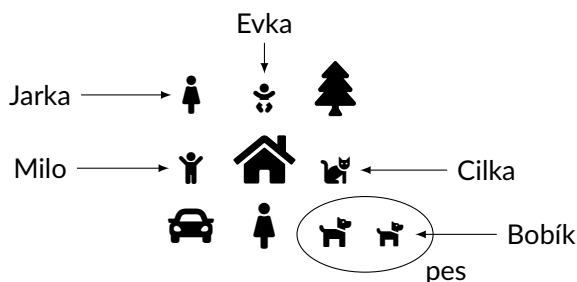
## 1.2. Sémantika atomických formúl

### Vyhodnotenie atomickej formuly

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

Pozrieme sa na túto situáciu a zistíme:

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



### Vyhodnotenie atomickej formuly

Ako môžeme tento postup matematicky alebo informaticky modelovať?  
Potrebujeme:

- matematický/informatický model situácie (stavu vybranej časti sveta),
- postup na jeho použitie pri vyhodnocovaní pravdivosti formúl.

### Matematický model stavu sveta

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

### Matematický model stavu sveta

Potrebujeme vedieť:

- ktoré objekty sú v popisovanej situácii prítomné,
- množina všetkých objektov — *doména*;
- pre každú konštantu  $c$  z jazyka  $\mathcal{L}$ , ktorý objekt z domény  $c$  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;
- priradenie objektov ku konštantám a množín/relácií k predikátom musí byť jednoznačné
- *interpretačná funkcia*.

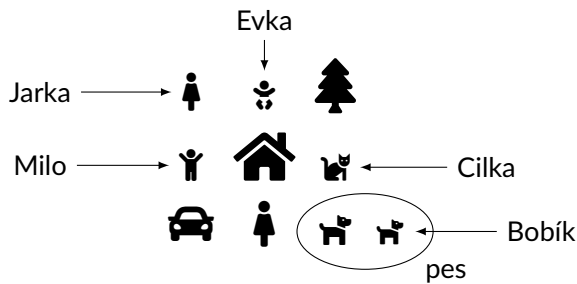
## Štruktúra pre jazyk

**Definícia 1.14.** Nech  $\mathcal{L}$  je jazyk atomických formúl 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  $\mathcal{L}$  priradzuje prvok  $i(c) \in D$ ;
- každému predikátovému symbolu  $P$  jazyka  $\mathcal{L}$  s aritou  $n$  priradzuje množinu  $i(P) \subseteq D^n$ .

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

## Príklad štruktúry



*Príklad 1.16.*

$$\begin{aligned}
\mathcal{M} &= (D, i), \quad D = \left\{ \text{ľudia}, \text{deti}, \text{strom}, \text{ľudia}, \text{dom}, \text{zvieratka}, \text{auta}, \text{ľudia}, \text{zvieratka}, \text{zvieratka} \right\} \\
i(\text{Bobík}) &= \text{ľudia} & i(\text{Cilka}) &= \text{zvieratka} \\
i(\text{Evka}) &= \text{deti} & i(\text{Jarka}) &= \text{ľudia} & i(\text{Milo}) &= \text{ľudia} \\
i(\text{pes}) &= \{ \text{ľudia}, \text{ľudia} \} \\
i(\text{dal}) &= \left\{ (\text{ľudia}, \text{deti}, \text{ľudia}), (\text{ľudia}, \text{ľudia}, \text{ľudia}), (\text{deti}, \text{ľudia}, \text{zvieratka}) \right\}
\end{aligned}$$

## Štruktúra ako informatický objekt












Štruktúru sme definovali pomocou *matematických* objektov.

Aký *informatický* objekt zodpovedá štruktúre?

*Databáza:*

Predikátové symboly jazyka  $\sim$  veľmi zjednodušená schéma DB (arita  $\sim$  počet stĺpcov)

Interpretácia predikátových symbolov  $\sim$  konkrétne tabuľky s dátami

$i(\text{pes}^1)$	$i(\text{dal}^3)$		
1	1	2	3
 			
			
			

## Štruktúry — upozornenia

Štruktúr pre daný jazyk je *nekonečne veľa*.

Doména štruktúry

- môže mať ľubovoľné prvky;
- nijak *nesúvisí* s intuitívnym významom interpretovaného jazyka;  
Jazyk o deťoch a zvieratkách — číselná doména štruktúry
- 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*.

### Pravdivosť atomickej formuly v štruktúre

Ako zistíme, či je atomická formula pravdivá v štruktúre?

**Definícia 1.17.** 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 určenia pravdivosti atómu v štruktúre

Príklad 1.18.

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

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

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  $(i(\text{Evka}), i(\text{Jarka}), i(\text{Cilka})) = (\text{stom, ľudia, mačka}) \in i(\text{dal})$ .

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

## 2. prednáška

# Výrokovologické spojky

---

### Rekapitulácia

Minulý týždeň sme sa naučili:

- Čo sú symboly jazyka logiky prvého rádu.
- Čo sú atomické formuly.
- Čo sú štruktúry.
  - Konštanty označujú objekty.
  - Predikáty označujú vzťahy a vlastnosti.
- Kedy sú atomické formuly pravdivé.
- Jazyk atomických formúl je oproti slovenčine veľmi slabý.
  - Môžu byť pravdivé vo veľmi čudných štruktúrach.
  - Veľa sme vyjadrovali približne.

## 2. Výrokovologické spojky

### Výrokovologické spojky

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

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

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

## Nevýrokovologické spojky

### Negatívny príklad

Spojka *pretože* nie je výrokovologická.

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

*Je pravdivý v situácii:* Je 18:00 a Karol je doma, aby nakŕmil psa Bobíka, ktorý by inak bol hladný až do 19:30, keď sa Jarka vráti zo školy, kde má cvičenia od 17:20 do 18:50.

*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> .

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

Zloženú formulu vždy *zátvorkujeme*.

### Formalizácia viacnásobných vetných členov konjunkciou

Zlučovacie viacnásobné vetné členy tiež formalizujeme ako konjunkcie:

- *Jarka aj Karol* sú doma. ( $\text{doma}(\text{Jarka}) \wedge \text{doma}(\text{Karol})$ )
- Karol *sa potkol a spadol*. ( $\text{potkol\_sa}(\text{Karol}) \wedge \text{spadol}(\text{Karol})$ )
- Jarka dostala Bobíka *od mamy a otca*. ( $\text{dostal}(\text{Jarka}, \text{Bobík}, \text{mama}) \wedge \text{dostal}(\text{Jarka}, \text{Bobík}, \text{otec})$ )

Podobne (viacnásobné zlučovacie) prívlastky vlastností:

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

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

## Disjunkcia

Disjunkcia  $\vee$  je binárna spojka, ktorá zodpovedá spojкам *alebo*, *či*, *bud'* ..., *alebo* ... v *inkluzívnom* význame (môžu nastať aj obe možnosti).

Disjunkciou formalizujeme vylučovacie súvetia:

- Jarka je doma *alebo* Karol je doma. ( $\text{doma}(\text{Jarka}) \vee \text{doma}(\text{Karol})$ )
- Bud' je Karol doma, *alebo* je Jarka v škole. ( $\text{doma}(\text{Karol}) \vee \text{v\_škole}(\text{Jarka})$ )

Zloženú formulu vždy *zátvorkujeme*.

## Formalizácia viacnásobných vetných členov disjunkciou

Viacnásobné vetné členy s vylučovacou spojkou 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 Bobíka od mamy *alebo* otca. ( $\text{dostal}(\text{Jarka}, \text{Bobík}, \text{mama}) \vee \text{dostal}(\text{Jarka}, \text{Bobík}, \text{otec})$ )
- Bobík je čierny *či* tmavohnedý psík. ( $((\text{čierny}(\text{Bobík}) \vee \text{tmavohnedý}(\text{Bobík})) \wedge \text{pes}(\text{Bobík}))$ )

## Exkluzívna disjunkcia

Konštrukcia *bud' ..., alebo ... neznamená* nutne exkluzívnu disjunkciu.

- Bobík a Cilka sa pobili. Bud' Bobík pohrýzol Cilku, *alebo* Cilka poškrabala Bobíka. (Mohlo sa stať jedno aj druhé.)

Niekedy samotné *alebo* znamená exkluzívnu disjunkciu.

- Jarka je doma *alebo* v škole. (Nemôže byť súčasne na dvoch miestach.)

Exkluzívnu disjunkciu môžeme vyjadriť zložitejšou formulou:  $((\text{doma}(\text{Jarka}) \vee \text{v\_škole}(\text{Jarka})) \wedge \neg(\text{doma}(\text{Jarka}) \wedge \text{v\_škole}(\text{Jarka})))$ .

## Jednoznačnosť rozkladu

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

Slovenské tvrdenia so spojkami nie sú vždy jednoznačné:

- Karol je doma a Jarka je doma alebo je Bobík šťastný.  
?  $((\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka})) \vee \text{šťastný}(\text{Bobík}))$   
?  $(\text{doma}(\text{Karol}) \wedge (\text{doma}(\text{Jarka}) \vee \text{šťastný}(\text{Bobík})))$
- Karol je doma alebo Jarka je doma a Bobík je šťastný.  
?  $((\text{doma}(\text{Karol}) \vee \text{doma}(\text{Jarka})) \wedge \text{šťastný}(\text{Bobík}))$   
?  $(\text{doma}(\text{Karol}) \vee (\text{doma}(\text{Jarka}) \wedge \text{šťastný}(\text{Bobík})))$

## Jednoznačnosť rozkladu v slovenčine

Slovenčina má prostriedky podobné zátvorkám:

- Karol aj Jarka sú (obaja) doma alebo je Bobík šťastný.  
 $((\text{doma}(\text{Karol}) \wedge \text{doma}(\text{Jarka})) \vee \text{šťastný}(\text{Bobík}))$
- Karol je doma a **bud'** je doma Jarka, alebo je Bobík šťastný. **Aj** Karol je doma, **aj** Jarka je doma alebo je Bobík šťastný.  
 $(\text{doma}(\text{Karol}) \wedge (\text{doma}(\text{Jarka}) \vee \text{šťastný}(\text{Bobík})))$
- **Doma** je Karol alebo Jarka a Bobík je šťastný.  
**Nieko** z dvojice Karol a Jarka je doma a Bobík je šťastný.  
 $((\text{doma}(\text{Karol}) \vee \text{doma}(\text{Jarka})) \wedge \text{šťastný}(\text{Bobík}))$
- **Bud'** je doma Karol, alebo je doma Jarka a Bobík je šťastný.  
 $(\text{doma}(\text{Karol}) \vee (\text{doma}(\text{Jarka}) \wedge \text{šťastný}(\text{Bobík})))$

Príslušnosť výrokov k spojкам vyjadrujú viacnásobný vetný člen (+*obaja*, *nieko* z) a kombinácie spojok *bud' ...*, *alebo ...*; *aj ...*, *aj ...*; *ani ...*, *ani ...*; *atď.*

## Oblasť platnosti negácie

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

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

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

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

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

## Negácia rovnostného atómu

Rovnosť nie je spojka, preto:

✓  $\neg \text{Jarka} \doteq \text{Karol} - \text{Jarka nie je Karol.}$

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

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 skráteno zapisovať  $\tau \neq \sigma$ .


## 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. výrok *ak by Sarah prišla, Jim by prišiel tiež* je nepravdivý, keď si myslíme, že išli rovnakým autobusom, ale Jim išiel iným a zmeškal ho.

*Keď ... , potom ...* má často význam časovej následnosti, ktorý implikácia 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* s 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:

Logikou prejdete, *ak* odovzdáte všetky domáce úlohy.

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

Žiaľ, z našich pravidiel vyplýva:

Logikou prejdete, *iba ak* odovzdáte všetky domáce úlohy.

Odovzdať úlohy *je nutné*, ale na prejdenie 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 ak  $B$ .
- $A$ , len ak  $B$ .
- $A$  nastane iba spolu s  $B$ .
- $A$  nenastane bez  $B$ .
- $B$ , ak  $A$ .
- $B$ , pokiaľ  $A$ .

## 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 Bobík s ním.

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

## 2.4. Syntax výrokovologických formúl

### Syntax a sémantika formúl s výrokovologickými spojkami

Podobne ako pri atomických formulách, aj pri formulách s výrokovologickými spojkami potrebujem *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 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*  $ar_{\mathcal{L}}(P) \in \mathbb{N}^+$ .

### 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 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.  $\neg \text{príde}(\text{Sarah})$ .
- Premenné 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 0 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  $((A \rightarrow B) \wedge (B \rightarrow A))$ .

*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?

### Indukcia na konštrukciu formuly

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

1. *každý atóm z  $\mathcal{A}_{\mathcal{L}}$  má vlastnosť  $P$ ,*
- 2.1. *ak formula  $A$  má vlastnosť  $P$ , tak aj  $\neg A$  má vlastnosť  $P$ ,*
- 2.2. *ak formuly  $A$  a  $B$  majú vlastnosť  $P$ , tak aj každá z formúl  $(A \wedge B)$ ,  $(A \vee B)$  a  $(A \rightarrow B)$  má vlastnosť  $P$ ,*

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

### Vytvárajúca postupnosť

**Definícia 2.11.** *Vytvárajúcou postupnosťou nad jazykom  $\mathcal{L}$  výrokovologickej časti logiky prvého rádu je ľubovoľná konečná postupnosť  $A_0, \dots, A_n$  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  $X$ .

## Formula a existencia vytvárajúcej postupnosti

**Tvrdenie 2.12.** Postupnosť symbolov  $A$  je formulou vtedy a len vtedy, keď existuje vytvárajúca postupnosť pre  $A$ .

Osnova dôkazu.  $(\Rightarrow)$  Indukciou na konštrukciu formuly

$(\Leftarrow)$  Indukciou na dĺžku vytvárajúcej postupnosti □

## (Ne)jednoznačnosť rozkladu formúl výrokovej logiky

Čo by sme zadefinovali „formuly“ takto?

### Definícia „formúl“

Nech  $\mathcal{L}$  je jazyk výrovkologickej 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 spojka  $b \in \{\wedge, \vee, \rightarrow\}$  také, že  $X = (A \ b \ B)$ .*

### Problémy s vytvárajúcou postupnosťou

Vytvárajúca postupnosť popisuje konštrukciu formuly podľa definície formúl:

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

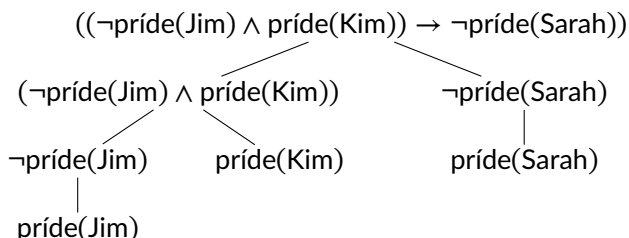
ale

- 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 ale vieme predstaviť ako *strom*:



Takéto stromy voláme *vytvárajúce*.

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

## 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 zadefinujeme?

## Priame 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*).

## Podformuly

**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

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

1. *báza indukcie: každá formula stupňa 0 má vlastnosť  $P$ ,*
2. *indukčný krok: pre každú formulu  $X$  z predpokladu, že všetky formuly menšieho stupňa ako  $\deg(X)$  majú vlastnosť  $P$ , vyplýva, že aj  $X$  má vlastnosť  $P$ ,*

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

## 2.5. Sémantika výrokovologických formúl

### Sémantika výrokovej logiky

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

### Štruktúra pre jazyk

Definícia štruktúry takmer nemeňte:

**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  $i(P) \subseteq D^n$ .

### Splnenie 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:

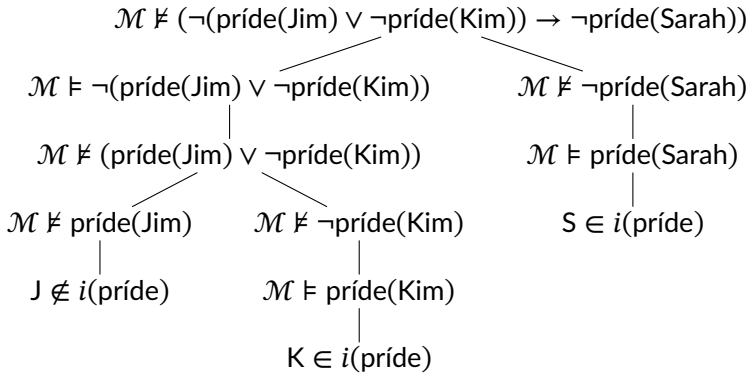
- $\mathcal{M} \models c_1 \doteq c_2$  vtt  $i(c_1) = i(c_2)$ ,
- $\mathcal{M} \models P(c_1, \dots, c_n)$  vtt  $(i(c_1), \dots, i(c_n)) \in i(P)$ ,
- $\mathcal{M} \models \neg A$  vtt  $\mathcal{M} \not\models A$ ,
- $\mathcal{M} \models (A \wedge B)$  vtt  $\mathcal{M} \models A$  a zároveň  $\mathcal{M} \models B$ ,
- $\mathcal{M} \models (A \vee B)$  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 vtt skracuje vtedy a len vtedy a  $\mathcal{M} \not\models A$  skracuje  $A$  nie je pravdivá v  $\mathcal{M}$ .

### Vyhodnotenie formuly

*Príklad 2.22* (Vyhodnotenie formuly v štruktúre). Majme štruktúru  $\mathcal{M} = (D, i)$  pre jazyk o party, kde  $D = \{A, K, J, S\}$ ,  $i(\text{Kim}) = K$ ,  $i(\text{Jim}) = J$ ,  $i(\text{Sarah}) = S$ ,  $i(\text{príde}) = \{K, S\}$ .

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



### Hľadanie štruktúry

*Príklad 2.23* (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  $\mathcal{M} \models \text{príde}(\text{Jim})$  alebo  $\mathcal{M} \not\models \text{príde}(\text{Kim})$  alebo  $i(\text{Sarah}) \notin i(\text{príde})$ .

Stačí teda zabezpečiť, aby  $i(\text{Sarah}) \notin i(\text{príde})$ .

## 2.6. 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).

Uprednostňujeme ich vyjadrovanie *samostatnými formulami*.  
Rovnaké dôvody ako pre vernosť.

### Logické dôsledky a konverzačné implikatúry

Niektoré tvrdenia *vyznievajú* silnejšie, ako naozaj sú:

- Prílohou sú *bud' zemiaky alebo šalát*. Znie ako exkluzívna disjunkcia.
- *Prejdete, ak všetky úlohy vyriešite na 100 %*. Znie mnohým ako ekvivalencia.

*Skutočný logický dôsledok* tvrdenia *nemôžeme poprieť* dodatkami bez sporu s pôvodným tvrdením.

- Keď k tvrdeniu *Karol a Jarka sú doma* dodáme *Ale Karol nie je doma*, dostaneme sa do sporu. Takže *Karol je doma* je skutočným dôsledkom pôvodného výroku.

### Logické dôsledky a konverzačné implikatúry

Dôsledok tvrdenia, ktorý *môžeme poprieť* dodatkami bez sporu s pôvodným tvrdením, sa nazýva *konverzačná implikatura* (H. P. Grice). Nie je skutočným logickým dôsledkom pôvodného tvrdenia.

- Prílohou sú *bud' zemiaky alebo šalát*. *Ale môžete si dať aj oboje*. Dodatok popiera exkluzívnosť, ale nie je v spore s tvrdením.
- *Prejdete, ak všetky úlohy vyriešite na 100 %*. *Ale nemusíte mať všetko na 100 %, aby ste prešli*. Dodatok popiera opačnú implikáciu, ale nie je v spore s tvrdením.

### 3. prednáška

## Výrokovologické vyplývanie

---

### Rekapitulácia

Minulý týždeň sme sa naučili:

- 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.

## 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.

Čo sú v nej: teórie, modely, logické dôsledky?

### 3.1. Teórie a ich modely

#### Príklad teórie

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 3.1.* Máme troch nových známych — Kim, Jima a Sarah. Organizujeme párty a  $P_0$ : chceme, aby na ňu prišiel niekto z nich. Od spoločných kamarátov sme sa ale dozvedeli o ich požiadavkách:

$P_1$ : Sarah nepríde na párty, ak príde Kim.

$P_2$ : Jim príde na párty, len ak príde Kim.

$P_3$ : Sarah nepríde bez Jima.

#### Výrokovologické teórie

V logike prvého rádu tvrdenia zapisujeme formulami.

*Príklad 3.2.*

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

**Definícia 3.3.** Nech  $\mathcal{L}$  je jazyk výrokovologickej časti logiky prvého rádu.

Každú množinu formúl jazyka  $\mathcal{L}$  budeme nazývať *teóriou* v jazyku  $\mathcal{L}$ .

#### Modely teórií

Neformálne je *modelom* teórie stav vybranej časti sveta.

Pre logiku prvého rádu stavy sveta vyjadrujú štruktúry.

*Príklad 3.4* (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 3.5** (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  $\mathcal{M}$ , skráteno  $\mathcal{M} \models T$ , 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  $\mathcal{M}$ , skráteno  $\mathcal{M} \not\models T$ , vtt  $T$  nie je pravdivá v  $\mathcal{M}$ .

## 3.2. Výrokovologické teórie a ohodnotenia

### Nekonečne veľa štruktúr

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

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

$$\begin{array}{lll}
 \mathcal{M}_1 = (\{k, j, s\}, i_1) & \mathcal{M}'_1 = (\{k, j, s, 0\}, i'_1) & \mathcal{M}''_1 = (\{k, j, s, 0, 1\}, i''_1) \quad \dots \\
 i_1(\text{Kim}) = k & i'_1(\text{Kim}) = k & i''_1(\text{Kim}) = k \\
 i_1(\text{Jim}) = j & i'_1(\text{Jim}) = j & i''_1(\text{Jim}) = j \\
 i_1(\text{Sarah}) = s & i'_1(\text{Sarah}) = s & i''_1(\text{Sarah}) = s \\
 i_1(\text{príde}) = \{k, j\} & i'_1(\text{príde}) = \{k, j\} & i''_1(\text{príde}) = \{k, j\}
 \end{array}$$

## Rozdiely modelov

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

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

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  $T_{\text{party}}$  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 3.6.** Nech  $\mathcal{L}$  je jazyk výrokovologickej časti logiky prvého rádu.

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

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

**Definícia 3.7.** 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 3.8.** 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 výrokovologické formuly  $A, B$  jazyka  $\mathcal{L}$  nasledovne:

- $v \models_p A$  vtt  $v(A) = t$ , ak  $A$  je predikátový atóm,
- $v \models_p \neg A$  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 skracuje *vtedy a len vtedy* a  $v \not\models_p A$  skracuje  *$A$  nie je pravdivá vo  $v$* .

## Vyhodnotenie formuly v ohodnotení

Príklad 3.9. Vyhodnoťme formulu

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

vo výrokovologickej 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 3.10.** 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 3.11.** 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  $v(A) \neq t$ .  $\square$

### Konštrukcia štruktúry zhodnej s ohodnotením

Dokážeme zostrojiť aj štruktúru z ohodnotenia, aby boli zhodné?

**Tvrdenie 3.12.** *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:*

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

*Potom  $\mathcal{M}$  je zhodná s  $v$ .*

Zhoda ohodnotenia a štruktúry je definované iba na *atómoch*.

Ako sa správajú na *zložitejších* formulách?

### Zhoda na všetkých výrokovologických formulách

**Tvrdenie 3.13.** *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  $\mathcal{M} \models A$ .

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  $v \not\models_p X$  vtt (podľa IP)  $\mathcal{M} \not\models X$  vtt  $\mathcal{M} \models \neg X$ . Ak  $X$  obsahuje  $\doteq$ ,  $\neg X$  ho obsahuje tiež, teda nie je výrokovologická a tvrdenie pre ňu platí triviálne.

2.2: IP: Nech tvrdenie platí pre formuly  $X$  a  $Y$ . Dokážme ho pre  $(X \wedge Y)$ ,  $(X \vee Y)$ ,  $(X \rightarrow Y)$ . 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  $\mathcal{M} \models (X \vee Y)$ .  $\square$

### 3.3. Vyplývanie, nezávislosť a nesplniteľnosť

#### Výrokovologické teórie

Vráťme sa naspäť k teóriám, modelom a vyplývaniu.

**Definícia 3.14.** 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 3.15.* 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 3.16* (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 3.17** (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  $v$ , skratene  $v \models_p T$ , 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  $v$ , skratene  $v \not\models_p T$ , 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 nesplniteľnosť

**Definícia 3.18** (Splniteľnosť a nesplniteľnosť). Teória je *výrokovologicky splniteľná* vtt má aspoň jeden výrokovologický model.

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

Zrejme teória nie je splniteľná vtt keď je nesplniteľná.

*Príklad 3.19.*  $T_{\text{party}}$  je evidentne splniteľná.

## 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 3.20.** 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 3.21.* Vyplýva príde(Kim) výrokovologicky z  $T_{\text{party}}$ ? Pretože vieme vymenovať všetky ohodnotenia pre  $\mathcal{L}_{\text{party}}$ , zistíme to ľahko:

	$v_i$			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	$T_{\text{party}}$	$p(K)$
	$p(K)$	$p(J)$	$p(S)$						
$v_0$	<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  $T_{\text{party}}$ .

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

## Príklad nezávislosti

*Príklad 3.22.* Vyplýva príde(Jim) výrokovologicky z  $T_{\text{party}}$ ?

	$v_i$			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	$T_{\text{party}}$	$p(J)$
	$p(K)$	$p(J)$	$p(S)$						
$v_0$	<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  $T_{\text{party}}$ .

## Výrokovologická nezávislosť

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

**Definícia 3.23.** 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 3.24* (pokračovanie príkladu 3.22). *Logický záver*: Formula  $\text{príde}(\text{Jim})$  je *nezávislá* od  $T_{\text{party}}$ .

*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. Jeho prítomnosť od požiadaviek *nezávisí*.

## Príklad vyplývania negácie

*Príklad 3.25.* Je  $\text{príde}(\text{Sarah})$  výrokovologickým dôsledkom  $T_{\text{party}}$  alebo nezávislá od  $T_{\text{party}}$ ?

	$v_i$			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	$T_{\text{party}}$	$p(S)$
	$p(K)$	$p(J)$	$p(S)$						
$v_0$	$f$	$f$	$f$	$\not\models_p$				$\not\models_p$	
$v_1$	$f$	$f$	$t$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	
$v_2$	$f$	$t$	$f$	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
$v_3$	$f$	$t$	$t$	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
$v_4$	$t$	$f$	$f$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$
$v_5$	$t$	$f$	$t$	$\models_p$	$\not\models_p$			$\not\models_p$	
$v_6$	$t$	$t$	$f$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$
$v_7$	$t$	$t$	$t$	$\models_p$	$\not\models_p$			$\not\models_p$	

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

## Vyplývanie negácie

**Tvrdenie 3.26.** 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 3.27** (pokračovanie príkladu 3.25). *Logický záver:* Z  $T_{\text{party}}$  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 3.28.** Je teória  $T'_{\text{party}} = T_{\text{party}} \cup \{(\neg \text{príde}(\text{Sarah}) \rightarrow \neg \text{príde}(\text{Kim}))\}$  splniteľná?

	$v_i$			$((p(K) \vee p(J)) \vee p(S))$	$(p(K) \rightarrow \neg p(S))$	$(p(J) \rightarrow p(K))$	$(p(S) \rightarrow p(J))$	$(\neg p(S) \rightarrow \neg p(K))$	$T'_{\text{party}}$
	$p(K)$	$p(J)$	$p(S)$						
$v_0$	$f$	$f$	$f$	$\not\models_p$					$\not\models_p$
$v_1$	$f$	$f$	$t$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$
$v_2$	$f$	$t$	$f$	$\models_p$	$\models_p$	$\not\models_p$			$\not\models_p$
$v_3$	$f$	$t$	$t$	$\models_p$	$\models_p$	$\not\models_p$			$\not\models_p$
$v_4$	$t$	$f$	$f$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
$v_5$	$t$	$f$	$t$	$\models_p$	$\not\models_p$				$\not\models_p$
$v_6$	$t$	$t$	$f$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
$v_7$	$t$	$t$	$t$	$\models_p$	$\not\models_p$				$\not\models_p$



*Logický záver:*  $T'_{\text{party}}$  je nesplnitelná, vyplýva z nej každá formula.

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

### Vyplývanie a nesplniteľnosť

Nesplniteľnosť ale nie neužitočná vlastnosť.

**Tvrdenie 3.29.** *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 3.30.** *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 atómoch teórie

**Definícia 3.31.** 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 3.32.** 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 ohodnotenia tých atómov, ktoré sa v nej vyskytujú.

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

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

## 4. prednáška

# Vlastnosti a vzťahy výrokovologických formúl

---

### Rekapitulácia

Minulý týždeň sme:

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

## 4. Vlastnosti a vzťahy výrokovologických formúl

### 4.1. Tautológie, splniteľné, falzifikovateľné a nespľniteľné 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

**Příklad 4.1.** Majme jazyk  $\mathcal{L}$  s  $\mathcal{C}_{\mathcal{L}} = \{\text{Pacient348}\}$ ,  $\mathcal{P}_{\mathcal{L}} = \{\text{očkovaný}^1, \text{chorý}^1\}$ . Je formula  $X = (\neg(\neg\text{očkovaný}(\text{Pacient348}) \vee \text{chorý}(\text{Pacient348})) \rightarrow (\text{očkovaný}(\text{Pacient348}) \wedge \neg\text{chorý}(\text{Pacient348})))$  tautológiou?

Označme  $O = \text{očkovaný}(\text{Pacient348})$  a  $C = \text{chorý}(\text{Pacient348})$ , teda  $X = (\neg(\neg O \vee C) \rightarrow (O \vee \neg C))$  a preskúmajme všetky výrokovologické ohodnotenia týchto atómov:

	$v_i$		$\neg O$	$(\neg O \vee C)$	$\neg(\neg O \vee C)$	$\neg C$	$(O \vee \neg C)$	$X$
	$O$	$C$						
$v_0$	$f$	$f$	$\models_p$	$\models_p$	$\not\models_p$	$\models_p$	$\models_p$	$\models_p$
$v_1$	$t$	$f$	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$
$v_2$	$f$	$t$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$
$v_3$	$t$	$t$	$\not\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$

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  $\models_p X$ ) vtt  $X$  je pravdivá v každom výrokovologickom ohodnotení  $v$  pre  $\mathcal{L}$  (teda pre každé výrokovologické ohodnotenie  $v$  pre  $\mathcal{L}$  platí  $v \models_p X$ ).

Definícia vyžaduje preveriť všetky možné ohodnotenia pre  $\mathcal{L}$ , teda ohod-

	$v_i$				$X$
	$A_1$	$A_2$	$\dots$	$X$	
notenia všetkých predikátových atómov jazyka $\mathcal{L}$ . Ale...	$v_0$	$f$	$f$	$\dots$	$\models_p$
	$v_1$	$f$	$f$	$\dots$	$\models_p$
			$\dots$		
	$v_k$	$t$	$f$	$\dots$	$\models_p$
			$\dots$		

## Postačujúca podmienka pre tautológiu

Na minulej prednáške sme spomenuli, že platí:

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

Stačí teda preverovať ohodnotenia atómov vyskytujúcich sa vo formule:

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

### Dôkaz zhody ohodnotení na formule

O pravdivosti týchto tvrdení sa vieme ľahko presvedčiť:

*Dôkaz tvrdenia 4.3.* Tvrdenie dokážeme indukciou na konštrukciu formuly:

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

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

2.1 Indukčný predpoklad (IP): Predpokladajme, že tvrdenie platí pre formulu  $X$ . Dokážme ho pre  $\neg X$ . Zoberme ľubovoľné ohodnotenia  $v_1$  a  $v_2$ , ktoré sa zhodujú na  $\text{atoms}(\neg X)$ . 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. □

### Splniteľnosť

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

Nazývame ich *splniteľné*. \_\_\_\_\_

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

**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  $v \models_p X$ ).

### 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*. \_\_\_\_\_

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

**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  $v \not\models_p X$ ).

### Nesplniteľnosť

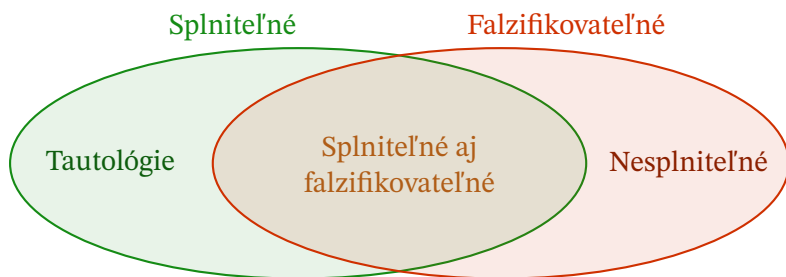
Nakoniec, mnohé formuly sú *nutne* nepravdivé, teda sú nepravdivé vo *všetkých* ohodnoteniach.

Nazývame ich *nesplniteľné*.

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

**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  $v \not\models_p X$ ).

„Geografia“ formúl podľa pravdivosti vo všetkých ohodnoteniach



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

## 4.2. Ekvivalencia

### Logická ekvivalencia

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

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

*Príklad 4.8.* V jazyku  $\mathcal{L}$  z príkladu 4.1 označme  $O$  = očkovaný(Pacient348) a  $C$  = chorý(Pacient348). Sú formuly  $X = \neg(O \rightarrow \neg C)$  a  $Y = (O \wedge C)$  výrokovologicke ekvivalentné?

Preskúmame všetky výrokovologické ohodnotenia atómov  $O$  a  $C$ :


$v_i$	$v_i$				$X$	$Y$
	$O$	$C$	$\neg C$	$(O \rightarrow \neg C)$	$\neg(O \rightarrow \neg C)$	$(C \wedge O)$
$v_0$	$f$	$f$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
$v_1$	$t$	$f$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
$v_2$	$f$	$t$	$\not\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
$v_3$	$t$	$t$	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$

$X$  je pravdivá v *práve tých* ohodnoteniach pre  $\mathcal{L}$ , v ktorých je pravdivá  $Y$ , preto  $X$  a  $Y$  sú výrokovologicke 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 *výrokovologicke ekvivalentné*, skratene  $X \Leftrightarrow_p Y$  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 práve uvedenej definície. Keď napíšeme  $X \Leftrightarrow_p Y$ , tvrdíme tým, že  $X$  a  $Y$  sú výrokovologicke 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.

## Známe ekvivalencie

**Veta 4.10.** *Nech  $\mathcal{L}$  je jazyk výrokovologickej časti logiky prvého rádu. Nech  $A$ ,  $B$  a  $C$  sú ľubovoľné výrokovologické formuly,  $\top$  je ľubovoľná tautológia a  $\perp$  je ľubovoľná nespĺniteľná formula 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 $\wedge$

## Známe ekvivalencie

**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

### Všeobecné dôkazy známych ekvivalencií

Pre *konkrétne* dvojice formúl v konkrétnom jazyku sa ekvivalencia dá dokázať rozborom všetkých ohodnotení ako v príklade 4.8.

Ak chceme dokázať napríklad ekvivalenciu  $(A \rightarrow B)$  a  $(\neg A \vee B)$  skutočne pre *ľubovoľné* formuly  $A$  a  $B$ , musíme postupovať *opatrnejšie*.

*Nemôžeme* predpokladať, že  $A$  a  $B$  sú atomické a ohodnotenia im *priamo* priradujú pravdivostné hodnoty  $f$  a  $t$ .

*Môžeme* však zobrať *ľubovoľné* ohodnotenie  $v$  a uvažovať o všetkých možnostiach, akými môžu byť  $A$  a  $B$  pravdivé alebo nepravdivé v tomto ohodnotení a ukázať, že v každom prípade bude  $(A \rightarrow B)$  pravdivá vo  $v$  vtt bude  $(\neg A \vee B)$  pravdivá vo  $v$ .

### Príklad dôkazu známej ekvivalencie

*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 *zo-všeobecniť* na všetky ohodnotenia pre  $\mathcal{L}$  a podľa definície 4.9 sú  $(A \rightarrow B)$  a  $(\neg A \vee B)$  výrokovologicky ekvivalentné.  $\square$

### 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, či dokonca vyplývaní.

## 4.3. Vzťah tautológií, vyplývania a ekvivalencie

### Tautológie a vyplývanie

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

Kedy je formula  $((A_1 \wedge A_2) \rightarrow B)$  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  $\{A_1, A_2\}$  výrokovo-logicky vyplýva  $B$ .

## Vzťahy výrokovo-logického vyplývania a tautológií

**Tvrdenie 4.11.** *Nech  $\mathcal{L}$  je jazyk výrokovo-logickej časti logiky prvého rádu. Nech  $S$  a  $T$  sú výrokovo-logické teórie a  $A$  je výrokovo-logická formula v  $\mathcal{L}$ , pričom  $S \subseteq T$ . Ak  $S \models_p A$ , tak  $T \models_p A$ .*

**Tvrdenie 4.12.** *Nech  $\mathcal{L}$  je jazyk výrokovo-logickej časti logiky prvého rádu. Nech  $T$  je výrokovo-logická teória, nech  $A, B, A_1, A_2, \dots, A_n$  sú výrokovo-logické formuly v  $\mathcal{L}$ . Potom:*

- a)  $A$  vyplýva z prázdnej teórie  $\emptyset$  vtt  $A$  je tautológia. (Skrátene:  $\emptyset \models_p A$  vtt  $\models_p A$ .)
- b)  $T \cup \{A\} \models_p B$  vtt  $T \models_p (A \rightarrow B)$ .
- c)  $\models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$  vtt  $\{A_1, A_2, \dots, A_n\} \models_p B$ .

## Dôkaz vzťahu vyplývania a tautológií ( $\Rightarrow$ )

*Dôkaz tvrdenia 4.12c).* Dôkaz tohto tvrdenia sme už naznačili, ale spravme ho podrobnejšie: Nech  $A_1, A_2, \dots, A_n, B$  sú výrokovo-logické formuly v ľubovoľnom jazyku  $\mathcal{L}$ .

( $\Rightarrow$ ) Predpokladajme, že  $X = (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$  je tautológia a dokážme, že potom z  $\{A_1, A_2, \dots, A_n\}$  vyplýva  $B$ .

Zoberme ľubovoľné výrokovo-logické ohodnotenie  $v$  pre  $\mathcal{L}$ . Musíme preň dokázať, že ak  $v \models_p \{A_1, A_2, \dots, A_n\}$ , tak  $v \models_p B$ . Predpokladajme teda, že  $v \models_p \{A_1, A_2, \dots, A_n\}$ . Potom je vo  $v$  pravdivá každá z formúl  $A_1$  až  $A_n$ , a teda aj o konjunkciách  $(A_1 \wedge A_2)$ ,  $((A_1 \wedge A_2) \wedge A_3)$ ,  $\dots$ ,  $((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n)$  postupne zistíme, že sú pravdivé vo  $v$ . Pretože  $X$  je tautológia, je pravdivá aj v ohodnotení  $v$ , a teda podľa definície pravdivosti a predchádzajúceho zistenia, musí byť pravdivý jej konzekvent  $B$ .

Zistili sme teda, že pre  $v$  platí, že ak  $v \models_p \{A_1, A_2, \dots, A_n\}$ , tak  $v \models_p B$ . Pretože  $v$  bolo ľubovoľné, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície vyplývania potom  $\{A_1, A_2, \dots, A_n\} \models_p B$ .  $\square$

## Dôkaz vzťahu vyplývania a tautológií ( $\Leftarrow$ )

*Dôkaz tvrdenia 4.12c) (pokračovanie).* ( $\Leftarrow$ ) Predpokladajme, že  $(*)$  z  $\{A_1, A_2, \dots, A_n\}$  vyplýva  $B$  a dokážme, že  $X = (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$  je tautológia.

Zoberme ľubovoľné výrokovologické ohodnotenie  $v$  pre  $\mathcal{L}$ . Musíme preň dokázať, že  $v \models_p X$ . Môžeme to napríklad urobiť rozborom týchto prípadov:

- Ak  $v \models_p A_i$  pre všetky  $i = 1, \dots, n$ , tak  $v \models_p \{A_1, A_2, \dots, A_n\}$ . Podľa predpokladu  $(*)$  a definície vyplývania potom musí  $v \models_p B$ , a teda platí, že  $v \models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$  alebo  $v \models_p B$ , a teda  $v \models_p X$ .
- Ak  $v \not\models_p A_i$  pre niektoré  $i \in \{1, \dots, n\}$ , tak  $v \not\models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_i) \wedge A_i)$  a postupným pridávaním ďalších konjunktov dostaneme, že  $v \not\models_p (((\dots (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_i) \dots) \wedge A_n) \rightarrow B)$ . Aj v tomto prípade teda platí, že  $v \not\models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$  alebo  $v \models_p B$ , a teda  $v \models_p X$ .

V oboch prípadoch, z ktorých jeden musí vždy nastať, sme dospeli k rovnakému záveru:  $v \models_p X$ . Pretože  $v$  bolo ľubovoľné, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície tautológie je  $X$  tautológiou.  $\square$

## Tautológie a ekvivalencia

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

Vtedy, keď je pravdivá v každom ohodnotení, teda keď v každom ohodnotení  $v$  máme  $v \models_p (X \rightarrow Y)$  a  $v \models_p (Y \rightarrow X)$ , teda keď v každom ohodnotení  $v$  máme buď  $v \not\models_p X$  alebo  $v \models_p Y$  a zároveň buď  $v \not\models_p Y$  alebo  $v \models_p X$ , teda keď v každom ohodnotení  $v$  platí, že ak  $v \models_p X$ , tak  $v \models_p Y$ , a ak  $v \models_p X$ , tak  $v \models_p Y$ , teda keď v každom ohodnotení  $v$  máme  $v \models_p X$  vtt  $v \models_p Y$ , teda keď  $X$  výrokovologicky ekvivalentná s  $Y$ .

## Vzťah výrokovologickej ekvivalencie a tautológií

**Tvrdenie 4.13.** *Nech  $\mathcal{L}$  je jazyk výrokovologickej časti logiky prvého rádu. Nech  $X$  a  $Y$  sú výrokovologické formuly v  $\mathcal{L}$ . Potom  $(X \leftrightarrow Y)$  je tautológia vtt  $X$  a  $Y$  sú výrokovologicky ekvivalentné. (Skrátene:  $\models_p (X \leftrightarrow Y)$  vtt  $X \Leftrightarrow_p Y$ .)*

Dôkaz je podobný dôkazu tvrdenia 4.12.

## 4.4. Ekvivalentné úpravy a CNF

### Reťazenie ekvivalentných úprav

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

$$\neg(O \rightarrow \neg C) \Leftrightarrow_p \neg(\neg O \vee \neg C) \Leftrightarrow_p (\neg\neg O \wedge \neg\neg C) \Leftrightarrow_p (O \vee C)$$

a nakoniec ste prehlásili, že prvá  $\neg(O \rightarrow \neg C)$  a posledná formula  $(O \vee C)$  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 4.14.** *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.  $\square$

## 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  $X \Leftrightarrow_p Z$ .*

## Substitúcia pri ekvivalentných úpravách

V reťazci ekvivalentných úprav

$$\neg(O \rightarrow \neg C) \Leftrightarrow_p \neg(\neg O \vee \neg C) \Leftrightarrow_p (\neg\neg O \wedge \neg\neg C) \Leftrightarrow_p (O \vee C)$$

v prvom a poslednom kroku nezodpovedá celá formula niektorej zo známych ekvivalencií z vety 4.10.

Podľa známej ekvivalencie sme nahradzali 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 induktívne definovanú (rekurzívnu) operáciu:

### Substitúcia rekurzívne

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

$$X[A|B] = B, \quad \text{ak } A = X$$

$$X[A|B] = X, \quad \text{ak } X \text{ je atóm a } A \neq X$$

$$(\neg X)[A|B] = \neg(X[A|B]), \quad \text{ak } A \neq \neg X$$

$$(X \ b \ Y)[A|B] = ((X[A|B]) \ b \ (Y[A|B])), \quad \text{ak } A \neq (X \ b \ Y).$$

### Korektnosť substitúcie ekvivalentnej formuly

Substitúciou ekvivalentnej podformuly, napríklad

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

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 ekvivalentné formuly jazyka  $\mathcal{L}$ . Potom formuly  $X$  a  $X[A|B]$  sú tiež ekvivalentné.*

Toto tvrdenie môžeme dokázať indukciou na konštrukciu formuly.

### Ekvivalentné úpravy a vstup pre SAT solver

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

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

## Konjunkcia a disjunkcia postupnosti formúl

**Definícia 4.18.** 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:**  $P, \neg O, \square, (\neg P \vee O \vee \neg C)$

**CNF:**  $P, \neg O, \top, (P \vee \neg O) (P \wedge \neg O \wedge C), \square, ((P \vee O) \wedge \square), ((\neg P \vee O) \wedge (O \vee C))$   
ak  $P$  = pacient(Edo),  $O$  = očkovaný(Edo),  $C$  = chorý(Edo).

## Existencia ekvivalentnej formuly v CNF

**Veta 4.21.** *Ku každej 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 **praktické cvičenie**.

## Konverzia formuly do ekvivalentnej v CNF

Algoritmus konverzie do CNF má dve fázy:

1. Upravíme formulu na *negačný normálny tvar* — nevyskytuje sa v ňom implikácia a negované sú iba atómy:
  - Nahradíme implikácie disjunkciami:  $(A \rightarrow B) \Leftrightarrow_p (\neg A \vee B)$
  - Presunieme  $\neg$  dovnútra pomocou de Morganových zákonov a zákona dvojitej negácie.
2. Odstránime konjunkcie vnorené v disjunkciách „roznásobením“ podľa distributívnosti a komutatívnosti:

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

## 5. prednáška

# Dôkazy a výrokovologické tablá

---

### Rekapitulácia

Minulý týždeň sme sa zaoberali:

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

## 5. Dôkazy a výrokovologické tablá

### Dôkazy a formalizácia

Minulý týždeň sme v rámci teoretických úloh dokazovali tvrdenia o vyplývaní a tautológiách:

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

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

- matematická „dátová štruktúra“: postupnosti symbolov s indukčnými pravidlami konštrukcie;

- javovská dátová štruktúra: stromy objektov podtried triedy Formula.

*Dôkazy* v slovenčine začneme *formalizovať* tento týždeň

## Čo sú dôkazy a prečo sa dokazuje

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

*Načo* sú vlastne dobré *dôkazy*?

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

Už 16 možností v 3. teoretickej úlohe bolo prácne rozobrať.

Ak je možností nekonečne veľa, rozbor všetkých možností ani nie je možný.

- Odvodzovaním podľa pravidiel dôkazov môžeme skúmať, aké dôsledky má naša teória aj bez konkrétneho cieľa.

## Prečo formalizovať dôkazy

*Načo* je dobré *formalizovať* dôkazy?

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

## 5.1. Druhy dôkazov

### Druhy dôkazov

V matematike sa na to používa viac typov dôkazov:

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

ktoré sa často kombinujú.

### Priamy dôkaz a analýza prípadov

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

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

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

### Príklad priameho dôkazu s analýzou prípadov

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

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

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

Ak nepríde Anka,  $X$  je pravdivé.

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

## Dôkaz analýzou prípadov

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

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

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

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

## Príklad priameho dôkazu s analýzou prípadov

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

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

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

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

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

## Výhody dôkazu sporom

Dôkaz sporom je veľmi konkrétna ukážka kritického, vedeckého myslenia:

1. Pochybujeme o pravdivosti tvrdenia.
2. Vyvrátením tejto pochybnosti sa presvedčíme o pravdivosti.

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

- dostaneme viac predpokladov;
- máme jednoduchý cieľ: nájsť spor.

## Odvodzovanie jednoduchých dôsledkov

Kroky dôkazu by mali odvodzovať *jednoduché dôsledky*.

Tie potom používame na odvodenie ďalších dôsledkov.

Aký dôsledok je jednoduchý?

Závisí od čitateľa dôkazu — musí byť schopný ho overiť.

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

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

## 5.2. Výrokovologické tablá

### Jednoduché dôsledky podľa definície pravdivosti formúl

Pozrime sa znova na dôkaz príkladu sporom:

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

### Príklad dôkazu sporom s formulami

*Príklad 5.3* (Párty po karanténe · formalizovaný dôkaz sporom). Dokážme,

$A_1 = (p(A) \rightarrow (p(B) \wedge p(C)))$	Anka príde, iba ak príde Betka
$A_2 = ((p(B) \vee p(D)) \rightarrow p(E))$	Ak príde Betka alebo Dávid, príde Erika
$A_3 = (p(F) \rightarrow \neg p(E))$	Evka nepríde, ak príde Fero.
že $z T = \{A_1, A_2, A_3\}$ , kde	
vyplýva	
$X = (p(A) \rightarrow \neg p(F))$	Ak príde Anka, tak nepríde Fero.



## Príklad dôkazu sporom s formulami

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

čo je v spore

(10)  $v \not\models_p p(E)$  z (9). Zároveň

so (7),

(11)  $v \not\models_p p(A)$ , alebo (12)  $v \models_p (p(B) \wedge p(C))$  podľa (1).

čo je v spore

(13)  $v \models_p p(B)$  z (12). Potom podľa

s (5),

(14)  $v \not\models_p (p(B) \vee p(D))$ , alebo (15)

(16)  $v \not\models_p (p(B))$  zo (14),

spor s (13);

## Tablový kalkul

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

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

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

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

## Označené formuly a ich sémantika

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

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

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

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

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

### Dôkaz sporom s označenými formulami

*Príklad 5.5* (Párty po karanténe · dôkaz s označenými formulami). Predpokladajme, pre nejakom ohodnotení  $v$  sú pravdivé označené formuly (1)  $\mathbf{T}(p(A) \rightarrow (p(B) \wedge p(C)))$ , (2)  $\mathbf{T}((p(B) \vee p(D)) \rightarrow p(E))$ , (3)  $\mathbf{T}(p(F) \rightarrow \neg p(E))$ , ale (4)  $\mathbf{F}(p(A) \rightarrow \neg p(F))$ . Podľa definície pravdivosti, sú vo  $v$  pravdivé: (5)  $\mathbf{T} p(A)$  zo (4) a súčasne (6)  $\mathbf{F} \neg p(F)$  zo (4), teda (7)  $\mathbf{T} p(F)$  z (6). Ďalej (8)  $\mathbf{F} p(F)$ , alebo (9) čo je v spore (10) so (7), (11) č s

### Kroky odvodenia

Všimnime si teraz kroky, ktoré sme v dôkaze robili:

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

### Priame odvodenie pravdivosti priamych podformúl

Z definície pravdivosti formúl ľahko dostaneme:

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

$Ak \ v \models_p \neg X, \text{ tak } v \not\models_p X.$	$Ak \ v \models_p \mathbf{T} \neg X, \text{ tak } v \models_p \mathbf{F} X.$
$Ak \ v \not\models_p \neg X, \text{ tak } v \models_p X.$	$Ak \ v \models_p \mathbf{F} \neg X, \text{ tak } v \models_p \mathbf{T} X.$
$Ak \ v \models_p (X \wedge Y), \text{ tak } v \models_p X.$	$Ak \ v \models_p \mathbf{T}(X \wedge Y), \text{ tak } v \models_p \mathbf{T} X.$
$Ak \ v \models_p (X \wedge Y), \text{ tak } v \models_p Y.$	$Ak \ v \models_p \mathbf{T}(X \wedge Y), \text{ tak } v \models_p \mathbf{T} Y.$
$Ak \ v \not\models_p (X \wedge Y), \text{ tak } v \not\models_p X.$	$Ak \ v \models_p \mathbf{F}(X \wedge Y), \text{ tak } v \models_p \mathbf{F} X.$
$Ak \ v \not\models_p (X \wedge Y), \text{ tak } v \not\models_p Y.$	$Ak \ v \models_p \mathbf{F}(X \wedge Y), \text{ tak } v \models_p \mathbf{F} Y.$
$Ak \ v \models_p (X \vee Y), \text{ tak } v \models_p X.$	$Ak \ v \models_p \mathbf{T}(X \vee Y), \text{ tak } v \models_p \mathbf{T} X.$
$Ak \ v \models_p (X \vee Y), \text{ tak } v \models_p Y.$	$Ak \ v \models_p \mathbf{T}(X \vee Y), \text{ tak } v \models_p \mathbf{T} Y.$
$Ak \ v \not\models_p (X \vee Y), \text{ tak } v \not\models_p X.$	$Ak \ v \models_p \mathbf{F}(X \vee Y), \text{ tak } v \models_p \mathbf{F} X.$
$Ak \ v \not\models_p (X \vee Y), \text{ tak } v \not\models_p Y.$	$Ak \ v \models_p \mathbf{F}(X \vee Y), \text{ tak } v \models_p \mathbf{F} Y.$
$Ak \ v \models_p (X \rightarrow Y), \text{ tak } v \models_p X.$	$Ak \ v \models_p \mathbf{F}(X \rightarrow Y), \text{ tak } v \models_p \mathbf{T} X.$
$Ak \ v \models_p (X \rightarrow Y), \text{ tak } v \models_p Y.$	$Ak \ v \models_p \mathbf{F}(X \rightarrow Y), \text{ tak } v \models_p \mathbf{F} Y.$
$Ak \ v \not\models_p (X \rightarrow Y), \text{ tak } v \not\models_p X.$	$Ak \ v \models_p \mathbf{T}(X \rightarrow Y), \text{ tak } v \models_p \mathbf{T} X.$
$Ak \ v \not\models_p (X \rightarrow Y), \text{ tak } v \not\models_p Y.$	$Ak \ v \models_p \mathbf{T}(X \rightarrow Y), \text{ tak } v \models_p \mathbf{T} Y.$

### Zjednodušujúce tablové pravidlá

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

$\frac{\mathbf{T} \neg X}{\mathbf{F} X}$	$\frac{\mathbf{F} \neg X}{\mathbf{T} X}$	$\frac{\mathbf{T}(X \wedge Y)}{\mathbf{T} X}$	$\frac{\mathbf{F}(X \vee Y)}{\mathbf{F} X}$	$\frac{\mathbf{F}(X \rightarrow Y)}{\mathbf{T} X}$
		$\frac{\mathbf{T}(X \wedge Y)}{\mathbf{T} Y}$	$\frac{\mathbf{F}(X \vee Y)}{\mathbf{F} Y}$	$\frac{\mathbf{F}(X \rightarrow Y)}{\mathbf{F} Y}$

Na tieto pravidlá sa dá pozeráť ako na *špeciálne prípady jedného pravidla*, ktorému sa hovorí  $\alpha$ , zjednodušenie alebo sploštenie (angl. *flatten*), pre rôzne spojky.

### Jednotný zápis označených formúl typu $\alpha$

**Definícia 5.7** (Jednotný zápis označených formúl typu  $\alpha$ ).

Označená formula  $A^+$  je *typu*  $\alpha$  vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly  $X$  a  $Y$ . Takéto formuly budeme označovať písmenom  $\alpha$ ;  $\alpha_1$  bude označovať príslušnú označenú formulu zo stredného stĺpca,  $\alpha_2$  príslušnú formulu z pravého stĺpca.

$\alpha$	$\alpha_1$	$\alpha_2$
$\mathbf{T}(X \wedge Y)$	$\mathbf{T} X$	$\mathbf{T} Y$
$\mathbf{F}(X \vee Y)$	$\mathbf{F} X$	$\mathbf{F} Y$
$\mathbf{F}(X \rightarrow Y)$	$\mathbf{T} X$	$\mathbf{F} Y$
$\mathbf{T} \neg X$	$\mathbf{F} X$	$\mathbf{F} X$
$\mathbf{F} \neg X$	$\mathbf{T} X$	$\mathbf{T} X$

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

## Analýza prípadov pravdivosti priamych podformúl

Z definície pravdivosti formúl ľahko dostaneme:

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

- *Ak  $v \models_p (X \wedge Y)$ , tak  $v \models_p X$  alebo  $v \models_p Y$ . Ak  $v \models_p \mathbf{F}(X \wedge Y)$ , tak  $v \models_p \mathbf{F}X$  alebo  $v \models_p \mathbf{F}Y$ .*
- *Ak  $v \models_p (X \vee Y)$ , tak  $v \models_p X$  alebo  $v \models_p Y$ . Ak  $v \models_p \mathbf{T}(X \vee Y)$ , tak  $v \models_p \mathbf{T}X$  alebo  $v \models_p \mathbf{T}Y$ .*
- *Ak  $v \models_p (X \rightarrow Y)$ , tak  $v \models_p X$  alebo  $v \models_p Y$ . Ak  $v \models_p \mathbf{T}(X \rightarrow Y)$ , tak  $v \models_p \mathbf{F}X$  alebo  $v \models_p \mathbf{T}Y$ .*

## Rozvetvujúce tablové pravidlá

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

$$\frac{\mathbf{F}(X \wedge Y)}{\mathbf{F}X \mid \mathbf{F}Y} \qquad \frac{\mathbf{T}(X \vee Y)}{\mathbf{T}X \mid \mathbf{T}Y} \qquad \frac{\mathbf{T}(X \rightarrow Y)}{\mathbf{F}X \mid \mathbf{T}Y}$$

Aj na tieto pravidlá sa dá pozeráť ako na špeciálne prípady jedného pravidla, ktorému sa hovorí  $\beta$  alebo vetvenie (angl. *split*), pre rôzne spojky.

## Jednotný zápis označených formúl typu $\beta$

**Definícia 5.10** (Jednotný zápis označených formúl typu  $\beta$ ).

Označená formula  $B^+$  je typu  $\beta$  vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly  $X$  a  $Y$ . Takéto formuly budeme označovať písmenom  $\beta$ ;  $\beta_1$  bude označovať príslušnú označenú formulu zo stredného stĺpca,  $\beta_2$  príslušnú formulu z pravého stĺpca.

$\beta$	$\beta_1$	$\beta_2$
$\mathbf{F}(X \wedge Y)$	$\mathbf{F}X$	$\mathbf{F}Y$
$\mathbf{T}(X \vee Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
$\mathbf{T}(X \rightarrow Y)$	$\mathbf{F}X$	$\mathbf{T}Y$

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

## Označovanie označených formúl a ich množín

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

$$S^+ = \{ \begin{array}{l} \mathbf{T}(p(A) \rightarrow (p(B) \wedge p(C))), \\ \mathbf{T}((p(B) \vee p(D)) \rightarrow p(E)), \\ \mathbf{T}(p(F) \rightarrow \neg p(E)), \\ \mathbf{F}(p(A) \rightarrow \neg p(F)) \end{array} \}$$

vedie k sporu, teda že  $S^+$  je nespĺniteľná.

*Dohoda 5.12.* Pre označené formuly budeme používať veľké písmená zo začiatku a konca abecedy s horným indexom + a prípadne s dolnými indexmi, napr.  $A^+$ ,  $X_7^+$ .

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

## Príklad tabla

*Príklad 5.12* (Párty po karanténe · tablo).

1.	$\mathbf{T}(p(A) \rightarrow (p(B) \wedge p(C)))$	$S^+$																
2.	$\mathbf{T}((p(B) \vee p(D)) \rightarrow p(E))$	$S^+$																
3.	$\mathbf{T}(p(F) \rightarrow \neg p(E))$	$S^+$																
4.	$\mathbf{F}(p(A) \rightarrow \neg p(F))$	$S^+$																
5.	$\mathbf{T} p(A)$	$\alpha 4$																
6.	$\mathbf{F} \neg p(F)$	$\alpha 4$																
7.	$\mathbf{T} p(F)$	$\alpha 6$																
8.	$\mathbf{F} p(F) \quad \beta 3$ *7, 8	<table><tr><td>9.</td><td><math>\mathbf{T} \neg p(E) \quad \beta 3</math></td></tr><tr><td>10.</td><td><math>\mathbf{F} p(E) \quad \alpha 9</math></td></tr><tr><td>11.</td><td><math>\mathbf{F} p(A) \quad \alpha 1</math> *5, 11</td></tr><tr><td>12.</td><td><math>\mathbf{T}(p(B) \wedge p(C)) \quad \beta 1</math></td></tr><tr><td>13.</td><td><math>\mathbf{T} p(B) \quad \alpha 12</math></td></tr><tr><td>14.</td><td><math>\mathbf{F}(p(B) \vee p(D)) \quad \beta 2</math></td></tr><tr><td>15.</td><td><math>\mathbf{T} p(E) \quad \beta 2</math> *9, 15</td></tr><tr><td>16.</td><td><math>\mathbf{F} p(B) \quad \alpha 14</math> *13, 16</td></tr></table>	9.	$\mathbf{T} \neg p(E) \quad \beta 3$	10.	$\mathbf{F} p(E) \quad \alpha 9$	11.	$\mathbf{F} p(A) \quad \alpha 1$ *5, 11	12.	$\mathbf{T}(p(B) \wedge p(C)) \quad \beta 1$	13.	$\mathbf{T} p(B) \quad \alpha 12$	14.	$\mathbf{F}(p(B) \vee p(D)) \quad \beta 2$	15.	$\mathbf{T} p(E) \quad \beta 2$ *9, 15	16.	$\mathbf{F} p(B) \quad \alpha 14$ *13, 16
9.	$\mathbf{T} \neg p(E) \quad \beta 3$																	
10.	$\mathbf{F} p(E) \quad \alpha 9$																	
11.	$\mathbf{F} p(A) \quad \alpha 1$ *5, 11																	
12.	$\mathbf{T}(p(B) \wedge p(C)) \quad \beta 1$																	
13.	$\mathbf{T} p(B) \quad \alpha 12$																	
14.	$\mathbf{F}(p(B) \vee p(D)) \quad \beta 2$																	
15.	$\mathbf{T} p(E) \quad \beta 2$ *9, 15																	
16.	$\mathbf{F} p(B) \quad \alpha 14$ *13, 16																	

## Tablo — dôkaz v tablovom kalkule

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



## Tablá a tablové pravidlá

### Pôvodné tablo Možné priame rozšírenie Pravidlá a označené formuly v nich

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

$\alpha$	$\alpha_1$	$\alpha_2$
$\mathbf{T}(X \wedge Y)$	$\mathbf{TX}$	$\mathbf{TY}$
$\mathbf{F}(X \vee Y)$	$\mathbf{FX}$	$\mathbf{FY}$
$\mathbf{F}(X \rightarrow Y)$	$\mathbf{TX}$	$\mathbf{FY}$
$\mathbf{T}\neg X$	$\mathbf{FX}$	$\mathbf{FX}$
$\mathbf{F}\neg X$	$\mathbf{TX}$	$\mathbf{TX}$

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

$\beta$	$\beta_1$	$\beta_2$
$\mathbf{F}(X \wedge Y)$	$\mathbf{FX}$	$\mathbf{FY}$
$\mathbf{T}(X \vee Y)$	$\mathbf{TX}$	$\mathbf{TY}$
$\mathbf{T}(X \rightarrow Y)$	$\mathbf{FX}$	$\mathbf{TY}$

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

## Uzavretosť a otvorenosť vetvy a tabla

**Definícia 5.14.** *Vetvou* tabla  $\mathcal{T}$  je každá cesta od koreňa  $\mathcal{T}$  k niektorému listu  $\mathcal{T}$ .

Označená formula  $X^+$  sa *vyskytuje na vetve*  $\pi$  v  $\mathcal{T}$  vtt  $X^+$  sa nachádza v niektorom vrchole na  $\pi$ . Skrátene to budeme zapisovať  $X^+ \in \text{formulas}(\pi)$ .

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

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

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

## Korektnosť tablového kalkulu

**Veta 5.16** (Korektnosť tablového kalkulu). *Nech  $S^+$  je množina označených formúl a  $\mathcal{T}$  je uzavreté tablo pre  $S^+$ . Potom je množina  $S^+$  nesplniteľná.*

**Dôsledok 5.17.** *Nech  $S$  je výrokovologická teória a  $X$  je výrokovologická formula. Ak existuje uzavreté tablo pre  $\{\mathbf{T} A \mid A \in S\} \cup \{\mathbf{F} X\}$  (skrátene  $S \vdash X$ ), tak z  $S$  výrokovologicky vyplýva  $X$  ( $S \models_{\mathbf{p}} X$ ).*

**Dôsledok 5.18.** *Nech  $X$  je výrokovologická formula. Ak existuje uzavreté tablo pre  $\{\mathbf{F} X\}$  (skrátene  $\vdash X$ ), tak  $X$  je tautológia ( $\models_{\mathbf{p}} X$ ).*

### **Spomeňte si 5.1**

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

## **Literatúra**

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

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