Předmět: IV028 Základní pojmy obecné logiky

Neručím za korektnost zápisu. Pokud najdete nějaké nepřesnosti, opravte dokument a dejte mi vědět, ať se taky neučím blbosti :D Jirka Mauritz.

1.Přednáška (NEBUDE U ZKOUŠKY)

- Historie
  - **Aristoteles** a jeho čtverec, z čehož vyplýva kategorický sylogismus – usuzování
  - **Stoici** – Když první tak druhé. Potom: Není druhé → není první (obměněná implikace)
  - **Francis Bacon** (středověk) – z premis vyplývá závěr, ale ze závěru nelze vyvozovat něco o premisách (klasická implikace)
  - **Leibnitz** – uvažoval o obecných pojmech, všeobecně uznávané syntaxe logiky, od Aristotela + nněco navíc; př.: pravidlo indentity
  - **Bolzano** – definoval pojmy, kombinoval logiku s psychologií; rozlišení abstraktního a reálného
  - **Tarsti** – definoval pravdu a vyplývání
  - **Gottlob Frege -**
    - na přelomu století 19. a 20. 2 proudy matematiky – **logicismus** (Frege, B.Russell) a **intuicismus(přirozená tvorba objektů je matematika, logika nic neřeší)**
    - 3+2 není to samé jako odmocnina z 25, přitom se rovná
  - **David Hilbert** - formalismus → formalizace matematiky → pouze logika
  - **Bernard Russell** – teorie tipů, Logikomiks
  - **Gödel**
  - **Gent**
  - **Gentzen**

2. Přednáška (logika pravdivostních funkcí)

- 2 operace – syntaktická – za větu dosazujeme jinou větu
    - sémantická – přiřazujeme hodnotu
- 0 a 1 jsou abstraktní hodnoty – my si určíme 1 – pravda 0 – nepravda
- existjí určité logické operace, ale např. Spojku protože nemůžeme označit za operaci – A protože B (za A mohu dosadit co chci a neurčuje mi to hodnotu
- pro 2 vstupní logické proměnné, můžeme vytvořit maximálně 2^4 =
- 16 operací – kombinace všech hodnot
    - identita – vše 1, kontradikce – vše 0
    - klasická disjunkce (nezáleží na pořadí)
    - klasická konjunkce (nezáleží na pořadí)
    - klasická implikace (záleží na pořadí) značíme podkovou (je podmnožinou, ale opačně) nebo šipkou (A implikuje B, jen když A->B je pravdivé !)
    - klasická ekvivalence – značíme třemi čarami,
      v angličtině značka iff (if and only if)
    - vylučovací nebo (xor) negace ekvivalence
    - negace konjunkce – značíme lomítkem – A/B – stačí k tomu, abychom nadefinovali ostatní logické operace:
        - negace A/A
        - konjunkce (A/B) / (A/B)
        - atd.
        - Tím vytváří použitelný axiomatický systém, ale je špatně čitelný
- A je tautologie (T) = je výrokově logicky pravdivá (je jich spočetně nekonečno)
    - př.: zákon vyloučení třetího A | !A ; existuje u některých výroků 3. možnost, př.: největší prvočíslo je liché (neexistuje největší prvočíslo → neurčitelné)
    - A->A
    - A <=> !!A
- A & !A – kontradikce (K) – opak tautologie
- T & A <=> A
- K % A <=> K
- T | A <=> T
- K | A <=> A
- pokud (A_1 A_2 ….A_n) ⊨ B (vyplývá) ekvivalentní k implikaci
- distributivita platí pro konjukci i disjunkci (A | (B&C)) <=> ((A&B) | (A&C))

- **Jazyk výrokové logiky**
  - potřebujeme abecedu, př.: p,q,r,p_1
  - synakse - ! (negace), → (implikace), () (závorky)
    - 1. určíme podmnožinu, kterou definujeme (množina proměnných) (**duf = dobře utvořená formule**)
    - 2. jestliže A,B jsou duf, pak !A, A->B jsou duf
    - 3. nic jiného není duf
  - každá konečná množina je rozhodnutelná
  - tvoříme množiny dobře utvořených formulí → musí být rozhodnutelné
- **Polská notace**
  - nepotřebujeme závorky – používáme N (negace), A(disjunkce), K(konjunkce), C(implikace)
  - používáme proměnné X,Y,Z,X_1 … (v příkladu špatně)
  - př.: (p → !(q & r)) → (q (r & !p)) se zapíše polsky jako C C p N K q r A q K r N p
  - to první C je ta celková implikace, druhé C je implikace v první závorce (prefix)

3. Přednáška

- **theoremy** – množina vět, které jsme dokázali – je to podmnožina z dobře utvořených formulí, každý theorem je tautologie
- množina je rozhodnutelná → konečná
- axiomy:
  - 1. p → (q → p)
  - 2. (p → (q → r)) → ((p → q) → (p → r))
  - 3. (!q → !p) → (p → q)
- **modus ponens** - pokud A → B a platí A, tak platí B (nad čarou premisy, pod čarou závěr) (namalovat !)
- **ponens –** pokud platí A, lze jej přepsat jakoukoli ekvivalentní formulí (pokud je theorem A, tak $A_{[\xi \to C]}$ je také theorem)
- **Formální důkaz**
  - vycházíme jen z formule, nedosazujeme všechny hodnoty, dokazujeme čistě synteticky
  - př.: p → p (ověříme, že je to tautologie, ANO)
    - důkaz (1.axiom 2. axiom 3. substituce 4. MP 1,3 5. subst. q|q->p 6. MP 1,5):
    - využíváme axiom 1 a 2
    - v 2. axiomu r nahradíme za p => (p → (q → p)) → ((p → q) → (p → p))
    - využijeme 1. axiom a vypustíme ho v tom druhém: ((p → q) → (p → p))
    - ((p → (q → p)) → (p → p)) místo q, dáme q → p
    - a nakonec opět nahradíme za 1. axiom **p → p**

- důkaz je konečná posloupnost daných formulí, z nichž každá je buď axiom nebo ji můžeme odvodit z některých předchozích formulí pomocí pravidel odvození
- **Sémantická konzistence = bezespornost**
  - každý theorem musí být logicky pravdivý
  - všechny nedobře utvořené formule nejsou dokazatelné
  - důkaz, že naše výroková logika je konzistentní:
    - dokazuji ze tří axiomů, že všechny theoremy jsou tautologií
    - jsem schopen u každého z axiomů dokázat, že jsou tautologie
    - důkaz metadůkazem – stačí se podívat na MP a ponens a vidím, že vše je tautologie
- **Sémantická úplnost**
  - každá tautologie je dokazatelná
- **Rozhodnutelnost**
  - existuje algoritmus, který rozhodne po konečném počtu kroků, že je rozhodnutelný
  - tento algoritmus je vlastně tabulka pravdivostních hodnot
- naše výroková logika splňuje všechny 3 vlastnosti
- systém může být rozhodnutelný, i když vypustíme sbstituci a používáme jen MP – druhý axiom je první, ale rozvinutý → nesubstituujeme za p
- **Důkaz z hypotéz**
- existují premisy A, B, C a chceme z nich ověřit D
- premisa je buď axiom nebo hypotéza
- hypotéza nemusí být tautologie, to musíme ověřit
- jestliže B je dokazatelné z hypotéz, tak z nich vyplývá → ověřujeme hypotézy (poté je tautologie)
- je dokazatelné $\vdash$ a vyplývá $\models$ je rozdíl !!!
- jestliže z $A_1 ... A_n$ vyplývá B, tak z $A_1 ... A_{n-1}$ vyplývá $A_n \rightarrow B$ => tímto způsobem dokážeme postupně B pomocí všech premis (A jsou hypotézy)
  - možnosti:
    - $B = A_n$, potom získáváme $A_n = A_n$
    - nebo $B = A_i$ kde $i != n$
    - přepis: $\vdash A_1 \rightarrow (A_2 \rightarrow (\ldots.(A_n \rightarrow B))))$
    - dokázali jsme: $(A \rightarrow (B \rightarrow C)) <=> ((A \&\& B) \rightarrow C)$
- příklad:
  - premisa: Není li středa, není schůze.
  - Dokazuji : Jestliže je středa, je schůze.
  - Vycházím z $!A \rightarrow !B$ a B takže $((!A \rightarrow !B) \&\& B) \rightarrow A$

- Úplnost teorie je odlišná od sémantické teorie – každá teorie je bud dokazatelná nebo vyvratitelná, například v aritmetice
- výroková logika je základem každé logiky
- **metadůkaz –** $A_1 A_2 \ldots A_n \vdash B$
    - B může být 1. Axiom 2. A_n 3. A_m kde m != n, 4. MP
    - metadůkaz je tvrzení, že B je dokazatelné z premis

4. Přednáška

- fukce – n vstupů a jeden výstup, deterministický systém (výstup je jednoznačně určen vstupy)
- realizace fce – nekonečně mnoho realizací
- máme operace konjunkce, disjunkce a negace
- literál – A || !A
    - 1. každý literál je elementární konjunkce
    - 2. jestliže A je elementární konjunkce, pak A && p je elementární konjunkce za předpokladu, že to nebude kontradikce
    - př.: A && !B je elementární konjunkce, můžeme psát AB
- jestliže K je elementární konjunkce, pak A || A je duf, jestliže nedojde K || !K
- A || B || C – A,B,C jsou elementární konjunkce
- úplná disjunktivní normální forma údnf - DNF pro literály $A_1 A_2 \ldots A_n$ které jsou elementární konjunkce, budou obsahovat všechny $A_1 A_2 \ldots A_n$
- jak z DNF A || AB || !ABC dostaneme ÚDNF ??
    - (A && B) || (A && !B) == A → proto můžeme do disjunktní formy přidávat proměnné:
    - A || AB || !ABC = AB || A!B || !ABC = ABC || AB!C || A!BC || A!B!C || !ABC

A	B	C	Výsledek	formule
1	1	1	1	A B C
1	1	0	1	A B !C
1	0	1	1	
1	0	0	0	
0	1	1	0	
0	1	0	1	!A B !C
0	0	1	1	!A !B C
0	0	0	0	

- nyní hledáme formuli, která bude realizovat fci: ABC || AB!C || A!BC || !AB!C || !A!BC (údnf)
- ke každé nekontradické fci lze nalézt údnf formuli, která je ekvivalentní
- jakákoli formule lze převést na údnf tak, že nejprve převedeme na dnf a poté na údnf, nebo tak, že si vytvoříme tabulku hodnot a předchozím způsobem uděláme

- ABC || AB!C || A!BC || !AB!C || !A!BC
- jednodušší formu vytvořím srovnáním s pravými sousedy
  (soused je formule vyhovující AB || A!B == A)
  - ABC a AB!C se liší jen o jednu neagci, proto můžu vyloučit C→ AB || AC || B!C || !BC

- ÚKNF – úplná konjunktivní normální forma

A	B	C	Výsledek	formule
1	1	1	1	
1	1	0	1	
1	0	1	1	
1	0	0	0	!A || B || C
0	1	1	0	A || !B || !C
0	1	0	1	
0	0	1	1	
0	0	0	0	A || B || C

(!A || B || C) && (A || !B || !C) && (A || B || C)

- vyloučíme ty, kteří nejsou sousedi → (B || C) && (A || !B || !C)

5. Predikátová logika

- pokud něco logicky vyplývá, nemůžeme říct, že i ve výrokové logice vyplývá
- věta: *Některé stoly jsou dřevěné.* – obsahuje predikát stůl a dřevěné
  - předmět má vlastnost být stolem
- predikát má vlastnost P(a), kde pro každé a přiřazujeme pravdu nebo nepravdu
- věta: *Karel je starší než Petr.* - zde je predikát P = je starší než Petr a dosazujeme a („Karel“)
- počet argumentů může být n - $<a_1,...a_n>$ - pokud je jich více než 1, mluvíme o vztazích
- všechny vlastnosti se charakterizují třídami př. být nemocný, být v konkrétní místnosti,
  - třída může být prázdná
- relace – soubor prvků, pro které platí něco
- hora – predikát; nejvyšší hora – není predikát →
  - hora Everest je nejvyšší, ale nejvyšší hora = Everest
- př.: predikát > aplikován na (3,7) je nepravdivý
- věta: *Někteří savci létají.* - létat je predikát, predikát je většinou sloveso, nebo vlastnost (být stolem); věta: *Karel létá.*
  - Někteří, savci, létat, Karel
  - x,y – proměnné – můžeme za ně dosazovat jména individuí, nebo udělovat hodnotu sémanticky

Syntaxe

- predikáty značíme P,Q,R..., horní index P^n kde n značí počet argumentů $P^2(x,y)$
- proměnné x,y,z,x_1 – záleží na doméně – charakterizujeme typ objektů, které za ně dosazujeme, př.: čísla, nábytek...
- výrokové spojky z výrokové logiky - !, →, &&, ||
- kvantifikátory – pro všechny ∀ – existuje ∃,
- 1. Co je zde duf? $P(t_1,...t_n)$ je duf t>0, t jsou termy:
  - term – individuové konstanty nebo proměnné
- 2. je-li A,B duf, pak !A, A && B, ….. je také duf
- 3. je-li α individuové proměnné, pak i ∀αA, ∃αA jsou duf
- 4. duf je jen to, co spadá pod 1., 2., 3.

Schémata

- 1. Každé A je B. (a) ∀x (A(x) → B(x))
- 2. Některé A je B. (i) ∃x (A(x) && B(x))
- 3. Žádné A není B. (e) ∀x (A(x) → !B(x))
- 4. Některé A nejsou B. (o) ∃x (A(x) && !B(x))
- Kde A, B jsou predikáty
- př.: Každý pes je šelma. - implikace – pokud je pes, pak je šelma
  - ∀x (P(x) → S(x)), kde predikáty P je „být pes“ a S je „být šelma“
- př.: Někteří psi jsou nebezpeční. - existuje pes, který je zároveň nebezpečný
  - ∃x (P(x) && S(x))
- př.: Žádný pes nelétá. - pro všechny psy platí, že pokud jsou psy, nelétají (opět implikace)
  - ∀x (P(x) → !L(x))
- př.: Někteří psi nežerou maso. - existují individua, kteří jsou psi a zároveň nežerou maso
  - ∃x (P(x) && !M(x))

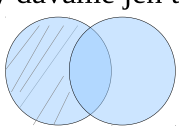
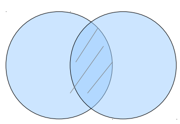
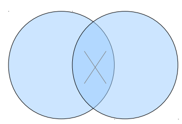
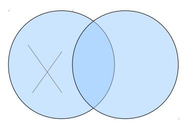
- pokud platí 1. tak neplatí 3., ale pokud neplatí 1. tak to neznamená, že platí 3.
- pokud 1. je pravda, pak 4. nemůže být pravda a navíc pokud 1. není pravda, pak 4. platí
- ∀x A → !∃x !A
- !∀x A → ∃x !A
- !(∃x(P(x) && Q(x)) → ∀x(!Q(x) && R(x,y))) – úkol – upravte tak, aby negace byla pouze před predikáty
- v relané formě například *Každý člověk má rád alespoň jednoho živočicha.* Převedeme na *Existuje člověk, který nemá rád žádného živočicha.*

6. Kategorický sylogismus

- věty: *Každý učitel je vysokoškolák.* *Někteří prátelé jsou učitelé.*
- Vyvození: *Někteří přátelé jsou vysokoškoláci.*
- Můžeme nahradit predikáty za symboly učitel(M), vysokoškolák(P), přítel(S)
  - M a P - toto je figura obrácené Z, spojene sou M-ka
  - S i M
  - => S i P

- P M M P P M → mám tři predikáty, jeden je společný
- S M M S M S

- pak určujeme který predikát platí → konečný počet možností
- pro náš příklad – obrácené Z, platí:
- a a **a** e
- a e **i** a
- a e **i** e

- věta: Všichni členové kongresu mají brýle. - může být pravdivá v reálu, ale není pravdivá logicky, protože zde máme predikáty, musíme dosadit
- oproti tomu matematická věta: Pokud je číslo x>2 a je prvočíslo, pak je liché → vždy bude pravdivé, ať už dosadíme jakékoli číslo
- **Frege –** zakladatel kvantifikátorů, do té doby aristetolovy a,e,i,o
  - umožnil vyjádřit např.: $\exists x\, (P(x) \rightarrow \forall y\, P(y))$ (Pokud někdo pije, pak pijí všichni.) → to je tautologie, protože pokud někdo nepije, pak je implikace pravdivá 0 → cokoliv, pokud pijí všichnu tak taky 1 → 1
- Vennovy diagramy – šrafování – prázdná, x – není prázdná
- křížky dáváme jen tam, kde víme, že něco je, a šrafování jen tam kde víme že není
- a 
- e 
- i 
- o 

- M i P & S i M → S i P (zkusit v diagramech)
- S a M & P a M → nemůžeme nic vyvodit, protože jsou zaškrtané S, P, ale žádné M a žádný křížek
- dále vyplývá: S a P → P i S

– S e P → P e S
– S i P → P i S
S o P → nelze

- 2 věty, které nejsou stejné:
  - Kdo nejde s námi, je proti nám. $\forall x\ (!P(x) \rightarrow A(x))$
  - Kdo není proti nám, je s námi. $\forall x\ (!A(x) \rightarrow P(x))$

- Každý člověk je smrtelný. Aristoteles je člověk. → Aristoteles je smrtelný
  - není sylogismus – Aristoteles není predikát, ale už přiřazujeme x : ne A(x), ale x=A

7.Predikátová logika

- axiomy musí být rozhodnutelné, tzn. existuje algoritmus, kterým zjistíme, zda nějaká duf vychází z axiomů
- pro predikátovou logiku platí axiomy výrokové plus další:
  - $\forall x\ P(x) \rightarrow P_{[x \rightarrow t]}$ tady za x dosadíme nějaký term, kde t je volné pro x v P
    - jestliže t je konstanta, nic neřešíme, jestliže je to proměnná, musí být volná, tzn. nesmí být před výrazem kvantifikátor s touto proměnnou
  - př.: $\forall x\ \exists y\ R(x,y) \rightarrow R(y,y)$ kde R je relace, například „menší než“ → pak to neplatí, protože y je vázaná proměnná, tedy není volná
    - př.: $\forall x\ P(x) \rightarrow P(x)$ – pokud se $\forall x$ vztahuje k celému výrazu, je to pravda, pokud ne a vztahuje se jen k prvnímu, tak tam je vázaná a v druhém P(x) je volná
- MP pro predikátovou logiku : pokud $A \rightarrow B$, tak $A \rightarrow \forall x\ B(x)$
- důkaz z hypotéz – nemůžeme závěr považovat za pravdivý, ale pokud položíme $H_1 \rightarrow H_1$, vycházíme z axiomů, v průběhu důkazu se můžeme zbavit závislosti na hypotéze a závěr je pravdivý
- snazší je dokazovat z pravidel než axiomů
- platí: každý teorém je tautologie a pokud závěr vyplývá z premis, tak je z nich dokazatelný

Vyhodnocování predikátových formulí

- univerzum – množina individuí, se kterými pracujeme, za co dosazujeme do výrazů, počítáme s tím, že není prázdná množina př.: čísla, lidé atd.

1. **Interpretace**

   - Int(e,v), kde v je valuace, e je výraz(expression)

   - z ní dokážeme odvodit pravdivost pro konkrétní x, pomocí valuace $v(x_1)$

   - interpretace konstanty je prvek univerza: Int(k) je prvkem U

   - interpretace predikátu nevede hned k absolutní hodnotě(individuu), nejprve ho musíme aplikovat na proměnnou: Int(P) je podmnožinou U, nebo Int(P) je prvekem U^2

     - př.: pokud U={a,b,c}, tak P je prvkem množiny podmnožin U^2 která má počet prvků 2^3 tedy 8

2. **Odvození pravdivostních hodnot z interpretace**

   1. Int($P(t_1, \dots t_n)$) je pravda, jestliže Int(t_1,v) …. Int(t_n,v) je prvkem Int(P,v)

      - př.: n=3, {<a,b,c>; <b,b,a>}

   2. Int ∀x A je pravda, pokud Int.....(A)=1 pro každou valuaci v

      pro ∃x je to stejné, jen opačně, tedy neplatí, pokud ...(výše)

      .

      .

      .

příklady:

Int(A,v) = Int(B,v) – pro každou valuaci

Int(A,v) = 1 - je pravdivá pro každé A

∀v Int(A,v) = 1 - je pravdivá k dané interpretaci

pro všechny Interpretace značíme ∀Int

∀Int ∀v (A=1) je pravdivá v každé interpretaci → logická pravdivost

- pozor, platí jen pokud platí pro všechny interpretace, pro všechny valuace nám to nestačí, stačilo ve výrokové logice

∀x (P(x) → Q(x)) Int(P = {a,b,d}) a Int(Q = {a,d}) → tady to nevyjde, protože b je v P ale není v Q, ale pokud to bude opačně, tedy Q(x) → P(x), tak to platí pro každou interpretaci (tedy pro a,d z Q jsou taky v P)

∀x P(x) → P(y) - ptám se jak mám ohodnotit, aby P(x) byla vždy pravda, protože P(x) je v daném univerzu, je pravdivé

P(x) → ∃y P(y) - řešíme sporem, kdy je neprava? Pokud pro P není žádný prvek v univerzu, tedy ani x a to není duf, takže formule je logicky pravdivá

8. Přirozená dedukce (Gentzenovské systémy)

- jeden axiom a řada pravidel místo řady axiomů
- používá sekvence: $A_1, \dots A_n \rightarrow B$
- pokud uplatníme sekvence $s_1 \dots s_n$ tak z toho vyplývá nějaká sekvence s
- pokud dokazujeme pravdivou větu, dokazujeme pomocí sekvencí, kde sekvence je odvozena buď z axiomu nebo z dokázané sekvence
- mnnožina důkazů se značí řeckým gamma
- **axiom a jeho odvození** (Γ,A =A je prvkem množiny Γ)
  - Γ,A → A
  - pokud Γ,A → B, tak potom Γ,A,C → B (při přidání premisi, se nezmění platnost obsahu)
  - Γ,A → B a zároveň Γ,A → !B tak Γ → !A (došli jsme ke sporu, není pravda premisa)
  - disjunkce je symetrická (nezáleží na pořadí)
    - (Γ → A) → (Γ → A|B) => (Γ → B) → (Γ → A|B)
- (Γ → A → C), (Γ → B → C), (Γ → A |B) => (Γ → C)

- konjunkce: $(\Gamma \rightarrow A), (\Gamma \rightarrow B) \Rightarrow (\Gamma \rightarrow A\&B)$
    - $(\Gamma, \rightarrow A \& B) \Rightarrow (\Gamma, \rightarrow A)$ a to stejné pro B
- zavedení implikace: $\Gamma, A \rightarrow B \Rightarrow (\Gamma, \rightarrow A \rightarrow B)$
- modus ponens $\Gamma \rightarrow (A \rightarrow B), (\Gamma \rightarrow A) \Rightarrow (\Gamma \rightarrow B)$
- zavedení negace: $(\Gamma \rightarrow A \rightarrow B), (\Gamma \rightarrow A \rightarrow !B) \Rightarrow (\Gamma \rightarrow !A)$
- $(\Gamma \rightarrow A), (\Gamma \rightarrow !A) \Rightarrow (\Gamma \rightarrow B)$ (došli jsem ke sporu – kontradikce, vyvodíme cokoli)
- dvojí negace: $(\Gamma \rightarrow !!A) \Rightarrow (\Gamma \rightarrow A)$ i oboustranná: $(\Gamma \rightarrow A) \Rightarrow (\Gamma \rightarrow !!A)$
- **základní axiom: $p \rightarrow p$**
  - odvození z axiomu:
    - $p \rightarrow p|!p$
    - $!p \rightarrow !p$
    - $!p \rightarrow p|!p$
    - $\rightarrow p|!p$
    - důkaz $(p \rightarrow q) \rightarrow (!q \rightarrow !p)$:
      - 1. $p \rightarrow q, !q, p \Rightarrow p$
      - 2. $p \rightarrow q, !q, p \Rightarrow p \rightarrow q$
      - 3. $p \rightarrow q, !q, p \Rightarrow q$
      - 4. $p \rightarrow q, !q, p \Rightarrow !q$
      - 5. $p \rightarrow q, !q \rightarrow (!q \rightarrow !p)$ (první !q šktneme)
      - 6. $(p \rightarrow q) \rightarrow (!q \rightarrow !p)$ (zavedení implikace)

Zavedení do predikátové logiky

- A(x) není to stejné jako P(x), A(x) znamená, že formule A obshauje proměnnou x, tzn. že x není jen volná proměnná ve formuli A, ale je vázaná
- zavedení obecného kvantifikátoru: $\Gamma \rightarrow A(x) \Rightarrow \Gamma\forall x\, A \rightarrow (x)$
- zavedení eliminace: $\Gamma \rightarrow \forall x\, A(x) \Rightarrow \Gamma \rightarrow A(t)$
- zavedení existenčního kvantifikátoru: $\Gamma \rightarrow A(x) \Rightarrow \Gamma \rightarrow \exists t\, A(t)$
- $(\Gamma \rightarrow \exists x\, A(x)), (\Gamma, A(x) \rightarrow C) \Rightarrow \Gamma \rightarrow C$

- $\forall x\, A(x) \rightarrow \exists x\, A(x)$
- 1. $\forall x\, A(x) \rightarrow A(t)$ (eliminace obecného kvantifikátoru)
- 2. $\forall x\, A(x) \rightarrow \exists x\, A(x)$
- axiomy:
- $\exists x\, \forall y\, A(x,y) \rightarrow \exists x\, \forall y\, A(x,y)$ (základní axiom), tedy $\Gamma = \{\exists x\, \forall y\, A(x,y)\}$
- $\exists x\, \forall y\, A(x,y), \forall y\, A(b,y) \rightarrow \forall y\, A(b,y)$ (zavedení obecného kvantifikátoru)

- $\exists x\, \forall y\, A(x,y), \forall y\, A(b,y) \rightarrow A(b,y)$
- $\exists x\, \forall y\, A(x,y), \forall y\, A(b,y) \rightarrow \exists x\, A(x,y)$ (zavedení existenčního kvantifikátoru)
- $\exists x\, \forall y\, A(x,y) \rightarrow \exists x\, A(x,y)$ (můžeme škrtnout druhou premisu)
- $\exists x\, \forall y\, A(x,y) \rightarrow \forall y\, \exists x\, A(x,y)$

- platí $\exists x\, \forall y\, A(x,y)$ <==> $\forall y\, \exists x\, A(x,y)$, ale nefunguje to na druhou stranu: neplatí, že $\forall y\, \exists x\, A(x,y)$ <==> $\exists x\, \forall y\, A(x,y)$
- příklad:
  - Premisy: Je-li středa, není schůze. Je schůze.
  - Z toho vyplývá: Není středa.
  - Důsledek: z $A_1 \dots A_n$ výplývá B, tedy B logicky vyplývý z vět A, to neznamená, že to je nebo není pravda

9. Predikátová logika 1. řádu s identitou

- existuje predikát =
- potom v univerzu jsou uspořádané dvojce, které jsou identické $\{\langle a_1,a_1\rangle, \langle a_2,a_2\rangle, \dots \langle a_n,a_n\rangle\}$
- obvyklý predikát P, Q.. může být interpretován jakkoli (libovolně), proto se zavedl identický predikát, který nesmíme interpretovat jinak než takto (pomocí univerza výše)
- v duf nám přibyde další bod: *Jsou-li t_1, t_2 termy, pak $t_1 = t_2$ je duf.*
- V axiomech přbyde jeden další: $x = x$
- Leibnitzovo pravidlo:
  - jestliže platí $t_1 = t_2$ a platí věta $(\dots t_1 \dots)$, tak platí věta $(\dots t_2 \dots)$ - tzn. mohu nahradit
- jestli nějaké proměnné přiřadíme term, musíme u všech výskytů této prměnné
- př.: $t_1 = t_2$: $3+2 = +\sqrt{25}$ 3+2 je liché => $+\sqrt{25}$ je liché
- ale př.: $3+2 = +\sqrt{25}$ a Karel počítá 3+2 => Karel počítá $+\sqrt{25}$ není pravda (tady nejde o výsledek ale o samou operaci 3+2 a ta je jiná)
- př.: Prezident ČR = manžel Libie Klausové & Franz chce být prezidentem => Franz chce být manžel Libie Klausové (neplatí, protože úřad prezidenta nesouvisí s rodinou)
- identita je symetrická - $t_1 = t_2 \rightarrow t_2 = t_1$ lze dokázat z Liebnitzova pravidla – dosadíme do věty t_2 za t_1 a naopak $(x=y \rightarrow (x=x \rightarrow y=x))$ a podle pravidla z výrokové logiky – $A \rightarrow (B \rightarrow B) = B \rightarrow (A \text{->} C)$ – tak $(x=y \rightarrow (x=y \rightarrow y=x))$

- **Numerické kvantifikátory**
  - **alespoň n**
    - existuje takové x, že A(x) platí alespoň pro n výskytů x

    - $P(x_1)\&P(x_2) \dots \&P(x_n)$ pro $x_i != x_j$ platí i !=j
  - **pro nejvýše n**
    - musí být menší nebo rovno počtu podmínek
    - $\forall x_1 \dots x_{n+1} (P(x_1) \& P(x_2) \dots P(x_n) \& P(x_{n+1}) \rightarrow x_{n+1} = x_1 | \dots. | x_{n+1} = x_n)$
  - pro existenční a obecný kvantifikátor je to n=1
  - **∃!x** znamená existuje přesně jedno x
- **Určité popisy**
- nemluvím o Moutn Everestu, ale o nejvyšší hoře, nemluvím o VK, ale o prezidentovi ČR
- pokud platí x, platí všechny termy, které jsem za něj schopen dosadit $\forall x\, A \rightarrow A_{[x \rightarrow t]}$
- například popis největší prvočíslo, nemůžeme dosadit žádnou konstantu, ale popis existuje
- Bernard Russel zavedl obrácené jota (zde budu psát j) a jxA – jediný objekt, který splňuje
  - setkáme se vždy jen v souvislosti s predikátem, jinak nemá smysl
  - př.: predikát P = je holohlavý a Q = být současný francouzský král
  - $\exists x\, Q(x) \;\&\; \forall y\, ((Q(y) \rightarrow x=y) \& P(x))$
    - existuje současný francouzský král a je jen jeden
  - negace tohoto výroku je $\exists x\, Q(x) \& \forall y(Q(y) \rightarrow y=x) \& !P(x)$
    - existuje takový současný král a není holohlavý
  - problém je, že pokud neexistuje král, tak věta ztrácí smysl
  - pokud z A výplýva B a z !A vyplývá B tak A nemůže být prava ani nepravda a věta ztrácí hodnotu → to se stalo zde (u toho krále), v obou příkladech předpokládám existeni krále
- tedy pokud zavádím objekt popisem, musím uvážit, že ten objekt taky nemusí existovat, kdežto pokud mluvím o konkrétním objektu, nemusím uvažovat jestli existuje, to je předpoklad
- př.: Jestli-že někdo chce žít v naší zemi, musí odpřísáhnout, že náš vládce je pod ochranou nejdokonalejší bytostí. → člověk, který nevěří, může bez problému odpřísáhnout, protože je pro něj pravda vše kvůli implikaci → Russelovo pravidlo není zcela v pořádku
- definice indentity záleží na univerzu (podobně jako definuji equals() v Javě – kdy se 2 objekty rovnají)
  - př.: indentita přirozených čísel $\{<a_i, a_i>\dots\}$
- Int_v (a=b) – je pravda, pokud Int(a) = Int(b)
    - → rovnsti se nevyhnu, první je objektová indentita, druhá je jazyková
- jazyková indentita závisí už na definici univerzu
- objektová porovnává výrazy, kdežto jazyková porovnává konkrétní hodnoty

- predikátová logika: můžeme porovnávat proměnné, konstanty nebo predikáty, proměnné a konstanty jsou z univerza U a P je podmnožina U^n identický predikát = je podmnožina U^2 – protože porovnáváme 2 objekty

- predikátová logika 1. řádu s indentitou je konzistentní, úplná a není rozhodnutelná → neexistuje algoritmus, který by generoval neteorémy
- A(x) je věta A, jterá obsahuje alespoň jeden výskyt proměnné x
- P(x) je predikát vyhodnocovaný interpretací
- příklad: ∃y P(x,y) & x != y
  - v(x) = 3 (tedy valuace x je 3) a v(y) = 4,
  - P {<2,4> <2,5> <3,3>} (uspořádané dvojce)
  - tak musí existovat dvojce <3,y>, => taková existuje jedna <3,3>, je tedy pravdivá, protože y je v druhé podmínce volná
  - kdyby byl výraz takto ∃y (P(x,y) & x != y) uzávorkované, tak v druhé podmínce už y není volná ale vázaná a tak je to nepravda (pro x=3 a y=4)
  - záleží na dosahu kvantifikátoru, v prvním případě je dosah jen na predikát P

10. Binární relace

- R(x,y) musí být z U^2 - arita se zapisuje v horním indexu, pro 2 je to binární
- zapisuje se xRy
- zavedeme !R (správě čára nad R) je doplněj k R - !xRy   x<y => x>=y
- u nad R : $xR^{u}y$ = yRx, tedy jen prohodíme prvky relace,   x<y => x>y
- xR∩Sy = xRy & xSy   R∩S = 0
- xR sjednoceno s Sy = xRy | xSy   (skládání relací)
- xR krát Sy = ∃R(xRz & zSy)
- xSy – x je sourozenec y
- R je podmnožinou S   ∀xy (xRy → xSy)

Reflexivita

- Refl(R): ∀x xRx   (všechny volné proměnné musí být v R sami se sebou) proměnná R je volná, je to vlastnost relace
  - př.: < není reflexivní <= je reflexivní
- Poloreflex(R): ∃x !xRx & ∃x xRx (existuje alespom jedno x, které není v R samo se sebou)
- Ireflex(R): ∀x !xRx   (neexistuje x, které by bylo v R samo se sebou)

Symetrie

- Sym(R):   ∀xy (xRy → yRx)
- Polosym(R): ∃xy (xRy & yRx) & ∃xy (xRy & !yRx)
- Asym(R):   ∀xy (xRy → !yRx)
- Antisym(R): ∀xy ((xRy & yRx) → x=y)   (důležité pro definování uspořádání)
- př.: podmnožina – není symetrická, je polosymetrická a není asymetrická

Tranzitivita

- Tranz(R): $\forall xyz\ (xRy \rightarrow (yRz \rightarrow xRz))$ nebo $\forall xyz\ ((xRy\ \&\ yRz) \rightarrow xRz)$

- Con(R): $\forall xy\ (xRy \mid yRx \mid x=y)$
- podobnost je trojčlenná, musíme porovnávat vzhledem k něčemu

Ekvivalence

- relace musí mít tyto vlastnosti Refl, Sym a Tranz
- platí, že pokud x je prvkem m_i tak není prvkem m_j (jeden prvek může být prvekm pouze jedné třídy ekvivalence)
- množiny jsou disjunktní – tedy nemají žádný společný prvek
- $m_i\ E_q\ m_j$ platí tehdy, jeli x_i a x_j patří do množiny m_k

Uspořádání

- relace s vlastnostmi Refl, Antisym a Tranz

- jestliže R je symetrická a tranzitivní, pak nemůže být ireflexivní (DOKÁZAT), počítáme s tím že relace R je neprázdná

- šipkové diagramy relačních schémat, reflexivita:
- $\exists x\ \forall y\ R(x,y) \rightarrow \forall y\ \exists x\ R(x,y)$ platí vždy (pokud vytvořím vztah pro každé x, tak logicky každé bude mít někoho, s kým je ve vztahu (alespoň ten jeden co sme vytvořili))
    - naopak to neplatí př.: pokud pro všechny čísla existuje nějaké číslo, které je větší, tak z toho nevyplývá, že existuje číslo, pro které platí, že všechny ostatní čísla jsou větší
- $\forall x\ !xRx\ \ \&\ \ \forall x \exists y\ xRy\ \ \&\ \ \forall xyz\ (xRy \rightarrow (yRz \rightarrow xRz))\ \ \&\ \ \forall xy\ (xRy \rightarrow\ !yRx)$
- ireflexivní, každé x je v relaci s nějakým y, tranzitivní, asymetrické
- lze dosáhnout jen v nespočetně nekonečném univerzu, př.: nemůžeme vyjádřit úhlopříčku čtverce bez reálných čísel, přestože strany čtverce jsou v přirozených

11. Predikátová logika s funkcemi

- $\exists\ x_1,x_2...x_n,y\ (P(x_1,x_2...x_n,y)\ \&\ \forall z(P(x_1,x_2...x_n,z) \rightarrow z=y))$
- $f_p(x_1, \dots x_n) = P(x_1,x_2, f_p(x_1,x_2))$
- tří argumentový predikát interpretujeme takto: $P(x_1,x_2,x_3) + (x_1,x_2) = P(x_1,x_2, f(x_1,x_2))$ – toto je funkce sčítání, pro $x_1 = 3$ a $x_2 = 7$, tak vrátí $x_3 = 10$
- takto jsou definované totální fce, jak by se definovali parciální fce?
    - $\forall\ x_1,x_2...x_n,y\ (\ P(x_1,x_2...x_n,y) \rightarrow (P(x_1,x_2...x_n,z) \rightarrow z=y)\ )$
- relace < - predikát není funkcionální
- relace je funkce
- takže < může být funkce, která pro dva vstupy vrací true nebo false (pokud x<y tak true)

Predikátová logika 2. řádu

- interpretace vypadá tak, že kromě obvyklých predikátů, které bereme jako proměnné, máme také individuové proměnné opatřené hodnotami
- potom lze těžko poznat rozdíl mezi proměnnou a hodnotou
- potom proměnné, tedy predikáty, tedy relace napíšeme normálně a neobvykle napíšeme relaci mezi třídami (symboly vyššího řádu)
- je exrpresivnější, lze zapsat co nelze zapsat v P.l.1.řádu
- P.logika 2. řádu není ani úplná natož rozhodnutelná
- pokud by byla P.l.2.řádu úplná, byla by P.l.1.řádu rozhodnutelná, to ale neplatí
- příklady zápisů, které lze napsat v P.l.2.řádu, ale nelze v 1. řádu:
  - $\forall p \ \exists q \ [p \rightarrow q]$ - ke každé třídě existuje její podtřída (podmnožina) toto je tautologie
  - nelze ale pro to napsat důkaz, dokazatelnost formulací je slabost P.l.2.řádu

Lambda kalkul

- typový a netypový
- Russel se tímto vyhýbá paradoxům, který kalkul řeší oproti predikátové logice

Definice

1. rovnostní definice (L = P)

- Aristotelská podoba definice:
  - člověk = živočich obdařený rozumem množina: neopeřený dvojnožec
  - kdyby množina člověk a neopeřený dvojnožec byly stejné, o rovnosti to nic neříká
  - musímě brát v potaz esenci množiny – tedy esence množiny člověk je to, že má rozum – postihli jsme esenci člověka a můžeme porovnávat
  - můžu říct – rovnostranný trojúhelník = trojůhelík, který má všechny strany stejné, ale také rovnostranný trojúhelník = trojúhelník, který má všechny úhly stejně velké – 2 různé definice, které platí jen pokud jsou na sobě vzájemně závislí
  - 3+2 není to samé jako odmocnina z 25, přitom se rovná – záleží, jestli se zajímáme o procesu, který není stejný, nebo o esenci, tedy o výsledek
  - při definici něco neznámého definuji pomocí známého
  - definice se děje přes nejbližší rod a pak přes specifické rozdíly

- Russelova podoba definice
  - nepohybujeme se zleva do prava ale naopak
  - Prvočíslo = přirozené číslo > 1, dělitelné přesně samo sebou a 1
  - definice zkratky
  - definuju objekt, ne výraz a proto je důležitá pravá strana, která ho popisuje

- Prvočíslo = přirozené číslo > 1, dělitelné přesně dvěma děliteli
  - toto je f_2, ale je stejná jako ta předchozí, jen je zadaná jinou konstrukcí:
  - $\forall f_g (\forall x (f(x) = g(x)) \rightarrow f=g)$

- **Explikace**
  - zpřesnění – definice potom platí v určité oblasti
  - př.: pojem síla – jinak ho chápeme normálně a jinak třeba ve fyzice (je to jinak definováno)
  - je použita v běžném životě, nezavádíme přesné definice, které by platili obecně
  - pokud platí různé explikace pro jeden výraz tak jsou různé významy, už to není to samé

2. **definice které nejsou rovnosti**

- $x + 0 = x$
- $x + Succ(y) = Succ(x+y)$
- Succ je funkce která vrací následníka

Domácí úkol - Důkaz:

- předpoklady: 1. $\forall xy (xRy \rightarrow yRx)$
  - 2. $\forall xyz ((xRy \;\&\; yRz) \rightarrow xRz)$
- závěr: $!(\forall x \; !xRx)$

- upravení závěru: $\exists x \; xRx$
- důkaz: relace R je neprázdná, takže obsahuje alespoň 2 prvky, například xRy
  - z prvního přepokladu symetrie je v relaci i yRx
  - z druhého předpokladu platí $((xRy \;\&\; yRx) \rightarrow xRx)$
  - z toho vyplývá, že prvek x je v relaci sám se sebou, to znamená že platí $\exists x \; xRx$
  - proto relace není ireflexivní, ale není ani reflexivní, protože prvek y není v R sám se sebou