...ivalence v PL:

$\forall x\,\varphi \Leftrightarrow \neg\exists x(\neg\varphi)$ $\quad \exists x\varphi \Leftrightarrow \neg\forall x(\neg\varphi)$ ①

$\forall x\,\varphi \Leftrightarrow \varphi,\ \exists x\varphi \Leftrightarrow \varphi$ pokud $x \notin FREE(\varphi)$ ②

$\forall x(\varphi \vee \delta) \Leftrightarrow (\forall x\varphi) \vee \delta$ pokud $x \notin FREE(\delta)$ ③

$\exists x(\varphi \wedge \delta) \Leftrightarrow (\exists x\varphi) \wedge \delta$

$\forall x(\varphi \to \delta) \Leftrightarrow (\exists x\varphi) \to \delta$ pokud $x \notin FREE(\delta)$ ④

$\exists x(\varphi \to \delta) \Leftrightarrow (\forall x\varphi) \to \delta$

$\forall x(\varphi \to \delta) \Leftrightarrow \varphi \to (\forall x\delta)$ pokud $x \notin FREE(\varphi)$ ⑤

$\exists x(\varphi \to \delta) \Leftrightarrow \varphi \to (\exists x\delta)$

$\forall x\,\varphi(x) \wedge \forall y\,\delta(y) \Leftrightarrow \forall x(\varphi(x) \wedge \delta(x))$ ⑥

...též pro $\exists$ a $\vee$, jsou jakkoby asociativní

...NF: $\varphi = Q_1 x_1 Q_2 x_2 \cdots (\delta(x_1, x_2 \ldots, y_1, y_2 \ldots))$ úplně volné prom.

šňůra kvantif. formule bez kvantif.

...) eliminovat zbytečné kvant. ②

...) eliminovat $\Leftrightarrow$ 3) přejmenovat proměnné • pokud je v průniku $FREE(\varphi)$ a $BOUND(\varphi)$ • pokud je kvantifikované více než jednou $\to$ nahradit v podformulích všechny volné výskyty 4) přesunout negace dovnitř ① De Morgan negace $\to$

5) přesunout kvant. doleva ④ ⑤

$(Q x\varphi) \wedge \delta \Rightarrow Qx(\varphi \wedge \delta)$

$(Q x\varphi) \vee \delta \Rightarrow Qx(\varphi \vee \delta)$

...fektivnost: lze algoritmicky ověřit, že je daný řetězec důkaz

$\Rightarrow$ teorie PL je efektivní, když je ověřitelné, co je jejím speciálním axiomem $\to$ lze ověřit, že je řetězec důkazem v T

...orektnost: nedají se dokázat nesmysly

...úplnost: co je pravdivé, je dokazatelné (máme dost axiomů)

...L i PL jsou kor. + úplné ($\vdash\varphi \Leftrightarrow \models\varphi$ - Post, $T\vdash\varphi \Leftrightarrow T\models\varphi$ - Gödel)

...ezespornost: axiomy si neprotiřečí

T je bezesporná $\Leftrightarrow$ T má model, sporná nemůže mít model

...ádná efekt. bezesp. teorie PL zahrnující Peanovu arit. ...nemůže být úplná; v systému —‖— není možné dokázat ...ho vlastní bezespornost

...elace: doplňková: $\overline{R} = A \times B \setminus R$

inverzní: $R^{-1} = \{[a,b];\ [b,a] \in R\}$

$R \circ S = \{[a,c],\ \exists b: [a,b] \in S \wedge [b,c] \in R\}$

$(R \circ S) \circ T = R \circ (S \circ T) \qquad (R \circ S)^{-1} = S^{-1} \circ R^{-1}$

Uspořádání: částečné - R + antisym. + T relace

úplné/lineární: každé dva prvky porovnatelné $\forall x\forall y (x \preceq y \vee y \preceq x \vee x = y)$

(**ostré:** T + asymet. $\forall x \forall y (x \prec y \to \neg(y \prec x))$) **Kvazi:** R + T relace

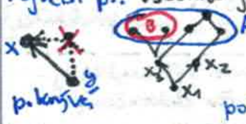
dobré: každá podmnožina obsahuje nejmenší prvek

minimální p.: nic není pod $\forall b \in M: b \preceq a \to a \preceq b$ (čili $a = b$)

maximální p.: nic není nad $\forall b \in M: a \preceq b \to b \preceq a$ —‖—

nejmenší p.: všechny prvky jsou větší $\forall b \in M: a \preceq b$

největší p.: všechno je pod $\forall b \in M: b \preceq a$ ← musí být porovnatelné



dolní závora: a je pod každým prvkem podmn. $x_1, x_2, x_3 \preceq \forall y \in A$ (podobně horní z.)

pokrývá; **pokrývá:** $x \neq y,\ y \preceq x,\ \neg\exists z: y \preceq z \preceq x \wedge z \neq x, y$

infimum: největší dolní závora (x_3 pro B) $\wedge$ ($\to$ průsek)

supremum: nejmenší horní závora $\vee$ ($\to$ spojení)

Zobrazení: $[a,b] \in R \wedge [a,c] \in R \to b = c$ $\quad F: A \to B$

injekce: prosté: $a \neq b \Rightarrow f(a) \neq f(b)$ **surjekce/na:** $H(f) = B$

zobr. něčeho (do): $D(f) = A$ **zobr. z:** $D(f) \subseteq A$ **bijekce:** injekce + surjekce, každý z B má 1 vzor z A

ekvivalence množin: bijekce existuje, relace $\sim$ $a \sim b \Leftrightarrow f(a) = f(b)$ je ekvivalencí na A, faktor. mn. $A/\sim\ = H(f)$

Operace: zobrazení $A \times A \xrightarrow{do} A$, binár. operace na A má max 1 e

op. je asociativní $\wedge\ \exists e \to$ každý prvek má max. 1 inverz

Algebry: grupoid (uzavřená) pologrupa (uz. + asociativní)

monoid (uz. + asoc. + $\exists e$) grupa (uz. + asoc. + $\exists e$ + každý má inverz)

podgrupa: je grupa, má stejný e ← tohle je špatně napsané, Ondřeji, prosím.

rozklady $G(M, \circ)$ podle podg. $H(N \subseteq M, \circ)$:

levý: $\{aH,\ a \in M\}$ kde $aH = \{a \circ h,\ h \in N\}$ - levé třídy

pravý: $\{Ha,\ a \in M\}$ kde $Ha = \{h \circ a,\ h \in N\}$ - pravé třídy

Lagrangeova věta: počet prvků podgr. je dělitelem počtu prvků gr.

$(H, \circ)$ je podgrupou $(G, \circ) \Leftrightarrow \forall a, b \in H: a \circ b^{-1} \in H$

normální podgrupa: $\forall a \in G, h \in H: a \circ h \circ a^{-1} \in H$

G je komut. $\Rightarrow (H, \circ)$ je komut. $\qquad \Leftrightarrow \{aH\} = \{Ha\}$

Morfismy: grupy $(A, *)$, $(B, \circ)$, $h: A \to B$, platí: $h(a * b) = h(a) \circ h(b)$

monomorf.: injektivní **epimorf.:** surjektivní

izomorf.: bijektivní **endomorf:** morf. $A \xrightarrow{do} A$ **aut.:** izom. A na A

Kongruence: ekvivalence slučitelná se všemi operacemi na algebře

$[a,b] \in R \wedge [c,d] \in R \to [a \circ c, b \circ d] \in R$

rozklad $\mathbb{Z}$ na zbytk. třídy po dělení m: $a \equiv b \pmod m$

Svazy: množina uspořádaná relací je svazově uspořádaná, když pro každou 2prvkovou množinu obsahuje její supr. a inf...

svaz $(X, \vee, \wedge)$: $\forall x, y, z \in X$:

$x \vee x = x \wedge x = x$ idempotence

$x \vee y = y \vee x \quad x \wedge y = y \wedge x$ komutativní

$x \vee (y \vee z) = (x \vee y) \vee z$, totéž s $\wedge$ asociativní

$x \wedge (x \vee y) = x \vee (x \wedge y) = x$ absorpce

podsvaz: $(Y, \vee_Y, \wedge_Y)$, zachovává v množině Y suprema a infima, jako byly v pův. svazu

izomorfismus svazů: $X \to Y$ bijekce, $\forall x, y \in X$:

$F(x \vee_X y) = f(x) \vee_Y f(y)$, $f(x \wedge_X y) = f(x) \wedge_Y f(y)$

modularita: $\forall xyz: x \preceq z \to x \vee (y \wedge z) = (x \vee y) \wedge z$

distributivita: $\forall xyz: x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

komplementarita: $\exists$ nejmenší prvek 0, největší 1, ke každému $x\ \exists\bar{x}$: $x \wedge \bar{x} = 0$, $x \vee \bar{x} = 1$

distributivní $\Rightarrow$ modulární

distributivní $\to$ každý prvek má max. 1 komplement

modulární $\Leftrightarrow$ neobsahuje podsvaz izomorf. s N_5

distribut. $\Leftrightarrow$ —‖— s N_5 ani s M_5

N_5

M_5

Booleovský svaz: distribut. a komplement. svaz s nejmenším a největším prvkem $\to$ **B. algebra:** $(X, \vee, \wedge, ', 0, 1)$

kde $'$ je operace komplementu

počet prvků Booleovské algebry je 2^n

upeň $d_G(v)$, nejvyšší Δ, nejnižší δ
-regulární graf: všechny vrcholy mají stupeň d
očet stupňů vždy $2|E|$
plný graf: n vrcholů spojených po všech dvojicích $|E| = \binom{n}{2}$
– bipartitní graf $K_{n,m}$ hvězda: $K_{1,n}$ Δ: K_3
dukovaný podgraf: obsahuje všechny hrany pro danou podm. V
omorfní grafy: stejný počet hran a vrcholů, zobrazuje každý vrchol na vrchol stejného stupně
osažitelnost: existuje cesta z u do v → ekvivalence $\sim$ na množině vrcholů → komponenty souvislosti = třídy $\sim$
ouvislý graf: právě jedna —‖—
trom = souvislý graf bez kružnic = min. souvislý a max. acyklický graf na dané množině V
obsahuje vrchol $d_G(v)=1$, s n vrcholy má $n-1$ hran

ed: posloupnost vrcholů a hran, mohou se opakovat
ah: sled bez opakování hran uzavřený: končí, kde začal
ulerovský g.: lze nakreslit jedním uzavř. tahem
⇔ je souvislý a všechny vrcholy jsou sudého stupně
mi-eulerovský g.: —‖— jedním otevřeným tahem
⇔ je souvislý a právě dva vrch. jsou lichého stupně
ovinný g.: nakreslení, kde se nekříží hrany – 3rozm. euklid. mnohostěny Stěna: topologicky souvislá oblast
$|V_G| + F - |E_G| = 2$ F je počet stěn
→ rov. graf s $v \geq 3$ vrcholy má max. $3v-6$ hran
→ rov. graf s —‖— bez Δ má max. $2v-4$ hran
→ rov. graf obsahuje vrchol stupně max. 5
→ rov. graf bez Δ —‖— max. 3
odrozdělení: nahrazení hrany cestou •—• → •—•—•
uratowski: graf je rovinný, když neobsahuje $\cong$ K_5 ani $K_{3,3}$
Vagner: —‖—, když jeho minory (odstranění vrcholů a smrštění hran) neobsahují K_5 ani $K_{3,3}$
amiltonovská kružnice: kruž. procházející všechny vrcholy
—‖— cesta: cesta —‖—

rientovaný g. = digraf: hrany jsou uspořádané dvojice
ostupný g.: existuje orientovaná cesta z u do v
abě souvislý – symetrizace je souvislá → slabě souvislé kompon.
osažitelný směrem ven: existuje vrchol v, že každý vrchol u grafu je dostupný z v vzájemná dosažitelnost – u je dosaž. z v a naopak → relace $\approx$ → silně souvislé komp.
ndenzace: nahrazení silně s.k. vrcholem → vždy acyklický
ořenový strom: kořen v (není koncem hrany), každý vrchol je dosažitelný z v, každý vrchol kromě v je koncem právě

BFS: FIFO (fronta) DFS: LIFO (zásobník) – každý vrchol 1x, každá hrana 2x while (found ≠ ∅) {u = odeber z found, u.zpracován = 1, zpracuj u, foreach (u.hrany) {zpracuj hranu, pokud !w.zpracován, found.add(w)}}}
Dijkstra: k ~~hranám~~ uzlům píšu vzdálenost a předchozího, vždy beru vrchol s minimální zapsanou vzdáleností, když u souседů najdu větší vzd., nahradím ji a předchozího
Jarník: nepřipojené = V, while nepř. ≠ ∅ {u = odeber u s minimálním číslem, projdi sousedy u′, pokud u′ ∈ nepřipoj. ∧ číslo u′ > váha hrany u–u′, nahraď číslo délkou hrany a poznač u jako předchůdce}

topologické usp. digrafu: $(u,v) \in E_D \Rightarrow u < v$, musí být acyklický → prováděj DFS, když už není kam jít, poznač čas dokončení, topolog. usp. jsou pak ty prvky seřazené naopak
Kosarajův alg.: hledá silně souv. komp.: 1) proveď DFS a ulož časy dokončení 2) otoč hrany 3) vem nejvyšší čas d. a odtud dělej DFS – postupně všechny.

VÝROKOVÁ L. formule: výr. proměnné $\in \mathcal{X}$ + výrok. spojky
syntaxe: abeceda + gramatika $\varphi ::= 0 \mid 1 \mid x \mid \neg\varphi \ldots$
sémantika: ohodnocení proměnných + sémantika spojek
model formule: ohodnocení I, které splňuje φ $I \models \varphi$
splnitelnost: existuje model
platnost (tautologie): $\forall I: I \models \varphi$ $\models \varphi$ opakem neplatnost
nesplnitelnost (kontradikce): neexistuje model $\models \neg\varphi$
$\models \varphi \Leftrightarrow \neg\varphi$ je nesplnitelná splnitelná $\Leftrightarrow \not\models \neg\varphi$
MODUS PONENS: $(\models \varphi \wedge \models \varphi \to \delta) \to \models \delta$ odloučení
Jestliže prší, je mokro. Prší. → Tedy je mokro.
MODUS TOLLENS: $(\models \neg\varphi \wedge \models \delta \to \varphi) \to \models \neg\delta$
Jestliže prší, je mokro. Není mokro. → Tedy neprší.
NOR: $\downarrow$ NAND: $\uparrow$ úplný syst. spojek: všechna jde vyjádřit $\{\neg, \vee\}, \{\neg, \wedge\}, \{\neg, \to\}, \{\uparrow\}, \{\downarrow\}$
De Morgan. $\neg(x \wedge y) \Leftrightarrow \neg x \vee \neg y$ $\neg(x \vee y) \Leftrightarrow \neg x \wedge \neg y$
$x \to y \Leftrightarrow \neg x \vee y \Leftrightarrow \neg(x \wedge \neg y)$ $x \leftrightarrow y \Leftrightarrow (x \to y) \wedge (y \to x)$

NNF: pouze $\wedge, \vee$ a $\neg$ před proměnnými
DNF: disjunkce konjunkcí proměnných/negací $(\cdots \wedge \neg \cdots) \vee (\cdots \wedge \cdots)$
→ z tabulky: vezmu řádky, ve kterých vyšla 1 $\begin{array}{ccc|c} x & y & z & \varphi \\ 1 & 0 & 1 & 1 \end{array}$: $(x \wedge \neg y \wedge z)$
CNF: konjunkce disjunkcí —‖—
→ z tabulky: nulové řádky a otočit $\begin{array}{ccc|c} x & y & z & \varphi \\ 1 & 0 & 1 & 0 \end{array}$: $(\neg x \vee y \vee \neg z) \wedge \cdots$

Axiomy VL: $A \to (B \to A)$
$(A \to (B \to C)) \to ((A \to B) \to (B \to C))$
$(\neg B \to \neg A) \to (A \to B)$
+ modus ponens $(A \wedge (A \to B)) \to B$ odvozovací pravidlo
důkaz formule φ: sekvence formulí končící φ, kde je každá formule axiomem, nebo vznikla z předchozích formulí pomocí odvozovacích pravidel

PREDIK. LOG. termy: vznik z proměnných a funkcí výroky nahrazeny predikáty nad termy
abeceda: proměnné, log. spojky, kvantifik., závorky, funkční symboly a predikátové symboly s aritou (počet parametrů) + predikát. symbol rovnosti =
signatura: $\langle \mathcal{F}, \mathcal{P} \rangle$ gramatika: term $t ::= x \mid f(t_1, t_2 \ldots)$
+ atomické formule $\varphi_a ::= p(t_1, t_2 \ldots)$ + formule $\varphi ::= \varphi_a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \forall\varphi \ldots$
vázaný výskyt proměnné ve formuli: proměnná je použita v kvantifikátoru – někde nad ní je
volný —‖—: není nad ní žádný kvantifikátor → „formule o ní nějak mluví, něco pomocí ní do formule vstupuje.“ může mít ve formuli vázaný i volný výskyt!
uzavřené formule: $FREE(\varphi) = \emptyset$
sémantika je daná realizacemi $I = (D_I, \alpha_I)$ D_I = doména
α_I = ohodnocení: pro funkční symboly funkce $D_I^n \to D_I$
pro predik. symboly relaci $p_I \subseteq D_I^n$ (n je arita f.s./p.s.)
+ ohodnocení proměnných na hodnoty z D_I
sémantika formule φ: určuje, zda v dané realizaci I platí φ
model formule: realizace I, ve které φ platí $I \models \varphi$
splnitelnost: existuje model
logická platnost: formule platí ve všech možných realizacích
substituce termu t za proměnnou x ve formuli: všechny volné výskyty x se nahradí t, zápis $\varphi[x/t]$
substituovatelnost: t je substituovatelný za x v φ, pokud žádný volný výskyt x neleží v oboru platnosti $\forall/\exists y$, když je y proměnná obsažená v t ⇒ nechci dostat t někam, kde by najednou bylo vázané
→ platí důsledky: $\forall x \varphi \Rightarrow \varphi[x/t]$ pro každé x platí φ, pak φ platí, když za x dosadím cokoliv.
$\varphi[x/t] \Rightarrow \exists x \varphi$ pokud platí φ, když v ní nahradím x za t, určitě existuje x, pro které platí

teorie: formalizuje matematické struktury – většinou nás zajímá platnost formulí jen v určitých realizacích
→ signatura $\delta_T = \langle \mathcal{F}_T, \mathcal{P}_T \rangle$ + axiomy A_T omezující realizace
→ T-realizace: realizace jazyka se sig. δ_T splňující A_T:
$I \models \varphi_A$ pro všechny $\varphi_A \in A_T$
T-platnost: φ je T-platná, když platí ve všech T-realizacích
Axiomy PL: stejné jako u VL + schéma axiomů kvantifikátorů: $(\forall x(\varphi \to \delta)) \to (\varphi \to \forall x(\delta))$ + sch. ax. substituce: pokud $x \notin FREE(\varphi)$ $(\forall x \varphi) \to \varphi[x/t]$ + ax. rovnosti
odvozovací pravidla: modus ponens + prav. zobecnění $\varphi \Rightarrow \forall x \varphi$
důkaz formule φ z množiny předpokl. T: ... každá formule je axiomem, prvkem T nebo vznikl z předchozích aplikací pravidel $T \vdash \varphi$

Relace

$D(R)$: $a \in D(R) \Leftrightarrow \exists b: aRb$

$H(R)$: $b \in H(R) \Leftrightarrow \exists a: aRb$

Doplňková: $\overline{R} = A^2 \setminus R$

Inverzní: $R^{-1} = \{[a,b];\ [b,a] \in R\}$

$R \circ S = \{[a,c];\ \exists b: [a,b] \in S \wedge [b,c] \in R\}$

$(R \circ S) \circ T = R \circ (S \circ T)$ $\quad (R \circ S)^{-1} = S^{-1} \circ R^{-1}$

Speciálky:

R na A: $\forall a \in A: aRa$

S na A: $\forall a,b \in A: aRb \Rightarrow bRa$

T na A: $\forall a,b,c \in A: aRb \wedge bRc \Rightarrow aRc$

AS na A: $\forall a,b \in A: aRb \wedge bRa \Rightarrow a=b$

1 může být na diagonále, jinak nikde osově 1–1

AR na A: $\forall a \in A: a\overline{R}a$ $(\neg aRa)$

souvislá: $\forall a,b \in A: a \neq b \Rightarrow aRb \vee bRa$

trichotomická: $\forall a,b \in A: a=b \vee aRb \vee bRa$

sym. uzávěr: $\overleftrightarrow{R}$ $\quad$ Tranz. uz.: R^+

Ekvivalence:

RST, $a \in A$, $\overline{a} = \{x \in A;\ xRa\}$,

$S = \{\overline{a},\ a \in A\} = A/R$, faktorová množina

Uspořádání

Částečné: R, AS, T $\quad$ Kvazi: R, T $\quad$ Dobré: každá podmn. má nejmenší prv.

Úplné/lineární: každé dva prvky množiny jsou porovnatelné

Minimální prvek: $a \in M$, $\forall b \in M: b \preceq a \Rightarrow a \leq b$ $\quad a = b$

Maximální: $a \preceq b \Rightarrow b \preceq a$ $\quad a=b$ $\quad$ ŽÁDNÝ PRVEK NENÍ NAD/POD

Nejmenší: $\forall b \in M: \underline{a} \preceq b$ $\quad$ VŠECHNY PRVKY JSOU VĚTŠÍ/MENŠÍ

Největší: $\forall b \in M: b \preceq \underline{a}$

Pokrývá: $x \prec z$ $\quad \neg \exists z: y \preceq z \preceq x$

V SUPREMUM: nejmenší horní závora

Dolní závora: pro podmn. $A \subseteq M$: [illegible] prvek $x \in M$: $\forall y \in A: x \preceq y$

INFIMUM: největší dolní závora

Zobrazení

$[a,b] \in R \wedge [a,c] \in R \Rightarrow b = c$

Obraz množ.: $F(M) = \{b;\ \exists a \in M: f(a) = b\}$

Úplný vzor množ.: $F^{-1}(M) = \{a;\ \exists b \in M: f(a) = b\}$

INJEKCE = prosté: $\forall a,b \in D(f): a \neq b \Rightarrow f(a) \neq f(b)$

SURJEKCE = zobrazení Z NA: použije se všechno z Y,

$F: X \to Y \Rightarrow \forall y \in Y: \exists x \in X: f(x) = y$ | má to vzor

$\Rightarrow H(f) = Y$

ZOBR. DO: použije všechno z X: $D(f) = X$

ZOBR. NA: „bez Z", $D(f) = X \wedge H(f) = Y$

BIJEKCE: injekce, A na B, surjekce

každý prvek z Y má právě jeden vzor z X

Ekvivalentní množiny: $\exists$ bijekce $A \leftrightarrow B \Rightarrow A \sim B$

relace $\sim$: $a \sim b \Leftrightarrow f(a) = f(b)$, $\sim$ je ekv. na A,

$A/\sim = H(f)$

Operace

zobrazení $A \times A$ do A

(komutativní, asociativní) VIM

neutrální prvek: $e: \forall a \in A: a \circ e = e \circ a = a$

inverz: $a, a' \in A: a \circ a' = a' \circ a = e$

Binární operace na A má nejvíce 1 neutr. pr.

(důkaz sporem)

op. je asociativní $\wedge\ \exists e \Rightarrow$ každý prvek má maximálně 1 inverzní prvek

Algebry s jednou operací

GRUPOID: uzavřená

POLOGRUPA: uzavřená + asociativní

MONOID: uzavřená + asoc. + $\exists e$

GRUPA: uzav. + asoc. + $\exists e$ + každý prvek má inverz

s.: v řádku grupy každý prvek max. 1×, => zákon o krácení sudoku

Lagrangeova v.: Počet prvků podgrupy je dělitelem počtu prvků grupy.

$(H,\circ)$ je podgrupou $(G,\circ) \Leftrightarrow \forall a,b \in H: a \circ b^{-1} \in H$

$(H,\circ)$ je NORMÁLNÍ podg. $(G,\circ) \Leftrightarrow \forall a \in G: \forall b \in H: a \circ b \circ a^{-1} \in H$ $\quad$ Levý rozklad = pravý rozklad

Homomorfismy

$h: A \to B$, $(A,*)$, $(B,\circ)$ jsou grupy:

$h(a * b) = h(a) \circ h(b)$ pro $\forall a,b \in A$

MONOMORF.: injektivní (každé b má max. jedno a)

EPIMORF.: surjektivní (všechno z B)

IZOMORF.: bijektivní (všechno se někam přiřadí, jsou si moc podobné)

ENDOMORF: $A \to A$

AUTOMORF.: bijektivní $A \leftrightarrow A$

Kongruence:

$(X,\circ)$, R je ekvivalence na X

$[a,b] \in R \wedge [c,d] \in R \Rightarrow [a \circ c, b \circ d] \in R$

výsledek operace leží v relaci, když vstupy leží v relaci

rozklad $\mathbb{Z}$ na zb. třídy po dělení m:

$a \equiv b \pmod m$ – dvě čísla jsou ekv. mod m, když mají stejný zbytek po dělení m

je kongr. k $+, -, \cdot$ $\quad a \equiv b \wedge c \equiv d \Rightarrow a+c \equiv b+d$

$(G,\circ)$, R je kongr. na G, e je neutr. pr.

$(H,\circ)$, $H = \{x;\ x \in G \wedge [x,e] \in R\}$ je normální podgr

?

Svazy

množina je svazově uspořádaná, když pro každou dvouprvkovou mn. obsahuje supremum i infimum

$\wedge$: průsek $\quad \vee$: spojení

$x \vee x = x \wedge x = x$ $\quad$ idempotence

$x \vee y = y \vee x$; $x \wedge y = y \wedge x$ $\quad$ komut.

asoc.

$x \wedge (x \vee y) = x$, $\quad x \vee (x \wedge y) = x$

$(X, \vee_X, \wedge_X)$, $(Y, \vee_Y, \wedge_Y)$ je podsvaz, když

$x \vee_Y y = x \vee_X y = \text{supremum}(x,y)$

$x \wedge_Y y = x \wedge_X y = \text{infimum}(x,y)$

$F: X \to Y$, $F(x \vee_X y) = f(x) \vee_Y f(y) \Rightarrow$ izomorf

(Výr)okový výrok – má smysl uvažovat o pravdivosti
– každá dva nezávislé
=> výroková proměnná $\in \mathbb{X}$

(F)ormule: výrok. proměnné + výrok. spojky
-> pravdivostní hod. dána ohodnocením výrok. prom.

$\varphi := 0 \mid 1 \mid X \mid (\neg\varphi_1) \mid$
$(\varphi_1 \wedge \varphi_2) \mid (\varphi_1 \vee \varphi_2) \mid$
$(\varphi_1 \rightarrow \varphi_2) \mid (\varphi_1 \Leftrightarrow \varphi_2)$

(S)yntaxe: abeceda + gramatika
$1, 0, \neg, \wedge, \vee, \rightarrow, \Leftrightarrow$ a $\mathbb{X}$

(S)émantika: co fráze znamenají, ve výrok. logice dané tabulkou
(M)odel formule: ohodnocení I, které splňuje φ

$I \models \varphi$

-> opak: $I \not\models \varphi$

(S)plnitelnost: existuje model
-> množina formulí je splnitelná, když je splnitelná jejich $\wedge$

$\exists I \left(I \models \bigwedge_{\varphi_i \in F} \varphi_i \right)$

(P)latnost: $\forall I : I \models \varphi$, značíme $\models \varphi$
(tautologie)
-> opak: $\exists I : I \not\models \varphi$, značíme $\not\models \varphi$
neplatnost

(N)esplnitelnost: neexistuje model: $\models \neg\varphi$
(P)latné $\varphi \Leftrightarrow$ nesplnitelné $\neg\varphi$
(S)plnitelné $\varphi \Leftrightarrow$ neplatné $\neg\varphi$

(S)ubstituce: $\models \varphi(x_1, x_2 \dots) \Leftrightarrow \models \varphi(\delta_1, \delta_2, \dots)$

(M)odus ponens: pravidlo odloučení
Jestliže prší, je mokro. $\wedge$ Prší. => Prší, tedy je mokro.
$\models \varphi \wedge \models \varphi \rightarrow \delta \Rightarrow \models \varphi$

(M)odus tollens: pravidlo popření
Jestliže prší, je mokro. $\wedge$ Není mokro. => Není mokro, (…)
$\models \neg\delta \wedge \models \varphi \rightarrow \delta \Rightarrow \models \neg\varphi$

NNF: pouze $\wedge, \vee, \neg$, vyjádřit $\Leftrightarrow, \rightarrow$ pomocí známých vztahů a u $\neg(\dots)$ De Morgan

Disjunktní NF: disjunkce konjunkcí literálů (prom. nebo její negace) $(\dots\wedge\dots) \vee (\dots\wedge\dots) \vee \dots$
1) převést do NNF 2) použít distributivitu
z tabulky ez: jedničkové řádky: $\begin{matrix} x & y & z \\ 1 & 0 & 1 \end{matrix} \Big| \begin{matrix} \varphi \\ 1 \end{matrix} \Rightarrow (x \wedge \neg y \wedge z) \vee \dots$

Konjunktivní NF: konjunkce disjunkcí literálů
z tabulky: nulové řádky a otočit: $\begin{matrix} x & y & z \\ 0 & 1 & 1 \end{matrix} \Big| \begin{matrix} \varphi \\ 0 \end{matrix} \Rightarrow (x \vee \neg y \vee \neg z) \wedge \dots$

úplný sys. logických spojek:
množina spojek taková, že TÍM JDE VŠECHNO VYJÁDŘIT
$\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \rightarrow\}$, $\{\uparrow\}$, $\{\downarrow\}$
neúplné jsou všechny podmn. $\{\vee, \wedge, \rightarrow, \Leftrightarrow\}$ (chybí $\neg$)

XOR: $\oplus$, $\varphi \oplus \delta \Leftrightarrow \neg(\varphi \Leftrightarrow \delta)$
NOR: Peirceova šipka $\downarrow$: $\varphi \downarrow \delta \Leftrightarrow \neg(\varphi \vee \delta)$
NAND: Shefferův op. $\uparrow$: $\varphi \uparrow \delta \Leftrightarrow \neg(\varphi \wedge \delta)$

Booleova algebra: distributivní komplementární svaz
$(\{0,1\}, \wedge, \vee, \neg, 0, 1)$
ASOCIATIVITA: $x \wedge (y \wedge z) \Leftrightarrow (x \wedge y) \wedge z$
$x \vee (y \vee z) \Leftrightarrow (x \vee y) \vee z$
DISTRIBUT.: $x \wedge (y \vee z) \Leftrightarrow (x \wedge y) \vee (x \wedge z)$
$x \vee (y \wedge z) \Leftrightarrow (x \vee y) \wedge (x \vee z)$
KOMPLEMENT.: $x \wedge \neg x \Leftrightarrow 0$, $x \vee \neg x \Leftrightarrow 1$
KOMUTAT.: $x \vee y = y \vee x$, $x \wedge y = y \wedge x$
NEUTRALITA: $x \vee 0 \Leftrightarrow x$, $x \wedge 1 \Leftrightarrow x$
ANIHILACE: $x \vee 1 \Leftrightarrow 1$, $x \wedge 0 \Leftrightarrow 0$
IDEMPOTENCE: $x \vee x = x \wedge x = x$
De Morgan: $\neg(x \wedge y) = \neg x \vee \neg y$
$\neg(x \vee y) = \neg x \wedge \neg y$

co říct na SZZ:
$x \rightarrow y \Leftrightarrow \neg x \vee y \Leftrightarrow \neg(x \wedge \neg y)$
$x \Leftrightarrow (…) \Leftrightarrow (x \rightarrow y) \wedge (y \rightarrow x)$

Axiomy výrokové logiky:
$A \rightarrow (B \rightarrow A)$
$(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
$(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$
+ modus ponens – odvozovací pravidlo

Axiomy predikátové logiky:
$(\forall x (\varphi \rightarrow \delta)) \rightarrow (\varphi \rightarrow (\forall x \delta))$
$(\forall x \varphi) \rightarrow \varphi[x/t]$ (t je substituovat.)
$\varphi \rightarrow \forall x \varphi$: pravidlo zobecnění
+ modus ponens + výrokové axiomy

důkazy formulí v PL jsou nad předpoklady T
$T \vdash \varphi$

entity = univerza = termy - vznik z proměnných a funkcí

výroky jsou nahrazeny predikáty nad termy

kvantifikátory - $\forall x$, $\exists x$

abeceda PL: logické spojky, proměnné, kvantifikátory, závorky

- funkční symboly: $\mathcal{F}$, arita /x = počet argumentů, /0 => konstanta
- predikátové symboly: $\mathcal{P}$, arita /x
- predikátový symbol rovnosti =

signatura: dvojice $\langle \mathcal{F}, \mathcal{P} \rangle$ => jazyk (+ jestli existuje =)

: Peanova aritmetika: $\langle \{0/0, S/1, +/2, \cdot/2\}, \emptyset \rangle$

gramatika: term $t ::= x \mid f(t_1, t_2, \dots, t_n)$

atomická formule: $\varphi_A ::= p(t_1, t_2, \dots, t_n)$

formule: $\varphi ::= \varphi_A \mid (\neg\varphi_1) \mid \dots \mid (\forall x \varphi_1) \mid (\exists x \varphi_1)$

výskyt ve formuli: vázaný x volný

- prom. může mít v jedné form. vázaný i volný výskyt

uzavřená formule = výrok <=> $FREE(\varphi) = \emptyset$

realizace: $I = (D_I, \alpha_I)$: doména (neprázd. mnž.)

+ ohodnocení: $\forall f/n \in \mathcal{F} : (f_I : D_I^n \to D_I) \in \alpha_I$ pro f.s. funkce

: např. $\alpha_I(+) = \{(0,0) \to 0, (1,0) \to 1, (2,3) \to 5\}$

$\alpha_I(\pi) = \{() \to 3{,}141592653\}$

$\forall p/n \in \mathcal{P} : (p_I \subseteq D_I^n) \in \alpha_I$ pro p.s. relace

: např. $\alpha_I(even/1) = \{0, 2, 4 \dots\}$

$\forall x \in \mathcal{X} : (x_I \in D_I) \in \alpha_I$ ohodnocení proměnných

sémantika závisí na konkrétní realizaci, určuje, jestli v ní formule platí, nebo ne: $I \models \varphi$

model formule: realizace I taková, která splňuje φ ($I \models \varphi$)

logicky platná formule: platí ve všech realizacích jazyka

(1) $\forall x \varphi \Leftrightarrow \neg\exists x (\neg\varphi)$ $\exists x \varphi \Leftrightarrow \neg\forall (\neg\varphi)$

(2) $\forall x \varphi \Leftrightarrow \varphi$, $\exists x \varphi \Leftrightarrow \varphi$ pokud $x \notin FREE(\varphi)$

(3) $\forall x (\varphi \vee \delta) \Leftrightarrow (\forall x \varphi) \vee \delta$ pokud $x \notin FREE(\delta)$

$\exists x (\varphi \wedge \delta) \Leftrightarrow (\exists x \varphi) \wedge \delta$ — || — δ

(4) $\forall x (\varphi \to \delta) \Leftrightarrow (\exists x \varphi) \to \delta$ — || — δ

$\exists x (\varphi \to \delta) \Leftrightarrow (\forall x \varphi) \to \delta$ — || — δ

(5) $\forall x (\varphi \to \delta) \Leftrightarrow \varphi \to (\forall x \delta)$ pokud $x \notin FREE(\varphi)$

$\exists x (\varphi \to \delta) \Leftrightarrow \varphi \to (\exists x \delta)$ — || — φ

(6) $(\forall x (P(x))) \wedge (\forall y (Q(y))) \Leftrightarrow \forall x (P(x) \wedge Q(x))$

$x \in FREE(\varphi)$ -> „formule φ o x nějak mluví" není t pro ni jen nějaký iterátor

častý zápis $\varphi(x_1, \dots, x_n)$ když $FREE(\varphi) \subseteq \{x_1, \dots, x_n\}$

$(\exists x (\varphi(x))) \vee (\exists y (\delta(y))) \Leftrightarrow \exists x (\varphi(x) \vee \delta(x))$ $x \notin FREE(\dots$

„$\exists$ je jaksi asociativní s $\vee$, je to jakoby nekonečná disjunkce, totéž $\forall$ s $\wedge$"

substituce: všechny volné výskyty proměnné nahradím termem

substituovatelnost: $[x/t]$ v φ když žádný VOLNÝ výskyt x ve φ neleží v oboru platnosti kvant. $\exists/\forall y$, když y je proměnná obsažená v t => nechci dostat t někam, kde by najednou bylo vázané

hnusná sémantika

pokud $[x/t]$ je substit. v φ: $\forall x \varphi \Rightarrow \varphi[x/t]$ $\varphi[x/t] \Rightarrow \exists x \varphi$

můžu si nějaké x vybrat a bude to platit

pokud pro každé x platí φ, pak φ platí, když za x dosadím „cokoliv"

pokud platí φ, když v ní x nahradím za t, pak určitě existuje x, pro které pl…