Uvod u matematičku logiku

Milenko Mosurović

Univerzitet Crne Gore

studijska godina 2020/21.

Šta proučavamo

Proučavamo iskaznu i predikatsku logiku prvog reda.

I kod iskazne i kod predikatske logike proučavamo 4 cjeline

1. Sintaksa (tj. koje simbole koristimo to nazivamo jezikom, koji su važeći nizovi simbola i to nazivamo formulama)
2. Semantika (tj. kako interpretiramo formule odnosno određujemo njihovo značenje tj. istinitosnu vrijednost).
3. Formalni pristup (na osnovu aksioma i pravila izvođenja dolazimo do istina). Napomena: u udžbeniku se ovo naziva sintaksa - sintaksni pristup.
4. Odnos 2 i 3 (da li nam semantički pristup i formalni pristup daju iste istine - Teorema korektnosti i Teorema potpunosti).

PREDIKATSKA LOGIKA PRVOG REDA

Predikatska logika-uvod

- Koristimo kraći naziv "predikatska logika" ili oznaku "PL" umjesto "predikatska logika prvog reda".
- Postoji i predikatska logika drugog reda koju mi nećemo proučavati pa nas kraći naziv neće dovesti do zabune.
- Iskazna logika ima ograničenu ekspresivnost tj. pomoću formula iskazne logike ne možemo zapisati mnoga matematička tvrđenja.
- Zato iskaznu logiku u nekom smislu proširujemo sa npr. kvantifikatorima ($\forall x$, $\exists x$).
- U iskaznoj logici elementarne iskaze smo zamijenili slovima a u PL možemo u nekom smislu da zapišemo i njihovu strukturu npr. pišemo $\exists x(x^2 + 1 = 0)$ umjesto slova s_i.
- Formulama PL možemo zapisati zakone matematičkih struktura pa je i interpretiramo koristeći matematičke strukture.

Primjeri matematičkih struktura i formula

- Koristimo skraćenicu MS umjesto "matematičke strukture".
- Umjesto MS koristi se i samo naziv "struktura".
- Intuitivno MS zadajemo: nepraznim skupom, kao i skupovima relacija, operacija i istaknutih elemenata zadatog skupa.
- Za sada navodimo primjere a kasnije precizne definicije.
- **Pr1**. Grupa je MS $\mathbb{G} = (G, *, e)$, gaje je $G \neq \emptyset$, $*$ binarna operacija skupa G i $e \in G$ istaknuti element, za koju važi: 1^o) operacija $*$ je asocijativna, 2^o) e je jedinični (neutralni) element 3^o) svaki element grupe ima inverzni (suprotni) element. Tako, MS $\mathbb{Z} = (Z, +, 0)$, gdje je Z skup cjelih brojeva ... je grupa. Grupa je i MS $\mathbb{Q} = (Q \backslash \{0\}, \cdot, 1)$, gdje je Q skup racionalnih brojeva.

  Asocijativnost operacije $*$ možemo zapisati formulom $\forall x \forall y \forall z \,((x * y) * z = x * (y * z))$.

- **Pr2**. Grupu $\mathbb{G}$ nazivamo komutativnom grupom ili Abelovom grupom ako je operacija $*$ komutativna tj. za operaciju $*$ važi zakon komutativnosti koji možemo zapisati formulom: $\forall x \forall y\,(x * y = y * x)$.
- **Pr3**. Polje je struktura $\mathbb{F} = (F, +, \cdot, 0, 1)$ sa nepraznim skupom F, binarnim operacijama $+$, $\cdot$ i dva istaknuta elementa 0, 1. Pri tome važi I) struktura $(F, +, 0)$ je Abelova grupa, II) struktura $(F \setminus \{0\}, \cdot, 1)$ je Abelova grupa, III) Operacija $\cdot$ je distributivna u odnosu na operaciju $+$.
- **Pr4**. Linearno uređenje je struktura $\mathbb{P} = (P, <)$ sa nerefleksivnom, tranzitivnom i linearnom relacijom $<$ nepraznog skupa P.
- **Pr5**. Uređeno polje je struktura $\mathbb{F} = (F, +, \cdot, <, 0, 1)$, gdje je struktura $\mathbb{F} = (F, +, \cdot, 0, 1)$ polje a $<$ je binarna relacija skupa F koja je saglasna sa obje operacije i takva da je struktura $(F, <)$ linearno striktno uređenje bez krajeva.

MS – Relacije, operacije i istaknuti elementi

- Neka je M neprazan skup.
- Skup $M^n = M \times \cdots \times M = \{(x_1, \ldots, x_n) \ : \ x_1, \ldots, x_n \in M\}$ je Dekartov n-ti stepen skupa M, za svako $n \geq 0$.
- Uzimamo $M^1 = M$; $\quad M^0 = \{\lambda\}$, gdje je λ prazan niz. Umjesto λ koriste se i druge oznake poput: $()$, $\emptyset$, ε i sl.
- **Def**. Element $c \in M$ je istaknuti element skupa M.
- **Def**. Relacija dužine n skupa M je skup r takav da je $r \subset M^n$.
- Umjesto $(x_1, \ldots, x_n) \in r$ koristimo i oznaku $r(x_1, \ldots, x_n)$. Dok za $n = 2$ umjesto $(x, y) \in \rho$ često pišemo $x \, \rho \, y$, npr. $x < y$.
- Relaciju $r \subset M^n$ može shvatiti i kao preslikavanje $r : M^n \to \{0, 1\}$ takvo da za sve $x_1, \ldots, x_n \in M$, $r(x_1, \ldots, x_n) = 1 \Leftrightarrow (x_1, \ldots, x_n) \in r$. Specijalno za $n = 0$ skup $M^0 = \{\lambda\}$ je jednočlan skup pa postoje dvije relacije dužine 0, označimo ih sa $\overline{0}$ i $\overline{1}$ i uzimamo $\overline{0}(\lambda) = 0$, $\overline{1}(\lambda) = 1$.

Na relacije $\overline{0}$ i $\overline{1}$ možemo gledati kao na neistinu i istinu.

- **Def**. Operacija dužine $k \geq 0$ skupa M je preslikavanje $f : M^k \to M$.
- Ako je $k = 0$ onda za svako $c \in M$ imamo operaciju $\overline{c} : M^0 \to M$ oderđenu sa $\overline{c}(\lambda) = c$. Ako identifikujemo c i $\overline{c}$, istaknuti element je operacija dužine nula skupa M.
- Ako je $k = 2$ umjesto $f(x, y)$ obično pišemo $x\,f\,y$, npr. $x + y$.
- Operaciji f dužine k možemo pridružiti relaciju r_f dužine $n = k + 1$ tako da za sve $x_1, \ldots, x_k, y \in M$ važi:
  $r_f(x_1, \ldots, x_k, y) \Leftrightarrow f(x_1, \ldots, x_k) = y$.

  Relacija r_f zadovoljava funkcionalne uslove tj. za svaku k-torku $(x_1, \ldots, x_k)$ postoji tačno jedno y tako da je $r_f(x_1, \ldots, x_k, y)$.
- Ako relacija r dužine $n \geq 1$ zadovoljava funkcionalne uslove onda joj možemo pridružiti operaciju dužine $k = n - 1$.

- **Def**. U opštem slučaju pod matematičkom strukturom podrazumjevamo matematički objekt koji sadrži sledeće komponente:
  1. Neprazan skup M koji nazivamo domenom strukture,
  2. Skupove relacija, operacija i istaknutih elemenata skupa M.
- Naveli smo definiciju MS u opštem slučaju. Naime skupovi relacija, operacija i istaknutih elemenata skupa M mogu biti prazni pa ih možemo i izostaviti.
- MS u opštem slučaju zapisujemo kao niz $\mathbb{M} = (M, \mathcal{R}, \mathcal{F}, \mathcal{C})$, gdje je M neprazan skup, $\mathcal{R}$ skup relacija, $\mathcal{F}$ skup operacija i $\mathcal{C}$ skup istaknutih elemenata skupa M. Pri tome u nizu navodime elemente skupova $\mathcal{R}, \mathcal{F}$ i $\mathcal{C}$ a ne same skupove.
- Kao što je ranije naznačeno operacije i istaknuti elementi su samo specijalan slučaj relacija. Pa smo mogli MS zadati kao domen i skup relacija na domenu. Ipak operacije i istaknute elemente izdvajamo zbog njihove važnosti u matematici.

Sintaksa PL

Da bi definisali sintaksu PL treba da definišemo:

1. Jezik PL. Tj. treba da navedemo simbole koje možemo da koristimo. Imamo logičke simbole-koje stalno koristimo u svim PL i nelogičke simbole-koji biramo prema potrebi.
2. Važeće nizove simbola (riječi) tj. formule PL. U PL imamo i "pomoćne" nizove simbola koji su važeći to su termi. Dakle, treba definisati terme i formule PL.

Jezik PL

- Neka je $V = \{v_0, v_1, \dots\}$ prebrojiv skup. Nazivamo ga skupom simbola individualnih promenljivih.
- Neka je dalje skup interpunkcijskih simbola $\hat{I} = \{(,)\} \cup \{,\}$ (tj. otvorena zagrada, zatvorena zagrada i zarez).
- Skup logički simboli jezika PL je: $\mathcal{L}_0 = V \cup \{\wedge, \vee, \rightarrow, \neg\} \cup \{\forall x : x \in V\} \cup \{\exists x : x \in V\} \cup \{=\} \cup \hat{I}$.

- Skup nelogičkih simbola jezika PL (ovi simboli određuju jezik) čine simboli relacija, operacija i istaknutih elemenata.
- Preciznije skup nelogičkih simbola jezika PL je $R \cup F \cup C$, gdje je
  - R skup simbola relacija-pri tome svaki simbol ima svoju dužinu,
  - F skup simbola operacija-pri tome svaki simbol ima svoju dužinu i
  - C skup simbola istaknutih elemenata.

  Pri tome skupovi R, F i C mogu biti i prazni.
- **Def**. Jezik PL u opštem slučaju je skup $\mathcal{L} = \mathcal{L}_0 \cup R \cup F \cup C$, gdje $\mathcal{L}_0$, R, F i C označavaju prethodno opisane skupove.
- Napomena. Pošto se $\mathcal{L}_0$ javlja u svakom jezicima obično se on podrazumjeva pa se kao simboli jezika navode samo simboli iz $R \cup F \cup C$.

- Ranije smo naveli primjere MS. Da bi formulama PL mogli da zapišemo svojstva tih stuktura preba da imamo odgovarajuće simbole tj. odgovarajući jezik.
- **Pr1**. Da bi zapisali svojstva grupe $\mathbb{G} = (G, *, e)$ možemo koristiti jezil $\mathcal{L}_G = \{*, e\}$, gdje je $*$ simbol binarne operacije, a e simbol istaknutog elementa.
  Uočimo da nam u ovom slučaju nisu potrebni simboli relacija. Simbol $*$ binarne operacije može "odgovarati" operaciji sabiranja u grupi $\mathbb{Z} = (Z, +, 0)$ ili operaciji množenja u grupi $\mathbb{Q} = (Q \setminus \{0\}, \cdot, 1)$.
- Jezik sa jednim simbolom binarne relacije i jednim simbolom istaknutog elementa poput jezika $\mathcal{L}_G = \{*, e\}$ možemo nazivati jezik teorije grupa. Naime u njemu možemo zapisati svojstva grupe. Mogli smo uzeti i $\mathcal{L}_G = \{+, 0\}$.
- **Pr2**. Slično prethodnom jezik $\mathcal{L}_F = \{+, \cdot, 0, 1\}$, gdje su $+$, $\cdot$ binarne operacije a 0 i 1 istaknuti elementi čini jezik teorije polja.

- **Pr3**. Jezik $\mathcal{L}_{FO} = \{+, \cdot, <, 0, 1\}$, gdje su $+$, $\cdot$ binarne operacije, $<$ binarna relacija a 0 i 1 istaknuti elementi čini jezik teorije uređenih polja.

- Prethodno smo dali definiciju jezika PL i objasnili kroz primjere. Sada ponavljamo glavnu definiciju koja obuhvata prethodno rečeno ali sažeto.

Jezik PL -kratko

- **Def**. Neka je $V = \{v_0, v_1, \ldots\}$ skup simbola individualnih promenljivih i $\hat{I} = \{(,)\} \cup \{,\}$ skup interpunkcijskih simbola. Jezik PL je skup $\mathcal{L} = \mathcal{L}_0 \cup R \cup F \cup C$, gdje je
  - $\mathcal{L}_0 = V \cup \{\wedge, \vee, \rightarrow, \neg\} \cup \{\forall x : x \in V\} \cup \{\exists x : x \in V\} \cup \{=\} \cup \hat{I}$.
  - R skup simbola relacija (tj. predikata) sa zadatim dužinama,
  - F skup simbola operacija (tj. funkcija) sa zadatim dužinama, i
  - C skup simbola istaknutih elemenata.

Termi i formule PL

- Kao što je prethodno rečeno PL ima dvije vrste sintaksnih objekata: terme i formule.
- **Pr**. Formula $\forall x \forall y\,(x + y = y + x)$ predstavlja zakon komutativnosti i možemo postaviti pitanje njene istinitnosne vrijednosti. Dio formule $x + y$ učestvuje u njenoj izgradnji ali pitanje istinitnosne vrijednosti za $x + y$ nema smisla. Možemo govoriti o vrijednosti izraza $x + y$ npr. za $x = 5$ i $y = 7$.

- Neka je dat jezik $\mathcal{L} = \mathcal{L}_0 \cup R \cup F \cup C$.
- **Def**. Skup terma jezika $\mathcal{L}$ je minimalni skup konačnih nizova simbola (jezika $\mathcal{L}$) koji zadovoljava sledeće uslove:
  1. Simboli individualnih promenljivih i simboli konstanti su termi tj. $v \in V$ i $c \in C$ su termi.
  2. Ako su $t_1, \ldots, t_k$ termi i $f \in F$ operacijski simbol dužine $k \geq 1$, onda je i $f(t_1, \ldots, t_k)$ term.

- **Def**. Formule jezika $\mathcal{L}$ su konačni nizovi simbola (jezika $\mathcal{L}$) i definišemo ih induktivno na sledeći način:
  1. Ako su t_1 i t_2 termi onda je $(t_1 = t_2)$ formula,
  2. Ako su $t_1, \cdots, t_n$ termi i $r \in R$ relacijski simbol dužine $n \geq 1$ onda je $r(t_1, \cdots, t_n)$ formula,
  3. Ako su A i B formule onda su i $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $\neg A$ formule,
  4. Ako je A formula a $x \in V$ individualna promenljiva onda su i $\forall x\, A$, $\exists x\, A$ formule.
  5. Formule se mogu dobiti samo na jedan od prethodno navedenih načina.

- Formule oblika $(t_1 = t_2)$ i $r(t_1, \cdots, t_n)$, tj. one koje su u definiciji navedene pod 1 i 2, nazivamo elementarne formule.
- Elementarne formule u suštini predstavljaju bazu pri induktivnom konstruisanju formula.
- U definicijama terma i formula zahtjevamo $k \geq 1$ i $n \geq 1$.

- Kao kod iskazne logike dogovaramo se da odstupamo od stroge definicije formule ako je iz zapisa jasno o kojoj formuli se radi npr. spoljne zagrade možemo izostaviti.
- **Pr1**. U jeziku $\mathcal{L}_G = \{+, 0\}$ možemo zapisati formule:
  $\forall x(x + 0 = x) \wedge \forall x(0 + x = x)$ - 0 je neutralni element
  $\forall x \exists y((x + y = 0) \wedge (y + x = 0))$ - svaki element ima inverzni
- **Pr2**. Formula $\forall x(\neg(x = 0) \to \exists y(x \cdot y = 1))$ nije formula jezika $\mathcal{L}_G$ ali jeste formula jezika $\mathcal{L}_F = \{+, \cdot, 0, 1\}$. Riječima prepričana formula: Svaki element različit od 0 ima inverzni u odnosu na operaciju "$\cdot$".
- **Def**. Skup podformula formule A, u oznaci $sub(A)$, definišemo indukcijom (po složenosti formule) na sledeći način:
  $sub(t_1 = t_2) = \{t_1 = t_2\}$;
  $sub(r(t_1, \cdots, t_n)) = \{r(t_1, \cdots, t_n)\}$;
  $sub(A \star B) = sub(A) \cup sub(B) \cup \{A \star B\}$, za $\star \in \{\wedge, \vee, \to\}$;
  $sub(Q\, A) = sub(A) \cup \{Q\, A\}$, za $Q \in \{\neg, \forall x, \exists x\}$.

Parametri formula

- U predikatskim formulama razlikuju se individualni simboli (tj. promjenljive) na koje "djeluje" neki kvantifikator, od onih na koje ne "djeluje" ni jedan kvantifikator.
- U formuli oblika QyA, formula A je oblast kvantifikatora Qy za $Q \in \{\exists, \forall\}$ i $y \in V$.
- **Def**. Javljanje promjenljive y je vezano u formuli A ako se y nalazi u oblasti kvantifikatora Qy. U suprotnom to javljanje je slobodno. ⌈ javljanje y u Qy ne računamo kao jvljanje ⌋

  Promjenljiva x je parametar (slobodna promjenljiva) formule A ako ima slobodno javljanje u formuli A.
- **Pr**. U formuli $\forall x(x+0=x) \wedge \exists y(x+y=0)$ prvo i drugo javljanje x je vezano a treće slobodno a javljanje y je vezano.
- Koristimo oznake: $A(x_1, \ldots, x_n)$ i $t(x_1, \ldots, x_n)$ da označimo da su svi parametri formule A i terma t među $x_1, \ldots, x_n$.

- **Pr1**. Formula $A = \forall x \forall y(x + y = y + x)$ nema parametara i izražava zakon komutativnosti.
  Formula $B(y) = \exists x(y = x + x)$ ima jedan parametar y i izražava relaciju "y je paran broj".
- **Pr2**. Formule $A(x, y, z) = \exists u(x = z \cdot u) \wedge \exists u(y = z \cdot u)$ i $B(x, y, z, v) = (\,\exists u(x = v \cdot u) \wedge \exists u(y = v \cdot u)\,) \rightarrow \exists u(z = v \cdot u)$ imaju parametre i označavaju redom da z djeli x i y i ako je v djelilac od x i y onda je djelilac i od z. Tako formula $A(x, y, z) \wedge \forall v B(x, y, z, v)$ označava $z = NZD(x, y)$.
- **Def**. Promjenljiva y je slobodna za promjenljivu x u formuli A ako x nema slobodno javljanje u oblasti kvantifikatora Qy u formuli A.
- Prethodna definicija znači da y možemo staviti umjesto x u formuli A tj. x možemo zamjeniti sa y.
- Term $t(x_1, \ldots, x_n)$ je slobodan za promjenljivu x u formuli A ako su sve promjenljive $x_1, \ldots, x_n$ slobodne za promjenljivu x u formuli A.

Semantika PL

- Intuitivno: Najmanji sintaksni objekat koji dobija istinitosnu vrijednost u iskaznoj logici je iskazna promjenljiva, a u PL je to predikat sto je u direktnoj vezi sa nazivima ovih logika.
- Za PL treba da odredimo kako da tumačimo: 1^o) simbole jezika - nelogičke (pa uvodimo interpretaciju); 2^o) individualne simbole jezika i treme (pa uvodimo valuaciju i vrijednost terma); 3^o) formule tj. logičke veznike (pa uvodimo relaciju istinitosti).

Interpretacija jezik PL

- Ako je dat neprazan skup M onda je
  - $Rel(M) = \bigcup_{n\in\mathbb{N}}\{r : r \subset M^n\}$ - skup svih relacija skupa M,
  - $Fun(M) = \bigcup_{k\in\mathbb{N}}\{f | f : M^k \to M\}$ - skup svih operacija (funkcija) skupa M,
  - M - skup svih (istaknutih) elemenata skupa M.

- **Def**. Interpretacija jezika $\mathcal{L} = \mathcal{L}_0 \cup R \cup F \cup C$ na nepraznom skupu M je preslikavanje

$$I \ : \ R \cup F \cup C \to Rel(M) \cup Fun(M) \cup M, \qquad \text{koje:}$$

  - svakom relacijskom simbolu $r \in R$ pridružuje relaciju $I(r) \in Rel(M)$ iste dužine kao r;
  - svakom simbolu operacije $f \in F$ pridružuje operaciju $I(f) \in Fun(M)$ iste dužine kao f;
  - svakom simbolu istaknutog elementa $c \in C$ pridružuje element $I(c) \in M$.
- Napomena. Smatramo da je interpretacija proširena i na simbol jednakosti $= \in \mathcal{L}_0$ sa $I(=) = \{(x, x) \ : \ x \in M\}$. Znači simbol jednakosti se uvjek interpretira kao jednakost.
- **Def**. Interpretacija I jezika $\mathcal{L}$ određuje strukturu $\mathbb{M}_I = (M, I(R), I(F), I(C))$ koju nazivamo model jezika $\mathcal{L}$.
- Klasu svih modela jezika $\mathcal{L}$ označavamo sa $Mod(\mathcal{L}) = \{\mathbb{M}_I \ : \ \mathbb{M}_I - \text{model za } \mathcal{L}\}$.

- Ako imamo jezik $\mathcal{L}$ moguće je napraviti novi jezik izostavljanjem nekih simbola ili dodavanjem novih simbola. U tom slučaju govorimo o redukciji odnosno proširenju jezika $\mathcal{L}$.
- Ako je $\mathcal{L} \subset \mathcal{L}'$ onda je $\mathcal{L}'$ proširenje jezika $\mathcal{L}$ dok je jezik $\mathcal{L}$ redukcija jezika $\mathcal{L}'$.
- Možemo govoriti o redukciji i ekspanziji modela. Ako je $\mathbb{M}$ model za jezik $\mathcal{L}$ a $\mathbb{M}'$ model za jezik $\mathcal{L}'$ i ako je $\mathcal{L} \subset \mathcal{L}'$ onda je $\mathbb{M}$ redukcija modela $\mathbb{M}'$ dok je $\mathbb{M}'$ ekspanzija modela $\mathbb{M}$.
- **Pr**. Jezik teorije polja $\mathcal{L}_F = \{+, \cdot, 0, 1\}$ je proširenje jezika teorije grupa $\mathcal{L}_G = \{+, 0\}$. Pa je model $\mathbb{Q}_F = (Q, +, \cdot, 0, 1)$ ekspanzija modela $\mathbb{Q}_G = (Q, +, 0)$, gdje je Q skup racionalnih brojeva a $+, \cdot$ operacije sabiranja i množenja racionalnih brojeva i 0, 1 redmo nula i jedinica iz skupa Q.
- Napomena. U primjeru se simbol $+$ interpretira kao operacija sabiranja dok simbol $\cdot$ se interpretira kao operacija množenja a simboli 0 i 1 kao racionalne konstante nula i jedan.

Valuacija i vrijednost terma

- **Pr**. Istinitost formule $x+y=z$ zavisi od vrijednosti x,y,z,$x+y$. Npr. $2+3=5$ je tačno, dok $2+3=7$ je netačno u skupu prirodnih brojeva. Dakle treba zadati vrijednosti individualnih simbola (poput x,y) i odrediti vrijednost terma (poput $x+y$) da bi provjerili istinitost formule.
- Neka je $\mathbb{M}=(M, I(R), I(F), I(C))$ model jezika $\mathcal{L}=R\cup F\cup C$.
- **Def**. Valuacija individualnih simbola u modelu $\mathbb{M}$ je niz $a=(a_0, a_1, \dots)$ elemenata skupa M.
  Sa M^N označavati skup svih valuacija modela $\mathbb{M}$.
- **Def**. Vrijednost terma t za valuaciju a u modelu $\mathbb{M}$, u oznaci $[t]_a^M$, definišemo induktivno po složenosti terma t:
  - $[v_n]_a^M = a_n$ za svako $v_n\in V$,
  - $[c]_a^M = c_M$ za svaki simbol $c\in C$, gdje je $c_M = I(c)\in M$,
  - $[f(t_1,\dots,t_k)]_a^M = f_M([t_1]_a^M,\dots,[t_k]_a^M)$ za svaki simbol $f\in F$, gdje je $f_M = I(f)\in Fun(M)$.

- **Pr1**. Jezik $\mathcal{L} = \{+, 0\}$ u skupu Z možemo interpretirati sa $I(+) = +$ (tj. sabiranje), $I(0) = 0 \in Z$ ili sa $I_1(+) = \cdot$ (tj. množenje) i $I_1(0) = 1 \in Z$. Tada za valuaciju $a = (2, 3, \dots)$ važi $[v_0 + v_1]_a^{M_I} = 2 + 3 = 5$ i $[v_0 + v_1]_a^{M_{I_1}} = 2 \cdot 3 = 6$. Slično $[v_0 + 0]_a^{M_I} = 2 + 0 = 2$ i $[v_0 + 0]_a^{M_{I_1}} = 2 \cdot 1 = 2$.
- **Pr2**. Jezik $\mathcal{L} = \{b, c\}$, gdje je b unarna a c binarna operacija u skupu riječi nad azbukom $\{0, 1\}$ možemo interpretirati kao $I(b) = BrisiZnak$ -briše prvo slovo riječi, $I(c) = Nadovezi$ -nadovezuje drugu na prvu riječ. Za valuaciju $a = (110, 01, 11, \dots)$, imamo $[b(v_0)cv_1]_a^M = 1001$.
- Neka je a valuacija u modelu $\mathbb{M}$, x promenljiva i $b \in M$. Sa $a(x/b)$ označavamo valuaciju koja se dobija iz valuacije a tako što promenljiva x ima vrijednost b. Za promjenljivu $x = v_k$, $a(v_k/b) = (a_0, \dots, a_{k-1}, b, a_{k+1}, \dots)$.

Relacija istinitosti

- Neka je A formula jezika $\mathcal{L}$, $\mathbb{M}$ molel jezika $\mathcal{L}$ i a valuacija promenljivih u modelu $\mathbb{M}$. Uvešćemo relaciju istinitosti $\models$ između para $(\mathbb{M}, a)$ i formule A, u oznaci $(\mathbb{M}, a) \models A$, koju čitamo formula A je istinita u modelu $\mathbb{M}$ za valuaciju a.
- Prethodnu relaciju čitamo i na druge načine (kraće) poput: "A je istinita za a u $\mathbb{M}$", "A važi u $\mathbb{M}$ za a", i sl.
- Umjesto oznake $(\mathbb{M}, a) \models A$ ja ću koristiti oznaku $M, a \models A$, dok se u literaturi obično koristi oznaka $M \models_a A$.
- **Def**. Relaciju istinitosti $M, a \models A$ definišemo induktivno po složenosti formule na sledeći način:

1. $M, a \models t_1 = t_2 \Leftrightarrow [t_1]_a^M = [t_2]_a^M$
2. $M, a \models r(t_1, \dots, t_n) \Leftrightarrow ([t_1]_a^M, \cdots, [t_n]_a^M) \in r_M$, gdje je $I(r) = r_M \in Rel(M)$

3. $M, a \models A \wedge B \Leftrightarrow M, a \models A$ i $M, a \models B$
4. $M, a \models A \vee B \Leftrightarrow M, a \models A$ ili $M, a \models B$
5. $M, a \models A \rightarrow B \Leftrightarrow M, a \models A$ implicira $M, a \models B$
6. $M, a \models \neg A \Leftrightarrow$ nije $M, a \models A$ (označavamo i sa $M, a \not\models A$)
7. $M, a \models \exists x A \Leftrightarrow$ za neko $b \in M$, $M, a(x/b) \models A$
8. $M, a \models \forall x A \Leftrightarrow$ za svako $b \in M$, $M, a(x/b) \models A$

- Istinitost formule $A(x_1, \ldots, x_n)$ zavisi samo od "vrijednosti" parametara. Zato $M, a \models A(x_1, \ldots, x_n)$ označavamo sa $M \models A(a_1, \ldots, a_n)$ gdje je $a_i = [x_i]_a^M$.
- **Pr1**. Jezik $\mathcal{L} = \{m, b\}$, gdje je m unarni predikat a b binarni predikat u skupu osoba možemo interpretirati sa $I(m) = JeMuškarac$ -tačan ako je osoba muškog pola, $I(b) = JeBratOd$-tačan ako je prva osoba brat od druge osobe. Za valuaciju $a = (Ana, Vuk, Nik, Jan, \ldots)$ i relaciju $JeBratOd = \{(Vuk, Ana)\}$ formula $m(v_1) \wedge b(v_1, v_0)$ je tačna, a formula $m(v_0)$ je netačna.

Logički zakoni u PL

- Neka je $\mathcal{L}$ jezik PL. Smatraćemo da su PF (predikatske formule) koje navodimo niže formule jezika $\mathcal{L}$.
- **Def**. Skup PF Σ važi u modelu M za valuaciju $a \in M^N$, u oznaci $M, a \models \Sigma$ ako za svaku PF $B \in \Sigma$ važi $M, a \models B$.
- **Def**. PF A je logička posljedica skupa formula Σ, u oznaci $\Sigma \models A$, ako za svaki model $M \in Mod(\mathcal{L})$ i svaku valuaciju $a \in M^N$, važi

$$M, a \models \Sigma \Rightarrow M, a \models A.$$

- **Def**. PF A je istinita u modelu M, u oznaci $M \models A$, ako za svaku valuaciju $a \in M^N$, važi $M, a \models A$.
- Za $M \models A$ kaže se i da je M model za formulu A.
- Kažemo da je M model za skup formula Σ i označavamo sa $M \models \Sigma$ ako za svaku formulu $B \in \Sigma$ važi $M \models B$.

- **Def** Za PF A kažemo da je valjana formula (ili logički zakon) jezika $\mathcal{L}$ i označavamo sa $\models A$ ako za svaki model $M \in Mod(\mathcal{L})$ važi $M \models A$.
- Drugim riječima, A je valjana formula ako je posljedica praznog skupa formula.

- Neka je $A(p_1, \ldots, p_n)$ IF i $B_1, \ldots, B_n$ PF jezika $\mathcal{L}$. Za formulu $A(B_1, \cdots, B_n)$ koja se dobija kada se sva javljanja iskaznog slova p_i zamjene formulom B_i, kažemo da je instanca iskazne formule A.
- **Teorema**. Svaka instanca iskazne tautologije je logički zakon PL.
- Uputstvo za dokaz. Ako instanca $A(B_1, \cdots, B_n)$ nije logički zakon onda biramo valuaciju $v(p_i) = 1 \Leftrightarrow M, a \models B_i$. Tada je $v(A) = 0$.
- Zadatak. (MP u PL) Dokazati $\models A$ i $\models A \rightarrow B$ onda $\models B$.

Korektne supstitucije

- Neka je A formula, u i t termi jezika $\mathcal{L}$ i x promjenljiva.

$*$ Sa $u(x/t)$ označavamo term koji se iz terma u dobija zamjenom svih javljanja promjenljive x sa termom t.

$*$ Sa $A(x/t)$ označavamo formulu koji se iz formule A dobija zamjenom svih slobodnih javljanja promjenljive x sa termom t.

- **Teorema 1.** Neka je $\mathbb{M}$ model, u i t termi jezika $\mathcal{L}$ i x promjenljiva. Za svaku valuaciju $a \in M^N$, važi

$$[u(x/t)]_a^M = [u]^M_{a(x/[t]^M_a)}.$$

- **Dokaz**. Dokaz izvodimo indukcijom po složenosti terma u.

1^o Za $u = c \in C$ imamo da je $u(x/t) = c$ pa je $[u(x/t)]_a^M = [c]_a^M = I(c) = c_M \in M$.

Dok je $[u]^M_{a(x/[t]^M_a)} = [c]^M_{a(x/[t]^M_a)} = I(c) = c_M$. Dakle važi $[u(x/t)]^M_a = [u]^M_{a(x/[t]^M_a)} = c_M$.

2^o Za $u = v_i \in V$ imamo dva slučaja $v_i \neq x$ i $v_i = x$.

- Ako je $v_i \neq x$ onda je $u(x/t) = v_i$ pa je $[u(x/t)]^M_a = [v_i]^M_a = a_i$.
  Dok je $[u]^M_{a(x/[t]^M_a)} = [v_i]^M_{a(x/[t]^M_a)} = a_i$.
  Dakle važi $[u(x/t)]^M_a = [u]^M_{a(x/[t]^M_a)} = a_i$.
- Ako je $v_i = x$ onda je $u(x/t) = t$ pa je $[u(x/t)]^M_a = [t]^M_a$.
  Dok je $[u]^M_{a(x/[t]^M_a)} = [x]^M_{a(x/[t]^M_a)} = [t]^M_a$.
  Dakle važi $[u(x/t)]^M_a = [u]^M_{a(x/[t]^M_a)} = [t]^M_a$.

Prethodna dva slučaja čine bazu indukcije. Dok sledeći slučaj čini indukcijski korak.

3^o Neka je term u oblika $u = f(t_1, \ldots, t_k)$ i neka tvrđenje važi za terme manje složenosti od terma u.
Onda je $u(x/t) = f(t_1(x/t), \ldots, t_k(x/t))$ pa je $[u(x/t)]_a^M = [f(t_1(x/t), \ldots, t_k(x/t))]_a^M = f_M([t_1(x/t)]_a^M, \ldots, [t_k(x/t)]_a^M)$, gdje je $f_M = I(f)$. Po ind.pp. $[t_i(x/t)]_a^M = [t_i]_{a(x/[t]_a^M)}^M$ tj. dobijamo
$[u(x/t)]_a^M = f_M([t_1]_{a(x/[t]_a^M)}^M, \ldots, [t_k]_{a(x/[t]_a^M)}^M)$
Dok je $[u]_{a(x/[t]_a^M)}^M = [f(t_1, \ldots, t_k)]_{a(x/[t]_a^M)}^M = f_M([t_1]_{a(x/[t]_a^M)}^M, \ldots, [t_k]_{a(x/[t]_a^M)}^M)$.
Dakle važi $[u(x/t)]_a^M = [u]_{a(x/[t]_a^M)}^M$.

- **Teorema 2.** Neka je $\mathbb{M}$ model jezika $\mathcal{L}$ i t term slobodan za promjenljivu x u formuli A. Tada,

$$M, a \models A(x/t) \;\Leftrightarrow\; M, a(x/[t]_a^M) \models A.$$

- **Dokaz**. Dokaz izvodimo indukcijom po složenosti formule A.

1. $A \equiv (t_1 = t_2)$
   $M, a \models A(x/t) \;\Leftrightarrow\; M, a \models (t_1 = t_2)(x/t) \;\Leftrightarrow\; M, a \models (t_1(x/t) = t_2(x/t)) \;\Leftrightarrow\; [t_1(x/t)]_a^M = [t_2(x/t)]_a^M \;\Leftrightarrow\; [t_1]^M_{a(x/[t]_a^M)} = [t_2]^M_{a(x/[t]_a^M)} \;\Leftrightarrow\; M, a(x/[t]_a^M) \models t_1 = t_2 \;\Leftrightarrow\; M, a(x/[t]_a^M) \models A$

2. $A \equiv r(t_1, \ldots, t_n), \quad I(r) = r_M$
   $M, a \models A(x/t) \;\Leftrightarrow\; M, a \models r(t_1, \ldots, t_n)(x/t) \;\Leftrightarrow\; M, a \models r(t_1(x/t), \ldots, t_n(x/t)) \;\Leftrightarrow\; ([t_1(x/t)]_a^M, \ldots, [t_n(x/t)]_a^M) \in r_M \;\Leftrightarrow\; ([t_1]^M_{a(x/[t]_a^M)}, \ldots, [t_n]^M_{a(x/[t]_a^M)}) \in r_M \;\Leftrightarrow\; M, a(x/[t]_a^M) \models r(t_1, \ldots, t_n) \;\Leftrightarrow\; M, a(x/[t]_a^M) \models A$

3. $A \equiv A_1 \wedge A_2$
   $M, a \models A(x/t) \;\Leftrightarrow\; M, a \models A_1(x/t) \wedge A_2(x/t) \;\Leftrightarrow$

$M, a \models A_1(x/t)$ i $M, a \models A_2(x/t) \;\Leftrightarrow\; M, a(x/[t]^M_a) \models A_1$ i $M, a(x/[t]^M_a) \models A_2 \;\Leftrightarrow\; M, a(x/[t]^M_a) \models A_1 \wedge A_2 \;\Leftrightarrow\; M, a(x/[t]^M_a) \models A$

4. $A \equiv A_1 \vee A_2, \quad A \equiv A_1 \rightarrow A_2, \quad A \equiv \neg A_1$ sami
5. $A \equiv \forall y B$ sami. Slično kao za $A \equiv \exists y B$.

6. $A \equiv \exists y B$
   $M, a \models A(x/t) \Leftrightarrow M, a \models (\exists y B)(x/t) \Leftrightarrow M, a \models \exists y(B(x/t))$
   $\Leftrightarrow$ za neko $c \in M$, $M, a(y/c) \models B(x/t) \;\Leftrightarrow$
   za neko $c \in M$, $M, a(y/c)(x/[t]^M_{a(y/c)}) \models B$
   ⌈ Term t je slobodan za x u formuli A pa se y ne javlja u t i $x \neq y$
   tj. $[t]^M_{a(y/c)} = [t]^M_a$ i $a(y/c)(x/[t]^M_a) = a(x/[t]^M_a)(y/c)$⌋
   $\Leftrightarrow$ za neko $c \in M$, $M, a(x/[t]^M_a)(y/c) \models B \;\Leftrightarrow\; M, a(x/[t]^M_a) \models \exists y B \;\Leftrightarrow\; M, a(x/[t]^M_a) \models A$

Logička svojstva kvantifikatora

- **Lema**. (o instancama kvantifikatora) Neka je term t slobodan za promjenljivu x u formuli A jezika $\mathcal{L}$. Tada,

$$\models \forall x A \to A(x/t) \;\text{ i }\; \models A(x/t) \to \exists x A.$$

- **Dokaz**.

  $\underline{\models \forall x A \to A(x/t)}$

  Neka je $M \in Mod(\mathcal{L})$ proizvoljan model jezika $\mathcal{L}$ i $a \in M^N$ proizvoljna valuacija u modelu M. Treba dokazati da je $M, a \models \forall x A \to A(x/t)$.

⋆ Ako $M, a \not\models \forall x A$ onda po semantici $M, a \models \forall x A \to A(x/t)$.

⋆ Neka je $M, a \models \forall x A$. Onda, za svako $c \in M$, $M, a(x/c) \models A$. Specijalno za $c = [t]_a^M \in M$ dobijamo $M, a(x/[t]_a^M) \models A$, odnosno $M, a \models A(x/t)$. Dakle, $M, a \models \forall x A \Rightarrow M, a \models A(x/t)$ tj. $M, a \models \forall x A \to A(x/t)$.

$\models A(x/t) \rightarrow \exists x A$

Neka su $M \in Mod(\mathcal{L})$ i $a \in M^N$ proizvoljni. Dokažimo $M, a \models A(x/t) \Rightarrow M, a \models \exists x A$.

Zaista, $M, a \models A(x/t) \ \Rightarrow \ M, a(x/[t]_a^M) \models A \ \Rightarrow$ za $c = [t]_a^M \in M$ važi $M, a(x/c) \models A \ \Rightarrow$ za neko $c \in M$, $M, a(x/c) \models A \ \Rightarrow M, a \models \exists x A$.

- Zadatak. Navesti primjere formule A i terma t tako da:
  $a)$ $\not\models \forall x A \rightarrow A(x/t)$; $b)$ $\not\models A(x/t) \rightarrow \exists x A$;
  $c)$ $\not\models \exists x A \rightarrow A(x/t)$; $d)$ $\not\models A(x/t) \rightarrow \forall x A$.

Rj. $a)$ $A(x) = \exists y(x < y)$, $t = y$. Npr. u skupu $\mathbb{N}$ važi $\forall x A \equiv \forall x \exists y(x < y)$ a ne važi $A(x/t) \equiv \exists y(y < y)$.
$c)$ $A(x) = \exists y(x = y + y)$, $t = z + z + 1$.
$b)$ i $d)$ sami.

- **Teorema**. (o Bernajsovim pravilima) Neka su A i B formule i neka promjenljiva x nije slobodna u formuli A. Tada,

$$\models A \to B \;\Rightarrow \models A \to \forall x B; \quad \models B \to A \;\Rightarrow \models \exists x B \to A.$$

- **Dokaz**.

  $\underline{\models A \to B \;\Rightarrow \models A \to \forall x B}$

  Neka su $M \in Mod(\mathcal{L})$ i $a \in M^N$ proizvoljini model i valuacija. Neka je dalje $M, a \models A$ (jer ako je $M, a \not\models A$ onda očito $M, a \models A \to \forall x B$). Za proizvoljno $b \in M$, pošto x nije slobodna u formuli A, važi $M, a(x/b) \models A$. S druge strane zbog $\models A \to B$ važi $M, a(x/b) \models A \to B$. Pa po semantičkim pravilima dobijamo $M, a(x/b) \models B$.

  Dakle, za svako $b \in M$, $M, a(x/b) \models B$ pa je $M, a \models \forall x B$ tj. $M, a \models A \to \forall x B$.

  Kako su M i a proizvoljni to važi $\models A \to \forall x B$.

$\models B \to A \;\Rightarrow \models \exists x B \to A$

Neka su $M \in Mod(\mathcal{L})$ i $a \in M^N$ proizvoljini model i valuacija i neka je $M, a \models \exists x B$. Tada, za neko $c \in M$, $M, a(x/c) \models B$. Pa zbog $\models B \to A$ važi $M, a(x/c) \models A$. Kako istinitost od A ne zavisi od x to je $M, a \models A$, odnosno $M, a \models \exists x B \to A$.

Dakle, za svaki model M i svaku valuaciju a, $M, a \models \exists x B \to A$ što znači $\models \exists x B \to A$.

Ekvivalencija u PL

- Formule A i B su logički ekvivalentne ako za svaki model $M \in Mod(\mathcal{L})$ i svaku valuaciju $a \in M^N$ važi: $M, a \models A \;\Leftrightarrow\; M, a \models B$.
- Zadatak. Dokazati da su formule A i B logički ekvivalentne akko $\models A \leftrightarrow B$.
- Znamo da je $A \leftrightarrow B$ skraćenica za $(A \to B) \wedge (B \to A)$.

- **Lema** (o preimenovanju vezanih promjenljivih) Ako formula A ne sadrži promjenljivu y, onda

$$\models \forall xA \leftrightarrow \forall yA(x/y) \quad \text{i} \quad \models \exists xA \leftrightarrow \exists yA(x/y).$$

- **Dokaz**. Neka su $M \in Mod(\mathcal{L})$ i $a \in M^N$ proizvoljini model i valuacija. Tada, $M, a \models \forall yA(x/y) \Leftrightarrow$
za svako $c \in M$, $M, a(y/c) \models A(x/y) \Leftrightarrow$
za svako $c \in M$, $M, a(y/c)(x/[y]^M_{a(y/c)}) \models A \Leftrightarrow$
$\lceil\ a(y/c)(x/[y]^M_{a(y/c)}) = a(y/c)(x/c) = a(x/c)(y/c)\ \rfloor$
za svako $c \in M$, $M, a(x/c)(y/c) \models A \Leftrightarrow$
za svako $c \in M$, $M, a(x/c) \models A \Leftrightarrow M, a \models \forall xA$.
Dakle, za svaki model M i svaku valuaciju a važi
$M, a \models \forall xA$ akko $M, a \models \forall yA(x/y)$
pa je $\models \forall xA \leftrightarrow \forall yA(x/y)$.

Dokaz za $\models \exists xA \leftrightarrow \exists yA(x/y)$ uradite sami.

- **Teorema** (o supstituciji ekvivalentnih formula). Neka su A, B i C predikatske formule. Tada, $\models B \leftrightarrow C \;\Rightarrow \models A \leftrightarrow A(B/C)$.
- Dokaz uradite sami.
- **Teorema** (pravilo generalizacije) Neka je A formula i x promjenljiva. Tada $\models A \;\Leftrightarrow \models \forall x A$.
- Dokaz (uputstvo za $\Rightarrow$). M, a -proizvoljni. Iz $\models A$ slijedi za svako $c \in M$, $M, a(x/c) \models A$ pa je $M, a \models \forall x A$. Dakle, $\models \forall x A$.
- Zadatak. Navesti primjer formule A za koju ne važi $\models A \leftrightarrow \forall x A$.
- Rj. $A(x) \equiv \exists y(s(y) = x)$. Naime u modelu $\mathbb{N}$,
  $N, a(x/1) \not\models A \rightarrow \forall x A$, jer $N, a(x/1) \models A$ a $N, a(x/0) \not\models A$.
  $\lceil$ $s(y)$ - interpretiramo kao sljedbenik od y $\rfloor$

Svojstva jednakosti

- Kongruencija je relacija ekvivalencije (refleksivna, simetrična i tranzitivna) koja je saglasna sa operacijama i relacijama.
- **Zadatak**. Dokazati da je jednakost kongruencija u svakoj strukturi. Preciznije: Neka su x, y, z, x_i, y_i, $1 \leq i \leq n$ promjenljive, f operacijski simbol dužine n i r relacijski simbol dužine n. Tada važi:

  $\models (x = x)$

  $\models (x = y) \rightarrow (y = x)$

  $\models (x = y) \wedge (y = z) \rightarrow (x = z)$

  $\models (x_1 = y_1) \wedge \cdots \wedge (x_n = y_n) \rightarrow (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))$

  $\models (x_1 = y_1) \wedge \cdots \wedge (x_n = y_n) \rightarrow (r(x_1, \ldots, x_n) \leftrightarrow r(y_1, \ldots, y_n))$
- Formula $\forall x_1 \cdots \forall x_n A$ je univerzalno zatvorenje formule $A(x_1, \ldots, x_n)$. Univerzalna zatvorenja prethodnih svojstava se uzimaju za aksiome jednakosti.

Kvantifikatori i negacija

- **Zadatak**. Dokazati uopštene De Morganove zakone:

$$\models \neg\forall x A \leftrightarrow \exists x \neg A \quad \text{i} \quad \models \neg\exists x A \leftrightarrow \forall x \neg A.$$

- **Zadatak**. Neka je $\mathbb{M} = (M, I(R), I(F), I(C))$ konačan model jezika $\mathcal{L} = R \cup F \cup C$ i neka je $M = \{b_1, \cdots, b_n\}$. Neka je dalje $\overline{\mathbb{M}} = (M, I(R), I(F), I(\overline{C}))$ prosta ekspanzija modela $\mathbb{M}$ za jezik $\overline{\mathcal{L}} = R \cup F \cup \overline{C}$, gdje je $\overline{C} = \{c_{b_i} \,:\, b_i \in M\}$ i $I(c_{b_i}) = b_i$ (tj. c_{b_i} je ime za b_i).

  Dokazati da za svaku valuaciju $a \in M^N$ važi:

$$\mathbb{M}, a \models \forall x A \;\Leftrightarrow\; \overline{\mathbb{M}}, a \models A(x/c_{b_1}) \wedge \cdots \wedge A(x/c_{b_n}) \text{ i}$$

$$\mathbb{M}, a \models \exists x A \;\Leftrightarrow\; \overline{\mathbb{M}}, a \models A(x/c_{b_1}) \vee \cdots \vee A(x/c_{b_n}).$$

- Prethodni zadatak nam govori kako eliminisati kvantifikatore u konačnom modelu. Uopšteno $\forall, \exists$ prestavljaju beskonačnu konjunkciju i disjunkciju.

Kvantifikatori i konjunkcija

- **Zadatak**. Neka su A i B formule. Tada,

a) $\models (\forall xA \wedge \forall xB) \leftrightarrow \forall x(A \wedge B)$;

b) $\models \exists x(A \wedge B) \rightarrow (\exists xA \wedge \exists xB)$;

c) $\models (\exists xA \wedge B) \leftrightarrow \exists x(A \wedge B)$, gdje B ne sadrži parametar x.

- Rj. a) Neka je M proizvoljan model, $a \in M^N$ proizvoljna valuacija i neka je $M, a \models (\forall xA \wedge \forall xB)$. Tada važi
$M, a \models (\forall xA \wedge \forall xB) \;\Leftrightarrow\; M, a \models (\forall xA)$ i $M, a \models (\forall xB) \;\Leftrightarrow$
za svako $c \in M$, $M, a(x/c) \models A$ i za svako $c \in M$, $M, a(x/c) \models B \;\Leftrightarrow$
za svako $c \in M$ važi $M, a(x/c) \models A$ i $M, a(x/c) \models B \;\Leftrightarrow$
za svako $c \in M$ važi $M, a(x/c) \models A \wedge B \;\Leftrightarrow\; M, a \models \forall x(A \wedge B)$.

  Dakle, za svako M i a, $M, a \models (\forall xA \wedge \forall xB)$ akko $M, a \models \forall x(A \wedge B)$ tj. $\models (\forall xA \wedge \forall xB) \leftrightarrow \forall x(A \wedge B)$.

Kvantifikatori i disjunkcija. Kvantifikatori i implikacija

Kvantifikatori i disjunkcija

- **Zadatak**. Neka su A i B formule. Tada,

a) $\models (\exists xA \vee \exists xB) \leftrightarrow \exists x(A \vee B)$;

b) $\models (\forall xA \vee \forall xB) \rightarrow \forall x(A \vee B)$;

c) $\models (\forall xA \vee B) \leftrightarrow \forall x(A \vee B)$, gdje B ne sadrži parametar x.

Kvantifikatori i implikacija

- **Zadatak**. Neka su A i B formule i x promjenljiva koja nije slobodna u formuli B,

a) $\models (\forall xA \rightarrow B) \leftrightarrow \exists x(A \rightarrow B)$;

b) $\models (B \rightarrow \forall xA) \leftrightarrow \forall x(B \rightarrow A)$;

c) $\models (\exists xA \rightarrow B) \leftrightarrow \forall x(A \rightarrow B)$;

d) $\models (B \rightarrow \exists xA) \leftrightarrow \exists x(B \rightarrow A)$.

Preneksni oblik formule

- **Def**. Za formulu oblika $Q_1 x_1 \cdots Q_n x_n A$, gdje je $Q_i \in \{\forall, \exists\}$ i A formula bez kvantifikatora, kažemo da ima preneksni oblik.
- **Teorema**. (o preneksnom obliku formule) Za svaku formulu A postoji formula A^* u preneksnom obliku, takva da $\models A \leftrightarrow A^*$.
- Uputstvo za dokaz. Indukcijom po složenosti formule A. Ako kvantifikator ne "prolazi" kroz veznike onda koristimo preimenovanje promjenljivih.
- **Pr.** Neka je $C \equiv (\exists x \forall y A(x,y) \wedge \exists x \forall y B(x,y))$. Ne možemo izvući $\exists x$ ispred formule, jer $\exists$ ne prolazi kroz veznik $\wedge$. Ako vezanu promenljivu x u formuli A preimenujemo u v koja se ne javlja u A i B onda po svojstvu c) možemo je izvući ispred.

  Dobijamo $C_1 \equiv \exists v(\forall y A(v,y) \wedge \exists x \forall y B(x,y))$. Slično odradimo za x u B a onda $\forall y$ prolazi kroz $\wedge$ svojstvo a).

  Konačno $C^* \equiv \exists v \exists u \forall y (A(v,y) \wedge B(u,y))$.

Formalizacija PL

Aksiome

- Insatnce iskaznih aksioma T_1 do T_{11};
- Neka je term t slobodan za promjenljivu x u formuli A

  $T_\forall: \quad \forall x A \to A(x/t),$

  $T_\exists: \quad A(x/t) \to \exists x A;$
- Neka su x, y, z, x_i, y_i, $1 \leq i \leq n$ promjenljive, f i r redom operacijski i relacijski simbol dužine n

  $E_1: \quad \forall x(x = x)$

  $E_2: \quad \forall x \forall y(x = y \to y = x)$

  $E_3: \quad \forall x \forall y \forall z((x = y \wedge y = z) \to x = z)$

  $E_4: \quad \forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$

  $E_5: \quad \forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \to (r(x_1, \ldots, x_n) \leftrightarrow r(y_1, \ldots, y_n))$

Pravila izvođenja

- MP (Modus ponens):
$$\frac{A,\ A \to B}{B}$$

- $BP\forall$ (Bernajsovo pravilo $\forall$):
  Neka promjenljiva x nije slobodna u formuli A
$$\frac{A \to B}{A \to \forall x B}$$

- $BP\exists$ (Bernajsovo pravilo $\exists$):
  Neka promjenljiva x nije slobodna u formuli B
$$\frac{A \to B}{\exists x A \to B}$$

Dokaz u predikatskom računu

- **Def**. Neka je Σ skup formula i A formula jezika $\mathcal{L}$. Konačan niz formula $A_1, \ldots, A_n$ je dokaz formule $A = A_n$ iz pretpostavki Σ ako za svako k, $1 \leq k \leq n$, važi jedan od uslova:
  1^o) $A_k \in T \cup \Sigma$;
  2^o) postoji $i, j < k$ tako da je $A_j = A_i \to A_k$ (tj. A_k dobijamo po MP);
  3^o) $A_k = C \to \forall x D$, x nije slobodna u C i postoji $i < k$ tako da je $A_i = C \to D$ (tj. A_k dobijamo po $BP\forall$);
  4^o) $A_k = \exists x C \to D$, x nije slobodna u D i postoji $i < k$ tako da je $A_i = C \to D$ (tj. A_k dobijamo po $BP\exists$).
- **Def**. Ako A ima dokaz iz Σ onda koristimo oznaku $\Sigma \vdash A$ i čitamo A je posljedica od Σ ili A je dokaziva iz Σ.
- **Def**. Ako je $\Sigma = \emptyset$ onda umjesto $\emptyset \vdash A$ pišemo $\vdash A$ i čitamo A ima dokaz ili A je teorema PR (predikatskog računa).

- **Teorema**. (pravilo generalizacije) Za svaku formulu A jezika $\mathcal{L}$ važi: $\dfrac{A}{\forall x A}$ tj. $A \vdash \forall x A$.

- **Dokaz**. Uzmimo neku formulu $B \in T_1$ u kojoj x nije slobodna. Imamo $\Sigma = \{A\}$ pa je dokaz niz formula $A_1 = A \in \Sigma$, $A_2 = A \to (B \to A) \in T_1$, $A_3 = B \to A$ (MP 1,2), $A_4 = B \to \forall x A$ ($BP\forall$ 3), $A_5 = B \in T_1$, $A_6 = \forall x A$ (MP 5,4).

- **Teorema**. (De Morganovi zakoni). Za svaku formulu A jezika $\mathcal{L}$ važi: a) $\vdash \forall x A \leftrightarrow \neg \exists \neg A$ i b) $\vdash \exists x A \leftrightarrow \neg \forall \neg A$.

- **Dokaz**. [b) $\to$:] Dokaz je niz formula $A_1 = \forall x \neg A \to \neg A \in T_\forall$, $A_2 = \neg\neg A \to \neg \forall x \neg A$ (KP 1), $A_3 = A \to \neg\neg A$ ($Z2\neg$), $A_4 = A \to \neg \forall x \neg A$ (TRANZ 2,3), $A_5 = \exists x A \to \neg \forall \neg A$ ($BP\exists$ 4).

Teorema.

a) Za svaku formulu A, važi: $\vdash \exists y \forall x A \to \forall x \exists y A$.

b) Ako je promjenljiva y slobodna za x u formuli A, onda važi: $\vdash \forall x A \to \forall y A(x/y)$ i $\vdash \exists x A \to \exists y A(x/y)$.

c) Dokazati da za proizvoljne formule A i B, u predikatskom računu važe sledeća pravila:

$$\frac{A \to B}{\forall x A \to \forall x B} \quad \text{i} \quad \frac{A \to B}{\exists x A \to \exists x B}.$$

d) Za svaku formulu $A(x_1, \cdots, x_n)$ jezika $\mathcal{L}$, važi: $\vdash A(x_1, \cdots, x_n) \Leftrightarrow \vdash \forall x_1 \cdots \forall x_n A(x_1, \cdots, x_n)$.

Dokaz.

a) Dokaz je niz formula: $A_1 = \forall x A \to A \in T_\forall$, $A_2 = A \to \exists y A \in T_\exists$, $A_3 = \forall x A \to \exists y A$ (TRANZ 1,2), $A_4 = \exists y \forall x A \to \exists y A$ ($BP\exists$ 3), $A_5 = \exists y \forall x A \to \forall x \exists y A$ ($BP\forall$ 4).

- **Teorema**. (dedukcije PR) Neka je Σ, A skup **rečenica** i B formula jezika $\mathcal{L}$. Tada,
$$\Sigma, A \vdash B \ \Rightarrow \ \Sigma \vdash A \to B.$$
- **Dokaz**. Dokaz se izvodi indukcijom po dužini dokaza za formulu B iz Σ, A. Novina je što se u induktivnom koraku formula može dobiti primjenom Bernajsovih pravila, a ostali slučajevi su isti kao u iskaznom računu.

  Neka tvrđenje važi za sve formule koje imaju dokaz dužine manje od k. Dokažimo da tvrđenje važi i za formulu koja ima dokaz $A_1, \ldots, A_k$ dužine k (i A_k dobijeno po BP).

⋆ $A_k = C \to \forall x D$ dobijena po $(BP\forall\ j)$, gdje je $j < k$, promjenljiva x nije slobodna u C i $A_j = C \to D$. Po ind. pp. $\Sigma \vdash A \to A_j$ tj. $\Sigma \vdash A \to (C \to D)$. Kako je $(A \to (C \to D)) \to ((A \wedge C) \to D)$ instanca iskazne teoreme to po MP dobijamo $\Sigma \vdash (A \wedge C) \to D$.

Kako je A rečenica to promjenljiva x nije slobodna u formuli $A \wedge C$ pa po $BP\forall$ dobijamo $\Sigma \vdash (A \wedge C) \to \forall x D$. Kako je $((A \wedge C) \to \forall x D) \to (A \to (C \to \forall x D))$ instanca iskazne teoreme to dobijamo $\Sigma \vdash A \to (C \to \forall x D)$ tj. $\Sigma \vdash A \to A_k$.

Napomena. Za prethodni dokaz nismo morali zahtjevati da A bude rečenica, dovoljan je zahtjev da x nije slobodna u A.

⋆ $A_k = \exists x D \to C$ dobijena po $BP\exists$ na $A_j = D \to C$, gdje je $j < k$ i promjenljiva x nije slobodna u C. Po ind. pp. $\Sigma \vdash A \to A_j$, što znači da postoji dokaz $B_1, \cdots, B_m$ za $B_m = A \to (D \to C)$ iz Σ. Dopunimo ovaj dokaz sa $B_{m+1} = (A \to (D \to C)) \to (D \to (A \to C)) \in \mathcal{T}_{IL}$, $B_{m+2} = D \to (A \to C)$ (MP, $m, m+1$), $B_{m+3} = \exists x D \to (A \to C)$ ($BP\exists$ $m+2$ jer x nije slobodna u $A \to C$ pošto je A rečenica), $B_{m+4} = (\exists x D \to (A \to C)) \to (A \to (\exists x D \to C)) \in \mathcal{T}_{IL}$, $B_{m+5} = A \to (\exists x D \to C) = A \to A_k$ (MP $m+3, m+4$).

- **Teorema**. (o preneksnom obliku) Za svaku formulu A postoji formula A^* u preneksnom obliku takva da je $\vdash A \leftrightarrow A^*$.

- **Teorema**. (opšta teorema korektnosti) Za savki skup rečenica Σ, A jezika $\mathcal{L}$,

$$\Sigma \vdash A \;\Rightarrow\; \Sigma \models A.$$

- **Teorema**. (opšta teorema potpunosti) Neka je A formula i Σ skup rečenica jezika $\mathcal{L}$. Tada ,

$$\Sigma \models A \;\Rightarrow\; \Sigma \vdash A.$$

- **Teorema**. Neka je A formula PL. Tada,

$$\models A \Leftrightarrow \vdash A.$$

DODATAK

ne dolazi na ispitu

Modalne logike

- Imamo veliki broj modalnih logika. Mi ovde navodimo jednu od osnovnih modalnih logika K_m. (K je u čast Kripke.)
- Jezik logike K_m je jezik iskazne logike proširen sa m modalnih operatora $\Box_1, \ldots, \Box_m$ i sa operatorima koji su njima dualni $\Diamond_1, \ldots, \Diamond_m$.
- Formule u logici K_m gradimo koristeći sledeća sintaktička pravila:

$$\phi ::= p|(\phi_1 \wedge \phi_2)|(\phi_1 \vee \phi_2)|(\phi_1 \to \phi_2)|\neg\phi|\Box_i\phi|\Diamond_i\phi$$

  gde je p iskazni simbol, ϕ (moguće sa indeksom) formula, $\Box_i$ i $\Diamond_i$, $0 \leq i \leq m$ modalni operatori.
- Logika K_1 se označava sa K i u njoj $\Box\phi$ obično čitamo "nužno" ϕ a $\Diamond\phi$ čitamo "moguće" ϕ. Čitamo ih i drugačije.
- $\Diamond\phi$ je skraćenica za $\neg\Box\neg\phi$

- Semantika modalnih logika se zasniva na pojmu (Kripke) strukture, koja se definiše kao $M = (S, R_1, \ldots, R_m, \Pi)$, gdje S označava neprazan skup stanja (ili svjetova), R_i je binarna relacija na S koja odgovara operatoru $\Box_i$, a Π je preslikavanje iz S u skupove iskaznih simbola, tako da $\Pi(s)$ određuje (sadrži) simbole koji su istiniti u stanju s.
- Istinitosna relacija $M, s \models \phi$ (obično čita: "Formula ϕ važi u stanju s strukture M") se definiše induktivno:

$$
\begin{array}{lll}
M, s \models p & \text{akko} & p \in \Pi(s) \\
M, s \models (\phi_1 \wedge \phi_2) & \text{akko} & M, s \models \phi_1 \text{ i } M, s \models \phi_2 \\
M, s \models (\phi_1 \vee \phi_2) & \text{akko} & M, s \models \phi_1 \text{ ili } M, s \models \phi_2 \\
M, s \models (\phi_1 \rightarrow \phi_2) & \text{akko} & M, s \models \phi_1 \text{ povlači } M, s \models \phi_2 \\
M, s \models \neg\phi & \text{akko} & M, s \not\models \phi \\
M, s \models \Diamond_i\phi & \text{akko} & \exists s'.(s, s') \in R_i \text{ i } M, s' \models \phi \\
M, s \models \Box_i\phi & \text{akko} & \forall s'.(s, s') \in R_i \Rightarrow M, s' \models \phi
\end{array}
$$

- Operator $\Box\varphi$ možemo tumačiti kao "U svim dostupnim (vidljivim) svjetovima važi φ" a operator $\Diamond\varphi$ kao "Postoji dostupan (vidljiv) svijet u kom je φ".

- Operator $\Box_i\varphi$ možemo tumačiti kao "Agent i zna φ".

  Neke od aksioa logike znanja (modalne logike S):

  $\Box\varphi \to \varphi$ - ako nešta zna onda je to tačno

  $\Box\varphi \to \Box\Box\varphi$ - ako nešta zna onda on zna da to zna

  $\neg\Box\varphi \to \Box\neg\Box\varphi$ - ako nešta ne zna onda on zna da to ne zna

- U vremenskim logikama (npr. kad je model, tj. Kripke struktura, skup prirodnih brojeva) operator $\Box\varphi$ možemo tumačiti kao "U svim momentima budućnosti važi φ" a operator $\Diamond\varphi$ kao "Postoji moment budućnosti u kom je φ".

Deskriptivne logike

- Deskriptivne logike (Description logics) su namenjene za reprezentaciju znanja i rasudjivanje u sistemima vještačke inteligencije.
- Nastale su krajem XX vijeka sa ciljem da se formalizuju prethodno razvijeni sistemi vještačke inteligencije (bazirani na frejmovima, semantičkim mrežama,...).
- Zbog svojih dobrih osobina uzete su kao osnova za izgradnju ontoloških jezika semantičkog web-a.
- OWL 1 (Web Ontology Language), baziran na DL $\mathcal{SHOIN}$, je preporučen, od W3C kao standard 2004. godine.
- OWL 2, baziran na DL $\mathcal{SROIQ}$, je preporučen kao standard 2009. godine.

- Deskriptivne logike gradimo koristeći odgovarajuće konstruktore i simbole iz sledeća tri skupa:
  - imena koncepata: $A_1, A_2, \ldots$;
  - imena svojstava: $P_1, P_2, \ldots$;
  - imena objekata: $\alpha_1, \alpha_2, \ldots$.
- Navodimo jednu od osnovnih deskriptivnih logika $\mathcal{ALC}$ (sintaksna varijanta od K_m).
- Pravila za formiranje $\mathcal{ALC}$-koncepata i $\mathcal{ALC}$-svojstava su data sledećom sintaksom:

$$C ::= \top | \bot | A | C_1 \sqcap C_2 | C_1 \sqcup C_2 | \neg C | \exists R.C | \forall R.C$$

$$R ::= P$$

gde je A atomarni koncept tj. ime koncepta, C (moguće sa indeksom) označava koncept, P, R označavaju svojstva, koja su ovde samo atomarna tj. imena svojstava.

- Semantiku zadajemo pomoću *interpretacije* $I = \langle \Delta^I, \cdot^I \rangle$, gdje je Δ^I *domena interpretacije* a $\cdot^I$ *funkcija interpretacije* koja svakom atomarnom pojmu A pridružuje $A^I \subset \Delta^I$, svakom atomarnom svojstvu P pridružuje $P^I \subset \Delta^I \times \Delta^I$ i svakom imenu objekta α pridružuje jedan element (objekt) α^I iz Δ^I. Često se piše α umesto α^I.
- Funkcija interpretacije se proširuje na složene pojmove saglasno sledećim pravilima semantike:

$$
\begin{aligned}
&\top^I = \Delta^I \\
&\bot^I = \emptyset \\
&(\neg C)^I = \Delta^I - C^I \\
&(C_1 \sqcap C_2)^I = C_1^I \cap C_2^I \\
&(C_1 \sqcup C_2)^I = C_1^I \cup C_2^I \\
&(\exists R.C)^I = \{d \in \Delta^I \mid \exists d'.(d, d') \in R^I \text{ i } d' \in C^I\} \\
&(\forall R.C)^I = \{d \in \Delta^I \mid \forall d'.(d, d') \in R^I \text{ sledi } d' \in C^I\}
\end{aligned}
$$

- Jedna baza znanja napisana u logici $\mathcal{ALC}$ mogla bi da izgleda:

$$
\begin{aligned}
&\mathit{Petar} \ : \ \exists \textbf{ima}.\mathrm{Automobil} \\
&\mathit{Petar}\ \textbf{voli}\ \mathit{Jugo}45 \\
&\mathit{Jugo}45 \ : \ \mathrm{Zastava} \\
&\mathsf{Mu\check{s}ki\_kupac} \ = \ \mathsf{Mu\check{s}ko} \sqcap \mathrm{Kupac} \\
&\mathsf{Savremeni\_automobil} \ = \ \mathrm{Automobil} \sqcap \exists \textbf{ima}.\mathsf{Ra\check{c}unar}
\end{aligned}
$$

- U ovom primeru *Petar* i *Jugo*45 su imena objekata koja označavaju redom konkretnu ličnost i konkretan tip automobila, Automobil, Zastava itd., su koncepti (unarni predikati) koji označavaju određenu klasu objekata, dok su **ima** i **voli** imena svojstava koja označavaju binarnu relaciju između objekata.
- Čitanje tvrđenja je direktno: "Petar ima automobil", "Petar voli Jugo45", "Savremeni automobil je automobil koji ima računar'.

Sistemi bazirani na Deskriptivnim logikama

Baza znanja

TBox

Otac $\equiv$ Muškarac $\sqcap$ $\geq$ 1imaDijete

ABox

imaDijete(Milenko,Ana)   Muškarac(Milenko)

Sistem za rasudjivanje

- RBox (role hierarchy) je dio od TBox-a

Sistemi bazirani na Deskriptivnim logikama

Baza znanja

TBox

$\text{Otac} \equiv \text{Muškarac} \sqcap \geq 1\text{imaDijete}$

ABox

imaDijete(Milenko,Ana) Muškarac(Milenko)

Sistem za rasudjivanje

- RBox (role hierarchy) je dio od TBox-a

Otac(Milenko)

Primijer baze znanja

TBox

Žene $\sqsubseteq$ Osobe

Muškarci $\equiv$ Osobe $\sqcap \neg$Žene

Majke $\equiv$ Žene$\sqcap \geq 1$*imaDijete*

Očevi $\equiv$ Muškarci$\sqcap \geq 1$*imaDijete*

Roditelji $\equiv$ Očevi $\sqcup$ Majke

Babe $\equiv$ Majke $\sqcap \exists$*imaDijete*.Roditelji

MajkeBezĆerki $\equiv$ Majke $\sqcap \forall$*imaDijete*.$\neg$Žene

RBox

imaDijete$\sqsubseteq$*imaPotomka*

imaPotomka$\circ$*imaPotomka*$\sqsubseteq$*imaPotomka*

imaDijete$\circ$*imaDijete*$\sqsubseteq$*imaUnuče*

ABox

imaDijete(Milenko,Ana), *imaDijete*(Milka,Milenko), Žene(Milka), Muškarci(Milenko), Žene(Ana).

KRAJ!