Matematička logika u računarstvu

1. čas: Strukture prvog reda

Logika je propast duha.

Antoan de Sent Egziperi, *Vojni pilot*

Jezici prvog reda

Definicija

Jezik prvog reda $\mathcal{L}$ određuju:

- skup *funkcijskih* simbola $\mathcal{F}$ i brojem $n_f \in \mathbb{N}^+$ za svaki $f \in \mathcal{F}$;
- skup *relacijskih* simbola $\mathcal{R}$ i brojem $n_R \in \mathbb{N}^+$ za svaki $R \in \mathcal{R}$;
- skup *konstantnih* simbola $\mathcal{C}$.

Brojevi n_f i n_R su *arnost*, tj. *dužina* odgovarajućeg simbola.

Primeri

- jezik prstena $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$, $n_+ = n_\cdot = 2$, $n_- = 1$;
- jezik uređenih prstena $\mathcal{L}_{or} = \mathcal{L}_r \cup \{<\}$, $n_< = 2$;
- jezik grupa $\mathcal{L}_{gp} = \{\cdot, ^{-1}, e\}$, $n_\cdot = 2$, $n_{-1} = 1$;
- jezik grafova $\mathcal{L} = \{R\}$, $n_R = 2$;
- jezik čistog skupa $\mathcal{L} = \varnothing$.

Strukture prvog reda

Definicija

$\mathcal{L}$-strukturu $\mathcal{M} = (M, s^{\mathcal{M}})_{s \in \mathcal{L}}$ određuju:

- neprazan skup M – *univerzum* ili *domen* od $\mathcal{M}$;
- funkcija $f^{\mathcal{M}} : M^{n_f} \to M$ za svaki $f \in \mathcal{F}$;
- skup $R^{\mathcal{M}} \subseteq M^{n_R}$ za svaki $R \in \mathcal{R}$;
- element $c^{\mathcal{M}} \in M$ za svaki $c \in \mathcal{C}$;

Primer

- $(\mathbb{Z}, +, -, \cdot, 0, 1)$, $(\mathbb{Q}, +, -, \cdot, 0, 1)$, $(\mathbb{R}, +, -, \cdot, 0, 1)$;
- $(\mathbb{R}, +, -, \cdot, <, 0, 1)$;
- $(\mathbb{N}, <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$, $(\mathbb{R}, <)$, $(\mathbb{N}, |)$, $(\mathbb{Z}, |)$.

Utapanja

Definicija

Neka su $\mathcal{M}$ i $\mathcal{N}$ dve $\mathcal{L}$-strukture. *$\mathcal{L}$-utapanje* $\eta : \mathcal{M} \to \mathcal{N}$ je 1-1 preslikavanje $\eta : M \to N$ takvo da:

- $\eta(f^{\mathcal{M}}(a_1, \ldots, a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), \ldots, \eta(a_{n_f}))$ za sve $f \in \mathcal{F}$ i $a_1, \ldots, a_{n_f} \in M$;
- $(a_1, \ldots, a_{n_R}) \in R^{\mathcal{M}}$ akko $(\eta(a_1), \ldots, \eta(a_{n_R})) \in R^{\mathcal{N}}$ za sve $R \in \mathcal{R}$ i $a_1, \ldots, a_{n_f} \in M$;
- $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

Ako je $M \subseteq N$ i $\iota : \mathcal{M} \to \mathcal{N}$, gde je ι inkluziono preslikavanje, kažemo da je $\mathcal{M}$ *podstruktura* od $\mathcal{N}$: $\mathcal{M} \leqslant \mathcal{N}$.
Ako je η i na, kažemo da je *izomorfizam*: $\eta : \mathcal{M} \xrightarrow{\cong} \mathcal{N}$.
Izomorfizam $\mathcal{M} \xrightarrow{\cong} \mathcal{M}$ je *automorfizam* strukture $\mathcal{M}$. Skup svih automorfizam od $\mathcal{M}$ obeležavamo sa $\mathrm{Aut}(\mathcal{M})$.

Utapanja

Primeri

- $(\mathbb{N}, <) \leqslant (\mathbb{Z}, <) \leqslant (\mathbb{Q}, <) \leqslant (\mathbb{R}, <)$;
- $(\mathbb{Z}, +, 0) \leqslant (\mathbb{R}, +, 0)$;
- $\eta : (\mathbb{Z}, +, <, 0) \to (\mathbb{R}, \cdot, <, 1)$ gde $\eta(x) = e^x$.

Tvrđenje

Neka su $\mathcal{M}, \mathcal{N}, \mathcal{K}$ tri $\mathcal{L}$-strukture.

- Ako $\eta : \mathcal{M} \to \mathcal{N}$ i $\zeta : \mathcal{N} \to \mathcal{K}$, onda $\zeta \circ \eta : \mathcal{M} \to \mathcal{K}$.
- Ako $\eta : \mathcal{M} \xrightarrow{\cong} \mathcal{N}$, onda $\eta^{-1} : \mathcal{N} \xrightarrow{\cong} \mathcal{M}$.
- $\mathrm{Aut}(\mathcal{M})$ je grupa u osnosu na kompoziciju funkcija.

Podstrukture

Tvrđenje

$\mathcal{M} \leqslant \mathcal{N}$ akko:

- $M \subseteq N$;
- $f^{\mathcal{M}}(a_1, \ldots, a_{n_f}) = f^{\mathcal{N}}(a_1, \ldots, a_{n_f})$ za sve $f \in \mathcal{F}$ i $a_1, \ldots, a_{n_f} \in M$ (specijalno, M je zatvoreno za funkciju $f^{\mathcal{N}}$);
- $R^{\mathcal{M}} = M^{n_R} \cap R^{\mathcal{N}}$ za sve $R \in \mathcal{R}$;
- $c^{\mathcal{M}} = c^{\mathcal{N}}$ za sve $c \in \mathcal{C}$ (specijalno, $c^{\mathcal{N}} \in M$).

Termi

$\mathcal{L}$-terme zapisujemo koristeći simbole jezika $\mathcal{L}$, simbole promenljivih $x, y, z, \ldots, x_0, x_1, x_2, \ldots$ (skup promenljivih obeležavamo sa Var) i pomoćne simbole zagrada i zapete.

Definicija

Skup $\mathcal{L}$-terma je najmanji skup $\mathcal{T}$ takav da:

- $\mathcal{C} \subseteq \mathcal{T}$;
- $\text{Var} \subseteq \mathcal{T}$;
- ako $f \in \mathcal{F}$ i $t_1, \ldots, t_{n_f} \in \mathcal{T}$, onda $f(t_1, \ldots, t_{n_f}) \in \mathcal{T}$.

Alternativno, $\mathcal{T} = \bigcup_{n=0}^{\infty} \mathcal{T}_n$ gde:

- $\mathcal{T}_0 = \mathcal{C} \cup \text{Var}$;
- $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{f(t_1, \ldots, t_{n_f}) \mid f \in \mathcal{F},\ t_1, \ldots, t_{n_f} \in \mathcal{T}_n\}$.

Vrednost terma

Fiksirajmo $\mathcal{L}$-strukturu $\mathcal{M}$.

Definicija

Valuacija je (bilo koje) preslikavanje $v : \mathrm{Var} \to M$.

Definicija

Vrednost terma t u valuaciji v, $t^{\mathcal{M}}[v]$, definišemo rekurentno:

- $t^{\mathcal{M}}[v] = c^{\mathcal{M}}$ ako je $t = c \in \mathcal{C}$;
- $t^{\mathcal{M}}[v] = v(x)$ ako je $t = x \in \mathrm{Var}$;
- $t^{\mathcal{M}}[v] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[v], \ldots, t_{n_f}^{\mathcal{M}}[v])$ ako je $t = f(t_1, \ldots, t_{n_f})$.

Vrednost terma

Tvrđenje

Vrednost terma zavisi samo od vrednosti valuacije u promenljivama koje se pojavljuju u termu.

U svakom termu pojavljuje se samo konačno mnogo promenljivih. Pišemo $t = t(\bar{x})$, gde $\bar{x} = (x_1, \ldots, x_m)$, da naglasimo da su promenljive koje se pojavljuju u termu t neke od $x_1, \ldots, x_m$. Tada pišemo $t^{\mathcal{M}}(\bar{a})$, $\bar{a} = (a_1, \ldots, a_m) \in M^m$, umesto $t^{\mathcal{M}}[v]$, gde je v bilo koja valuacija takva da $v(x_i) = a_i$.

Ako je $t = t(\bar{x})$, $|\bar{x}| = m$, term t određuje funkciju $t^{\mathcal{M}} : M^m \to M$ sa $\bar{a} \mapsto t^{\mathcal{M}}(\bar{a})$.

Vrednost terma

Tvrđenje

Ako je $\eta : \mathcal{M} \to \mathcal{N}$, t term i v valuacija, tada je

$$\eta(t^{\mathcal{M}}[v]) = t^{\mathcal{N}}[\eta \circ v].$$

Specijalno, ako je $t = t(\bar{x})$, $\eta(t^{\mathcal{M}}(\bar{a})) = t^{\mathcal{N}}(\eta(\bar{a}))$.

Tvrđenje

Neka je $A \subseteq M$. Najmanja podstruktura od $\mathcal{M}$ koja sadrži A definisana je na domenu:

$$\langle A \rangle = \{t^{\mathcal{M}}[v] \mid t \in \mathcal{T},\ v : \mathrm{Var} \to A\}.$$

Za $\langle A \rangle$ kažemo da je *podstruktura generisana sa A.*

Smena

Definicija

Ako su t, s termi i x promenljiva, sa $t[s/x]$ obeležavamo term t u kome smo sva pojavljivanja promenljive x zamenili termom s.

Lema

$$(t[s/x])^{\mathcal{M}}[v] = t^{\mathcal{M}}[v_{s^{\mathcal{M}}[v]/x}],$$

gde sa $v_{a/x}$, $a \in M$, obeležavamo valuaciju:

$$v_{a/x}(y) = \begin{cases} a & \text{ako } y = x \\ v(y) & \text{ako } y \neq x \end{cases}.$$

Formule

$\mathcal{L}$-formule zapisujemo koristeći simbole za zapis terma, znak $=$, veznik $\rightarrow$, konstantu $\bot$ i kvantifikator $\forall$.

Definicija

Skup $\mathcal{L}$-formula je najmanji skup, zloupotrebom notacije takođe označen sa $\mathcal{L}$ (smisao oznake uvek će biti jasan iz konteksta), takav da:

- $\bot \in \mathcal{L}$;
- $t_1 = t_2$ pripada $\mathcal{L}$, gde $t_1, t_2 \in \mathcal{T}$;
- $R(t_1, \ldots, t_{n_R})$, gde $R \in \mathcal{R}$ i $t_1, \ldots, t_{n_R} \in \mathcal{T}$;
- ako $\varphi, \psi \in \mathcal{L}$, onda $(\varphi \rightarrow \psi)$ pripada $\mathcal{L}$;
- ako $\varphi \in \mathcal{L}$ i $x \in \mathrm{Var}$, onda $(\forall x)\, \varphi$ pripada $\mathcal{L}$.

Za formule iz prve tri tačke kažemo da su *atomske*.

Formule

Alternativno, $\mathcal{L} = \bigcup_{n=0}^{\infty} \mathcal{L}_n$ gde:

- $\mathcal{L}_0 = \{\bot\} \cup \{t_1 = t_2 \mid t_1, t_2 \in \mathcal{T}\} \cup \{R(t_1, \ldots, t_{n_R}) \mid R \in \mathcal{R},\ t_1, \ldots, t_{n_R} \in \mathcal{T}\}$;
- $\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{(\varphi \to \psi) \mid \varphi, \psi \in \mathcal{L}_n\} \cup \{(\forall x)\, \varphi \mid \varphi \in \mathcal{L}_n,\ x \in \mathrm{Var}\}$.

Skraćenice:

- $\top := \bot \to \bot$;
- $\neg\varphi := \varphi \to \bot$;
- $\varphi \vee \psi := \neg\varphi \to \psi$;
- $\varphi \wedge \psi := \neg(\varphi \to \neg\psi)$;
- $\varphi \leftrightarrow \psi := (\varphi \to \psi) \wedge (\psi \to \varphi)$;
- $(\exists x)\, \varphi := \neg(\forall x)\, \neg\varphi$;
- $t_1 \neq t_2 := \neg\ t_1 = t_2$;

Tačnost formule

Fiksirajmo $\mathcal{L}$-strukturu $\mathcal{M}$. Oznake **t**/**n** čitamo kao tačno/netačno.

Definicija

Tačnost formule φ u valuaciji v, $\varphi^{\mathcal{M}}[v]$, definišemo rekurentno:

- $\varphi^{\mathcal{M}}[v] = \mathbf{n}$ ako je $\varphi = \bot$;
- $\varphi^{\mathcal{M}}[v] = \mathbf{t}$ akko $t_1^{\mathcal{M}}[v] = t_2^{\mathcal{M}}[v]$, ako je φ formula $t_1 = t_2$;
- $\varphi^{\mathcal{M}}[v] = \mathbf{t}$ akko $(t_1^{\mathcal{M}}[v], \ldots, t_{n_R}^{\mathcal{M}}[v]) \in R^{\mathcal{M}}$, ako je φ formula $R(t_1, \ldots, t_{n_R})$;
- $\varphi^{\mathcal{M}}[v] = \mathbf{n}$ akko $\psi^{\mathcal{M}}[v] = \mathbf{t}$ i $\theta^{\mathcal{M}}[v] = \mathbf{n}$, ako je φ formula $\psi \to \theta$;
- $\varphi^{\mathcal{M}}[v] = \mathbf{t}$ akko $\psi^{\mathcal{M}}[v_{a/x}] = \mathbf{t}$ za sve $a \in M$, ako je φ formula $(\forall x)\,\psi$.

Tačnost formule

Komentari

- Formule $\top$, $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \leftrightarrow \psi$ imaju očekivane vrednosti.
- Ako je φ formula $(\exists x)\,\psi$, $\varphi^{\mathcal{M}}[v] = \mathbf{t}$ akko $\psi^{\mathcal{M}}[v_{a/x}] = \mathbf{t}$ za neko $a \in M$.

Definicija

Pišemo:

- $(\mathcal{M}, v) \models \varphi$ ako $\varphi^{\mathcal{M}}[v] = \mathbf{t}$; inače, $(\mathcal{M}, v) \not\models \varphi$;
- $\mathcal{M} \models \varphi$, $\mathcal{M}$ je *model* za φ, ako $(\mathcal{M}, v) \models \varphi$ za sve $v : \mathrm{Var} \to M$; inače, $\mathcal{M} \not\models \varphi$, $\mathcal{M}$ je *kontramodel* za φ;
- $\models \varphi$, φ je *valjana*, ako $\mathcal{M} \models \varphi$ za sve $\mathcal{M}$; inače, $\not\models \varphi$, φ nije valjana.

Tačnost formule

Tvrđenje

Neka je $\eta : \mathcal{M} \to \mathcal{N}$, φ beskvantorna formula i $v : \mathrm{Var} \to M$. Tada $(\mathcal{M}, v) \models \varphi$ akko $(\mathcal{N}, \eta \circ v) \models \varphi$.

Tvrđenje

Neka je $\mathcal{M} \leqslant \mathcal{N}$, φ beskvantorna formula i $v : \mathrm{Var} \to M$. Tada $(\mathcal{M}, v) \models \varphi$ akko $(\mathcal{N}, v) \models \varphi$.

Zadatak

Dokazati da je bitno da je φ beskvantorna formula.

Zadatak

Dokazati $\models (\exists x)(\forall y)\, \varphi \to (\forall y)(\exists x)\, \varphi$ i dati primer formule φ takav da $\not\models (\forall x)(\exists y)\, \varphi \to (\exists y)(\forall x)\, \varphi$.

Slobodno i vezano pojavljivanje promenljive

Definicija

Pojavljivanje promenljive u formuli je *vezano* ako je pod dejstvom kvantifikatora; inače je *slobodno*. Primetimo da ista promenljiva može da ima i slobodna i vezana pojavljivanja.

Ako formula φ nema slobodna pojavljivanja promenljivih, kažemo da je φ *rečenica*.

Tvrđenje

Tačnost $\varphi^{\mathcal{M}}[v]$ zavisi samo od vrednosti valuacije v u promenljivama koje imaju slobodna pojavljivanja u formuli φ.

Specijalno, tačnost rečenice ne zavisi od valuacije (samo od strukture).