

Indukcija

Ukvarjali se bomo z najmanjšimi množicami, zaprtimi za dana pravila.

Primeri ind. množic

- naravna števila - \mathbb{N}

$$\frac{}{\underline{0 \in \mathbb{N}}} \quad \frac{n \in \mathbb{N}}{\underline{n^+ \in \mathbb{N}}}$$

predpostavke



$$\underline{P_1 \ P_2 \ \dots \ P_n}$$

\exists

zaključek

- seznamni elementov iz $A - A^*$

$$\frac{}{\underline{[] \in A^*}} \quad \frac{x \in A \quad x \in A^*}{\underline{x::x \in A^*}}$$

- aritmetični izrazi - \mathbb{E}

$$e ::= \underline{m} | e_1 + e_2 | e_1 * e_2 | -e$$

$$\frac{m \in \mathbb{Z}}{\underline{m \in \mathbb{E}}} \quad \frac{e_1 \in \mathbb{E} \quad e_2 \in \mathbb{E}}{e_1 + e_2 \in \mathbb{E}} \quad \frac{e_1 \in \mathbb{E} \quad e_2 \in \mathbb{E}}{e_1 * e_2 \in \mathbb{E}} \quad \frac{e \in \mathbb{E}}{-e \in \mathbb{E}}$$

Primeri ind. relacij

- soda naravna števila - m soda

$$\frac{}{\underline{0 \text{ soda}}} \quad \frac{m \text{ soda}}{\underline{m^+ \text{ soda}}}$$

- urejenost naravnih števil - $m \leq m$

$$\frac{(m \in \mathbb{N})}{\underline{0 \leq m}} \quad \frac{m \leq m}{\underline{m^+ \leq m^+}}$$

$$\frac{\underline{0 \leq 1}}{\underline{1 \leq 2}} \quad \underline{2 \leq 3}$$

- elementi seznamov - $x \in xs$

$$\frac{(x \in A) \ (x \in A^*)}{\underline{x \in x :: x S}} \quad \frac{(y \in A) \ x \in xs}{\underline{x \in y :: x S}}$$

$$\frac{}{\underline{m \leq' m}}$$

$$\frac{m \leq' m}{\underline{m \leq' m^+}}$$

• operacijska semantika jezika IMP

$$\frac{\begin{array}{l} S, e \Downarrow m \\ \text{Sintakse} \quad \text{Semantika} \end{array}}{S, b \Downarrow r}$$

$$S, c \Downarrow S'$$

$$\frac{\begin{array}{c} S, m \Downarrow m \\ l \mapsto m \in S \end{array}}{S, l \Downarrow m}$$

$$\frac{S, e_1 \Downarrow m_1 \quad S, e_2 \Downarrow m_2}{S, e_1 + e_2 \Downarrow m_1 + m_2}$$

$$\frac{S, b \Downarrow \# \quad S, c_1 \Downarrow S'}{S, \text{if } b \text{ then } c_1 \text{ else } c_2 \Downarrow S'}$$

$$\frac{S, b \Downarrow ff \quad S, c_2 \Downarrow S'}{S, \text{if } b \text{ then } c_1 \text{ else } c_2 \Downarrow S'}$$

$$\frac{\begin{array}{c} \overline{D, 1 \Downarrow 1 \quad C, 1 \Downarrow 1} \\ \overline{C, 3 \Downarrow 3 \quad C, 1+1 \Downarrow 2} \\ \overline{C, 3 \leftarrow 1+1 \Downarrow ff \quad C, \text{skip} \Downarrow []} \end{array}}{C, \text{if } 3 < 1+1 \text{ then } \dots \text{ else skip} \Downarrow []}$$

Ind. relacije kot ind. množice

Induktivno relacije bomo namesto s podmnožico $R \subseteq X$ predstavili z družino induktivnih množic $(R_x)_{x \in X}$, kjer bo R_x neprazna natanko tedaj, kadar bo $x \in R$.

- Sedeževila - $(\text{Sode}_m)_{m \in \mathbb{N}}$

$$\frac{\text{nic je } \text{Sodo} \in \text{Sodo}_0}{\text{nasi! Nasli! Sode} \Rightarrow \text{je Sod d} \in \text{Sodo}_{n++}}$$

Indukcija

Vsaka ind. množica ima ustrezno načelo indukcije, ki pove, da predikat P velja za vse elemente, kadar velji za zaključke vseh pravil ob ind. predpostavkah pripadajočih predpostavk pravil.

$$\frac{H_1 \dots H_n}{?} \quad P(H_1) \wedge \dots \wedge P(H_n) \Rightarrow P(?)$$

• načelo indukcije za \leq

P... predikat ne $m \leq m$ oz. ne parit m, m

$$(\forall m. P(0 \leq m)) \wedge (\forall m, m. P(m \leq m) \Rightarrow P(m+ \leq m+)) \Rightarrow \forall m, m. P(m \leq m)$$

Primer: \leq je tranzitivna

$$\underline{m \leq m} \wedge \underline{m \leq p} \Rightarrow \underline{m \leq p}$$

$$m \leq m \Rightarrow (m \leq p \Rightarrow m \leq p)$$

Dokaz

Z indukcijo na $m \leq m$. Ločimo prvo zadnje uporabljenega pravila:

- $m = 0$ in pravilo je bilo $\frac{0 \leq m}{0 \leq p}$. Teden je $\frac{0 \leq p}{0 \leq p}$ po istem pravilu.

- $m = m^+$, $m = m^+$ in pravilo je bilo $\frac{m' \leq m'}{m^+ \leq m^+}$. Teden je edina možnost za $m \leq p$ je, da je $p = p^+$ in $\frac{m' \leq p'}{m^+ \leq p^+}$.

Po I.P. velja $m' \leq p'$, zato velja $m \leq p$ po pravilu $\frac{m' \leq p'}{m^+ \leq p^+}$.

Konstrukcija ind. množic

Vsako množico pravil bomo predstavili s preslikavo F , ki množico X shilca $\cup F X$.

- naravna števila \mathbb{N}

$$X \mapsto 1 + X \quad 0 := l_1(*) \\ m^+ := l_2(n) \\ \emptyset, 1 + \emptyset, 1 + (1 + \emptyset), \dots \\ l_1(*), l_1(*), l_2(l_1(*)), \dots$$

$$A + B = \{l_1(a) \mid a \in A\} \cup \{l_2(b) \mid b \in B\}$$

$$1 = \{*\}$$

- seznamni A^*

$$X \mapsto 1 + A \times X \quad [] := l_1(*) \\ x :: xs = l_2((x, xs))$$

- aritmetični razli \mathbb{E}

$$X \mapsto \mathbb{Z} + X \times X + X \times X + X \quad m := l_1(n) \\ e_1 + e_2 := l_2((e_1, e_2)) \\ \vdots$$

V splošnem bomo družino pravil zapisali s preslikavo, ki ima za vsako pravilo en sumand, ki ustrezza predpostavkom pravila.

Predpostavimo, da F zadovlja pogojeva:

- monotonost: $X \subseteq Y \Rightarrow FX \subseteq FY$
- definiranost s končnimi podmnožicami (Scottova zveznost):

$$FX = \bigcup_{A \subseteq \text{končna } X} FA$$

Primeri preiskav, ki zadovljajo pogojeva:

- konstantna $X \mapsto A$ ✓
- vsota $X \mapsto FX + GX$, ker F, G zadovljata pogojeve

$$X \subseteq Y \Rightarrow FX \subseteq FY \wedge GX \subseteq GY \Rightarrow FX + GX \subseteq FY + GY$$

$$FX + GX = \bigcup_{A \subseteq \text{končne } X} FA + \bigcup_{A \subseteq \text{končne } X} GA$$

$$= \{ l_1(x) \mid \exists A \subseteq X. x \in FA \} \cup \{ l_2(y) \mid \exists A \subseteq X. y \in GA \}$$

$$= \bigcup_{A \subseteq \text{končne } X} (FA + GA)$$

■

- produkt **vaje**

- potencije množice

$$I_0 := \emptyset \quad I_{n+1} := F I_n \quad I = \bigcup_{n=0}^{\infty} I_n$$

Vej je:

- I je zaprta za F $F I \subseteq I$

- I je najmanjše množice, zaprta za F $FX \subseteq X \Rightarrow I \subseteq X$

- $I = FI$

Dokaz:

- $FI = F \left(\bigcup_{n=0}^{\infty} I_n \right) = \bigcup_{A \subseteq I} FA \subseteq \bigcup_{A \subseteq I} I = I$

$$A \subseteq I \Rightarrow \exists n. A \subseteq I_n \Rightarrow \exists n. FA \subseteq FI_n = I_{n+1} \subseteq I$$

- Vzamimo X , da je $FX \subseteq X$. ko je F monototon

$$I_0 = \emptyset \subseteq X \quad I_{n+1} = FI_n \subseteq FX \subseteq X$$

$$I = \bigcup_{n=0}^{\infty} I_n \subseteq X.$$

- D.N.

V zemnina I in množico P , povejmo s preslikavo F kot zgoraj in predikat P na I .
Naj bo $Q = \{x \in I \mid P(x)\}$. Če je $FQ \subseteq Q$, potem je $I \subseteq Q$, zato
velja $\forall x \in I. P(x)$.

Primer

$$I = \mathbb{N}, Fx = 1 + x$$

$$FQ \subseteq Q = \{m \in \mathbb{N} \mid P(m)\}$$

||

$$1 + Q = \{0\} \cup \{m^+ \mid m \in \mathbb{N} \wedge P(m)\}$$

Kaj smo izpustili

- konstrukcijo drugih induktivnih množic
- rekurzijo
 $\text{eval}: E \rightarrow \mathbb{Z} (\mathbb{R})$

$$\text{eval}(m) = m$$

$$\text{eval}(e_1 + e_2) = \text{eval}(e_1) + \text{eval}(e_2)$$

$$\text{eval}(e_1 * e_2) = \text{eval}(e_1) * \text{eval}(e_2)$$

$$\text{eval}(-e) = -\text{eval}(e)$$

Če imamo preslikavo

$$\alpha: Fx \rightarrow X, \text{ potem}$$

obstaja enolična preslikava

$$f: I \rightarrow X, \text{ da velja}$$

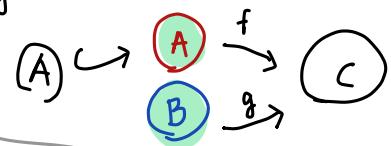
$$\begin{array}{ccc} Fx & \xrightarrow{\alpha} & Fx \\ \parallel & \downarrow & \dots \text{algebra } x \\ I & \xrightarrow[f]{\quad} & X \end{array}$$

$$\mathbb{N} \cup \emptyset = \emptyset$$

$$\mathbb{N} + \emptyset = \{l_n(0), l_1(1), \dots\}$$

$$\{\dots, l_2(-1), l_2(0), l_2(1), \dots\}$$

$$\begin{array}{c} f: A \rightarrow C \\ g: B \rightarrow C \end{array} \Leftrightarrow [f \mid g]: A + B \rightarrow C$$



$$\emptyset \rightarrow \emptyset \qquad \emptyset \rightarrow \mathbb{R}$$

$$\emptyset \times \emptyset \rightarrow \emptyset \qquad \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$$

$$\emptyset \times \emptyset \rightarrow \emptyset \qquad \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$$

$$\emptyset \rightarrow \emptyset \qquad \mathbb{R} \rightarrow \mathbb{R}$$

$$\underbrace{\emptyset + \emptyset \times \emptyset + \emptyset \times \emptyset + \emptyset}_{F\emptyset} \rightarrow \emptyset$$

$$\underbrace{\emptyset + \mathbb{R} \times \mathbb{R} + \mathbb{R} \times \mathbb{R} + \mathbb{R}}_{F\mathbb{R}} \rightarrow \mathbb{R}$$

