Indukcija

Induktivne množice

Naravna števila

Induktivne množice so definirane kot najmanjše množice, ki so zaprte za dane konstrukcije elementov. Na primer, množico naravnih števil $\mathbb{N}$ lahko definiramo kot **najmanjšo** množico, ki:

vsebuje 0 in za poljuben n vsebuje tudi njegovega naslednika n^+.

Pravili dostikrat zapišemo tudi v obliki: $$ \frac{}{0 \in \mathbb{N}} \quad \frac{n \in \mathbb{N}}{n^+ \in \mathbb{N}} $$ V splošnem bomo uporabljali pravila oblike $$ \frac{h_1 \quad h_2 \quad \cdots \quad h_n}{c}, $$ kjer nad črto pišemo *predpostavke* $h_1, \dots, h_n$, pod črto pa *zaključek* c. Pravilom oblike $$ \frac{}{\quad c \quad}, $$ ki nad črto nimajo predpostavk, pravimo *aksiomi*.

Katere elemente vsebuje $\mathbb{N}$?

1. Zaradi prvega pogoja mora veljati $0 \in \mathbb{N}$.
2. Sedaj mora zaradi drugega pogoja $\mathbb{N}$ vsebovati tudi 0^+, ki ga označimo z 1.
3. Podobno nadaljujemo in vidimo, da $\mathbb{N}$ vsebuje tudi $1^+ = 2$.

Na vsakem koraku dobimo novo naravno število in obratno, vsak element $\mathbb{N}$ dobimo tako, da končno mnogokrat uporabimo eno od zgoraj naštetih pravil (čeprav resda prav veliko izbire nimamo).

Aritmetični izrazi

Podobno lahko mnnožico aritmetičnih izrazov $\mathbb{E}$, ki smo jo definirali že z BNF sintakso $$ e ::= n \ |\ e_1 + e_2 \ |\ e_1 * e_2 \ |\ -e, $$ definiramo tudi kot najmanjšo množico, ki:

- vsebuje vsako celo število n,
- za poljubna izraza $e_1, e_2 \in \mathbb{E}$ vsebuje tudi izraz $e_1 + e_2$,
- za poljubna izraza $e_1, e_2 \in \mathbb{E}$ vsebuje tudi izraz $e_1 * e_2$ in
- za poljuben izraz $e \in \mathbb{E}$ vsebuje tudi izraz $-e$;

oziroma s pravili $$ \frac{}{n \in \mathbb{E}}(n \in \mathbb{N}) \quad \frac{e_1 \in \mathbb{E}\quad e_2 \in \mathbb{E}}{e_1 + e_2 \in \mathbb{E}} \quad \frac{e_1 \in \mathbb{E}\quad e_2 \in \mathbb{E}}{e_1 * e_2 \in \mathbb{E}} \quad \frac{e \in \mathbb{E}}{-e \in \mathbb{E}} $$ Opazimo, da smo pri prvem pravilu $n \in \mathbb{N}$ zapisali kot stranski pogoj, saj je množica $\mathbb{N}$ že definirana in ni podana z napisanimi pravili.

Tudi tu vse elemente $\mathbb{E}$ dobimo tako, da končno mnogokrat uporabljamo pravila.

1. Najprej vidimo, da $\mathbb{E}$ vsebuje vsa števila $\dots, -2, -1, 0, 1, 2, \dots$.
2. Sedaj iz preostalih treh pravil sledi, da mora $\mathbb{E}$ tega mora vsebovati tudi vse njihove vsote $(0 + 0), (0 + 1), (1 + 0), (-2 + 3), \dots$, njihove produkte $(0 \ast 0), (0 \ast 1), (1 \ast 0), (-2 \ast 3), \dots$ ter njihove negacije $-0, -1, -(-42), \dots$
3. Nato vidimo, da mora $\mathbb{E}$ vsebovati tudi vse kombinacije elementov, ki smo jih obili v prejšnjih korakih, na primer $(-2 + 3) \ast (0 \ast 1)$ ali $-(-42) + (6 \ast 7)$.

Če postopek nadaljujemo, dobimo vse elemente množice $\mathbb{E}$, vsakega v končno mnogo korakih. Vsakemu elementu $e \in \mathbb{E}$ pripada tudi natanko določeno *drevo izpeljave*, iz katerega se vidi, kako smo prišli do dejstva, da $\mathbb{E}$ vsebuje e. V tem drevesu je e koren, pravila so vozlišča, aksiomi pa listi. Na primer, elementu $42 + (6 \ast 7)$ pripada drevo $$ \frac { \frac {} {42 \in \mathbb{E}} \quad \frac {\frac{}{6 \in \mathbb{E}} \quad \frac{}{7 \in \mathbb{E}}} {6 \ast 7 \in \mathbb{E}} } {42 + (6 \ast 7) \in \mathbb{E}} $$ Vidimo, da na n-tem koraku dobimo ravno tiste elemente z drevesom izpeljave višine n.

Induktivno podane relacije

Pri teoriji programskih jezikov bomo pogosto uporabljali induktivno podane relacije, s katerimi bomo na primer definirali, kdaj se en izraz evalvira v drugega ali pa kdaj ima dani izraz veljaven tip. V preostanku tega razdelka pa si bomo izbrali bolj enostaven primer in sicer soda naravna števila.

Ker so relacije definirane kot podmnožice domene, bi lahko induktivno podane relacije podali kot najmanjše podmnožice, zaprte za dana pravila. Tako bi množico sodih naravnih števil definirali kot najmanjšo podmnožico $S \subseteq \mathbb{N}$, zaprto za pravili: $$ \frac{}{0 \in S} \quad \frac{n \in S}{n + 2 \in S} $$ Da pa bomo vse spravili pod eno samo definicijo, hkrati pa še bolj zvesto sledili pristopu, ki ga uporablja Agda, bomo raje definirali družino množic sodo_n, ki bodo predstavljale dokaze, da je n sodo število. Množica sodo_n bo torej neprazna, kadar bo n sodo, in prazna, kadar bo n liho. Zgornji pravili bi tako lahko napisali kot: $$ \frac{}{\mathsf{nicJeSodo} \in \mathsf{sodo}_0} \quad \frac{p \in \mathsf{sodo}*n}{\mathsf{sodoPlusDvaJeSodo} , p \in \mathsf{sodo}*{n + 2}} $$ Za množice sodo_n imamo torej dva konstruktorja. Konstanto $\mathsf{nicJeSodo}$ ter konstruktor $\mathsf{sodoPlusDvaJeSodo}$, ki dokaže, da je $n + 2$ sodo, kadar obstaja dokaz p, da je n sodo. Preverimo lahko, da je množica sodo_n neprazna natanko tedaj, kadar je $n \in S$.

Pri relacijah bomo pravila za konstrukcijo množic pisali malo drugače, da bomo bolj poudarili njihovo vsebino: $$ \def\sc#1{\small\dosc#1\csod} \def\dosc#1#2\csod{{\rm #1{\scriptsize #2}}} \frac{}{0 , \mathsf{sodo}} \sc{NIC}\sc{JE}\sc{SODO} \quad \frac{n , \mathsf{sodo}}{n + 2 , \mathsf{sodo}} \sc{SODO}\sc{PLUS}\sc{DVA}\sc{JE}\sc{SODO} $$ Če nas imena pravil (torej konstruktorjev) ne bodo zanimala, jih bomo izpustili.

Konstrukcija induktivnih množic

Predstavitev množice pravil s preslikavo

Induktivne množice bomo gradili po korakih: v prvem koraku bomo dodali vse elemente, ki sledijo iz aksiomov, nato tiste, ki imajo drevesa izpeljave z globino 1, tiste z globino 2 in tako naprej. Pri tem bomo vsako množico pravil predstavili s preslikavo F, ki množico X slika v množico $F X$, sestavljeno iz vseh zaključkov pravil, katerih predpostavke so vsebovane v X. Množica X bo torej zaprta za pravila natanko tedaj, kadar bo $F X \subseteq X$. "Ulomke", kot smo jih pisali doslej, bomo uporabljali še naprej, vendar nam bodo le služili kot krajši zapis preslikave F.

Za primer si oglejmo množico naravnih števil. Spomnimo se na pravili: $$ \frac{}{0 \in \mathbb{N}} \quad \frac{n \in \mathbb{N}}{n^+ \in \mathbb{N}} $$ Ker so naravna števila dveh različnih oblik (nič oz. naslednik), bomo v konstrukciji množice $F X$ nastopala disjunktna vsota. Ničla nima nobenega dodatnega argumenta, zato jo bomo predstavili z $\iota_1(\ast)$, kjer je $\ast$ edini element singletona 1. Naslednik pa ima en argument, ki mora priti iz množice predpostavk, zato ga bomo predstavili z $\iota_2(x)$, kjer je $x \in X$. Zato bomo množico pravil za naravna števila predstavili s preslikavo $F X = 1 + X$. Število 2 bi predstavljal element $\iota_2(\iota_2(\iota_1(\ast))$

V splošnem vsakemu pravilu ustreza en sumand v disjunktni vsoti, sestavljen iz množic, ki ustrezajo predpostavkam pravil. Recimo, pravilom za aritmetične izraze $$ \frac{}{n \in \mathbb{E}}(n \in \mathbb{N}) \quad \frac{e_1 \in \mathbb{E}\quad e_2 \in \mathbb{E}}{e_1 + e_2 \in \mathbb{E}} \quad \frac{e_1 \in \mathbb{E}\quad e_2 \in \mathbb{E}}{e_1 * e_2 \in \mathbb{E}} \quad \frac{e \in \mathbb{E}}{-e \in \mathbb{E}} $$ ustreza preslikava $$ F X = \mathbb{N} + (X \times X) + (X \times X) + X $$

Konstrukcija induktivnih množic

Predpostavimo, da je preslikava F:

- monotona, torej da iz $X \subseteq Y$ velja $F X \subseteq F Y$, in
- definirana z vrednostmi na končnih podmnožicah, torej da je $F X = \bigcup_{A \subseteq^{\text{končna}} X} F A$

Naj bo A poljubna množica ter naj bosta F in G preslikavi, ki zadoščata zgornjima dvema pogojema. Tedaj zgornjima dvema pogojema zadoščajo tudi preslikave

- $X \mapsto A$,
- $X \mapsto F X + G X$ in
- $X \mapsto F X \times G X$

ter s tem tudi preslikavi, s katerima smo definirali naravna števila in aritmetične izraze. Primer preslikave, ki ne zadošča drugemu pogoju je potenciranje $X \mapsto \mathcal{P} X$.

Definirajmo zaporedje $$ I_0 = \emptyset \qquad I_{n + 1} = F I_n $$ ter pokažimo, da je $I = \bigcup_{n = 0}^{\infty} I_n$ najmanjša množica, zaprta za F. Preverimo lahko, da I_n vsebuje natanko tiste elemente, katerih drevo izpeljave ima globino kvečjemu n.

Pokažimo najprej, da je $F I \subseteq I$. Ker je F definirana z vrednostmi na končnih podmnožicah, velja $$ F I = \bigcup_{A \subseteq^{\text{končna}} I} F A $$ Ker je $I = \bigcup_{n = 0}^{\infty} I_n$, za vsako končno $A \subseteq I$ obstaja tak n, da je $A \subseteq I_n$. Ker je F monotona, je $F A \subseteq F I_n = I_{n + 1} \subseteq I$. Torej je tudi $\bigcup_{A \subseteq^{\text{končna}} I} F A \subseteq I$.

Vzemimo še množico X, da velja $F X \subseteq X$ ter pokažimo, da je $I \subseteq X$. Z indukcijo najprej pokažimo, da je $I_n \subseteq X$. Ker je $I_0 = \emptyset \subseteq X$, je osnovni korak trivialen. Sedaj predpostavimo, da velja $I_n \subseteq X$. Tedaj velja tudi $I_{n + 1} = F I_n \subseteq F X \subseteq X$, saj je preslikava F monotona. Ker so vsi členi $I_n \subseteq X$, velja tudi $I = \bigcup_{n = 0}^{\infty} I_n \subseteq X$.

Dokazovanje z indukcijo

To lastnost lahko uporabimo za *dokazovanje z indukcijo*. Vsak predikat P na I lahko predstavimo z množico $Q = \{ x \in I \mid P(x) \}$. Če velja $F Q \subseteq Q$, mora biti $Q = I$, saj je I najmanjša množica, zaprta za F. Na primer, za $F X = 1 + X$ in $I = \mathbb{N}$ se trditev $F Q \subseteq Q$ prevede na $1 + Q \subseteq Q$. To pomeni, da mora veljati $\iota_1(\ast) \in Q$ ter $\iota_2(n) \in Q$ za vsak $n \in Q$. Prvi pogoj nam pove, da je $0 \in Q$, drugi pogoj pa, da iz $n \in Q$ sledi $n^+ \in Q$, kar je skupaj ravno običajno načelo indukcije

$$ P(0) \land (\forall n \in \mathbb{N}. P(n) \Rightarrow P(n^+)) \implies \forall m \in \mathbb{N}. P(m) $$

Za aritmetične izraze in $F X = \mathbb{N} + (X \times X) + (X \times X) + X$ podobno dobimo načelo indukcije

$$\begin{aligned} &(\forall n \in \mathbb{N} . P(n)) \ &\land (\forall e_1, e_2 \in \mathbb{E}. P(e_1) \land P(e_2) \Rightarrow P(e_1 + e_2)) \ &\land (\forall e_1, e_2 \in \mathbb{E}. P(e_1) \land P(e_2) \Rightarrow P(e_1 \ast e_2)) \ &\land (\forall e \in \mathbb{E}. P(e) \Rightarrow P(-e)) \ &\implies \forall e \in \mathbb{E}. P(e) \end{aligned}$$