Indukcija in dobra osnovanost

Dobra osnovanost

Indukcija na naravnih številih

Poznamo že indukcijo na naravnih številih. Zapišemo jo lahko na več načinov, kjer naslednika števila n označimo n^+:

1. Kot aksiom o predikatih na naravnih številih:

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

2. Kot lastnost podmnožic naravnih števil:

   $$\forall\, S \in \mathcal{P}(\mathbb{N}) \,.\, 0 \in S \land (\forall\, k \in \mathbb{N} \,.\, k \in S \Rightarrow k^+ \in S) \Rightarrow S = \mathbb{N}$$

Uporabljali bomo verzijo s podmnožicami. Najprej jo predelajmo v ekvivalentno obliko:

$$\forall\, S \in \mathcal{P}(\mathbb{N}) \,.\, 0 \in S \land (\forall\, k \in \mathbb{N} \,.\, k \in S \Rightarrow k^+ \in S) \Rightarrow S = \mathbb{N}$$
$$\forall\, S \in \mathcal{P}(\mathbb{N}) \,.\, 0 \in S \land (\forall\, m \in \mathbb{N} \,.\, (\forall\, k \in \mathbb{N} \,.\, k^+ = m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N}$$
$$\forall\, S \in \mathcal{P}(\mathbb{N}) \,.\, (\forall\, m \in \mathbb{N} \,.\, (\forall\, k \in \mathbb{N} \,.\, k^+ = m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N}$$

Kaj smo dosegli? Bazo indukcije in indukcijski korak smo združili v eno samo predpostavko

$$\forall\, m \in \mathbb{N} \,.\, (\forall\, k \in \mathbb{N} \,.\, k^+ = m \Rightarrow k \in S) \Rightarrow m \in S \qquad (1)$$

Če vstavimo $m := 0$, dobimo:

$$(\forall\, k \in \mathbb{N} \,.\, k^+ = 0 \Rightarrow k \in S) \Rightarrow 0 \in S$$
$$(\forall\, k \in \mathbb{N} \,.\, \bot \Rightarrow k \in S) \Rightarrow 0 \in S$$
$$(\forall\, k \in \mathbb{N} \,.\, \top) \Rightarrow 0 \in S$$
$$\top \Rightarrow 0 \in S$$
$$0 \in S$$

Če vstavimo $m := n^+$ dobimo:

$$\forall\, m \in \mathbb{N} \,.\, (\forall\, k \in \mathbb{N} \,.\, k^+ = n^+ \Rightarrow k \in S) \Rightarrow n^+ \in S$$
$$\forall\, m \in \mathbb{N} \,.\, (\forall\, k \in \mathbb{N} \,.\, k = n \Rightarrow k \in S) \Rightarrow n^+ \in S$$
$$\forall\, m \in \mathbb{N} \,.\, n \in S \Rightarrow n^+ \in S$$

To pa sta ravno običajna pogoja za indukcijo.

Ali lahko izrazimo indukcijo na naravnih številih tudi brez operacije naslednik? Da, s pomočjo relacije $<$:

$$\forall\, S \in \mathcal{P}(\mathbb{N}) \,.\, (\forall\, m \in \mathbb{N} \,.\, (\forall\, k \in \mathbb{N} \,.\, k < m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N}$$

Temu principu pravimo tudi *krepka indukcija*, z besedami jo povemo takole: Za podmnožico $S \subseteq \mathbb{N}$ velja $S = \mathbb{N}$, če za vse $m \in \mathbb{N}$ velja:

> Če so vsa števila manjša od m v S, potem je tudi m v S.

Denimo, da S res ima dano lastnost. Ali je $0 \in S$? Da, ker za vse predhodnike 0 velja, da so S (saj jih ni). Ali je $1 \in S$? Da, saj za vse predhodnike 1 velja, da so v S. Ali je $2 \in S$? Da, saj za vse predhodnike 2 velja, da so v S. In tako naprej.

Dobra osnovanost

Princip indukcije na naravnih številih posplošimo.

Definicija: Relacija $R \subseteq A \times A$ je **dobro osnovana**, če velja:

$$\forall S \in P(A) . (\forall y \in A . (\forall x \in A . x R y \Rightarrow x \in S) \Rightarrow y \in S) \Rightarrow S = A.$$

Množici $S \subseteq A$, ki zadošča pogoju

$$\forall y \in A . (\forall x \in A . x R y \Rightarrow x \in S) \Rightarrow y \in S$$

pravimo **R-progresivna** množica.

Kaj smo pravzaprav naredili: opazili smo, da ima relacija "k je neposredni predhodnik m" na N pomembno lastnost (1). Zanima nas, ali imajo tudi druge relacije to lastnost, saj nam bodo omogočile neke vrste posplošen princip indukcije. Z definicijo smo dali relacijam, ki nas zanimajo, ime.

Primer: dvojiška drevesa

Naravna števila N so *induktivno definirana množica*. To pomeni, da elemente N opredelimo s pravili, ki povedo, kako se gradi naravna števila:

1. $0 \in N$
2. če je $n \in N$, potem je $n^+ \in N$

Množica N vsebuje natanko tiste elemente, ki jih lahko zgradimo s pomočjo teh pravil:

$$0, 0^+, 0^{++}, 0^{+++}, 0^{++++}, \ldots$$

Tu sta 0 in $^+$ mišljena kot simbolni oznaki, podobno kot ι_1 in ι_2 v definiciji vsote množic.

Na tak način lahko definiramo tudi druge množice. Na primer, **dvojiška drevesa** so induktivno definirana množica Tree, s predpisoma:

1. $\mathtt{empty} \in \mathtt{Tree}$
2. če je $t_1 \in \mathtt{Tree}$ in $t_2 \in \mathtt{Tree}$, potem je $\mathtt{tree}(t_1, t_2) \in \mathtt{Tree}$

Z besedami: drevo je bodisi prazno, bodisi je sestavljeno iz dveh *poddreves*. Ali znamo našteti vsa drevesa, ali še bolje, jih narisati?

```
empty,
tree(empty, empty)
tree(empty, tree(empty, empty)),
tree(tree(empty, empty), empty),
tree(tree(empty, empty), tree(empty, empty)),
⋮
```

Definirajmo relacijo $R \subseteq \mathtt{Tree} \times \mathtt{Tree}$ s predpisom:

$$t R s \Leftrightarrow \exists u \in \mathtt{Tree} . s = \mathtt{tree}(t, u) \vee s = \mathtt{tree}(u, t)$$

To je relacija "neposredno poddrevo". Ta relacija je dobro osnovana (česar ne bomo dokazali) in nje pa dobimo naslednji princip indukcije za dvojiška drevesa.

Indukcija za dvojiška drevesa: Naj bo $S \subseteq Tree$ podmnožica dreves, za katero velja:

1. Prazno drevo je v S.
2. Za vsa drevesa t_1 in t_2 velja: če je $t_1 \in S$ in $t_2 \in S$, potem je $tree(t_1, t_2) \in S$.

Tedaj je $S = Tree$.

Princip povejmo še kot logični princip:

Indukcija za dvojiška drevesa: Naj bo φ lastnost dvojiških dreves, za katero velja:

1. Baza indukcije: $\varphi(empty)$
2. Indukcijski korak: za vsa drevesa t_1 in t_2, če velja $\varphi(t_1)$ in $\varphi(t_2)$, potem $\varphi(tree(t_1, t_2))$.

Tedaj $\forall\ t \in Tree,\ \varphi(t)$.

Kot vidimo, imamo v indukcijskem koraku *dve* indukcijski predpostavki, ker ima vsako sestavljeno drevo dve poddrevesi.

Dobra osnovanost in padajoče verige

Kako pa bi dobili kak protiprimer, se pravi, relacijo, ki ni dobra osnovanost? Poiskati moramo kako lastnost, ki jo imajo vse dobre osnovanosti.

Definicija: Naj bo $R \subseteq A \times A$ relacija na A. **Padajoča veriga** (za relacijo R) je zaporedje $a : N \to A$, za katerega velja $\forall\ i \in N\ .\ a(i+1)\ R\ a(i)$.

Se pravi, da je padajoča veriga zaporedje, za katerega velja

$$\cdots\ a_4\ R\ a_3\ R\ a_2\ R\ a_1\ R\ a_0$$

Cikel je končna podmnožica $\{a_0, \ldots, a_n\}$ da velja

$$a_0\ R\ a_1\ R\ \cdots\ R\ a_n\ R\ a_0$$

Iz takega cikla dobimo padajočo verigo, tako da cikel ponavljamo v nedogled:

$$\cdots\ R\ a_0\ R\ \cdots\ R\ a_n\ R\ a_0\ R\ a_1\ R\ \cdots\ R\ a_n\ R\ a_0$$

Lemma: V dobri osnovanosti ni ciklov in ni padajočih verig.

Dokaz. Dovolj je pokazati, da ni padajočih verig, saj iz cikla dobimo padajočo verigo. Denimo, da je $a : N \to A$ padajoča veriga za $R \subseteq A \times A$. Dokazali bomo, da R ni dobro osnovana. Se pravi, da moramo poiskati R-progresivno podmnožico $S \subseteq A$, za katero velja $S \neq A$. Vzemimo $S := A \setminus \{ a(i) \mid i \in N \}$. Očitno velja $S \neq A$, saj je $a(0) \in A$ in $a(0) \notin S$. Preverimo, da je S progresivna, se pravi, da je

$$\forall\ y \in A\ .\ (\forall\ x \in A\ .\ x\ R\ y \Rightarrow x \in S) \Rightarrow y \in S$$

Naj bo $y \in A$ in denimo, da velja

$$\forall\ x \in A\ .\ x\ R\ y \Rightarrow x \in S \qquad (2)$$

Dokazati moramo $y \in S$. Obravnavamo dve možnosti:

1. Če $y \in S$, potem seveda sledi $y \in S$.
2. Če $y \notin S$, potem obstaja $i \in N$, da je $y = a(i)$. Ker je $a(i+1)\ R\ a(i)$, iz predpostavke (2) sledi $y = a(i) \in S$.

Torej v vsakem primeru velja $y \in S$. □

Protiprimer: Sedaj lahko zlahka priskrbimo kak protiprimer. Na primer, cela števila Z z relacijo $R \subseteq Z \times Z$

$$a\ R\ b \Leftrightarrow a + 1 = b$$

niso dobro osnovana, ker imajo padajočo verigo

$$\cdots\ R\ (-3)\ R\ (-2)\ R\ (-1)\ R\ 0$$

Prav tako ni dobro osnovana relacija < na intervalu $[0,1]$, ker imamo padajočo verigo $a(n) = 2^{-n}$.

Dobra urejenost

Posplošimo sedaj še krepko indukcijo na naravnih številih. Tokrat bomo najprej posplošili strogo urejenost <.

Stroge urejenosti

Definicija: Relacija $R \subseteq A \times A$ je **stroga urejenost**, če je

1. irefleksivna: $\forall\ x \in A\ .\ \neg\ (x\ R\ x)$
2. tranzitivna: $\forall\ x, y, z \in A\ .\ x\ R\ y \wedge y\ R\ z \Rightarrow x\ R\ z$

Stroga urejenost je **linearna**, če je še

1. sovisna: $\forall\ x, y \in A\ .\ x\ R\ y \vee x = y \vee y\ R\ x.$

Za stroge urejenosti uporabljamo simbole <, $\subset$, $<$, $\sqsubset$ ipd.

Relaciji < in ≤ na številih sta med seboj povezani, saj denimo za realna števila velja

$$x < y \Leftrightarrow x < y \wedge x \neq y$$

in

$$x \leq y \Leftrightarrow x < y \vee x = y \qquad (3)$$

To velja v splošnem. Stroa urejenost < na množici A porodi delno urejenost ≤ na A, definirano s predpisom:

$$x \leq y \quad \Leftrightarrow \quad x = y \vee x \leq y$$

V obratno smer, delna urejenost $\sqsubseteq$ določa strogo urejenost $\sqsubset$, definirano s predpisom

$$a \sqsubset b \quad \Leftrightarrow \quad a \neq b \wedge a \sqsubseteq b \qquad (4)$$

Seveda je treba preveriti naslednja dejstva:

- če je $<$ stroga urejenost, potem je $\leq$ definirana s (3) delna urejenost
- če je $\sqsubseteq$ delna urejenost, potem je $\sqsubset$ definirana s (4) stroga urejenost.

Tako lahko prehajamo med delno in strogo urejenostjo.

Dobra ureditev

Definicija: Relacija je **dobra ureditev**, če je dobro osnovana in stroga linearna ureditev.

Izrek: Relacija je dobra ureditev natanko tedaj, ko je dobro osnovana in sovisna.

Dokaz. V eno smer je ekvivalenca očitna, zato dokažimo samo obratno smer. Denimo, da je $R \subseteq A \times A$ dobro osnovana in sovisna relacija. Doazujemo, da je dobra ureditev, se pravi, da potrebujemo še irefleksivnost in tranzitivnost R:

- R je irefleksivna: če bi veljalo $x \; R \; x$ za $x \in A$, potem R ne bi bila dobro osnovana, ker bi vsebovala padajočo verigo $\cdots \; x \; R \; x \; R \; x$.

- R je tranzitivna: denimo, da velja $x \; R \; y$ in $x \; R \; z$. Dokazujemo $x \; R \; z$. Ker je R sovisna, velja $x \; R \; z$ ali $x = z$ ali $z \; R \; x$. Pokažimo, da $x = z$ in $z \; R \; x$ nista možna:

    1. če je $x = z$, potem velja $x \; R \; y$ in $y \; R \; x$, torej x in y tvorita cikel, a R je dobro osnovana, zato to ni možno.

    2. če velja $z \; R \; x$, potem dobimo cikel $x \; R \; y \; R \; z \; R \; x$, kar spet ni možno. □

Lema: Denimo, da je $<$ stroga urejenost na neprazni množici B. Če B nima $\leq$-minimalnega elementa, potem ima padajočo verigo.

Dokaz. Denimo, da B nima minimalnega elementa, torej

$$\neg \; \exists \; x \in B \; . \; \forall \; y \in B \; . \; y \leq x \Rightarrow y = x.$$

To je ekvivalentno

$$\forall \; x \in B \; . \; \exists \; y \in B \; . \; y \leq x \wedge y \neq x$$

kar je ekvivalentno

$$\forall \; x \in B \; . \; \exists \; y \in B \; . \; y < x. \qquad (5)$$

Padajočo verigo $b : N \to B$ definiramo z zaporedjem izbir: ker je B neprazna, lahko izberemo neki element $b(0) \in B$. Denimo, da smo za neki $i \in N$ že izbrali elemente $b(0), \ldots, b(i)$ tako, da velja

$$b(i) < b(i-1) < \ldots < b(1) < b(0).$$

Ker B nima minimalnega elementa, $b(i)$ ni minimalni, torej po (5) obstaja tak $y \in B$, da je $y < b(i)$. Torej lahko izberemo $b(i+1) \in B$, da velja $b(i+1) < b(i)$. □

Pozor: v zgornjem dokazu smo uporabili *aksiom odvisne izbire*, ki je poseben primer aksioma izbire in o katerem bomo še govorili.

Izrek: Naj bo $\sqsubset$ relacija na A. Tedaj so ekvivalentne naslednje izjave:

1. $\sqsubset$ je dobro osnovana
2. vsaka *neprazna* $S \subseteq A$ ima $\sqsubseteq$-minimalni element

3. A nima $\sqsubset$-padajoče verige.

Dokaz.

(1) $\Rightarrow$ (2) Denimo, da je $S \subseteq A$ neprazna. Če uporabimo (1) na $A \setminus S$ dobimo

$$(\forall\, y \in A\,.\, (\forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \in A \setminus S) \Rightarrow y \in A \setminus S) \Rightarrow A \setminus S = \varnothing$$

Ker je S neprazna, dobimo zaporedje ekvivalentnih izjav:

$$(\forall\, y \in A\,.\, (\forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \in A \setminus S) \Rightarrow y \in A \setminus S) \Rightarrow \bot$$

$$\neg\, (\forall\, y \in A\,.\, (\forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \in A \setminus S) \Rightarrow y \in A \setminus S)$$

$$\exists\, y \in A\,.\, (\forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \in A \setminus S) \wedge y \notin A \setminus S$$

$$\exists\, y \in A\,.\, (\forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \notin S) \wedge y \in S$$

$$\exists\, y \in S\,.\, \forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \notin S$$

$$\exists\, y \in S\,.\, (\forall\, x \in A\,.\, x \sqsubset y \Rightarrow x \notin S)$$

Torej obstaja element $y \in S$ z lastnostjo, da pod njim ni nobenega elementa iz S, kar pa pomeni, da je y iskani minimalni element.

(2) $\Rightarrow$ (3) Denimo, da je $a : N \to A$ padajoča veriga. Tedaj slika $\{\, a(n) \mid n \in N \,\}$ ne bi imela minimalnega elementa, v nasprotju z (2).

(3) $\Rightarrow$ (1) Denimo, da je $S \subseteq A$ progresivna. Trdimo, da množica $C := A \setminus S$ nima minimalnega elementa. Če bi bil $c \in C$ minimalni v C, bi to pomenilo

$$\forall\, x \in A\,.\, x \sqsubset c \Rightarrow x \notin C,$$

kar je ekvivalentno

$$\forall\, x \in A\,.\, x \sqsubset c \Rightarrow x \in S.$$

Ker je S progresivna, od tod sledi $c \in S$, kar ni mogoče.

Dokazati moramo, da je C prazna. Če ne bi bila, bi lahko uporabili lemo in dobili padajočo verigo v A, kar je v nasprotju s (3). □

Izrek: Naj bo $\sqsubset$ stroga urejenost na A. Tedaj so ekvivalentne naslednje izjave:

1. $\sqsubset$ je dobro urejena
2. vsaka *neprazna* množica $S \subseteq A$ ima $\sqsubset$-prvi element: to je tak $x \in S$, da velja $\forall\, y \in S\,.\, x \neq y \Rightarrow x \sqsubset y$.
3. A nima $\sqsubset$-padajoče verige in $\sqsubset$ je sovisna

Dokaz je podoben dokazu prejšnjega izreka. Poskusite ga dokazati sami tako, da predelate dokaz prejšnjega izreka.

Primeri:

1. Naravna števila N urejena z relacijo $<$.

2. Končna množica $\{0, \ldots, n\}$ urejena z relacijo $<$.

3. Če sta $(P, \leq_P)$ in $(Q, \leq_Q)$ dobri urejenosti, potem je dobro urejena tudi $P + Q$ z relacijo $\sqsubseteq$, ki P postavi pred Q:

$$
\begin{aligned}
&u \sqsubseteq v \Leftrightarrow \\
&\quad (\exists\, x \in P \,.\, \exists\, y \in Q \,.\, u = \iota_1(x) \wedge v = \iota_2(y)) \vee \\
&\quad (\exists\, x \in P \,.\, \exists\, y \in P \,.\, u = \iota_1(x) \wedge v = \iota_1(y) \vee x \leq_P y) \vee \\
&\quad (\exists\, x \in Q \,.\, \exists\, y \in Q \,.\, u = \iota_2(x) \wedge v = \iota_2(y) \vee x \leq_Q y).
\end{aligned}
$$

4. S prejšnjim primerom lahko seštevamo dobre urejenosti, na primer $N + 3$ je dobra urejenost

$$0 < 1 < 2 < \cdots < \omega < \omega + 1 < \omega + 2$$

Ali pa $\omega + \omega$

$$0 < 1 < 2 < \cdots < \omega < \omega + 1 < \omega + 2 < \cdots$$