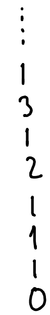
Dobra osnovanost & dobra urejenost

$\mathbb{N}$ indukcija

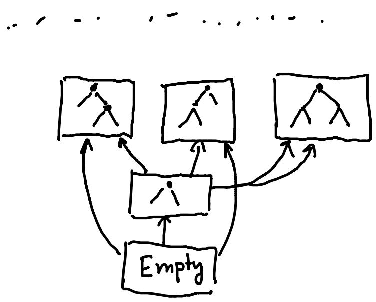
$\downarrow$ dobra osnovanost

Končna dvojiška drevesa

$\mathbb{N}$



Tree:



Dobra urejenost

Stroga urejenost $<$: 1. irefleksivna $\neg(x<x)$

2. tranzitivna

Stroga linearna urejenost : 3. sovisna $x<y \vee x=y \vee y<x$

$(x \neq y \Rightarrow x<y \vee y<x)$

Delna ureditev $\leq$ | Stroga ureditev $<$

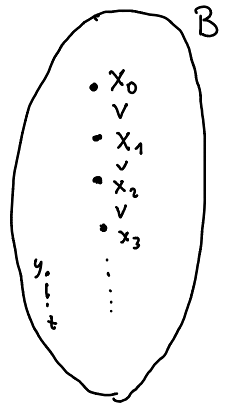
$$x \leq y \iff x<y \vee x=y$$

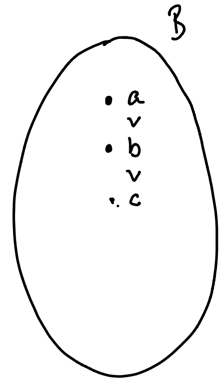
$$x < y \iff x \leq y \wedge x \neq y$$

Def: Relacija je <u>dobra ureditev</u>, če je dobro osnovana & stroga linearna.

Izrek: Relacija je dobra ureditev $\iff$ dobro osnovana & sovisna

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





Odvisna izbira!

$$\forall y \in B \,.\, \exists z \in B \,.\, z < y$$

Izrek: Naj bo $\sqsubset$ relacija na A. Ekvivalentno je:

1. $\sqsubset$ je dobro osnovana
2. vsaka <u>neprazna</u> $S \subseteq A$ ima $\sqsubseteq$-minimalni element,
3. $\sqsubset$ nima padajoče verige.

$x \in S$ je $\sqsubseteq$-minimalni: $\forall y \in S .\, y \sqsubseteq x \Rightarrow x = y$

Izrek: Naj bo $\sqsubset$ stroga urejenost na A. Ekvivalentno je:

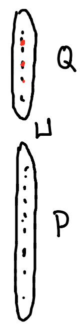
1. $\sqsubset$ je dobro urejena
2. vsaka <u>neprazna</u> $S \subseteq A$ ima $\sqsubseteq$-prvi element
3. $\sqsubset$ nima padajoče verige in je sovisna.

$x \in S$ je $\sqsubseteq$-prvi: $\forall y \in S .\, x \sqsubseteq y$.

Primeri:

1. $(\mathbb{N}, <)$ dobra urejenost
2. $(\{0,1,2,\dots,n\}, <)$ dobra ✓
3. $(P, <_P)$ in $(Q, <_Q)$ dobro urejeni

"Q postavimo nad P"



Nova dobra urejenost:

$P+Q$ z relacijo $\sqsubset$:

$\iota_1(x) \sqsubset \iota_2(y)$ za $x \in P,\ y \in Q$

$\iota_2(y) \sqsubset \iota_1(x)$ ne velja nikoli

$\iota_1(x) \sqsubset \iota_1(x') \iff x <_P x'$

$\iota_2(y) \sqsubset \iota_2(y') \iff y <_Q y'$

Uporabimo:

$0 < 1 < 2 < 3 < \dots\dots < \omega$

$\underset{\underset{<}{P}}{\mathbb{N}} + \underset{Q}{\{\omega\}}$

$\underbrace{0 < 1 < 2 < 3 < \dots\dots}_{\mathbb{N}} < \omega < \underbrace{\omega+1 < \omega+2 < \omega+3 < \dots\dots}_{\mathbb{N}}$

Kodiranje matematičnih objektov z množicami

Kodiranje z množicami

- relacija $R \subseteq A \times A$ .... relacija .... podmnožica $A \times A$
- funkcija $f : A \to B$ .... funkcijska relacija .... podmnožica $A \times B$
- kvocientna množica $A/R \subseteq P(A)$

Kartezični produkt $A \times B$:

urejeni par (x, y) ...... Kuratowski: $\{\{x\}, \{x,y\}\}$

$\{\{3\},\{5,3\}\}$ .... $(3,5)$

$\{\{6,5,6\},\{6,6,6,6\}\}$ ... $(6,5)$

$\quad\quad\quad \shortparallel$

$\{\{6,5\},\{6\}\}$

$\{\{3\}\} = \{\{3\},\{3,3\}\}$ .... $(3,3)$

.... $\{x,y\}$ izgubimo vrstni red urejenega para

..... $\{x,\{y\}\}$ slabo? Premislek

$\{\{\{3\}\},\{\{2\}\}\}$

$(\{\{3\}\},\{2\})$

$(\{\{2\}\},\{3\})$

dva različna imata isto kodiranje. Slabo.

Vsota $A + B$: $\iota_0(x) = (0, x)$ ... $\{\{0\},\{0,x\}\}$

$\iota_1(y) = (1, y)$ ... $\{\{1\},\{1,y\}\}$

Naravna števila $\mathbb{N}$:

operacija naslednik na množicah

$$x^+ = x \cup \{x\}$$

$$0 = \emptyset$$

$$n^+ = n \cup \{n\}$$

$$0 = \emptyset$$

$$1 = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$$

$$2 = 1 \cup \{1\} = \{0, 1\}$$

$$3 = 2 \cup \{2\} = \{0, 1, 2\} = \{\overset{0}{\emptyset}, \overset{1}{\{\emptyset\}}, \overset{2}{\{\emptyset, \{\emptyset\}\}}\}$$

n kodiramo z množico (kodiranih) predhodnikov n

Cela števila:

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/_\sim$$

$[(a,b)]_\sim$ predstavlja razliko "$a-b$"

$[(3,5)]_\sim$ razlika 3 in 5

$[(10,12)]_\sim$ razlika 10 in 12

$$\underset{\text{"}a-b\text{"}}{(a,b)} \sim \underset{\text{"}c-d\text{"}}{(c,d)} \iff a+d = c+b$$

Celo število "dva": $\{(2,0), (3,1), (4,2), (5,3), \ldots\}$

Racionalna števila:

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{N} \setminus \{0\}))/_\approx$$ podobno

Realna števila:

$$\mathbb{R} \subseteq P(\mathbb{Q})$$

Zermelo-Fraenkelovi aksiomi teorije množic

Ekstenzionalnost: množici A in B, ki imata iste elemente, sta enaki.

Neurejeni par: za vsak x in y je $\{x, y\}$ množica, ki vsebuje natanko x in y:

$$\forall x\, y\, z\, .\, z \in \{x, y\} \Leftrightarrow z = x \vee z = y$$

Okrajšava: $\{x\} = \{x, x\}$.

Unija: za vsako množico A je $\cup A$ množica, ki vsebuje natanko vse elemente množic iz A

unija množice množic

$$\forall A\, x\, .\, x \in \cup A \Leftrightarrow \exists B \in A\, .\, x \in B$$

Prazna množica: množica $\varnothing$ nima elementa:

$$\forall x\, .\, x \notin \varnothing$$

Neskončna množica:
obstaja množica, ki vsebuje $\varnothing$ in je zaprta za operacijo naslednik ($x^+ = x \cup \{x\}$).

$$\exists A\, .\, \varnothing \in A \wedge \forall x \in A\, .\, x^+ \in A$$

Podmnožica:
za vsako množico A in formulo ϕ je $\{x \in A \mid \phi(x)\}$ množica, ki vsebuje natanko vse element iz A, ki zadoščajo ϕ:

$$\forall y\, .\, y \in \{x \in A \mid \phi(x)\} \Leftrightarrow \phi(y)$$

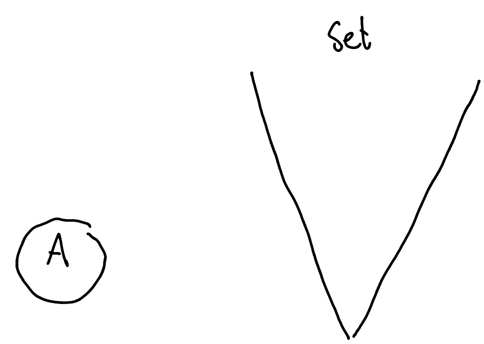
Potenčna množica:
za vsako množico A je P(A) množica, ki vsebuje natanko vse njene podmnožice:

$$\forall S\, .\, S \in P(A) \Leftrightarrow S \subseteq A$$

Zamenjava:
če je A množica in $f : A \to \mathrm{Set}$ preslikava, je razred

$$\{\, y \mid \exists x \in A\, .\, y = f(x) \,\}$$

množica.



Dobra osnovanost:
relacija $\in$ je dobro osnovana. $\Longrightarrow x \notin x$

$\neg(x \in y \in x)$

$y \in \{x \mid \varphi(x)\} \Longleftrightarrow \varphi(y)$

Aksiom izbire:
vsaka družina nepraznih množic ima funkcijo izbire.

Zamenjava:

$f_0 = \mathbb{N}$

$f_1 = P\mathbb{N}$

$f_2 = P(P\mathbb{N})$

$f_3 = P^3(\mathbb{N})$

$f_n = P^n(\mathbb{N})$

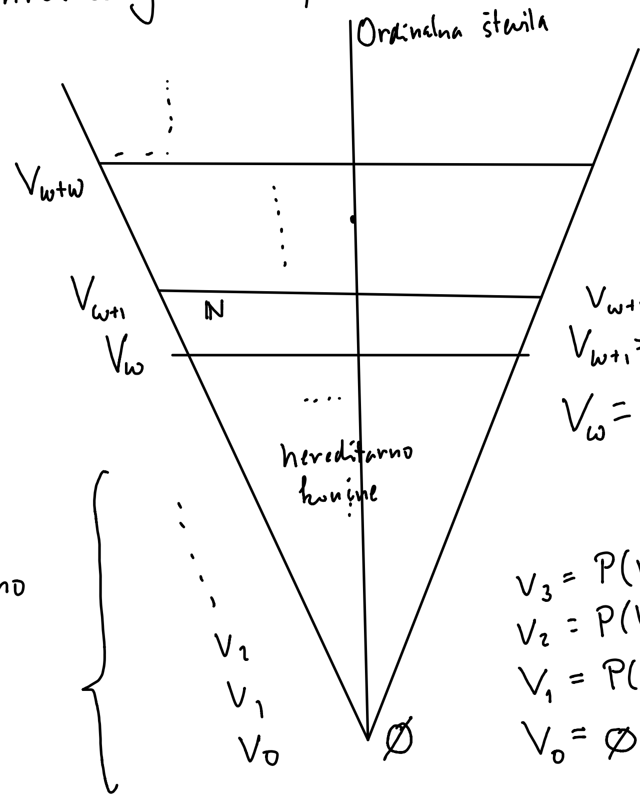
$\vdots$

$\{P^n(\mathbb{N}) \mid n \in \mathbb{N}\}$

$\{y \mid \exists n \in \mathbb{N}.\ y = P^n(\mathbb{N})\}$

Kumulativna hierarhija množic

Ideja: množice "gradimo", začenši s $\emptyset$



$V_{\omega+2} = P(V_{\omega+1})$

$V_{\omega+1} = P(V_\omega)$

$V_\omega = \bigcup_{n \in \mathbb{N}} V_n$

hereditarno končne

$V_3 = P(V_2)$

$V_2 = P(V_1) = \{\emptyset, \{\emptyset\}\}$

$V_1 = P(V_0) = P(\emptyset) = \{\emptyset\}$

$V_0 = \emptyset$

$2^{16} = 65536$

$2^4 = 16$

$2^2 = 4$

$2^1 = 2$

$2^0 = 1$

0

$\mathbb{N} = \{\underset{V_0}{0}, \underset{V_1}{1}, \underset{V_2}{2}, 3, 4, \ldots\} \subseteq V_\omega$

$\mathbb{N} \in P(V_\omega) = V_{\omega+1}$

Aksiom izbire & Zornova lema

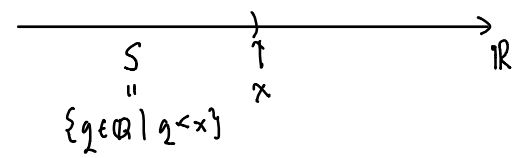
<u>Def</u>: <u>Veriga</u> v delni urejenosti $(P, \leq)$ je podmnožica $V \subseteq P$, ki je z $\leq$ linearno urejena: $\forall x, y \in V.\ x \leq y \vee y \leq x$.

Primer: $(P(\mathbb{Q}), \subseteq)$

veriga v $P(\mathbb{Q})$: $\mathbb{R} \subseteq P(\mathbb{Q})$

$\mathbb{R} = \{ S \subseteq \mathbb{Q} \mid S \text{ je Dedekindov rez} \}$

$S, T \in \mathbb{R}$



$S \subseteq T \iff S \leq T$

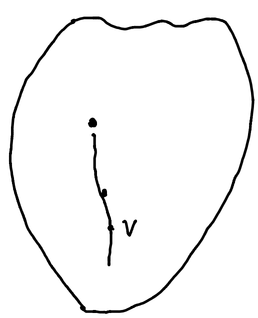
relacija "manjše ali enako" na realnih
linearna

<u>Zornova lema</u>:

Naj bo $(P, \leq)$ delna urejenost.
Če ima vsaka veriga v P zgornjo mejo v P, potem ima P maksimalni element.

Dokaz: v zapiskih.

Zornova lema $\iff$ aksiom izbire (v teoriji množic brez aksioma izbire)



Izrek: Vsak vektorski prostor ima bazo.

Dokaz: V vektorski prostor

$$L = \{ S \subseteq V \mid S \text{ linearno neodvisna} \}$$

Baza $B \subseteq V$ je:
1. linearno odvisna
2. ne moremo dodati še enega vektorja v B, da bo še vedno linearno neodvisna

Sklep: baza je maksimalni element delne ureditve $(L, \subseteq)$.

Ali L ima maksimalni element?

Da, po Zornovi lemi: preveriti:

denimo, da je $W \subseteq L$ veriga v L.

Tedaj je $\bigcup W \in L$ in je zgornja meja za W. $\boxtimes$