Cantorjev izrek: $|A| < |\mathcal{P}(A)|$ za vsako množico A.

Dokaz:

1) $|A| \leq |\mathcal{P}(A)|$

Iščemo injektivno $f: A \to \mathcal{P}(A)$

$x \mapsto \{x\}$

Injektivnost:

$$f(x) = f(y)$$
$$\{x\} = \{y\}$$
$$x \in \{y\}$$
$$x = y$$

2) $|A| \neq |\mathcal{P}(A)|$

$\neg \exists g: A \to \mathcal{P}(A).\ g$ bijektivna

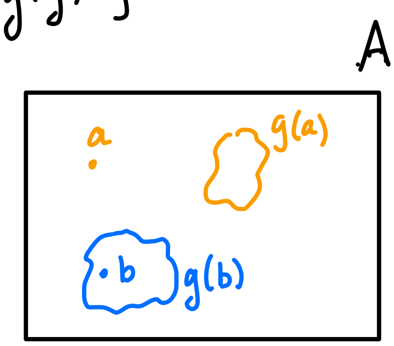
$\forall g: A \to \mathcal{P}(A).\ g$ ni bijektivna

Naj bo $g: A \to \mathcal{P}(A)$ preslikava.

Dokažimo: g ni surjektivna

$$\neg \forall S \in \mathcal{P}(A).\ \exists x \in A.\ g(x) = S$$
$$\exists S \in \mathcal{P}(A).\ \forall x \in A.\ g(x) \neq S$$

Podamo $S := \{y \in A \mid y \notin g(y)\}$



Preverimo: $\forall x \in A.\ g(x) \neq S$.

Naj bo $x \in A$. Dokazujemo $g(x) \neq S$.

Predpostavimo $g(x) = S$. Iščemo protislovje:

1) velja $x \notin S$: $\quad S = g(x) = \{ y \in A \mid y \notin g(y) \}$

če bi veljalo $x \in S$, po definiciji S sledi $x \notin g(x)$, protislovje.

2) velja $x \in S$:

$$x \in S \iff$$
$$x \in \{ y \in A \mid y \notin g(y) \} \iff$$
$$\underset{\checkmark}{x \in A} \land \underset{\text{po (1)}}{x \notin g(x)}.$$

$\blacksquare$

Če je $A = \mathbb{N}$:

imamo $g : \mathbb{N} \to \mathcal{P}(\mathbb{N})$, iščemo $S \subseteq \mathbb{N}$, da $\forall n.\, g(n) \neq S$

	0	1	2	3	4	5	6	.....
$g(0)$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	...
$g(1)$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	...
$g(2)$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	...
$g(3)$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	...
$\vdots$								
S	$\bot$	$\bot$	$\top$	$\bot$				

$g(0) = \{0, 3, 4, \ldots\}$

$g(1) = \{0, 1, 2, 5, \ldots$

$S = \{ n \in \mathbb{N} \mid n \notin g(n) \}$

$0 \notin g(0)$

$1 \notin g(1)$

Aksiom izbire

Aksiom izbire: Vsaka družina nepraznih množic ima funkcijo izbire.

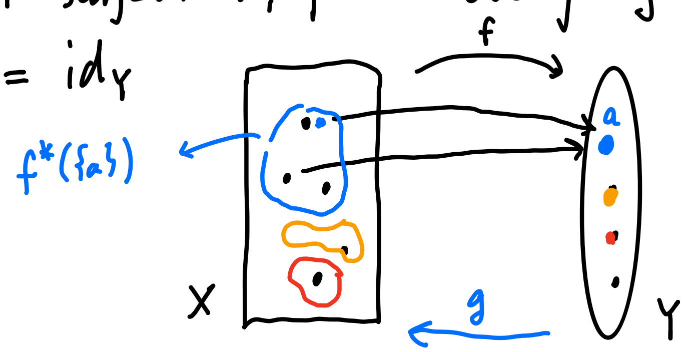
Funkcija izbire za družino $A : I \to \mathrm{Set}$ je
$f : I \to \bigcup A$, da $\forall i \in I.\ f(i) \in A_i$

Družina nepraznih množic: $A : I \to \mathrm{Set}$, da $\forall i \in I.\ A_i \neq \emptyset$.
(Neprazna družina: $B : J \to \mathrm{Set}$, da $J \neq \emptyset$.)

Primer: $I = \mathbb{N}$ $\quad A_n = \{ k \in \mathbb{N} \mid k \text{ deli } n \}$
$f(n) := n$ ali $f(n) := 1$

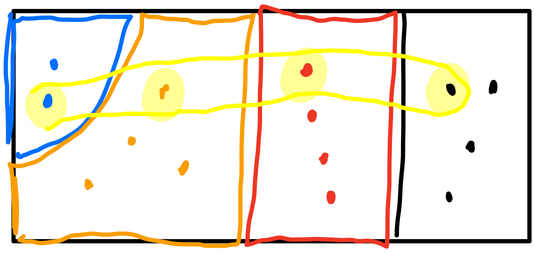
Ekvivalentne izjave:

1) Aksiom izbire
2) Produkt $\prod_{i \in I} A_i$ družine nepraznih množic $A : I \to \mathrm{Set}$ je neprazen.
3) Vsaka surjekcija ima prerez:
   Če je $f : X \to Y$ surjektivna, potem obstaja $g : Y \to X$,
   da je $f \circ g = \mathrm{id}_Y$



4) Vsaka ekvivalenčna relacija ima izbor predstavnikov

A $\quad \sim$ ekv. rel.

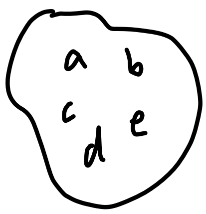


5) Vsako množico lahko dobro uredimo:

Za vsako $A \in \mathrm{Set}$ obstaja relacija $<$ na A, da je $<$ dobra ureditev.

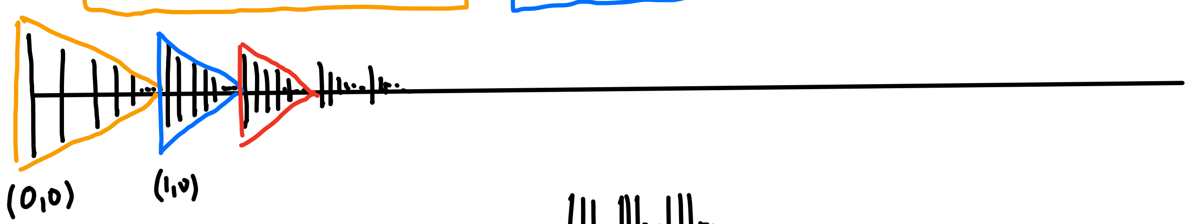
__Primer:__

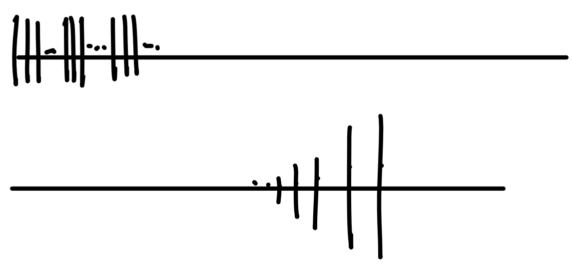
$A =$



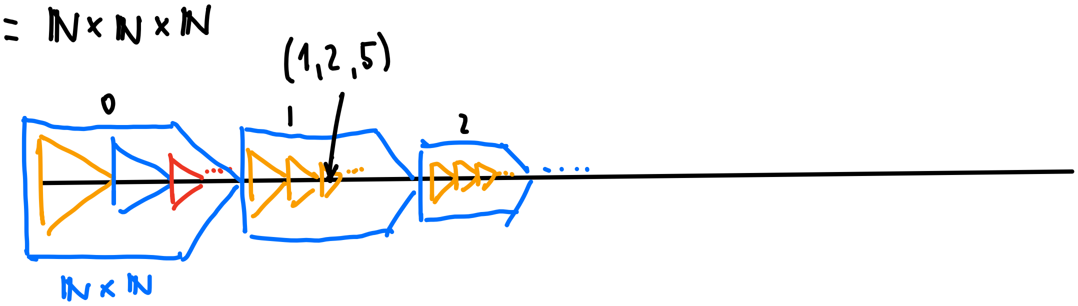
$A = \mathbb{N} \times \mathbb{N}$ leksikografska

$(0,0) < (0,1) < (0,2) < \cdots < (1,0) < (1,1) < (1,2) < \cdots < (2,0) < \cdots < (3,0) < \cdots$





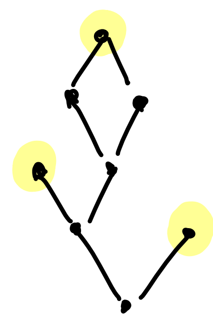
$A = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$



$A = \mathbb{N}^{\mathbb{N}}$?!

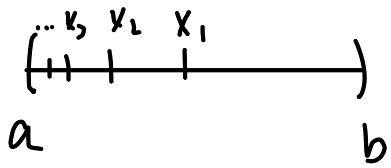
6) Zornova lema:

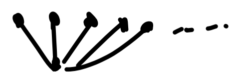
Naj bo $(P, \leq)$ delna ureditev, $P \neq \emptyset$ v kateri ima vsaka veriga zgornjo mejo. Tedaj ima P maksimalni element.

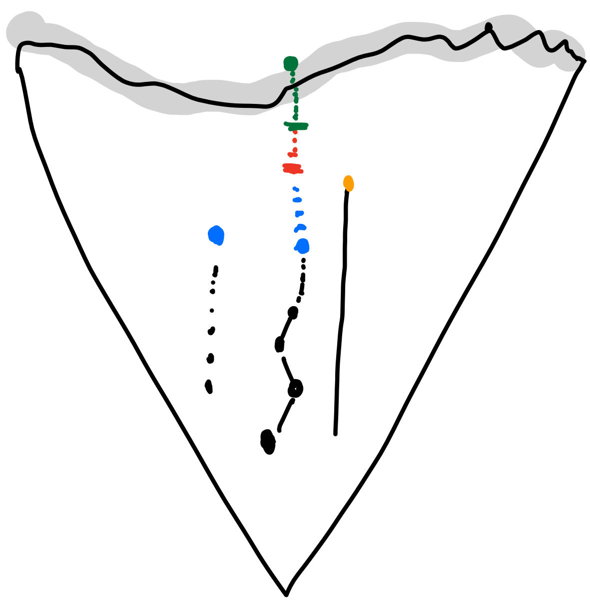


$(\mathcal{P}_{\text{končne}}(\mathbb{N}), \subseteq)$ nima maksimalnega elementa

$$\begin{array}{c} \vdots \\ \{0,2,4,6\} \\ \cup\!\!| \\ \{0,2,4\} \\ \cup\!\!| \\ \{0,2\} \\ \cup\!\!| \\ \{0\} \end{array}$$







$P, \leq$

7) Vsak vektorski prostor ima bazo.

V vektorski prostor.

Baza = maksimalna linearno neodvisna podmnožica V

$P = \{ S \subseteq V \mid S$ je linearno neodvisna$\}$

urejena z $\subseteq$

Baza = maksimalni element $(P, \subseteq)$

Uporabimo Zornovo lemo:

$L \subseteq P$ je veriga za $\subseteq$

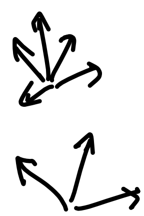
↑ elementi L so lin. neodvisne podmnožice V

tvorijo verigo: $\forall S, T \in L .\ S \subseteq T \vee T \subseteq S$

Ali je L omejena v P?

Da, omejena je z

$\bigcup L$



$\xRightarrow{\text{Zorn}}$ P ima maksimalni element (baza za V).