Diskrétní struktury 1

Nekonečno

Radim Bělohlávek

KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI

Proč se zabýváme nekonečnem?

- řada množin, které potřebujeme při praktických úvahách, je nekonečných
- potřebujeme vědět, jak se s nekonečnými množinami pracuje
- mnoho úvah o algoritmech obsahuje úvahy o nekonečných množinách
- nekonečno je jeden z nejzáhadnějších jevů

Některé otázky

- jak měřit velikost množin, zejména nekonečných?
- co znamená, že dvě množiny jsou stejně velké?
- která množina je větší, $\mathbb{N}$ nebo $\mathbb{Q}$? $\mathbb{Q}$ nebo $\mathbb{R}$?
- ...

Konečné a nekonečné množiny

Intuitivně:
A je konečná, pokud lze její prvky „očíslovat“ čísly $1, \ldots, n$.

Definice Množina A je konečná, pokud existuje $n \in \mathbb{N}$ a bijekce

$$f : \{1, 2, \ldots, n\} \to A.$$

Množina A je nekonečná, pokud není konečná.

Je-li A konečná, číslo n z definice se nazývá počet prvků (také mohutnost, velikost) A, značí se $|A|$.

Příklad $\{2,3,5,7\}$ je konečná, protože pro $n = 4$ je např. zobrazení $f : \{1,2,3,4\} \to \{2,3,5,7\}$ definované

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 5, \quad f(4) = 7$$

je bijekce. Tedy $|\{2,3,5,7\}| = 4$.

Příklad Množina S všech kladných sudých čísel je nekonečná.

Je to celkem zřejmé. Ale argument: Kdyby $f : \{1,\dots,n\} \to S$ byla bijekce, vezměme $m =$ největší z $f(1),\dots,f(n)$. Pak $2(m+1)$ je sudé, ale protože $2(m+1) > m$, není obrazem žádného i, což je spor s tím, že f je bijekce.

Příklad Množina $\mathbb{R}$ je nekonečná. Jasné (např. podobným argumentem).

Spočetné množiny

Intuitivně:
A je spočetná, pokud lze její prvky seřadit do posloupnosti (konečné nebo nekonečné).

Definice Množina A je spočetná, pokud je

konečná,

nebo existuje bijekce $f : \mathbb{N} \to A$ (pak je tzv. nekonečná spočetná, popř. spočetně nekonečná).

Tedy A je spočetná, právě když existuje posloupnost

$$a_1, \ldots, a_n \quad \text{nebo} \quad a_1, a_2 \ldots$$

ve které se vyskytují všechny prvky z A (f je surjekce) a neopakují se v ní (f je injekce).

Příklad (nekonečné spočetné množiny)

- $\mathbb{N}$

  Základní nekončená spočetná množina: identita $f(n) = n$ je bijekce $f : \mathbb{N} \to \mathbb{N}$.

- $\{2, 4, 6, 8, \dots\}$

  Zobrazení $f : \mathbb{N} \to \{2, 4, 6, 8, \dots\}$ dané $f(n) = 2n$ je bijekce.

- $\mathbb{N} \cup \{0\}$

  Zobrazení $f : \mathbb{N} \to \mathbb{N} \cup \{0\}$ dané $f(n) = n - 1$ je bijekce.

Příklad (nekonečné spočetné množiny, pokrač.)

- $\mathbb{Z}$

  Požadovaná posloupnost z prvků $\mathbb{Z}$ je např.

  $$0, -1, 1, -2, 2, -3, 3, \dots$$

  Jinými slovy, bijekce $f : \mathbb{N} \to \mathbb{Z}$ z definice je

  $$f(1) = 0, f(2) = -1, f(3) = 1, f(4) = -2, f(5) = 2, \dots$$

  (Napište explicitní vzorec pro $f(n)$.)

- $\{k, k+1, k+2, \dots\}$ pro libovolné $k \in \mathbb{Z}$

  Zobrazení $f : \mathbb{N} \to \{k, k+1, k+2, \dots\}$ dané $f(n) = n + (k-1)$ je bijekce.

K poslednímu příkladu:

- $\{k, k+1, \ldots\}$ pro libovolné $k \in \mathbb{Z}$

  Zobrazení $f : \mathbb{N} \to \{k, k+1, k+2, \ldots\}$ dané $f(n) = n + (k-1)$ je bijekce.

Neplyne ale spočetnost $\{k, k+1, \ldots\}$ z toho, že $\{k, k+1, \ldots\} \subseteq \mathbb{Z}$ a že $\mathbb{Z}$ je spočetná?

Ano. Dokonce obecně platí:

Věta Každá nekonečná podmnožina spočetné množiny je spočetná.

(Důsledek: Pokud A je spočetná a $B \subseteq A$, pak B je spočetná.)

- Netriviální otázka: Definice spočetné množiny nevylučuje množiny, které jsou větší než konečné, ale menší než spočetné. Věta říká, že takové neexistují.
- Dokážeme později.

Příklad

$\{0,1\}^*$ je množina všech tzv. řetězců (slov, konečných posloupností) nad abecedou $\{0,1\}$.
Například následující jsou prvky množiny $\{0,1\}^*$:

$$01, 11, 10, 0, 111, 01010101, \varepsilon \text{ (prázdný řetězec)}.$$

Následující posloupnost je nekonečná, obsahuje všechny řetězce z $\{0,1\}^*$ a prvky se v ní neopakují:

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, 0001, \ldots$$

Prokazuje tedy, že $\{0,1\}^*$ je nekonečná spočetná množina.

Uspořádání řetězců

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, 0001, \dots$$

je obecně důležité (tzv. shortlex):

1. kratší řetězce jsou před delšími,
2. stejně dlouhé řetězce jsou uspořádány lexikograficky

Podobně lze seřadit do posloupnosti všechna slova nad libovolnou konečnou abecedou. Tedy:

Věta Množina Σ^* všech řetězců na konečnou abecedou $\Sigma = \{a_1, \dots, a_n\}$ je spočetná.

Např. $\Sigma = \{a, b, \dots, z\}$, $\Sigma^* = \{\varepsilon, a, computer, world, ssca, \dots\}$.

Důležitý důsledek:

Je-li možné nějaké objekty kódovat (reprezentovat, popsat) jako řetězce nad nějakou konečnou abecedou Σ, je množina těchto kódů (popisů) spočetná, a tedy i množina daných objektů je spočetná.

Argument:
O = množina uvažovaných objektů; kódování = prosté zobrazení $c : O \to \Sigma^*$;
$c(O)$ = množina kódů; pak $c(O) \subseteq \Sigma^*$ a vzhledem ke spočetnosti Σ^* je i $c(O)$ spočetná.

Příklad
Množina všech zdrojových kódů v jazyku C (Python, Lisp, . . .) je spočetná.

Odbočka: lexikografické a shortlex uspořádání

Dána abeceda $\Sigma = \{a_1, \dots, a_n\}$ a na ní lineární uspořádání $\leq$; předp. $a_1 < \cdots < a_n$.

délka $|u|$ řetězce $u \in \Sigma^*$ je počet znaků v u: $|010| = 3$, $|0| = 1$, $|\varepsilon| = 0$

Lexikografické (slovníkové) uspořádání $\leq_l$: pro $u = u_1 \cdots u_p, v = v_1 \cdots v_q \in \Sigma^*$ je

$$u \leq_l v \quad \text{p. k.} \quad u = v \text{ nebo } \text{ pro nějaké } i \text{ je } u_1 \cdots u_{i-1} = v_1 \cdots v_{i-1} \text{ a } u_i < v_i$$

Shortlex uspořádání $\leq_s$: pro $u = u_1 \cdots u_p, v = v_1 \cdots v_q \in \Sigma^*$ je

$$u \leq_s v \quad \text{p. k.} \quad |u| < |v| \text{ nebo } (|u| = |v| \text{ a } u \leq_l v).$$

Rozdíl mezi $\leq_l$ a $\leq_s$:

- $\leq_s$ je stejného typu jako přirozené uspořádání $\mathbb{N}$ ($\leq_s$ vytváří posloupnost)
- $\leq_l$ není stejného typu jako přirozené uspořádání $\mathbb{N}$ (netvoří takovou posloupnost):
  - např. množina $A = \{1, 01, 001, 0001, \dots\}$ nemá nejmenší prvek vzhledem k $\leq_l$
  - ale každá podmnožina $A \subseteq \mathbb{N}$ má nejmenší prvek

Konec odbočky

Odbočka: algoritmický pohled

Spočetné množiny lze chápat jako množiny, o kterých lze uvažovat jako o množinách, jejichž prvky mohou být postupně vypisovány nějakým algoritmem (který případně pracuje nekonečně dlouho).

Algoritmus vypisující $\{1, \ldots, n\}$ (konečná spočetná):

for $i \leftarrow 1$ to n do print(i)

Algoritmus vypisující$\{1, 2, \ldots\}$ (nekonečná spočetná):

$i \leftarrow 1$
while *true* do
  print(i)
  $i \leftarrow i + 1$

Takové množiny se nazývají algoritmicky vyčíslitelné (nebo rekurzívně vyčíslitelné).

Každá algoritmicky vyčíslitelná množina je tedy spočetná.

Ale: Existuje spočetná množina, která není algoritmicky vyčíslitelná! (ukážeme)
Konec odbočky

Příklad (nekonečné spočetné množiny, pokrač.)

– $\mathbb{Q}$

  – čísla $r \in \mathbb{Q}$ lze chápat (vyjádřit) jako zlomky $\frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$
  – připustíme-li pro $r \neq 0$ pouze $\frac{p}{q}$, kde p a q jsou nesoudělná, a $r = 0$ pouze zlomek $\frac{0}{1}$, je každé $r \in Q$ vyjádřeno právě jedním $\frac{p}{q}$
    (takové $\frac{p}{q}$ jsou v tzv. kanonickém tvaru)

První argument prokazující spočetnost (detaily přednáška):

  – nakreslíme množinu $\mathbb{Z} \times \mathbb{N}$,
  – její prvky $\langle p, q \rangle$ lze seřadit do posloupnosti,
  – z ní vybrat jen $\langle p, q \rangle$ takové, že $\frac{p}{q}$ je v kanonickém tvaru
  – vybraná podposloupnost tedy obsahuje právě všechna racionální čísla a ta se v ní neopakují

Druhý argument: později.

Existují nekonečné množiny, které nejsou spočetné?

Definice konečných a spočetných množin dává následující obrázek:

- konečné množiny
- nekonečné množiny
  - spočetné množiny
  - ???

Definice Množina se nazývá nespočetná, pokud není spočetná (tedy je nekonečná, ale neexistuje bijekce mezi $\mathbb{N}$ a tou množinou).

Tedy nespočetná množina je „ještě větší“ než $\mathbb{N}$ (a každá jiná spočetná množina).

Věta Množina $2^{\mathbb{N}}$ všech podmnožin množiny $\mathbb{N}$ je nespočetná.

Důkaz Provedeme tzv. diagonální metodou.

Sporem. Předpokládejme, že $2^{\mathbb{N}}$ je spočetná.

Pak existuje bijekce $f : \mathbb{N} \to 2^{\mathbb{N}}$, $f(i) = A_i$, a tedy posloupnost $A_1, A_2, \ldots$ všech podmnožin množiny $\mathbb{N}$.

Sestrojíme nyní množinu $B \subseteq \mathbb{N}$, která je různá od každé z $A_1, A_2, \ldots$, to bude spor.

Každou množinu A_i reprezentujeme řádkem 0 a 1:

	1	2	3	4	$\cdots$	j	$\cdots$
A_i	0	0	1	0	$\cdots$	a_{ij}	$\cdots$

tedy $1 \notin A_i$, $2 \notin A_i$, $3 \in A_i$, $4 \notin A_i$ a

$$j \in A_i, \text{ pokud } a_{ij} = 1, \quad j \notin A_i, \text{ pokud } a_{ij} = 0.$$

Uvažujme schéma a jeho hlavní diagonálu:

	1	2	3	4	$\cdots$
A_1	$\boldsymbol{a_{11}}$	a_{12}	a_{13}	a_{14}	$\cdots$
A_2	a_{21}	$\boldsymbol{a_{22}}$	a_{23}	a_{24}	$\cdots$
A_3	a_{31}	a_{32}	$\boldsymbol{a_{33}}$	a_{34}	$\cdots$
A_4	a_{41}	a_{42}	a_{43}	$\boldsymbol{a_{44}}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

a definujme množinu B jako množinu, jejíž řádek b vznikne „negací“ hlavní diagonály.

Tedy pro každé $i \in \mathbb{N}$ definujeme $b_i = 1 - a_{ii}$ neboli

$$i \in B, \text{ právě když } i \notin A_i.$$

Pak B je podmnožinou $\mathbb{N}$, ale $B \neq A_1$, $B \neq A_2$, ..., protože B a A_i se liší v prvku i. $\square$

Věta Množina 2^A všech podmnožin libovolné nekonečné spočetné množiny A je nespočetná.

Důkaz Diagonální metodou jako pro důkaz předchozí věty pro $A = \mathbb{N}$. $\square$

Z toho plyne, že řada důležitých množin je nespočetných.

Definice Formální jazyk na konečnou abecedou Σ je libovolná množina $L \subseteq \Sigma^*$. Řetězce $w \in L$ se nazývají slova jazyka L.

- $\{b_n \cdots b_1 0 \mid b_i \in \{0,1\}\}$, tj. $\{0, 00, 10, 000, 010, \dots\}$, je formální jazyk nad $\{0,1\}$. Sestává ze slov představujících zápisy sudých nezáporných čísel ve dvojkové soustavě.
- $\{x, y, (x+y), (x*x), (x*(y+y)), \dots\}$ je jazyk nad $\{x, y, (,), *, +\}$, jehož slova jsou správně utvořené aritmetické výrazy nad danými proměnnými a symboly operací.

Věta Množina všech formálních jazyků nad libovolnou konečnou abecedou je nespočetná.

Důkaz Důsledek předchozí věty a tvrzení (dříve), že množina Σ^* všech řetězců nad Σ je spočetná. $\square$

To má důležitý důsledek:

Existuje množina řetězců nad $\{0, 1\}$, která není algoritmicky vyčíslitelná.

Množina všech řetězců z $\{0, 1\}^*$ je spočetná. Každá $A \subseteq \{0, 1\}^*$ je tedy spočetná.

Některé podmnožiny množiny $A \subseteq \{0, 1\}^*$ jsou algoritmicky vyčíslitelné (viz výše), např. jistě všechny konečné, pak např. následující:

- $\{1, 11, 111, 1111, \dots\}$,
- $\{01, 0011, 000111, \dots\}$,
- $\{1, 0110, 0011100, 0001111000, \dots\}$,
- $\{u \in \{0, 1\}^* \mid u$ obsahuje stejný počet 0 a $1\}$

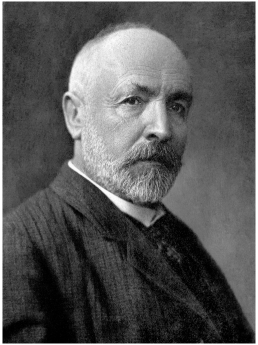
Ale existují množiny binárních řetězců, které nelze vypisovat pomocí algoritmů!
Je jich dokonce víc než těch, které vypisovat lze.

Zdůvodnění:

- algoritmus je reprezentován řetězcem znaků nad konečnou abecedou, tedy algoritmů je spočetně mnoho
- množin řetězců nad $\{0, 1\}$ je nespočetně mnoho
- existuje tedy množina $A \subseteq \{0, 1\}^*$, pro kterou neexistuje algoritmus, který ji vypisuje

Diagonální metoda (také Cantorova diagonální metoda):

– důležitá myšlenka, objevuje se např. i v úvahách o algoritmech a výpočtech



Georg Cantor (1845–1918)

– německý matematik, vytvořil teorii množin (dnes tzv. intuitivní, naivní)
– Georg Cantor: Ueber eine elementare Frage der Mannigfaltigkeitslehre. Jahresbericht der Deutschen Mathematiker Vereinigung 1(1891), 75–78.

Věta Množina $\mathbb{R}$ je nespočetná.

Důkaz (původním Cantorovým argumentem): Stačí ukázat, že $(0,1)$ není spočetný. Každé reálné $r \in (0,1)$ lze vyjádřit pomocí desetinného rozvoje

$$r = 0, r_1 r_2 r_3 \cdots .$$

Předpokládejme, že místo konečných rozvojů uvažujeme jen nekonečné rozvoje s periodou 9. Tj. místo $0,378$ uvažujeme $0,377999\cdots$ apod. Pak má každé číslo právě jeden rozvoj.

Kdyby bylo možné čísla z $(0,1)$ seřadit do posloupnosti $r_1, r_2, \ldots,$ mohli bychom uvažovat číslo $s = 0, s_1 s_2 \cdots$ definované pomocí diagonály schématu

$$\begin{array}{c|cccc} & 1 & 2 & 3 & \cdots \\ \hline r_1 & \mathbf{r_{11}} & r_{12} & r_{13} & \cdots \\ r_2 & r_{21} & \mathbf{r_{22}} & r_{23} & \cdots \\ r_3 & r_{31} & r_{32} & \mathbf{r_{33}} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

předpisem: pro $i \in \mathbb{N}$ je s_i libovolné z $\{1, \ldots, 9\} - \{r_{ii}\}$.

Pak s má uvažovaný rozvoj a $s \neq r_1$, $s \neq r_2$, $\ldots$, což je spor s předpokladem. $\square$

Další vlastnosti spočetných množin

Věta Pro libovolnou nekonečnou množinu A existuje injektivní zobrazení $f : \mathbb{N} \to A$.
(Tedy A obsahuje nekonečnou spočetnou podmnožinu; totiž $f(\mathbb{N})$.)

Důkaz $f : \mathbb{N} \to A$ budeme definovat indukcí:

1. Def. $f(1)$ jako libovolný prvek z A.
2. Předp., že pro $n \in \mathbb{N}$ jsou definovány $f(1), \dots, f(n)$ a že jsou po dvou různé.

   Pak $\{f(1), \dots, f(n)\} \subseteq A$ je konečná, je různá od A, a tedy existuje $a \in A - \{f(1), \dots, f(n)\}$.

   Položme $f(n+1) = a$.

Podle principu definice matematickou indukcí existuje injektivní zobrazení $f : \mathbb{N} \to A$. $\square$

(Ke zmíněnému principu se vrátíme.)

Často používané tvrzení k prokázání spočetnosti:

Věta Pokud A je spočetná a $B \subseteq A$, pak B je spočetná.

Důkaz Je-li B konečná, je dle definice spočetná.

Je-li B nekonečná, existuje dle věty výše injekce $f : \mathbb{N} \to B$. Uvažujme $f(\mathbb{N})$. Pak:

$$f(\mathbb{N}) \subseteq B \subseteq A,$$

přitom existuje bijekce množiny A na $f(\mathbb{N})$.

(Bijekci $g : A \to f(\mathbb{N})$ dostaneme např. jako $g = h^{-1} \circ f$, kde $h : \mathbb{N} \to A$ je bijekce.)

Tvrzení nyní plyne z následujícího lemma (jeho důkaz později):

Lemma Existuje-li bijekce množiny A_1 na A_3 a je-li $A_3 \subseteq A_2 \subseteq A_1$, pak existuje bijekce množiny A_1 na A_2.

$\square$

Věta Kartézský součin $A \times B$ spočetných množin A a B je spočetná množina.

Důkaz 1. Jsou-li A a B konečné, je $A \times B$ konečná (a tedy spočetná).

2. Je-li jedna nekonečná (např. $A = \{a_1, a_2, \dots\}$) a druhá konečná ($B = \{b_1, \dots, b_k\}$), lze prvky $\langle a_i, b_j \rangle \in A \times B$ uspořádat do posloupnosti

$$\langle a_1, b_1 \rangle, \langle a_1, b_2 \rangle, \dots, \langle a_1, b_k \rangle, \langle a_2, b_1 \rangle, \dots, \langle a_2, b_k \rangle, \langle a_3, b_1 \rangle, \dots$$

(bijekce $f : \mathbb{N} \to A \times B$ je $f(n) = \langle a_i, b_j \rangle$, kde $i = \lceil n/k \rceil$ a $j = ((n-1) \bmod k) + 1$)

3. Jsou-li nekonečné, $A = \{a_1, a_2, \dots\}$ a $B = \{b_1, b_2, \dots\}$, definujme $f : A \times B \to \mathbb{N}$ takto:

$$f(a_i, b_j) = 2^i \cdot 3^j.$$

Protože 2 a 3 jsou prvočísla, je $2^i \cdot 3^j = 2^k \cdot 3^l$, právě když $i = k$ a $j = l$, tedy f je injekce. Máme tedy bijekci $A \times B$ na $f(A \times B)$.

$f(A \times B) \subseteq \mathbb{N}$ a $\mathbb{N}$ je spočetná je (viz věta) $f(A \times B)$ spočetná. Tedy i $A \times B$ je spočetná. $\square$

Věta Jsou-li $A_1, \ldots, A_n$ spočetné množiny, je i $A_1 \times \cdots \times A_n$ spočetná množina.

Důkaz Matematickou indukcí s použitím předchozí věty.

1. pro $n = 1$ zřejmé.

2. Předpokládejme, že tvrzení platí pro n a uvažujme $A_1 \times \cdots \times A_{n+1}$.

Pak $A_1 \times \cdots \times A_n$ je spočetná a dle předchozí věty je i $(A_1 \times \cdots \times A_n) \times A_{n+1}$ spočetná. Je zřejmé, že $f : A_1 \times \cdots \times A_n) \times A_{n+1} \to A_1 \times \cdots \times A_{n+1}$ definovaná

$$f(\langle\langle a_1, \ldots, a_n\rangle, a_{n+1}\rangle) = \langle a_1, \ldots, a_{n+1}\rangle$$

je bijekce.

Tedy i $A_1 \times \cdots \times A_{n+1}$ je spočetná. $\square$

Věta Sjednocení spočetného systému spočetných množin je spočetná množina.

Důkaz Uvažujme systém $\{A_i \mid i \in I\}$, kde I je spočetná a každá A_i je spočetná, a jeho sjednocení $\bigcup_{i \in I} A_i$.

Když jsou I i všechny A_i konečné, je i $\bigcup_{i \in I} A_i$ konečná.

Předpokládejme tedy, že I nebo některá A_i je nekonečná.

Přednáška.

$\square$

Jednoduché důsledky předchozích tvrzení:

$\mathbb{Q}$ je spočetná (už víme):

- rozložme $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$
- ukážeme, že $\mathbb{Q}^+ = \{\frac{p}{q} \in \mathbb{Q} \mid p, q \in \mathbb{N}$ nesoudělná $\}$ je spočetná:
  - zobrazení $f\mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$ definované $f(\frac{p}{q}) = \langle p, q \rangle$ je bijekce množiny $\mathbb{Q}^+$ na podmnožinu $f(\mathbb{Q}^+)$ spočetné množiny $\mathbb{N} \times \mathbb{N}$, proto je $\mathbb{Q}^+$ je spočetná.
- $\mathbb{Q}^-$ je spočetná ($x \mapsto -x$ je bijekce $\mathbb{Q}^-$ na $\mathbb{Q}^+$) a $\{0\}$ je spočetná,
- tedy i $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$ je spočetná.

Σ^* je spočetná pro každou spočetnou Σ (už víme pro konečnou Σ):

- Každý řetězec $a_1 \cdots a_n \in \Sigma^*$ lze jednoznačně reprezentovat n-ticí $\langle a_1, \ldots, a_n \rangle \in \Sigma^n$.
  (prázdný řetězec ε pak prvkem $\emptyset$; pozn.: $\Sigma^0 = \{\emptyset\}$)
- Zřejmě tedy existuje bijekce množiny Σ^* na $\bigcup_{n=0}^{\infty} \Sigma^n$.
  ($\varepsilon \mapsto \emptyset$ a $a_1 \cdots a_n \mapsto \langle a_1, \ldots, a_n \rangle$)
- $\bigcup_{n=0}^{\infty} \Sigma^n$ je spočetná (je to sjednocení spočetného systému spočetných množin).
- Tedy i Σ^* je spočetná.

Jak porovnávat množiny podle jejich velikosti?

Pro konečné množiny A a B platí (ověřte):

- $|A| = |B|$, právě když existuje bijekce $f : A \to B$.
- $|A| < |B|$, právě když existuje injekce $f : A \to B$ a neexistuje injekce $g : B \to A$.

Pomocí pokročilejšího aparátu teorie množin lze dokázat, že pro obecné množiny A a B nastane právě jedna z možností:

1. Existuje bijekce $f : A \to B$.
   Pak se A a B považují za stejně velké (jsou tzv. ekvivalentní; mají stejnou mohutnost).
2. Existuje injekce $f : A \to B$ a neexistuje injekce $g : B \to A$.
   Pak se A považuje za menší než B (A má menší mohutnost než B).
3. Existuje injekce $f : B \to A$ a neexistuje injekce $g : A \to B$.
   Pak se A považuje za větší než B (A má větší mohutnost než B).

Kardinální číslo

Kardinální číslo (kardinalita) množiny A je objekt, označujeme ho $|A|$, přiřazený množině A tak, že $|A| = |B|$, právě když A a B jsou ekvivalentní.

Definici nebudeme uvádět (viz literatura o teorii množin).

Pro konečnou A lze $|A|$ ztotožnit s počtem prvků množiny A (ten jsme značili $|A|$).

Pro nekonečnou množinu složitější. Pro zajímavost:

- Cantor: $|A|$ je třída všech množin ekvivalentních s A (problematické z hlediska axiomatických teorií množin)
- axiomatické přístupy (ZFC): $|A|$ je nejmenší ordinální číslo ekvivalentní s A

Pro možnosti 1., 2. a 3. výše pak píšeme $|A| = |B|$, $|A| < |B|$ a $|A| > |B|$.

Značení:

- $\aleph_0 = |\mathbb{N}|$, tj. mohutnost množiny $\mathbb{N}$
- $\aleph_1 = |\mathbb{R}|$, tj. mohutnost množiny $\mathbb{R}$
- víme, že $\aleph_0 < \aleph_1$

Cantorova-Bernsteinova věta

Věta Pokud pro množiny A a B existuje injekce $f : A \to B$ a injekce $g : B \to A$, pak existuje bijekce množiny A na množinu B.

Důkaz Nebudeme dělat (komentář na přednášce).

Poznámka

- Dokresluje výše uvedené možnosti 1., 2. a 3.:
- Pokud existuje injekce A do B i injekce B do A, je to případ 1 (existuje bijekce A na B).
- Dokázal G. Cantor s použitím tzv. axiomu výběru.
- 1897 pak F. Bernstein bez axiomu výběru, konstruktivní důkaz.

Cantorova věta

Věta Pro každou množinu A platí $|A| < |2^A|$.

Tedy existuje injekce $f : A \to 2^A$, ale neexistuje injekce $g : 2^A \to A$.

Před důkazem:

- S ohledem na to, že $a \mapsto \{a\}$ je injekce A do 2^A, a s ohledem na Cantorovu-Bernsteinovu větu lze Cantorovu větu ekvivalentně formulovat takto:

  Neexistuje bijekce $f : A \to 2^A$.
- Pro konečné množiny známe, protože pak $|2^A| = 2^{|A|}$.
- Ukazuje, že existují větší a větší množiny, nekonečná hierarchie nekonečen.
- Víme, že $|\mathbb{N}| < |\mathbb{R}|$. Ale ještě větší než $\mathbb{R}$ je množina $2^{\mathbb{R}}$. Ještě větší je $2^{2^{\mathbb{R}}}$ atd.
- S tím souvisí slavná tzv. hypotéza kontinua (komentář na přednášce):

  Neexistuje množina A, pro kterou $|\mathbb{N}| < |A| < |\mathbb{R}|$.

Důkaz Cantorovy věty ($|A| < |2^A|$)

Stačí dokázat, že neexistuje surjekce $f : A \to B$.

Dokážeme sporem. Předpokládejme, že $f : A \to 2^A$ je surjekce.

Uvažujme množinu $D \in 2^A$ definovanou následovně:

$$a \in D, \text{ právě když } a \notin f(a).$$

(např. pro $A = \mathbb{N}$, $a = 2$, pro $f(a) = \{1, 3, 5\}$ je $2 \notin D$, pro $f(a) = \mathbb{N}$ je $a \in D$)

f je surjekce, tedy existuje $d \in A$ t.ž. $f(d) = D$.
Pak

$$d \in D, \text{ p.k. } d \notin f(d), \text{ p.k. } d \notin D,$$

což je spor. $\square$

Myšlenka podobná jako u dříve uvedené diagonální metody. Srovnejte s předchozím důkazem, že $2^{\mathbb{N}}$ je nespočetná (z toho plyne $|\mathbb{N}| < |2^{\mathbb{N}}|$).