Mohutnosti množin

Konečné množiny

Definice. Množina X se nazývá **konečná**, jestliže existuje přirozené číslo n a prostá funkce $f : X \to n$.

Definice. Množina X se nazývá **nekonečná**, jestliže není konečná. :-)

Definice. Předpokládejme, že X je konečná množina. Dále nechť n je nejmenší přirozené číslo takové, že existuje prostá funkce $f : X \to n$. Pak n se nazývá **mohutnost množiny** X nebo že n je **počet prvků množiny** X. Potom píšeme $|X| = n$. Jsou-li X a Y konečné množiny, přičemž současně $|X| = n$ a $|Y| = n$, pak píšeme: $|X| = |Y|$.

Věta. Je-li A konečná množina a $|A| = n$, pak jestliže $f : A \to n$ je prostá funkce, potom f je bijekce.

Důkaz. Předpokládáme, že A je konečná množina a $|A| = n$. Pokud je $A = \emptyset$, pak $|A| = 0$ a $f : A \to 0$ je zřejmě surjektivní. Nyní předpokládejme, že A je neprázdná množina a nechť $f : A \to n$ je prostá funkce. Zřejmě $n \neq 0$. Sporem předpokládejme, že funkce f není surjektivní. Pak existuje $k \in n$ takové, že $k \notin ran(f)$. Dále nechť m je takové přirozené číslo, pro které platí $n = m^+$. Jelikož $k \in n = m^+$, potom buď $k = m$ nebo $k \in m$. Pokud by platilo $k = m$, pak $f : A \to m$ je prostá funkce. Protože $m < n$, dostáváme spor s tím, že $|A| = n$. Pokud by platilo $k \in m$, pak položíme:

$$g(a) = \begin{cases} k, & \text{pokud } f(a) = m, \\ f(a), & \text{pokud } f(a) \neq m. \end{cases}$$

protože je funkce f prostá, je funkce $g : A \to m$ také prostá. Protože $m \in n$, plyne odsud $|A| \in n$, což je spor s tím, že $|A| = n$. □

Věta. Nechť A je konečná množina a $f : A \to A$ je prostá funkce. Pak f je surjektivní.

Věta. Jsou-li A a B konečné množiny, pak $|A| = |B|$ právě tehdy, když existuje bijekce $f : A \to B$.

Důkaz. Provádět jej nebudeme.□

Věta. Pro všechna přirozená čísla n platí $|n| = n$.

Dirichletův zásuvkový princip

Věta (Dirichletův zásuvkový princip). Nechť m a n jsou přirozená čísla a nechť $f : n \to m$ je funkce. Jestliže $m \in n$, pak f není prostou funkcí.

Důkaz. Předpokládejme sporem, že m, n jsou přirozená čísla taková, že $m < n$ a $f : n \to m$ je prostá funkce. Protože je $m \subset n$, lze definovat prostou funkci $g : m \to n$ takto:

$$g(k) = k$$

pro všechna $k \in m$. Dále položme $h = g \circ f$. Potom $h : n \to n$ je prostá funkce. Díky předcházející větě je funkce h surjektivní. Tedy

$$n = ran(h) = \{g(f(k)) : k \in n\} = \{f(k) : k \in n\} = ran(f) \subset m.$$

Odtud plyne, že $n \subset m \in n$, což znamená, že $m \in m$. To je spor s tím, že pro každé přirozené číslo m platí $m \notin m$. □

Důsledek. Nechť $f : \omega \to A$ je prostá funkce. Pak je množina A nekonečná.

Důkaz. Ponecháme jako cvičení. □

(*Řešení cvičení.* Sporem předpokládejme, že A je konečná množina. Pak existuje přirozené číslo m a prostá funkce $f : A \to m$. Pak je složená funkce $h = g \circ f : \omega \to m$ také prostá funkce. Pokud je nyní n takové přirozené číslo, že $m \in n$, pak je restrikce složené funkce h na n také prostá funkce. Protože $m \in n$, dostáváme spor s Dirichletovým zásuvkovým principem.)

Věta. Nechť X je množina je množina všech binárních posloupností, tj.

$$X = \{f : f : \omega \to \{0, 1\}\}.$$

Potom X je nekonečná množina.

Důkaz. Nebudeme jej provádět. □

Věta. Je-li A konečná množina a $f : A \to A$ je surjektivní funkce, pak f je prostou funkcí a tedy je bijekcí.

Důkaz. Ponecháme jako cvičení. □

(*Řešení cvičení.* ...)

Věta. Nechť A je konečná množina. Potom je potenční množina $P(A)$ též konečná.

Důkaz. Ponecháme jako cvičení. □

(*Řešení cvičení.* ...)

Spočetné množiny

Definice. Množina X se nazývá **spočetná**, jestliže existuje prostá funkce $f : X \to \omega$.

Poznámka. Je-li X konečná množina, pak je zřejmé, že X je spočetná množina.

Definice. Řekneme, že množina X je **nekonečnou spočetnou** množinou, jestliže X je nekonečná a spočetná množina.

Příklad. Množina $X = \omega$ je nekonečná spočetná množina.

Věta. Nechť A a B jsou množiny a nechť B je spočetná množina. Je-li pak funkce $f : A \to B$ prostá, pak A je spočetná množina.

Důkaz. Nechť A, B jsou množiny a nechť B je spočetná množina. Dále nechť $f : A \to B$ je prostá funkce. Z definice spočetnosti plyne existence prosté funkce $g : B \to \omega$. Potom složená funkce $h = g \circ f : A \to \omega$ je prostá funkce. Tudíž A je spočetná množina. □

Věta. Nechť A, B jsou množiny a nechť $A \subset B$. Je-li B spočetná množina, pak A je spočetná množina.

Důkaz. Nechť A, B jsou množiny a nechť $A \subset B$. Dále nechť $i : A \to B$ je injektivní funkce definovaná předpisem $i(a) = a$ pro všechna $a \in A$. Nyní je tvrzení věty důsledkem předchozí věty. □

Věta. Jsou-li A a B spočetné množiny, pak i množina $A \cup B$ je spočetná množina.

Důkaz. Nechť A a B jsou spočetné množiny. Z definice spočetnosti existují prosté funkce $f : A \to \omega$ a $g : B \to \omega$.

Pro důkaz poslední věty "Jsou-li A a B spočetné množiny, pak i množina $A \cup B$ je spočetná množina" potřebujeme zkonstruovat prostou funkci množiny $A \cup B$ do ω.

Definujme funkci $h : A \cup B \to \omega$ následujícím předpisem:

$$h(x) = \begin{cases} 2 \cdot f(x) & \text{pokud } x \in A \\ 2 \cdot g(x) + 1 & \text{pokud } x \in B \setminus A \end{cases}$$

Ověřme, že funkce h je prostá:

1. Pro libovolné $x, y \in A$ platí: pokud $h(x) = h(y)$, pak $2 \cdot f(x) = 2 \cdot f(y)$, tedy $f(x) = f(y)$. Jelikož f je prostá, máme $x = y$.
2. Pro libovolné $x, y \in B \setminus A$ platí: pokud $h(x) = h(y)$, pak $2 \cdot g(x) + 1 = 2 \cdot g(y) + 1$, tedy $g(x) = g(y)$. Jelikož g je prostá, máme $x = y$.
3. Pro $x \in A$ a $y \in B \setminus A$ platí: $h(x) = 2 \cdot f(x)$ je sudé číslo, zatímco $h(y) = 2 \cdot g(y) + 1$ je liché číslo. Proto $h(x) \neq h(y)$.

Tím jsme ověřili, že funkce h je prostá, a tedy množina $A \cup B$ je spočetná. □

Poznámka: Tato konstrukce funguje obecně, ať už jsou množiny A a B disjunktní či nikoliv. Pokud x leží v průniku $A \cap B$, přiřadíme mu hodnotu podle první podmínky, tedy $h(x) = 2 \cdot f(x)$.

Věta. Nechť A je nekonečná spočetná množina. Potom existuje bijekce $g : \omega \to A$.

Důkaz. Jelikož A je spočetná množina, existuje podle definice prostá funkce $f : A \to \omega$. Označme množinu $B = f(A) = \{f(a) \mid a \in A\} \subseteq \omega$.

Vzhledem k tomu, že f je prostá a A je nekonečná, musí být i množina B nekonečná podmnožina ω.

Nyní zkonstruujeme bijekci mezi ω a B. Jelikož B je nekonečná podmnožina ω, můžeme její prvky uspořádat vzestupně:

$$B = \{b_0, b_1, b_2, \ldots\}$$

kde $b_0 < b_1 < b_2 < \ldots$ jsou všechny prvky množiny B uspořádané podle velikosti.

Definujme funkci $h : \omega \to B$ předpisem $h(n) = b_n$ pro každé $n \in \omega$. Tato funkce přiřazuje číslu n n-tý nejmenší prvek množiny B.

Funkce h je zjevně:

1. Prostá: pokud $m \neq n$, pak $b_m \neq b_n$ (jsou to různé prvky uspořádané posloupnosti), tedy $h(m) \neq h(n)$.
2. Na: každý prvek $b \in B$ je n-tým nejmenším prvkem B pro nějaké $n \in \omega$, takže $h(n) = b$.

Tedy $h : \omega \to B$ je bijekce.

Dále uvažujme funkci $f^{-1} : B \to A$ definovanou předpisem $f^{-1}(b) = a$, kde $a \in A$ je prvek splňující $f(a) = b$. Tato funkce existuje a je bijekce, protože f je prostá funkce z A na B.

Nyní můžeme definovat hledanou bijekci $g : \omega \to A$ jako složení funkcí:

$$g = f^{-1} \circ h$$

Funkce g je bijekce, protože je složením dvou bijekcí. Pro každé $n \in \omega$ platí:

$$g(n) = f^{-1}(h(n)) = f^{-1}(b_n)$$

Tím jsme zkonstruovali bijekci $g : \omega \to A$, což bylo požadováno. □

Nespočetné množiny

Definice. Množina X se nazývá **nespočetná**, jestliže není spočetná, tj. jestliže neexistuje prostá funkce $f : X \to \omega$.

Poznámka. Jako první Georg Cantor dokázal existenci nespočetných množin. Metodě, kterou Cantor použil, se říká **Cantorova diagonalizace**.

Věta. Nechť $\mathcal{F}$ je množina je množina všech binárních posloupností, tj.

$$\mathcal{F} = \{f : f : \omega \to \{0, 1\}\}.$$

Potom X je nespočetná množina.

Důkaz. Předpokládejme sporem, že X je spočetná množina. Nyní z toho, že množina všech binárních posloupností je nekonečnou množinou, plyne, že existuje bijekce $h : \omega \to \mathcal{F}$. Pro každé $i \in \omega$ definujme $f_i = h(i)$. Potom

$$\mathcal{F} = \{f_0, f_1, f_2, \ldots\} \tag{(1)}$$

Nyní definujme binární posloupnost $g : \omega \to \{0, 1\}$ takovou, že pro každé $i \in \omega$ je $g \neq f_i$. Definujme g takto:

$$g(i) = \begin{cases} 0 & \text{pokud } f_i(i) = 1 \\ 1 & \text{pokud } f_i(i) = 0, \end{cases}$$

pro každé $i \in \omega$. Je zřejmé, že $g : \omega \to \{0, 1\}$ a tedy $g \in \mathcal{F}$. Z definice posloupnosti g plyne, že $g \neq f_i$ pro každé $i \in \omega$. To je spor s tím, že h je bijekce. □

Poznámka. Očíslovaný seznam všech binárních posloupností $f_0, f_1, f_2, \ldots$ lze zapsat v následující vertikální tabulce:

$$\begin{aligned}
f_0 &= \langle f_0(0),\ f_0(1),\ f_0(2),\ f_0(3),\ f_0(4),\ f_0(5),\ \ldots \rangle \\
f_1 &= \langle f_1(0),\ f_1(1),\ f_1(2),\ f_1(3),\ f_1(4),\ f_1(5),\ \ldots \rangle \\
f_2 &= \langle f_2(0),\ f_2(1),\ f_2(2),\ f_2(3),\ f_2(4),\ f_2(5),\ \ldots \rangle \\
f_3 &= \langle f_3(0),\ f_3(1),\ f_3(2),\ f_3(3),\ f_3(4),\ f_3(5),\ \ldots \rangle \\
f_4 &= \langle f_4(0),\ f_4(1),\ f_4(2),\ f_4(3),\ f_4(4),\ f_4(5),\ \ldots \rangle \\
f_5 &= \langle f_5(0),\ f_5(1),\ f_5(2),\ f_5(3),\ f_5(4),\ f_5(5),\ \ldots \rangle \\
&\vdots
\end{aligned}$$

Pokud budeme předpokládat, že například $f_0(0) = 0$, $f_1(1) = 1$, $f_2(2) = 0$, $f_3(3) = 0$, $f_4(4) = 1$ a $f_5(5) = 1$, pak posloupnost g bude mít hodnoty $g(0) = 1$, $g(1) = 0$, $g(2) = 1$, $g(3) = 1$, $g(4) = 0$ a $g(5) = 0$. Tedy posloupnost g se liší od každé posloupnosti f_i právě v i-tém členu. Tímto způsobem Cantor dokázal, že množina všech binárních posloupností je nespočetná.

$$\begin{aligned}
f_0 &= \langle\ \mathbf{0}\ ,\ f_0(1),\ f_0(2),\ f_0(3),\ f_0(4),\ f_0(5),\ \ldots \rangle \\
f_1 &= \langle f_1(0),\ \mathbf{1}\ ,\ f_1(2),\ f_1(3),\ f_1(4),\ f_1(5),\ \ldots \rangle \\
f_2 &= \langle f_2(0),\ f_2(1),\ \mathbf{0}\ ,\ f_2(3),\ f_2(4),\ f_2(5),\ \ldots \rangle \\
f_3 &= \langle f_3(0),\ f_3(1),\ f_3(2),\ \mathbf{0}\ ,\ f_3(4),\ f_3(5),\ \ldots \rangle \\
f_4 &= \langle f_4(0),\ f_4(1),\ f_4(2),\ f_4(3),\ \mathbf{1}\ ,\ f_4(5),\ \ldots \rangle \\
f_5 &= \langle f_5(0),\ f_5(1),\ f_5(2),\ f_5(3),\ f_5(4),\ \mathbf{1}\ ,\ \ldots \rangle \\
&\vdots \\
g &= \langle\ \mathbf{1}\ ,\ \mathbf{0}\ ,\ \mathbf{1}\ ,\ \mathbf{1}\ ,\ \mathbf{0}\ ,\ \mathbf{0}\ ,\ \ldots \rangle
\end{aligned}$$

Věta. Nechť A a B jsou množiny. Je-li množina A nespočetná a existuje prostá funkce $g : A \to B$, pak B je nespočetná množina.

Důkaz. Důkaz se provede sporem. Předpokládáme, že množina B je naopak spočetná. Nyní protože je funkce $g : A \to B$ prostá, plyne odsud, že je i množina A spočetná. To je spor s tím, že množina A je nespočetná. □

Lemma. Existuje prostá funkce $f : \mathcal{F} \to \mathbb{R}$, kde $\mathcal{F}$ je množina všech binárních posloupností a $\mathbb{R}$ je množina reálných čísel.

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

Důkaz. Jedná se o důsledek předchozí věty a lemmatu. □

Ekvipotence množin

Definice. Nechť A a B jsou množiny. Řekneme, že množiny A a B jsou **ekvipotentní** nebo že mají stejnou **mohutnost**, jestliže existuje bijekce $f : A \to B$. V takovém případě píšeme $|A| =_c |B|$.

Poznámka. Jsou-li A a B konečné množiny, pak $|A| =_c |B|$ právě tehdy, když $|A| = |B|$. Tedy pro konečné množiny je ekvipotence shodná s rovností počtu prvků.

Ekvipotence ω a $\mathbb{Z}$ resp. $\mathbb{Q}$

Věta. $|\omega| =_c |\mathbb{Z}|$ a $|\omega| =_c |\mathbb{Q}|$.

Důkaz.

Konstrukce bijekce $f : \omega \to \mathbb{Z}$:

$$f(n) = \begin{cases} 0, & n = 0, \\ k, & n = 2k-1,\ k \geq 1, \\ -k, & n = 2k,\ k \geq 1. \end{cases}$$

Popis.

- Pro $n = 0$ máme $f(0) = 0$.

- Pro lichá $n \geq 1$ (tj. $n = 2k-1$) přiřadíme $f(n) = k > 0$.

- Pro sudá $n \geq 2$ (tj. $n = 2k$) přiřadíme $f(n) = -k < 0$.

Injektivita.

- Pokud $n_1, n_2 > 0$ oba liché a $f(n_1) = f(n_2)$, pak $k_1 = k_2 \Rightarrow$ $n_1 = 2k_1 - 1 = 2k_2 - 1 = n_2$.
- Analogicky pro obě sudá n_1, n_2.
- Nelze mít rovnost mezi hodnotou kladnou a zápornou ani mezi nulou a které-koliv nenulovou hodnotou, neboť znaménka (resp. nula) se liší.

Surjektivita. Každé $z \in \mathbb{Z}$ je buď 0 (obraťme $n = 0$), nebo kladné ($z = k > 0$, má protějšek $n = 2k-1$), nebo záporné ($z = -k < 0$, má protějšek $n = 2k$).

Tím je f bijekcí a tedy $|\omega| =_c |\mathbb{Z}|$.

Část 1: Jiný důkaz toho, že $|\omega| =_c |\mathbb{Z}|$

Připomeňme, že $\omega = \{0, 1, 2, 3, \ldots\}$ je množina přirozených čísel (včetně nuly) a $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ je množina celých čísel. Množiny A a B jsou ekvipotentní, píšeme $|A| =_c |B|$, pokud existuje bijekce $f : A \to B$.

Potřebujeme najít bijekci $f : \omega \to \mathbb{Z}$. Definujme funkci f následovně:

$$f(n) = \begin{cases} n/2 & \text{pokud } n \text{ je sudé} \\ -(n+1)/2 & \text{pokud } n \text{ je liché} \end{cases}$$

Ověřme, že f je bijekce:

1. **f je prostá (injektivní):** Předpokládejme, že $f(n_1) = f(n_2)$ pro $n_1, n_2 \in \omega$.
   - Pokud jsou n_1, n_2 obě sudá, pak $n_1/2 = n_2/2$, z čehož plyne $n_1 = n_2$.
   - Pokud jsou n_1, n_2 obě lichá, pak $-(n_1+1)/2 = -(n_2+1)/2$, z čehož plyne $n_1 + 1 = n_2 + 1$, a tedy $n_1 = n_2$.
   - Pokud je n_1 sudé a n_2 liché, pak $f(n_1) = n_1/2 \geq 0$ a $f(n_2) = -(n_2+1)/2 < 0$. Protože nezáporné číslo se nemůže rovnat zápornému číslu, $f(n_1) \neq f(n_2)$. Tento případ tedy nemůže nastat, pokud $f(n_1) = f(n_2)$.

   Funkce f je tedy prostá.

2. **f je na (surjektivní):** Nechť $z \in \mathbb{Z}$ je libovolné celé číslo. Hledáme $n \in \omega$ takové, že $f(n) = z$.
   - Pokud $z \geq 0$, zvolme $n = 2z$. Protože $z \geq 0$, je n sudé přirozené číslo (nebo nula), tedy $n \in \omega$. Pak $f(n) = f(2z) = (2z)/2 = z$.
   - Pokud $z < 0$, položme $z = -k$ pro nějaké $k \in \mathbb{Z}, k > 0$. Hledáme liché n takové, že $f(n) = -(n+1)/2 = -k$. To znamená $(n+1)/2 = k$, neboli $n + 1 = 2k$, a tedy $n = 2k - 1$. Protože $k \geq 1$, je $n = 2k - 1 \geq 2(1) - 1 = 1$. Tedy n je liché přirozené číslo, $n \in \omega$. Pak $f(n) = f(2k-1) = -((2k-1)+1)/2 = -(2k)/2 = -k = z$.

   Pro každé $z \in \mathbb{Z}$ jsme našli $n \in \omega$ takové, že $f(n) = z$. Funkce f je tedy na.

Protože $f : \omega \to \mathbb{Z}$ je prostá i na, je to bijekce. Tím jsme dokázali, že $|\omega| =_c |\mathbb{Z}|$.

Část 2: Důkaz $|\omega| =_c |\mathbb{Q}|$

Připomeňme $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0\}$ je množina racionálních čísel. Budeme postupovat tak, že ukážeme, že $\mathbb{Q}$ je nekonečná spočetná množina. Podle věty uvedené v textu ("Nechť A je nekonečná spočetná množina. Potom existuje bijekce $g : \omega \to A$.") pak bude platit $|\omega| =_c |\mathbb{Q}|$.

1. $\mathbb{Q}$ **je nekonečná:** Množina celých čísel $\mathbb{Z}$ je podmnožinou $\mathbb{Q}$ ($\mathbb{Z} \subset \mathbb{Q}$, protože každé $z \in \mathbb{Z}$ lze psát jako $z/1$). Jelikož jsme v části 1 ukázali, že $\mathbb{Z}$ je ekvipotentní s nekonečnou množinou ω, je $\mathbb{Z}$ nekonečná. Proto i její nadmnožina $\mathbb{Q}$ musí být nekonečná.

2. $\mathbb{Q}$ **je spočetná:** Podle definice je množina spočetná, pokud existuje prostá funkce z ní do ω. Použijeme větu: "Nechť A a B jsou množiny a nechť B je spočetná množina. Je-li pak funkce $f : A \to B$ prostá, pak A je spočetná množina." Ukážeme, že existuje prostá funkce z $\mathbb{Q}$ do nějaké známé spočetné množiny.
   - Uvažujme množinu $\mathbb{Z} \times \mathbb{N}$. Tato množina je spočetná.

(Důkaz spočetnosti $\mathbb{Z} \times \mathbb{N}$: Víme, že $|\mathbb{Z}| =_c |\omega|$ a $|\mathbb{N}| =_c |\omega|$ (např. bijekce $n \mapsto n+1$ z ω do $\mathbb{N}$ a její inverze). Existují tedy bijekce $f_Z : \mathbb{Z} \to \omega$ a $f_N : \mathbb{N} \to \omega$. Pak funkce $F : \mathbb{Z} \times \mathbb{N} \to \omega \times \omega$ definovaná jako $F(z, n) = (f_Z(z), f_N(n))$ je bijekce. Množina $\omega \times \omega$ je spočetná, protože existuje prostá funkce $h : \omega \times \omega \to \omega$, například $h(a, b) = 2^a 3^b$ (jednoznačnost prvočíselného rozkladu zaručuje prostotu) nebo Cantorova párovací funkce. Protože existuje bijekce z $\mathbb{Z} \times \mathbb{N}$ do spočetné množiny $\omega \times \omega$, je i $\mathbb{Z} \times \mathbb{N}$ spočetná.)

- Nyní zkonstruujme prostou funkci $j : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$. Každé racionální číslo $q \in \mathbb{Q}$ lze jednoznačně zapsat ve tvaru $q = p/r$, kde $p \in \mathbb{Z}$, $r \in \mathbb{N}$ ($r \geq 1$) a p, r jsou nesoudělná (jejich největší společný dělitel je 1). Definujme $j(q) = (p, r)$. Ověřme, že j je prostá. Nechť $q_1, q_2 \in \mathbb{Q}$ a $j(q_1) = j(q_2)$. To znamená, že $(p_1, r_1) = (p_2, r_2)$, kde $q_1 = p_1/r_1$ a $q_2 = p_2/r_2$ jsou zápisy v základním tvaru. Rovnost dvojic znamená $p_1 = p_2$ a $r_1 = r_2$. Potom ale $q_1 = p_1/r_1 = p_2/r_2 = q_2$. Funkce j je tedy prostá.
- Máme prostou funkci $j : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ a víme, že množina $\mathbb{Z} \times \mathbb{N}$ je spočetná. Podle výše zmíněné věty je tedy i množina $\mathbb{Q}$ spočetná.

3. **Závěr:** Dokázali jsme, že $\mathbb{Q}$ je nekonečná a spočetná množina. Podle věty "Nechť A je nekonečná spočetná množina. Potom existuje bijekce $g : \omega \to A$." tedy existuje bijekce $g : \omega \to \mathbb{Q}$. To znamená, že $|\omega| =_c |\mathbb{Q}|$.

Tím je důkaz obou částí věty dokončen. □

Striktní nerovnost mezi mohutnostmi

Definice. Řekneme, že množina A má **striktně menší mohutnost** než množina B a píšeme: $|A| <_c |B|$, jestliže existuje prostá funkce $f : A \to B$ a neexistuje bijekce $g : A \to B$.

Věta (G. Cantor). Nechť A je libovolná množina. Potom $|A| <_c |P(A)|$, kde $P(A)$ je potenční množina množiny A.

Důkaz. Musíme ukázat dvě věci:

1. Existuje prostá funkce $f : A \to P(A)$.
2. Neexistuje bijekce (a tedy ani surjekce) $g : A \to P(A)$.

Ad 1. Definujme funkci $f : A \to P(A)$ předpisem $f(a) = \{a\}$ pro každé $a \in A$. Funkce f přiřazuje každému prvku a z množiny A jednoprvkovou množinu $\{a\}$, která je prvkem potenční množiny $P(A)$. Ověřme, že f je prostá. Nechť $a_1, a_2 \in A$ a $f(a_1) = f(a_2)$. To znamená $\{a_1\} = \{a_2\}$. Dvě množiny jsou si rovny právě tehdy, když mají stejné prvky. Proto musí platit $a_1 = a_2$. Funkce f je tedy prostá.

Ad 2. Předpokládejme sporem, že existuje surjektivní funkce $g : A \to P(A)$. To znamená, že ke každé podmnožině $S \subseteq A$ (tj. ke každému $S \in P(A)$) existuje alespoň jedno $a \in A$ takové, že $g(a) = S$.

Nyní zkonstruujme specifickou podmnožinu D množiny A, známou jako Cantorova diagonální množina:

$$D = \{a \in A \mid a \notin g(a)\}$$

Množina D obsahuje právě ty prvky a z A, které nepatří do množiny $g(a)$, kterou jim funkce g přiřazuje. Jelikož D je podmnožina A, platí $D \in P(A)$.

Protože jsme předpokládali, že g je surjektivní, musí existovat nějaký prvek $d \in A$ takový, že $g(d) = D$. Nyní se ptejme: Platí $d \in D$ nebo $d \notin D$?

- **Případ 1:** Předpokládejme, že $d \in D$. Podle definice množiny D, pokud $d \in D$, pak musí platit $d \notin g(d)$. Ale víme, že $g(d) = D$. Dosazením dostáváme: pokud $d \in D$, pak $d \notin D$. To je spor.
- **Případ 2:** Předpokládejme, že $d \notin D$. Podle definice množiny D, pokud $d \notin D$, znamená to, že prvek d nesplňuje podmínku pro zařazení do D, tj. neplatí $d \notin g(d)$. Musí tedy platit opak: $d \in g(d)$. Ale víme, že $g(d) = D$. Dosazením dostáváme: pokud $d \notin D$, pak $d \in D$. To je opět spor.

Oba možné případy vedou ke sporu. To znamená, že náš původní předpoklad o existenci surjektivní funkce $g : A \to P(A)$ musí být nepravdivý. Pokud neexistuje surjektivní funkce z A do $P(A)$, nemůže existovat ani bijektivní funkce z A do $P(A)$.

Závěr: Ukázali jsme, že existuje prostá funkce $f : A \to P(A)$ a že neexistuje bijekce $g : A \to P(A)$. Podle definice striktně menší mohutnosti tedy platí $|A| <_c |P(A)|$. □

Věta (G. Cantor). $|\omega| <_c |\mathbb{R}|$. Tedy množina $\mathbb{R}$ má větší mohutnost než množina ω.

Hypotéza kontinua a metoda forcingu

Hypotéza kontinua. Hypotéza kontinua je hypotéza, že neexistuje množina $A \subset \mathbb{R}$ taková, že $|\omega| <_c |A| <_c |\mathbb{R}|$. Tedy mezi množinami ω a $\mathbb{R}$ neexistuje žádná jiná množina.

Kurt Gödel v roce 1940 ukázal, že hypotéza kontinua je *konzistentní* s axiomy teorie množin ZFC (nelze ji v ZFC vyvrátit). Paul Cohen v roce 1963 dokázal, že i její negace je konzistentní s ZFC (nelze ji v ZFC dokázat). Dohromady to znamená, že hypotéza kontinua je na axiomech ZFC *nezávislá*.

Metoda forcingu. Paul Cohen pro důkaz nezávislosti hypotézy kontinua vyvinul metodu zvanou **forcing**. Tato metoda umožňuje konstruovat nové modely teorie množin, ve kterých platí nebo neplatí určité výroky, jako je hypotéza kontinua.

Definice. Nechť A a B jsou množiny. Řekneme, že množina A **má mohutnost menší nebo rovnou** než množina B a píšeme $|A| \leq_c |B|$, jestliže existuje prostá funkce $f : A \to B$.

Cantor-Bernstein-Schröderova věta

Věta (Cantor-Bernstein-Schröderova). Nechť A a B jsou množiny. Pak platí:

$$|A| \leq_c |B| \text{ a } |B| \leq_c |A| \implies |A| =_c |B|.$$

Důkaz.

Předpokládáme, že existují prosté (injektivní) funkce $f : A \to B$ a $g : B \to A$. Naším cílem je zkonstruovat bijektivní funkci $h : A \to B$.

Pro libovolný prvek $x \in A$ nebo $x \in B$ můžeme sledovat jeho "předky" pomocí inverzních funkcí f^{-1} a g^{-1} (pokud existují). Pro daný prvek $a \in A$ můžeme vytvořit posloupnost předků:

$$a, \quad g^{-1}(a), \quad f^{-1}(g^{-1}(a)), \quad g^{-1}(f^{-1}(g^{-1}(a))), \quad \dots$$

Tato posloupnost je definována pouze tehdy, pokud jsou příslušné inverzní obrazy definovány. Jelikož f a g jsou pouze injektivní, nemusí být definovány pro všechny prvky. Posloupnost předků pro prvek a končí, pokud narazíme na prvek, který nemá předka (tj. prvek v A, který není v obrazu $g(B)$, nebo prvek v B, který není v obrazu $f(A)$).

Rozdělíme množinu A na tři disjunktní podmnožiny podle původu jejího řetězce předků:

1. A_A: Množina prvků $a \in A$, jejichž řetězec předků končí v množině A (tj. končí prvkem $a_0 \in A \setminus g(B)$).
2. A_B: Množina prvků $a \in A$, jejichž řetězec předků končí v množině B (tj. končí prvkem $b_0 \in B \setminus f(A)$).
3. A_∞: Množina prvků $a \in A$, jejichž řetězec předků je nekonečný.

Analogicky rozdělíme množinu B na tři disjunktní podmnožiny B_A, B_B, B_∞.

Lze ukázat, že:

- Funkce f zobrazuje A_A do B_A, A_B do B_B a A_∞ do B_∞.
- Funkce g zobrazuje B_A do A_A, B_B do B_B a B_∞ do A_∞.
- Restrikce $f|_{A_A} : A_A \to B_A$ je bijekce.
- Restrikce $f|_{A_\infty} : A_\infty \to B_\infty$ je bijekce.
- Restrikce $g|_{B_B} : B_B \to A_B$ je bijekce. Proto její inverze $(g|_{B_B})^{-1} : A_B \to B_B$ je také bijekce.

Nyní můžeme definovat bijekci $h : A \to B$ následovně:

$$h(a) = \begin{cases} f(a) & \text{pokud } a \in A_A \text{ nebo } a \in A_\infty \\ (g|_{B_B})^{-1}(a) & \text{pokud } a \in A_B \end{cases}$$

Tato funkce h je definována pro všechny $a \in A = A_A \cup A_B \cup A_\infty$. Funkce h je bijekcí, protože je složena z bijekcí na disjunktních částech definičního oboru a oboru hodnot:

- h mapuje A_A bijektivně na B_A pomocí f.
- h mapuje A_∞ bijektivně na B_∞ pomocí f.
- h mapuje A_B bijektivně na B_B pomocí $(g|_{B_B})^{-1}$.

Jelikož $B = B_A \cup B_B \cup B_\infty$ a tyto množiny jsou disjunktní, je h bijekcí z A do B. Tím je existence bijekce dokázána a platí $|A| =_c |B|$. $\square$

(Alternativní důkazová konstrukce)

Nechť $f : A \to B$ a $g : B \to A$ jsou injektivní. Definujme množinu $C = A \setminus g(B)$. Toto jsou prvky v A, které nemají předka v B skrze g. Definujme množinu "potomků" C v A opakovanou aplikací $g \circ f$:

$$A^* = \bigcup_{n=0}^{\infty} (g \circ f)^n(C) = C \cup (g \circ f)(C) \cup (g \circ f)^2(C) \cup \dots$$

kde $(g \circ f)^0$ je identita na A. Definujme funkci $h : A \to B$ takto:

$$h(a) = \begin{cases} f(a) & \text{pokud } a \in A^* \\ g^{-1}(a) & \text{pokud } a \notin A^* \end{cases}$$

- **Korektnost definice:** Pokud $a \notin A^*$, pak $a \notin C = A \setminus g(B)$, což znamená $a \in g(B)$. Protože g je injektivní, existuje právě jedno $b \in B$ takové, že $g(b) = a$. Toto b označujeme $g^{-1}(a)$. Funkce h je tedy dobře definovaná.
- **Injektivita:** Ukáže se, že pokud $a_1 \neq a_2$, pak $h(a_1) \neq h(a_2)$ rozborem případů, zda a_1, a_2 patří či nepatří do A^*. Klíčovým krokem je ukázat, že $f(A^*)$ a $g^{-1}(A \setminus A^*)$ jsou disjunktní podmnožiny B.
- **Surjektivita:** Pro libovolné $b \in B$ se ukáže, že existuje $a \in A$ takové, že $h(a) = b$. Rozliší se případy, zda $g(b)$ patří do A^* či nikoliv.

Jelikož h je injektivní i surjektivní, je to bijekce a platí $|A| =_c |B|$. □

Věta. $|\mathbb{R}| =_c |P(\omega)|$.

Důkaz. Použijeme Cantor-Bernstein-Schröderovu větu. K tomu potřebujeme ukázat existenci dvou prostých funkcí:

1. Prosté funkce $f : \mathbb{R} \to P(\omega)$.
2. Prosté funkce $g : P(\omega) \to \mathbb{R}$.

Ad 1: Existence prosté funkce $f : \mathbb{R} \to P(\omega)$

Víme, že množina racionálních čísel $\mathbb{Q}$ je spočetná, tedy $|\mathbb{Q}| =_c |\omega|$. Existuje tedy bijekce $b : \mathbb{Q} \to \omega$. Tato bijekce indukuje bijekci $B : P(\mathbb{Q}) \to P(\omega)$ definovanou jako $B(S) = \{b(q) \mid q \in S\}$ pro $S \subseteq \mathbb{Q}$.

Definujme funkci $h : \mathbb{R} \to P(\mathbb{Q})$ předpisem:

$$h(x) = \{q \in \mathbb{Q} \mid q < x\}$$

Ukážeme, že h je prostá. Nechť $x, y \in \mathbb{R}$ a $x \neq y$. Bez újmy na obecnosti předpokládejme $x < y$. Podle vlastnosti hustoty racionálních čísel v reálných číslech existuje $q_0 \in \mathbb{Q}$ takové, že $x < q_0 < y$. Potom $q_0 \in h(y)$ (protože $q_0 < y$), ale $q_0 \notin h(x)$ (protože $q_0 > x$). Tudíž $h(x) \neq h(y)$. Funkce h je tedy prostá.

Nyní definujme $f : \mathbb{R} \to P(\omega)$ jako složení $f = B \circ h$. Jelikož h je prostá a B je bijekce (tedy také prostá), je jejich složení f také prostá funkce. Tím jsme dokázali existenci prosté funkce z $\mathbb{R}$ do $P(\omega)$, což znamená $|\mathbb{R}| \leq_c |P(\omega)|$.

Ad 2: Existence prosté funkce $g : P(\omega) \to \mathbb{R}$

Připomeňme, že $P(\omega)$ je množina všech podmnožin $\omega = \{0, 1, 2, \ldots\}$. Každé podmnožině $S \subseteq \omega$ můžeme jednoznačně přiřadit její charakteristickou funkci $\chi_S : \omega \to \{0, 1\}$, kde $\chi_S(n) = 1$ pokud $n \in S$ a $\chi_S(n) = 0$ pokud $n \notin S$. Označme $\mathcal{F}$ množinu všech takových charakteristických funkcí (binárních posloupností). Existuje zřejmá bijekce mezi $P(\omega)$ a $\mathcal{F}$, takže $|P(\omega)| =_c |\mathcal{F}|$. Stačí tedy ukázat existenci prosté funkce $g : \mathcal{F} \to \mathbb{R}$.

Definujme funkci $g : \mathcal{F} \to \mathbb{R}$ následovně. Pro $f \in \mathcal{F}$, $f = (f(0), f(1), f(2), \ldots)$, položme:

$$g(f) = \sum_{n=0}^{\infty} \frac{f(n)}{3^{n+1}}$$

Tato funkce zobrazuje binární posloupnost f na reálné číslo v intervalu $[0, 1/2]$ zapsané v ternární (trojkové) soustavě jako $0.f(0)f(1)f(2)\ldots_3$. V tomto zápisu se vyskytují pouze číslice 0 a 1.

Ukážeme, že g je prostá. Nechť $f_1, f_2 \in \mathcal{F}$ a $f_1 \neq f_2$. Pak existuje nejmenší index $k \in \omega$ takový, že $f_1(k) \neq f_2(k)$. Bez újmy na obecnosti předpokládejme $f_1(k) = 0$ a $f_2(k) = 1$. Potom:

$$g(f_1) = \sum_{n=0}^{k-1} \frac{f_1(n)}{3^{n+1}} + \frac{0}{3^{k+1}} + \sum_{n=k+1}^{\infty} \frac{f_1(n)}{3^{n+1}}$$

$$g(f_2) = \sum_{n=0}^{k-1} \frac{f_2(n)}{3^{n+1}} + \frac{1}{3^{k+1}} + \sum_{n=k+1}^{\infty} \frac{f_2(n)}{3^{n+1}}$$

Protože $f_1(n) = f_2(n)$ pro $n < k$, máme:

$$g(f_2) - g(f_1) = \frac{1}{3^{k+1}} + \sum_{n=k+1}^{\infty} \frac{f_2(n) - f_1(n)}{3^{n+1}}$$

Odhadneme sumu:

$$\left| \sum_{n=k+1}^{\infty} \frac{f_2(n) - f_1(n)}{3^{n+1}} \right| \leq \sum_{n=k+1}^{\infty} \frac{|f_2(n) - f_1(n)|}{3^{n+1}} \leq \sum_{n=k+1}^{\infty} \frac{1}{3^{n+1}}$$

Tato geometrická řada má součet:

$$\sum_{n=k+1}^{\infty} \frac{1}{3^{n+1}} = \frac{1}{3^{k+2}} + \frac{1}{3^{k+3}} + \cdots = \frac{1}{3^{k+2}} \left(1 + \frac{1}{3} + \frac{1}{3^2} + \ldots\right) = \frac{1}{3^{k+2}} \frac{1}{1 - 1/3} = \frac{1}{3^{k+1}}$$

Tedy:

$$g(f_2) - g(f_1) \geq \frac{1}{3^{k+1}} - \sum_{n=k+1}^{\infty} \frac{f_1(n)}{3^{n+1}} \geq \frac{1}{3^{k+1}} - \sum_{n=k+1}^{\infty} \frac{1}{3^{n+1}} = \frac{1}{3^{k+1}} - \frac{1}{2 \cdot 3^{k+1}} = \frac{1}{2 \cdot 3^{k+1}} > 0$$

Proto $g(f_1) \neq g(f_2)$. Funkce g je tedy prostá. (Alternativně: Reprezentace reálného čísla v ternární soustavě je nejednoznačná pouze tehdy, končí-li nekonečnou posloupností číslic 2. Jelikož naše reprezentace používá pouze číslice 0 a 1, je vždy jednoznačná.)

Existuje tedy prostá funkce $g : \mathcal{F} \to \mathbb{R}$. Protože $|P(\omega)| =_c |\mathcal{F}|$, existuje i prostá funkce z $P(\omega)$ do $\mathbb{R}$, což znamená $|P(\omega)| \leq_c |\mathbb{R}|$.

Závěr: Ukázali jsme, že $|\mathbb{R}| \leq_c |P(\omega)|$ a $|P(\omega)| \leq_c |\mathbb{R}|$. Podle Cantor-Bernstein-Schröderovy věty z toho plyne, že $|\mathbb{R}| =_c |P(\omega)|$. □