7.5 Cardinality

Def. Sets X & Y are said to have the same cardinality if and only if there is a bijection $f: X \to Y$. In this case, we write $X \sim Y$.

THM. (i) $A \sim A$. (ii) $A \sim B \Rightarrow B \sim A$ (iii) $A \sim B$, $B \sim C \Rightarrow A \sim C$. (iv) If A & B are finite, then $A \sim B$ iff $N(A) = N(B)$.

Proof. (i) id_A (ii) If $f: A \to B$ is a bijection, then $f^{-1}: B \to A$ is also a bijection. (iii) If $f: A \to B$, $g: B \to C$ are bijections, so is $g \circ f: A \to C$. (iv) Proved in section 7.2.

Lemma. (Decomposition THM). Give $f: X \to Y$, $g: Y \to X$, there exists sets A, A', B, B', s.t., $X = A \cup A'$, $Y = B \cup B'$, $A \cap A' = \phi$, $B \cap B' = \phi$ and $f(A) = B$, $g(B') = A'$.

Proof. We call a subset E of X seperated if $E \cap g(Y \setminus f(E)) = \phi$. Let $\Gamma = \{E \subseteq X \mid E \text{ is seperated}\}$, and $A = \bigcup_{E \in \Gamma} E$.

For any $E \in \Gamma$, we have $E \subseteq A \Rightarrow f(E) \subseteq f(A)$

$\Rightarrow Y \setminus f(A) \subseteq Y \setminus f(E)$

$\Rightarrow g(Y \setminus f(A)) \subseteq g(Y \setminus f(E))$

But $E \cap g(Y \setminus f(E)) = \phi$. So $E \cap g(Y \setminus f(A)) = \phi$.

If $A \cap g(Y \setminus f(A)) \neq \emptyset$, then $\exists x \in A$ and $x \in g(Y \setminus f(A))$.

But $A = \bigcup_{E \in \Gamma} E$. So $x \in E$ for some $E \in \Gamma$.

$\Rightarrow x \in E \cap g(Y \setminus f(A))$ for this E. This is a contradiction.

Thus $A \cap g(Y \setminus f(A)) = \phi$.

Define $A' = g(Y \setminus f(A))$. Then $A \cap A' = \phi$.

If $A \cup A' \neq X$, then $\exists\, x \in X$, s.t., $x \notin A$, $x \notin A'$.

Consider $\tilde{A} = A \cup \{x\}$. $A \subseteq \tilde{A} \Rightarrow f(A) \subseteq f(\tilde{A})$

$\Rightarrow Y \setminus f(\tilde{A}) \subseteq Y \setminus f(A) \Rightarrow g(Y \setminus f(\tilde{A})) \subseteq g(Y \setminus f(A))$

But $\tilde{A} \cap g(Y \setminus f(A)) = \phi$. So $\tilde{A} \cap g(Y \setminus f(\tilde{A})) = \phi$.

So $\tilde{A} \in \Gamma$, and, therefore, $\tilde{A} \subseteq A \Rightarrow x \in A$.

This is a contradiction. $\Rightarrow A \cup A' = X$

Now let $B = f(A)$, $B' = Y \setminus f(A)$. The sets A, A', B, B' satisfy all the conditions in the lemma.

THM. If there is an injection $f: X \to Y$ and an injection $g: Y \to X$, then $X \sim Y$.

Proof. By the lemma, $\exists\ A, A', B, B'$ s.t.,

$A \cup A' = X$, $B \cup B' = Y$, $A \cap A' = \phi$, $B \cap B' = \phi$,

$f(A) = B$, $g(B') = A'$. Consider the maps

$f|_A : A \to B$, $g|_{B'} : B' \to A'$. Since f & g are injective, $f|_A$ & $g|_{B'}$ are bijections.

Define $h: X \to Y$ by $h(x) = \begin{cases} f(x), & x \in A \\ g^{-1}(x), & x \in A' \end{cases}$.

It's clear that h is bijective. So $X \sim Y$.

Def. $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$. A set X is called countably infinite if $X \sim \mathbb{Z}^+$. A set Y is called countable if Y is finite or countably infinite.

Eg. $\mathbb{Z}$ is countably infinite.

$f: \mathbb{Z} \to \mathbb{Z}^+$, $f(x) = \begin{cases} 2x+1, & x \geq 0 \\ 2|x|, & x < 0 \end{cases}$, is bijective.

Eg. $2\mathbb{Z}^+ := \{2x \mid x \in \mathbb{Z}^+\}$ is countably infinite.

$f: \mathbb{Z}^+ \to 2\mathbb{Z}^+$, $f(x) = 2x$, is a bijection.

Eg. $\mathbb{Q}^+ :=$ set of positive rational #s is countably infinite.

$$\begin{array}{c|ccccc}
 & 1, & 2, & 3, & 4, & 5 \\
1 & \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \\
2 & \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} \\
3 & \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5}
\end{array}$$

Put p/q at p-th row & q-th column.

The numbering of the fractions define a relation from $\mathbb{Q}^+ \to \mathbb{Z}^+$, i.e., $r \in \mathbb{Q}^+$ is related to n if and only if the n-th fraction $= r$. This is not a function, since very r is related to infinitely many positive integers. Let $X_r \subseteq \mathbb{Z}^+$ be the set of integers related to $r \in \mathbb{Q}^+$. If $r_1 \neq r_2$, then $X_{r_1} \cap X_{r_2} = \phi$.

By Well-Ordering Principle, $\exists!\ x_r \in X_r$, s.t., $x_r \leq x$ for any $x \in X_r$. Define $f: \mathbb{Q}^+ \to \mathbb{Z}^+$ by $f(r) = x_r$. Then f is injective. Define $g: \mathbb{Z}^+ \to \mathbb{Q}^+$ by $g(n) = n$. g is also injective. Then, by the THM, $\mathbb{Q}^+ \sim \mathbb{Z}^+$.

Eg. $\mathbb{Q} :=$ set of rational #'s is countably infinite.

Since $\mathbb{Q}^+$ is countably infinite, we can order all positive rational #'s as $r_1, r_2, r_3, \cdots$. So we can write all rational #s as

$$\begin{array}{cccc}
0 & r_1 & r_2 & r_3 \\
 & -r_1 & -r_2 & -r_3 & \cdots
\end{array}$$

The numbering on the diagram is a bijection $\mathbb{Q} \to \mathbb{Z}^+$.

THM. Let X be any set. There are no bijections $f: X \to \mathcal{P}(X)$.

Proof. If $X = \emptyset$, THM is trivially true. Now assume $X = \emptyset$, and there is a bijection $f: X \to \mathcal{P}(X)$. Let $A \subset X$ be $A = \{x \in X \mid x \notin f(x)\}$. Since f is a bijection, $\exists!\, a \in X$, s.t., $f(a) = A$. If $a \in A$, then $a \notin f(a)$, i.e., $a \notin A$. If $a \notin A$, then $a \notin f(a) \Rightarrow a \in A$.

We have contradictions either way. This means such bijection f can not exist.

THM. There are no bijections $f: \mathbb{Z}^+ \to [0,1)$.

Proof. Any $x \in [0,1)$ has (1 or 2) binary decimal reps. If $x \neq 0$ has a finite rep $x = 0.r_1 r_2 r_3 \cdots r_k$, where $r_k = 1$, then $x = 0.r_1 r_2 \cdots r_{k-1} 0111\cdots$. If x does not have a finite rep, then x has a unique infinite rep. Anyway, $x \in (0,1)$ always has a unique infinite binary decimal rep.

Let $x = 0.r_1 r_2 r_3 \cdots$ be the infinite rep of x. Define $A_x = \{n \in \mathbb{Z}^+ \mid r_n \neq 0\}$. Then $g: [0,1) \to \mathcal{P}(\mathbb{Z}^+)$, $g(x) = A_x$, if $x \neq 0$, $g(0) = \emptyset$, is an injection.

For any $A \in \mathcal{P}(\mathbb{Z}^+)$, define $h(A) = \sum_{n \in A} 3^{-n}$.

This gives a function $h: \mathcal{P}(\mathbb{Z}^+) \to [0,1)$.

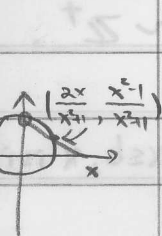
Let $A_1 \neq A_2 \in \mathcal{P}(\mathbb{Z}^+)$. By Well-Ordering Principle, $\exists!$ least element n of $(A_1 \cup A_2) \setminus (A_1 \cap A_2)$.

Then $|h(A_1) - h(A_2)| \geq 3^{-n} - \sum_{k \in (A_1 \cup A_2) \setminus (A_1 \cap A_2)} 3^{-k}$

$\geq 3^{-n} - \sum_{k=n+1}^{\infty} 3^{-k} = 3^{-n} - \frac{3^{-n}}{2} = \frac{3^{-n}}{2} \neq 0$.

$\Rightarrow h(A_1) \neq h(A_2) \Rightarrow h$ is an injection

$\Rightarrow [0,1) \sim \mathcal{P}(\mathbb{Z}^+)$ and $[0,1) \not\sim \mathbb{Z}^+$.



THM. $\mathbb{R} \sim [0,1) \sim$ any interval (finite / infinite, open / closed)

Proof. Given any $x \in \mathbb{R}$, the intersection of the open segment from $(x,0)$ to $(0,1)$ with the unit circle is $P_x = \left(\frac{2x}{x^2+1}, \frac{x^2-1}{x^2+1}\right)$. Since $P_x \in$ unit circle, $P_x \neq (0,1)$, $\exists!\ \theta_x \in (0,1)$, s.t., $P_x = \left(\cos(2\pi\theta_x + \frac{\pi}{2}), \sin(2\pi\theta_x + \frac{\pi}{2})\right)$. Define $f: \mathbb{R} \to [0,1)$ by $f(x) = \theta_x$. This is an injection. $g: [0,1) \to \mathbb{R}$, $g(x) = x$, is also an injection.

$\Rightarrow \mathbb{R} \sim [0,1)$.

For any interval $I \subset \mathbb{R}$, $h: I \to \mathbb{R}$, $h(x) = x$, is an injection. For appropriate $a, b \in \mathbb{R}$, $\lambda: [0,1) \to I$, $\lambda(x) = ax + b$, $a \neq 0$, is also injective. So $\lambda \circ f: \mathbb{R} \to I$ is injective $\Rightarrow$ $I \sim \mathbb{R}$.

Here we showed that $\mathbb{R}$, and any interval $I \subseteq \mathbb{R}$, is uncountable.

THM. If A and B are countable, so is $A \cup B$.

Proof. $A = \{a_1, a_2, a_3, \dots\}$

$B = \{b_1, b_2, b_3, \dots\}$

THM. If A is countable, $B \subset A$, then B is also countable.

Proof. If B is finite, then B is countable. If B is infinite, then $\exists$ sequence $\{b_n\}_{n=1}^{\infty} \subset B$, s.t., $b_n \neq b_m$ if $n \neq m$. Define $f: \mathbb{Z}^+ \to B$ by $f(n) = b_n$. f is injective. Since A is countable, $\exists$ injective function $g: A \to \mathbb{Z}^+$.

Then $g|_B : B \to \mathbb{Z}^+$ is also injective $\Rightarrow B \sim \mathbb{Z}^+$.

Eg. $C = \{x \mid a \le x \le b,\ x \text{ is rational}\}$. $D = \{x \mid a \le x \le b,\ x \text{ is irrational}\}$

Then C is countable, D is uncountable

Proof. $C \subseteq \mathbb{Q} \Rightarrow C$ is countable.

If D is countable, then $C \cup D = [a,b]$ is countable, which is not true. $\Rightarrow D$ is uncountable.

THM. If A is countable, $B = \{X \mid X \subseteq A,\ X \text{ is finite}\}$, then B is countable.

If A is finite, so is B. $\Rightarrow$ ✓. Assume A is countably infinite.

Proof. $f: A \to B$, $f(x) = \{x\}$, is injective.

Let $g: A \to \mathbb{Z}^+$ be a bijection. then $f \circ g^{-1} : \mathbb{Z}^+ \to B$ is injective.

Define $h: B \to \mathbb{Z}^+$ by $h(X) = \sum_{x \in X} 10^{g(x)}$.

This is also an injection $\Rightarrow B \sim \mathbb{Z}^+$.

THM. If A & B are countable, then $A \times B$ is contable.

Proof.
$$\begin{array}{cccccc}
 & a_1 & a_2 & a_3 & \cdots & \\
b_1 & (a_1,b_1) & (a_2,b_1) & (a_3,b_1) & \to & \to \\
b_2 & (a_1,b_2) & (a_2,b_2) & (a_3,b_2) & & \\
b_3 & (a_1,b_3) & (a_2,b_3) & (a_3,b_3) & & \\
\vdots & & & & &
\end{array}$$

THM. The set of compter programs (in each language) is countable.

Proof. After fixing the language, compter programs $\xleftrightarrow{1-1}$ finite bit strings. Given a bit string $S = \varepsilon_1 \varepsilon_2 \varepsilon_3 \cdots$, define $A_S = \{n \in \mathbb{Z}^+ \mid \varepsilon_n = 1\}$, $B_S = \{n \in \mathbb{Z}^+ \mid \varepsilon_n = 0\}$. Let $X = \{Y \subseteq \mathbb{Z}^+ \mid Y \text{ is finite}\}$. Define $f: \underbrace{\{\text{bit strings}\}}_{\text{finite}} \to X \times X$

by $f(s) = (A_s, B_s)$. This is an injection.

$\Rightarrow$ {finite bit strings} $\sim$ range of $f \subset X \times X$.

But $X \times X$ is countable $\Rightarrow$ range of f is countable

$\Rightarrow$ {finite bit strings} is countable.

THM. (Given any computer language,) $\exists$ a function $f: \mathbb{Z}^+ \to \{0,1\}$, s.t., no computer program for this function can be written.

Proof. Let $X = \{ f \mid f: \mathbb{Z}^+ \to \{0,1\} \}$. Define $H: X \to \mathcal{P}(\mathbb{Z}^+)$ by $H(f) = \{ n \mid f(n) = 1 \}$.

Then H is a bijection, and $H^{-1}: \mathcal{P}(\mathbb{Z}^+) \to X$ is defined by $H^{-1}(A) = f$, where $A \subseteq \mathbb{Z}^+$, $f: \mathbb{Z}^+ \to \{0,1\}$

$f(n) = \begin{cases} 1, & n \in A \\ 0, & n \notin A. \end{cases}$

But $\mathcal{P}(\mathbb{Z}^+)$ is uncountable. So is X.

But the set of computer programs is countable.

$\Rightarrow \exists$ non-programmable functions.