Discrete Mathematics

Cantor’s theorem, the halting problem, countable, Schröder-Bernstein theorem, basic rules of counting, multiset, permutation

Liangfeng Zhang

School of Information Science and Technology

ShanghaiTech University

Cantor's Diagonal Argument

1890/91, Cantor (1845-1918), the creator of the theory of sets

Question: Show that $|A| \neq |\mathbb{Z}^+|$.

The Diagonal Argument:

1) Suppose that $|A| = |\mathbb{Z}^+|$. Then there is a bijection $f\colon \mathbb{Z}^+ \to A$
2) Represent the function f as a list:

$$\begin{array}{c|l}
f(1) & a_1 \cdots\cdots\cdots\cdots \\
f(2) & a_2 \cdots\cdots\cdots\cdots \\
\vdots & \quad\ \vdots \\
f(i) & a_i \cdots\cdots\cdots\cdots \\
& \qquad\qquad\qquad\quad x \\
\vdots & \quad\ \vdots
\end{array}$$

- Every element of $\mathbb{Z}^+$ appears once in the left-hand side
- Every element of A appears once in the right-hand side

3) Construct an element x by considering the diagonal of the list
4) Show that $x \neq a_i$ for all $i \in \mathbb{Z}^+$
5) Show that $x \in A$
6) 4) and 5) give a contradiction

Cantor's Theorem

THEOREM: (Cantor) Let A be any set. Then $|A| < |\mathcal{P}(A)|$.

- $\mathcal{P}(A)$: the power set of a set A, i.e., the set of all subsets of A
  - For example: $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $|A| \leq |\mathcal{P}(A)|$
  - The function $f: A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ is injective.
- $|A| \neq |\mathcal{P}(A)|$
  - Assume that there is a bijection $g: A \to \mathcal{P}(A)$
  - Define two lists $L = \{a\}_{a\in A}$ $(= A)$ and $R = \{g(a)\}_{a\in A}$ $\left(= \mathcal{P}(A)\right)$
  - Define $X = \{a : a \in A \text{ and } a \notin g(a)\}$
  - We must have that $X \in R$. It is clear that $X \subseteq A$ and hence $X \in \mathcal{P}(A) = R$
  - We must have that $X \notin R$. Suppose that $X = g(x)$ for some $x \in A$
    - If $x \in X$, then $x \notin g(x) = X$ $\rightarrow\leftarrow$
    - If $x \notin X$, then $x \in g(x) = X$ $\rightarrow\leftarrow$

The Halting Problem

1936, Turing (1912-1954)

Function $\mathrm{HALT}(P, I) = \begin{cases} \text{"halts"} & \text{if } P(I) \text{ halts;} \\ \text{"loops forever"} & \text{if } P(I) \text{ loops forever.} \end{cases}$

- P: a program; I: an input to the program P.

QUESTION: Is there a Turing machine computing HALT?

- Turing machine: can be represented as a an element of $\{0,1\}^*$
  - $\{0,1\}^* = \bigcup_{n\geq 0}\{0,1\}^n$: the set of all finite bit strings

THEOREM: There is no Turing machine computing HALT.

- Assume there is a Turing machine **HALT** computing HALT
- Define a new Turing machine **Turing**(P) that runs on any Turing machine P
  - If $\mathbf{HALT}(P, P) =$ "halts", loops forever
  - If $\mathbf{HALT}(P, P) =$ "loops forever", halts
- **Turing**(**Turing**) loops forever $\Rightarrow$ $\mathbf{HALT}(\mathbf{Turing}, \mathbf{Turing}) =$ "halts"
  $\Rightarrow$**Turing(Turing)** halts
- **Turing**(**Turing**) halts $\Rightarrow$ $\mathbf{HALT}(\mathbf{Turing}, \mathbf{Turing}) =$ "loops forever"
  $\Rightarrow$**Turing(Turing)** loops forever

Countable and Uncountable

DEFINITION: A set A is **countable** if $|A| < \infty$ or $|A| = |\mathbb{Z}^+|$; otherwise, it is said to be **uncountable**.

- countably infinite: $|A| = |\mathbb{Z}^+|$

EXAMPLE:

- $\mathbb{Z}^+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}^+, \mathbb{Q}$ are countable
- $\mathbb{R}^+, \mathbb{R}, (0,1), [0,1]$ are uncountable

THEOREM: A set A is countably infinite iff its elements can be arranged as a sequence $a_1, a_2, \ldots$

- If A is countably infinite, then there is a bijection $f\colon \mathbb{Z}^+ \to A$
- If $A = \{a_1, a_2, \ldots\}$, then the $f\colon \mathbb{Z}^+ \to A$ defined by $f(i) = a_i$ is a bijection
    - $a_i = f(i)$ for every $i = 1,2,3 \ldots$

Countable and Uncountable

THEOREM: Let A be countably infinite, then any infinite subset $X \subseteq A$ is countable.

- Let $A = \{a_1, a_2, \dots\}$. Then $X = \{a_{i_1}, a_{i_2}, \dots\}$ X is countable

THEOREM: Let A be uncountable, then any set $X \supseteq A$ is uncountable.

- If X is countable, then A is finite or countably infinite

THEOREM: If A, B are countably infinite, then so is $A \cup B$

- $A = \{a_1, a_2, a_3, \dots\}, B = \{b_1, b_2, b_3, \dots\}$
- $A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \dots\}$ //no elements will be included twice
    - application: the set of irrational numbers is uncountable

THEOREM: If A, B are countably infinite, then so is $A \times B$

- $A = \{a_1, a_2, a_3, \dots\}, B = \{b_1, b_2, b_3, \dots\}$
- $A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), (a_3, b_1), (a_1, b_4), \dots\}$

Schröder-Bernstein Theorem

QUESTION: How to compare the cardinality of sets in general?

- $|\mathbb{Z}^-| = |\mathbb{Z}^+| = |\mathbb{Z}| = |\mathbb{Q}^-| = |\mathbb{Q}^+| = |\mathbb{Q}| = |\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$
- $|\mathbb{R}^-| = |\mathbb{R}^+| = |\mathbb{R}| = |(0,1)| = |[0,1]| = |(0,1]| = |[0,1)|$
- $|\mathbb{Z}^+| \neq |[0,1)|$: in fact $|\mathbb{Z}^+| < |[0,1)|$
- $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)|$
- $|\mathcal{P}(\mathbb{Z}^+)|?\, |[0,1)|$: which set has more elements?

THEOREM: If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

EXAMPLE: Show that $|(0,1)| = |[0,1)|$

- $|(0,1)| \leq |[0,1)|$
  - $f: (0,1) \to [0,1)\ \ x \to \frac{x}{2}$ is injective
- $|[0,1)| \leq |(0,1)|$
  - $g: [0,1) \to (0,1)\ \ x \to \frac{x}{4} + \frac{1}{2}$ is injective

Schröder-Bernstein Theorem

EXAMPLE: $|\mathcal{P}(\mathbb{Z}^+)| = |[0,1)|$

- $|\mathcal{P}(\mathbb{Z}^+)| \leq |[0,1)|$
  - $f: \mathcal{P}(\mathbb{Z}^+) \to [0,1) \quad \{a_1, a_2, \dots\} \mapsto 0.\cdots 1_{a_1} \cdots 1_{a_2} \cdots$ is an injection.
- $|[0,1)| \leq |\mathcal{P}(\mathbb{Z}^+)|$
  - $\forall x \in [0,1), x = 0.r_1 r_2 \cdots \ \left(r_1, r_2, \cdots \in \{0, \dots, 9\}, \text{no } \dot{9}\right)$
    - $0 \leftrightarrow 0000, 1 \leftrightarrow 0001, \dots, 9 \leftrightarrow 1001$
    - x has a binary representation $x = 0.b_1 b_2 \cdots$
      - $f: [0,1) \to \mathcal{P}(\mathbb{Z}^+) \ \ x \mapsto \{i: i \in \mathbb{Z}^+ \wedge b_i = 1\}$ is an injection

THEOREM: $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| = |[0,1)| = |(0,1)| = |\mathbb{R}|$

$\aleph_0$ $\quad 2^{\aleph_0}$ $\quad c$

The continuum hypothesis: There is no cardinal number between $\aleph_0$ and c, i.e., there is no set A such that $\aleph_0 < |A| < c$.

Basic Rules of Counting

DEFINITION: Let A be a finite set. A **partition** of set A is a family $\{A_1, A_2, \dots, A_k\}$ of *nonempty* subsets of A such that

- $\bigcup_{i=1}^{k} A_i = A$
- $A_i \cap A_j = \emptyset$ for all $i, j \in [k]$ with $i \neq j$.

The Sum Rule: Let A be a finite set. Let $\{A_1, A_2, \dots, A_k\}$ be a partition of A. Then $|A| = |A_1| + |A_2| + \cdots + |A_k|$.

The Product Rule: Let $A_1, A_2, \dots, A_k$ be finite sets. Then

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \times |A_2| \times \cdots \times |A_k|.$$

The Bijection Rule: Let A and B be two finite sets. If there is a bijection $f: A \to B$, then $|A| = |B|$.

Permutations of Set

DEFINITION: Let $A = \{a_1, \ldots, a_n\}$ and $r \in [n]$. An **r-permutation of A** is a sequence of r distinct elements of A.

- An n-permutation of A is simply called a **permutation** of A.
  - The 2-permutations of $A = \{1,2,3\}$ are 1,2; 1,3; 2,1; 2,3; 3,1; 3,2

THEOREM: An n-element set has $P(n, r) = n!/(n-r)!$ Different r-permutations.

DEFINITION: Let $A = \{a_1, \ldots, a_n\}$ and $r \geq 1$. An **r-permutation of A with repetition** is a sequence of r elements of A.

- The 2-permutations of $A = \{1,2,3\}$ with repetition are
  - 1,1; 1,2; 1,3; 2,1; 2,2; 2,3; 3,1; 3,2; 3,3

THEOREM: An n-element set has n^r different r-permutations with repetition.

Multiset

DEFINITION: A **multiset** is a collection of elements which are not necessarily different from each other.

- An element $x \in A$ has **multiplicity** m if it appears m times in A.
- A multiset A is called an ***n*-multiset** if it has n elements.
- $A = \{n_1 \cdot a_1, n_2 \cdot a_2, \dots, n_k \cdot a_k\}$: an $(n_1 + n_2 + \cdots + n_k)$-multiset
  - a_i has multiplicity n_i for all $i \in [n]$.
- $T = \{t_1 \cdot a_1, t_2 \cdot a_2, \dots, t_k \cdot a_k\}$ is called an ***r*-subset** of A if
  - $0 \le t_i \le n_i$ for every $i \in [k]$, and
  - $t_1 + t_2 + \cdots + t_k = r$

EXAMPLE: $A = \{1 \cdot \mathrm{a}, 2 \cdot \mathrm{b}, 3 \cdot \mathrm{c}, 100 \cdot \mathrm{z}\}, T = \{1 \cdot \mathrm{b}, 98 \cdot \mathrm{z}\}$

- A is a 106-multiset; the multiplicities of a, b, c, z are 1,2,3,100, resp.
- T is a 99-subset of A

Permutations of Multiset

DEFINITION: Let $A = \{n_1 \cdot a_1, \ldots, n_k \cdot a_k\}$ be an n-multiset. A **permutation** of A is a sequence $x_1, x_2, \cdots, x_n$ of n elements, where a_i appears exactly n_i times for every $i \in [k]$.

- r**-permutation** of A: a permutation of some r-subset of A
  - $A = \{1 \cdot \mathrm{a}, 2 \cdot \mathrm{b}, 3 \cdot \mathrm{c}\}$
  - a, b, c, b, c, c is a permutation of A; bcb is a 3-permutation of A;

THEOREM: Let $A = \{n_1 \cdot a_1, n_2 \cdot a_2, \ldots, n_k \cdot a_k\}$ be a multiset.

Then A has exactly $\frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdots n_k!}$ permutations.

REMARK: Let $A = \{a_1, a_2, \ldots, a_n\}$ be a set of n elements.

- r-permutation of A w/o repetition: r-permutation of $\{1 \cdot a_1, \ldots, 1 \cdot a_n\}$.
- r-permutation of A with repetition: r-permutation of $\{\infty \cdot a_1, \ldots, \infty \cdot a_n\}$.