Discrete Mathematics

the halting problem, countable, Schröder-Bernstein theorem
the sum rule, the product rule, the bijection rule
permutations of set and multiset, T-Route

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

The Halting Problem

停机问题

program　input　string

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

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

QUESTION: Is there a Turing machine **HALT**?

- Turing machine: can be represented as an element of $\{0,1\}^*$ 二元字符串
  - $\{0,1\}^* = \bigcup_{n\geq 0} \{0,1\}^n$: the set of all finite bit strings

THEOREM: There is no Turing machine **HALT**.

- Assume there is a Turing machine **HALT**
- Define a new Turing machine **Turing**(P) that runs on any Turing machine P

规定
  - If $\mathbf{HALT}(P, P) =$ "halts", loops forever
  - If $\mathbf{HALT}(P, P) =$ "loops forever", halts

矛盾
- **Turing**(**Turing**) loops forever⇒ **HALT**(**Turing**, **Turing**) = "halts"⇒**Turing(Turing) halts**
- 2 **Turing**(**Turing**) halts ⇒ **HALT**(**Turing**, **Turing**) = "loops forever"⇒**Turing(Turing)** loops forever

Countable and Uncountable

可数, 可列

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

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

可列无穷集合

EXAMPLE:

可列集的笛卡尔积还是可列集

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

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

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

Countable and Uncountable

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

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

THEOREM: If A is uncountable, then any super set $X \supseteq A$ is uncountable.

超集

反证 $|X| < \infty \,/\, |X| = |\aleph^{+}|$

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

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

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

无理数

$\mathbb{R} \setminus \mathbb{Q}$

若L可列

又∵$\mathbb{Q}$可列

∴$\mathbb{R} = (\mathbb{R}\setminus\mathbb{Q}) \cup \mathbb{Q}$

矛盾

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

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

按下标求和排列

$|\mathbb{R}\setminus\mathbb{Q}| = |\mathbb{R}|$

Schröder-Bernstein Theorem

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

- $|\mathbb{Z}^-| = |\mathbb{Z}^+| = |\mathbb{Z}| = |\mathbb{Q}^-| = |\mathbb{Q}^+| = |\mathbb{Q}| = |\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$
- $|\mathbb{R}^-| = |\mathbb{R}^+| = |\mathbb{R}| = |(0,1)| = |[0,1]| = |(0,1]| = |[0,1)|$

上 < 下

- $|\mathbb{Z}^+| \neq |(0,1)|$: In fact, we have that $|\mathbb{Z}^+| < |(0,1)| = |\mathbb{R}|$

$|\mathbb{Z}^+| \leq |(0,1)|$ $\quad n \mapsto \frac{1}{2n}$

- $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)|$
- $|\mathbb{R}|$? $|\mathcal{P}(\mathbb{Z}^+)|$: which set has more elements?

$|\mathbb{Z}^+| \neq |(0,1)|$

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

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

存在 $A \to B$ 单射，
$B \to A$ 单射
则有 $A \to B$ 双射

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

$x \to x$

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

Schröder-Bernstein Theorem

$\{x \mid x \subseteq \mathbb{Z}^+\}$

A $\quad$ $0.b_1b_2\cdots$

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

- $|\mathcal{P}(\mathbb{Z}^+)| \le |[0,1)|$
  - $f: \mathcal{P}(\mathbb{Z}^+) \to [0,1) \quad \{a_1, a_2, \ldots\} \mapsto 0.\,0\cdots 1_{a_1} 0\cdots 1_{a_2} \cdots$ is an injection.
- $|[0,1)| \le |\mathcal{P}(\mathbb{Z}^+)|$
  - $\forall x \in [0,1),\ x = 0.r_1r_2\cdots\ \left(r_1, r_2, \cdots \in \{0, \ldots, 9\},\ \text{no } \dot{9}\right)$
    - $0 \leftrightarrow 0000,\ 1 \leftrightarrow 0001, \ldots, 9 \leftrightarrow 1001$
    - x has a binary representation $x = 0.b_1b_2\cdots$
      - $f: [0,1) \to \mathcal{P}(\mathbb{Z}^+)\ \ x \mapsto \{i : i \in \mathbb{Z}^+ \wedge b_i = 1\}$ is an injection

$0.0000\,1001$ $\quad$ $5 \quad 8$ $\quad$ $\{5, 8\}$

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

阿列夫0 $\Leftarrow$ $\aleph_0$ $\qquad 2^{\aleph_0} \qquad c$

连续统假设

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

$|\mathbb{R}|$

$|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| < |\mathcal{P}(\mathcal{P}(\mathbb{Z}^+))| \cdots$

Basic Rules of Counting

划分

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

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

加法原则

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

乘法原则

The Product Rule: Let $A_1, A_2, \ldots, A_k$ 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 $|A| = |B|$.

一一对应原则/相等原则

Basic Rules of Counting

合数

EXAMPLE: Find # of all/composite divisors of $N = 2^{100} \times 3^{200}$.

- $A = \{n \in \mathbb{Z}^+ : n|N\}$: the # of all divisors of N is $|A|$
  - $n|N$ must have the form $n = 2^a 3^b,\ 0 \le a \le 100,\ 0 \le b \le 200$
  - $|A|$ = # of ways of constructing an integer of the form $2^a 3^b$
  - $D_1 = \{2^0, 2^1, \dots, 2^{100}\}$; $D_2 = \{3^0, 3^1, \dots, 3^{200}\}$
  - $|A| = |D_1 \times D_2| = |D_1| \times |D_2| = 101 \times 201$
- $A_1 = \{n \in A : n \text{ is prime}\}$; $A_2 = \{n \in A : n \text{ is composite}\}$; $A_3 = \{1\}$
  - # of composite divisors of N is $|A_2|$
  - $\{A_1, A_2, A_3\}$ is a partition of A.
    - $|A| = |A_1| + |A_2| + |A_3|$
      - $|A_2| = |A| - |A_1| - |A_3|$
      - $|A_1| = 2,\ |A_3| = 1$
      - $|A_2| = 101 \times 201 - 2 - 1 = 20298$

1不是合数

排列

Permutations of Set

r排列

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

不同的

of A is a sequence of r <u>distinct</u> 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.

A的 r可重复排列

DEFINITION: Let $A = \{a_1, \ldots, a_n\}$ and $r \in [n]$. 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

多重集 (元素可重

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

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

1+2+3+100

- 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
  - $A = \{1 \cdot \mathrm{a},\ 2 \cdot \mathrm{b},\ 3 \cdot \mathrm{c}\}$ r排列：A的r子集的排列
  - 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.

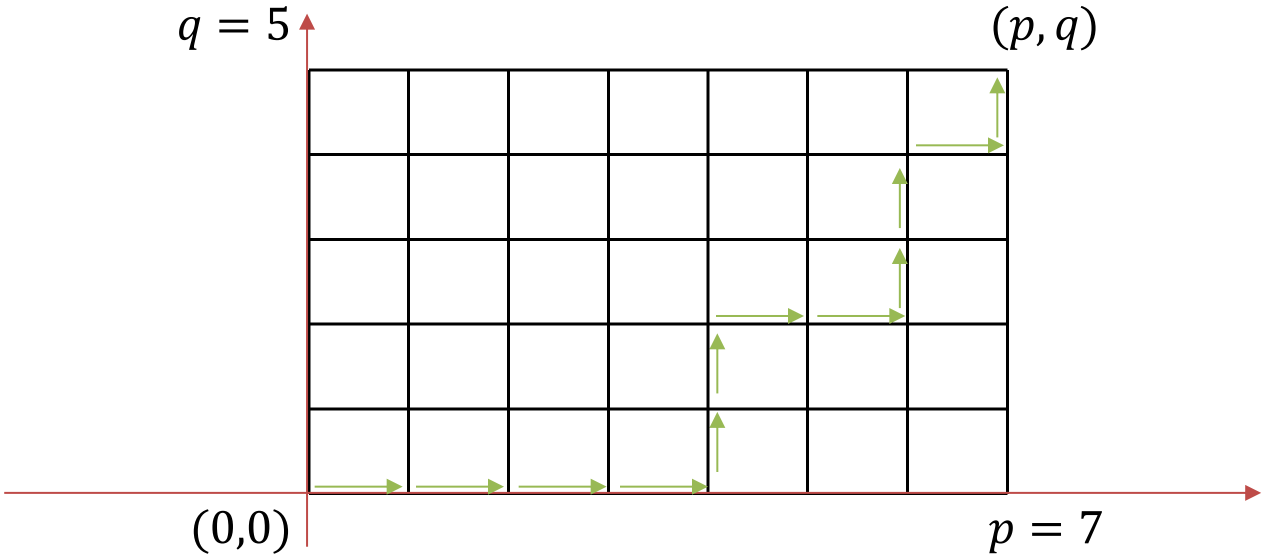
Then A has exactly $\dfrac{(n_1 + n_2 + \cdots + n_k)!}{n_1! n_2! \cdots n_k!}$ permutations.

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 $\{\infty \cdot a_1,\ \ldots, \infty \cdot a_n\}$.

Shortest Path

DEFINITION: A ***p*** × ***q*-grid** is a collection of pq squares of side length 1, organized as a rectangle of side length p and q.



THEOREM: # of shortest paths from (0,0) to (p, q) is $\frac{(p+q)!}{p!q!}$.

- Let $A = \{p \cdot\rightarrow\ ,\ q \cdot\uparrow\}$ be a $(p + q)$-multiset.
- # of shortest paths=# of permutations of A.

T-Route T路

DEFINITION: Let $A = (x, y),\ B \in \mathbb{Z}^2$. //**integral points**整点

- A **T-Step** at A is a segment from A to $(x+1, y+1)$ or $(x+1, y-1)$.
- A **T-Route** from A to B is a route where each step is a T-step.