Lecture 5-6: Counting methods

Main points:

- **inclusion-exclusion**:
- **relation**: equivalent relation, poset
- **double counting**
- **mapping:** couting in infinite set, (Cantor) diagonal method

1 集合，关系，与函数

1.1 集合

我们简单回顾集合的基本概念和运算。

把一些东西放在一起，就组成了一个集合，那每一个东西叫做一个元素。

比如自然数集 $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. 素数集，$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$. 整数集 $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$. $\mathbb{R}$表示实数集等。

设A和B是两个集合，a是某个元素。集合的一般描述方式为

$$A = \{a : a\text{满足某种性质}\}.$$

基本运算：

- 元素属于一个集合：$a \in A$；
- 元素不属于一个集合：$a \notin A$；
- 子集，即一个集合的元素全部在另一个集合里面：$B \subseteq A$；真子集：$B \subsetneq A$；
- 两个集合的交集：$A \cap B = \{x : x \in A \text{ and } x \in B\}$；
- 两个集合的并集：$A \cup B = \{x : x \in A \text{ or } x \in B\}$；
- 两个集合的差集：$A \setminus B = A - B = \{x : x \in A \text{ and } x \notin B\}$.
- 补集，如果$B \subseteq A$，则B在A种的补集定义为：$B^c = A - B$.
- 两个集合的对称差集：$A \Delta B = (A - B) \cup (B - A)$；
- 空集：$\emptyset = \{\}$；
- 笛卡尔乘积：$A \times B = \{(a, b) : a \in A, b \in B\}$；

- 幂集,由某个集合的所有子集组成的集合：$\mathcal{P}(A)$或2^A，即 $\mathcal{P}(A) = \{B : B \subseteq A\}$；
- 集合的势（或者叫集合的大小），即集合中元素的个数：$|A|$。

使用韦恩图往往可以帮助对集合进行运算（见《离散数学》p.97）。
下面看一些例子和性质。

- 交换律：$A \cup B = B \cup A$；$A \cap B = B \cap A$；
- 结合律：$(A \cup B) \cup C = A \cup (B \cup C)$； $(A \cap B) \cap C = A \cap (B \cap C)$；
- 分配律：$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$； $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$；
- 笛卡尔乘积$A \times B$里的元素(a, b)是一个有序对，即，a与b在这个地方的顺序是重要的。因此，一般来说，$A \times B \neq B \times A$。换句话说，笛卡尔乘积不具有交换律。例如： $A = \{1, 2\}$，$B = \{2, 3, 4\}$，则

$$A \times B = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$$
$$B \times A = \{(2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)\}.$$

  因此，$A \times B \neq B \times A$。不过，当$A$和$B$都是有限集时，仍然有 $|A \times B| = |B \times A| = |A| \cdot |B|$.

- 空集：注意：$\emptyset \neq \{\emptyset\}$. $|\emptyset| = 0$，$|\{\emptyset\}| = 1$.
- 幂集的例子。例如：$A = \{1, 2\}$，则

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

  基本性质：$|\mathcal{P}(A)| = 2^{|A|}$.

- $\{1\} \neq \{\{1\}\}$.

1.2 关系

Definition 1. 从A到B的二元关系：笛卡尔积$A \times B$的任意一个子集都叫做一个二元关系。

关系在生活与应用中无处不在。

Example 2. 前面拉姆齐定理中人与人的认识关系，就是一个二元关系。比如

$$A = \{\text{刘备}, \text{关羽}, \text{张飞}, \text{孙悟空}, \text{猪八戒}, \text{沙和尚}, \text{林冲}, \text{武松}, \text{鲁智深}, \text{贾宝玉}, \text{林黛玉}, \text{薛宝钗}\}.$$

如果我们考虑集合A里的人的“认识”这种关系，就可以用$A \times A$上的二元关系来描述。比如 (林冲, 武松) 和 (林黛玉, 薛宝钗) 都属于这个二元关系。但是 (张飞, 孙悟空) 就不属于这个二元关系。问：这个二元关系是一个从A到A的函数吗？

数学中的许多常见关系也可以用二元关系来描述。比如，整数集$\mathbb{Z}$上的数字大小关系：

$$\{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \leq b\}.$$

任意一个集合A里的子集的包含关系：

$$\{(B,C) \in \mathcal{P}(A) \times \mathcal{P}(A) : B \subseteq C\}.$$

等等。

某些数学对象其实也是一个二元关系。比如：圆。我们知道，单位圆的方程是$x^2 + y^2 = 1$. 因此，单位圆也可以如下描述：

$$\{(x,y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}.$$

注：这是数学和计算机科学中一个重要的观点：性质$\Longleftrightarrow$满足性质的对象的集合。在这种观点下，当我们讨论或处理与某性质有关的问题时，我们便可以去处理对应的集合。

有限集上的二元关系的其他表示方法：矩阵表示，有向图表示。

举例：整除关系 $S = \{1, 2, \ldots, 10\}$. $R : \{(a,b) : a \mid b, a, b \in S\}$. 给出矩阵表示和有向图表示。

如果某个问题涉及到一系列集合 $A_1, A_2, \ldots, A_k$，则它们笛卡尔积 $A_1 \times A_2 \times \cdots \times A_k$ 的子集就叫做k-元关系。比如，数据库的数据集，或者机器学习中的数据集，都往往涉及到许多不同的features，因此，那里的数据集，一般都是一个多元关系。比如 Iris flower dataset （鸢尾花数据集）。

1.2.1 equivalent relation

A binary relation R on a set S is called an equivalent relation if it satisfies

- reflexsive（自反）: $(x,x) \in R$, for every $x \in S$
- symmetric（对称）: $(x,y) \in R$ implies $(y,x) \in R$
- transitive（传递）: $(x,y), (y,z) \in R$ implies $(x,z) \in R$.

Examples 1: Congruence relation. On the set of natural number $\mathbb{N} = \{0, 1, 2, \ldots\}$, define the following relation

$$R_p = \{(x,y) : x, y \in \mathbb{N}, p \mid (x - y)\}.$$

It is an equivalent relation:

- reflexsive: $(x,x) \in R$: because $p \mid (x - x)$;
- symmetric: $(x,y) \in R$ implies $(y,x) \in R$: because if $p \mid (x - y)$ then $p \mid (y - x)$
- transitive: $(x,y), (y,z) \in R$ implies $(x,z) \in R$: because if $p \mid (x - y)$ and $p \mid (y - z)$ then $p \mid (x - y + y - z)$, i.e, $p \mid (x - z)$.

An equivalent relation R on set S naturally induces a **partition** of the set S into disjoint subsets. For example, fix an element x, consider the subset

$$S_x = \{y \in S : (x, y) \in R\} \subseteq S.$$

These subsets are called *equivalent classes*. One can show that for different $x \neq x'$:

- either $S_x \cap S_{x'} = \emptyset$
- or $S_x = S_{x'}$

Hence, these different S_x would give a partition of S.

For example, R_5 partitions $\mathbb{N}$ as follows into 5 equivalent classes:

$$\mathbb{N} = \{0, 5, 10, 15, \ldots\} \cup \{1, 6, 11, 16, \ldots\} \cup \{2, 7, 12, 17, \ldots\} \cup \{3, 8, 13, 18, \ldots\} \cup \{4, 9, 14, 19, \ldots\}.$$

This equivalence relation is the reason that one can do modular arithmetics on the equivalent classes, which is important for mathematics and computer science (e.g., encryption, Hash functions, etc)

Q: given two numbers x, y, how to test whether $(x, y) \in R_p$?

A: this is easy, one simply do the division to check whether $p \mid (x - y)$, so, we only need to do subtraction $x - y$ and division, both can be done fast. In other words, **this problem is polynomial time solvable, i.e., it is in P.**

Example 2: We can define an equivalent relation R_A on the set of all possible computer programs as follows: let x and y denote two computer programs, $(x, y) \in R$ iff x and y satisfy the following: for any given input, both programs x and y generate the same output. It's easy to verify that this is an equivalent relation.

Q: given two computer programs x, y, how to test whether $(x, y) \in R_A$? In other words, how to test whether two computer programs always generate the same output?

A: (based on Turing machine models) **No algorithms can do the job! In other words, this problem is undecidable.**

A little more: Because if there is an algorithm solving the above problem, there will also be another algorithm solving the Halting problem: whether a computer program halts for all input, or will run forever for some input. One of Turing's most famous results is that no algorithm can solve the Halting problem! To answer, in a mathematically rigorous way, that whether there are computational problems that can not be solved by any algorithm, requires firstly to rigorously define what an algorithm is. This is precisely the initial motivation for Turing to consider Turing machine for which he used to define the notion of algorithms, and went on to show the Halting

problem, a very natural task, that cannot be solved by any algorithm. Based on Turing's model, von Neumann together with other scientists created our modern computers!

Pause for a moment, think and appreciate how seemingly purely logical wondering **fundamentally** changes human history and **greatly** advances human civilization!

Example 3: Graph isomorphism. We will discuss this when we discuss the graph theory.

Q: given two graphs G_1, G_2, how to test whether they are isomorphic?

A: Computer scientists suspect that **this problem is of intermediate difficulty, it is inbetween P and NP**, i.e., there is no polynomial time to solve it, but brute force (exponential time algorithm) is not the best.

Equivalent relations are useful for classification and counting.

1.2.2 poset

poset = partially ordered set. A poset is a pair (S, R) where S is a set and R is a relation satisfying:

- reflexsive（自反）: $(x, x) \in R$, for every $x \in S$
- antisymmetric（反对称）: if $(x, y) \in R$ and $x \neq y$, then $(y, x) \notin R$
- transitive（传递）: $(x, y), (y, z) \in R$ implies $(x, z) \in R$.

Example 1: $(\mathbb{N}, \leq)$ is a poset.
Example 2: Let S be a set. Then $(\mathcal{P}(S), \subseteq)$ is a poset.
Example 3: a divides b over natural numbers: $\{(a, b) : a \mid b, a, b \in \mathbb{N}\}$.

1.3 函数

Definition 3. 从A到B的函数（映射）：函数是一种特殊的关系。要求满足如下条件：对每一个$a \in A$，都有且仅有唯一的$b \in B$，满足(a, b)在这个二元关系中。

下面简单复习函数$f : A \to B$的基本概念。

- 定义域：A；
- 设$a \in A$，则$f(a)$叫做a在函数f下在B中的像；
- 像集：$f(A) = \{f(a) : a \in A\}$，即所有像组成的集合；当然有 $f(A) \subseteq B$ 成立，但是$f(A)$不一定等于B；
- f是单射：$a, a' \in A$，若$a \neq a'$则$f(a) \neq f(a')$；

- f是满射：$f(A) = B$；
- f是双射：既是单射，又是满射。当f是双射时，可以定义逆函数：

$$f^{-1} : B \to A, \quad b \mapsto a,$$

满足$f(a) = b$.

- 复合函数：若$f : A \to B$，且$g : B \to C$，则可以定义复合函数

$$g \circ f : A \to C, \quad a \mapsto c,$$

其中 $c = g(b)$ 而 $b = f(a)$. 注意：给定a后，b和c都唯一确定，因此复合函数$g \circ f$的定义是正确的。

- 函数的相等：两个函数$f : A \to B$与$g : A \to B$ 相等，当且仅当，对每一个$a \in A$，都有 $f(a) = g(a)$。
- 当f是双射时，有：

$$f^{-1} \circ f : A \to A, \quad a \mapsto a.$$

而且

$$f \circ f^{-1} : A \to A, \quad a \mapsto a.$$

所以此时，$f^{-1} \circ f = f \circ f^{-1}$.

- 给定集合A和B，从A到B的所有函数的集合一般记作B^A.

Example 4. 用符号$[n]$代表集合$[n] = \{1, 2, \ldots, n\}$。问：$\{0,1\}^{[3]}$是什么？

根据定义，这是从$[3]$到$\{0,1\}$的所有函数的集合。具体写出来如下：

$$\begin{aligned}
&f_0 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 0, \quad 2 \mapsto 0, \quad 3 \mapsto 0;\\
&f_1 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 0, \quad 2 \mapsto 0, \quad 3 \mapsto 1;\\
&f_2 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 0, \quad 2 \mapsto 1, \quad 3 \mapsto 0;\\
&f_3 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 0, \quad 2 \mapsto 1, \quad 3 \mapsto 1;\\
&f_4 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 1, \quad 2 \mapsto 0, \quad 3 \mapsto 0;\\
&f_5 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 1, \quad 2 \mapsto 0, \quad 3 \mapsto 1;\\
&f_6 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 1, \quad 2 \mapsto 1, \quad 3 \mapsto 0;\\
&f_7 : [3] \mapsto \{0,1\}, \quad 1 \mapsto 1, \quad 2 \mapsto 1, \quad 3 \mapsto 1.
\end{aligned}$$

可以看出，其实，$\{0,1\}^{[3]}$这个从$[3]$到$\{0,1\}$的所有函数的集合，就是所有长度是3的0、1字符串的集合。因此，$\{0,1\}^{[n]}$ 常常写成 $\{0,1\}^n$. 容易看出 $|\{0,1\}^n| = 2^n$.

一般地，如果A与B都是有限集，则有 $|B^A| = |B|^{|A|}$. 这是因为，函数 $f : A \to B$ 其实就是对每个$a \in A$，选取一个$b \in B$与a对应。因为对于每个$a \in A$都有$|B|$种不同的选法，因此，总共不同的函数

个数就是$|A|$个$|B|$相乘： $|B| \times \cdots \times |B| = |B|^{|A|}$. 从这里可以明白，为什么从$A$到$B$的所有函数的集合记号用$B^A$，而不用$A^B$.

如上我们讨论的都是一元函数 $f : A \times B$，即变量只有一个的函数。某些问题有多个变量，就需要考虑多元函数 $f : A_1 \times \cdots \times A_k \times B$. 从集合与函数的观点来看，一元函数与多元函数没有本质的区别，因为定义域不管是A，还是 $A_1 \times \cdots \times A_k$，都是一个集合而已（后者是$k$个集合的笛卡尔积，但仍然是一个集合）。所以，数学抽象的意义之一就在于，一些看起来不同的对象，在抽象的观点下，都是同一类对象。当然，在具体分析函数时，多元函数的分析往往复杂得多。

2 计数的基本方法

前面学过的鸽笼原理，也可以看作一种基本的计数方法。不过鸽笼原理一般只用于得到某种下界（即：某个笼子种至少有多少只鸽子）。如果还要得到上界，或者精确的计算，有时需要别的方法。本节介绍一些最基本的方法。

2.1 计数方法一：容斥原理

在计数时，如果问题涉及好几个集合，并且这些集合都是有限集，则往往可以使用容斥原理。比如，如下最基本的问题：如果知道了集合A和集合B的大小，那么$A \cup B$的大小是多少呢？$A \cap B$的大小是多少呢？稍加思考（或观察韦恩图），可得如下等式：

$$|A| + |B| = |A \cup B| + |A \cap B|.$$

等价地，

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

类似地，如果有三个集合A, B, C，那么（通过观察韦恩图可得）

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Theorem 5 (容斥原理). 设有n个有限集$A_1, A_2, \ldots, A_n$，则

$$\begin{aligned} |\cup_{i=1}^n A_i| = &\sum_{i=1}^n |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \\ &+ (-1)^{t-1} \sum_{1 \le i_1 < i_2 < \cdots < i_t \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_t}| \\ &+ (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|. \end{aligned} \tag{1}$$

下面看几个例子。

Example 6. 计算$\{1, 2, \ldots, 100\}$里不能被2、3或5整除的数的个数。

解答. 设$A=\{1,2,\ldots,100\}$. 令

$$B=\{x\in A:2\mid x\},\quad |B|=50,$$
$$C=\{x\in A:3\mid x\},\quad |C|=33,$$
$$D=\{x\in A:5\mid x\},\quad |D|=20,$$

所求的答案是$100-|B\cup C\cup D|$. 根据容斥原理，有

$$|B\cup C\cup D|=|B|+|C|+|D|-|B\cap C|-|B\cap D|-|C\cap D|+|B\cap C\cap D|.$$

注意有，

$$B\cap C=\{x\in A:6\mid x\},\quad |B\cap C|=16,$$
$$B\cap D=\{x\in A:10\mid x\},\quad |B\cap D|=10,$$
$$C\cap D=\{x\in A:15\mid x\},\quad |C\cap D|=6,$$
$$B\cap C\cap D=\{x\in A:30\mid x\},\quad |C\cap D|=3.$$

因此， $|B\cup C\cup D|=50+33+20-16-10-6+3=74$. 故得所求答案是$100-74=26$. □

下面是一个运用容斥原理的经典的例子。

Example 7 (错位排列). 设一副牌有n张，每张牌上标有一个1到n之间不同的数字。洗几次牌后，如果对每一个i，第i张牌的标号都不是i，我们就说牌形成了一个错位排列，换句话说：每张牌的位置都是错的。问：在所有可能的牌的排列中，每张牌的位置都是错的的可能性是多少？

验证你的直觉： 每张牌的位置都是错的的可能性是多少？
(A) 小于50%　　(B) 大于50%.

解答. 用P_i表示标号为i的牌在正确的位置（即在第i个位置）的所有排列的集合。那么，至少有一张牌在正确的位置的所有排列数是： $|\cup_{i=1}^n P_i|$。故，每张牌的位置都是错的的排列数是： $n!-|\cup_{i=1}^n P_i|$。

利用容斥原理5计算$|\cup_{i=1}^n P_i|$。我们看其中的一般项为

$$(-1)^{t-1}\sum_{1\le i_1<i_2<\cdots<i_t\le n}|P_{i_1}\cap P_{i_2}\cap\cdots\cap P_{i_t}|. \tag{2}$$

其中， $P_{i_1}\cap P_{i_2}\cap\cdots\cap P_{i_t}$ 表示第 $i_1,i_2,\ldots,i_t$ 张牌都在正确的位置。由对称性， $|P_{i_1}\cap P_{i_2}\cap\cdots\cap P_{i_t}|$ 不依赖于 $i_1,i_2,\ldots,i_t$ 的值[1]。易见：

$$|P_{i_1}\cap P_{i_2}\cap\cdots\cap P_{i_t}|=(n-t)!$$

又注意到，(2)中一共有 $\binom{n}{t}$ 项。因此，

$$(-1)^{t-1}\sum_{1\le i_1<i_2<\cdots<i_t\le n}|P_{i_1}\cap P_{i_2}\cap\cdots\cap P_{i_t}|=(-1)^{t-1}\binom{n}{t}(n-t)!=(-1)^{t-1}\frac{n!}{t!}. \tag{3}$$

[1]比如：第1、3、27张牌在正确位置的排列个数，和第7、15、19张牌在正确位置的排列个数，两者相等。

因此，用容斥原理公式(1)得，

$$|\cup_{i=1}^{n} P_i| = \sum_{t=1}^{n} (-1)^{t-1} \frac{n!}{t!}$$

从而得到，每张牌都在错误位置的可能性是，

$$\frac{n! - |\cup_{i=1}^{n} P_i|}{n!} = \frac{n! - \sum_{t=1}^{n} (-1)^{t-1} \frac{n!}{t!}}{n!} = 1 - \sum_{t=1}^{n} (-1)^{t-1} \frac{1}{t!} = \sum_{t=0}^{n} (-1)^{t} \frac{1}{t!}.$$

根据e^x的泰勒展开式， $e^x = \sum_{t=0}^{\infty} \frac{x^t}{t!}$，有：当 $n \to \infty$ 时， $\lim_{n\to\infty} \sum_{t=0}^{n} \frac{(-1)^t}{t!} = e^{-1} \approx 37\%$. □

你猜对了吗？

2.2 计数方法二：双计数

双计数就如同生活中我们看问题时，站在不同的角度，就能看到同一事物的不同方面。生活中，尝试用另一个角度看问题，往往能有所收获。计数也是如此。

双计数操作如下：对一个恰当的（往往是二元的）集合用两种不同的方式计数。下面看两个例子[2]。

Example 8. *正20面体（每个面都是三角形）有多少条边？*

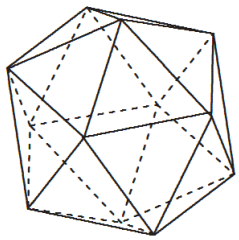

图 1: 正20面体。

当然我们可以找一个正20面体，如图1，去数它的边，但有没有不用那么费劲的方法呢？

解答. 我们要计数的对象是边的个数，考虑与边密切联系的面。因此，令

$$A = \text{正20面体所有边的集合}, \quad B = \text{正20面体所有面的集合}.$$

我们知道$|B| = 20$，想问$|A| =$?

考虑如下集合

$$C = \{(e, f) : e \in A, f \in B, e \in f\} \subseteq A \times B.$$

也就是说，我们考虑（边，面）这样的二元对，满足边在面上。

用两种观点来看C的大小$|C|$。

[2]在课堂上我们也将用图的语言来描述双计数

- 从边的观点：每条边都在两个面上。因此， $|C| = 2|A|$.
- 从面的观点：因为每个面都是三角形，所以每个面都对应三条边。因此， $|C| = 3|B|$.

从而得

$$2|A| = |C| = 3|B|.$$

因此， $|A| = 3|B|/2 = 30$. □

Example 9. 定义 $[n]^{(r)} = \{T \subseteq \{1, 2, \ldots, n\} : |T| = r\}$. 设 $\mathcal{A} \subseteq [n]^{(r)}$. 设$s > r$。定义

$$\mathcal{B} = \{B \in [n]^{(s)} : \exists\ A \in \mathcal{A},\ s.t.\ A \subseteq B\}.$$

$|\mathcal{B}|$有多大呢（当然$|\mathcal{B}|$依赖于$|\mathcal{A}|$）？

解答. 上界：根据定义 $\mathcal{B} \subseteq [n]^{(s)}$，所以 $|\mathcal{B}| \leq \left|[n]^{(s)}\right| = \binom{n}{s}$.

下界：考虑如下集合

$$M = \{(A, B) \in \mathcal{A} \times \mathcal{B} : A \subseteq B\}.$$

分别采用$\mathcal{A}$和$\mathcal{B}$的观点来计算$|M|$。

- 从$\mathcal{A}$的观点：对每个$A \in \mathcal{A}$，A包含在$\binom{n-r}{s-r}$个不同的B中。因此， $|M| = |\mathcal{A}|\binom{n-r}{s-r}$.
- 从$\mathcal{B}$的观点：对每个$B \in \mathcal{B}$，B最多包含$\binom{s}{r}$个不同的A。因此， $|M| \leq |\mathcal{B}|\binom{s}{r}$.

从而有，

$$|\mathcal{A}|\binom{n-r}{s-r} = |M| \leq |\mathcal{B}|\binom{s}{r}.$$

所以， $|\mathcal{B}| \geq \frac{\binom{n-r}{s-r}}{\binom{s}{r}}|\mathcal{A}| = \frac{\binom{n}{s}}{\binom{n}{r}}|\mathcal{A}|$.

综合上、下界，我们得到

$$\frac{|\mathcal{A}|}{\binom{n}{r}}\binom{n}{s} \leq |\mathcal{B}| \leq \binom{n}{s}. \tag{4}$$

□

体会一下(4)中下界的直观含义。

2.3 计数方法三：构造映射

这一节我们用构造映射的方法来比较集合的大小。特别是对于无限集。

验证你的直觉： 下面哪些正确？

(A) $|\mathbb{N}| < |\mathbb{Z}| < |\mathbb{Q}| < |\mathbb{R}|$　　(B) $|\mathbb{Z}| = 2|\mathbb{N}|$　　(C) $|\mathbb{Q}| = |\mathbb{Z}|$　　(D) $|\mathbb{R}| > |(0, 1)|$

给定一个有限的集合，$|A|$就是A里的元素个数。如果A是无限的集合，我们还没有准确定义$|A|$的含义。尽管如此，我们先使用$|A|$来表示（无论有限还是无限）集合A的“大小”。对有限的集合来说，如果$A \subsetneq B$，那么$|A| < |B|$. 但是对于无限的集合呢？我们如何比较无限的集合的大小？

Definition 10. 设A和B是两个集合，则，

- 若存在某个单射函数$f : A \to B$，则$|B| \geq |A|$;
- 若存在某个满射函数$f : A \to B$，则$|A| \geq |B|$;
- 若存在某个双射函数$f : A \to B$，则$|A| = |B|$.

Proposition 11. *(1)* $|\mathbb{N}| = |\mathbb{Z}|$,

(2) $|\mathbb{N}| = |\mathbb{Q}|$,

(3) $|(-1, 1)| = |\mathbb{R}|$,

(4) $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

证明. 分别构造如下的双射：

(1) 考虑映射

$$f : \mathbb{Z} \to \mathbb{N},$$
$$0 \mapsto 0, \quad 1 \mapsto 1, \quad -1 \mapsto 2, \quad 2 \mapsto 3, \quad -2 \mapsto 4, \quad \cdots$$

容易看出，f是双射。

(2) 类似（1）可证。

(3) 函数$f(x) = \tan(\pi x/2)$是双射.

(4) 考虑映射

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N},$$
$$(0,0) \mapsto 0, \quad (0,1) \mapsto 1, \quad (1,0) \mapsto 2, \quad (0,2) \mapsto 3, \quad (1,1) \mapsto 4, \quad (2,0) \mapsto 5, \quad \cdots$$

容易看出，f是双射。

□

命题11告诉我们，对于无穷集合的大小，不能简单地像有限集合那样，根据$A \subsetneq B$，便得出$|A| < |B|$。比如，上面已经证明，虽然 $\mathbb{N} \subsetneq \mathbb{Z}$，但却有 $|\mathbb{N}| = |\mathbb{Z}|$。那么，$\mathbb{R}$和$\mathbb{N}$比较又如何呢？从十九世纪下半叶到二十世纪初期，数学家康托尔在研究这个问题的过程中，发明了如下著名的对角线构造方法。

Proposition 12. *(1)* $|\mathbb{N}| < |[0, 1]|$,

(2) 对任意集合A，都有$|A| < |\mathcal{P}(A)|$.

证明. （1），(2)可以类似地证明。

(1) 首先，容易看出 $|\mathbb{N}| \leq |[0,1]|$. 因为可以构造单射函数 $g : \mathbb{N} \to [0,1]$，定义为 $g(0) = 0$，对$k \geq 1$, $g(k) = 1/k$。

现在用反证法来证明（1）。假设（1）不成立，那么因为我们已证明 $|\mathbb{N}| \leq |[0,1]|$ 始终成立，故，若（1）不成立，则必有 $|\mathbb{N}| = |[0,1]|$. 所以，$[0,1]$与$|\mathbb{N}|$存在双射。设f是一个双射如下

$$f : \mathbb{N} \to [0,1]$$
$$0 \mapsto x_1, \quad 1 \mapsto x_2, \quad 2 \mapsto x_3, \quad 3 \mapsto x_4, \quad \cdots$$

换句话说，$[0,1]$可以写成

$$[0,1] = \{x_1, x_2, x_3, x_4, \cdots\}. \tag{5}$$

我们如下来表示x_k：

$$x_k = 0.x_{k1}x_{k2}x_{k3}x_{k4}\cdots$$

其中 $x_{ki} \in \{0, 1, \ldots, 9\}$. 现在构造如下表格

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & \cdots \\ x_{21} & x_{22} & x_{23} & x_{24} & \cdots \\ x_{31} & x_{32} & x_{33} & x_{44} & \cdots \\ x_{41} & x_{42} & x_{43} & x_{44} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

我们关注其对角线，并考察数字y如下

$$y = 0.y_1y_2y_3y_4\cdots$$

满足

$$y_1 \neq x_{11}, \quad y_2 \neq x_{22}, \quad y_3 \neq x_{33}, \quad y_4 \neq x_{44}, \quad \cdots$$

显然， $y \in [0,1]$。然而，根据构造，对所有的$k \in \mathbb{N}$都有 $y \neq x_k$. 因此，根据(5)又有 $y \notin [0,1]$，这与$y \in [0,1]$矛盾。

(2) 如果$|A|$是有限集，前面已经提到过 $|\mathcal{P}(A)| = 2^{|A|} > |A|$，结论成立。以下考虑$A$是无限集合的情况。

因为$|A| \leq |\mathcal{P}(A)|$ （为什么？），用反证法，假设结论不成立，则有$|A| \geq |\mathcal{P}(A)|$，从而有 $|A| = |\mathcal{P}(A)|$。换言之，有A与$\mathcal{P}(A)$之间的双射。设$f : A \to \mathcal{P}(A)$ 是一个双射。即，对任意 $x \in A$，存在唯一的$f(x) \subseteq A$. 以下我们构造一个A的子集 $S \subseteq A$，满足如下性质：对任何$x \in A$，都有$f(x) \neq S$。这就与f是双射矛盾。

S构造如下：对任意$x \in A$，我们已知$f(x) \subseteq A$是A的子集。若$x \in f(x)$，则让S不包含x，反之，若$x \notin f(x)$，则让S包含x。即：

$$x \in f(x) \Longrightarrow x \notin S, \qquad x \notin f(x) \Longrightarrow x \in S.$$

根据定义，S当然是A的子集。但是，根据以上定义，很明显我们有$f(x) \neq S$。由于x是任意的，因此S不在f的像集里面，这表明f不是满射，这与f是双射矛盾（因为双射必须是满射）。

□

对角线构造法+反证法，是离散数学和计算机科学中一个很基本的方法。

根据命题12就得到如下推论。

Corollary 13. *(1)* $|\mathbb{N}| < |\mathbb{R}|$.

(2) $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots$.

证明. 对（1），由 $[0,1] \subseteq \mathbb{R}$ 可得 $|[0,1]| \leq |\mathbb{R}|$. 因此，由命题12得 $|\mathbb{N}| < |[0,1]| \leq |\mathbb{R}|$.

对（2），在命题12的（2）中令 $A = \mathbb{N}$ 则得到 $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. 再令 $A = \mathcal{P}(\mathbb{N})$ 则得到 $|\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))|$. 等等。 □

特别地，推论13种的（2）告诉我们：有无穷多种不同的“无穷大”。

根据上面对集合大小的讨论，可以总结成如下的定义。

Definition 14. 一个集合A如果满足$|A| \leq |\mathbb{N}|$，则A叫做是可数集，否则，A叫做不可数集.

如上我们证明了，有理数，整数，及$\mathbb{N} \times \mathbb{N}$等都是可数集。而实数集或任何开区间$(a,b)$或闭区间$[a,b]$均是不可数集。实数集的大小，一般用 $|\mathbb{R}| = \aleph_0$ 表示。特别地，实数集包含的数字比自然数“多”，即$|\mathbb{R}| = \aleph_0 > |\mathbb{N}|$，而有理数则和自然数“一样多”。因此，这也就说明：无理数比有理数“多”。数学后来进一步严格地发展了集合及测度等概念，就可以进一步说明，无理数不仅比有理数多，而且“多得多”。

总之，以康托尔 (Georg Cantor) 为代表的数学家对无限这一概念的深入研究，大大加深了人类对无限的理性认识。这是人类理性认识自然的一个里程碑。