

组合数学笔记

Combinatorics Note

葛骏 Atlas

2019 年 8 月 4 日

目录

1 什么是组合数学	2
2 排列和组合	3
2.1 四个基本计数原理	3
2.1.1 加法原理	3
2.1.2 乘法原理	3
2.1.3 减法原理	4
2.1.4 除法原理	4
2.2 集合的排列	4
2.2.1 集合的排列公式	5
2.2.2 循环排列公式	5
2.3 集合的组合（子集）	5
2.3.1 集合的组合公式	6
2.3.2 集合组合公式的推论	6
2.3.3 组合的性质一：帕斯卡公式	6
2.3.4 组合的性质二	7
2.4 多重集合的排列	7
2.4.1 无限重复数的多重集合排列	7
2.4.2 有限重复数的多重集合的排列	7
2.4.3 只有两类对象的多重集合的排列	7
2.4.4 带标签的盒子	8
2.4.5 非攻击性车	8
2.5 多重集合的组合	9
2.5.1 无限重复数的多重集合的组合	9
2.6 有限概率	11
3 鸽巢原理	11
4 附录 A	11
4.1 数学归纳法正确性的证明	11
4.2 排列与组合	12
4.2.1 结论“乘法原理是加法原理的推论”的证明	12
4.2.2 补集	12
4.2.3 2.2.1 排列公式的证明	12
4.2.4 2.2.2 循环排列公式的证明	12
4.2.5 2.3.1 集合的组合公式的证明	13
4.2.6 2.4.1 无限重复数的多重集合的排列公式的证明	13
4.2.7 2.4.2 有限重复数的多重集合的排列公式证明	13
4.3 其他	13
4.3.1 算术基本定理	13

前言

本文简介 本文是葛骏研究学习组合数学的时候整理写出，以备自用。本文参考教材是机器工业出版社 (China Machine Press) 出版的, 由美国威斯康星大学麦迪逊分校 (University of Wisconsin–Madison) 的理查德·A·布鲁尔迪教授 (Richard A. Brualdi) 所著作，北京师范大学冯速等人翻译的《组合数学 (第五版)》 (Introductory Combinatorics Fifth Edition)。

由于本文作者本人水平有限，故文中不免有纰漏、错误。(准确的说，会有很多!) 而且想到本文是自用的，所以写作之时，常常心不在焉。倘若您读到本文纰漏之处，还望与我联系交流学习更正，谢谢。

1 什么是组合数学

组合数学所关心的问题 就是把某个集合中的对象排列成某种模式，使其满足一定的规则。组合数学中反复出现两种通用的问题。

- 排列的存在性。
- 排列的列举或分类。

还有两种常常出现的组合问题

- 研究已知的排列。
- 构造最优排列。

组合数学 是研究离散构造的存在、计数、分析和优化等问题的一门学科。

组合数学验证发现的重要工具是**数学归纳法**。

数学归纳法¹ 是一种数学证明方法。运用数学归纳法 (第一数学归纳法) 解决问题一般分为三个步骤：

1. **归纳奠基** 证明 $n = 1$ 时，定理成立。
2. **归纳假设** 假设 $n = k$ 时定理成立。
3. **归纳递推** 由归纳假设推出 $n = k + 1$ 时定理成立。

从而可以判断定理成立。

需要注意的是，虽然“数学归纳法”中有“归纳”二字，但并非数学归纳法是有漏洞的归纳推理法，实际上，数学归纳法是严谨的 (附录 A 中有数学归纳法正确性的证明)，数学归纳法属于严谨的**演绎推理法**。

组合数学解决问题的一般步骤

1. 建立数学模型;
2. 研究模型;

¹在本文的教科书中，作者默认读者掌握了数学归纳法，因此我查阅了《数据结构与算法分析——C++ 语言描述 (第四版)》 (Data Structures and Algorithm Analysis in C++ Fourth Edition), 「美」马克·艾伦·韦斯 (Mark Allen Weiss) 著，冯舜玺翻译)，以及百度百科和维基百科关于数学归纳法的词条。

3. 计算若干小案例，树立信心，洞察一切；
4. 运用详细的推理和巧思最终找到问题的答案。

2 排列和组合

2.1 四个基本计数原理

划分 设 S 是集合，集合 S 的一个**划分** (*partition*) 满足下面条件的 S 的子集 S_1, S_2, \dots, S_n 的集合。即使得 S 的每一个元素恰好只属于这些子集中的一个子集：

$$S = S_1 \cup S_2 \cup \dots \cup S_m$$

$$S_i \cap S_j = \emptyset (i \neq j)$$

注意：划分可以是空的。集合 S 的**对象数目**记作 $|S|$

2.1.1 加法原理

设集合 S 被划分成两两不相交的部分 S_1, S_2, \dots, S_n 。则集合 S 的对象数目可以通过确定它的每一个部分的对象数目并且如此相加而得到：

$$|S| = |S_1| + |S_2| + \dots + |S_n|$$

运用加法原理的技巧是把集合 S 划分成少量的易处理部分。

用**选择的术语**对加法原理的描述如下：如果有 p 种方法能够从一个堆中选出一个物体，又有 q 种方法从另外一堆中选出一个物体，那么从这两堆中选出一个物体有 $p + q$ 种方法。

2.1.2 乘法原理

令 S 是对象的有序对 (a, b) 的集合，其中第一个对象 a 来自大小为 p 的一个集合，而对于对象 a 的每个选择，对象 b 有 q 种选择。于是， S 的大小为 $p \times q$ ：

$$|S| = p \times q$$

实际上，乘法原理是加法原理的一个推论。（此结论证明详见附录 A）

乘法原理的第二种实用形式 如果一个任务有 p 种结果，而不论这项任务的结果，另一项任务都有 q 种结果，那么，这两项任务连续执行就有 $p \times q$ 种结果。

乘法原理的推广 实际上乘法原理可以推广到任意有限多个集合的情形。

在乘法原理中，对象 b 的 q 种选择可以随着 a 的选择而变化。唯一的要求是，选择的个数应是相同的 q 个，而不必是相同的选择。

2.1.3 减法原理

令 A 是一个集合, U 是包含 A 的一个更大的集合。设

$$\overline{A} = U \setminus A = \complement_U A = \{x \in U \mid x \notin A\}$$

是 A 在 U 中的补。那么 A 中的对象数目由下列法则给出:

$$|A| = |U| - |\complement_U A|$$

2

2.1.4 除法原理

令 S 是一个有限集合, 把它划分成 k 个部分, 使得每一部分包含的对象数目相同, 于是, 此划分中的部分的数目又下列公式给出:

$$k = \frac{|S|}{\text{在一个部分中的对象数目}}$$

多重集合

在考虑下一小节的内容前, 我们需要先了解**多重集合** (*multiset*)。多重集合中, 除了其元素不必不同外, 其余与集合别无二致。

因此, 多重集合没有所谓“互异性”。我们要表示一个由一个 1, 两个 2, 两个 3 的多重集合时, 应该写成 $\{1 \cdot 1, 2 \cdot 2, 2 \cdot 3\}$ ³。其中各元素的计量数被称为**重复数**, 重复数也可以是无穷大的。

我们再来讨论一些一般的想法。很多计数问题都可以归类为下面的类型之一:

1. 计数对象的**有序**排列的个数或对象的**有序**选择的个数

- (a) 任何对象都不能重复;
- (b) 允许对象重复 (但可能是有限制的)。

2. 计数对象的**无序**排列数目或者对象的**无序**选择个数

- (a) 任何对象都不能重复
- (b) 允许对象重复 (但可能是有限制的)。

有时候, 不区分对象是否重复, 而区分是从集合或者多重集合中进行选择也许会更方便。在 (1) 中的考虑到顺序的放置或选择, 我们称之为**排列** (*permutation*); 而 (2) 中与顺序无关的放置或者选择, 我们称之为**组合** (*combination*)。

2.2 集合的排列

令 r 是正整数。说到一个 n 元素集合的 r **排列**, 我们理解为 n 个元素中的 r 个元素的**有序**放置。我们用 $P(n, r)$ ⁴ (或者标准的 A_n^r) 表示 n 元素集合的 r 排列数目。 n 元素集合 S 的 n 排列可以简单的说成 S 的排列或者 n 个元素的排列。

² 此处定义中, 连等号的前三项是补集的三种表示方式, 对补集的详细解释详见附录 A

³ 多重集合也可以用集合 (传统的集合) 表示, 如多重集合 $\{1, 2, 2, 3, 3\}$ 用传统集合 (点集) 表示成 $\{(1, 1), (2, 2), (3, 2)\}$ 。

⁴ 书上如是写。

2.2.1 集合的排列公式

对于正整数 n 和 $r, r \leq n$ 有

$$P(n, r) = A_n^r = n \times (n-1) \times (n-2) \times \cdots \times (n-r+1)$$

5

阶乘 对于非负整数 n 我们定义 $n!$ (读做 n 的阶乘) 如下:

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1$$

并且约定: $0! = 1$ 。因此, 原公式可以写成如下漂亮的形式:

$$P(n, r) = A_n^r = \frac{n!}{(n-r)!}$$

由此可知, n 元素的排列数目为 $n!$

上面讨论过的排列, 更恰当的应该被称为**线性排列** (*linear permutation*), 就像把对象排成一条线。考虑把对象排成一个圆, 那么排列 $\{1, 2, 3\}$ 就等价于 $\{3, 1, 2\}$, 排列的数目就会相应减少。(如图)

1

2

3

这种排列, 我们称之为**循环排列**。

2.2.2 循环排列公式

n 元素集合的循环 r 排列的数目是

$$\frac{A_n^r}{r} = \frac{n!}{r \cdot (n-r)!}$$

6

我们来看一下计数循环排列的另一种方法。假设要计算 A, B, C, D, E, F 的循环排列数目 (想象要给他们在一张圆桌上安排座位), 我们可以令其中一人 (例如 A) 处在一个固定的位置 (可以称之为“桌头”)。这样的话, 上述的循环排列就相当于 B, C, D, E, F 的线性排列, 即为 $5!$ 。在讨论一些不能用上述公式解决的循环排列问题时, 这种思路很有用。

2.3 集合的组合 (子集)

设 S 是一个 n 元素集合。集合 S 的一个组合通常表示集合 S 的一个无序选择。实际上组合和子集在本质上是可互换的。通常我们使用方便的子集 (*subset*) 而不是组合 (*combination*)⁷, 除非要强调选择的过程。我们用

$$\binom{n}{r} = C_n^r = C(n, r) = {}_n C_r$$

⁵该公式可用乘法原理证明, 详见附录 A

⁶证明过程详见附录 A

⁷汉语看起来差不多。

表示 n 元素集合的 r 子集数目。

现在设 r 是一个非负整数。提到 n 元素集合的一个 r 组合，实际上是指 n 元素集合的一个 r 子集。

2.3.1 集合的组合公式

对于 $0 \leq r \leq n$, 有

$$A_n^r = r!C_n^r$$

所以

$$C_n^r = \frac{A_n^r}{r!} = \frac{n!}{r!(n-r)!}$$

8

2.3.2 集合组合公式的推论

对于 $0 \leq r \leq n$, 有

$$C_n^r = C_n^{(n-r)}$$

这一推论可以直接由公式导出 (r 带入 $n-r$)。

2.3.3 组合的性质一: 帕斯卡公式

对于所有满足 $1 \leq k \leq n-1$ 的整数 n 和 k , 有

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$$

要验证这个式子可以把这些值带入组合公式。还可以用**组合推理证明** (*combinatorial proof*) 加以证明

组合推理证明 设 S 是 n 元素集合。我们指定 S 中的一个元素 x 。设 $S \setminus \{x\}$ 是 S 中除去 x 后得到的集合。把 S 的 k 子集的集合 X 划分成两个部分 A, B 。在 A 中放入不包含 x 的所有 k 子集, 在 B 中放入包含 x 的 k 子集。 X 的大小是 $|X| = C_n^k$ 因此, 根据加法原理有

$$C_n^k = |A| + |B|$$

A 中的 k 子集正好是集合 $S \setminus \{x\}$ 的 $n-1$ 个元素的 k 子集, 因此, A 的大小是

$$|A| = C_{n-1}^k$$

而 B 中的 k 子集可以通过把元素 x 加到 $S \setminus \{x\}$ 的 $k-1$ 子集中得到, 所以 B 的大小是

$$|B| = C_{n-1}^{k-1}$$

把上面两个公式合起来, 得到

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$$

⁸证明详见附录 A

2.3.4 组合的性质二

对于 $n \geq 0$ 有：

$$\sum_{i=0}^n C_n^i = 2^n$$

且这个共同值等于 n 元素的子集数量。

证明 S 的每个子集是相对于 $r = 0, 1, \dots, n$ 的 r 子集。根据加法原理得

$$S \text{ 的子集数量} = \sum_{i=0}^n C_n^i$$

我们还可以这样计数 S 的子集。把一个子集的选择分解成 n 项任务：设 S 的元素是 x_1, x_2, \dots, x_n 。在选择 S 的一个子集的过程中，对于 S 中的 n 个元素中的每一个元素，都要作两种选择：或者进入这个子集，或者不进入。根据乘法原理， S 的子集共有 2^n 种。

$$\sum_{i=0}^n C_n^i = 2^n$$

上述证明过程说明我们可以通过两种不同的方式计数一个子集的对象，在组合数学中，这被称为“双计数”技术。

2.4 多重集合的排列

我们首先计算的是每个元素都有无限重复数的多重集合的排列。

2.4.1 无限重复数的多重集合排列

设 S 是有 k 种不同对象的多重集合，并且每种对象的重复数都是无限的。那么 S 的 r 排列数目就是 k^r 。

这个定理的另一种描述是： k 个不同对象（每一个对象的供给都是无穷的）的 r 排列数量等于 k^r 。我们注意到，当 S 的 k 种不同对象的重复数都至少为 r 时，定理也成立。⁹

2.4.2 有限重复数的多重集合的排列

设 S 是有 k 种不同对象的多重集合，并且对象 a_i 的重复数为 n_i , $i = 1, 2, \dots, k$, $|S| = n = \sum_{j=1}^k n_j$ 则 S 的排列数为

$$\frac{n!}{\prod_{i=1}^k n_i!}$$

2.4.3 只有两类对象的多重集合的排列

如果多重集合 S 只有两种类型的对象 a_1, a_2 ，且他们的重复数为 n_1, n_2 ，其中 $n = n_1 + n_2$ ，那么按照 2.4.2 的定理， S 的排列数为

$$\frac{n!}{n_1!n_2!} = \frac{n!}{n!(n-n_1)!} = C_n^{n_1}$$

⁹证明详见附录 A

即等于 n 的 n_1 子集数量。换言之，我们可以把 $C_n^{n_1}$ 看作 n 对象集合的 n_1 子集数量，也可以看作一个有两个类型对象且重复数分别为 n_1 和 $n - n_1$ 的多重集合的排列个数。

2.4.2 的定理中出现的数 $\frac{n!}{\prod_{i=1}^k n_i!}$ 还有另外一种解释：把一个对象集合划分成指定大小的各个部分其中这些部分都有指定的**标签**。例如集合 $\{a, b, c, d\}$ 的 2 子集划分，如果划分没有标签，那么一共有三种不同的划分。（例如 $\{a, b\}, \{c, d\}$ ）但如果给这些部分做上标签，那么划分数会增加到 6 个（例如有红蓝两种盒子，对于上例，有红盒 $\{a, b\}$ ，蓝盒 $\{c, d\}$ ；蓝盒 $\{a, b\}$ 红盒 $\{c, d\}$ ）。

在一般情形下，我们可以用 B_1, B_2, \dots, B_k 标记这些部分，并把这些部分想象成一些盒子。这时，下面的定理成立。

2.4.4 带标签的盒子

设 n 是正整数，并设 n_1, n_2, \dots, n_k 是正整数且 $n = n_1 + n_2 + \dots + n_k$ 把 n 对象的集合划分成 k 个带有标签的盒子，且第 i 个盒子含有 $n_i (i = 1, 2, \dots, k)$ 个对象。这样划分的方法数等于：

$$\frac{n!}{\prod_{i=1}^k n_i!}$$

如果这些盒子没有标签，且 $n_1 = n_2 = \dots = n_k$ ，那么划分数等于

$$\frac{n!}{k! \prod_{i=1}^k n_i!}$$

现在我们来考虑一个例子，这个例子涉及国际象棋的一些知识，国际象棋中的棋子“车”，对其同行同列的其他棋子具有攻击性，数学地说，假设有一 8×8 的国际象棋棋盘，棋盘上的方格用有序数对 (i, j) 描述，其中 i 是行， j 是列。所以，我们说一个“车”是“非攻击性的车”当且仅当该车所在行和列上没有其他棋子。

假设我们的“车”彼此之间没有区别。我们可以先假设这些车都按一行排开（即 i 按 1 8 递增），这时只考虑其他棋子，可得使他们都是非攻击性车的方法数为 $8!$ （集合 $\{1, 2, \dots, 8\}$ 的排列数）。

当我们考虑“车”之间的区别时，假设车之间的颜色都不同，即有 8 种颜色。我们还要考虑在每个方格中放入的是什么（颜色的）车，因此要在上面的方法数的基础上乘以 $8!$ 。

现在假设 8 个有颜色的车，其中有的车颜色相同，有的不同。例如，假设有红 (R) 车 1 个，蓝 (B) 车 3 个，黄 (Y) 车 4 个。现在从 1 到 8 行观察，看到的是多重集合 $\{1 \cdot R, 3 \cdot B, 4 \cdot Y\}$ 的一个排列。即

$$\frac{8!}{1!3!4!}$$

因此根据乘法原理，可得

$$8! \frac{8!}{1!3!4!}$$

这个例子具有相当的普遍性，可以总结出下列结论。

2.4.5 非攻击性车

有 k 种颜色共 n 个车，第 i 种颜色有 $n_i (i = 1, 2, \dots, k)$ 个。把这些车放置在一个 $n \times n$ 的棋盘使得车都成为非攻击性车的方法数等于

$$\frac{(n!)^2}{\prod_{i=1}^k n_i!}$$

特殊情况：当这些车都有不同的颜色，那么上述公式给出的答案是 $(n!)^2$ ；如果这些车的颜色都相同，那么上述公式给出的答案是 $n!$

2.5 多重集合的组合

如果 S 是多重集合, 那么 S 的 r 组合是 S 中的 r 个对象的无序选择。因此, 多重集合 S 的一个 r 组合本身也是一个多重集合, 更简单来说是一个多重子集。与集合的组合不同, 我们通常称多重集合的组合为组合, 而不是多重子集。

2.5.1 无限重复数的多重集合的组合

设 S 是有 k 种类型对象的多重集合, 每种元素的重复数均为无限, 那么 S 的 r 组合的个数是:

$$C_{r+k-1}^r = C_{r+k-1}^{k-1}$$

证明 设 S 的 k 种类型对象是 $a_i (i = 1, 2, \dots, k)$, 使得

$$S = \{\infty \cdot a_i\} (i = 1, 2, \dots, k)$$

S 的任意组合均呈 $\{x_i \cdot a_i\} (i = 1, 2, \dots, k)$ 的形式, 其中 x_i 皆为非负整数, 且 $r = \sum_{i=1}^k x_i$ 。反过来, 每个满足 $r = \sum_{i=1}^k x_i$ 的非负整数序列 x_1, x_2, \dots, x_k 对应于 S 的一个组合, 因此 S 的 r 组合的个数等于方程

$$r = \sum_{i=1}^k x_i$$

的解的个数, 其中 x_i 皆为非负整数。我们证明, 这些解的个数等于有两种不同类型对象且有 $r + k - 1$ 个对象的多重集合

$$T = \{r \cdot 1, (k-1) \cdot *\}$$

¹⁰ 的排列的个数。给定 T 的一个排列, $k-1$ 个 $*$ 把 r 个 1 分成 k 组。第一个 $*$ 左边有 x_1 个 1, 第一个和第二个 $*$ 之间有 x_2 个 $*$, \dots , 最后一个 $*$ 的右边有 x_k 个 1。于是 x_1, x_2, \dots, x_k 是满足和为 r 的非负整数。反之, 给定非负整数 $x_i (i = 1, 2, \dots, k)$, 满足和为 r , 我们可以倒推以构造一个 T 的排列。于是, 多重集合 S 的 r 组合的个数等于多重集合 T 的排列的个数。所以

$$\frac{(r+k-1)!}{r!(k-1)!} = C_{r+k-1}^r$$

2.5.1 定理在对象的重复数都至少为 r 时, 定理依然成立。

上述证明过程的思考 在上述证明过程中, 我们定义了有 k 种不同类型对象的多重集合 S 的 r 组合与下面的方程的非负整数解有一一对应的关系

$$x_1 + x_2 + \dots + x_k = r$$

在这一对应中, x_i 代表 r 组合中第 i 类型对象的个数。可以通过对 x_i 的限制来实现对每种类型对象在 r 组合中出现的限制。考虑下面一个例子

¹⁰这种方法被称为“隔板法”。

例子 设 S 是有 4 种类型对象的多重集合 $\{10 \cdot a, 10 \cdot b, 10 \cdot c, 10 \cdot d\}$ 。每一种类型对象至少出现一次的 S 的 10 组合的个数是多少？

本题的答案时下面的方程的正整数解的个数

$$x_1 + x_2 + x_3 + x_4 = 10$$

因为重复数和要计数的组合的长度，因此可以忽略 S 的重复数。进行变量代换

$$y_1 = x_1 - 1, y_2 = x_2 - 1, y_3 = x_3 - 1, y_4 = x_4 - 1$$

则方程变为

$$y_1 + y_2 + y_3 + y_4 = 6$$

其中 y_i 是非负整数，根据定理 2.5.1, 新方程的非负整数解的个数等于

$$C_{6+4-1}^6 = 84$$

组合中每种类型对象出现次数的下界 也可以通过变量替换来处理。对此，我们给出下面的例子以说明。

例子 下面的方程

$$x_1 + x_2 + x_3 + x_4 = 20$$

的整数解的个数是多少？其中

$$x_1 \geq 3, x_2 \geq 1, x_3 \geq 0, x_4 \geq 5$$

引入新变量

$$y_1 = x_1 - 3, y_2 = x_2 - 1, y_3 = x_3 - 0, y_4 = x_4 - 5$$

此时方程变为

$$y_1 + y_2 + y_3 + y_4 = 11$$

诸 x_i 的下界能够得到满足当且仅当这些 y_i 非负。新方程的非负整数解的个数也是原来方程的（非负）¹¹整数解的个数，等于

$$C_{11+4-1}^{11} = 364$$

有限重复数的多重集合的组合 设 S 是有 k 种不同对象的的多重集合，其中对象 a_i 的重复数为 $n_i (i = 1, 2, \dots, k)$ 。 S 的 r 组合数量与下面的方程的整数解的个数相同：

$$x_1 + x_2 + \dots + x_k = r$$

其中

$$0 \leq x_1 \leq n_1, 0 \leq x_2 \leq n_2, \dots, 0 \leq x_k \leq n_k$$

现在我们有诸 x_i 的上界，但它们的处理方法与下界的处理方法不同，我们将在了解容斥原理后再解决这个问题。

¹¹题目中给出的限定条件已经确定解一定为非负整数

2.6 有限概率

有限概率的背景是这样的，有一个实验 ϵ ，在进行这个实验时，它产生的结果是某有限结果集合中的一个。假设每一个结果都是**等可能的** (*equallylikely*) (即没有哪一个结果比其他结果更有可能出现。) 这时我们说这个实验是**随机的** (*randomly*)。所有可能结果的集合被称为这个实验的**样本空间** (*sample space*)，并把它记作 S 。因此， S 是一个有限集合，比如说有下面 n 个元素的集合：

$$S = \{s_1, s_2, \dots, s_n\}$$

当我们进行实验 ϵ 时，每有一个 s_i 都有 n 分之一的出现机会，所以说结果 s_i 的概率是 $1/n$ ，写作

$$Prob(s_i) = 1/n (i = 1, 2, \dots, n)$$

一个**事件** (*event*) 就是样本空间的一个子集 E ，但是我们通常是用描述式的语言给出这个 E 。

概率 在样本空间为 S 的实验中，事件 E 的**概率** (*probability*) 定义为 S 中属于 E 的结果的比率，因此，

$$Prob(E) = \frac{|E|}{|S|}$$

根据定义，事件 E 满足

$$0 \leq Prob(E) \leq 1$$

其中，当 $Prob(E) = 0$ 当且仅当 E 是一个空事件 \emptyset (即不可能事件)，而 $Prob(E) = 1$ 当且仅当 E 是整个样本空间 E (即肯定出现的事件)。

3 鸽巢原理

4 附录 A

4.1 数学归纳法正确性的证明

¹² 实际上，数学归纳法一般被认为是自然数的一种公理。

皮亚诺公理 (自然数公理) 是意大利数学家朱塞佩·皮亚诺 (*Giuseppe Peano*) 提出的关于自然数的五条公理系统。根据这五条公理可以建立起一**阶算术系统**，也称皮亚诺算术系统。基本内容：

1. 0 是自然数；
2. 每一个确定的自然数 a ，都有一个确定的后继数 a' ($a' = a + 1$)， a' 也是自然数；
3. 对于每一个自然数 b, c ， $b = c$ 当且仅当 $b' = c'$ ；
4. 0 不是任何自然数的后继数；
5. 任意关于自然数的命题，如果证明它对自然数 0 为真，且假定它对自然数 a 为真时，可以证明对 a' 也为真。那么，命题对所有自然数都为真。

¹² 本小节参考了百度百科和维基百科数学归纳法词条、皮亚诺公理词条、朱塞佩·皮亚诺词条

数学归纳法的正确性也可以在另一些公理的基础上予以证明。比如“最小自然数原理”(每个非空的正整数集合都有一个最小的元素)

假设定理 $K(n)$ 完成了上述前两步骤, 即证明了 $n = 1$ 和 $n = k$ 时 K 为真。假设存在不成立的自然数所构成的集合 S , 其中必定有一个最小的元素 i , 因为 $1 \notin S$, 那么 $i > 1$

因为 i 是集合 S 中的最小元素, 因此 $i - 1 \notin S$, 也就是说 $K(i - 1)$ 是成立的, 那么 $K(i)$ 也应该成立。这与假设出现了矛盾。

由此可证数学归纳法的正确性。

4.2 排列与组合

4.2.1 结论“乘法原理是加法原理的推论”的证明

设 $a_1, a_2, a_3, \dots, a_p$ 是对象 a 的 p 个不同选择。我们把 S 划分成部分 S_1, S_2, \dots, S_p , 其中 S_i 是 S 中第一个对象 $a_i (i = 1, 2, \dots, p)$ 的有序对的集合。每个 S_i 的大小为 q , 根据加法原理有

$$|S| = |S_1| + |S_2| + \dots + |S_p| = q + q + \dots + q (p \text{ 个 } q) = p \times q$$

上述推倒过程中运用到了整数的乘法就是重复的加法这样的基本事实。

4.2.2 补集

¹³ 在集合论和数学的其他分支中, 存在补集的两种定义: **相对补集**和**绝对补集**。

相对补集 若 A 和 B 是集合, 则 A 在 B 中的相对补集是所有属于 B 但不属于 A 的元素的集合。记为 $B \setminus A$ 或者 $B - A$ 或者 $\mathbb{C}_B A$

绝对补集 若给定全集 U , 则 A 的绝对补集是 A 在 U 中的相对补集, 记为 A^C 或者 $\mathbb{C}_U A$

4.2.3 2.2.1 排列公式的证明

在构建 n 元素集合的 r 排列时, 我们可以用 n 种方法选择第一项, 不论第一项如何选择, 都可以用 $n - 1$ 种方法选择第二项, \dots , 不论前 $r - 1$ 项如何选出, 都可以用 $n - (r - 1)$ 种方法选择第 r 项。根据乘法原理, 这 r 项可以用 $n \times (n - 1) \times \dots \times (n - r + 1)$ 种方法选出。

4.2.4 2.2.2 循环排列公式的证明

能够把线性 r 排列的集合划分成若干个部分, 使得两个线性 r 排列对应于同一个循环 r 排列当且仅当这两个线性 r 排列在同一部分中。因此, 循环 r 排列的数目就等于划分的部分的数目。由于每一个部分都含有 r 个线性 r 排列, 因此部分数目是

$$\frac{A_n^r}{r} = \frac{n!}{r \cdot (n - r)!}$$

¹³ 本小节参考了维基百科的“补集”词条

4.2.5 2.3.1 集合的组合公式的证明

令 S 是一个 n 元素集合。 S 的每一个 r 排列都恰由下面两个任务的执行结果产生：

1. 从 S 中选出 r 个对象；
2. 以某种顺序摆放选出的 r 个对象

执行第一个任务的方法数目是 C_n^r ，执行第二个任务的方法数是 $A_r^r = r!$ ，根据乘法原理，我们有

$$A_n^r = r!C_n^r$$

又因为 $A_n^r = \frac{n!}{(n-r)!}$ ，所以

$$C_n^r = \frac{A_n^r}{r!} = \frac{n!}{r!(n-r)!}$$

4.2.6 2.4.1 无限重复数的多重集合的排列公式的证明

在构造 S 的 r 排列的过程中，我们可以把第一项选择为 k 个类型中任意类型的一个对象。类似的，第二项、第三项。因为 S 的对象拥有无限的重复数（或者是足够的重复数）。任意一项的选择的数量都是 k ，不依赖与其他选择，根据乘法原理，可以有 k^r 种选择方法。

4.2.7 2.4.2 有限重复数的多重集合的排列公式证明

设 S 是有 k 种不同对象的多重集合，并且对象 a_i 的重复数为 n_i ， $i = 1, 2, \dots, k$ ， $|S| = n = \sum_{j=1}^k n_j$ 。我们想要这 n 个对象的排列数量。可以这样考虑：一共有 n 个位置，我们想要在每一个位置放置 S 中的一个对象。首先，我们确定放置 a_1 的位置，因为在 S 中， a_1 的数量是 n_1 ，因此必须从 n 个位置中选出 n_1 个位置的子集。这样的方法数是 $C_n^{n_1}$ ，下一步，要放置 a_2 ，此时还剩下 $n - n_1$ 个位置，这样做的方法数是 $C_{n-n_1}^{n_2}$ 以此类推，根据乘法原理，我们发现 S 的排列个数是：

$$C_n^{n_1} C_{n-n_1}^{n_2} \cdots C_{n-n_1-n_2-\cdots-n_{k-1}}^{n_k}$$

化简得

$$\frac{n!}{\prod_{i=1}^k n_i!}$$

4.3 其他

4.3.1 算术基本定理

¹⁴ 在计算例题：

确定下面这个数

$$3^4 \times 5^2 \times 11^7 \times 13^8$$

的正整数因子的个数。

时用到。

¹⁴ 本小节参考了维基百科的“基本算术定理”词条

算术基本定理 又名**正整数唯一分解定理**。每个大于 1 的自然数，要么本身就是质数，要么可以写为 2 个或以上的质数的积，而且这些质因子按大小排列之后，写法仅有一种方式。

$$\forall A \in N, A > 1 \exists \prod_{i=1}^n p_i^{a_i} = A \text{ 其中 } p_1 < p_2 < p_3 < \cdots < p_n \text{ 而且 } p_i \text{ 是一个质数 } a_i \in Z^+$$

因此，例题的因子总数是

$$5 \times 3 \times 8 \times 9 = 1080$$

。