

# 容斥原理

[longhuan@sjtu.edu.cn](mailto:longhuan@sjtu.edu.cn)

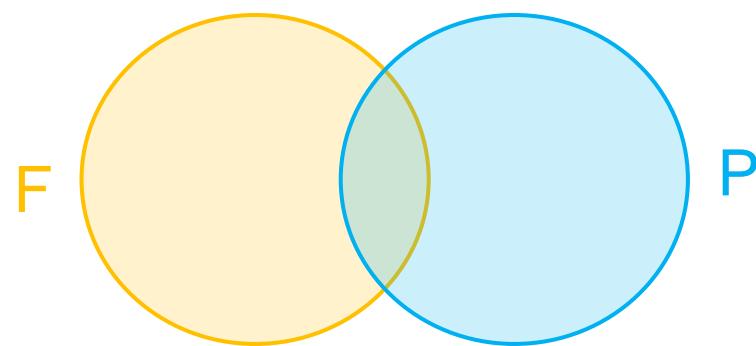


“One of the most useful principles of enumeration in discrete probability and combinatorial theory is the celebrated *principle of inclusion–exclusion*. When skillfully applied, this principle has yielded the solution to many a combinatorial problem.”

**Gian-Carlo Rota** (April 27, 1932 – April 18, 1999) was an Italian-born American mathematician and philosopher.

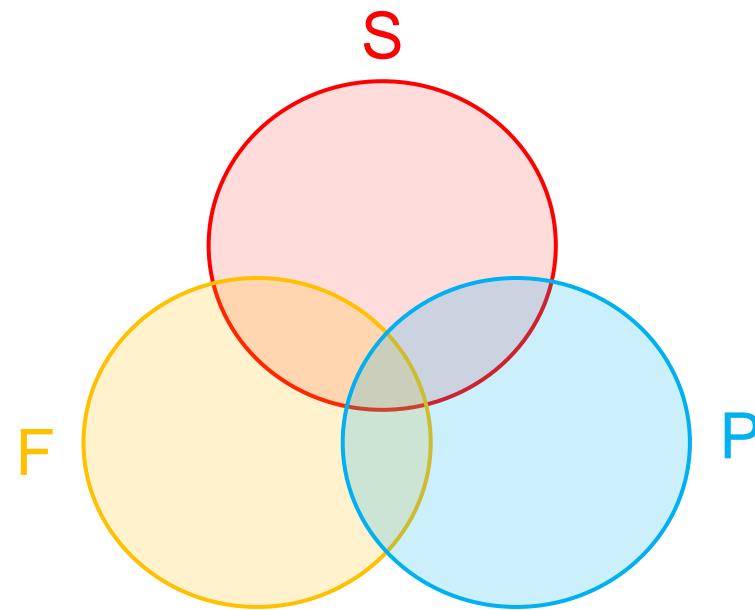
- **问题:** 上海交大计算机某班本学期一共有二门选修课（形式化方法F，概率学P），所有学生都选了至少一门选修课。已知有25个学生选了形式化方法，有28个学生选了概率学。有7个学生选了形式化方法和概率。

问：此班上一共有多少名学生？



$$\begin{aligned}|F \cup P| &= |F| + |P| - |F \cap P| \\&= 25 + 28 - 7 \\&= 46\end{aligned}$$

- **问题：**上海交大计算机某班本学期一共有三门选修课（信息安全S，形式化方法F，概率学P），所有学生都选了至少一门选修课。已知有30个学生选了信息安全，有25个学生选了形式化方法，有28个学生选了概率学。有5个学生选了信息安全和形式化方法，有7个学生选了形式化方法和概率，有9个学生选了信息安全和概率。特别地有5个精力特别充沛的学生同时选了这三门选修课。问：此班上一共有多少名学生？



$$\begin{aligned}
 & |S \cup F \cup P| \\
 &= |S| + |F| + |P| - |S \cap F| - |S \cap P| - |F \cap P| + |S \cap F \cap P| \\
 &= 30 + 25 + 28 - 5 - 9 - 7 + 5 = 67.
 \end{aligned}$$

# 容斥原理

- 容斥定理(*Inclusion-exclusion principle*):

对任意有限集合 $A_1, A_2, \dots, A_n$ , 有

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_{k=1}^n (-1)^{k-1} \sum_{I \in \binom{\{1,2,\dots,n\}}{k}} \left| \bigcap_{i \in I} A_i \right| \\ &= \sum_{\emptyset \neq I \subseteq \{1,2,\dots,n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \end{aligned}$$

$$|S \cup F \cup P| = |S| + |F| + |P| - |S \cap F| - |S \cap P| - |F \cap P| + |S \cap F \cap P|$$

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k-1} \sum_{I \in \binom{\{1, 2, \dots, n\}}{k}} \left| \bigcap_{i \in I} A_i \right|$$

- 证明：（数学归纳法）
  - $n = 2$  时定理成立。
  - 假设对任意  $n - 1$  定理成立。
  - 继续证明规模为  $n$  时定理成立，此时：

$$\begin{aligned}
 |\bigcup_{i=1}^n A_i| &= \left| \left( \bigcup_{i=1}^{n-1} A_i \right) \cup A_n \right| \\
 &= \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n| - \left| \left( \bigcup_{i=1}^{n-1} A_i \right) \cap A_n \right| \\
 &= \left| \bigcup_{i=1}^{\textcolor{red}{n-1}} A_i \right| + |A_n| - \left| \bigcup_{i=1}^{\textcolor{red}{n-1}} (A_i \cap A_n) \right| \\
 &= \cdots
 \end{aligned}$$

# 应用一：错排公式

- **错排：** $n$  个有序的元素应有  $n!$  种不同的排列。如若一个排列式的所有的元素都不在原来的位置上，则称这个排列为**错排**。
- **问题：**任给一个  $n$ ，求出  $1, 2, \dots, n$  的错排个数  $D(n)$  共有多少个？

**解：**用  $S_n$  表示所有  $\{1, 2, \dots, n\}$  上的排列。则  $|S_n| = n!$ 。

对  $i = 1, 2, \dots, n$  定义  $A_i = \{\pi \in S_n : \pi(i) = i\}$ 。  
则  $D(n) = n! - |A_1 \cup \dots \cup A_n|$

$$D(n) = n! - |A_1 \cup \dots \cup A_n|$$

$$A_i = \{\pi \in S_n : \pi(i) = i\}$$

- $|A_i| = (n-1)!$
- $i < j, |A_i \cap A_j| = (n-2)!$
- $i_1 < i_2 < \dots < i_k, |A_{i1} \cap A_{i2} \cap \dots \cap A_{ik}| = (n-k)!$
- 根据 **容斥原理**:  $|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^n (-1)^{k-1} \frac{n!}{k!}$
- 故  $D(n) = n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right)$

$$\lim_{n \rightarrow \infty} D(n) = n!/e$$

## 应用二：欧拉函数 $\varphi$

- **欧拉函数 $\varphi$ :** 给定自然数 $n$ , 欧拉函数 $\varphi(n)$  定义为不超过 $n$ 且与 $n$ 互素的自然数的个数  
$$\varphi(n) = |\{m \in \{1, 2, \dots, n\}: \gcd(n, m) = 1\}|.$$
- 问题: 求欧拉函数。
- 例:
  - $\varphi(3) = 2$  (1,2)
  - $\varphi(8) = 4$  (1,3,5,7)
  - $\varphi(12) = 4$  (1,5,7,11)

## 应用二：欧拉函数 $\varphi$

- **欧拉函数 $\varphi$ :** 给定自然数 $n$ , 欧拉函数 $\varphi(n)$  定义为不超过 $n$ 且与 $n$ 互素的自然数的个数  $\varphi(n) = |\{m \in \{1, 2, \dots, n\}: \gcd(n, m) = 1\}|.$
- **问题:** 求欧拉函数。
- **解:** 根据整数分解定理,  $n$ 可被唯一地分解成 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ 。其中  $\alpha_i > 1$ 且 $p_i$ 为素数,  $p_1 < p_2 < \cdots < p_r$ .
  - 如果 $1 \leq m < n$ 且 $m$ 与 $n$ 不互素, 则必存在某个 $1 \leq i \leq r$  有  $p_i | m$ .
  - $1 \leq i \leq r$  令  $A_i = \{m \in \{1, 2, \dots, n\}: p_i | m\}$
  - 则  $\varphi(n) = n - |A_1 \cup A_2 \cup \cdots \cup A_r|$

$$\varphi(n) = n - |A_1 \cup A_2 \cup \dots \cup A_r|$$

$$1 \leq i \leq r \quad A_i = \{m \in \{1, 2, \dots, n\}: p_i|m\}$$

- $|A_i| = \frac{n}{p_i}$
- $i < j \quad |A_i \cap A_j| = \frac{n}{p_i p_j}$

- $i_1 < i_2 < \dots < i_k,$

$$|A_{i1} \cap A_{i2} \cap \dots \cap A_{ik}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}$$

- 根据**容斥原理**并整理化简后，

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$



- 欧拉函数在信息安全领域有重要应用，是第一个公钥密码方案**RSA**的基础。