吴宏锋 邹建成 陈小光◎编著

Xinxi Anquan de
Shuxue Jichu

信息安全的数学基础

北京邮电大学出版社
www.buptpress.com

信息安全的数学基础

吴宏锋　邹建成　陈小光　编著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

《信息安全的数学基础》围绕信息安全相关课程所需的数学基础，介绍组合数学、抽象代数、数论的基本原理和方法。本书的内容包括组合数学基础、群、环、域、整数、同余、数论函数、Legendre 符号、Jacobi 符号等。本书根据信息时代的需要精选内容，抓住主线，整合知识点，简洁且通俗易懂，注重培养学生科学的思维方式。本书各章末尾都附有相当数量的习题，便于教学与自学。

《信息安全的数学基础》可作为信息安全专业、密码学专业、计算机专业的本科生和研究生的教科书，也可以供从事信息安全工作的科研人员参考。

图书在版编目(CIP)数据

信息安全的数学基础 / 吴宏锋，邹建成，陈小光编著. -- 北京 : 北京邮电大学出版社，2016.7
ISBN 978-7-5635-4730-2

Ⅰ. ①信… Ⅱ. ①吴… ②邹… ③陈… Ⅲ. ①信息安全－应用数学 Ⅳ. ①TP309②O29

中国版本图书馆 CIP 数据核字（2016）第 071913 号

书　　名：信息安全的数学基础
著作责任者：吴宏锋　邹建成　陈小光　编著
责任编辑：刘　颖
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京通州皇家印刷厂
开　　本：787 mm×960 mm　1/16
印　　张：5.75
字　　数：121 千字
印　　数：1—2 000 册
版　　次：2016 年 7 月第 1 版　2016 年 7 月第 1 次印刷

ISBN 978-7-5635-4730-2　　定　价：18.00 元

前　言

近年来随着信息技术的迅猛发展，人们对信息安全的需求越来越广泛，各高校也陆续开设了相关的课程，包括密码学、信息安全、编码理论等等。信息安全是一个涉及数学、计算机与信息科学等多个领域的交叉学科，数学在信息安全中骑着核心作用。目前国内已出版了不少信息安全的数学基础等相关方面的书籍。本书旨在为信息安全专业、密码学专业等所需的数学知识提供一个简明而完备的入门教程，使读者了解组合理论、群论、初等数论、域论等方面的基础知识，拓展学生的数学视野，并为进一步学习更专业的知识提供便利。本书在编写过程中力求做到叙述简明，科学严谨，并不假定读者具有很多的数学知识，大学低年级的学生不查看其它书籍资料就能看懂本书。

本书可作为信息安全专业、密码学专业、计算机专业的本科生和研究生的教科书，也可供从事信息安全工作的科研人员参考。

在本书的编写过程中，我们参考了国内外许多相关的书籍，我们将它们一一列在本书最后的参考文献中。本书中很多章节的内容、例题、习题都并非作者原创，而是取材于这些参考文献，在此一并致谢。由于水平有限，书中难免有疏漏和不当之处，敬请读者批评指正。

目　录

第1章 预备知识

本章作为开端，简要回顾一些基础知识。这一章我们介绍集合论的一些基本知识。集合是数学的基本概念之一，但是，值得注意的是集合这一基本概念，没有一个严谨的数学定义，只有一个描述性的说明。但这里介绍的集合论通常称为朴素的集合论，不涉及逻辑学中的悖论，本书中的集合指的是具有一定属性的事物形成的一个集体。我们假设读者已经熟悉集合论的基本概念，如交集、并集、子集、包含、映射以及德·摩根(De Morgan)定律等。进一步的内容参看文献[9]。

1.1 集 合

定义 1.1.1 把人们直观或思维中某些确定的能够区分的对象汇合在一起，使之成为一个整体，这一整体就是**集合**。组成集合的这些对象称为这一集合的**元素**(或简称为**元**)。

没有任何元素的集合称为空集，记作$\varnothing$。

设A是一个集合，a是一个元素。如果a是A的元素，记作$a\in A$，读作a**属于**A。如果a不是A的元素，则记作$a\notin A$，读作a**不属于**A。

定义 1.1.2 如果集合A的每一个元素都是集合B的元素，即若$a\in A$，则$a\in B$，记作$A\subset B$或$B\supset A$，分别读作A包含于B和B包含A。

如果$A\subset B$，则称A为B的子集。如果A是B的子集，但A又不等于B，即B中至少有一个元素不是A的元素，则称A为B的真子集。

定义 1.1.3 给定集合X，称X所有子集构成的集合为集合X的**幂集**，记作$P(X)$。

定义 1.1.4 给定集合X，称X中的元素个数为集合X的**基数**，记为$|X|$。若$|X|=n$，称X为一个n-集合。

若X为一个n-集合，则显然$|P(X)|=2^n$。

定义 1.1.5 设A和B是两个集合，集合

$$\{x\mid x\in A\text{ 或 }x\in B\}$$

称为集合A与B的并集或并，记作$A\cup B$。集合

$$\{x\mid x\in A\text{ 并且 }x\in B\}$$

称为集合A与B的交集或交，记作$A\cap B$。

若$A\cap B=\varnothing$，则称A与B不相交。反之，若$A\cap B\neq\varnothing$，则称A与B有非空交。

定义 1.1.6 集合

$$\{x \mid x \in A \text{ 并且 } x \notin B\}$$

称为集合 A 与 B 的差集，记作 $A-B$ 或 $A \backslash B$。

定理 1.1.1 设 A,B,C 都是集合，则以下等式成立：

(1) $A \cup A=A, A \cap A=A$；

(2) (交换律) $A \cup B=B \cup A, A \cap B=B \cap A$；

(3) (结合律) $(A \cup B) \cup C=A \cup (B \cup C), (A \cap B) \cap C=>A \cap (B \cap C)$；

(4) (分配律) $(A \cap B) \cup C=(A \cup C) \cap (B \cup C), (A \cup B) \cap C=(A \cap C) \cup (B \cap C)$；

(5) (De Morgan 律) $A-(B \cup C)=(A-B) \cap (A-C), A-(B \cap C)=(A-B) \cup (A-C)$。

1.2 集合上的关系

设 X,Y 是任意两个集合。任取 $x \in X, y \in Y$，给定顺序的元素对 (x,y) 称为一个有序对。这时两个有序对 $(x_1,y_1)=(x_2,y_2)$ 当且仅当 $x_1=x_2, y_1=y_2$。全体有序对的集合

$$X \times Y=\{(x,y) \mid x \in X, y \in Y\}$$

称为两个集合 X 和 Y 的笛卡儿积(Cartesion 积)。

当 $|X|=m, |Y|=n$ 时，显然有 $|X \times Y|=m \times n$。

一个从 X 到 Y 的**关系** R，记为 $R: X \to Y$，定义为 $X \times Y$ 的一个子集。若 $|X|=m$, $|Y|=n$，则从 X 到 Y 的关系有 2^{mn} 个。

关系 R 的定义域为 $\{x \in X \mid$ 存在 $y \in Y$ 使得 $(x,y) \in \mathbf{R}\}$，值域为 $\{y \in Y \mid$ 存在 $x \in X$，使得 $(x,y) \in \mathbf{R}\}$。若 $(x,y) \in \mathbf{R}$，则称 x 与 y 有关系 R。对于 $x \in X$，x 的像为 $R(x)=\{y \in Y \mid (x,y) \in \mathbf{R}\}$，故 R 的值域为 $\bigcup_{x \in X} R(x)$。对于 $y \in Y$，y 的原像为 $R^{-1}(y)=\{x \in X \mid (x,y) \in \mathbf{R}\}$. R 的反关系 $R^{-1}: Y \to X$ 定义为 $R^{-1}=\{(y,x) \mid (x,y) \in \mathbf{R}\}$。

例如，实数集合 $\mathbf{R}$ 中的小于顺序“$<$”是 R 上的一个二元关系，空间两直线平行或者不平行也是一个关系。

设 R 是 X 上的一个关系，即一个 X 到 X 的关系，称 R 是自反的，若对任意 $x \in X$, $(x,x) \in \mathbf{R}$；R 是对称的，对 $x,y \in X$，若 $(x,y) \in \mathbf{R}$，则 $(y,x) \in \mathbf{R}$；R 是反对称的，若对 $(x,y) \in \mathbf{R}, (y,x) \in \mathbf{R}$，则有 $x=y$；R 是传递的，对 $x,y,z \in X$，若 $(x,y) \in \mathbf{R}, (y,z) \in \mathbf{R}$，则 $(x,z) \in \mathbf{R}$。

定义 1.2.1 设 R 是集合 X 上的一个关系，若 R 是自反的、对称的和传递的，则称 R 是定义在 X 上的一个等价关系。此时，若 $(x,y) \in \mathbf{R}$，则称 x 等价于 y，记作 $x \sim y$。

显然，“平行”是一个等价关系，“小于关系”则不是等价关系。设 R 为一等价关系，对任意 $x \in X$，则 x 的像 $[x]=\{y \in X \mid (x,y) \in \mathbf{R}\}$ 称为包含元素 x 的等价类。由于 $a \sim a$，有 $a \in \bar{a}$。任意元素 $a' \in \bar{a}$ 都称为类 $\bar{a}$ 的**代表元**。

定义 1.2.2 若 X 的非空子集的集合 $P=\{X_1, \cdots, X_k\}$ 满足 $X=\bigcup_{i=1}^{k} X_i$，且 $X_i \cap X_j=$

$\varnothing$，$i\neq j$，则称 P 是集合 X 的一个**划分**。

非空集合 S 的任一等价关系～确定 S 的一个划分，这是因为 $a\in\bar{a}$，所以 $S=\bigcup_{a\in S}\bar{a}$。若 $\bar{a}\cap\bar{b}\neq\varnothing$ 且 $s\in\bar{a}\cap\bar{b}$，则 $s\in\bar{a}$，$s\in\bar{b}$，于是 $a\sim b$，$\bar{a}=\bar{b}$，即不同的等价类互不相交，因此所有的等价类构成集合 S 的一个划分。

反之，集合 S 的一个划分 $\{S_\lambda\}$ 确定一个等价关系如下：规定 $a\sim b\Leftrightarrow a,b$ 属于同一个 S_λ。

定义 1.2.3 设 f 是从 X 到 Y 的一个关系，若 f 满足 $|f(x)|=1$，$\forall x\in X$，则称 f 是从 X 到 Y 的一个**映射**。对于函数 f，若对 $x_1\neq x_2\in X$ 有 $f(x_1)\neq f(x_2)$，则称 f 为**单射**，若对于任意 $Y\in Y$ 都有 $f^{-1}(y)\neq\varnothing$，则称 f 为**满射**。

X 到 X 的映射也称为 X 上的一个变换。两个映射相等 $F=G$，是指它们有相同的定义域和值域且 $\forall x\in X,F(x)=G(x)$。

定义 1.2.4 将每个元素 $x\in X$ 映到自身的映射 $i_x:X\to X$ 称为单位映射或恒等映射。

定义 1.2.5 设 $f:X\to Y,g:Y\to X$ 是两个映射，则合成映射 fg 和 gf 是确定的。如果 $fg=i_Y$，那么 f 称为 g 的**左逆**，g 称为 f 的**右逆**。如果 $fg=e_Y$，$gf=i_X$，则称 g 为 f 的一个逆，记作 f^{-1}。

映射有下面的一些属性，读者可自行检验。

性质 1.2.1

(1) f 有左逆当且仅当 f 是单射；

(2) f 有右逆当且仅当 f 是满射；

(3) f 有左逆 g，同时又有右逆 h，则 $g=h$；

(4) f 有逆当且仅当 f 是一个一一映射；

(5) 若 f 有逆，则 f 的逆 f^{-1} 是唯一的，且 $(f^{-1})^{-1}=f$。

若 $|X|=m$，$|Y|=n$，则从 X 到 Y 的映射有 n^m 个。对于映射 f，若 f^{-1} 也是映射，则称 f 为**双射**。显然 f 为双射当且仅当 f 既为单射又为满射。

定理 1.2.1 设 X,Y 为两个基数相同的有限集，f 为 X 到 Y 的一个映射，则 f 为单射当且仅当 f 为满射。

定义 1.2.6 设 X,Y 是两个集合，A 是 X 的一个子集。映射 $f:X\to Y$ 和 $g:A\to Y$ 如果满足条件 $g\subset f$，即对于任意的 $a\in A$ 有 $f(a)=g(a)$，则称 g 是 f 的限制，也称 f 是 g 的一个扩张，记作 $g=f|_A$。

定义 1.2.7 设 $X_1,\cdots,X_n$ 是 $n\geqslant 1$ 个集合，$1\leqslant i\leqslant n$。从笛卡儿积 $X=X_1\times X_2\times\cdots\times X_n$ 到它的第 i 个坐标集 X_i 的投射 $P_i:X\to X_i$ 定义为对每一个 $x=(x_i,x_2,\cdots,x_n)\in X$，$p_i(x)=x_i$。

一个集合的等价关系能产生新的集合。由等价关系与划分之间的一一对应，对应于等价关系～的划分通常记作 $S/\sim$，称为 S 关于～的商集。集合 S 到商集～存在一个自然映射(或典范投影)：

$$p: x \to \bar{x}, x \in S$$

它是一个满射，并且 $p(a)=p(b)$ 当且仅当 $a \sim b$。

设 X, Y 是两个集合，且 $f: X \to Y$ 是一个映射。二元关系 R_f 定义为

$$\forall x_1, x_2 \in X, x_1 R_f x_2 \Leftrightarrow f(x_1)=f(x_2)$$

可检验 R_f 是 X 上的一个等价关系。对任意的 $x \in X$，$\bar{x}=\{x' \mid f(x')=f(x)\}$。规定 $\overline{f}(\bar{x})=f(x)$，则映射 $f: X \to Y$ 诱导一个映射 $\overline{f}: X/R_f \to Y$。映射 $\overline{f}$ 由 $\overline{f}p(x)=f(x)$ 确定，其中 p 是上面的自然映射。

1.3 偏序集合

定义 1.3.1 设 X 是一个非空集合，P 是定义在 X 上的具有自反性、反对称性及传递性的二元关系。则称 $\boldsymbol{P}=(X,P)$ 为一个**偏序集**(poset)。有时在不引起混淆的情况下，也直接称 X 是一个偏序集。符合上述性质的关系称为**偏序关系**。

通常用 $x \leqslant y$ 来描述 X 中的元素 x, y 满足偏序集 (X,P) 中 P 所规定的关系，即 $(x,y) \in P$ 记为 $x \leqslant y$，这样偏序集 (X,P) 也可写成 $(X,\leqslant)$。根据“$\leqslant$”，自然地定义 X 上二元关系“$<$”：$x<y$ 表示 $x \leqslant y$ 且 $x \neq y$。

例 1.3.1 设 $\mathbf{Z}^+$ 为全体正整数组成的集合。对于 $a, b \in \mathbf{Z}^+$，规定 $a \leqslant b$ 当且仅当 $a \mid b$，则易验证 $\mathbf{Z}^+$ 成为一个偏序集。

例 1.3.2 设 S 是一个集合，$P(S)$ 为 S 的幂集，对于 $A, B \in P(S)$，规定 $A \leqslant B$ 当且仅当 $A \subseteq B$，则易验证 $P(S)$ 成为一个偏序集。当 S 是无限集时，令 $P_f(S)$ 表示 S 所有有限子集组成的集合，对于 $A, B \in P_f(S)$，仍如上规定 $A \leqslant B$，则 $P_f(S)$ 也成为一个偏序集。

例 1.3.3 设 V 是域 F 上的一个线性空间，$L(V)$ 为 V 的所有子空间所组成的集合，对于 $U, W \in L(V)$，规定 $U \leqslant W$ 当且仅当 $U \subseteq W$，则易验证 $L(V)$ 成为一个偏序集。当 V 的维数无限时，令 $L_f(V)$ 表示由 V 的所有有限维子空间所组成的集合，对于 $U, W \in L_f(V)$，仍如上规定 $U \leqslant W$，则易见 $L_f(V)$ 也是一个偏序集。

定义 1.3.2 偏序集的**极小元**是一个元素 a，使得没有异于 a 的元素 x 满足 $x \leqslant a$，即若有 $x \leqslant a, x \in X$，则必有 $x=a$。类似地，一个**极大元**是一个元素 b，使得没有异于 b 的元素 y 满足 $b \leqslant y$。

设 A 为偏序集合 S 的一个子集，元素 $a \in S$ 称为 A 的一个下界，如果对于所有的 $a \in A$ 都有 $s \leqslant a$。类似的，元素 $a \in S$ 称为 A 的一个上界，如果对于所有的 $a \in A$ 都有 $a \leqslant s$。如果 A 有一个下界 s 且 $s \in A$，则 s 称为 A 的一个最小元素。如果 A 有一个上界 s 且 $s \in A$，则 s 称为 A 的一个最大元素。注意集合 A 可以没有下界或者有多个下界，同样的，A 可以没有最小(大)元素。但若 A 有最小(大)元素，则它是唯一的。

下面我们叙述两个重要的等价原理：极大原理和 Zorn 引理。

极大原理 设 T 为由集合 S 的若干子集组成的非空集合，T 按包含关系成一个偏序

集合。如果 T 的每个链都有上界，则 T 有一个极大元素。

Zorn 引理 若一个偏序集 S 的每个链都有上界，则 S 有一个极大元素。

极大原理和 Zorn 引理有广泛的应用，它可以简化很多证明，也可以证明一些其他方法不能证明的结果。例如，我们可以证明平面上的任何有界区域 D 内皆有极大的开圆盘，证法如下：令 S 为 D 内所有开圆盘构成的集合，按照包含关系构成一个偏序集合。由于 D 内至少有一个开圆盘，所以 S 是非空的。如果一些开圆盘构成的集合 $\{D_i \mid i \in I\}$ 成为一个链，则 $\bigcup_{i\in I} D_i$ 也是 D 的一个开圆盘，且是此链的一个上界。于是根据 Zorn 引理，有界区域 D 内必有极大的开圆盘。

1.4 排列与组合

这一节我们介绍组合计数的最基本概念，主要取材于参考文献[9]。处理计数问题最基础的原理是加法原理和乘法原理，两者分别对应不同的情形和独立的步骤，是最为基本的想法。

定理 1.4.1 （加法原理）设 $S_1,\cdots,S_m$ 是集合 X 的一个划分，则

$$|X| = |S_1| + \cdots + |S_m|$$

若完成一件事情有 m 个方案，第 $i(i=1,\cdots,m)$ 个方案有 n_i 种方法可以实现，那么完成这件事情共有 $n_1+\cdots+n_m$ 种方法。

定理 1.4.2 （乘法原理）设 $S_1,\cdots,S_m$ 是 m 个有限集，则

$$|S_1 \times S_2 \times \cdots \times S_m| = |S_1| \cdot |S_2| \cdots \cdot |S_m|$$

若完成一件事情需要 m 个步骤，第 $i(i=1,\cdots,m)$ 个步骤有 n_i 种方法可以实现，如果每个步骤中方法的选取均与前面的步骤无关，那么完成这件事情共有 $n_1 \cdot n_2 \cdots n_m$ 种方法。

排列(permutation)与组合(combination)是计数理论中最基本的概念。把集合 $\{a_1, a_2,\cdots,a_n\}$ 中的 n 个元素排成一排，有 $n(n-1)\cdots 2\cdot 1$ 种不同的排法，即 $n!$。每一个这样的排列称为一个 n-排列。而利用此集合中 r 个元素排成的一排，称为这 n 个元素的一个 r-排列. n 个不同元素的 r-排列的个数为 $n(n-1)\cdots(n-(r-1)) = \dfrac{n!}{(n-r)!}$。以上结果可以看作是应用了乘法原理。

集合 $\{a_1,a_2,\cdots,a_n\}$ 中的元素通常默认为互异的。如果排列中允许有相同的元素，例如，把 3 个 A，2 个 B，4 个 C 和 1 个 D 这 10 个字母排成一排，有多少种不同的排法(即有多少个不同的长为 10 的字)？如果把这 10 个字母都看成是不同的，即 3 个 A 看成 A_1，A_2，A_3 等，则有 10! 个字，但这时这 3 个 A 的任一种排列都得到同一个字，其他的字母也是这样，所以最后的答案为 $\dfrac{10!}{3!\ 2!\ 4!\ 1!}$。这种排列称为**有重复元素的排列**。

类似地，由 r 个 C 及 $n-r$ 个 R 可构成 $\dfrac{n!}{r!\ (n-r)!}$ 个长为 n 的字。如果用 C 表示

“选取”，用 R 表示“拒绝”，则上面的问题可改成：“从 n 个不同的物体中选取 r 个的选法数是多少？”每一个这样的选取称为这 n 个元素的一个 r-组合。注意到每一个(无序的)r-组合对应着 $r!$ 个(有序的)r-排列(r-组合有时候也称为 r 个元素的“无序排列”)，所以 n 个元素的 r-组合数等于 $\dfrac{n!}{r!\ (n-r)!}$，记为 $\binom{n}{r}$(读作“n 选取 r”)。因此，一个 n-集合的所有 r-子集个数为 $\binom{n}{r}=\dfrac{n!}{r!\ (n-r)!}$。

现在，有重复元素的排列又可以看作是多重组合。一般地，将 r_1 个 a_1，r_2 个 a_2，…，r_k 个 a_k($r_1+\cdots+r_k=n$)排成一排。这相当于在 n 个位置中选取出 r_1 个位置留给 a_1，再从剩下的 $n-r_1$ 个位置中选取出 r_2 个位置留给 a_2，…，最后的 r_k 个位置留给 a_k。因此，总的排法数为

$$\begin{aligned}&\binom{n}{r_1}\binom{n-r_1}{r_2}\binom{n-r_1-r_2}{r_3}\cdots\binom{n-r_1-\cdots-r_{k-1}}{r_k}\\&=\frac{n!}{r_1!\ (n-r_1)!}\ \frac{(n-r_1)!}{r_2!\ (n-r_1-r_2)!}\cdots\frac{(n-r_1-\cdots-r_{k-1})!}{r_k!\ 0!}\\&=\frac{n!}{r_1!\ r_2!\ \cdots r_k!}\end{aligned}$$

称以上的取法数为**多重选取数或多重组合数**。

通过以上的讨论，可总结出关于排列、组合(即选取)和多重选取(即多重组合，或有重复元素的排列)的计数公式。

定义 1.4.1 (排列)排列数即 $\mathrm{P}(n,r)=n(n-1)\cdot(n-r-1)=\dfrac{n!}{(n-r)!}$，其计数的是在 n 个元素中取出 r 个排成一排的方法数。

定义 1.4.2 (组合或选取)组合数，或称为选取数，即 $\mathrm{C}(n,r)=\mathrm{P}(n,r)/r!=\dfrac{n!}{(n-r)!\ r!}=\binom{n}{r}$，读作“$n$ 选取 r”，其计数的是从 n 个元素中选取 r 个的方法数。

一般地，如果 $n<r$，则默认 $\mathrm{P}(n,r)=\mathrm{C}(n,r)=0$。事实上，这样的排列或组合原本就不存在。

定义 1.4.3 (有重复元素的排列或多重选取)关于参数为 $n,r_1,\cdots,r_k$ 的多重选取数即 $\binom{n}{r_1,r_2,\cdots,r_k}=\dfrac{n!}{r_1!\ r_2!\ \cdots r_k!}$，其中要求 $n=\sum_{i=1}^{k}r_i$。

显然，参数为 n,r_1,r_2 的多重选取数即 $\binom{n}{r_1,r_2}=\binom{n}{r_1}=\mathrm{C}(n,r_1)$。

从 n 个不同元素中取出 r 个元素排成一个圆环，称为“环排列”。按某种固定的顺序

(如逆时针)看去,完全相同者被认为是同一个环排列(但 $a-b-c-a$ 和 $a-c-b-a$ 则被认为是不同的)。对固定的 n 个元素,取其中 r 个进行环排列,每一个环排列均对应 r 种不同的"直线排列",且不同环排列展成的直线排列彼此也必不相同。注意到把全部环排列展开所得的直线排列,恰好就是全部的直线排列,因此可得到从 n 个元素中取出 r 个元素组成的环排列个数为 $\frac{n!}{(n-r)!}\cdot\frac{1}{r}$。特别地,将 n 个元素全部取出的环排列个数为 $\frac{n!}{n}=(n-1)!$。

定义 1.4.4 (环排列)从 n 个不同元素中取出 r 个排成一个圆环的方法数是 $\frac{n!}{(n-r)!}\cdot\frac{1}{r}$。

例 1.4.1 8对夫妇坐成一排,每对夫妇要坐在一起,有多少种不同坐法?若在圆桌旁就坐,有多少种不同坐法?

解:8对夫妇排成一排(不考虑每对夫妇如何坐)有 $8!$ 种安排,而每对夫妇有 $2!=2$ 种坐法,所以答案为 $2^8\cdot 8!$。若这8对夫妇坐在一个圆桌旁,此时这8对夫妇排成一个圆排列有 $7!$ 种方法,每对夫妇仍有 $2!=2$ 种坐法,答案为 $2^8\cdot 7!$。

例 1.4.2 4个 C 和8个 R 的排列中没有两个 C 是相邻的,有多少种这样的排列?

解:先把这8个 R 排成一排,这只有一种方式。然后再把4个 C 插入这些 R 的前后及中间这9个位置中。注意条件要求任意两个 C 不能相邻,即等价于这9个位置中每个位置最多插入一个 C。从而答案就是从9个位置中选出4个位置插入 C 的方法数,即 $\binom{9}{4}$。

在某些已排好物体的前后及中间位置上再加入其他物体,这种方法称为"插空法",是一种简单而重要的计数方法。

例 1.4.3 把集合 $\{1,2,\cdots,n\}$ 划分成 b_1 个1元集,b_2 个2元集,$\cdots$,b_k 个 k 元集,其中 $\sum_{i=1}^{k} ib_i=n$,这样的分法有多少种?

解:n 个元素的全排列有 $n!$ 种。而对于每个划分,其中 b_i 个 i 元集是没有顺序的,且划分中每个集合的元素也是没有顺序的,因此每个划分对应 $b_1!\ b_2!\ \cdots b_k!\ (1!)^{b_1}(2!)^{b_2}\cdots(k!)^{b_k}$ 个不同的 n-排列。所以答案为

$$\frac{n!}{b_1!\ b_2!\ \cdots b_k!\ (1!)^{b_1}(2!)^{b_2}\cdots(k!)^{b_k}}$$

或者从多重选取数出发,再考虑到划分得到的 i 元集彼此之间是没有顺序的,则有

$$\frac{\binom{n}{1,\cdots,1,2,\cdots,2,\cdots,k,\cdots,k}}{b_1!\ b_2!\ \cdots b_k!}$$

种分法，这和上面的答案一样。（以上多重选取公式中的 i 有 b_i 个，$1\leqslant i\leqslant k$。）

注：进一步，一个 n 元集的全体划分数为

$$\sum_{b_1+2b_2+\cdots+nb_n=n}\frac{n!}{b_1!b_2!\cdots b_n!(1!)^{b_1}(2!)^{b_2}\cdots(n!)^{b_n}}$$

例 1.4.4 用 p_n 表示随机选取的 n 个人中至少有 2 人生日相同的概率（不考虑闰年的情况），则 n 最小为多少可使得 $p_n>\frac{1}{2}$？

解：容易计算 n 个人中任 2 人生日都不相同的概率为

$$\frac{365\times364\times\cdots\times(365-n+1)}{365^n}$$

故

$$p_n=1-\frac{365!}{(365-n)!\ 365^n}$$

利用 Stirling 公式 $n!\approx n^n\mathrm{e}^{-n}\sqrt{2\pi n}$，有

$$p_n\approx1-\left(\frac{365}{365-n}\right)^{365.5-n}\mathrm{e}^{-n}$$

计算可知，最小的满足条件的 n 是 23。同样可以得到，若 $n\geqslant41$，则 $p_n\geqslant0.9$。

如果允许重复，那么从 n 个不同物体中选取 r 个物体排成一排的方法数当然是 n^r。那么组合数是多少？也就是说，如果 n 个不同物体中的每一个都可以被重复选取任意多次，那么选取一个基数是 r 的多重集有多少种方法？设第 i 个物体被选取了 x_i 次，则此问题等价于求方程

$$x_1+x_2+\cdots x_n=r$$

的非负整数解的个数。这又等价于求包含 r 个“|”和 $n-1$ 个“+”的序列个数（例如，|||+++||+||就表示方程 $x_1+x_2+x_3+x_4=7$ 的一个非负整数解(3,0,2,2)），所以答案是 $\binom{r+n-1}{r}$。

定理 1.4.3 令 S 为具有 n 种类型元素的一个多重集，每种元素均可以被重复选取任意多次，则 S 的 r-组合数为

$$\binom{r+n-1}{r}$$

例 1.4.5 一家面包房生产 8 种面包。如果将一打面包装进盒内，则一共可能有多少种不同的盒装组合？若每盒必定包含所有的 8 种呢？

解：由上述定理，所求结果依次为

$$\binom{12+8-1}{12}=\binom{19}{12}$$

及

$$\binom{4+8-1}{4}=\binom{11}{4}$$

例 1.4.6 方程 $x_1+x_2+x_3+x_4=20$ 满足 $x_1\geqslant 3, x_2\geqslant 1, x_3\geqslant -1, x_4\geqslant 0$ 的整数解有多少个?

解:令 $y_1=x_1-3, y_2=x_2-1, y_3=x_3+1, y_4=x_4$,则问题等价于求方程 $y_1+y_2+y_3+y_4=17$ 的非负整数解的个数,故所求解的个数为

$$\binom{17+4-1}{17}=\binom{20}{17}$$

按照前面的约定,关于组合数$\binom{n}{k}$,有

$$\binom{n}{k}=\begin{cases}\dfrac{n!}{k!\ (n-k)!}, & n\geqslant k,\\ 0, & n<k.\end{cases}$$

定理 1.4.4 (二项式定理)设 n 为正整数,则

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$

二项式定理的证明有很多种,可以用归纳法,也可以考虑基本的组合意义,这里就略过了。今后,组合数$\binom{n}{k}$也称为二项式系数。以下性质都是二项式定理显而易见的推论。

性质 1.4.1 设 $n\geqslant k\geqslant 0$,则

$$\binom{n}{k}=\binom{n}{n-k}$$

性质 1.4.2 设 $n\geqslant 0$,则

$$2^n=\sum_{k=0}^{n}\binom{n}{k}$$

性质 1.4.3 设 $n\geqslant 1$,则

$$0=\sum_{k=0}^{n}(-1)^k\binom{n}{k}$$

推论 1.4.1 设 $n\geqslant 1$,则

$$\sum_{k\text{为奇数}}\binom{n}{k}=\sum_{k\text{为偶数}}\binom{n}{k}$$

下面给出推论 1.4.1 的一个组合证明。

证明 设

$$X=\{1,2,\cdots,n\}$$

$$A=\{S\subseteq X\mid |S|\text{为偶数且}\ 1\in S\}$$

$$B=\{S\subseteq X\mid |S|\text{为奇数且}\ 1\in S\}$$

$$C=\{S\subseteq X\mid |S|\text{为偶数且}\ 1\notin S\}$$

$$D=\{S\subseteq X\mid |S|\text{为奇数且}\ 1\notin S\}$$

构造映射 $f:A\to D$ 为 $f(S)=S,\{1\}$，显然 f 为双射，所以 $|A|=|D|$，类似地 $|B|=|C|$，因此

$$\sum_{k\text{为奇数}}\binom{n}{k}=|B|+|D|=|A|+|C|=\sum_{k\text{为偶数}}\binom{n}{k}$$

定理 1.4.5 （多项式定理）设 n 为正整数，则

$$(x_1+x_2+\cdots+x_k)^n=\sum_{n_1+n_2+\cdots+n_k=n}\binom{n}{n_1,n_2,\cdots,n_k}x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$$

其中，

$$\binom{n}{n_1,n_2,\cdots,n_k}=\frac{n!}{n_1!\ n_2!\ \cdots n_k!}$$

即多重选取数，今后也称为多项式系数。

证明：只须考虑 $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$ 在 $(x_1+x_2+\cdots+x_k)^n$ 展开式中的系数，并应用多重选取的定义。

例 1.4.7 确定 $(x_1+x_2+\cdots+x_5)^{10}$ 的展开式中 $x_1^3x_2x_3^4x_5^2$ 的系数。

解：根据多项式定理知，所求系数应为

$$\binom{10}{3,1,4,0,2}=\frac{10!}{3!\ 4!\ 2!}=12\ 600$$

容斥原理又称筛法，是一个古老而简便的工具。它是利用集合之间的交、并运算来对集合内元素计数的方法。例如，假设 A 和 B 是两个有限集合，我们熟知

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

例 1.4.8 某班有 100 人，其中会打篮球的有 45 人，会打乒乓球的有 53 人，会打排球的有 55 人；既会打篮球也会打乒乓球的有 28 人，既会打篮球也会打排球的有 32 人，既会打乒乓球也会打排球的有 35 人；三种球都会打的有 20 人。问三种球都不会打的有多少人？

解：设 $E_1=\{$此班会打篮球的人$\}$，$E_2=\{$此班会打乒乓球的人$\}$，$E_3=\{$此班会打排球

的人}，则由条件知：$|E_1|=45$，$|E_2|=53$，$|E_3|=55$；$|E_1\cap E_2|=28$，$|E_1\cap E_3|=32$，$|E_2\cap E_3|=35$；$|E_1\cap E_2\cap E_3|=20$。

可如下算出三种球都不会打的人数。先从总人数中减掉会打三种球中某一种的人数；此时会打两种球的人被减掉了两次，为得到所求，应加上他们；第二步中会打三种球的人被加了三次，从而应再减一次。易知这样所得结果确是所求，即结果为

$$\begin{aligned}&100-|E_1|-|E_2|-|E_3|+|E_1\cap E_2|+|E_1\cap E_3|+|E_2\cap E_3|-|E_1\cap E_2\cap E_3|\\&=100-45-53-55+28+32+35-20=22\end{aligned}$$

所以三种球都不会打的有22人。

对于此类问题，可借助文氏图(Venn Diagram)来获得直观的解答，也可以选择集合的角度，本题中根据条件得到了7个关于集合的等式后，可设只会打某一种球、只会打某两种球、三种球都会打的人数为7个未知量，由上述等式列出7个线性方程，通过解这个线性方程组求得各部分的人数。但这种方法不具备一般性，无法引出容斥原理的思想。

例1.4.9 求1到500中不能被2和3整除的整数个数。

解：这是熟知的初等问题。答案是

$$500-\left\lfloor\frac{500}{2}\right\rfloor-\left\lfloor\frac{500}{3}\right\rfloor+\left\lfloor\frac{500}{6}\right\rfloor=167$$

定理1.4.6 (经典的容斥原理)设S为一有限集，$P=\{P_i,\cdots,P_m\}$为一族性质。对$\{1,\cdots,m\}$的任一子集I，令X_I表示S中满足性质P_i(对所有$i\in I$)的那些元素构成的集合。特别地，$I=\{i\}$时，简记$X_{\{i\}}$为X_i。记$\overline{X_I}=S,X_I$。则集合S中不具有P中任何一种性质的元素个数由下式给出：

$$\begin{aligned}|\overline{X_1}\cap\overline{X_2}\cap\cdots\cap\overline{X_m}|&=|S|-\sum_i|X_i|+\sum_{i<j}|X_i\cap X_j|-\sum_{i<j<k}|X_i\cap X_j\cap X_k|\\&\quad+\cdots+(-1)^m|X_1\cap X_2\cap\cdots\cap X_m|\\&=\sum_{I\subseteq[m]}(-1)^{|I|}|X_I|\end{aligned}\tag{*}$$

证明：对任意$x\in S$，记集合$[m]=\{1,\cdots,m\}$，$J_x=\{i\in[m]\mid x=X_i\}$。按$J_x$是否为空集讨论：

(i) $J_x=\varnothing$，即x不在任意一个X_i中。此时x对(*)式左端的贡献为1；对于右端，x仅对$|S|$贡献1，对其余和式贡献为0，从而x对右端贡献也为1。故(*)式成立。

(ii) $J_x\neq\varnothing$，即x在某些X_i中。设$j=|J_x|$，则$j>0$。此时x对(*)式左端的贡献为0；对于右端，注意$x\in X_I$等价于$I\subseteq J_x$，从而x对(*)式右端的贡献为

$$\sum_{I\subseteq J_x}(-1)^{|I|}=\sum_{i=0}^{j}(-1)^i\binom{j}{i}=(1-1)^j=0$$

故(*)式成立。

综合(i)和(ii)，定理成立。

容斥原理是一个很有用的计数原则，它的另一表述为，设S是一个n元集，E_1，