离散数学讲义

清华大学数学科学系
艾颖华

目录

第一章　计数问题

什么是离散数学? 维基百科 (Wikipedia) 上说: 离散数学是研究离散的, 而不是连续的数学结构的学问. 如何判断某个数学结构是连续的还是离散的? 如果某数学结构中的量可以连续的变化, 例如取值为实数, 则称该数学结构是连续的; 如果某数学结构中的量只能取有限或可数多个分立的值, 则称该数学结构是离散的. 这样我们可以粗略的说: 研究与实数有关的数学结构的学问称为连续数学, 例如微积分, 几何学, 拓扑学等; 除此之外的学问都可以归类为离散数学.

部分是由于计算机的普及和发展, 在过去几十年中离散数学的研究显著增加, 成长为数学中的重要分支.

1.1　Fubini 定理

设 E, B 是有限集合, $p : E \to B$ 是映射. 对每个元素 $b \in B$, 令

$$F_b = p^{-1}(b) = \{e \in E | p(e) = b\},$$

称为 b 在 p 下的原像集, 则 E 分解为不交并

$$E = \cup_{b \in B} F_b.$$

定理 1.1.1 (离散版本 Fubini 定理)**.** *对任何映射 $f : E \to \mathbf{R}$, 有*

$$\sum_{e \in E} f(e) = \sum_{b \in B} \left(\sum_{e \in F_b} f(e) \right) = \sum_{b \in B} \sum_{e \in E, p(e) = b} f(e).$$

我们也将上述等式称之为按 $p(e)$ 的值分类求和.

设 A, B 是有限集合, 考虑它们的笛卡尔乘积 $A \times B = \{(a, b) | a \in A, b \in B\}$. 设 E 是 $A \times B$ 的子集, 则 E 到 A, B 有自然的投影映射 $p_1 : E \to A$ 与 $p_2 : E \to B$, 分别定义为

$$p_1(a, b) = a, \quad p_2(a, b) = b, \quad \forall (a, b) \in E.$$

利用定理1.1.1, 可得如下的结果, 我们称之为 “换序求和”.

定理 1.1.2 (换序求和)**.** 对任何映射 $f : E \to \mathbf{R}$, 有

$$\sum_{(a,b)\in E} f(a,b) = \sum_{a\in A}\sum_{b\in B,(a,b)\in E} f(a,b) = \sum_{b\in B}\sum_{a\in A,(a,b)\in E} f(a,b).$$

证明: 按照 $p_1 : E \to A$ 的值分类求和, 可得

$$\sum_{(a,b)\in E} f(a,b) = \sum_{a\in A}\sum_{(x,y)\in E,p_1(x,y)=a} f(x,y) = \sum_{a\in A}\sum_{(a,y)\in E} f(a,y) = \sum_{a\in A}\sum_{b\in B,(a,b)\in E} f(a,b).$$

类似的, 按照 $p_2 : E \to B$ 的值分类求和, 可得

$$\sum_{(a,b)\in E} f(a,b) = \sum_{b\in B}\sum_{a\in A,(a,b)\in E} f(a,b).$$

结合这两个等式, 即得到

$$\sum_{a\in A}\sum_{b\in B,(a,b)\in E} f(a,b) = \sum_{b\in B}\sum_{a\in A,(a,b)\in E} f(a,b).$$

□

我们总结一下换序求和的规则: 可交换外层求和 $\sum\limits_{a\in A}$ 与内层求和 $\sum\limits_{b\in B}$ 的次序, 但要保持约束条件 $(a,b) \in E$ 照写, 这样交换求和顺序前后和式的值不变. 换序求和是我们以后经常使用的计算方法.

例 1.1.3. 设 $(a_{ij})_{1\le i\le m,1\le j\le n}$ 是 $m \times n$ 个数, 则有

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}.$$

当 $m = n$ 时, 有

$$\sum_{i<j} a_{ij} = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} a_{ij} = \sum_{j=2}^{n}\sum_{i=1}^{j-1} a_{ij}.$$

1.2 加法原理与乘法原理

假设 S 是有限集合, 则人们可以数 S 包含的元素个数, 用 $|S|$ 或 $\#S$ 表示. 这就引出离散数学的一个分支: 计数组合学.

定理 1.2.1. 设 A, B 是有限集合. 如果存在双射 $f : A \to B$, 则 $|A| = |B|$.

定理 1.2.2 (加法原理)**.** (1) 如果 A 可以分解为若干个互不相交的子集之并 $A = \cup_{i=1}^{k} A_i$, 则 $|A| = \sum_{i=1}^{k} |A_i|$.

(2) 设 A, B 是有限集合, $p : A \to B$ 是映射. 对 $b \in B$, 令 $F_b = p^{-1}(b)$ 为 b 在 p 下的原像集, 则有

$$|A| = \sum_{b \in B} |F_b|,$$

定理 1.2.3 (乘法原理)**.** 如果构造 S 的每个元素 s 都需要 n 步, 第一步有 m_1 种选择; 在第一步完成之后第二步有 m_2 种选择;..., 在前 $k-1$ 步完成之后第 k 步有 m_k 种选择 $(k = 2, \ldots, n)$. 这样, S 的元素个数为 $m_1 m_2 \cdots m_n$.

证明: 将 S 的每个元素等同为 $(x_1, \ldots, x_n)$, 其中 x_i 是构造 s 时第 i 步进行的操作. 定义

$$S_k = \{(x_1, \ldots, x_k) | \text{ 存在} s \in S \text{ 使得} s \text{ 的前} k \text{ 步构造依次为} x_1, \ldots, x_k\},$$

则 $S_n = S$. 定义映射 $p : S_n \to S_{n-1}$ 为

$$p(x_1, \ldots, x_{n-1}, x_n) = (x_1, \ldots, x_{n-1}).$$

条件表明: 对每个 $(x_1, \ldots, x_{n-1}) \in S_{n-1}$, 它在 p 下的原像集 $p^{-1}((x_1, \ldots, x_{n-1}))$ 都是 m_n 元集合. 由此可得

$$|S_n| = \sum_{(x_1, \ldots, x_{n-1}) \in S_{n-1}} \#p^{-1}((x_1, \ldots, x_{n-1})) = \sum_{(x_1, \ldots, x_{n-1}) \in S_{n-1}} m_n = |S_{n-1}| \cdot m_n.$$

□

例 1.2.4. 设要构造长度为 n 个单词, 第 1 个位置上可以选用 k_1 个字母之一; 第 2 个位置上可以选用 k_2 个字母之一;...; 第 n 个位置上可以选用 k_n 个字母之一. 在此规则下, 所能构造出的单词的数目为 $k_1 k_2 \cdots k_n$. 用集合的语言说, 有

$$|S_1 \times S_2 \times \cdots \times S_n| = |S_1| \cdot |S_2| \cdot \cdots \cdot |S_n|.$$

特别的, 由 k 个字母构成的长度为 n 的单词的总数为 k^n, 即 $|S^n| = |S|^n$.

推论 1.2.5. 设 X 是 n 元集合, 则 X 共有 2^n 个不同的子集.

证明: 不妨设 $X = \{1, 2, \ldots, n\} = [n]$, 定义 $\chi : 2^X \to \{0, 1\}^n$ 为

$$\chi(A)_i = \begin{cases} 0, & \text{如果} i \notin A, \\ 1, & \text{如果} i \in A. \end{cases}$$

易验证 χ 是双射, 因而有 $\#2^X = \#\{0, 1\}^n = 2^n$. □

命题 1.2.6. (1) n 个对象的排列的数目为 $n!$.

(2) 设 X 是 n 元集合, 则 X 的有序 k 元子集的数目为 $n(n-1)\cdots(n-k+1)$.

(3) n 元集合 X 的所有 k-元子集的数目为 $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$.

证明: (2) X 的有序 k 元子集构成的集合为

$$S = \{(x_1, \ldots, x_k) | x_i \in X, \text{且对} i \neq j \text{有} x_i \neq x_j\},$$

利用乘法原理即可得 $|S| = n(n-1)\cdots(n-k+1)$.

(3) 令 $T = \{A | A \subseteq X \text{且} |A| = k\}$ 是由 X 的所有 k 元子集所构成的集合. 考虑映射 $f : S \to T$ 为

$$f((x_1, \ldots, x_k)) = \{x_1, \ldots, x_k\}.$$

注意到, 对每个 $A \in T$, 有

$$f^{-1}(T) = \{(x_1, \ldots, x_k) | x_i \in T \text{且对} i \neq j \text{有} x_i \neq x_j\},$$

即 $f^{-1}(T)$ 恰为 T 的全排列所构成的集合. 由 (1) 的结论有 $\#f^{-1}(T) = k!$, 进而有

$$|S| = \sum_{A \in T} \#f^{-1}(T) = \sum_{A \in T} k! = |T| \cdot k!,$$

得到 $|T| = \frac{|S|}{k!} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \binom{n}{k}$.

□

命题 1.2.7. *二项式系数满足如下等式:*

(1) $\binom{n}{k} = \binom{n}{n-k}$.

(2) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

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

(4) $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

证明: (2) 注意到 $\binom{n-1}{k-1} = \frac{k}{n}\binom{n}{k}$, $\binom{n-1}{k} = \frac{n-k}{n}\binom{n}{k}$ 即可.

□

例 1.2.8. (1) $\sum_{i=0}^{k} (-1)^i \binom{n}{i} = (-1)^k \binom{n-1}{k}$.

(2) $\sum_{i=0}^{k} \binom{n+i}{i} = \binom{n+k+1}{k}$.

(3) $\sum_{i} \binom{n}{i}\binom{m}{k-i} = \binom{n+m}{k}$.

(4) $\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$.

证明: (1) 利用 $\binom{n}{i}=\binom{n-1}{i-1}+\binom{n-1}{i}$, 可得

$$\sum_{i=0}^{k}(-1)^i\binom{n}{i}=\sum_{i=0}^{k}(-1)^i\left(\binom{n-1}{i-1}+\binom{n-1}{i}\right)=(-1)^k\binom{n-1}{k}.$$

(2) 利用 $\binom{n+i}{i}=\binom{n+i+1}{i}-\binom{n+i}{i-1}$ 可得

$$\sum_{i=0}^{k}\binom{n+i}{i}=\sum_{i=0}^{k}\left(\binom{n+i+1}{i}-\binom{n+i}{i-1}\right)=\binom{n+k+1}{k}.$$

(3) 注意到

$$\begin{aligned}(1+x)^{n+m}=(1+x)^n\cdot(1+x)^m&=\left(\sum_{i=0}^{n}\binom{n}{i}x^i\right)\cdot\left(\sum_{j=0}^{m}\binom{m}{j}x^j\right)\\&=\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k}\binom{n}{i}\binom{m}{k-i}\right)x^k.\end{aligned}$$

□

例 1.2.9. 把 n 个不同物体分成 k 组, 第 i 组 n_i 个物体 $(1\le i\le k)$, 方法总数为 $\frac{n!}{n_1!n_2!\cdots n_k!}$.

解. 分组方案可以分成 k 步, 第 i 步的操作是: 在前 $i-1$ 步选完后剩下的物体中选择 n_i 个构成第 i 组. 利用乘法原理可得分组方案的总数目为

$$\binom{n}{n_1}\cdot\binom{n-n_1}{n_2}\cdot\cdots\cdot\binom{n-n_1-\cdots-n_{k-1}}{n_k}=\frac{n!}{n_1!n_2!\cdots n_k!}.$$

□

注 1.2.10. 对满足 $n_1+\cdots+n_k=n$ 的非负整数 $n_1,\ldots,n_k$, 记

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

称之为多项式系数 (*multinomial coefficient*), 它等于 $(x_1+\cdots+x_k)^n$ 展开式中 $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$ 项的系数. 它的另一个组合解释是: 用 n_1 个 1,...,n_k 个 k 所能构成的长为 n 的字符串的数目.

命题 1.2.11. *多项式系数满足如下递推关系:*

$$\binom{n}{n_1,n_2,\cdots,n_k}=\binom{n-1}{n_1-1,n_2,\cdots,n_k}+\binom{n-1}{n_1,n_2-1,\cdots,n_k}+\cdots+\binom{n-1}{n_1,n_2,\cdots,n_k-1}.$$

证明: $\binom{n}{n_1,n_2,\cdots,n_k}$ 是在计数映射 $f:[n]\to[k]$ 的数目, 要求 $\#f^{-1}(i)=n_i$. 把 f 按照 $f(n)$ 的值分类, 第 i 类的 f 满足 $f(n)=i$. 这一类的 f 只需确定 $g=f|_{[n-1]}:[n-1]\to[k]$, 它满足

$$\#g^{-1}(j)=\begin{cases} n_j, & \text{如果}j\neq i \\ n_i-1, & \text{如果}j=i \end{cases}$$

这种 g 的数目为 $\binom{n-1}{n_1,\cdots,n_i-1,\cdots,n_k}$. □

例 1.2.12. 给定非负整数 $m_1,m_2,\ldots,m_n$, 满足 $m_1+2m_2+\cdots+nm_n=n$. 把 n 个不同物体分组, 要求恰有 m_1 个 1 元组, m_2 个 2 元组,..., m_n 个 n 元组, 则方法总数为

$$\frac{n!}{m_1!\cdots m_n!(1!)^{m_1}(2!)^{m_2}\cdots(n!)^{m_n}}.$$

证明: 考虑这 n 个物体的带编号的分组, 要求按照编号递增的顺序, 各组的规模分别为

$$\underbrace{1,\ldots,1}_{m_1\text{个}},\underbrace{2,\ldots,2}_{m_2\text{个}},\cdots,\underbrace{n,\ldots,n}_{m_n\text{个}}.$$

记这样的带编号的分组方案的集合为 S, 可将 S 视为由所有映射 $f:[n]\to[m_1+\cdots+m_n]$ 构成的集合

$$S=\{\text{映射}f:[n]\to[m_1+\cdots+m_n]|\#f^{-1}(1)\leq\cdots\leq\#f^{-1}(m_1+\cdots+m_n)\text{且其中有}m_i\text{个值为}i\}.$$

由多重组合数的定义可知

$$|S|=\frac{n!}{(1!)^{m_1}(2!)^{m_2}\cdots(n!)^{m_n}}.$$

记不带编号的分组方案的集合为 T. 考虑映射 $p:S\to T$, 它定义为

$$p(f)=\{f^{-1}(1),f^{-1}(2),\cdots,f^{-1}(m_1+\cdots+m_n)\}.$$

换句话说, $p(f)$ 是 "忘记"f 分组方案中的编号. 对于不带编号的分组方案 $t\in T$, $p^{-1}(t)$ 的每个成员相当于给 t 分成的小组赋予编号, 并且要求规模小的组编号小. 注意到 t 共分成 m_1 个 1 元组,..., m_n 个 n 元组, 对这些组编号的总数目为 $(m_1)!\cdots(m_n)!$, 即对任何 $t\in T$, 都有 $\#p^{-1}(t)=(m_1)!\cdots(m_n)!$. 由此可得

$$|S|=\sum_{t\in T}\#p^{-1}(t)=\sum_{t\in T}(m_1)!\cdots(m_n)!=(m_1)!\cdots(m_n)!\cdot|T|,$$

即有

$$|T|=\frac{|S|}{(m_1)!\cdots(m_n)!}=\frac{n!}{m_1!\cdots m_n!(1!)^{m_1}(2!)^{m_2}\cdots(n!)^{m_n}}.$$

□

例 1.2.13. 将 n 个全同的硬币分给 k 个人, 每个人至少一个硬币, 方法总数为 $\binom{n-1}{k-1}$.

证明: 设第 i 个人分到 x_i 个硬币, 则要求 x_i 是正整数且 $x_1+\cdots+x_k=n$. 问题等价于计数方程 $x_1+\cdots+x_k=n$ 的正整数解 $(x_1,\cdots,x_k)$ 的数目. 设所有这样的解构成的集合为 S, 设 $[n-1]$ 的所有 $k-1$ 元子集构成的集合为 T, 考虑映射 $f:S\to T$ 为

$$f(x_1,\cdots,x_k)=\{x_1,x_1+x_2,\cdots,x_1+\cdots+x_{k-1}\}.$$

注意到 $1\le x_1<x_1+x_2<\cdots<x_1+\cdots+x_{k-1}<x_1+\cdots+x_k=n$, 可知 f 的确是取值在 T 中. 对任何 $T=\{t_1,\cdots,t_{k-1}\}\in T$, 不妨设 $t_1<t_2<\cdots<t_{k-1}$, 则

$$f(x_1,\cdots,x_k)=T\iff x_1=t_1,x_2=t_2-t_1,\cdots,x_{k-1}=t_{k-1}-t_{k-2},x_k=n-t_{k-1}.$$

特别的 f 是双射, 从而有 $|S|=|T|=\binom{n-1}{k-1}$. □

例 1.2.14. 将 n 个全同的硬币分给 k 个人, 方法总数为 $\binom{n+k-1}{k-1}$.

证明: 等价于计数方程 $x_1+\cdots+x_k=n$ 的非负整数解, 令 $y_i=1+x_i$, 则 y_i 是正整数且满足 $y_1+\cdots+y_k=n+k$. 利用前例的结论, $y_1+\cdots+y_k=n+k$ 的正整数解的数目为 $\binom{n+k-1}{k-1}$. □

1.3 容斥原理

定理 1.3.1 (容斥原理)**.** 设 $A_1,\ldots,A_n$ 是有限集合, 则有

$$|A_1\cup\cdots\cup A_n|=\sum_i|A_i|-\sum_{i<j}|A_i\cap A_j|+\cdots+(-1)^{n-1}|A_1\cap\cdots\cap A_n|.$$

证法一. 利用等式 $|X|=\sum_{x\in X}1$ 可得

$$\begin{aligned}\mathrm{RHS}&=\sum_i\sum_{x\in A_i}1-\sum_{i<j}\sum_{x\in A_i\cap A_j}1+\cdots+(-1)^{n-1}\sum_{x\in A_1\cap\cdots\cap A_n}1\\&=\sum_x\sum_{i,A_i\ni x}1-\sum_x\sum_{i<j,A_i\ni x,A_j\in x}1+\cdots+(-1)^{n-1}\sum_x\sum_{A_1\ni x,\cdots,A_n\ni x}1\\&=\sum_x\left(\sum_{i,A_i\ni x}1-\sum_{i<j,A_i\ni x,A_j\ni x}1+\cdots+(-1)^{n-1}\sum_{A_1\ni x,\cdots,A_n\ni x}1\right).\end{aligned}$$

设对每个 $x\in A_1\cup\cdots\cup A_n$, 共有 $d(x)$ 个 A_i 包含 x, 则 $d(x)\ge1$. 进一步可得

$$\begin{aligned}\mathrm{RHS}&=\sum_{x\in A_1\cup\cdots\cup A_n}\left(\binom{d(x)}{1}-\binom{d(x)}{2}+\cdots+(-1)^{d(x)-1}\binom{d(x)}{d(x)}\right)\\&=\sum_{x\in A_1\cup\cdots\cup A_n}1\\&=|A_1\cup\cdots\cup A_n|,\end{aligned}$$

其中我们用到了, 对正整数 d 有 $\sum_{i=0}^{d}(-1)^i\binom{d}{i}=0$.

□

证法二. 对 n 归纳. 可直接验证 $n=1,2$ 版本的容斥原理. 设 $n\le m(m\ge 2)$ 时容斥原理成立, 考虑 $n=m+1$ 的情形, 利用归纳假设可得

$$
\begin{aligned}
&|A_1\cup\cdots\cup A_{m+1}|\\
=&|(A_1\cup\cdots\cup A_m)\cup A_{m+1}|\\
=&|A_1\cup\cdots\cup A_m|+|A_{m+1}|-|(A_1\cup\cdots\cup A_m)\cap A_{m+1}|\\
=&|A_1\cup\cdots\cup A_m|+|A_{m+1}|-|(A_1\cap A_{m+1})\cup\cdots\cup(A_m\cap A_{m+1})|\\
=&\left(\sum_{k=1}^{m}(-1)^{k-1}\sum_{i_1<\cdots<i_k\le m}|A_{i_1}\cap\cdots\cap A_{i_k}|\right)+|A_{m+1}|-\left(\sum_{l=1}^{m}(-1)^{l-1}\sum_{j_1<\cdots<j_l\le m}|(A_{j_1}\cap A_{m+1})\cap\cdots\cap(A_{j_l}\cap A\right.\\
=&\left(\sum_{k=1}^{m}(-1)^{k-1}\sum_{i_1<\cdots<i_k\le m}|A_{i_1}\cap\cdots\cap A_{i_k}|\right)+|A_{m+1}|+\left(\sum_{l=1}^{m}(-1)^{l}\sum_{j_1<\cdots<j_l\le m}|A_{j_1}\cap\cdots\cap A_{j_l}\cap A_{m+1}|\right)\\
=&\sum_{k=1}^{m+1}(-1)^{k-1}\sum_{i_1<\cdots<i_k\le m+1}|A_{i_1}\cap\cdots\cap A_{i_k}|,
\end{aligned}
$$

这就完成了整个证明. □

例 1.3.2 (derangements, 错位排序)**.** 称置换 $\pi:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ 是一个错位排序, 如果对每个 i 都有 $\pi(i)\ne i$. 设错位排序 $\pi:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ 的数目为 d_n, 则

$$d_n=n!\cdot(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^n\frac{1}{n!}).$$

证明: 令 $A_i=\{\text{置换}\pi|\pi(i)=i\}$, 则所有错位排序构成的集合为

$$D_n=\cap_{i=1}^{n}(A_i)^c=(\cup_{i=1}^{n}A_i)^c.$$

注意到, 对 $i_1<\ldots<i_k$, 有

$$\#A_{i_1}\cap\cdots\cap A_{i_k}=\#\{\text{置换}\pi|\pi(i_1)=i_1,\cdots,\pi(i_k)=i_k\}=(n-k)!.$$

结合容斥原理可得

$$
\begin{aligned}
|A_1\cup\cdots\cup A_n|&=\sum_i|A_i|-\sum_{i<j}|A_i\cap A_j|+\cdots+(-1)^{n-1}|A_1\cap\cdots\cap A_n|\\
&=\binom{n}{1}\cdot(n-1)!-\binom{n}{2}\cdot(n-2)!+\cdots+(-1)^{n-1}\binom{n}{n}\cdot(n-n)!,
\end{aligned}
$$

进而有

$$d_n = n! - |A_1 \cup \cdots \cup A_n| = n! \cdot (1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}).$$

□

例 1.3.3 (满射的数目)**.** 给定正整数 m, n, 则从 $[n]$ 到 $[m]$ 的满射的数目为

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

证明: 对 $i = 1, \ldots, m$ 令

$$A_i = \{f : [n] \to [m] | i \notin f([n])\} = \{f : [n] \to [m] \backslash \{i\}\},$$

则 $|A_i| = (m-1)^n$. 对任何 $i_1 < \cdots < i_k$ 有

$$\begin{aligned} |A_{i_1} \cap \cdots \cap A_{i_k}| &= \#\{f : [n] \to [m] | i_1, \cdots, i_k \notin f([n])\} \\ &= \#\{f : [n] \to [m] \backslash \{i_1, \cdots, i_k\}\} \\ &= (m-k)^n. \end{aligned}$$

设全体满射 $f : [n] \to [m]$ 构成的集合为 S, 则 $S^c = A_1 \cup A_2 \cup \cdots \cup A_m$, 利用容斥原理可得

$$\begin{aligned} |S^c| &= \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{m-1} |A_1 \cap \cdots \cap A_m| \\ &= m \cdot (m-1)^n - \binom{m}{2} \cdot (m-2)^n + \cdots + (-1)^{m-1} \binom{m}{m} \cdot (m-m)^n, \end{aligned}$$

即有

$$|S| = m^n - \binom{m}{1} (m-1)^n + \cdots + (-1)^m \binom{m}{m} \cdot (m-m)^n = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n.$$

□

1.4 递推关系

例 1.4.1 (Fibonacci)**.** 一个农夫养兔子. 假设每只兔子在两个月大时开始产子, 从第二个月开始每月产一只兔子. 假设兔子不会死, 且都是母兔. 如果农夫第一个月有一只新生的兔子, 求第 n 月时兔子的总数目 F_n.

解. 设第 n 个月的兔子的集合为 R_n, 则 $R_n = R_{n-1} \cup \{第n月新生的兔子\}$. 在第 $n+1$ 个月, R_n 中属于 R_{n-1} 的那部分兔子各产一只兔子, 第 n 月新生的兔子在第 $n+1$ 个月尚不能生产, 故有 $R_{n+1} \backslash R_n \cong R_{n-1}$, 得到 $\{F_n\}$ 满足递推关系: $F_{n+1} = F_n + F_{n-1}$, 且 $F_1 = F_2 = 1$. 人们把这个数列称为斐波那契数列. □

如何求出斐波那契数列的通项公式?

方法一. 可将递推关系表述为

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix},$$

记 $\mathbf{v}_n = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$, $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, 则有 $\mathbf{v}_n = A\mathbf{v}_{n-1}$, 从而有 $\mathbf{v}_n = A^{n-1}\mathbf{v}_1$. 为了计算 A^{n-1}, 考虑 A 是否能对角化, 如果 $A = S \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} S^{-1}$, 则 $A^{n-1} = S \begin{pmatrix} \lambda_1^{n-1} & 0 \\ 0 & \lambda_2^{n-1} \end{pmatrix} S^{-1}$. 由此可将 F_n 表示成 $F_n = C_1\lambda_1^n + C_2\lambda_2^n$ 的形式, 其中 C_1, C_2 是待定的系数, 可由初始值 F_1, F_2 解出 C_1, C_2.

具体计算如下. A 的特征多项式为 $p_A(\lambda) = \det(\lambda I - A) = \lambda(\lambda - 1) - 1$, 有两个特征根 $\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$. 设 $F_n = C_1\lambda_1^n + C_2\lambda_2^n$, 则由初值条件

$$C_1 \frac{1+\sqrt{5}}{2} + C_2 \frac{1-\sqrt{5}}{2} = 1, \quad C_1 (\frac{1+\sqrt{5}}{2})^2 + C_2 (\frac{1-\sqrt{5}}{2})^2 = 1$$

可解出 $C_1 = \frac{1}{\sqrt{5}} = -C_2$. 这就得到斐波那契数列的通项公式

$$F_n = \frac{1}{\sqrt{5}} (\lambda_1^n - \lambda_2^n) = \frac{1}{\sqrt{5}} \left((\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n \right).$$

□

方法二. 考虑一般的 k 阶线性递推数列 $\{x_n\}$, 它满足递推关系

$$x_{n+k} = a_{k-1}x_{n+k-1} + \cdots + a_0 x_n. \tag{1.1}$$

定义该数列的特征方程为 $x^k = a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$, 称特征方程的根为该数列的特征根. 对于每个特征根 λ, 由 $\lambda^k = a_{k-1}\lambda^{k-1} + \cdots + a_1\lambda + a_0$ 可知

$$\lambda^{n+k} = a_{k-1}\lambda^{n+k-1} + \cdots + a_1\lambda^{n+1} + a_0\lambda^n,$$

这表明数列 $\{\lambda^n\}$ 满足递推关系(1.1).

(1) 如果特征方程有 k 个不同的根 $\lambda_1,\dots,\lambda_k$. 令 $y_n = C_1\lambda_1^n + \cdots + C_k\lambda_k^n$, 取 $C_1,\dots,C_k$ 使得对 $1 \le i \le k$ 都有 $x_i = y_i$. 由于 $\{x_n\}$ 与 $\{y_n\}$ 满足相同的递推关系(1.1), 且前 k 项对应项相等, 则容易用归纳法证明对每个 n 都有 $x_n = y_n$, 从而求出了 $\{x_n\}$ 的通项公式

$$x_n = C_1\lambda_1^n + \cdots + C_k\lambda_k^n.$$

(2) 如果特征方程有重根. 设 λ 是特征多项式 $p(x)$ 的 m 重根, 则 λ 是

$$q_0(x) = x^n p(x) = x^{n+k} - a_{k-1}x^{n+k-1} - \cdots - a_0x^n$$

的至少 m 重根. 求导可知 λ 是 $q_0'(x)$ 的至少 $m-1$ 重根, 进而也是 $xq_0'(x)$ 的至少 $m-1$ 重根, 即 λ 是

$$q_1(x) = (n+k)x^{n+k} - a_{k-1}(n+k-1)x^{n+k-1} - \cdots - a_nnx^n$$

的至少 $m-1$ 重根. 重复此推理可得 λ 是

$$q_2(x) = xq_1'(x) = (n+k)^2x^{n+k} - a_{k-1}(n+k-1)^2x^{n+k-1} - \cdots - a_nn^2x^n$$

的至少 $m-2$ 重根. 依此进行下去, 对 $t \le m-1$, λ 是

$$q_t(x) = (n+k)^tx^{n+k} - a_{k-1}(n+k-1)^tx^{n+k-1} - \cdots - a_nn^tx^n$$

的至少 $m-t$ 重根. 这样对 $0 \le t \le m-1$ 就有

$$(n+k)^t\lambda^{n+k} - a_{k-1}(n+k-1)^t\lambda^{n+k-1} - \cdots - a_nn^t\lambda^n = 0,$$

这表明对 $0 \le t \le m-1$ 数列 $\{n^t\lambda^n\}$ 满足递推关系(1.1)

假设特征多项式的全部根为 $\lambda_1,\dots,\lambda_s$, 它们的重数分别为 $m_1,\dots,m_s$, 则与 (1) 类似, 可以证明 $\{x_n\}$ 的通项公式为

$$x_n = \sum_{i=1}^{s}\sum_{j=0}^{m_i-1} C_{i,j}n^j\lambda_i^n,$$

其中系数 $\{C_{ij}\}$ 由初值 $x_1,\dots,x_k$ 决定.

对于斐波那契数列, 其特征方程为 $x^2 = x+1$, 有两个特征根 $\lambda_{1,2} = \frac{1\pm\sqrt{5}}{2}$, 故有 $x_n = C_1\lambda_1^n + C_2\lambda_2^n$, 再由初值 F_1, F_2 解出 $C_1 = \frac{1}{\sqrt{5}} = -C_2$. □

命题 1.4.2. (1) $\sum_{i=0}^{n} F_i = F_{n+2} - 1$.

(2) $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.

(3) $F_n^2 + F_{n-1}^2 = F_{2n-1}$.

证明: 可由通项公式直接验证. □

例 1.4.3. 给定正整数 n,k. 将 n 个不同物体分成 k 个不带标号的组, 要求每组至少一个物体. 设分组方案的数目为 $S(n,k)$, 称之为第二类 Stirling 数.

解. 将分组方案分成两类. (1) 第一类分组方案中第 n 个物体单独一组. 只需再将前 $n-1$ 个物体分成 $k-1$ 组, 故第一类方案的数目为 $S(n-1,k-1)$. (2) 第二类分组方案中第 n 个物体不是单独一组. 可将第二类分组方案分两步完成: 第一步将前 $n-1$ 个物体分成 k 组, 第二步将 n 加入到之前得到的 k 个组的某一个中. 由乘法原理, 第二类方案的数目为 $S(n-1,k)\cdot k$.

由此可得 $S(n,k)$ 满足如下递推关系:

$$S(n,k)=S(n-1,k-1)+kS(n-1,k).$$

利用上式可计算 n,k 较小情形的 Stirling 数. 还可以对 n 用归纳法证明如下恒等式

$$\sum_{k=0}^{n}S(n,k)x(x-1)\cdots(x-k+1)=x^n.$$

$S(n,k)$ 还与例1.3.4中所得到的满射的数目有关. 设将 $[n]$ 分拆成 k 个 (不带标号的) 组的所有方案构成的集合为 P, 则 $|P|=S(n,k)$. 令 M 为从到 $[n]$ 到 $[k]$ 的所有满射 $f:[m]\to[k]$ 所构成的集合. 定义映射 $p:M\to P$ 为

$$p(f)=\{f^{-1}(1),\cdots,f^{-1}(k)\}.$$

易知, 对任何 $A=\{A_1,\ldots,A_k\}\in P$, 有 $\#p^{-1}(A)=k!$, 从而有 $|M|=k!\cdot|P|$, 可得

$$S(n,k)=|P|=\frac{1}{k!}|M|=\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n.$$

□

定义 1.4.4. 令 $[n]=\{1,2,...,n\}$. 称 $[n]$ 的子集族 $P=\{A_1,...,A_k\}$ 为 $[n]$ 的一个分组方案, 如果 k 是正整数, $A_1,...,A_k$ 是 $[n]$ 的非空子集, 且满足

$$\cup_{t=1}^{k}A_t=[n],\quad \text{且}A_i\cap A_j=\emptyset,\forall i\neq j.$$

定理 1.4.5. *设函数 f,g 都有 n 阶导数, 则*

$$(g\circ f)^{(n)}(x)=\sum_{[n]\text{的分组方案}P=\{A_1,\ldots,A_k\}}g^{(k)}(f(x))\cdot\prod_{i=1}^{k}f^{(|A_i|)}(x).$$

证明: 对 n 用归纳法, 假设 n 时命题成立, 来证明 $n+1$ 的情形.

注意到, 对 $[n]$ 的分组方案 $P=\{A_1,...,A_k\}$, 可构造出 $(k+1)$ 个 $[n+1]$ 的分组方案:

$$\{\{n+1\},A_1,...,A_k\},\quad \{A_1\cup\{n+1\},A_2,...,A_k\},\quad ...,\{A_1,...,A_{k-1},A_k\cup\{n+1\}\},$$

当 P 取遍 $[n]$ 的分组方案时, 上述构造不重复的取遍了 $[n+1]$ 的所有分组方案. 由此及归纳假设, 可得

$$\begin{aligned}
&\sum_{[n+1]\text{的分组方案}Q=\{B_1,...,B_k\}} g^{(k)}(f(x))\cdot\prod_{i=1}^{k}f^{(|B_i|)}(x)\\
=&\sum_{[n]\text{的分组方案}P=\{A_1,...,A_k\}} g^{(k+1)}(f(x))\cdot f^{(1)}(x)\cdot\prod_{i=1}^{k}f^{(|A_i|)}(x)\\
&+\sum_{[n]\text{的分组方案}P=\{A_1,...,A_k\}} g^{(k)}(f(x))\cdot f^{(|A_1|+1)}(x)\cdot\prod_{i=2}^{k}f^{(|A_i|)}(x)+...\\
&+\sum_{[n]\text{的分组方案}P=\{A_1,...,A_k\}} g^{(k)}(f(x))\cdot\prod_{i=1}^{k-1}f^{(|A_i|)}(x)\cdot f^{(|A_k|+1)}(x)\\
=&\left(\sum_{[n]\text{的分组方案}P=\{A_1,...,A_k\}} g^{(k)}(f(x))\cdot\prod_{i=1}^{k}f^{(|A_i|)}(x)\right)'\\
=&\left((g\circ f)^{(n)}\right)'(x)\\
=&(g\circ f)^{(n+1)}(x),
\end{aligned}$$

这就完成了归纳法. □

1.5 抽屉原理

定理 1.5.1 (鸽笼原理, 抽屉原理)**.** *将多于 nk 个物体放入 n 个抽屉中, 则必有一个抽屉中放有至少 $k+1$ 个物体.*

命题 1.5.2. *设 $p:E\to B$ 是有限集合之间的映射, 则存在 $b_0,b_1\in B$, 使得*

$$|p^{-1}(b_0)|\le\frac{|E|}{|B|}\le|p^{-1}(b_1)|.$$

例 1.5.3. 在边长 70cm 的正方形内任取 50 个点, 则存在两个取出的点距离小于 15cm.

证明: 将 70×70 的正方形分割成 49 个 10×10 的小正方形. 共选出了 50 个点, 由抽屉原理可知必有两个点位于同一个小正方形中, 它们的距离

$$d=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}\le10\sqrt{2}<15.$$

□

例 1.5.4 (Erdös)**.** 设 $a_1, \ldots, a_n$ 是 n 个整数, 则可从中选出若干个 (至少一个), 使得选出的数的和能被 n 整除.

证明*:* 记 $S_i = a_1 + \cdots + a_i$, 考虑 $S_1, \ldots, S_n$ 除以 n 的余数. 如果存在 S_i 除以 n 的余数为零, 则选出 $a_1, \ldots, a_i$, 它们的和能被 n 整除. 如果 $S_1, \ldots, S_n$ 除以 n 的余数都不为零, 则余数只能取 $1, \ldots, n-1$ 共 $n-1$ 个值, 由抽屉原理知存在两个 $S_i, S_j (i < j)$ 它们除以 n 的余数相同, 从有 $S_j - S_i = a_{i+1} + \cdots + a_j$ 能被 n 整除, 选出 $a_{i+1}, \ldots, a_j$ 即可. □

第二章　组合概率论

2.1　有限概率空间

定义 2.1.1. (1) 所谓一个有限概率空间是指一个有限集 Ω, 且对每个 $\omega \in \Omega$ 赋予了非负实数 p_ω, 满足 $\sum_{\omega\in\Omega} p_\omega = 1$. 称 p_ω 为 ω 的概率.

(2) 给定有限概率空间 Ω, 定义一个事件为一个子集 $E \subseteq \Omega$. 事件 E 的概率为 $P(E) = \sum_{\omega\in E} p_\omega$. E 的补集 E^c 表示 E 不发生的事件, 其概率为 $P(E^c) = 1 - P(E)$.

(3) 称 Ω 是均匀 (分布) 概率空间, 如果对每个 $\omega \in \Omega$ 都有 $p_\omega = \frac{1}{|\Omega|}$.

例 2.1.2. (1) 有限概率空间就是带权重的有限集合 (Ω, p), 其中权重函数 $p : \Omega \to \mathbf{R}_{\geq 0}$ 满足 $\sum_{\omega\in\Omega} p(\omega) = 1$.

(2) 设 (A, p) 与 (B, q) 是两个概率空间, 则迪卡尔积 $A \times B$ 上有自然的概率空间结构, 只需对 $(a, b) \in A \times B$ 赋予概率 $p(a) \cdot q(b)$ 即可. 特别的, 设 Ω 是概率空间, 则 Ω^n 上有自然的概率空间结构: 定义 $(\omega_1, \ldots, \omega_n)$ 的概率为 $p_{\omega_1} \cdots p_{\omega_n}$.

(3) 扔材料均匀的硬币, 有两种结果, 概率都是 $\frac{1}{2}$, 则可把扔硬币所得结果的概率空间等同为均匀概率空间 $\{0, 1\}$. 进而, 连续扔 n 次硬币所得结果的概率空间等同为均匀概率空间 $\{0, 1\}^n$. 具体的说, 连续扔 n 次硬币, 恰扔出 k 个 1 的概率为 $\frac{1}{2^n} \cdot C_n^k$.

引理 2.1.3. (1) 设 $0 \leq t \leq m$, 则有

$$e^{-t^2/(m-t+1)} \leq \frac{C_{2m}^{m-t}}{C_{2m}^m} \leq e^{-t^2/(m+t)}.$$

(2) 如果 $t \geq \sqrt{m \ln C} + \ln C$, 则有 $\frac{C_{2m}^m}{C_{2m}^{m-t}} \geq C$; 如果 $t \leq \sqrt{m \ln C} - \ln C$, 则有 $\frac{C_{2m}^m}{C_{2m}^{m-t}} \leq C$.

(3) 设 $0 \leq k \leq m$, 则有

$$\sum_{i=0}^{k-1} C_{2m}^i < 2^{2m-1} \cdot \frac{C_{2m}^k}{C_{2m}^m}.$$

证明: (1) 注意到

$$\frac{C_{2m}^{m-t}}{C_{2m}^{m}} = \frac{m!m!}{(m-t)!(m+t)!} = \frac{(m-t+1)\cdots m}{(m+1)\cdots(m+t)}$$
$$= (1-\frac{t}{m+1})(1-\frac{t}{m+2})\cdots(1-\frac{t}{m+t}).$$

对 $0<u<1$, 由函数 $f(x)=\ln x$ 在区间 $[1-u,1]$ 上的 Lagrange 中值定理可知存在 $\xi\in(1-u,1)$ 使得

$$\frac{f(1)-f(1-u)}{1-(1-u)} = f'(\xi) = \frac{1}{\xi} \in (1, \frac{1}{1-u}),$$

从而得到如下有用的不等式

$$-\frac{u}{1-u} < \ln(1-u) < -u, \quad \forall 0<u<1.$$

由此可得

$$e^{-\frac{t^2}{m+1-t}} \le e^{-(\frac{t}{m+1-t}+\cdots+\frac{t}{m+t-t})} \le \frac{C_{2m}^{m-t}}{C_{2m}^{m}} \le e^{-(\frac{t}{m+1}+\cdots+\frac{t}{m+t})} \le e^{-\frac{t^2}{m+t}}.$$

(2) 由 (1) 的结论, 有 $e^{\frac{t^2}{m-t+1}} \ge \frac{C_{2m}^{m}}{C_{2m}^{m-t}} \ge e^{\frac{t^2}{m+t}}$. 当 $t \ge \sqrt{m\ln C}+\ln C$ 时, 有

$$t(t-\ln C) \ge (\sqrt{m\ln C}+\ln C)\sqrt{m\ln C} \ge m\ln C,$$

即 $\frac{t^2}{m+t} \ge \ln C$, 从而有 $\frac{C_{2m}^{m}}{C_{2m}^{m-t}} \ge e^{\frac{t^2}{m+t}} \ge C$. 当 $t \le \sqrt{m\ln C}-\ln C$ 时, 有

$$t(t+\ln C) \le (\sqrt{m\ln C}-\ln C)\sqrt{m\ln C} \le (m+1)\ln C,$$

即有 $\frac{t^2}{m-t+1} \le \ln C$, 从而有 $\frac{C_{2m}^{m}}{C_{2m}^{m-t}} \le e^{\frac{t^2}{m-t+1}} \le C$.

(3) 先证明对 $1\le i\le k$ 有

$$\frac{C_{2m}^{k-i}}{C_{2m}^{k}} \le \frac{C_{2m}^{m-i}}{C_{2m}^{m}}.$$

注意到, 对满足 $b>m-k$ 的正数 a,b 有 $\frac{a}{b} \le \frac{a+m-k}{b-(m-k)}$, 由此可得

$$\frac{C_{2m}^{k-i}}{C_{2m}^{k}} = (\frac{k-i+1}{2m-k+1})\cdot\cdots\cdot(\frac{k}{2m-k+i})$$
$$\le (\frac{m-i+1}{m+1})\cdot\cdots\cdot(\frac{m}{m+i})$$
$$= \frac{C_{2m}^{m-i}}{C_{2m}^{m}}.$$

由此可得

$$\frac{1}{C_{2m}^{k}}\sum_{i=0}^{k-1} C_{2m}^{i} = \sum_{j=1}^{k}\frac{C_{2m}^{k-j}}{C_{2m}^{k}} \le \sum_{j=1}^{k}\frac{C_{2m}^{m-j}}{C_{2m}^{m}} \le \frac{1}{C_{2m}^{m}}\sum_{l=0}^{m-1} C_{2m}^{l} = \frac{1}{C_{2m}^{m}}\cdot\frac{2^{2m}-C_{2m}^{m}}{2} < \frac{2^{2m-1}}{C_{2m}^{m}},$$

这就完成了 (3) 的证明. □

定理 2.1.4. 给定 $0 \le t \le m$. 连续扔 $2m$ 次硬币, 则扔得 1 的次数小于 $m-t$ 或大于 $m+t$ 的概率不超过 $e^{-t^2/(m+t)}$.

证明: 记所述的概率为 a, 则利用引理2.1.3的结论可得:

$$\begin{aligned} a &= \frac{1}{2^{2m}}\left(C_{2m}^0 + \cdots + C_{2m}^{m-t-1} + C_{2m}^{m+t+1} + \cdots + C_{2m}^{2m}\right) \\ &= \frac{1}{2^{2m-1}} \sum_{i=0}^{m-t-1} C_{2m}^i \\ &\le \frac{C_{2m}^{m-t}}{C_{2m}^m} \\ &\le e^{-t^2/(m+t)}. \end{aligned}$$

□

定理 2.1.5. 给定正数 ϵ. 连续扔 n 次硬币, 设扔得 1 的次数占比在区间 $[0.5-\epsilon, 0.5+\epsilon]$ 之中的概率为 c_n, 则有 $\lim_{n\to\infty} c_n = 1$.

证明: 不妨设 $\epsilon < \frac{1}{2}$. 对偶数 $n = 2m$, 取 $t = [2m\epsilon]$, 则扔得 1 的次数占比不在区间 $[0.5-\epsilon, 0.5+\epsilon]$ 之中等价于: 扔得 1 的次数 l 满足 $l < m - 2m\epsilon$ 或 $l > m + 2m\epsilon$. 由 $t = [2m\epsilon] \le 2m\epsilon$ 知

$$l < m - 2m\epsilon \Rightarrow l < m - t, \quad l > m + 2m\epsilon \Rightarrow l > m + t,$$

从而有 $1 - c_{2m}$ 不超过扔得 1 的次数小于 $m-t$ 或大于 $m+t$ 的概率. 由定理2.1.4可知

$$1 - c_{2m} \le e^{-\frac{t^2}{m+t}} \le e^{-\frac{t^2}{2m}} \le e^{-\frac{(2m\epsilon-1)^2}{2m}},$$

由夹逼定理可得 $\lim_{m\to\infty}(1 - c_{2m}) = 0$.

对奇数 n, 可以类似的处理. □

设 E_1, E_2 是两个事件, 则 $E_1 \cap E_2$ 表示 E_1, E_2 都发生的事件, $E_1 \cup E_2$ 表示 E_1, E_2 中至少一个发生的事件. 这些事件概率之间的关系由带权重的容斥原理描述:

$$P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2).$$

对多个事件, 有如下的定理.

定理 2.1.6 (带权重的容斥原理)**.** 设 $E_1, \ldots, E_n \subseteq \Omega$ 是有限概率空间 Ω 的 n 个事件, 则有

$$P(E_1 \cup \cdots \cup E_n) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} P(E_{i_1} \cap \cdots \cap E_{i_k}).$$

证明: 仿照定理1.3.2的证明即可. □

2.2 大数定律 (*Law of large numbers*)

定义 2.2.1. 所谓一个随机变量是指一个从概率空间 (Ω, p) 到 $\mathbf{R}$ 的映射 $X : \Omega \to \mathbf{R}$. X 取值在 $V \subseteq \mathbf{R}$ 中的概率为

$$P(X \in V) = P(\{\omega \in \Omega | X(\omega) \in V\}) = \sum_{\omega \in \Omega, X(\omega) \in V} p_\omega.$$

特别的, X 取值为 a 的概率为

$$P(X = a) = \sum_{\omega \in \Omega, X(\omega) = a} p_\omega.$$

定义随机变量 X 的期望为

$$E[X] = \sum_{\omega \in \Omega} X(\omega) p_\omega.$$

定义随机变量 X 的方差 $\mathrm{Var}(X)$ 为 $(X - E[X])^2$ 的期望, 即

$$\mathrm{Var}(X) = E[(X - E[X])^2] = E[X^2] - (E[X])^2.$$

定理 2.2.2 (Markov's inequality)**.** *设 X 是非负的随机变量, 则对任何正数 $\lambda > 0$, 有*

$$P(X \geq \lambda) \leq \frac{E[X]}{\lambda}.$$

证明: 由期望的定义, 有

$$E[X] = \sum_{a \geq 0} a \cdot P(X = a) \geq \sum_{a \geq \lambda} a \cdot P(X = a) \geq \lambda \sum_{a \geq \lambda} P(X = a) = \lambda \cdot P(X \geq \lambda),$$

由此即得 $P(X \geq \lambda) \leq \frac{E[X]}{\lambda}$. □

定理 2.2.3 (Chebyshev's inequality)**.** *设 X 是一个随机变量, 则对任何正数 $\lambda > 0$, 有*

$$P\left(|X - E[X]| > \lambda Var(X)^{1/2}\right) \leq \frac{1}{\lambda^2}.$$

证明: 对非负随机变量 $(X - E[X])^2$ 使用 Markov 不等式, 可得

$$P\left((X - E[X])^2 > \lambda^2 \mathrm{Var}(X)\right) \leq \frac{E[(X - E[X])^2]}{\lambda^2 \mathrm{Var}(X)} = \frac{1}{\lambda^2}.$$

□

设 X, Y 分别是概率空间 Ω_1, Ω_2 上的随机变量, 按如下方式定义 $X+Y$ 为概率空间 $\Omega_1 \times \Omega_2$ 上的随机变量:

$$(X + Y)(\omega_1, \omega_2) = X(\omega_1) + Y(\omega_2).$$

命题 2.2.4. $X+Y$ 的期望与方差分别为

$$E[X+Y]=E[X]+E[Y],\quad Var(X+Y)=Var(X)+Var(Y).$$

定理 2.2.5 (大数定律)**.** 设 X 是有限概率空间 Ω 上的随机变量, 它的期望为 μ. 定义概率空间 Ω^n 上的随机变量 $\overline{X}_n$ 为

$$\overline{X}_n=\frac{1}{n}(X_1+\cdots+X_n).$$

对任何正数 ϵ, 有

$$\lim_{n\to\infty}P(|\overline{X}_n-\mu|\geq\epsilon)=0.$$

证明*:* 利用命题2.2.4可知:

$$E[\overline{X}_n]=\mu,\quad \mathrm{Var}(\overline{X}_n)=\frac{\mathrm{Var}(X)}{n}.$$

由 Chebyshev 不等式可得

$$P(|\overline{X}_n-\mu|\geq\epsilon)\leq\frac{\mathrm{Var}(\overline{X}_n)}{\epsilon^2}=\frac{\mathrm{Var}(X)}{n\epsilon^2},$$

再利用夹逼定理可得

$$\lim_{n\to\infty}P(|\overline{X}_n-\mu|\geq\epsilon)=0.$$

□

例 2.2.6. 扔硬币的结果构成一致概率空间 $\Omega=\{$正, 反$\}$, 考虑 Ω 上的随机变量 X, 当结果为正面朝上时 X 等于 1, 当结果为反面朝上时 X 等于 0, 则随机变量

$$\overline{X}_n=\frac{1}{n}(X_1+\cdots+X_n).$$

描述扔 n 次硬币正面朝上次数占总次数的比例. 这样, 前述大数定律断言:

$$P(\text{正面朝上次数占比偏离0.5的幅度超过}\epsilon)\leq\frac{1}{4n\epsilon^2},$$

这就给出了定理2.1.5的结论.

2.3 Lovasz Local Lemma

定义 2.3.1. 设 E,E' 是两个事件, 称 E 与 E' 是独立的, 如果 $P(E\cap E')=P(E)P(E')$.

这样, 如果 E 与 E' 是独立的, 则有 $P(E\cup E')=P(E)+P(E')-P(E)P(E')$.

人们也可用条件概率来定义独立事件. 如果 E 与 E' 是事件且 $P(E')\neq 0$, 定义

$$P(E|E')=\frac{P(E\cap E')}{P(E')},$$

称之为 E' 发生时 E 发生的条件概率. 这样, E 与 E' 是独立的当且仅当 $P(E|E')=P(E)$, 即 E' 发生不影响 E 发生的概率, 对称的, E 发生不影响 E' 发生的概率.

定义 2.3.2. 给定事件 E 与 $E_1,E_2,\ldots,E_k$. 称 E 与一族事件 $\{E_1,E_2,\ldots,E_k\}$ 无关, 如果对 $\{E_1,E_2,\ldots,E_k,E_1^c,E_2^c,\ldots,E_k^c\}$ 的任何子集 $\{B_1,\ldots,B_l\}$ 都有

$$P(E|B_1\cap\cdots\cap B_l)=P(E).$$

定理 2.3.3 (Lovasz Local Lemma)**.** *设给定了一族事件 $E_1,\ldots,E_n$ 以及一个以 $\{1,\ldots,n\}$ 为顶点集合的图 G. 对 $1\leq i\leq n$, 令 $S_i=\{j|j\neq i$且在图G中j与i不相邻$\}$ 为 G 中与 i 不相邻的顶点构成的集合. 假设对每个 $1\leq i\leq n$, 都有 E_i 与事件族 $\{E_j\}_{j\in S_i}$ 无关.*

假设存在 k 个实数 $0\leq x_1,\ldots,x_n<1$ 满足对每个 $1\leq i\leq n$ 都有

$$P(E_i)\leq x_i\prod_{j\text{与}i\text{相邻}}(1-x_j). \tag{2.1}$$

在此条件下, 如下不等式成立:

$$P(E_1\cup\cdots\cup E_n)\leq 1-(1-x_1)\cdots(1-x_n).$$

特别的, 有 $E_1\cup\cdots\cup E_n\neq\Omega$.

证明: 对 $[n]$ 的任何子集 T, 约定记号 $E_T^c=\cap_{j\in T}E_j^c$.

(1) 先证明: 对每个 i, 以及每个不包含 i 的子集 T, 都有

$$P(E_i|E_T^c)\leq x_i. \tag{2.2}$$

对 $|S|$ 归纳. 当 $|T|=0$ 时, 要证明的不等式为 $P(E_i)\leq x_i$, 由条件(2.1)即得证. 考虑 $|T|\geq 1$ 的情形, 设 $|T|$ 更小的版本已经成立. 用 $N(i)$ 表示 i 在 G 中所有邻点构成的集合, 记 $T_1=T\cap N(i)$, $T_2=T\backslash T_1$. 如果 $T_1=\emptyset$, 则 $T\subseteq S_i$, 由条件 E_i 与事件族 $\{E_j\}_{j\in S_i}$ 无关, 则有 $P(E_i|E_T^c)=P(E_i)$, 结合条件(2.1)可知 (2.2)成立. 以下假设 $|T_1|\geq 1$, 设 $T_1=\{j_1,\ldots,j_k\}$, 则有

$$P(E_i|E_T^c)=\frac{P(E_i\cap E_{T_1}^c\cap E_{T_2}^c)/P(E_{T_2}^c)}{P(E_{T_1}^c\cap E_{T_2}^c)/P(E_{T_2}^c)}=\frac{P(E_i\cap E_{T_1}^c|E_{T_2}^c)}{P(E_{T_1}^c|E_{T_2}^c)}\leq\frac{P(E_i|E_{T_2}^c)}{P(E_{T_1}^c|E_{T_2}^c)}=\frac{P(E_i)}{P(E_{T_1}^c|E_{T_2}^c)}.$$

利用归纳假设, 可进一步估计上式右边的分母:

$$\begin{aligned} P(E_{T_1}^c|E_{T_2}^c) &= P(E_{j_1}^c|E_{j_2}^c \cap \cdots \cap E_{j_k}^c \cap E_{T_2}^c) \cdot \cdots \cdot P(E_{j_k}^c|E_{T_2}^c) \\ &= (1 - P(E_{j_1}|E_{j_2}^c \cap \cdots \cap E_{j_k}^c \cap E_{T_2}^c)) \cdot \cdots \cdot (1 - P(E_{j_k}|E_{T_2}^c)) \\ &\geq (1 - x_{j_1}) \cdot \cdots \cdot (1 - x_{j_k}). \end{aligned}$$

由此可得

$$P(E_i|E_T^c) \leq \frac{P(E_i)}{P(E_{T_1}^c|E_{T_2}^c)} \leq \frac{x_i \prod_{j\text{与}i\text{相邻}}(1 - x_j)}{(1 - x_{j_1}) \cdot \cdots \cdot (1 - x_{j_k})} \leq x_i,$$

从而完成了(2.2)的证明.

(2) 利用 (1) 的结论, 有

$$\begin{aligned} P(E_1^c \cap \cdots \cap E_n^c) &= P(E_1^c|E_2^c \cap \cdots \cap E_n^c) \cdot \cdots \cdot P(E_{n-1}^c|E_n^c) \cdot P(E_n^c) \\ &= (1 - P(E_1|E_2^c \cap \cdots \cap E_n^c)) \cdot \cdots \cdot (1 - P(E_{n-1}|E_n^c)) \cdot (1 - P(E_n)) \\ &\geq (1 - x_1) \cdot \cdots \cdot (1 - x_{n-1}) \cdot (1 - x_n) \\ &> 0. \end{aligned}$$

□

第三章　初等数论

3.1　整除

定义 3.1.1. 设 a,b 是整数, 称 a 整除 b, 或者 a 是 b 的因子, 或 b 是 a 的倍数, 如果存在整数 m 使得 $b=am$.

如果 a 整除 b, 则记为 $a\mid b$; 如果 a 不整除 b, 则记为 $a\nmid b$. 一般的, 只对非零整数 a 讨论它是否整除另一个整数 b.

命题 3.1.2 (带余除法)**.** *设 a 是正整数, 则对任何整数 b, 存在整数 q,r 使得 $0\le r<a$, 且 $b=aq+r$.*

定义 3.1.3. 设 a,b 是整数, 称满足 $d\mid a,d\mid b$ 的最大正整数 d 为 a,b 的最大公约数, 记作 $\gcd(a,b)$ 或 (a,b). 称满足 $a\mid m,b\mid m$ 的最小正整数 m 为 a,b 的最小公倍数, 记作 $\operatorname{lcm}(a,b)$ 或 $[a,b]$.

命题 3.1.4 (Euclid Algorithm, 辗转相除法)**.** *给定正整数 $a\ge b$. 设 a 对 b 做带余除法为 $a=q_1b+r_1$, b 对 r_1 做带余除法为 $b=q_2r_1+r_2$. 对 $i\ge 1$, 设 r_i 对 r_{i+1} 做带余除法为 $r_i=q_{i+2}r_{i+1}+r_{i+2}$. 设 $m+1$ 是使得 $r_i=0$ 成立的最小正整数 i, 则有*

$$(a,b)=(b,r_1)=(r_1,r_2)=\cdots=(r_m,r_{m+1})=r_m.$$

证明: 注意到, 如果 $x=qy+r$, 则 $d\mid x,d\mid y$ 当且仅当 $d\mid y,d\mid r$, 从而有 $(x,y)=(y,r)$. □

命题 3.1.5. *设 a,b 是正整数, 则用 Euclid Algorithm 计算 a,b 的最大公约数需要做至多 $\log_2 a+\log_2 b$ 次带余除法.*

证明: 在命题3.1.4中共做了 $m+1$ 次带余除法. 注意到, 对每次带余除法 $x=qy+r(x\ge y\ge 1,0\le r<y)$, 有

$$xy=(qy+r)y\ge(y+r)y>2yr.$$

由此可得在 Euclid Algorithm 中有

$$ab > 2br_1 > 2^2 r_1 r_2 > \cdots > 2^m r_{m-1} r_m \geq 2^m \cdot 2 \cdot 1,$$

从而有 $m+1 < \log_2(ab)$, 即为求出 (a,b) 只需做少于 $\log_2(ab)$ 次带余除法. □

定理 3.1.6 (Bezout 定理)**.** *设 a,b 是整数, 则存在整数 u,v 使得*

$$au + bv = (a,b).$$

特别的, 如果 a,b 互质, 则存在整数 u,v 使得 $au+bv=1$.

证法一. 令 S 为由所有形如 $au+bv(u,v \in \mathbf{Z})$ 的整数构成的集合. 注意到, 若 $x,y \in S$, 则对任何整数 s,t, 有 $sx+ty \in S$.

在 Euclid Algorithm 中有 $a,b \in S$, 从而可得 $r_1 = a - q_1 b \in S$, $r_2 = b - q_2 r_1 \in S$, 依次进行下去, 在 $r_{i-1}, r_i \in S$ 的基础上进一步可得 $r_{i+1} = r_{i-1} - q_{i+1} r_i \in S$. 这样, 有限步之后有 $r_m \in S$, 此即 $(a,b) \in S$. □

证法二. 记 $(a,b)=d$. 设 S 定义如前, 我们来证明 $S = \{dx | x \in \mathbf{Z}\} = d\mathbf{Z}$. 首先, 对任何 $x \in S$, 存在 $u,v \in \mathbf{Z}$ 使得 $x = au+bv$, 可知 $d \mid x$, 这表明 $S \subseteq d\mathbf{Z}$. 其次, 设 x_0 是 $S \cap \mathbf{Z}_+$ 的最小元素, 断言: x_0 整除 S 中任何元素 x. 这是由于, 设 x 对 x_0 的带余除法为 $x = qx_0 + r$, $0 \leq r < x_0$, 由 $x, x_0 \in S$ 知 $r = x - qx_0 \in S$. 结合 x_0 是 S 中的最小正元素且 $0 \leq r < x_0$, 只能 $r=0$, 即有 x_0 整除 x, 从而完成了断言的证明.

注意到, $a,b \in S$, 由断言可知 $x_0 \mid x, x_0 \mid b$, 即 x_0 是 a,b 的公因子, 因而有 $x_0 \leq d$; 再由 $x_0 \in S \subseteq d\mathbf{Z}$ 可知 $d \mid x_0$, 即有 $d \leq x_0$. 结合这两个不等式可得 $x_0 = d$, 即 $d \in S$, 进而 $d\mathbf{Z} \subseteq S$. 这样, 既有 $S \subseteq d\mathbf{Z}$ 又有 $d\mathbf{Z} \subseteq S$, 因此 $S = d\mathbf{Z}$. □

命题 3.1.7. *设 a,b,c 是正整数, 满足 $a \mid bc$, 且 a 与 b 互素, 则有 $a \mid c$.*

证明: 设 $bc = am$. 由 Bezout 定理3.1.6知存在整数 u,v, 使得

$$au + bv = (a,b) = 1.$$

由此可得

$$amv = bcv = c(1-au),$$

进而有

$$\frac{c}{a} = mv + cu \in \mathbf{Z},$$

即有 $a \mid c$. □

定理 3.1.8. *每个正整数都可以表示成有限多个素数的乘积, 若不计素因子相乘的顺序则前述分解是唯一的.*

证明: 先证明分解的存在性. 对 n 用归纳法, $n=1$ 时显然成立, 假设 $n<m(m\geq 2)$ 时素因子分解式存在, 考虑 $n=m$ 的情形. 若 m 是素数, 则它可表示为一个素数 m 的积; 若 m 是合数, 则它有异于 $1,m$ 的因子 m_1, 令 $m_2=\frac{m}{m_1}$, 则 $m_1,m_2<m$, 由归纳假设 m_1,m_2 都能分解为素数之积, 把 m_1,m_2 的分解式相乘就得到 m 的分解式.

分解的唯一性. 设 n 有两种分解

$$n=p_1\cdots p_k=q_1\cdots q_l.$$

先证明存在 $q_i=p_1$. 否则的话, 设每个 q_i 都不等于 p_1, 则有 $(p_1,q_i)=1$, 利用 Bezout 定理 (定理3.1.6) 知存在整数 u_i,v_i 使得 $p_1u_1+q_iv_i=1$. 由此可得

$$p_1\cdots p_kv_1\cdots v_l=\prod_{i=1}^{l}(q_iv_i)=\prod_{i=1}^{l}(p_1u_1-1).$$

上式左边可写成 p_1x, 右边展开后可写成 $p_1y+(-1)^l$, 其中 x,y 是整数. 这样就有 $(-1)^l=p_1(x-y)$, 得到 $0<|x-y|=\frac{1}{p_1}\leq\frac{1}{2}$, 矛盾!

适当重排后不妨设 $q_1=p_1$, 则

$$p_2\cdots p_k=q_2\cdots q_l$$

都是 $\frac{n}{p_1}$ 的素因子分解式, 由归纳假设 $\frac{n}{p_1}$ 的素因子分解式是唯一的, 所以 $p_2,\ldots,p_k$ 与 $q_2,\ldots,q_l$ 只相差一个重排. □

一般将 n 的素因子分解式记为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

其中 $p_1,\ldots,p_k$ 是 n 的不同的素因子, 称 α_i 为 n 的素因子 p_i 的个数或重数, 记为 $v_{p_i}(n)=\alpha_i$. 容易验证, 对整数 x,y 与素数 p, 有

$$v_p(xy)=v_p(x)+v_p(y),\quad v_p(x+y)\geq\min\{v_p(x),v_p(y)\}.$$

命题 3.1.9. *设 a,b 的素因子分解式为*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\quad b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k},$$

其中 $p_1,\ldots,p_k$ 是不同的素数, $\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_k$ 是非负整数, 则有

(1) a 与 b 的最大公约数与最小公倍数分别为

$$(a,b)=p_1^{\min\{\alpha_1,\beta_1\}}p_2^{\min\{\alpha_2,\beta_2\}}\cdots p_k^{\min\{\alpha_k,\beta_k\}},\quad [a,b]=p_1^{\max\{\alpha_1,\beta_1\}}p_2^{\max\{\alpha_2,\beta_2\}}\cdots p_k^{\max\{\alpha_k,\beta_k\}}.$$

特别的, 有 $(a,b)[a,b]=ab$.

(2) a 的不同正因子的数目为 $(1+\alpha_1)\cdots(1+\alpha_k)$.

(3) a 的所有正因子的总和为

$$\prod_{i=1}^{k}(1+p_i+\cdots+p_i^{\alpha_i})=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}.$$

证明: (1) 设 x 是 a,b 的公因数, 则 x 的素因子必属于 $\{p_1,\ldots,p_k\}$. 设 $x=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$, 由 $x\mid a, x\mid b$ 可知对每个 i 有 $\gamma_i\le\alpha_i,\gamma_i\le\beta_i$, 即 $\gamma_i\le\min\{\alpha_i,\beta_i\}$. 这样, a,b 的每个公因数都小于等于 $p_1^{\min\{\alpha_1,\beta_1\}}p_2^{\min\{\alpha_2,\beta_2\}}\cdots p_k^{\min\{\alpha_k,\beta_k\}}$, 从而有 $(a,b)=p_1^{\min\{\alpha_1,\beta_1\}}p_2^{\min\{\alpha_2,\beta_2\}}\cdots p_k^{\min\{\alpha_k,\beta_k\}}$.

(2) a 的所有正因子为

$$p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k},\quad 0\le\gamma_i\le\alpha_i,\forall i,$$

共有 $(1+\alpha_1)\cdots(1+\alpha_k)$ 个.

(3) 利用 (2) 中对 a 的所有正因子的描述, 可得

$$\prod_{i=1}^{k}(1+p_i+\cdots+p_i^{\alpha_i})=\sum_{0\le\gamma_1\le\alpha_1,\cdots,0\le\gamma_k\le\alpha_k}p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k},$$

上式右边等于 a 的所有正因子的总和. □

定理 3.1.10 (Euclid). *存在无穷多个不同的素数.*

证明: 用反证法, 假设只有有限多个素数 $p_1,\ldots,p_m$. 考虑 $n=p_1\cdots p_m+1$, 由定理3.1.8 知 n 可分解为至少一个素因子的乘积. 任取 n 的素因子 q, 则 q 不等于 $p_1,\ldots,p_m$ 中的任何一个, 否则的话若 $q=p_i$, 则有 $1=n-p_1\cdots p_m=p_ix-p_iy$, 其中 x,y 是整数, 这显然矛盾! 这样, 我们就找到除 $p_1,\ldots,p_m$ 素数 q, 与假设 $p_1,\ldots,p_m$ 是全部的素数矛盾! □

命题 3.1.11. *对任何正整数 k, 存在连续 k 个数都是合数.*

证明: 考虑 $(k+1)!+2,(k+1)!+3,\ldots,(k+1)!+(k+1)$, 它们是连续的 k 个合数. □

定理 3.1.12 (素数定理). *用 $\pi(n)$ 表示 $1,2,\ldots,n$ 中素数的个数, 则有*

$$\lim_{n\to\infty}\frac{\pi(n)}{n/\ln n}=1.$$

证明: 1896 年, Jacques Hadamard 与 Charles Jean de la Vallee Poussin 独立的证明了素数定理. 1949 年, Atle Selberg 与 Paul Erdös 给出了一个相对初等的证明. □

3.2 同余

例 3.2.1. 称整数 a, b 模 m 同余, 记作 $a \equiv b \pmod{m}$, 如果 $m \mid a-b$.

对于加减法与乘法运算, 人们可以像处理等式一样处理同余式. 设 $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, 则有

$$a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\ m), \quad a_1 - a_2 \equiv b_1 - b_2 (\mathrm{mod}\ m), \quad a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\ m).$$

需要小心的是, 不能将同余式两边的公共因子直接消去, 即从 $ac \equiv bc \pmod{m}$ 不能推出 $a \equiv b \pmod{m}$. 实际上, 只有如下结论.

命题 3.2.2. *设 $ab \equiv ac \pmod{m}$, 则有*

$$b \equiv c \pmod{\frac{m}{(a,m)}}.$$

特别的, 如果 a 与 m 互素, 则从 $ab \equiv ac \pmod{m}$ 可得到 $b \equiv c \pmod{m}$.

证明: 由同余式的定义, 有 $m \mid a(b-c)$, 即

$$\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(b-c).$$

注意到, $\frac{m}{(a,m)}$ 与 $\frac{a}{(a,m)}$ 互素, 则由上式可得

$$\frac{m}{(a,m)} \mid b-c,$$

即有 $b \equiv c \pmod{\frac{m}{(a,m)}}$. □

命题 3.2.3. *设 a 与 m 互素, 则对任何整数 b, 存在唯一的 $x \in \{0, 1, \ldots, m-1\}$ 使得*

$$ax \equiv b \pmod{m}.$$

换句话说, 映射 $f(x) = ax (mod\ m)$ 是集合 $\{0, \ldots, m-1\}$ 上的一个置换.

证明: 对 $i, j \in \{0, \ldots, m-1\}$, 若 $ai \equiv aj \pmod{m}$, 则由命题3.2.2 知 $i \equiv j \pmod{m}$, 因而有 $i = j$. 这就证明了 f 是单射, 有限集到自身的单射也是满射, 所以 f 是双射. □

定理 3.2.4 (Fermat 小定理)**.** *设 p 是素数, 则对任何整数 a, 有 $a^p \equiv a \pmod{p}$.*

证明: 只需考虑 a 与 p 互素的情形. 此时, 由命题3.2.3 可知 $f(x) = ax (\mathrm{mod}\ p)$ 建立了从 $\{1, \ldots, p-1\}$ 到其自身的双射. 换句话说,

$$f(1) (\mathrm{mod}\ p), \cdots, f(p-1) (\mathrm{mod}\ p)$$

是 $1,\ldots,p-1$ 的一个重新排列. 由此可得

$$\prod_{i=1}^{p-1}(ai) \equiv 1\cdot 2\cdot\cdots\cdot(p-1) \pmod{p},$$

两边同消去与 p 互素的项 $1\cdot 2\cdot\cdots\cdot(p-1)$, 即得到 $a^{p-1}\equiv 1 \pmod{p}$.

□

证法二. 先证明对 $0<k<p$ 有 $p \mid C_p^k$. 注意到, 对 $0<k<p$, 有

$$kC_p^k = \frac{p!}{(k-1)!(p-k)!} = pC_{p-1}^{k-1}.$$

由二项式系数的组合含义知 C_{p-1}^{k-1} 是整数, 因而有 $p \mid kC_p^k$. 结合 k 与 p 互素, 即得 $p \mid C_p^k$.

这样, 对整数 $a\geq 1$, 有

$$a^p = ((a-1)+1)^p = \sum_{k=0}^{p} C_n^k (a-1)^{p-k} \equiv (a-1)^p + 1 \pmod{p}.$$

由此即得

$$a^p \equiv (a-1)^p + 1 \equiv (a-2)^p + 2 \equiv \cdots \equiv 1^p + (a-1) \equiv a \pmod{p}.$$

□

注 3.2.5. 在上述证法二中, 我们证明了对素数 p 有

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

定义 3.2.6. 设 n 是正整数, 用 $\varphi(n)$ 表示 $1,2,\ldots,n$ 中与 n 互素的数的个数, 称 $\varphi(n)$ 为 Euler 函数.

命题 3.2.7. *设正整数 n 的素因子分解式为 $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, 其中 $p_1,\ldots,p_k$ 是互不相同的素数, $\alpha_1,\ldots,\alpha_k$ 是正整数, 则有*

$$\varphi(n) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}) = n\prod_{\text{素数}p\mid n}(1-\frac{1}{p}).$$

定理 3.2.8 (Euler 定理)**.** *设 m 是正整数, 则对与 m 互素的整数 a, 有*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

证明: 令 $C = \{1 \le x \le m | (x,m) = 1\}$, 则对 $x \in C$, 有 $f(x) = ax (\mathrm{mod}\ m)$ 与 m 互素, 即 f 将 C 的元素映射到 C 中. 由命题3.2.3 可知 f 诱导 A 到 A 的双射, 换句话说即 $\{f(x)|x \in C\}$ 是 C 的一个排列, 由此可得

$$\prod_{x\in C}(ax) \equiv \prod_{x\in C} f(x) = \prod_{x\in C} x \pmod m,$$

两边同消去与 m 互素的项 $\prod_{x\in C} x$, 即得到 $a^{|C|} \equiv 1 \pmod m$. □

3.3 剩余系

定义 3.3.1 (等价关系)**.** 所谓集合 X 上的一个等价关系是指 $X \times X$ 的一个子集 R, 要求 R 满足如下三个条件:

(1)(自反性) 对任何 $x \in X$, 有 $(x,x) \in R$;

(2)(对称性) 如果 $(x,y) \in R$, 则 $(y,x) \in R$;

(3)(传递性) 如果 $(x,y),(y,z) \in R$, 则 $(x,z) \in R$.

如果 $(x,y) \in R$, 则称 x 与 y 等价, 记为 $x \sim y$. 这样, 等价关系的上述三条性质就可以表述为: (1) 对任何 $x \in X$ 有 $x \sim x$; (2) 若 $x \sim y$ 则 $y \sim x$; (3) 若 $x \sim y$ 且 $y \sim z$, 则 $x \sim z$.

例 3.3.2. 给定正整数 n, 则模 n 同余给出 $\mathbf{Z}$ 上的一个等价关系: 定义 $x \sim y$ 当且仅当 $x \equiv y \pmod n$.

例 3.3.3. 设 $\sim$ 是 X 上的一个等价关系, 对每个 $x \in X$, 称集合

$$\{y \in X | y \sim x\}$$

为 x 在此等价关系下所在的等价类, 记为 $[x]$.

命题 3.3.4. *任何两个等价类或者不相交, 或者相等. 进而可知, X 被分拆称为若干个彼此不相交的等价类的并集.*

证明: 设 $[x]$ 与 $[y]$ 相交非空, 来证明 $[x] = [y]$. 为此, 取 $z \in [x] \cap [y]$, 则有

$$x \sim z, \quad z \sim y,$$

由传递性可得 $x \sim y$. 这样, 对任何 $w \in X$ 有

$$w \sim x \iff w \sim y,$$

即有 $[x] = [y]$. □

定义 3.3.5. 设 $\sim$ 是 X 上的一个等价关系, 用 $X/\sim$ 表示所有等价类所构成的集合, 称为 X 在等价关系 $\sim$ 下的商集.

定义 3.3.6. 模 n 给出 $\mathbf{Z}$ 上的等价关系: $x\sim y \iff x\equiv y \pmod n$. 称 $\mathbf{Z}$ 在此等价关系下的商集 $\mathbf{Z}/\sim$ 为 "整数模 n 所得的环", 记为 $\mathbf{Z}/n\mathbf{Z}$, 或 $\mathbf{Z}/n$, 或 $\mathbf{Z}_n$. 它有 n 个元素, 分别是模 n 余 $0,1,\ldots,n-1$ 的所有数构成的等价类:

$$\begin{aligned}
&[0]=\{\ldots,-n,0,n,\ldots\},\\
&[1]=\{\ldots,-n+1,1,n+1,\ldots\},\\
&\cdots\cdots\\
&[n-1]=\{\ldots,-1,n-1,2n-1,\ldots\}.
\end{aligned}$$

$\mathbf{Z}_n$ 上有加法与乘法两种运算, 分别定义为:

$$[x]+[y]=[x+y],\quad [x]\cdot[y]=[xy].$$

由命题3.2.3, 当 a 与 n 互素时, 同余方程 $ax\equiv 1 \pmod n$ 有唯一的解 $x\in\{1,\ldots,n-1\}$. 对此 x, 有

$$[a]\cdot[x]=[x]\cdot[a]=[1],$$

称 $[x]$ 为 $[a]$ 在模 n 下乘法的逆元, 记作 $[a]^{-1}$. 当 a 与 n 不互素时, 同余方程 $ax\equiv 1 \pmod n$ 无解, $[a]$ 没有逆元. 特别的, 若 n 是素数 p, 则 $\mathbf{Z}_p$ 中的非零元都有乘法下的逆元, 所以人们称 $\mathbf{Z}_p$ 是一个域.

数论的中心问题之一是求解不定方程. 设 $f(x_1,\ldots,x_m)$ 是给定的多项式, 人们关心有哪些整数组 $(x_1,\ldots,x_m)$ 满足

$$f(x_1,\ldots,x_m)=0.$$

处理不定方程的基本方法是模一个素数 p 考虑: 若 $(x_1,\ldots,x_m)$ 满足上述方程, 则

$$f(x_1,\ldots,x_m)=0 \pmod p,$$

即 $([x_1],\ldots,[x_m])\in(\mathbf{Z}_p)^m$ 满足

$$f([x_1],\ldots,[x_m])=[0]\in\mathbf{Z}_p,$$

因而是 f 在 $\mathbf{Z}_p$ 中的解. 这样, 为了求解 f 在 $\mathbf{Z}$ 中的解, 人们需要先在 $\mathbf{Z}_p$ 中求解 f, 由此获得 f 在 $\mathbf{Z}$ 中解的信息.

例 3.3.7 ($\mathbf{Z}_p$ 中的线性方程组)**.** 由于 $\mathbf{Z}_p$ 中非零元都有逆, 求解线性方程组的 Gauss 消元法对于 $\mathbf{Z}_p$ 中的线性方程组仍然有效.

第四章　图论

4.1　图

定义 4.1.1. 所谓一个图是指一个有序对 $G=(V,E)$, 其中 V 是一个集合, 称其元素为图 G 的顶点; E 是由 V 的若干个 2 元子集所构成的子集族, 称其成员 $\{v,w\}$ 为图 G 的边, 也将它记为 "边 vw".

若 $\{v,w\}\in E$, 则称 v 与 w 相邻, 并称 w 为 v 的邻点. 称顶点 v 处连出的边的数目为 v 的度, 记作 $\deg(v)$ 或 $d(v)$.

例 4.1.2. (1) 如果 G 共有 n 个顶点, 则称 G 是一个 n 阶图.

(2) 称 G 是 n 阶完全图, 如果 G 共有 n 个顶点, 且任何两个顶点之间都有边. 将 n 阶完全图记为 K_n.

(3) 对于图 $G=(V,E)$, 定义图 $\overline{G}=(V,E^c)$, 它与 G 有相同的顶点集, 它的边集与 G 的边集互为补集. 称 $\overline{G}$ 为 G 的补图.

(4) 称图 $G_1=(V_1,E_1)$ 是图 $G=(V,E)$ 的一个子图, 如果 $V_1\subseteq V$ 且 $E_1\subseteq E$. 换句话说, 取出 V 的子集 V_1 作为顶点集, 并在 G 的端点位于 V_1 中的那些边中选出一部分作为边集, 就得到一个子图.

(5) 称图 $G_1=(V_1,E_1)$ 是图 $G=(V,E)$ 的一个诱导子图, 如果 $V_1\subseteq V$, 且

$$E_1=\{e\in E|e\text{ 的端点都在}V_1\text{ 中}\}.$$

换句话说, 取 V 的子集 V_1 作为顶点集, 并把 G 的端点在 V_1 中那些边全部取出作为边集, 就得到一个诱导子图. 一般将此诱导子图记为 $G[V_1]$.

命题 4.1.3 (握手定理)**.** 图 G 中所有顶点的度数之和等于边数的 2 倍, 即

$$\sum_{v\in V}\deg(v)=2|E|.$$

特别的, 奇度顶点的个数为偶数.

证明: 利用 $\deg(v)$ 的定义, 有

$$\deg(v) = \sum_{e\in E \text{ 且} v\in e} 1,$$

由此可得

$$\sum_{v\in V}\deg(v) = \sum_{v\in V}\sum_{e\in E \text{ 且} v\in e} 1 = \sum_{e\in E}\sum_{v\in e} 1 = \sum_{e\in E} 2 = 2|E|.$$

□

定义 4.1.4. 设 x, y 是图 G 的顶点, 所谓一条从 x 到 y 的道路是指顶点序列

$$x = v_0, v_1, \ldots, v_k = y,$$

要求 $v_0v_1, \cdots, v_{k-1}v_k$ 都是图 G 的边. 称 x, y 为上述道路的端点, 称上述道路的长度为 k.

如果 $x = y$, 则称上述道路为一条长为 k 的圈.

没有重复顶点的道路称为简单道路; 除了起点与终点相同外没有重复顶点的道路称为简单圈. 以后我们说道路与圈的时候, 一般指的是简单道路与简单圈.

命题 4.1.5. (1) 如果图 G 中每个顶点的度都大于 1, 则 G 中存在简单圈.

(2) 如果图 G 中每点的度都是偶数, 且 G 至少含有一条边, 则 G 有简单圈.

(3) 如果 $|E| \geq |V|$, 则图中必有简单圈.

证明: (1) 考虑 G 中最长的简单道路 $v_0v_1\ldots v_k$, 不妨设 $v_k \neq v_0$. 由于 v_k 至少两个邻点, 它有异于 v_{k-1} 的邻点 x. 若 $x \notin \{v_0, \cdots, v_{k-1}\}$, 则得到更长的简单路 $v_0v_1\ldots v_kx$, 矛盾! 若 x 等于某个 $v_i (i < k-1)$, 则得到圈 $v_iv_{i+1}\ldots v_kv_i$.

(2) 删去所有孤立顶点, 所得的非空的图中每点的度至少为 2, 利用 (1) 的结论可知其中有圈.

(3) 若每点的度至少为 2, 则由 (1) 知图中有圈. 假设存在顶点 x 使得 $\deg(x) \leq 1$. 删去 x 得到图 G', 则 $|E'| \geq |E| - 1 \geq |V| - 1 = |V'|$, 对 G' 使用归纳假设可知其中有圈. □

定义 4.1.6. 称图 G 是连通图, 如果对 G 的任何两个顶点 x, y, 都存在从 x 到 y 的道路.

对一般的图 G, 可定义 V 上的一个等价关系: $x \sim y$ 当且仅当存在从 x 到 y 的道路. 称此等价关系下的等价类为 G 的连通分支, 将 G 的连通分支的数目记为 $\beta_0(G)$.

命题 4.1.7. (1) 若 G 是连通图, 则 $|E| \geq |V| - 1$.

(2) 对一般的图 G, 有 $\beta_0(G) \geq |V| - |E|$.

证明: (1) 对 G 的顶点数 $|V|$ 归纳. 当 $|V| = 1$ 时, 命题显然成立. 考虑 $|V| > 1$ 的情形. 如果 G 中每个顶点的度都大于 1, 则有

$$|E| = \frac{1}{2}\sum_{v\in V}\deg(v) \geq \frac{1}{2}\sum_{v\in V} 2 = |V|.$$

以下假设存在 $\deg(v) \le 1$. 由 G 连通及 $|V| > 1$, 可知 $\deg(v) = 1$. 设 x 的唯一的邻点为 y, 删去顶点 x 与边 $\{x, y\}$ 得到图 $G' = (V', E')$. 易验证 G' 也连通, 由归纳假设有 $|E'| \ge |V'| - 1$. 注意到 $|V'| = |V| - 1$, $|E'| = |E| - 1$, 因而有 $|E| \ge |V| - 1$. □

定义 4.1.8. 图 G 的一个欧拉路是指通过每条边都恰好一次的道路. 如果欧拉路的起点与终点相等, 则称之为一个欧拉圈.

定理 4.1.9. *连通图 G 有欧拉路的充分必要条件是: 图中奇度顶点的数目为 0 或者 2. 进一步, 当奇度顶点的数目为 2 时, 欧拉路的起点和终点都是奇度顶点; 当奇度顶点的数目为 0 时, 欧拉路的起点和终点重合, 构成欧拉圈.*

证明: "⇒" 设 G 有欧拉路, 对于欧拉路的中间顶点 (非起点与终点)v, 每次到达 v 后必须马上离开 v, 因而 $\deg(v)$ 是偶数. 这样, 奇度顶点至多两个. 由握手定理, 奇度顶点的数目是偶数, 所以只能是 0 或 2.

"⇐" 设图 G 中奇度顶点的数目是 0 或 2, 来证明存在欧拉路. 先考虑 G 没有奇度顶点的情形. 由命题4.1.5, 存在简单圈 C, 删去 C 后所得的图分解成若干个连通分支之并 $G_1 \cup \cdots \cup G_k$. 显然 G_i 中每点的度都是偶数, 由 (对边数的) 归纳假设可知每个 G_i 都有欧拉圈. 由于 G 是连通的, 每个 G_i 与 C 必有公共顶点, 任意选取 G_i 与 C 的一个公共点 v_i. 现在可按如下方式得到 G 的欧拉圈: 任选 C 的顶点 v, 从 v 出发沿着 C 走, 对每个 i, 第一次到达 v_i 后, 沿着 G_i 的欧拉圈走一圈回到 v_i, 再继续沿着 C 前进, 最后回到 v.

再考虑 G 有两个奇度顶点 x, y 的情形. 如果 xy 不是边, 则添加一条新边 xy 得到图 G', G' 中每点的度都是偶数, 因而有欧拉圈, 在此欧拉圈中删去新边 xy 即得到 G 的一个欧拉路. 如果 xy 是 G 的边, 则删去 xy 得到图 G'', G'' 中每点的度都是偶数. 设 G'' 分解为若干个连通分支的并 $G'' = G_1 \cup \cdots \cup G_k$, $C = xy$, 则与前一情形的证明类似, 每个 G_i 都有欧拉圈, 且 G_i 都与 C 有公共顶点. 这样, 可沿着 C 走, 并把所有 $G_1, \cdots, G_k$ 的欧拉圈接成 G 的欧拉圈. □

4.2 树

称简单图 T 是一棵树 (*tree*), 如果 T 是连通的, 且没有圈. 称若干棵树的不交并为一个森林 (*forest*).

定理 4.2.1. (1) *简单图 T 是树的充分必要条件是: T 连通, 且删去任何一条边之后不再连通.*

(2) *简单图 T 是树的充分必要条件是: T 无圈, 且再增添任何一条边之后图中就有圈.*

证明: (1) "⇒" 设 T 是树, 来证明 T 删去任何一条边之后不再连通. 用反证法, 假设存在边 $e = xy$ 使得删去 e 之后所得的图 G' 连通. 由于 G' 连通, x, y 在 G' 中有道路相连, 取出 G' 中

从 x 到 y 的最短道路 P. 由于 P 的最短性可知其顶点互不相同, 这样 P 与 e 在 T 中构成一个简单圈, 与 T 是树矛盾!

"⇐" 设 T 连通且删去任何一条边之后不再连通, 来证明 T 无圈. 假设 T 有圈 C, 则任意删去圈 C 的一条边 e 之后所得的图 G' 仍然连通. 这是因为, 如果 T 中从 x 到 y 的道路中含有边 e, 则可把该道路中的所有 e 都替换成道路 $C\backslash\{e\}$, 得到 G' 中从 x 到 y 的道路.

(2)"⇒" 设 T 是树, 来证明 T 再增添任何一条边之后图中就有圈. 设 xy 不是 T 的边, 由于 T 连通, 其中存在连接 x, y 的道路. 取出 T 中从 x 到 y 的最短道路 P, 则在增添边 xy 后所得的图中 P 与 xy 构成一个简单圈.

"⇐" 设 T 无圈, 且再增添任何一条边之后图中就有圈, 来证明 T 连通. 用反证法, 假设 T 不连通, 在 T 的某两个连通分支中各取一个顶点 x, y, 则 xy 不是 T 的边. 由条件增添边 $e = xy$ 后有圈 C, 则 $C\backslash\{e\}$ 是连接 x, y 的道路, 这与 x, y 位于不同的连通分支矛盾! □

命题 4.2.2. *树中任何两个不同顶点之间有唯一的简单路相连.*

证明: 设 x, y 是树 T 的两个顶点. 由于 T 连通, 存在 x 到 y 的道路. 取出从 x 到 y 的最短道路, 可知它是简单道路. 这表明 x, y 之间有简单路相连.

再证明 x, y 之间的简单路唯一. 用反证法, 设 x, y 之间有两个不同的简单道路:

$$P = xu_1 \cdots u_{k-1}y, \quad Q = xv_1 \cdots v_{l-1}y,$$

不妨设 $u_1 \neq v_1$, 否则的话考虑从 $u_1 = v_1$ 到 y 的简单路的唯一性. 若 $\{u_1, \cdots, u_{k-1}\}$ 与 $\{v_1, \cdots, v_{l-1}\}$ 不相交, 则 $xu_1 \cdots u_{k-1}yv_{l-1} \cdots v_1x$ 是简单圈, 与 T 无圈矛盾! 若 $\{u_1, \cdots, u_{k-1}\}$ 与 $\{v_1, \cdots, v_{l-1}\}$ 相交, 考虑使得 $u_i = v_j$ 成立且使 $i+j$ 最小的指标对 (i, j), 则 $\{u_1, \cdots, u_{i-1}\}$ 与 $\{v_1, \cdots, v_{j-1}\}$ 不相交, 得到 $xu_1 \cdots u_{i-1}u_iv_{j-1} \cdots v_1x$ 是长度为 $i + j \geq 3$ 的简单圈, 也与 T 无圈矛盾!

□

命题 4.2.3. (1) *设 T 是树, 则 $|E| = |V| - 1$.*

(2) *设树 T 至少有两个顶点, 则 G 中存在两个度为 1 的顶点.*

(3) *每棵树可以通过如下方法构造出: 从一个顶点出发, 每次新增一个顶点, 并新增一条从新顶点到某个已有顶点的边.*

证明: (1) 结合命题4.1.5与命题4.1.7即可.

(2) 否则的话, 有

$$2|V| - 2 = 2|E| = \sum_{v \in V} \deg(V) \geq 1 + 2(|V| - 1) = 2|V| - 1,$$

矛盾!

(3) 利用 (2) 的结论, 存在顶点 x 使得 $\deg(x) = 1$(这种顶点称为树的 leaf). 删去 x 以及 x 连出的唯一的那条边, 得到图 T', 则 T' 无圈且连通, 即 T' 也是树. 利用归纳假设知 T' 可由 (3) 中所述的方式构造出, 在此基础上最后添加顶点 x, 即得到 T 的满足要求的构造方式. □

定理 4.2.4 (Cayley)**.** 顶点标号为 $1, 2, \ldots, n$ 的 n 阶树的数目为 n^{n-2}.

算法 4.2.5 (普吕弗 (Prüfer) 序列)**.** 设 T 是顶点标号为 $1, 2, \ldots, n$ 的 n 阶树, 按如下算法给出 T 的普吕弗 *(Prüfer)* 序列 $P(T)$*:* 令 $T_1 = T$. 在第 i 步, 找出 T_i 的标号最小的 *leaf* x_i, 找出 x_i 在 T_i 中的唯一的邻点 y_i. 在 T_i 中删去顶点 x_i 以及它连出的边 x_iy_i 得到树 T_{i+1}. 如此 $n-1$ 步后得到 1 阶树 T_n. 称序列 $(y_1, y_2, \cdots, y_{n-2})$ 为 T 的普吕弗 *(Prüfer)* 序列, 记为 $P(T)$.

普吕弗序列有如下性质:

- $\{x_1, x_2, \cdots, x_{n-1}, y_{n-1}\} = [n]$ 且 $y_{n-1} = n$. 这是由于对 $1 \le i \le n-1$, 树 T_i 都是至少 2 阶的, 因而有至少两个 leaf, 其 leaf 的最小标号 x_i 不等于 n.
- T_k 的顶点集为 $\{x_k, \cdots, x_{n-1}, y_{n-1}\}$, 边集为 $\{x_ky_k, \cdots, x_{n-1}y_{n-1}\}$.
- 设 v 是 T_k 的顶点, 即 $v \ne x_1, \cdots, x_{k-1}$, 则 v 在 T_k 中的度为

$$d_{T_k}(v) = 1 + (v \text{ 在} \{y_k, \cdots, y_{n-2}\} \text{ 中出现的次数}).$$

  由此可得: v 是 T_k 的 leaf, 当且仅当 $v \notin \{x_1, \cdots, x_{k-1}\} \cup \{y_k, \cdots, y_{n-2}\}$.

- 对 $1 \le k \le n-1$, x_k 是不属于 $\{x_1, \cdots, x_{k-1}\} \cup \{y_k, \cdots, y_{n-2}\}$ 的最小正整数.
- 普吕弗序列是从顶点标号为 $1, 2, \ldots, n$ 的 n 阶树的集合 $\mathcal{T}$ 到 $[n]^{n-2}$ 的单射.

算法 4.2.6 (从普吕弗序列重构树)**.** 设 $(y_1, \cdots, y_{n-2}) \in [n]^{n-2}$ 是任何序列, 递归的定义 $x_1, \cdots, x_{n-1}$ 为*:* x_k 是不属于 $\{x_1, \cdots, x_{k-1}\} \cup \{y_k, \cdots, y_{n-2}\}$ 的最小正整数. 再令 $y_{n-1} = n$. 这么定义出的序列 $x_1, \cdots, x_{n-1}$ 满足如下性质*:*

- $x_1, x_2, \cdots, x_{n-1}$ 两两不同且都小于 n, 从而有 $\{x_1, x_2, \cdots, x_{n-1}, y_{n-1}\} = [n]$.
- 对 $1 \le l \le n-2$, 有 $y_l \notin \{x_1, \cdots, x_l\}$, 从而可得 $y_l \in \{x_{l+1}, \cdots, x_{n-1}, y_{n-1}\}$.
- 定义图 G_k 为*:* 顶点集为 $\{x_k, \cdots, x_{n-1}, y_{n-1}\}$, 边集为 $\{x_ky_k, \cdots, x_{n-1}y_{n-1}\}$, 则 G_k 是由 G_{k+1} 在其顶点 y_k 向图外新增一条悬挂边得到. 由此可得每个 G_k 都是树, 特别的 G_1 是 n 阶树.
- $P(G_1) = (y_1, \cdots, y_{n-2})$, 由此说明普吕弗序列是从顶点标号为 $1, 2, \ldots, n$ 的 n 阶树的集合 $\mathcal{T}$ 到 $[n]^{n-2}$ 的满射.

由这两个算法可知, 普吕弗序列给出从顶点标号为 $1,2,\ldots,n$ 的 n 阶树的集合 $\mathfrak{T}$ 到 $[n]^{n-2}$ 的一一对应, 从而证明了 Cayley 定理. 除此之外, 普吕弗序列还有如下用途:

- 给出了树 T 的最有效的存储方法, 只需记录其吕弗序列 $P(T)$, 即可利用算法4.2.6重构 T. 这样, 只需要 $(n-2)\lceil\log_2(n+1)\rceil$ 个字节就可以存储 T 的全部信息.
- 给出了生成随机树的办法: 只需随机生成序列 $(y_1,\ldots,y_{n-2})\in[n]^{n-2}$ 即可得到一棵随机树.

定义 4.2.7. 设 $G=(V,E)$ 与 $G'=(V',E')$ 是两个图, 称 G 与 G' 同构, 记为 $G\cong G'$, 如果存在双射 $f:V\to V'$, 使得对任何 $x,y\in V$, 有

$$\{x,y\}\in E \iff \{f(x),f(y)\}\in E'.$$

定义 4.2.8. 选定了一个 (特殊) 顶点的树称为一棵有根树 (*rooted tree*), 并称选定那个顶点为根 (*root*).

设 T 是有根树, r 是根. 由命题4.2.2, 对每个顶点 $v\neq r$, 存在从 v 到 r 的唯一的简单路. 定义 $d(v,r)$ 为此简单路的长度, 可依照 $d(v,r)$ 的值将 T 的顶点分层:

$$V(T)=\cup_{i=0}^{\infty}V_k,\quad V_k=\{v\in V(T)|d(v,r)=k\}.$$

在此分层下, 每个 $v\in V_k(k>1)$ 的邻点中恰有一个属于 V_{k-1}, 其他邻点属于 V_{k+1}.

定理 4.2.9. *设顶点不带标号的 n 个顶点的树一共有 T_n 棵 (即不区分彼此同构的树), 则有*

$$\frac{n^{n-2}}{n!}\le T_n\le 4^{n-1}.$$

证明: 用 $\mathfrak{T}$ 表示顶点集合为 $[n]$ 的树所构成的集合, 在其上定义等价关系:

$$T\sim T' \iff T\cong T',$$

则 $T_n=|\mathfrak{T}/\!\sim|$ 是等价类的个数. 对于每个等价类 $[T]$, $T'\in[T]$ 当切仅当 T' 与 T 是同构的图, 即存在顶点集合之间的双射 $\alpha:[n]\to[n]$ 使得

$$x,y \text{ 在}T \text{ 中相邻} \iff \alpha(x),\alpha(y) \text{ 在}T' \text{ 中相邻},$$

即有 T' 的边集等于

$$E'=\{\alpha(x)\alpha(y)|xy\in E\}=\alpha(E).$$

注意到共有 $n!$ 个不同的双射 α 且不同的 α 有可能给出相同的 $\alpha(E)$, 故每个等价类 $[T]$ 的元素个数不超过 $n!$. 由此可得

$$n^{n-2} = |\mathfrak{T}| = \sum_{[T]} |[T]| \leq \sum_{[T]} n! = n! \cdot T_n,$$

即有 $\frac{n^{n-2}}{n!} \leq T_n$.

T_n 上界的估计要用到所谓的 $p$lanar code. □

4.3 图上的优化算法

定义 4.3.1. 设 G 是连通图, 称 G 的子图 T 是 G 的一棵生成树, 如果 T 是树且 T 包含 G 的所有顶点.

推论 4.3.2. 每个连通图都有生成树.

证明: 设 G 是连通图. 若删去 G 的任何边之后所得图都不连通, 则 G 是树, 它是自身的生成树. 若存在 G 的边 e 使得删去 e 之后所得的图 G' 连通, 则由 (对边数的) 归纳假设可知 G' 有生成树 T, 显然 T 也是 G 的生成树. □

定义 4.3.3. 所谓一个加权图 (*weighted graph*) 是指一个图 $G = (V, E)$ 以及其边集上的一个函数 $f : E \to \mathbf{R}$. 称 $f(e)$ 为边 e 的权或花费.

问题 4.3.4. 给定加权的连通图 G. 如何找出它的生成树 T, 使得 T 的总花费

$$c(T) = \sum_{e \in T} f(e)$$

最小? 称这样的 T 为最便宜的生成树.

算法 4.3.5 (贪婪算法)**.** 在保持 T 无圈的条件下选权最小的边入选 T. 具体的说, 可执行如下算法. 令 $T_0 = D_0 = \emptyset$, 对每个 $i \geq 1$, 令 e 为 $E \backslash (T_{i-1} \cup D_{i-1})$ 中权最小的边, 若权最小的边不唯一, 则任选其中一条. 若 $T_{i-1} \cup \{e\}$ 中不存在简单圈, 则令 $T_i = T_{i-1} \cup \{e\}$, $D_i = D_{i-1}$; 若 $T_{i-1} \cup \{e\}$ 存在简单圈, 则令 $T_i = T_{i-1}$, $D_i = D_{i-1} \cup \{e\}$. 当 $T_k \cup D_k = E$ 时终止算法, 输出 $T = T_k$.

定理 4.3.6. 算法*4.3.5*给出的 T 是最便宜的生成树. 如果所有边的权互不相同, 则最便宜的生成树是唯一的.

证明: 算法4.3.5可简单叙述为: 在保持 T 无圈的条件下选权最小的边入选 T. 由此可知算法最终输出的 T 无圈. 注意我们约定 T 的顶点集合为 $V(G)$, 只是用贪婪算法确定其边集. 若最终输出的 T 不连通, 设有至少两个连通分支 T_1, T_2, 由于 G 连通知存在边 e 的两个顶点分别在 T_1, T_2 中, 在考虑 e 时选 e 入 T 不会产生圈, 故 $e \in T$, 这与 T_1, T_2 是连通分支矛盾! 这样, T 是包含 G 所有顶点的无圈连通图, 即是 G 的一个生成树.

下面来证明贪婪算法给出的生成树 T 是最便宜的. 设 A 是 G 的任何生成树, 来证明 $c(T) \leq c(A)$. 将 A 的边按照权重递增的顺序记为 $A = \{a_1, \ldots, a_m\}$, 将 T 的边按照入选 T 的早晚顺序记为 $T = \{e_1, \ldots, e_m\}$. 我们来证明对每个 i 都有 $c(e_i) \leq c(a_i)$, 由此即得到 $c(T) \leq c(A)$. 用反证法, 假设

$$c(e_i) > c(a_i) \geq c(a_{i-1}) \geq \cdots \geq c(a_1).$$

在不引起混淆的情况下, 我们也用 T_i 表示图 $(V(G), T_i = \{e_1, \ldots, e_i\})$, 用 A_i 表示图 $(V(G), A_i = \{a_1, \ldots, a_i\})$. 注意到, e_i 是端点属于 T_{i-1} 的不同连通分支的那些边中权重最小的那条边, 由此可得对 $1 \leq j \leq i$ 有 a_j 的端点属于 T_{i-1} 的同一连通分支. 由此可得 A_i 的连通分支的数目不小于 T_{i-1} 的连通分支的数目. 对于无圈图 H, 有 $\beta_0(H) = |V(H)| - |E(H)|$, 则前述表明

$$|V(G)| - i = \beta_0(A_i) \geq \beta_0(T_{i-1}) = |V(G)| - (i-1),$$

矛盾! □

定义 4.3.7. 设 G 是图, 称经过 G 的每个顶点一次并回到起点的简单圈为 G 的哈密尔顿圈.

问题 4.3.8 (旅行商问题, Travelling salesman problem)**.** *设 $G = K_n$ 是带非负权的加权图, 如何找出 G 的总权最小的哈密尔顿圈?*

一般的旅行商问题非常复杂, 我们这里假设权重满足三角不等式: 对任何三个顶点 x, y, z 有

$$f(xy) + f(yz) \geq f(xz).$$

算法 4.3.9 (Tree Shortcut)**.** *找出 G 的最便宜生成树 T, 保持 T 在右手边绕着 T 走一圈, 得到一条经过每个顶点至少一次的道路 C. 之后再修改 C: 选定 C 的一点前进. 若有 C 的相继两边 xy, yz 且 y 是之前已经访问过顶点, 则修改 xy, xz 为一条边 xz. 到无法再修改时, 就得到一个哈密尔顿圈.*

定理 4.3.10. *设 K_n 的权非负的且满足三角不等式, 则上述 Tree Shortcut 算法给出的哈密顿圈的总权不超过图中最便宜哈密尔顿圈总权的两倍.*

证明: 设 Tree Shortcut 算法给出的哈密顿圈为 D, 图中最便宜哈密尔顿圈为 D_0. 由三角不等式, 每一次两边换成一边的修改后总权不增, 由此可得

$$c(D) \leq c(C) = 2c(T).$$

取 D_0 的任何一边 e, 则 $D_0\backslash\{e\}$ 是 G 的生成树, 因而有

$$c(T) \leq c(D_0\backslash\{e\}) \leq c(D_0).$$

结合起来即得到 $c(D) \leq 2c(D_0)$.

□

4.4 完全匹配

定义 4.4.1. 称图 G 是二部分图, 如果可将 $V(G)$ 表示成两个子集的不交并 $V(G) = A \cup B$, 使得 A 中的顶点彼此不相邻且 B 中的顶点也彼此不相邻. 将这样的二部分图记作 $G = (A, B, E)$.

定义 4.4.2. 设 $G = (A, B, E)$ 是二部分图, 所谓 G 的一个匹配, 是指 E 的子集 M, 要求 M 的成员彼此没有公共顶点. 称匹配 M 是从 A 到 B 的完全匹配, 如果对 A 中每点 a, M 中都有以 a 为顶点的边. 进一步, 称 M 是完美匹配 (*p*erfect matching), 如果每个顶点是 M 中某边的端点.

对 $S \subseteq A$, 定义

$$N(S) = \{b \in B | \exists a \in S \text{ 使得} ab \in E\},$$

它是 S 的点的所有邻点所构成的集合.

定理 4.4.3 (Hall)**.** *设 $G = (A, B, E)$ 是二部分图, 存在从 A 到 B 的完全匹配的充分必要条件是: 对任何 $S \subseteq A$, 都有 $|N(S)| \geq |S|$.*

证明: 必要性. 设 M 是从 A 到 B 的完全匹配. 设 M 中以 $a \in A$ 为左端点的边为 $af(a) \in M$, 则 f 给出了单射 $f : A \to B$, 满足对任何 $a \in A$ 有 $af(a) \in M$. 对任何 $S \subseteq A$, 有 $f(S) \subseteq N(S)$. 结合 f 是单射可得

$$|N(S)| \geq |f(S)| = |S|.$$

必要性. 设对任何 $S \subseteq A$ 都有 $|N(S)| \geq |S|$, 来证明存在从 A 到 B 的完全匹配. 我们对 $|A|$ 归纳. $|A| = 1$ 的情形命题显然成立. 假设当 $|A| < n$ 时命题成立, 来考虑 $|A| = n$ 的情形. 分两种情况讨论.

(1) 如果存在 A 的非空真子集 S 使得 $|N(S)| = |S|$. 对二部分图 $S \cup N(S))$ 用归纳假设可知它有从 S 到 $N(S)$ 的完全匹配 M_1. 再考虑二部分图 $G' = (A' = A\backslash S, B' = B\backslash N(S))$, 对任

何 $T \subseteq A\backslash S$, 设 T 在 B' 中的邻点集合为 N', 则 $S \cup T$ 在 B 中的邻点集为 $N(S) \cup N'$, 由条件有 $|N(S) \cup N'| \geq |S \cup T|$, 可得 $|N'| \geq |T|$. 对 G' 用归纳假设可知它有从 A' 到 B' 的完全匹配 M_2. 这样就找到从 A 到 B 的完全匹配 $M_1 \cup M_2$.

(2) 如果对 A 的非空真子集 S 都有 $|N(S)| \geq |S| + 1$. 任取 $a \in A$ 以及它的邻点 b. 对任何非空子集 $S \subseteq A\backslash\{a\}$, 有 $|N(S)| \geq |S| + 1$, 可知 $|N(S)\backslash\{b\}| \geq |S|$. 对二部分图 $G' = (A\backslash\{a\}, B\backslash\{b\})$ 用归纳假设可知它有从 $A\backslash\{a\}$ 到 $B\backslash\{b\}$ 的完全匹配. 再添上边 ab 就得到从 A 到 B 的完全匹配. □

推论 4.4.4. *设 G 是二部图且所有顶点的度都相等, 则 G 有完美匹配.*

证明: 设 $G = A \cup B$, 且每个顶点的度都等于 d. 图 G 的边数为

$$d \cdot |A| = \sum_{a \in A} \deg(a) = |E| = \sum_{b \in B} \deg(b) = d \cdot |B|,$$

可知 $|A| = |B|$. 对 A 的任何子集 S, S 的点只能连边到 $N(S)$ 中. 考虑从 S 到 $N(S)$ 所连边的数目, 可得

$$d \cdot |S| = \sum_{a \in S} \deg(a) = \sum_{b \in N(S)} \#\{b \text{ 在} S \text{ 中的邻点}\} \leq \sum_{b \in N(S)} d = d \cdot |N(S)|,$$

因而有 $|N(S)| \geq |S|$. 利用 Hall 定理可知存在从 A 到 B 的完全匹配 M. 结合前述 $|A| = |B|$, 完全匹配 M 用到了 G 的所有顶点. □

问题 4.4.5. *如何找出完全匹配?*

定义 4.4.6. 设 M 是二部图 $G = (A \cup B, E)$ 的一个匹配, 称 G 的顶点 v 是自由顶点, 如果 M 中没有以 v 为顶点的边. 称简单路 P 是相对于匹配 M 的增广路 (*a*ugmenting path), 如果 P 的起点 u 是 A 的自由顶点, 终点是 B 的自由顶点, 且 P 的第偶数条边都属于 M, 其余边属于 $E - M$.

简单路 P 是增广路, 如果它的端点都是自由顶点, 且属于 M 的边与不属于 M 的边在 P 上交替出现.

命题 4.4.7 (Berge's lemma)**.** *M 是 G 的边数最大的匹配, 当且仅当不存在相对于 M 的增广路.*

证明: "⇒" 用反证法, 假设 M 是边数最大的匹配, 且存在一条相对于 M 的增广路

$$P : u = u_0 \to v_1 \to u_1 \to \cdots \to v_k \to u_k \to v_{k+1} = v,$$

其中 $u_1v_1,\ldots,u_kv_k\in M$, $u_0v_1,\ldots,u_kv_{k+1}\in E-M$. 可将 M 修改成边数加 1 的匹配

$$M'=(M\backslash\{u_1v_1,\ldots,u_kv_k\})\cup\{u_0v_1,\ldots,u_kv_{k+1}\},$$

这与 M 是边数最大的匹配矛盾!

"⇐" 用反证法, 假设不存在相对于 M 的增广路, 但存在匹配 M' 使得 M' 的边数更大. 考虑由 $A\cup B$ 为顶点集合, 以 $M\Delta M'=(M\cup M')-(M\cap M')$ 为边集的二部分图 G'. 注意到 G' 中每个顶点处有至多一条属于 M 的边与至多一条属于 M' 的边, 可知每个顶点的度至多为 2. 考虑 G' 的任何一个连通分支 H, 则有

$$|V(H)|-1\le|E(H)|=\frac{1}{2}\sum_{v\in V(H)}\deg(v)\le|V(H)|.$$

分两种情况: 若 $|E(H)|=|V(H)|$, 则 H 中有圈 C, 由于 C 中顶点在 C 中已经有两个邻点, 则它们没有连向 C 外的边, 可得 C 自己构成一个连通分支, 因而 $H=C$; 若 $|E(H)|=|V(H)|-1$, 则 H 是最小的连通图, 即 H 是树, 因而无圈. 取 H 中最长的简单路 Q, 则 Q 的两端点度为 1(否则有圈), 中间顶点度为 2, 这样 Q 中的点没有连向 Q 外的边, 可得 Q 自己构成一个连通分支, 因而有 $H=Q$. 这样, 我们证明了 G' 的每个连通分支都是圈或简单路. 注意到, 每个圈上 M 的边与 M' 的边交替出现, 因而圈上 M 与 M' 的边一样多. 由假设 M' 的边更多, 则存在 G' 的一个简单路连通分支 P, 其上 M' 的边更多, 由此可得 P 是相对于 M 的一个增广路, 这与假设不存在相对于 M 的增广路矛盾! □

算法 4.4.8. *设已经找到匹配 M, 执行如下的算法 (称之为 M-算法): 令 U 为 A 中未被 M 匹配的顶点的集合, W 为 B 中未被 M 匹配的顶点的集合, 称 $U\cup W$ 中的点为自由顶点. 称顶点 x 是 "可达" 的, 如果存在起点属于 U 终点为 x 的简单路 P, 要求 P 的第奇数条边不属于 M, 第偶数条边属于 M, 称这样的路为 "$\overline{M}$-M" 交替路. 初始时令 $S=U$. 定义 T 为与 S 中顶点匹配的点构成的集合. 逐个的搜索 S 的顶点, 看它是否有连到 $B\backslash T$ 的边.*

- *若搜索到某条边 sr, $s\in S$,$r\in B\backslash T$, 且发现 $r\in W$. 由 $s\in S$ 的构造方式, s 是 "可达" 的, 即存在从某个 $u\in U$ 到 s 的 "$\overline{M}$-M" 交替路到达 s, 再加上边 sr, 即得到从 u 到 r 的增广路. 利用此增广路将 M 修改成边数多 1 的匹配 M', 退出当前的 M-算法, 开始 M'-算法.*
- *若搜索到某条边 sr, $s\in S$,$r\in B\backslash T$, 且发现 $r\notin W$. 由于 r 不自由, 它被 M 匹配到某个 $q\in A$, 则 $q\notin S$, 且 q 是 "可达的". 用 $S\cup\{q\}$ 代替 S, 并继续搜索 S 有无到 $B\backslash T$ 的边.*
- *若搜索不到 S 到 $B\backslash T$ 的边, 则检查此时的 U. 若 $U=\emptyset$, 则 M 是完全匹配, 输出 M 并终止整个算法. 若 U 非空, 则 $|N(S)|=|T|=|S|-|U|<|S|$. 由 Hall 定理知道图 G 不存在完美匹配, 输出 "G 无完美匹配" 并终止整个算法.*

4.5 欧拉公式

定义 4.5.1. 称 G 是平面图, 如果可将 G 的顶点用平面上的点表示, 将 G 的边用连接顶点的 (没有自交点的) 连续曲线表示, 且要求不同的边至多相交于它们的公共顶点处. 如果 G 没有满足上述条件的表示, 则称 G 不是平面图.

设 G 是平面图, 将 G 画在平面上, 它将平面分成若干个连通的区域, 称每个这样的区域为一个面. 这些面中恰有一个是无界的, 除它之外的其他面都是有界的.

定理 4.5.2 (Euler 公式)**.** *设连通的平面图 G 共有 v 个顶点, e 条边, 它将平面分成 f 个面 (包含最外面那个无界的面), 则有*

$$v - e + f = 2.$$

证明: 固定 v, 对 e 进行归纳. 由于 G 连通, 有 $e \geq v - 1$. 当 $e = v - 1$ 时, G 是树, 此时 $f = 1$, 欧拉公式显然成立. 假设 $e \leq m - 1 (m \geq v)$ 时欧拉公式成立, 考虑 $e = m$ 的情形. 由于 $e \geq v$, 图中有圈, 设 a 是圈上的一边, 则恰有两个不同的面 f_1, f_2 包含 a 为其边界的一部分. 令 $G' = G - a$ 为将 a 删去所得的图, 则 G' 是连通的平面图, 其顶点数 $v' = v$, 边数 $e' = e - 1$. 考察 G' 将平面分成的区域, 除了 f_1, f_2 外 G 分平面所得其他区域都不变, 只有 f_1, f_2 合成了一个新区域. 由此可得 $f' = f - 1$. 对 G' 用归纳假设可得 $v' - e' + f' = 2$, 即有 $v - (e - 1) + (f - 1) = 2$, 这就证明了 G 的欧拉公式.

□

命题 4.5.3. *设平面图 G 共有 $n \geq 3$ 个顶点, 则*

(1) *G 至多有 $3n - 6$ 条边.*

(2) *G 有一个顶点的度不超过 5.*

证明: (1) 只需对阶数 $v \geq 3$ 的连通的平面图 G 证明 $e \leq 3v - 6$. 为此, 注意到

$$3f \leq \sum_{\text{面}F} (F\text{的边数}) = \sum_{\text{面}F} \sum_{\text{边}a \subset F} 1 = \sum_{\text{边}a} \sum_{\text{面}F \supset a} 1 = \sum_{\text{边}a} 2 = 2e.$$

结合欧拉公式 $v - e + f = 2$ 可得

$$3(2 + e - v) \leq 2e,$$

即有 $e \leq 3v - 6$.

(2) 反证法, 假设 G 中每点的度都大于 5, 则有

$$e = \frac{1}{2} \sum_{\text{顶点}x} \deg(x) \geq \frac{1}{2} \sum_{\text{顶点}x} 6 = 3v,$$

与 (1) 的结论矛盾! □

推论 4.5.4. K_5 与 $K_{3,3}$ 都不是平面图.

证明: 由命题4.5.3可知 K_5 不是平面图. 对于 $G = K_{3,3}$, 注意到图中的每个简单圈的长度都是偶数, 因而都不小于 4. 这样, 若 G 是平面图, 则

$$4f \leq \sum_{\text{面}F}(F\text{的边数}) = 2e,$$

结合欧拉公式可得 $e \leq 2v - 4$, 但 $v = 6, e = 9$, 矛盾! □

4.6 图的染色

定义 4.6.1. 图 $G = (V, E)$ 的一个顶点染色是指一个映射 $c : V \to S$, 要求对任何边 uv 都有 $c(u) \neq c(v)$. 称 S 的元素为颜色.

定义 G 的色数为对 G 的顶点染色所需颜色数目的最小值, 记 G 的色数为 $\chi(G)$. 如果 $\chi(G) \leq k$, 则称 G 可以 k 染色.

命题 4.6.2. 简单图 G 可二染色当且仅当 G 中没有长度为奇数的圈.

命题 4.6.3 (Brooks)**.** 设简单图 G 中每个顶点的度都不超过 d, 则 G 可 $d+1$ 染色.

证明: 删去一个顶点, 用归纳假设. □

定理 4.6.4. 任何平面图都可以 5 染色.

证明: 对顶点数目 v 归纳. 当 $v \leq 5$ 时, 命题显然成立. 假设 $v = n - 1$ 时命题成立, 考虑 $n(n \geq 6)$ 阶平面图 G, 来证明 G 可 5 染色. 用反证法, 假设 G 不可 5 染色.

由命题4.5.3, 存在顶点 x 的度不超过 5. 令 $H = G - \{x\}$ 为 G 删去顶点 x 所得的平面图, 由归纳假设知 H 可 5 染色. 不妨设颜色集合为 [5]. 考虑 x 的邻点的颜色. 若 x 的邻点至多用到 4 中颜色, 则可以将 x 染成这四种颜色之外的那种颜色, 得到 G 可 5 染色, 矛盾! 以下假设 x 的邻点用到了所有 5 种颜色, 则 x 恰 5 个邻点且它们颜色互不相同. 从 x 处看, 设它引出的 5 条边按照顺时针顺序依次排列为 $xx_1, xx_2, xx_3, xx_4, xx_5$, 设 x_i 的颜色为 $i(1 \leq i \leq 5)$. 对于 $i \neq j$, 令 $H_{i,j}$ 为 H 的所有 i, j 两色顶点所构成的诱导子图.

考虑 x_1, x_3 在 $H_{1,3}$ 中所在的连通分支. 若 x_1, x_3 在 $H_{1,3}$ 的不同连通分支中, 则将 x_1 所在连通分支中 1 色点变成 3 色点, 3 色点变成 1 色点. 这样得到 H 的另一个染色方案, 满足邻点均不同色. 注意到, x 的邻点没用到颜色 1, 可将 x 染成颜色 1, 得到 G 可 5 染色, 矛盾! 这样, x_1, x_3 在 $H_{1,3}$ 同一连通分支中, 因而在 $H_{1,3}$ 中存在从 x_1 到 x_3 的道路 P.

类似的, 在 $H_{2,4}$ 中存在从 x_2 到 x_4 的道路 Q. 注意到, $C = Px_3xx_1$ 是平面上的封闭圈, 它将平面分成内外两个区域, x_2, x_4 一个在圈内一个在圈外. 由于 Q 连接 x_2 到 x_4, 它必与 C 相交, 但 Q 的点是 $2, 4$ 色而 C 的点是 $1, 3$ 色, 矛盾! □

4.7 图的交叉数 (crossing number)

问题 4.7.1. 如果 G 不是平面图, 将 G 画在平面上, 最少会产生多少个交叉点? 允许两条边在边内部相交产生交叉点, 但不允许多于两条边经过同一个交叉点.

定义 4.7.2. 用 $\mathrm{cr}(G)$ 表示将 G 画在平面上所产生的交叉点数目的最小值, 称为 G 的交叉数 ($c$rossing number).

G 是平面图当且仅当 $\mathrm{cr}(G)=0$.

命题 4.7.3. 如果简单图 G 含有至少 3 个顶点, 则有

$$cr(G) \geq |E| - 3|V| + 6.$$

证明: 设将 G 画在平面上共产生 C 个交叉点. 把所有交叉点视为新增的顶点, 得到平面图 G', 则 G' 的顶点数目为 $V' = n + C$, 边数为 $E' = \frac{1}{2}(2E + 4C) = m + 2C$. 由命题4.5.3 有 $E' \leq 3V' - 6$, 由此即得 $C \geq E - 3V + 6$. □

定理 4.7.4 (Crossing number inequality, 1982 年). 设简单图 G 满足 $|E| \geq 4|V|$, 则有

$$cr(G) \geq \frac{|E|^3}{64|V|^2}.$$

证明: 记 $|V| = n, |E| = m$. 考虑 G 的子图 H, 让 G 的每个顶点入选 H 的概率为 p, 这里 $p \in (0, 1]$ 待定. 设 H 的交叉点数, 顶点数, 边数分别为 $C_H, , n_H, m_H$, 由命题4.7.3的结论有 $C_H \geq m_H - 3n_H$. 由此可知

$$E[C_H - (m_H - 3n_H)] \geq 0.$$

简单的算两次表明:

$$E[C_H] = p^4 C, \quad E[m_H] = p^2 m, \quad E[n_H] = pn,$$

代入前述有关期望值的不等式可得

$$C \geq \frac{mp - 3n}{p^3}.$$

取 $p = \frac{4n}{m} \in (0, 1]$, 就得到所要证明的不等式. □

设 P 是平面上的有限点集, L 是由平面上有限多条直线构成的集合, 定义

$$I = \{(p, l) : p \in P, l \in L, \text{且} p \in l\}.$$

定理 4.7.5 (Szemeredi-Trotter theorem, 1983 年). 假设每个 $l \in L$ 至少经过 P 中两个点, 且 $|I| \geq 8|P|$, 则有 $|I| \leq 8|L|^{\frac{2}{3}} \cdot |P|^{\frac{2}{3}}$.

证明: 设 $l \in L$ 上有 $a(l)$ 个 P 中的点, 这些点在 l 上截出 $a(l)-1$ 条线段 (另外还截出两条射线, 不予考虑). 当 l 取遍 L 的成员时, 把前述所有 $\sum\limits_{l\in L}(a(l)-1)=E$ 条线段视为简单图 G 的所有边, 将 P 视为 G 的顶点集. 注意到, 由假设每个 $a(l)\geq 2$, 可知

$$E=\sum_{l\in L}(a(l)-1)\geq\sum_{l\in L}\frac{a(l)}{2}=\frac{|I|}{2}\geq 4|P|.$$

设 G 一共产生 C 个交叉点, 显然有 $C\leq|L|^2$. 利用 Crossing number inequality 的结论可得

$$|L|^2\geq C\geq\frac{E^3}{64|P|^2}\geq\frac{|I|^3/8}{64|P|^2},$$

得到所要证明的不等式. □

第五章　Block Design

5.1　Block Design

问题 5.1.1. 给定 v 元集合 X, 是否存在 X 的 b 个 k 元子集 $Y_1, \ldots, Y_b$, 使得对 X 中任何两个不同元素 x, x' 都恰好有 λ 个 Y_i 包含 x, x'?

人们称上述问题为 *block design*, 称每个 Y_i 为一个 *block*. 为了描述 X 的元素与子集 $Y_1, \ldots, Y_b$ 的关系, 引入如下二部图 G. 顶点集为 $X \cup \{Y_1, \ldots, Y_b\}$, 在 $x \in X$ 与 Y_i 之间连边当且仅当 $x \in Y_i$. 在此二部图中, 每个 Y_i 的度为 k, 每个 $x \in X$ 的度 $\deg(x)$ 等于包含 x 的 Y_i 的个数.

引理 5.1.2. 在 *block design* 中, 对每个 $x \in X$ 都有 $\deg(x) = \frac{(v-1)\lambda}{k-1}$.

证明: 从两方面来计算

$$N = \#\{(x, x', Y_i) | x' \in X, x' \neq x, x \in Y_i, x' \in Y_i\}.$$

一方面, 对每个固定的 x', 有 λ 个 Y_i 同时包含 x, x', 因而 $N = (v-1)\lambda$. 另一方面, 对每个包含 x 的 Y_i, 恰有 $k-1$ 个 x' 满足 $x' \in Y_i$ 且 $x' \neq x$, 因而 $N = \deg(x)(k-1)$. 结合起来即得到

$$(v-1)\lambda = \deg(x)(k-1).$$

□

由上述引理, 可设每个 $x \in X$ 都包含在 r 个 Y_i 中. 这样, block design 中共有 5 个参数 v, k, λ, r, b, 满足如下两个约束:

$$(v-1)\lambda = (k-1)r, \quad vr = bk,$$

后者来自于对 G 的边数的两种计数. 利用这两个约束, 可从 v, k, λ 解出 r, b, 故称此 block design 为 (v, k, λ)-design. 当 $k = v$ 时, 有唯一的 block $Y = X$, 为了方便起见, 我们把这种平凡的构造排除在外, 即以下都假设 $k < v$. 在此假设下, 还有 $\lambda < r$.

命题 5.1.3 (*Fisher's inequality*)**.** *在 block design 中, 有 $b \geq v$.*

证明: 用反证法, 假设 $b < v$. 设 X 的元素为 $1, 2, \ldots, v$, 对每个元素 i 赋予未知元 x_i, 考虑齐次线性方程组

$$\sum_{i \in Y_t} x_i = 0, \quad t = 1, \cdots, b.$$

此齐次线性方程组的未知元个数 v 大于方程个数 b, 因而存在非零解 $(x_1, \ldots, x_v)$. 由此可得

$$\begin{aligned}
0 &= \sum_{t=1}^{b} \left(\sum_{i \in Y_t} x_i \right)^2 \\
&= \sum_{t=1}^{b} \sum_{i \in Y_t} x_i^2 + 2 \sum_{t=1}^{b} \sum_{i<j, \text{ 且} i \in Y_t, j \in Y_t} x_i x_j \\
&= \sum_{i=1}^{v} \sum_{t \leq b \text{ 且} Y_t \ni i} x_i^2 + 2 \sum_{i<j} \sum_{t \leq b \text{ 且} Y_t \ni i, Y_t \ni j} x_i x_j \\
&= r \sum_{i=1}^{v} x_i^2 + 2\lambda \sum_{i<j} x_i x_j \\
&= (r - \lambda) \sum_{i=1}^{v} x_i^2 + \left(\sum_{i=1}^{v} x_i \right)^2,
\end{aligned}$$

结合 $r > \lambda$, 可得 $x_1 = \cdots = x_v = 0$, 与前述 $(x_1, \ldots, x_v)$ 是非零解矛盾! □

例 5.1.4. 存在 $(6, 3, 2)$-design. 令 $X = \{0, 1, 2, \ldots, 5\}$, 如下 10 个 3 元 block 构成 $(6, 3, 2)$-design:

$$\{0,1,2\}, \{0,1,3\}, \{0,2,4\}, \{0,3,5\}, \{0,4,5\}, \{1,2,5\}, \{1,3,4\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}.$$

例 5.1.5. 存在 $(7, 3, 1)$-design. 令 $X = \{0, 1, 2, \ldots, 6\}$, 如下 7 个 3 元 block 构成 $(7, 3, 1)$-design:

$$\{1,2,3\}, \{3,4,5\}, \{5,6,1\}, \{1,0,4\}, \{3,0,6\}, \{5,0,2\}, \{2,4,6\},$$

此构造来自所谓的 Fano plane. Fano plane 一共 7 个点, 7 条线. 每条线恰过三个点, 对应于上述 7 个 block 之一.

命题 5.1.6. *在 block design 给出的二部图 G 中, 存在从 X 到 $\{Y_1, \ldots, Y_b\}$ 的完全匹配.*

证明: 只需验证 Hall 定理的条件成立: 即对 X 的任何子集 S 有 $|S| \leq |N(S)|$. 计数顶点在 S 与 $N(S)$ 中的边的数目 M, 可得

$$r \cdot |S| = \sum_{i \in S} \deg(i) = M \leq \sum_{Y_t \in N(S)} \deg(Y_t) = k \cdot |N(S)|. \tag{5.1}$$

由等式 $vr = bk$ 及 Fisher's inequality $b \geq v$ 可得 $k \leq r$, 代入(5.1)即得 $|S| \leq |N(S)|$. □

5.2 施泰纳三元系

称一个 $(v, k = 3, \lambda = 1)$-design 为一个施泰纳三元系 (*Steiner System*). 利用前一节中的等式约束, 可得

$$r = \frac{(v-1)\lambda}{k-1} = \frac{v-1}{2}, \quad b = \frac{vr}{k} = \frac{(v-1)v}{6}.$$

由后一等式可知 $3|v-1$ 或 $3|v$, 结合 $2|v-1$ 即得到 $v \equiv 1, 3 \pmod 6$. 由我们假设 $v > k = 3$, 故候选的 v 为

$$v = 7, 9, 13, 15, \cdots.$$

Bose 在 1935 年, Skolem 在 1958 年独立的证明了对上述候选的 v 都存在施泰纳三元系.

定义 5.2.1. 称 X 的子集 A 为施泰纳三元系 $(X, \{Y_1, \ldots, Y_b\})$ 的代表集, 如果 A 与每个 Y_t 都相交非空.

定理 5.2.2. *设 A 是施泰纳三元系 $(X, \{Y_1, \ldots, Y_b\})$ 的代表集, 则有 $|A| \geq \frac{v-1}{2}$.*

证明: 不妨设存在 $x \notin A$. 设包含 x 的 $r = \frac{v-1}{2}$ 个 Y_t 分别为

$$Y_i = \{x, a_i, b_i\}, \quad 1 \leq i \leq r.$$

由于任何两个元素 y, z 恰同属于一个 Y_t, 可知对 $s \neq t$ 总有 $|Y_s \cap Y_t| \leq 1$. 特别的, 前述 $a_1, b_1, a_2, b_2, \cdots, a_r, b_r$ 彼此不同. 由假设 A 包含每个 $\{a_i, b_i\}(1 \leq i \leq r)$ 中至少一个元素, 因而有 $|A| \geq r = \frac{v-1}{2}$. □

定理 5.2.3. *设 $(X, \{Y_1, \ldots, Y_b\})$ 是一个施泰纳三元系. 将 X 的元素任意二染色, 则存在 Y_t 使得 Y_t 的三个元素同色.*

证明: 用反证法, 设可将 X 红蓝二染色, 使得每个 Y_t 都不单色. 设三个元素是两红一蓝的 Y_t 共 y 个, 三个元素是两蓝一红的 Y_t 共 z 个, 设 X 的红蓝元素个数分别为 R, B. 计数三元组

$$(x, x', Y_t) : x, x' \text{ 皆红, 且} x, x' \in Y_t$$

的数目, 可得 $C_R^2 = y$. 类似的, 还有

$$C_B^2 = z, \quad RB = 2y + 2z.$$

结合这三个等式可得

$$RB = R^2 - R + B^2 - B \geq 2RB - R - B,$$

即有 $\frac{1}{R} + \frac{1}{B} \geq 1$. 由此可解出 $(R, B) = (1, 2), (2, 1), (2, 2)$, 分别给出 $v = R + B = 3, 4$, 矛盾! □

第六章　附录

6.1　第一次作业

作业 6.1.1. 求满足 $x_1 + x_2 + \cdots + x_k \le n$ 的有序非负整数组 $(x_1, x_2, \ldots, x_k)$ 的数目. (提示: 等价于找正整数 $y_i = x_i + 1$ 满足 $y_1 + y_2 + \cdots + y_k \le n + k$, 再转化为 $\{y_i\}$ 的部分和序列)

作业 6.1.2. 从 $[n] = \{1, 2, \ldots, n\}$ 中选出 r 个数, 要求选出的数中没有两个数相邻. 求满足条件的选法的总数. (提示: 要求取 $x_1 < x_2 < \ldots < x_r$ 两两不相邻, 等价于取 $x_1 < x_2 - 1 < x_3 - 2 < \cdots < x_r - (r-1)$)

作业 6.1.3. 绕着圆桌均匀放置着 n 个座位, 我们将数字 $1, 2, \ldots, r$ 依顺时针顺序放到这些座位上 (每个座位上至多放一个数字), 要求 1 与 2 的座位不相邻, 2 与 3 的座位不相邻, ..., $r-1$ 与 r 的座位不相邻, r 与 1 的座位不相邻. 如果两种这样的放置方式可以通过旋转从一种变成另一种, 则视它们为同样的放置方式. 在这种意义下, 一共有多少种不同的放置方式?(提示: 等价于找正整数 $y_1, \ldots, y_r$ 满足 $y_1 + \cdots + y_r = n - r$)

作业 6.1.4. 当 A 遍 $[n]$ 的所有子集时, 计算和式 $\sum_{A \subseteq [n]} |A|$ 的值.

作业 6.1.5. 证明:

$$\sum_{k=0}^{n} C_k^a C_{n-k}^b = C_{n+1}^{a+b+1}.$$

(提示: 一个可能的证法是考虑 $[n+1]$ 的 $a+b+1$ 元子集 $\{x_1 < x_2 < \ldots < x_{a+b+1}\}$ 的数目, 并按照 x_{a+1} 的值分类)

作业 6.1.6. (1) 给定正整数 n 与 k, 求有序组 $(A_1, \ldots, A_k)$ 的数目, 其中 $A_1, \ldots, A_k \subseteq [n]$ 且满足 $A_1 \cup \ldots \cup A_k = [n]$.(提示: 将 $A_1, \ldots, A_k$ 的特征向量排成一个 $k \times n$ 的 $0, 1$ 表格. 可逐列的构造此表格, 再用乘法原理)

(2) 求有序组 (B_1, B_2) 的数目, 其中 $B_1, B_2 \subseteq [n]$ 且满足 $B_1 \cap B_2 = \emptyset$.

作业 6.1.7. 设 $f : [n] \to [n]$ 是双射. 以 $1, 2, \ldots, n$ 为顶点画一个图: 如果 $f(i) = j$, 则画一个从 i 指向 j 的箭头, 把所有这样的 n 个箭头都画出, 得到图 G. 如果顶点 $i_1, i_2, \ldots, i_k$ 之间的箭头

为

$$i_1 \to i_2 \to \cdots \to i_k \to i_1,$$

则称 $i_1, i_2, \ldots, i_k$ 构成一个长度为 k 的 “有向圈”.

(1) 证明: G 可以分拆成若干个互不相交的 “有向圈” 的并.(提示: 从任何元素 i 出发, 沿着箭头前进 $i \to f(i) \to f^{(2)}(i) \to \cdots$, 由元素的有限性, 上述走法一定会回到某个经过的顶点, 再由 f 是单射可知一定只能回到 i, 由此得到一个有向圈. 删掉此有向圈, 做类似的推理)

(2) 设 f 确定的图 G 分解成 m_1 个长为 1 的有向圈, m_2 个长为 2 的有向圈,..., m_n 个长为 n 的有向圈, 其中 $m_1, \ldots, m_n$ 是非负整数, 满足 $\sum\limits_{i=1}^{n} i m_i = n$. 证明: 这种 f 的总数目为

$$\frac{n!}{(m_1)!(m_2)!\cdots(m_n)!1^{m_1}2^{m_2}\cdots n^{m_n}} = \frac{n!}{(\prod_{i=1}^{n}(m_i)!)\cdot(\prod_{i=1}^{n} i^{m_i})}.$$

(提示: 构造 f 等价于: 先把 $[n]$ 分解为 m_1 个 1 元组, m_2 个 2 元组,..., m_n 个 n 元组; 其次把每个组用箭头连成有向圈, 对于 i 元组, 将它连成有向圈的方法数目为 $(i-1)!$)

6.2 第二次作业

作业 6.2.1. 证明一般的多项式公式

$$(x_1 + \cdots + x_k)^n = \sum_{\alpha_1,\ldots,\alpha_k \in \mathbf{Z}_{\geq 0}, \alpha_1+\cdots+\alpha_k = n} \binom{n}{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \cdots x_k^{\alpha_k},$$

上述求和式是对满足 $\alpha_1 + \cdots + \alpha_k = n$ 的所有有序非负整数组 $(\alpha_1, \ldots, \alpha_k)$ 求和. (提示: 可对 n 进行归纳; 或者直接计算

$$\begin{aligned}
(x_1 + \cdots + x_k)^n &= \sum_{i_1=1}^{k}\sum_{i_2=1}^{k}\cdots\sum_{i_n=1}^{k} x_{i_1}x_{i_2}\cdots x_{i_n} \\
&= \sum_{\text{映射}f:[n]\to[k]} x_1^{|f^{-1}(1)|}\cdots x_k^{|f^{-1}(k)|} \\
&= \sum_{\alpha_1+\cdots+\alpha_k=n} \left(\sum_{\text{映射}f:[n]\to[k]\text{满足}\#f^{-1}(i)=\alpha_i} x_1^{\alpha_1}\cdots x_k^{\alpha_k} \right) \\
&= \sum_{\alpha_1+\cdots+\alpha_k=n} \binom{n}{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1}\cdots x_k^{\alpha_k}.
\end{aligned}$$

)

作业 6.2.2. 给定 k 个不同的素数 $p_1 < p_2 < \cdots < p_k$. 从 1 到 n 中有多少个数与 $p_1, \ldots, p_k$ 都互素?(提示: 令 $A_i = \{x | 1 \leq x \leq n$ 且x 是p_i 的倍数$\}$, 则 $|A_i| = [\frac{n}{p_i}]$, 其中 $[a]$ 表示不超过 a 的最大整数. 再用容斥原理)

作业 6.2.3. 给定 m 个实数 $x_1,\dots,x_m$. 对 $[m]$ 的任何子集 $A\subseteq[m]$, 定义 $P(A)=\sum_{i\in A}x_i$, 约定 $P(\emptyset)=0$.

(1) 设 $A_1,\dots,A_n$ 是 $[m]$ 的子集. 证明:

$$\begin{aligned}&P(A_1\cup\cdots\cup A_n)\\=&\sum_{i=1}^{n}P(A_i)-\sum_{i<j}P(A_i\cap A_j)+\sum_{i<j<k}P(A_i\cap A_j\cap A_k)-\cdots+(-1)^{n-1}P(A_1\cap\cdots\cap A_n)\\=&\sum_{k=1}^{n}(-1)^{k-1}\sum_{i_1<\cdots<i_k}P(A_{i_1}\cap\cdots\cap A_{i_k}).\end{aligned}$$

(2) 设 $x_1,\dots,x_m$ 都是非负实数. 证明: 对奇数 r, 如下不等式成立

$$P(A_1\cup\cdots\cup A_n)\le\sum_{k=1}^{r}(-1)^{k-1}\sum_{i_1<\cdots<i_k}P(A_{i_1}\cap\cdots\cap A_{i_k});$$

对偶数 r, 如下不等式成立

$$P(A_1\cup\cdots\cup A_n)\ge\sum_{k=1}^{r}(-1)^{k-1}\sum_{i_1<\cdots<i_k}P(A_{i_1}\cap\cdots\cap A_{i_k}).$$

(提示: 仿照讲义上容斥原理的证明, 利用交换求和的技巧)

作业 6.2.4. 定义 Lucas 数列为 $L_1=1,L_2=3$, 且对每个正整数 n 有 $L_{n+2}=L_{n+1}+L_n$.

(1) 求出 Lucas 数列的通项公式.

(2) 证明如下等式:

$$2F_{k+n}=F_kL_n+F_nL_k;\quad 2L_{k+n}=5F_kF_n+L_kL_n;\quad L_{4k}=L_{2k}^2-2;\quad L_{4k+2}=L_{2k+1}^2+2,$$

其中 $\{F_n\}$ 是 Fibonacci 数列.

作业 6.2.5. (1) 考虑集合 $[n]$ 的子集 A, 要求 A 中不存在两个相邻元素. 设满足条件的子集 A 的数目为 a_n(空子集与 1 元子集都视为满足条件). 求 a_n.

(2) 考虑集合 $[n]$ 的子集 A, 要求 A 中不存在三个相邻元素. 设满足条件的子集 A 的数目为 b_n(空子集, 1 元子集, 2 元子集都视为满足条件). 求 b_n.

(3) 如果将 $[n]$ 的元素按顺时针方向依次放置在圆周上, 约定 i 与 $i+1$ 相邻 $(1\le i\le n-1)$, 且 n 与 1 也相邻. 设在这种意义下, $[n]$ 的不含相邻元素的子集的数目为 c_n. 求 c_n.

(提示: (1) 考虑是否取元素 1, 可得 $a_n=a_{n-1}+a_{n-2}$.

(2) 设从 1 开始连续取了 x 个元素, 则 $0\le x\le 2$, 按照 x 的值分三类, 可得 $b_n=b_{n-1}+b_{n-2}+b_{n-3}$.

(3) 考虑是否取元素 1, 可得 $c_n=a_{n-1}+a_{n-3}$.)

6.3 第三次作业

作业 6.3.1. (1) 假设一年共 366 天, 随机的取 k 个人, 则其中存在两个人生日同月同日的概率 (记为 P_k) 是多少?

(2) 证明: 当 $2 \le k \le 366$ 时, 有

$$e^{-\frac{(k-1)k}{2(n-k+1)}} < 1 - P_k < e^{-\frac{(k-1)k}{2n}},$$

其中 $n = 366$.

(3) 已知 $P_k > \frac{1}{2}$, 求 k 的最小值.

(提示: 参考教材 2.5 节; 可搜索网页计算二次方程的根)

作业 6.3.2. 设 m 是正整数, t 是整数且满足 $0 \le t \le m$. 证明: 对于正数 $C \ge 1$, 如下两个命题成立:

(1) 如果 $t \ge \sqrt{m \ln C} + \ln C$, 则有 $\frac{C_{2m}^m}{C_{2m}^{m-t}} \ge C$;

(2) 如果 $t \le \sqrt{m \ln C} - \ln C$, 则有 $\frac{C_{2m}^m}{C_{2m}^{m-t}} \le C$.

作业 6.3.3. (1) 确定 Markov 不等式取等号的条件.

(2) 确定 Chebyshev 不等式取等号的条件.

作业 6.3.4 (Borel-Cantelli 引理). 设 Ω 是有限概率空间, $E_1, \dots, E_n$ 是一族事件 (即它们都是 Ω 的子集). 设 m 是给定的正整数, 定义

$$F = \{\omega \in \Omega | E_1, \dots, E_n \text{中至少有} m \text{个} E_i \text{包含} \omega\},$$

称之为 "事件 $E_1, \dots, E_n$ 中至少 m 个发生" 的事件. 证明:

$$P(F) \le \frac{P(E_1) + \cdots + P(E_n)}{m}.$$

(提示: 对每个 $\omega \in \Omega$, 设 $E_1, \dots, E_n$ 中恰有 $d(\omega)$ 个 E_i 包含 ω. 利用交换求和的方法证明

$$\sum_{i=1}^{n} P(E_i) = \sum_{i=1}^{n} \sum_{\omega \in \Omega, \omega \in E_i} p_\omega = \sum_{\omega \in \Omega} d(\omega) p_\omega,$$

之后再模仿 Markov 不等式的证明方法即可.)

作业 6.3.5. 设 X 是概率空间 Ω 上的非负随机变量, 记 X 的期望为 $E[X] = \mu$. 定义随机变量 Y 为

$$Y(\omega) = \begin{cases} X(\omega), & \text{如果} X(\omega) > \frac{\mu}{2}, \\ 0, & \text{如果} X(\omega) \le \frac{\mu}{2}. \end{cases}$$

(1) 证明: $E[Y] \geq \frac{1}{2}E[X]$.

(2) 设正数 M 是 X 的一个上界, 即满足对每个 $\omega \in \Omega$ 都有 $X(\omega) \leq M$. 证明: $P(X > \frac{1}{2}\mu) \geq \frac{1}{2M}E[X]$.

(提示: 记 $A = \{\omega | X(\omega) > \frac{\mu}{2}\}$, $B = \Omega \backslash A$, 则有

$$E[X] = \sum_{\omega \in A} X(\omega)p_\omega + \sum_{\omega \in B} X(\omega)p_\omega \leq E[Y] + \frac{\mu}{2}P(B) \leq E[Y] + \frac{\mu}{2},$$

其中最后一步用到了 $\mu \geq 0$.)

6.4 第四次作业

作业 6.4.1. 设 a, b, c 是正整数, 满足 $a \mid bc$, 且 a 与 b 互素. 证明: $a \mid c$.

作业 6.4.2. 设 a, b 是不同的整数.

(1) 证明: 对任何整系数多项式 $f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0$, 有

$$a - b \mid f(a) - f(b).$$

(2) 证明: 对于正整数 n, 有

$$\left(a - b, \frac{a^n - b^n}{a - b}\right) = \left(a - b, nb^{n-1}\right).$$

(提示: 考虑分解式

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}).$$

(2) 计算 $\frac{a^n - b^n}{a - b}$ 除以 $a - b$ 的余数.)

作业 6.4.3. 设 $f(x) = a_n x^n + \cdots + a_0$ 是整系数多项式, 且 $a_n \neq 0$. 证明: 如果既约分数 $\frac{p}{q}$ 是 $f(x) = 0$ 的根, 则有 $p \mid a_0$, $q \mid a_n$.

作业 6.4.4. 设 n 是正整数. 证明: 对素数 p, $n!$ 中 p 因子的个数为

$$v_p(n!) = \sum_{i=1}^{\infty} [\frac{n}{p^i}] = [\frac{n}{p}] + [\frac{n}{p^2}] + \cdots .$$

(提示: 把 $v_p(k)$ 表示成和式

$$v_p(k) = \max\{i \in \mathbf{Z}_{\geq 0} : p^i \mid k\} = \sum_{i \in \mathbf{Z}_+ \text{且} p^i \mid k} 1,$$

代入 $v_p(n!)$ 的计算式, 并交换求和顺序.)

作业 6.4.5. 给定正整数 n. 设所有不超过 n 的素数为 $p_1, p_2, \ldots, p_k$.

(1) 证明:

$$1+\frac{1}{2}+\cdots+\frac{1}{n}<\frac{p_1}{p_1-1}\cdot\frac{p_2}{p_2-1}\cdot\cdots\cdot\frac{p_k}{p_k-1}$$

(2) 证明:

$$\frac{1}{p_1-1}+\cdots+\frac{1}{p_k-1}>\ln(\ln(n+1)).$$

(3) 证明:

$$\frac{1}{p_1}+\cdots+\frac{1}{p_k}>\ln\ln n-1.$$

(提示: (1) 利用算术基本定理先证明

$$1+\frac{1}{2}+\cdots+\frac{1}{n}\le(1+\frac{1}{p_1}+\cdots+\frac{1}{p_1^n})\cdot\cdots\cdot(1+\frac{1}{p_k}+\cdots+\frac{1}{p_k^n}).$$

(2), (3) 用到不等式 $\frac{1}{x}<\ln\frac{x}{x-1}<\frac{1}{x-1}$ 以及

$$\sum_{i=1}^{k}\frac{1}{p_i-1}-\sum_{i=1}^{k}\frac{1}{p_i}=\sum_{i=1}^{k}\frac{1}{(p_i-1)p_i}\le\frac{1}{1\cdot2}+\cdots+\frac{1}{k\cdot(k+1)}<1.$$

)

6.5 第五次作业

作业 6.5.1. 称两条有公共顶点的边所构成的图形为一个角. 设 G 是 n 阶图, 每个顶点的度分别为 $d_1, \ldots, d_n$.

(1) 证明: 图中角的数目 C 为

$$C=\sum_{i=1}^{n}C_{d_i}^2.$$

(2) 对于 G 的两个顶点 u, v, 如果 uv 不是 G 的边, 则在 u, v 之间画一条虚边. 证明: 图中由一实边与一虚边所构成的角的数目 D 为

$$D=\sum_{i=1}^{n}d_i(n-1-d_i).$$

(3) 将 G 的 n 个顶点所构成的 C_n^3 个三角形按照它的边界含有几条实边分类: 设三条实边的三角形共 x 个, 两实边一虚边的三角形共 y 个, 一实边两虚边的三角形共 z 个. 证明:

$$3x+y=C,\quad 2y+2z=D.$$

(4) 综合前面小问的结论, 证明:

$$x \geq \frac{4|E|}{3n}\left(|E| - \frac{n^2}{4}\right) + \frac{z}{3} \geq \frac{4|E|}{3n}\left(|E| - \frac{n^2}{4}\right).$$

(提示: 把角按照顶点分类计数可得到 (1), (2). 再去数每一个三角形中各种类型的角有几个.)

作业 6.5.2. 设图 G 共有 n 个顶点与 $m \geq 1$ 条边. 证明: 存在顶点集合 $V(G)$ 的非空子集 H, 使得 H 中每个顶点在 H 中都有至少 $\frac{m}{n}$ 个邻点. (提示: 如果 G 中每点的度都至少 $\frac{m}{n}$, 则取 $H = V(G)$. 以下假设存在 $\deg(x) < \frac{m}{n}$. 将 x 删去, 得到图 G', 则 G' 的顶点数为 $n' = n - 1$, 边数 $m' = m - \deg(x) > m - \frac{m}{n}$. 对 G' 用归纳假设, 存在 G' 的顶点集的子集 H 使得 H 中每个顶点在 H 中都有至少 $\frac{m'}{n'}$ 个邻点, 再注意到

$$\frac{m'}{n'} > \frac{m - \frac{m}{n}}{n-1} = \frac{m}{n}$$

即可.)

作业 6.5.3. (1) 设图 G 中每个顶点的度都不小于 δ, 其中 $\delta \geq 2$ 是给定的正整数. 证明: 图 G 中存在长度至少为 $\delta + 1$ 的简单圈.

(2) 可将 G 的边集表示为若干个简单圈的不交并的充分必要条件是: G 的每个顶点的度都是偶数.

(提示 (1): 取 G 中最长的简单路 $v_0v_1 \ldots v_k$, 考虑 v_k 的邻点, 它们一定属于 $\{v_0, \cdots, v_{k-1}\}$ 且至少有 δ 个, 可知 v_k 的邻点中必有一个形如 v_i 且 $i \leq k - \delta$. 这就找到简单圈 $v_iv_{i+1} \cdots v_kv_i$, 其长度为 $k - i + 1 \geq \delta + 1$.)

作业 6.5.4. 设 n 阶图 G 的边数大于 C_{n-1}^2. 证明: G 是连通的. (提示: 用反证法, 假设 G 不连通. 取一个连通分支 A, 记 $B = A^c$, $|A| = a$, 则 $1 \leq a \leq n - 1$, 由此可估计 G 的边数:

$$|E| \leq C_a^2 + C_{n-a}^2 \leq C_{n-1}^2 + C_1^2 = C_{n-1}^2.$$

)

作业 6.5.5. 定义数列 $\{N_r\}$ 为:

$$N_1 = 3, \quad N_r = r(N_{r-1} - 1) + 2, \forall r \geq 2.$$

证明: 将 N_r 阶完全图的每条边任意的用 r 种颜色之一染色, 则图中必有同色三角形. (提示: 任取一顶点 v, 它连出 $N_r - 1 = r(N_{r-1} - 1) + 1$ 条边, 由抽屉原理知这些边染成 r 种颜色后一定存在至少 N_{r-1} 条同色. 不妨设 v 至少引出 N_{r-1} 条染成颜色 1 的边, 设这些边的异于 v 的顶点构成的集合为 H. 若 H 中有颜色 1 的边, 则加上顶点 v 后构成单色三角形; 若 H 中没有颜色 1 的边, 则 H 的边只用了 $r - 1$ 种颜色染色, 由于 $|H| \geq N_{r-1}$, 由 (对 r 的) 归纳假设知 H 中有单色三角形.)

作业 6.5.6 (Schur). 设 N_r 为上一题中所定义的正整数. 证明: 如果将 $1, 2, \cdots, N_r$ 中的每个数任意的用 r 种颜色之一染色, 则一定存在三个同色的数 x, y, z 满足 $x + y = z$.

6.6 第六次作业

作业 6.6.1. (1) 设 G 是连通的 n 阶图, 且边数为 $n-1$. 证明: G 是树.

(2) 设 T 是 n 阶树, 且恰好有两个度为 1 的顶点. 证明: T 是一个长为 $n-1$ 的简单路.

(3) 设 T 是第 (2) 小问中的图 (称之为 *path graph*). 证明: 存在映射 $f : V(T) \to \{1, 2, \ldots, n\}$, 使得当 $\{x, y\}$ 取遍 T 的所有 $n-1$ 条边时, 所得到 $|f(x) - f(y)|$ 的值两两不同.(人们猜测: 对于所有树 T, 都有这样的 f 存在.)

作业 6.6.2. (1) 设 G 是 n 阶简单图, 其顶点分别为 $v_1, \ldots, v_n$. 定义 G 的邻接矩阵 $A = (a_{ij})$ 为:

$$a_{ij} = \begin{cases} 1, & \text{如果} v_i \text{ 与} v_j \text{ 相邻}, \\ 0, & \text{如果} v_i = v_j \text{ 或} v_i \text{ 与} v_j \text{ 不相邻}. \end{cases}$$

证明: A^2 的矩阵元 $(A^2)_{ij}$ 等于顶点 v_i 与顶点 v_j 的公共邻点的数目. 更一般的, 证明 A^k 的矩阵元 $(A^k)_{ij}$ 等于从顶点 v_i 到顶点 v_j 的长为 k 的 (不一定简单的) 道路的数目.

作业 6.6.3. 《离散数学》146 页练习 8.2.3. 设 T 是树, 将 T 的顶点 v 删去, 得到的图分成若干个连通分支, 称每个这样的连通分支为 v 处的一个 "分支". 证明: 存在顶点 v, 使得 v 处的每个 "分支" 的顶点数目都不超过 $\frac{|V(G)|}{2}$.

(提示: 记 v 处的顶点数目最大的分支为 T_v, 要证明存在 v 使得 $|V(T_v)| \le \frac{|V(G)|}{2}$. 设

$$V(T_v) = \min_{x \in V(T)} |V(T_x)|,$$

我们断言 v 满足条件. 用反证法, 假设 $|V(T_v)| > \frac{|V(G)|}{2}$. 考虑 v 在 T_v 中唯一的那个邻点 w, 设 T_v 删去 w 后分解成连通分支 $T_1, \ldots, T_l$ 之并. 结合 $|V(T_v)| > \frac{|V(G)|}{2}$ 以及

$$V(T_v) = \{w\} \cup V(T_1) \cup \cdots \cup V(T_l),$$

可得 $|V(T_w)| \le |V(T_v)| - 1$, 矛盾!)

作业 6.6.4. 《离散数学》155 页练习 8.5.4.

作业 6.6.5. 《离散数学》156 页练习 8.5.10.

作业 6.6.6. 设 T 是顶点编号为 $1, 2, \ldots, n$ 的树. 令 $T_1 = T$, 归纳的定义 T_i 如下: 设已经定义好 T_i, 令 x_i 为 T_i 的 leaf 的编号的最小值, 设 x_i 在 T_i 中的唯一的邻点为 y_i, 定义 T_{i+1} 为由 T_i 删去 x_i 所得的图. 称 $P(T) = (y_1, y_2, \ldots, y_{n-2})$ 为 T 的普吕弗序列.

(1) 证明: $y_{n-1}=n$, 且 $\{x_1,\ldots,x_{n-1},y_{n-1}\}=\{1,2,\ldots,n\}$.

(2) 证明: x_k 等于不在 $\{x_1,\ldots,x_{k-1}\}\cup\{y_k,\ldots,y_{n-2}\}$ 中出现的最小正整数.

(3) 请画出一个至少 10 阶的顶点编号的树 T. 给出它的普吕弗序列, 并从 $P(T)$ 重构出 T.

6.7 第七次作业

作业 6.7.1. 《离散数学》160 页练习 9.1.1.

(提示: 这是找最便宜生成树的另一个算法: 在保持图连通的条件下, 每一步删去权重最大的边, 直到不能再删任何边为止. 可具体执行如下算法: 令 $D_0=\emptyset$, $K_0=\emptyset$ (这里 D 表示删除, K 表示保留). 在第 i 步, 选出 $E\backslash(D_{i-1}\cup K_{i-1})$ 中权重最大的边 e(若不唯一则任选一条), 如果 $(E\backslash D_{i-1})\backslash\{e\}$ 构成连通图, 则令 $D_i=D_{i-1}\cup\{e\}, K_i=K_{i-1}$; 如果 $(E\backslash D_{i-1})\backslash\{e\}$ 不构成连通图, 则令 $D_i=D_{i-1}, K_i=K_{i-1}\cup\{e\}$. 直到 $D_l\cup K_l=E$ 时终止算法, 输出 $T=K_l$.

我们来证明上述算法给出的 T 是最便宜的生成树. 对边数用归纳法, $|E(G)|=1$ 的情形显然成立. 设 $|E(G)|<m$ 是结论成立, 考虑 $|E(G)|=m$ 的情形. 设 e 是 G 中权重最大的边, 分两种情形讨论.

(1) 如果 $G'=G\backslash\{e\}$ 连通, 则 $e\notin T$. 设 A 是 G 的任何生成树. 若 $e\notin A$ 则 A,T 都是 G' 的生成树且 T 是对 G' 用 "悲观算法" 选出的生成树, 由归纳假设可得 $c(T)\le c(A)$. 若 $e\in A$, 则 $A\backslash\{e\}$ 是两颗树之并 $A_1\cup A_2$, 由于它在连通图 G' 中, 存在 G' 的边 f 连接 A_1 与 A_2 的顶点. 令 $A'=(A\backslash\{e\})\cup\{f\}$, 则 A' 是 G 的生成树且 $c(A')\le c(A)$. 这样 A' 不含 e, 由前述必有 $c(T)\le c(A')$, 从而 $c(T)\le c(A')\le c(A)$.

(2) 如果 $G'=G\backslash\{e\}$ 不连通, 则 G' 分解成两个连通分支之并 $G'=G_1\cup G_2$ 且 G_1 与 G_2 之间只有唯一一条边 e. 这样, T,A 都必须包含 e, 且有分解 $T\backslash\{e\}=T_1\cup T_2, A\backslash\{e\}=A_1\cup A_2$, 其中 T_i,A_i 是 G_i 的生成树. 注意到, T_i 是对 G_i 用 "悲观算法" 选出的生成树, 由归纳假设有 $c(T_i)\le c(A_i)$. 结合起来即得到 $c(T)\le c(A)$.)

作业 6.7.2. 《离散数学》163 页练习 9.2.3. 设 G 是连通的加权图, 且所有边的权重互不相同. 证明: G 的最便宜生成树是唯一的.

(提示: 用反证法, 设 T_1,T_2 是两个不同的最便宜生成树, 考虑 $T_1\Delta T_2=(T_1\backslash T_2)\cup(T_2\backslash T_1)$ 中权重最小的边 e. 不妨设 $e\in T_2\backslash T_1$, e 的两个端点在树 T_1 中有唯一的最短路 P 相连, P 的边不能全都属于 $T_1\cap T_2$. 设 P 的边 $f\in T_1\backslash T_2$, 则 $c(e)<c(f)$. 这样, 可将 T_1 修改成更便宜的生成树 $T_1'=(T_1\backslash\{f\})\cup\{e\}$, 与 T_1 是最便宜生成树矛盾!)

作业 6.7.3. 《离散数学》163 页练习 9.2.4. 设 G 是连通的加权图, 且每边的权都是正数.

(a) 求 G 的生成树 T, 使得 $\prod_{e\in T}c(e)$ 最小.

(b) 求 G 的生成树 T, 使得 $\max_{e\in T}c(e)$ 最小.

(提示: (a) 等价于 $\sum_{e\in T}\ln(c(e))$ 最小. (b) 利用本次作业第一题的算法.)

作业 6.7.4. 《离散数学》176 页练习 10.4.7.

(提示: 讲义中 Hall 定理的归纳证明已经包含此题所需要的论断.)

作业 6.7.5. 《离散数学》177 页练习 10.4.9.

(提示: 只需验证 Hall 定理的条件成立. 用反证法, 假设存在 $S\subset A$ 使得 $|S|>|N(S)|$, 任取 $a\in S$, $b\in N(S)^c$, 则有

$$|N(S)|\geq \deg(a),\quad |S^c|\geq \deg(b),$$

由此即得矛盾! 从这个证明可知, 只需要每点的度大于等于 $\frac{m}{2}$, 就可保证存在完美匹配.)

作业 6.7.6. 设 G 是 $n(n\geq 3)$ 阶图. 证明: 如果每个顶点的度都不小于 $\frac{n}{2}$, 则图中存在 Hamliton 圈.

(提示: 先证明 G 连通, 否则存在一个连通分支的阶不超过 $\frac{n}{2}$, 从而该分支内顶点的度均不超过 $\frac{n}{2}-1$, 矛盾! 其次, 考虑最长简单路 $P=v_0v_1\dots v_k$, 由其最长性可知 v_0,v_k 的邻点都在此路中. 设 v_0 的全部邻点为 $v_1=v_{i_1},\dots,v_{i_t}$, 则 v_k 必与某个 v_{i_j-1} 相邻, 否则 $\deg(v_k)\leq k-t\leq n-1-\deg(v_0)\leq \frac{n}{2}-1$, 矛盾! 这样, P 的所有顶点按如下顺序构成一个简单圈 Q:

$$v_0\to v_{i_j}\to v_{i_j+1}\to\cdots\to v_k\to v_{i_j-1}\to v_{i_j-2}\cdots\to v_0.$$

注意到, Q(记为 $Q=w_0w_1\cdots w_kw_0$) 到 Q 外的点不能连边, 否则的话设有边 uw_i, 则可找到比 P 更长的简单路

$$u\to w_i\to w_{i+1}\to\cdots\to w_k\to w_0\to w_1\to\cdots\to w_{i-1},$$

矛盾! 结合之前证明过的 G 连通, 即可知 Q 包含了 G 的所有顶点, 从而是一个 Hamilton 圈.)

6.8 第八次作业

作业 6.8.1. 证明: 图 G 可以顶点二染色的充分必要是 G 中不存在长度为奇数的简单圈.

作业 6.8.2. 《离散数学》195 页练习 12.3.4.

作业 6.8.3. 阅读《离散数学》第 12.3 小节并完成 195 页练习 12.3.7.

作业 6.8.4. 《离散数学》204 页练习 13.3.4.

作业 6.8.5. 《离散数学》210 页练习 13.4.5. 设 G_n 是从 n 阶完全图 K_n 删去一个哈密尔顿圈 (上的所有边) 所得的图. 求 G_n 的色数.

(提示: 只考虑 $n > 3$ 的情形. 沿着该哈密尔顿圈将顶点依次标号为 $1, \ldots, n$, 则删去的边为 $12, 23, \ldots, (n-1)n, n1$. 注意到, 对每个顶点 i, 能与它同色的顶点只有 $i-1, i+1$, 且 $i-1$ 与 $i+1$ 不能同色, 这表明每种颜色至多用于两个顶点. 由此可得 $n \leq 2\chi(G_n)$, 即 $\chi(G_n) \geq [\frac{n+1}{2}]$.

另一方面, 构造染色方案为: 对 $1 \leq i \leq n$, 将顶点 i 染第 $[\frac{i+1}{2}]$ 色. 可得 G_n 可以 $[\frac{n+1}{2}]$ 色染色.)

作业 6.8.6. 叙述并证明《离散数学》226 页定理 14.4.1. 再解答 227 页练习 14.4.3.

作业 6.8.7. 《离散数学》227 页练习 14.4.3. 设 X 是 v 元集, $Y_1, \ldots, Y_b$ 是 X 的一个施泰纳三元系. 设 S 是 X 的 $\frac{v-1}{2}$ 元子集, 已知 $\{Y_i | 1 \leq i \leq b, Y_i \subseteq S\}$ 构成 S 的施泰纳三元系. 证明: 对每个 $i = 1, \ldots, b$ 都有 $Y_i \cap S \neq \emptyset$.

(提示: 由条件知若 Y_i 含有 S 中两个元素则 $Y_i \subseteq S$. 这样, 所有的 Y_i 按照 $|Y_i \cap S| \in \{0, 1, 3\}$ 分成三类. 设满足 $|Y_i \cap S|$ 等于 $0, 1, 3$ 的 Y_i 分别各有 x, y, z 个. 计数两个脚都属于 S 的角可得 $C^2_{\frac{v-1}{2}} = 3z$; 计数两个脚一个属于 S 另一个不属于 S 的角可得 $\frac{v-1}{2} \cdot \frac{v+1}{2} = 2y$. 由此可得

$$x = b - y - z = \frac{1}{3}C_v^2 - \frac{(v-1)(v+1)}{8} - \frac{1}{3}C^2_{\frac{v-1}{2}} = 0,$$

这就证明了每个 Y_i 都与 S 相交非空.)