Jianting's Lecture Review Notes

离散数学
Discrete Mathematics

2020 Fall

Instructor : 王国亮

Textbook : Lecture Notes

Review for Discrete Mathematics

Jianting Feng

21st November 2020

BEIJING INSTITUTE OF TECHNOLOGY

前言

Figure 1

Instructor: David G.L. Wang (Middle) and all classmates(include me)

这是笔者 2020 年秋于北京理工大学（Beijing Institute of Techn）学习离散数学（Discrete Mathematics）课程时的笔记整理。

Contents

Chapter 1

计数 Enumerate

1.1 集合分拆与重集

Definition 1.1.1 (集合分拆)**.** 集合分拆是指将集合 $[n] \triangleq \{1, 2, \cdots, n\}$ 中的元素分为数个不同的非空集合 $B_1, B_2, \cdots, B_r$，并且保证每个元素一定要在某个 B_i 中，这样的 B_i 被称为 *blocks*。

Definition 1.1.2 (第二类斯特林数（The Stirling number of the second kind）)**.** 第二类斯特林数 $S(n, k)$ 是将集合 $[n]$ 分拆为 k 个不同的非空的 *blocks* 的方法总数。$[n]$ 的 *matching* 是指每个 *block* 包含最多两个元素。

Proposition 1.1.1. 对于任意 $n, k \geq 1$,

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

1.2 整数分拆与组合（partitons and compositions）

Definition 1.2.1. 正整数 n 的一个分拆是指一列正整数 λ，常记做

$$\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_r) \vdash n,$$

满足

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1 \ and \ \sum_{i=1}^{r}\lambda_i = n.$$

令 $p(0) = 1$ 且 $p(n)$ 是 $n \geq 1$ 的分拆总数，这样的 $p(n)$ 被称为分拆函数（*partition function*）。

Definition 1.2.2. 一个 n 的 *composition* 是一列非负整数 μ 记为

$$\mu = (\mu_1, \mu_2, \cdots, \mu_r) \models n,$$

满足

$$\sum_{i=1}^{n}\mu_i = n$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
p(n)	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176	231

Table 1.1
分拆函数 $p(n)$ 的值

Definition 1.2.3. 对于任意一个分拆 $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_r \vdash n$，我们可以画一个左对齐的图，一共有 r 行，每一行都有 λ_i 个点（*dots*）。这样的图被称为 λ 的 *Ferrers diagram*。如果用方格（*squares*）代替点，则得到的图被称为 *Young diagram*。相应的分拆 λ 被称作该图的 *shape*，记做 $sh\lambda$。将 *Young diagram* 沿其主对角线翻转（*flip*）得到的新的 *Young diagram* 被称作原 *Young diagram* 的共轭（*conjugate*）。一个分拆是自共轭（*self-conjugate*）的当且仅当它的共轭等于自身。*Young diagram* 的 *Durfee square* 是指该图内部中最大的正方形（*square*）。

Proposition 1.2.1. 将正整数 n 分拆为 m 份的分拆的数量等于将 n 分拆为若干份，每一份最大为 m 的分拆数。

Proof. 考虑 Young diagram 的共轭即可。 □

Proposition 1.2.2. n 的自共轭的分拆总数等于将 n 分拆为若干个不同的奇数的分拆数。

Definition 1.2.4. *Euler* 函数是指

$$\phi(q) = \prod_{n \geq 1} (1 - q^n)$$

Corollary 1.2.0.1. 欧拉函数的倒数 $1/\phi(q)$ 是分拆函数 $p(n)$ 的生成函数，即

$$\sum_{n \geq 0} p(n) q^n = \frac{1}{\phi(q)}$$

Theorem 1.2.1. 将一个整数 n 分拆为每一部分都是奇数的分拆数等于将其分拆为不同部分的分拆数。

Proof. 考虑代数证明，令 a_n 为将 n 分拆为奇数部分的分拆数，b_n 为将 n 分拆为不同部分的分拆数。则有

$$\sum_{n \geq 0} b_n q^n = \prod_{n \geq 1} (1 + q^n) = \prod \frac{1 - q^{2n}}{1 - q^n} = \prod_{n \text{ odd}} \frac{1}{1 - q^n} = \sum_{n \geq 0} a_n q^n$$

提取 q^n 的系数即可。 □

Theorem 1.2.2 (五角数定理（Pentagonal number theorem））**.**

$$\begin{aligned} \phi(q) &= \prod_{n \geq 1} (1 - q^n) = \sum_{n \in \mathbb{Z}} (-1)^n q^{\frac{3n^2 - n}{2}} \\ &= 1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \cdots . \end{aligned}$$

1.3 置换与词

Definition 1.3.1. 置换（*permutation*）是一个集合到自己的双射。集合 $[n]$ 上的置换常被记做 $\mathfrak{S}_n$。对合（*involution*）是每个 *cycle* 至多为 2 的置换（满足 $\pi^2 = \pi$）。一个错排（*derangement*）是指没有不动点的置换 $\pi \in \mathfrak{S}_n$，即对于任意 $i \in [n]$，我们都有 $\pi(i) \neq i$。一个置换 $\pi = \pi_1 \cdots \pi_n$ 反转（*reversal*）是 $\pi_n \pi_{n-1} \cdots \pi_1$。置换 π 的补是 $\sigma_1 \sigma_2 \cdots \sigma_n$ 其中 $\sigma_i = n + 1 - \pi_i$。词（*word*）是在一个重集上的置换，形如 $w_1 w_2 \cdots w_n$ 其中 w_i 允许有重复。

令 $\pi \in \mathfrak{S}_n$，c_i 为 π 中长度为 i 的 cycle 的数量，则 π 中的 cycle 的总数为

$$c(\pi) = c_1 + c_2 + \cdots + c_n$$

我们将整数分拆 $1^{c_1} 2^{c_2} \cdots n^{c_n}$ 为 π 的 type，则有

$$c_1 + 2c_2 + \cdots + nc_n = n$$

Example 1.3.1. 置换 $\pi = (125)(34)$ 的 *type* 是

$$1^0 2^1 3^1 4^0 5^0 \vdash 5$$

Proposition 1.3.1. 对于置换 $\sigma \in \mathfrak{S}_n$，我们称它是 π 的共轭，如果存在 $\tau \in \mathfrak{S}_n$ 满足

$$\sigma = \tau^{-1} \pi \tau$$

两个 $\mathfrak{S}_n$ 中的置换彼此共轭当且仅当它们有相同的 *type*。

Proposition 1.3.2. 在 $\pi \in \mathfrak{S}_n$ 中 *type* 为 $c = 1^{c_1} 2^{c_2} \cdots n^{c_n}$ 的置换总数为 $\frac{n!}{z_c}$，其中

$$z_c = 1^{c_1} c_1! 2^{c_2} c_2! \cdots n^{c_n} c_n!$$

Definition 1.3.2.

$$s(n,k) = (-1)^{n-k} c(n,k)$$

为第一类斯特林数（*Stirling numbers of the first knd*），其中 $c(n,k)$ 是 $\mathfrak{S}_n$ 中有 k 个 *cycle* 的置换数量，被称为无符号的第一类斯特林数（*signless Stirling number of the first kind*）。

Definition 1.3.3 (置换统计量（Permutation statistics）)**.** 设 $\pi = \pi_1 \pi_2 \cdots \pi_n \in \mathfrak{S}_n$.

1. π 的 *descent* 是满足如下条件的 i 的个数，$i \in [n-1]$ 满足

   $$\pi_i > \pi_{i+1}$$

   π 的 *ascent* 是是满足如下条件的 i 的个数，$i \in [n-1]$ 满足

   $$\pi_i < \pi_{i+1}$$

   major index $maj(\pi)$ 是 π 的所有的 *descent* 的和，*i.e.*,

   $$maj(\pi) = \sum_{\pi_i > \pi_{i+1}} i$$

2. π 的 *inversion* 是满足如下条件的 *pair* 的个数，π_i, π_j 满足

$$i < j \quad and \quad \pi_i > \pi_j$$

3. π 的 *excedance* 是是满足如下条件的 i 的个数，$i \in [n]$ 满足 $\pi > i$

4. π 的 *peak* 是数 $i \in \{2, 3, \cdots, n-1\}$ 满足

$$\pi_{i-1} < \pi_i \quad and \quad \pi_i > \pi_{i+1.}$$

   π 的 *valley* 是数 $i \in \{2, 3, \cdots, n-1\}$ 满足

$$\pi_{i-1} > \pi_i \quad and \quad \pi_i < \pi_{i+1.}$$

5. π 的 *left-to-right maxima* 是数 π_i 的集合满足对于任意 $j < i$

$$\pi_i > \pi_j$$

   同样我们可以定义 *left-to-right minima*，*right-to-left maxima*，*right-to-left minima*

Example 1.3.2. $\pi = 25431 \in \mathfrak{S}_5$ 的 *descent set* 为 $\{2, 3, 4\}$，*ascent set* 为 $\{1\}$，*inversion set* 是 $\{(5, 4), (5, 3), (5, 1), (4, 3), (4, 1), (3, 1), (2, 1)\}$，*excedance set* 为 $\{1, 2, 3\}$，因此

$$des(\pi) = 3, maj(\pi) = 9, asc(\pi) = 1, inv(\pi) = 7, exc(\pi) = 3$$

left-to-right maxima 为 $\{2, 5\}$，*left-to-right minima* 为 $\{2\ 1\}$,*right-to-left maxima* 为 $\{1, 3, 4, 5\}$，*right-to-left minima* 为 $\{1\}$。

Definition 1.3.4. 第 n 个欧拉多项式（*Eulerian polynomial*）为

$$A_n(x) = \sum_{\pi \in \mathfrak{S}_n} x^{1+des(\pi)} = \sum_{k=1}^{n} A(n, k) x^k$$

系数为

$$A(n, k) = |\{\pi \in \mathfrak{S}_n : des(\pi) = k - 1\}|$$

被称为欧拉数（*Eulerian number*）。

Note 1.3.1. 事实上，$A(n, k)$ 为长为 n 的置换中 *descent* 为 *k-1* 的置换的个数。

Definition 1.3.5. 任意一个和 *descent numbers* 同分布的统计量被称为 *Eulerian statistic.* 任何一个和 *inversion numbers* 同分布的统计量被称为 *Mahonian statistic.*

Definition 1.3.6. 设 $L = (a_0, a_1, \cdots, a_n)$ 是一列正数。我们称 L 是 *unimodal* 的如果存在一个指标 $1 \leq k \leq n$ 满足

$$a_0 \leq a_1 \leq \cdots \leq a_k \geq a_{k+1} \geq \cdots \geq a_n,$$

我们称 L 是 *log-concave* 的如果对于所有 k 都有

$$a_{k-1} a_{k+1} \leq a_k^2$$

L 是 *real-rooted* 的如果多项式 $\sum\limits_{j=0}^{n} a_j x^j$ 的根都是实根。

Example 1.3.3. $\binom{n}{k}$ 是 *unimodal*，*log-concave* 且 *real-rooted* 的。

Theorem 1.3.1. 设 $L = (a_0, a_1, \cdots, a_n)$ 是一列正数，则我们有如下的结论

1. 如果 L 是 *real-rooted* 的，则 L 是 *log-concave*；
2. 如果 L 是 *log-concave* 的，则 L 是 *unimodal*；
3. 如果 L 是 *real-rooted* 的，则它有一个或两个最大值。

Theorem 1.3.2. 欧拉数序列 $\{A(n,k)\}_k$ 是 *real-rooted, i.e.,Eulerian* 多项式的所有零点都是实数。

Chapter 2

组合数与组合恒等式 Combinatorial numbers and identities

2.1 二项式系数

Theorem 2.1.1 (二项式定理（Binomial theorem）)**.** 令 $n \geq 1$ 为正整数。那么有

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

Proposition 2.1.1. 二项式系数满足下列恒等式

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

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1},$$

$$\binom{a}{b}\binom{b}{c} = \binom{a}{c}\binom{a-c}{b-c},$$

$$\sum_k \binom{n}{k} = 2^k,$$

$$\sum_j \binom{n}{j}\binom{m}{k-j} = \binom{n+m}{k},$$

$$\sum_j \binom{n}{j}^2 = \binom{2n}{n},$$

$$\sum_j (-1)^j \binom{n}{j} = 0,$$

$$\sum_j \binom{n}{j} 2^j = 3^n,$$

$$\sum_k \binom{n}{k}\binom{k}{m} = \binom{n}{m} 2^{n-m}.$$

Proposition 2.1.2 (Hockey-stick identity)**.**

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

Proof. 用两种方法计数（counting by two ways），其中一边是考虑固定最大的元素即可。 □

Proposition 2.1.3. 对于任意 $0 \le k \le n$，

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

Proof. 使用 telescoping method，注意使用2.1.1中的第二个式子即可。 □

Theorem 2.1.2 (Multinomial theorem)**.** 设 $n \in \mathbb{N}$，则

$$(\sum_{j=1}^{m} x_j)^n = \sum_{k_1+k_2+\cdots+k_m=n k_1,\cdots,\_m\in\mathbb{N}} \binom{n}{k_1, k_2, \cdots, k_m} \prod_{j=1}^{m} x_j^{k_j}$$

Proposition 2.1.4. 将 n 个完全相同的物品分给 k 个人的分法数为

$$\left(\tbinom{n+1}{k-1}\right)$$

若要求每个人都分到一件，则分法数为

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

Proof. 使用 method of stars and bars

★★★★★★★

★★★★ , ★ , ★★

★★★★ , , ★★★

注意在 $n+1$ 个位置能放置 $k-1$ 个 bar 即可。 □

Theorem 2.1.3. 对于任意 $n \in \mathbb{Z}$ 和 $k \in \mathbb{N}$，有

$$\left(\tbinom{n}{k}\right) = \binom{n+k-1}{k}$$

2.2 Catalan 数

Definition 2.2.1. 第 n 个 *Catalan* 数为

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

Catalan 数满足如下的递推公式，对于任意 $n \geq 0$，

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$$

通过递推公式容易得到 Catalan 数的生成函数

$$C(z) = \frac{1-\sqrt{1-4z}}{2z}$$

Theorem 2.2.1. *Catalan* 数 C_n 是以下结构的数量：

1. 凸 $n+2$ 边形的三角剖分数量；
2. n 个顶点的二叉树；
3. $n+1$ 个顶点的平面树；
4. $2n$ 长的投票序列（*Ballot sequences*）；
5. 对 $n+1$ 个 x 加括号（*Parenthesizations or bracketings*）；
6. 长为 $2n$ 的 *Dyck paths* 的数量。

2.3 Bell 数

Definition 2.3.1. 第 n 个 *Bell* 数 B_n 为集合 $[n]$ 的拆分总数，即

$$B_n = \sum_{k=0}^{n} S(n,k)$$

Chapter 3

数论 Number Theory

3.1 整数的整除性

Definition 3.1.1. 给定两个整数 a 和 b 且 $b \neq 0$，则存在唯一的整数满足

$$a = qb + r \quad and \quad 0 \leq r < |b|$$

Definition 3.1.2. *Divisor function*$\sigma_x(n)$ 定义为

$$\sigma_x(n) = \sum_{d|n} d^x$$

其中 $x \in \mathbb{R}$，$n \in \mathbb{Z}^+$

Definition 3.1.3. 一个数论函数 $f(n)$ 被称为积性（*multiplicative*）的如果满足

$$gcd(n, n') = 1 \Rightarrow f(nn') = f(n)f(n')$$

Proposition 3.1.1. 对于 $a, b, c \in \mathbb{Z}$，我们有如下结论：

1. 若 $b|a$ 且 $c|b$，则 $c|a$
2. 若 $b|a$，则 $bc|ac$
3. 若 $c|a$ 且 $c|b$，则 $c|(ma + nb)$ 对于任意 $m, n \in \mathbb{Z}$.

Proposition 3.1.2. 如果 $f(n)$ 是积性函数，那么下面的函数也是

$$g(n) = \sum_{d|n} f(n).$$

Proof. 假设 $gcd(n, n') = 1$，则

$$g(nn') = \sum_{c|nn'} f(c) = \sum_{d|n, d'|n'} f(dd') = \sum_{d|n} f(d) \sum_{d'|n'} f(d') = g(n)g(n')$$

□

Theorem 3.1.1 (裴蜀定理)**.** 令 $a, b \in \mathbb{Z} \backslash \{0\}$，且有 $d = gcd(a, b)$，则存在 $x, y \in \mathbb{Z}$ 使得

$$ax + by = d$$

进一步，形如 $ax + by$ 的数都是 d 的倍数。

Proposition 3.1.3. 如果 $ka \equiv kb(mod\ m)$ 且 $gcd(k, m) = d$，则有

$$a \equiv b(mod\ m/d)$$

进一步，若 $gcd(k, m) = 1$，则有 $a \equiv b(mod\ m)$

Definition 3.1.4. 对于任意 $m \in \mathbb{Z}^+$ 记 $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ 为 m 的完全剩余系。用 $\mathbb{Z}_m^*$ 表示 $\mathbb{Z}_m$ 的子集满足其中的元素都与 m 互素。*Euler totient function* 被定义为 $\phi(m) = |\mathbb{Z}_m^*|$，称作 m 的完全剩余类，容易知道 $(\mathbb{Z}_m^*, \cdot)$ 构成一个群（满足结合律、单位元、逆元）。

Theorem 3.1.2 (中国剩余定理（Chinese remainder theorem）)**.** 令 $m_1, \cdots, m_k$ 两两互素，令 $a_1, \cdots, a_k$，则下面的同余方程组一定有解

$$\begin{cases} x \equiv a_1 \quad \bmod m_1 \\ x \equiv a_2 \quad \bmod m_2 \\ \vdots \\ x \equiv a_k \quad \bmod m_k \end{cases}$$

且任意两个解都关于 $\prod_{j=1}^{k} m_j$ 同余。

Proof. 取如下的 x 即可

$$x = \sum_{j=1}^{k} n_j M_j a_j$$

其中 $M_j = \prod_{i \neq j} m_i$，$n_j M_j \equiv 1 \mod a_j$，即 $n_j = M_j^{-1}$（即 M_j 在 $\mathbb{Z}_{a_j}$ 中的逆元） □

Definition 3.1.5 (本原单位根)**.** 令 $n \in \mathbb{Z}^+$，复数 $\xi \in \mathbb{C}$ 是 n 次单位根如果

$$\xi^n = 1.$$

如果满足

$$\xi^r \neq 1$$

对于任意 $1 \leq r \leq n-1$，称 ξ 是一个本原单位根。

Proposition 3.1.4. n 次单位根为

$$\xi_h = e^{2\pi i h/n}, \quad h = 0, 1, \cdots, n-1.$$

进一步有，

1. ξ_h 是 n 次本原根当且仅当 $gcd(h, n) = 1$
2. ξ_h 是第 r 个 n 的某个因此次本原根

3.2 质数

Definition 3.2.1. 一个整数 p 满足 $p > 1$ 且 p 没有除了自己本身和 1 两个因子之外的其他因子，则 p 称为质数（*prime*），否则称为合数（*composite*）。

Theorem 3.2.1 (欧几里得第一定理)**.** 如果 p 是一个质数且 $p \mid ab$，则要么 $p \mid a$ 或 $p \mid b$。

Proof. 设 $p \nmid a$，则由质数的定义 $gcd(p, a) = 1$，由 Bezout 定理，存在 $s, t \in \mathbb{Z}$ 使得

$$ps + at = 1$$

同乘 b，有

$$psb + abt = b$$

由 $p \mid ab$，所以 $p \mid b$。 □

Theorem 3.2.2. 任意 k 个连续的正整数都可以被 $k!$ 除尽。

Proof. 由组合数的定义

$$\frac{n(n-1)\cdots(n-k+1)}{k!} = \binom{n}{k} \in \mathbb{Z}$$

而上式左端即为 k 个连续的正整数的乘积，通过调整 n 的值即可证明结论。 □

Corollary 3.2.2.1. 如果 p 是一个质数，则 $p \mid \binom{p}{k}$ 对于任意 $1 \leq k \leq p-1$

Proof. 容易知道

$$p \cdot \frac{(p-1)!}{k!(p-k)!} = \binom{p}{k} \in \mathbb{Z}$$

由于 p 是质数，故分母 $k!(p-k)!$ 与 p 互素，所以一定有

$$\frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$$

因此，$p \mid \binom{p}{k}$。 □

Theorem 3.2.3 (欧几里得第二定理)**.** 质数的个数有无限个。

Proof. 反证法，假设素数有有限个 $p_1, p_2, \cdots, p_k$，则

$$p_1 p_2 \cdots p_k + 1$$

一定有素因子 p_i，这是不可能的。 □

Theorem 3.2.4 (算数基本定理（The fundamental theorem of arithmetic）)**.** 任意一个大于 1 的数要么是素数，要么可以被唯一分解为素因子的乘积。

Theorem 3.2.5. *令 $a, b \in \mathbb{Z}^+$，若*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \quad \text{与} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

则有

$$gcd(a,b) = \prod_{i=1}^{m} p_i^{\min(\alpha_i,\beta_i)}$$
$$lcm(a,b) = \prod_{i=1}^{m} p_i^{\max(\alpha_i,\beta_i)}$$

并且有 $gcd(a,b) \cdot lcm(a,b) = ab$

Note 3.2.1. 事实上，这给出了最大公约数与最小公倍数的一种表示方法。

Theorem 3.2.6. *1. 有无穷的 $4n+3$ 型质数；*

2. 有无穷的 $6n+5$ 型质数。

Proof. 只证 1，若只有有限多个 $4n+3$ 型质数，设最大的为 p，则

$$2^2 \cdot 3 \cdot 5 \cdot \cdots \cdot p - 1$$

也是 $4n+3$ 型质数，同时大于 p，矛盾。 □

Theorem 3.2.7 (Dirichlet 定理)**.** *设 a 是正整数而且 a, b 没有除 1 外其他因子，则有无限多个 $an+b$ 型质数。*

Theorem 3.2.8 (素数定理)**.** *记 $\pi(x)$ 为不超过 x 的素数的个数，则*

$$\pi(x) \sim \frac{x}{\log x}$$

换句话说，第 n 个质数 p_n 满足

$$p_n \sim n \log n$$

3.3 Euler totient 函数与 Mobius 反演公式

Definition 3.3.1 (Mobius 函数)**.** *一个整数 n 被称为是一个 square 如果存在整数 k 满足 $n = k^2$，cube 的定义类似。Mobius 函数 $\mu(n)$ 被定义为*

1. *$\mu(1) = 1$*
2. *$\mu(n) = 0$ 如果 n 是一个 square*
3. *$\mu(p_1 p_2 \cdots p_k) = (-1)^k$，如果 $p_1, p_2, \cdots, p_k$ 是不同的质数*

Example 3.3.1.

$$\mu(2) = -1, \mu(4) = 0, \mu(6) = 1$$

下面的定理给出了 $Mobius$ 函数的一些性质

Proposition 3.3.1. *1.* 对于任意 $n \in \mathbb{Z}^+$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{如果} n = 1; \\ 0, & \text{如果} n \geq 2 \end{cases}$$

2. 对于任意 $n \in \mathbb{Z}^+$,

$$\sum_{d|n} |\mu(d)| = 2^k$$

其中 k 为 n 的素因子个数

Theorem 3.3.1 (Mobius 反演公式)**.**

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) g(n/d)$$

Proof. 从左到右

$$\sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(d) \sum_{c|(n/d)} f(c) = \sum_{cd|n} \mu(d) f(c) = \sum_{c|n} f(c) \sum_{d|(n/c)} \mu(d) = f(n)$$

从右向左

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{c|d} \mu(c) g(d/c) = \sum_{d'|n} g(d') \sum_{c|(n/d')} \mu(c) = g(n)$$

□

Theorem 3.3.2. 假设 $gcd(m, m') = 1$，则

$$\mathbb{Z}_{mm'} = \{am' + a'm : a \in \mathbb{Z}_m, a' \in \mathbb{Z}_{m'}\}$$
$$\mathbb{Z}^*_{mm'} = \{am' + a'm : a \in \mathbb{Z}^*_m, a' \in \mathbb{Z}^*_{m'}\}$$

Proposition 3.3.2. 下面的这些函数是积性函数

1. 最大公约数函数 $gcd(n, k)$ 对任意给定的整数 k
2. *divisor function* $\sigma_k(n)$ 对于任意 $k \in \mathbb{N}$
3. *Mobius* 函数 $\mu(n)$
4. *Euler totient* 函数 $\phi(n)$.

Theorem 3.3.3. 设 $n \in \mathbb{Z}^+$，则

$$\phi(n) = n \prod_{prime\ p|n} (1 - \frac{1}{p}) = \sum_{d|n} d \cdot \mu(\frac{n}{d})$$

Theorem 3.3.4. 设 $n \in \mathbb{Z}^+$，则

$$\sum_{d|n} \phi(d) = n$$

Note 3.3.1. 上式实际上说明了 $\phi(n)$ 的 *Mobius* 反演为 n。

Theorem 3.3.5 (Fermat 小定理)**.** 设 $a \in \mathbb{N}$，若 p 是质数，则有

$$a^p \equiv a \mod p$$

或者

$$a^{p-1} \equiv 1 \mod p$$

Theorem 3.3.6 (Fermat-Euler 定理)**.** 若 $gcd(a, m) = 1$，则

$$a^{\phi(m)} \equiv 1 \mod m.$$

3.4 二次剩余

Definition 3.4.1. 设 $m \in \mathbb{Z}^+$，a 为模 m 的剩余，我们称 a 是二次剩余（*quadratic residue*）如果下面的同余方程有解

$$x^2 \equiv a \mod m$$

，否则称为二次非剩余（*quadratic nonresidue*）。对于一个奇质数 p 和整数 m，定义 *Legendre* 符号为

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{如果 } a \text{ 是 } p \text{ 的二次剩余且 } p \nmid a \\ -1, & \text{如果 } a \text{ 是 } p \text{ 的二次非剩余} \\ 0, & \text{如果 } p \mid a \end{cases}$$

我们可以将 *Legendre* 符号推广到 *Jacobi* 符号

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{\alpha_j}$$

其中 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 是 n 的素因子分解，特别地

$$\left(\frac{n}{1}\right) = 1.$$

Proposition 3.4.1. *Jacobi* 符号满足下列的性质

1. 当 $n = p$ 时，*Jacobi* 符号就是 *Legendre* 符号
2. 对于任意整数 m，都有
$$\left(\frac{a}{n}\right) = \left(\frac{a + mn}{n}\right)$$

3. *Jacobi* 符号等于零当且仅当 $gcd(a,n) \neq 1$

4. *Jacobi* 符号对于每一个变量都是积性函数，*i.e.*

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \quad \text{和} \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

Theorem 3.4.1 (Wilson 定理)**.** 对于任意素数 p，有

$$(p-1)! \equiv -1 \mod p$$

Theorem 3.4.2 (Euler 判别法)**.** 若 p 是奇质数且 p 不整除 a，则

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

其中是 *Legendre* 符号

Example 3.4.1. 对于给定数，寻找其为二次剩余的模数。如令 $a = 17$，则 $p = 3$，有 $17^{\frac{3-1}{2}} \equiv 2 \mod 3 \equiv -1 \mod 3$，于是 17 不是 3 的二次剩余。

Theorem 3.4.3 (Gauss 引理)**.** 若 p 是奇质数且 p 不整除 a，则 *Legendre* 符号

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

其中 μ 是下列集合中数模去 p 大于 $p/2$ 的数的个数

$$S'_p(a) = \{a, 2a, \cdots, \frac{p-1}{2} \cdot a\}$$

Theorem 3.4.4. 设 p 是一个奇素数，则共有 $(p-1)/2$ 个二次剩余和 $(p-1)/2$ 个二次非剩余，并且满足如下的关系

1. 两个二次剩余的乘积仍是二次剩余

2. 两个二次剩余的乘积是二次非剩余

3. 二次剩余和二次非剩余的乘积是二次非剩余

Example 3.4.2. 设 $p = 11$ 和 $a = 7$，则 $S'_{11}(7) = \{7, 14, 21, 28, 35\}$，模掉 11 后，大于 11/2 的个数 $\mu = 3$，于是 $\left(\frac{7}{11}\right) = -1$，即 7 不是 11 的二次剩余。

Proposition 3.4.2. *1.* -1 是 $4n+1$ 型质数的二次剩余，是 $4n+3$ 型质数的二次非剩余

2. 2 是 $8n \pm 1$ 型质数的二次剩余，是 $8n \pm 3$ 型质数的二次非剩余

3. -3 是 $6n+1$ 型质数的二次剩余，是 $6n+5$ 型质数的二次非剩余

4. 7 是 $10n \pm 1$ 型质数的二次剩余，是 $10n \pm 3$ 型质数的二次非剩余

Theorem 3.4.5 (Gauss 二次互反律)**.**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Example 3.4.3.

$$\begin{aligned}\left(\frac{1001}{9907}\right) &= \left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right) = \left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right) = \left(\frac{449}{103}\right) \\ &= \left(\frac{37}{103}\right) = \left(\frac{103}{37}\right) = \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3 = -1\end{aligned}$$

Note 3.4.1. 注意到 29 是 $8n \pm 3$ 型奇素数

Example 3.4.4.

$$\left(\frac{37}{89}\right) = \left(\frac{89}{37}\right) = \left(\frac{15}{37}\right) = \left(\frac{5}{37}\right)\left(\frac{3}{37}\right) = \left(\frac{37}{5}\right)\left(\frac{37}{3}\right) = \left(\frac{2}{5}\right)\left(\frac{1}{3}\right) = -1$$

Chapter 4

图论 Graph Theory

4.1 基本定义与概念

Definition 4.1.1 (图)**.** 一个图 *(graph)* 是一个二元有序对 (V, E), 其中 V 是所有顶点 (*vertices*) 的集合, E 是所有边 *edges* 的集合。一条边 (u, v) 常被写作 uv。$V(G)$ 和 $E(G)$ 分别为图 G 的顶点和边的集合。一个图 G 的阶 (*order*) 是图的顶点个数 (*cardinality*) $|V(G)|$。对于 $v \in V(G)$, 如果存在 $uv \in E(G)$, 我们称 u 和 v 是邻接 (*adjacent*) 的, 否则称为非邻接 (*nonadjacent*) 的。顶点 v 的邻居 (*neighborhood*), 被记做 $N_G(v)$ 是所有与 v 邻接的顶点的集合。

Definition 4.1.2 (简单图)**.** 一个简单图是一个既没有重边 (*multiple edge*) 也没有环 (*loop*) 的图。

Definition 4.1.3 (补图)**.** 给定一个简单图 $G = (V, E)$, 它的补图 (*complement*) 的定义为简单图

$$\bar{G} = (V, \bar{E}),$$

其中 $\bar{E} = V^2 \backslash E$。意思是 $\bar{G}$ 中的点之间有边相连当且仅当在 G 里面他们没有边相连。我们构建补图时可先构建完全图 $K_{|V(G)|}$, 再删除 G 中出现过的边即可。

Definition 4.1.4 (团)**.** 团 (*clique*) 是 G 中的一组满足两两之间有边连接的顶点的集合。图 G 的团数 (*clique number*) 是指图 G 中最大的团的阶数。

Definition 4.1.5 (独立集)**.** 图 G 独立集 (*independent set*) 或稳定集 (*stable set*) 是一族两点之间互不相连的定点的集合。G 的独立数 (*independent number*), 记为 $\alpha(G)$, 是 G 中最大的独立集的阶数 (*order*)。

Definition 4.1.6 (孤立点)**.** 一个顶点被称为孤立点当且仅当它没有邻居, *i.e.*

$$N_G(v) = \emptyset$$

Definition 4.1.7 (邻接矩阵与关联矩阵)**.** 图 G 是一个顶点和边分别为

$$V = \{v_1, v_2, \cdots, v_n\} \text{ 和} E = \{e_1, e_2, \cdots, e_m\}$$

图 G 的邻接矩阵（*adjacency matrix*）是指矩阵 $(a_{ij})_{n\times n}$，其中 a_{ij} 是顶点 v_i 和 v_j 间的边数(简单图中只能为 *0* 或 *1*)。图 G 的关联矩阵（*incidence matrix*）是指矩阵 $(b_{ij})_{n\times m}$，其中

$$b_{ij} = \begin{cases} 1, \text{如果顶点 } v_i \text{ 与边 } e_j \text{ 相连} \\ 0, \text{其他情况} \end{cases}$$

一个图的谱（*spectrum*）是指邻接矩阵的所有特征值的集合。

Definition 4.1.8 (度数)**.** 图 G 的一个顶点 v 的度数（*degree*）是与 v 连接的边的数量，常被记做 $deg_G(v)$。度序列（*degree sequence*）是指一个由所有顶点的度从大到小排列而成的序列。一个图被称为正则的（*regular*）如果所有顶点的度相同。一个图被称为 k-正则（*k-regular*）如果它的所有顶点的度数都相同且为 k。一个图被称为 *cubic* 的如果它是 *3*-正则的。图 G 的最大与最小度被分别记为 $\Delta(G)$ 与 $\delta(G)$。如果一个顶点的度为 1 则它被称为叶（*leaf*）。一个连接叶的边被称为叶边（*leaf edge*）。

Note 4.1.1. 一个环（*loop*）对度的贡献为 2。

Theorem 4.1.1 (握手引理（the Handshaking Lemma）)**.** 对于任何有限图 $G = (V, E)$，我们有

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

Note 4.1.2. 很自然的能看出图 G 中一定有偶数个度数为奇数的顶点。

Theorem 4.1.2. 一个非降的非负整数序列 $d_1 \geq d_2 \geq \cdots \geq d_n$ 成为一个度序列的充分必要条件为 $\sum\limits_{i=1}^{n} d_i$ 是偶数。

Definition 4.1.9. 设 $G = (V, E)$ 是一个简单图。G 的子图（*subgraph*）是图 (V', E')，其中 $E' \subseteq E$，$V' \subseteq V$，并且 V' 包含 E' 中所有边的端点。生成子图（*spanning subgraph*）也称作 G 的一个因子（*factor*），是一个子图并且包含原图 G 的所有端点。G 有 k-因子（*k-factor*）是指一个每个顶点的度都为 k 的生成子图。图 G 的分解（*factorization*）是指将一个图的所有边都分拆为因子（*factors*）。诱导子图（*induced subgraph*）是子图 (V', G')，如果 V' 中的顶点在 G 中相连，则他们一定在 G' 中相连。一个顶点集 $U \subseteq V$ 的邻居（*neighborhood*）定义为 U 中所有顶点的邻居的并，即

$$N_G(U) = \bigcup_{v\in U} N_G(v)$$

Definition 4.1.10. 一个 *walk* 是一个边（*edges*）的序列。*walk* 的长度是指它所含的边的个数。一个 *walk* 是闭合的（*closed*）当且仅当它的起始点和终点相同。一个 *trail* 是一个 *walk* 且不经过重复的边。一个 *path* 是一个 *trail* 且不经过重复的顶点。两个顶点的距离被定义为两个顶点间最短的 *path* 的长度。一张图的直径（*diameter*）是最短距离的最大值。图的 *Eulerian path* 是一

个 *trail* 而且访问过所有边，一个 *Eulerian circuit* 是一条到访过所有边的 *trail*。一个图被称为 *Eulerian* 如果它包含一个 *Eulerian* 回路。*Hamiltonian path* 是一个生成子图（到访所有顶点）。

Definition 4.1.11. 一个 *k-cycle* 是简单图 G 中的闭合 $walkv_1v_2\cdots v_kv_1$ 并且不经过重复的边，进一步，一个 *k-cycle* 同构与 C_k。一个图被称为 *acyclic* 如果它不包含 *cycle*，这样的图被称为森林（*forest*）。图的围长（*girth*）是指图中最短的圈常，*circumference* 是指图中最长的圈的长度。一个图是 *Hamiltonian* 的当且仅当它的 *circumference* 等于它的度数（*order*）。

Definition 4.1.12. 一个图被称为连通的（*connected*）如果每一对顶点之间都有一条 *path*，否则被称为不连通的（*disconnected*）。一个连通分支（*connected component*）是指图 G 中最大的连通子图，一个奇分支（*odd component*）是一个阶为奇数的分支，否则称为偶分支。

Definition 4.1.13. 对于 $k \in \mathbb{Z}^+$，一个图被称为 *k-connected* 的如果去除任意 $k-1$ 个顶点后该图都是连通的。图 G 连通度（*connectivity*），记做 $\kappa(G)$ 是最大的 k 使得图 G 是 *k-connected*。

Theorem 4.1.3. 一个简单图 G 是连通的如果

$$\delta(G) \geq \frac{|V(G)|}{2}.$$

Definition 4.1.14. 令 $k \geq 2$。一个 k 部图（*k-partite*）是指图 $G = (V, E)$ 满足它可以被分解为 k 个非空稳定集（*stable sets*）（内部不连通）。一个图被称为多部图（*multipartite*）如果 $k \geq 2$。一个 2-*partite* 图也被称为 *bipartite* 图。它的顶点集可被分解为

$$V = V_1 \sqcup V_2$$

Theorem 4.1.4. 任意的连通二部图的分解是惟一的。

Theorem 4.1.5. 一个有限连通图是欧拉图当且仅当所有顶点的度数都是偶数。

Definition 4.1.15. 如下是一些常见图的例子

1. 空图（*empty graph*）是指图 (V, E) 满足 $V = E = \emptyset$
2. n 阶完全图（*complete graph*），记做 K_n 是指有 n 个顶点且任意两个顶点都相邻的图。
3. 完全 k-部图（*complete k-partite graph*），记做 $K_{n_1,n_2,\cdots,n_K} = (V, E)$ 是指简单图其顶点被分为了非空集合 $V_1, V_2, \cdots, V_k$，其中 $k \geq 2$ 且 $|V_i| = n_i$ 对于任意 i 成立且满足
4.
$$E = \bigcup_{i \neq j} (V_i \times V_j).$$

   意思是任意两个不属于同一部分的顶点都有边相连。

   完全多部图是指完全 k-部图且 $k \geq 2$。一个完全二部图形为 K_{n_1,n_2}。*Turan* 图是一个完全 k-部图 $K_{n_1,n_2,\cdots,n_K}$ 且满足

$$|n_i - n_j| \leq 1$$

   对于任意 i 和 j 都成立。

5. n 阶 *path graph*，记做 P_n，是指一个简单图 (V,E)，其中

$$V = \{v_1, v_2, \cdots, v_n\} \text{ 并且}$$
$$E = \{v_1v_2, v_2v_3, \cdots, v_{n-1}v_n\}$$

6. n 阶 *cycle graph*，记做 C_n，是指简单图 (V,E)，其中

$$V = \{v_1, v_2, \cdots, v_n\} \text{ 并且}$$
$$E = \{v_1v_2, v_2v_3, \cdots, v_{n-1}v_n, v_nv_1\}$$

   C_3, C_4, C_5, C_6 分别被称为 *triangle, rectangle, pentagon* 和 *hexagon*。

7. 树（*tree*）是一个不含 *cycle* 的连通图。星（*star*）是一个形如 K_1, n 的图，其中 $k \geq 2$。*claw* 是 *star* $K_1, 3$，*caterpillar* 是一个树且满足它们所有顶点距离中心 *path* 的距离小于 1，*lobster* 是一个树且满足它们所有顶点距离中心 *path* 的距离小于 2。

8. 一个 n 阶（$n \geq 4$）轮图（*wheel graph*），记做 W_n，是一个简单图 (V,E) 满足

$$V = \{v_1, v_2, \cdots, v_n\} \text{ 并且}$$
$$E = \{v_0v_i : 1 \leq i \leq n-1\} \cup \{v_1v_2, v_2v_3, \cdots, v_{n-1}v_n, v_nv_1\}.$$

9. 一个通过 n 阶完全图 K_n 删去一个顶点的图常被记做 $K_n - e$。钻石（*diamond graph*）是指图 $K_4 - e$

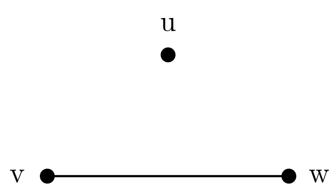
10. *Petersen graph* 是指简单图 $G = (V,E)$ 满足

$$V = \binom{[5]}{2} \text{ 和} E = \{uv \in V^2 : u \cap v = \emptyset\}$$

   它有 10 个顶点 15 条边。

11. 超立方图（*hypercube graph*），记做 Q_k 是一个简单图，顶点集合是一个 k 维 01 向量，两个顶点相邻当且仅当只有一个位置上的数不同。

Proposition 4.1.1. 令 G 是一个简单图，G 是一个完全多部图当且仅当 G 是 $K_1 + K_2$-*free* 的



Proof. 首先证明必要性，假设 $G = K_{n_1,\cdots,n_k} = (V,E)$ 是一个完全多部图，顶点可以被划分为

$$V = \sqcup_{i=1}^k V_i.$$

则对于任意 $u, v, w \in V$ 满足

$$uv \notin E \text{和} uw \notin E.$$

由于 $uv \notin E$ 于是 u, v 在同一个部分，称作 V_i，由 $uw \notin E$，我们知道 $w \in V_i$。于是有 $vw \notin E$，于是得出 G 是 $K_1 + K_2$-free 的。

下面证明充分性，假设 G 是 $K_1 + K_2$-free 的，需证 G 是完全多部图，假设 $uv \notin E$，则 w 要么与 u, v 都相连要么都不相连，这定义了 G 上的一个等价关系。 □

Proposition 4.1.2. *Petersen graphP 满足下列性质：*

1. *P 是三正则（cubic）的；*
2. *两个不相邻的顶点有一个共同的 neighbor；*
3. *P 的 girth 是 5；*
4. *P 有 10 个 claw，有 10 个长为 6 的 cycle。*

Definition 4.1.16. 设 G 和 H 是两个图。一个 G 与 H 之间的同构映射（*isomorphism*）是一个双射 $f : V(G) \to V(H)$ 满足

$$uv \in E(G) \Leftrightarrow f(u)f(v) \in E(H)$$

即在 G 中相连的两个顶点在 H 中也相连。

Definition 4.1.17. 令 G 是一个简单图，G 的顶点覆盖（*vertex cover*）是一组与所有边都相接的顶点。顶点覆盖数（*vertex cover number*）是 G 中最小的 *vertexcover* 中的顶点个数，记做 $\beta(G)$。边覆盖（*edge cover*）是指一组与所有边都相接的顶点个数。如果一族顶点 S，对于任意顶点 $v \in V(G)$，要么 v 在 S 中要么 v 与 S 中的某个顶点 u 相邻，则被称为 *dominatingset*。*dominating number* 是指 G 中的最小的 *dominating set* 的大小，记做 $\gamma(G)$。

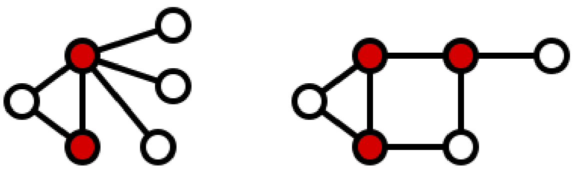


Figure 4.1
Vertex cover

Definition 4.1.18. 如下是对图 $G = (V, E)$ 的一些简单的操作（*operation*）

1. 删除 G 中的一个顶点（*deleting a vertex*）v 是指从顶点集删去该点后删掉所有与该点相连的边

$$(V \backslash \{v\}, E \backslash \{vu, u \in N(v)\})$$

2. 删除 G 中的一条边（*deleting an edge*）e

$$(V, E \backslash \{e\})$$

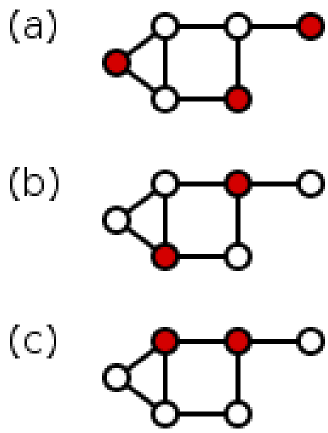


Figure 4.2
dominating set

3. 两张图的不交并（*disjoint union*），记做 $G+H$，是指

$$G+H=(V\sqcup V',E\sqcup E')$$

4. 两张图的并（*union*）记做 $G\vee H$，是指

$$G\vee H=(V\sqcup V',E\sqcup E'\cup(V\times V'))$$

是指将 $G+H$ 的边并上所有 $V\times V'$ 的边，即连接 V 与 V' 所有的顶点。

5. 复制顶点（*duplicating a vertex*）v 是指

$$(V\cup\{v'\},E\cup\{v'x:vx\in E\}).$$

v' 被称为 v 的一个 *twin*，意思是将 v 复制出一个 v'，原先与 v 相连的顶点在新图中都与 v' 相连。

6. G 的线图（*line graph*），记做 $L(G)$，是指图 E,F，若边 $e,e'\in E$ 在 G 中相邻，则在 $L(G)$ 中该两点相连。

7. 图 G 的 *subdivision* 是指将 G 中的某些边中加入内点，再连接起来。

8. 一个图 H 被称作 G 的一个 *minor* 如果它能通过删除 G 边或顶点和在 G 中连线得到的。

9. 一个图 H 被称作 G 的一个 *topological minor* 如果它包含一个是 H 的 *subdivision* 的子图。

下面是这些操作的具体图例， 下面的定理是极值图论（extremal graph theory）

Theorem 4.1.6. 一个 *triangle-free* 的 n 顶点简单图中边数最大为 $\lfloor n^2/4\rfloor$

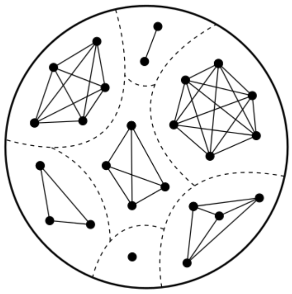


Figure 4.3
disjoint union of some complete graphs

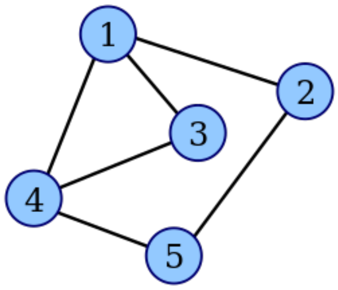


Figure 4.4
Graph G

Proof. 设 G 是一个 n 个顶点的 triangle-free 简单图，令 A 是最大的独立集，其中 $\alpha = |A|$。因为 G 是 triangle-free 的，于是每个顶点的 neighborhood 都是稳定的，即对于任意 v

$$\deg v \leq \alpha$$

。因为 $V \backslash A$ 和 G 的所有顶点都相连，利用均值不等式既有

$$|E| \leq \sum_{V \in V \backslash A} \deg v \leq \alpha(n-\alpha) \leq (\frac{n}{2})^2$$

□

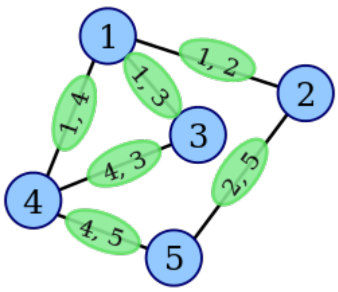


Figure 4.5
Vertices in $L(G)$constructed from edges in G

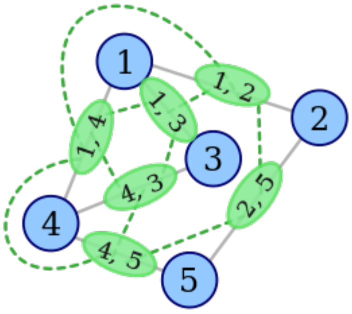


Figure 4.6
Added edges in $L(G)$

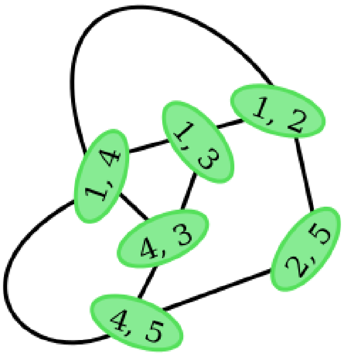


Figure 4.7
The line graph $L(G)$

Theorem 4.1.7. *(Turan 定理)* 设 $p \geq 2$ 和 $n \geq p+1$。令 S 是一个不包含 *p-cliques* 且有 n 个顶点的简单图。则所有满足这样的条件拥有最多边数的图同构与一个 $p-1$ 部 *Turan* 图。

Definition 4.1.19. 一个有向图（*directed graph or digraph*），是一张每条边都有一个或两个方向的图，每一条边被称为一个 *arc*。如果图中有一条从 u 到 v 的有向边，则称 v 是 u 的 *successor* 并称 u 是 v 的 *predecessor*。进入 v 的边数称为 v 的入度（*indegree*），反之为出度（*outdegree*）。一个有向图 D 的 *underlying graph* 是指去除 D 中边的方向。一个有向图是弱连通（*weakly connected*）的如果它的 *underlying graph* 是连通的，有向图 D 任意两个顶点 u, v 都有一条 *directed path* 相连则称它是强连通（*strongly connected*）。强连通分支（*strong component*）是有向图中最大的强连通子图。

Definition 4.1.20. 竞赛图（*tournament*）是一个被指定方向的完全有向图。*king* 是一个有向

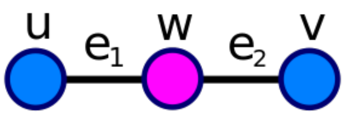


Figure 4.8
subdivision of uv

图中的顶点满足所有的顶点都可以至多两步到达 *king*。

Proposition 4.1.3. 任意一个竞赛图都有一个 *king*。

4.2 树 Trees

Theorem 4.2.1. 简单图 G 是 n 阶树（*Tree*）如果下面等价的断言成立

1. G 连通（*connected*）无圈（*acyclic*）。
2. 任意两个顶点有且只有一条路径（*path*）。
3. G 是一个极大连通图，即任意删除一条边 G 都不连通。
4. G 是最小无圈图，即任意连一条边后 G 至少会变成有圈图。
5. G 连通且有 $n-1$ 条边。
6. G 无圈且有 $n-1$ 条边。