1 代数结构

1.1 群的定义

定义 1 (3.2.1). 若 G 为一非空集合，若其上代数运算满足结合律，则称 G 为**半群**；若 G 中还存在幺元，则称 G 为**幺半群**。

定义 2 (3.2.3). 若幺半群 G 上代数运算满足每个元素都有逆，就称 G 为**群**；如果该运算满足交换律，就称 G 为**交换群**。

例 1 (3.2.4). 半群 G 有左幺元 1_L，每个元素有左逆元，则 G 是群。

1.2 置换群

注 1. 映射从右往左复合！

命题 1 (3.2.12). S_n 中所有偶置换对于置换乘法构成一个群。

推论 1 (3.2.15). 设 $\sigma \in S_n$ 的轮换分解中有 c 个轮换，则 $(-1)^{\mathrm{sgn}(\sigma)} = (-1)^{n-c}$。

定义 3. 设 G 是群，$a, b \in G$，令 a**共轭作用**于 b，就是计算 aba^{-1}，后者称为与 b**共轭**的元素。如果与 b 共轭的元素只有 b，就说明 b 与 G 中任意元素都可交换，所有这样的 b 构成的集合称为 G 的**中心** Z_G。

1.3 子群

定义 4 (3.2.20). 设 G 是群，若 $\varnothing \neq H \subseteq G$ 在 G 的运算下也构成一个群，就称 H 为 G 的一个**子群**，记作 $H \leqslant G$。

定理 1 (3.2.22). 设 G 是群，非空集合 $H \subseteq G$ 是 G 的子群当且仅当 $\forall a, b \in H, ab^{-1} \in H$。

例 2 (3.2.23). 任意群 G 都有 $Z_G \leqslant G$。证明只需要验证上述等价条件。

例 3 (3.2.24). 设 G 是群，$H \leqslant G$，取定 $g \in G$，则 $gHg^{-1} \leqslant G$，称为 H 的**共轭子群**。

例 4 (3.2.25). 设 G 是群，$H, K \leqslant G$，则 $H \cup K \leqslant G$ 当且仅当 $H \subseteq K$ 或 $K \subseteq H$。

定义 5 (3.2.26). 设 S 是群 G 的非空子集，G 中所有包含 S 的子群的交称为 S**生成**的子群，记为 $\langle S \rangle$。若 $G = \langle S \rangle$，则称 G 由 S 生成，S 称为**生成元集合**。

1.4 阶与 Lagrange 定理

定义 6 (3.2.28). g 是群 G 中元素，称最小满足 $g^n = 1$ 的正整数 n 为 g 的**阶**，记为 $\mathrm{ord}(g)$。如果不存在，则认为 $\mathrm{ord}(g) = \infty$。

定理 2 (3.2.29). 设群 G 中元素 g 具有有限的阶，则 $\langle g \rangle = \{1, g, g^2, \cdots, g^{\mathrm{ord}(g)-1}\}$，称为 g 生成的**循环群**。

定义 7 (3.2.36). 设 G 是群，$H \leqslant G, a \in G$，称 $aH = \{ah : h \in H\}$ 为 H 的一个**左陪集**，$Ha = \{ha : h \in H\}$ 为 H 的一个**右陪集**。a 称为**陪集代表元**，注意代表元不唯一。

定理 3 (3.2.38, 陪集分解). 设 G 是群，$H \leqslant G$，则 H 的任意两个左 (右) 陪集都相等或者不交，且 G 可以表示为若干个左 (右) 陪集的不交并。

推论 2 (3.2.39, Lagrange). 设 G 是有限群，$H \leqslant G$，则 $|H|$ 是 $|G|$ 的因子。这个倍数称为 H 的**指数**，记为 $[G : H]$。

推论 3 (3.2.40, 望远镜法则). 设 G 是有限群，$K \leqslant H \leqslant G$，则 $[G : K] = [G : H][H : K]$。

例 5 (3.2.41). 设 G 是有限群，$H, K \leqslant G$，则 $|HK| = \frac{|H||K|}{|H \cap K|}$。

推论 4 (3.2.42). 设 G 是有限群，则 $\forall g \in G, \mathrm{ord}(g) \mid |G|$，从而有 $g^{|G|} = 1$。

推论 5 (3.2.44). 素阶群一定是循环群。

定理 4 (3.2.45). 设 $G = \langle g \rangle$ 是循环群，则其一切子群都是循环群。无限循环群的全部子群是 $\{\langle g^t \rangle : t \in \mathbb{Z}_{\geqslant 0}\}$，$m$ 阶循环群的全部子群是 $\{\langle g^d \rangle : d|m\}$。循环群任一大小子群唯一。

1.5 群同态与正规子群

定义 8 (3.2.46). 设 G, H 是两个群，映射 $\sigma : G \to H$ 称为**同态**，如果它保运算

$$\forall x, y \in G, \sigma(x)\sigma(y) = \sigma(xy)$$

如果同态 σ 是单射，就称为**单同态**或**嵌入**，如果是满射就称为**满同态**，如果是双射就称为**同构**，记作 $G \cong H$。

定义 9 (3.2.51). 设 $\sigma : G \to H$ 是同态，称 $\{g \in G : \sigma(g) = 1_H\}$ 为**同态核**，记为 $\ker \sigma$。

命题 2. 设 $\sigma : G \to H$ 是同态，$\ker \sigma = K$，则左陪集 aK(右陪集 Ka) 给出了该同态下像为 $\sigma(a)$ 的一切元素。

例 6 (3.2.55). H 是子群当且仅当 $HH^{-1} = H$。设 G 是群，$H, K \leqslant G$，则 $HK \leqslant G$ 当且仅当 $HK = KH$。

定义 10. 把陪集的全体 $\{gK : g \in G\}$ 在“按代表元相乘”的运算下构成的群称为 G 模 K 的**商群**。

定义 11 (3.2.58). 设 G 是群，$H \leqslant G$，称 H 是 G 的**正规子群**，如果 $\forall g \in G$ 都有 $gH = Hg$，记为 $H \lhd G$。

推论 6 (3.2.59). 交换群的任意子群都是正规子群。$H \lhd G$ 的充要条件是 $\forall g \in G, h \in H, ghg^{-1} \in H$。

命题 3. 同态核与正规子群是一回事。一方面同态核一定是正规子群，另一方面对于正规子群 $N \lhd G$，构造**典范同态** $G \to G/N : g \to gN$，可以使同态核恰好为 N。

命题 4. 设 G 是群，$H \leqslant G$，若 $[G : H] = 2$，则 H 是 G 的正规子群。

命题 5. 设 G 是有限交换群，$|G| = n$，p 是素数且 $p \mid n$，则 G 中存在 p 阶元。

1.6 四个同构定理

定理 5 (3.2.61, 第一同构定理). 设 $\varphi : G \to H$ 是群同态，则 $G/\ker\varphi \cong \mathrm{im}\ \varphi$。

推论 7 (3.2.63, 循环群分类定理). 无限循环群都同构于 $\mathbb{Z}$，有限循环群都同构于某个 $\mathbb{Z}_n$。

定理 6 (3.2.64, 第二同构定理). 设 G 是群，若 $N \lhd G, H \leqslant G$，则 $H \cap N \lhd H, N \lhd NH \leqslant G$，且 $NH/N \cong H/(H \cap N)$。

证明 1. 注意

$$NH = \bigcup_{h \in H} Nh = \bigcup_{h \in H} hN = HN$$

故由 3.2.55 知 $NH \leqslant G$，根据定义验证 $N \lhd NH$。考虑映射 π

$$H \to NH/N : h \to hN$$

$\ker \pi = \{h \in H, hN = N\} = H \cap N$，由于是同态，根据第一同构定理，得到 $NH/N \cong H/(H \cap N)$，从而 $H \cap N \lhd H$。

定理 7 (3.2.65, 第三同构定理). 设 G 是群，$N, M \lhd G$ 且 $N \leqslant M$，则 $G/M \cong (G/N)/(M/N)$。

证明 2. 考虑映射 π

$$G/N \to G/M : gN \to gM$$

由 $N \leqslant M$ 只映射良定，而 $\ker \pi = \{gN \in G/N : gM = M\} = M/N$，由于 π 是同态，由第一同构定理知 $(G/N)/(M/N) \cong G/N$。M/N 是 G/N 的正规子群。

1.7 群直积

定义 12 (3.3.35). 设 G_1, G_2 是群，在 $G_1 \times G_2$ 上定义运算 $(g_1, g_2) \times (g_1', g_2') = (g_1 g_1', g_2 g_2')$，得到的群称为 G_1 与 G_2 的**直积**，G_1, G_2 称为**直积因子**。

例 7 (3.3.36). 设 G, H 分别为 m, n 阶循环群，则 $G \times H$ 是循环群当且仅当 $\gcd(m, n) = 1$。

定理 8 (3.3.38). 设 H, K 是群 G 的子群，若(i)$G = HK$ (ii)$H \cap K = \{1\}$ (iii)H, K 中元素可交换，即 $\forall h \in H, k \in K, hk = kh$，则 $G \cong H \times K$，此时称 G 为 H, K 的**内直积**。

1.8 有限交换群结构

引理 1 (3.3.41). 任意有限交换群都是其 Sylow 子群 (阶为 p^r 的子群) 的内直积。

引理 2 (3.3.42). 设 A 是有限交换 p 群 (阶为 p^r)，则 A 循环当且仅当它只有一个 p 阶子群。

引理 3 (3.3.42). 设 A 是非循环有限 p 群，设 a 是 A 中的最高阶元素，则存在 $B \leqslant A$ 使得 $A = \langle a \rangle B$。

定理 9 (3.3.44). 有限交换 p 群可分解为循环子群的直积 $A = \langle a_1 \rangle \times \cdots \times \langle a_t \rangle$，其中 t 和每个直积因子的阶 $p^{m_1}, \cdots, p^{m_t}$ 由 A 唯一决定。

定理 10 (3.3.45, 有限交换群结构定理, 初等因子). 设 G 是 n 阶交换群，则

$$G \cong \prod_{i=1}^{s} (\mathbb{Z}_{p_i^{l_{i1}}} \times \cdots \times \mathbb{Z}_{p_i^{l_{ik_i}}})$$

其中 $l_{i1} \leqslant \cdots \leqslant l_{ik_i}, \sum_{j=1}^{k_i} l_{ij} = e_i$。多重集

$$\{p_1^{l_{11}}, \cdots, p_1^{l_{1k_1}}, \cdots, p_s^{l_{s1}}, \cdots, p_s^{l_{sk_s}}\}$$

由 G 唯一决定，称为 G 的**初等因子**。

定理 11 (3.3.46, 有限交换群结构定理, 不变因子). 设 G 是 n 阶交换群，则

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$$

其中 $k = \max_{j=1}^{s} k_s, d_1 | \cdots | d_k, \prod_{j=1}^{k} d_j = n$ 由 G 唯一决定，称为 G 的**不变因子**。

推论 8 (3.3.48). 有限交换群 G 是循环群 (不变因子分解中 $k = 1$) 当且仅当 $\forall m \in \mathbb{Z}_{\geqslant 1}, x^m = 1$ 在 G 中的解至多 m 个。

1.9 环和域的定义

定义 13 (3.4.1). R 是一非空集合，有两种代数运算，满足(i)$(R, +)$ 构成交换群，(ii)$(R, \times)$ 构成幺半群，(iii)(左右) 乘法分配律成立，就称 R 是**环**。如果乘法还是交换的，就称 R 是**交换环**。注意我们默认环有乘法幺元。

定义 14 (3.4.4). 若环 R 满足 $R^* = R \setminus \{0\}$ 对乘法构成群，就称 R 是**除环**或**体**。

环中的可逆元称为**单位**，所有单位构成环的**单位群**，于是除环也可以说是单位群等于 R^* 的环。

定义 15 (3.4.7). 若 $a, b \in R^*$ 满足 $a, b = 0$，则称 a 是**左零因子**，b 是**右零因子**。无零因子交换环称为**整环**，交换除环称为**域**。

命题 6 (3.4.10). 有限整环是域。只需要验证每个非零元可逆。

1.10 环同态与理想

定义 16 (3.4.12). 设 R, R' 是两个环，映射 $\sigma : R \to R'$ 称为**环同态**，如果它保运算

$$\sigma(x+y) = \sigma(x) + \sigma(y), \sigma(xy) = \sigma(x)\sigma(y), \sigma(1_R) = 1_{R'}$$

注 2. $\sigma(1_R) = 1_{R'}$ 是必需的，因为乘法只构成幺半群，但如果是域同态，就不需要这条。此外域同态一定是单同态或零同态。

定义 17 (3.4.15). 设 R 是环，加法子群 $S \subseteq R$ 称为**左理想**，如果 $\forall r \in R, rS \subseteq S$；称为**右理想**，如果 $\forall r \in R, Sr \subseteq S$；同时是左理想和右理想的 S 称为**理想**。“黑洞”

推论 9. $\{0\}, R$ 是 R 是平凡理想。非平凡理想的元素都不可逆。

定义 18 (3.4.19). 设 R 是环，若 $S \subseteq R$ 在 R 的运算下构成一个环，就称 S 是 R 的**子环**。

命题 7. 非平凡理想都不是子环。包含 1_R 的理想就是整个 R。

定义 19. 理想是加法的正规子群，因此 $\{a + I : a \in R\}$ 构成一个环，称为 R 对 I 的**商环** R/I。

定理 12. 设 $f : R_1 \to R_2$ 是环同态，则 $\ker f$ 是 R_1 的理想。

定义 20 (3.4.22). 设 $a \in R$，R 中所有含 a 的理想的交 (显然还是理想) 称为 a 的**主理想**，记为 (a)。若环 R 中的理想都是主理想，则称 R 是**主理想环**。同样可定义子集 S**生成**的理想和**生成元集合**。

命题 8 (3.4.25). $\mathbb{Z}, F[x]$ 是主理想环。“带余除法”

2 组合计数

2.1 Pólya 方法

引理 4 (3.3.23, Burnside). 设有限置换群 G 作用在 X 上，$\mathrm{fixed}(g)$ 表示 $g \in G$ 置换下的不动点集合，$\mathrm{Stab}(x)$ 表示 G 中满足 $gx = x$ 的 g 的集合，$\mathrm{orb}(x) = \{gx : g \in G\}$ 为 x 的轨道。

$$\begin{aligned} |X \setminus G| &= \sum_{x \in X} \frac{1}{|\mathrm{orb}(x)|} = \frac{1}{|G|} \sum_{x \in X} |\mathrm{Stab}(x)| \\ &= \frac{1}{|G|} \sum_{g \in G} |\mathrm{fixed}(g)| \end{aligned}$$

定理 13 (4.3.6, Pólya). A 是元素集，B 是色盘，G 是 A 上的置换群，$c(\sigma)$ 表示 $\sigma \in G$ 的轮换分解中轮换数 (环数)，则 G 在 B^A 上的轨道数量为

$$\frac{1}{|G|} \sum_{\sigma \in G} |B|^{c(\sigma)}$$

2.2 组合恒等式

定理 14 (组合数上指标求和/平行求和).

$$\sum_{k=0}^{m} \binom{k}{n} = \binom{m+1}{n+1}$$

定理 15 (Vandermonde 恒等式).

$$\sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k} = \binom{m+n}{r}$$

定理 16 (Lucas).

$$\binom{n}{k} = \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} \binom{n \bmod p}{k \bmod p} \mod p$$

定理 17 (组合反演式).

$$b_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k a_k \Leftrightarrow a_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k b_n$$

2.3 Ramsey 理论

定理 18 (4.4.8, Ramsey). 设 $k,l \geqslant 2$ 是正整数，总存在一个最小的正整数 $R(k,l)$(称为 **Ramsey 数**)，使得当 $n \geqslant R(k,l)$ 时，完全图 K_n 的任意红蓝边染色要么包含一个边全为红色的 K_k，要么包含一个边全为蓝色的 K_l。

证明 3. 证明 $R(k,l) \leqslant R(k-1,l)+R(k,l-1)$，从而有上界 $R(k,l) \leqslant \binom{k+l-2}{k-1}$。

定理 19 (4.4.11, 4.4.12). $R(3,3)=6, R(4,3)=R(3,4)=9, R(4,4)=18.$

定理 20 (4.4.13, Ramsey 定理的推广). 设 $r,k \geqslant 1, q_i \geqslant r$，则存在一个最小的正整数 $R(q_1,\cdots,q_k;r)$，使得当 $|S| \geqslant R(q_1,\cdots,q_k;r)$ 时，可以把 S 的所有 r 元子集写成 k 个集族的不交并 $\binom{S}{r}=\bigsqcup_{i=1}^k T_i$，使得“存在 $S_i \subseteq S, |S_i|=q_i$ 且 $\binom{S_i}{r} \subseteq T_i$”对至少一个 i 成立。

Ramsey 是其在 $r=2, q=\{k,l\}$ 时的推论。

3 图论

3.1 图的基本概念

定理 21 (5.1.21, 握手定理). $2|E|=\sum_{v\in V} d(v)$

定理 22 (5.1.28, Mantel). n 个顶点的图 G 不包含三角形作为子图，则它至多有 $\lfloor \frac{n^2}{4} \rfloor$ 条边。*考虑 $\mathcal{N}(x)$ 是独立集。*

命题 9 (5.1.30). 若图 G 有 n 个顶点且 $\delta(G) \geqslant \frac{n-1}{2}$，则 G 连通。*证明 $dist(u,v) \leqslant 2$。*

引理 5 (5.1.31). 设图 G 满足 $\delta(G) \geqslant 2$，则 G 必包含一个至少长为 $\delta(G)$ 的路径和一个至少长为 $\delta(G)+1$ 的圈。

命题 10 (5.1.34). 设图 G 中至少有一个圈，则最短圈长度 $g(G) \leqslant 2\ \mathrm{diam}\ G+1$。

定理 23 (5.1.42, Landau). n 阶竞赛图中一定存在一个点可以通过不超过两条边到达所有点。*验证出度最大的点。*

推论 10 (5.1.43). 强连通竞赛图一定存在长度为 3 的圈。

3.2 树

命题 11 (5.2.4). 设 T 是一棵有 n 条边的树，若 G 满足 $\delta(G) \geqslant n$，则 T 一定是 G 的子图。

定理 24 (5.2.7, Cayley). 以 $[n]$ 为顶点标号的树有 n^{n-2} 种。*用 Prüfer 序列证明即可。*

3.3 Euler 图与 Hamilton 图

定理 25 (5.5.1). 无向图 G 是 Euler 图当且仅当 G 连通且每个点的度数都是偶数，等价于 G 连通且是若干边不交圈的并。

定理 26 (5.5.4). 有向图 G 是 Euler 图当且仅当 G 强连通且每个点的入度等于出度，等价于 G 强连通且是若干边不交有向圈的并。

定理 27 (5.5.6). (必要条件) 若 G 是 Hamilton 图，则对任意 $S \subseteq V(G), G\setminus S$ 至多有 $|S|$ 个连通分量。

从圈里删去 k 个点，剩下的部分至多有 k 个连通分量。

定理 28 (5.5.9, Dirac). (充分条件) 设 G 有 $n \geqslant 3$ 个顶点且 $\delta(G) \geqslant \frac{n}{2}$，则 G 是 Hamilton 图。

欲证否“存在 G 不是 Hamilton 图且 $\delta(G) \geqslant \frac{n}{2}$”，把 G 扩充为极大非 Hamilton 图，不改变 $\delta(G) \leqslant \frac{n}{2}$ 的性质，此时图中存在一条 Hamilton 路径 $u \to v$ 且 $d(u)+d(v) \geqslant n$，据此构造一条 Hamilton 回路以导出矛盾。

推论 11 (5.5.10). 设 G 有 $n \geqslant 3$ 个顶点且任意两个不相邻的顶点 u,v 都满足 $d(u)+d(v) \geqslant n$，则 G 是 Hamilton 图。

推论 12 (5.5.11, Ore). 设 G 有 $n \geqslant 3$ 个顶点且某两个不相邻的顶点 u,v 满足 $d(u)+d(v) \geqslant n$，则 G 是 Hamilton 图当且仅当 $G+uv$ 是 Hamilton 图。

3.4 匹配与覆盖

定理 29 (5.6.6, Hall). 二部图 $G(X,Y)$ 存在一个饱和 X 的完美匹配当且仅当 $\forall S \subseteq X, |\mathcal{N}(S)| \geqslant |S|$。

证明 4. 必要性显然。充分性考虑对 $|X|$ 归纳。如果存在 $S \subsetneq X$ 使得 $|\mathcal{N}(S)|=|S|$，那么 (根据归纳假设) 匹配 S 与 $\mathcal{N}(S)$，验证 $(X\setminus S, Y\setminus \mathcal{N}(S))$ 仍满足条件；若任意 $S \subsetneq X$ 均 $|\mathcal{N}(S)|>|S|$，那么随便匹配一条边后仍满足条件。得证。

命题 12 (稳定婚姻). 算法流程：每轮尚未匹配的左侧点向匹配度最高且没有被拒绝过的右侧点发申请，右侧点在收到的申请中找匹配度最高的匹配并拒绝其余。

定理 30. 上述算法一定能结束，且最后得到了一个稳定的最大匹配。

3.5 平面图

定理 31 (5.7.14, Euler). 设 G 是连通平面图，n,e,f 分别表示其顶点数，边数和面数，那么 $n-e+f=2$。如果有 p 个连通分量，那么就 $n-e+f=p+1$。

定理 32 (5.7.17). 设 G 是至少有三个顶点的简单可平面图，则 $|E(G)| \leqslant 3|V(G)|-6$。若 G 中无三角形，命题可加强为 $|E(G)| \leqslant 2|V(G)|-4$。

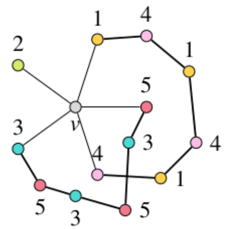
证明 5. 不妨认为 G 是连通的。每个面的长度至少为 3，因此 $2e \geqslant 3f = 3(2-n+e)$，整理得到 $e \leqslant 3n-6$。没有三角形就可以加强为 $2e \geqslant 4f$，类似可得结论。

例 8 (5.7.18). K_5 和 $K_{3,3}$ 都不是平面图。

定理 33 (5.7.21, Kuratowski). 一个图是可平面图当且仅当不包含 K_5 和 $K_{3,3}$ 作为子图。

定理 34 (5.8.19, Heawood). 任何平面图都是 5-可着色的。

证明 6. 对点数作归纳。根据 5.7.17 可知一定存在度数不超过 5 的点 v，只需要证明 v 有五个邻居且五个邻居都染不同色是不可能的。



1, 4 两点必然通过粉橙二色连通，3, 5 两点必然通过红蓝二色连通，这样产生了交叉，与平面性矛盾。

4 离散概率

定理 35 (6.1.4, union bound).

$$\Pr\left[\bigcup_{i=1}^n A_i\right] \leqslant \sum_{i=1}^n \Pr[A_i]$$

定义 21 (6.1.5). 设 $\Pr[A]>0$，称 $\frac{\Pr[AB]}{\Pr[A]}$ 为已知 A 发生的条件下 B 发生的概率，记为**条件概率** $\Pr[B|A]$。

命题 13 (6.1.7, Bayes). $A_1,\cdots,A_n$ 构成样本空间 Ω 的划分，那么对于任意事件 A

$$\Pr[A_i|A]=\frac{\Pr[A|A_i]\Pr[A_i]}{\sum_{j=1}^n \Pr[A|A_j]\Pr[A_j]}$$

其中 $\Pr[A_i]$ 称为**先验概率**，$\Pr[A_i|A]$ 称为**后验概率**。

定理 36 (**6.1.16, Markov Inequality**). 设随机变量 X 的支撑非负，期望存在，那么对于 $\forall\varepsilon>0$ 有 $\Pr[X\geqslant\varepsilon]\leqslant\frac{\mathbb{E}[X]}{\varepsilon}$。

推论 13 (**6.1.17**). 设随机变量 X 的 $2k$ 阶**中心矩** $\mathbb{E}[(X-\mathbb{E}[X])^{2k}]$ 存在，那么 $\forall\varepsilon>0$

$$\Pr[|X-\mathbb{E}[X]|\geqslant\varepsilon]\leqslant\frac{\mathbb{E}[(X-\mathbb{E}[X])^{2k}]}{\varepsilon^{2k}}$$

$k=1$ 时就是 **Chebyshev Inequality**。

定理 37 (**Stirling 公式**).

$$n!\sim\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n\qquad(n\to+\infty)$$

4.1 随机方法

例 9 (**6.1.10, Karger**). 最小割随机算法：每次随机图中的一条边并收缩两点，重复 $n-2$ 次后输出剩下两点之间连边数。
设 k 个最小割大小，则图中有至少 $\frac{kn}{2}$ 条边，因为每个点度数至少为 k。A_i 表示第 i 次没有收缩掉最小割中的一条边，则
$\Pr[A_1]=1-\frac{k}{\frac{kn}{2}}=1-\frac{2}{n},\Pr[A_i|\bigcap_{j=1}^{i-1}A_j]=1-\frac{2}{n-i+1}$，
故 $\Pr[A_1\cdots A_{n-2}]\geqslant\frac{2}{n(n-1)}=\Omega(n^{-2})$。

例 10 (**6.3.2**). 任取一张 n 点 m 条边的图 G，则 K_n 可以被 $O(n^2\log n/m)$ 个 G 的副本覆盖。考虑一条边未被覆盖的概率，*union bound*。

例 11 (**6.3.3**). 存在一个大小为 $O(k2^k\log n)$ 的集合系 $\mathcal{F}$，可以打散任何一个 $[n]$ 的大小为 k 的子集 A。考虑一个集合不能被表出的概率，*union bound*。

4.2 期望的线性性

定理 38.

$$\Pr[X\geqslant\mathbb{E}[X]]>0,\Pr[X\leqslant\mathbb{E}[X]]>0$$

例 12 (**6.3.5**). 存在一张 n 点竞赛图有至少 $n!2^{-n}$ 条 Hamilton 路径。证明这个值就是期望。

例 13. 任何图 $G(V,E)$ 中都包含一个至少有 $\frac{|E|}{2}$ 条边的二部图。证明这个值就是期望。

例 14 (**6.3.6**). 图 $G(V,E)$ 中一定有不小于 $\sum_{v\in V}\frac{1}{d(v)+1}$ 的独立集。随机点排列，选比邻居都大的作为独立集。

推论 14 (**6.3.8**). 满足不存在大小为 $r+1$ 的团的 n 点图至多有 $\left(1-\frac{1}{r}\right)\frac{n^2}{2}$ 条边。对上一题结果用均值不等式。

例 15 (**6.3.11**). 设 $S\subseteq\mathbb{Z}\setminus\{0\},|S|=n$，则 S 中一定包含一个大小至少为 $\frac{n}{3}$ 的子集，其中不存在两个数相加等于第三个数。取 $u\sim U[0,1]$，考虑 $\{s\in S:\{su\}\in(\frac{1}{3},\frac{2}{3})\}$。

4.3 改造法

例 16 (**5.6.20, Arnautov–Payan**). 设 G 有 n 个顶点且 $\delta(G)=k$，则图中有一个大小不超过 $n\frac{1+\log(k+1)}{k+1}$ 的支配集。
以 p 的概率取 V 的子集 X，取 $Y=X\cup(V\setminus(X\cup\mathcal{N}(X)))$ 作为支配集，一个点属于 Y 的概率 $\leqslant p+(1-p)^{\delta+1}$，即 $\mathbb{E}[|Y|]\leqslant n(p+e^{-p(\delta+1)})$，调整到 $p^*=\frac{\ln(\delta+1)}{\delta+1}$ 得到结果。

例 17 (**6.3.13**). 若 $|V|\leqslant 2|E|$，则图 $G(V,E)$ 的最大独立集大小 $\geqslant\Omega\left(\frac{|V|^2}{|E|}\right)$。
$\mathbb{E}[|S*|]\geqslant\mathbb{E}[|S|]-\mathbb{E}[|\binom{S}{2}\cap E|]=p|V|-p^2|E|$，取 $p=\frac{|V|}{2|E|}$。

例 18 (**6.3.14**). 存在 $M\in\{0,1\}^{n\times n}$ 满足 M 中有 $\Omega(n^{2-\frac{2}{k+1}})$ 个 1，且不存在全 1 的 $k\times k$ 子矩阵。
$\mathbb{E}[\#1]\geqslant n^2p-\binom{n}{k}^2p^{k^2}\geqslant n^2p-n^{2k}p^{k^2}$。

4.4 LLL

定理 39 (**6.3.16, Lovász Local Lemma**). 设 $A_1,\cdots,A_n$ 是同一概率空间上的事件，依赖图 $G=([n],E)$。如果存在实数 $0\leqslant x_i<1$ 满足 $\forall 1\leqslant i\leqslant n,\Pr[A_i]\leqslant x_i\prod_{(i,j)\in E}(1-x_j)$，那么 $\Pr[\bigcap_{i=1}^n\overline{A_i}]\geqslant\prod_{i=1}^n(1-x_i)>0$。

证明 7.

$$\Pr[\bigcap_{i=1}^m\overline{A_i}]=\prod_{i=1}^m(1-\Pr[A_i|\bigcap_{j=1}^{i-1}\overline{A_j}])$$

需要证明 $\Pr[A_i|\bigcap_{j\in S}\overline{A_j}]\leqslant x_i$。归纳，把 S 拆成 S_1,S_2，其中 S_1 是与 A_i 有依赖的

$$\Pr[A_i|\bigcap_{j\in S}\overline{A_j}]=\frac{\Pr[A_i\cap(\bigcap_{j\in S_1}\overline{A_j})|\bigcap_{k\in S_2}\overline{A_k}]}{\Pr[\bigcap_{j\in S_1}\overline{A_j}|\bigcap_{k\in S_2}\overline{A_k}]}$$

分子放缩成 $\Pr[A_i]\leqslant x_i\prod_{(i,j)\in E}(1-x_j)$，分母根据 union bound 以及归纳假设 $\geqslant\prod_{j\in S_1}(1-x_j)$，故得证。

推论 15 (**6.3.18, Symmetric Lovász**). 设 $A_1,\cdots,A_n$ 是满足 $\Pr[A_i]\leqslant p<1$ 的事件，且每个 A_i 和至多 d 个其他事件相关，同时 $\mathrm{e}p(d+1)\leqslant 1$，那么 $\Pr[\bigcap_{i=1}^n\overline{A_i}]>0$。
取 $x_i=\frac{1}{d+1}$

例 19 (**6.3.20**). 可以用 $O(\sqrt{n})$ 种颜色对 K_n(n 点完全图) 的边染色，使得图中不存在同色的 K_3。
$\mathrm{e}\frac{1}{k^2}(3(n-3)+1)<1$, LLL。

例 20. $11n$ 个点围成一圈，染成 n 种颜色，每种颜色各 11 个，则一定可以选出 n 个两两不同色的点在圆周上不相邻。
A_i 表示 i 和 $i+1$ 同时选中，欲证 $Pr[\bigcap_{i=1}^{11n}\overline{A_i}]>0$。
$Pr[A_i]=\frac{1}{121}$，d 取 42 因为 $A_{i-1},A_{i+1},\{A_{j-1},A_j:c_j=c_i\},\{A_{k-1},A_k:c_k=c_{i+1}\}$ 是直接相关的。$ep(d+1)=\frac{43e}{121}=0.96600098036<1$。

5 不等式

定理 40 (**均值不等式**).

$$\frac{n}{\sum_{i=1}^n\frac{1}{x_i}}\leqslant\sqrt[n]{\prod_{i=1}^n x_i}\leqslant\frac{1}{n}\sum_{i=1}^n x_i\leqslant\sqrt{\frac{\sum_{i=1}^n x_i^2}{n}}$$

定理 41 (**Cauchy**).

$$\left(\sum_{i=1}^n a_ib_i\right)^2\leqslant\sum_{i=1}^n a_i^2\sum_{i=1}^n b_i^2$$

定理 42.

$$\left(\frac{n}{\mathrm{e}}\right)^n\leqslant n!\leqslant n\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n$$

$$\left(\frac{n}{k}\right)^k\leqslant\binom{n}{k}\leqslant\left(\frac{\mathrm{e}n}{k}\right)^k,\binom{n}{k}\leqslant\frac{n^k}{k!}$$

$$\frac{2^{2n}}{2\sqrt{n}}\leqslant\binom{2n}{n}\leqslant\frac{2^{2n}}{\sqrt{2n}}$$

$$(1-p)^n\leqslant\mathrm{e}^{-np},\ln(1-x)\leqslant -x$$