

组合学初步

(学习笔记)^{1.75 版}

曲卷猫 & 曲豆豆 整理

本笔记使用 L^AT_EX 排版, 使用 Tikz, Python, Geogebra 插图
整理过程中难免添油加醋过度解读, 敬请读者谅解

2024 年 6 月 17 日



图: 曲豆豆穿上博士服, 就好像真的是博士一样.

目录

1	组合计数基础	4
1.1	排列与组合	4
1.2	映射与 Stirling 数	8
1.3	多项式乘法及其组合意义	12
1.4	容斥原理	16
1.5	数论应用: 欧拉函数 ϕ 与 Möbius 函数 μ	22
2	母函数方法	25
2.1	形式幂级数环	25
2.2	母函数方法	30
2.3	指数型母函数	35
2.4	概率论应用: 随机游走	43
3	极值集合论 I: 基本概念与方法	47
3.1	算两次	47
3.2	抽屉原理	52
3.3	Sperner 定理	55
3.4	Bollobás 定理	59
3.5	Erdős-Ko-Rado 定理	60
3.6	Schur 引理与 \mathbb{F}_p 上的费马大定理	64
4	图论初步	66
4.1	图的基本概念	66
4.2	树, 平面图与 Euler 公式	71
4.3	生成树与 Cayley 公式	77
4.4	拓扑学应用: Brouwer 不动点定理	83
5	相异代表元系	89
5.1	相异代表元系与 Hall 定理	89
5.2	二部图的匹配	92

5.3	Hall 定理的若干应用	96
6	Turán 问题	98
6.1	Mantel 定理	98
6.2	Turán 定理	101
6.3	Ajtai-Komlós-Szemerédi 定理	105
6.4	Kövari-Sós-Turán 定理	110
7	Ramsey 理论	113
7.1	Ramsey 数 $R(s, t)$	113
7.2	多色 Ramsey 数 $R_k(s_1, s_2, \dots, s_k)$	118
7.3	超图 Ramsey 数 $R^{(r)}(s, t)$	120
7.4	练习: Ramsey 数 $R(3, n)$ 的渐近估计	124
8	概率方法	129
8.1	概率的次可加性	129
8.2	期望的线性性与平均值原理	134
8.3	删除技巧	137
8.4	练习: Ramsey 数 $R(3, n)$ 的渐近估计 II	142
8.5	Lovász 局部性引理	148
9	极值集合论 II: 线性代数方法	152
9.1	奇偶镇问题与 Fisher 不等式	152
9.2	欧氏空间 \mathbb{R}^n 中的 2-距离点集	157
9.3	代数簇与 L -相交族	161
9.4	矩曲线与 Bollobás 定理的变式	165
10	谱方法	166
10.1	图的邻接矩阵与谱	166
10.2	Laplace 矩阵与 Kirchhoff 矩阵树定理 (待重写)	167
10.3	多重图 (待补)	174

1. 组合计数基础

1.1 排列与组合

1.1.记号. 我们采用如下通用记号约定:

- 若不特别说明,一般的数字 n 默认**正整数**,一般的集合 X 默认**有限集**.
- 对于集合 X , 记 $|X| := \sum_{x \in X} 1$, 即 X 的元素个数. $|X|$ 也可记作 $\#X$.
- 对于 n 个集合 X_1, \dots, X_n , 如果 $X_i \cap X_j = \emptyset, \forall i \neq j$, 则 $\bigcup_{i=1}^n X_i$ 也可以记作 $\bigsqcup_{i=1}^n X_i$, 称为**无交并**. 特别地, 若 $A \cap B = \emptyset$, 则 $A \cup B$ 也可记作 $A \sqcup B$.
- 对于集合 X, Y , 记**笛卡尔积** $X \times Y := \{(x, y) \mid x \in X, y \in Y\}$. 此外, 记 $X^n := \{(x_1, \dots, x_n) \mid x_i \in X, i = 1, \dots, n\}$, 即取值于 X 的 n 元有序组之全体.
- 对于映射 $f: X \rightarrow Y$ 以及 $y \in Y$, 记 $f^{-1}(y) := \{x \in X \mid f(x) = y\}$ 为 y 关于 f 的**原像集**.

1.2.记号. 设 n 为正整数, 则

- 记集合 $[n] := \{1, 2, \dots, n\}$. 特别规定 $[0] := \emptyset$.
- **阶乘** $n! := 1 \times 2 \times 3 \times \dots \times n$, 特别规定 $0! = 1$.
- 对于 $0 \leq k \leq n$, **排列数** $(n)_k := n(n-1) \cdots (n-k+1) = \frac{n!}{(n-k)!}$.
- 对于 $0 \leq k \leq n$, **组合数** $\binom{n}{k} := \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}$.

1.3.性质. 以下 3 条事实是显然的, 称为**组合计数基本原理**:

1. 对于集合 X, Y , 则 $|X| = |Y|$ 当且仅当存在双射 $f: X \rightarrow Y$.
2. 对于集合 X, Y , 若 $X \cap Y = \emptyset$, 则 $|X \sqcup Y| = |X| + |Y|$.
3. 对于集合 X, Y , 则 $|X \times Y| = |X| \cdot |Y|$.

1.4.记号. 对于集合 X ,

- $2^X := \{A \mid A \subseteq X\}$, 即 X 的全体子集构成的集合.
- $\binom{X}{k} := \{A \subseteq X \mid |A| = k\}$, 即 X 的全体 k 元子集构成的集合.

例如, 若 $X = [3]$, 则

$$\begin{aligned}\binom{X}{0} &= \{\emptyset\} \\ \binom{X}{1} &= \{\{1\}, \{2\}, \{3\}\} \\ \binom{X}{2} &= \{\{1, 2\}, \{1, 3\}, \{2, 3\}\} \\ \binom{X}{3} &= \{\{1, 2, 3\}\} \\ 2^X &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}\end{aligned}$$

1.5.性质. 对于集合 X , 以下是众所周知的基本常识:

$$|2^X| = 2^{|X|}, \quad \left| \binom{X}{k} \right| = \binom{|X|}{k}.$$

其证明与组合意义都众所周知, 不再赘述.

1.6.性质. 以下组合恒等式成立:

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

$$3. \binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}.$$

证明. 虽然可以代入组合数公式 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ 暴力验证, 但我们还是希望“用组合的观点”理解它们.

1. 我们知道, $\binom{n}{k}$ 是从 $[n]$ 当中挑选 k 个元素的方法数; 若挑选了某 k 个, 则剩下 $(n-k)$ 个元素未被挑选, 这自然给出“从 n 个元素中挑选 k 个”与“从 n 个元素挑选 $n-k$ 个”之间的一一对应, 从而得证.
2. 对于 $[n]$ 的 k 元子集 A , 则要么 $1 \in A$, 要么 $1 \notin A$. 若 $1 \notin A$, 则需要从 $[n] \setminus \{1\}$ 中挑选 k 个; 若 $1 \in A$, 只需再从 $[n] \setminus \{1\}$ 中挑选 $k-1$ 个. 从而得证.
3. 最后看第三个. 设想某个班有 n 个学生, 从中选出 k 个人参加某小组活动, 并在这 k 人当中选出 1 名组长, 则安排方案有多少种. 一方面, 先选出参加活动的 k 人, 共 $\binom{n}{k}$ 种选法, 然后再从 k 人当中选出组长, 因此总共 $k \binom{n}{k}$ 种方案; 另一方面, 也可以先从 n 个人当中指定组长, 再从剩余 $(n-1)$ 人当中选出 $(k-1)$ 名组员, 因此共有 $n \binom{n-1}{k-1}$ 种活动方案. 因此 $k \binom{n}{k} = n \binom{n-1}{k-1}$, 得证.

□

1.7.例题. (Vandermonde 卷积公式). 对于正整数 m, n , 成立

$$\binom{m+n}{k} = \sum_{\substack{i+j=k \\ i,j \geq 0}} \binom{m}{i} \binom{n}{j}. \quad (1)$$

证明. 直接代入组合数公式 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ 并不能轻易证明此式; 而在组合的观点下, 它显然成立. 设想有 m 个男生与 n 个女生当中挑选 k 个人,

一方面, 显然有 $\binom{m+n}{k}$ 种挑选方法; 另一方面, 考虑选出来的 k 人当中男女各多少, 若选出 i 个男生 j 个女生, 则这样的取法有 $\binom{m}{i}\binom{n}{j}$ 种, 再让 i, j 取遍 $\{(i, j) \mid i + j = k, i, j \geq 0\}$ 即可. \square

可见, 适当构造组合模型, 并用不同的方法计数, 能够得到不平凡的恒等式.

1.8. 性质. 关于 n 个未知数 x_1, \dots, x_n 的不定方程

$$\begin{cases} x_1 + x_2 + \cdots + x_n = k \\ x_i \in \{0, 1\}, \quad \forall i = 1, \dots, n \end{cases}$$

有 $\binom{n}{k}$ 组不同的解.

这是显然的. 为满足此方程, n 个未知数里面必然有 k 个取值为 1; 这相当于从 n 个未知数里挑选 k 个.

1.9. 性质. 关于 n 个未知数 x_1, \dots, x_n 的不定方程

$$\begin{cases} x_1 + x_2 + \cdots + x_n = k \\ x_i \in \mathbb{Z}_{\geq 0}, \quad \forall i = 1, \dots, n \end{cases}$$

有 $\binom{k+n-1}{k}$ 组不同的解.

这是经典的“隔板插球”问题. 设想有 n 个不同的箱子与 k 个相同的球, 将这 k 个球放入这 n 个箱子, 若第 i 个箱子里放入 x_i 个球, 则 (x_1, \dots, x_n) 是上述不定方程的一组解. 容易验证该不定方程的解与将球放入箱子的方法一一对应, 从而解的个数等于将球放入箱子的方法数.

为了把球放到箱子里, 先把这 k 个球从左往右排成一排, 在相邻两球的间隙处插入隔板, 用 $(n-1)$ 个隔板把球分成 n 堆, 这 n 堆从左往右依次放入 n 个箱子里. 于是, 只需考虑有多少种插入隔板的方式. 将 k 个球与 $(n-1)$ 个隔板都视为物体, 共有 $(k+n-1)$ 个物体从左向右排成一排, 占据 $(k+n-1)$ 个位置. 这 $(k+n-1)$ 个位置里面, 有 k 个位置是球, 因此共有 $\binom{k+n-1}{k}$ 种情形.

1.10.习题. 从 $\{1, 2, \dots, n\}$ 中选出 r 个不同的整数, 要求这 r 个整数中的任何两个都不相邻. 则符合要求的选法有多少种?

解. 将选中的 r 个整数视为隔板, 未选中的整数视为球, 则“任何两个选中的整数都不相邻”即任何两个隔板都不能紧挨着, 这当且仅当任何两个隔板之间都必有球. 同上一题, 考虑“隔板插球”与“箱子放球”的一一对应, 从而只需考虑 $(r+1)$ 个不同的箱子当中, 除了第 1 个箱子与最后一个箱子之外, 其余 $(r-1)$ 个箱子里都至少有 1 个球的情形. 于是, 不妨先将第 $2, 3, \dots, r$ 个箱子里各放 1 个球, 然后还剩下 $(n-r) - (r-1) = (n-2r+1)$ 个球. 之后就转化为把 $(n-2r+1)$ 个球放入 $(r+1)$ 个箱子里的问题, 因此共有 $\binom{(n-2r+1) + (r+1) - 1}{n-2r+1} = \binom{n-r+1}{r}$ 种方案. \square

另解. 除了把问题强行转化为 1.9, 我们还有更简洁的方法. 依然将选中的数字视为隔板, 未选中的数字视为球. 则一共有 $(n-r)$ 个球. 注意到隔板的位置一定是在相邻两球之间, 或者第一个球的左侧, 或者最后一个球的右侧, 一共 $(n-r+1)$ 个可供插隔板的“空隙”. 任何两个隔板不能紧挨着, 相当于每个“空隙”至多被插入一个隔板. 即 $(n-r+1)$ 个空隙当中的 r 个空隙里面有隔板, 故共有 $\binom{n-r+1}{r}$ 种情形. \square

1.2 映射与 Stirling 数

1.11.记号. 对于集合 X, Y , 记

$$Y^X := \{f: X \rightarrow Y\},$$

即从 X 到 Y 的映射构成的集合.

1.12.性质. 对于集合 X, Y , 成立

1. $|Y^X| = |Y|^{|X|}$.
2. $\#\{f \in Y^X \mid f \text{ 是单射}\} = (|Y|)_{|X|} := |Y|(|Y|-1)\cdots(|Y|-|X|+1)$.

证明. 记 $X = \{x_1, \dots, x_m\}$, $Y = \{y_1, \dots, y_n\}$, 其中 $m := |X|$, $n := |Y|$. 对于映射 $f: X \rightarrow Y$, 则对每个 $x \in X$, $f(x)$ 都有 $|Y|$ 种可能的取值, 因此共有 $\prod_{x \in X} |Y| = |Y|^{|X|}$ 种可能的情况. 接下来考虑单射的个数. 设 $f: X \rightarrow Y$ 是单射, 则不妨先确定 $f(x_1)$ 的取值, 这有 $|Y|$ 种情况; 确定 $f(x_1)$ 之后, $f(x_2)$ 将只有 $(|Y| - 1)$ 种合法的取值, 以此类推. 因此从 X 到 Y 的单射的个数为 $|Y|(|Y| - 1) \cdots (|Y| - |X| + 1)$. \square

自然要问, 对于集合 X, Y , 从 X 到 Y 的**满射**有多少个?

1.13. 记号. 对于 (非空) 集合 X , 记 $S_X := \{f \in X^X \mid f \text{ 是双射}\}$. S_X 种的元素称为集合 X 的**置换**, 或者**重排**. 对于正整数 n , 记 $S_n := S_{[n]}$.

众所周知, 对任意 $f, g \in S_X$, 复合映射 $f \circ g \in S_X$, 逆映射 $f^{-1} \in S_X$, 恒等映射 $\text{id}: X \rightarrow X$ 也属于 S_X , 因此 S_X 关于映射的复合运算构成群, 这个群称为集合 X 的**置换群**. 容易证明, 若 $|X| = n$, 则有**群同构** $S_X \cong S_n$, 因此我们不妨只考虑 S_n . 众所周知, S_n 中的元素都可唯一分解为两两不交的**轮换**之积.

1.14. 定义. 对于集合 X , 以及 $\mathcal{A} \subseteq 2^X$, 即 \mathcal{A} 是由 X 的某些子集构成的集合, 如果 \mathcal{A} 中的元素都非空且两两不交, 且 $\bigsqcup_{A \in \mathcal{A}} A = X$, 则称 \mathcal{A} 是 X 的一个**划分**.

1.15. 定义. 对于正整数 r, n , 令

$$\begin{aligned} (-1)^{n-r} s(r, n) &:= \# \{f \in S_r \mid f \text{ 形如 } n \text{ 个不交轮换之积}\} \\ S(r, n) &:= \# \left\{ \mathcal{A} \subseteq 2^{[r]} \mid \emptyset \notin \mathcal{A}, |\mathcal{A}| = n, \bigsqcup_{A \in \mathcal{A}} A = [r] \right\}. \end{aligned}$$

$s(r, n)$ 与 $S(r, n)$ 分别称为**第一类 Stirling 数**与**第二类 Stirling 数**.

可见, $S(r, n)$ 是将 $[r]$ 划分为 n 个非空子集的方法数.

1.16. 性质. 从 $[r]$ 到 $[n]$ 的满射的个数为 $S(r, n) \cdot n!$.

证明. 对于满射 $f: [r] \rightarrow [n]$, 考虑集合 $\mathcal{A} := \{f^{-1}(y) \subseteq [r] \mid y \in [n]\}$, 则 \mathcal{A} 给出了 $[r]$ 的一个 n 元划分. 反之, $[r]$ 的每个 n 元划分都自然地对应于 $n!$ 个从 $[r]$ 到 $[n]$ 的满射. 因此 $[r]$ 到 $[n]$ 的满射共有 $S(r, n) \cdot n!$ 个. \square

1.17.性质. 对任意 $x \in \mathbb{C}$, 以及正整数 n , 成立

$$x^n = \sum_{k=0}^n S(n, k)(x)_k.$$

证明. 将上式等号两边视为关于 x 的多项式, 因此只需证明 x 为正整数的情形. 现在令 $x = m \in \mathbb{Z}_+$. 考虑从 $[n]$ 到 $[m]$ 的映射个数, 一方面, 它显然为 m^n ; 另一方面, 对于映射 $f: [n] \rightarrow [m]$, 考虑对 f 的像集 $f([n])$ 进行分类, 先确定 f 的像集有多少个元素, 再确定 f 的像集有哪些元素, 从而

$$\begin{aligned} m^n = |[m]^{[n]}| &= \sum_{k=0}^n \sum_{X \in \binom{[m]}{k}} \# \{f: [n] \rightarrow [m] \mid f([n]) = X\} \\ &= \sum_{k=0}^n \sum_{X \in \binom{[m]}{k}} \# \{f: [n] \rightarrow X \mid f \text{ 为满射}\} \\ &= \sum_{k=0}^n \sum_{X \in \binom{[m]}{k}} k! S(n, k) = \sum_{k=0}^n \frac{m!}{k!(m-k)!} k! S(n, k) \\ &= \sum_{k=0}^n S(n, k) \cdot (m)_k, \end{aligned}$$

故得证. □

1.18.引理. 对于正整数 n, k , 记 $c(n, k) := (-1)^{n-k} s(n, k)$, 其中 $s(n, k)$ 是第一类 Stirling 数. 则成立递推关系

$$c(n, k) = (n-1)c(n-1, k) + c(n-1, k-1).$$

易知 $c(n, k)$ 是 S_n 中的形如 k 个不交轮换之积的置换的个数.

证明. 若 $f \in S_n$ 形如 k 个不交轮换之积, 则这样的 f 有 $c(n, k)$ 个. 另一方面, 对于这样的 f , 如果 $f(1) = 1$, 则 f 在子集 $[n] \setminus \{1\}$ 上的限制映射自然看成 S_{n-1} 中的形如 $(k-1)$ 个不交轮换之积的置换, 因此满足 $f(1) = 1$ 的这样的 f 共有 $c(n-1, k-1)$ 个. 而如果 $f(1) \neq 1$, 记 $y := f(1) \neq 1$, 则 y 有 $(n-1)$ 中不同选取, 对于每个可能的 y , 考虑如下映射 \mathcal{F}_y :

$$\mathcal{F}_y: \left\{ f \in S_n \left| \begin{array}{l} f(1) = y, \\ f \text{ 形如 } k \text{ 个不交轮换之积} \end{array} \right. \right\} \rightarrow \left\{ \tilde{f} \in S_{[n] \setminus \{1\}} \left| \begin{array}{l} \tilde{f} \text{ 形如 } k \text{ 个} \\ \text{不交轮换之积} \end{array} \right. \right\}$$

$$f \mapsto \mathcal{F}_y[f]: x \mapsto \begin{cases} y & \text{若 } x = f^{-1}(1) \\ f(x) & \text{其他情况} \end{cases}$$

则容易验证 \mathcal{F}_y 良定, 且是一一映射. (翻译成成人话, 意思是说, 如果 $f(1) \neq 1$, 则 $1 \in [n]$ 所在 f -轨道的长度大于 1, 把 $1 \in [n]$ 从该轮换中删去, 再连接 $f^{-1}(1)$ 与 $f(1)$, 就得到一个长度比原来小 1 的新的轮换, 如此修改后的 f 自然是 $[n] \setminus \{1\}$ 的置换, 且形如 k 个不交轮换之积.) 因此满足 $f(1) = y$ 的这样的 f 共有 $c(n-1, k)$ 个. 综上所述, $c(n, k) = (n-1)c(n-1, k) + c(n-1, k-1)$. 得证. \square

1.19. 推论. 对于 $x \in \mathbb{C}$, 以及正整数 n , 成立

$$(x)_n = \sum_{k=0}^n s(n, k) x^k.$$

证明. 或许可以寻求等号两边的组合意义, 但别忘了数学归纳法. 对 n 归纳, $n=1$ 时显然成立. 对于一般的 n , 利用归纳假设以及上一题的递推关系, 可知

$$\begin{aligned} \sum_{k=0}^n s(n, k) x^k &= \sum_{k=0}^n (-1)^{n+k} c(n, k) x^k \\ &= \sum_{k=0}^n (-1)^{n+k} [(n-1)c(n-1, k) x^k + c(n-1, k-1) x^k] \\ &= (1-n) \sum_{k=0}^n (-1)^{n-1+k} c(n-1, k) x^k \\ &\quad + x \sum_{k=0}^{n-1} (-1)^{n-1+k} c(n-1, k) x^k \\ &= (1-n)(x)_{n-1} + x(x)_{n-1} = (x)_n, \end{aligned}$$

从而得证. \square

1.20. 考虑线性空间 $V_n := \{f \in \mathbb{C}[x] \mid \deg f \leq n\}$, 即由 x 的不超过 n 次的多项式构成的空间. 则 $\{1, x, x^2, \dots, x^n\}$ 与 $\{1, (x)_1, (x)_2, \dots, (x)_n\}$ 显然都是 V_n 的基, 容易看出这两组基之间的过渡矩阵都是上三角的. 不如补充定义

$S(0,0) = s(0,0) = 0$, 于是1.19与1.17表明, Stirling 数构成这两组基之间的过渡矩阵的矩阵元.

1.3 多项式乘法及其组合意义

1.21. 记号. 设 $f(x)$ 是关于变元 x 的多项式, 则对正整数 n , 记

$$[x^n]f := f(x) \text{ 的 } x^n \text{ 项系数.}$$

例如, 若 $f(x) = -3 + 5x + 7x^3$, 则 $[x^0]f = -3$, $[x^1]f = 5$, $[x^2]f = 0$, $[x^3]f = 7$. 一般地, 由微积分中众所周知的泰勒公式可知,

$$[x^n]f = \frac{f^{(n)}(0)}{n!},$$

其中 $f^{(n)}$ 为 f 的 n 阶导函数.

1.22. 性质. 设 f_1, \dots, f_n 都是关于变元 x 的多项式, 记 $f := f_1 f_2 \cdots f_n$, 则对任意 $k \geq 0$,

$$[x^k]f = \sum_{\substack{i_1 + \cdots + i_n = k \\ i_j \geq 0, \forall j=1, \dots, n}} \prod_{j=1}^n [x^{i_j}]f_j.$$

证明. 直接用多项式乘法展开, 然后合并同类项即可, 这是显然的. □

1.23. 推论.(二项式定理). 对于正整数 n , 成立

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

证明. 此定理众所周知, 但这里还是要象征性证明一下. 在1.22中, 取 $f_1 = f_2 = \cdots = f_n = 1+x$, $f := f_1 f_2 \cdots f_n = (1+x)^n$, 从而对每个 $k \geq 0$,

$$\begin{aligned} [x^k]f &= \sum_{\substack{i_1 + \cdots + i_n = k \\ i_j \geq 0, \forall j=1, \dots, n}} [x^{i_j}](1+x) = \sum_{\substack{i_1 + \cdots + i_n = k \\ i_j = 0, 1}} 1 \\ &= \# \{ (i_1, i_2, \dots, i_n) \mid i_1 + \cdots + i_n = k, i_j = 0, 1 \} \\ &= \binom{n}{k}. \end{aligned}$$

注意最后一个等号利用了1.8. □

1.24.推论. 若 I_1, I_2, \dots, I_n 都是 $\mathbb{Z}_{\geq 0}$ 的有限子集, 记多项式 $f_j(x) = \sum_{i \in I_j} x^i$, $j = 1, \dots, n$, 则关于未知数 x_1, \dots, x_n 的不定方程

$$\begin{cases} x_1 + x_2 + \dots + x_n = k \\ x_j \in I_j, \quad \forall j = 1, 2, \dots, n \end{cases}$$

的解的个数为 $[x^k](f_1 f_2 \cdots f_n)$.

证明. 这个是显然的. □

1.25. 从而我们建立了多项式乘法与组合问题之间的联系. 作为简单应用, 我们可以立刻给出 Vandermonde 卷积公式 1.7 的一个另证:

$$\begin{aligned} \binom{n+m}{k} &= [x^k](1+x)^{n+m} = [x^k]((1+x)^n(1+x)^m) \\ &= \sum_{\substack{i+j=k \\ i,j \geq 0}} ([x^i](1+x)^n) \cdot ([x^j](1+x)^m) \\ &= \sum_{\substack{i+j=k \\ i,j \geq 0}} \binom{n}{i} \binom{m}{j}. \end{aligned}$$

1.26.例题. 证明如下等式:

$$\sum_{k=0}^n k \binom{n}{k} = n \cdot 2^{n-1}.$$

证法一. (构造组合模型). 设想某个班级有 n 名同学, 需要从中挑选若干同学 (至少 1 人) 参加某小组活动, 参加小组活动的同学之中需要有 1 人担任组长, 那么总共有多少种活动安排方案.

一方面, 若选择 k 人参加活动 ($k = 1, 2, \dots, n$), 则有 $\binom{n}{k}$ 种选法, 之后在参加活动的 k 人之中选出组长, 因此恰有 k 人参加的活动方案共有 $k \binom{n}{k}$ 种, 总共有 $\sum_{k=1}^n k \binom{n}{k} = \sum_{k=0}^n k \binom{n}{k}$ 种活动方案.

另一方面, 先从全班 n 人之中选定组长, 然后依次询问剩余 $(n-1)$ 个人中的每一个人是否参加, 由此易知共有 $n \cdot 2^{n-1}$ 种活动方案. □

除了构造组合模型, 微积分也是强力的手段:

另证. (用微积分). 将等式 $(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$ 两边对 x 求导, 得到

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

然后令 $x = 1$, 得证. □

除了关于一个变元 x 的多项式, 我们也可以考虑关于 n 个变元 x_1, \dots, x_n 的多项式. 多元多项式的乘法当然也具有组合意义.

1.27. 定义. (多重组合数). 设 $k_1, k_2, \dots, k_n \in \mathbb{Z}_{\geq 0}$, $k := k_1 + k_2 + \dots + k_n$, 则记

$$\binom{k}{k_1, k_2, \dots, k_n} := \frac{k!}{k_1! k_2! \dots k_n!}.$$

考虑这样的组合问题: k 个不同的球放入 n 个不同的箱子里, 要求第 i 个箱子里放 k_i 个球, $i = 1, \dots, n$, 试求符合要求的方案个数. 为得到符合要求的方案, 先将这 k 个球从左到右排成一队, 共有 $k!$ 种方法; 接下来, 把最左边 k_1 个球放入 1 号箱, 1 号箱完成之后再最左边 k_2 个球放入 2 号箱, ..., 不断进行下去. 然而, 在一开始, 最左边的 k_1 个球之间无论如何排队 ($k_1!$ 种情况), 最终全都进入 1 号箱, 不同的排队方式导致最终同样的将球放入箱子的方案; 这对进入 2 号箱, ..., n 号箱的球也如此. 因此共有 $\frac{k!}{k_1! k_2! \dots k_n!} = \binom{k}{k_1, k_2, \dots, k_n}$ 种符合要求的方案.

1.28. 性质. 设 x_1, \dots, x_n 是 n 个变元, 则对 $k \geq 0$, 成立

$$(x_1 + x_2 + \dots + x_n)^k = \sum_{\substack{k_1 + k_2 + \dots + k_n = k \\ k_i \geq 0}} \binom{k}{k_1, k_2, \dots, k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}.$$

证明. 对每一组 (k_1, \dots, k_n) , 考察 $(x_1 + \dots + x_n)^k$ 的 $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ 项系数. 注意 $(x_1 + \dots + x_n)^k$ 是 k 个一次多项式的乘积, 这 k 个多项式之中的每一个都在展开式的每一项中贡献 x_1, \dots, x_n 之一. 为得到 $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ 项, 这 k 个多项式中需要有 k_1 个贡献 x_1 , k_2 个贡献 x_2 , ..., k_n 个贡献 x_n . 于是由多重组

合数的组合意义易知展开式中共有 $\binom{k}{k_1, k_2, \dots, k_n}$ 项对 $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ 有贡献. 从而易证. \square

1.29.性质. 设 x_1, \dots, x_n 为 n 个变元, 则成立

$$\prod_{i=1}^n (1 + x_i) = \sum_{A \subseteq [n]} \prod_{i \in A} x_i. \quad (2)$$

证明. 肉眼观察等号左边, 在心里将等号左边全部展开, 即得证. \square

下面介绍一例多元多项式在组合计数中的应用.

1.30.例题. 设 p 为奇素数, m, n 为正整数且 $m \leq n$. 求集合

$$\left\{ A \in \binom{[np]}{mp} \mid \sum_{a \in A} a \equiv 0 \pmod{p} \right\}$$

的元素个数 $X_{m,n}$.

解. 考虑二元多项式

$$f(x, y) := \prod_{k=1}^{np} (1 + xy^k),$$

则对于任意非负整数 u , 容易验证

$$[x^u]f(x, y) = \sum_{v \geq 1} y^v \# \left\{ A \in \binom{[np]}{u} \mid \sum_{a \in A} a = v \right\}.$$

考虑 p 次单位根 $\zeta_p := e^{\frac{2\pi i}{p}}$, 每个非负整数 $0 \leq \ell \leq p-1$, 记

$$f_\ell(x) := f(x, \zeta_p^\ell) = \prod_{k=1}^{np} (1 + \zeta_p^{k\ell} x),$$

则容易验证

$$[x^{mp}]f_\ell(x) = \sum_{v=0}^{p-1} \zeta_p^{\ell v} \# \left\{ A \in \binom{[np]}{mp} \mid \sum_{a \in A} a \equiv v \pmod{p} \right\}.$$

将上式对 ℓ 求和, 并注意当 $1 \leq v \leq p-1$ 时成立 $\sum_{\ell=0}^{p-1} \zeta_p^{\ell v} = 0$, 可得

$$[x^{mp}] \sum_{\ell=0}^{p-1} f_{\ell}(x) = p \# \left\{ A \in \binom{[np]}{mp} \left| \sum_{a \in A} a \equiv 0 \pmod{p} \right. \right\} = pX_{m,n}.$$

而另一方面,

$$\begin{aligned} \sum_{\ell=0}^{p-1} f_{\ell}(x) &= \sum_{\ell=0}^{p-1} \prod_{k=1}^{np} (1 + \zeta_p^{\ell k} x) \\ &= (1+x)^{np} + \sum_{\ell=1}^{p-1} \prod_{k=1}^{np} (1 + (\zeta_p^{\ell})^k x) \\ &= (1+x)^{np} + \sum_{\ell=1}^{p-1} \prod_{k=1}^p (1 + (\zeta_p^{\ell})^k x)^n \\ &= (1+x)^{np} + \sum_{\ell=1}^{p-1} (1+x^p)^n \\ &= (1+x)^{np} + (p-1)(1+x^p)^n, \end{aligned}$$

因此

$$[x^{mp}] \sum_{\ell=0}^{p-1} f_{\ell}(x) = \binom{np}{mp} + (p-1) \binom{n}{m}.$$

综上两方面, 可得

$$X_{m,n} = \frac{1}{p} \left(\binom{np}{mp} + (p-1) \binom{n}{m} \right).$$

□

1.4 容斥原理

1.31. 对于集合 A, B , 我们知道, 如果 $A \cap B = \emptyset$, 那么 $|A \cup B| = |A| + |B|$. 而如果 A, B 的交集非空, 则用 $|A| + |B|$ 来计数 $A \cup B$ 的元素个数, 就会将 $A \cap B$ 中的每个元素重复计数一遍. 为得到正确的结果, 只需再减去 $|A \cap B|$. 因此,

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

这是小学生也能通过画图理解的容斥原理.

然而, 如何将两个集合 A, B 的情形推广到多个集合?

1.32. 记号. 在一定语境下, 假设我们谈论的所有集合都是某个集合 Ω 的子集.

- 对于集合 A , 记 $A^c := \bar{A} := \Omega \setminus A$, 称为集合 A 在 Ω 中的补集.
- 对于集合 A , 定义函数 $\mathbf{1}_A: \Omega \rightarrow \{0, 1\}$ 如下:

$$\mathbf{1}_A(x) := \begin{cases} 1 & \text{若 } x \in A \\ 0 & \text{若 } x \notin A \end{cases},$$

函数 $\mathbf{1}_A$ 称为集合 A 的特征函数.

- 对于给定的集合 A_1, A_2, \dots, A_n , 则对每个 $\emptyset \neq I \subseteq [n]$, 记

$$A_I := \bigcap_{i \in I} A_i.$$

此外, 特别规定 $A_\emptyset = \Omega$.

补集的运算律众所周知, 这里不再赘述. 关于特征函数, 特别注意如下运算律:

$$\mathbf{1}_{A \cap B} = \mathbf{1}_A \cdot \mathbf{1}_B, \quad \mathbf{1}_{A^c} = 1 - \mathbf{1}_A. \quad (3)$$

1.33. 定理.(容斥原理). 给定全集 Ω 的子集 A_1, \dots, A_n , 则

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| = \sum_{k=1}^n (-1)^{k+1} \left(\sum_{I \in \binom{[n]}{k}} |A_I| \right) \quad (4)$$

$$\left| \bigcap_{i=1}^n A_i^c \right| = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I| = \sum_{k=0}^n (-1)^k \left(\sum_{I \in \binom{[n]}{k}} |A_I| \right). \quad (5)$$

容易验证上述两式等价, 不妨只证其中一个.

证法一. 事实上, 我们断言:

$$\mathbf{1}_{A_1^c \cap \dots \cap A_n^c}(x) = \sum_{k=0}^n (-1)^k \sum_{I \in \binom{[n]}{k}} \mathbf{1}_{A_I}(x). \quad (6)$$

假如我们证明此式, 则将此式两边求和 $\sum_{x \in \Omega}$, 注意 $|A| = \sum_{x \in \Omega} \mathbf{1}_A(x)$, 即可得到(5).

为证明(6), 只需证明它对每个 $x \in \Omega$ 都成立. 任意给定 $x \in \Omega$, 记

$$\ell := \#\{i \in [n] \mid x \in A_i\},$$

即 x 恰属于 A_1, \dots, A_n 之中的 ℓ 个集合. 如果 $\ell = 0$, 则易知(6)等号两边都为 1, 从而相等. 如果 $\ell \neq 0$, 则 x 必属于 A_1, \dots, A_n 中的某个集合, 从而 $x \notin A_1^c \cap \dots \cap A_n^c$, 因此 (6) 式等号左边为 0. 而由 ℓ 的定义易知 $\sum_{I \in \binom{[n]}{k}} \mathbf{1}_{A_I}(x) =$

$$\binom{\ell}{k}, \text{ 因此(6)式等号右边} = \sum_{k=0}^{\ell} (-1)^k \binom{\ell}{k} = (1-1)^{\ell} = 0.$$

综上所述, (6)得证, 从而定理证毕. \square

这个证明富有启发性, 启发我们“看每一个元素对左右两边的贡献”.

另证. 记 $A := A_1 \cup A_2 \cup \dots \cup A_n$, 则容易验证

$$\prod_{k=1}^n (\mathbf{1}_A - \mathbf{1}_{A_k}) = 0,$$

这是因为, 对每个 $x \in \Omega$, 如果 $x \notin A$, 则 $x \notin A_1$, 从而 $\mathbf{1}_A(x) = \mathbf{1}_{A_1}(x) = 0$; 而如果 $x \in A$, 则 x 必然属于某个 A_k , 因此 $\mathbf{1}_A(x) = \mathbf{1}_{A_k}(x) = 1$, 故 $\mathbf{1}_A(x) - \mathbf{1}_{A_k}(x) = 0$.

另一方面, 利用(2)将上式左边展开, 再注意特征函数与集合运算的关系(3), 最后再求和 $\sum_{x \in \Omega}$, 即可得到(4)式. 细节留给读者. \square

接下来看容斥原理的一些应用.

1.34.例题. 回忆1.15中定义的第二类 Stirling 数 $S(n, k)$. 证明:

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

证明. 由1.16, 只需考虑从 $[n]$ 到 $[k]$ 的满射的个数. 不如反其道而行之, 考察不是满射的映射有多少. 记全集 $\Omega := [k]^{[n]}$, 即从 $[n]$ 到 $[k]$ 的所有映射之全体. 对每个 $i \in [k]$, 令

$$A_i := \{f: [n] \rightarrow [k] \setminus \{i\}\},$$

即像集不含有 i 的映射之全体. 显然 A_i 中的元素不是满射; 并且易知, 若 f 不是满射, 则 f 必属于某个 A_i . 因此

$$\{f \in \Omega \mid f \text{ 为满射}\} = \Omega \setminus \bigcup_{i=1}^k A_i = A_1^c \cap A_2^c \cap \cdots \cap A_k^c.$$

直接套用容斥原理的公式(5), 有

$$\begin{aligned} |A_1^c \cap \cdots \cap A_k^c| &= \sum_{i=0}^k (-1)^i \sum_{I \in \binom{[k]}{i}} |A_I| \\ &= \sum_{i=0}^k (-1)^i \sum_{I \in \binom{[k]}{i}} \#\{f: [n] \rightarrow [k] \setminus I\} \\ &= \sum_{i=0}^k (-1)^i \sum_{I \in \binom{[k]}{i}} (k-i)^n = \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n. \end{aligned}$$

因此 $S(n, k) = \frac{1}{k!} |A_1^c \cap \cdots \cap A_k^c| = \frac{1}{k!} \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n$, 得证. \square

1.35.例题.(错排问题). 对于正整数 n , 记 $D_n := \{f \in S_n \mid f(i) \neq i, \forall i \in [n]\}$, 则

$$|D_n| = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

证明. 首先断言 $|D_n|$ 满足递推关系

$$|D_n| = (n-1)(|D_{n-1}| + |D_{n-2}|).$$

这是因为, 对于 $f \in D_n$, 则 $f(1) \neq 1$, 从而 $y := f(1)$ 有 $(n-1)$ 种取法; 一旦取定 y , 然后再分 $f(y) = 1$ 与 $f(y) \neq 1$ 两种情况讨论, 与引理1.18的思路类似, 留给读者. 再由初始条件 $|D_1| = 0, |D_2| = 1$ 容易求得数列 $|D_n|$ 的通项.

为此, 令 $p_n := \frac{|D_n|}{n!}$, 则递推关系改写为

$$(p_n - p_{n-1}) = -\frac{1}{n}(p_{n-1} - p_{n-2}),$$

从而易知 $p_n - p_{n-1} = \frac{(-1)^n}{n!}$, $p_n = \sum_{k=0}^n \frac{(-1)^k}{k!}$, 因此 $|D_n| = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$. \square

除了考虑递推关系并使用代数技巧, 容斥原理更加直接粗暴:

另证. 记全集 $\Omega := S_n$. 对于 $i = 1, \dots, n$, 记

$$A_i := \{f \in S_n \mid f(i) = i\},$$

则易知 $D_n^c = A_1 \cup A_2 \cup \dots \cup A_n$, 因此直接套用容斥原理(5)可得

$$\begin{aligned} |D_n| &= |A_1^c \cap \dots \cap A_n^c| = \sum_{k=0}^n (-1)^k \sum_{I \in \binom{[n]}{k}} |A_I| \\ &= \sum_{k=0}^n (-1)^k \sum_{I \in \binom{[n]}{k}} \#\{f \mid f(i) = i, \forall i \in I\} \\ &= \sum_{k=0}^n (-1)^k \sum_{I \in \binom{[n]}{k}} |S_{[n] \setminus I}| = \sum_{k=0}^n (-1)^k \binom{n}{k} (n-k)! \\ &= n! \sum_{k=0}^n \frac{(-1)^k}{k!}. \end{aligned}$$

\square

第一个证明中出现的 $p_n := \frac{|D_n|}{n!}$ 有如下概率论理解: 从 S_n 中随机抽取一个置换 f , 则事件 $f \in D_n$ 的概率为 p_n . 特别注意, 当 $n \rightarrow +\infty$ 时,

$$\lim_{n \rightarrow +\infty} p_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = \frac{1}{e}.$$

1.36. 习题. 试求集合 $\mathcal{A} := \left\{ (A_1, A_2, \dots, A_k) \mid A_i \subseteq [n], \bigcup_{i=1}^k A_i = [n] \right\}$

的元素个数.

解. 记全集 $\Omega := (2^{[n]})^k = \{(A_1, A_2, \dots, A_k) \mid A_i \subseteq [n]\}$. 对每个 $\ell \in [n]$, 记

$$\mathcal{A}_\ell := \left\{ (A_1, \dots, A_k) \in \Omega \mid \bigcup_{i=1}^k A_i \subseteq [n] \setminus \{\ell\} \right\}$$

则易知 $\mathcal{A}^c = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_n$, 因此直接套用容斥原理(5)得

$$\begin{aligned} |\mathcal{A}| &= |\mathcal{A}_1^c \cap \dots \cap \mathcal{A}_n^c| = \sum_{j=0}^n (-1)^j \sum_{I \in \binom{[n]}{j}} |\mathcal{A}_I| \\ &= \sum_{j=0}^n (-1)^j \sum_{I \in \binom{[n]}{j}} \# \left\{ (A_1, \dots, A_k) \in \Omega \mid \bigcup_{i=1}^k A_i \subseteq [n] \setminus I \right\} \\ &= \sum_{j=0}^n (-1)^j \sum_{I \in \binom{[n]}{j}} \# \{ (A_1, \dots, A_k) \in \Omega \mid A_i \subseteq [n] \setminus I, i = 1, \dots, k \} \\ &= \sum_{j=0}^n (-1)^j \binom{n}{j} (2^{n-j})^k = (2^k - 1)^n. \end{aligned}$$

□

除了使用容斥原理, 还可以寻找递推关系.

另解. 将题设条件中的集合 \mathcal{A} 重新记为 $\mathcal{A}_{n,k}$; 也就是说, 对任意 $n \geq 0$, $k > 0$, 记

$$\mathcal{A}_{n,k} := \left\{ (A_1, A_2, \dots, A_k) \mid A_i \subseteq [n], \bigcup_{i=1}^k A_i = [n] \right\}.$$

对于 $n \geq 1$, 定义映射 $\varphi_n: \mathcal{A}_{n,k} \rightarrow \mathcal{A}_{n-1,k}$ 如下:

$$\varphi_n: (A_1, A_2, \dots, A_k) \mapsto (A'_1, A'_2, \dots, A'_k),$$

其中 $A'_i := A_i \setminus \{n\} \subseteq [n-1]$. 容易验证映射 φ_n 良定, 并且是满射, 并且对任意 $\mathbf{A} \in \mathcal{A}_{n-1,k}$, 原像集 $\varphi_n^{-1}(\mathbf{A})$ 的元素个数是 $2^k - 1$. 因此 $|\mathcal{A}_{n,k}| = (2^k - 1)|\mathcal{A}_{n-1,k}|$. 由此递推关系可知 $|\mathcal{A}_{n,k}| = (2^k - 1)^n |\mathcal{A}_{0,k}| = (2^k - 1)^n$. □

1.5 数论应用: 欧拉函数 ϕ 与 Möbius 函数 μ

1.37. 记号. 设 n 为正整数. 采用数论中的如下记号:

- 若 $n > 1$, 则 n 可唯一地分解为 $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, 其中 p_1, \dots, p_r 为不同的素数, $a_i > 0$. 对于整数 a, b , “ $a|b$ ” 是指 a 整除 b , 即 $\frac{b}{a} \in \mathbb{Z}$.
- 记 $\phi(n)$ 为与 n 互素的不超过 n 的正整数的个数, 即

$$\phi(n) := \#\{k \in [n] \mid \gcd(k, n) = 1\} \quad (7)$$

函数 $\phi: \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ 称为 **欧拉函数**.

- **Möbius 函数** $\mu: \mathbb{Z}_+ \rightarrow \{-1, 0, 1\}$ 定义如下:

$$\mu(n) := \begin{cases} 1 & \text{若 } n \text{ 形如偶数个互不相同的素数之积} \\ -1 & \text{若 } n \text{ 形如奇数个互不相同的素数之积} \\ 0 & \text{其余情况} \end{cases} \quad (8)$$

特别地, $\phi(1) = \mu(1) = 1$. 对于 $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, 则 $\mu(n) \neq 0$ 当且仅当 $a_1 = a_2 = \cdots = a_r = 1$, 此时 $\mu(n) = (-1)^r$. 而欧拉函数 ϕ 有如下显式表达式:

1.38. 定理. 若 n 有素因子分解 $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, 则

$$\phi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

证明. 利用容斥原理. 令全集 $\Omega := [n]$. 若 $k \in [n]$ 与 n 不互素, 则 k 必然含有 p_1, \dots, p_r 之中的某个素因子. 对每个 $i \in [r]$, 记 $A_i := \{d \in [n] \mid p_i | d\}$. 因此由容斥原理(5)可得

$$\begin{aligned} \phi(n) &= |A_1^c \cap \cdots \cap A_r^c| = \sum_{I \subseteq [r]} (-1)^{|I|} |A_I| \\ &= \sum_{I \subseteq [r]} (-1)^{|I|} \#\left\{d \in [n] \mid \frac{d}{\prod_{i \in I} p_i} \in \mathbb{Z}\right\} \end{aligned}$$

$$= \sum_{I \subseteq [r]} (-1)^{|I|} \frac{n}{\prod_{i \in I} p_i} = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right),$$

其中最后一步利用了1.29的结论 (把那里的 x_i 换成 $-\frac{1}{p_i}$). 得证. \square

1.39.推论. 对于正整数 n , 成立

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

证明. 注意上述定理证明的中间过程, 有

$$\frac{\phi(n)}{n} = \sum_{I \subseteq [r]} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i},$$

由 Möbius 函数的定义易知上式右边恰为 $\sum_{d|n} \frac{\mu(d)}{d}$, 得证. \square

1.40.推论. 函数 ϕ 与 μ 都是积性函数, 即, 若 m, n 互素, 则

$$\phi(mn) = \phi(m) \cdot \phi(n), \quad \mu(mn) = \mu(m) \cdot \mu(n).$$

证明. 由1.38 容易看出 ϕ 是积性函数; 而 μ 的积性可直接由定义看出. \square

1.41.定理. 对于正整数 n , 成立

$$\sum_{d|n} \phi(d) = n, \quad \sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}.$$

其中 $\sum_{d|n}$ 是指 d 取遍 n 的所有正因子 (包括 1 与 n 本身) 的求和.

证明. 对于函数 ϕ , 先考虑 n 为某个素数的幂次, 即 $n = p^a, a \geq 1$ 的情形. 此时

$$\begin{aligned}\sum_{d|n} \phi(d) &= \sum_{k=0}^a \phi(p^k) = 1 + \sum_{k=1}^a p^k \left(1 - \frac{1}{p}\right) \\ &= 1 + \left(\frac{p^{a+1} - 1}{p - 1} - 1\right) \left(1 - \frac{1}{p}\right) \\ &= p^a = n.\end{aligned}$$

而对于一般情形 $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, 注意 1.40, 有

$$\begin{aligned}\sum_{d|n} \phi(d) &= \sum_{\substack{1 \leq b_i \leq a_i \\ i=1,2,\dots,r}} \phi(p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}) = \sum_{\substack{1 \leq b_i \leq a_i \\ i=1,2,\dots,r}} \phi(p_1^{b_1}) \phi(p_2^{b_2}) \cdots \phi(p_r^{b_r}) \\ &= \prod_{i=1}^r \left(\sum_{b=0}^{a_i} \phi(p_i^b) \right) = \prod_{i=1}^r p_i^{a_i} = n.\end{aligned}$$

再看 Möbius 函数 μ . 不妨 $n > 1$, 令 $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, 则

$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{\substack{1 \leq b_i \leq a_i \\ i=1,2,\dots,r}} \mu(p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}) = \sum_{I \subseteq [r]} \mu \left(\prod_{i \in I} p_i \right) = \sum_{I \subseteq [r]} (-1)^{|I|} \\ &= \sum_{k=0}^r \sum_{I \in \binom{[r]}{k}} (-1)^k = \sum_{k=0}^r (-1)^k \binom{r}{k} = (1 - 1)^r = 0.\end{aligned}$$

□

事实上, 等式 $\sum_{d|n} \phi(d) = n$ 还有更简洁的证明, 这个证明无需利用 $\phi(d)$ 的具体表达式, 而只用到最基础的群论知识.

另证. 考虑 n 阶循环群 $G = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, 则显然 $|G| = n$. 另一方面, 对于 G 中的元素 a , 我们回忆, a 的阶是指使得 $a^d = \bar{0}$ 的最小正整数 d . 众所周知, G 中任何元素的阶一定整除 $n = |G|$. 将 G 中的元素按阶分类, 对于每个 $d|n$, 容易验证 G 中的阶为 d 的元素共有 $\phi(d)$ 个 (留给读者练习). 因此, $|G| = \sum_{d|n} \phi(d)$. 从而得证. □

1.42.定理.(Möbius 反演公式). 设 f, g 是定义在 \mathbb{Z}_+ 上的函数, 则

$$f(n) = \sum_{d|n} g(d) \quad \text{当且仅当} \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

证明. 假设第一式成立, 注意利用 1.41, 可得

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) g(d') = \sum_{\substack{d, d' \geq 1 \\ (dd')|n}} \mu(d) g(d') \\ &= \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d) = g(n). \end{aligned}$$

反之, 由第二式推第一式的方法完全类似, 留给读者. □

在上述 Möbius 反演公式中, 取 $f(n) = n, g(n) = \phi(n)$, 则能看出 1.39 与 1.41 之间的内在联系.

2. 母函数方法

2.1 形式幂级数环

我们从一道简单题目说起:

2.43.例题. 将 k 个完全相同的球放入 a, b, c 三个不同箱子中, 要求 a, b 两个箱子里放入偶数个球, 则符合要求的方案有多少?

设 a, b, c 三个箱子里的球的个数分别为 x_1, x_2, x_3 , 则

$$\begin{cases} x_1 + x_2 + x_3 = k \\ x_1, x_2, x_3 \in \mathbb{Z}_{\geq 0}, \quad x_1, x_2 \text{ 是偶数.} \end{cases} \quad (9)$$

问题转化为求上述不定方程的解 (x_1, x_2, x_3) 的个数.

解. 此问题过于简单, 过于特殊, 初中数学的奇技淫巧足够应对. 注意我们对 x_1, x_2 有附加限制 (要求是偶数), 而对 x_3 没有额外要求, 于是不妨先考虑 x_3 的可能取值. 注意 $x_1 + x_2$ 一定是偶数, 从而 $x_3 = k - (x_1 + x_2)$ 与 k 具有相同的奇偶性. 这启发我们分类讨论 k 的奇偶性.

如果 $k = 2m - 1$, ($m \geq 1$) 为奇数, 则 x_3 必为奇数, 其取值范围只可能是 $\{2m' - 1 \mid 1 \leq m' \leq m\}$. 对于 $m' \in [m]$, 当 $x_3 = 2m' - 1$ 时, 有

$$x_1 + x_2 = 2(m - m'),$$

易知满足此方程的非负偶数解 (x_1, x_2) 有 $(m - m' + 1)$ 组. 让 m' 取遍 $1, 2, \dots, m$, 可知原方程组的解 (x_1, x_2, x_3) 的个数为

$$\sum_{m'=1}^m (m - m' + 1) = \frac{m(m+1)}{2}.$$

而 $k = 2m$ 为偶数的情形完全类似, 留给读者. 最终答案为:

$$\begin{cases} \frac{m(m+1)}{2} & \text{若 } k = 2m - 1 \\ \frac{(m+1)(m+2)}{2} & \text{若 } k = 2m \end{cases}. \quad (10)$$

□

2.44. 聪明伶俐的中学生并不会觉得这题有多少意思, 而愚笨迟钝的大学生也许会品出另一番滋味. 我们不妨提出更一般的问题:

若 I_1, I_2, \dots, I_n 都是 $\mathbb{Z}_{\geq 0}$ 的子集 (可以是**无限集**), 则关于未知数 x_1, \dots, x_n 的不定方程

$$\begin{cases} x_1 + x_2 + \dots + x_n = k \\ x_j \in I_j, \quad \forall j = 1, 2, \dots, n \end{cases}$$

有多少组解?

特别地, 当 $n = 3$, $I_1 = I_2 = \{0, 2, 4, 6, \dots\}$, $I_3 = \mathbb{Z}_+$ 时, 就是上一题. 回忆**1.24**, 我们已经解决 I_1, \dots, I_n 都为有限集的特殊情形, 即, 把有限集 I_j 对应于多项式 $f_j(x) = \sum_{i \in I_j} x^i$, 则方程组解的个数与多项式乘积的系数有关系.

于是自然希望, $\mathbb{Z}_{\geq 0}$ 的无限子集也应该能对应到某个“无限项的多项式”, 即, **幂级数**; 并且理解幂级数运算的组合含义.

2.45. 定义. 设 R 是交换环 (例如 $\mathbb{C}, \mathbb{R}, \mathbb{Z}$ 等), 记集合

$$R[[x]] := R^{\mathbb{Z}_{\geq 0}} = \{(a_0, a_1, a_2, \dots) \mid a_i \in R, i \geq 0\},$$

即取值于 R 的序列构成的集合. 并规定集合 $R[[x]]$ 上的加法与乘法如下:

$$1. (a_0, a_1, \dots) + (b_0, b_1, \dots) := (a_0 + b_0, a_1 + b_1, \dots).$$

$$2. (a_0, a_1, \dots) \cdot (b_0, b_1, \dots) := (c_0, c_1, \dots), \text{ 其中 } c_n := \sum_{k=0}^n a_k b_{n-k}.$$

则容易验证 $(R[[x]], +, \cdot)$ 构成交换环 (要验证乘法满足结合律! 留给读者.), 称为环 R 上的**形式幂级数环**.

2.46. 我们更习惯将形式幂级数环 $R[[x]]$ 中的元素 (a_0, a_1, \dots) 记为 $\sum_{k=0}^{\infty} a_k x^k$,

其中 x 是形式变元. 则形式幂级数环的加法, 乘法可改写为

$$\begin{aligned} \sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k &= \sum_{k=0}^{\infty} (a_k + b_k) x^k, \\ \left(\sum_{k=0}^{\infty} a_k x^k \right) \left(\sum_{k=0}^{\infty} b_k x^k \right) &= \sum_{k=0}^{\infty} \left(\sum_{\ell=0}^k a_{\ell} b_{k-\ell} \right) x^k. \end{aligned}$$

上述运算法则与微积分中的幂级数运算完全相同.

2.47. 记号. 设 R 是交换环, 形式幂级数 $f = \sum_{k=0}^{\infty} a_k x^k \in R[[x]]$.

- 与多项式类似, 对于 $k \geq 0$, 记

$$[x^k]f := a_k,$$

即 x^k 项的系数, 或者说是序列 (a_0, a_1, \dots) 的第 k 分量.

- 定义映射 $\frac{d}{dx}: R[[x]] \rightarrow R[[x]]$ 如下:

$$\frac{d}{dx}: (a_0, a_1, a_2, \dots, a_n, \dots) \mapsto (1a_1, 2a_2, \dots, (n+1)a_{n+1}, \dots).$$

映射 $\frac{d}{dx}$ 称为形式幂级数环 $R[[x]]$ 上的**求导**.

用看起来更舒服的记号, 求导映射 $\frac{d}{dx}$ 的定义式可改写为

$$\frac{d}{dx} \left(\sum_{k=0}^{\infty} a_k x^k \right) := \sum_{k=0}^{\infty} (k+1) a_{k+1} x^k = \sum_{k=1}^{\infty} k a_k x^{k-1}.$$

这似乎与微积分中“某个运算”非常像呀. 可以证明形式幂级数环 $R[[x]]$ 的乘法运算与求导运算满足如下关系: 对任意 $f, g \in R[[x]]$, 成立

$$\frac{d}{dx}(f \cdot g) = \frac{df}{dx} \cdot g + f \cdot \frac{dg}{dx}.$$

这似乎很像微积分里的某个运算法则呀.

2.48. 上述关于形式幂级数的一系列定义与性质, 用到任何微积分知识了吗? 虽然大家心里都清楚它背后的想法来自微积分, 但形式幂级数环是纯粹的代数对象, 因为无法在抽象的环 R 上谈论极限, 连续性, 可微性等概念; 并且“ x ”仅仅是抽象的符号, 不能简单粗暴认为是取值于 R 的变量. 所谓无穷求和 $\sum_{k=0}^{\infty} a_k x^k$ 以及求导 $\frac{d}{dx}$, 并非某种极限, 仅仅是抽象定义的代数对象与运算规则.

2.49. 暂且不谈一般的交换环 R , 组合学里常用的情形是 $R = \mathbb{C}$ (或者 \mathbb{R}). 此时, 可以谈论形式幂级数 $f(x) = \sum_{k=0}^{\infty} a_k x^k$ 的收敛性. 如下**收敛半径公式**众所周知: 记

$$\rho := \frac{1}{\limsup_{k \rightarrow \infty} \sqrt[k]{|a_k|}},$$

那么对于复数 $z \in \mathbb{C}$, 若 $|z| < \rho$, 则级数 $\sum_{k=0}^{\infty} a_k z^k$ 收敛. 这个 ρ 称为形式幂级数 $f \in \mathbb{C}[[x]]$ 的**收敛半径**. 如果 $\rho > 0$, 则形式幂级数 $f(x)$ 可以视为定义在 $x = 0$ 附近的函数, 该函数有良好的微分学性质, 可以对它施展微积分的各种技术. 如果收敛半径 $\rho = 0$, 即 $f(x) \in \mathbb{C}[[x]]$ 在 $x = 0$ 之外处处发散, 此时 $f(x)$ 不能对应于某个通常意义下的函数. 尽管如此, 依然可以在形式幂级数环的意义下谈论它的乘法, 求导等运算; 换言之, 无需考虑是否收敛.

在形式幂级数理论的保证下, 很容易将**1.24**的结论推广:

2.50.性质. 若 I_1, I_2, \dots, I_n 都是 $\mathbb{Z}_{\geq 0}$ 的子集 (可以是**无限集**), 记形式幂级数 $f_j(x) = \sum_{i \in I_j} x^i \in \mathbb{C}[[x]]$, $j = 1, \dots, n$, 则关于未知数 x_1, \dots, x_n 的不定方程

$$\begin{cases} x_1 + x_2 + \dots + x_n = k \\ x_j \in I_j, \quad \forall j = 1, 2, \dots, n \end{cases}$$

的解的个数为 $[x^k](f_1 f_2 \cdots f_n)$.

容易验证这里的 f_j 一定是收敛的, 收敛半径至少是 1.

2.51. 重新看例题 2.43. 记

$$f_1(x) = f_2(x) = \sum_{\ell=0}^{\infty} x^{2\ell}, \quad f_3(x) = \sum_{\ell=0}^{\infty} x^{\ell},$$

由前文讨论可知, 符合要求的方案数, 即方程(9)解的个数恰为 $[x^k](f_1 f_2 f_3)$. 注意 $f_1(x) = f_2(x) = \frac{1}{1-x^2}$, $f_3(x) = \frac{1}{1-x}$, 记 $f(x) := f_1(x) f_2(x) f_3(x)$, 则

$$\begin{aligned} f(x) &= \frac{1}{(1-x)^3} \frac{1}{(1+x)^2} \\ &= \frac{1}{4} \frac{1}{(1-x)^3} + \frac{1}{4} \frac{1}{(1-x)^2} + \frac{1}{8} \frac{1}{(1+x)^2} + \frac{3}{16} \frac{1}{1+x} + \frac{3}{16} \frac{1}{1-x}. \end{aligned}$$

再注意泰勒公式, 经计算得

$$[x^k]f = \frac{f^{(k)}(0)}{k!} = \frac{1}{8} \left[(k+1)(k+4+(-1)^k) + \frac{3}{2}(1+(-1)^k) \right]. \quad (*)$$

(容易验证上述 (*) 式与(10)式等价.)

2.52. 例题. 对于 $n \geq 0$, 记 a_n 为方程 $3x + 2y = n$ 的非负整数解 (x, y) 的个数. 求数列 a_n 的通项公式.

解法一. 依然是简单的中学数学. 考虑 n 除以 6 的余数, 分成 6 种情况仔细讨论即可, 细节留给读者. 答案为

$$a_n = \begin{cases} \lfloor n/6 \rfloor & n \equiv 1 \pmod{6} \\ \lfloor n/6 \rfloor + 1 & n \equiv 0, 2, 3, 4, 5 \pmod{6} \end{cases}$$

其中, 对于实数 x , $\lfloor x \rfloor$ 表示 x 的整数部分, 即不超过 x 的最大整数 (向下取整). □

解法二. 记 $x_1 := 3x$, $x_2 := 2y$, 并且记集合 $I_1 := \{0, 3, 6, 9, \dots\}$, $I_2 := \{0, 2, 4, 6, \dots\}$, 则显然 a_n 是方程组

$$\begin{cases} x_1 + x_2 = n \\ x_1 \in I_1, \quad x_2 \in I_2 \end{cases}$$

解的个数. 这就转化为2.50, 然后只剩暴力计算. 按部就班, 记 $f_1(x) = \sum_{\ell \in I_1} x^\ell = \frac{1}{1-x^3}$, 以及 $f_2(x) = \sum_{\ell \in I_2} x^\ell = \frac{1}{1-x^2}$, 则

$$\begin{aligned} f_1(x)f_2(x) &= \frac{1}{(1-x^3)(1-x^2)} \\ &= \frac{1}{6} \cdot \frac{1}{(x-1)^2} + \frac{1}{4} \left(\frac{1}{x+1} - \frac{1}{x-1} \right) + \frac{1}{3} \cdot \frac{1}{x^2+x+1} \\ &= \frac{1}{6} \cdot \frac{1}{(x-1)^2} + \frac{1}{4} \left(\frac{1}{x+1} - \frac{1}{x-1} \right) - \frac{i}{3\sqrt{3}} \left(\frac{1}{x-\omega} - \frac{1}{x-\omega^2} \right), \end{aligned}$$

其中 $i = \sqrt{-1} \in \mathbb{C}$ 为虚数单位, $\omega := e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ 是三次单位根, 故

$$\begin{aligned} a_n &= [x^n](f_1f_2) = \frac{1}{n!} \frac{d^n}{dx^n}(f_1f_2) \Big|_{x=0} \\ &= \frac{n+1}{6} + \frac{1+(-1)^n}{4} + \frac{i}{3\sqrt{3}} (\omega^{2n+2} - \omega^{n+1}). \end{aligned}$$

□

2.53. 接上题, 由 a_n 的组合含义可知 a_n 一定是整数, 然而有意思的是, 解法二给出的通项公式当中明显出现分数, 根号, 甚至虚数. (是不是很惊讶?!) 可以验证上题两种解法给出的 a_n 通项公式其实等价. 注意 $\omega = e^{\frac{2\pi i}{3}}$, 利用三角函数的定义式 $\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$, 可将 a_n 的通项公式进一步化简为

$$a_n = \frac{n+1}{6} + \frac{1+(-1)^n}{4} + \frac{2}{3\sqrt{3}} \sin \frac{2(n+1)\pi}{3}.$$

2.54. 习题. 用本节所介绍的形式幂级数方法重新求解1.9.

留给读者练习.

2.2 母函数方法

形式幂级数环 $\mathbb{C}[[x]]$ 是解决组合问题的强大工具. 我们来看更多例子.

2.55.记号. 对于数列 a_0, a_1, a_2, \dots , 我们习惯把

$$f(x) := \sum_{k=0}^{\infty} a_k x^k \in \mathbb{C}[[x]]$$

俗称为该数列的**母函数**.

2.56.记号. 对于**复数** $z \in \mathbb{C}$, 以及非负整数 $k \in \mathbb{Z}_{\geq 0}$, 记

$$\binom{z}{k} := \frac{z(z-1)\cdots(z-k+1)}{k!}.$$

不妨这样稍微将组合数的概念推广一下. 在此记号下, 有:

2.57.性质. 对任意实数 $r \in \mathbb{R}$, 以及 $x \in (-1, 1)$, 成立

$$(1+x)^r = \sum_{k=0}^{\infty} \binom{r}{k} x^k,$$

特别地, 对于正整数 n , 成立

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

证明. 利用微积分中的泰勒公式即可. 容易验证 $\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}$. □

2.58.例题. 将编号分别为 $1, 2, \dots, n$ 的 n 个不同的球放入编号分别为 a, b, c 的 3 个不同箱子中, 要求任何两个编号相邻的球不能都放入 a 箱子. 符合上述要求的方案数记为 a_n , 求 a_n 的通项公式.

例如, $n=3$ 的时候, 我们把“1 号球放入 a , 2 号球放入 c , 3 号球放入 c ”简记为“ acc ”, 以此类推. 这样子, 每一种放球的方案就对应于一个由 a, b, c 构成的长度为 n 的**字符串**. 于是, 题设条件“两个编号相邻的球不能都放入 a 箱子”相当于说, 相应的字符串中不能出现连续 2 个 a .

- 当 $n=1$ 时, 符合要求的方案共有: a, b, c 三种.

• 当 $n = 2$ 时, 符合要求的方案共有: $ab, ac, ba, bb, bc, ca, cb, cc$ 八种.

从而 $a_1 = 3, a_2 = 8$.

证明. 现在求一般的 a_n . 对于 $n \geq 3$, 考虑 1 号球被放入哪个箱子里. 如果 1 号球被放入 a 箱, 则 2 号球将不能放入 a 箱, 只能放入 b 或 c ; 放完 2 号球之后, 其余 $(n-2)$ 的球的安排方式有 a_{n-2} 种. 如果 1 号球不在 a 箱, 则 1 号球被放入 b 或 c ; 放完 1 号球后, 其余 $(n-1)$ 个球的安排方式有 a_{n-1} 种, 因此

$$a_n = 2a_{n-1} + 2a_{n-2}, \quad \forall n \geq 3.$$

只需再结合初值条件 $a_1 = 3, a_2 = 8$ 求解递推关系即可. 这是众所周知的二阶线性递推数列, 求解方法有多种. 这里介绍母函数方法.

记 $f(x) := \sum_{n=1}^{\infty} a_n x^n$. 那么有

$$\begin{aligned} f(x) &= 3x + 8x^2 + \sum_{n=3}^{\infty} a_n x^n \\ &= 3x + 8x^2 + \sum_{n=3}^{\infty} (2a_{n-1} + 2a_{n-2}) x^n \\ &= 3x + 8x^2 + 2x(f(x) - 3x) + 2x^2 f(x), \end{aligned}$$

从而解得

$$\begin{aligned} f(x) &= \frac{2x^2 + 3x}{1 - 2x - 2x^2} \\ &= -\frac{\sqrt{3} + 3}{12} \frac{1}{x - \frac{\sqrt{3}-1}{2}} + \frac{\sqrt{3} - 3}{12} \frac{1}{x + \frac{\sqrt{3}+1}{2}} - 1. \end{aligned}$$

因此对于 $n \geq 1$, 由泰勒公式直接求导并化简得

$$a_n = \frac{f^{(n)}(0)}{n!} = \frac{3 + 2\sqrt{3}}{6} (1 + \sqrt{3})^n + \frac{3 - 2\sqrt{3}}{6} (1 - \sqrt{3})^n$$

□

由组合意义, a_n 显然是整数, 但其通项公式里出现一大串的根号. 观察上述通项公式, 注意 $|1 - \sqrt{3}| < 1$, 从而当 $n \rightarrow \infty$ 时, $\frac{3 - 2\sqrt{3}}{6} (1 - \sqrt{3})^n$ 非常快地收敛于 0. 不妨忽略掉这一项, 得到 a_n 的近似公式

$$a_n \approx \frac{3 + 2\sqrt{3}}{6} (1 + \sqrt{3})^n.$$

2.59.例题.(Catalan 数). 给定平面上的凸 $(n+2)$ -边形, 用 $(n-1)$ 条连接该多边形顶点的线段将该多边形分割为 n 个三角形. 试求所有可能的分割方法数 $C_n (n \geq 1)$.

在求解通项之前, 先来直接计算 C_n 的前几项.

• 显然 $C_1 = 1$.

• 当 $n = 2$ 时, 只有  两种情况, 故 $C_2 = 2$.

• 当 $n = 3$ 时, 只有形如  的 5 种分割, 故 $C_3 = 5$.

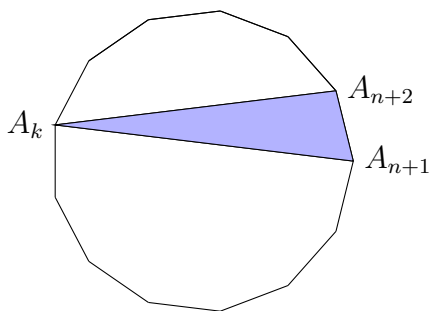
• $n = 4$ 的情形稍微复杂. 对于正六边形的分割, 共有如下三类:



每一类依次包括 6, 6, 2 种情形, 因此 $C_4 = 6 + 6 + 2 = 14$.

解. 对于 $n \geq 1$, 将正 $(n+2)$ -边形的顶点按逆时针依次记作 A_1, A_2, \dots, A_{n+2} . 将这个 $(n+2)$ 边形分割为 n 个小三角形, 只需要如下两步:

1. 先取定 $k \in \{1, 2, \dots, n\}$, 则线段 $A_k A_{n+1}$ 与 $A_k A_{n+2}$ 将这个 $(n+2)$ -边形分为三部分: $\triangle A_k A_{n+1} A_{n+2}$, 以及一个 $(k+1)$ -边形与一个 $(n-k+2)$ -边形, 如下图所示:



2. 再将 $(k+1)$ -边形与 $(n-k+2)$ -边形分割为三角形.

注意到, 如果该 $(n+2)$ 边形已经被分割成 n 个小三角形, 则线段 $A_{n+1} A_{n+2}$ 必为其中某个小三角形的一条边. 换言之, 上述两步操作无非是: 先确定以

$A_{n+1}A_{n+2}$ 为边的那个小三角形, 再确定其余的小三角形. 因此易知数列 C_n 满足递推关系

$$C_n = \sum_{k=1}^n C_{k-1}C_{n-k}, \quad n \geq 1,$$

其中我们额外规定 $C_0 = 1$.

考虑母函数 $f(x) := \sum_{n=0}^{\infty} C_n x^n \in \mathbb{C}[[x]]$, 则

$$\begin{aligned} f(x) &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n-1} C_k C_{n-1-k} \right) x^n \\ &= 1 + x \sum_{n=0}^{\infty} \left(\sum_{k=0}^n C_k C_{n-k} \right) x^n \\ &= 1 + x[f(x)]^2, \end{aligned}$$

解得 $f(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$. 注意 $\lim_{x \rightarrow 0} f(x) = f(0) = 1$, 故舍去 $f(x) = \frac{1 + \sqrt{1-4x}}{2x}$. 因此有

$$\begin{aligned} f(x) &= \frac{1 - \sqrt{1-4x}}{2x} = -\frac{1}{2x} \sum_{n=1}^{\infty} \binom{1/2}{n} (-4x)^n \\ &= 1 + \sum_{n=1}^{\infty} \frac{2^n(2n-1)!!}{(n+1)!} x^n = \sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} x^n. \end{aligned}$$

比较系数得

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

□

上述 C_n 是组合数学中的一个重要的数列, 称为 **Catalan 数**. 除了分割多边形的方法数, 它还有其它非常丰富的组合意义.

2.60. 习题. 对于正整数 n , 在某个圆周上依次标记 $2n$ 个不同的点. 我们希望用 n 条线段将这些点两两相连, 从而把这 $2n$ 个点分成 n 组; 并且要求这 n 条线段中的任意两条都不能相交. 将所有可能的情况个数记为 T_n . 求 T_n 的通项.

不妨从某个点开始, 将这 $2n$ 个点按顺时针依次编号 $1, 2, 3, \dots, 2n$. 把连接第 i 个点与第 j 个点的线段记作 (i, j) . 先来考察 T_n 的前几项.

- $n = 1$ 时: 只有连接 $1, 2$ 两点这种情况, $T_1 = 1$.
- $n = 2$ 时: 可能的情况有 $\{(1, 2), (3, 4)\}$ 与 $\{(1, 4), (2, 3)\}$, 共两种. $T_2 = 2$.
- $n = 3$ 时: 可能的情况有

$$\{(1, 2), (3, 4), (5, 6)\}, \quad \{(1, 2), (3, 6), (4, 5)\}, \quad \{(1, 4), (2, 3), (5, 6)\},$$

$$\{(1, 6), (2, 3), (4, 5)\}, \quad \{(1, 6), (2, 5), (3, 4)\},$$

共五种, 从而 $T_3 = 5$.

解. 方便起见, 不如补充规定 $T_0 = 1$. 对于一般的 n , 首先考虑点 1 与哪个点相连. 如果点 1 与点 i 相连, 则余下的 $(2n - 2)$ 个点自然被分为两组: $A_i := \{j \in \mathbb{Z} \mid 1 < j < i\}$, $B_i := \{j \in \mathbb{Z} \mid i < j \leq 2n\}$. 注意 A_i 中的点与 B_i 中的点不可能有线段相连, 否则相应的线段就会与线段 $(1, i)$ 相交. 由此, 易知 T_n 满足如下递推关系:

$$T_n = T_0 T_{n-1} + T_1 T_{n-2} + \cdots + T_{n-1} T_0.$$

之后同上一题, $T_n = \frac{1}{n+1} \binom{2n}{n}$ 为 Catalan 数. □

2.3 指数型母函数

除了上一节所介绍的通常的母函数, 指数型母函数也是组合计数中的强力工具.

2.61. 记号. 对于数列 a_0, a_1, a_2, \dots , 称

$$g(x) := \sum_{k=0}^{\infty} \frac{a_k}{k!} x^k$$

为该数列的 **指数型母函数**.

我们知道, 阶乘 $k!$ 的组合意义是全排列的个数, 即置换群 S_k 的元素个数, 可见上述指数型母函数往往与顺序、置换有联系. 事实上, 指数型母函数常用来处理与**集合分拆** (即把某个集合划分为满足一定条件的若干子集之并) 有关的问题.

2.62. 例题. 将 k 个**不同**的球放入 a, b, c 三个不同箱子中, 要求 a, b 两个箱子里放入偶数个球, 则符合要求的方案有多少?

注意本题与**2.43**的区别. 后者只需要考虑每个箱子里放几个球, 而本题不仅要考虑每个箱子“放几个球”, 还要考虑“放哪几个球”.

证明. 记符合要求的方案个数为 T_k , 则对每一组 (x_1, x_2, x_3) , 箱子 a, b, c 分别放 x_1, x_2, x_3 个球的方案有 $\binom{k}{x_1, x_2, x_3}$ 种 (回忆多重组合数**1.27**). 取遍所有符合要求的 (x_1, x_2, x_3) , 可知

$$T_k = \sum_{\substack{x_1+x_2+x_3=k \\ x_i \geq 0, x_1, x_2 \text{ 是偶数}}} \binom{k}{x_1, x_2, x_3},$$

从而 $\frac{T_k}{k!} = \sum_{\substack{x_1+x_2+x_3=k \\ x_i \geq 0, x_1, x_2 \text{ 是偶数}}} \frac{1}{x_1!x_2!x_3!}$. 补充定义 $T_0 = 1$, 则易知在 $\mathbb{C}[[x]]$ 中成立

$$\begin{aligned} \sum_{k=0}^{\infty} \frac{T_k}{k!} x^k &= \left(\sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!} \right)^2 \left(\sum_{k=0}^{\infty} \frac{x^k}{k!} \right) \\ &= \left(\frac{e^x + e^{-x}}{2} \right)^2 \cdot e^x = \frac{1}{4} e^{3x} + \frac{1}{2} e^x + \frac{1}{4} e^{-x} \\ &= \sum_{k=0}^{\infty} \frac{3^k + 2 + (-1)^k}{4k!} x^k, \end{aligned}$$

比较系数得 $T_k = \frac{3^k + 2 + (-1)^k}{4}$. □

2.63. 例题. 对于 $n \geq 1$, 记 S_n 为 n 元置换群 (回忆**1.13**). 引入数列 $\{h_n\}$ 如下: 对于 $n \geq 1$,

$$h_n := \# \{f \in S_n \mid f \circ f \circ f = \text{id}\},$$

此外特别规定 $h_0 = 0$. 求指数型母函数 $H(x) := \sum_{n=0}^{\infty} \frac{h_n}{n!} x^n$ 的显式表达式.

解. 设 $f \in S_n$ 满足 $f \circ f \circ f = \text{id}$, 将 f 分解为若干不交轮换之积, 则每个轮换的长度只能为 1 或 3. 为确定这些轮换, 只需先将 $[n]$ 划分为若干元素个数为 1 或 3 的子集的无交并; 然后, 每个元素个数为 1 的子集视为长度为 1 的轮换, 而每个元素个数为 3 的子集可以对应两种不同的 3-轮换. 记 f 包含 s 个 1-轮换与 t 个 3-轮换, 则 $s, t \geq 0, s + 3t = n$. 综上所述可知,

$$h_n = \sum_{\substack{s, t \geq 0 \\ s + 3t = n}} \frac{n!}{s!t!(3!)^t} \cdot 2^t = \sum_{\substack{s, t \geq 0 \\ s + 3t = n}} \frac{n!}{s!t!} \cdot \left(\frac{1}{3}\right)^t,$$

因此

$$\begin{aligned} H(x) &= \sum_{n=0}^{\infty} \frac{h_n}{n!} x^n = \sum_{n=0}^{\infty} \sum_{\substack{s, t \geq 0 \\ s + 3t = n}} \frac{x^{s+3t}}{s!t!} \left(\frac{1}{3}\right)^t \\ &= \sum_{n=0}^{\infty} \sum_{\substack{s, t \geq 0 \\ s + 3t = n}} \frac{x^s}{s!} \cdot \frac{(x^3/3)^t}{t!} = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{x^s}{s!} \cdot \frac{(x^3/3)^t}{t!} \\ &= \left(\sum_{s=0}^{\infty} \frac{x^s}{s!} \right) \left(\sum_{t=0}^{\infty} \frac{(x^3/3)^t}{t!} \right) = e^{x + \frac{x^3}{3}}. \end{aligned}$$

□

用计算机将 $H(x) = e^{x + \frac{x^3}{3}}$ 在 $x = 0$ 处展开, 得

$$\begin{aligned} H(x) &= 1 + x + \frac{1}{2}x^2 + \frac{1}{2}x^3 + \frac{3}{8}x^4 + \frac{7}{40}x^5 + \frac{9}{80}x^6 + \frac{39}{560}x^7 \\ &\quad + \frac{137}{4480}x^8 + \frac{641}{40320}x^9 + \frac{3449}{403200}x^{10} + O(x^{11}), \end{aligned}$$

从而数列 $\{h_n\}$ 的前几项如下:

$$\begin{aligned} h_0 &= h_1 = h_2 = 1, & h_3 &= 3, & h_4 &= 9, & h_5 &= 21, & h_6 &= 81, & h_7 &= 351 \\ h_8 &= 1233, & h_9 &= 5769, & h_{10} &= 31041 \end{aligned}$$

2.64.例题. 某班有 n 位学生, 将这些学生分成若干学习小组, 要求每个小组至少有 2 位同学. 记符合要求的分组方法数为 h_n , 并特别规定 $h_0 = 1$. 求数列 $\{h_n\}$ 的指数型母函数 $H(x) = \sum_{n=0}^{\infty} \frac{h_n}{n!} x^n$ 的表达式.

解. 设班里有 n 个同学, 给定一个分组方案, 若在该分组方案下, 组员个数为 k 的小组有 n_k 个 ($n_k \geq 0, k = 2, 3, \dots$), 注意 $2n_2 + 3n_3 + 4n_4 + \dots = n$, 则这样的分组方式有 $\frac{n!}{\prod_{k \geq 2} n_k! (k!)^{n_k}}$ 种. 从而

$$h_n = \sum_{\substack{n_2, n_3, \dots \geq 0 \\ 2n_2 + 3n_3 + \dots = n}} \frac{n!}{\prod_{k \geq 2} n_k! (k!)^{n_k}},$$

所以 $\{h_n\}$ 的指数型母函数 $H(x)$ 具有表达式

$$\begin{aligned} H(x) &= \sum_{n=0}^{\infty} \sum_{\substack{n_2, n_3, \dots \geq 0 \\ 2n_2 + 3n_3 + \dots = n}} \frac{x^n}{\prod_{k \geq 2} n_k! (k!)^{n_k}} = \sum_{n=0}^{\infty} \sum_{\substack{n_2, n_3, \dots \geq 0 \\ 2n_2 + 3n_3 + \dots = n}} \prod_{k=2}^{\infty} \frac{1}{n_k!} \left(\frac{x^k}{k!} \right)^{n_k} \\ &= \sum_{n_2, n_3, \dots \geq 0} \prod_{k=2}^{\infty} \frac{1}{n_k!} \left(\frac{x^k}{k!} \right)^{n_k} = \prod_{k=2}^{\infty} \left(\sum_{n_k=0}^{\infty} \frac{1}{n_k!} \left(\frac{x^k}{k!} \right)^{n_k} \right) \\ &= \exp \left(\sum_{k=2}^{\infty} \frac{x^k}{k!} \right) = e^{e^x - 1 - x}. \end{aligned}$$

□

用计算机将 $H(x) = e^{e^x - 1 - x}$ 在 $x = 0$ 处展开, 其前几项如下:

$$\begin{aligned} H(x) &= 1 + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{6}x^4 + \frac{11}{120}x^5 + \frac{41}{720}x^6 + \frac{9}{280}x^7 \\ &\quad + \frac{143}{8064}x^8 + \frac{685}{72576}x^9 + \frac{8861}{1814400}x^{10} + O(x^{11}), \end{aligned}$$

从而数列 h_n 的前几项如下:

$$\begin{aligned} h_0 &= 1, & h_1 &= 0, & h_2 &= h_3 = 1, & h_4 &= 4, & h_5 &= 11, & h_6 &= 41, & h_7 &= 162, \\ h_8 &= 715, & h_9 &= 3425, & h_{10} &= 17722. \end{aligned}$$

2.65.例题. 对于正整数 n , 记集合

$$A_n := \{f: [n] \rightarrow \mathbb{Z}_+ \mid \text{存在非负整数 } i, \text{ 使得 } f \text{ 的值域恰为 } [i]\},$$

特别规定 $[0] := \emptyset, A_0 := \{\emptyset\}$. 记 a_n 为 A_n 的元素个数 (特别地, $a_0 = 1$). 求数列 a_n 的指数型母函数 $A(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$ 的具体表达式.

解. 对于数列 $f \in A_n$, 设 f 的值域为 $[i]$ ($i \geq 0$), 然后对每个 $k \in [i]$, 记 $n_k := |f^{-1}(k)|$, 则 $n_k \geq 1$, 且 $n_1 + n_2 + \cdots + n_i = n$. 由此易知

$$a_n = \sum_{i=0}^{\infty} \sum_{\substack{n_1, n_2, \dots, n_i \geq 1 \\ n_1 + n_2 + \cdots + n_i = n}} \binom{n}{n_1, n_2, \dots, n_i},$$

所以 $\{a_n\}$ 的指数型母函数 $A(x)$ 具有表达式

$$\begin{aligned} A(x) &= \sum_{n=0}^{\infty} \sum_{i=0}^{\infty} \sum_{\substack{n_1, n_2, \dots, n_i \geq 1 \\ n_1 + n_2 + \cdots + n_i = n}} \frac{x^n}{n_1! n_2! \cdots n_i!} \\ &= \sum_{i=0}^{\infty} \sum_{n=0}^{\infty} \sum_{\substack{n_1, n_2, \dots, n_i \geq 1 \\ n_1 + n_2 + \cdots + n_i = n}} \prod_{k=1}^i \frac{x^{n_k}}{n_k!} \\ &= \sum_{i=0}^{\infty} \sum_{n_1, n_2, \dots, n_i \geq 1} \prod_{k=1}^i \frac{x^{n_k}}{n_k!} = \sum_{i=0}^{\infty} \prod_{k=1}^i \left(\sum_{n_k=1}^{\infty} \frac{x^{n_k}}{n_k!} \right) \\ &= \sum_{i=1}^{\infty} (e^x - 1)^i = \frac{1}{2 - e^x}. \end{aligned}$$

□

用计算机将 $A(x) = \frac{1}{2 - e^x}$ 在 $x = 0$ 处展开, 其前几项如下:

$$\begin{aligned} A(x) &= 1 + x + \frac{3x^2}{2} + \frac{13x^3}{6} + \frac{25x^4}{8} + \frac{541x^5}{120} + \frac{1561x^6}{240} + \frac{47293x^7}{5040} \\ &\quad + \frac{36389x^8}{2688} + \frac{7087261x^9}{362880} + \frac{34082521x^{10}}{1209600} + O(x^{11}). \end{aligned}$$

从而求得 a_n 的前几项如下:

$$\begin{aligned} a_0 &= a_1 = 1, & a_2 &= 3, & a_3 &= 13, & a_4 &= 75, & a_5 &= 541, & a_6 &= 4683, \\ a_7 &= 47293, & a_8 &= 545835, & a_9 &= 7087261, & a_{10} &= 102247563. \end{aligned}$$

2.66. 再附上例题2.65的若干另解. 笔者在很久以前, 习惯于先寻找数列的递推关系, 然后将递推关系翻译成母函数所满足的 (代数或者微分) 方程, 通过解方程求得母函数. 这也是求解组合计数问题的基本方法.

在例题2.65中, 首先注意, A_n 中的元素是长度为 n 的正整数列, 并且该数列的值域是“连续不断的”. 对于数列 $(a_1, a_2, \dots, a_n, a_{n+1}) \in A_{n+1}$, 该数列

中的项可以分为如下三类: 小于 a_{n+1} 的项, 大于 a_{n+1} 的项, 以及等于 a_{n+1} 的项. 设这三类的个数分别为 k, ℓ, m , 则 $m \geq 1$ 并且 $k + \ell + m = n + 1$. 记第一类, 第二类元素的下标构成的集合分别为 X_-, X_+ , 则 $X_- \in \binom{[n]}{k}$, $X_+ \in \binom{[n]}{\ell}$. 数列中的这两类项分别构成长度为 k, ℓ 的两个子列, 其值域显然都是“连续不断的”, 从而它们可分别视为 A_k, A_ℓ 中的元素. 上述操作可以反过来: 给定 $n \geq 1$ 以及任意 $k, \ell \geq 0$ 使得 $k + \ell \leq n$, 则每个 $(X_-, X_+, f_-, f_+) \in \binom{[n]}{k} \times \binom{[n]}{\ell} \times A_k \times A_\ell$ 都可“重构”出 A_{n+1} 中的一个元素. 将上述想法用形式化的语言表述如下:

例题 2.65 解法二. 为此, 我们来寻找数列 a_n 的递推关系. 取定 $n \geq 0$, 记

$$\mathcal{I}_n := \{(k, \ell) \in \mathbb{Z}^2 \mid k, \ell \geq 0, k + \ell \leq n\}.$$

对于 \mathcal{I}_n 的每一对 (k, ℓ) , 记集合

$$\begin{aligned} \mathcal{A}_{k, \ell} &:= \left\{ (X_-, X_+, f_-, f_+) \left| \begin{array}{l} X_- \in \binom{[n]}{k}, X_+ \in \binom{[n]}{\ell}, X_+ \cap X_- = \emptyset \\ f_- \in A_k, f_+ \in A_\ell \end{array} \right. \right\} \\ &= \left\{ (X_-, X_+) \left| X_- \in \binom{[n]}{k}, X_+ \in \binom{[n]}{\ell}, X_+ \cap X_- = \emptyset \right. \right\} \times A_k \times A_\ell. \end{aligned}$$

断言: 存在 A_{n+1} 与 $\bigsqcup_{(k, \ell) \in \mathcal{I}_n} \mathcal{A}_{k, \ell}$ 之间的一一对应, 从而 $a_{n+1} = \sum_{(k, \ell) \in \mathcal{I}_n} |\mathcal{A}_{k, \ell}|$.

事实上, 对于 $f \in A_{n+1}$, 记

$$X_- := \{i \in [n] \mid f(i) < f(n+1)\}$$

$$X_+ := \{i \in [n] \mid f(i) > f(n+1)\}$$

(都可以是空集), 则显然 $X_+ \cap X_- = \emptyset$. 记 $k := |X_-|, \ell := |X_+|$. 注意存在唯一单调递增的双射 $\varphi_-: [k] \rightarrow X_-$, 存在唯一的单调递增双射 $\varphi_+: [\ell] \rightarrow X_+$. 记

$$f_-(i) := f(\varphi_-(i)), \quad f_+(i) := f(\varphi_+(i)) - f(n+1),$$

则易知 $f_- \in A_k, f_+ \in A_\ell$. 综上所述, $f \mapsto (X_-, X_+, f_-, f_+)$ 给出了从 A_{n+1} 到 $\bigsqcup_{(k, \ell) \in \mathcal{I}_n} \mathcal{A}_{k, \ell}$ 的一个映射. 可以验证这是一一映射 (留给读者. 请读者具体

写出此映射的逆映射). 因此

$$\begin{aligned}
 a_{n+1} &= |A_{n+1}| = \sum_{(k,\ell) \in \mathcal{I}_n} |\mathcal{A}_{k,\ell}| \\
 &= \sum_{\substack{k,\ell \geq 0 \\ k+\ell \leq n}} \# \left\{ (X_-, X_+) \left| X_- \in \binom{[n]}{k}, X_+ \in \binom{[n]}{\ell}, X_- \cap X_+ = \emptyset \right. \right\} \cdot a_k a_\ell \\
 &= \sum_{\substack{k,\ell \geq 0 \\ k+\ell \leq n}} \binom{n}{k} \binom{n-k}{\ell} a_k a_\ell = \sum_{\substack{k,\ell,m \geq 0 \\ k+\ell+m=n}} \frac{n!}{k!\ell!m!} a_k a_\ell,
 \end{aligned}$$

由此递推关系易知

$$\sum_{n=0}^{\infty} \frac{a_{n+1}}{n!} x^n = \left(\sum_{k=0}^{\infty} \frac{a_k}{k!} x^k \right) \left(\sum_{\ell=0}^{\infty} \frac{a_\ell}{\ell!} x^\ell \right) \left(\sum_{m=0}^{\infty} \frac{x^m}{m!} \right)$$

因此数列 a_n 的指数型母函数 $A(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$ 满足微分方程

$$A'(x) = A^2(x) \mathbf{e}^x,$$

解得 $A(x) = \frac{1}{C - \mathbf{e}^x}$. 代入初值 $A(0) = a_0 = 1$ 可确定常数 $C = 2$. 因此,

$$A(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = \frac{1}{2 - \mathbf{e}^x}.$$

特别地, 数列 a_n 满足 $a_n = A^{(n)}(0)$. □

2.67. 笔者后来发现, 上题其实有更简单的解法. 对于长度为 n 的有穷数列 $f \in A_n$, 考虑这个数列的最大值在哪些地方取到. 该数列未取到最大值的那些项构成一个子列, 记该子列的长度为 k . 显然 $k \leq n-1$, 且该子列属于集合 A_k . 由此也可建立数列 $\{a_n\}$ 的递推关系. 整理如下:

例题 2.65 解法三. 对于 $n \geq 1$, 断言: 存在 A_n 与 $\bigsqcup_{k=0}^{n-1} \binom{[n]}{k} \times A_k$ 的一一对应,

从而 $a_n = \sum_{k=0}^{n-1} \binom{n}{k} a_k$. 事实上, 对于 $f \in A_n$, 记

$$X_f := \left\{ i \in [n] \left| f(i) < \max_{j \in [n]} f(j) \right. \right\}.$$

记 X_f 中的全体元素为 $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, 其中 $k := |X_f| \leq n-1$. 之后令

$$\begin{aligned}\bar{f}: [k] &\rightarrow \mathbb{Z}_+ \\ s &\mapsto f(i_s),\end{aligned}$$

则容易验证 $\bar{f} \in A_k$. 这就给出了映射

$$\begin{aligned}\varphi: A_n &\rightarrow \bigsqcup_{k=0}^{n-1} \binom{[n]}{k} \times A_k \\ f &\mapsto (X_f, \bar{f}).\end{aligned}$$

易知上述定义的 φ 是双射 (细节留给读者), 因此当 $n \geq 1$ 时成立 $a_n = \sum_{k=0}^{n-1} \binom{n}{k} a_k$, 从而整理得

$$2 \frac{a_n}{n!} = \sum_{k=0}^n \frac{1}{(n-k)!} \frac{a_k}{k!}, \quad \forall n \geq 1.$$

从而指数型母函数 $A(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$ 满足方程 $2A(x) = e^x A(x) + 1$, 解得

$$A(x) = \frac{1}{2 - e^x}.$$

□

2.68. 例题. 对于正整数 n , 如果 $[n]$ 的排列 (a_1, a_2, \dots, a_n) 满足

$$\forall k \in [n-1], \quad (-1)^k (a_k - a_{k+1}) > 0,$$

即 $a_1 < a_2 > a_3 < a_4 > \cdots$, 则称该排列是 (长度为 n 的) 蛇. 记 s_n 为长度为 n 的蛇的个数, 并额外规定 $s_0 = 1$, 求 $\{s_n\}$ 的指数型母函数 $S(x) := \sum_{n=0}^{\infty} \frac{s_n}{n!} x^n$.

显然 $s_0 = s_1 = 1$. 长度为 2 的蛇只有 $(1, 2)$, 从而 $s_2 = 1$; 长度为 3 的蛇只有 $(1, 3, 2)$ 与 $(2, 3, 1)$ 两条, 从而 $s_3 = 2$. 长度为 4 的蛇有如下 5 条:

$$(1, 3, 2, 4) \quad (1, 4, 2, 3) \quad (2, 3, 1, 4) \quad (2, 4, 1, 3) \quad (3, 4, 1, 2),$$

从而 $s_4 = 5$. 一般情况下, 我们先寻找 $\{s_n\}$ 的递推关系.

解. 当 $n \geq 2$ 时, 设 (a_1, a_2, \dots, a_n) 是一条长度为 n 的蛇. 考察 $[n]$ 中的最大数 n 出现在这条蛇的哪个位置. 注意到, 使得 $a_i = n$ 的正整数 i 只能是偶数; 此外, 若 $a_{2k} = n$, 则 $(a_1, a_2, \dots, a_{2k-1})$ 与 $(a_{2k+1}, a_{2k+2}, \dots, a_n)$ 都是蛇. 由此易知 $\{s_n\}$ 满足如下递推关系:

$$s_0 = s_1 = 1,$$

$$s_n = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n-1}{2k-1} s_{2k-1} s_{n-2k}, \quad n \geq 2.$$

从而当 $n \geq 2$ 时, 对于形式变元 x 有

$$\frac{d}{dx} \left(\frac{s_n}{n!} x^n \right) = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{s_{2k-1}}{(2k-1)!} x^{n-2k} \right) \left(\frac{s_{n-2k}}{(n-2k)!} x^{n-2k} \right).$$

分别考察 $S(x)$ 的偶函数部分与奇函数部分

$$F(x) := \sum_{n=0}^{\infty} \frac{s_{2n}}{(2n)!} x^{2n} = 1 + \sum_{n=1}^{\infty} \frac{s_{2n}}{(2n)!} x^{2n}$$

$$G(x) := \sum_{n=0}^{\infty} \frac{s_{2n+1}}{(2n+1)!} x^{2n+1} = x + \sum_{n=1}^{\infty} \frac{s_{2n+1}}{(2n+1)!} x^{2n+1},$$

则容易验证 $F(x), G(x)$ 满足微分方程

$$\frac{d}{dx} F(x) = F(x)G(x), \quad \frac{d}{dx} G(x) = 1 + G^2(x).$$

结合初值条件 $s_0 = s_1 = s_2 = 1$ 容易解得

$$F(x) = \sec x, \quad G(x) = \tan x,$$

从而 $S(x) = F(x) + G(x) = \sec x + \tan x$. □

此题给出了三角函数 $\tan x, \sec x$ 在 $x = 0$ 处泰勒展开系数的一种组合意义.

2.4 概率论应用: 随机游走

母函数的技巧不仅可以解决某些组合计数问题, 还能应用于概率论等其它领域. 这里举一例说明.

2.69. 例题. 有一只青蛙在数轴上的整数点之间不断跳跃, 遵循如下规则:

- 青蛙的初始位置位于 $x = 1$ 处;
- 青蛙每次会以 $\frac{1}{2}$ 的概率向左跳跃 1 格 (即 -1) 或者向右跳跃 2 格 (即 $+2$);
- 青蛙的各次跳跃行为彼此独立.

试求青蛙能够到达 $x = 0$ 点的概率.

2.70. 作为受过严肃数学教育 (尤其是学过严肃的概率论) 的人, 看到概率论问题, 首先要建立适当的数学模型, 先把概率空间, 事件, 概率测度都说清楚. 在这个问题中, **基本事件空间**可如下选取:

$$\Omega := \{-1, 2\}^{\mathbb{Z}^+} = \{\mathbf{a} = (a_1, a_2, a_3, \dots) \mid a_i = -1, 2, i \geq 1\}$$

即, Ω 中的元素是由 $-1, 2$ 组成的无穷序列. 对于 $\mathbf{a} \in \Omega$, $a_i = -1, 2$ 的意思分别是: 青蛙第 i 次向左跳跃 1 格或向右跳跃 2 格. 对于每个 $i = 1, 2, \dots$, 记 $F_i^+ := \{\mathbf{a} \in \Omega \mid a_i = 2\}$, $F_i^- := \{\mathbf{a} \in \Omega \mid a_i = -1\}$. 令 $\mathcal{F} \subseteq 2^\Omega$ 为由 $\{F_i^\pm\}_{i \geq 1}$ 所生成的 σ -代数, 集合 \mathcal{F} 中的元素为此概率模型中的**事件**. 对于任意 $n \geq 1$, 以及任意 $\mathbf{b} \in \Omega$, 规定 $\mathbb{P}(\{\mathbf{a} \in \Omega \mid a_i = b_i, i = 1, 2, \dots, n\}) = \frac{1}{2^n}$, 易知此 \mathbb{P} 可延拓至 \mathcal{F} , 使之成为**概率测度**. 从而建立概率模型 $(\Omega, \mathcal{F}, \mathbb{P})$. 在此语言框架下, 事件“青蛙能够到达 $x = 0$ ”是指集合

$$A := \left\{ \mathbf{a} \in \Omega \mid \exists i > 0, \sum_{k=1}^i a_k = -1 \right\}.$$

可以验证 $A \in \mathcal{F}$, 即 A 确实是一个事件.

先初步考虑一下. 如果青蛙第一步就向左跳, 那就从起始位置 $x = 1$ 直接跳到目标位置 $x = 0$ 了. 因此青蛙能够到达 $x = 0$ 的概率至少是 $\frac{1}{2}$.

2.71. 现在开始求解此题. 记事件 A_i 为“青蛙在第 i 次跳跃后**首次**到达 $x = 0$ ”, 换言之,

$$A_i = \left\{ \mathbf{a} \in \Omega \mid \sum_{k=1}^i a_k = -1, \text{ 且对任意 } j < i, \sum_{k=1}^j a_k \neq -1 \right\},$$

则事件 $A = \bigsqcup_{i=1}^{\infty} A_i$, 从而 $\mathbb{P}(A) = \sum_{i=1}^{\infty} \mathbb{P}(A_i)$. 之后就是组合计数了.

对于 $i \geq 1$, 记 p_i 为从 $x = 1$ 经过 i 次跳跃首次到达 $x = 0$ 的方法数, 即

$$p_i := \# \left\{ (a_1, \dots, a_i) \in \{-1, 2\}^i \mid \sum_{k=1}^i a_k = -1, \text{ 且对任意 } j < i, \sum_{k=1}^j a_k \neq -1 \right\},$$

则显然 $\mathbb{P}(A_i) = \frac{p_i}{2^i}$, 从而所求概率 $\mathbb{P}(A) = \sum_{i=1}^{\infty} \frac{p_i}{2^i}$.

2.72. 补充定义 $p_0 = 0$, 考虑数列 $\{p_i\}$ 的母函数 $f(x) := \sum_{i=0}^{\infty} p_i x^i$, 则

$$\mathbb{P}(A) = \sum_{i=1}^{\infty} \frac{p_i}{2^i} = f\left(\frac{1}{2}\right).$$

下面来研究数列 p_i 的递推关系. 青蛙从 $x = 1$ 起跳, 如果第一步不幸向右跳, 那么接下来就要考虑“从 $x = 3$ 经过多少步才能够跳到 $x = 0$ ”的问题. 这启发我们引入另外两串数列

$$q_i := \# \left\{ (a_1, \dots, a_i) \in \{-1, 2\}^i \mid \sum_{k=1}^i a_k = -2, \text{ 且对任意 } j < i, \sum_{k=1}^j a_k \neq -2 \right\},$$

$$r_i := \# \left\{ (a_1, \dots, a_i) \in \{-1, 2\}^i \mid \sum_{k=1}^i a_k = -3, \text{ 且对任意 } j < i, \sum_{k=1}^j a_k \neq -3 \right\},$$

并补充定义 $q_0 = r_0 = 0$. 与 p_i 类似, 易知 q_i, r_i 的组合意义, 并且显然

$$p_i = \begin{cases} 1 & i = 1 \\ r_{i-1} & i > 1 \end{cases}. \quad (*)$$

2.73. 现在考察 q_i . 易知 q_i 是青蛙从 $x = N + 2$ 经过 i 次跳跃首次到达 $x = N$ 的所有可能方法数 (这里 N 是任意给定的整数). 注意从 $x = N + 2$ 跳到 $x = N$, 中间必须经过 $x = N + 1$. 如果青蛙在第 ℓ 步首次到达 $x = N + 1$, 那么青蛙要在剩余的 $i - \ell$ 次跳跃首次到达 $x = N$, 因此

$$q_i = \sum_{\ell=1}^{i-1} p_{\ell} p_{i-\ell} = \sum_{\ell=0}^i p_{\ell} p_{i-\ell},$$

从而 $\sum_{i=0}^{\infty} q_i x^i = \left(\sum_{i=0}^{\infty} p_i x^i \right)^2 = f^2(x)$. 同理, 如果青蛙从 $N+3$ 跳到 N , 中间必须经过 $N+2$, 考虑青蛙首次到达 $N+2$ 的时刻, 易知

$$r_i = \sum_{\ell=1}^{i-1} p_{\ell} q_{i-\ell} = \sum_{\ell=0}^i p_{\ell} q_{i-\ell},$$

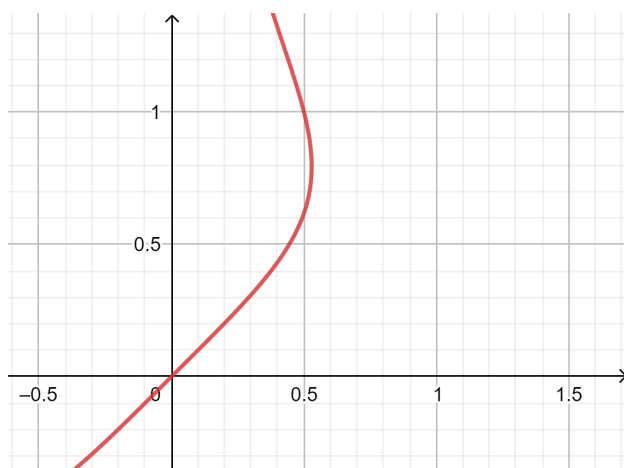
从而 $\sum_{i=0}^{\infty} r_i x^i = \left(\sum_{i=0}^{\infty} p_i x^i \right) \left(\sum_{i=0}^{\infty} q_i x^i \right) = f^3(x)$. 再注意2.72的 (*), 可得

$$f^3(x) = \sum_{i=0}^{\infty} c_i x^i = \sum_{i=1}^{\infty} a_{i+1} x^i = \frac{1}{x} (f(x) - x),$$

即 $f(x) = x f^3(x) + x$. $f(x)$ 是由此式所确定的隐函数. 我们难以具体地把 $f(x)$ 解出来, 本题中只需求出 $\mathbb{P}(A) = f(\frac{1}{2})$. 令 $x = \frac{1}{2}$, 得 $\mathbb{P}(A)^3 - 2\mathbb{P}(A) + 1 = 0$, 容易解得 $\mathbb{P}(A) = 1, \frac{\sqrt{5}-1}{2}, \frac{-\sqrt{5}-1}{2}$ (舍去).

2.74. 所以这个概率到底是 1 还是 $\frac{\sqrt{5}-1}{2}$? 从感觉上来说, 青蛙每次向左或者向右的机会均等, 但向右的时候跳两格, 因此青蛙的位置很可能会越来越向右. 这么看来, 青蛙最终能够到达 $x=0$ 的概率不太可能是 1. 但概率论的经验表明, 人类朴素的直觉往往不可靠, 我们不可妄下结论.

其实非常简单, 毕竟函数 $y = f(x)$ 被 $y = xy^3 + x$ 完全确定. 不如画出曲线 $y = xy^3 + x$ 的图像:



直接观察可知 $f(\frac{1}{2}) \neq 1$. (注意 $f(x)$ 应该是连续函数, 考虑 x 从 0 连续地变化到 $\frac{1}{2}$, 观察图像可知 y 相应地从 0 连续地变化到 $\frac{\sqrt{5}-1}{2}$, 而不是 1. 这个思路能用数学分析的各种办法来严格说清楚, 这里从略). 因此青蛙能够到达 $x=0$ 的概率为 $\frac{\sqrt{5}-1}{2}$.

3. 极值集合论 I: 基本概念与方法

给定正整数 n , 设集族 $\mathcal{F} \subseteq 2^{[n]}$, 即, \mathcal{F} 是 $[n]$ 的若干子集构成的集合. 所谓极值集合论, 主要研究这样一类问题: 如果集族 \mathcal{F} 满足某些限制条件, 那么 \mathcal{F} 的元素个数至多 (至少) 是多少?

本章首先是组合数学入门, 介绍组合数学的两个基本方法: 算两次与抽屉原理; 然后作为极值集合论入门, 介绍极值集合论的 3 个经典结果:

1. Sperner 定理;
2. Bollobás 定理;
3. Erdős-Ko-Rado 定理.

3.1 算两次

所谓“算两次”, 是指通过用两种不同方法来计算某个给定集合 X 的元素个数. 这是组合数学的基本技巧之一. 集合 X 的元素个数 $|X|$ 是确定的, 从而用不同的方法计算 $|X|$ 会得到相同的结果. 例如 1.6 与 1.7 的证明方法就是典型的“算两次”; 此外, 1.41 的另证所使用的方法也是“算两次”, 即用两种不同方法来计算 $|G|$. 以下是最常见的“算两次”模型:

3.75. 定理.(Fubini). 设 A, B 为非空有限集, $S \subseteq A \times B$. 对于每个 $a \in A$, 记 $L_a := \{b \in B \mid (a, b) \in S\}$; 对每个 $b \in B$, 记 $R_b := \{a \in A \mid (a, b) \in S\}$. 则以下等式成立:

$$\sum_{a \in A} |L_a| = \sum_{b \in B} |R_b|.$$

证明. 显然上式等号两边都等于 $|S|$, 从而得证. □

用算两次方法能够证明组合恒等式, 我们再看一例.

3.76.例题. 对于正整数 m, n , 成立

$$\sum_{k=0}^m \binom{m}{k} \binom{n+k}{m} = \sum_{k=0}^n \binom{m}{k} \binom{n}{k} 2^k. \quad (11)$$

先看如下言语粗俗但富有启发性的“不靠谱证明”:

证明. 设想有 m 个男生与 n 个女生, 考虑如下的活动: 给一部分男生糖吃, 从总共的 $(m+n)$ 个人里面挑选 m 个人吃屎, 要求被选中吃屎的男生必须吃过糖. 那么符合要求的活动方案有多少种?

一方面, 先考虑吃糖的男生有几个. 若有 k 个男生吃糖, 则被选中吃屎的 m 个人只可能来自这 k 个吃糖的男生以及 n 个女生, 因此 k 个男生吃糖的方案共有 $\binom{m}{k} \binom{n+k}{m}$ 种, 总方案数为 $\sum_{k=0}^m \binom{m}{k} \binom{n+k}{m}$.

另一方面, 先考虑吃屎的女生有几个. 若吃屎的女生有 k 个, 则还须另选 $(m-k)$ 个男生吃屎, 这 $(m-k)$ 个吃屎的男生必须吃过糖; 而余下的 k 个不吃屎的男生中的每一个都可能吃糖或者没吃糖, 因此 k 个女生吃屎的方案共有 $\binom{n}{k} \binom{m}{m-k} 2^k = \binom{n}{k} \binom{m}{k} 2^k$ 种, 从而总方案数为 $\sum_{k=0}^n \binom{n}{k} \binom{m}{k} 2^k$.

用两种方法计数同一个问题, 结果必然相等, 得证. \square

围绕一个组合恒等式, 我们可以尽可能编故事来解释其组合含义, 故事可以要多离谱有多离谱, 全靠一张嘴. 这种“编故事”的方法不够严肃有失体面, 甚至容易挑起性别对立. 我们把上述证明思路翻译为如下文明用语:

严肃而文明的表达. 取定 $(m+n)$ 个两两不同的元素 $x_1, \dots, x_m; y_1, \dots, y_n$, 记集合 $X = \{x_1, \dots, x_m\}, Y = \{y_1, \dots, y_n\}$. 记

$$\Omega := 2^X \times 2^{X \sqcup Y}$$

$$\Phi := \{(A, B) \in \Omega \mid B \cap X \subseteq A, |B| = m\}.$$

一方面, 注意无交并 $\Phi = \bigsqcup_{k=0}^{|X|} \left\{ (A, B) \in \Omega \mid \begin{array}{l} |B| = m, B \cap X \subseteq A \\ |A| = k \end{array} \right\}$, 再注意

$$\begin{aligned} & \left\{ (A, B) \in \Omega \mid \begin{array}{l} |B| = m, B \cap X \subseteq A \\ |A| = k \end{array} \right\} \\ &= \left\{ (A, B) \in \Omega \mid |A| = k, B \in \binom{Y \sqcup A}{m} \right\} \\ &= \bigsqcup_{A \in \binom{X}{k}} \left\{ (A, B) \in \Omega \mid B \in \binom{Y \sqcup A}{m} \right\}, \end{aligned}$$

从而由基本计数原理1.3可知,

$$\begin{aligned} |\Phi| &= \sum_{k=0}^{|X|} \# \left\{ (A, B) \in \Omega \mid \begin{array}{l} |B| = m, B \cap X \subseteq A \\ |A| = k \end{array} \right\} \\ &= \sum_{k=0}^m \sum_{A \in \binom{X}{k}} \# \left\{ (A, B) \in \Omega \mid B \in \binom{Y \sqcup A}{m} \right\} \\ &= \sum_{k=0}^m \sum_{A \in \binom{X}{k}} \# \left\{ B \in 2^{X \sqcup Y} \mid B \in \binom{Y \sqcup A}{m} \right\} \\ &= \sum_{k=0}^m \sum_{A \in \binom{X}{k}} \# \binom{Y \sqcup A}{m} = \sum_{k=0}^m \sum_{A \in \binom{X}{k}} \binom{n+k}{m} = \sum_{k=0}^m \binom{m}{k} \binom{n+k}{m}. \end{aligned}$$

而另一方面, 注意无交并 $\Phi = \bigsqcup_{k=0}^{|Y|} \left\{ (A, B) \in \Omega \mid \begin{array}{l} |B| = m, B \cap X \subseteq A \\ |B \cap Y| = k \end{array} \right\}$,

直接验证可知, 对于每个 k , 映射

$$\begin{aligned} f_k: & \left\{ (A, B) \in \Omega \mid \begin{array}{l} |B| = m, B \cap X \subseteq A \\ |B \cap Y| = k \end{array} \right\} \\ & \rightarrow \binom{Y}{k} \times \left\{ (A', B') \in X^2 \mid \begin{array}{l} |B'| = m - k \\ A' \in 2^{X \setminus B'} \end{array} \right\} \\ & (A, B) \mapsto (B \cap Y, A \setminus (B \cap X), B \cap X) \end{aligned}$$

是**一一对应**, 因此由基本计数原理可得

$$|\Phi| = \sum_{k=0}^{|Y|} \# \left\{ (A, B) \in \Omega \mid \begin{array}{l} |B| = m, B \cap X \subseteq A \\ |B \cap Y| = k \end{array} \right\}$$

$$\begin{aligned}
&= \sum_{k=0}^{|Y|} \left| \binom{Y}{k} \right| \# \left\{ (A', B') \in X^2 \mid \begin{array}{l} |B'| = m - k \\ A' \in 2^{X \setminus B'} \end{array} \right\} \\
&= \sum_{k=0}^n \binom{n}{k} \sum_{B' \in \binom{X}{m-k}} |2^{X \setminus B'}| = \sum_{k=0}^n \binom{n}{k} \sum_{B' \in \binom{X}{m-k}} 2^k \\
&= \sum_{k=0}^n \binom{n}{k} \binom{m}{m-k} 2^k = \sum_{k=0}^n \binom{n}{k} \binom{m}{k} 2^k.
\end{aligned}$$

综上所述, (11)式的等号两边都等于 $|\Phi|$, 故它们相等. \square

(但是, 如此“严肃而文明”真的好吗? 以后在书写证明过程时将避免“过于粗俗”与“过于文明”这两种极端.)

3.77.例题. 对于自然数 $n \geq 0$, 记 $C_n := \frac{1}{n+1} \binom{2n}{n}$ 为 Catalan 数 (见例题2.59). 证明如下等式:

$$\sum_{\substack{i+j+k=n \\ i,j,k \geq 0}} C_{i+j} C_{j+k} C_{k+i} = \frac{3}{2n+3} C_{2n+1}.$$

证明. 考虑平面内的某个正 $(2n+3)$ -边形 $A_1 A_2 \cdots A_{2n+3}$, 再记 O 为其几何中心. 像例题2.59那样用其对角线分割为 $(2n+1)$ 个三角形, 这样的划分方式共有 C_{2n+1} 种, 记 \mathcal{P}_n 为这 C_{2n+1} 种分割方式构成的集合.

由于正奇数边形的任何对角线都不经过中心点 O , 因此对任意 $\mathbf{P} \in \mathcal{P}_n$, 在被分割所得的 $(2n+1)$ 个三角形当中存在唯一一个三角形, 使得中心点 O 落在在此三角形内部. 我们记这个三角形为 $\triangle_{\mathbf{P}}$.

引入集合

$$\Phi := \{(\mathbf{P}, i) \in \mathcal{P}_n \times [2n+3] \mid A_i \text{ 是三角形 } \triangle_{\mathbf{P}} \text{ 的一个顶点}\}.$$

我们对 $|\Phi|$ 算两次. 一方面, 先取定 $\mathbf{P} \in \mathcal{P}_n$, 然后再标记 $\triangle_{\mathbf{P}}$ 的其中一个顶点, 从而显然有

$$|\Phi| = 3C_{2n+1}.$$

另一方面, 也可以如此计数 $|\Phi|$:

1. 先取定 $i \in [2n+3]$;

2. 再取定 $j, k \in [2n+3]$ 使得点 O 落在 $\triangle A_i A_j A_k$ 的内部, 并且顶点 A_i, A_j, A_k 绕中心点 O 逆时针排列;
3. 再考虑使得 $\triangle_P = \triangle A_i A_j A_k$ 的 $P \in \mathcal{P}_n$ 有多少个.

记从 A_i 出发沿着该正多边形的边逆时针到 A_j , 中间间隔了 c 个顶点; 从 A_j 逆时针到 A_k 间隔 a 个顶点, 从 A_k 逆时针到 A_i 间隔 b 个顶点, 则

$$a, b, c \geq 0, \quad a + b + c = 2n.$$

此外, 由中心点 O 落在 $\triangle A_i A_j A_k$ 内部, 易知 $a, b, c \leq n$. 综上所述, 易知

$$|\Phi| = (2n+3) \sum_{\substack{0 \leq a, b, c \leq n \\ a+b+c=2n}} C_a C_b C_c.$$

而容易验证如下——对应:

$$\left\{ (a, b, c) \left| \begin{array}{l} 0 \leq a, b, c \leq n \\ a + b + c = 2n \end{array} \right. \right\} \rightarrow \left\{ (i, j, k) \left| \begin{array}{l} 0 \leq i, j, k \leq n \\ i + j + k = n \end{array} \right. \right\}$$

$$(a, b, c) \mapsto (n-a, n-b, n-c),$$

由此替换求和指标可得

$$|\Phi| = (2n+3) \sum_{\substack{0 \leq i, j, k \leq n \\ i+j+k=n}} C_{j+k} C_{k+i} C_{i+j}.$$

综上, 证毕. □

“算两次”方法除了能用来证明组合恒等式, 还有很多奇妙应用.

3.78. 例题. 对于正整数 n , 记

$$H(n) := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n},$$

$$T(n) := \# \left\{ d \in \mathbb{Z}_+ \left| \frac{n}{d} \in \mathbb{Z} \right. \right\} \quad (\text{即 } n \text{ 的正因子的个数}),$$

$$\overline{T(n)} := \frac{1}{n} \sum_{k=1}^n T(k) \quad (\text{即 } 1, 2, \dots, n \text{ 的正因子个数的平均数}),$$

则以下不等式成立:

$$\left| H_n - \overline{T(n)} \right| < 1.$$

我们知道, 如果 n 的素因子分解形如 $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, 则 n 的正因子个数 $T(n) = (a_1 + 1)(a_2 + 1) \cdots (a_s + 1)$. (留作练习). 可见 $T(n)$ 的值严重依赖 n 的素因子分解, 而素数分布的规律又神秘莫测. 本题表明, $1, 2, \dots, n$ 的正因子个数的平均值约等于 $H(n)$, 这是非常不平凡的结果.

证明. 记集合 $A = B = [n]$, 定义 $A \times B$ 的子集 S 如下:

$$S := \{(i, j) \in A \times B \mid i \text{ 能够整除 } j\}$$

接下来利用 3.75. 一方面,

$$|S| = \sum_{j=1}^n \#\{i \in [n] \mid i \text{ 能够整除 } j\} = \sum_{j=1}^n T(j) = n\overline{T(n)};$$

而另一方面,

$$|S| = \sum_{i=1}^n \#\{j \in [n] \mid j \text{ 是 } i \text{ 的倍数}\} = \sum_{i=1}^n \lfloor \frac{n}{i} \rfloor,$$

其中 $\lfloor x \rfloor$ 为 x 的向下取整. 因此,

$$\begin{aligned} \left| \overline{T(n)} - H(n) \right| &= \left| \frac{1}{n} \sum_{i=1}^n \lfloor \frac{n}{i} \rfloor - \sum_{i=1}^n \frac{1}{i} \right| \leq \frac{1}{n} \sum_{i=1}^n \left| \lfloor \frac{n}{i} \rfloor - \frac{n}{i} \right| \\ &\leq \frac{1}{n} \sum_{i=1}^n 1 = 1. \end{aligned}$$

□

以后将遇到“算两次”方法的更多应用.

3.2 抽屉原理

3.79. 将 3 个苹果放到 2 个抽屉里, 则某个抽屉里有至少 2 个苹果. 类似地, 将 100 个苹果放到 3 个抽屉里, 则某个抽屉里有至少 34 个苹果, 这是因为, 假如每个抽屉都至多 33 个苹果, 则苹果总数 $\leq 33 \times 3 = 99$, 与总共 100 个苹果矛盾. 这就是所谓**抽屉原理**.

3.80.定理.(抽屉原理). 设 X_1, X_2, \dots, X_k 是 k 个两两不交的集合, $X := \bigsqcup_{i=1}^k X_i$.

给定非负整数 n_1, n_2, \dots, n_k . 如果

$$|X| \geq 1 + \sum_{i=1}^k (n_i - 1),$$

则存在 $i \in [k]$ 使得 $|X_i| \geq n_i$.

证明. 用反证法, 留给读者. □

苹果放进抽屉的道理大家都懂, 然而什么是“苹果”, 什么是“抽屉”?

3.81.例题. 设 n 是正整数. 已知集合 $S \subseteq [2n]$ 中的任何两个不同元素都没有整除关系, 求 $|S|$ 的最大值.

解. 首先注意到, $S = \{n+1, n+2, \dots, 2n\}$ 显然满足要求, 即其中的任何两个不同元素都没有整除关系. 因此 $|S|$ 可以取 n .

另一方面, 我们断言 $|S|$ 不可能超过 n , 换言之, 如果 $|S| \geq n+1$, 则必然存在 $i, j \in S$ 使得 i 整除 j . 注意任何正整数 m 都能唯一地写成

$$m = (2r+1) \cdot 2^s, \quad r, s \in \mathbb{Z}_{\geq 0}.$$

对每个 $r \geq 0$, 记正整数集的子集 $X_r := \{(2r+1) \cdot 2^s \mid s \geq 0\}$. 从而对于 $S \subseteq [2n]$, 易知可将 X 划分为 n 个集合的无交并:

$$S = \bigsqcup_{r=0}^{n-1} (X_r \cap S).$$

如果 $|S| \geq n+1$, 则有抽屉原理可知必存在某个 $i \in \{0, 1, \dots, n-1\}$ 使得 $|S \cap X_i| \geq 2$. 注意 $S \cap X_i$ 中的任何两个元素都显然具有整除关系, 断言得证. 综上所述, $|S|$ 的最大值为 n . □

3.82.例题.(Dirichlet, 1879). 证明: 对任意 $n \in \mathbb{Z}_+$, $x \in \mathbb{R}$, 存在有理数 $\frac{p}{q} \in \mathbb{Q}$,

使得 $1 \leq q \leq n$, 并且 $\left| x - \frac{p}{q} \right| \leq \frac{1}{nq}$.

证明. 不妨 $x > 0$. 对于实数 x , 记 $\{x\} := x - \lfloor x \rfloor$, 称为 x 的小数部分. 则对任意 $i \in [n+1]$, 显然 $\{ix\} \in [0, 1)$. 将区间 $[0, 1)$ 平均分成 n 个子区间的无交并:

$$[0, 1) = [0, \frac{1}{n}) \sqcup [\frac{1}{n}, \frac{2}{n}) \sqcup \cdots \sqcup [\frac{n-1}{n}, 1),$$

则由抽屉原理, $\{ix\}, i = 1, 2, \dots, n+1$ 这 $n+1$ 个元素当中必有两个落在同一个子区间当中, 不妨记为 $\{ix\}, \{jx\}, 1 \leq i < j \leq n+1$. 于是显然 $|\{ix\} - \{jx\}| < \frac{1}{n}$,

$$\begin{aligned} |(j-i)x - (\lfloor jx \rfloor - \lfloor ix \rfloor)| &< \frac{1}{n} \\ \left| x - \frac{\lfloor jx \rfloor - \lfloor ix \rfloor}{j-i} \right| &< \frac{1}{n(j-i)}. \end{aligned}$$

取 $p := \lfloor jx \rfloor - \lfloor ix \rfloor, q := j-i$ 即可. □

3.83.例题.(Erdős-Szekeres, 1935). 给定正整数 m, n , 则对于长度为 $(mn+1)$ 的任何有限实数列 $a_0, a_1, a_2, \dots, a_{mn}$, 必存在长度为 $(m+1)$ 的单调递增子列, 或者存在长度为 $(n+1)$ 的单调递减子列.

注意这里的“单调递增”并非指严格递增, 例如 $1, 1, 1, 2, 2, 4, \dots$ 也属于单调递增数列. 单调递减也同样. 此外还要注意, 长度为 1 的数列 (即, 只有一项) 显然是单调递增的, 也显然是单调递减的.

证明. 对于每个 $0 \leq i \leq mn$, 记 f_i 是以 a_i 为首项的单调递增子列的最大长度. 于是, 如果某个 i 满足 $f_i \geq m+1$, 则由 f_i 的定义立刻推出该数列存在长度为 $m+1$ 的单调递增子列, 得证.

于是, 不妨假设对任意 i 都成立 $1 \leq f_i \leq m$. 从而自然有映射

$$\begin{aligned} \{0, 1, \dots, mn\} &\rightarrow \{1, 2, \dots, m\} \\ i &\mapsto f_i, \end{aligned}$$

如此将 $(mn+1)$ 个苹果放入 m 个抽屉中, 某个抽屉里必然有至少 $(n+1)$ 个苹果. 即, 存在 $0 \leq i_0 < i_1 < \cdots < i_n \leq mn$, 使得 $f_{i_0} = f_{i_1} = \cdots = f_{i_n}$. 断言: 数列 $a_{i_0}, a_{i_1}, \dots, a_{i_n}$ 单调递减, 从而存在长度为 $(n+1)$ 的单调递减子列. 其证明留给读者 (反证法, 利用 f_i 的定义), 定理得证. □

以后将遇到抽屉原理的更多应用.

3.3 Sperner 定理

3.84.定义. 设 n 为正整数, 集族 $\mathcal{F} \subseteq 2^{[n]}$. 如果 \mathcal{F} 中的任何两个不同元素 A, B 都满足 $A \not\subseteq B$ 且 $B \not\subseteq A$, 则称 \mathcal{F} 是**独立系统**.

换言之, 集族 \mathcal{F} 是独立系统, 当且仅当 \mathcal{F} 中的集合互不包含. 例如, 对任意 $k \leq n$, $[n]$ 的全体 k 元子集构成的集族 $\binom{[n]}{k}$ 显然是独立系统. 众所周知, 当 $k = \lfloor \frac{n}{2} \rfloor$ 或 $\lceil \frac{n}{2} \rceil$ 时, 组合数 $\binom{n}{k}$ 取到最大值 $\max_{0 \leq k \leq n} \binom{n}{k} = \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

自然的问题是, 如果 \mathcal{F} 是独立系统, 则 $|\mathcal{F}|$ 最大可能是多少? 由上述讨论, 可知 $|\mathcal{F}|$ 可以取到 $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. 事实上, $|\mathcal{F}|$ 不可能比这个数更大了, 因为如下定理:

3.85.定理.(Sperner, 1928). 若 $\mathcal{F} \subseteq 2^{[n]}$ 是独立系统, 则

$$|\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

我们将用 3 种方法证明此定理; 其中第二种证法需要用到某个引理, 该引理也 2 种证法. 这些不同证法各有精彩之处, 值得欣赏. 逻辑框架如下:

$$\text{Sperner 定理} \left\{ \begin{array}{l} \text{证法 1: 算两次 (LYM 不等式)} \\ \text{证法 2: 抽屉原理 (利用某引理)} \left\{ \begin{array}{l} \text{引理证法 1: 数学归纳法} \\ \text{引理证法 2: 组合构造} \end{array} \right. \\ \text{证法 3: Bollobás 定理 3.91 的直接推论} \end{array} \right.$$

3.86.

Sperner 定理证法一. 我们称集族 $\mathcal{C} \subseteq 2^{[n]}$ 为**链**, 如果 \mathcal{C} 中的任何两个不同元素都具有严格包含关系. 换言之, 集族 $\mathcal{C} \subseteq 2^{[n]}$ 是链, 当且仅当 \mathcal{C} 中的所有元素能够排成严格单调递增的集合序列:

$$\mathcal{C}: A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_k$$

对于链 \mathcal{C} , 称 $|\mathcal{C}|$ 为链 \mathcal{C} 的**长度**. 注意链的长度最多为 $(n+1)$. 长度为 $(n+1)$ 的链称为**极大链**. 设 \mathcal{C} 为 $2^{[n]}$ 的极大链, 则显然 \mathcal{C} 必形如

$$\emptyset = A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n = [n],$$

使得 $|A_k| = k, \forall k \in [n]$.

断言: $2^{[n]}$ 的极大链与 $[n]$ 的全排列之间有自然的一一对应, 从而特别地, $2^{[n]}$ 恰有 $n!$ 条不同的极大链. 这是因为, 设 \mathcal{C} 为极大链, 则 \mathcal{C} 必形如 $\emptyset \subsetneq \{x_1\} \subsetneq \{x_1, x_2\} \subsetneq \{x_1, x_2, x_3\} \subsetneq \cdots \subsetneq [n]$. 依次记录后一个集合比前一个集合新增的元素, 得到序列 x_1, x_2, \dots, x_n , 这是 $[n]$ 的一个全排列. 反之, 对于 $[n]$ 的每一个全排列 x_1, x_2, \dots, x_n , 考虑极大链 $\emptyset \subsetneq \{x_1\} \subsetneq \{x_1, x_2\} \subsetneq \{x_1, x_2, x_3\} \subsetneq \cdots \subsetneq [n]$. 易知这是一一对应. 从而断言得证.

现在设 $\mathcal{F} \subseteq 2^{[n]}$ 是独立系统. 记集合

$$\mathcal{S} := \{(\mathcal{C}, A) \mid \mathcal{C} \subseteq 2^{[n]} \text{ 是极大链}, A \in \mathcal{F} \cap \mathcal{C}\}.$$

由独立系统与链的定义可知, 对任何链 \mathcal{C} , $|\mathcal{F} \cap \mathcal{C}| \leq 1$. 从而

$$|\mathcal{S}| = \sum_{\mathcal{C} \text{ 是极大链}} |\mathcal{F} \cap \mathcal{C}| \leq \sum_{\mathcal{C} \text{ 是极大链}} 1 = n!.$$

而另一方面,

$$\begin{aligned} |\mathcal{S}| &= \sum_{A \in \mathcal{F}} \#\{\mathcal{C} \text{ 是极大链} \mid A \in \mathcal{C}\} = \sum_{A \in \mathcal{F}} |A|!(n - |A|)! = \sum_{A \in \mathcal{F}} \frac{n!}{\binom{n}{|A|}} \\ &\geq \sum_{A \in \mathcal{F}} \frac{n!}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = |\mathcal{F}| \cdot \frac{n!}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}, \end{aligned}$$

因此 $|\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$, 得证. □

上述证法实际上证明了如下 **LYM 不等式**:

3.87.定理.(LYM 不等式: Lubell, 1966; Yamamoto, 1954; Meshalkin, 1963) 若集族 $\mathcal{F} \subseteq 2^{[n]}$ 是独立系统, 则

$$\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \leq 1.$$

我们将在后文介绍 LYM 不等式的推广—Bollobás 定理**3.91**.

利用抽屉原理, 还可以给出 Sperner 定理的另一种证明. 设集族 $\mathcal{C} \subseteq 2^{[n]}$ 是链, 如果存在某个 k 使得 \mathcal{C} 中各集合的元素个数依次为 $k, k+1, k+2, \dots, n-k$, 则称 \mathcal{C} 是**对称链**. 我们需要如下引理:

3.88.引理.(对称链分解). 设 n 是正整数, 则集族 $2^{[n]}$ 可划分为对称链的无交并; 换言之, 存在两两不交的对称链 C_1, C_2, \dots, C_m 使得 $2^{[n]} = \bigsqcup_{i=1}^m C_i$.

稍后再证这个引理. 先承认它, 并用它来给出 Sperner 定理的证法 2.

3.89.

Sperner 定理证法二. 任取 $2^{[n]}$ 的一个对称链分解 $2^{[n]} = \bigsqcup_{i=1}^k C_i$. 断言: 对称链

的条数 $k = \binom{n}{\lfloor \frac{n}{2} \rfloor}$. 这是因为, 由对称链的定义可知任何对称链必唯一穿过集族 $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$; 而另一方面, 由 $C_i, 1 \leq i \leq k$ 的定义可知集族 $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$ 中的任何集合都被 $C_i, 1 \leq i \leq k$ 中的唯一一条链穿过, 这就建立了 $\{C_i | 1 \leq i \leq k\}$ 与 $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$ 的一一对应, 因此 $k = \binom{n}{\lfloor \frac{n}{2} \rfloor}$, 断言得证.

于是, 任何集族 $\mathcal{F} \subseteq 2^n$ 都可划分为 $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ 个子集 (可以是空集) 的无交并

$$\mathcal{F} = \bigsqcup_{i=1}^{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \mathcal{F} \cap C_i.$$

如果 $|\mathcal{F}| > \binom{n}{\lfloor \frac{n}{2} \rfloor}$, 则由抽屉原理, 必存在某个 i 使得 $|\mathcal{F} \cap C_i| \geq 2$, 从而推出 \mathcal{F} 不是独立系统. 这就证明了 Sperner 定理. \square

3.90. 现在开始证明对称链分解引理3.88.

证法 1. 对 n 归纳. $n = 1$ 时, 注意 $C_1 := \{\emptyset, \{1\}\} = 2^{[1]}$ 本身就是对称链, 此时引理平凡地成立. 若 $n = 2$, 取 $C_1 := \{\emptyset, \{1\}, \{1, 2\}\}, C_2 := \{\{2\}\}$, 则 C_1 与 C_2 都是对称链, 且 $2^{[2]} = C_1 \sqcup C_2$.

一般地, 若 $2^{[n]}$ 存在对称链分解 $2^{[n]} = \bigsqcup_{i=1}^m C_i$, 则对每个 $i \in [m]$, 将 $2^{[n]}$ 的对称链 C_i 中的集合按包含关系升序排列为

$$C_i: \quad A_{i,k_i} \subsetneq A_{i,k_i+1} \subsetneq \cdots \subsetneq A_{i,n-k_i},$$

并且定义 $2^{[n+1]}$ 的链 $\mathcal{C}'_i, \mathcal{C}''_i$ 如下:

$$\mathcal{C}'_i: A_{i,k_i+1} \subsetneq A_{i,k_i+2} \subsetneq \cdots \subsetneq A_{i,n-k_i}$$

$$\mathcal{C}''_i: A_{i,k_i} \subsetneq A_{i,k_i} \cup \{n+1\} \subsetneq A_{i,k_i+1} \cup \{n+1\} \subsetneq \cdots \subsetneq A_{i,n-k_i} \cup \{n+1\}.$$

断言 $2^{[n+1]} = \bigsqcup_{i=1}^m (\mathcal{C}'_i \sqcup \mathcal{C}''_i)$ 是 $2^{[n+1]}$ 的对称链分解, 细节留给读者. \square

证法 2. 对于每个 $A \in 2^{[n]}$, 记 χ_A 为由符号 ‘(’ 与 ‘)’ 构成的长度为 n 的字符串:

$$\chi_A := a_1 a_2 \cdots a_n, \quad \text{其中 } a_i = \begin{cases} \text{'('} & \text{如果 } i \in A \\ \text{')'} & \text{如果 } i \notin A \end{cases}.$$

从而 $A \mapsto \chi_A$ 给出了 $2^{[n]}$ 与长度为 n 的括号序列 $\{a_1 a_2 \cdots a_n \mid a_i = \text{'(' 或 ')'}\}$ 之间的一一对应. 例如, 若 $n = 5, A = \{1, 2, 4\}$, 则相应的字符串 $\chi_A = ((()())$.

现在, 考虑对字符串 $\chi_A = a_1 a_2 \cdots a_n$ 的如下操作:

1. 检查是否存在 $i \in [n-1]$, 使得 $a_i = \text{'('}$, 且 $a_{i+1} = \text{')'}$.
2. 若发现满足上述要求的 i , 则将 a_i 与 a_{i+1} 从该字符串中删去, 得到长度为 $n-2$ 的新的字符串.
3. 不断重复前两步操作, 直到不能继续下去.

例如, 若 $\chi_A = \text{'(())(())(())'}$, 则首先将 '(())(())(())' 的红色括号都删去, 得到 '(())(())(())' ; 然后将 '(())(())(())' 中的红色括号删去, 得到 '(())(())(())' , 之后无法再删掉括号, 结束. 显然任何字符串 χ_A 经过此删除操作后, 最终得到的字符串必形如 '(())(())(())' .

对于 $A \in 2^{[n]}$, 令 $D_A := \{i \in [n] \mid \chi_A \text{ 第 } i \text{ 个位置的括号被删除}\}$, 再令 χ'_A 为 χ_A 的所有的被删除的括号按原顺序排成的字符串. 例如:

$$\text{若 } \chi_A = \text{'(())(())(())'}, \text{ 则 } D_A = \{3, 4, 5, 6\}, \chi'_A = \text{'(())'}$$

$$\text{若 } \chi_A = \text{'(())(())(())'}, \text{ 则 } D_A = \{1, 2, 3, 4, 5, 6, 8, 9\}, \chi'_A = \text{'(())(())(())'}$$

其中红色括号是被删除的, 集合 D_A 记录了所有被删除的括号的位置.

对于 $A, B \in 2^{[n]}$, 如果 $D_A = D_B$ 且 $\chi'_A = \chi'_B$, 则称 A 与 B 是“同类型”的. 显然如此定义的“同类型”是 $2^{[n]}$ 上的等价关系. 可以证明, 该等价关系的每个等价类都是对称链 (留给读者练习). 从而得证. \square

3.4 Bollobás 定理

3.91.定理.(Bollobás, 1965) 已知 $2m$ 个有限集合 $A_1, \dots, A_m; B_1, \dots, B_m$ 满足: 对任意 $i, j \in [m]$, $A_i \cap B_j = \emptyset$ 当且仅当 $i = j$, 则成立

$$\sum_{i=1}^m \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1.$$

证明. 记 $X := \bigcup_{i=1}^m (A_i \cup B_i)$, $n := |X|$. 我们对 n 归纳, 如下:

- $n = 1$ 时, 不妨 $A_1 \neq \emptyset$, 此时必有 $A_1 = X$, $B_1 = \emptyset$, $m = 1$. 因此
$$\sum_{i=1}^m \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} = \frac{1}{\binom{1}{1}} = 1.$$
- 假设当 $|X| \leq n-1$ 时命题成立, 则 $|X| = n$ 时, 对于每个 $x \in X$, 记指标集

$$\mathcal{I}_x := \{i \in [m] \mid x \notin A_i\},$$

再记集族

$$\mathcal{F}_x := \{A_i \mid i \in \mathcal{I}_x\} \cup \{B_i \setminus \{x\} \mid i \in \mathcal{I}_x\}.$$

容易验证对任意 $i, j \in \mathcal{I}_x$, $A_i \cap (B_j \setminus \{x\}) = \emptyset$ 当且仅当 $i = j$. 又因为 $x \notin \bigcup \mathcal{F}_x$, 从而 $|\bigcup \mathcal{F}_x| < n$. 对集族 \mathcal{F}_x 使用归纳假设, 可得

$$\sum_{i \in \mathcal{I}_x} \frac{1}{\binom{|A_i|+|B_i \setminus \{x\}|}{|A_i|}} \leq 1, \quad \forall x \in X.$$

将上式两边对 $x \in X$ 求和, 然后交换求和次序可得

$$\begin{aligned} n &\geq \sum_{x \in X} \sum_{i \in \mathcal{I}_x} \frac{1}{\binom{|A_i|+|B_i \setminus \{x\}|}{|A_i|}} = \sum_{i=1}^m \sum_{x \in X \setminus A_i} \frac{1}{\binom{|A_i|+|B_i \setminus \{x\}|}{|A_i|}} \\ &= \sum_{i=1}^m \left(\frac{n - |A_i| - |B_i|}{\binom{|A_i|+|B_i|}{|A_i|}} + \frac{|B_i|}{\binom{|A_i|+|B_i|-1}{|A_i|}} \right) \\ &= n \sum_{i=1}^m \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}}. \end{aligned}$$

从而得证. \square

3.92. Bollobás 定理3.91可直接得到 LYM 不等式3.87, 从而再次证明3.85.

LYM 不等式3.87的另证. 对于独立系统 $\mathcal{F} = \{A_1, \dots, A_m\} \subseteq 2^{[n]}$, 记 $B_i := [n] \setminus A_i$ 为 A_i 的补集, $i \in [m]$. 则容易验证 $\{A_i, B_i\}_{i \in [m]}$ 满足 Bollobás 的题设条件, 之后留给读者. \square

3.5 Erdős-Ko-Rado 定理

除了上一节所研究的独立系统, 我们也对如下“相交系统”感兴趣:

3.93. 定义. 设 n 为正整数, 集族 $\mathcal{F} \subseteq 2^{[n]}$. 如果 \mathcal{F} 中的任何两个元素 A, B 都满足 $A \cap B \neq \emptyset$, 则称 \mathcal{F} 是相交系统.

3.94. 给定正整数 n , 以下是相交系统的两个最典型例子:

1. $\mathcal{F} := \{A \subseteq [n] \mid 1 \in A\}.$

即, 集族 \mathcal{F} 中的所有集合都包含 1. 显然 \mathcal{F} 中的任何两个集合都相交, 从而 \mathcal{F} 是相交系统. 容易验证 $|\mathcal{F}| = 2^{n-1}$.

2. $\mathcal{F} := \left\{A \subseteq [n] \mid |A| > \frac{n}{2}\right\}.$

则由抽屉原理易知 \mathcal{F} 中的任何两个集合都相交, 从而 \mathcal{F} 是相交系统.

容易验证 $|\mathcal{F}| = \begin{cases} 2^{n-1} & n \text{ 为奇数} \\ 2^{n-1} - \frac{1}{2} \binom{n}{n/2} & n \text{ 为偶数} \end{cases}$, 特别地, $|\mathcal{F}| \leq 2^{n-1}$.

与独立系统类似, 自然要问: “最大”的相交系统有多大? 答案很简单:

3.95. 性质. 若 $\mathcal{F} \subseteq 2^{[n]}$ 是相交系统, 则 $|\mathcal{F}| \leq 2^{n-1}$.

证明. 只需注意对任意 $A \in 2^{[n]}$, A 与 $A^c := [n] \setminus A$ 不可能都属于 \mathcal{F} . 再注意 $2^{[n]}$ 可分解为 2^{n-1} 个形如 $\{A, A^c\}$ 的子集的无交并 (换言之, 将 $2^{[n]}$ 中的元素“两两配对”); 如果 $|\mathcal{F}| > 2^{n-1}$, 则由抽屉原理可知, 必然存在某个 $A \in 2^{[n]}$, 使得 $A \in \mathcal{F}$ 且 $A^c \in \mathcal{F}$, 与 \mathcal{F} 是相交系统矛盾. \square

此外, 由3.94中的例子可知 $|\mathcal{F}|$ 可以取到上界 2^{n-1} .

3.96.定理.(Erdős-Ko-Rado, 1961) 设正整数 n, k 满足 $n \geq 2k$, $\mathcal{F} \subseteq \binom{[n]}{k}$ 是相交系统, 则 $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

首先注意条件 $n \geq 2k$, 如果此条件不满足, 即当 $k > \frac{n}{2}$ 时, 由抽屉原理可知 $\mathcal{F} := \binom{[n]}{k}$ 显然是独立系统, 而且显然使得 $|\mathcal{F}|$ 取到最大, 这种情况是平凡的. 再注意, 当 $n \geq 2k$ 时, 定理中的上界 $\binom{n-1}{k-1}$ 也是可以取到的, 例如 $\mathcal{F} := \left\{ A \in \binom{[n]}{k} \mid 1 \in A \right\}$. Erdős-Ko-Rado 定理3.96 (简称 **EKR 定理**) 有多种证明方法, 首先介绍原始证明:

EKR 定理3.96证法 I. (Erdős-Ko-Rado, 1961)

给定相交系统 $\mathcal{F} \subseteq \binom{[n]}{k}$, 对每一组 $1 \leq i < j \leq n$, 定义算子

$$s_{ij}: \mathcal{F} \rightarrow \binom{[n]}{k}$$

如下:

$$s_{ij}(A) := \begin{cases} (A \setminus \{j\}) \sqcup \{i\} & \text{如果 } j \in A, i \notin A, \text{ 并且 } (A \setminus \{j\}) \sqcup \{i\} \notin \mathcal{F}, \\ A & \text{其余情形} \end{cases},$$

称上述定义的算子 s_{ij} 为**压缩算子**. 容易验证压缩算子具有如下基本性质:

- 压缩算子 $s_{ij}: \mathcal{F} \rightarrow \binom{[n]}{k}$ 是单射, 从而 $|s_{ij}(\mathcal{F})| = |\mathcal{F}|$.
- $s_{ij}(\mathcal{F})$ 依然是相交系统.
- 对任意 $A \in \mathcal{F}$, $\sum_{k \in s_{ij}(A)} k \leq \sum_{k \in A} k$, 等号成立当且仅当 $s_{ij}(A) = A$.

上述性质当中, 第 1, 3 条是显然的, 下面验证第 2 条. 对任意 $A, B \in \mathcal{F}$, 只需证明 $s_{ij}(A) \cap s_{ij}(B) \neq \emptyset$. 为此, 分类讨论如下:

1. 如果存在 $k \neq j$ 使得 $k \in A \cap B$, 则易知 $k \in s_{ij}(A) \cap s_{ij}(B)$, 从而 $s_{ij}(A) \cap s_{ij}(B) \neq \emptyset$.
2. 接下来不妨 $A \cap B = \{j\}$. 若 $i \in A \cup B$, 不妨 $i \in A$, 此时 $s_{ij}(A) = A$, 并且无论 $s_{ij}(B)$ 何种情况, $s_{ij}(A) \cap s_{ij}(B)$ 必含有 i 或 j , 从而非空.
3. 最后, 不妨 $A \cap B = \{j\}$ 且 $i \notin A \cup B$. 此时必有 $s_{ij}(A) \neq A, s_{ij}(B) \neq B$, 从而 $s_{ij}(A) \cap s_{ij}(B) = \{i\} \neq \emptyset$. 这是因为, 如果 $s_{ij}(A) = A$, 则由压缩算子的定义可知 $A' := (A \setminus \{j\}) \sqcup \{i\} \in \mathcal{F}$, 但另一方面, 易知 $A' \cap B = \emptyset$, 与 \mathcal{F} 是相交系统矛盾.

如果对任意 $1 \leq i < j \leq n$, 都成立 $s_{ij}(\mathcal{F}) = \mathcal{F}$, 则称集族 \mathcal{F} 是不可压缩的.

现在开始证明 EKR 定理 3.96. 由压缩算子的性质, 总可以不妨假设集族 $\mathcal{F} \subseteq \binom{[n]}{k}$ 不可压缩. 现在固定正整数 k , 我们对 n 归纳.

1. 起始步: $n = 2k$. 此时注意对任意 $A \in \mathcal{F} \subseteq \binom{[n]}{k}$, 补集 $A^c := [n] \setminus A \notin \mathcal{F}$, 这表明

$$|\mathcal{F}| \leq \frac{1}{2} \binom{n}{k} = \frac{1}{2} \binom{2k}{k} = \binom{2k-1}{k-1} = \binom{n-1}{k-1},$$

得证.

2. 如果 $n > 2k$, 此时记

$$\begin{aligned} \mathcal{F}_1 &:= \{A \in \mathcal{F} \mid n \notin A\} \subseteq \binom{[n-1]}{k} \\ \mathcal{F}_2 &:= \{A \in \mathcal{F} \mid n \in A\}, \end{aligned}$$

则 $\mathcal{F} = \mathcal{F}_1 \sqcup \mathcal{F}_2$, 并且 $\mathcal{F}'_2 := \{A \setminus \{n\} \mid A \in \mathcal{F}_2\} \subseteq \binom{[n-1]}{k-1}$. 断言: \mathcal{F}'_2 是相交系统. 若不然, 则存在 $A, B \in \mathcal{F}$ 使得 $A \cap B = \{n\}$. 注意

$$|A \cup B| = |A| + |B| - |A \cap B| = 2k - 1 < n,$$

从而存在 $i \in [n] \setminus (A \cup B)$. 注意我们总假设集族 \mathcal{F} 不可压缩, 从而 $s_{in}(A) = A$, 这迫使 $A' := (A \setminus \{n\}) \sqcup \{i\} \in \mathcal{F}$. 而容易验证 $A' \cap B = \emptyset$, 这与 \mathcal{F} 是相交系统矛盾, 断言得证. 于是由归纳假设,

$$|\mathcal{F}| = |\mathcal{F}_1| + |\mathcal{F}_2| = |\mathcal{F}_1| + |\mathcal{F}'_2| \leq \binom{n-2}{k-1} + \binom{n-2}{k-2} = \binom{n-1}{k-1}.$$

综上, 定理得证. □

3.97. 接下来介绍的第二种证法用到了“算两次”的技巧, 这是当前人类普遍认为的最简洁优雅证明.

EKR 定理**3.96**证法 2. (Katona, 1972)

考虑加法群 $\mathbb{Z}/n\mathbb{Z}$, 记集合

$$\mathcal{M} := \{f: \mathbb{Z}/n\mathbb{Z} \rightarrow [n] \mid f \text{ 是一一映射}\},$$

则 $|\mathcal{M}| = n!$. 对于 $f \in \mathcal{M}$ 以及 $A \in \mathcal{F}$, 如果存在 $i_0 \in \mathbb{Z}/n\mathbb{Z}$ 使得

$$A = \{f(i_0), f(i_0 + 1), \dots, f(i_0 + k - 1)\},$$

则记 $A \triangleleft f$. 考察集合

$$X := \{(A, f) \in \mathcal{F} \times \mathcal{M} \mid A \triangleleft f\}.$$

一方面, 注意 \mathcal{F} 中的任何两个集合都相交, 从而

$$|X| = \sum_{f \in \mathcal{M}} \#\{A \in \mathcal{F} \mid A \triangleleft f\} \leq \sum_{f \in \mathcal{M}} k = kn!.$$

另一方面, 易知

$$|X| = \sum_{A \in \mathcal{F}} \#\{f \in \mathcal{M} \mid A \triangleleft f\} = \sum_{A \in \mathcal{F}} nk!(n-k)! = nk!(n-k)!|\mathcal{F}|,$$

所以 $|\mathcal{F}| \leq \frac{kn!}{nk!(n-k)!} = \binom{n-1}{k-1}$, 定理得证. □

我们还将后文介绍 Erdős-Ko-Rado 定理的一个推广, 详见**5.159**.

3.98.段子. Erdős-Ko-Rado 定理之中的“Ko”是指中国数学家柯召.

柯召 (1910.4.12-2002.11.8), 字惠棠, 浙江温岭人, 数学家, 中国科学院院士, 被称为中国近代数论的创始人, 二次型研究的开拓者. 1933 年毕业于清华大学, 1937 年获英国曼彻斯特大学博士学位, 1950 年加入九三学社, 1955 年当选为中国科学院院士.

柯召主要从事数论, 组合论和代数的研究. 数论方面, 在表二次型为线性型平方和的研究上取得一系列重要成果; 不定方程方面, 突破了 100 多年来未能解决的 Catalan 猜想的二次“幂”情形, 获一系列重要结果, 被国际上誉为“柯氏定理”, 所创造的方法至今仍被广泛引用; 组合论方面, 他和 Erdős, Rado 一起给出了组合论中著名的 Erdős-Ko-Rado 定理, 这个定理已成为组合数学中的一个经典结果, 开辟了极值集论迅速发展的道路.

3.6 Schur 引理与 \mathbb{F}_p 上的费马大定理

3.99. 数学家 Pierre de Fermat 于 1637 年提出如下著名猜想: 若正整数 $k \geq 3$, 则方程 $x^k + y^k = z^k$ 不存在非平凡整数解, 换言之, 该方程的整数解只可能是 $(x, y, z) = (0, 0, 0)$. 这个问题吸引了无数数学家, 然而直到 1995 年才被数学家 Andrew Wiles 证明. 这正是众所周知的费马大定理. 虽说 $x^k + y^k = z^k$ 在 \mathbb{Z} 中不存在 (非平凡) 解, 然而本节将证明, 对于任意充分大的素数 p , 此方程在有限域 \mathbb{F}_p 中一定存在 (非平凡) 解.

3.100. 引理. (Issai Schur, 1916) 给定正整数 $k \geq 2$. 证明: 存在 (与 k 有关的) 整数 $N = N(k)$, 使得对任何映射 $\varphi: [N] \rightarrow [k]$, 必存在 $x, y, z \in [N]$, 使得

$$\varphi(x) = \varphi(y) = \varphi(z) \quad \text{并且} \quad x + y = z.$$

证明. 假设正整数 N 不满足题设, 我们将证明 $N < ek!$, 从而推出任何大于 $[ek!]$ 的整数 N 都满足题设. 现在取定 $\varphi: [N] \rightarrow [k]$.

- 取 $c_1 \in [k]$, 使得 $|\varphi^{-1}(c_1)| = \max_{c \in [k]} |\varphi^{-1}(c)|$. 记 $A_1 := \varphi^{-1}(c_1) \subseteq [N]$, $n_1 := |A_1|$. 由 c_1 的定义可知 $kn_1 \geq N$.
- 将 A_1 中的全部元素记为 $x_1^{(1)} < x_2^{(1)} < \cdots < x_{n_1}^{(1)}$. 记集合

$$B_1 := \left\{ x_i^{(1)} - x_1^{(1)} \mid 2 \leq i \leq n_1 \right\}.$$

则 $|B_1| = n_1 - 1$. 注意 N 不满足题设, 由此容易推出 $B_1 \cap A_1 = \emptyset$, 从而 $\varphi(B_1) \subseteq [k] \setminus \{c_1\}$. 记 $\varphi_1 := \varphi|_{B_1}$ 为映射 φ 在子集 B_1 上的限制. 取 $c_2 \in [k] \setminus \{c_1\}$, 使得 $|\varphi_1^{-1}(c_2)| = \max_{c \in [k] \setminus \{c_1\}} |\varphi_1^{-1}(c)|$, 记 $A_2 := \varphi_1^{-1}(c_2)$, $n_2 := |A_2|$. 则由 c_2 的定义可知 $(k-1)n_2 \geq |B_1| = n_1 - 1$.

- 将 A_2 中的全部元素记为 $x_1^{(2)} < x_2^{(2)} < \cdots < x_{n_2}^{(2)}$. 记集合

$$B_2 := \left\{ x_i^{(2)} - x_1^{(2)} \mid 2 \leq i \leq n_2 \right\}.$$

则 $|B_2| = n_2 - 1$. 注意 N 不满足题设, 由此容易推出 $B_2 \cap (A_1 \sqcup A_2) = \emptyset$, 从而 $\varphi_1(B_2) \subseteq [k] \setminus \{c_1, c_2\}$. 记 $\varphi_2 := \varphi|_{B_2}$ 为映射 φ 在子集 B_2 上的限制. 取 $c_3 \in [k] \setminus \{c_1, c_2\}$, 使得 $|\varphi_2^{-1}(c_3)| = \max_{c \in [k] \setminus \{c_1, c_2\}} |\varphi_2^{-1}(c)|$, 记 $A_3 := \varphi_2^{-1}(c_3)$, $n_3 := |A_3|$. 则由 c_3 的定义可知 $(k-2)n_3 \geq |B_2| = n_2 - 1$.

不断重复以上步骤, 得到 $[k]$ 中元素的排列 c_1, c_2, \dots, c_k , 以及 $[N]$ 的 k 个两两不交的子集 A_1, A_2, \dots, A_k , 使得它们关于 φ 的像集 $\varphi(A_i) = \{c_i\}$; 并且, $n_i := |A_i|$ 满足 $N \leq kn_1$, $(k-i)n_{i+1} \geq n_i - 1, \forall i \geq 1$, 此外特别注意 $n_k = 1$. 因此,

$$\begin{aligned} N &\leq kn_1 \leq k((k-1)n_2 + 1) = k + k(k-1)n_2 \\ &\leq k + k(k-1) + k(k-1)(k-2)n_3 \\ &\leq \dots \\ &\leq k + k(k-1) + k(k-1)(k-2) + \dots + k!n_k \\ &= \sum_{i=0}^{k-1} \frac{k!}{i!} \leq k! \sum_{i=0}^{\infty} \frac{1}{i!} = ek!. \end{aligned}$$

从而证毕. □

利用 Ramsey 理论可以得到上述引理的另一证明, 详见 7.192.

3.101. 定理. 对任意正整数 k , 存在 N , 使得对任意素数 $p \geq N$, 关于 x, y, z 的方程

$$x^k + y^k = z^k$$

在有限域 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ 内有非平凡解 (即 $(x, y, z) = (0, 0, 0)$ 之外的解).

证明. 给定正整数 N , 对于任意素数 $p \geq N$, 众所周知乘法群 $\mathbb{F}_p^\times := \mathbb{F}_p \setminus \{0\}$ 是循环群, 取其生成元 $g \in \mathbb{F}_p^\times$, 于是 \mathbb{F}_p^\times 中的任何元素 a 都可唯一表示成 $a = g^d = g^{ik+j}$, 使得 $0 \leq j \leq k-1$. 定义映射 $\varphi: [p-1] \cong \mathbb{F}_p^\times \rightarrow [k]$ 如下:

$$\varphi: a = g^{ik+j} \mapsto j+1.$$

由引理 3.100 可知, 当 N 充分大时, 必存在 $a, b, c \in [p-1]$ 使得 $\varphi(a) = \varphi(b) = \varphi(c)$ 并且 $a + b = c$. 由 $\varphi(a) = \varphi(b) = \varphi(c)$ 可知 a, b, c 必形如

$$\begin{cases} a \equiv g^{i_1 k + j} \pmod{p} \\ b \equiv g^{i_2 k + j} \pmod{p} \\ c \equiv g^{i_3 k + j} \pmod{p} \end{cases},$$

因此在 \mathbb{F}_p 中成立 $g^{i_1 k + j} + g^{i_2 k + j} = g^{i_3 k + j}$, 于是 $(x, y, z) := (g^{i_1}, g^{i_2}, g^{i_3})$ 满足要求. □

4. 图论初步

4.1 图的基本概念

4.102.定义. 所谓图, 是指二元组 $G = (V, E)$, 其中 V 是有限集, $E \subseteq \binom{V}{2}$.

对于图 $G = (V, E)$,

- 集合 V 称为 G 的**顶点集**, V 中的元素称为图 G 的**顶点**.
- 集合 E 称为图 G 的**边集**, E 中的元素称为图 G 的**边**.
- 对于顶点 v_1, v_2 , 如果 $\{v_1, v_2\} \in E$, 则称顶点 v_1, v_2 **相邻**(或者“有边相连”), 记作 $v_1 \sim_E v_2$ 或者 $v_1 \sim_G v_2$, 在特定语境下也常常简记为 $v_1 \sim v_2$ 或者 $v_1 v_2 \in E$.
- $v(G) := |V|$, 称为图 G 的**顶点数**, $e(G) := |E|$ 称为图 G 的**边数**.
- 对于 $v \in V$, 记 $N_G(v) := \{v' \in V \mid v \sim_E v'\}$, 即与 v 相邻的顶点之全体, 称为顶点 v 的**邻居集**; 记 $d_G(v) := |N_G(v)|$, 称为顶点 v 的**度数**.

4.103.引理.(握手引理). 对于图 $G = (V, E)$, 则

1. G 的所有顶点的度数之和是边数的 2 倍, 从而必为偶数.
2. G 的度数为奇数的顶点有偶数个.
3. 若 G 存在度数为奇数的顶点, 则 G 至少还会存在另一个度数为奇数的顶点.

证明. 只证 (1), 而 (2)(3) 是 (1) 的显然推论. 考虑集合

$$S := \{(v, e) \in V \times E \mid v \in e\},$$

对 $|S|$ 算两次, 分别有

$$|S| = \sum_{v \in V} \#\{e \in E \mid v \in e\} = \sum_{v \in V} d_G(v)$$

$$|S| = \sum_{e \in E} \# \{v \in V \mid v \in e\} = \sum_{e \in E} 2 = 2e(G),$$

从而 $\sum_{v \in V} d_G(v) = 2e(G)$, 得证. \square

这个引理的证明是“算两次”方法3.75最经典的应用之一.

4.104. 习题. 若图 G 的顶点数 ≥ 2 , 则图 G 必有两个顶点的度数相同.

证明. 设 G 的顶点个数为 n . 显然 G 的每个顶点的度数只可能为 $0, 1, 2, \dots, n-1$ 这 n 种可能的情况, 从而函数 $d_G: V \rightarrow \{0, 1, 2, \dots, n-1\}$ 是从 n 元集合到 n 元集合的映射, 因此 d_G 为单射当且仅当 d_G 为满射. 如果 d_G 为满射, 则存在顶点 $v_1, v_2 \in V$ 使得 $d_G(v_1) = 0, d_G(v_2) = n-1$. $d_G(v_1) = 0$ 表明 v_1 与其余所有顶点都不相邻, 特别地有 $v_1 \not\sim v_2$; 而 $d_G(v_2) = n-1$ 表明 v_2 与其余所有顶点都相邻, 特别地有 $v_1 \sim v_2$, 这产生矛盾. 因此 d_G 不是满射, 从而不是单射. 换言之, G 必存在度数相同的两个顶点. \square

4.105. 习题. 对于图 $G = (V, E)$, 记 $d_{\text{avg}} := \frac{2e(G)}{v(G)}$ 为所有顶点的平均度数; 对于顶点 $v \in V$, 记 $r(v) := \sum_{v' \in N_G(v)} d_G(v')$ 为顶点 v 的所有邻居的度数之和.

证明: 存在顶点 $v \in V$, 使得 $r(v) \geq d_{\text{avg}} d_G(v)$.

证明. 如果对任意 $v \in V$ 都有 $r(v) < d_{\text{avg}} d_G(v)$, 那么

$$\sum_{v \in V} r(v) < d_{\text{avg}} \sum_{v \in V} d_G(v) = 2e(G) d_{\text{avg}} = \frac{4e(G)^2}{v(G)};$$

另一方面, 由 Cauchy-Schwartz 不等式可得

$$\begin{aligned} \sum_{v \in V} r(v) &= \sum_{v \in V} \sum_{w \in N_G(v)} d_G(w) = \sum_{w \in V} \sum_{v \in N_G(w)} d_G(w) \\ &= \sum_{w \in V} d_G(w)^2 \geq \frac{1}{v(G)} \left(\sum_{w \in V} d_G(w) \right)^2 = \frac{4e(G)^2}{v(G)}, \end{aligned}$$

这产生矛盾. 从而得证. \square

4.106. 定义.(图范畴). 对于图 $G = (V, E)$ 与 $G' = (V', E')$,

1. 映射 $f: V \rightarrow V'$ 称为 G 与 G' 的**同态**, 如果任意 $u, v \in V$,

$$u \sim_E v \implies [f(u) = f(v) \text{ 或 } f(u) \sim_{E'} f(v)].$$

图的同态也常常简记为 $f: G \rightarrow G'$.

2. 对于图同态 $f: G \rightarrow G'$, 如果 f 是从 V 到 V' 的一一映射, 并且逆映射 $f^{-1}: V' \rightarrow V$ 是 G' 到 G 的同态, 则称 f 是图 G 与 G' 的**同构**; 此时也称图 G 同构于 G' , 记作 $G \cong G'$.

我们往往把同构的图视为相同的图.

4.107. 我们来考察图的一些抽象例子.

1. 设 $G = (V, E)$ 为图, 则对任意 $V' \subseteq V, E' \subseteq \binom{V'}{2} \cap E$, 二元组 $G' := (V', E')$ 也是图. 这样的图称为 G 的**子图**.
2. 设 $G = (V, E)$ 为图, 对任意 $V' \subseteq V$, 令 $E' := \binom{V'}{2} \cap E$, 称 $G|_{V'} := (V', E')$ 是 G 在 V' 上的**限制子图**.
3. 对于 $G = (V, E)$, 令 $E^c := \binom{V}{2} \setminus E$, 称 $G^c := (V, E^c)$ 是 G 的**补图**.
4. 对于图 $G = (V, E)$ 与 $G' = (V', E')$. 如果 G 的任何子图都不同构于 G' , 则称图 G **不含有** G' ; 否则称 G **含有** G' .

4.108. 以下是一些具体例子:

1. $I_n := ([n], \emptyset)$ 称为 n 阶**独立图**. 即, I_n 的顶点集为 $[n]$, 边集为 \emptyset .

2. $K_n := I_n^c$ 称为 n 阶**完全图**.

换言之, $K_n := ([n], \binom{[n]}{2})$, 其任何两个不同顶点都相邻.

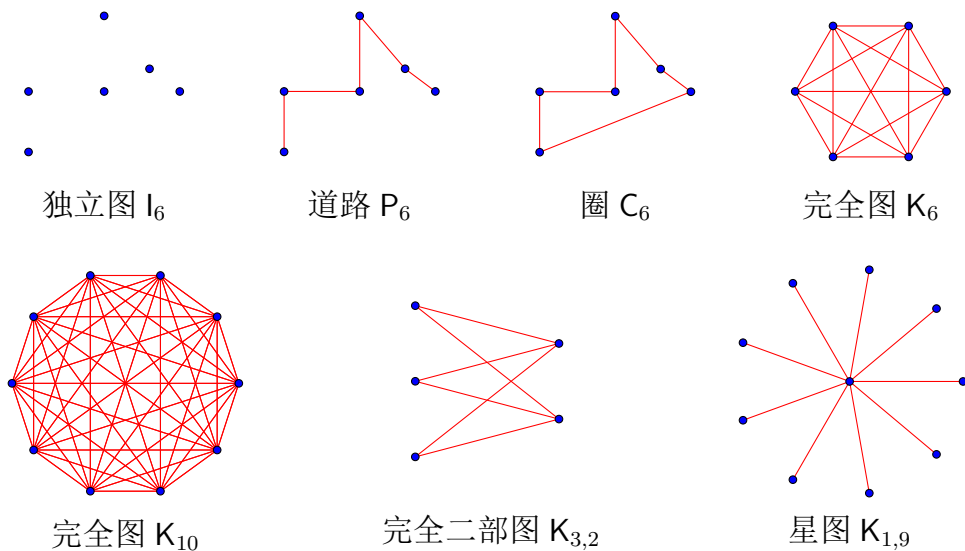
3. $P_n := ([n], \{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}\})$ 称为长度为 $(n-1)$ 的**道路**.

注意 P_n 有 n 个顶点, $(n-1)$ 条边.

4. $C_n := ([n], \{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}, \{n, 1\}\})$ 称为长度为 n 的**圈**.

5. 对于图 $G = (V, E)$, 如果存在 V 的划分 $V = V_1 \sqcup V_2$, 使得 V_i 中的任何两点都不相邻 ($i = 1, 2$), 则称 G 是**二部图**.
6. 对于二部图 $G = (V_1 \sqcup V_2, E)$, 如果边集 $E = \{\{v_1, v_2\} \mid v_1 \in V_1, v_2 \in V_2\}$, 则称 G 是**完全二部图**. 记 $|V_1| = m, |V_2| = n$, 把相应的完全二部图记为 $K_{m,n}$. 特别地, 同构于 $K_{1,n}$ 的图称为**星图**.

图 $G = (V, E)$ 可用如下众所周知的方式直观展示, 例如:



4.109.定义. 设 V' 是图 $G = (V, E)$ 的顶点集 V 的子集. 如果限制子图 $G|_{V'}$ 同构于独立图 (换言之, V' 中的任何两点都不相邻), 则称 V' 是图 G 的**独立集**.

- 图 G 的独立集的顶点个数的最大值记作 $\alpha(G)$, 即,

$$\alpha(G) := \max_{V' \text{ 是 } G \text{ 的独立集}} |V'|.$$

上述 $\alpha(G)$ 称为图 G 的**独立数**.

例如, 我们可用图论的语言重新表述 Sperner 定理**3.85**. 给定正整数 n , 记 $V := 2^{[n]}$, $E := \{\{A, B\} \mid A, B \in V, A \subseteq B \text{ 或 } B \subseteq A\}$, 则 $G := (V, E)$ 构成图. 换言之, 将 $[n]$ 的每个子集都视为一个顶点, 两个顶点相邻当且仅

当相应的集合具有包含关系. 于是, 集族 $\mathcal{F} \subseteq 2^{[n]} = V$ 是**独立系统** (见定义3.84) 当且仅当 \mathcal{F} 是图 G 的独立集. 从而 Sperner 定理断言, 对于上述图 G , $\alpha(G) = \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

4.110.例题. 验证图的同构: $C_4 \cong K_{2,2}$.

证明. 留给读者. □

4.111.定义. 对于图 $G = (V, E)$ 以及正整数 n , 图 G 的 **n -点染色**是指映射 $\varphi: V \rightarrow [n]$. 若 $\varphi(v) = i \in [n]$, 则称顶点 v “被染上第 i 种颜色”.

- 若 n -点染色 $\varphi: V \rightarrow [n]$ 满足性质: “任何相邻两顶点的颜色不相同”, 则称该染色与边集 E **相容**.
- 对于图 $G = (V, E)$, 记

$$\chi(G) := \min \{n \mid \text{存在与边集 } E \text{ 相容的 } n\text{-点染色}\},$$

称为图 G 的**染色数**.

容易验证独立数 $\alpha(G)$ 与染色数 $\chi(G)$ 满足如下关系:

4.112.性质. 对任意图 $G = (V, E)$, 成立 $\chi(G) \cdot \alpha(G) \geq |V|$.

证明. 若 $\chi(G) = m$, 则存在与边集 E 相容的 m -点染色 $\varphi: V \rightarrow [m]$. 则对任意 $i \in [m]$, 由有关定义可知 $\varphi^{-1}(\{i\}) \subseteq V$ 是 G 的独立子集, 从而 $|\varphi^{-1}(\{i\})| \leq \alpha(G)$. 再注意 $V = \bigsqcup_{i \in [m]} \varphi^{-1}(\{i\})$, 因此

$$|V| = \sum_{i=1}^m |\varphi^{-1}(\{i\})| \leq \sum_{i=1}^m \alpha(G) = \chi(G) \cdot \alpha(G).$$

□

4.113.段子. 关于染色数 $\chi(G)$, 首先我们知道

$$\chi(K_n) = n, \quad \chi(I_n) = 1,$$

而对于一般的图 $G = (V, E)$, 计算其染色数是非常困难的问题 (涉及 “P=NP”)

4.2 树, 平面图与 Euler 公式

图 $G(V, E)$ 有众所周知的几何直观, 即把“顶点”与“边”按字面意思理解. 回忆拓扑学里众所周知的 **CW 复形** (也叫**胞腔复形**) 的概念 (不熟悉拓扑学的读者可以选择性跳过有关内容, 而用最直观朴素的方式理解.), 我们用最自然的方式将图 $G = (V, E)$ 视为 1 维 CW 复形.

4.114. 定义. 对于图 $G = (V, E)$, 定义 1 维 CW 复形 X_G 如下:

1. 将顶点集 V 视为离散拓扑空间.
2. 对于每条边 $\{u, v\} \in E$, 取一个 1 维胞腔 (即同胚于 $[0, 1]$ 的拓扑空间), 将 $u, v \in V$ 分别粘接到此胞腔的两个端点.

上述操作所构造的 1 维 CW 复形记作 X_G . 特别地, X_G 是拓扑空间.

例如, 对于 $n \geq 2$, 道路 P_n 所对应的 CW 复形 X_{P_n} 拓扑同胚于 1 维闭圆盘 $\mathbb{D}^1 \cong [0, 1]$. 再比如, 对于 $n \geq 3$, 圈 C_n 的 CW 复形 X_{C_n} 拓扑同胚于圆周 S^1 .

4.115. 性质. (函子性). 给定图 $G = (V, E)$ 与 $G' = (V', E')$, 则图同态 $f: G \rightarrow G'$ 自然诱导拓扑空间的连续映射 $X_f: X_G \rightarrow X_{G'}$, 使得

1. 对于恒等同态 $\text{id}: G \rightarrow G$, 则 $X_{\text{id}} = \text{id}: X_G \rightarrow X_G$.
2. 对任意 $f: G \rightarrow G', g: G' \rightarrow G''$, 成立 $X_{g \circ f} = X_g \circ X_f$.

证明. 都是显然的废话, 留给读者验证, 或者选择无视. □

4.116. 定义. 对于图 $G = (V, E)$,

1. 如果 X_G 是连通的拓扑空间, 则称图 G 是**连通图**.
2. 如果拓扑空间 X_G 与 $X_{G'}$ 同胚, 则称图 G 与 G' **同胚**.

上述概念也可以不借助拓扑空间的语言, 而完全用图论 (集合论) 语言来等价表述. 容易验证, 对于图 G, G' ,

1. 图 $G = (V, E)$ 是连通图, 当且仅当对于 G 的任何两个不同顶点 u, v , 存在一系列顶点 v_1, v_2, \dots, v_m , 使得 $u \sim_E v_1, v_1 \sim_E v_2, \dots, v_{m-1} \sim_E v_m, v_m \sim_E v$.

2. 对于图 $G = (V, E)$, 考虑如下两种类型的基本操作:

- 取定一条边 $e = \{u, v\} \in E$. 将边 e 从 E 中删除. 在 V 中增加一个新的顶点 x . 在 E 中增加两条边 $\{u, x\}, \{v, x\}$.
- 若 $v \in V$ 的度数为 2, 并且 v 的两个邻居不相邻, 则连接 v 的两个邻居, 并删除顶点 v 以及以 v 为端点的边.

那么, 图 G 同胚于 G' , 当且仅当 G 能够经过有限步上述基本操作变为 G' .

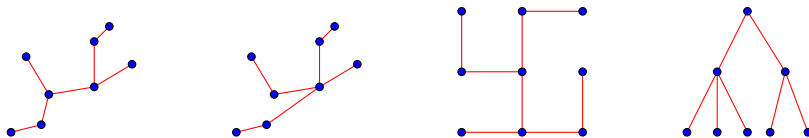
与拓扑学类似, 有了连通性的概念之后自然可以谈论图的**连通分支**. 同构的图必然同胚, 反之则不然.

4.117. 习题. 若图 G 有 n 个顶点, 且每个顶点的度数都 $\geq \frac{n-1}{2}$, 则 G 是连通图.

证明. 设 u, v 是 $G = (V, E)$ 中的任何两个顶点, 如果 u, v 不相邻, 则考虑它们的邻交集 $N_G(u), N_G(v)$ 都是 $V \setminus \{u, v\}$ 的子集. 断言 $N_G(u) \cap N_G(v)$ 非空, 否则 $n - 2 = |V \setminus \{u, v\}| \geq |N_G(u)| + |N_G(v)| \geq \frac{n-1}{2} + \frac{n-1}{2} = n - 1$, 矛盾. 这表明 u, v 至少有一个公共邻居, 从而存在从 u 到 v 的长度为 2 的路径. 因此 G 连通. \square

4.118. 定义. 连通且不含有圈的图称为**树**.

这里的“不含有圈”是指它的任何子图都不同构于 C_k ($\forall k \geq 3$). 例如, 容易验证 $P_n, K_{1,n}$ 都是树. 再比如, 以下也都是树:



4.119. 性质.(树的基本性质). 设 $G = (V, E)$ 是树, 则

1. G 的任何两个顶点都存在唯一道路相连.
2. 若 $|V| \geq 2$, 则 G 必存在度数为 1 的顶点. (树中的度数为 1 的顶点称为 **树叶**).
3. 若 $v \in V$ 是树叶, 则限制子图 $G|_{V \setminus \{v\}}$ 也是树. (“摘树叶”)
4. $|V| = |E| + 1$.

证明. (1). 只证连接两顶点 u, u' 的道路的唯一性. 如果 u, v_1, \dots, v_k, u' 与 $u, w_1, \dots, w_\ell, u'$ 是连接 u, u' 的两条不同道路, 则考虑如下两种情况: 如果存在 i, j 使得 $v_i = w_j$, 则 $u, v_1, \dots, (v_i = w_j), w_{j-1}, \dots, w_1, u$ 是圈, 与 G 不含圈矛盾; 否则 $u, v_1, \dots, v_k, u', w_\ell, \dots, w_1, u$ 是圈, 与 G 不含圈矛盾.

(2) 对顶点数 $|V|$ 归纳, $|V| = 2$ 时显然. 一般地, 任取 $v \in V$, 如果 $d_G(v) > 1$, 考虑删掉顶点 v 之后所得的图 $G' := G|_{V \setminus \{v\}}$, 则 G' 显然也不含有圈, 并且 G' 不连通 (留给读者证明). 任取 G' 的连通分支 G_1 , 则 G_1 也是树, 且其顶点数小于 $|V|$. 如果 G_1 只有一个顶点, 则结束; 否则由归纳假设, 取 $v_1 \in G_1$ 使得 $d_{G_1}(v_1) = 1$. 如果 $v_1 \not\sim_E v$, 则易知 $d_G(v_1) = 1$, 命题得证; 而如果 $v_1 \sim_E v$, 则令 G_2 为 G_1 删去顶点 v_1 所得的图, 易知 G_2 也是树. 若 G_2 只有一个顶点, 则结束, 否则取 $v_2 \in G_2$ 使得 $d_{G_2}(v_2) = 1$, 然后讨论 v_2 是否与 v_1 相邻. 不断重复以上操作, 上述操作显然在有限步之内停止, 从而得到度数为 1 的顶点.

(3) 显然. 至于 (4), 只需对顶点个数 $|V|$ 归纳. 对于树 $G = (V, E)$, 任取树叶 $v \in V$, 记 G 删去顶点 v 所得的树为 G' , 则 G' 的顶点数与边数都比 G 少 1. 从而“摘树叶”操作不改变 $|V| - |E|$ 的值. 不断“摘树叶”即可证明. \square

4.120.定理.(树的等价定义). 对于图 $G = (V, E)$, 以下等价:

1. G 是树 (即, 连通且不含圈);
2. G 是极小连通图 (即, G 连通, 并且去掉任何一条边后不再连通);
3. G 是极大无圈图 (即, G 不含圈, 但添加任何一条边之后就含有圈);
4. G 连通且 $|V| = |E| + 1$,

5. G 不含圈且 $|V| = |E| + 1$.

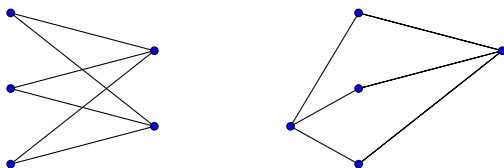
证明. 留给读者练习. □

4.121. 定义. 对于图 $G = (V, E)$ 如果相应的拓扑空间 X_G 能够嵌入欧氏平面 \mathbb{R}^2 , 则称图 G 是 **平面图**.

粗俗地讲, $G = (V, E)$ 是平面图当且仅当存在两两互异的点 $X_v \in \mathbb{R}^2$, $v \in V$, 使得对任意 $e = \{u, v\} \in E$, 存在 \mathbb{R}^2 的连接 X_u 与 X_v 的连续曲线段, 使得所有这些曲线段 (去除两个端点) 互不相交.



例如, 完全图 K_4 是平面图. 尽管上图左边看似有两条边相交, 但是只需要将右上角的顶点适当地向左下角移动, 就能避免边的相交 (得到上图右边). 再比如, 完全二部图 $K_{2,3}$ 是平面图, 尽管下图左边看起来有边相交, 但我们可以用另一种方式 (下图右边) 在平面上画出 $K_{2,3}$, 使得任何两条边 (端点除外) 都不相交. 此外, I_n, P_n, C_n 显然都是平面图.



4.122. 性质. 设 $G = (V, E)$ 是平面图, 则

1. 任取 $w \notin V, v \in V$, 记 $V' := V \sqcup \{w\}$, $E' := E \cup \{\{v, w\}\}$, 则 (V', E') 也是平面图.
2. 树是平面图.

证明. (1) 在直观上看是显然的, 证明细节从略. 至于 (2), 考虑不断摘去树叶, 利用 (1) 对顶点个数归纳即可. □

4.123.定理.(平面图的 Euler 公式). 设 $G = (V, E)$ 是连通的平面图, 取定平面嵌入 $\varphi: X_G \rightarrow \mathbb{R}^2$, 记 $|F| := \mathbb{R}^2 \setminus X_G$ 的连通分支个数, 称为平面图 G 的**面数**. 那么, $|F|$ 与嵌入映射 φ 的选取无关, 并且满足如下公式:

$$|F| + |V| - |E| = 2,$$

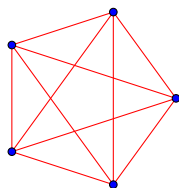
其中 $|V|, |E|$ 分别是图 G 的顶点数与边数.

证明概要. 设 $G = (V, E)$ 为平面图, 则将 X_G 视为 \mathbb{R}^2 的子集. 如果 G 含有圈, 记 $v_0v_1\dots v_kv_0$ 是 G 中的圈, 则删去边 v_0v_1 . 删去边之后所得的图记为 G' , 易知 G' 仍然为连通图. 注意 G' 的顶点数与原来相同, 边数与面数都比原来减少 1, 从而上述操作不改变 $|F| + |V| - |E|$ 的值. 不断进行上述的删除边的操作, 直到不能进行, 最终得到连通无圈图, 即树. 故只需证明 G 是树的情形.

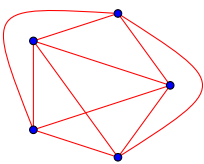
现在设 $G = (V, E)$ 是树, 考虑不断删除 G 的树叶. 删除树叶的操作会使顶点数与边数减 1 而不改变面数, 从而不改变 $|F| + |V| - |E|$. 最终只需证明 $G \cong I_1$ (只有一个顶点的独立图) 的情形. 此时 $|F| = |V| = 1, |E| = 0$, 从而 $|F| + |V| - |E| = 2$. □

4.124.推论. 完全图 K_5 与完全二部图 $K_{3,3}$ 都不是平面图.

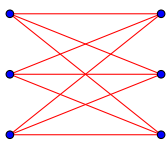
证明之前, 不妨先尝试在平面上画出这两个图.



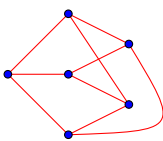
完全图 K_5



完全图 K_5



完全二部图 $K_{3,3}$



完全二部图 $K_{3,3}$

会发现, 无论如何尝试 (比如上图右边), 总会有相交的边.

证明. 先证明 K_5 不是平面图. 反证法, 如果 K_5 是平面图, 则将 X_{K_5} 嵌入 \mathbb{R}^2 , 记 F 为 $\mathbb{R}^2 \setminus X_{K_5}$ 的所有连通分支 (即“面”) 构成的集合. 则由欧拉公式可知 $|F| = 2 + |E| - |V| = 2 + 10 - 5 = 7$. 考虑集合

$$\Phi := \{(e, f) \in E \times F \mid e \text{ 是 } f \text{ 的一条边界}\}.$$

对 $|\Phi|$ 算两次, 注意每个面至少由 3 条边围成, 而每条边恰好是 2 个面的公共边, 从而

$$\begin{aligned} |\Phi| &= \sum_{e \in E} 2 = 20 \\ |\Phi| &\geq \sum_{f \in F} 3 = 21, \end{aligned}$$

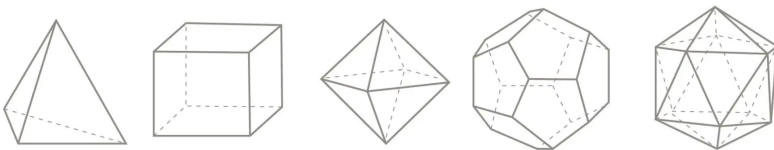
产生矛盾. 至于 $K_{3,3}$, 注意 $K_{3,3}$ 不含有 C_3 , 因此如果 $K_{3,3}$ 是平面图, 那么它的每一个面都被至少被 4 条边围成. 然后方法类似, 留给读者. \square

4.125. 定理. (Kuratowski). 对于图 $G = (V, E)$, G 是平面图当且仅当 G 不含有同胚于 K_5 或 $K_{3,3}$ 的子图.

证明. “仅当”是显然的; 而“当”比较困难, 这里从略, 仅供读者了解. \square

4.126. 平面图 Euler 公式 4.123 的一个重要应用是分类三维欧氏空间 \mathbb{R}^3 中的正多面体. 众所周知, \mathbb{R}^3 中的多面体是指被有限多个平面所围成的区域. 多面体的表面, 棱, 顶点按照众所周知的直观方式来定义. 多面体 P 称为凸多面体, 如果连接 P 中任何两点的线段都位于 P 中. 凸多面体称为正多面体, 如果该多面体的所有表面都是全等的正多边形, 并且任何两个相邻的表面的二面夹角相等.

4.127. 定理. 三维欧氏空间中的正多面体只有五种: 正 4 面体, 正 6 面体, 正 8 面体, 正 12 面体, 正 20 面体. (如下图所示)



证明. 给定正多面体 P , 即 V 为多面体 P 的所有顶点构成的集合, E 为多面体 P 的所有棱构成的集合, 用最自然的方式将 $G := (V, E)$ 视为图. 注意 G 一定是平面图 (例如可以这样看: 任取多面体 P 内部的点 O , 以 O 为球心作半径充分大的球面 S^2 , 使得多面体 P 在该球面所围成的内部区域中. 然后以 O 为中心, 将 P 的顶点与棱都投影到球面上, 这就自然给出 X_G 到球面 S^2 的嵌入. 任取点 $p \in S^2 \setminus X_G$, 注意戳破一个点的球面 $S \setminus \{p\}$ 拓扑同胚于平面 \mathbb{R}^2 . 如此就将 X_G 嵌入到平面 \mathbb{R}^2 之中), 并且 G 作为平面图的面数, 边数, 顶点数恰好就是多面体 P 的表面的个数, 棱的个数, 顶点的个数.

记正多面体 P 的面数, 边数, 顶点数分别为 f, e, v ; 每个表面的边数为 n , 过每个顶点的棱的个数 (即图 G 每个顶点的度数) 为 d , 则易知

$$nf = 2e = vd$$

(这是简单的“算两次”练习, 留给读者). 再注意正多面体的几何性质: P 的每个表面都是正 n 边形, 正 n 边形的每个内角的度数为 $\frac{n\pi}{n-2}$, P 的每个顶点都是 d 个表面的公共点, 从而易知 $d \cdot \frac{n\pi}{n-2} < 2\pi$, 即 $d < 2 + \frac{4}{n-2} \leq 6$. 因此 d 的取值只能是 3, 4, 5. 最后再注意平面图的 Euler 公式 $f + v - e = 2$, 经过初等数学计算容易求出 (f, e, v, n, d) 的正整数解只可能是

$$(4, 4, 6, 3, 3), \quad (6, 12, 8, 4, 3), \quad (8, 12, 6, 3, 4),$$

$$(12, 30, 20, 5, 3), \quad (20, 30, 12, 3, 5),$$

(计算过程留给读者练习) 这分别对应五种正多面体. □

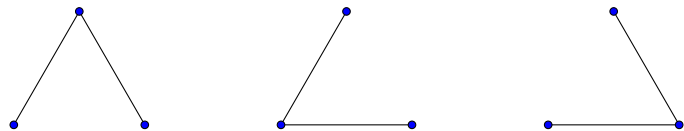
4.3 生成树与 Cayley 公式

4.128. 设 $G = (V, E)$ 是连通图, 则由 4.120 可知存在子集 $E' \subseteq E$, 使得 (V, E') 是树, 并且此时有 $|E'| = |V| - 1$. 满足上述性质的子图 (V, E') 称为图 G 的**生成树**. 具体地做, 如果 G 含有圈, 那么删去圈中的任一条边, 易知删去这条边之后所得的图仍然连通; 这样不断删去 G 中的边, 直到不含圈为止, 最终得到的就是 G 的一棵生成树.

4.129. 一个自然的问题是:

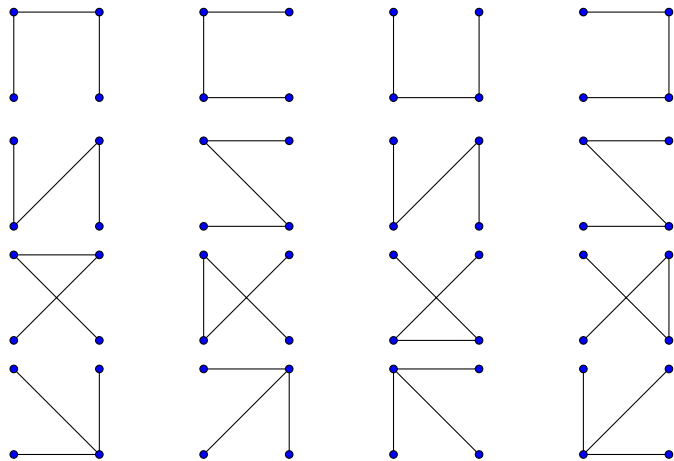
完全图 K_n 多少棵不同的生成树?

或者更一般地, 设 G 是任意给定的图, 则 G 有多少棵生成树? 对于图 G , 记 $ST(G)$ 为 G 的生成树的个数 (当 G 不是连通图时, 规定 $ST(G) = 0$). 不如先看 $n = 3, 4, 5, 6$ 的简单例子. 首先, $n = 3$ 时, K_3 有且仅有如下 3 棵生成树:



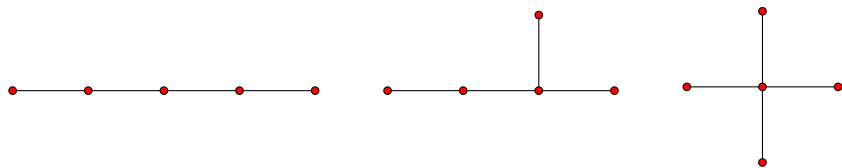
即, $ST(K_3) = 3$.

- $n = 4$ 时, 暴力穷举 K_4 的全部生成树如下:



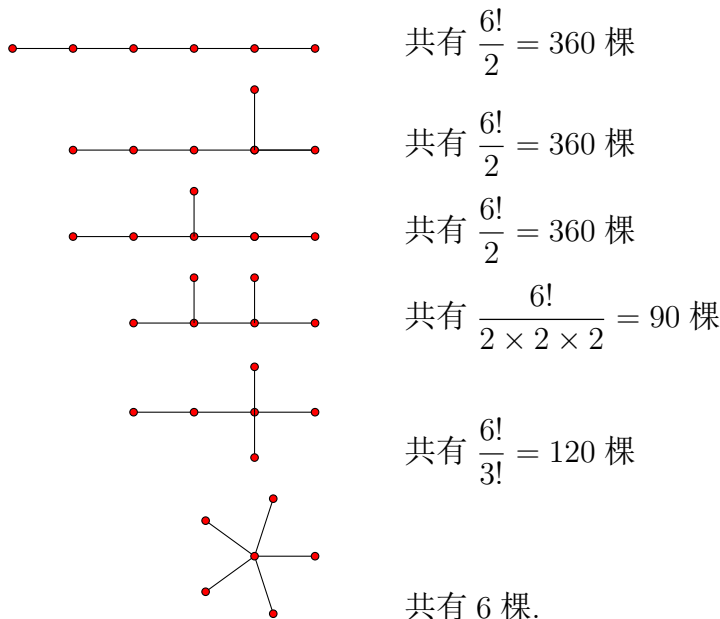
可见 K_4 共有 16 棵生成树, $ST(K_4) = 16$.

- $n = 5$ 的情况就开始复杂了, 最好不要暴力穷举. 注意 K_5 的生成树一定是具有 5 个顶点的树; 而 5 个顶点的树在同构意义下只有如下 3 类:



稍微讨论一下, 易知 K_5 当中的形如这 3 类的生成树的个数分为 $\frac{5!}{2} = 60, 5 \times 4 \times 3 = 60$ 以及 5. (计算过程留给读者). 从而 K_5 的生成树共有 $60 + 60 + 5 = 125$ 棵, $ST(K_5) = 125$.

- 再具体算一下 $n = 6$ 的情形. 暴力穷举可知, 有 6 顶点的树在同构意义下一共有 6 类, 然后分别计数每一类在 K_6 中的个数, 如下:



因此 $ST(K_6) = 360 + 360 + 360 + 90 + 120 + 6 = 1296$.

一般地, 有如下公式:

4.130. 定理. (Cayley, 1889) 对于 $n \geq 3$, 有 $ST(K_n) = n^{n-2}$.

证法 1. 记 K_n 的顶点集 $V = \{v_1, \dots, v_n\}$. 设 $T = (V, E')$ 是 K_n 的一棵生成树, 记 $d_i := d_T(v_i)$ 为树 T 的顶点 $v_i \in V$ 的度数. 则 $d_i \geq 1$ 且 $\sum_{i=1}^n d_i = 2(|V| - 1) = 2n - 2$.

1. 断言: 若 n 元正整数组 (d_1, d_2, \dots, d_n) 满足 $\sum_{i=1}^n d_i = 2n - 2$, 则

$$\# \left\{ \begin{array}{l} T \text{ 是 } K_n \text{ 的} \\ \text{生成树} \end{array} \middle| d_T(v_i) = d_i, \forall i \in [n] \right\} = \frac{(n-2)!}{(d_1-1)!(d_2-1)! \cdots (d_n-1)!}.$$

为证明此断言, 考虑对 n 归纳. $n = 2$ 时直接验证. 一般地, 若该断言对 $(n-1)$ 成立, 则对于满足 $\sum_{i=1}^n d_i = 2n - 2$ 的 n 个正整数 $\{d_i\}$, 易知必存

在某个 $d_i = 1$ (若所有 $d_i \geq 2$, 则它们之和 $\geq 2n$, 矛盾), 不妨 $d_n = 1$. 令 \mathcal{F} 是 K_n 的满足 $d_T(v_i) = d_i, \forall i \in [n]$ 的全部生成树 T 构成的集合. 则对每个 $T \in \mathcal{F}$, 必有 $d_T(v_n) = 1$, 换言之, 顶点 $v_n \in V$ 是树叶, 有唯一的邻居. 考察树叶 $v_n \in V$ 的邻居是谁: 对每个 $i \in [n-1]$, 记

$$\mathcal{F}_i := \{T \setminus \{v_n\} \mid T \in \mathcal{F}, v_n \sim_E v_i\},$$

其中 $T \setminus \{v_n\}$ 是指删除 T 的顶点 v_n 所得到的具有 $(n-1)$ 个顶点的树. 由归纳假设易知

$$|\mathcal{F}_i| = \frac{(n-3)!}{(d_1-1)! \cdots (d_i-2)! \cdots (d_n-1)!} = \frac{d_i-1}{n-2} \cdot \frac{(n-2)!}{(d_1-1)! \cdots (d_n-1)!}$$

因此

$$\begin{aligned} |\mathcal{F}| &= \sum_{i=1}^{n-1} |\mathcal{F}_i| = \frac{(n-2)!}{(d_1-1)! \cdots (d_n-1)!} \sum_{i=1}^{n-1} \frac{d_i-1}{n-2} \\ &= \frac{(n-2)!}{(d_1-1)! \cdots (d_n-1)!}, \end{aligned}$$

断言得证.

2. 求遍所有可能的 (d_1, \dots, d_n) , 注意1.28可得

$$\begin{aligned} \text{ST}(K_n) &= \sum_{\substack{d_1, \dots, d_n \geq 1 \\ d_1 + \dots + d_n \leq 2n-2}} \frac{(n-2)!}{(d_1-1)! \cdots (d_n-1)!} \\ &= \sum_{\substack{d_1, \dots, d_n \geq 0 \\ d_1 + \dots + d_n \leq n-2}} \frac{(n-2)!}{d_1! \cdots d_n!} = n^{n-2}. \end{aligned}$$

从而得证. □

4.131. 生成树计数的 Cayley 公式4.130 有多种证明方法. 为介绍第二种证法, 我们需要引入更多概念. 设 $T = (V, E)$ 是树, 任意取定顶点 $v_0 \in V$, 将这个取定的点称为**树根**. 由树的定义可知, 对于任何顶点 $u \neq v_0$, 存在从树根 v_0 到 u 的**唯一**道路 $v_0 v_1 \cdots v_{k-1} u$ (注意这是 T 的同构于 P_k 的子图), 将这条道路记作 P_u ; 此时称顶点 u 的**深度**为 k , 记作 $\text{depth}_{T, v_0}(u) = k$. 特别地, $\text{depth}_{T, v_0}(u) = 1$ 当且仅当 u 是 v_0 的邻居. 特别规定树根 v_0 的深度为 0.

- 设 $T = (V, E)$ 是树, 取定树根 $v_0 \in V$. 对于任意顶点 $u_1, u_2 \in V$, 如果 $u_1 \in P_{u_2}$, 则称 u_1 是 u_2 的**祖先**, 记作 $u_1 \succeq_{v_0} u_2$, 简记为 $u_1 \succeq u_2$. 此时也称 u_2 是 u_1 的**后代**, 记作 $u_2 \preceq u_1$.

按惯例, 如果 $u_1 \succeq u_2$ 不成立, 则记 $u_1 \not\succeq u_2$.

- 特别注意, 按照这里的约定, 成立 $u \succeq u$. 容易验证 \succeq 是顶点集 V 上的**偏序关系**. 再注意树根 v_0 是 V 中所有元素的祖先.
- 若 $u_1 \succeq u_2$, 并且 u_1 与 u_2 相邻, 则称 u_1 是 u_2 的**父亲**. 容易验证, 若 $u \neq v_0$, 则 u 存在唯一的父亲, 将这个唯一的父亲记作 $F_{T, v_0}(u)$, 简记为 $F(u)$; 若 $\text{depth}_{T, v_0}(u) = k > 0$, 则树根 v_0 是 u 的父亲的父亲的... 的父亲 (重复 k 遍, 即“ k -祖父”).
- (注意以上所有概念均与树根 v_0 的选取有关; 换言之, “祖先”, “父亲”这些概念都是相对的. 树 $T = (V, E)$ 的任何顶点都可视为树根.)

4.132. 现在给出 Cayley 公式 4.130 的第二种证明. 记 K_n 的顶点集 $V = \{v_1, \dots, v_n\}$. 设 T 是 K_n 的生成树, 将 v_n 视为 T 的树根.

定理 4.130 证法 2. 沿用前文的术语与记号约定. 按树根 v_n 的邻居个数 (换言之, 深度为 1 的顶点的个数) 来分类计数 K_n 的生成树. 对于 $k \in [n-1]$, 记

$$N_k := \left\{ T \mid \begin{array}{l} T \text{ 是 } K_n \text{ 的生成树} \\ d_T(v_n) = k \end{array} \right\},$$

则显然 $\text{ST}(K_n) = \sum_{k=1}^{n-1} |N_k|$, 并且 $|N_{n-1}| = 1$. 接下来具体计算每个 $|N_k|$.

1. 为此, 企图寻找数列 $\{|N_k|\}_{k=1,2,\dots,n-1}$ 的递推关系. 首先注意这样的事实: 设 $T = (V, E') \in N_k$, 则对于任何与树根 v_n 不相邻 (并且不等于 v_n) 的顶点 $u \in V$ (换言之, $\text{depth}_{T, v_n}(u) \geq 2$), 显然 u 的父亲 $F_{T, v_n}(u) \neq v_n$; 记

$$E'' := (E' \setminus \{\{u, F_{T, v_n}(u)\}\}) \sqcup \{\{u, v_n\}\},$$

易知 $T' := (V, E'') \in N_{k+1}$. 总之, 上述操作将 N_k 中的元素变为 N_{k+1} 中的元素. 并且 N_{k+1} 中的任何元素显然都可由 N_k 中的元素经上述操作得到.

2. 现在将上述想法精确表述出来, 记集合

$$\begin{aligned}\mathcal{A}_k &:= \{(T, u) \in N_k \times V \mid \text{depth}_{T, v_n}(u) \geq 2\} \\ \mathcal{B}_{k+1} &:= \left\{ (T', u, u') \in N_{k+1} \times V \times V \mid \begin{array}{l} \text{depth}_{T', v_n}(u) = 1, \\ u' \not\leq u, u' \neq v_n \end{array} \right\},\end{aligned}$$

对于 $(T, u) \in \mathcal{A}_k$, 记 $T = (V, E')$, 按照第 1 步所介绍的方法得到 $T' = (V, E'')$. 于是,

$$\varphi_k: (T, u) \mapsto (T', u, F_{T, v_n}(u))$$

给出了从 \mathcal{A}_k 到 \mathcal{B}_{k+1} 的映射. 容易验证上述映射是一一映射 (留给读者), 从而 $|\mathcal{A}_k| = |\mathcal{B}_{k+1}|$.

3. 注意 N_k 的定义, 直接计算得

$$\begin{aligned}|\mathcal{A}_k| &= \sum_{T \in N_k} \# \{u \in V \mid \text{depth}_{T, v_n}(u) \geq 2\} \\ &= \sum_{T \in N_k} (n - 1 - k) = (n - 1 - k)|N_k|, \\ |\mathcal{B}_{k+1}| &= \sum_{T' \in N_{k+1}} \sum_{u' \in V \setminus \{v_n\}} \# \{u \in V \mid \text{depth}_{T', v_n}(u) = 1, u \not\leq u'\} \\ &= \sum_{T' \in N_{k+1}} \sum_{u' \in V \setminus \{v_n\}} k = k(n - 1)|N_{k+1}|,\end{aligned}$$

故有递推关系 $(n - 1 - k)|N_k| = k(n - 1)|N_{k+1}|$. 记 $m_k := \frac{|N_k|}{\binom{n-2}{k-1}}$, 则

$$m_k = (n - 1)m_{k+1},$$

解得 $m_k = (n - 1)^{n-1-k}$, 从而 $|N_k| = \binom{n-2}{k-1}(n - 1)^{n-1-k}$. 因此

$$\begin{aligned}\text{ST}(\mathbf{K}_n) &= \sum_{k=1}^{n-1} |N_k| = \sum_{k=1}^{n-1} \binom{n-2}{n-1-k} (n - 1)^{n-1-k} \\ &= \sum_{k=0}^{n-2} \binom{n-2}{k} (n - 1)^k = (n - 1 + 1)^{n-2} = n^{n-2}.\end{aligned}$$

□

我们还将给出 Cayley 公式 4.130 的第 3 种证明, 甚至给出计算 $\text{ST}(G)$ 的一般公式, 这将用到线性代数工具. 详见 10.272 与 10.276.

4.4 拓扑学应用: Brouwer 不动点定理

4.133. 已知 $f: [0, 1] \rightarrow [0, 1]$ 是连续函数, 证明: 存在 $x_0 \in [0, 1]$ 使得 $f(x_0) = x_0$. 这是一道简单的高数习题, 利用连续函数介值定理可轻易证明. 此结论可以推广到高维情形: 记 n 维闭圆盘

$$\mathbb{D}^n := \left\{ (x_1, x_2, \dots, x_n) \in \mathbb{R}^n \left| \sum_{i=1}^n x_i^2 \leq 1 \right. \right\},$$

则有如下断言: 任何连续映射 $f: \mathbb{D}^n \rightarrow \mathbb{D}^n$ 必存在不动点, 即存在 $x_0 \in \mathbb{D}^n$ 使得 $f(x_0) = x_0$. 这是拓扑学中著名的 **Brouwer 不动点定理** (并非简单的高数习题).

4.134. Brouwer 不动点定理有多种不同证法, 例如

- 代数拓扑方法 (利用上同调群), 见任何一本代数拓扑学教材.
- 几何 + 分析方法 (利用微分形式积分的 Stokes 公式), 将在本节回顾.
- 图论方法 (利用 Sperner 引理), 将在本节详细介绍.

其中图论方法没有用到任何“高级工具”, 仅仅用到图论的最入门知识以及本科低年级的数学分析. 在介绍图论方法之前, 先顺便介绍一下几何 + 分析方法 (不熟悉微分形式的读者可跳过).

Brouwer 不动点定理的“几何 + 分析”证法. 记 \mathbb{S}^{n-1} 为闭球 \mathbb{D}^n 的边界, 即

$$\mathbb{S}^{n-1} := \partial \mathbb{D}^n := \left\{ (x_1, x_2, \dots, x_n) \in \mathbb{R}^n \left| \sum_{i=1}^n x_i^2 = 1 \right. \right\}.$$

1. 断言: 不存在光滑映射 $f: \mathbb{D}^n \rightarrow \mathbb{S}^{n-1}$, 使得 $f|_{\mathbb{S}^{n-1}} = \text{id}$. 这是因为, 如果存在这样的 f , 记 $i: \mathbb{S}^{n-1} \hookrightarrow \mathbb{D}^n$ 为自然的包含映射, 则 $f \circ i = \text{id}_{\mathbb{S}^{n-1}}$. 取 \mathbb{S}^{n-1} 的体积形式 ω , 则 $\int_{\mathbb{S}^{n-1}} \omega = 1$. 而另一方面, 注意 $d\omega = 0$, 从而由 Stokes 公式得

$$\begin{aligned} \int_{\mathbb{S}^{n-1}} \omega &= \int_{\mathbb{S}^{n-1}} (f \circ i)^* \omega = \int_{\mathbb{S}^{n-1}} i^* (f^* \omega) \\ &= \int_{\partial \mathbb{D}^n} f^* \omega = \int_{\mathbb{D}^n} d(f^* \omega) = \int_{\mathbb{D}^n} f^* (d\omega) = 0, \end{aligned}$$

产生矛盾, 从而断言得证.

2. 断言: 若 $f: \mathbb{D}^n \rightarrow \mathbb{D}^n$ 是光滑映射, 则 f 必存在不动点. 这是因为, 如果 f 不存在不动点, 即对任意 $\mathbf{x} \in \mathbb{D}^n$ 都有 $f(\mathbf{x}) \neq \mathbf{x}$, 那么考虑以 $f(\mathbf{x})$ 为起点, 经过 \mathbf{x} 的射线, 这条射线与 \mathbb{S}^{n-1} 有唯一的公共点, 记作 $g(\mathbf{x})$. 则 $\mathbf{x} \mapsto g(\mathbf{x})$ 定义了从 \mathbb{D}^n 到 \mathbb{S}^{n-1} 的光滑映射, 并且映射 g 显然满足 $g|_{\mathbb{S}^{n-1}} = \text{id}$, 与 (1) 中的断言矛盾. 从而断言证毕.
3. 现在证明 Brouwer 不动点定理. 设 $f: \mathbb{D}^n \rightarrow \mathbb{D}^n$ 是连续映射, 则对每个 $k \geq 1$, 取光滑映射 $f_k: \mathbb{D}^n \rightarrow \mathbb{D}^n$ 使得 $\sup_{\mathbf{x} \in \mathbb{D}^n} \|f - f_k\| < \frac{1}{k}$ (即, 用光滑映射一致逼近连续映射. 众所周知这肯定能做到, 例如可以用 Stone-Weierstrass 定理). 则由断言 (2) 可知, 对每个 $k \geq 1$, 存在 $\mathbf{x}_k \in \mathbb{D}^n$ 使得 $f_k(\mathbf{x}_k) = \mathbf{x}_k$. 这就得到紧集 \mathbb{D}^n 上的点列 $\{\mathbf{x}_k\}$. 任取该点列的某个收敛子列, 其极限记为 \mathbf{x}_0 . 则容易证明 \mathbf{x}_0 是 f 的不动点 (简单的数学分析习题, 留给读者). 定理得证.

□

4.135. 现在介绍 Brouwer 不动点定理的图论方法. 首先考虑这样一道小题:

对任意正整数 $N > 2$, 证明: 对任意映射 $\varphi: [N] \rightarrow [2]$, 如果 $\varphi(1) = 1, \varphi(N) = 2$, 则必存在 $i \in [n-1]$ 使得 $\varphi(i) \neq \varphi(i+1)$, 并且满足此条件的 i 恰有奇数个.

不如用一种几何直观的方式来重新叙述此题. 考虑闭区间 $I := [0, 1]$ 的任意分割

$$0 = x_1 < x_2 < \cdots < x_{N-1} < x_N = 1.$$

注意上述分割将 $[0, 1]$ 分成 $(N-1)$ 个小区间. 对于映射 $\varphi: [N] \rightarrow [2]$, 如果 $\varphi(i) = 1$, 则将点 x_i 染为红色; 如果 $\varphi(i) = 2$, 则将点 x_i 染为蓝色. 于是, 每个小线段 $[x_i, x_{i+1}]$ 的两个端点的颜色可能相同可能不同. 此题目断言: 如果区间 I 两个端点 x_1, x_N 的颜色不同, 则 (无论如何选取 N 与 φ) 必存在端点异色的小线段 $[x_i, x_{i+1}]$, 并且端点异色的小线段恰有奇数个.

证明. 证明留给读者. 考虑对 N 归纳.

□

上述命题称为一维 Sperner 引理. (注意这是 Sperner 引理, 而不是 3.85 中的 Sperner 定理!) 这个“染色游戏”可以自然推广至高维. 先看二维的情况.

4.136.引理.(Sperner, 1928). 考虑平面 \mathbb{R}^2 上的三角形闭区域 $\triangle ABC$ 的任

意三角剖分 $\triangle ABC = \bigcup_{i=1}^N \triangle_i$, 使得:

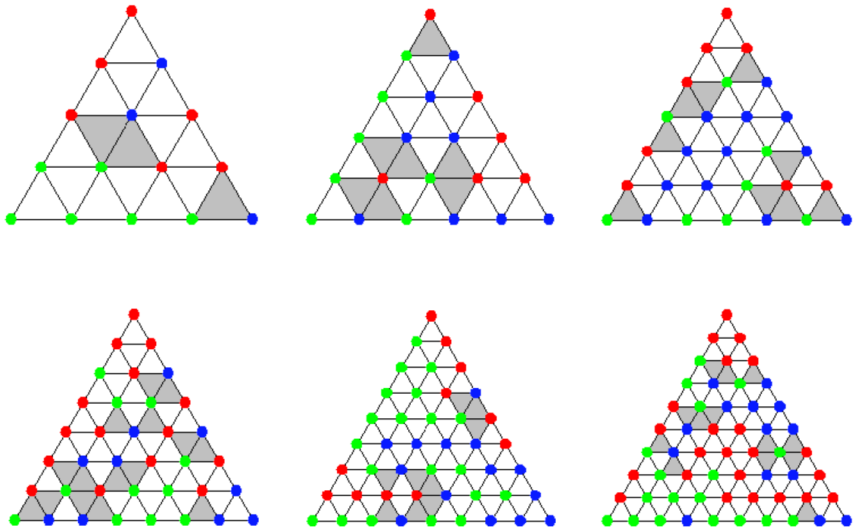
1. 每个“小三角形” \triangle_i 都是包含于 $\triangle ABC$ 的三角形闭区域.
2. “小三角形” \triangle_i 的顶点不能位于其余任何小三角形的边上或内部. (从而任何两个小三角形要么交集为空, 要么共享一个顶点或者共享一条边).

记 X 为所有小三角形的全部顶点构成的集合. 注意大三角形 $\triangle ABC$ 的三个顶点 A, B, C 一定也在 X 中. 则对任意的顶点染色 $\varphi: X \rightarrow [3]$, 如果 φ 满足如下要求

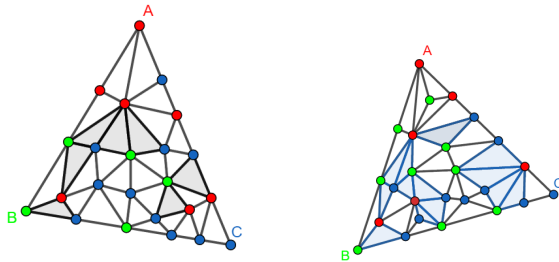
1. $\varphi(A) = 1, \varphi(B) = 2, \varphi(C) = 3$.
2. 对于 $x \in X$, 如果 x 在线段 AB 上, 则 $\varphi(x) \in \{1, 2\}$; 如果 x 在线段 BC 上, 则 $\varphi(x) \in \{2, 3\}$; 如果 x 在线段 CA 上, 则 $\varphi(x) \in \{1, 3\}$,

那么必存在 i , 使得小三角形 \triangle_i 的三个顶点的颜色互不相同; 并且这样小三角形恰有奇数个.

在证明之前, 不妨先看一些例子. 不妨令颜色 1, 2, 3 分别为红色, 绿色, 蓝色. 以下是三角剖分, 小三角形顶点染色的一些例子: 灰色阴影部分为三个顶点颜色互不相同的小三角形.



对大三角形 $\triangle ABC$ 的三角剖分可以非常地任意, 不一定要像上述例子那样分成全等的小三角形, 比如还可以这样:



而 Brouwer 不动点定理的证明则基于这个 Sperner 引理.

4.137. 现在证明二维 Sperner 引理**4.136**.

二维 *Sperner* 引理的证明. 对于满足上述要求的三角剖分 $\triangle ABC = \bigcup_{i=1}^N \triangle_i$, 记 $V' := \{\triangle_i \mid 1 \leq i \leq N\}$ 为所有小三角形构成的集合. 再记 $\triangle^c := \mathbb{R}^2 \setminus \triangle ABC$, 即大三角形的外部区域. 记 $V := V' \sqcup \{\triangle^c\}$. 换言之, 上述三角剖分将平面 \mathbb{R}^2 分成 N 个小三角形区域以及一个无界的外部区域共 $(N+1)$ 个不同区域, 这 $N+1$ 个不同区域构成的集合记作 V . 定义集合 $E \subseteq \binom{V}{2}$ 如下: 对于 $u, v \in V$, $\{u, v\} \in E$ 当且仅当区域 u, v 具有公共边, 且公共边的两个端点的颜色分别是 1, 2. 记 $G := (V, E)$, 则 G 为图. (换言之, 将每个小三角形与外部区域 \triangle^c 视为图 G 的顶点). 容易验证图 G 满足如下性质 (留给读者证明):

- 如果 $v \in V$ 是小三角形, 那么 $d_G(v) \in \{0, 1, 2\}$, 并且小三角形 v 的三个顶点颜色互不相同当且仅当 $d_G(v) = 1$ (从而当且仅当 v 的度数是奇数).
- 外部区域 $\triangle^c \in V$ 的度数 $d_G(\triangle^c)$ 必为奇数 (这利用了一维 Sperner 引理).

由于 $d_G(\triangle^c)$ 是奇数, 从而由握手引理**4.103(3)** 可知, 图 G 一定还存在其他的度数为奇数的顶点, 即三个顶点颜色互不相同的小三角形. 握手引理还断言, 任何图 G 当中的度数为奇数的顶点由偶数个, 从而除了 \triangle^c , 图 G 还有奇数个度数为奇数的顶点. 从而二维 Sperner 引理得证. \square

4.138. 现在用二维 Sperner 引理来证明二维 Brouwer 不动点定理: 连续映射 $f: \mathbb{D}^2 \rightarrow \mathbb{D}^2$ 必存在不动点.

二维 Brouwer 不动点定理的证明. 平面上的闭圆盘 $\mathbb{D}^2 := \{(x, y) \mid x^2 + y^2 \leq 1\}$ 拓扑同胚于三角形闭区域

$$\Delta := \{(x, y) \mid x, y \geq 0, x + y \leq 1\},$$

故只需证明三角形区域的情形, 即任何连续映射 $f: \Delta \rightarrow \Delta$ 都存在不动点.

1. 对于 Δ 中的每个点 $\mathbf{x} = (x, y)$, 将 $f(\mathbf{x})$ 的横, 纵坐标分别记作 x', y' . 定义 Δ 的子集 M_1, M_2, M_3 如下:

$$\begin{aligned} M_1 &:= \left\{ \mathbf{x} = (x, y) \in \Delta \mid \frac{x' + y'}{\sqrt{2}} \geq \frac{x + y}{\sqrt{2}} \right\} \\ M_2 &:= \{ \mathbf{x} = (x, y) \in \Delta \mid x' \leq x \} \\ M_3 &:= \{ \mathbf{x} = (x, y) \in \Delta \mid y' \leq y \} \end{aligned}$$

(注意 Δ 有三条边, $\frac{1 - (x + y)}{\sqrt{2}}, x, y$ 的几何意义分别是点 \mathbf{x} 到这三条边的距离. 粗俗地说, M_i 中的点经过 f 作用之后会比原来更靠近“第 i 条边”). 容易验证 (留给读者练习), 点集 M_i 满足如下性质:

- M_i 为闭集, $i = 1, 2, 3$.
- $\Delta = M_1 \cup M_2 \cup M_3$.
- $\mathbf{x} \in \Delta$ 是 f 的不动点, 当且仅当 $\mathbf{x} \in M_1 \cap M_2 \cap M_3$.

2. 对每个 $k \geq 1$, 取 Δ 的三角剖分 $V'_k := \left\{ \Delta_i^{(k)} \mid i = 1, 2, \dots, N_k \right\}$, 使得

$$\text{diam}(V'_k) := \max_{1 \leq i \leq N_k} \sup_{\mathbf{x}, \mathbf{y} \in \Delta_i^{(k)}} \|\mathbf{x} - \mathbf{y}\| < \frac{1}{k}.$$

(粗俗地说, 取一串“越来越细”的剖分). 记 X_k 为 V'_k 的全部小三角形的全部顶点构成的集合. 固定每个 k , 易知存在满足如下性质的染色 $\varphi_k: X_k \rightarrow [3]$:

- 对任意 $\mathbf{x} \in X_k$, 如果 $\varphi_k(\mathbf{x}) = i$, 则 $\mathbf{x} \in M_i$, ($i = 1, 2, 3$).

- $\varphi_k(0, 0) = 1, \varphi_k(1, 0) = 2, \varphi_k(0, 1) = 3$.
- 对于 $\mathbf{x} = (x, y) \in X_k$: 如果 $x = 0$, 则 $\varphi_k(\mathbf{x}) \in \{1, 3\}$; 如果 $y = 0$, 则 $\varphi_k(\mathbf{x}) \in \{1, 2\}$; 如果 $x + y = 1$, 则 $\varphi_k(\mathbf{x}) \in \{2, 3\}$.

利用 M_i 的定义及性质, 容易证明上述 φ_k 的存在性 (留给读者).

3. 注意 $\varphi_k: X_k \rightarrow [3]$ 满足二维 Sperner 引理的条件, 从而由 Sperner 引理可知必存在三个顶点颜色互异的小三角形. 取 $\triangle^{(k)} \in V'_k$, 使得它的三个顶点颜色互异. 记 $\triangle^{(k)}$ 的三个顶点分别为 $\mathbf{x}_1^{(k)}, \mathbf{x}_2^{(k)}, \mathbf{x}_3^{(k)}$, 使得 $\mathbf{x}_i^{(k)} \in M_i, i = 1, 2, 3$. 再注意三角剖分的选取, 可知

$$\|\mathbf{x}_i^{(k)} - \mathbf{x}_j^{(k)}\| \leq \frac{1}{k}, \quad \forall i, j \in [3].$$

这样就得到了 M_1 中的一串点列 $\{\mathbf{x}_1^{(k)}\}_{k=1}^\infty$. 注意 M_1 是有界闭集, 从而紧致. 取该点列的收敛子列 $\{\mathbf{x}_1^{(s_k)}\}_{k=1}^\infty$, 记 $\mathbf{x} := \lim_{k \rightarrow \infty} \mathbf{x}_1^{(s_k)}$, 注意 $\mathbf{x} \in M_1$. 容易证明 $\lim_{k \rightarrow \infty} \mathbf{x}_2^{(s_k)} = \lim_{k \rightarrow \infty} \mathbf{x}_3^{(s_k)} = \mathbf{x}$, 从而 $\mathbf{x} \in M_2 \cap M_3$. 因此 $\mathbf{x} \in M_1 \cap M_2 \cap M_3$ 是 f 的不动点. 定理得证.

□

4.139. 上述证明过程完全可以类似推广到 n 维. 证明 n 维的 Brouwer 不动点定理 (即, 连续映射 $f: \mathbb{D}^n \rightarrow \mathbb{D}^n$ 必有不动点), 需要用到所谓 n 维 Sperner 引理. 例如 $n = 3$ 是, 要考虑将四面体剖分为若干“小四面体”, 然后对剖分的端点按某些要求染 4 种颜色, 那么必存在奇数个四个端点颜色互异的小四面体.

一般地, 对 n 维单纯形 \triangle^n (三角形, 四面体的自然的高维推广), 将它的全部 $(n+1)$ 个 0 维表面 (即, 顶点) 分别记作 $\mathbf{x}_0, \dots, \mathbf{x}_n$. 对于 \triangle^n 的任意单纯剖分, 将每个剖分点都染上给定 $n+1$ 种颜色之一, 使得落在 k 维表面 $\mathbf{x}_{i_1}\mathbf{x}_{i_2}\cdots\mathbf{x}_{i_k}$ 的剖分点的颜色只能属于 $\{i_1, i_2, \dots, i_k\}$. 则 n 维 Sperner 引理断言: 必然存在某个小单纯形, 使得它的 $(n+1)$ 个顶点的颜色互不相同; 并且这样的小单纯形恰有奇数个.

n 维 Sperner 引理的证明与 2 维情形完全类似, 要用到握手引理. 证明的关键之处在于说明“外部区域”的度数是奇数, 而这依赖于 $(n-1)$ 维 Sperner 引理. 于是, n 维 Sperner 定理的证明需要对维数 n 进行归纳. 证明细节留给

读者, 与 2 维情形并无本质不同. 由 n 维 Sperner 引理证明 n 维 Brouwer 不动点定理的过程与 2 维情形完全类似, 留给读者. 从而, n 维 Brouwer 不动点定理得证.

5. 相异代表元系

5.1 相异代表元系与 Hall 定理

5.140. 定义. 设 X_1, X_2, \dots, X_m 是由有限集构成的有限序列. 如果元素 x_1, x_2, \dots, x_m 两两互异, 并且 $x_i \in X_i, \forall i \in [m]$, 则称序列 x_1, \dots, x_m 是集合列 X_1, \dots, X_m 的一个相异代表元系.

注意这里用的是集合序列, 而不是集合族, 这样的好处是, 可以允许 X_1, \dots, X_n 之中的某些集合相同. 自然要问, 什么样的集合序列能存在相异代表元系?

5.141. 性质. 设 X_1, \dots, X_m 是集合序列. 如果该集合列存在相异代表元系, 那么对任意 $I \subseteq [m]$, 必有 $\left| \bigcup_{i \in I} X_i \right| \geq |I|$.

证明. 过于显然, 留给读者. □

上述性质给出了存在相异代表元系的一个显然的必要条件, 这个条件称为 Hall 条件. 而不显然的是, Hall 条件竟然也是存在相异代表元系的充分条件.

5.142. 定理. (Hall, 1935) 集合列 X_1, \dots, X_m 存在相异代表元系当且仅当它满足 Hall 条件.

证明. 必要性显然, 只证充分性, 即证明满足 Hall 条件的集合列一定有相异代表元系. 现在设 X_1, \dots, X_m 满足 Hall 条件, 则由 Hall 条件容易推出所有 X_i 都是非空集合. 现在对集合列的长度 m 归纳. $m = 1$ 时显然成立. 对于 $m \geq 2$, 分以下两种情况讨论

- 如果对 $[m]$ 的任何真子集 \mathcal{I} 都成立 $\left| \bigcup_{i \in \mathcal{I}} X_i \right| > |\mathcal{I}|$, 则任取 $x_1 \in X_1$, 然后对每个 $2 \leq i \leq m$, 记 $X'_i := X_i \setminus \{x_1\}$. 则对任何 $\mathcal{I} \subseteq \{2, 3, \dots, m\}$,

$$\begin{aligned} \left| \bigcup_{i \in \mathcal{I}} X'_i \right| &= \left| \left(\bigcup_{i \in \mathcal{I}} X_i \right) \setminus \{x_1\} \right| \geq \left| \bigcup_{i \in \mathcal{I}} X_i \right| - 1 \\ &\geq (|\mathcal{I}| + 1) - 1 = |\mathcal{I}|, \end{aligned}$$

因此 X'_2, X'_3, \dots, X'_m 满足 Hall 条件, 从而由归纳假设可知存在 $x_i \in X'_i$, $2 \leq i \leq m$ 使得 x_2, \dots, x_m 两两互异. 由 X'_i 的定义可知 $x_i \neq x_1$, $2 \leq i \leq m$. 因此 x_1, x_2, \dots, x_m 是 X_1, X_2, \dots, X_m 的相异代表元系, 得证.

- 若不然, 则存在 $[m]$ 的某个真子集 \mathcal{J} , 使得 $\left| \bigcup_{i \in \mathcal{J}} X_i \right| = |\mathcal{J}|$. 此时, 不妨 $\mathcal{J} = \{1, 2, \dots, k\}$. 注意子列 X_1, X_2, \dots, X_k 显然也满足 Hall 条件, 由归纳假设, 取相异代表元系 x_1, x_2, \dots, x_k . 对每个 $k < j \leq m$, 记 $X'_j := X_j \setminus \{x_1, x_2, \dots, x_k\}$. 断言: 集合列 $X'_{k+1}, X'_{k+2}, \dots, X'_m$ 也满足 Hall 条件. 这是因为, 假如存在 $\mathcal{J}' \subseteq \{k+1, \dots, m\}$ 使得 $\left| \bigcup_{j \in \mathcal{J}'} X_j \right| < |\mathcal{J}'|$, 则

$$\left| \bigcup_{j \in \mathcal{J}' \sqcup [k]} X_j \right| = \left| \left(\bigcup_{j \in \mathcal{J}'} X'_j \right) \cup \{x_1, \dots, x_k\} \right| < |\mathcal{J}'| + k = |\mathcal{J}' \sqcup [k]|,$$

与 X_1, \dots, X_m 满足 Hall 条件矛盾, 断言得证. 从而由归纳假设, 取 X'_{k+1}, \dots, X'_m 的相异代表元系 x_{k+1}, \dots, x_m . 则容易验证 $x_1, \dots, x_k; x_{k+1}, \dots, x_m$ 是 X_1, \dots, X_m 的一个相异代表元系.

综上, 定理得证. □

Hall 定理有很多神奇的应用, 我们将在后文介绍之.

5.143. 习题. (Hall 定理加强版) 已知集合列 X_1, \dots, X_m 满足 Hall 条件, 并且正整数 r 满足 $\min_{i \in [m]} |X_i| \geq r$. 证明: 集合列 X_1, \dots, X_m 的相异代表元系的个数

至少为

$$f(r, m) := \prod_{i=1}^{\min\{r, m\}} (r + 1 - i).$$

证明. 对集合列长度 m 归纳. $m = 1$ 时显然. 之后完全按照 Hall 定理 5.142 的证明过程, 分两种情况讨论即可.

- 若对 $[m]$ 的任何真子集 \mathcal{I} 都有 $\left| \bigcup_{i \in \mathcal{I}} X_i \right| > |\mathcal{I}|$, 此时任取 $x_1 \in X_1$, 集合列 X_2^*, \dots, X_n^* 也满足 Hall 条件, 其中 $X_i' := X_i \setminus \{x_1\}$. 注意 $\min_{2 \leq i \leq m} |X_i'| \geq r - 1$, 从而由归纳假设, X_2', \dots, X_m' 的相异代表元系至少有 $f(r - 1, m - 1)$ 个. 而 x_1 有至少 r 种选法, 于是易知 X_1, \dots, X_m 的相异代表元系的个数至少为 $rf(r - 1, m - 1) = f(r, m)$.
- 若不然, 则存在 $1 \leq i_1 < i_2 < \dots < i_k \leq m$, 使得 $\left| \bigcup_{j=1}^k X_{i_j} \right| = k$, 类似可知 X_1, \dots, X_m 的相异代表元系的个数至少为 $f(r, k) \cdot f(\max\{r - k, 1\}, m - k) = f(r, m)$.

综上, 命题得证. □

5.144. 习题. 对于集合列 X_1, \dots, X_m , 如果

$$\sum_{1 \leq i < j \leq m} \frac{|X_i \cap X_j|}{|X_i| \cdot |X_j|} < 1,$$

则该集合列存在相异代表元系.

证明. 考虑如下随机事件: 对每个 $i \in [m]$, 从集合 X_i 之中随机抽取元素 x_i , 如此得到 (x_1, x_2, \dots, x_m) . 只需证明事件“ x_1, \dots, x_m 两两互异”的概率大于 0. 注意

$$\mathbb{P}(x_1, \dots, x_m \text{ 并非两两互异}) \leq \sum_{1 \leq i < j \leq m} \mathbb{P}(x_i = x_j) = \sum_{1 \leq i < j \leq m} \frac{|X_i \cap X_j|}{|X_i| \cdot |X_j|} < 1,$$

因此 $\mathbb{P}(x_1, \dots, x_m \text{ 两两互异}) > 0$, 得证. □

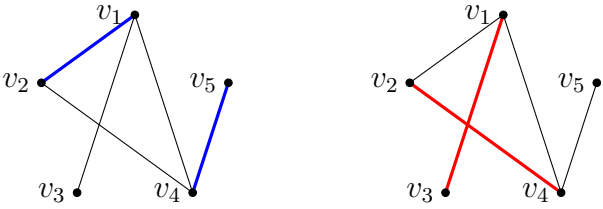
上述方法称为“**概率方法**”, 是组合数学里的常用方法, 我们在后文还会专门介绍. 其实并不难将上述证明过程翻译为组合计数的语言, 从而避免使用概率语言. 具体细节留给读者.

5.2 二部图的匹配

5.145.定义. 设 $G = (V, E)$ 是图, E' 是 E 的子集. 如果对任意 $e_1, e_2 \in E'$, 成立 $e_1 \cap e_2 = \emptyset$, 则称 E' 是图 G 的一个**匹配**.

换言之, E' 是 G 的匹配, 当且仅当 E' 中的任何两条边都没有公共端点. 按此定义, \emptyset 与 E 的一元子集显然都是 G 的匹配, 这些匹配是平凡的. 再比如, 如果 G 的顶点集 $V = \{v_1, v_2, v_3, v_4, v_5\}$, 边集 $E = \{e_1, e_2, e_3, e_4, e_5\}$, 其中

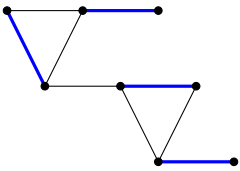
$$e_1 = \{v_1, v_2\}, \quad e_2 = \{v_1, v_3\}, \quad e_3 = \{v_1, v_4\}, \quad e_4 = \{v_2, v_4\}, \quad e_5 = \{v_4, v_5\},$$



则 $E' := \{e_1, e_5\}$ 是图 G 的匹配 (如上图, E' 中的边被蓝色加粗); $E'' = \{e_2, e_4\}$ 也是 G 的匹配 (红色加粗). 粗俗地说, 所谓“匹配”, 就是将图 G 的某一部分顶点通过相连的边来“两两配对”.

5.146.定义. 设 E' 是图 $G = (V, E)$ 的匹配. 如果 $\bigsqcup_{e \in E'} e = V$, 则称 E' 是图 G 的**完美匹配**.

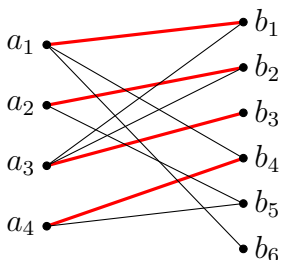
换言之, E' 是 G 的完美匹配当且仅当 G 的每个点都是 E' 中某个边的端点; 粗俗地说, 每个顶点都和其他顶点“配对成功”. 显然, 若图 G 存在完美匹配, 则 G 的顶点个数必须是偶数. 再比如, 下图之中蓝色加粗的边构成该图的完美匹配.



我们目前更关心一类特殊的图, 即**二部图**, 的匹配. 我们回忆, 图 $G = (V, E)$ 称为二部图, 如果存在顶点集 V 的划分 $V = V_1 \sqcup V_2$, 使得 V_1, V_2 非空, 并且 V_i 的任何两个顶点都不相邻, $i = 1, 2$.

5.147. 定义. 设 $G = (A \sqcup B, E)$ 为二部图, 顶点集 $V = A \sqcup B$, $E' \subseteq E$ 是 G 的匹配. 如果 $A \subseteq \bigsqcup_{e \in E'} e$, 则称 E' 是二部图 G 的 **A-匹配**.

例如, 若 $A = \{a_1, a_2, a_3, a_4\}$, $B = \{b_1, b_2, \dots, b_6\}$, 图 G 如下图所示



则其中红色加粗的边构成二部图 G 的 A -匹配.

5.148. 定理.(Hall 定理, 二部图版本) 设 $G = (A \sqcup B, E)$ 是二部图, 其顶点集 $V = A \sqcup B$, $A = \{a_1, \dots, a_m\}$, $B = \{b_1, \dots, b_n\}$. 则下列命题等价:

1. 二部图 G 存在 A -匹配.
2. 集合列 $N_G(a_1), N_G(a_2), \dots, N_G(a_m)$ 存在相异代表元系, 其中 $N_G(a_i)$ 是 a_i 的邻居集, 即与 a_i 相邻的所有顶点构成的集合.

$$3. \text{ 对任意 } \mathcal{I} \subseteq [m] \text{ 都成立 } \left| \bigcup_{i \in \mathcal{I}} N_G(a_i) \right| \geq |\mathcal{I}|.$$

证明. (1) 与 (2) 显然等价, (3) 是相应的 Hall 条件, 再用定理 5.142. □

其实就是将 Hall 定理 5.142 换一种说法. 但这个“二部图匹配版本”的 Hall 定理似乎更加直观一些. 一个常用的推论为:

5.149. 推论. 设二部图 $G = (A \sqcup B, E)$ 满足: A 中的每个顶点的度数都为 d_A , B 中的每个顶点的度数都为 d_B , 并且 $d_A \geq d_B > 0$. 那么 G 存在 A -匹配.

证明. 只需验证 Hall 条件. 对任意 $A' = \{a_1, \dots, a_k\} \in \binom{A}{k}$, 记 $B' := \bigcup_{i=1}^k N_G(a_i)$, 再记 $S := \{(a, b) \in A' \times B' \mid \{a, b\} \in E\}$. 考虑对 S 算两次. 一

方面,显然有

$$|S| = \sum_{a \in A'} \#\{b \in B' \mid a \sim_E b\} = kd_A$$

$$|S| = \sum_{b \in B'} \#\{a \in A' \mid a \sim_E b\} \leq \sum_{b \in B'} d_B = d_B \cdot |B'|$$

因此 $|B'| \geq k \cdot \frac{d_A}{d_B} \geq k$, 从而 Hall 条件成立. 得证. \square

对一般的图 G , 我们还常考虑让尽量更多的顶点参与到匹配中. 换言之, 想知道 $\max \{|E'| \mid E' \subseteq E \text{ 是 } G \text{ 的匹配}\}$ 的值是多少. 一般地, 如果匹配 $E' \subseteq E$ 是 G 的所有匹配当中元素个数最大的, 则称 E' 是 G 的**最大匹配**.

事实上, 某种意义下与”匹配”相对应的概念是:

5.150.定义. 设 $G = (V, E)$ 是图, $V' \subseteq V$.

1. 如果对任意 $e \in E, e \cap V' \neq \emptyset$, 则称 V' 是图 G 的一个**顶点覆盖**.
2. 如果 V' 是 G 的所有顶点覆盖之中元素个数最小的, 则称 V' 是 G 的一个**最小顶点覆盖**.

以下性质显然成立:

5.151.性质. 设 $G = (V, E)$ 是图, $E' \subseteq E$ 是 G 的匹配, $V' \subseteq V$ 是 G 的顶点覆盖, 则 $|V'| \geq |E'|$. 特别地, G 的最小顶点覆盖的顶点数不小于 G 的最大匹配的边数.

证明. 由顶点覆盖的定义可知对任意 $e \in E'$ 都有 $V' \cap e \neq \emptyset$. 再由匹配的定义可知 E' 中的边两两不交, 从而

$$|V'| \geq \left| V' \cap \left(\bigsqcup_{e \in E'} e \right) \right| = \left| \bigsqcup_{e \in E'} (V' \cap e) \right| = \sum_{e \in E'} |V' \cap e| \geq \sum_{e \in E'} 1 = |E'|.$$

\square

而不显然的是, 若 G 是二部图, 则上述不等式实际上取到等号, 换言之, G 的最大匹配的边数恰为最小顶点覆盖的顶点数.

5.152.定理.(König-Egerváry, 1931) 若 $G = (V, E)$ 是二部图, E' 是 G 的一个最大匹配, V' 是 G 的一个最小顶点覆盖, 则 $|E'| = |V'|$.

证明. 记 $V = A \sqcup B$ 为顶点集的相应划分. 取定 G 的最小顶点覆盖 V' , 记 $V' = A' \sqcup B'$, 其中 $A' := V' \cap A$, $B' := V' \cap B$. 由之前讨论可知, 只需证明存在 G 的某个匹配 E'' , 使得 $|E''| \geq |V'|$. 记 $\bar{A}' := A \setminus A'$, 类似定义 $\bar{B}' := B \setminus B'$. 断言: 存在 G 的匹配 $E_{A'}$, 使得 $A' \subseteq \bigcup_{e \in E_{A'}} e \subseteq A' \sqcup \bar{B}'$.

(换言之, $E_{A'}$ 是限制子图 $G|_{A' \sqcup \bar{B}'}$ 的 A' -匹配. 从而此时必有 $|E_{A'}| = |A'|$). 为证明此断言, 只需验证相应的 Hall 条件. 若相应的 Hall 条件不成立, 则存在 A' 的子集 A'' , 使得 $\bar{B}'' := \bar{B}' \cap \left(\bigcup_{a \in A''} N_G(a) \right)$ 满足 $|\bar{B}''| < |A''|$. 此时, 容易验证 $(A' \setminus A'') \sqcup (B' \sqcup \bar{B}'')$ 也是 G 的顶点覆盖, 并且顶点数严格小于 $|V'|$, 这与 V' 是最小顶点覆盖矛盾. 从而断言得证. 同理, 限制子图 $G|_{\bar{A}' \sqcup B'}$ 存在 B' -匹配, 记作 $E_{B'}$. 容易验证 $E'' := E_{A'} \sqcup E_{B'}$ 是 G 的匹配, 并且 $|E''| = |E_{A'}| + |E_{B'}| = |A'| + |B'| = |V'|$. 从而定理得证. \square

5.153. 上述 König-Egerváry 定理也可翻译成别的话语. 对于二部图 $G = (A \sqcup B, E)$, 记 $A = \{a_1, \dots, a_m\}$, $B = \{b_1, \dots, b_n\}$. 注意到二部图 G 可以通过如下方式自然地用 $m \times n$ 矩阵来描述: 考虑矩阵 $\mathbf{X} = (x_{ij}) \in \mathbb{R}^{m \times n}$, 其中

$$x_{ij} := \begin{cases} 1 & a_i b_j \in E \\ 0 & a_i b_j \notin E \end{cases}.$$

可见, \mathbf{X} 是 **0-1 矩阵**, 即所有矩阵元的值都是 0 或 1. 注意到 \mathbf{X} 的非零矩阵元与图 G 的边有自然的一一对应. 于是我们将二部图 G 翻译为 0-1 矩阵 \mathbf{X} . 对于矩阵 \mathbf{X} 的两个非零矩阵元, 如果它们不在同一行且不在同一列, 则称这两个非零矩阵元**相互独立**. (容易验证, 两个非零矩阵元相互独立当且仅当它们对应的图 G 的两条边没有公共端点. 这样就容易把“匹配”的概念翻译到矩阵上). 另一方面, 如果矩阵 $\mathbf{X}' \in \mathbb{R}^{s \times t}$, 则暂时将 $s + t$ 称为矩阵 \mathbf{X}' 的“**规模**”. 对于二部图 G 所对应的矩阵 \mathbf{X} , 注意 \mathbf{X} 的子矩阵与顶点集 V 的子集有自然一一对应. $V' \subseteq V$ 是 G 的顶点覆盖当且仅当相应的子矩阵 \mathbf{X}' 包含 \mathbf{X} 的全部非零元. 于是, 我们有如下定理:

5.154.定理.(König-Egerváry 定理的矩阵版本) 对于矩阵 $\mathbf{X} \in \mathbb{R}^{m \times n}$, 则

$$\begin{aligned} & \mathbf{X} \text{ 的两两独立的非零矩阵元的最大个数} \\ &= \text{包含 } \mathbf{X} \text{ 的全体非零元的子矩阵的最小规模.} \end{aligned}$$

证明. 只需把矩阵 \mathbf{X} 的非零元都看成 1. 这与定理 5.152 等价. \square

5.3 Hall 定理的若干应用

Hall 定理 5.142 有许多神奇应用, 我们举例说明之.

5.155. 定义. 给定正整数 $r \leq n$, 以及矩阵 $\mathbf{L} \in \mathbb{R}^{r \times n}$. 如果 \mathbf{L} 的所有矩阵元都取值于 $\{1, 2, \dots, n\}$, 并且 \mathbf{L} 的每一行, 每一列的各元素都互不相同, 则称 \mathbf{L} 为 **拉丁矩阵**. 特别地, $r = n$ 时的拉丁矩阵也叫做 **拉丁方阵**.

由定义易知, 若 $\mathbf{L} \in \mathbb{R}^{r \times n}$ 是拉丁矩阵, 则 \mathbf{L} 的每一行都恰好不重复地取遍 $1, 2, \dots, n$. 众所周知的 **数独** 就是一类特殊的 9×9 拉丁方阵 (不仅要求每行每列的各元素都互不相同, 还要求每个“九宫格”里的元素也互不相同)

5.156. 定理. (Ryser, 1951) 给定正整数 $r < n$, 以及拉丁矩阵 $\mathbf{L} \in \mathbb{R}^{r \times n}$, 则总可以给 \mathbf{L} 再添加新的一行, 使得所得到的 $(r+1) \times n$ 矩阵依然是拉丁矩阵. 特别地, 总可以将 \mathbf{L} 扩充为 $n \times n$ 拉丁方阵.

证明. 记 $\mathbf{L} = (\ell_{ij})$. 对于每个 $1 \leq j \leq n$, 记集合 $S_j := \{\ell_{ij} \mid i \in [r]\}$, 以及 $S_j^c := [n] \setminus S_j$. 如果真的可以给 \mathbf{L} 新增一行 (使之成为 $(r+1) \times n$ 拉丁矩阵), 则新增的那一行的第 j 列的取值只可能在 S_j^c 之中. 只需证明集合列 $S_1^c, S_2^c, \dots, S_n^c$ 存在相异代表元系即可. 而这是显然的, 只需注意每个 S_j^c 恰有 $n-r$ 个元素, 而 $[n]$ 中的每个元素都恰好属于 $\{S_j\}$ 之中的 $n-r$ 的集合, 再注意推论 5.149 即可. 定理得证. \square

现在介绍 Hall 定理的第 2 个应用.

5.157. 定义. 设 $\mathbf{S} \in \mathbb{R}^{n \times n}$ 是 n 阶实方阵,

1. 如果 \mathbf{S} 每一行, 每一列都恰有一个矩阵元的为 1, 且其余矩阵元都为 0, 则称 \mathbf{S} 是 **置换矩阵**.
2. 如果 \mathbf{S} 的所有矩阵元都非负, 并且每一行, 每一列的所有矩阵元之和都是 1, 则称 \mathbf{S} 是 **双随机矩阵**.

易知 $n \times n$ 置换矩阵与置换群 S_n 中的元素有自然一一对应. 易知置换矩阵显然是双随机矩阵. 此外, 设 $\mathbf{S}_1, \dots, \mathbf{S}_m$ 是置换矩阵, 则对于任意常数

$\lambda_i \in [0, 1]$, $\sum_{i=1}^m \lambda_i = 1$, 容易验证矩阵 $\mathbf{S} := \sum_{i=1}^m \lambda_i \mathbf{S}_i$ 是双随机矩阵. 一般地, 若 V 为实线性空间, X 是 V 的子集, $\mathbf{v} \in V$, 如果存在 X 中的有限多个向量 $\mathbf{x}_1, \dots, \mathbf{x}_m$ 以及参数 $\lambda_1, \dots, \lambda_m \in [0, 1]$ 使得 $\sum_{i=1}^m \lambda_i = 1$, 并且 $\mathbf{v} = \sum_{i=1}^m \lambda_i \mathbf{x}_i$, 则称 \mathbf{v} 形如 X 的凸组合. 于是, 置换矩阵的凸组合一定是双随机矩阵. 而不显然的是, 双随机矩阵一定形如置换矩阵的凸组合, 这正是著名的 Birkhoff-von Neumann 定理:

5.158.定理.(Birkhoff, 1949; von Neumann, 1953) n 阶实方阵 \mathbf{S} 是双随机矩阵当且仅当它形如置换矩阵的凸组合.

证明. 只需证“仅当”. 设 $\mathbf{S} = (s_{ij}) \in \mathbb{R}^{n \times n}$ 为双随机矩阵. 注意 \mathbf{S} 每一行之和都是 1, 从而 \mathbf{S} 每一行都至少有一个非零矩阵元, 因此 \mathbf{S} 至少有 n 个非零矩阵元. \mathbf{S} 的每一列也同理. 由此易知, 如果 \mathbf{S} 恰有 n 个非零矩阵元, 则 \mathbf{S} 的每一行, 每一列都只有一个非零矩阵元, 从而易知 \mathbf{S} 是置换矩阵, 显然形如置换矩阵的凸组合. 一般地, 对 \mathbf{S} 的非零矩阵元的个数 s 归纳. 归纳起始步 $s = n$ 已证明. 当 $s > n$ 时, 对每个 $i \in [n]$ 记集合 $X_i := \{j \in [n] \mid s_{ij} > 0\}$. 断言集合列 X_1, \dots, X_n 满足 Hall 条件. 这是因为, 若存在 $\mathcal{I} \subseteq [n]$ 使得 $Y := \bigcup_{i \in \mathcal{I}} X_i$ 满足 $|Y| < |\mathcal{I}|$, 则不妨 $\mathcal{I} = \{1, 2, \dots, k\}$,

$Y = \{1, 2, \dots, \ell\}, \ell < k$, 于是 \mathbf{S} 可分块写为 $\mathbf{S} = \begin{pmatrix} \mathbf{S}_{11} & \mathbf{0} \\ * & * \end{pmatrix}$, 其中 $\mathbf{S}_{11} \in \mathbb{R}^{k \times \ell}$.

对 \mathbf{S}_{11} 的所有矩阵元之和算两次:

$$\begin{aligned} \sum_{(i,j) \in [k] \times [\ell]} s_{ij} &= \sum_{i=1}^k \sum_{j=1}^{\ell} s_{ij} = \sum_{i=1}^k 1 = k \\ \sum_{(i,j) \in [k] \times [\ell]} s_{ij} &= \sum_{j=1}^{\ell} \sum_{i=1}^k s_{ij} \leq \sum_{j=1}^{\ell} 1 = \ell, \end{aligned}$$

与 $k > \ell$ 矛盾, 从而断言得证. 取 X_1, \dots, X_n 的相异代表元系 y_1, y_2, \dots, y_n , 定义矩阵 $\mathbf{Y} = (y_{ij}) \in \mathbb{R}^{n \times n}$ 如下: $y_{ij} = \begin{cases} 1 & \text{若 } j = y_i \\ 0 & \text{其余情况} \end{cases}$, 则 \mathbf{Y} 是置换矩阵. 再

令 $\lambda_0 := \min_{1 \leq i \leq n} s_{i, y_i}$, 则易知 $\mathbf{S}' := \frac{1}{1 - \lambda_0} (\mathbf{S} - \lambda_0 \mathbf{Y})$ 也是双随机矩阵, 并且其

非零矩阵元的个数严格小于 s , 从而由归纳假设, S' 形如置换矩阵的凸组合. 因此 $S = (1 - \lambda_0)S' + \lambda_0 Y$ 也形如置换矩阵的凸组合, 定理得证. \square

利用 Hall 定理, 可以得到 Erdős-Ko-Rado 定理3.96 的一个推广.

5.159.定理. 设正整数 n, k 满足 $k \leq \frac{n}{2}$, A_1, \dots, A_m 是 $[n]$ 的一族子集, 它们两两交集非空且互不包含, 并且 $|A_i| \leq k, \forall i \in [m]$. 则 $m \leq \binom{n-1}{k-1}$.

证明. 记 $\mathcal{A} := \{A_1, \dots, A_m\}$. 不妨 $k = \max_{A \in \mathcal{A}} |A|$. 记 $\ell := \min_{A \in \mathcal{A}} |A|$. 对 $(k - \ell)$ 归纳. 归纳起始步 $k - \ell = 0$ 的情形, 直接使用 Erdős-Ko-Rado 定理3.96 即可, 从而起始步得证. 若 $k - \ell > 0$, 则 $\ell \leq k - 1 \leq \frac{n}{2} - 1$. 不妨 $\mathcal{A}' := \{A \in \mathcal{A} \mid |A| = \ell\} = \{A_1, A_2, \dots, A_s\}$. 再令 $\mathcal{B} := \binom{[n]}{\ell+1} = \{B_1, \dots, B_t\}$. 定义二部图 $G = (\mathcal{A}' \sqcup \mathcal{B}, E)$ 如下: $A_i \sim_E B_j$ 当且仅当 $A_i \subseteq B_j$. 则在 G 中, \mathcal{A}' 中每个顶点的度数均为 $n - \ell$, 而 \mathcal{B} 中每个顶点的度数至多为 $\ell + 1$, 注意 $\ell + 1 \leq n - \ell$, 采用与推论5.149的证明过程类似的方法容易说明二部图 G 存在 \mathcal{A}' -匹配. 换言之, 对每个 $A_i \in \mathcal{A}'$, 存在集合 $A'_i \in \binom{[n]}{\ell+1}$ 使得 $A_i \subseteq A'_i$, 并且 A'_1, A'_2, \dots, A'_s 互不相同. 又因为 \mathcal{A} 中的集合互不包含, 从而易知 $A'_1, \dots, A'_s; A_{s+1}, \dots, A_m$ 不互相同. 容易验证, 集族 $\{A'_1, \dots, A'_s; A_{s+1}, \dots, A_m\}$ 依然满足题设, 并且其中集合的元素个数最小值严格大于 ℓ , 从而由归纳假设可知 $m \leq \binom{n-1}{k-1}$, 得证. \square

6. Turán 问题

6.1 Mantel 定理

6.160. 对于图 G, H , 我们回忆, 如果 G 存在同构于 H 的子图, 则称 G 含有 H ; 否则称 G 不含 H . 显然, G 含有 H 的一个必要条件是, G 的顶点数不小于 H 的顶点数. 再注意, 如果顶点数 $v(G) \geq v(H)$, 则当 G 的边数 $e(G)$ 足够大时, G 一定会含有 H (比如当 G 是完全图时, 显然 G 含有 H). 一个自然的问题是:

给定正整数 n 与图 H , 则

有 n 个顶点, 且不含 H 的图最多有几条边?

上述问题称为 **Turán 问题**, 这是极值图论中的重要问题之一.

6.161. 定义. 设 H 是图, 正整数 $n \geq e(H)$, 则记

$$\text{ex}(n, H) := \max \{ \ell \in \mathbb{Z}_+ \mid \text{存在图 } G, \text{ 使得 } G \text{ 有 } n \text{ 个顶点 } \ell \text{ 条边, 且 } G \text{ 不含 } H \},$$

称之为图 H 的 **Turán 数**.

首先, 至少显然有 $\text{ex}(n, H) \leq \binom{n}{2} = \frac{n(n-1)}{2}$. 因为当 $n \geq e(H)$ 时, n 个顶点的完全图一定含有 H . 对一般的图 H , 求 $\text{ex}(n, H)$ 的具体表达式是非常困难的问题. 我们似乎只能估计一下 $\text{ex}(n, H)$ 的大致范围, 或者当 $n \rightarrow \infty$ 时的增长阶数. 不过对于“最简单的”图 $C_3 \cong K_3$, 有如下结果:

6.162. 定理.(Mantel, 1907). $\text{ex}(n, K_3) = \lfloor \frac{n^2}{4} \rfloor$. 换言之, 若图 G 有 n 个顶点, 且边数大于 $\lfloor \frac{n^2}{4} \rfloor$, 则 G 必含有三角形 (长度为 3 的圈 $C_3 \cong K_3$); 另一方面, 存在 n 个顶点 $\lfloor \frac{n^2}{4} \rfloor$ 条边但不含三角形的图.

证法 1. 设图 $G = (V, E)$ 具有 n 个顶点, 且不含三角形. 设 v_0 是 G 的度数最大的顶点, 记 $s := d_G(v_0)$. 则 v_0 的邻居集合 $N_G(v_0)$ 当中有 s 个元素. 注意 G 不含三角形, 从而易知 $N_G(v_0)$ 中的任何两点都不相邻. 记 $N' := V \setminus (\{v_0\} \cup N_G(v_0))$, 则 $|N'| = n - s - 1$. 由 s 的定义可知 N' 中的每个点的度数都不超过 s . 因此 G 的总边数 $e(G)$ 满足

$$\begin{aligned} e(G) &\leq d_G(v_0) + \sum_{v \in N'} d_G(v) \\ &\leq s + (n - s - 1)s = (n - s)s \leq \frac{n^2}{4}. \end{aligned}$$

这表明 $\text{ex}(n, C_3) \leq \lfloor \frac{n^2}{4} \rfloor$. 另一方面, 注意完全二部图 $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$ 显然不含三角形, 且边数为 $\lfloor \frac{n^2}{4} \rfloor$, 从而 $\text{ex}(n, C_3) \geq \lfloor \frac{n^2}{4} \rfloor$. 定理得证. \square

进一步, 考虑证明过程中的不等式估计的每一步的取等条件, 容易验证: 具有 n 个顶点 $\lfloor \frac{n^2}{4} \rfloor$ 条边且不含三角形的图只可能是 $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$.

证法 2. 设 $G = (V, E)$ 的顶点数与边数分别为 n, e . 断言: 对任意图 G 都一定成立

$$\sum_{v \in V} d_G(v)^2 = \sum_{\{u, v\} \in E} (d_G(u) + d_G(v)).$$

这是与握手引理 4.103 类似的基本结果, 用“算两次”的方法证明之. 令

$$S := \{(v, e_1, e_2) \in V \times E \times E \mid v \in e_1 \cap e_2\},$$

对 $|S|$ 算两次, 有

$$\begin{aligned} |S| &= \sum_{v \in V} \# \{(e_1, e_2) \in E^2 \mid v \in e_1, v \in e_2\} = \sum_{v \in V} d_G(v)^2, \\ |S| &= \sum_{\{u, v\} \in E} \# \{e_2 \in E \mid u \in e_2 \text{ 或 } v \in e_2\} = \sum_{\{u, v\} \in E} (d_G(u) + d_G(v)), \end{aligned}$$

从而断言得证. 注意到, 如果图 G 不含三角形, 那么 G 的任何一条边的两个顶点都没有公共邻居, 因此对任意 $\{u, v\} \in E$ 都有 $d_G(u) + d_G(v) \leq n$. 因此

$$en \geq \sum_{\{u, v\} \in E} (d_G(u) + d_G(v)) = \sum_{v \in V} d_G(v)^2 \geq \frac{1}{n} \left(\sum_{v \in V} d_G(v) \right)^2 = \frac{4e^2}{n},$$

因此 $e \leq \frac{n^2}{4}$, 得证. □

6.163. Mantel 定理还有很多种不同的漂亮证明. 回忆独立集的概念 (见 4.109), 我们以此给出 Mantel 定理的第三种证明:

证法 3. 设 $G = (V, E)$ 的顶点数与边数分别为 n, e . 设 A 是 G 的一个最大独立集, 即, $A \subseteq V$ 是独立集, 并且 V 的任何比 A 元素个数更多的子集都不是独立集. 如果图 G 不含三角形, 则对任意 $v \in V$, 顶点 v 的邻居集 $N_G(v)$ 一定是独立集, 从而 $d_G(v) \leq |A|$. 记 $B := V \setminus A$, 则由 A 是独立集可知, 图 G 的每一条边都至少由一个顶点位于 B 中, 因此 G 的边数 e 满足

$$e \leq \sum_{v \in B} d_G(v) \leq \sum_{v \in B} |A| = |B| \cdot |A| \leq \frac{(|A| + |B|)^2}{4} = \frac{n^2}{4}.$$

□

6.164.定理.(Moon-Moser, 1962) 已知图 G 的顶点数与边数分别为 v, e , 则 G 中的三角形 (即, 同构于 C_3 的子图) 的个数 $t(G)$ 满足

$$t(G) \geq \frac{4e}{3n} \left(e - \frac{n^2}{4} \right).$$

证明. 记图 G 的顶点集与边集分别为 V, E . 对每一条边 $e = \{u, v\} \in E$, 记 $t(e)$ 为顶点 u, v 的公共邻居数. 注意 $t(e)$ 也恰好是 G 中的以 e 为其中一条边的三角形的个数. 由容斥原理, 注意

$$\begin{aligned} n - 2 &= |V \setminus \{u, v\}| \geq \#((N_G(u) \setminus \{v\}) \cup (N_G(v) \setminus \{u\})) \\ &= (d_G(u) - 1) + (d_G(v) - 1) - t(e), \end{aligned}$$

因此 $d_G(u) + d_G(v) \leq n + t(e)$. 再注意 Mantel 定理 6.162 证法 2 中的某中间结论, 有

$$\sum_{v \in V} d_G(v)^2 = \sum_{e=\{u,v\} \in E} (d_G(u) + d_G(v)) \leq \sum_{e \in E} (n + t(e)) = ne + 3t(G).$$

从而 $ne + 3t(G) \geq \sum_{v \in V} d_G(v)^2 \geq \frac{1}{n} \left(\sum_{v \in V} d_G(v) \right)^2 = \frac{4e^2}{n}$, 解得 $t(G) \geq \frac{4e}{3n} \left(e - \frac{n^2}{4} \right)$. □

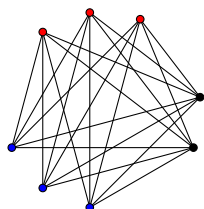
6.2 Turán 定理

我们已经知道 n 个顶点且不含 K_3 的图的最大边数 $\text{ex}(n, K_3) = \lfloor \frac{n^2}{4} \rfloor$. 事实上, 我们其实知道所有 $\text{ex}(n, K_r)$, $r \geq 3$ 的具体值, 这是著名的 **Turán 定理**. 为介绍此定理, 首先将“二部图”的概念推广至一般的“ r -部图”.

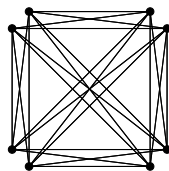
6.165.定义. 对于图 $G = (V, E)$, 如果存在 V 的划分 $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_r$, 使得对任意 $i \in [r]$, $V_i \neq \emptyset$ 并且 V_i 中的任何两点都不相邻, 则称图 G 为 **r -部图**.

这显然是二部图的概念的自然推广: $r = 2$ 的情形就是之前介绍的二部图. 类似可以定义**完全 r -部图**, 大致来说就是“有尽可能多的边”的 r -部图.

如果 $G = (V, E)$ 关于顶点集划分 $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_r$ 是完全 r -部图, 记 $s_i := |V_i|$, 则称 $G \cong K_{s_1, s_2, \dots, s_r}$. (与完全图 K_n , 完全二部图 $K_{s,t}$ 的记号完全类似). 例如



完全 3-部图 $K_{2,3,3}$



完全 4-部图 $K_{2,2,2,2}$

以下关于 r -部图的断言显然成立:

6.166. 引理. 设图 $G = (V, E)$ 是 r -部图, 则 G 不存在同构于 K_{r+1} 的子图.

证明. 记 $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_r$ 是顶点集的相应划分. 则由抽屉原理可知, 图 G 的任意 $r+1$ 个顶点之中至少有两个顶点属于同一个 V_i , 从而这两个顶点不相邻, 从而 G 在这 $r+1$ 个顶点上的限制子图不同构于 K_{r+1} . \square

现在, 考察一类特殊的完全 r -部图:

6.167. 定义. 对于正整数 $n \geq r > 0$, 定义具有 n 个顶点的完全 r -部图

$$T_r(n) := K_{t_1, t_2, \dots, t_r},$$

其中 $\sum_{i=1}^r t_i = n$, 并且 t_1, t_2, \dots, t_r “尽可能地非常接近”, 即, $t_i = \lfloor \frac{n}{r} \rfloor$ 或者 $\lceil \frac{n}{r} \rceil$. 这样的完全 r -部图称为 **Turán 图**.

例如 $T_3(7) \cong K_{2,2,3}$, $T_3(8) \cong K_{2,3,3}$, $T_4(8) \cong K_{2,2,2,2}$, $T_4(9) \cong K_{2,2,2,3}$ 等等. 一般地, 若 $n = tr + s$, 其中 $0 \leq s \leq r-1$, 则容易验证 $T_r(n)$ 的边数

$$\begin{aligned} e(T_r(n)) &= (t+1)^2 \binom{s}{2} + t(t+1)s(r-s) + t^2 \binom{r-s}{2} \\ &= \frac{r-1}{2r} n^2 - \frac{s(r-s)}{2r}. \end{aligned}$$

(留给读者验证). 从而结合引理 6.166 可知, $\text{ex}(n, K_{r+1}) \geq \frac{r-1}{2r} n^2 - \frac{s(r-s)}{2r}$, 其中 s 是 n 除以 r 所得的余数. 事实上, $T_r(n)$ 是最佳的:

6.168.定理.(Turán, 1941) 对于正整数 n, r , 记 s 为 n 除以 r 的余数. 则

$$\text{ex}(n, K_{r+1}) = \frac{r-1}{2r}n^2 - \frac{s(r-s)}{2r}.$$

此外, 若图 G 由 n 个顶点 $\text{ex}(n, r+1)$ 条边并且不含有 K_{r+1} , 则 G 同构于 Turán 图 $T_r(n)$.

证明. 记 $n = tr + s$, 其中 $0 \leq s \leq r-1$. 对 t 归纳. 首先 $t = 0$ 时, $n = s < r$, 显然此时 $\text{ex}(n, T_{r+1}) = e(K_r) = \frac{r(r-1)}{2}$, 易验证符合要求. 一般地, 若该命题对任何 $t' < t$ 都成立, 则对于 $n = tr + s$ 个顶点的图 $G = (V, E)$, 如果 G 不含有 K_{r+1} , 则只需证明 $G = (V, E)$ 的边数不超过 $\frac{r-1}{2r}n^2 - \frac{s(r-s)}{2r}$. 现在取定 G , 不妨在保证 G 不含有 K_{r+1} 的前提下尽可能给 G 增加新的边, 则 G 必含有 K_r (否则, 给 G 任意新增一条边, 所得到的图仍然不含有 K_{r+1}). 取 $H \in \binom{V}{r}$, 使得 $G|_H \cong K_r$, 记 $V' := V \setminus H$, 限制子图 $G' := G|_{V'}$. 则 G' 的顶点个数为 $n - r = (t-1)r + s$. 注意图 G' 显然不含有 K_{r+1} , 从而由归纳假设可知 G' 的边数不超过 $\frac{r-1}{2r}(n-r)^2 - \frac{s(r-s)}{2r}$. 最后再注意到 V' 中的任何一个点在 H 中的邻居个数至多为 $r-1$ (如果 V' 中的某个点与 H 中的所有点都相邻, 则推出 G 含有 K_{r+1} , 矛盾), 综上所述有

$$\begin{aligned} e(G) &\leq e(K_r) + e(G') + (n-r)(r-1) \\ &\leq \frac{r(r-1)}{2} + \frac{r-1}{2r}(n-r)^2 - \frac{s(r-s)}{2r} + (r-1)(n-r) \\ &= \frac{r-1}{2r}n^2 - \frac{s(r-s)}{2r}. \end{aligned}$$

从而证明了 $\text{ex}(n, K_{r+1}) = \frac{r-1}{2r}n^2 - \frac{s(r-s)}{2r}$.

分析上述不等号成立条件, 结合归纳假设可知当不等号取等时, G' 同构于 Turán 图 $T_r(n-r)$, 从而 G' 为完全 r -部图; 并且 G' 中的每个顶点都恰与 H 的 $(r-1)$ 个顶点相邻. 记 $V' = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_r$, 使得 V_i 中的任何两点均不相邻. 记 $H = \{h_1, \dots, h_r\}$. 对每个 $i \in [r]$, 断言存在 $\sigma(i) \in [r]$, 使得 h_i 与 $V_{\sigma(i)}$ 中的所有顶点都不相邻 (否则 G 将含有 K_{r+1}). 容易验证 $\sigma: [r] \rightarrow [r]$ 是一一映射, 记 $V'_i := V_i \sqcup \{h_{\sigma^{-1}(i)}\}$, 则容易验证 G 关于顶点集划分 $V = V'_1 \sqcup V'_2 \sqcup \cdots \sqcup V'_n$ 构成完全 r -部图, 并且同构于 Turán 图 $T_r(n)$. \square

我们也可以从另一个角度来理解 Turán 定理. 对于具有 n 个顶点的图 G , Turán 定理表明当边数“足够多”时, G 就会有“足够大”的完全子图; 等价地, 考察 G 的补图, 可知当边数“足够少”时, G 就会有“足够大”的独立子图, 从而独立数 $\alpha(G)$ (见定义 4.109) 就足够大.

6.169.推论. 对于 n 个顶点的图 $G = (V, E)$, 记 $d_{\text{avg}} := \frac{2e}{n}$ 为图 G 各顶点的平均度数, 其中 $e = e(G)$ 为图 G 的边数, 则成立

$$\alpha(G) \geq \frac{n}{1 + d_{\text{avg}}},$$

其中 $\alpha(G)$ 为图 G 的独立数, 见定义 4.109.

证明. 由 $\alpha(G)$ 的定义可知, 图 G 不含独立子图 $K_{\alpha(G)+1}$, 从而补图 G^c 不含完全子图 $K_{\alpha(G)+1}$, 因此 Turán 定理表明 G^c 的边数 $|E^c| = \binom{n}{2} - e$ 满足

$$\binom{n}{2} - e \leq \text{ex}(n, K_{\alpha(G)+1}) \leq \frac{\alpha(G) - 1}{2\alpha(G)} n^2,$$

解得 $\alpha(G) \geq \frac{n^2}{n + 2e} = \frac{n}{1 + d_{\text{avg}}}$, 得证. □

6.170.推论.(渐近版本 Turán 定理) 若图 G 的顶点个数为 n , 且不含 K_{r+1} , 则

$$e(G) \leq \frac{r-1}{2r} n^2,$$

其中 $e(G)$ 是图 G 的边数.

这是 Turán 定理 6.168 的平凡推论, 但这里要介绍一种不平凡的优美证法, 这种证法建立了 Turán 问题与组合优化之间的联系.

证明. 不妨 $G = (V, E)$ 的顶点集 $V = [n]$. 定义 \mathbb{R}^n 的子集

$$P := \left\{ \mathbf{p} = (p_1, p_2, \dots, p_n)^T \in [0, 1]^n \mid \sum_{i=1}^n p_i = 1 \right\},$$

则每个 $\mathbf{p} \in P$ 自然视为定义在顶点集 V 上的函数 $i \mapsto p_i$. 定义泛函

$$L: P \rightarrow \mathbb{R}$$

$$\mathbf{p} \mapsto L[\mathbf{p}] := \sum_{\{i,j\} \in E} p_i p_j$$

注意 L 是定义在 P 上的连续函数, 而注意 P 是 \mathbb{R}^n 的紧子集, 从而 L 的最大值存在. 在 L 的所有最大值点当中取 \mathbf{p} 使得 \mathbf{p} 的非零分量的个数最少. 固定此 \mathbf{p} , 记 $H := \{i \in [n] = V \mid p_i > 0\}$. 断言: 限制子图 $G|_H$ 是完全图. 这是因为, 假如存在不同的 $i, j \in H$ 使得 i, j 不相邻, 记 $S_i := \sum_{k \in N_G(i)} p_k$,

$S_j := \sum_{k \in N_G(j)} p_k$ (我们回忆, $N_G(i)$ 是指顶点 i 的邻居集), 不妨 $S_i \geq S_j$;

定义 $p'_k := \begin{cases} p_k & k \neq i, j \\ p_i + p_j & k = i \\ 0 & k = j \end{cases}$, 则容易验证 $\mathbf{p}' := (p'_1, \dots, p'_n)^T \in P$, 并且

$L[\mathbf{p}'] \geq L[\mathbf{p}]$, 但 \mathbf{p}' 的非零分量个数严格小于 \mathbf{p} 的非零分量个数, 这与 \mathbf{p} 的选取矛盾, 从而断言得证. 由题设, G 不含 K_{r+1} , 从而 $s := |H| \leq r$. 因此

$$\begin{aligned} L[\mathbf{p}] &= \sum_{\substack{i,j \in H \\ i < j}} p_i p_j = \frac{1}{2} \left[\left(\sum_{i \in H} p_i \right)^2 - \sum_{i \in H} p_i^2 \right] = \frac{1}{2} \left(1 - \sum_{i \in H} p_i^2 \right) \\ &\leq \frac{1}{2} \left(1 - \frac{1}{s} \left(\sum_{i \in H} p_i \right)^2 \right) = \frac{s-1}{2s} \leq \frac{r-1}{2r}. \end{aligned}$$

另一方面, 取 $\mathbf{q} = \left(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n} \right)^T \in P$, 则

$$L[\mathbf{p}] \geq L[\mathbf{q}] = \frac{1}{n^2} e(G),$$

因此图 G 的边数 $e(G) \leq \frac{r-1}{2r} n^2$. □

除了采用“组合优化”方法, 我们还将用**概率方法**给出此定理的又一漂亮证明, 见后文[8.220](#).

6.3 Ajtai-Komlós-Szemerédi 定理

对于具有 n 个顶点的图 G , 朴素的直觉表明, G 的边数 $e = |E|$ 越少, 则独立数 $\alpha(G)$ 越大. 确切地说 (回忆[6.169](#)), 至少可以保证 $\alpha(G) \geq \frac{n}{1 + d_{\text{avg}}}$,

其中 $d_{\text{avg}} = \frac{2e}{n}$ 为所有顶点的平均度数, 一定程度上反映了边数的多少.

若给图 G 附加额外条件: G 不含三角形 (即不存在同构于 K_3 的子图), 则 $\alpha(G)$ 有更好的下界估计. 这是本节所要探讨的内容.

6.171. 定理. (Ajtai-Komlós-Szemerédi, 1980) 记图 $G = (V, E)$ 的顶点数与边数分别为 n, e , 若图 G 不含三角形, 则

$$\alpha(G) \geq 0.01n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}},$$

其中 $d_{\text{avg}} := \frac{2e}{n}$ 为图 G 的各顶点的平均度数.

证明. 对图 G 的顶点个数 n 归纳, 如下:

1. 如果 $n < e^{99}$, 则平均度数 $d_{\text{avg}} < n - 1 < e^{99} - 1$, 此时容易验证

$$0.01 \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} \leq \frac{1}{d_{\text{avg}} + 1},$$

因此由 6.169 可得 $\alpha(G) \geq \frac{1}{d_{\text{avg}} + 1} \geq 0.01 \frac{\ln d_{\text{avg}}}{d_{\text{avg}}}$, 得证.

(特别注意, e 是图 G 的边数, 而 $e \approx 2.71828$ 是自然对数的底.)

接下来不妨假设 $d_{\text{avg}} \geq e^{99} - 1$.

2. 如果存在顶点 $v \in V$, 使得 $d_G(v) \geq 10d_{\text{avg}}$, 则记 $V' := V \setminus \{v\}$, $G' := G|_{V'}$ 为从图 G 中删去顶点 v 及其相连的边所得的子图. 显然 $\alpha(G') \leq \alpha(G)$. 注意 G' 的顶点数 $n' = n - 1$, 顶点平均度数 $d'_{\text{avg}} = \frac{2(e - d_G(v))}{n'}$, 于是

$$\begin{aligned} d'_{\text{avg}} &\leq \frac{2(e - 10d_{\text{avg}})}{n - 1} = \frac{n - 20}{n - 1} d_{\text{avg}}, \\ d'_{\text{avg}} &\geq \frac{2(e - (n - 1))}{n - 1} \geq d_{\text{avg}} - 2 \geq e^{99} - 3 > e, \end{aligned}$$

再注意函数 $f(x) := \frac{\ln x}{x}$ 在 $(e, +\infty)$ 单调递减, 从而

$$n' \frac{\ln d'_{\text{avg}}}{d'_{\text{avg}}} \geq n' \frac{\ln \left(\frac{n-20}{n-1} d_{\text{avg}} \right)}{\frac{n-20}{n-1} d_{\text{avg}}} = \frac{(n-1)^2 \ln d_{\text{avg}}}{n-20} + \frac{(n-1)^2 \ln \frac{n-20}{n-1}}{n-20} \frac{1}{d_{\text{avg}}}$$

$$\begin{aligned}
&= n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} + \frac{1}{(n-20)d_{\text{avg}}} \left[(18n+1) \ln d_{\text{avg}} + (n-1)^2 \ln \left(1 - \frac{19}{n-1} \right) \right] \\
&> n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} + \frac{1}{(n-20)d_{\text{avg}}} [40n - 40(n-1)] > n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}},
\end{aligned}$$

因此由归纳假设可知 $\alpha(G) \geq \alpha(G') \geq n' \frac{\ln d'_{\text{avg}}}{d'_{\text{avg}}} > n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}}$, 得证.

3. 不妨假设 G 的任何顶点的度数都小于 $10d_{\text{avg}}$. 此时, 取顶点 $v \in V$, 使得

$$r(v) := \sum_{w \in N_G(v)} d_G(w) \geq d_{\text{avg}} d_G(v)$$

(回忆习题4.105). 记 $V' := V \setminus (\{v\} \sqcup N_G(v))$, $d := d_G(v)$, 子图 $G' := G|_{V'}$. 则子图 G' 的顶点数 $n' = n - 1 - d$. 注意到, 对于图 G' 的任何独立子集 X , $X \sqcup \{v\}$ 显然是 G 的独立子集, 这表明

$$\alpha(G) \geq \alpha(G') + 1.$$

再注意图 G 不含三角形, 所以易知 G' 的边数 e' 满足

$$e' = e - r(v) \leq e - dd_{\text{avg}}$$

(上式中的等号是关键, 非常妙), 从而 G' 的顶点平均度数 d'_{avg} 满足

$$d'_{\text{avg}} = \frac{2e'}{n'} \leq \frac{n-2d}{n-1-d} d_{\text{avg}}.$$

记函数

$$\varphi(x) := \begin{cases} \frac{\ln x}{x}, & x \geq 233 \\ \frac{x}{x+1}, & 0 < x < 233, \end{cases},$$

则由归纳假设以及推论6.169可知 $\alpha(G') \geq 0.01n'\varphi(d'_{\text{avg}})$. 另一方面, 易知

$$\begin{aligned}
n'\varphi(d'_{\text{avg}}) &\geq n' [\varphi(d_{\text{avg}}) + (d'_{\text{avg}} - d_{\text{avg}})\varphi'(d_{\text{avg}})] \\
&\geq (n-1-d) \left[\frac{\ln d_{\text{avg}}}{d_{\text{avg}}} + \frac{1-d}{n-1-d} \frac{1-\ln d_{\text{avg}}}{d_{\text{avg}}} \right]
\end{aligned}$$

$$\begin{aligned}
&= n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} - 2 \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} + \frac{1-d}{d_{\text{avg}}} \\
&\geq n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} - 2 - 10 > n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}} - 100
\end{aligned}$$

(注意 $d = d_G(v) < 10d_{\text{avg}}$, 以及 $d_{\text{avg}} \geq e^{99} - 1$). 因此

$$\alpha(G) \geq \alpha(G') + 1 \geq 0.01n'\varphi(d'_{\text{avg}}) + 1 \geq 0.01n \frac{\ln d_{\text{avg}}}{d_{\text{avg}}},$$

得证.

综上, 定理证毕. □

6.172. 定理6.171的证明过程中的想法实际上是一个很自然的**贪婪算法**: 对于一个图 G , 如何构造 G 的一个独立集? 任取图 G 的顶点 v , 从 G 中删去顶点 v 及其全部邻居, 所得的图叫做 G' ; 任取 G' 的顶点 v' , 从 G' 中删去顶点 v' 及其全部邻居..... 反复上述操作, 则所有被删去的点显然构成 G 的一个独立子集. 此想法集中体现于定理6.171证明过程第3步.

而其证明过程中的关键技术有两个: 其一是习题4.105, 采用“**概率方法**”证明满足某种特殊性质的顶点的存在性 (后文将详细介绍何为“概率方法”); 其二是注意到可微的凸函数 $f(x)$ 满足不等式 $f(x) \geq f(x_0) + (x - x_0)f'(x)$.

将上述想法与技术理解透彻, 可以提炼出更佳的结果:

6.173.定理.(Shearer, 1983) 记图 $G = (V, E)$ 的顶点数与边数分别为 n, e , 若图 G 不含三角形, 则

$$\alpha(G) \geq nf(d_{\text{avg}}),$$

其中 $d_{\text{avg}} := \frac{2e}{n}$ 为图 G 的各顶点的平均度数, 函数 f 满足

$$f(t) := \frac{t \ln t - t + 1}{(t-1)^2}.$$

证明. 我们希望找到一个合适的函数 $f(x)$, 使得任何不含三角形的图 G 都满足

$$\alpha(G) \geq nf(t),$$

为书写方便, 这里将图的顶点平均度数 $d_{\text{avg}} := \frac{2e}{n}$ 用字母 t 来表示. 此外, 还希望函数 $f(x)$ 是连续可微, 单调递减的凸函数. 目前函数 $f(x)$ 待定, 我们来寻找它. 对于图 G 的顶点 $v \in V$, 记 $d_v := d_G(v)$ 为顶点 v 的度数, 以及

$$Q_v := \sum_{w \in N_G(v)} d(w)$$

为顶点 v 的所有邻居的度数之和. 取定 $v \in V$, 记 $V' := V \setminus (\{v\} \sqcup N_G(v))$, 以及子图 $G' := G|_{V'}$, 则 $\alpha(G) \geq \alpha(G') + 1$, 并且图 G' 的顶点数 n' 与边数 e' 分别为

$$n' = n - 1 - d(v), \quad e' = e - Q(v)$$

(注意第二个等式用到了 G 不含三角形), 从而 G' 的顶点平均度数

$$t' := \frac{2e'}{n'} = \frac{nt - 2Q_v}{n - 1 - d_v}.$$

如果能证明不等式

$$n'f(t') + 1 \geq nf(t)$$

成立, 那么就可以使用数学归纳法 (注意 $\alpha(G) \geq \alpha(G') + 1$ 以及归纳假设 $\alpha(G') \geq n'f(t')$) 来证明此命题. 而

$$\begin{aligned} n'f(t') + 1 &\geq n'[f(t) + (t' - t)f'(t)] + 1 \\ &= nf(t) + [t(d_v + 1) - 2Q_v]f'(t) - (d_v + 1)f(t) + 1 \\ &=: nf(t) + R_v, \end{aligned}$$

其中对于任意顶点 $v \in G$, 记 $R_v := [t(d_v + 1) - 2Q_v]f'(t) - (d_v + 1)f(t) + 1$. 因此, 我们只需要证明图 G 当中存在顶点 v 使得 $R_v \geq 0$. 模仿习题4.105的证明方法, 考察当 v 取遍图 G 的所有顶点时 R_v 的平均值:

$$\begin{aligned} \frac{1}{n} \sum_{v \in V} R_v &= \left(t(t+1) - \frac{2}{n} \sum_{v \in V} d_v^2 \right) f'(t) - (t+1)f(t) + 1 \\ &\geq \left(t(t+1) - \frac{2}{n^2} (2e)^2 \right) f'(t) - (t+1)f(t) + 1 \\ &= t(1-t)f'(t) - (t+1)f(t) + 1 \end{aligned}$$

(注意 $f'(t) \leq 0$). 所以, 如果函数 $f(x)$ 满足微分方程

$$x(1-x)f'(x) - (x+1)f(x) + 1 = 0,$$

那么 R_v 的平均值 $\frac{1}{n} \sum_{v \in V} R_v$ 非负, 从而存在 $v \in V$ 使得 $R_v \geq 0$, 完成证明. 最后, 求解此微分方程可得

$$f(x) = \frac{x \ln x - x + 1}{(x-1)^2},$$

并且容易验证上述特解 $f(x)$ 确实是连续可微, 单调递减的凸函数. □

6.4 Kövari-Sós-Turán 定理

我们已经求出 $\text{ex}(n, K_{r+1})$ 的具体值. 对于更一般的图 G , 具体计算 $\text{ex}(n, G)$ 是极其困难 (甚至不可能) 的, 我们往往退而求其次, 对 $\text{ex}(n, G)$ 作近似估计.

6.174. 定理. (Reiman, 1958) 设 $n \geq 4$, 则 $\text{ex}(n, C_4) \leq \frac{n}{4} (1 + \sqrt{4n-3})$.

证明. 设图 $G = (V, E)$ 具有 n 个顶点, e 条边, 且不含 C_4 . 考虑集合

$$S := \left\{ (v, \{u_1, u_2\}) \in V \times \binom{V}{2} \mid v \text{ 与 } u_1, u_2 \text{ 都相邻} \right\}.$$

对于 G 的任意两个不同顶点 u_1, u_2 , 注意与 u_1, u_2 都相邻的顶点至多有 1 个 (否则 G 含有 C_4). 对 $|S|$ 算两次, 有

$$\begin{aligned} |S| &= \sum_{v \in V} \# \left\{ \{u_1, u_2\} \in \binom{V}{2} \mid v \text{ 与 } u_1, u_2 \text{ 都相邻} \right\} = \sum_{v \in V} \binom{d_G(v)}{2} \\ |S| &= \sum_{\{u_1, u_2\} \in \binom{V}{2}} \# \{v \in V \mid v \text{ 与 } u_1, u_2 \text{ 都相邻}\} \leq \sum_{\{u_1, u_2\} \in \binom{V}{2}} 1 = \binom{n}{2}. \end{aligned}$$

再注意握手引理 4.103, 有 $\sum_{v \in V} d_G(v) = 2e$, 从而整理得

$$\binom{n}{2} \geq \sum_{v \in V} \binom{d_G(v)}{2} = \sum_{v \in V} \frac{d_G(v)(d_G(v)-1)}{2}$$

$$= \frac{1}{2} \sum_{v \in V} d_G^2(v) - e \geq \frac{1}{2n} \left(\sum_{v \in V} d_G(v) \right)^2 - e = \frac{2e^2}{n} - e,$$

解得 $e \leq \frac{n}{4} (1 + \sqrt{4n-3})$. 得证. \square

注意 $C_4 \cong K_{2,2}$. 事实上, 上述方法可以自然推广到一般的 $K_{s,t}$, 得到如下定理:

6.175.定理.(Kövari-Sós-Turán, 1954).

$$\text{ex}(n, K_{s,t}) \leq \frac{1}{2}(t-1)^{\frac{1}{s}} \cdot n^{2-\frac{1}{s}} + \frac{1}{2}(s-1)n.$$

特别地, 当 $n \rightarrow \infty$ 时, $\text{ex}(n, K_{s,t}) \sim O(n^{2-\frac{1}{s}})$.

注意 $K_{s,t} \cong K_{t,s}$, 即 s, t 地位相同, 可以互换.

证明. 设图 $G = (V, E)$ 的顶点数为 n , 边数为 e , 且图 G 不含 $K_{s,t}$. 如果 $e \leq \frac{1}{2}sn$, 则不等式 $e \leq \frac{1}{2}(t-1)^{\frac{1}{s}} \cdot n^{2-\frac{1}{s}} + \frac{1}{2}(s-1)n$ 自动成立. 从而不妨 $e > \frac{1}{2}sn$. 记集合

$$S := \left\{ (v, W) \in V \times \binom{V}{s} \mid \forall w \in W, v \sim_E w \right\}.$$

注意对任意 $W \in \binom{V}{s}$, 与 W 的所有顶点都相邻的顶点至多有 $(t-1)$ 个 (否则 G 含有 $K_{s,t}$), 从而对 $|S|$ 算两次可得

$$|S| = \sum_{v \in V} \# \left\{ W \in \binom{V}{s} \mid \forall w \in W, v \sim_E w \right\} =: \sum_{v \in V} f(d_G(v))$$

$$|S| = \sum_{W \in \binom{V}{s}} \# \{v \in V \mid \forall w \in W, v \sim_E w\} \leq (t-1) \binom{n}{s},$$

其中函数 $f(x) = \begin{cases} 0 & x < s \\ \binom{x}{s} & x \geq s \end{cases}$. 注意 $f(x)$ 是凸函数, 并且当 $x \geq s$ 时有

$f(x) \geq \frac{(x-s+1)^s}{s!}$, 从而由凸函数的 Jensen 不等式可得

$$\frac{t-1}{n} \binom{n}{s} \geq \frac{1}{n} \sum_{v \in V} f(d_G(v)) \geq f\left(\frac{1}{n} \sum_{v \in V} d_G(v)\right)$$

$$= f\left(\frac{2e}{n}\right) \geq \frac{1}{s!} \left(\frac{2e}{n} - s + 1\right)^s,$$

再注意 $\binom{n}{s} \leq \frac{n^s}{s!}$, 从而易知 $e \leq \frac{1}{2}(t-1)^{\frac{1}{s}} \cdot n^{2-\frac{1}{s}} + \frac{1}{2}(s-1)n$, 得证. \square

6.176. 习题. 已知平面 \mathbb{R}^2 上有 n 个不同的点 p_1, p_2, \dots, p_n 以及 n 条不同的直线 $\ell_1, \ell_2, \dots, \ell_n$. 记 $N := \#\{(p_i, \ell_j) \mid i, j \in [n], \text{直线 } \ell_j \text{ 经过点 } p_i\}$. 证明: 存在与 n 无关的常数 $C > 0$, 使得 $N \leq Cn^{\frac{3}{2}}$.

证明. 记 $V := \{p_1, p_2, \dots, p_n; \ell_1, \ell_2, \dots, \ell_n\}$, 以及 $E := \{(p_i, \ell_j) \mid \text{直线 } \ell_j \text{ 经过点 } p_i\}$, 则 $G := (V, E)$ 是具有 $2n$ 个顶点的图, 且 N 恰为 G 的边数. 注意平面上任何两条 (不同的) 直线至多有一个公共点, 且两点确定唯一一条直线, 这说明图 G 不含子图 C_4 . 因此由 6.174 可知

$$N \leq \text{ex}(2n, C_4) \leq \frac{n}{2} (1 + \sqrt{8n-3}),$$

特别地, 可以取 $C = \sqrt{2} + \frac{1}{2}$, 得证. \square

6.177. 习题. 设 p 为奇素数, 考虑有限域 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. 记集合 $V := \mathbb{F}_p^\times \times \mathbb{F}_p$, 其中 $\mathbb{F}_p^\times := \mathbb{F}_p \setminus \{0\}$ 是 \mathbb{F}_p 的乘法单位群. 记集合

$$E := \left\{ \{(a_1, b_1), (a_2, b_2)\} \in \binom{V}{2} \mid a_1 a_2 = b_1 + b_2 \right\},$$

其中的加法与乘法都是有限域 \mathbb{F}_p 中的运算. 则 $G := (V, E)$ 是图. 试证明:

1. 图 G 的边数 e 与顶点数 n 满足关系 $e = \frac{n-1}{2} \left(\sqrt{n + \frac{1}{4}} - \frac{1}{2} \right)$.
2. 图 G 不含 C_4 .
3. 由此推出 $\limsup_{n \rightarrow \infty} \frac{\text{ex}(n, C_4)}{n^{\frac{3}{2}}} = \frac{1}{2}$.

证明. 注意 \mathbb{F}_p^\times 关于 \mathbb{F}_p 的乘法构成 $(p-1)$ 阶循环群, 而 \mathbb{F}_p 关于加法构成 p 阶循环群. 显然 G 的顶点数为 $n = p(p-1)$. 对于顶点 $v = (a, b) \in V$, 容

易验证 $d_G(v) = \begin{cases} p-1 & \text{如果 } b \neq a^2/2 \\ p-2 & \text{如果 } b = a^2/2 \end{cases}$, 因此 G 的边数 $e = \frac{1}{2} \sum_{v \in V} d_G(v) = \frac{1}{2}(p-1)(p^2 - p - 1)$, 因此 $e = \frac{n-1}{2} \left(\sqrt{n + \frac{1}{4}} - \frac{1}{2} \right)$. 图 G 不含 C_4 , 当且仅当 G 的任意两个顶点至多有一个公共邻居. 对 G 中的任意两个顶点 $(a_1, b_1), (a_2, b_2)$, 如果顶点 (a', b') 是它们的公共邻居, 那么 $\begin{cases} a_1 a' = b_1 + b' \\ a_2 a' = b_2 + b' \end{cases}$, 从而只可能 $(a', b') = \left(\frac{b_2 - b_1}{a_2 - a_1}, \frac{a_1 b_2 - a_2 b_1}{a_2 - a_1} \right)$. 这就证明了 G 不含 C_4 . 而 (3) 是本题与 6.174 的显然推论. \square

7. Ramsey 理论

林子大了, 什么鸟都有.

——中国传统民谚

7.1 Ramsey 数 $R(s, t)$

7.178. 例题. 世界上任意 6 个人, 一定有 3 人互相认识或者 3 人互相不认识.

证明. 记 V 为给定的这 6 个人构成的集合, 令 $E := \{(v_1, v_2) \mid v_1, v_2 \text{ 相互认识}\}$, 得到图 $G := (V, E)$. 问题转化为: 任何顶点数为 6 的图都必存在子图 K_3 或者三元独立集. 取定 $v \in V$, 注意 v 与其余 5 个顶点要么相邻要么不相邻, 从而由抽屉原理可知: v 与至少 3 个顶点都相邻, 或者 v 与至少三个顶点都不相邻. 不妨假设前者成立, 设 v 与 u_1, u_2, u_3 都相邻. 如果 u_1, u_2, u_3 之中的某两个顶点相邻, 则这两个顶点与 v 三者两两相邻, 得证; 如果 u_1, u_2, u_3 两两不相邻, 则这它们构成三元独立集, 也得证. 从而证毕. \square

(本题还有另证, 见后文 7.187.)

7.179. 定义. 完全图 K_n 的 k -边染色 是指映射 $f: E \rightarrow [k]$, 其中 E 是 K_n 的边集; 对于边 $e \in E$, $f(e)$ 称为边 e 的颜色. 称 K_n 的子图 G 关于染色 f 是同色的, 如果 G 的所有边的颜色都相同.

注意这里是对图 G 的边进行染色, 而非4.111的顶点染色. 当 $k = 2$ 时, 常习惯称边 $e \in E$ 的颜色为红色或蓝色.

例如7.178显然可以转化为完全图 K_6 的 2-边染色问题. 即, 两人认识则相应的边染红色, 否则染蓝色. 只需证明 K_6 的任何 2-边染色都必存在同色三角形.

7.180.定义. 对于正整数 $s, t \geq 2$, 记


$$R(s, t) := \min \left\{ n \mid \begin{array}{l} K_n \text{ 的任何 2-边染色} \\ \text{都含有红色 } K_s \text{ 或者蓝色 } K_t \end{array} \right\},$$

称为**Ramsey 数**.

粗俗地说, 至少 $R(s, t)$ 个人才能保证其中一定有 s 个人互相认识或者 t 个人互相不认识. 7.178表明 $R(3, 3) \leq 6$. 首先, 易知以下成立

1. $R(s, t) = R(t, s), R(k, 2) = k$.
2. $R(3, 3) = 6$.



证明. (1) 显然成立; 注意 K_5 的 2-边染色  不含同色三角形, 从而 $R(3, 3) > 5$. 再结合7.178可得 $R(3, 3) = 6$. □

7.181.定理.(Ramsey, 1930) 对于 $s, t \geq 2$, 成立 $R(s, t) < \infty$. 具体地说,

$$R(s, t) \leq R(s-1, t) + R(s, t-1),$$

从而特别地有 $R(s, t) \leq \binom{s+t-2}{s-1}$.

证明. 记 $n := R(s-1, t) + R(s, t-1)$, 只需证明 K_n 的任何 2-边染色都存在红色 K_s 或蓝色 K_t . 任取 K_n 的顶点 v , 则其余 $(n-1)$ 个顶点与 v 所连的 $n-1$ 条边要么是红色要么是蓝色, 从而由抽屉原理可知这 $n-1$ 条边中必有 $R(s-1, t)$ 条红边或者 $R(s, t-1)$ 条蓝边. 不妨假设前者成立, 记 $n' := R(s-1, t)$, 设顶点 $v_1, \dots, v_{n'}$ 与 v 相连的边都是红色. 由 $n' = R(s-1, t)$ 的定义可知, $\{v_1, \dots, v_{n'}\}$ 必有红色 K_{s-1} 或蓝色 K_t , 若是前者, 则相应的红色

K_{s-1} 与顶点 v 一起构成红色 K_s ; 若是后者, 则 K_n 存在蓝色 K_t , 得证. 再注意 $R(k, 2) = k = \binom{k+2-2}{k-1}$, 然后用数学归纳法易知

$$R(s, t) \leq R(s-1, t) + R(s, t-1) \leq \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} = \binom{s+t-2}{s-1}.$$

□

此外, 我们还有对 $R(s, t)$ 的稍微精细一点点的上界估计:

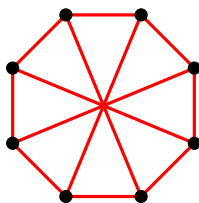
7.182. 引理. 设 $s, t \geq 2$, 如果 $R(s-1, t)$ 与 $R(s, t-1)$ 都是偶数, 则

$$R(s, t) \leq R(s-1, t) + R(s, t-1) - 1.$$

证明. 记 $n := R(s-1, t) + R(s, t-1) - 1$, 则 n 是奇数. 只需证明 K_n 的任何 2-边染色都必含有红色 K_s 或蓝色 K_t . 对 K_n 的每个顶点 v , 记 A_v 为与 v 连接红边的顶点构成的集合, B_v 为与 v 连接蓝边的顶点构成的集合, 则显然 $|A_v| + |B_v| = n - 1 = R(s-1, t) + R(s, t-1) - 2$. 按照 7.181 的证明方式, 只要再考虑如下情况: 任意顶点 v 都满足 $|A_v| = R(s-1, t) - 1$, $|B_v| = R(s, t-1) - 1$. 注意此时 $|A_v|, |B_v|$ 都是奇数. 断言: 这种情况其实并不存在. 这是因为, 若将 K_n 的所有红边都去掉, 则得到的子图有 n (奇数) 个顶点, 且每个顶点的度数都是奇数, 这与握手引理 4.103 矛盾. □

7.183. 推论. $R(3, 4) = 9$.

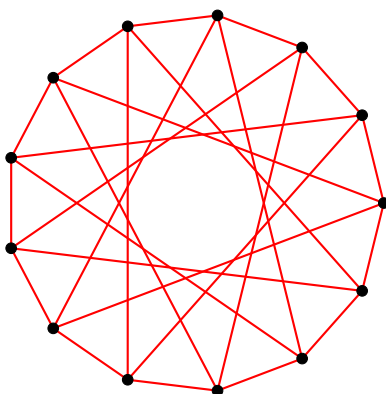
证明. 由于 $R(2, 4) = 4$, $R(3, 3) = 6$ 都是偶数, 从而 $R(3, 4) \leq 4 + 6 - 1 = 9$. 另一方面, 考虑完全图 K_8 的如下 2-边染色 (省略蓝边)



注意此图不含红色 K_3 , 并且不含蓝色 K_4 . 因此 $R(3, 4) > 8$. 得证. □

7.184. 定理. $R(3, 5) = 14$.

证明. 首先, $R(3, 5) \leq R(2, 5) + R(3, 4) = 5 + 9 = 14$.



另一方面, 考虑 K_{13} 的上述染色 (省略蓝边), 可知 $R(3, 5) > 13$. □

7.185.段子. 一般来说, 求出 $R(s, t)$ 的具体值是极端困难的问题. 对于 $R(s, t)$ 的具体值, 除了 $R(2, t)$, $R(3, 3)$, $R(3, 4)$, $R(3, 5)$, 人类目前 (截止 2021 年) 只知道

$$R(3, 6) = 18, \quad R(3, 7) = 23, \quad R(3, 8) = 28, \quad R(3, 9) = 36$$

$$R(4, 4) = 18, \quad R(4, 5) = 25.$$

至于 $R(5, 5)$, $R(6, 6)$, 人类目前最好的结果是

$$43 \leq R(5, 5) \leq 48, \quad 102 \leq R(6, 6) \leq 165$$

人类 (以及各种超级计算机) 做到这种程度真的已经尽力了. 求解 $R(5, 5)$, $R(6, 6)$ 的困难程度可由下述段子来描述:

Erdős asks us to imagine an alien force, vastly more powerful than us, landing on Earth and demanding the value of $R(5, 5)$ or they will destroy our planet. In that case, he claims, we should marshal all our computers and all our mathematicians and attempt to find the value. But suppose, instead, that they ask for $R(6, 6)$. In that case, he believes, we should attempt to destroy the aliens.

— Joel Spencer

7.186. 习题. 给定正整数 ℓ . 证明: 存在 $N > 0$, 使得任何长度 $\geq N$ 的 (有限) 实数列都存在长度为 ℓ 的单调子列.

这是 Erdős-Szekeres 定理 (例题 3.83) 的显然推论, 只需取 $N = (\ell-1)^2 + 1$ 即可. 除此之外, 本题还可以用 Ramsey 理论给出另一种证明:

证明. 断言 $N := R(\ell, \ell)$ 符合要求. 这是因为, 对任何长度为 N 的实数列 a_1, a_2, \dots, a_N , 考虑完全图 $K_N = ([n], E = \binom{[n]}{2})$. 定义 K_N 的 2-边染色如下: 边 $\{i, j\}$ 是红色当且仅当 $(i-j)(a_i - a_j) \geq 0$; 否则染蓝色. 由 $R(\ell, \ell)$ 的定义可知, 图 K_N 必含有红色 K_ℓ 或者蓝色 K_ℓ , 这分别对应于数列 a_1, \dots, a_N 的长度为 ℓ 的单调递增子列或者 (严格) 单调递减子列. 得证. \square

7.187. 习题. (Goodman, 1959) 给定完全图 K_n 的 2-边染色, 记红边的总数为 e , 则 K_n 的同色三角形的个数 T 满足

$$T \geq \binom{n}{3} + \frac{2e^2}{n} - (n-1)e.$$

特别地, $T \geq \binom{n}{3} - \frac{n(n-1)^2}{8}$, 由此推出 $R(3, 3) \leq 6$.

证明. 完全图 $K_n = (V, E)$ 之中总共有 $\binom{n}{3}$ 个三角形. 记 S 为异色三角形的个数, 则 $S + T = \binom{n}{3}$. 对每个顶点 $v \in V$, 记 d_v 为以 v 为端点的红边个数. 则握手引理表明 $2e = \sum_{v \in V} d_v$. 再记

$$t_v := \# \left\{ \{u_1, u_2\} \in \binom{V \setminus \{v\}}{2} \mid \text{边 } u_1v \text{ 与边 } u_2v \text{ 颜色不同} \right\},$$

则显然有 $t_v = d_v(n-1-d_v)$. 此外, 由简单的“算两次”可得异色三角形总数 S 与 t_v 之间的关系: $2S = \sum_{v \in V} t_v$ (留给读者), 因此

$$\begin{aligned} S &= \frac{1}{2} \sum_{v \in V} d_v(n-1-d_v) = (n-1)e - \frac{1}{2} \sum_{v \in V} d_v^2 \\ &\leq (n-1)e - \frac{1}{2n} \left(\sum_{v \in V} d_v \right)^2 = (n-1)e - \frac{2e^2}{n}. \end{aligned}$$

从而 $T = \binom{n}{3} - S \geq \binom{n}{3} + \frac{2e^2}{n} - (n-1)e$. 其余都显然. □

7.2 多色 Ramsey 数 $R_k(s_1, s_2, \dots, s_k)$

现在考虑 Ramsey 数的推广. 推广方式之一是考虑染多种颜色.

7.188. 定义. 设正整数 $k \geq 2, s_1, s_2, \dots, s_k \geq 2$, 记

$$R_k(s_1, s_2, \dots, s_k) := \min \left\{ n \mid \begin{array}{l} \text{完全图 } K_n \text{ 的任何 } k\text{-边染色都一定存在} \\ i \in [k], \text{ 使得 } K_n \text{ 含有 } i\text{-同色完全子图 } K_{s_i} \end{array} \right\}$$

首先依然要验证 $R_k(s_1, \dots, s_k)$ 的存在性.

7.189. 定理. 设正整数 $k \geq 2, s_1, s_2, \dots, s_k \geq 2$, 则

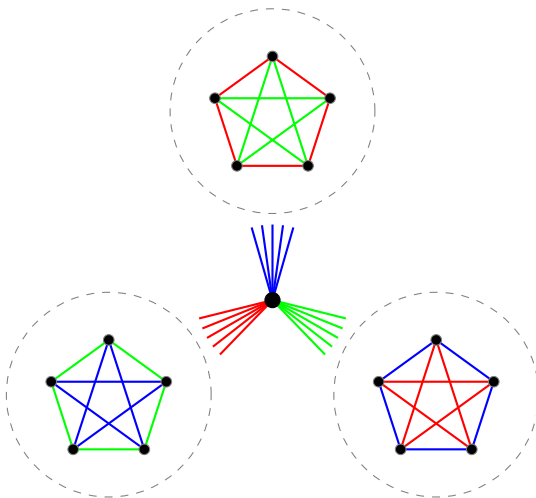
1. 设 σ 是置换群 S_k 中的任何元素, 则有 $R_k(s_1, \dots, s_k) = R_k(s_{\sigma(1)}, \dots, s_{\sigma(k)})$.
2. $R_k(s_1, \dots, s_{k-1}; 2) = R_{k-1}(s_1, \dots, s_{k-1})$.
3. $R_k(s_1, \dots, s_k) \leq \sum_{i=1}^k R_k(s_1, \dots, s_i - 1; \dots, s_k) - (k-2)$.
4. $R_k(s_1, \dots, s_k) \leq R_{k-1}(s_1, \dots, s_{k-2}, R(s_{k-1}, s_k))$.

特别地, $R_k(s_1, \dots, s_k) < \infty$.

证明. (1)(2) 显然成立. 至于 (3), 记 $N := \sum_{i=1}^k R_k(s_1, \dots, s_i - 1; \dots, s_k) - (k-2)$, 任取完全图 K_N 的顶点 v , 考虑以 v 为端点的 $N-1$ 条边的颜色. 用抽屉原理即可, 与 7.181 完全类似, 留给读者练习. 再看 (4), 注意到对于任何 k -边染色, 设想某个色盲将第 $(i-1)$ 种颜色与第 i 种颜色视为同种颜色, 这样就得到了 $(k-1)$ -边染色, 之后顺理成章. □

7.190. 定理. $R_3(3, 3, 3) = 17$.

证明. 首先, $R_3(3, 3, 3) \leq R_3(2, 3, 3) + R_3(3, 2, 3) + R_3(3, 3, 2) - (3 - 2) = 3R_3(3, 3) - 1 = 17$. 下面只需再证明 $R_3(3, 3, 3) > 16$, 即证明存在 K_{16} 的 3-边染色, 使得在此染色下不存在同色三角形. 这样的图是存在的, 比如这样:



如图将 K_{16} 的 16 个顶点分成四组: 中心点以及 3 个 K_5 . 图中任何两个 K_5 之间的边未画出, 请读者按一定规律给这些边染色, 使得此图中没有同色三角形, 从而证明 $R_3(3, 3, 3) > 16$. \square

7.191. 推论. 对任意 $k \geq 3$, 成立 $2^{k+1} < R_k(3, 3, \dots, 3) < 3k!$.

证明. 对 k 归纳. 先证明 $R_k(3, \dots, 3) > 2^{k+1}$. $k = 3$ 时已经证明 $R_3(3, 3, 3) = 17 > 16$. 一般地, 若 $R_k(3, \dots, 3) > 2^{k+1}$, 则存在完全图 $K_{2^{k+1}}$ 的 k -边染色 $\varphi_k: \binom{[2^{k+1}]}{2} \rightarrow [k]$, 使得在该染色下不存在同色三角形. 现在考虑完全图 $K_{2^{k+2}}$, 记其顶点集 $V = \{u_1, \dots, u_{2^{k+1}}; v_1, \dots, v_{2^{k+1}}\}$, 定义 $(k+1)$ -边染色 $\varphi_{k+1}: \binom{V}{2} \rightarrow [k+1]$ 如下:

$$\varphi_{k+1}(\{u_i, u_j\}) = \varphi_{k+1}(\{v_i, v_j\}) = \varphi_k(\{i, j\}), \quad \varphi_{k+1}(\{u_i, v_j\}) = k+1,$$

易知 $K_{2^{k+2}}$ 在 $(k+1)$ -边染色 φ_{k+1} 下不存在同色三角形, 从而 $R_{k+1}(3, \dots, 3) > 2^{k+2}$. 归纳完毕. 再证 $R_k(3, \dots, 3) < 3k!$, $k = 3$ 时已经证明. 一般地, 由 7.189 的 (3) 可知 $R_k(3, \dots, 3) \leq kR_{k-1}(3, \dots, 3)$, 之后归纳易得. \square

7.192. 具体计算 $R(s, t)$ 的值已经是无比恐怖极端困难的问题了, 遑论更多颜色的 $R_k(s_1, \dots, s_k)$ 的具体计算. 其实, $R_k(s_1, \dots, s_k)$ 的存在性就已经能发挥神奇的威力. 例如可以给出 Schur 引理**3.100**的一个更简洁的另证:

Schur 引理**3.100**的另证. 断言 $N := R_k(3, 3, \dots, 3)$ 满足要求. 这是因为, 将 $[N]$ 视为完全图 K_N 的顶点集, 对任意 $\varphi: [N] \rightarrow [k]$, 定义完全图 K_N 的 k -边染色 $\Phi: \binom{[N]}{2} \rightarrow [k]$ 如下:

$$\Phi(\{i, j\}) := \varphi(|i - j|).$$

由 Ramsey 数的定义可知, 完全图 K_N 必存在关于染色 Φ 的同色三角形, 换言之, 存在 $i < j < \ell \in [N]$, 使得 $\varphi(j - i) = \varphi(\ell - j) = \varphi(\ell - i)$. 令 $x := \ell - j$, $y := j - i$, $z := \ell - i$, 则显然 $x + y = z$ 并且 $\varphi(x) = \varphi(y) = \varphi(z)$, 得证. \square

7.3 超图 Ramsey 数 $R^{(r)}(s, t)$

现在考虑 Ramsey 数的另一种推广. 我们回忆, 图 $G = (V, E)$ 的边集 E 是 $\binom{V}{2}$ 的子集, 俗话说就是“一条边连接两个顶点”. 现在, 如果允许“一条边连接多个顶点”, 则可将图的概念推广为:

7.193. 定义. 设 $r \geq 2$ 是正整数. 所谓 **r -超图**是指二元组 $H^{(r)} = (V, E)$, 其中 V 是任意集合, $E \subseteq \binom{V}{r}$.

容易看出, $r = 2$ 时的超图就是通常的图 (定义**4.102**). 与图类似, 有:

- V 称为超图的**顶点集**, 其中元素称为**顶点**.
- E 称为超图的**边集**, 其中元素称为 (r 维)**“超边”**.
- 超图的**子图**, **同构**等概念与通常的图完全类似, 留给读者.
- $K_n^{(r)} := ([n], \binom{[n]}{r})$ 称为 n 阶**完全 r -超图**. 易知这是完全图 K_n 的自然推广.

7.194. 记 $n := |V|$ 为超图 $H^{(r)} = (V, E)$ 的顶点个数, 则超图 $H^{(r)}$ 的边集 E 自然视为集合 $[n]$ 的一个子集族. 反之, 若子集族 $\mathcal{F} \subseteq [n]$ 满足: $\forall A \in \mathcal{F}$,

$|A| = r$, 则集合族 \mathcal{F} 自然视为 r -超图, 使得 \mathcal{F} 是该超图的边集. 也就是说, 超图其实是一种特殊的集合族, 特殊之处在于该集合族中每个集合的元素个数都相同. 将有关概念之间的关系总结如下:

$$\text{图} \xrightarrow{\text{推广}} \text{超图} \xrightarrow{\text{推广}} \text{一般的集族 } \mathcal{F} \subseteq 2^{[n]}$$

极值集合论的一些结论也可以翻译成超图的语言. 例如 Erdős-Ko-Rado 定理 3.96 可重新表述为:

设 $H^{(r)} = (V, E)$ 是顶点个数为 n 的 r -超图, 并且 $r \leq \frac{n}{2}$. 如果 $H^{(r)}$ 的任何两条边都相交 (即, 任意 $e_1, e_2 \in E, e_1 \cap e_2 \neq \emptyset$), 则该超图的边数 $|E| \leq \binom{n-1}{r-1}$.

7.195. 定义. 设 $K_n^{(r)} = (V, E)$ 是完全 r -超图, 则

1. $K_n^{(r)}$ 的 **2-边染色** 是指映射 $\varphi: E \rightarrow \{\text{红}, \text{蓝}\}$. 类似定义 **k -边染色**, 留给读者.
2. 对于正整数 $s, t \geq r$, 记

$$R^{(r)}(s, t) := \min \left\{ n \in \mathbb{Z}_+ \mid \begin{array}{l} K_n^{(r)} \text{ 的任何 2-边染色} \\ \text{都含有红色 } K_s^{(r)} \text{ 或者蓝色 } K_t^{(r)} \end{array} \right\},$$

称为 **r -超图 Ramsey 数**.

读者也可自行定义 “ r -超图 k -边染色 Ramsey 数” $R_k^{(r)}(s_1, s_2, \dots, s_k)$.

7.196. 定理. 设正整数 $r \geq 2, s, t \geq r$, 则成立

1. $R^{(r)}(s, t) = R^{(r)}(t, s), R^{(r)}(s, r) = s$.
2. $R^{(r)}(s, t) \leq R^{(r-1)}(R^{(r)}(s-1, t), R^{(r)}(s, t-1)) + 1$.

特别地, $R^{(r)}(s, t) < \infty$.

证明. (1) 显然成立. 只证 (2). 记 $N := R^{(r-1)}(R^{(r)}(s-1, t), R^{(r)}(s, t-1)) + 1$, 只需证明完全 r -超图 $K_N^{(r)} = (V, E)$ 在任何 2-边染色下都存在红色 $K_s^{(r)}$ 或者蓝色 $K_t^{(r)}$. 现在, 对任意给定的 2-边染色 $\varphi: E \rightarrow \{\text{红}, \text{蓝}\}$, 取定顶点 $v \in V$,

记 $V' := V \setminus \{v\}$, $E' := \binom{V'}{r-1}$, 则 (V', E') 是完全 $(r-1)$ -超图, 同构于 $K_{N-1}^{(r-1)}$. 定义 (V', E') 的 2-边染色 $\psi: E' \rightarrow \{\text{浅红}, \text{浅蓝}\}$ 如下: $\psi(e') := \begin{cases} \text{浅红}, & \text{如果 } \varphi(e' \sqcup \{v\}) = \text{红} \\ \text{浅蓝}, & \text{如果 } \varphi(e' \sqcup \{v\}) = \text{蓝} \end{cases}, \forall e' \in E'$. 则由

$$N-1 = R^{(r-1)}(R^{(r)}(s-1, t), R^{(r)}(s, t-1))$$

的定义可知, (V', E') 在 2-边染色 ψ 下必含有浅红色 $K_{R^{(r)}(s-1, t)}^{(r-1)}$ 或者浅蓝色 $K_{R^{(r)}(s, t-1)}^{(r-1)}$, 不妨假定前者成立. 记该浅红色 $K_{R^{(r)}(s-1, t)}^{(r-1)}$ 的顶点集 $W = \{v_1, \dots, v_M\}$, 其中 $M := R^{(r)}(s-1, t)$, 则 φ 在 $\binom{W}{r}$ 的限制映射自然视为 r -超图 $(W, \binom{W}{r})$ 的 2-边染色. 由 $M = R^{(r)}(s-1, t)$ 的定义可知, $(W, \binom{W}{r})$ 在染色 φ 下必含有红色 $K_{s-1}^{(r)}$ 或者蓝色 $K_t^{(r)}$. 若是后者, 则命题得证; 若是前者, 则由“浅红”的定义易知 W 中任意一个红色 $K_{s-1}^{(r)}$ 与 $v \in V$ 一起构成红色 $K_s^{(r)}$, 得证. \square

7.197.段子. 关于超图 Ramsey 数的具体数值, 除了 $R^{(r)}(s, r) = s$ 的平凡情况, 人类目前 (截止 2021 年) 所知道的**唯一**非平凡的例子是:

$$R^{(3)}(4, 4) = 13.$$

尽管由定理 7.196 以及定理 7.181 可以轻易得到

$$\begin{aligned} R^{(3)}(4, 4) &\leq R(R^{(3)}(3, 4), R^{(3)}(4, 3)) + 1 \\ &= R(4, 4) + 1 \leq R(3, 4) + R(4, 3) + 1 = 9 + 9 + 1 = 19, \end{aligned}$$

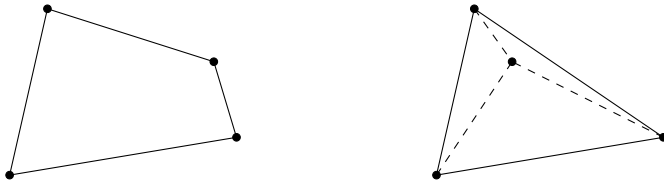
但接下来就异常困难. Giraud 在 1969 年证明了 $R^{(3)}(4, 4) \leq 15$. 同一年, Isbell 构造了完全 3-超图 $K_{12}^{(3)}$ 的 2-边染色, 使得在该染色下该超图不含有同色的 $K_4^{(3)}$, 从而证明 $R^{(3)}(4, 4) > 12$. 多年后, 在计算机的帮助下, Brendan D. McKay, Stanislaw P. Radziszowski 在 1991 年证明了 $R^{(3)}(4, 4) \leq 13$, 因此 $R^{(3)}(4, 4) = 13$.

具体计算 Ramsey 数 (或者退而求其次, 估计 Ramsey 数的取值范围) 对人类来说实在过于困难, 不像是人类能做的题. 能够理解 $R^{(r)}(s, t)$ 的**存在性**

就已经是人类文明前进的一大步了. 下面欣赏一例超图 Ramsey 理论在离散几何中的应用.

7.198. 我们回忆一些平面几何的概念. 平面 \mathbb{R}^2 上的点集 X 处于一般位置是指: X 中任意三点都不共线. 此外, 我们还要回忆, 对于 $X \subseteq \mathbb{R}^2$, 如果连接 X 中任何两个点的线段都包含于 X , 则称 X 是凸集. 包含 X 的所有凸集之交 (即, 包含 X 的最小凸集) 称为 X 的凸包. 如果 $|X| = n$ 且 X 的凸包是平面 n 边形区域, 则称 X 中的 n 个点构成凸 n 边形.

例如 $n = 4$ 时, 如下图所示, 左边的 4 个点构成凸 4 边形; 而右边的 4 个点不构成凸 4 边形, 因为这 4 个点的凸包是三角形.



设 X 是平面上 n 个处于一般位置的 n 个点构成的集合. 由初等平面几何容易证明: X 构成凸 n 边形当且仅当 X 中的任何 4 个点都构成凸 4 边形.

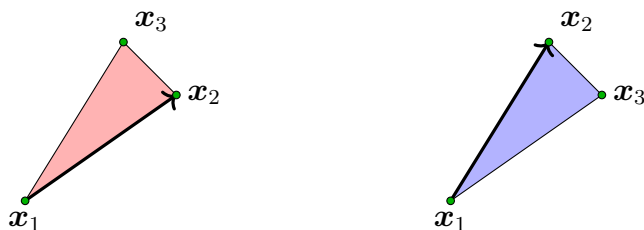
7.199. 定理. (Erdős-Szekeres, 1935) 对任意正整数 n , 都存在正整数 N' , 使得任何 $N \geq N'$ 都满足: 平面 \mathbb{R}^2 上任何 N 个处于一般位置的点当中都存在 n 个点构成凸 n 边形.

粗俗地说, 上述 Erdős-Szekeres 定理断言: 只要平面上的点的个数足够多, 总能从中找到构成凸 n 边形的 n 个点.

证明. 断言 $N := R^{(3)}(n, n)$ 符合要求, 即平面上的任何 N 个处于一般位置的点当中都能找到构成凸 n 边形的 n 个点. 现在, 设 $V : \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N\} \subseteq \mathbb{R}^2$ 处于一般位置. 将 V 视为完全 3-超图 $K_N^{(3)}$ 的顶点集. 接下来特别选取边集 $E := \binom{N}{3}$ 的某个 2-边染色.

对任意的超边 $e = \{\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k\} \in E (i < j < k)$, 注意直线 $\mathbf{x}_i\mathbf{x}_j$ 将平面分为两部分, 下标最大的点 \mathbf{x}_k 位于这两部分之一. 从下标最小的点 \mathbf{x}_i 出发, 沿着射线 $\overrightarrow{\mathbf{x}_i\mathbf{x}_j}$ 前进, 如果下标最大的点 \mathbf{x}_k 在前进方向的左侧, 则规定超边 $e = \{\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k\}$ 的颜色为红; 否则规定 e 的颜色为蓝. 这就给出了

$K_N^{(3)} = (V, E)$ 的一个 2-边染色.



例如在左图中 x_3 在 $\overrightarrow{x_1x_2}$ 的左侧, 从而超边 $\{x_1, x_2, x_3\}$ 被染成红色; 而右图中的 $\{x_1, x_2, x_3\}$ 被染成蓝色.

从而由 Ramsey 数 $N = R^{(3)}(n, n)$ 的定义可知, 在上述染色下, 必能从 V 中选出 n 个点, 使得由这 n 个点构成的任何三元组的颜色都是红色或都是蓝色. 不妨前者成立, 记 $X := \{x_{i_1}, x_{i_2}, \dots, x_{i_n}\} \subseteq V$ 使得以 X 为端点的任何超边均为红色, 其中下标 $i_1 < i_2 < \dots < i_n$. 容易验证, 按下标从小到大顺序在平面上依次连接这些点所得到折线段 $x_1x_2 \cdots x_k$ 围成凸 n 边形 (也可以直接验证 X 中的任何 4 点都构成凸 4 边形, 从而推出 X 构成凸 n 边形), 得证. \square

7.4 练习: Ramsey 数 $R(3, n)$ 的渐近估计

在 Ramsey 数 $R(s, t)$ 的研究中, 人们除了关心 s, t 较小时 $R(s, t)$ 的具体值, 也关心当 s, t 很大时 $R(s, t)$ 的渐近估计, 其中如下两个问题格外重要:

- 当 $n \rightarrow \infty$ 时, $R(3, n)$ 的增长速度如何?
- 当 $n \rightarrow \infty$ 时, $R(n, n)$ 的增长速度如何?

我们将在本节以及后续章节初步探讨上述问题, 逐步给出 $R(3, n)$ 与 $R(n, n)$ 的越来越精确的上下界估计. 本节给出 $R(3, n)$ 的上, 下界的初步估计. 先从一个简单习题说起:

7.200. 习题. 对于正整数 $n \geq 3$, 成立 $2n - 2 < R(3, n) \leq \binom{n+1}{2}$.

证明. $R(3, n) \leq \binom{n+1}{2}$ 是定理 7.181 的直接推论. 另一方面, 取完全图 K_{2n-2} 的顶点集 V 的划分 $V = V_1 \sqcup V_2$, 使得 $|V_1| = |V_2| = n - 1$, 然后

考虑 K_{2n-2} 的如下 2-边染色: 若该边的两顶点都属于 V_1 或都属于 V_2 , 则该边染蓝色; 若该边的一个顶点属于 V_1 而另一个顶点属于 V_2 , 则该边染红色. 经过上述染色后的 K_{2n-2} 显然不含红色 K_3 , 也显然不含蓝色 K_n . 这就说明了 $R(3, n) > 2n - 2$. \square

特别地, 当 $n \rightarrow \infty$ 时, $n \lesssim R(3, n) \lesssim n^2$.

其实 $R(3, n)$ 的上界可以继续改进:

7.201.定理.(Shearer, 1983) 对于充分大的正整数 n , 成立

$$R(3, n) \leq (1 + o(1)) \frac{n^2}{\ln n}.$$

证明. 这其实是定理6.173的推论. 依然记函数 $f(t) := \frac{t \ln t - t + 1}{(t - 1)^2}$. 任意给定 $\varepsilon > 0$, 断言: 当正整数 n 充分大时, 对于任何顶点个数为 $N := \left\lceil (1 + \varepsilon) \frac{n^2}{\ln n} \right\rceil$ 的图 G , 如果 G 不含三角形, 则 G 的独立数 $\alpha(G) \geq n$.

如果上述断言成立, 则对任意 $\varepsilon > 0$, 当 n 足够大时,

$$R(3, n) \leq N < (1 + 2\varepsilon) \frac{n^2}{\ln n}.$$

从而由 ε 的任意性可知定理得证. 下面只需证明断言.

对于具有 $N := \left\lceil (1 + \varepsilon) \frac{n^2}{\ln n} \right\rceil$ 个顶点且不含三角形的图 G , 记 $t := \frac{2e}{n}$ 为图 G 的顶点平均度数, 则首先注意到 $t \leq \alpha(G)$. 这是因为, 注意图 G 不含三角形, 所以对于任何顶点 v , 邻居集 $N_G(v)$ 都是独立集, 从而 $d_G(v) \leq \alpha(G)$ 对任意顶点 v 成立. 再由定理6.173, 可知当 n 充分大时,

$$\begin{aligned} \alpha(G) &\geq N f(t) \geq (1 + \varepsilon) \frac{n^2}{\ln n} f(\alpha(G)) \\ &\geq (1 + \varepsilon) \frac{n^2}{\ln n} \left(\frac{\ln \alpha(G)}{\alpha(G)} - \frac{1}{\alpha(G) - 1} \right) \geq \frac{n^2}{\ln n} \cdot \frac{\ln \alpha(G)}{\alpha(G)} \end{aligned}$$

(首先要验证当 $n \rightarrow \infty$ 时 $\alpha(G) \rightarrow \infty$, 这留给读者), 所以有

$$\frac{\alpha(G)^2}{\ln \alpha(G)} \geq \frac{n^2}{\ln n},$$

因此由函数 $\varphi(x) := \frac{x^2}{\ln x}$ 的单调性可得 $\alpha(G) \geq n$, 得证. \square

接下来开始研究 $R(3, n)$ 的下界.

7.202.定理.(Erdős, 1957) Ramsey 数 $R(3, n)$ 满足

$$\lim_{n \rightarrow \infty} \frac{R(3, n)}{n} = \infty.$$

这显然是比 $R(3, n) > 2n - 2$ 更好的下界估计.

证明. 任意取定正整数 k . 对于实数 $r > 0$, 定义图 $G = (V, E)$ 如下:

- 顶点集 $V := \{\mathbf{v} \in \mathbb{Z}^k \subseteq \mathbb{R}^k \mid \|\mathbf{v}\| \leq r\}$,
- 边集 E : 两顶点 $\mathbf{v}_1, \mathbf{v}_2$ 有边两连 $\Leftrightarrow \|\mathbf{v}_1 - \mathbf{v}_2\| > \sqrt{3}r$.

(若图 G 两顶点相邻, 则视它们被红边相连; 若两顶点不相邻, 则视它们被蓝边相连. 从而自然将图 G 视为完全图 $K_{|V|}$ 的 2-边染色). 易知当 r 足够大时, 图 G 的顶点个数 $|V|$ 约等于 \mathbb{R}^k 中半径为 r 的球的体积 $a_k r^k$, 其中 $a_k = \frac{\pi^{\frac{k}{2}}}{\Gamma(\frac{k}{2} + 1)}$. 特别地, 当 r 足够大时, $|V| > \frac{1}{2}a_k r^k$.

断言: 图 G 不含三角形 (相应地, 完全图 $K_{|V|}$ 不含红色 K_3). 这是因为, 如果存在 $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$ 使得它们两两相邻, 则

$$\|\mathbf{a} - \mathbf{b}\| > \sqrt{3}r, \quad \|\mathbf{b} - \mathbf{c}\| > \sqrt{3}r, \quad \|\mathbf{c} - \mathbf{a}\| > \sqrt{3}r,$$

$$\text{则 } \begin{cases} \|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 - 2\mathbf{a} \cdot \mathbf{b} > 3r^2 \\ \|\mathbf{b}\|^2 + \|\mathbf{c}\|^2 - 2\mathbf{b} \cdot \mathbf{c} > 3r^2 \\ \|\mathbf{c}\|^2 + \|\mathbf{a}\|^2 - 2\mathbf{c} \cdot \mathbf{a} > 3r^2 \end{cases}, \text{ 三式相加并整理得}$$

$$\begin{aligned} \|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 + \|\mathbf{c}\|^2 &> \frac{9}{2}r^2 + (\mathbf{a} \cdot \mathbf{b} + \mathbf{b} \cdot \mathbf{c} + \mathbf{c} \cdot \mathbf{a}) \\ &\geq \frac{9}{2}r^2 - \frac{1}{2}(\|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 + \|\mathbf{c}\|^2), \end{aligned}$$

因此

$$\|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 + \|\mathbf{c}\|^2 > 3r^2,$$

这与 $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$ 产生矛盾. 断言得证.

接下来研究图 G 的独立子图 (换言之, 完全图 $K_{|V|}$ 的蓝色完全子图). 对于顶点集 V 的子集 V' , 如果 V' 中的任何两点都不相邻, 即在 \mathbb{R}^k 中的欧氏

距离 $\leq \sqrt{3}r$, 则显然 V' 能被 \mathbb{R}^k 中的某个直径为 $\sqrt{3}r$, 即半径为 $\frac{\sqrt{3}}{2}r$ 的球所覆盖. 因此当 r 足够大时, $|V'| < 2a_k \left(\frac{\sqrt{3}}{2}r\right)^k - 1$. 这表明, 如果正整数 n 满足 $n \geq 2a_k \left(\frac{\sqrt{3}}{2}r\right)^k$, 则图 G 不含 n 元独立子集 (相应地, $K_{|V|}$ 不含蓝色 K_n). 此时有 $R(3, n) > |V|$.

现在, 对于充分大的正整数 n , 取正实数 r 使得 $n = 2a_k \left(\frac{\sqrt{3}}{2}r\right)^k$, 则

$$R(3, n) > |V| > \frac{1}{2}a_k r^k = \frac{1}{4} \left(\frac{2\sqrt{3}}{3}\right)^k n.$$

最后注意 k 的任意性, 令 $k \rightarrow \infty$ 即得证. □

上述方法可以继续改进, “抠得更仔细一些”, 就能得到:

7.203. 定理. (Erdős, 1957) 存在正数 $\varepsilon > 0$, 使得当 n 充分大时成立

$$R(3, n) > n^{1+\varepsilon}.$$

例如, 可以取 $\varepsilon = 0.01$.

证明. 取定正整数 k , 图 $G = G(V, E)$ 的定义同定理 7.202, 不过在这里我们取 $r = 100\sqrt{k}$ (这里的 100 可以换成其它足够大的正数). 则图 G 不含三角形; 并且如果 $V' \subseteq V$ 是 G 的独立集, 则 V' 包含于 \mathbb{R}^k 中的某个半径为 $\frac{\sqrt{3}}{2}r$ 的闭球.

现在来估计顶点个数 $|V|$. 对于格点 $\mathbf{v} = (v_1, \dots, v_k) \in V \subseteq \mathbb{Z}^k$, 考虑以 \mathbf{v} 为中心的单位立方体 $I_{\mathbf{v}} := \left\{ \mathbf{u} = (u_1, \dots, u_k) \in \mathbb{R}^k \mid |u_i - v_i| < \frac{1}{2}, i = 1, \dots, k \right\}$. 注意 $I_{\mathbf{v}}$ 是边长为 1 的 k 维立方体, 其直径 (斜对角线长) 为 \sqrt{k} ; 此外 $\{I_{\mathbf{v}} \mid \mathbf{v} \in V\}$ 两两不交, 从而 $|V| = \text{Vol} \left(\bigcup_{\mathbf{v} \in V} I_{\mathbf{v}} \right)$, 其中 Vol 是欧氏空间 \mathbb{R}^k 通常定义的体积 (测度). 容易验证 $B(\mathbf{0}, r - \sqrt{k}) \subseteq \bigcup_{\mathbf{v} \in V} I_{\mathbf{v}}$ (其中 $B(\mathbf{v}, R)$ 是以 \mathbf{v} 为球心, R

为半径的开球), 因此

$$\begin{aligned} |V| &= \text{Vol} \left(\bigcup_{v \in V} I_v \right) \geq \text{Vol} \left(B(\mathbf{0}, r - \sqrt{k}) \right) \\ &= (99\sqrt{k})^k \frac{\pi^{\frac{k}{2}}}{\Gamma(\frac{k}{2} + 1)} \geq \frac{2}{k} \left(99\sqrt{2\pi e} \right)^k, \end{aligned}$$

其中注意到, 不等式 $\Gamma(u+1) \leq \frac{u^{u+1}}{e^u}$ 在 u 很大时成立.

对于 $\mathbf{u} \in \mathbb{R}^k$, 记闭球 $B' := \overline{B(\mathbf{u}, r')}$, 其中 $r' = \frac{\sqrt{3}}{2}r$. 记 $V' = V \cap B' \subseteq \mathbb{Z}^k$, 容易验证 $\bigcup_{v \in V'} I_v \subseteq B(\mathbf{u}, r' + \sqrt{k})$, 从而

$$\begin{aligned} |V'| &= \text{Vol} \left(\bigcup_{v \in V'} I_v \right) \leq \text{Vol} \left(B(\mathbf{u}, r' + \sqrt{k}) \right) \\ &= \left[\left(\frac{100\sqrt{3}}{2} + 1 \right) \sqrt{k} \right]^k \frac{\pi^{\frac{k}{2}}}{\Gamma(\frac{k}{2} + 1)} \leq \left(90\sqrt{2\pi e} \right)^k, \end{aligned}$$

其中注意到, 不等式 $\Gamma(u+1) \geq \frac{u^u}{e^u}$ 在 u 很大时成立.

综上可知, 对于正整数 n, k , 如果 $n > \left(90\sqrt{2\pi e} \right)^k$, 则 $R(3, n) > \frac{2}{k} \left(99\sqrt{2\pi e} \right)^k$. 现在, 对于充分大的正整数 n , 取正整数 k 使得

$$\left(90\sqrt{2\pi e} \right)^k < n, \quad \left(90\sqrt{2\pi e} \right)^{k+1} \geq n,$$

于是有

$$\begin{aligned} R(3, n) &> \frac{2}{k} \left(99\sqrt{2\pi e} \right)^k > \frac{2 \ln(90\sqrt{2\pi e})}{\ln n} \cdot \frac{1}{99\sqrt{2\pi e}} \left(99\sqrt{2\pi e} \right)^{k+1} \\ &= \frac{C}{\ln n} \left[\left(90\sqrt{2\pi e} \right)^{k+1} \right]^\lambda \geq \frac{C}{\ln n} n^\lambda > n^{1.01} \quad (n \rightarrow \infty), \end{aligned}$$

其中常数 $C := \frac{2 \ln(90\sqrt{2\pi e})}{99\sqrt{2\pi e}}$, $\lambda := \frac{\ln(99\sqrt{2\pi e})}{\ln(90\sqrt{2\pi e})} \approx 1.016 > 1.01$, 得证. \square

8. 概率方法

概率论的知识和方法可以应用到组合数学中, 并产生神奇的效果. 概率方法最早由数学家 Erdős 发明, 被用于估计 Ramsey 数 $R(s, s)$ 的下界 (回忆 7.180).

8.204. 这里默认读者了解概率论的基本概念: 概率空间 Ω , σ -代数 \mathcal{F} 以及概率测度 \mathbb{P} . 而在组合数学当中, 与之前一样, 我们的研究对象往往是有限集. 我们特别关心概率空间 Ω 是有限集的情形. 此时取 σ -代数 $\mathcal{F} = 2^\Omega$, 概率测度 \mathbb{P} 自然视为函数 $\mathbb{P}: \Omega \rightarrow [0, 1]$, 并且 $\sum_{\omega \in \Omega} \mathbb{P}(\omega) = 1$. 概率空间 Ω 的子集 X 称为事件, $\mathbb{P}(X) := \int_X d\mathbb{P} = \sum_{\omega \in X} \mathbb{P}(\omega)$ 称为事件 X 的概率.

8.1 概率的次可加性

8.205. 给定概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$, 以及事件 $A, B \in \mathcal{F}$, 则众所周知成立

$$\mathbb{P}(A \cup B) \leq \mathbb{P}(A) + \mathbb{P}(B),$$

这个性质称为概率的次可加性. (一般地, 上式可以推广至可数无限多个事件, 这是概率论的基本原理. 但我们暂时只关心 Ω 是有限集的情况, 此时至多只有有限个不同的事件, 从而可以暂时不管“无限”的情形.)

概率方法最早被用于研究 Ramsey 数的下界估计, 如下:

8.206. 性质. (Erdős, 1947) 如果正整数 $n > s > 0$ 满足 $\binom{n}{s} 2^{1-\binom{s}{2}} < 1$, 则 Ramsey 数 $R(s, s) > n$.

证明. 考虑 n 个顶点的完全图 $G \cong K_n$, 不妨 G 的顶点集记 $V = [n]$, 边集 $E = \binom{[n]}{2}$. 将 G 的每条边都以 $\frac{1}{2}$ 的概率随机染为红色或蓝色, 各条边的染色彼此独立. 考虑事件 X : 图 G 含有同色的 K_s . 如果事件 X 的概率严格小于 1, 即事件 X 可能不发生, 则表明确实存在 K_n 的 2-边染色, 使得该图在此染色之下不含有同色 K_s , 从而推出 $R(s, s) > n$. 于是只需证明 $\mathbb{P}(X) < 1$. 对于每个 $S \in \binom{V}{s}$, 定义事件 X_S : $G|_S$ 是同色完全图, 则易知 $\mathbb{P}(X_S) = 2^{1-\binom{s}{2}}$.

再注意到 $X = \bigcup_{S \in \binom{V}{s}} X_S$, 因此由概率的次可加性得

$$\mathbb{P}(X) = \mathbb{P}\left(\bigcup_{S \in \binom{V}{s}} X_S\right) \leq \sum_{S \in \binom{V}{s}} \mathbb{P}(X_S) = \binom{n}{s} 2^{1-\binom{s}{2}} < 1,$$

从而得证. □

8.207. 推论. 当正整数 $s \rightarrow \infty$ 时, 成立

$$R(s, s) > \left(\frac{1}{e\sqrt{2}} + o(1)\right) s \cdot 2^{s/2}.$$

证明. 对于任意正整数 $n > s$, 注意 $\binom{n}{s} < \frac{n^s}{s!}$, 从而容易验证 $n := (s!)^{1/s} \cdot 2^{\frac{s-1}{2} - \frac{1}{s}}$ 满足 $\binom{n}{s} 2^{1-\binom{s}{2}} < 1$, 从而 $R(s, s) > (s!)^{1/s} 2^{\frac{s-1}{2} - \frac{1}{s}}$. 再由众所周知的 Stirling 公式

$$s! \sim \sqrt{2\pi s} \left(\frac{s}{e}\right)^s, \quad s \rightarrow \infty$$

可知 $(s!)^{1/s} = \frac{s}{e} + o(1)$. 因此当 $s \rightarrow \infty$ 时,

$$R(s, s) > (s!)^{1/s} 2^{\frac{s-1}{2} - \frac{1}{s}} = \left(\frac{1}{e\sqrt{2}} + o(1)\right) s \cdot 2^{s/2}.$$

□

8.208. 与上述将图的边随机染色的想法类似, 我们考虑这样的概率模型: 给定顶点集 $V = [n]$, 其中任何两个顶点之间有边相邻的概率都为 $p \in [0, 1]$, 并且它们彼此独立. 如此随机决定任何两点之间是否有边相连, 所得到的图称为**随机图**, 记作 $G(n, p)$, 视为取值于图的随机变量. (其实“随机图”有很多种不同的概率模型, 这里介绍的只是其中一种). 我们通常默认 $p = \frac{1}{2}$, 即对于任意两个顶点, 它们之间有边相连的概率为 $\frac{1}{2}$.

设 A 是关于图的某个性质, 即, 对任意一个图 $G = (V, E)$, 要么 G 满足性质 A , 要么不满足. 则对于给定的 n , 在随机图 $G(n, \frac{1}{2})$ 意义下, A 自然视为一个随机事件; 并且易知事件 A 的概率

$$\mathbb{P}_n(A) = \frac{\#\{E \subseteq 2^{[n]} \mid \text{图 } G := ([n], E) \text{ 满足性质 } A\}}{2^{\binom{n}{2}}}.$$

设 A 是图的某个性质, 对于随机图 $G(n, p)$, 如果

$$\lim_{n \rightarrow \infty} \mathbb{P}_n(A) = 1,$$

则称随机图 $G(n, p)$ **几乎一定** 满足性质 A .

8.209.例题. 随机图 $G(n, \frac{1}{2})$ 几乎一定不是二部图.

证明. 考虑性质 A : 图 G 是二部图. 则只需证明 $\lim_{n \rightarrow \infty} \mathbb{P}_n(A) = 0$. 我们回忆, 如果 $G = (V, E)$ 是二部图, 则存在 V 的划分 $V = V_1 \sqcup V_2$ 使得 V_i 中的任何两点都不相邻, $\forall i = 1, 2$. 现在, 给定 n , 设图 G 的顶点集 $V = [n]$. 对于 V 的任何子集 S , 记 $s := |S|$, 考虑事件 A_S : “ S 中的任何两个顶点都不相邻, 且 $V \setminus S$ 中的任何两个顶点都不相邻”. 则显然 $A = \bigcup_{S \subseteq V} A_S$, 因此

$$\begin{aligned} \mathbb{P}_n(A) &= \mathbb{P}_n\left(\bigcup_{S \subseteq V} A_S\right) \leq \sum_{S \subseteq V} \mathbb{P}_n(A_S) = \sum_{S \subseteq V} 2^{-\binom{s}{2} - \binom{n-s}{2}} \\ &= \sum_{S \subseteq V} 2^{-(s^2 - ns + n^2 + \frac{n}{2})} \leq \sum_{S \subseteq V} 2^{-\frac{3}{4}n^2 + \frac{n}{2}} = 2^{-\frac{3}{4}n^2 + \frac{3}{2}n} \rightarrow 0 \quad (n \rightarrow \infty), \end{aligned}$$

从而得证. □

众所周知, 图的概念有很多种不同版本的推广, 拓展 (比如之前介绍的“超图”), 其中有**有向图**格外重要. 粗略地说, **有向图**就是“给通常的图的每一条边赋以方向”.

8.210.定义. 所谓**有向图**, 是指二元组 $\vec{G} = (V, A)$, 其中 V 是非空集合, $A \subseteq V \times V$; 并且满足: 若 $(v_1, v_2) \in A$, 则 $(v_2, v_1) \notin A$.

- V 称为有向图的**顶点集**, 其中元素称为**顶点**; 而 A 中的元素称为**有向边**, 或者**弧**. 对于有向边 $a = (v_1, v_2) \in A$, 称 v_1 是有向边 a 的**始点**, v_2 是有向边 a 的**终点**.

- 我们习惯将 $(v_1, v_2) \in A$ 记作 $v_1 \rightarrow_A v_2$ 或者 $v_2 \leftarrow_A v_1$ (箭头的下标 A 可省略), 直观地表示为从 v_1 指向 v_2 的箭头.
- 从有向图的定义可以推出, 对任意 $v \in V$, 一定有 $(v, v) \notin A$, 即不允许出现“自己指向自己的箭头”.
- 对于有向图 $\vec{G} = (V, A)$, 记 $E := \left\{ \{v_1, v_2\} \in \binom{V}{2} \mid v_1 \rightarrow_A v_2 \text{ 或 } v_2 \rightarrow_A v_1 \right\}$, 则称图 $G := (V, E)$ 是有向图 \vec{G} 的**底图**. (粗俗地说, 把有向边的“方向”都忘记, 就得到底图.)
- 如果有向图 \vec{G} 的底图同构于完全图, 则称 \vec{G} 为**竞赛图**.

(设想 n 个人参加某项循环赛, 任何两人之间都比赛一场, 如果 a 战胜 b , 则记作从 a 指向 b 的箭头. 这样就得到一个有向图, 它的底图是完全图 K_n . 可见**竞赛图**可用来描述参赛选手之间的相互输赢, 这也是“竞赛图”名称的由来.)

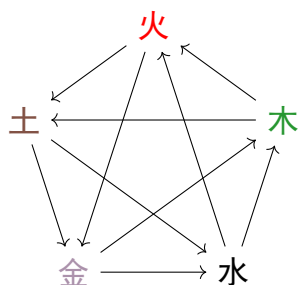


图: 五行相生相克, 视为竞赛图

8.211.例题.(Erdős, 1963). 设 $\vec{G} = (V, A)$ 是竞赛图, k 是正整数. 如果对任意 $H \in \binom{V}{k}$, 都存在顶点 $v \in V \setminus H$, 使得 $v \rightarrow h$ 对任意 $h \in H$ 都成立, 则称竞赛图 \vec{G} 具有性质 S_k . 证明: 如果正整数 n 满足

$$\binom{n}{k} \left(1 - \frac{1}{2^k}\right)^{n-k} < 1,$$

则存在 n 个顶点且满足性质 S_k 的竞赛图.

注意 $\binom{n}{k}$ 随 n 增加而多项式增长, $\left(1 - \frac{1}{2^k}\right)^{n-k}$ 随 n 增加而指数衰减, 因此当 n 足够大时, 题设条件一定满足.

证明. 将完全图 K_n 的每一条边都以 $\frac{1}{2}$ 的概率随机赋以方向, 并且任何两条边的方向选取都彼此独立, 从而得到随机竞赛图 $\vec{G}(n)$. 记事件 B : “竞赛图 \vec{G} 不满足性质 S_k ”, 则只需证明 $\mathbb{P}_n(B) < 1$.

记 V 为随机竞赛图 $G(n)$ 的顶点集, $|V| = n$. 对于每个 $H \in \binom{V}{k}$, 记事件 B_H : “对任意顶点 $v \in V \setminus H$, 存在顶点 $h \in H$, 使得 $h \rightarrow v$ ”. 则易知 $B = \bigcup_{H \in \binom{V}{k}} B_H$. 而容易计算事件 B_H 的概率 $\mathbb{P}(B_H) = \left(1 - \frac{1}{2^k}\right)^{n-k}$, 因此

$$\mathbb{P}(B) \leq \sum_{H \in \binom{V}{k}} \mathbb{P}(B_H) = \binom{n}{k} \left(1 - \frac{1}{2^k}\right)^{n-k} < 1,$$

从而得证. □

(我们其实证明了随机竞赛图 $\vec{G}(n)$ 几乎一定满足性质 S_k , 这里“几乎一定”的含义与 8.208 完全类似, 留给读者补充.)

图论中还有一类问题格外重要, 即“超图染色问题”.

8.212. 对于图 $G(V, E)$, 我们回忆染色数 $\chi(G)$ 的概念 (见 4.111). 大致来说, 将图的顶点染色 (并非 Ramsey 问题的边染色), 并要求相邻的顶点的颜色不相同, $\chi(G)$ 是符合上述要求染色的颜色种类数的最小值. 这个染色问题可以推广至超图 (见 7.193). 我们回忆, r -超图 $H^{(r)} = (V, E)$ 的“超边” $e \in E$ 是顶点集 V 的 r 元子集, 换言之, “每一条超边都有 k 个端点”. 图的 (顶点) 染色问题可自然推广到超图, 如下:

8.213. 定义. 设 $H^{(r)} = (V, E)$ 是 r -超图.

1. 对于正整数 k , 如果存在映射 $\varphi: V \rightarrow [k]$, 使得对任意 $e \in E$,

$$\#\{\varphi(v) \mid v \in e\} > 1,$$

则称超图 $H^{(r)}$ 是可 k -染色的. 此时, 映射 φ 称为超图 $H^{(r)}$ 的与 E 相容的 k -染色. (这是顶点染色, 而非 Ramesy 问题中的 k -边染色).

2. 记 $\chi(H^{(r)}) := \min \{k \geq 1 \mid H^{(r)} \text{ 可 } k\text{-染色}\}$, 称为超图 $H^{(r)}$ 的染色数.

显然这里的染色数 $\chi(H^{(r)})$ 在 $r = 2$ 时恰为通常图的染色数 (见4.111). 一般地, 确定通常的图的染色数已经无比困难, 更何况超图. 对于超图来说, 我们退而求其次, 暂时只关心超图是否可 2-染色. 显然, 超图的边数越多, 则该超图越不容易 2-染色. 一个重要的问题是: 不可 2-染色的 r -超图至少有几条边?

对于正整数 r , 记

$$m(r) := \min \{m \mid \text{存在不可 2-染色的具有 } m \text{ 条边的 } r\text{-超图}\},$$

即, 不可 2-染色的 r -超图所可能具有的最小边数.

8.214.定理.(Erdős, 1963). $m(r) \geq 2^{r-1}$. 换言之, 对任意 r -超图 $H^{(r)} = (V, E)$, 如果边数 $|E| < 2^{r-1}$, 则 $H^{(r)}$ 可 2-染色.

证明. 设超图 $H^{(r)} = (V, E)$ 的边数 $|E| < 2^{r-1}$, 考虑将 $H^{(r)}$ 的每个顶点以 $\frac{1}{2}$ 的概率随机染为红, 蓝两色, 并且各个顶点的染色彼此独立. 对每一条超边 $e \in E$, 记事件 $A_e :=$ “边 e 的 r 个顶点同色”, 则 $\mathbb{P}(A_e) = 2^{1-r}$. 从而

$$\mathbb{P}\left(\bigcap_{e \in E} \bar{A}_e\right) = 1 - \mathbb{P}\left(\bigcup_{e \in E} A_e\right) \geq 1 - \sum_{e \in E} \mathbb{P}(A_e) = 1 - |E| \cdot 2^{1-r} > 0,$$

由此可知 $H^{(r)}$ 可 2-染色, 得证. □

8.2 期望的线性性与平均值原理

8.215. 设概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$, 其中 Ω 是有限集, $\mathcal{F} = 2^\Omega$. 则 Ω 上的随机变量是指函数 $X: \Omega \rightarrow \mathbb{R}$, 其期望 $\mathbb{E}[X]$ 是指

$$\mathbb{E}[X] := \int_{\Omega} X \, d\mathbb{P} = \sum_{\omega \in \Omega} X(\omega) \mathbb{P}(\omega).$$

以下事实众所周知:

- 对于事件 $A \in \mathcal{F}$, 定义该事件的特征函数 $\mathbf{1}_A: \Omega \rightarrow \mathbb{R}$ 如下:

$$\mathbf{1}_A(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \omega \notin A \end{cases},$$

则 $\mathbf{1}_A$ 是随机变量, 并且满足 $\mathbb{E}[\mathbf{1}_A] = \mathbb{P}(A)$.

- 对于随机变量 X, Y 与实数 α, β , 成立

$$\mathbb{E}[\alpha X + \beta Y] = \alpha \mathbb{E}[X] + \beta \mathbb{E}[Y],$$

此性质称为期望的线性性.

- (平均值原理). 对任意随机变量 X , 容易证明

$$\mathbb{P}(X \geq \mathbb{E}[X]) > 0,$$

同样也有 $\mathbb{P}(X \leq \mathbb{E}[X]) > 0$.

8.216. 设 A 是正整数集 \mathbb{Z}_+ 的非空子集, 如果对任意 $x, y \in A$ 都成立 $x + y \notin A$, 则称 A 是避免求和的. (允许 $x = y$ 的情况). 例如, 对于正整数 n , 易知集合

$$\left\{k \in [n] \mid k \geq \lceil \frac{n}{2} \rceil + 1\right\} \quad \text{与} \quad \{k \in [n] \mid k \text{ 是奇数}\}$$

都是“避免求和”的.

事实上, 容易证明, 如果 $A \subseteq [n]$ 是避免求和的, 则 $|A| \leq \lceil \frac{n}{2} \rceil$. 这是因为, 将 A 中元素从小到大依次记作 $a_1 < a_2 < \dots < a_m$, 其中 $m = |A|$, 则容易验证 $A' := \{a_2 - a_1, a_3 - a_1, \dots, a_m - a_1\}$ 与 A 的交集为空, 又因为 $A \sqcup A' \subseteq [n]$, 从而 $n \geq |A \sqcup A'| = |A| + |A'| = 2m - 1$, 因此 $m \leq \frac{n+1}{2}$.

8.217. 定理.(Erdős, 1965). 设 A 是 \mathbb{Z}_+ 的非空有限子集, 则存在 A 的子集 B , 使得 B 是避免求和的, 并且 $|B| \geq \frac{1}{3}|A|$.

证明. 取足够大的素数 p , 使得 $p > \max_{a \in A} a$. 考虑有限域 \mathbb{F}_p 及其乘法群 \mathbb{F}_p^\times . 注意 \mathbb{F}_p 的子集

$$S := \begin{cases} \{k+2, k+3, \dots, 2k+2\} & \text{若 } p = 3k+1 \\ \{k+1, k+2, \dots, 2k+1\} & \text{若 } p = 3k+2 \end{cases}$$

在 $\text{mod } p$ 意义下是避免求和的. 现在, 对每个 $x \in \mathbb{F}_p^\times$, 记集合

$$A_x := \{a \in A \mid ax \in S \subseteq \mathbb{F}_p\},$$

则易知 A_x 是避免求和的.

考虑在 \mathbb{F}_p^\times 中随机抽取元素 x (每个元素被选中的概率均为 $\frac{1}{p-1}$), 将集合 A_x 的元素个数 $|A_x|$ 视为随机变量. 注意 $|A_x| = \sum_{a \in A} \mathbf{1}_{\{ax \in S\}}$, 从而

$$\mathbb{E}[|A_x|] = \sum_{a \in A} \mathbb{P}(ax \in S) \geq \frac{|A|}{3},$$

因此存在 $x \in \mathbb{F}_p^\times$ 使得 $|A_x| \geq \frac{|A|}{3}$. □

8.218. 段子. 上述定理当中的常数 “ $\frac{1}{3}$ ” 是否是最佳的? 答案是肯定的. Eberhard, Green 与 Manners 于 2014 年证明了: 对任意 $\varepsilon > 0$, 存在 $A \subseteq \mathbb{Z}_+$, 使得 A 的任何避免求和的子集 B 都满足 $|B| \leq \left(\frac{1}{3} + \varepsilon\right) |A|$. 详见 Eberhard, S., Green, B., & Manners, F. (2014). *Sets of integers with no large sum-free subset*. *Annals of Mathematics*, 621-652.

我们再看概率方法的又一应用. 对于图 $G = (V, E)$, 记 $\alpha(G)$ 为图 G 的独立数, 即最大独立集的顶点个数 (回忆 4.109). 关于 $\alpha(G)$ 有如下结论:

8.219. 定理. 对于任意图 $G = (V, E)$, 都成立

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{1 + d_G(v)},$$

其中 $d_G(v)$ 为顶点 v 的度数.

注意函数 $f(x) = \frac{1}{1+x}$ ($x > 0$) 是凸函数, 以及凸函数的 Jensen 不等式, 可知此定理比 6.169 更强.

证明. 不妨设图 G 的顶点集 $V = [n]$. 考虑置换群 S_n , 将 S_n 中的元素 $\pi: [n] \rightarrow [n]$ 视为顶点集 V 上的函数. 对于 $\pi \in S_n$ 以及顶点 $v \in V$, 如果对任意邻居 $v' \in N_G(v)$ 都成立 $\pi(v) < \pi(v')$, 则称 v 是函数 π 的极小值点 (即在该点处的函数值比在它所有邻居处的函数值都小). 容易验证, 对任意 $\pi \in S_n$, 函数 π 的全部极小值点构成的集合是 G 的独立集 (留给读者).

现在, 从 S_n 等概率地随机选取 π , 则对任意顶点 $v \in V$, 容易验证事件 A_v : “ v 是函数 π 的极小值点” 的概率 $\mathbb{P}(A_v) = \frac{1}{1 + d_G(v)}$. 记随机变量

$X :=$ “函数 $\pi \in S_n$ 的极小值点的个数”, 则 $X = \sum_{v \in V} \mathbf{1}_{A_v}$, 因此

$$\mathbb{E}[X] = \sum_{v \in V} \mathbb{E}[\mathbf{1}_{A_v}] = \sum_{v \in V} \mathbb{P}(A_v) = \sum_{v \in V} \frac{1}{1 + d_G(v)}.$$

因此存在 $\pi \in S_n$, 使得 π 的极小值点的个数不少于 $\sum_{v \in V} \frac{1}{1 + d_G(v)}$, 这些极小值点构成 G 的一个独立集, 从而 $\alpha(G) \geq \sum_{v \in V} \frac{1}{1 + d_G(v)}$. \square

8.220. 利用上述定理, 我们能够再次证明渐近版本 Turán 定理 6.170.

渐近版本 Turán 定理 6.170 的另证. 记图 $G = (V, E)$ 的顶点数和边数分别为 n, m , 注意 $\sum_{v \in V} d_G(v) = 2m$, 从而

$$\begin{aligned} \alpha(G) &\geq \sum_{v \in V} \frac{1}{1 + d_G(v)} = \frac{1}{n + 2m} \left(\sum_{v \in V} \frac{1}{1 + d_G(v)} \right) \left(\sum_{v \in V} (1 + d_G(v)) \right) \\ &\geq \frac{n^2}{2m + n}. \end{aligned}$$

注意上式对任何图都成立. 现在, 假如 G 不含有 K_{r+1} , 则 G 的补图 $G' := (V, E' := \binom{V}{2} \setminus E)$ 满足 $\alpha(G') \leq r$, 因此

$$r \geq \alpha(G') \geq \frac{n^2}{2|E'| + n} = \frac{n^2}{n^2 - 2m},$$

解得 $m \leq \frac{r-1}{2r} n^2$, 从而得证. \square

8.3 删除技巧

8.221. 我们已经介绍了如下两个平凡的概率论事实

- 若事件 A 的概率 $\mathbb{P}(A) > 0$, 则事件 A 可能发生;
- 对于随机变量 X , 则事件 “ $X \geq \mathbb{E}[X]$ ” 可能发生

在组合数学中不平凡的应用. 它们的基本想法为: 为证明满足某性质的组合对象的存在性, 只需适当构造概率模型, 并证明“所希望的事件”的概率大于零. 这个想法可以继续推广. 一般来说, “所希望的事件”所要求的性质可能太强; 我们可退而求其次, 允许事件中带有“不太多的”瑕疵, 即证明“稍微次一些的事件可能发生”, 之后再通过其他手段来去掉其中瑕疵, 得到真正希望发生的事件. 我们从具体例子中来体会这种想法.

第一个例子依然是 Ramsey 数的下界估计, 将改进 8.206 的结果:

8.222. 性质. 设正整数 $n \geq k > 0$, 则成立

$$R(k, k) > n - \binom{n}{k} 2^{1-\binom{k}{2}},$$

特别地, 当 $k \rightarrow \infty$ 时,

$$R(k, k) > \left(\frac{1}{e} + o(1) \right) k \cdot 2^{k/2}.$$

相比于 8.207, 这里的下界为之前的 $\sqrt{2}$ 倍, 结果更优.

证明. 考虑对完全图 K_n 进行随机 2-边染色. 记 K_n 的顶点集为 V , 则对每个 $S \in \binom{V}{k}$, 记事件 A_S : “限制子图 $K_n|_S$ 关于该染色是同色的”, 则 $\mathbb{P}(A_S) = 2^{1-\binom{k}{2}}$. 记随机变量 $X := “K_n$ 的同色 K_k 子图的个数”, 则 $X = \sum_{A \in \binom{V}{k}} \mathbf{1}_{A_S}$, 从而 $E[X] = \sum_{A \in \binom{V}{k}} \mathbb{P}(A_S) = \binom{n}{k} 2^{1-\binom{k}{2}}$, 因此存在 K_n 的 2-边染色, 使得其同色 K_k 子图的个数不超过 $E[X] = \binom{n}{k} 2^{1-\binom{k}{2}}$.

取定该 2-边染色. 对于每一个同色 K_k 子图, 从其中任选一个顶点, 这样总共至多选中 $\binom{n}{k} 2^{1-\binom{k}{2}}$ 个顶点. 把这些被选中的顶点 (以及以它们为端点的边) 从 K_n 当中删去, 这个操作将同色 K_k 子图全部破坏掉. 这样就构造出一个具有至少 $n - \binom{n}{k} 2^{1-\binom{k}{2}}$ 个顶点的完全图及其 2-边染色, 使得在该染色下没有同色 K_k , 因此 $R(k, k) > n - \binom{n}{k} 2^{1-\binom{k}{2}}$.

特别地, 取 $n = \lceil \frac{k}{e} 2^{\frac{k}{2}} \rceil$, 并注意 Stirling 公式 $k! \sim \sqrt{2\pi k} \left(\frac{k}{e} \right)^k$, 从而

$$R(k, k) > n - \binom{n}{k} 2^{1-\binom{k}{2}} > n - \frac{n^k}{k!} 2^{-\frac{k^2}{2} + \frac{k}{2} + 1}$$

$$\begin{aligned}
&\geq \left(\frac{1}{e} k \cdot 2^{k/2} - 1 \right) - \left(\frac{k}{e} \right)^k \frac{1}{k!} 2^{\frac{k}{2}+1} \\
&= \left(\frac{1}{e} + o(1) \right) k \cdot 2^{k/2}, \quad k \rightarrow \infty.
\end{aligned}$$

□

在此例中, 我们真正希望发生的事件是“没有同色 K_k 子图”; 而这里退而求其次, 先暂时允许存在“少量的”同色 K_k 子图 (即“瑕疵”), 然后把把这些瑕疵“破坏掉”. 这种技巧俗称“删除技巧”.

8.223. 设 $X \geq 0$ 为随机变量, 如下 **Markov 不等式** 众所周知: 对任意 $t > 0$,

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

这是因为 $\mathbb{E}[X] = \int_{\Omega} X \, d\mathbb{P} \geq \int_{\{X \geq t\}} X \, d\mathbb{P} \geq \int_{\{X \geq t\}} t \, d\mathbb{P} = t\mathbb{P}(X \geq t)$, 从而推出 Markov 不等式成立. 特别地, 当随机变量 X 取值于非负整数时, 有如下推论:

8.224. 推论. 设 $X_n \geq 0$ 是一列非负整数值的随机变量, 并且满足

$$\lim_{n \rightarrow \infty} \mathbb{E}[X_n] = 0,$$

则 $\lim_{n \rightarrow \infty} \mathbb{P}(X_n = 0) = 1$.

证明. 这是因为 $\mathbb{P}(X_n = 0) = \mathbb{P}(X_n \leq 0.1) \leq \frac{\mathbb{E}[X_n]}{0.1} \rightarrow 0, n \rightarrow \infty$, 得证. □

8.225. 定义. 对于图 $G = (V, E)$, 记

$$g(G) := \min \{k \geq 3 \mid \text{图 } G \text{ 含有圈 } C_k\};$$

而若 G 不含圈, 则规定 $g(G) = \infty$. 换言之, $g(G)$ 为图 G 的“最短圈”的长度, 称为图 G 的**腰围**.

凭直觉, 图 G 的边越多, 则图 G 越可能含有长度很短的圈, 从而 $g(G)$ 就越小. 与之相对应, 回忆染色数 $\chi(G)$ 的概念 4.111, 直观地看, 图 G 的边越多, 则对染色的限制条件就越多, 从而更难用较少种类的颜色来完成染色, 因此

$\chi(G)$ 就会很大. 综上, 有如下朴素的直觉: 如果 $g(G)$ 很大, 则图 G 非常“稀疏” (边数不会太多), 而 $\chi(G)$ 很大则表明图 G 非常“稠密”. 这两者看似矛盾, 因此不太可能 $\chi(G)$ 与 $g(G)$ 都很大. 但很不幸这个直觉是错的, Erdős 证明了如下定理: 对任意正整数 k , 存在图 G 使得 $\chi(G) \geq k$ 且 $g(G) \geq k$, 也就是说, 图的染色数和腰围可以都非常大. 这个定理的首个证明就是采用概率方法, 而非具体构造. 接下来将介绍此定理的证明, 首先需要如下引理:

8.226. 引理. 任意取定数列 $p_n \in (0, 1)$, $n = 1, 2, 3, \dots$, 考虑随机图序列 $G_n := G(n, p_n)$ (回忆 8.208), 则

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\alpha(G_n) \leq \left\lceil \frac{2 \ln n}{p_n} \right\rceil \right) = 1 \quad \text{关于 } \{p_n\} \text{ 一致,}$$

这里 $\alpha(G_n)$ 是随机图 G_n 的独立数, 视为随机变量.

证明. 记 $t_n := \left\lceil \frac{2 \ln n}{p_n} \right\rceil$, 容易验证 $n e^{-p_n \frac{t_n}{2}} \leq 1$ 总是成立. 记随机变量 $X_n :=$ “ G_n 的 $(t_n + 1)$ 元独立子集的个数”, 则

$$\begin{aligned} \mathbb{E}[X_n] &= \sum_{S \in \binom{[n]}{t_n+1}} \mathbb{P}(S \text{ 是 } G_n \text{ 的独立子集}) \\ &= \binom{n}{t_n+1} (1-p_n)^{\binom{t_n+1}{2}} \leq \frac{n^{t_n+1}}{(t_n+1)!} e^{-p_n \binom{t_n+1}{2}} \\ &= \frac{1}{(t_n+1)!} \left(n e^{-p_n \frac{t_n}{2}} \right)^{t_n+1} \leq \frac{1}{(t_n+1)!} \rightarrow 0, \quad n \rightarrow \infty. \end{aligned}$$

再由推论 8.224 可得

$$\lim_{n \rightarrow \infty} \mathbb{P}(\alpha(G_n) \leq t_n) = \lim_{n \rightarrow \infty} \mathbb{P}(X_n = 0) = 1,$$

引理得证. □

8.227. 定理. (Erdős, 1959) 对任意正整数 k , 存在图 G 使得

$$\chi(G) \geq k \quad \text{且} \quad g(G) \geq k,$$

其中 $\chi(G)$ 是 G 的染色数 (见 4.111), $g(G)$ 是 G 的腰围 (见 8.225).

证明. 考虑一系列随机图 $G_n = G(n, p_n)$, 其中概率 $p_n \in (0, 1)$ 待定. 记 $t_n := \lceil \frac{2 \ln n}{p_n} \rceil$. 则由引理 8.226 可知 $\lim_{n \rightarrow \infty} \mathbb{P}(\alpha(G_n) \leq t_n) = 1$.

考虑随机变量 Y_n : “随机图 G_n 的长度小于 k 的圈个数”, 则易知

$$\begin{aligned} \mathbb{E}[Y_n] &= \sum_{i=3}^{k-1} \sum_{S \in \binom{[n]}{i}} \frac{i!}{2^i} p_n^i = \sum_{i=3}^{k-1} \frac{n(n-1) \cdots (n-i+1)}{2^i} p_n^i \\ &\leq \sum_{i=3}^{k-1} (np_n)^i \leq \frac{(np_n)^k - 1}{np_n - 1}. \end{aligned}$$

现在, 取 $p_n := n^{-\frac{k-1}{k}}$, 则 $np_n = n^{\frac{1}{k}}$, 从而由 Markov 不等式得

$$\mathbb{P}(Y_n > \frac{n}{2}) \leq \frac{\mathbb{E}[Y_n]}{n/2} = \frac{2(n-1)}{n(n^{\frac{1}{k}} - 1)} \rightarrow 0, \quad n \rightarrow \infty.$$

因此当 n 足够大时, 存在 n 个顶点的图 G 使得

$$\begin{aligned} \alpha(G) &\leq \lceil \frac{2 \ln n}{p_n} \rceil = \lceil 2n^{1-\frac{1}{k}} \ln n \rceil \leq 3n^{1-\frac{1}{k}} \ln n, \\ \text{且 } Y_n &\leq \frac{n}{2}. \end{aligned}$$

对 G 的每一个长度小于 k 的圈, 从该圈中任意选定一个顶点, 由于图 G 的长度小于 k 的圈的个数不超过 $\frac{n}{2}$, 所以上述操作至多选定了 $\frac{n}{2}$ 个不同顶点. 将这些被选中的顶点 (以及以它们为端点的边) 从 G 中删除, 得到的图记作 G' , 则 G' 的顶点数 $v(G') \geq \frac{n}{2}$, 且 G' 不含有长度小于 k 的圈, 从而 $g(G') \geq k$. 由于 G' 是 G 的限制子图, 从而易知 $\alpha(G') \leq \alpha(G)$. 再由独立数与染色数的关系 4.112 可知

$$\chi(G') \geq \frac{v(G')}{\alpha(G')} \geq \frac{n/2}{3n^{1-\frac{1}{k}} \ln n} = \frac{n^{\frac{1}{k}}}{6 \ln n} \rightarrow \infty, \quad n \rightarrow \infty.$$

因此当 n 足够大时, 相应的 G' 满足 $g(G') \geq k$ 且 $\chi(G') \geq k$, 得证. □

我们希望图 G 不含有“短圈”(即长度小于 k 的圈). 而在证明之中, 我们先允许出现“少量的”短圈, 然后再设法把短圈都“破坏掉”, 得到不含短圈的图. 这是删除技巧的又一绝妙运用.

作为推论, 上述定理给出 Ramsey 数 $R(3, n)$ 的更好的下界估计. 我们回忆, 定理 7.203 断言, 当 n 足够大时有 $R(3, n) > n^{1.01}$. 若读者有闲工夫, 可以

细抠该定理的证明过程, 把指数 1.01 稍微再弄大一些; 然而无论怎么抠, 这个 1.01 也不会明显改进多少. 而概率方法所得结果将是突破性的.

8.228. 推论. 存在常数 $C > 0$, 使得当 n 足够大时, Ramsey 数 $R(3, n)$ 满足

$$R(3, n) > C \left(\frac{n}{\ln n} \right)^{\frac{3}{2}}.$$

例如, 可以取 $C = 0.01$.

证明. 在定理 8.227 的证明过程中, 取 $k = 3$, 可知对于任意足够大的正整数 m , 存在图 $G = (V, E)$, 使得 $g(G) > 3$ (换言之, 图 G 不含三角形), 并且

$$\alpha(G) \leq \lceil 2m^{\frac{2}{3}} \ln m \rceil, \quad |V| \geq \frac{1}{2}m.$$

这意味着 $R(3, \lceil 2m^{\frac{2}{3}} \ln m \rceil + 1) > \frac{1}{2}m$ 对足够大的正整数 m 都成立.

现在, 对于充分大的 n , 取正整数 m 使得

$$\lceil 2m^{\frac{2}{3}} \ln m \rceil + 1 \leq n < \lceil 2(m+1)^{\frac{2}{3}} \ln(m+1) \rceil + 1,$$

则有 $m^{\frac{2}{3}} \ln m \leq n < 3m^{\frac{2}{3}} \ln m$. 特别地, $m^{\frac{2}{3}} \leq n$, 从而 $\ln m \leq \frac{3}{2} \ln n$, 因此

$$\begin{aligned} R(3, n) &\geq R\left(3, \lceil 2m^{\frac{2}{3}} \ln m \rceil + 1\right) \\ &> \frac{1}{2}m > \frac{1}{2} \left(\frac{n}{3 \ln m} \right)^{\frac{3}{2}} = \frac{3^{-\frac{3}{2}}}{2} \left(\frac{n}{\ln m} \right)^{\frac{3}{2}} \\ &\geq \frac{3^{-\frac{3}{2}}}{2} \left(\frac{2}{3} \frac{n}{\ln n} \right)^{\frac{3}{2}} = \frac{\sqrt{2}}{27} \left(\frac{n}{\ln n} \right)^{\frac{3}{2}} > 0.01 \left(\frac{n}{\ln n} \right)^{\frac{3}{2}}, \end{aligned}$$

从而得证. □

8.4 练习: Ramsey 数 $R(3, n)$ 的渐近估计 II

8.229. 作为补充内容, 本节企图改进 $n \rightarrow \infty$ 时 Ramsey 数 $R(3, n)$ 的渐近下界. 回忆之前的工作:

- 由简单的直接构造可知 $R(3, n) > 2n - 2$. (见习题 7.200).

- 由复杂的直接构造可知存在常数 $\varepsilon > 0$ 使得 $R(3, n) > n^{1+\varepsilon}$.

(见定理7.203).

- 由简单的概率构造可知存在常数 $C > 0$ 使得 $R(3, n) > C \left(\frac{n}{\ln n} \right)^{\frac{3}{2}}$.

(见推论8.228).

而本节将采用较复杂的概率与组合技巧以及更细致的不等式估计, 证明存在常数 $C > 0$, 使得当 n 充分大时成立

$$R(3, n) > C \left(\frac{n}{\ln n} \right)^2,$$

再次提高 $R(3, n)$ 的下界. 注意这个下界已经非常接近习题7.200所给出的上界 $R(3, n) \leq \binom{n+1}{2} \approx \frac{1}{2}n^2$. 上述结论依然来自数学家 Erdős.

本节采用如下临时记号:

8.230.记号. 设 $A > 0$ 是某个确定的 (很大的) 正实数, 对于正整数 n , 记 (与 n 有关的) 正整数 x 与正实数 $p \in (0, 1)$ 如下:

$$x := \left\lfloor An^{\frac{1}{2}} \ln n \right\rfloor, \quad p := 2A^{-\frac{1}{2}}n^{-\frac{1}{2}}.$$

记集合 $V = [n] = \{1, 2, \dots, n\}$, 并且用字母 H 来表示集合 $\binom{V}{x}$ 中的元素.

对于图 $G = (V, E)$, 以及 $H \in \binom{V}{x}$, 引入如下临时记号:

- 对于 $v \in V$, 记 $d_H(v) := \#\{v' \in H \mid v' \sim_E v\}$, 称为顶点 v 的 H -度数.
- 记集合 $E|_H := E \cap \binom{H}{2}$, 即限制子图 $G|_H$ 的边集.
- 记集合 $Z_G(H) := \left\{ \{v_1, v_2\} \in \binom{H}{2} \mid \exists v' \in V \setminus H, (v' \sim_E v_1 \text{ 且 } v' \sim_E v_2) \right\}$.

对每个 $n \geq 1$, 考察随机图 $G = G(n, p)$, 其中 $p = 2A^{-\frac{1}{2}}n^{-\frac{1}{2}}$, 则随机图 G 的顶点集为 $V = [n]$, 边集 $E \subseteq \binom{V}{2}$ 视为随机变量. 本节的主要结论是:

8.231.定理.(Erdős, 1960) 沿用8.230的记号, 则随机图 $G = G(n, p)$ 满足

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\forall H \in \binom{V}{x}, \exists e_H \in E|_H, e_H \notin Z_G(H) \right) = 1.$$

先看此定理与 Ramsey 数的关系. 假设此定理成立, 则有如下推论:

8.232.推论. 对于充分大的正整数 n , 存在具有 n 个顶点的图 G , 使得 G 不含三角形, 且独立数 $\alpha(G) < x := \left\lfloor An^{\frac{1}{2}} \ln n \right\rfloor$.

此推论表明, 当 n 充分大时成立 $R\left(3, \left\lfloor An^{\frac{1}{2}} \ln n \right\rfloor\right) > n$. 于是老办法按部就班地计算就能推出, 存在常数 $C > 0$, 使得当 n 充分大时成立

$$R(3, n) > C \left(\frac{n}{\ln n} \right)^2,$$

得到本节所希望的结果.

证明. 假设定理 8.231 成立, 则当 n 充分大时, 取满足定理 8.231 所述性质的图 $G = (V, E)$, 其中顶点集 $V = [n]$, 记边数 $y := |E|$. 注意到, 对于任意 $H \in \binom{V}{x}$, e_H 的存在性表明限制子图 $G|_H$ 不是独立图, 这就推出 $\alpha(G) < x$. 然而不幸的是, 定理 8.231 所述性质并不能保证 G 不含有三角形. 为得到真正想要的图, 需要对 G 进行改造, 改造的方式是删除 G 的某些边. 具体地说, 记 G 的边集 $E = \{e_1, e_2, \dots, e_y\}$, 通过如下算法来构造 E 的子集 E' :

- 首先令 $E' = \{e_1\}$,
- 对每个 $i = 1, 2, \dots, y$:
 - 如果存在 $1 \leq j < k < i$, 使得 $e_j, e_k \in E'$, 并且 e_i, e_j, e_k 是 G 的某个三角形的三边, 则 e_i 不是 E' 中的元素;
 - 否则将 e_i 添加到 E' 当中.
- 输出 E' .

记 $G' = (V, E')$, 则由 E' 的上述构造易知 G' 不含三角形. 再验证 G' 不含有 x 个顶点的独立子集. 对任意 $H \in \binom{V}{x}$, 考察满足定理 8.231 所述性质的边 $e_H \in E$. 如果 $e_H \in E'$, 则显然 $G'|_H$ 不是独立图, 得证; 而如果 $e_H \notin E'$, 则由 E' 的定义可知存在 $e_j, e_k \in E'$, 使得三边 e_H, e_j, e_k 构成三角形, 从而 e_H 的定义迫使边 e_j, e_k 的端点都在 H 中, 于是 e_j, e_k 也是限制子图 $G'|_H$ 的边, 从而 $G'|_H$ 不是独立图. 综上所述, $\alpha(G') < x$, 图 G' 即为所求. \square

接下来开始证明定理8.231. 为此需要一系列技术性引理. 取定 $H \in \binom{V}{x}$, 则 $\forall v \in V \setminus H$, 易知

$$\mathbb{E}[d_H(v)] = px = 2A^{\frac{1}{2}} \ln n + o(1), \quad n \rightarrow \infty.$$

而下述引理表明, “ H -度数过大的点的个数很少” 几乎一定成立.

8.233. 引理. 对于每个正整数 k , 记

$$d_k := \lfloor 2^k A^{\frac{2}{3}} \ln n \rfloor, \quad w_k := \lfloor \frac{n}{4^k k^2} \rfloor,$$

则随机图 $G = G(n, p)$ 满足如下性质:

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\forall H \in \binom{V}{x}, \forall k \in \mathbb{Z}_+, \# \{v \in V \setminus H \mid d_H(v) \geq d_k\} < w_k \right) = 1.$$

证明. 先取定 $H \in \binom{V}{x}$, $v \in V \setminus H$ 以及 $k \in \mathbb{Z}_+$. 注意到 $d_H(v) \leq |H| = x$, 从而如果 $d_H(v) \geq d_k$ 成立, 那么必有 $d_k \leq x$, 从而 (当 n 足够大时) 容易验证 $k \leq \ln n$. 这表明当 $k > \ln n$ 时 $\mathbb{P}(d_H(v) \geq d_k) = 0$. 而当 $k \leq \ln n$ 时, 有

$$\begin{aligned} \mathbb{P}(d_H(v) \geq d_k) &\leq \sum_{H' \in \binom{V}{d_k}} \mathbb{P}(\forall v' \in H', v' \sim_E v) = \binom{x}{d_k} p^{d_k} \\ &\leq \left(\frac{ex}{d_k} \right)^{d_k} \leq \left(\frac{e \cdot 2A^{\frac{1}{2}} \ln n}{2^{k-1} A^{\frac{2}{3}} \ln n} \right)^{d_k} < 2^{-kd_k} < n^{-k \cdot 2^{k-1} A^{\frac{2}{3}}}. \end{aligned}$$

注意上述推导利用了组合不等式

$$\binom{u}{v} < \frac{u^v}{v!} < \left(\frac{eu}{v} \right)^v, \quad \forall u > v > 0,$$

并且常数 A 需要足够大, 具体地说, 需要 $A > (4e)^6$.

因此, 对于 $H \in \binom{V}{x}$ 以及正整数 $k \leq \lfloor \ln n \rfloor$, 成立

$$\begin{aligned} &\mathbb{P}(\# \{v \in V \setminus H \mid d_H(v) \geq d_k\} \geq w_k) \\ &\leq \sum_{V' \in \binom{V \setminus H}{w_k}} \mathbb{P}(\forall v' \in V', d_H(v') \geq d_k) \leq \binom{n}{w_k} n^{-k \cdot 2^{k-1} A^{\frac{2}{3}} w_k} \end{aligned}$$

$$\begin{aligned}
&< \left(\frac{\mathbf{e}n}{w_k} \cdot n^{-k \cdot 2^{k-1} A^{\frac{2}{3}}} \right)^{w_k} < \left(4^{k+1} \mathbf{e} k^2 \cdot n^{-k \cdot 2^{k-1} A^{\frac{2}{3}}} \right)^{w_k} \\
&< \exp \left(-k \cdot 2^{k-1} A^{\frac{2}{3}} w_k \ln n + 6k w_k \ln \ln n \right) \\
&< \exp \left(-A^{\frac{2}{3}} n \ln n + o(n \ln n) \right),
\end{aligned}$$

并且上式最右边的 $o(n \ln n)$ 沿 $n \rightarrow \infty$ 关于 $k \leq \lfloor \ln n \rfloor$ 一致. 又因为

$$\binom{n}{x} < \left(\frac{\mathbf{e}n}{x} \right)^x < \exp \left(\frac{1}{2} A n^{\frac{1}{2}} \ln^2 n + o(n^{\frac{1}{2}} \ln^2 n) \right),$$

所以当 $n \rightarrow \infty$ 时,

$$\begin{aligned}
&\mathbb{P} \left(\exists H \in \binom{V}{x}, \exists k \in \mathbb{Z}_+, \# \{v \in V \setminus H \mid d_H(v) \geq d_k\} \geq w_k \right) \\
&\leq \sum_{H \in \binom{V}{x}} \sum_{k=1}^{\lfloor \ln n \rfloor} \mathbb{P} (\# \{v \in V \setminus H \mid d_H(v) \geq d_k\} \geq w_k) \\
&\leq \binom{n}{x} \ln n \cdot \mathbb{P} (\# \{v \in V \setminus H \mid d_H(v) \geq d_k\} \geq w_k) \\
&< \exp \left(-A^{\frac{2}{3}} n \ln n + o(n \ln n) \right) \rightarrow 0,
\end{aligned}$$

引理得证. □

8.234. 引理. 对足够大的正整数 n , 以及图 $G = (V, E)$, $H \in \binom{V}{x}$, 如果

$$\forall k \in \mathbb{Z}_+, \quad \# \{v \in V \setminus H \mid d_H(v) \geq d_k\} < w_k,$$

那么 $|Z_G(H)| < \frac{1}{2} \binom{x}{2}$. 其中 d_k, w_k 见 8.233, $Z_G(H)$ 见 8.230.

证明. 首先容易验证如下不等式, 留给读者练习:

$$|Z_G(H)| \leq \sum_{v \in V \setminus H} \binom{d_H(v)}{2}.$$

(提示: 对 $\# \left\{ (\{v_1, v_2\}, w) \in \binom{H}{2} \times (V \setminus H) \mid w \sim_E v_1, w \sim_E v_2 \right\}$ 算两次.)

另一方面, 补充定义 $d_0 := 0$, 则有

$$\begin{aligned} \sum_{v \in V \setminus H} \binom{d_H(v)}{2} &= \sum_{k=1}^{\infty} \sum_{\substack{v \in V \setminus H \\ d_{k-1} \leq d_H(v) < d_k}} \binom{d_H(v)}{2} \\ &< \frac{1}{2} \sum_{k=1}^{\infty} w_k d_k^2 \leq \frac{1}{2} \sum_{k=1}^{\infty} \frac{n}{4^k k^2} \cdot 4^k A^{\frac{4}{3}} \ln^2 n = \frac{\pi^2}{12} A^{\frac{4}{3}} n \ln^2 n. \end{aligned}$$

而当 n 足够大时, $\frac{1}{2} \binom{x}{2} > \frac{1}{5} x^2 > \frac{1}{6} A^2 n \ln^2 n$.

综上所述, (如果常数 $A > \frac{\pi^3}{2\sqrt{2}}$) 有 $|Z_G(H)| \leq \frac{1}{2} \binom{x}{2}$, 引理证毕. \square

8.235. 结合引理8.233与引理8.234, 可知随机图 $G(n, p)$ 满足

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\exists H \in \binom{V}{x}, |Z_G(H)| > \frac{1}{2} \binom{x}{2} \right) = 0.$$

有了上述准备, 现在可以证明定理8.231了.

定理8.231的证明. 沿用前文记号与结论, 容易验证当 $n \rightarrow \infty$ 时成立

$$\begin{aligned} &\mathbb{P} \left(\exists H \in \binom{V}{x}, \forall e_H \in E|_H, e_H \in Z_G(H) \right) \\ &\leq \mathbb{P} \left(\exists H \in \binom{V}{x}, \left(|Z_G(H)| \leq \frac{1}{2} \binom{x}{2} \wedge (\forall e_H \in E|_H, e_H \in Z_G(H)) \right) \right) \\ &\quad + \mathbb{P} \left(\exists H \in \binom{V}{x}, |Z_G(H)| > \frac{1}{2} \binom{x}{2} \right) \\ &\leq \sum_{\substack{H \in \binom{V}{x} \\ |Z_G(H)| \leq \frac{1}{2} \binom{x}{2}}} \mathbb{P}(\forall e_H \in E|_H, e_H \in Z_G(H)) + o(1) \\ &= \sum_{\substack{H \in \binom{V}{x} \\ |Z_G(H)| \leq \frac{1}{2} \binom{x}{2}}} (1-p)^{\binom{x}{2} - |Z_G(H)|} + o(1) \leq \binom{n}{x} e^{-\frac{1}{2} p \binom{x}{2}} + o(1) \\ &< \left(\frac{en}{x} \right)^x e^{-\frac{1}{4} p x^2} + o(1) \\ &< \exp \left(\frac{1}{2} (A - A^{\frac{3}{2}}) n^{\frac{1}{2}} \ln^2 n + o(n^{\frac{1}{2}} \ln^2 n) \right) + o(1) \rightarrow 0 \end{aligned}$$

从而得证. \square

至此, 再结合定理7.201, 我们得到如下结果:

8.236. 定理. 存在常数 C , 使得当正整数 n 充分大时, Ramsey 数 $R(3, n)$ 满足

$$C \left(\frac{n}{\ln n} \right)^2 < R(3, n) \leq (1 + o(1)) \frac{n^2}{\ln n}.$$

注意定理8.231, 容易验证常数 C 可以取为 $C = \frac{1}{10A^2}$ (留给读者验证); 而结合引理8.233等内容可知, 保险起见可以取 $A = 10^7 > (4e)^6$. 于是可以取 $C = 10^{-15}$.

8.237. 段子. $R(3, n)$ 的渐近估计的故事还有后续:

- (Kim, 1995) 存在常数 C , 使得当 n 足够大时, $R(3, n) \geq C \frac{n^2}{\ln n}$.
- (Bohman-Keevash, 2016; Fiz Pontiveros-Griffiths-Morris, 2018) 当 n 足够大时,

$$R(3, n) \geq \left(\frac{1}{4} - o(1) \right) \frac{n^2}{\ln n}.$$

上述结果的证明需要用到更深的概率方法, 这超出本讲义的范围. 而定理7.201中的 $(1 + o(1)) \frac{n^2}{\ln n}$ 是人类目前已知最佳渐近上界, 是人类目前已知最佳下界的 4 倍.

8.5 Lovász 局部性引理

8.238. 设 B_1, B_2, \dots, B_m 是若干“坏的事件”, 其概率分别为 $\mathbb{P}(B_i) = p_i < 1$. 我们希望这些坏的事件都不发生. 我们想知道, 在什么条件下, 才能保证这些坏的事件真的有可能都不发生, 即 $\mathbb{P}(\overline{B_1} \overline{B_2} \cdots \overline{B_n}) > 0$. 以下是两种极端情形:

1. 如果每一个坏的事件发生的概率都很小, 则它们有可能都不发生.

具体地, 如果 $\sum_{i=1}^m p_i < 1$, 则

$$\mathbb{P}(B_1 \cup B_2 \cup \cdots \cup B_m) \leq \sum_{i=1}^m \mathbb{P}(B_i) < 1,$$

因此 $\mathbb{P}(\overline{B_1} \overline{B_2} \cdots \overline{B_n}) = 1 - \mathbb{P}(B_1 \cup B_2 \cup \cdots \cup B_m) > 0$.

2. 如果这些坏的事件彼此独立, 则它们有可能都不发生.

$$\text{此时 } \mathbb{P}(\overline{B_1}\overline{B_2}\cdots\overline{B_n}) = \prod_{i=1}^m (1 - p_i) > 0.$$

而对于介于以上两种极端情形之间的情况 (比如, 每件坏事的概率都比较小但又不是特别小, 这些坏事并非彼此独立但“基本上是独立的”), 我们也有相应的概率论工具来处理, 这个工具就是 **Lovász 局部性引理** (见后文 8.241). 本节将介绍此引理以及在组合数学中的应用.

8.239. 定义. 给定概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$, 事件 $A \in \mathcal{F}$, 以及事件族 $\mathcal{B} \subseteq \mathcal{F}$. 如果对于 \mathcal{B} 的任意有限子集 $\{B_1, B_2, \dots, B_m\}$ 都成立

$$\mathbb{P}(A|C_1C_2\cdots C_m) = \mathbb{P}(A),$$

其中 $C_i = B_i$ 或 $\overline{B_i}$, 则称事件 A **独立于** 事件族 \mathcal{B} .

由定义容易验证, A 独立于事件族 $\mathcal{B} \Rightarrow A$ 与 \mathcal{B} 中的每个事件都相互独立. 但反之未必成立, 请读者自行举出反例 (尝试 $|\mathcal{B}| = 2$ 的简单情形).

8.240. 定理. (Spencer, 1977) 给定概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$, 以及 n 个事件 $B_1, B_2, \dots, B_n \in \mathcal{F}$. 对每个 $i \in [n]$, 给定指标集 $N(i) \subseteq [n] \setminus \{i\}$, 使得事件 B_i 独立于事件族 $\{B_j | j \notin N(i) \cup \{i\}\}$. 如果实数 $x_1, x_2, \dots, x_n \in [0, 1]$ 满足

$$\mathbb{P}(B_i) \leq x_i \prod_{j \in N(i)} (1 - x_j), \quad \forall i \in [n],$$

$$\text{则 } \mathbb{P}(\overline{B_1}\overline{B_2}\cdots\overline{B_n}) \geq \prod_{i=1}^n (1 - x_i).$$

证明. 断言: 对任意 $i \in [n]$ 以及 $S \subseteq [n] \setminus \{i\}$, 成立

$$\mathbb{P}\left(B_i \mid \bigcap_{j \in S} \overline{B_j}\right) \leq x_i.$$

假如断言成立, 则由条件概率的有关公式容易得到

$$\begin{aligned} \mathbb{P}(\overline{B_1}\overline{B_2}\cdots\overline{B_n}) &= \mathbb{P}(\overline{B_1})\mathbb{P}(\overline{B_2} | \overline{B_1})\mathbb{P}(\overline{B_3} | \overline{B_1}\overline{B_2}) \cdots \mathbb{P}(\overline{B_n} | \overline{B_1}\overline{B_2}\cdots\overline{B_{n-1}}) \\ &\geq (1 - x_1)(1 - x_2) \cdots (1 - x_n), \end{aligned}$$

从而定理得证. 于是只需证明此断言. 给定 $i \in [n]$ 以及指标集 $S \subseteq [n] \setminus \{i\}$, 我们通过对 $|S|$ 归纳来证明断言. 起始步: 当 $|S| = 0$ 时, $S = \emptyset$, 此时

$$\mathbb{P}\left(B_i \mid \bigcap_{j \in S} \overline{B}_j\right) = \mathbb{P}(B_i) \leq x_i \prod_{j \in N(i)} (1 - x_j) \leq x_i,$$

得证. 归纳步: 取定 $i \in [n]$, 若正整数 k 使得该断言对任意 $|S| < k$ 都成立, 则当 $|S| = k$ 时, 注意 $i \notin S$, 记 $S_1 := S \cap N(i)$, $S_2 := S \setminus N(i)$. 注意条件概率公式 $\mathbb{P}(A \mid BC) = \frac{\mathbb{P}(AB \mid C)}{\mathbb{P}(B \mid C)}$, 从而

$$\begin{aligned} \mathbb{P}\left(B_i \mid \bigcap_{j \in S} \overline{B}_j\right) &= \frac{\mathbb{P}\left(B_i \cap \bigcap_{j \in S_1} \overline{B}_j \mid \bigcap_{j \in S_2} \overline{B}_j\right)}{\mathbb{P}\left(\bigcap_{j \in S_1} \overline{B}_j \mid \bigcap_{j \in S_2} \overline{B}_j\right)} \leq \frac{\mathbb{P}\left(B_i \mid \bigcap_{j \in S_2} \overline{B}_j\right)}{\mathbb{P}\left(\bigcap_{j \in S_1} \overline{B}_j \mid \bigcap_{j \in S_2} \overline{B}_j\right)} \\ &= \frac{\mathbb{P}(B_i)}{\mathbb{P}\left(\bigcap_{j \in S_1} \overline{B}_j \mid \bigcap_{j \in S_2} \overline{B}_j\right)} \leq \frac{x_i \prod_{j \in N(i)} (1 - x_j)}{\mathbb{P}\left(\bigcap_{j \in S_1} \overline{B}_j \mid \bigcap_{j \in S_2} \overline{B}_j\right)}. \end{aligned}$$

另一方面, 记 $S_1 = \{j_1, j_2, \dots, j_r\} \subseteq N(i)$, $A := \bigcap_{j \in S_2} \overline{B}_j$, 注意使用归纳假设, 有

$$\begin{aligned} \mathbb{P}\left(\bigcap_{j \in S_1} \overline{B}_j \mid \bigcap_{j \in S_2} \overline{B}_j\right) &= \mathbb{P}(\overline{B}_{j_1} \mid A) \mathbb{P}(\overline{B}_{j_2} \mid \overline{B}_{j_1} \cap A) \cdots \mathbb{P}(\overline{B}_{j_r} \mid \overline{B}_{j_1} \cdots \overline{B}_{j_{r-1}} \cap A) \\ &\geq (1 - x_{j_1})(1 - x_{j_2}) \cdots (1 - x_{j_r}) \geq \prod_{j \in N(i)} (1 - x_j). \end{aligned}$$

因此 $\mathbb{P}(B_i) \leq \frac{x_i \prod_{j \in N(i)} (1 - x_j)}{\prod_{j \in N(i)} (1 - x_j)} = x_i$, 断言得证. □

8.241. 推论. (Erdős - Lovász, 1975) 给定概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$ 以及 n 个事件 $B_1, B_2, \dots, B_n \in \mathcal{F}$, $p \in [0, 1)$, $d \in \mathbb{Z}_{\geq 0}$ 满足如下: 对任意 $i \in [n]$, $\mathbb{P}(B_i) \leq p$, 并且存在 $N(i) \subseteq [n] \setminus \{i\}$ 使得 $|N(i)| \leq d$, 并且 B_i 独立于事件族 $\{B_j \mid j \notin \{i\} \cup N(i)\}$. 如果 $p(d+1) \leq \frac{1}{e}$, 则 $\mathbb{P}(\overline{B}_1 \overline{B}_2 \cdots \overline{B}_n) > 0$.

证明. 对每个 $i \in [n]$, 取 $x_i := \frac{1}{d+1}$, 则

$$x_i \prod_{j \in N(i)} (1 - x_j) = \frac{1}{d+1} \prod_{j \in N(i)} (1 - x_j) \geq \frac{1}{d+1} \left(1 - \frac{1}{d+1}\right)^d$$

$$> \frac{1}{e(d+1)} \geq p \geq \mathbb{P}(A_i),$$

从而 $x_i = \frac{1}{d+1}$ 满足定理 8.240 的条件, 于是 $\mathbb{P}(\overline{B}_1 \overline{B}_2 \cdots \overline{B}_n) \geq \prod_{i=1}^n (1 - x_i) > 0$, 从而得证. \square

接下来看 Lovász 引理的应用.

8.242.定理.(Spencer, 1977) 如果正整数 $n > k > 0$ 满足不等式

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

则 Ramsey 数 $R(k, k) > n$.

证明. 考虑完全图 $G = K_n$ 的随机 2-边染色, 记 K_n 的顶点集为 $[n]$. 对于每个 $R \in \binom{[n]}{k}$, 记事件 E_R : “限制子图 $G|_R$ 是同色完全图”, 则 $\mathbb{P}(E_R) = 2^{1-\binom{k}{2}} =: p$. 对于 $R, S \in \binom{[n]}{k}$, 容易验证事件 E_R 与 E_S 相互独立当且仅当 $|R \cap S| \leq 1$. 更进一步, 对每个 $R \in \binom{[n]}{k}$, 记指标集 $N_R := \left\{ S \in \binom{[n]}{k} \mid |R \cap S| \geq 2 \right\}$, 则容易验证事件 E_R 独立于事件族 $\{E_S \mid S \notin N_R \cup \{R\}\}$. 再注意

$$|N_R| = \# \left\{ S \in \binom{[n]}{k} \mid |R \cap S| \geq 2 \right\} \leq \binom{k}{2} \binom{n}{k-2} =: d.$$

由题设可知 $p(d+1) < \frac{1}{e}$, 因此由 Lovász 引理 8.241 立刻得到 $\mathbb{P}\left(\bigcap_{R \in \binom{[n]}{k}} \overline{E}_R\right) > 0$, 从而存在 K_n 的 2-边染色, 使得在该染色不存在同色 K_k , 因此 $R(k, k) > n$. \square

8.243.推论. 当正整数 $k \rightarrow \infty$ 时, Ramsey 数 $R(k, k)$ 满足

$$R(k, k) > \left(\frac{\sqrt{2}}{e} + o(1) \right) k \cdot 2^{k/2}.$$

证明. 与8.207, 8.222完全类似, 留给读者练习. \square

相比于8.222, 这里将 $R(k, k)$ 的下界又扩大了 $\sqrt{2}$ 倍. 这是人类迄今为止对 $R(k, k)$ 下界的最佳估计.

8.244. Lovász 引理的另一个应用是研究“超图 2-染色问题”(回忆8.213). 设 $H^{(r)} = (V, E)$ 为 r -超图. 我们知道, 边数 $|E|$ 越大, 超图就越“不太可能 2-染色”; 但考虑一种极端情况: 如果对任意 $e_1, e_2 \in E$ 都有 $e_1 \cap e_2 = \emptyset$, 则该超图显然可 2-染色(即使边数 $|E|$ 可能非常大). 可见, 影响超图“可 2-染色性”的因素不仅仅是边数, 还有边与边的“位置关系”(是否相交).

8.245.定理.(Erdős-Lovász, 1975). 设 $H^{(r)} = (V, E)$ 为 r -超图, 并且每条边都至多与其他 $\frac{2^{r-1}}{e} - 1$ 条边相交, 则 $H^{(r)}$ 可 2-染色.

证明. 将超图 $H^{(r)}$ 的每个顶点以 $\frac{1}{2}$ 的概率独立地随机染为红或蓝色. 对每条边 $f \in E$, 记事件 B_f : “ f 的所有端点颜色相同”, 则 $\mathbb{P}(B_f) = 2^{1-r} =: p$; 再记 $N(f) := \{f' \in E \setminus \{f\} \mid f \cap f' \neq \emptyset\}$, 则由题设知 $|N(f)| \leq d := \frac{2^{k-1}}{e} - 1$, 并且事件 B_f 独立于事件族 $\{B_{f'} \mid f' \in E, f' \notin N(f) \cup \{f\}\}$. 注意到 $p(d+1) = 2^{1-r} \frac{2^{r-1}}{e} = \frac{1}{e}$, 因此由 Lovász 引理立刻得到 $\mathbb{P}\left(\bigcap_{f \in E} \overline{B}_f\right) > 0$, 因此 $H^{(r)}$ 可 2-染色. \square

9. 极值集合论 II: 线性代数方法

本章介绍线性代数的如下基本事实

已知 V 是某个域 \mathbb{F} 上的有限维线性空间, $\{v_1, v_2, \dots, v_m\}$ 是 V 中的线性无关向量组, 则 $m \leq \dim_{\mathbb{F}} V$

在组合数学(尤其是极值集合论)中的应用.

9.1 奇偶镇问题与 Fisher 不等式

设想在某一个小镇里有若干做题家, 这些做题家们根据兴趣爱好组建了若干学习小组. 如果每个小组恰有奇数个成员, 并且任何两个不同小组的

公共成员恰有偶数个, 则称这个小镇是“奇偶镇”. 关于“奇偶镇”, 有如下经典结果:

9.246.定理. 设 n 为正整数, 集族 $\mathcal{F} \subseteq 2^{[n]}$ 满足如下性质:

1. 对任意 $A \in \mathcal{F}$, $|A|$ 为奇数;
2. 对任意 $A \neq B \in \mathcal{F}$, $|A \cap B|$ 为偶数,

则 $|\mathcal{F}| \leq n$.

证明. 对于每个 $A \in \mathcal{F}$, 定义有限域 \mathbb{F}_2 上的 n 维向量 $\mathbf{1}_A \in (\mathbb{F}_2)^n$ 如下:

$$\mathbf{1}_A(i) = \begin{cases} 1 & i \in A \\ 0 & i \notin A \end{cases}, \quad \forall i \in [n].$$

断言: 向量组 $\{\mathbf{1}_A \mid A \in \mathcal{F}\}$ \mathbb{F}_2 -线性无关, 从而该向量组的向量个数 $|\mathcal{F}| \leq \dim(\mathbb{F}_2)^n = n$. 下证断言. 引入 $(\mathbb{F}_2)^n$ 上的二次型 “ \cdot ” 如下: 对于向量 $\mathbf{v} = (v_1, \dots, v_n)$, $\mathbf{w} = (w_1, \dots, w_n)$, 令 $\mathbf{v} \cdot \mathbf{w} := \sum_{i=1}^n v_i w_i$. 则由题设条件易知, 对任意 $A \neq B \in \mathcal{F}$,

$$\mathbf{1}_A \cdot \mathbf{1}_A = 1, \quad \mathbf{1}_A \cdot \mathbf{1}_B = 0,$$

由此易证断言. 得证. □

此外注意, 上述定理中的不等号可以取到. 例如, 集族 $\mathcal{F} := \{\{i\} \mid i \in [n]\}$ 满足题设条件, 并且 $|\mathcal{F}| = n$. 除了这个平凡的例子, 由证明过程可以看出, $(\mathbb{F}_2)^n$ 的任何一组“正交基”都可视为满足题设条件的集族.

除了上述“奇偶镇”, 当然还可以考虑“偶奇镇”, “偶偶镇”等.

9.247.定理. 设 n 为正整数, 集族 $\mathcal{F} \subseteq 2^{[n]}$ 满足如下性质:

1. 对任意 $A \in \mathcal{F}$, $|A|$ 为偶数;
2. 对任意 $A \neq B \in \mathcal{F}$, $|A \cap B|$ 为奇数,

则 $|\mathcal{F}| \leq n$.

这个问题与上一题看上去非常相似 (注意它们的区别), 但实际上更加复杂.

证明. 先证明 $|\mathcal{F}| \leq n+1$. 记集族 $\mathcal{F}^* := \{A \cup \{n+1\} \mid A \in \mathcal{F}\} \subseteq 2^{[n+1]}$, 则易知 \mathcal{F}^* 满足上一题的题设条件, 从而 $|\mathcal{F}| = |\mathcal{F}^*| \leq n+1$. 接下来只需证明 $|\mathcal{F}| \neq n+1$. 反证法, 如果 $\mathcal{F} = \{A_1, A_2, \dots, A_{n+1}\}$, 沿用上题记号, 则 $(\mathbb{F}_2)^n$ 中的向量组 $\{\mathbf{1}_{A_i}\}_{i=1}^{n+1}$ 线性相关, 因此存在不全为 0 的常数 $\alpha_i \in \mathbb{F}_2$ ($i \in [n+1]$) 使得 $\sum_{i=1}^{n+1} \alpha_i \mathbf{1}_{A_i} = \mathbf{0}$. 另一方面, 由题设条件可知

$$\mathbf{1}_{A_i} \cdot \mathbf{1}_{A_j} = \begin{cases} 1 & i \neq j \\ 0 & i = j \end{cases}, \quad \forall i, j \in [n+1],$$

因此易知

$$\left(\sum_{i=1}^{n+1} \alpha_i \right) - \alpha_j = 0, \quad \forall j \in [n+1],$$

特别地, n 是偶数, 并且 $\alpha_1 = \alpha_2 = \dots = \alpha_{n+1} = 1$, $\sum_{i=1}^{n+1} \mathbf{1}_{A_i} = \mathbf{0}$. 注意 n 是偶数, 则容易验证集合族 $\mathcal{F}^c := \{A_i^c \mid i \in [n+1]\}$ 也满足题设条件, 其中 $A_i^c := [n] \setminus A_i$, 因此同理也有 $\sum_{i=1}^{n+1} \mathbf{1}_{A_i^c} = \mathbf{0}$, 从而

$$\mathbf{0} = \sum_{i=1}^{n+1} (\mathbf{1}_{A_i} + \mathbf{1}_{A_i^c}) = \sum_{i=1}^{n+1} \mathbf{1}_{[n+1]},$$

从而 $n+1$ 是偶数, 这与 n 是偶数矛盾. 从而得证. \square

上述定理中, $|\mathcal{F}|$ 可以取到上界 n . 例如 \mathcal{F} 为圈 C_n 的边集 (记号见 4.108).

9.248.定理. (Babai-Frankl, 1992) 设 n 为正整数, 集族 $\mathcal{F} \subseteq 2^{[n]}$ 满足如下:

1. 对任意 $A \in \mathcal{F}$, $|A|$ 为偶数;
2. 对任意 $A \neq B \in \mathcal{F}$, $|A \cap B|$ 为偶数,

则 $|\mathcal{F}| \leq 2^{\lfloor \frac{n}{2} \rfloor}$.

证明. 仍记 $\mathcal{F} = \{A_1, \dots, A_m\}$, 对每个 $i \in [m]$, 与9.246一样, 考虑向量 $\mathbf{1}_{A_i} \in (\mathbb{F}_2)^n$. 则题设条件表明 $\mathbf{1}_{A_i} \cdot \mathbf{1}_{A_j} = 0, \forall i, j \in [m]$. 记 $\mathbb{F}_2^n := (\mathbb{F}_2)^n$ 的子空间 $U := \text{span}_{\mathbb{F}_2} \{\mathbf{1}_{A_i} \mid i \in [m]\}$. 令 $(\mathbb{F}_2^n)^*$ 为 \mathbb{F}_2^n 的对偶空间. 通过二次型 \cdot , 自然将 \mathbb{F}_2^n 与 $(\mathbb{F}_2^n)^*$ 等同. 考虑子空间 U 的正交补

$$U^\perp := \{f \in (\mathbb{F}_2^n)^* \mid f(v) = 0, \forall v \in U\} \subseteq (\mathbb{F}_2^n)^*,$$

则由题设条件可知 $U \subseteq U^\perp$, 从而 $\dim U \leq \dim U^\perp$. 以下结论众所周知:

设 V 为域 \mathbb{F} 上的有限维线性空间, U 是 V 的线性子空间, $U^\perp \subseteq V^*$ 是 U 的正交补, 则 $\dim U + \dim U^\perp = \dim V$.

将此结论用于本题, 有

$$n = \dim \mathbb{F}_2^n = \dim U + \dim U^\perp \geq 2 \dim U,$$

从而 $\dim U \leq \lfloor \frac{n}{2} \rfloor$. 因此 $|\mathcal{F}| \leq |U| = 2^{\dim U} \leq 2^{\lfloor \frac{n}{2} \rfloor}$, 得证. \square

下面介绍线性代数方法的另一个应用——组合设计中的 Fisher 不等式.

上述定理中的上界 $2^{\lfloor \frac{n}{2} \rfloor}$ 可以取到. 记 $k := \lfloor \frac{n}{2} \rfloor$, 对每个 $i \in [k]$, 记集合

$A_i = \{2i-1, 2i\} \subseteq [n]$. 令 $\mathcal{F} := \left\{ \bigcup_{i \in J} A_i \mid J \subseteq [k] \right\}$, 则 \mathcal{F} 满足题设条件, 且 $|\mathcal{F}| = 2^{\lfloor \frac{n}{2} \rfloor}$.

9.249.定理.(Fisher 不等式). 设正整数 $n \geq k > 0$, 子集族 $\mathcal{F} \subseteq 2^{[n]}$ 满足: 任意 $A \neq B \in \mathcal{F}, |A \cap B| = k$, 则 $|\mathcal{F}| \leq n$.

证明. (Babai-Frankl, 1992). 记 $\mathcal{F} = \{A_1, A_2, \dots, A_m\}$, 对每个 $i \in [m]$, 记向量 $\mathbf{v}_i := \mathbf{1}_{A_i} \in \mathbb{R}^n$, 其中 \mathbf{v}_i 的第 j 分量 $\mathbf{v}_i(j) := \begin{cases} 1 & j \in A_i \\ 0 & j \notin A_i \end{cases}$ (注意这里是 \mathbb{R} -向量, 而不再是 \mathbb{F}_2 -向量), $\forall j \in [n]$. 断言: 向量组 $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ \mathbb{R} -线性无关, 从而 $|\mathcal{F}| = m \leq \dim_{\mathbb{R}} \mathbb{R}^n = n$, 完成证明.

下证断言. 如果 $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ 线性相关, 则存在不全为 0 的实数 $\lambda_1, \dots, \lambda_m$ 使得 $\sum_{i=1}^m \lambda_i \mathbf{v}_i = \mathbf{0}$. 另一方面, 考察 \mathbb{R}^n 的标准欧氏内积 \cdot , 注意 $\mathbf{v}_i \cdot \mathbf{v}_j =$

$$\begin{cases} |A_i| & i = j \\ k & i \neq j \end{cases}, \text{ 并且显然 } |A_i| \geq k, \text{ 从而}$$

$$\begin{aligned} 0 &= \left(\sum_{i=1}^m \lambda_i \mathbf{v}_i \right) \cdot \left(\sum_{i=1}^m \lambda_i \mathbf{v}_i \right) = \sum_{i=1}^m \lambda_i^2 |A_i| + 2k \sum_{i < j} \lambda_i \lambda_j \\ &= \sum_{i=1}^m \lambda_i^2 (|A_i| - k) + k \left(\sum_{i=1}^m \lambda_i^2 + 2 \sum_{i < j} \lambda_i \lambda_j \right) \\ &= \sum_{i=1}^m \lambda_i^2 (|A_i| - k) + k \left(\sum_{i=1}^m \lambda_i \right)^2 > 0, \end{aligned}$$

矛盾. 故断言得证. \square

9.250. 习题.(De Bruijn-Erdős). 设 $P = \{x_1, x_2, \dots, x_n\}$ 是平面 \mathbb{R}^2 的有限点集. 如果 P 中所有的点不在同一条直线上, 则两两连接 P 中的点, 至少能确定 n 条不同直线.

证明. 记 $L := \{\ell \subseteq \mathbb{R}^2 \text{ 是直线} \mid |\ell \cap P| \geq 2\}$, 即两两连接 P 中的点所确定的全部直线构成的集合. 对每个 $i \in [n]$, 记 $L_i := \{\ell \in L \mid x_i \in \ell\}$. 注意任何两个不同的点确定唯一一条直线, 从而

$$|L_i \cap L_j| = 1 \quad \forall i \neq j,$$

此外再注意, 集合 L_1, L_2, \dots, L_n 两两互异 (否则只可能 P 中的点在同一条直线上), 因此集合族 $\mathcal{L} := \{L_1, L_2, \dots, L_n\}$ 满足 $|\mathcal{L}| = n$. 对集合族 \mathcal{L} 使用 Fisher 不等式 9.249, 可知 $|\mathcal{L}| \leq |L|$, 即 $|L| \geq n$, 得证. \square

9.251. 习题.(Nagy, 1972) 给定正整数 n , 定义图 $G = (V, E)$ 如下:

- 顶点集 $V = \binom{n}{3}$,
- 边集 $E = \left\{ \{A, B\} \in \binom{V}{2} \mid |A \cap B| = 1 \right\}$,

则图 G 不含完全子图 K_{n+1} , 也不含独立子集 I_{n+1} . 从而推出 Ramsey 数

$$R(n+1, n+1) > \binom{n}{3}.$$

证明. 若图 G 的 m 个顶点 A_1, \dots, A_m 两两相邻, 则子集族 $\mathcal{A} = \{A_1, \dots, A_m\} \subseteq 2^{[n]}$ 满足 $|A_i \cap A_j| = 1, \forall i \neq j$, 因此由 Fisher 不等式可知 $m = |\mathcal{A}| \leq n$, 换言之, 图 G 的完全子图的顶点数不超过 n . 而如果 $\{A_1, \dots, A_m\}$ 两两不相邻, 则当 $i \neq j$ 时 $|A_i| \cap A_j$ 只可能为偶数, 从而由 9.246 可知 $m \leq n$, 换言之, 图 G 的独立子集的顶点数也不超过 n . 得证. \square

我们曾用概率方法 (8.207, 8.222, 8.243) 不断刷新 Ramsey 数 $R(k, k)$ 的下界, 得到了迄今为止人类已知最佳结果. 本题对 Ramsey 数的估计结果虽然远不如概率方法, 但它的证明方法是具体构造, 而非仅仅说明存在性. 这种具体构造也具有相当的价值.

9.2 欧氏空间 \mathbb{R}^n 中的 2-距离点集

9.252. 引理. 设 $A := \{\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_m\}$ 是 n 维欧氏空间 \mathbb{R}^n 的有限点集, 如果 A 中任何两点之间的距离都相等, 则 $m \leq n$ (换言之, $|A| \leq n + 1$).

这是众所周知的结论, 而且容易用数学归纳法证明, 当取到等号时, A 是某个正单纯形的顶点集, 特别地, $n = 2$ 时 A 为正三角形的顶点集, $n = 3$ 时 A 为正四面体的顶点集. 不过, 我们在此用线性代数方法给出此定理的另证.

证明. 不妨 A 中任何两点的距离都为 1. 对每个 $i \in [m]$, 记向量 $\mathbf{v}_i := \overrightarrow{\mathbf{a}_0 \mathbf{a}_i}$, 则 $\mathbf{v}_i \cdot \mathbf{v}_i = 1$. 再注意当 $i \neq j$ 时 $1 = \|\mathbf{a}_i - \mathbf{a}_j\|^2 = (\mathbf{v}_i - \mathbf{v}_j) \cdot (\mathbf{v}_i - \mathbf{v}_j)$, 从而易知 $\mathbf{v}_i \cdot \mathbf{v}_j = \frac{1}{2}$. 则容易验证 m 阶实对称方阵

$$G := (G_{ij}), \quad G_{ij} = \mathbf{v}_i \cdot \mathbf{v}_j = \begin{cases} 1 & i = j \\ \frac{1}{2} & i \neq j \end{cases}$$

行列式非零, 从而可逆, 由此推出向量组 $\{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subseteq \mathbb{R}^n$ 线性无关, 故 $m \leq \dim \mathbb{R}^n = n$, 得证. \square

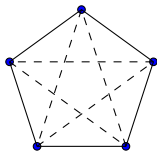
将上述问题稍加推广, 我们考虑这样的问题:

9.253. 定义. 设 $A \subseteq \mathbb{R}^n$, 如果 $\#\{\|\mathbf{a} - \mathbf{b}\| \mid \mathbf{a} \neq \mathbf{b} \in A\} \leq 2$, 则称 A 是欧氏空间 \mathbb{R}^n 的 2-距离点集.

换言之, A 是 2-距离点集当且仅当 A 的所有的点之间至多有两种不同的距离. 容易证明, \mathbb{R}^n 的 2-距离点集一定是有限集 (中学数学简单习题, 考虑抽屉原理), 从而自然提出这样的问题: \mathbb{R}^n 的 2-距离点集最多可以有多少个点? 我们将 \mathbb{R}^n 的 2-距离点集的元素个数的最大值记作 a_n , 即

$$a_n := \max \{|X| \mid X \subseteq \mathbb{R}^n \text{ 为 2-距离点集}\}.$$

显然 $a_1 = 3$. 此外容易证明 $a_2 = 5$, 这是因为: 一方面注意下图



是 \mathbb{R}^2 的由 5 个点构成的 2-距离点集, 从而 $a_2 \geq 5$; 另一方面, 如果 $X \subseteq \mathbb{R}^2$ 是 2-距离的, 并且至少有 6 个点, 则由 7.178 (即, $R(3, 3) = 6$) 可知, 其中必有 3 个点构成某正三角形的顶点, 再之后的细节留给读者.

一般地, 计算 a_n 的具体数值也是极端恐怖困难的问题. 我们退而求其次, 希望给出 a_n 的较好估计. 首先, 我们通过具体构造来估计 a_n 的下界:

9.254. 习题. 证明: $a_n \geq \binom{n+1}{2}$, 其中 a_n 的定义见 9.253.

证明. 考虑集族 $\mathcal{F} := \left\{ \binom{[n+1]}{2} \right\}$, 对于每个 $F \in \mathcal{F}$, 记 \mathbb{R}^{n+1} 的点 $\mathbf{1}_F := (x_1, \dots, x_{n+1})$, 使得

$$x_i = \begin{cases} 1 & i \in F \\ 0 & i \notin F \end{cases}, \quad \forall i \in [n+1],$$

则容易验证集合 $A := \{\mathbf{1}_F \mid F \in \mathcal{F}\}$ 是 \mathbb{R}^{n+1} 的 2-距离点集, 且 $|A| = \binom{n+1}{2}$. 考虑 \mathbb{R}^{n+1} 的 n 维超平面

$$\Pi := \left\{ (x_1, \dots, x_{n+1}) \in \mathbb{R}^{n+1} \mid \sum_{i=1}^{n+1} x_i = 2 \right\},$$

将 Π 与 \mathbb{R}^n 等同. 注意 $A \subseteq \Pi$, 从而 A 自然视为 $\Pi \cong \mathbb{R}^n$ 的 2-距离点集. 这表明 $a_n \geq \binom{n+1}{2}$, 得证. \square

而对 a_n 的上界估计就非常有趣了, 这要用到更多的线性代数方法:

9.255. 利用向量组的线性无关性来研究组合问题, 首先要适当选取线性空间. 而 n 元多项式构成的线性空间格外重要. 容易证明以下事实:

给定域 \mathbb{F} , 正整数 m 以及非空集合 Ω , 设函数 $f_1, \dots, f_m: \Omega \rightarrow \mathbb{F}$, 如果存在 Ω 中的 m 个不同元素 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$, 使得

$$f_i(\mathbf{v}_i) \neq 0, \quad f_i(\mathbf{v}_j) = 0, \quad \forall i > j \in [m],$$

则 $\{f_1, \dots, f_m\}$ \mathbb{F} -线性无关.

证明上述断言, 只需注意方阵 $(f_i(\mathbf{v}_j)) \in \mathbb{F}^{m \times m}$ 是上三角阵, 且对角元非零. 特别地, Ω 常取为 \mathbb{F}^n , 函数 f_1, \dots, f_m 为其上的 n 元多项式函数.

9.256.定理.(Larman-Rogers-Seidel, 1977) 数列 a_n 的含义见 9.253, 则成立

$$a_n \leq \frac{1}{2}(n+1)(n+4).$$

证明. 取 \mathbb{R}^n 的一组标准正交基 $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$, 若 $A = \{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_m\} \subseteq \mathbb{R}^n$ 为 2-距离点集, 其两两之间的距离为 c 或 d , 再记

$$\mathbf{a}_i = \sum_{k=1}^n a_{ik} \mathbf{e}_k, \quad \forall i \in [m].$$

对每个 $i \in [m]$, 定义 \mathbb{R}^n 上的多项式 $f_i(\mathbf{x}) \in \mathbb{R}[x_1, \dots, x_n]$ 如下

$$\begin{aligned} f_i(\mathbf{x}) &:= (\|\mathbf{x} - \mathbf{a}_i\|^2 - c^2)(\|\mathbf{x} - \mathbf{a}_i\|^2 - d^2) \\ &= \left(\sum_{k=1}^n x_k^2 - 2 \sum_{k=1}^n a_{ik} x_k + \tilde{c} \right) \left(\sum_{k=1}^n x_k^2 - 2 \sum_{k=1}^n a_{ik} x_k + \tilde{d} \right), \end{aligned}$$

其中 $\tilde{c} := \sum_{k=1}^n a_{ik}^2 - c^2$, $\tilde{d} := \sum_{k=1}^n a_{ik}^2 - d^2$ 为常数. 容易验证,

$$f_i(\mathbf{a}_j) = \begin{cases} 0 & i \neq j \\ c^2 d^2 & i = j \end{cases}, \quad \forall i, j \in [m],$$

从而由9.255可知多项式族 $F := \{f_1, f_2, \dots, f_m\}$ \mathbb{R} -线性无关, 此外 $|F| = m$. 考虑多项式空间 $\mathbb{R}[x_1, \dots, x_n]$ 的如下子空间:

$$V := \text{span} \left\{ \left(\sum_{k=1}^n x_k^2 \right)^2, x_i \left(\sum_{k=1}^n x_k^2 \right), x_i x_j, x_i, 1 \mid 1 \leq i \leq j \leq n \right\},$$

则 $\dim V = 1 + n + \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+4)}{2}$. 再注意 $F \subseteq V$, 从而

$$m = |F| \leq \dim V = \frac{(n+1)(n+4)}{2},$$

定理得证. □

可以继续改进上述证明, 从而刷新 a_n 的上界:

9.257.定理.(Blokhuys, 1984) 数列 a_n 的含义见9.253, 则成立

$$a_n \leq \frac{1}{2}(n+1)(n+2).$$

证明. 继续使用9.256的记号. 事实上, 可以证明多项式族 $\{f_1, \dots, f_m; x_1, \dots, x_n; 1\} \subseteq V$ 线性无关, 从而得证. 现在只需证明此断言. 假设存在常数 $\lambda_1, \dots, \lambda_m; \mu_1, \dots, \mu_n$ 以及 $\omega \in \mathbb{R}$, 使得

$$\sum_{i=1}^m \lambda_i f_i(\mathbf{x}) + \sum_{k=1}^n \mu_k x_k + \omega \equiv 0 \quad (1)$$

恒成立, 则将 $\mathbf{x} = \mathbf{a}_i$ 代入 (1) 式可得

$$c^2 d^2 \lambda_i + \sum_{k=1}^n \mu_k a_{ik} + \omega = 0, \quad \forall i \in [m]. \quad (2)$$

另一方面, 对于任意参数 $t \in \mathbb{R}$, 将 $\mathbf{x} = t\mathbf{e}_k$ 代入 (1) 式, 得

$$\sum_{i=1}^m \lambda_i (t^2 - 2ta_{ik} + \|\mathbf{a}_i\|^2 - c^2) (t^2 - 2ta_{ik} + \|\mathbf{a}_i\|^2 - d^2) + t\mu_k + \omega = 0,$$

比较上式两边 t^4, t^3 的系数, 可知

$$\sum_{i=1}^m \lambda_i = 0, \quad \sum_{i=1}^m \lambda_i a_{ik} = 0 \quad (3)$$

对任意 $k \in [n]$ 都成立. 现在, 将 (2) 两边同乘 λ_i 并对 i 求和, 利用 (3) 可得 $c^2 d^2 \sum_{i=1}^m \lambda_i^2 = 0$, 因此 $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$. 之后易知 $\mu_1 = \cdots = \mu_n = \omega = 0$, 从而断言得证. \square

9.3 代数簇与 L -相交族

本节介绍“线性无关方法”的更进一步应用. 我们回忆, 9.255给出了判断一族函数 $f_i: \Omega \rightarrow \mathbb{F}$ 线性无关的一个充分条件. 函数 f_i 的定义域 Ω 通常取为有限维线性空间 \mathbb{F}^n , 就像在9.256当中那样. 然而, Ω 的选取并不仅限于 \mathbb{F}^n , 可以取成更一般的空间.

9.258. 我们浅尝一点点古典代数几何学的一些最入门的概念. 设 \mathbb{F} 为域, 我们往往私下里把多项式环 $\mathbb{F}[x_1, \dots, x_n]$ 中的元素想象成空间 \mathbb{F}^n 上的“好的”函数, 换言之, 把 $\mathbb{F}[x_1, \dots, x_n]$ 想象成 \mathbb{F}^n 上的 (具有某种好的性质的) 函数空间. 设 I 为多项式环 $\mathbb{F}[x_1, \dots, x_n]$ 的一个理想, 记 I 中多项式的公共零点集

$$\mathcal{Z}(I) := \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}^n \mid f(\mathbf{x}) = 0, \forall f \in I\}.$$

\mathbb{F}^n 的形如上述的子集称为仿射代数簇. 我们在中学阶段已经接触过很多仿射代数簇的例子, 例如平面中的直线, 圆锥曲线等.

对于 $\mathbb{F}[x_1, \dots, x_n]$ 的理想 I , 商环 $\mathbb{F}[x_1, \dots, x_n]/I$ 有自然的 \mathbb{F} -线性空间结构. 一个重要的观察是, 商环 $\mathbb{F}[x_1, \dots, x_n]/I$ 中的元素能够自然地视为定义在 $\mathcal{Z}(I)$ 上的函数 (留给读者思考). 特别地, 在9.255中, 我们可以把 Ω 取为某个仿射代数簇 $\mathcal{Z}(I) \subseteq \mathbb{F}^n$, 把 f_i 视为 $\mathbb{F}[x_1, \dots, x_n]/I$ 中的元素.

我们来看它在组合数学中的应用.

9.259. 定义. 给定正整数 n , 以及集合 $L \subseteq [n]$. 对于集族 $\mathcal{F} \subseteq 2^{[n]}$, 如果对任意 $A \neq B \in \mathcal{F}$ 都满足 $|A \cap B| \in L$, 则称集族 \mathcal{F} 是 L -相交族.

对于特殊的 L , 我们之前已经见过具体例子:

- 若 L 由 $[n]$ 中全体偶数构成, 则满足9.246的题设的 \mathcal{F} 是 L -相交族.
- 若 L 中只有一个元素 k , 即 $L = \{k\}$, 则满足9.249题设的 \mathcal{F} 是 L -相交族.

对于一般的 L 相交族, 人类有如下结果:

9.260.定理.(Frankl-Wilson, 1981) 给定 $L \subseteq [n]$. 若 $\mathcal{F} \subseteq 2^{[n]}$ 是 L -相交族, 则

$$|\mathcal{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}.$$

证明. 记 $\mathcal{F} = \{A_1, A_2, \dots, A_m\}$, 不妨 $|A_1| \leq |A_2| \leq \dots \leq |A_m|$. 对每个 $i \in [m]$, 考察向量 $\mathbf{1}_{A_i} \in \mathbb{R}^n$, 定义多项式 $f_i(\mathbf{x}) \in \mathbb{R}[x_1, \dots, x_n]$ 如下:

$$f_i(\mathbf{x}) := \prod_{\substack{\ell \in L \\ \ell < |A_i|}} (\mathbf{x} \cdot \mathbf{1}_{A_i} - \ell).$$

则易验证对任意 $i > j \in [m]$,

$$\begin{aligned} f_i(\mathbf{1}_{A_i}) &= \prod_{\substack{\ell \in L \\ \ell < |A_i|}} (|A_i| - \ell) \neq 0 \\ f_i(\mathbf{1}_{A_j}) &= \prod_{\substack{\ell \in L \\ \ell < |A_i|}} (|A_i \cap A_j| - \ell) = 0. \end{aligned}$$

因此由9.255可知多项式族 $\{f_1, \dots, f_m\}$ \mathbb{R} -线性无关.

事实上, 设 I 为 $\mathbb{R}[x_1, \dots, x_n]$ 的由 $\{x_i^2 - x_i \mid i \in [n]\}$ 所生成的理想, 则容易验证 $\mathbf{1}_{A_i} \in \mathcal{Z}(I)$, $\forall i \in [m]$. 记 $\pi: \mathbb{R}[x_1, \dots, x_n] \rightarrow \mathbb{R}[x_1, \dots, x_n]/I$ 为商映射, $\tilde{f}_i := \pi(f_i) \in \mathbb{R}[x_1, \dots, x_n]/I$, $i = 1, \dots, m$. 则 \tilde{f}_i 自然视为 $\mathcal{Z}(I)$ 上的函数. 在9.255中令 $\Omega = \mathcal{Z}(I)$, 类似讨论容易验证 $\{\tilde{f}_1, \dots, \tilde{f}_m\}$ 也是 \mathbb{R} -线性无关的. 考察 $\mathbb{R}[x_1, \dots, x_n]/I$ 的如下 \mathbb{R} -子空间

$$V := \text{span} \{ \pi(x_{i_1} \cdots x_{i_k}) \mid 0 \leq k \leq |L|, 1 \leq i_1 < \dots < i_k \leq n \},$$

则易知 $\{\tilde{f}_1, \dots, \tilde{f}_m\} \subseteq V$, 且 $\dim_{\mathbb{R}} V = \sum_{k=0}^{|L|} \binom{n}{k}$. 之后从略, 得证. □

用同样的方法, 也可以证明以下:

9.261.定理.(Deza - Frankl - Singhi, 1983) 给定正整数 n 与素数 p , 以及集合 $L \subseteq \mathbb{F}_p$. 如果族 $\mathcal{F} \subseteq 2^{[n]}$ 满足以下性质:

- $|A| \notin L \pmod p, \quad \forall A \in \mathcal{F},$
- $|A \cap B| \in L \pmod p, \quad \forall A \neq B \in \mathcal{F},$

则成立 $|\mathcal{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}.$

证明. 与9.260的证明过程完全类似, 只需将 \mathbb{R} 换成有限域 \mathbb{F}_p , 再稍微修改 $f_i(\mathbf{x})$ 的定义即可. 细节留给读者. \square

特别地, p 取 2 时的特殊情形恰为“奇偶镇问题”9.246, 9.247.

9.262.定理.(Frankl-Wilson, 1981) 设 p 为素数, 定义图 G_p 如下:

- 顶点集 $V = \binom{[p^3]}{p^2 - 1},$
- 边集 $E = \left\{ \{A, B\} \in \binom{V}{2} \mid |A \cap B| \not\equiv -1 \pmod p \right\}.$

则 G_p 不含有完全子图 K_{t+1} , 且不含有独立子集 I_{t+1} , 其中 $t := \sum_{i=0}^{p-1} \binom{p^3}{i}.$

证明. 若 $\mathcal{A} = \{A_1, A_2, \dots, A_m\} \subseteq V \subseteq 2^{[p^3]}$ 之中的任何两点都相邻, 则考察 $L := \{0, 1, 2, \dots, p-2\} \subseteq \mathbb{F}_p, |L| = p-1$ 易知 \mathcal{A} 满足9.261的题设, 从而 $m \leq \sum_{i=0}^{p-1} \binom{p^3}{i} = t.$ 若 $\mathcal{B} = \{B_1, B_2, \dots, B_m\} \subseteq V \subseteq 2^{[p^3]}$ 之中的任何两点都不相邻, 则考察 $L := \{p-1, 2p-1, \dots, p^2-p-1\} \subseteq [p^3], |L| = p-1,$ 易知 \mathcal{B} 满足9.260的题设条件, 因此 $m \leq \sum_{i=0}^{p-1} \binom{p^3}{i} = t.$ 证毕. \square

9.263.推论. 存在常数 $C > 0$, 使得当正整数 n 充分大时, Ramsey 数

$$R(n, n) \geq n^{C \frac{\ln n}{\ln \ln n}}.$$

例如, 上式中可以取 $C = 0.02$.

这个渐近下界的估计优于9.251, 但依然远不如概率方法所得.

证明. (应该留给读者练习, 但这里还是打算稍微写一下细节.)

对于正整数 p , 记

$$t_p := \sum_{i=0}^{p-1} \binom{p^3}{i}, \quad N_p := \binom{p^3}{p^2-1},$$

则9.262表明当 p 为素数时成立 $R(t_p+1, t_p+1) > N_p$. 现在, 对于任意充分大的一般的正整数 n , 设 $p = p(n)$ 为使得 $t_p+1 \leq n$ 成立的最大素数, 再令 q 为 p 之后的下一个素数, 则 $t_q+1 > n$. 由数论中关于素数分布的相关结论可知, 当 p 充分大时, $q < 2p$.

• 断言: 当 n 充分大时, 成立不等式

$$p^p < n < p^{5p}. \quad (1)$$

欲证此断言, 首先注意如下众所周知的不等式: 对任意充分大的正整数 m ,

$$\left(\frac{m}{e}\right)^m < m! < m \cdot \left(\frac{m}{e}\right)^m. \quad (2)$$

再注意 p, q 的定义, 以及 $q < 2p$, 可知

$$\begin{aligned} n &< t_q + 1 \leq t_{2p} = \sum_{i=0}^{2p-1} \binom{8p^3}{i} \\ &< 2p \binom{8p^3}{2p} < 2p \cdot \frac{(8p^3)^{2p}}{(2p)!} \\ &< 2p \cdot \frac{(8p^3)^{2p}}{\left(\frac{2p}{e}\right)^{2p}} = 2p \cdot (4ep^2)^{2p} < p^{5p}. \end{aligned}$$

类似地, 从 $n > t_p + 1$ 出发, 并利用 (2) 式, 可得

$$\begin{aligned} n &\geq t_p + 1 = 1 + \sum_{i=0}^{p-1} \binom{p^3}{i} > \binom{p^3}{p-1} = \frac{(p^3)!}{(p-1)!(p^3-p+1)!} \\ &> \frac{(p^3)^{p^3}}{(p-1)^p(p^3-p+1)^{p^3-p+2}} > \frac{p^{3p^3}}{p^p \cdot p^{3(p^3-p+2)}} = p^{2p-6} > p^p. \end{aligned}$$

• 断言: $p > \frac{1}{5} \cdot \frac{\ln n}{\ln \ln n}$. (这是不等式 (1) 的直接推论, 留给读者).

综上所述,我们有:

$$\begin{aligned}
 R(n, n) &\geq R(t_p + 1, t_p + 1) > N_p = \binom{p^3}{p^2 - 1} \\
 &= \frac{(p^3)!}{(p^2 - 1)!(p^3 - p^2 + 1)!} > \frac{(p^3)^{p^3}}{(p^2 - 1)^{p^2}(p^3 - p^2 + 1)^{p^3 - p^2 + 2}} \\
 &> \frac{p^{3p^2}}{p^{2p^2} \cdot p^{3(p^3 - p^2 + 2)}} = p^{p^2 - 6} > p^{\frac{1}{2}p^2} = (p^{5p})^{\frac{1}{10p}} \\
 &> n^{\frac{1}{50} \cdot \frac{\ln n}{\ln \ln n}}.
 \end{aligned}$$

从而常数 C 可以取 $\frac{1}{50} = 0.02$, 命题得证. \square

9.4 矩曲线与 Bollobás 定理的变式

9.264. 设 \mathbb{F} 是无限域, n 为正整数, 则 \mathbb{F}^n 中的曲线

$$\mathbf{m}_n = \{(1, a, a^2, \dots, a^{n-1}) \in \mathbb{F}^n \mid a \in \mathbb{F}\}$$

称为**矩曲线**. 容易验证矩曲线满足如下性质:

\mathbf{m}_n 上的任何 n 个不同向量都 \mathbb{F} -线性无关.

上述断言的证明是容易的, 是众所周知的 **Vandermonde** 行列式的直接推论. 矩曲线的上述性质也可以用来解决组合数学问题.

9.265. 定理. 如果 $2m$ 个有限集 $A_1, A_2, \dots, A_m; B_1, B_2, \dots, B_m$ 同时满足如下性质

- $A_i \cap B_i = \emptyset, A_i \cap B_j \neq \emptyset, \forall 1 \leq i < j \leq m;$
- 存在正整数 r, s , 使得 $\forall i \in [m]$, 都有 $|A_i| = r, |B_i| = s,$

那么必有 $m \leq \binom{r+s}{r}.$

读者可将此定理的与 Bollobás 定理**3.91**相比较.

证明. 记 $X := \bigcup_{i=1}^m (A_i \cup B_i)$, 任取矩曲线 $\mathbf{m}_{r+1} \subseteq \mathbb{R}^{r+1}$ 中的 $|X|$ 个不同点, 并与 X 建立一一对应. 从而, 集合 A_i, B_j 中的元素可以视作 \mathbf{m}_{r+1} 上的向量.

对每个 $i \in [m]$, 定义多项式

$$f_i(\mathbf{x}) := \prod_{\mathbf{v} \in B_i} (\mathbf{x} \cdot \mathbf{v}) \in \mathbb{R}[x_0, x_1, \dots, x_r].$$

则 f_i 是 s 次齐次多项式, 从而

$$f_i \in V := \text{span} \{x_0^{i_0} x_1^{i_1} \cdots x_r^{i_r} \mid i_0 + i_1 + \cdots + i_r = s, i_j \geq 0\},$$

而易知 $\dim V = \binom{r+s}{r}$. 于是, 只需再说明多项式族 $\{f_1, f_2, \dots, f_m\}$ 线性无关.

特别注意 A_i 是由 r 个线性无关的向量组成的集合, 其张成的子空间 $\Pi_i := \text{span} A_i$ 的余维数为 1; 对每个 $i \in [m]$, 取定超平面 Π 的法向量 $\mathbf{a}_i \in \mathbb{R}^{r+1}$. 注意到, 对于 $\mathbf{v} \in \mathbb{R}^{r+1}$ 以及 $i, j \in [m]$, 则 $f_i(\mathbf{a}_j) = 0$ 当且仅当存在 $\mathbf{b} \in B_i$ 使得 $\mathbf{b} \perp \mathbf{a}_j$, 这当且仅当 $\mathbf{b} \in \mathbf{a}_j^\perp = \Pi_j := \text{span} A_j$; 而另一方面, 矩曲线 \mathbf{m}_{r+1} 上的任何 $r+1$ 个向量都线性无关, 但 $\dim \Pi_j = r$, 这就迫使 $\mathbf{b} \in A_j$. 于是, $f_i(\mathbf{a}_j) = 0$ 当且仅当 $A_j \cap B_i \neq \emptyset$. 从而由题设条件以及 9.255 可知多项式族 $\{f_1, \dots, f_m\}$ 线性无关, 得证.

□

10. 谱方法

本章依然介绍线性代数在组合数学中的应用. 相比上一章的“线性无关方法”, 本章将建立组合数学对象与矩阵的联系, 并着重运用矩阵特征值 (也称为“谱”) 与特征向量的相关知识来研究组合问题.

10.1 图的邻接矩阵与谱

图可以用矩阵来表示:

10.266. 定义. 设 $G = (V, E)$ 为图, 顶点集 $V = \{v_1, v_2, \dots, v_n\}$, 定义 n 阶实方阵 $A_G = (a_{ij}) \in \mathbb{R}^{n \times n}$ 如下:

$$a_{ij} := \begin{cases} 1 & v_i \sim_E v_j \\ 0 & v_i \not\sim_E v_j \end{cases}.$$

矩阵 A_G 称为图 G 的邻接矩阵.

邻接矩阵的每个矩阵元都为 0 或 1. 根据定义可知, 邻接矩阵的第 i 行第 j 列非零, 当且仅当图 G 的第 i 和第 j 个顶点有边相连. 注意 A_G 是对称矩阵, 且对角元全为 0, 从而 $\text{tr} A_G = 0$. 由实对称矩阵的性质可知, A_G 有 n 个 (计重数) 实特征值

$$\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n,$$

并且存在 \mathbb{R}^n 的一组单位正交基 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in \mathbb{R}^n$, 使得

$$A_G \mathbf{v}_i = \mu_i \mathbf{v}_i, \quad \forall i \in [n].$$

A_G 的特征值 $\mu_1, \mu_2, \dots, \mu_n$ 称为图 G 的谱.

特别注意 $\sum_{i=1}^n \mu_i = \text{tr} A_G = 0$, 从而最大谱 $\mu_1 \geq 0$, 最小谱 $\mu_n \leq 0$.

10.2 Laplace 矩阵与 Kirchhoff 矩阵树定理 (待重写)

图可以用矩阵来描述. 以下两种描述方法都简单粗暴 (无比自然).

10.267.定义. 设 $G = (V, E)$ 是图, $V = \{v_1, \dots, v_n\}$, $E = \{e_1, \dots, e_m\}$. 则

- 定义矩阵 $A = A(G) = (a_{ij}) \in \mathbb{R}^{n \times n}$ 如下

$$a_{ij} := \begin{cases} 1 & \text{如果 } i \neq j \text{ 且 } v_i, v_j \text{ 有边相连} \\ 0 & \text{其余情况} \end{cases},$$

称为图 G 的邻接矩阵.

- 定义矩阵 $N = N(G) = (n_{ij}) \in \mathbb{R}^{n \times m}$ 如下

$$n_{ij} := \begin{cases} 1 & \text{若顶点 } v_i \text{ 是边 } e_j \text{ 的端点} \\ 0 & \text{其余情况} \end{cases},$$

称为图 G 的关联矩阵.

由定义可知, 邻接矩阵 \mathbf{A} 一定是对称矩阵. 而关联矩阵在描述图 G 的子图上更有优势: 容易看出, 删去 G 的某些边所得子图的关联矩阵, 恰为删去 G 的关联矩阵的相应的列所得子矩阵. 我们回忆, 图 G 由一类特殊的子图, 叫做**生成树**, 见4.129, 生成树包含 G 的全部顶点以及某一部分的边. 反映在关联矩阵上, 生成树对应于 \mathbf{N} 的某些 $n \times (n-1)$ -子矩阵.

除了邻接矩阵和关联矩阵, 另一个重要的矩阵如下:

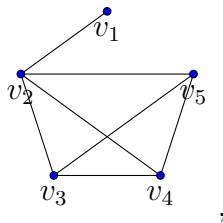
10.268.定义. 设 $G = (V, E)$ 为图, 其中顶点集 $V = \{v_1, v_2, \dots, v_n\}$. 则记 n 阶实方阵 $\mathbf{L} = \mathbf{L}(G) = (\ell_{ij}) \in \mathbb{R}^{n \times n}$ 如下:

$$\ell_{ij} = \begin{cases} d_G(v_i) & \text{若 } i = j; \\ -1 & \text{若 } i \neq j \text{ 且 } v_i \sim_E v_j, \\ 0 & \text{其余情况} \end{cases}$$

称为图 G 的**Laplace 矩阵**.

换言之, $\mathbf{L} = \mathbf{D} - \mathbf{A}$, 其中对角矩阵 $\mathbf{D} := \begin{pmatrix} d_G(v_1) & & & & \\ & d_G(v_2) & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & d_G(v_n) \end{pmatrix},$

\mathbf{A} 是 G 的邻接矩阵. 注意 $\mathbf{L}(G)$ 与图 G 的顶点编号顺序有关. 在相差顶点编号顺序意义下, 其 Laplace 矩阵相差行列置换. 例如, 如果 $G = (V, E)$ 如下图所示



则其 Laplace 矩阵 $\mathbf{L}(G) = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ -1 & 4 & -1 & -1 & -1 \\ 0 & -1 & 3 & -1 & -1 \\ 0 & -1 & -1 & 3 & -1 \\ 0 & -1 & -1 & -1 & 3 \end{pmatrix}.$

10.269.性质. 对于图 G , 则其 Laplace 矩阵 \mathbf{L} 满足:

1. L 的每一行, 每一列的各矩阵元之和都是 0.

2. L 是实对称正定矩阵, 且 $\det L = 0$.

证明. 由 Laplace 矩阵的定义可直接看出 L 是对称矩阵, 并且容易验证其每一行, 每一列的各矩阵元之和都为 0. 最后再看正定性, 只需注意到对任何 n 维列向量 $\mathbf{a} = (a_1, a_2, \dots, a_n)^T \in \mathbb{R}^n$, 都成立

$$\mathbf{a}^T L \mathbf{a} = \sum_{e=\{v_i, v_j\} \in E} (a_i - a_j)^2$$

(上式留给读者验证), 因此 L 是正定矩阵; 此外由 L 的定义容易看出, $(1, 1, \dots, 1)^T$ 是 L 的特征向量, 相应特征值是 0. 故 L 不可逆, $\det L = 0$. \square

10.270. 回忆一些线性代数的记号. 给定域 \mathbb{F} , 对于方阵 $A = (a_{ij}) \in \mathbb{F}^{n \times n}$, 记 $A_{ij} \in \mathbb{F}^{(n-1) \times (n-1)}$ 为删除 A 第 i 行与第 j 列所得的子矩阵; $A_{ij} := (-1)^{i+j} \det A_{ij}$ 是 A 的第 (i, j) 个代数余子式. 记 $A^* := (A_{ij}) \in \mathbb{F}^{n \times n}$, 则众所周知 $AA^* = A^*A = (\det A)I$.

10.271. 引理. 设 $A = (a_{ij}) \in \mathbb{F}^{n \times n}$ 是任意域 \mathbb{F} 上的方阵, 并且 A 的每一行, 每一列的各元素之和都是 0, 则 A 的全部 n^2 个代数余子式都相等.

证明. 记 $J := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$, 即所有矩阵元都是 1 的 n 阶方阵. 考察行

列式 $\det(A + J)$. 将 $A + J$ 的第 2, 3, ..., n 行全部加到第 1 行, 然后再将新得到的矩阵的第 2, 3, ..., n 列全部加到第 1 列, 可得

$$\det(A + J) = \det \left(\begin{array}{c|ccc} n^2 & n & \cdots & n \\ \hline n & & & \\ \vdots & & & \\ n & & & \end{array} \begin{array}{c} A_{11} + J_{11} \\ \\ \\ \end{array} \right) = n \det \left(\begin{array}{c|ccc} n & 1 & \cdots & 1 \\ \hline n & & & \\ \vdots & & & \\ n & & & \end{array} \begin{array}{c} A_{11} + J_{11} \\ \\ \\ \end{array} \right)$$

$$= n \det \left(\begin{array}{c|ccc} n & 1 & \cdots & 1 \\ \hline 0 & & & \\ \vdots & & \mathbf{A}_{11} & \\ 0 & & & \end{array} \right) = n^2 A_{11}.$$

容易将上述方法推广到一般, 从而说明对任意 $i, j \in [n]$, 都有 $\det(\mathbf{A} + \mathbf{J}) = n^2 A_{ij}$, 从而全部 n^2 个代数余子式 A_{ij} 都相等. \square

特别地, 设 \mathbf{L} 为图 G 的 Laplace 矩阵, 则由上述引理可知 \mathbf{L} 的所有代数余子式都相等. Laplace 矩阵的一个“意料之外的”奇妙应用在于计算任意图 G 的生成树的个数 $\text{ST}(G)$, 回忆 4.129. 我们之前对完全图的情况给出了 $\text{ST}(K_n)$ 的 Cayley 公式 4.130, 但那里给出的证明方法严重依赖完全图, 几乎不可能推广到一般的图 G . 而一般结论为:

10.272.定理.(Kirchhoff, 1847) 对于任意图 G , 成立

$$\text{ST}(G) = \det \mathbf{L}_{11},$$

其中 $\mathbf{L} = (\ell_{ij})$ 为 G 的 Laplace 矩阵, \mathbf{L}_{11} 是删去 \mathbf{L} 的第一行与第一列之后所得的子矩阵.

注意 $\det \mathbf{L}_{11}$ 是 \mathbf{L} 的某个代数余子式. 特别注意, 由性质 10.269 与引理 10.271 可知, \mathbf{L} 的所有代数余子式都相同. 上述定理将最小生成树的个数转化为某个行列式的计算, 这非常令人意想不到. 然而“更意想不到的是, 我们居然能证明它是对的”, 而且证明并不难. 为证明上述定理, 我们需要一些引理:

10.273.引理.(Laplace 矩阵的分解) 设 $G = (V, E)$ 为图, $V = \{v_1, \dots, v_n\}$, $E = \{e_1, \dots, e_m\}$. 注意关联矩阵 \mathbf{N} 的每一列都恰有两个 1, 其余全是 0. 对于 \mathbf{N} 的每一列, 任意选定其中一个 1, 将其值改为 -1 , 如此操作之后所得矩阵记为 \mathbf{M} . (易知矩阵 \mathbf{M} 有 2^m 种可能的取值, 其中 $m := |E|$). 则对于任何满足上述性质的 \mathbf{M} , 都成立

$$\mathbf{L} = \mathbf{M} \mathbf{M}^T.$$

(若读者熟悉“有向图”, 则自然将 \mathbf{M} 视为某个有向图的“关联矩阵”).

证明. 记 $M = (\epsilon_1, \epsilon_2, \dots, \epsilon_m)$, 其中 $\epsilon_j \in \mathbb{R}^n$ 为列向量, 它的 n 个分量之中恰有一个 1, 恰有一个 -1 , 其余分量全为 0; 并且 ϵ_j 的第 i 个分量非零, 当且仅当 $v_i \in e_j$. 再注意 $MM^T = \sum_{j=1}^m \epsilon_j \epsilon_j^T$, 之后直接用矩阵乘法的运算法则以及 M, N, L 的定义, 逐个分量直接验证即可, 留给读者. \square

10.274. 引理. 设图 $G = (V, E)$ 有 n 个顶点, $(n-1)$ 条边; 任意取定满足引理 10.273 的矩阵 $M \in \mathbb{R}^{n \times (n-1)}$. 去掉 M 的某一行, 得到的 $(n-1)$ 阶方阵记为 M_1 . 则:

1. 若 G 不是树, 则 $\det M_1 = 0$;
2. 若 G 是树, 则 $\det M_1 = \pm 1$.

证明. 记 G 的顶点集 $V = \{v_1, \dots, v_n\}$, 边集 $E = \{e_1, \dots, e_{n-1}\}$.

1. 如果 G 不是树, 断言 $\text{rank } M \leq n-2$, 如果此断言成立, 则由秩的等价定义 (非零子式最大阶数) 可知 M 的任何 $(n-1)$ -阶子式都等于零, 特别地 $\det M_1 = 0$. 现在证明该断言. 注意 $|V| = |E| + 1$, 从而由 4.120 可知 G 不是连通图, 因此至少有两个连通分支. 不失一般性, 设 $V = V_1 \sqcup V_2$ 满足 $V_1 = \{v_1, \dots, v_s\}$ 与 $V_2 = \{v_{s+1}, \dots, v_n\}$, 并且使得 G 的任何一条边的两个端点要么都在 V_1 中, 要么都在 V_2 中. 不妨 e_1, \dots, e_t 的端点都在 V_1 中, e_{t+1}, \dots, e_{n-1} 的端点都在 V_2 中. 则 M 可分块写为

$$M = \begin{pmatrix} M_1 & \mathbf{0} \\ \mathbf{0} & M_2 \end{pmatrix},$$

其中 $M_1 \in \mathbb{R}^{s \times t}$, $M_2 \in \mathbb{R}^{(n-s) \times (n-1-t)}$. 注意 $M_i, i = 1, 2$ 的每一列也都恰有一个 1 与一个 -1 , 且该列的其余分量都是 0, 因此 M_i 的各行之和为 $\mathbf{0}$, 因此 M_i 的各行线性相关, 从而 $\text{rank } M_1 \leq s-1$, $\text{rank } M_2 \leq n-s-1$, 因此 $\text{rank } M = \text{rank } M_1 + \text{rank } M_2 \leq (s-1) + (n-s-1) \leq n-2$, 断言得证. 从而完成 (1) 的证明.

2. 若 G 是树, 此时通过对 G 的顶点个数 n 归纳. 归纳起始步 $n = 2$ 是平凡的. 现在不妨 $n > 2$. 不妨 v_1 是 G 的一片树叶 (度数为 1 的顶点), v_2

是 v_1 的唯一邻居, 连接 v_1, v_2 的边是 e_1 , 则 M 可分块写为

$$M = \left(\begin{array}{c|c} 1 & \mathbf{0} \\ -1 & \mathbf{a} \\ \hline \mathbf{0} & M'_1 \end{array} \right) \quad \text{或} \quad \left(\begin{array}{c|c} -1 & \mathbf{0} \\ 1 & \mathbf{a} \\ \hline \mathbf{0} & M'_1 \end{array} \right),$$

不妨假设是前者; 其中 $\mathbf{a}^T \in \mathbb{R}^{n-2}$, $M'_1 \in \mathbb{R}^{(n-2) \times (n-2)}$. 去掉 G 中的树叶 v_1 以及边 e_1 所得的图记作 G' , 则易知 G' 是树, 且顶点个数为 $n-1$. 并且易知 $M' := \begin{pmatrix} \mathbf{a} \\ M'_1 \end{pmatrix}$ 是关于 G' 的 M -矩阵. 从而由归纳假设可知, M' 的任何 $(n-2)$ 阶子式都等于 ± 1 , 特别地, $\det M'_1 = \pm 1$. 现在考察删除 M 的某一行所得子矩阵 M_1 的行列式. 若 M_1 是删去 M 的第 1 行所得, 则

$$\det M_1 = \det \begin{pmatrix} -1 & \mathbf{a} \\ \mathbf{0} & M'_1 \end{pmatrix} = -\det M'_1 = \pm 1,$$

同样地, 若 M_1 是删去 M 的第 2 行所得, 也易知 $\det M_1 = \pm 1$; 若 M_1 是删去 M 的第 s 行所得, $s \geq 3$, 则记 M'_1 删去第 $(s-2)$ 行所得子矩阵为 M''_1 , 则由归纳假设可知 $\det \begin{pmatrix} \mathbf{a} \\ M''_1 \end{pmatrix} = \pm 1$, 将 $\det M_1$ 按第 1 列展开, 得

$$\det M_1 = \det \begin{pmatrix} 1 & \mathbf{0} \\ -1 & \mathbf{a} \\ \mathbf{0} & M'_1 \end{pmatrix} = \det \begin{pmatrix} \mathbf{a} \\ M''_1 \end{pmatrix} + \det \begin{pmatrix} \mathbf{0} \\ M'_1 \end{pmatrix} = \pm 1.$$

从而得证. □

10.275. 我们现在开始证明 Kirchhoff 矩阵树定理 10.272. 证明的关键在于上述两个引理, 以及线性代数中众所周知的 **Cauchy-Binet 公式** (矩阵乘法与行列式的关系).

定理 10.272 的证明. 记图 G 的顶点集 $V = \{v_1, \dots, v_n\}$, 边集 $E = \{e_1, \dots, e_m\}$, 不妨 $m \geq n-1$ (否则 G 不连通, 从而 $\text{ST}(G) = 0$; 此时也易知 $\det L_{11} = 0$).

记 \mathbf{L} 为 G 的 Laplace 矩阵, \mathbf{M} 的含义同 10.273, 使得 $\mathbf{L} = \mathbf{M}\mathbf{M}^T$, 记 \mathbf{M}_1 为删掉 \mathbf{M} 的第 1 行所得的子矩阵, 则

$$\mathbf{L}_{11} = \mathbf{M}_1 \mathbf{M}_1^T.$$

对任意 $S \in \binom{[m]}{n-1}$, 记 $E_S := \{e_i \mid i \in S\} \in \binom{E}{n-1}$, 记 $G_S := (V, E_S)$ 为 G 的子图. 注意 G 的所有生成树都形如某个 G_S . 另一方面, 记 $\mathbf{M}_1^S \in \mathbb{R}^{(n-1) \times (n-1)}$ 为 \mathbf{M}_1 的由所有第 j 列 ($j \in S$) 按原顺序所排成的子矩阵. 注意 \mathbf{M}_1^S 恰为 G_S 所对应的某个 \mathbf{M} -矩阵删掉第 1 行所得, 因此当 G_S 是树 (从而 G 的生成树) 时 $\det \mathbf{M}_1^S = \pm 1$, 否则 $\det \mathbf{M}_1^S = 0$. 综上所述, 由线性代数中的 Cauchy-Binet 公式得,

$$\begin{aligned} \det \mathbf{L}_{11} &= \det(\mathbf{M}_1 \mathbf{M}_1^T) = \sum_{S \in \binom{[m]}{n-1}} (\det \mathbf{M}_1^S)^2 \\ &= \sum_{\substack{S \in \binom{[m]}{n-1} \\ G_S \text{ 是树}}} (\det \mathbf{M}_1^S)^2 + \sum_{\substack{S \in \binom{[m]}{n-1} \\ G_S \text{ 不是树}}} (\det \mathbf{M}_1^S)^2 \\ &= \sum_{\substack{S \in \binom{[m]}{n-1} \\ G_S \text{ 是树}}} 1 + \sum_{\substack{S \in \binom{[m]}{n-1} \\ G_S \text{ 不是树}}} 0 = \text{ST}(G), \end{aligned}$$

定理得证. □

10.276. 特别地, 如果 $G \cong K_n$ 是完全图, 则有:

定理 4.130 证法 3. 注意 K_n 的 Laplace 矩阵为

$$\mathbf{L} = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix},$$

从而由定理 10.272 以及引理 10.271 可知,

$$\text{ST}(K_n) = \det \mathbf{L}_{11} = \frac{1}{n^2} \det(\mathbf{L} + \mathbf{J}) = \frac{1}{n^2} \cdot n^n = n^{n-2}.$$

从而再次证明 Cayley 公式 4.130. □

10.3 多重图 (待补)

(引入多重图的概念, 给出矩阵树定理的另一种证明. 下述是伪证, 待完善.)

证明. 对 $G = (V, E)$ 的边数 $|E|$ 归纳.

1. 记 G 的顶点集 $V = \{v_1, v_2, \dots, v_n\}$. 当 $|E| = 0$ 时, G 同构于独立图 I_n , 显然 $\text{ST}(G) = 0$; 而此时 $\mathbf{L} = \mathbf{0}$, 也显然 $\det \mathbf{L}_{11} = 0$. 一般地, 若 $|E| \neq 0$, 不妨假设顶点 v_1 与 v_2 相邻, 则 G 的 Laplace 矩阵 \mathbf{L} 可分块地写为

$$\mathbf{L} = \left(\begin{array}{cc|c} d_1 & -1 & \mathbf{a}_1^T \\ -1 & d_2 & \mathbf{a}_2^T \\ \hline \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{M} \end{array} \right),$$

其中 $d_i := d_G(v_i)$, $\mathbf{a}_1, \mathbf{a}_2 \in \mathbb{R}^{n-1}$, $\mathbf{M} \in \mathbb{R}^{(n-2) \times (n-2)}$.

2. 记 $E' := E \setminus \{\{v_1, v_2\}\}$, $G' := (V, E')$. 换言之, G' 是删去 G 的边 v_1v_2 所得的图, 这是 G 的一个子图. 再令 $V'' := \{v'_1, v'_2, \dots, v'_{n-1}\}$, 其中

$$v'_i := \begin{cases} \{v_1, v_2\} & i = 1 \\ \{v_{i+1}\} & i = 2, 3, \dots, n-1 \end{cases},$$

并且定义 $E'' \subseteq \binom{V''}{2}$ 如下:

$$E'' := \{\{v'_i, v'_j\} \mid \exists u_i \in v'_i, \exists u_j \in v'_j, u_i \sim_E u_j\},$$

记 $G'' := (V'', E'')$. 粗俗地说, 将 G 的两个不同顶点 v_1, v_2 “视为同一个顶点”, 所得的图即为 G'' . 与“子图”的概念对偶, G'' 是 G 的“商图”. 注意以下关系显然成立:

$$\text{ST}(G) = \text{ST}(G') + \text{ST}(G'').$$

此式有误!!!! 必须引入多重图的概念!!!

这是因为, 设 T 是 G 的一棵生成树, 则自然分为两种情况: v_1v_2 是 T 的一条边, 或者不是 T 的一条边. 若是前者, 则 T 自然视为 G'' 的生成树; 若是后者, 则 T 自然视为 G' 的生成树. 反之, G', G'' 的生成树都可自然视为 G 的生成树. 以上构成一一对应 (细节留给读者).

3. 注意 G' 与 G'' 的边数都小于 G 的边数, 从而适用于归纳假设. 容易验证 G' 与 G'' 的 Laplace 矩阵分别为

$$\mathbf{L}' = \left(\begin{array}{cc|c} d_1 - 1 & 0 & \mathbf{a}_1^T \\ 0 & d_2 - 1 & \mathbf{a}_2^T \\ \hline \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{M} \end{array} \right), \quad \mathbf{L}'' = \left(\begin{array}{c|c} * & * \\ \hline * & \mathbf{M} \end{array} \right),$$

从而由归纳假设可知

$$\begin{aligned} \text{ST}(G) &= \text{ST}(G') + \text{ST}(G'') = \det \mathbf{L}'_{11} + \det \mathbf{L}''_{11} \\ &= \det \left(\begin{array}{c|c} d_2 - 1 & \mathbf{a}_2^T \\ \hline \mathbf{a}_2 & \mathbf{M} \end{array} \right) + \det \mathbf{M} \\ &= \det \left(\begin{array}{c|c} d_2 - 1 & \mathbf{a}_2^T \\ \hline \mathbf{a}_2 & \mathbf{M} \end{array} \right) + \det \left(\begin{array}{c|c} 1 & \mathbf{a}_2^T \\ \hline \mathbf{0} & \mathbf{M} \end{array} \right) \\ &= \det \left(\begin{array}{c|c} d_2 & \mathbf{a}_2^T \\ \hline \mathbf{a}_2 & \mathbf{M} \end{array} \right) = \det \mathbf{L}_{11}, \end{aligned}$$

从而得证. □