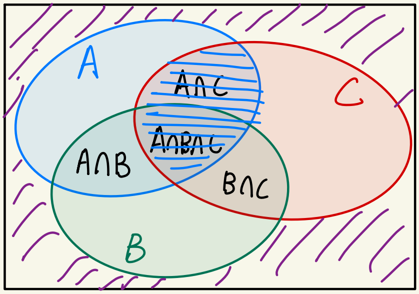
3. The Sieve Methods

筛法

PIE (Principle of Inclusion-Exclusion)

容斥原理



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

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

$\Downarrow$

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i\cap A_j| + \cdots + (-1)^{n-1}\cdot |A_1\cap\cdots\cap A_n|$$

$$= \sum_{\substack{I\subseteq[n]\\ I\neq\phi}} (-1)^{|I|-1}\cdot\left|\bigcap_{i\in I} A_i\right|$$

$|\cdot|$ 可以对任意测度成立!

e.g. Probability measure

Suppose $A_1, A_2, \cdots, A_n \subseteq U$. universe

希望去回避(不具有)的性质 → 筛 Sieve

$$|\bar{A}_1\cap\bar{A}_2\cap\cdots\cap\bar{A}_n| = \left|U - \bigcup_{i=1}^{n} A_i\right|$$

$$= |U| - \sum_{\substack{I\subseteq[n]\\ I\neq\phi}} (-1)^{|I|-1}\left|\bigcap_{i=1}^{n} A_i\right|$$

$$= \sum_{I\subseteq[n]} (-1)^{|I|} |A_I|$$

满足I中性质的集合

标记: $A_I = \bigcap_{i\in I} A_i$

$A_\phi = U$

① 定义 U, $A_1\cdots A_n$ "坏事件"

② 应用PIE计数 $\left|\bigcap_{i=1}^{n}\bar{A}_i\right| = \sum_{I\subseteq[n]} (-1)^{|I|}\cdot|A_I|$.

Example. Surjection 满射

$\# \text{ of } f: [n] \xrightarrow{\text{onto}} [m]$

不能有漏掉的元素

$U = [n] \to [m]$

$A_i = [n] \to ([m] \setminus \{i\})$

"坏事件"：漏掉了第 i 个元素

（不管是否漏掉了其他的元素）

PIE

$A_\phi = U$

$A_I = \bigcap_{i \in I} A_i = [n] \to ([m] \setminus I)$

每个元素有 $(m-|I|)$ 种映射方式

$\Rightarrow |A_I| = (m-|I|)^n$

$$\Rightarrow \left|\bigcap_{i\in[m]} \overline{A_i}\right| = \sum_{I \subseteq [m]} (-1)^{|I|} \cdot |A_I| = \sum_{k=0}^{m} (-1)^k \cdot \binom{m}{k} (m-k)^n$$

满射

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

$(f^{-1}(0), f^{-1}(1), \cdots, f^{-1}(m-1))$: ordered m-partition $[n]$

(n distinct balls. m distinct bins)

$\downarrow$

$$\left|[n] \xrightarrow{\text{onto}} [m]\right| = m! \cdot \left\{ {n \atop m} \right\} = \sum_{k=1}^{m} (-1)^{m-k} \binom{m}{k} k^n,$$

$\Rightarrow$ 第 II 型 Stirling 数：$\left\{ {n \atop m} \right\} = \frac{1}{m!} \cdot \sum_{k=1}^{m} (-1)^{m-k} \binom{m}{k} k^n$

Example. Derangement 错排

A $\boxed{1}$ $\boxed{2}$ $\boxed{3}$ ---- $\boxed{54}$

B $\boxed{27}$ $\boxed{31}$ $\boxed{16}$ ---- $\boxed{9}$

What is the probability that no 2 cards are the same in each pair ?

permutation of $[n]$:

$\forall i \in [n] : \pi(i) \neq i$

Goal: permutations with no fixed points ☆

U: permutations of $[n]$

$\underline{\underline{U = S_n}}$

坏事件 $A_i = \{\pi \mid \pi(i) = i\}$

$\Downarrow$

$I \subseteq [n]$. $A_I = \{\pi \mid \forall i \in I, \pi(i) = i\}$

I中所含均为不动点 其余的不管(全排列)

$f_=$

$f_\geq$ ✓

$$\left|\bigcap_{i=1}^{n} \bar{A}_i\right| = \sum_{I \subseteq [n]} (-1)^{|I|} \cdot |A_I| \quad |A_I| \to (n - |I|)!$$

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

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$$= n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!} \xrightarrow{n \to \infty} \frac{n!}{e}$$

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

Probability $\doteq \frac{1}{e}$

More generally, $\boxed{\text{permutation with restricted positions}}$

π: permutation of $[n]$

derangement: $\forall i \in [n]$: $\pi(i) \neq i$

generally, $\pi(i_1) \neq j_1$, $\pi(i_2) \neq j_2$, ...

forbidden pairs

$B \subseteq [n] \times [n]$, s.t. $\forall i \in [n]$. $(i, \pi(i)) \notin B$

想要回避掉满足该二元表示的点

	1	2	3	4	5
1	X		O		
2		X			O
3			X	O	
4	O			X	
5		O			X

"a placement of non-attacking rooks"

For a particular set of forbidden positions $B \subseteq [n] \times [n]$

X 的位置

$G_\pi = \{(i, \pi(i)) \mid i \in [n]\}$ → O 的位置

$N_0 = \left| \{ \pi \mid B \cap G_\pi = \phi \} \right|$ → goal!

"坏事件" r_k = # of ways of placing k non-attacking rooks in B

$= \left| \{ S \in \binom{B}{k} \mid \forall (i_1, j_1), (i_2, j_2) \in S : i_1 \neq i_2,\ j_1 \neq j_2 \} \right|$

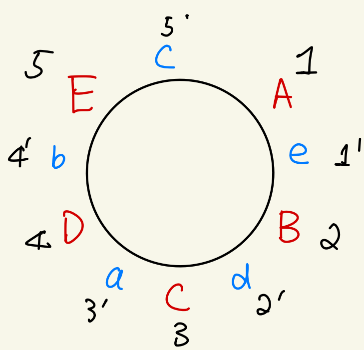
满足规则的前提下，在禁区放k个点

$$\boxed{N_0 = \sum_{k=0}^{n} (-1)^k \underbrace{r_k}_{\text{"fixed"}} \underbrace{(n-k)!}_{\text{全排列}}} \rightarrow \sum_{I \subseteq \binom{[n]}{k}} |A_I| = r_k \cdot (n-k)!$$

e.g. (derangement) $B = \{(1,1), (2,2), \cdots, (n,n)\}$ $\quad r_k = \binom{n}{k}$

$$N_0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Problème des ménages



n couples sit around a table

- male - female alternative ✓
- no one sit next to spouse.

① "Lady First": $2(n!)$

② "Gentlemen, please sit."

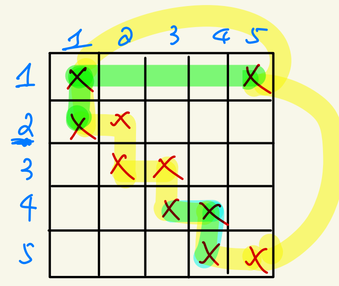
A B C D E
a b c d e
→ e d a b c

→ permutation π of $[n]$

i: husband of the lady at the i-th position.

$\pi(i)$: his seat.

$$\begin{cases} \pi(i) \neq i \\ \pi(i) \neq (i-1) \pmod n \end{cases}$$

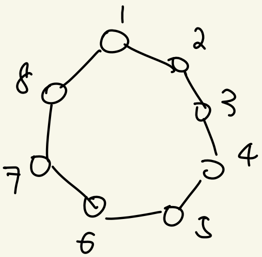


$B = \{(i,i),\ (i,\ i-1 \bmod n)\}$

r_k : # of ways of placing non-attacking rooks in B

⇒ # of ways of choosing k non-consecutive points from a circle of $2n$ points

不同行: mapping
不同列: non-attacking



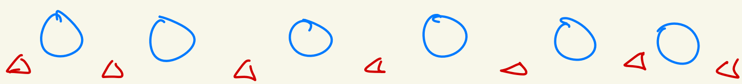
* 在2n个点的圈上找出k个不相邻的点共有多少种选法?

$$r_k = \frac{2n}{2n-k}\cdot\binom{2n-k}{k}$$

线 m objects in a line: ① ② ③ ---- ⓜ

$L(m,k)$: choose k non-consecutive objects

剩m-k个:



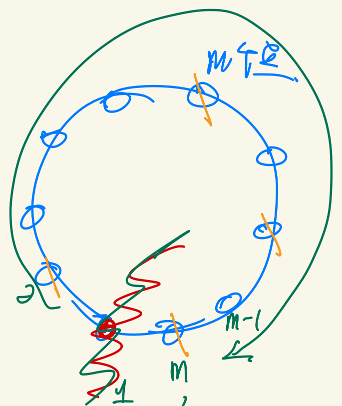
m-k+1个空档 插入k个元素 $L(m,k) = \binom{m-k+1}{k}$

环 $C(m,k)$: choose k non-consecutive objects

double counting

双重计数: 两种不同的方法去算相同的结果.

等式一边含有未知量



① 选k个不相邻的点	① 任选一点断开
② 选一个剩下的点,将环断成线	② 在一条线(m-1个元素)选k个不相邻的
⇒ $C(m,k)\cdot(m-k)$ =	⇒ $m\cdot L(m-1,k)$

$$\Rightarrow C(m,k) = \frac{m}{m-k}\cdot L(m-1,k) = \frac{m}{m-k}\cdot\binom{m-k}{k}$$

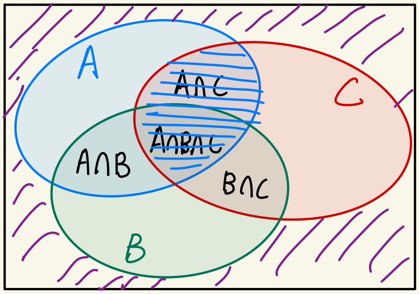
Recall: Principle of Inclusion-Exclusion

$A_1, A_2, \cdots, A_n \subseteq U$. $\quad \left|\bigcap_{i=1}^{n} \bar{A_i}\right| = \sum_{I \subseteq [n]} (-1)^{|I|} \left|\bigcap_{i \in I} A_i\right|$

$f_=$ ×

$f_\geq$

Inversion



Partially Observed Sets (Posets) 偏序集

" $\leq_P$ "

- reflexivity: $x \in P$: $x \leq x$
- antisymmetry: $x \leq y$, $y \leq x \Rightarrow x = y$
- transitivity: $x \leq y$, $y \leq z \Rightarrow x \leq z$

$x \geq y$.

$x < y$.

function $\alpha: P \times P \to \mathbb{R}$. (treated as matrices)

incidence algebra of poset:

$$I(P) = \{\alpha: P \times P \to \mathbb{R} \mid \alpha(x,y) = 0 \text{ for all } x \not\leq_P y\}$$

$\alpha(x,y) \neq 0$ only if $x \leq_P y$.

加法 $\alpha, \beta \in I(P)$: $\alpha + \beta \in I(P)$

数乘 $\alpha \in I(P)$: $c\alpha \in I(P)$. $c \in \mathbb{R}$

乘法 $\alpha \cdot \beta \in I(P)$: matrix multiplication

↓

closed!

$$(\alpha\beta)(x,y) = \sum_{z \in P} \alpha(x,z) \cdot \beta(z,y) = \sum_{x \leq z \leq y} \alpha(x,z) \cdot \beta(z,y)$$

def (zeta-function) $\zeta(x,y) = \begin{cases} 1, & \text{if } x \leq_P y \\ 0, & \text{otherwise.} \end{cases}$

↓

invertible!

def (Möbius-function) $\mu \in I(P)$ s.t. $\mu\zeta = I$

identity matrix

$$\Leftrightarrow \boxed{\mu(x,y) = \begin{cases} -\sum_{x\le z<y} \mu(x,z). & \text{if } x<y \\ 1. & \text{if } x=y \\ 0. & \text{if } x \not\le y \end{cases}} \quad (*)$$

Lemma. $\forall x, y \in P$: $\sum_{x\le z\le y} \mu(x,z) = \begin{cases} 1. & \text{if } x=y \\ 0 & \text{otherwise} \end{cases}$

Proof: $(\mu\zeta)(x,y) = \sum_{x\le z\le y} \mu(x,z)\cdot\zeta(z,y) = \sum_{x\le z\le y} \mu(x,z)$

$\mu\zeta = I \Rightarrow (\mu\zeta)(x,y) = \begin{cases} 1, & \text{if } x=y \\ 0. & \text{otherwise} \end{cases}$ $\square$,

$$\mu(x,y) = \sum_{x\le z\le y} \mu(x,z) - \sum_{x\le z<y} \mu(x,z) \Rightarrow (*).$$

Computing Möbius Function

$P = [n]$ $\le$ total order:

$$\boxed{\mu(i,j) = \begin{cases} 1. & \text{if } i=j \\ -1 & \text{if } i+1=j \\ 0 & \text{if otherwise} \end{cases}}$$

a_i b_i

- $i+1=j$: $\mu(i,j) = -\sum_{i\le z<j} \mu(i,z) = -\mu(i,i) = -1$
- $i+k=j$ $(k>1)$: $\mu(i,j) = -\sum_{i\le z<j} \mu(i,z)$

$= \underbrace{-\mu(i,i) - \mu(i,i+1)}_{0} - \mu(i,i+2) - \cdots - \mu(i,i+k-1)$

For general posets P.

difficult to compute $\mu(\cdot,\cdot)$.

$\Downarrow$

product rule

Lemma. P, Q posets. $P \times Q$ cartesian product.

$(x, y), (x', y') \in P \times Q$.

$(x, y) \leq (x', y')$ iff $x \leq_P x'$, $y \leq_Q y'$.

$$\mu_{P\times Q}((x,y),(x',y')) = \mu_P(x,x') \cdot \mu_Q(y,y')$$

Posets of Subsets

Boolean Algebra of rank $|U|$

finite universe U. $P = 2^U$. $S, T \subseteq U$. $S \leq_P T$ iff $S \subseteq T$.

Möbius function
$$\boxed{\mu(S,T) = \begin{cases} (-1)^{|T|-|S|}, & \text{if } S \subseteq T \\ 0, & \text{otherwise} \end{cases}}$$

Proof: $S \in \{0,1\}^U$ where $S(x) = \begin{cases} 1, & \text{if } x \in S \\ 0, & \text{if } x \notin S \end{cases}$

$\forall x \in U$ define poset $P_x = \{0, 1\}$ $0 \leq 1$.

$\mu_x(0,0) = 1$ $\mu_x(0,1) = -1$

$\mu_x(1,0) = 0$ $\mu_x(1,1) = 1$

$P = \prod_{x \in U} P_x$ $\Rightarrow$ By product rule of Möbius function,

$$\mu(S,T) = \prod_{x \in U} \mu_x(S(x), T(x))$$

$$= \prod_{\substack{x\in S \\ x \in T}} 1 \cdot \prod_{\substack{x \in S \\ x \notin T}} 0 \cdot \prod_{\substack{x \notin S \\ x \in T}} (-1) \cdot \prod_{\substack{x \notin S \\ x \notin T}} 1 = \begin{cases} (-1)^{|T|-|S|} & S \subseteq T \\ 0, & \text{otherwise} \end{cases} \qquad \square$$

Posets of Divisors

整除n的元素

$P = \{a > 0 \mid a | n\}$. $a, b \in P$. $a \leq_P b$ iff $a | b$

Möbius function $\mu(a,b) = \begin{cases} (-1)^r, & \text{if } \frac{b}{a} \text{ 是r个互不相同的质数的乘积} \\ 0, & \text{otherwise} \end{cases}$

Proof: $n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} \Longleftrightarrow (n_1, n_2, \cdots, n_k)$ 同构

$a \in P \rightarrow$ tuple $(a_1, a_2, \cdots, a_k)$ $\quad a_i \le n_i, \; i \in [k]$

$P_i = \{1, 2, \cdots, n_i\}$ poset with $\le$ total order

$$P = \prod_{i=1}^{k} P_i \Rightarrow \mu(a,b) = \prod_{i=1}^{k} \mu(a_i, b_i)$$

$$= \prod_{\substack{1\le i\le k \\ a_i = b_i}} 1 \cdot \prod_{\substack{1\le i\le k \\ a_i+1=b_i}} (-1) \cdot \prod_{\substack{1\le i\le k \\ b_i - a_i \notin \{0,1\}}} 0 = \begin{cases} (-1)^{\sum_i (b_i - a_i)} & \text{if all } b_i - a_i \in \{0,1\} \\ 0 & \text{otherwise} \end{cases} \quad \square$$

Möbius Inversion Formula

P: finite poset. μ: Möbius function. $f, g: P \to \mathbb{R}$

$$\boxed{\forall x \in P \quad g(x) = \sum_{y \le x} f(y) \iff \forall x \in P \quad f(x) = \sum_{y \le x} g(y) \cdot \mu(y, x)}$$

$f, g: P \to \mathbb{R}$ vector

$\zeta, \mu: P \times P \to \mathbb{R}$ matrix

$\Rightarrow$ matrix-vector multiplication!

$$(f\zeta)(x) = \sum_{y \in P} f(y) \cdot \zeta(y, x) = \sum_{y \le x} f(y)$$

$$(g\mu)(x) = \sum_{y \in P} g(y) \cdot \mu(y, x) = \sum_{y \le x} g(y) \cdot \mu(y, x)$$

$\zeta \cdot \mu = I$

$\Downarrow$

矩阵右乘 $\quad f\zeta = g \iff f = g\mu$

Dual form:

$$\boxed{\forall x \in P. \quad g(x) = \sum_{y \ge x} f(y) \iff \forall x \in P. \quad f(x) = \sum_{y \ge x} \mu(x, y) g(y)}$$

$\zeta f = g \iff f = \mu g$ $\quad$ 矩阵左乘.

Principle of Inclusion-Exclusion

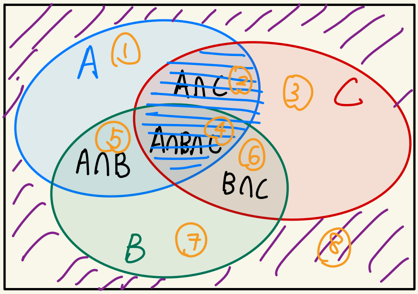
$A_1, A_2, \cdots, A_n \subseteq U$. $J \subseteq \{1, 2, \cdots, n\}$

- $f(J) = \left| \left(\bigcap_{i \in J} A_i \right) \setminus \left(\bigcup_{i \notin J} A_i \right) \right|$

exactly in A_i, $i \in J$

"disjoint" 原子块

- $g(J) = \left| \bigcap_{i \in J} A_i \right|$



$\Rightarrow g(J) = \sum_{I \supseteq J} f(I)$

原子块

$J = \{B, C\}$

$f(J) = |⑥|$

$g(J) = |④ + ⑥|$

$J = \{B\}$

$f(J) = |⑦|$

$g(J) = |④ + ⑤ + ⑥ + ⑦|$

$\Rightarrow$ By Möbius inversion formula (dual form)

$$f(J) = \sum_{I \supseteq J} \mu(J, I) \cdot g(I)$$

$$= \sum_{I \supseteq J} (-1)^{|I| - |J|} \cdot \left| \bigcap_{i \in I} A_i \right|$$

(posets of subsets)

Consider $J = \phi$: $f(\phi)$: # of element satisfying no properties in $A_1, A_2, \cdots, A_n$

$$\Rightarrow f(\phi) = \left| U \setminus \bigcup_i A_i \right| = \sum_{I \subseteq [n]} (-1)^{|I|} \cdot \left| \bigcap_{i \in I} A_i \right|$$

PIE ☆

* Möbius inversion upon posets of divisors:

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

$$\Leftrightarrow f(n) = \sum_{d | n} g(d) \cdot \mu\left(\frac{n}{d}\right)$$

number-theoretical Möbius function