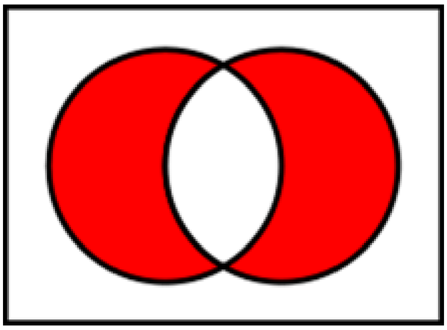
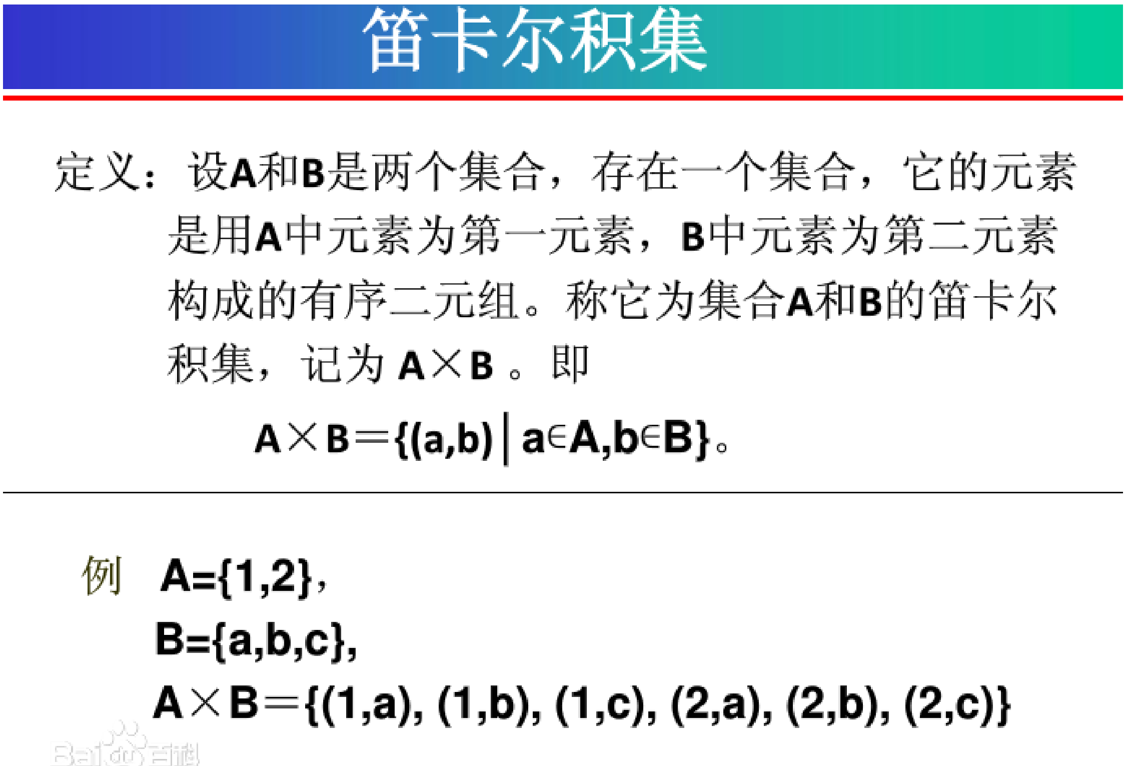
Ch 01 集合论

集合

- $A \oplus B$对称差



- P(A) 幂集，A的子集形成的集合
- partition划分，所有子元素交集为空，并集为全集
- onto function/surjective function 满射函数，说值域任何元素都有至少有一个变量与之对应
- injective function/one-to-one function/single-rooted 单射函数，不同原像对应不同像
- bijective function 双射函数=满射+单射
- 笛卡尔积



罗素悖论

理发师悖论

小城里的理发师放出豪言：他只为，而且一定要为城里所有不为自己刮胡子的人刮胡子。

但问题是：理发师该为自己刮胡子吗？如果他为自己刮胡子，那么按照他的豪言“只为城里所有不为自己刮胡子的人刮胡子”他不应该为自己刮胡子；但如果他不为自己刮胡子，同样按照他的豪言“一定要为城里所有不为自己刮胡子的人刮胡子”他又应该为自己刮胡子。

罗素悖论

$A = \{S|S\ is\ a\ set\}$

Theorem There is no set to which every set belongs. [Russell, 1902]

Proof:

Let A be a set; we will construct a set not belonging to A. Let

$$B=\{x\in A \mid x\notin x\}$$

We claim that $B\notin A$. we have, by the construction of B.

$$B\in B \text{ iff } B\in A \text{ and } B\notin B$$

If $B\in A$, then this reduces to

$B\in B$ iff $B\notin B$, Which is impossible, since one side must be true and the other false. Hence $B\notin A$

罗素悖论：设有一性质P(例如："年满三十岁"就是一个性质)，并立以一性质函数：$P(x)$，且其中的自变量x有此特性：$x \notin x$

,

现假设由性质P能够确定一个满足性质P的集合A——也就是说 $A = \{x \mid x \notin x\}$。那么现在的问题是$A \in A$是否成立?

首先，若$A \in A$，则A是A的元素，那么A具有性质P，由性质函数P可以得知$A \notin A$；

其次，若$A \notin A$，根据定义，A是由所有满足性质P的类组成，也就是说，A具有性质P，所以$A \in A$。

自然数

自然数表示

- By *von Neumann*:

Each natural number is the set of all smaller natural numbers.

$$0=\emptyset$$

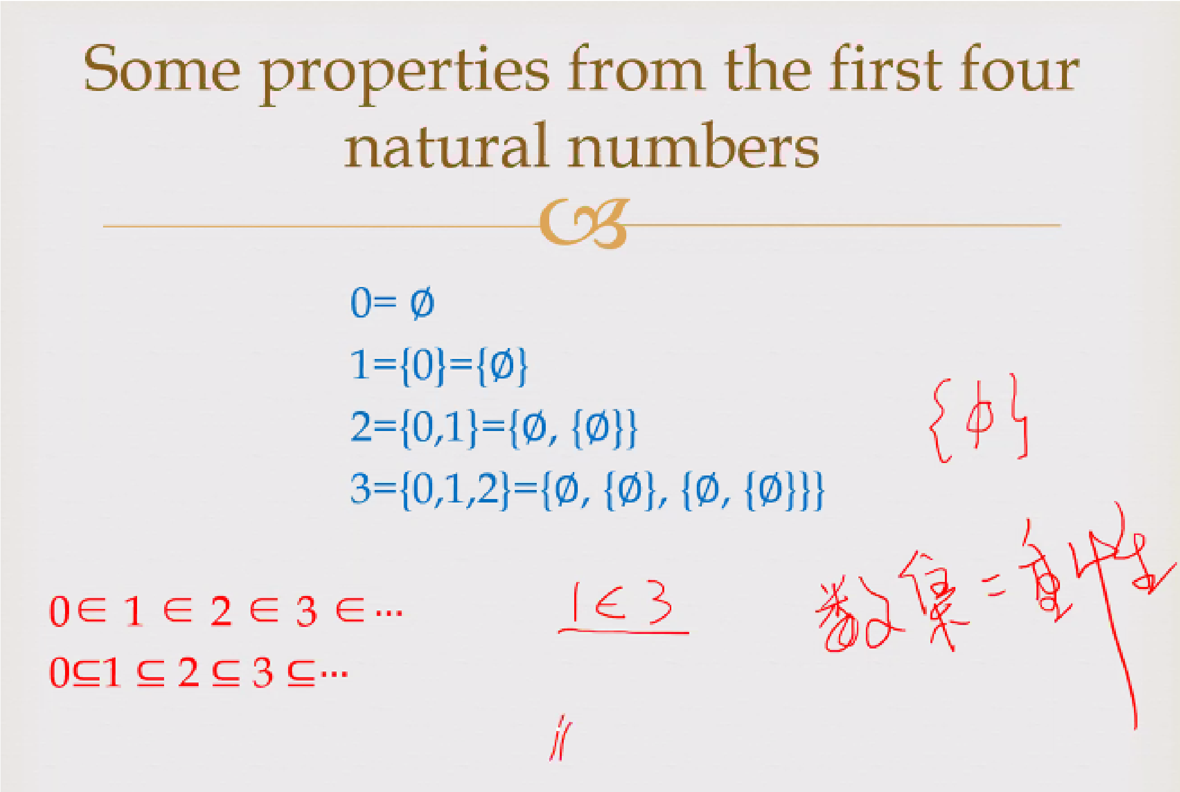
$$1=\{0\}=\{\emptyset\}$$

$$2=\{0,1\}=\{\emptyset, \{\emptyset\}\}$$

$$3=\{0,1,2\}=\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

$$\ldots\ldots$$

表示的数集二重性

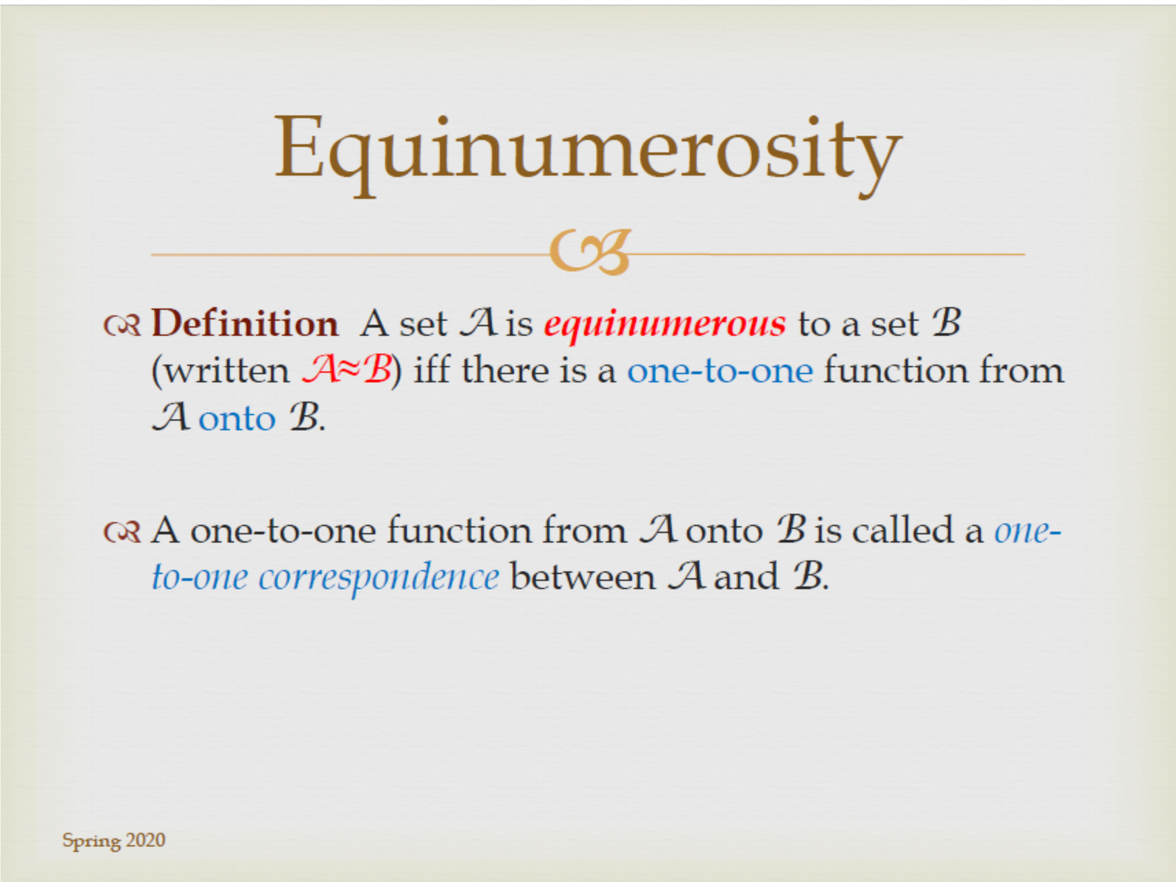


可以由自然数定义整数，由整数定义有理数。并且可以构造实数

等势 equinumerosity

定义

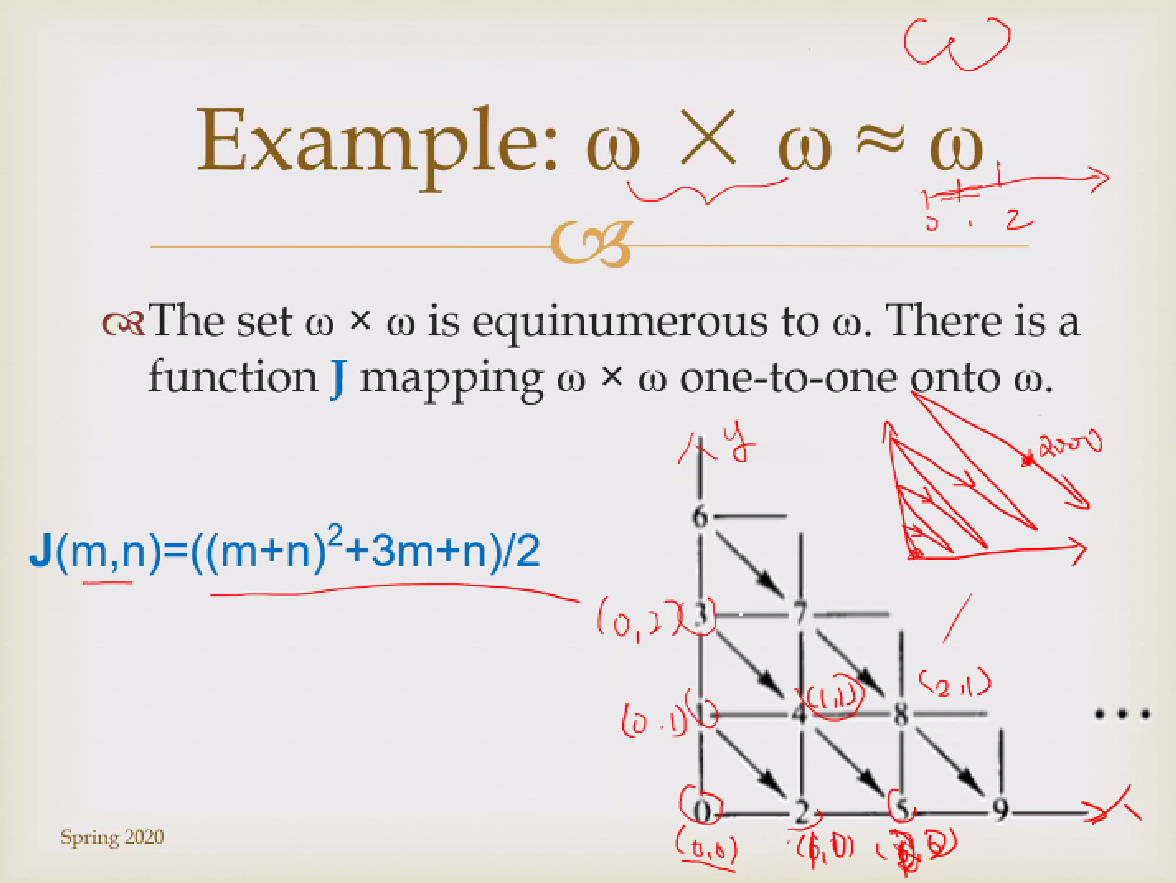
集合A到B有双射函数



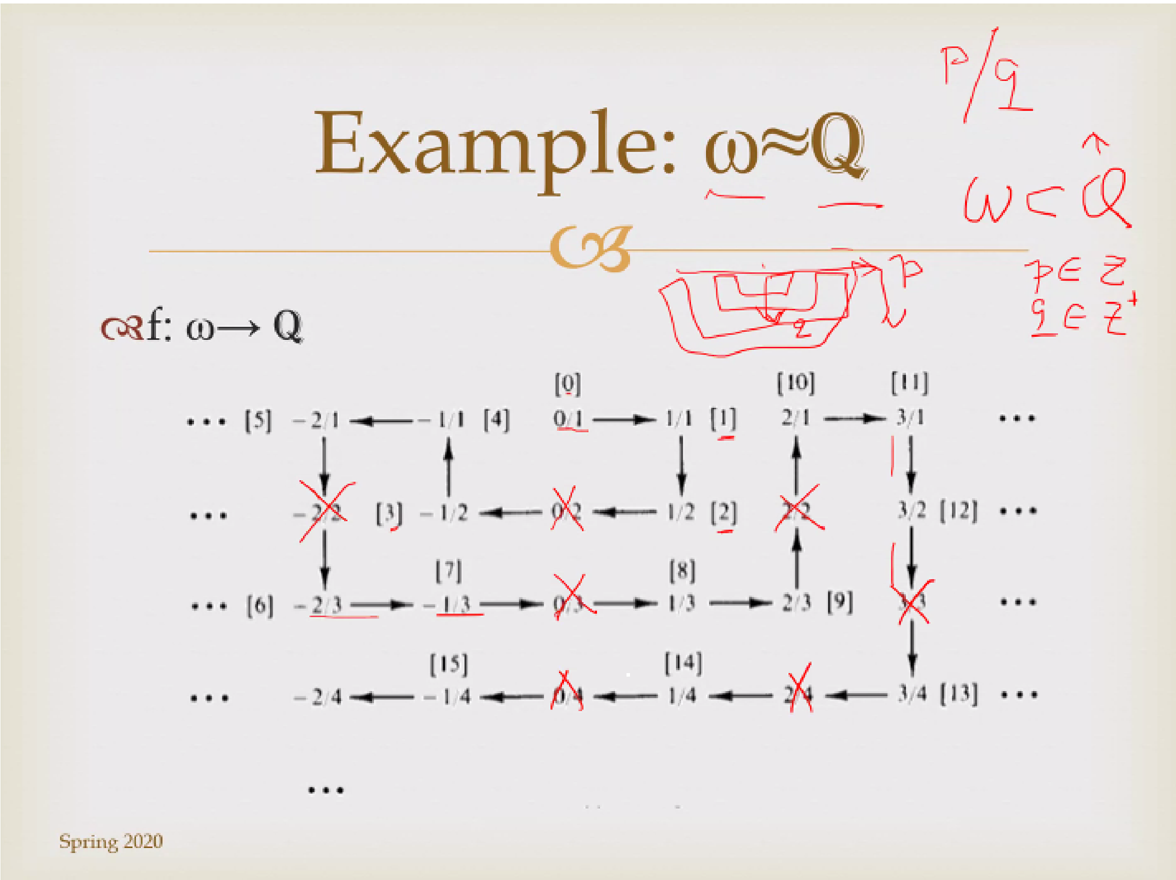
例题

找双射函数

高维自然数到自然数



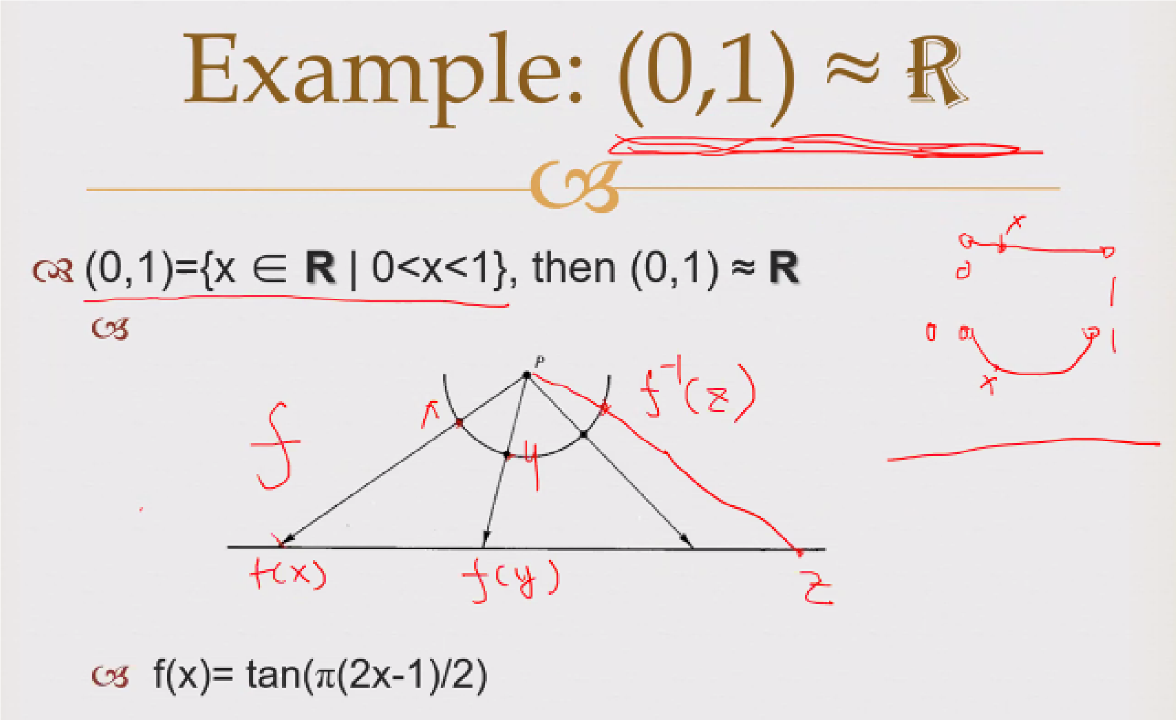
自然数到有理数



- 单射 不同的自然数编号都对应不同有理数

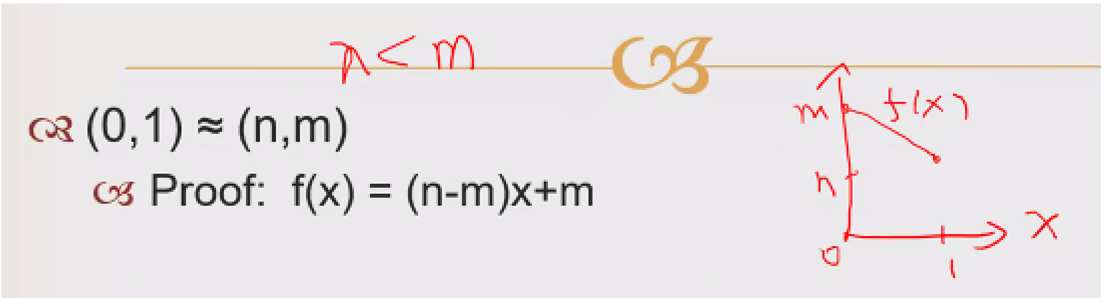
- 满射 每个有理数都能找到对应自然数，因为这个序列是无限的

(0, 1)到实数

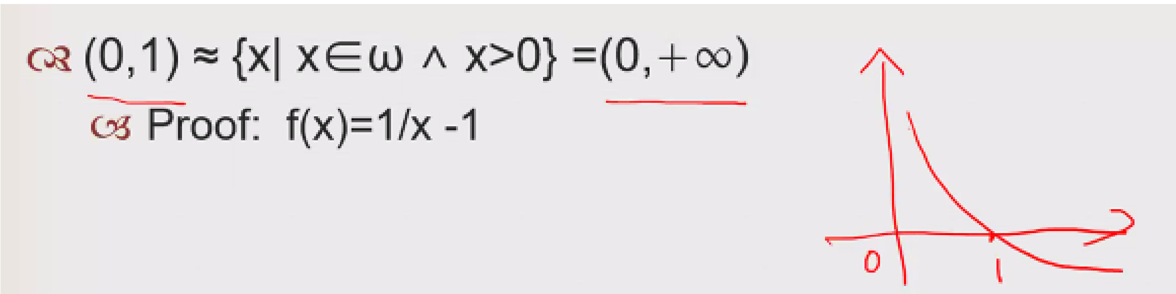


0,1直线弯曲为一个半圆

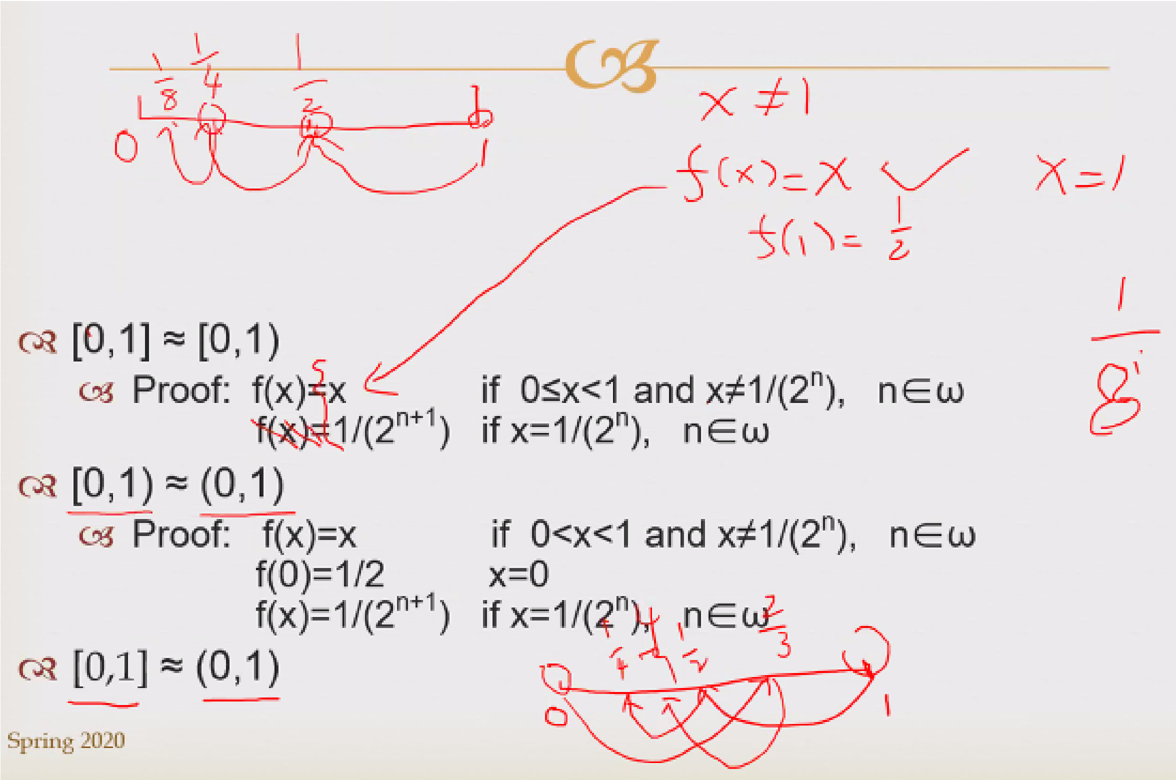
(0, 1)到(n, m)



(0, 1)到正实数



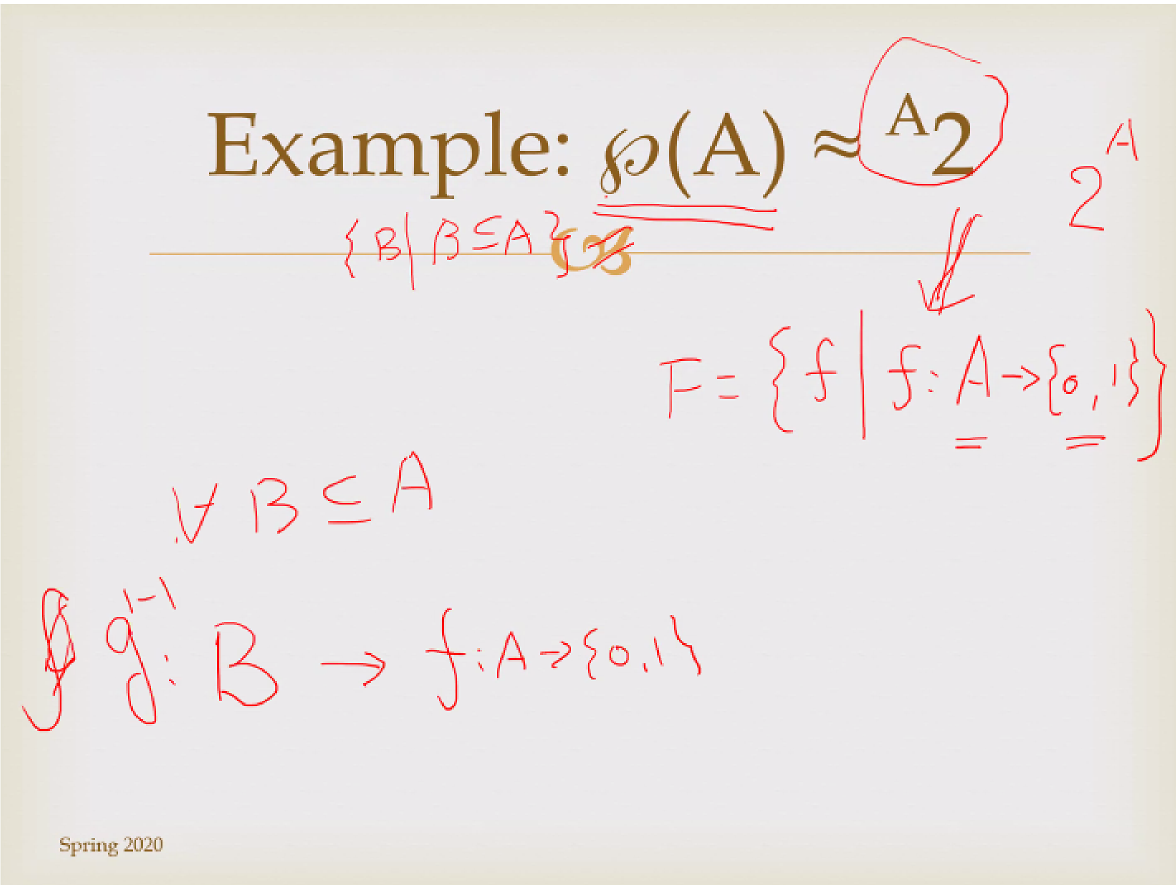
0, 1区间

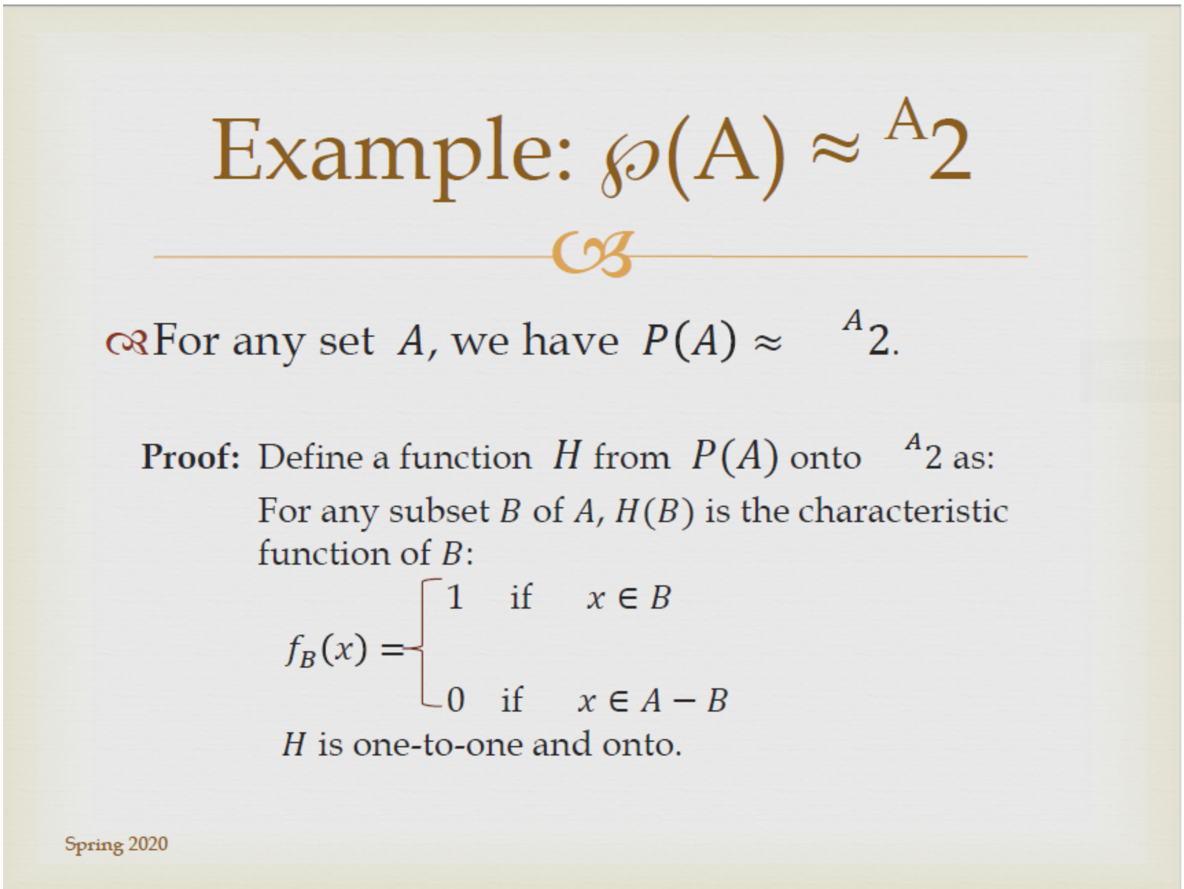


- 0->2/3->4/9...
- 1->1/2->1/4

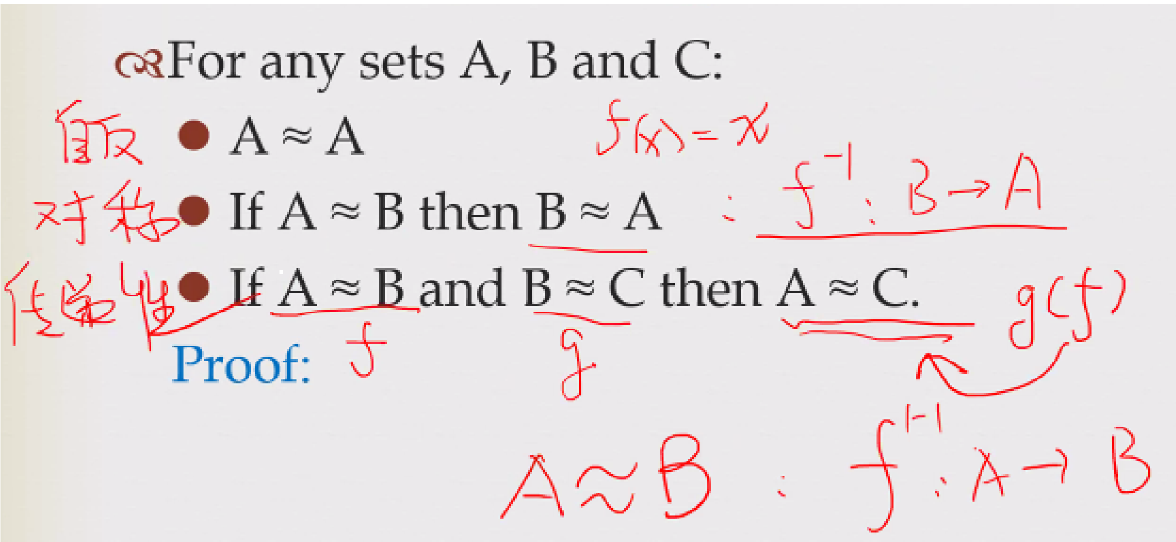
$$P(A) =^{A} 2$$

A子集的集合到以A为定义域的布尔函数的集合





性质



等价关系

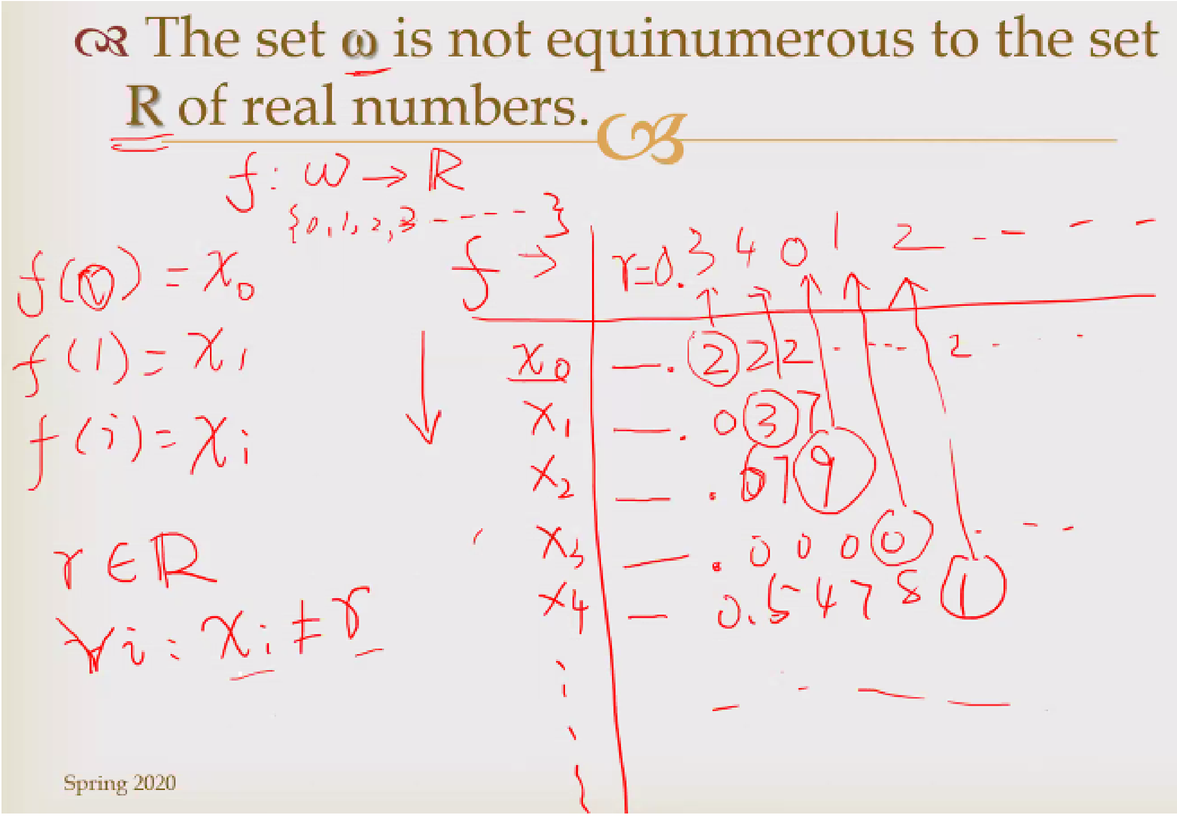
- 自反
- 对称
- 传递

不等势

自然数集与实数集不等势

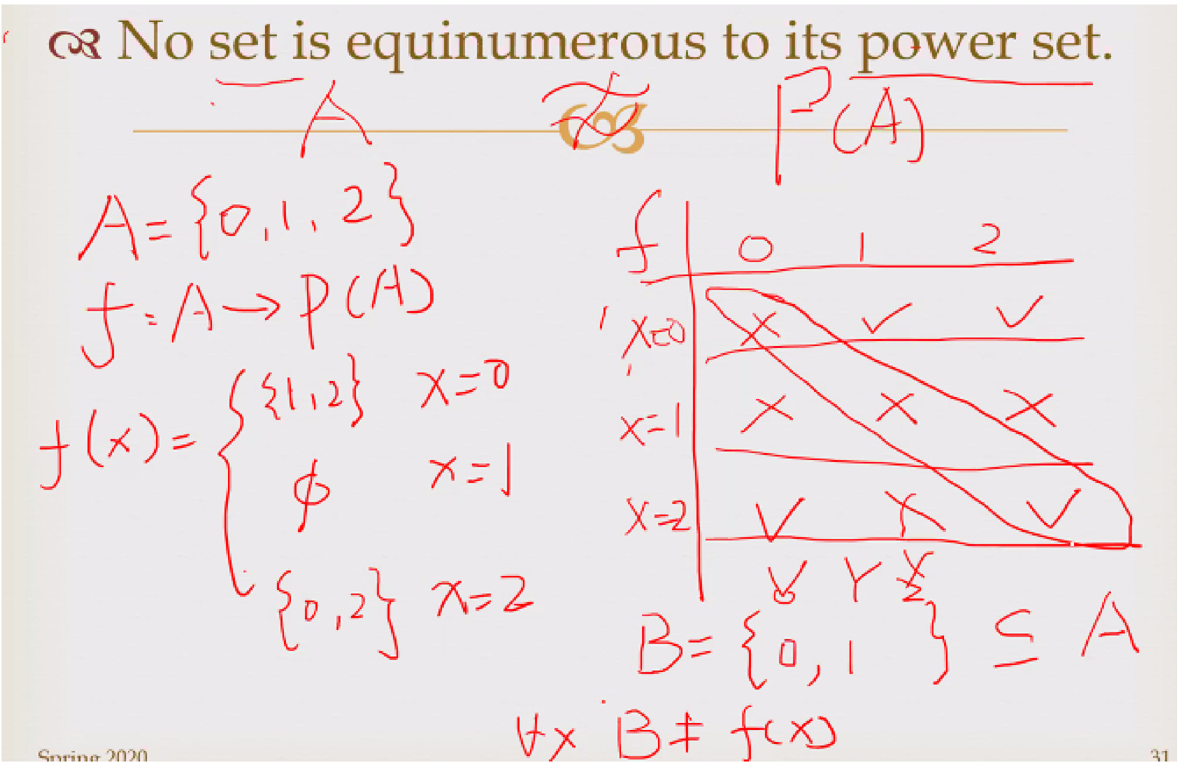
没有集合和其自身的幂集等势

对角线方法——证明自然数集与实数集不等势



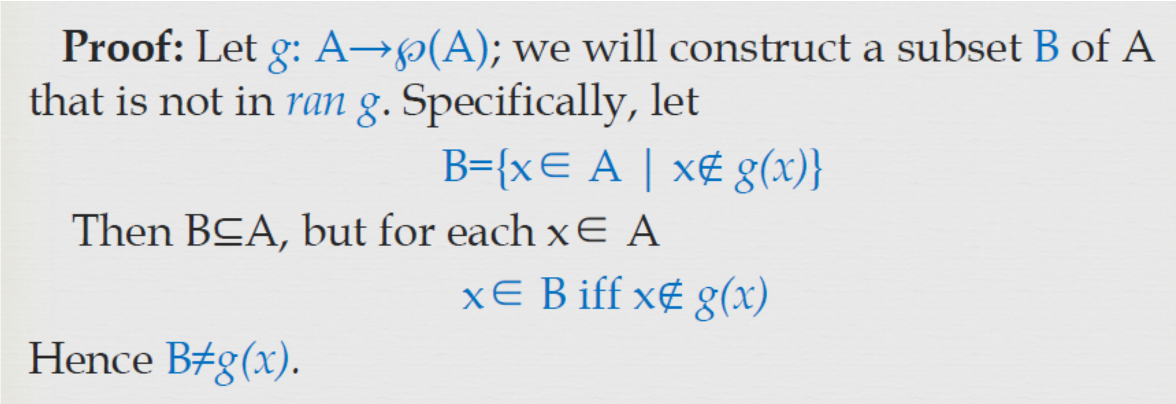
存在多余的r，矛盾，非双射

对角线方法——证明没有集合和其自身的幂集等势



构造方法：对角线××√ -> √√×，与任何一个f(x)都不一样

形式化证明：



应用

程序为自然数（哥德尔编码）

N到N的函数为R=P(N)

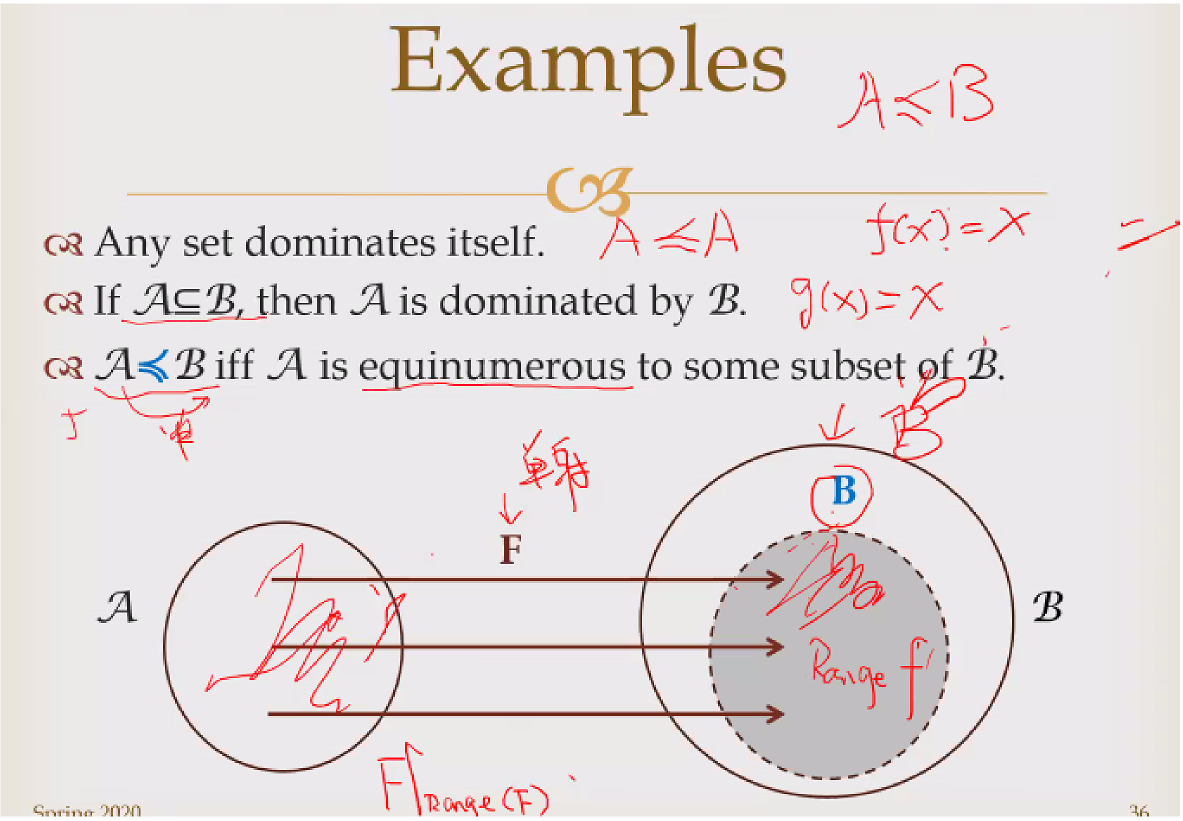
程序无法表示所有函数

序关系 Ordering

定义

A is dominated by B iff A到B有单射函数

例子



S-B 定理

Cantor.

— Schröder-Bernstein Theorem

√ If $A \preccurlyeq B$ and $B \preccurlyeq A$, then $A \approx B$.

$f: A \to B$ 单

$g: B \to A$ 单

$\Rightarrow \exists \overset{1-1}{h}: A \to B$

$A = B = \mathbb{N}$

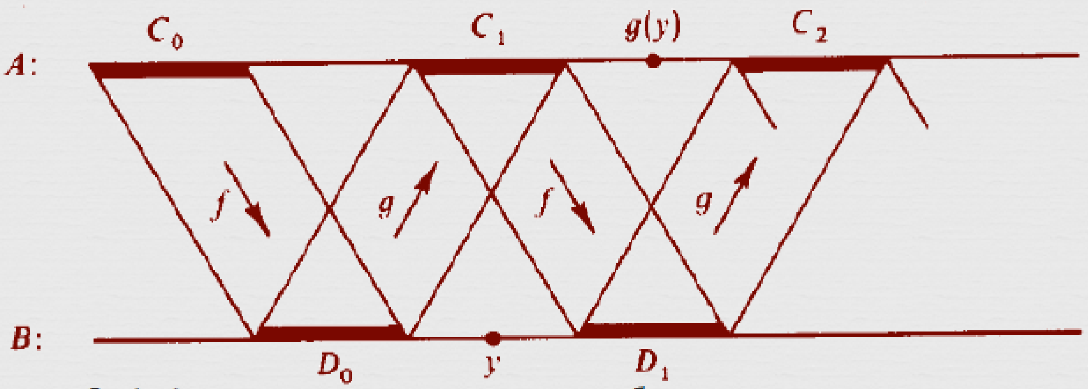
$\begin{cases} f(x) = 2x \\ g(x) = 3x \end{cases}$

$g \circ f(x) = 3 \cdot (2x) = 6x \longrightarrow \cdots$

$f: A \to B,\ g: B \to A$. Define C_n by recursion:

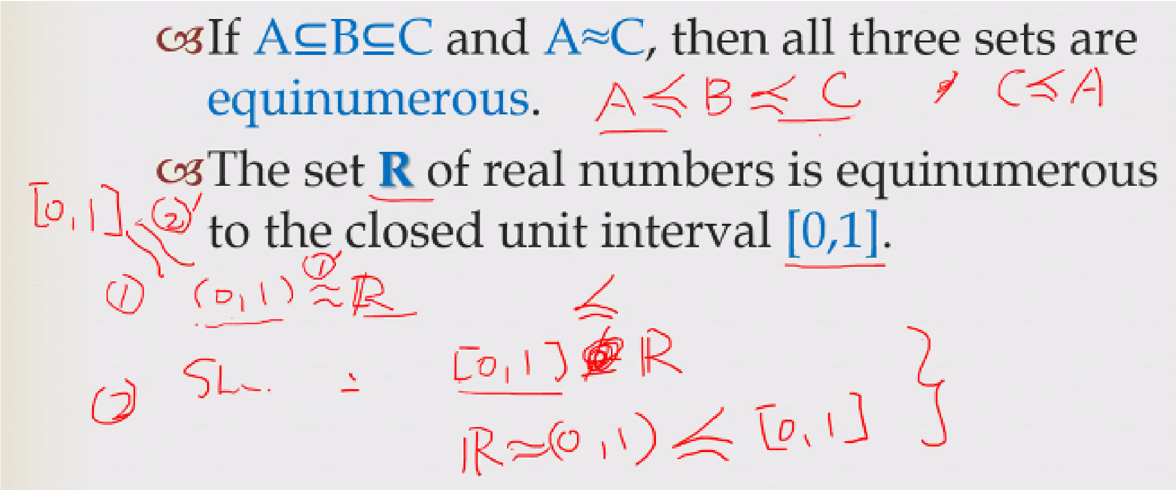
$C_0 = A - ran\ g$ and $C_n^+ = g[f[C_n]]$

$$h(x) = \begin{cases} f(x) & \text{if } x \in C_n \text{ for some } n, \\ g^{-1}(x) & \text{otherwise} \end{cases}$$

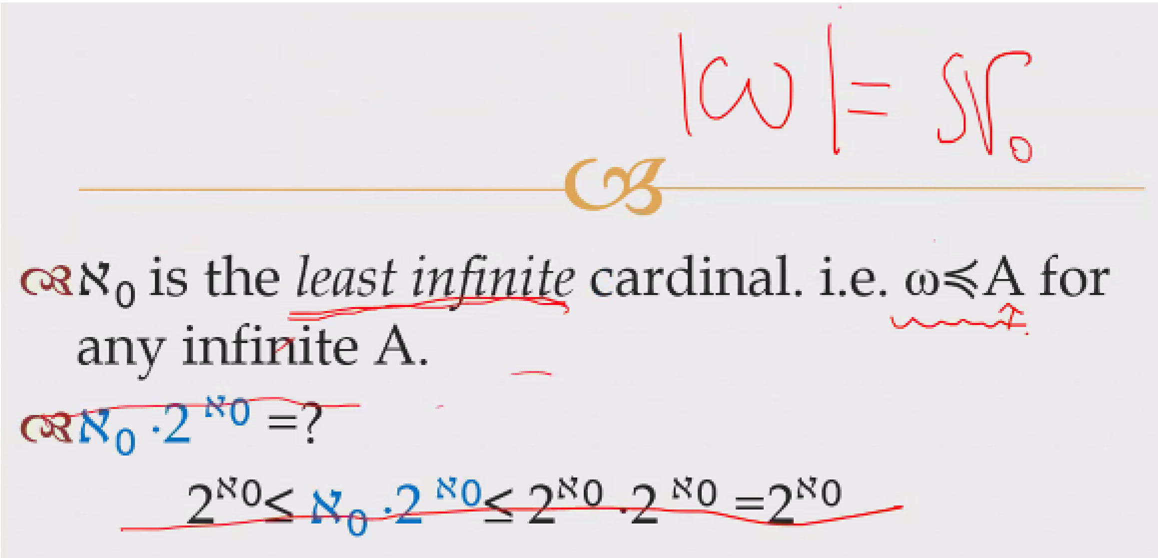


$h(x)$ is one-to-one and onto.

应用



基数



可数集 countable sets

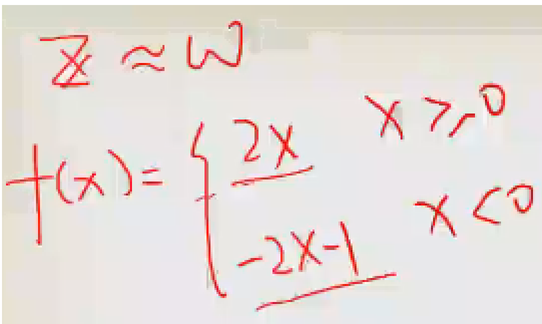
可数集：被自然数集dominated

自然数集是最小的无限集，任何无限集dominate自然数集

A是可数集 iff A是有限集或A与自然数集等势（A为无限集且A被自然数集dominate，可知A与自然数集等势）

例子

整数集为可数集



有理数集为可数集

Q与自然数集等势，前边有证明

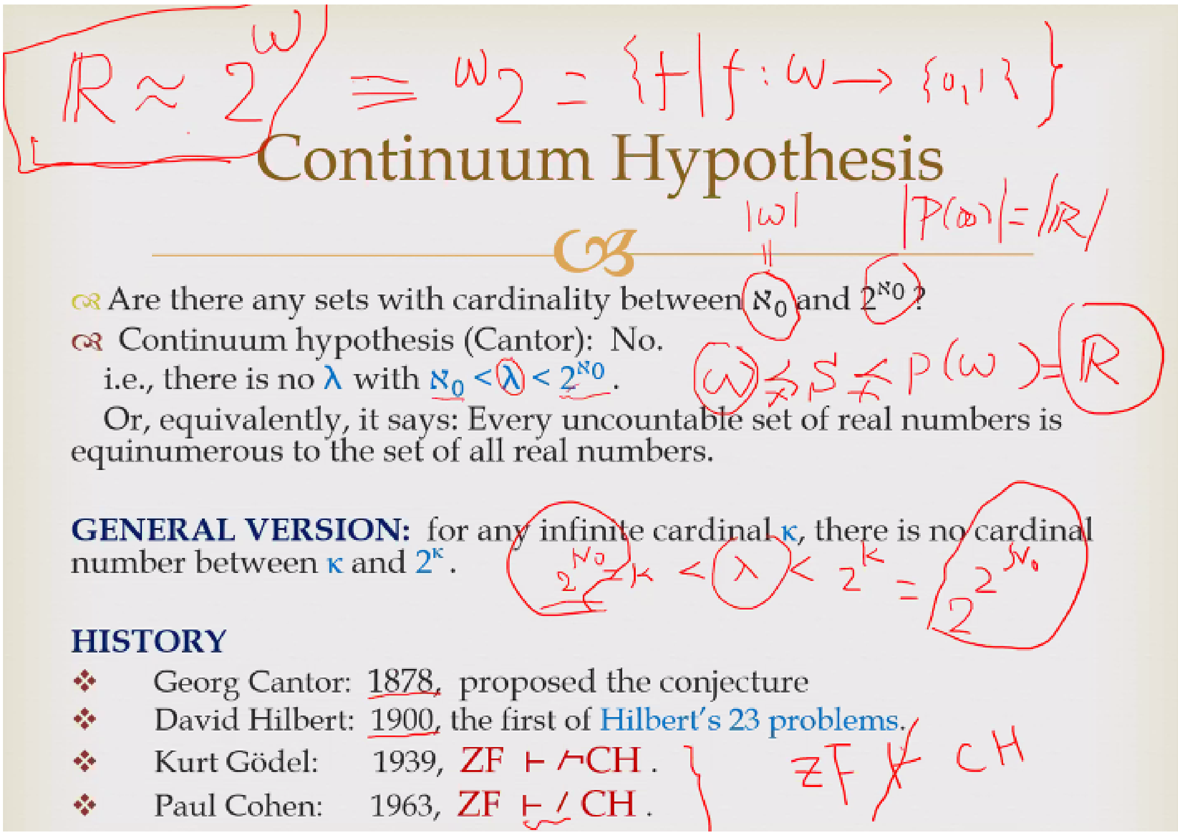
实数集不可数

$N \leq R$

$N \neq R$

一些性质

- 可数集的子集为可数集
- 两个可数集的并集为可数集
- 可数集的笛卡尔积为可数集
- 无限集的幂集不可数，证明：最小无限集自然数集的幂集不可数



$R \approx 2^{\omega}$证明

对于每个 $E \in 2^A$, 可以唯一的对应一个特征函数

$$\chi_E(x) = \begin{cases} 1, & x \in E \\ 0, & x \in A - E \end{cases}$$

反之亦然. 这说明 A 上所有特征函数的全体与 2^A 对等.

定理 1.3.10. $\aleph = 2^{\aleph_0}$.

证明 用 $\mathcal{F}_{\mathbb{N}}$ 表示 $\mathbb{N}$ 上特征函数的全体, 只需证 $\mathcal{F}_{\mathbb{N}}$ 与 $(0, 1]$ 对等. 对任意的 $\varphi \in \mathcal{F}_{\mathbb{N}}$, 作映射

$$f : \varphi \to \sum_{n=1}^{\infty} \frac{\varphi(n)}{3^n}$$

易知, f 是从 $\mathcal{F}_{\mathbb{N}}$ 到 $(0, 1]$ 的单射, 故 $\overline{\overline{\mathcal{F}_{\mathbb{N}}}} \leqslant \overline{\overline{(0, 1]}}$.

另一方面, 对每一个 $x \in (0, 1]$, 用 2 进制表示为 (不进位)

$$x = \sum_{n=1}^{\infty} \frac{a_n}{2^n}, \quad a_n \in \{0, 1\}$$

定义映射

$$g : x \to \varphi \in \mathcal{F}_{\mathbb{N}}, \quad \varphi(n) = a_n, \quad n = 1, 2, \cdots$$

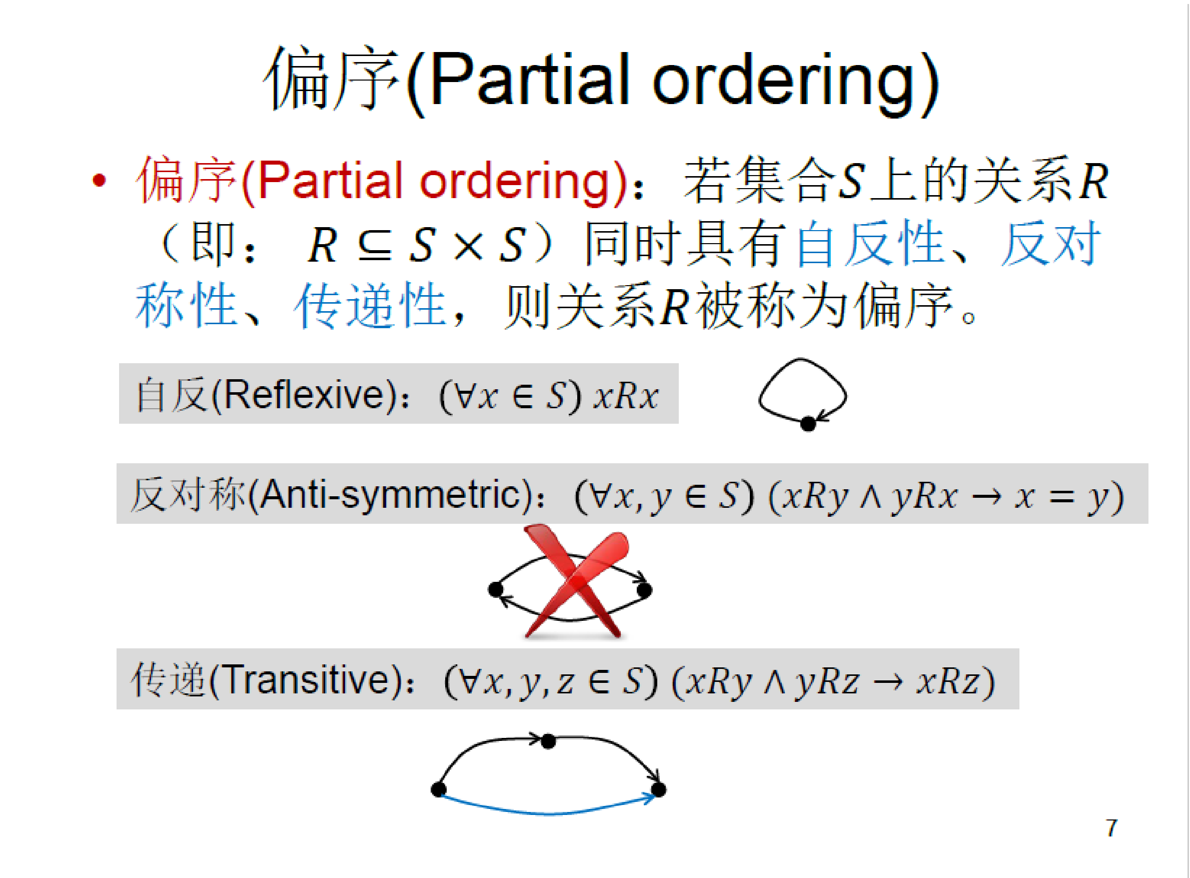
易知, g 是从 $(0, 1]$ 到 $\mathcal{F}_{\mathbb{N}}$ 的单射, 故 $\overline{\overline{(0, 1]}} \leqslant \overline{\overline{\mathcal{F}_{\mathbb{N}}}}$.

由伯恩斯坦定理, $\overline{\overline{(0, 1]}} = \overline{\overline{\mathcal{F}_{\mathbb{N}}}}$.

Ch 02 序 Orderings

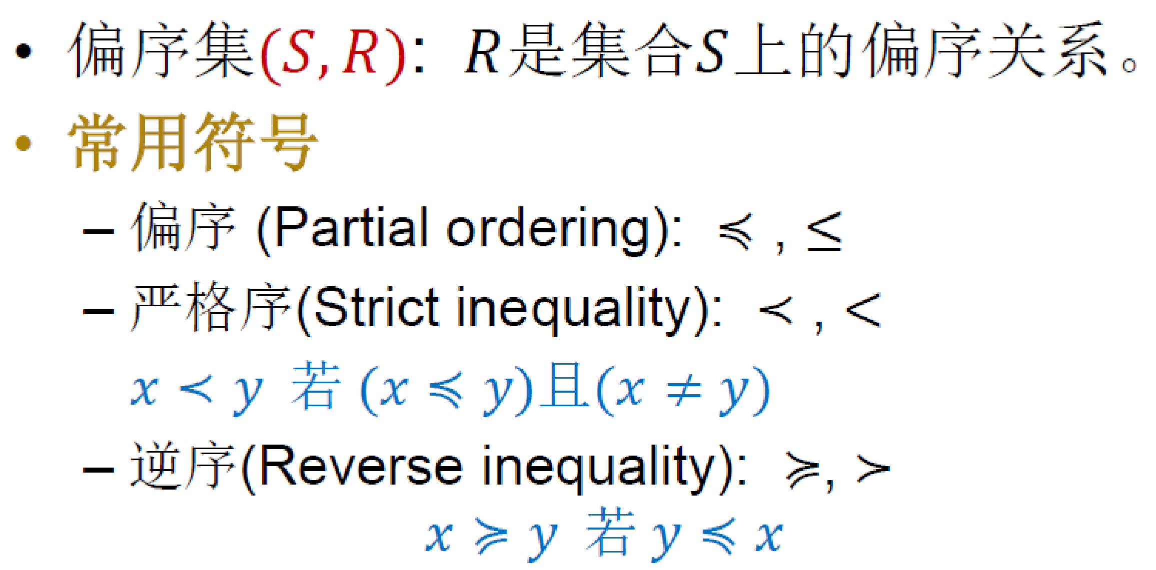
偏序

偏序是笛卡尔积上的二元关系



对称关系：xRy -> yRx，并非反对称取反

符号约定



线性序

定义

集合S上的关系R被称为线性序，若R满足：

- R是偏序
- 对任意S中元素x, y，都有xRy或yRx，任意两元素都可以互相比较

举例

- $(N, \leq)$
- $(Z, \leq), (R, \leq)$

偏序非线性例子

- 自然数集上的整除关系$(N, |)$

  $a \mid b$当且仅当存在自然数c，使得$b = a \times c$
- 集合A上的子集关系$(2^A, \subseteq)$
- 冰箱选择

字典序

(S, R)

一个重要的序

$(S_1, \leq_1), (S_2, \leq_2), \dots, (S_n, \leq_n)$是$n$个线性序，

$(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in S_1 \times S_2 \times \dots \times S_n$，

n元字典序(Lexicographic ordering)：

$(a_1, a_2, \dots, a_n) \leq_{\text{lex}} (b_1, b_2, \dots, b_n)$ 当且仅当

- $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$，或 $\forall i:\ a_i = b_i$
- 存在$i \in \{1,2, \dots, n\}$ $(\forall j < i)$ $a_j = b_j$ 且 $a_i <_i b_i$。

$1 \leq j \leq i-1$

例：S_k是 26个英文字母，$\leq_k$是字母序 $a<b<c<d \cdots$

则 $abcdef \leq_{\text{lex}} abeaay$

$c<e$

证明是线性序：

$(S_1, \leq_1), (S_2, \leq_2), \dots, (S_n, \leq_n)$是$n$个线性序， n个

$(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in S_1 \times S_2 \times \dots \times S_n$，

n元字典序(Lexicographic ordering)： n元

$(a_1, a_2, \dots, a_n) \leq_{\text{lex}} (b_1, b_2, \dots, b_n)$ 当且仅当

- $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$，或
- 存在$i \in \{1,2, \dots, n\}$ $(\forall j < i)$ $a_j = b_j$ 且 $a_i <_i b_i$。

$x \underset{i}{\leq} y \underset{j}{\leq} z$

n元字典序是线性序。

$$x = (a_1, a_2, \dots, a_i, \dots a_j, \dots, a_n)$$
$$y = (b_1, b_2, \dots, b_i, \dots b_j, \dots, b_n)$$
$$z = (c_1, c_2, \dots, c_i, \dots c_j, \dots, c_n)$$

$a_i < b_i = c_i$

紧前元 Immediate predecessor

x是y前元，且不存在z夹在xy之间

- 立即前元(Immediate predecessor) 紧前元

对偏序集$(S, \preccurlyeq)$，元素$x, y \in S$，如果以下两个条件成立，称x是y的立即前元：

1. $x \prec y$,
2. $\neg(\exists\, z \in S)(x \prec z \prec y)$。

用符号$x \lessdot y$表示立即前元关系。

- 例：

$(N, |)$

- $2 \lessdot 4 \lessdot 8$，但是 2 不是8 的立即前元。（$\lessdot$不具有传递性）
- $3 \lessdot 6$, $3 \lessdot 9$
- 对任意素数x,有 $1 \lessdot x$

（多个元素可能有同一立即前元）

2, 3, 5

- $2 \lessdot 10$, $5 \lessdot 10$

哈斯图 hasse diagram

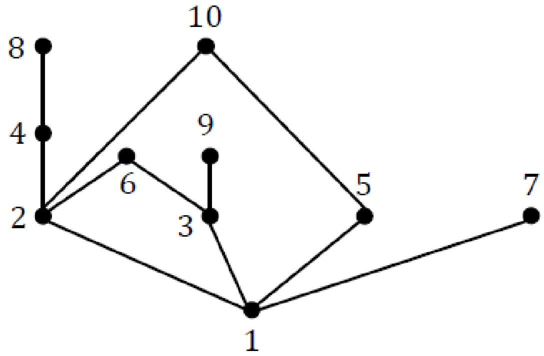
只画紧前元关系，大的画在上边

- **哈斯图：** 给定偏序集$(S, \preccurlyeq)$，S为有限集
  - 只保留立即前元关系对应的边。
  - 若$x \lessdot y$，则代表的y点画在代表x的点的上方。

- 例：

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

- 例：
  $(\{1,2,\ldots,10\}, |)$

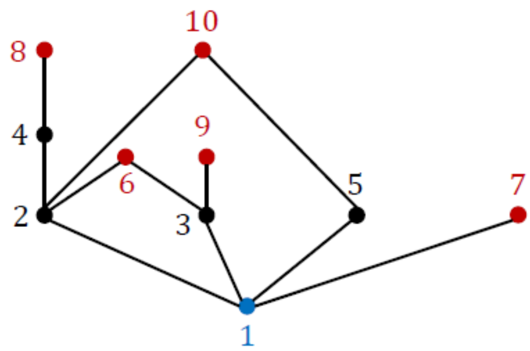


极小极大元

极小：找不到比它小的

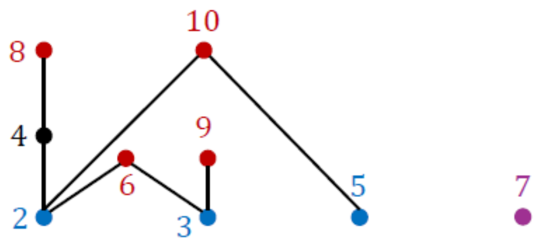
极大：找不到比它大的

- 偏序集$(S, \preccurlyeq)$，称$a \in S$是此有序集上的
  - 极小元(Minimal element)：
    如果$\neg(\exists x \in S) x \prec a$;
  - 极大元(Maximal element)：
    如果$\neg(\exists x \in S) x \succ a$;
- 例：
  $(\{1,2,\ldots,10\}, |)$



19

- 例：
  $(\{2,\ldots,10\}, |)$



7既是极小元，又是极大元

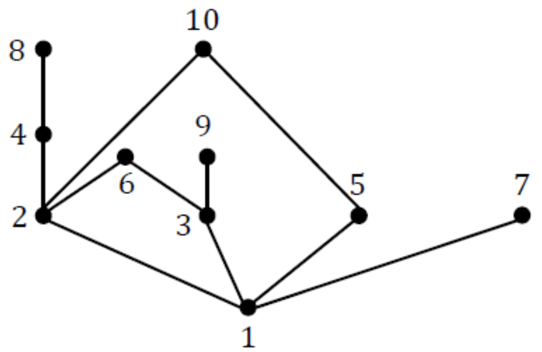
最小元最大元

最小：比任何都要小（要能比较）

最大：比任何都要大（要能比较）

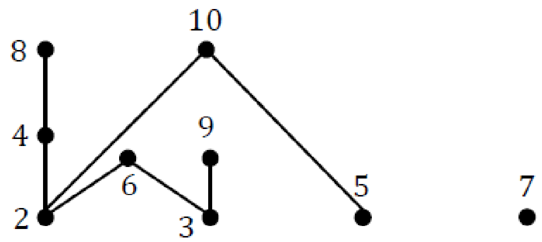
- 偏序集$(S, \preccurlyeq)$，称$a \in S$是此有序集上的
  - 最小元(Smallest element)：
    如果$(\forall x \in S)\ a \preccurlyeq x$;　$(\forall x)(x \in S \to a \leq x)$
  - 最大元(Largest element)：
    如果$(\forall x \in S)\ a \succcurlyeq x$;　$(\forall x)(x \in S \to x \leq a)$

- 例：
  $(\{1, 2, \ldots, 10\}, |)$



1为最小元，无最大元

- 例：
  $(\{2, \ldots, 10\}, |)$



无最小元和最大元

总结

- 偏序集$(S, \preccurlyeq)$，称$a \in S$是此有序集上的
  - 极小元(Minimal element)：
    如果$\neg(\exists x \in S)\, x \prec a$;
  - 极大元(Maximal element)：
    如果$\neg(\exists x \in S)\, x \succ a$;
- 偏序集$(S, \preccurlyeq)$，称$a \in S$是此有序集上的
  - 最小元(Smallest element)：
    如果$(\forall x \in S)\ a \preccurlyeq x$;
  - 最大元(Largest element)：
    如果$(\forall x \in S)\ a \succcurlyeq x$;

最大元（最小元）必是极大元（极小元），反之不成立。

存在性

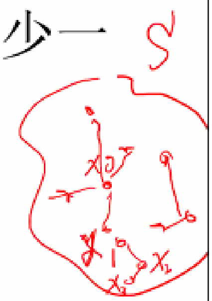
- 偏序集$(S,\preccurlyeq)$
  - S无限：
    极大元、极小元、最大元、最小元都不一定存在。
    反例：$(Z,\leq)$，$(N,\leq)$
  - S有限：
    最大元、最小元不一定存在。
    极大元、极小元一定存在。

订正：N应为R

证明有限偏序集一定含极小元

有限偏序必含极小元

- **定理：** 任意有限偏序集$(S,\preccurlyeq)$中存在至少一个极小元。



- 证明：

任意取S中的元素x_0：

情况1：如果x_0是极小元，则定理得证；

情况2：否则，一定能找到$x_1 \prec x_0$。

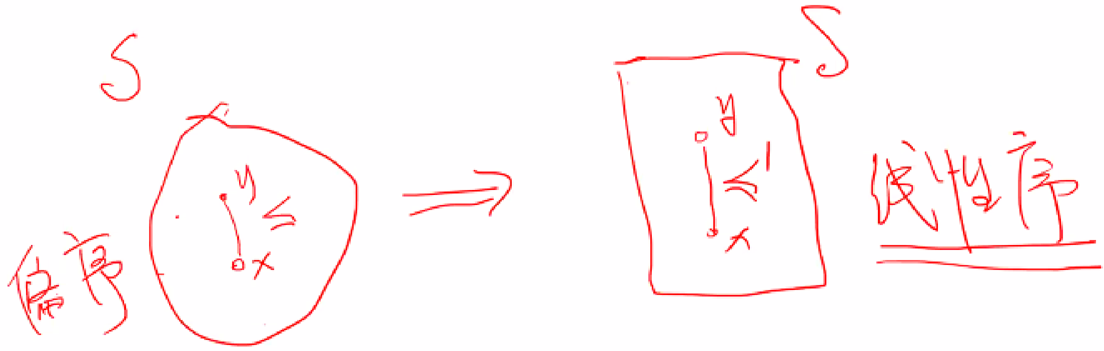
对x_1重复前述讨论，因为S有限，故情况2必在有限步后不成立。从而情况1成立。

线性扩充定理

有限偏序集->线性序集

- 线性扩充(Linear extensions):对有限偏序集$(S,\preccurlyeq)$,存在一个线性序集$(S,\preccurlyeq')$满足

$$x \preccurlyeq y \rightarrow \quad x \preccurlyeq' y.$$



归纳法证明

线性扩充定理

- 线性扩充(Linear extensions):对有限偏序集$(S,\preccurlyeq)$,存在一个线性序集$(S,\preccurlyeq')$满足

$$x \preccurlyeq y \rightarrow \quad x \preccurlyeq' y.$$

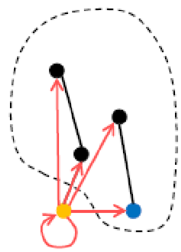
- 证明：（归纳法）
  - $|S| = 1$，$(S,\preccurlyeq') = (S,\preccurlyeq)$。
  - $|S| > 1$：取$(S,\preccurlyeq)$中的一个极小元x_0，$S' = S\backslash\{x_0\}$。

  $(S',\preccurlyeq)$是一个偏序集，且$|S'| < |S|$。

  根据归纳假设，存在$(S',\preccurlyeq)$的线性扩充$(S',\preccurlyeq'')$，

  构造$(S,\preccurlyeq')$为：$\preccurlyeq' = \preccurlyeq'' \cup \{(x_0, y) \mid y \in S\}$.

  可证$(S,\preccurlyeq')$是一个线性序。



一般地，线性扩充不唯一。

27

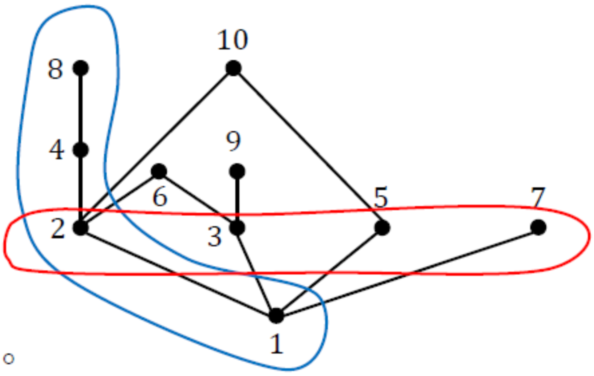
或者“宽”或者“高”

链与反链

对有限偏序集$(S,\preccurlyeq)$，$x,y\in S$，称x,y

例：$(\{1,2,\dots,10\},|)$

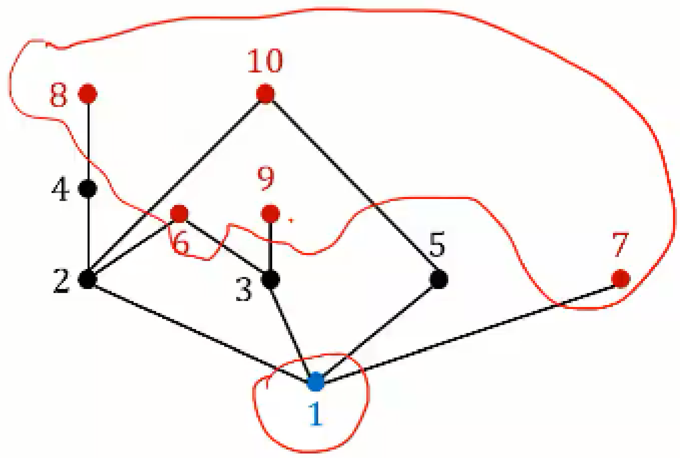
- 可比较(Comparable)：若$x\preccurlyeq y$ 或 $y\preccurlyeq x$。
- 不可比较(Incomparable)：若$x\not\preccurlyeq y$ 且 $y\not\preccurlyeq x$。



- 链：可比较元素的集合。
- 反链：不可比较元素的集合。

- 链-形成线性序，可比较元素的集合
- 反链/独立集-任意两个元素不可互相比较，不可比较元素的集合

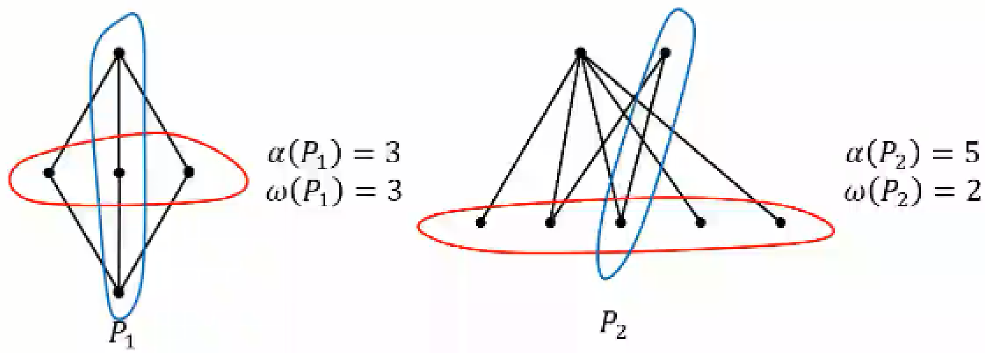
极大元、极小元的集合一定组成反链



最大独立集和最长链

给定有限偏序集 $P=(S,\preccurlyeq)$

- $\alpha(P)=\max\{|A|: A$是P上的反链（独立集）$\}$
- $\omega(P)=\max\{|A|: A$是P上的链$\}$



最长链长度=最小反链划分数

定理： 给定有限偏序集 $P=(S,\preccurlyeq)$，将S划分成若干不相交的反链集，取最小划分数t，即

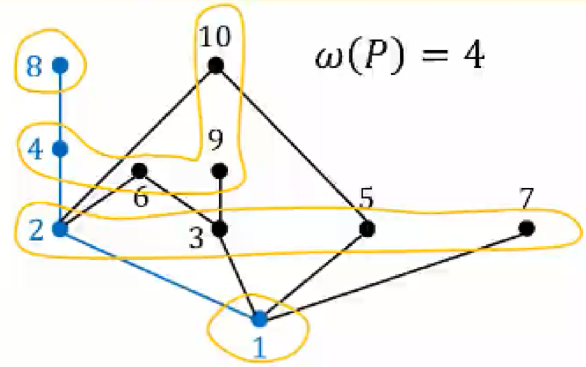
$$t=\min\left\{k\;\middle|\;\begin{array}{l}S=A_1\cup\cdots\cup A_k,\\ 1\le i\le k,\ A_i\ \text{是反链},\\ \text{任意}1\le i\ne j\le k,\ A_i\cap A_j=\emptyset.\end{array}\right\}$$

则$t=\omega(P)$.

例子：考虑极小元

贪心法，先选取极小元组成反链，再去掉该反链，如此重复

例：



$\omega(P)=4$

$A_4=\{8\}$

$A_3=\{4,6,9,10\}$

$A_2=\{2,3,5,7\}$

$A_1=\{1\}$

证明

证明1

证明：$\omega(P)\le t$

$S=A_1\cup A_2\cup\cdots\cup A_t$，其中$\{A_1,\ldots,A_t\}$为不相交的反链划分，

$C\subseteq S$ 是P中任意一条链，有 $|C\cap A_i|\le 1$.

$\cancel{|C\cap A_i|=2}$ (x,y)

$$\begin{aligned}|C|=|C\cap S|&=|C\cap(A_1\cup A_2\cup\cdots\cup A_t)|\\&=|(C\cap A_1)\cup\cdots\cup(C\cap A_t)|\\&\le t\end{aligned}$$

$\omega(P)$

$(C\cap A_i)\cap(A_j\cap C)=\phi$

$\le\sum_{i=1}^{t}|C\cap A_i|\le t$

18

找到有长度为t的链即可

证明：$\omega(P)\ge t$

$A_1=S$ 的极小元集合，✓

$A_{i+1}=S\setminus(A_1\cup\cdots\cup A_i)$ 的极小元集合。

每一个A_i都是一个反链（独立集）。

有限步后$A_1\cup\cdots\cup A_m=S$。

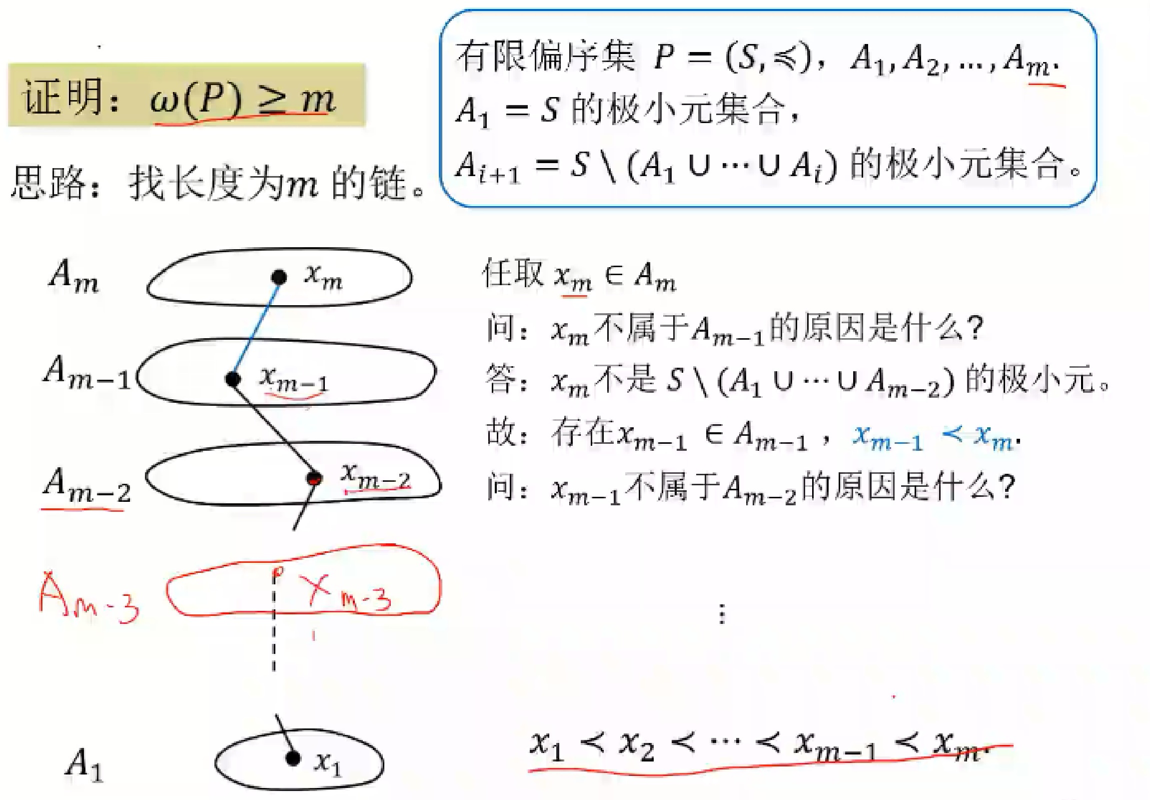
由t的最小性，$m\ge t$。 只需证明，$\omega(P)\ge m$。

A_m

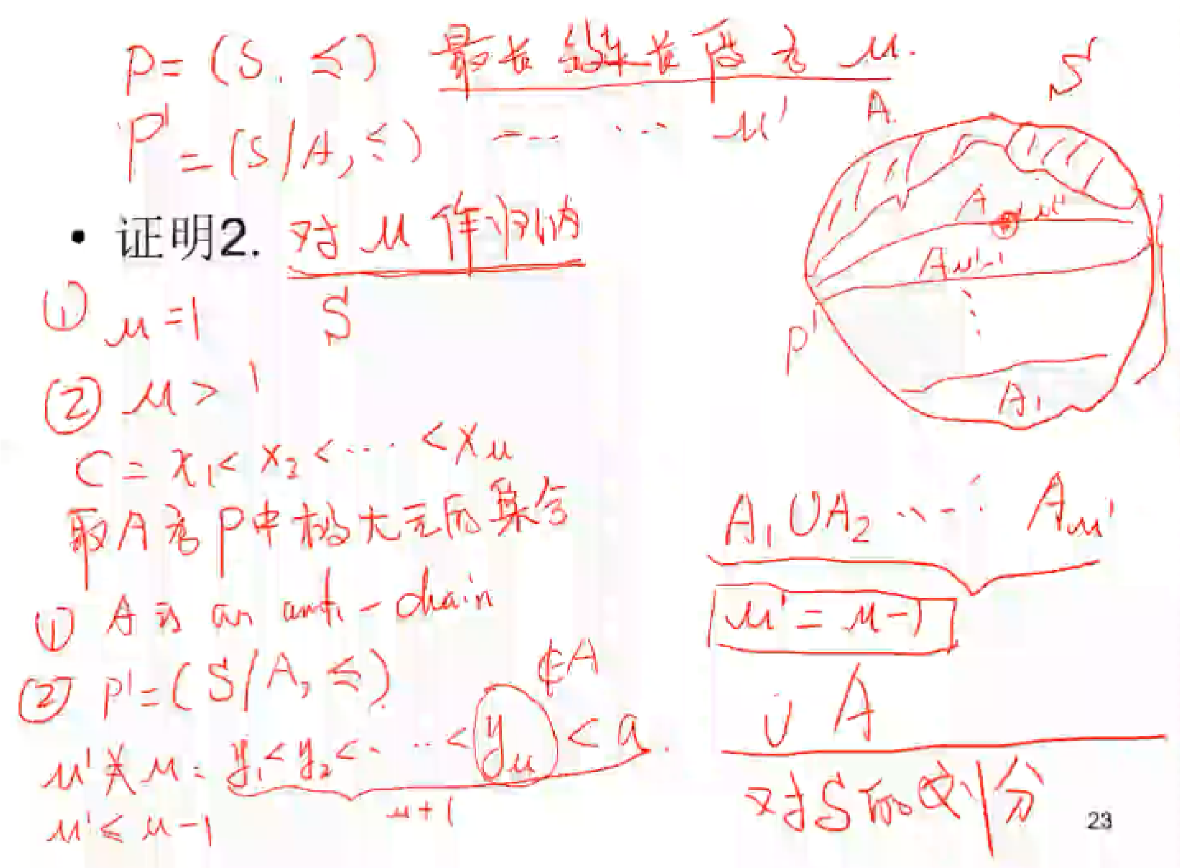
A_1

19

只需找到长度为m的链即可



证明2 归纳法证明



应用

应用1

$\alpha(P)$最大反链大小

$\omega(P)$最长链长度

- **定理：** 给定有限偏序集 $P=(S,\preccurlyeq)$，
  $\max\{|C|: C\text{是}P\text{上的链}\} = \min\{|\Pi|: \Pi\text{是}S\text{的反链划分}\}$.
- **推论：** 给定有限偏序集 $P=(S,\preccurlyeq)$

$$\alpha(P)\cdot\omega(P)\geq |S|.$$

证明：

Anti-chain

$$P = A_1 \cup A_2 \cup \cdots \cup A_t$$

$$t=\omega(P)$$

$$|A_i| \leq \alpha(P)$$

$\leq \alpha(p)$

$$|S| = |A_1| + |A_2| + \cdots + |A_t| \leq \alpha(P)\cdot\omega(P)$$

$= \omega(p)$

24

对任意有限偏序集 $P=(S,\preccurlyeq)$，$\alpha(P)$或$\omega(P)$之一至少为$\sqrt{|S|}$。

宽　高

直观：任意有限偏序集或者“宽”，或者“高”。

应用2

- Erdös-Szekeres引理：

任意含有n^2+1个元素的实数序列$(x_1,\ldots,x_{n^2+1})$中都含有一个长度为$n+1$的单调子序列。

例： $n=3$, $(1, 2, 10, 4, 3, 5, 1, 6, \cancel{5}, 8)$

证明

证明： 对 $(x_1,\dots,x_{n^2+1})$，设 $I=\{1,2,\dots,n^2+1\}$ 3和4

在集合 I 上定义关系 $\preccurlyeq$: $i \preccurlyeq j$ 当且仅当 $(i\le j)\wedge(x_i\le x_j)$

$(I,\preccurlyeq)$ 是偏序集。 $|I|=n^2+1$ $\sqrt{|I|}$ 不 n

高 • $\omega(I,\preccurlyeq)>n$: 非递减子序列 $x_{i1}\le x_{i2}\le\cdots\le x_{im}$.

宽 • $\alpha(I,\preccurlyeq)>n$: 独立集 $\{i_1,i_2,\dots,i_m\}$，设 $i_1<i_2<\cdots<i_m$

$x_{i1}>x_{i2}>\cdots>x_{im}$， 非递增子序列。

29

Dilworth定理

- **Dilworth定理：** 给定有限偏序集 $P=(S,\preccurlyeq)$，
  $\max\{|A|: A是P上的反链\}=\min\{|ß|: ß是S的链划分\}$.

是mirsky定理的对偶定理

- **Mirsky's theorem定理：** 给定有限偏序集 $P=(S,\preccurlyeq)$，
  $\max\{|C|: C是P上的链\}=\min\{|\Pi|: \Pi是S的反链划分\}$.
- **Dilworth定理：** 给定有限偏序集 $P=(S,\preccurlyeq)$，
  $\max\{|A|: A是P上的反链\}=\min\{|ß|: ß是S的链划分\}$.

证明

证明难点：无法像mirsky定理一样通过最小元来寻找反链划分，链的划分没有方法去寻找

使用归纳法证明：

显然有 $max\{|A|\}\le min\{m\}$

否则 A 中一定含有两个同一条链中的元素，则违反了 A 为反链的条件

Proof: $P=\bigcup_{i=1}^{m} C_i$ (C_i is a chain, $C_i\cap C_j=\phi$, ~)

A is an antitain

$\max|A|\le \min\{m|\cdots\}$ ($m<|A|$)

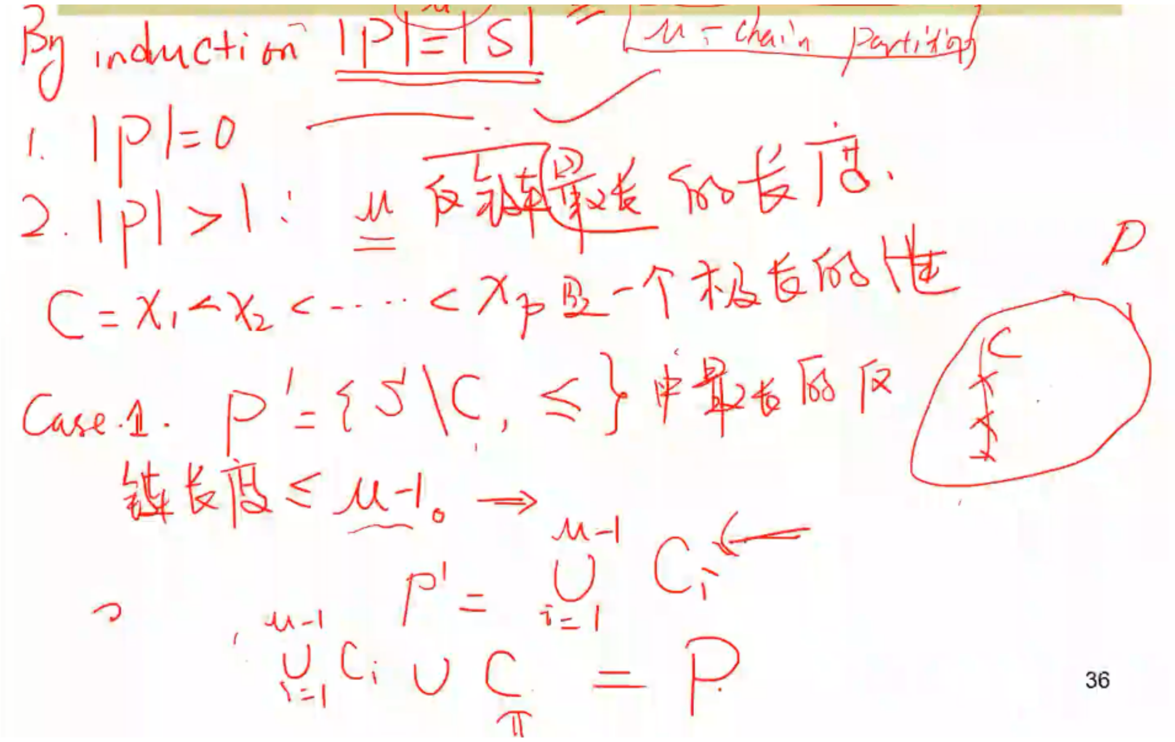
证明 $max\{|A|\}\ge min\{m\}$

构造一个链划分 m，使得 $max\{|A|\}\ge m$ 即可

设 $\mu=max\{|A|\}$，证明存在链划分 $m=\mu$

case1

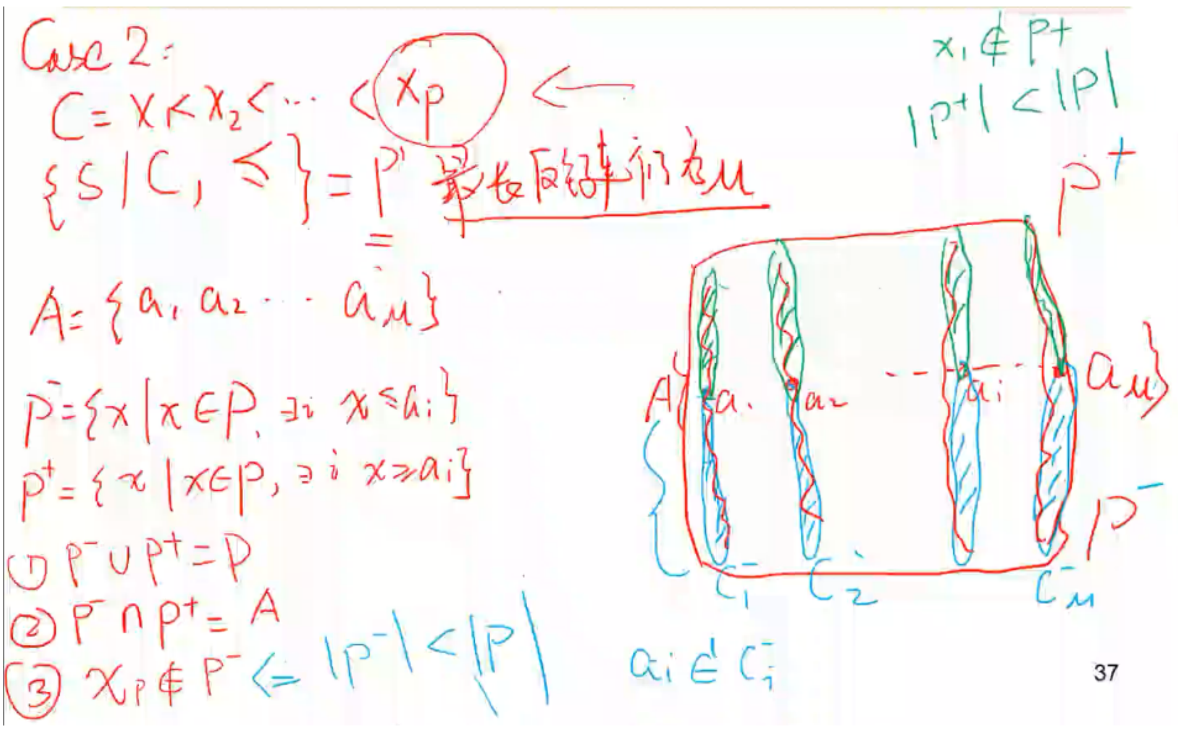
先去掉极长链，则最长反链长度 $\le\mu-1$，根据归纳假设此时 $m=\mu-1$，加上最长链，则 $m=m+1=\mu$



case2

去掉极长链后，最长反链长度仍然$=\mu$

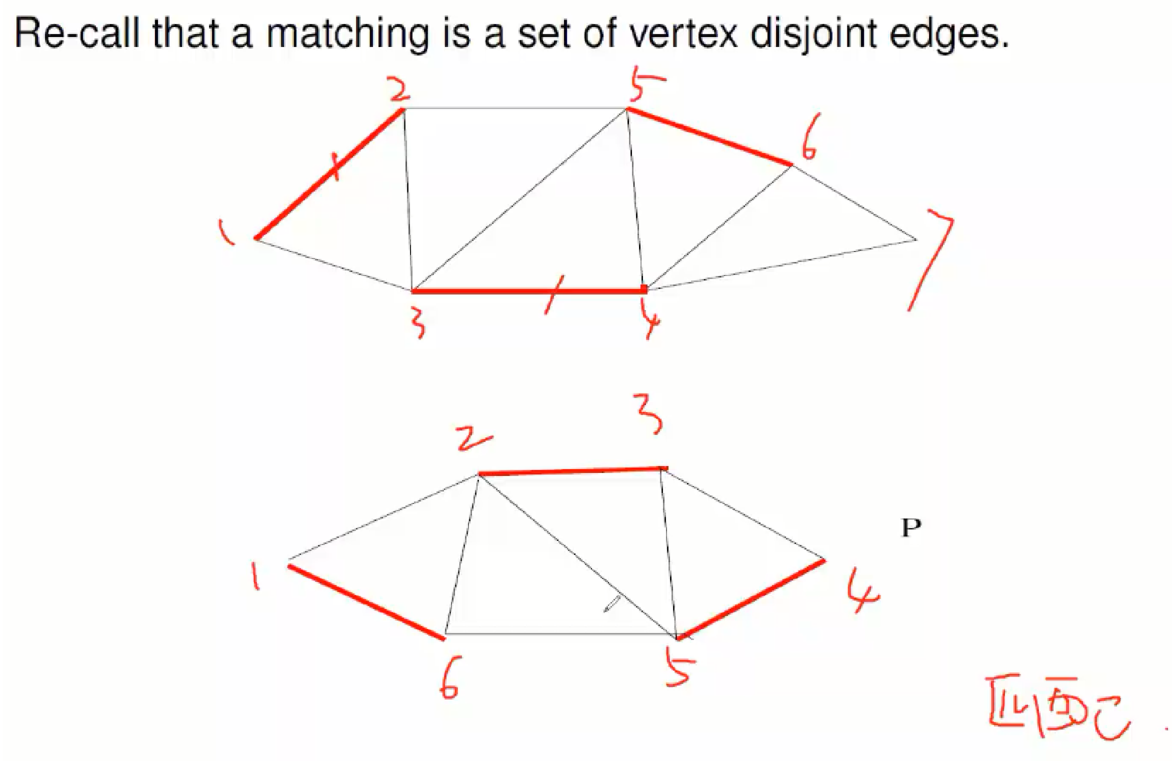
划分P^-和P^+，因为$x_P\notin P^-$，所以$|P^-|<|P|$，对P^-可以使用归纳假设，P^-中最长反链为μ，存在链划分$m=\mu$，且$a_1,a_2,\cdots$为各个链的头；因为$x_1\notin P^+$，所以$|P^+|<|P|$，对P^+可以使用归纳假设，P^+中最长反链为μ，存在链划分$m=\mu$，且$a_1,a_2,\cdots$为各个链的尾；故P^-和P^+的链可以连接起来，故链划分数$m=\mu$

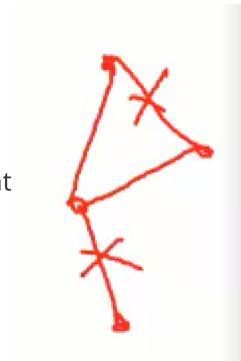


应用

匹配 match

两点间互相匹配，没有交集



disjoint 

Hall定理

任取左边子集，其相连的右边集合size要大于该子集

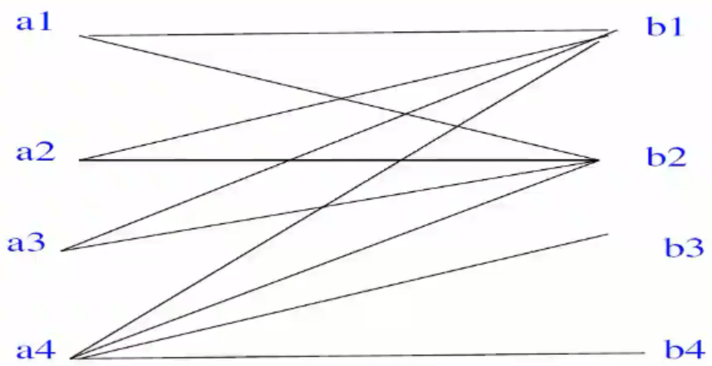
Theorem

(Hall) G contains a matching of size $|A|$ iff

完美匹配

$$|N(S)| \geq |S| \qquad \forall S \subseteq A.$$

$G = (A \cup B, E)$



$N(\{a_1, a_2, a_3\}) = \{b_1, b_2\}$ and so at most 2 of a_1, a_2, a_3 can be saturated by a matching.

证明

正向

If G contains a matching M of size $|A|$ then $M = \{(a, f(a)) : \ a \in A\}$, where $f : A \to B$ is a 1-1 function.

But then,

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

for all $S \subseteq A$.

反向

$|B| - k \geq h$

Let $G = (A \cup B, E)$ be a bipartite graph which satisfies Hall's condition. Define a poset $P = A \cup B$ and define $<$ by $a < b$ only if $a \in A, b \in B$ and $(a, b) \in E$.

$\in A \quad \in B$

(1) $\forall a \ a \le a$, $\forall b \ b \le b$

(2) $a < b$ iff $(a,b) \in E$

$(P, \le)$

Suppose that the largest anti-chain in P is $A = \{\underbrace{a_1, a_2, \dots, a_h}_{A}, \underbrace{b_1, b_2, \dots, b_k}_{B}\}$ and let $s = h + k$.

Now

$$N(\{\underbrace{a_1, a_2, \dots, a_h}_{S}\}) \subseteq B \setminus \{b_1, b_2, \dots, b_k\}$$

for otherwise A will not be an anti-chain. $|B| - k$

From Hall's condition we see that $h = |S| \le |N(S)| \le |B| - k$

$$|B| - k \ge h \text{ or equivalently } |B| \ge s.$$

利用dilworth定理，链划分数即为match的个数，包括m个配对，$|A|-m$个落单男生，$|B|-m$个落单女生

Now by Dilworth's theorem, P is the union of s chains:

A matching M of size m, $|A| - m$ members of A and $|B| - m$ members of B. $a_i < b_j$

But then

$$m + (|A| - m) + (\cancel{|B|} - m) = s \le |B|$$

and so $m \ge |A|$. □

$|A| + \cancel{|B|} - m$

$m \le |A|$ $\quad$ $m = |A|$

$\le \leftarrow$

1 (1) $a \le a, b \le b$

2 (2) $a < b$ iff $(a,b) \in E$

$A_n = \{a_1 \cdots a_h, b_1 \cdots b_k\}$ Anti-chain.

Chain partition $= \{\underbrace{\{a_1,b_1\} \{a_2,b_2\} \cdots \{a_m,b_m\}}_{m} \underbrace{\{a\}\{a\}}_{|A|-m} \underbrace{\{b\}\{b\}}_{|B|-m}$

$m \ge |A|$，又因为配对的个数不可能大于男生个数，$m = |A|$

Ch 03 组合

n balls are put into m bins

balls per bin	unrestricted	≤ 1	≥ 1
n distinct balls, m distinct bins.	m^n	$(m)_n$	$m!\left\{ n \atop m \right\}$
n identical balls, m distinct bins.	$\binom{n+m-1}{m-1}$	$\binom{m}{n}$	$\binom{n-1}{m-1}$
n distinct balls, m identical bins.	$\sum_{k=1}^{m} \left\{ n \atop k \right\}$	$\begin{cases} 1 & n \leq m \\ 0 & n > m \end{cases}$	$\left\{ n \atop m \right\}$
n identical balls, m identical bins.	$\sum_{k=1}^{m} p_k(n)$	$\begin{cases} 1 & n \leq m \\ 0 & n > m \end{cases}$	$p_m(n)$

- distinct 不同
- identical 相同

n个不同球放m个不同盒子

每个球m种不同放法

应用

证明集合$X, |X| = n$，有2^n个子集

构造特征函数

for any $A \subseteq X$, define $f_A : X \to \{0,1\}$ as

$$\boxed{f_A(x) = \begin{cases} 1 & if\ x \in A \\ 0 & if\ x \notin A \end{cases}}$$

每个特征函数对应一个子集取法，共有2^n个特征函数

n个不同球放m个不同盒子 每个盒子至多放一个球

第一个球m种不同放法，第二个球只能从剩下m-1个盒子中选择

$(x)_n = x(x-1)\cdots(x-n+1)$

应用 factorial

集合本身到本身的双射，有$(n)_n = n!$种

n个相同球放m个不同盒子

隔板法，$\binom{n+m-1}{m-1}$

组合数性质

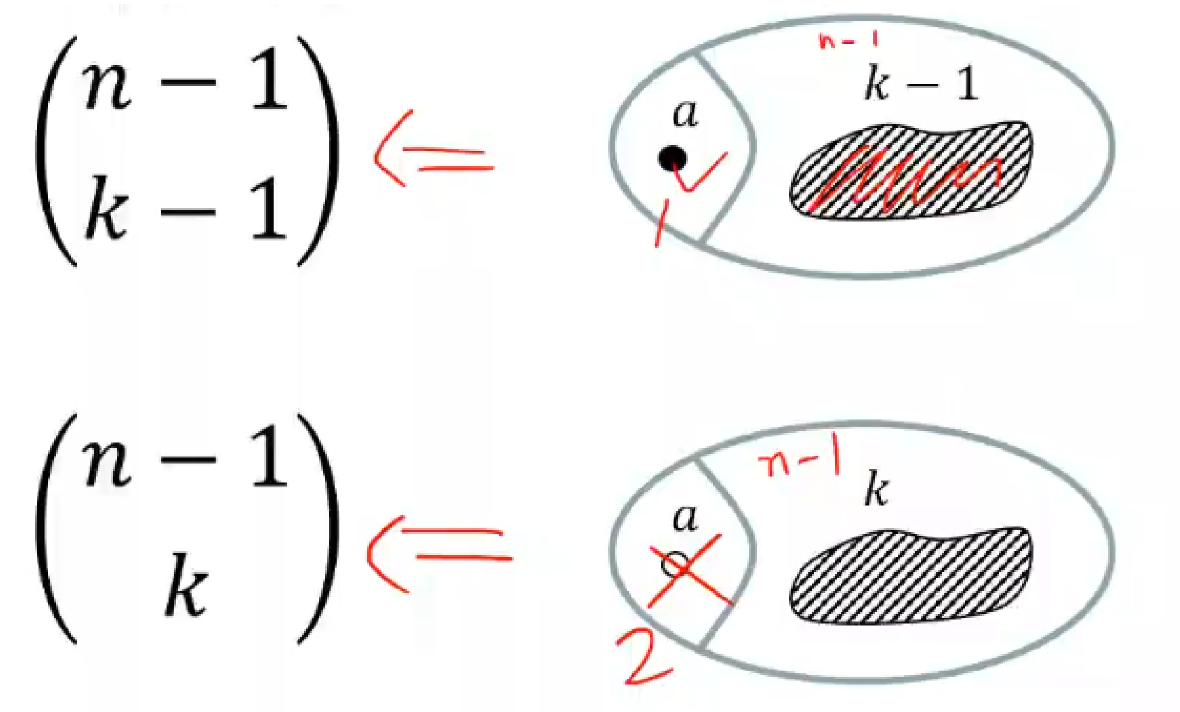
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

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

proof. n选k个，等于n选n-k个丢弃

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

proof. n中选k的两种选法，从一个特殊点a来考虑



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

$\sum\limits_{k=0}^{n} \binom{m+k-1}{k} = \binom{n+m}{n}$

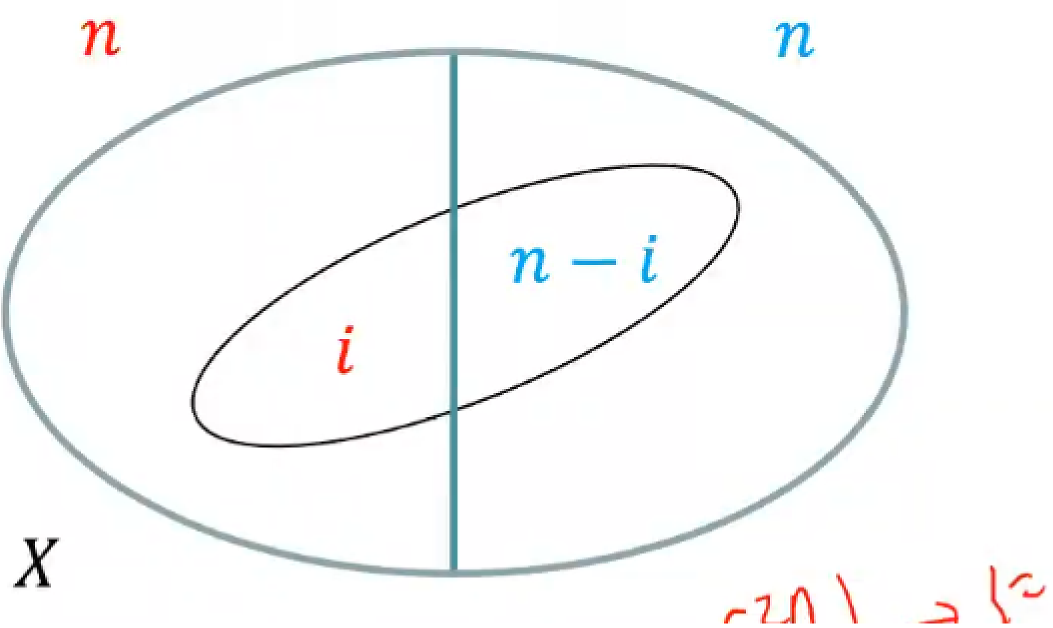
以上两个作业中有证明

$\sum\limits_{k=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$

proof. 2n中选n个的取法

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$$

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$$



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

proof. 类似上个结论

继续推广

$$\binom{n_1 + \cdots + n_p}{m} = \sum_{k_1+\cdots+k_p=m} \binom{n_1}{k_1}\binom{n_2}{k_2}\cdots\binom{n_p}{k_p}$$

多重集 multiset number

集合中允许一个元素反复出现

$A=\{1,2,3\}$ $\begin{pmatrix} \{1,2\} & \{1,3\} & \{2,3\} \\ \{1,1\} & \{2,2\} & \{3,3\} \end{pmatrix}$

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

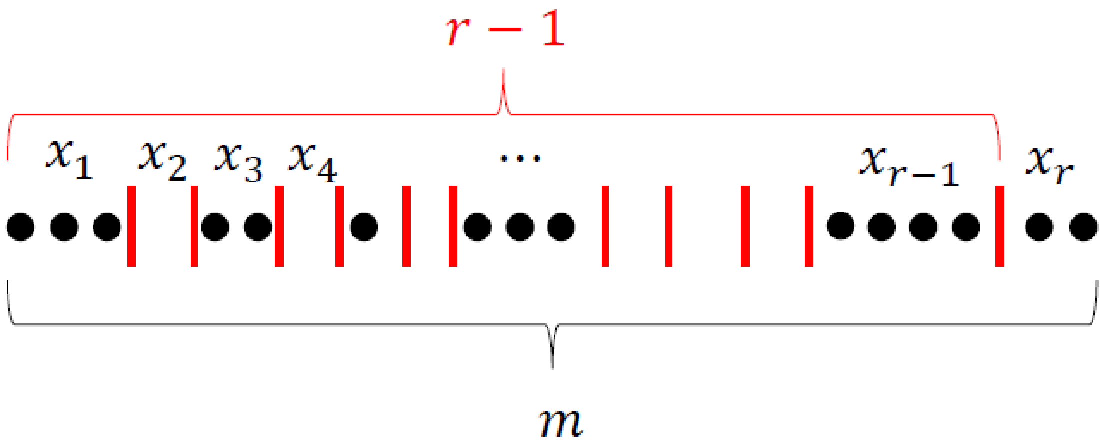
proof. 就是$x_1+x_2+\cdots+x_n=k$非负整数解的个数

其中x_i代表第i个元素在集合中出现的次数

应用 非负解个数

$x_1+x_2+\cdots+x_r=m$，$m\ge r\ge 0$

隔板法，从$m+r-1$个挡板+球种选$r-1$个挡板，有$\binom{m+r-1}{r-1}$个非负解



$\boldsymbol{x_1=3, x_2=0, x_3=2, x_4=0, \cdots, x_{r-1}=4, x_r=2}$

n个相同球放m个不同盒子 每个盒子至多一个球

从m个盒子中选择n个放入球即可，$\binom{m}{n}$

n个相同球放m个不同盒子 每个盒子至少一个球

变量替换，$y_i=x_i-1$，$y_1+y_2+\cdots+y_r=m-r$

共有$\binom{m-1}{r-1}$

二项式定理

$(1+x)^n=\sum\limits_{k=0}^{n}\binom{n}{k}x^k$

proof. x^k对于所有$(1+x)$，共有$\binom{n}{k}$个选择了x

$x=1$, $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}=2^n$

$x=-1$, $\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}\cdots=\sum_{k=0}^{n}\binom{n}{k}(-1)^k=0$，n选奇=n选偶

前两个相加，$2[\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots]=2^n$ $= 2^{n-1}$，选奇选偶各一半

带重复的排列

几种不同颜色球，每种颜色球都相同，放入不同的盒子中

- With 5 different red balls, 3 different yellow balls, 4 different blue balls, we can get $(5+3+4)!=12!$ different sequences.

- **Question:** With 5 equal red balls, 3 equal yellow balls, 4 equal blue balls, how many different sequences can we get?

$k_1+k_2+\cdots+k_m=n$，k_i为第i类球的个数，n为总球数

排列有$\frac{n!}{k_1!k_2!\cdots k_m!}$种，写为$\binom{n}{k_1,k_2,\cdots,k_m}$

一些概念

多项式定理

$$(x_1+x_2+\cdots+x_m)^n = \sum_{\substack{k_1+\cdots k_m=n\\ k_1,\cdots,k_m\geq 0}} \binom{n}{k_1,k_2,\ldots,k_m} x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}.$$

In $(x+y+z)^{10}$ the coefficient of $x^2y^3z^5$ is $\binom{10}{2,3,5}=2520$.

x y z $\frac{10!}{2!\,3!\,5!}$

一般二项式定理

$$\binom{r}{k} = \frac{r(r-1)\cdots(r-k+1)}{k!} = \frac{(r)_k}{k!}$$

r为任意实数，k为正整数

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

$$= x^r + r x^{r-1} y + \frac{r(r-1)}{2!} x^{r-2} y^2 + \frac{r(r-1)(r-2)}{3!} x^{r-3} y^3 + \cdots$$

x，y为实数，$|x| > |y|$

应用

$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \frac{7}{256}x^5 - \cdots$$

$$(1+x)^{-1} = \frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 - x^5 + \cdots$$

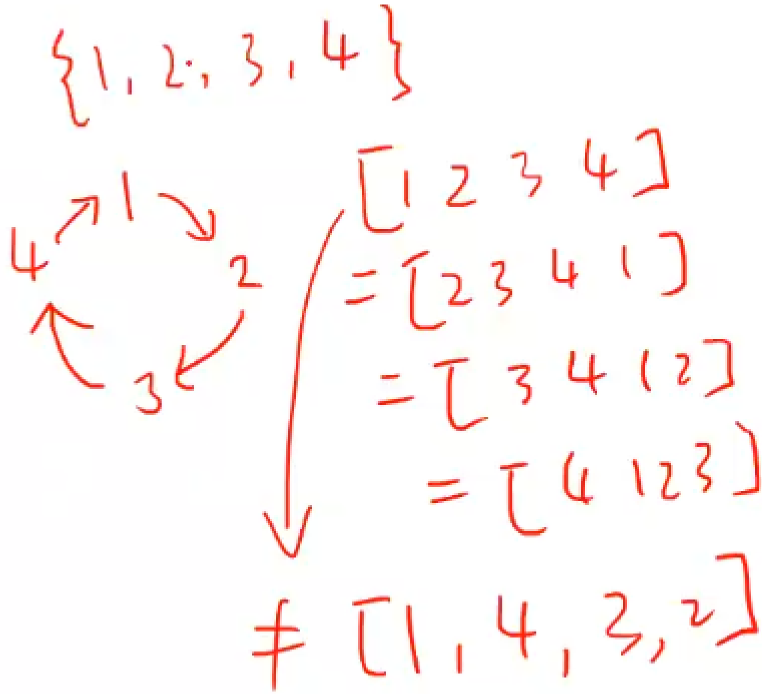
Generally: $r = -s$

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

$$\frac{1}{\sqrt{1+x}} = 1 - \frac{1}{2}x + \frac{3}{8}x^2 - \frac{5}{16}x^3 + \frac{35}{128}x^4 - \frac{63}{256}x^5 + \cdots$$

第一类斯特林数

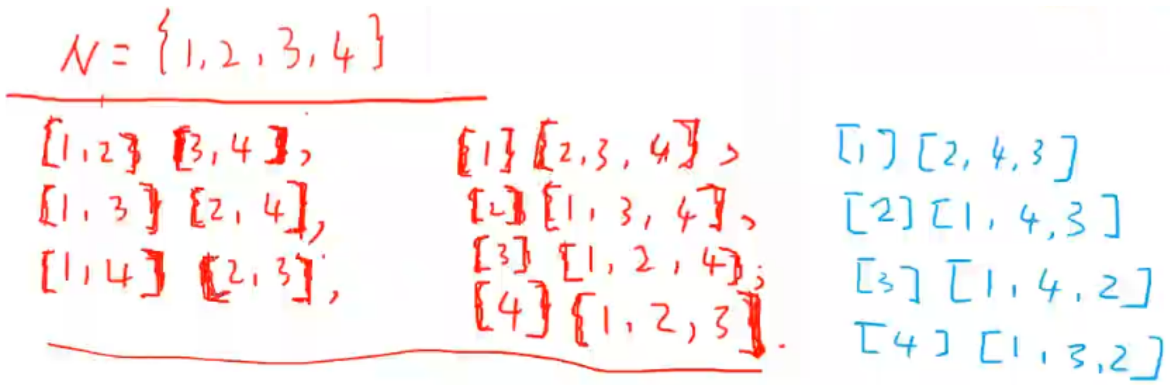
n个元素分为k个非空cycle



性质

- $\begin{bmatrix} n \\ k \end{bmatrix} \ge \begin{Bmatrix} n \\ k \end{Bmatrix}$一种子集对应很多种cycle

4选2的第一类斯特林数为11；4选2的第二类斯特林数为7



- $\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!$

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n! \text{ where } n \in Z^{+}.$$ n个

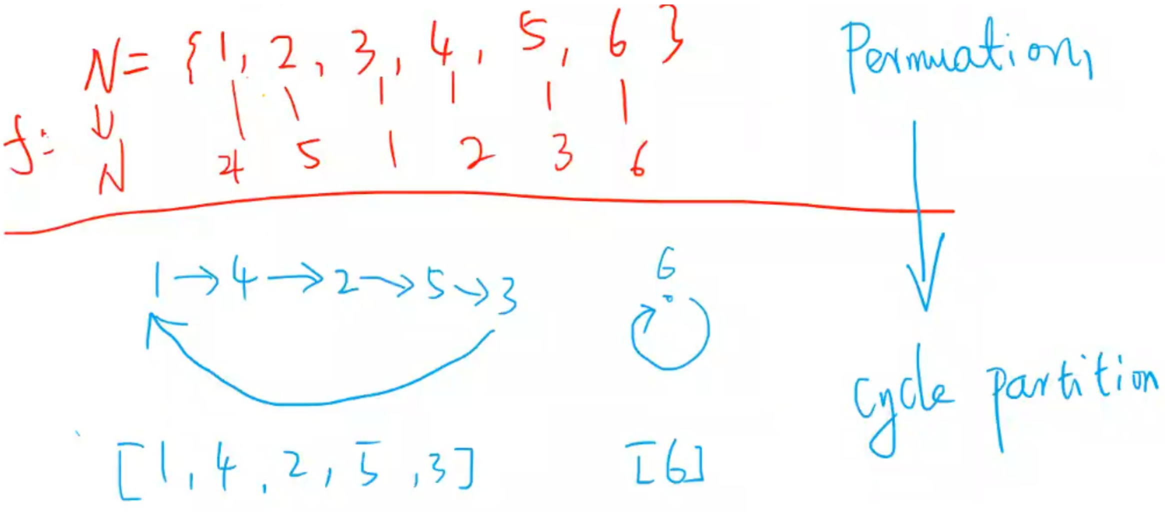
元素全排列，从任一个元素开始读

- $\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!$

- $\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n! \text{ where } n \in Z^{+}.$

proof. $n!$为N到N双射函数的size

双射函数与cycle partition一一对应，大小相等。



- $\begin{bmatrix} n \\ k \end{bmatrix} = (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$

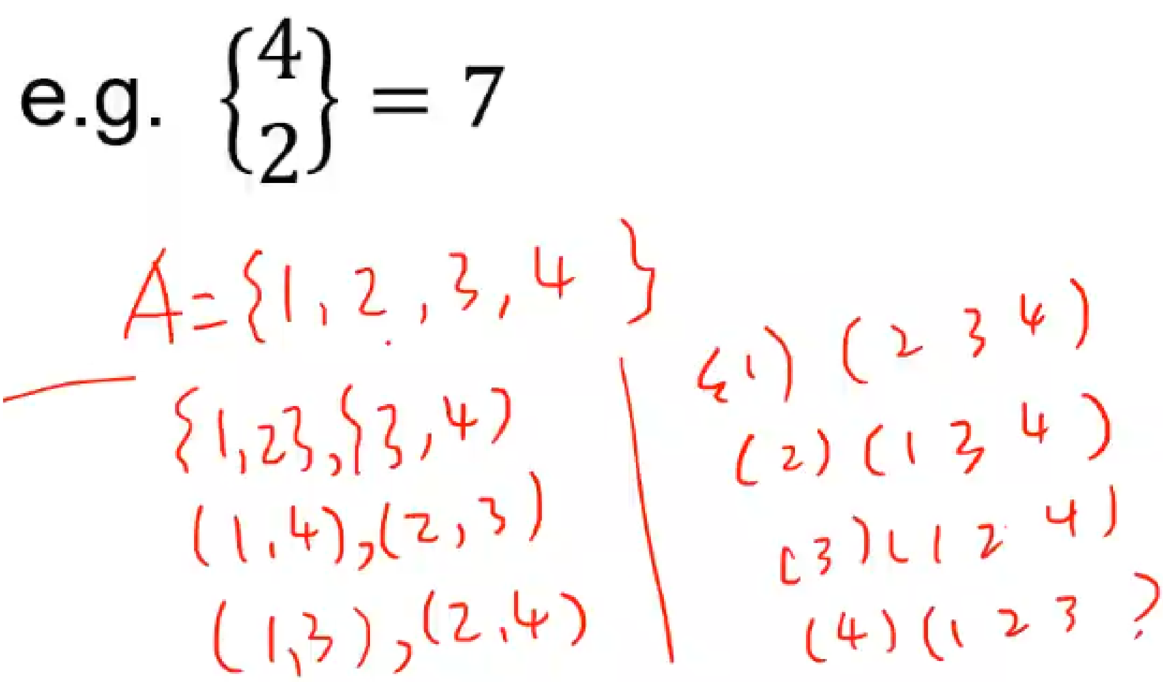
a不单独成一个cycle，n-1选k个cycle，a可插入任何位置；a单独成一个cycle，剩余n-1个选k-1个cycle

n个不同球放m个不同盒子 每个盒子至少放一个球

n个球分为m个非空子集，m个子集全排列对应m个盒子 $m!\left\{ n \atop m \right\}$

第二类斯特林数 stirling subset numbers

n个对象分为k个非空子集



n个对象分为2个非空子集

$$\left\{ n \atop 2 \right\} = 2^{n-1} - 1$$

先从n中命名一个点为a，从剩下的元素中选一个子集，有2^{n-1}种选法，子集∪a为一个集合；剩下元素为另一个集合。减去1是因为当子集选取剩下全部元素时，有一个集合为空，要去掉这种情况

$$\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$$

a不单独成集合，n-1个元素分为k个子集，a选一个加入；a单独成集合，剩下n-1个元素分为k-1个子集

n个不同球放m个相同盒子

n个球分为k个子集，$(0 \le k \le m)$ $\sum_{k=1}^{m} \left\{ {n \atop k} \right\}$

n个不同球放m个相同盒子 每个盒子至少放一个球

n个球分为m个子集 $\left\{ {n \atop m} \right\}$

n个相同球放m个相同盒子

因为m个盒子中有部分盒子可以不放球，相当于正整数n分为k个部分，$(0 \le k \le m)$，$\sum_{k=1}^{m} p_k(n)$

partition of a number

$P_k(n)$将一个正整数n分为k个部分的方法即 $\begin{cases} x_1 + x_2 + \cdots + x_k = n \\ x_1 \ge x_2 \ge \cdots \ge x_k \ge 1 \end{cases}$

例如 $\begin{matrix} P_2(7) = 3 & \{\{1,6\},\{2,5\},\{3,4\}\} \\ P_6(7) = 1 & \{\{1,1,1,1,1,2\}\} \end{matrix}$

有递归式$P_k(n) = P_{k-1}(n-1) + P_k(n-k)$

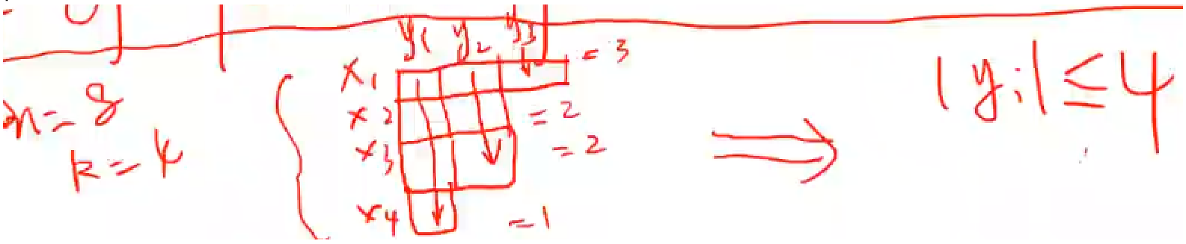
proof. 若$x_k = 1$，将n-1分为k-1个；若$x_k > 1$，所有$x > 1$，都减去1，相当于将$n-k$分为k个

$\sum_{k=1}^{m} p_k(n) = p_m(n+m)$

proof. 相当于先每个盒子里分了一个球，再对m个盒子进行$\sum_{k=1}^{m} p_k(n)$

$p_k(n)$与将n个元素分为任意k个部分，这些部分里最大一部分的size为k相同

proof.



从列来看分成y1，y2，y3三部分，最大size为4

n个相同球放m个相同盒子 每个盒子至少放一个球

相当于正整数n分为k个部分，$p_m(n)$

容斥原理

对任意有限集合$A_1, A_2, \ldots, A_n$，有

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n}(-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left|\bigcap_{i\in I} A_i\right| = \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|-1} \left|\bigcap_{i\in I} A_i\right|$$

证明

- $n=2$ 时定理成立。
- 假设对任意 $n-1$ 定理成立。
- 继续证明规模为 n 时定理成立，此时：

$$\begin{aligned}
\left|\cup_{i=1}^{n} A_i\right| &= \left|\left(\cup_{i=1}^{n-1} A_i\right) \cup A_n\right| \\
&= \left|\cup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\cup_{i=1}^{n-1} A_i\right) \cap A_n\right| \\
&= \left|\cup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\cup_{i=1}^{n-1} (A_i \cap A_n)\right| \\
&= \cdots
\end{aligned}$$

错排公式

n个有序元素进行排列后，所有元素都不在原来的位置

任给一个n，求出$1, 2, \cdots, n$错排个数$D(n)$个数

排列共有$n!$种，定义A_i为第i个元素映射到自己的排列的集合

$D(n)=n!-|A_1\cup\cdots\cup A_n|$即所有映射到自己的排列都不发生

$|A_i|=(n-1)!$除了第i个，其他可以任意映射

$i<j,|A_i\cap A_j|=(n-2)!$除了ij，其他可以任意映射

$i_1<i_2<\cdots<i_k,|A_{i1}\cap A_{i2}\cap\cdots\cap A_{ik}|=(n-k)!$

根据*容斥原理*：$|A_1\cup\cdots\cup A_n|=\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)!=\sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!}$

故$D(n)=n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!}\right)$

$$\boxed{\lim_{n\to\infty}D(n)=n!/e}$$

欧拉函数

$\phi(n)$为不超过n且和n互素的自然数个数（互素：最大因子为1，例如3和5互素）

$\varphi(3)=2\quad(1,2)$

例如 $\varphi(8)=4\quad(1,3,5,7)$

$\varphi(12)=4\quad(1,5,7,11)$

欧拉函数解析解

解： 根据整数分解定理，n可被唯一地分解成$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$。其中$\alpha_i>1$且$p_i$为素数，$p_1<p_2<\cdots<p_r$.

- 如果$1\le m<n$且m与n不互素，则必存在某个$1\le i\le r$ 有 $p_i|m$.
- $1\le i\le r$ 令 $A_i=\{m\in\{1,2,\dots,n\}: p_i|m\}$
- 则 $\varphi(n)=n-|A_1\cup A_2\cup\cdots\cup A_r|$

$$\varphi(n) = n - |A_1 \cup A_2 \cup \cdots \cup A_r|$$

$1 \le i \le r \quad A_i = \{m \in \{1,2,\ldots,n\}: p_i | m\}$

- $|A_i| = \dfrac{n}{p_i}$
- $i < j \quad |A_i \cap A_j| = \dfrac{n}{p_i p_j}$
- $i_1 < i_2 < \cdots < i_k$,

$$|A_{i1} \cap A_{i2} \cap \cdots \cap A_{ik}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{ik}}$$

- 根据***容斥原理***并整理化简后，

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

11

知道素分解->知道欧拉函数

应用于公钥：

1. 一个公钥对应一个私钥。
2. 密钥对中，让大家都知道的是公钥，不告诉大家，只有自己知道的，是私钥。
3. 如果用其中一个密钥加密数据，则只有对应的那个密钥才可以解密。
4. 如果用其中一个密钥可以进行解密数据，则该数据必然是对应的那个密钥进行的加密。

Ch 03 生成函数 generating function

- Problem: How many ways are there to pay the amount of 21 doublezons if we have
  - 6 one-doublezon coins;
  - 5 two-doublezon coins;
  - 4 five-doublezon coins.
- Solution:

$$i_1 + i_2 + i_3 = 21 \quad (*)$$

$i_1 \in \{0, 1, 2, 3, 4, 5, 6\}$; $i_2 \in \{0, 2, 4, 6, 8, 10\}$; $i_3 \in \{0, 5, 10, 15, 20\}$.

$$(1 + x + x^2 + x^3 + \cdots + x^6)(1 + x^2 + x^4 + x^6 + x^8 + x^{10}) \cdot (1 + x^5 + x^{10} + x^{15} + x^{20})$$

The coefficient of x^{21}
= the number of solutions of (*).

转化成x^{21}的系数

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

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$ x=1

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} \cdots = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$ x=-1

x=1

$$\boxed{\sum_{k=0}^{n} k \binom{n}{k} = n\, 2^{n-1}}$$

左右求一阶导后令x=1

生成函数

- $(a_0, a_1, a_2, \ldots)$ be a sequence of real numbers, then the generating function of this sequence is defined as

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

$$\frac{1}{(1-x)^n} = \underbrace{\binom{n-1}{n-1}}_{a_0} + \underbrace{\binom{n}{n-1}}_{a_1} x + \underbrace{\binom{n+1}{n-1}}_{a_2} x^2 + \cdots \underbrace{\binom{n+k-1}{n-1}}_{a_n} x^k + \cdots$$

$(1-x)^{-n}$

5

$(a_0, a_1, a_2, \ldots) \qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$

$(0, a_0, a_1, a_2, \ldots) \qquad a(x) = 0 + a_0 x + a_1 x^2 + \cdots = x \cdot a(x)$

$(0, 1, \frac{1}{2}, \frac{1}{3}, \ldots) \qquad a(x) = \frac{x}{1} + \frac{x^2}{2} + \frac{x^3}{3} + \cdots = -\ln(1-x) \quad -1 < x < 1$

$(1, \frac{1}{1!}, \frac{1}{2!}, \frac{1}{3!}, \ldots) \qquad a(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x$

生成函数操作

做加法

Operations with Sequences -Addition

$(a_0, a_1, a_2, \ldots) \qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$

$(b_0, b_1, b_2, \ldots) \qquad b(x) = b_0 + b_1 x + b_2 x^2 + \cdots$

$(a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) \qquad a(x) + b(x)$

线性

$$(a_0, a_1, a_2, \dots) \qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

$$(\alpha a_0, \alpha a_1, \alpha a_2, \dots) \qquad \alpha \cdot a(x)$$

右移

$$(a_0, a_1, a_2, \dots) \qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

$$(\underbrace{0, 0, \cdots, 0}_{n}, a_0, a_1, a_2, \dots) \qquad x^n \cdot a(x)$$

左移

$$(a_0, a_1, a_2, \dots) \qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

$$(a_3, a_4, a_5, \dots) \qquad \frac{a(x) - a_0 - a_1 x - a_2 x^2}{x^3}$$

替换

线性

$$(a_0, a_1, a_2, \dots) \qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

$$(a_0, \alpha a_1, \alpha^2 a_2, \dots) \qquad a(\alpha x)$$

Example:

$$(1, 1, 1, \dots) \qquad a(x) = \frac{1}{1 - x}$$

$$(1, 2, 4, 8, \dots) \qquad a(2x) = \frac{1}{1 - 2x}$$

$$(a_0, 0, a_2, 0, a_4, 0 \dots) \qquad \frac{1}{2}(a(x) + a(-x))$$

方

Substituting $-x^n$

$(a_0, a_1, a_2, \dots)$ $\quad a(x) = a_0 + a_1x + a_2x^2 + \cdots$

$(a_0, 0,0, a_1, 0,0, a_2, 0,0, \dots)$ $\quad a_0 + a_1x^3 + a_2x^6 + \cdots = a(x^3)$

Example:

$(1,1,2,2,4,4,8,8,\dots)$ i.e., $a_n = 2^{\lfloor n/2 \rfloor}$ $\quad \dfrac{1+x}{1-2x^2}$

$(1,2,4,8,\dots)$ $\quad \dfrac{1}{1-2x}$

$(1,0,2,0,4,0,8,\dots)$ $\quad \dfrac{1}{1-2x^2}$

$(0,1,0,2,0,4,0,8,\dots)$ $\quad \dfrac{x}{1-2x^2}$

12

求导

$(a_0, a_1, a_2, \dots)$ $\quad a(x) = a_0 + a_1x + a_2x^2 + \cdots$

$(a_1, 2a_2, 3a_3, \dots)$ $\quad a'(x)$

Example:

$(1^2, 2^2, 3^2, 4^2, \dots)$ i.e., $a_k = (k+1)^2$ $\quad \dfrac{2}{(1-x)^3} - \dfrac{1}{(1-x)^2}$

$(1,1,1,1,\dots)$ $\quad \dfrac{1}{1-x}$

$(1,2,3,4,\dots, \underline{k+1}, \dots)$ $\quad \left(\dfrac{1}{1-x}\right)' = \dfrac{1}{(1-x)^2}$

$(2\cdot 1, 3\cdot 2, 4\cdot 3, \dots, \underline{(k+1)^2 + k + 1}, \dots$ $\quad \left(\dfrac{1}{1-x}\right)'' = \dfrac{2}{(1-x)^3}$

积分

$(a_0, a_1, a_2, \dots)$ $\quad a(x) = a_0 + a_1x + a_2x^2 + \cdots$

$(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \dots)$ $\quad \int_0^x a(t)dt$

卷积

$(a_0, a_1, a_2, \dots)$ $\qquad a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$

$(b_0, b_1, b_2, \dots)$ $\qquad b(x) = b_0 + b_1 x + b_2 x^2 + \cdots$

$(c_0, c_1, c_2, \dots)$ $\qquad \boxed{a(x) \cdot b(x)}$

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$
$$\vdots$$
$$c_k = \sum_{i,j \geq 0; i+j=k} a_i b_j$$

16

解生成函数

- Recurrence relation
  Define g_i recursively.
- Manipulation:
  New equivalence concerning $G(x)$.
- Solving
  Closed form for $G(x)$.
- Expanding
  New form for g_i.

TABLE 1 Useful Generating Functions.	
$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k = 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k)$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^k x^k = 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	$C(n,k)a^k$
$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk} = 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	$C(n,k/r)$ if $r \mid k$; 0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if $k \le n$; 0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2x^2 + \cdots$	a^k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if $r \mid k$; 0 otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k = 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k) = C(n+k-1,n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k = 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n+k-1,k) = (-1)^k C(n+k-1,n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^k x^k = 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)a^k = C(n+k-1,n-1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$1/k!$
$\ln(1+x) = \sum_{k=0}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k$

1、等差数列的前 n 项和公式

$$S_n = \frac{n(a_1 + a_n)}{2} = na_1 + \frac{n(n-1)d}{2}$$

2、等比数列的前 n 项和公式

$$S_n = \begin{cases} na_1 (q = 1) \\ \frac{a_1(1-q^n)}{1-q} = \frac{a_1 - a_n q}{1-q} (q \neq 1) \end{cases}$$

3、常用几个数列的求和公式

(1)、$S_n = \sum_{k=1}^{n} k = 1 + 2 + 3 + \ldots + n = \frac{1}{2} n(n+1)$

(2)、$S_n = \sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{1}{6} n(n+1)(2n+1)$

(3)、$S_n = \sum_{k=1}^{n} k^3 = 1^3 + 2^3 + 3^3 + \ldots + n^3 = [\frac{1}{2} n(n+1)]^2$

应用

- A box contains 30 red, 40 blue, and 50 green balls; balls of the same color are indistinguishable. How many ways are there of selecting a collection of 70 balls from the box?
- Solution:

$$(1 + x + x^2 + \cdots + x^{30}) \cdot (1 + x + x^2 + \cdots + x^{40}) \cdot (1 + x + x^2 + \cdots + x^{50})$$

$$= \left(\frac{1 - x^{31}}{1 - x}\right) \cdot \left(\frac{1 - x^{41}}{1 - x}\right) \cdot \left(\frac{1 - x^{51}}{1 - x}\right)$$

$$= \frac{1}{(1 - x)^3} (1 - x^{31})(1 - x^{41})(1 - x^{51})$$

$$(1+x+x^2+\cdots+x^{30})\cdot(1+x+x^2+\cdots+x^{40})$$
$$\cdot(1+x+x^2+\cdots+x^{50})$$
$$=\frac{1}{(1-x)^3}(1-x^{31})(1-x^{41})(1-x^{51})$$

$G(x)$

x^{70}

$$\frac{1}{(1-x)^n}=\binom{n-1}{n-1}+\binom{n}{n-1}x+\binom{n+1}{n-1}x^2+\cdots\binom{n+k-1}{n-1}x^k+\cdots$$

$$=\left(\binom{2}{2}+\binom{3}{2}x+\binom{4}{2}x^2+\cdots\right)(1-x^{31}-x^{41}-x^{51}+\cdots)$$

x^{70} 39 x^{29} x^{19}

Thus the coefficient of x^{70} is:

$$=\binom{70+2}{2}-\binom{70+2-31}{2}-\binom{70+2-41}{2}-\binom{70+2-51}{2}$$
$$=1061$$

斐波那契

f_i

Fibonacci Sequence

$G(x)$ (2)

- $f_n=f_{n-1}+f_{n-2}$
- $F(x)=f_0+f_1x+f_2x^2+\cdots+f_{n-2}x^{n-2}+f_{n-1}x^{n-1}+f_nx^n+\cdots$
- $xF(x)=\quad f_0x+f_1x^2+f_2x^3+\cdots\cdots\cdots+f_{n-2}x^{n-1}+f_{n-1}x^n+\cdots$
- $x^2F(x)=\quad f_0x^2+f_1x^3+f_2x^4+\cdots\cdots\cdots\cdots+f_{n-2}x^n+f_{n-1}x^{n+1}+\cdots$

$$F(x)-xF(x)-x^2F(x)=f_0+(f_1-f_0)x$$

$$F(x)=\frac{x}{1-x-x^2}$$
$$=\frac{a}{1-\lambda_1x}+\frac{b}{1-\lambda_2x}=\frac{1}{\sqrt5}\left(\frac{1}{1-\frac{1+\sqrt5}{2}x}-\frac{1}{1-\frac{1-\sqrt5}{2}x}\right)$$

$n.$

$$f_n=\frac{1}{\sqrt5}\left[\left(\frac{1+\sqrt5}{2}\right)^n-\left(\frac{1-\sqrt5}{2}\right)^n\right]$$

$$\frac{1}{1-x}=1+x+x^2+\cdots+x^n+\cdots \quad (-1<x<1)$$

$$G(x)=\frac{1}{\sqrt{5}}\cdot\frac{1+\sqrt{5}}{2}\cdot[1+\frac{1+\sqrt{5}}{2}x+(\frac{1+\sqrt{5}}{2})^2x^2+\cdots+(\frac{1+\sqrt{5}}{2})^nx^n+\cdots]$$

$$-\frac{1}{\sqrt{5}}\cdot\frac{1-\sqrt{5}}{2}\cdot[1+\frac{1-\sqrt{5}}{2}x+(\frac{1-\sqrt{5}}{2})^2x^2+\cdots+(\frac{1-\sqrt{5}}{2})^nx^n+\cdots]$$

$$G(x)=F_0+F_1x+F_2x^2+\cdots+F_nx^n+\cdots$$

$$F_n=\frac{1}{\sqrt{5}}[(\frac{\sqrt{5}+1}{2})^{n+1}-(\frac{1-\sqrt{5}}{2})^{n+1}]$$

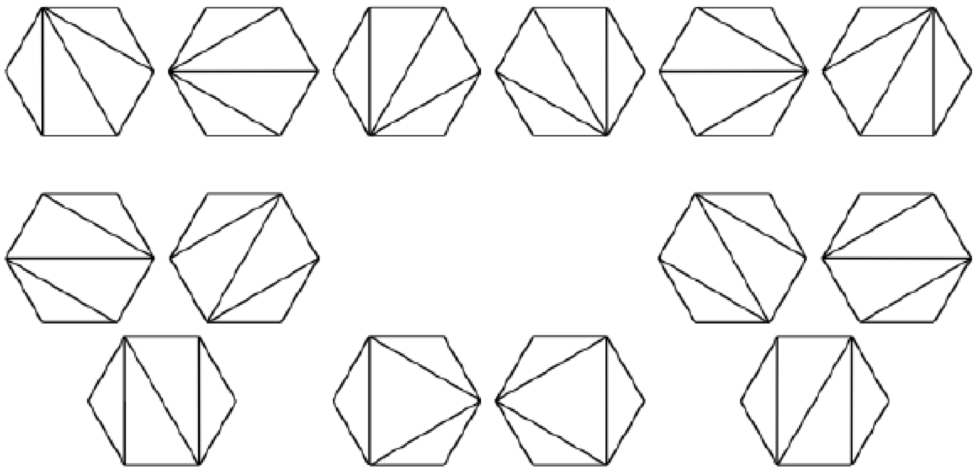
三角划分

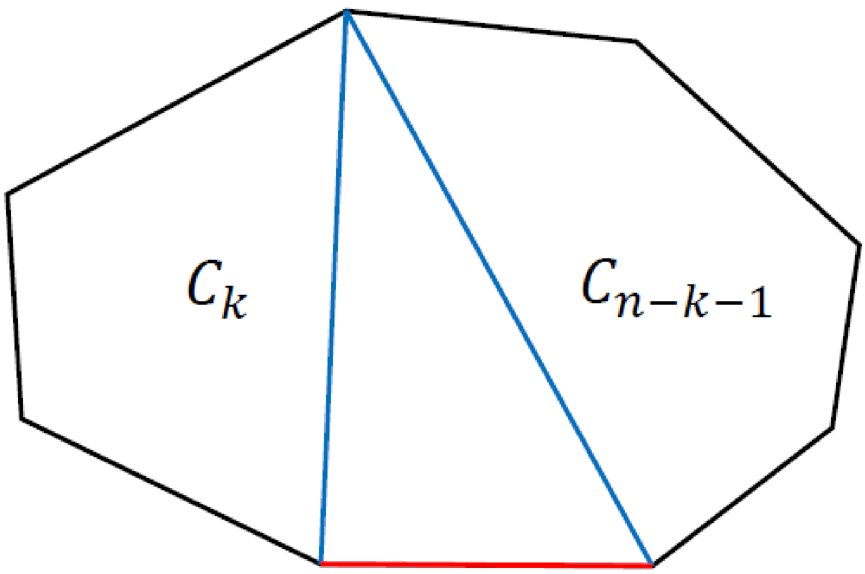
卡塔兰数

Catalan Number

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

Number of different ways a convex polygon with $n + 2$ sides can be cut into triangles by connecting vertices with straight lines (a form of Polygon triangulation).





$$C_0 = 1,\ C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1}$$

写出生成函数并化简

$$G(x) = \sum_{n\geq 0} C_n x^n = C_0 + C_1 x + C_2 x^2 + C_3 x^3 + \cdots$$

$$\left(G(x)\right)^2 = \sum_{n\geq 0} \sum_{k=0}^{n} C_k C_{n-k} x^n$$

$$x\left(G(x)\right)^2 = \sum_{n\geq 0} \sum_{k=0}^{n} C_k C_{n-k} x^{n+1}$$

$$= \sum_{n\geq 1} \sum_{k=0}^{n-1} C_k C_{n-k-1} x^n$$

$$G(x) = \sum_{n\geq 0} C_n x^n = C_0 + \sum_{n\geq 1} \sum_{k=0}^{n-1} C_k C_{n-k-1} x^n$$

$$= 1 + x\left(G(x)\right)^2$$

$$G(x) = 1 + x\left(G(x)\right)^2 \qquad \Rightarrow \qquad G(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

$$\lim_{x\to 0} G(0) = C_0 = 1 \qquad \Rightarrow \qquad G(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

$$\sqrt{1-4x} = \sum_{n\geq 0}^{\infty} \binom{1/2}{n} (-4x)^n = 1 + \sum_{n\geq 1}^{\infty} \binom{1/2}{n} (-4x)^n$$

$$= 1 + \sum_{n\geq 0}^{\infty} \binom{1/2}{n+1} (-4x)^{n+1} = 1 - 4x \sum_{n\geq 0}^{\infty} \binom{1/2}{n+1} (-4x)^n$$

$$G(x) = \frac{4x \sum_{n\geq 0}^{\infty} \binom{1/2}{n+1} (-4x)^n}{2x} = 2 \sum_{n\geq 0}^{\infty} \binom{1/2}{n+1} (-4x)^n$$

$$
\begin{aligned}
C_n = 2\binom{1/2}{n+1}(-4)^n &= 2\,\frac{(\frac{1}{2})(\frac{1}{2}-1)\cdots(\frac{1}{2}-n)}{(n+1)!}(-4)^n \\
&= \frac{2^n}{(n+1)!}\prod_{k=1}^{n}(2k-1) \quad = \frac{2^n}{(n+1)!}\prod_{k=1}^{n}\frac{(2k-1)2k}{2k} \\
&= \frac{1}{n!\,(n+1)!}\prod_{k=1}^{n}(2k-1)2k \\
&= \frac{(2n)!}{n!\,(n+1)!} \quad = \frac{1}{n+1}\binom{2n}{n}
\end{aligned}
$$

29

卡塔兰数其他应用

Number of expressions containing n pairs of parentheses which are correctly matched.

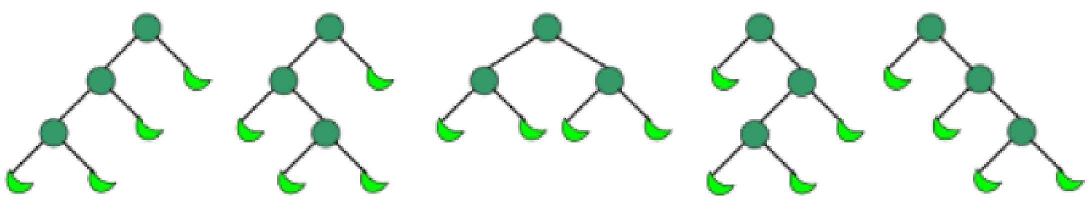
((()))　　()(())　　()()()　　(())()　　(()())

证明：令1表示进栈，0表示出栈，则可转化为求一个*2n*位、含*n*个1、*n*个0的二进制数，满足从左往右扫描到任意一位时，经过的0数不多于1数。显然含*n*个1、*n*个0的*2n*位二进制数共有$\binom{2n}{n}$个，下面考虑不满足要求的数目。

考虑一个含*n*个1、*n*个0的2n位二进制数，扫描到第*2m+1*位上时有*m+1*个0和*m*个1（容易证明一定存在这样的情况），则后面的0-1排列中必有*n-m*个1和*n-m-1*个0。将*2m+2*及其以后的部分0变成1、1变成0，则对应一个*n+1*个0和*n-1*个1的二进制数。反之亦然（相似的思路证明两者一一对应）。

从而$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$。证毕。

Number of full binary trees with $n + 1$ leaves

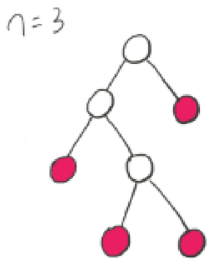


2.3 二叉树

题目描述

`n + 1` 个叶子节点能够构成多少种形状不同的（国际）满二叉树

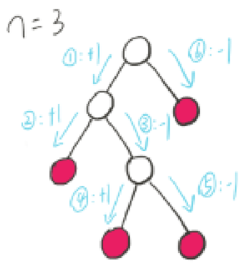
（国际）满二叉树定义：如果一棵二叉树的结点要么是叶子结点，要么它有两个子结点，这样的树就是满二叉树。



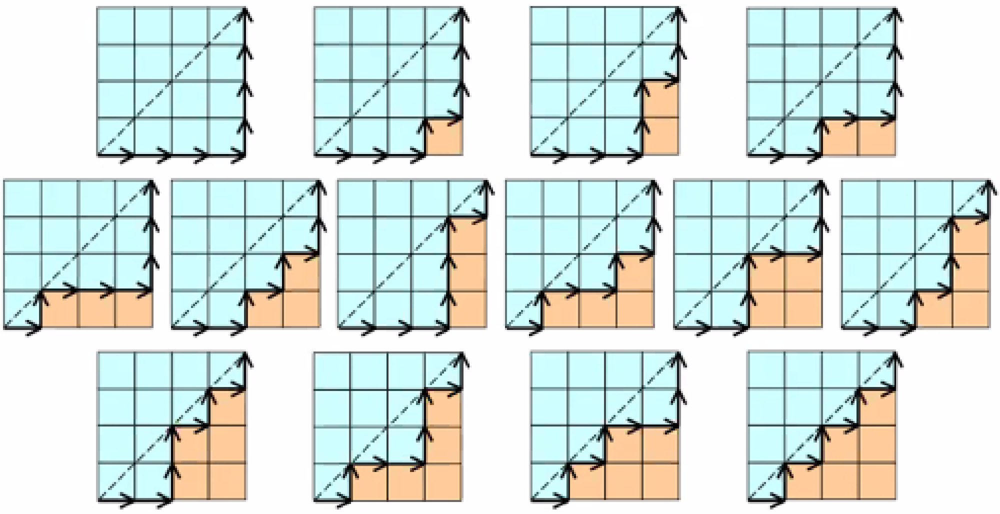
思路

使用深度优先搜索这个满二叉树，向左扩展时标记为 +1，向右扩展时标记为 -1。

由于每个非叶子节点都有两个左右子节点，所有它必然会先向左扩展，再向右扩展。总体下来，左右扩展将会形成匹配，即变成进出栈的题型。`n + 1` 个叶子结点会有 2n 次扩展，构成 $\frac{C_{2n}^{n}}{n+1}$ 种形状不同的满二叉树。



Number of monotonic lattice paths along the edges of a grid with $n \times n$ square cells, which do not pass above the diagonal.



Ch 03 Recurrence relation

齐次

第n个值依赖于前n-1个值，bias=0

Homogeneous linear recurrence of k^{th} degree with constant coefficients

$$h_n = a_{k-1}h_{n-1} + a_{k-2}h_{n-2} + \cdots + a_1 h_{n-k-1} + a_0 h_{n-k}$$

特征方程

Characteristic polynomial of the above recurrence

$$p(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0 = 0$$

$$x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0 = 0 \quad (☆)$$

$$\Rightarrow (x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_k) = 0$$

$$x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0 = 0 \quad (\star)$$

$$(x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_k) = 0$$

- If $\lambda_i \neq \lambda_j$ whenever $i \neq j$

  Then $h_n = c_1\lambda_1^n + c_2\lambda_2^n + \cdots + c_k\lambda_k^n$

- If $p(x) = (x-\lambda_1)^{s_1}(x-\lambda_2)^{s_2}\cdots(x-\lambda_q)^{s_q}$

  Then $h_n = (c_{11}+c_{12}n+\cdots+c_{1s_1}n^{s_1-1})\lambda_1^n$

  $+(c_{21}+c_{22}n+\cdots+c_{2s_2}n^{s_2-1})\lambda_2^n$

  $\vdots$

  $+(c_{q1}+c_{q2}n+\cdots+c_{qs_q}n^{s_q-1})\lambda_q^n$

6

例子

斐波那契

- $f_n = f_{n-1} + f_{n-2} \quad (n \geq 2)$

  $f_0 = 0, f_1 = 1, f_2 = 1$
- $x^2 - x - 1 = 0 \quad (\star)$
- $x = \frac{1\pm\sqrt{5}}{2}$ $\lambda_1 \neq \lambda_2$
- $f_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$
- $f_0 = 0 \Rightarrow a + b = 0 \Rightarrow a = -b$

  $$f_1 = 1 \Rightarrow a\left(\frac{1+\sqrt{5}}{2}\right) + b\left(\frac{1-\sqrt{5}}{2}\right) = 1 \Rightarrow a = \frac{1}{\sqrt{5}}$$
- $f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$

7

例子二

- $h_n = -h_{n-1} + 3h_{n-2} + 5h_{n-3} + 2h_{n-4} \quad (n \geq 4)$
  $h_0 = 1, h_1 = 0, h_2 = 1, h_3 = 2$
- $x^4 + x^3 - 3x^2 - 5x - 2 = 0 \quad (☆)$
- $x = -1, -1, -1, 2$
- $h_n = c_1(-1)^n + c_2 n(-1)^n + c_3 n^2(-1)^n + c_4 2^n$
- $$\begin{cases} (n=0) & c_1 + c_4 = 1 \\ (n=1) & -c_1 - c_2 - c_3 + 2c_4 = 0 \\ (n=2) & c_1 + 2c_2 + 4c_3 + 4c_4 = 1 \\ (n=3) & -c_1 - 3c_2 - 9c_3 + 8c_4 = 2 \end{cases}$$
- $c_1 = \frac{7}{9},\ c_2 = -\frac{3}{9},\ c_3 = 0,\ c_4 = \frac{2}{9}$
- $h_n = \frac{7}{9}(-1)^n - \frac{3}{9}n(-1)^n + \frac{2}{9}2^n$

$h_n = (\quad)\lambda_i^n + c_j\lambda_2^n$

非齐次

汉诺塔问题

$$h_0 = 0$$
$$h_1 = 1$$
$$h_2 = 3$$
$$\vdots$$
$$h_n = 2h_{n-1} + 1$$

$$\begin{aligned} h_n &= 2h_{n-1} + 1 \\ &= 2(2h_{n-2}+1) + 1 = 2^2 h_{n-2} + 2 + 1 \\ &= 2^2(2h_{n-3}+1) + 2 + 1 = 2^3 h_{n-3} + 2^2 + 2 + 1 \\ &\ \vdots \\ &= 2^{n-1}(h_0 + 1) + 2^{n-2} + \cdots + 2^2 + 2 + 1 \\ &= 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1 \\ &= 2^n - 1 \end{aligned}$$

非齐次问题

Non-homogeneous linear recurrence of k^{th} degree with constant coefficients

$$h_n = a_{k-1}h_{n-1} + a_{k-2}h_{n-2} + \cdots + a_0 h_{n-k} + b_n$$

Every solution to nonhomogeneous equation is of the form:

Some specific solution + Solution to homogeneous.

原始问题解=齐次方程解+特解

猜测特解经验

- If b_n is of n's k –degree polynomial, then the specific solution is more likely to be n's k –degree polynomial as well.
  - If $b_n = c$ try $h_n = r$
  - If $b_n = dn + c$ try $h_n = rn + s$
  - If $b_n = rn^2 + sn + t$ try $h_n = fn^2 + dn + c$
- If b_n is of n's exponential form, then the specific solution is more likely to be n's exponential form as well.
  - If $b_n = d^n$ try $h_n = pd^n$

16

例子

例子一

- $h_n = 3h_{n-1} - 4n \quad (n \geq 1)$ with $h_0 = 2$
- Homogeneous part: $h_n = 3h_{n-1}, \quad x - 3 = 0 \quad (☆)$
- $h_n = c3^n \quad (n \geq 1)$
- Find one specific solution for $h_n = 3h_{n-1} - 4n \quad (n \geq 1)$
  - Try $h_n = rn + s$
  - $rn + s = 3(r(n-1) + s) - 4n$ ① ②
  - $rn + s = (3r - 4)n + (-3r + 3s)$
    $\Rightarrow r = 2, s = 3 \Rightarrow h_n = 2n + 3$ √
- $h_n = c3^n + 2n + 3$
- $(n = 0) \quad 2 = c \times 3^0 + 2 \times 0 + 3 \Rightarrow c = -1$
- $h_n = -3^n + 2n + 3 \qquad (n \geq 0)$

例子二

猜测错误

- $h_n = 3h_{n-1} + 3^n \quad (n \geq 1)$ with $h_0 = 2$
- Homogeneous part: $h_n = c3^n$ $\Leftarrow$ $x-3=0$
- Find one specific solution for $h_n = 3h_{n-1} + 3^n \,(n \geq 1)$
  - Try $h_n = p3^n$ X
  - $p3^n = 3p3^{n-1} + 3^n \Rightarrow p = p + 1 \Rightarrow$ Impossible!

继续猜测

- Try $h_n = pn3^n$
- $pn3^n = 3p(n-1)3^{n-1} + 3^n \Rightarrow p = 1 \Rightarrow h_n = n3^n$ √

- $h_n = c3^n + n3^n$
- $(n = 0) \quad c(3^0) + 0(3^0) = 2 \Rightarrow c = 2$
- $h_n = 2 \times 3^n + n3^n = (2 + n)3^n \qquad (n \geq 0)$

解决非线性问题->通过将其转换为线性

Polya's Theory of Counting

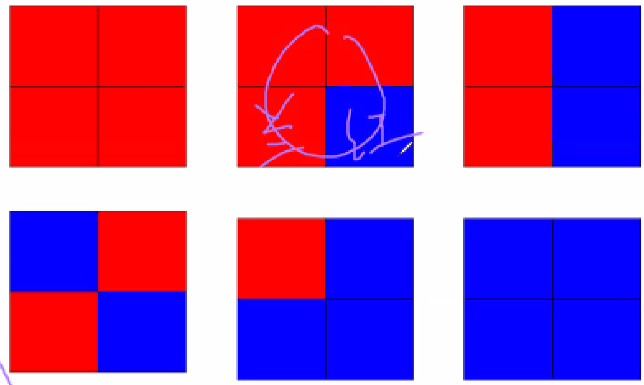
例子

Now consider an $n \times n$ "chessboard" where $n \geq 2$. Here we color the squares Red and Blue and two colorings are different only if one cannot be obtained from another by a rotation or a reflection. For $n = 2$ there are 6 colorings.

2^{n^2}

$n = 2$

2^4



6

① $90^\circ \times n$

② 左右

上下

③

是封闭的，如何做都会反映为集合中一种

In addition there is a set G of permutations of X. This set will have a group structure:

Given two members $g_1, g_2 \in G$ we can define their composition $g_1 \circ g_2$ by $g_1 \circ g_2(x) = g_1(g_2(x))$ for $x \in X$. We require that G is *closed* under composiiton i.e. $g_1 \circ g_2 \in G$ if $g_1, g_2 \in G$.

群

满足A1\A2\A3三个性质

We also have the following:

$x \in X$

A1 The *identity* permutation $1_X \in G$.

$1_x(x) = x$

A2 $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ (Composition is associative).

A3 The inverse permutation $g^{-1} \in G$ for every $g \in G$.

$e_0 = 0$ $\quad e_0^{-1} = e_0$

$g \longrightarrow g^{-1}$ $\quad g \circ g^{-1} = 1_x$

(A set G with a binary relation $\circ$ which satisfies **A1,A2,A3** is called a **Group**).

$e_1 = 90^\circ$

$e_1^{-1} = 270^\circ$

orbit

从X出发能够到达的所有着色

Orbits: If $x \in X$ then its orbit
$O_x = \{y \in X : \exists g \in G \text{ such that } g * x = y\}$.

两个orbit无交集

Lemma 1 The orbits partition X.
Proof $x = 1_X * x$ and so $x \in O_x$ and so $X = \bigcup_{x \in X} O_x$.

Suppose now that $O_x \cap O_y \neq \emptyset$ i.e. $\exists g_1, g_2$ such that $g_1 * x = g_2 * y$. But then for any $g \in G$ we have

$$g * x = (g \circ (g_1^{-1} \circ g_2)) * y \in O_y$$

and so $O_x \subseteq O_y$. Similarly $O_y \subseteq O_x$. Thus $O_x = O_y$ whenever $O_x \cap O_y \neq \emptyset$. □

两个概念

The two problems we started with are of the following form: Given a set X and a group of permutations *acting* on X, compute the number of orbits i.e. distinct colorings.

A subset H of G is called a *sub-group* of G if it satisfies *axioms* **A1,A2,A3** (with G replaced by H).

The *stabilizer* S_x of the element x is $\{g : g * x = x\}$. It is a sub-group of G.

- A1: $1_X * x = x$.
- A3: $g, h \in S_x$ implies $(g \circ h) * x = g * (h * x) = g * x = x$.

A2 holds for any subset.

证明

Lemma 2
If $x \in X$ then $|O_x||S_x| = |G|$.
Proof Fix $x \in X$ and define an equivalence relation $\sim$ on G by

$$g_1 \sim g_2 \text{ if } g_1 * x = g_2 * x.$$

Let the equivalence classes be $A_1, A_2, \ldots, A_m$. We first argue that

$$|A_i| = |S_x| \qquad i = 1, 2, \ldots, m. \tag{1}$$

Fix i and $g \in A_i$. Then

$$\begin{aligned} h \in A_i \leftrightarrow g * x = h * x \leftrightarrow (g^{-1} \circ h) * x = x \\ \leftrightarrow (g^{-1} \circ h) \in S_x \leftrightarrow h \in g \circ S_x \end{aligned}$$

where $g \circ S_x = \{g \circ \sigma : \ \sigma \in S_x\}$.

Thus $|A_i| = |g \circ S_x|$. But $|g \circ S_x| = |S_x|$ since if $\sigma_1, \sigma_2 \in S_x$ and $g \circ \sigma_1 = g \circ \sigma_2$ then

$$g^{-1} \circ (g \circ \sigma_1) = (g^{-1} \circ g) \circ \sigma_1 = \sigma_1 = g^{-1} \circ (g \circ \sigma_2) = \sigma_2.$$

This proves (1).

Finally, $m = |O_x|$ since there is a distinct equivalence class for each distinct $g * x$. $\square$

Let $\nu_{X,G}$ denote the number of orbits.
Theorem 1

$$\nu_{X,G} = \frac{1}{|G|} \sum_{x \in X} |S_x|.$$

Proof

$$\begin{aligned} \nu_{X,G} &= \sum_{x \in X} \frac{1}{|O_x|} \\ &= \sum_{x \in X} \frac{|S_x|}{|G|}, \end{aligned}$$

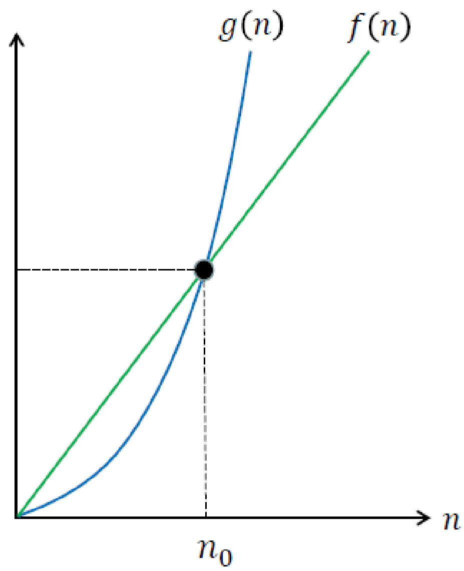
from Lemma 1. $\square$

Ch 04 O 函数的渐进比较

定义：f,g：$N \to R$ 是两个从自然数到实数的单变量方程

$$f(n) = O(g(n))$$

表示存在常数n_0和C，使得对所有$n \geq n_0$，不等式$|f(n)| \leq C \cdot g(n)$ 成立。



直观：f的增长不比g快很多。即：$\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} \nrightarrow \infty$

4

符号	定义	含义
$f(n) = O(g(n))$	$\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} \nrightarrow \infty$	f的增长不比g快很多
$f(n) = o(g(n))$	$\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} = 0$	f的增长远远慢于g
$f(n) = \Omega(g(n))$	$g(n) = O(f(n))$	f的增长至少和g一样快
$f(n) = \Theta(g(n))$	$f(n) = O(g(n))$且 $f(n) = \Omega(g(n))$	f和g几乎是同一数量级
$f(n) \sim g(n)$	$\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} = 1$	$f(n)$和$g(n)$几乎是一样的

调和级数的估值

分段

- 估计调和级数的值：用数列对调和级数的加项做分类。
- $1,\quad \frac{1}{2}, \frac{1}{3},\quad \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7},\quad \frac{1}{8}, \frac{1}{9}, \cdots, \frac{1}{15},\quad \frac{1}{16}, \frac{1}{17}, \cdots$

$$\underbrace{\left(\frac{1}{2^1}, \frac{1}{2^0}\right]}_{G_1} \quad \underbrace{\left(\frac{1}{2^2}, \frac{1}{2^1}\right]}_{G_2} \quad \underbrace{\left(\frac{1}{2^3}, \frac{1}{2^2}\right]}_{G_3} \quad \underbrace{\left(\frac{1}{2^4}, \frac{1}{2^3}\right]}_{G_4} \quad \underbrace{\left(\frac{1}{2^5}, \frac{1}{2^4}\right]}_{G_5}$$

$$\begin{aligned} G_k &= \left\{\frac{1}{i} \,\middle|\, \frac{1}{2^k} < \frac{1}{i} \le \frac{1}{2^{k-1}}\right\} \\ &= \left\{\frac{1}{2^k-1}, \frac{1}{2^k-2}, \frac{1}{2^k-3}, \cdots, \frac{1}{2^{k-1}}\right\} \end{aligned}$$

进行放缩

$$\underbrace{1,}_{G_1} \quad \underbrace{\frac{1}{2}, \frac{1}{3},}_{G_2} \quad \underbrace{\frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7},}_{G_3} \quad \underbrace{\frac{1}{8}, \frac{1}{9}, \cdots, \frac{1}{15},}_{G_4} \cdots$$

$$\begin{aligned} G_k &= \left\{\frac{1}{i} \,\middle|\, \frac{1}{2^k} < \frac{1}{i} \le \frac{1}{2^{k-1}}\right\} \\ &= \left\{\frac{1}{2^k-1}, \frac{1}{2^k-2}, \frac{1}{2^k-3}, \cdots, \frac{1}{2^{k-1}}\right\} \\ &= \left\{\frac{1}{2^{k-1}}, \frac{1}{2^{k-1}+1}, \frac{1}{2^{k-1}+2}, \cdots, \frac{1}{2^k-1}\right\} \end{aligned}$$

$|G_k| = 2^{k-1}$

每一个G_k中的调和级数加项和：

$$\sum_{x \in G_k} x \le |G_k| \max G_k$$
$$= 2^{k-1} \cdot \frac{1}{2^{k-1}}$$
$$= 1$$
$$\sum_{x \in G_k} x \ge |G_k| \min G_k$$
$$> 2^{k-1} \cdot \frac{1}{2^k}$$
$$= \frac{1}{2}$$

$$H_n = \underbrace{1}_{G_1} + \underbrace{\frac{1}{2} + \frac{1}{3}}_{G_2} + \frac{1}{4} + \cdots + \underbrace{\frac{1}{n-2} + \frac{1}{n-1} + \frac{1}{n}}_{G_t}$$

$$G_k = \left\{ \frac{1}{i} \,\middle|\, \frac{1}{2^k} < \frac{1}{i} \le \frac{1}{2^{k-1}} \right\}$$

$$\frac{1}{2} < \sum_{x \in G_k} x \le 1$$

$$2^{k-1} \le i < 2^k$$

$$k = \lfloor \log_2 i \rfloor + 1 \quad \text{故} \quad t = \lfloor \log_2 n \rfloor + 1$$

$$H_n \le t \cdot 1 \le \log_2 n + 1$$

$$H_n > (t-1) \cdot \frac{1}{2} \ge \frac{1}{2} \lfloor \log_2 n \rfloor$$

得到结果

$$H_n = \Theta(\log_2 n) = \Theta(\ln n)$$

Ch 04 阶乘估值、二项式系数估值

阶乘估值

粗糙估计

$$n! = \prod_{i=1}^{n} i \le \prod_{i=1}^{n} n = n^n$$

$$n! = \prod_{i=2}^{n} i \ge \prod_{i=2}^{n} 2 = 2^{n-1}$$

进行改进：降低上界/提高下界

改进1

上界拆为两半估计/下界舍弃前半段

$$n! = \prod_{i=1}^{n} i \le \left(\prod_{i=1}^{n/2} \frac{n}{2}\right)\left(\prod_{i=n/2+1}^{n} n\right) = \left(\frac{n}{\sqrt{2}}\right)^n \quad \boxed{< n^n}$$

$$n! = \prod_{i=1}^{n} i \ge \prod_{i=n/2+1}^{n} i > \prod_{i=n/2+1}^{n} \frac{n}{2} = \left(\frac{n}{2}\right)^{n/2} = \left(\sqrt{\frac{n}{2}}\right)^n \quad \boxed{> 2^n}$$

$F = \{f \mid f:\{1,2,\cdots n\} \to \{1,2,\cdots,n\}\}$ 中任取一个函数g，g是单射函数的概率是多少?

$$\frac{n!}{n^n} \le \frac{\left(\frac{n}{\sqrt{2}}\right)^n}{n^n} = 2^{-n/2}$$

4

高斯估值

上界改进

$$\left(\sqrt{\frac{n}{2}}\right)^n \le n! \le \left(\frac{n}{\sqrt{2}}\right)^n$$

$$\Uparrow$$

算数-几何均值不等式(Arithmetic-geometric mean inequality)：对任意实数x, y，必有：

$$\sqrt{xy} \le \frac{x+y}{2}$$

$$n! = 1 \cdot 2 \cdot \cdots k \cdots \cdot n$$
$$n! = n \cdot (n-1) \cdot \cdots (n+1-k) \cdots \cdot 1$$
$$n! = \sqrt{n! \cdot n!} = \sqrt{\prod_{i=1}^{n} i(n+1-i)}$$
$$= \prod_{i=1}^{n} \sqrt{i(n+1-i)} \le \prod_{i=1}^{n} \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n$$

下界改进

$$\left(\sqrt{\frac{n}{2}}\right)^n \le n! \le \left(\frac{n+1}{2}\right)^n$$

$$i(n+1-i) \ge n$$
$$i = 1, 2, \dots, n.$$

$$\Uparrow$$

$$n! = 1 \cdot 2 \cdot \cdots k \cdots \cdot n$$
$$n! = n \cdot (n-1) \cdot \cdots (n+1-k) \cdots \cdot 1$$
$$n! = \sqrt{n! \cdot n!} = \sqrt{\prod_{i=1}^{n} i(n+1-i)}$$
$$= \prod_{i=1}^{n} \sqrt{i(n+1-i)}$$
$$\ge \prod_{i=1}^{n} \sqrt{n} = n^{n/2}$$

进一步优化

$1 + x \le e^x$

上界

$$e\left(\frac{n}{e}\right)^n \le \boxed{n! \le en\left(\frac{n}{e}\right)^n}$$

$$1 + x \le e^x$$

证明：上界（归纳法）

- $n = 1$：$1 \ge 1!$；
- 设 $n = k$ 时结论成立；
- $n = k + 1$：

$$n! = n \cdot (n-1)! \le n \cdot e(n-1)\left(\frac{n-1}{e}\right)^{n-1}$$

$$= en\left(\frac{n}{e}\right)^n \cdot e \cdot \left(\frac{n-1}{n}\right)^n$$

而 $e \cdot \left(\frac{n-1}{n}\right)^n = e \cdot \left(1 - \frac{1}{n}\right)^n \le e \cdot \left(e^{-1/n}\right)^n = e \cdot e^{-1} = 1$

下界

$$\boxed{e\left(\frac{n}{e}\right)^n \le n!} \le en\left(\frac{n}{e}\right)^n$$

$$1 + x \le e^x$$

证明：下界（归纳法）

- $n = 1$：$1 \le 1!$；
- 设 $n = k$ 时结论成立；
- $n = k + 1$：

$$n! = n \cdot (n-1)! \ge n \cdot e\left(\frac{n-1}{e}\right)^{n-1}$$

$$= e\left(\frac{n}{e}\right)^n \cdot e \cdot \left(\frac{n-1}{n}\right)^{n-1}$$

$$n! \geq e\left(\frac{n}{e}\right)^n \cdot e \cdot \left(\frac{n-1}{n}\right)^{n-1}$$

$$\text{而 } e \cdot \left(\frac{n-1}{n}\right)^{n-1} = e \cdot \left(\frac{n}{n-1}\right)^{1-n} = e \cdot \left(1+\frac{1}{n-1}\right)^{1-n}$$

$$= e \cdot \left(\left(1+\frac{1}{n-1}\right)^{n-1}\right)^{-1}$$

$$\geq e \cdot \left(\left(e^{\frac{1}{n-1}}\right)^{n-1}\right)^{-1} = e \cdot e^{-1} = 1$$

斯特林Stirling公式

渐进相等

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

$$\text{即} \quad \lim_{n\to\infty} \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{n!} = 1$$

二项式系数估值

初步估值

由定义显然 $\binom{n}{k} \le n^k$

当 $n \ge k > i \ge 0$ 时 $\dfrac{n-i}{k-i} \ge \dfrac{n}{k}$

故 $$\binom{n}{k} = \prod_{i=0}^{k-1} \frac{n-i}{k-i} \ge \left(\frac{n}{k}\right)^k$$

二项式定理估值

二项式定理(*Binomial Theorem*):
对任意非负整数n，如下等式成立：

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

对 $n \ge 1, 1 \le k \le n$

取 $0 < x < 1$

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

显然 $\binom{n}{0} + \binom{n}{1} x + \cdots + \binom{n}{k} x^k \le (1+x)^n$

故有 $\dfrac{1}{x^k}\binom{n}{0} + \dfrac{1}{x^{k-1}}\binom{n}{1} x + \cdots + \binom{n}{k} \le \dfrac{(1+x)^n}{x^k}$，且$0 < x < 1$

故有 $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \le \dfrac{(1+x)^n}{x^k}$

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k} \le \frac{(1+x)^n}{x^k}$$

取 $x=\frac{k}{n}$

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k} \le \left(1+\frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k \qquad 1+x\le e^x$$

$$\le \left(e^{k/n}\right)^n \left(\frac{n}{k}\right)^k$$

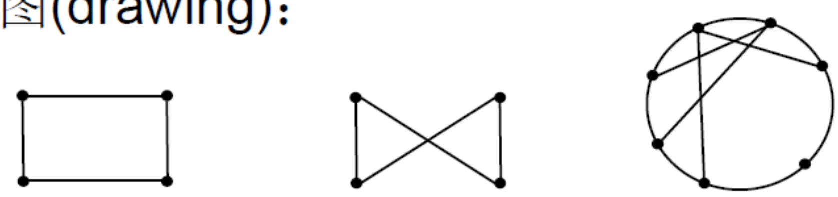
$$= \left(\frac{en}{k}\right)^k$$

$$\binom{n}{k} \le \binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k} \le \left(\frac{en}{k}\right)^k$$

Ch 05 图论 introduction

基本概念

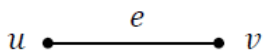
- **定义：** 图G是一个有序对(V,E)，其V中是一个集合被称为**顶点集**， E是一组由二元V元素组成的集合，称为**边集**， 既 $E\subseteq\binom{V}{2}$ Simple
- 图G，为方便常用 $V(G),E(G)$ 来分别表示“G的顶点集”和“G的边集”。
- 画图(drawing)：



G_1 G_2 G_3

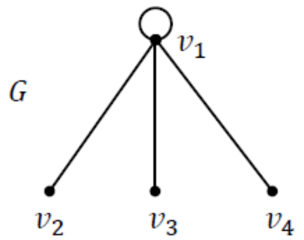
无自环和重边，$\binom{V}{2}$中元素不重复，无重边

- 阶(Order)：图顶点的个数，即$|V|$。亦常用$|G|$表示。
- 若$e=\{u,v\}\in E$，则称点u和v在图G中是相邻的(adjacent)，或称u是v的邻居(neighbor)。此时亦称e和u,v相关联(incident)。
  - 显然，一条边与且只与两个顶点相关联。



- 常用$N(u)$表示与顶点u相邻的点集。

例：



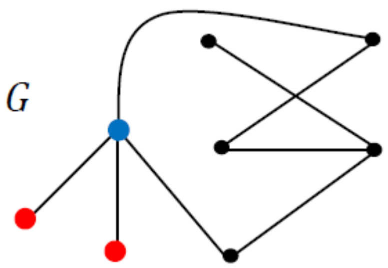
$|G|=4,\ N(v_1)=\{v_1,v_2,v_3,v_4\}$

顶点的度

- 给定图$G=(V,E)$，$v\in \mathrm{V}$，定义该顶点在图G中的度(degree)为：

$$\deg_G(v)=|u:\{u,v\}\in G|=|N(v)|$$

- 一般地，$\delta(G)$表示图G的最小度，$\Delta(G)$表示最大度。
- 显然$\deg_G(v)\le |E|$。



$\delta(G)=1$
$\Delta(G)=4$

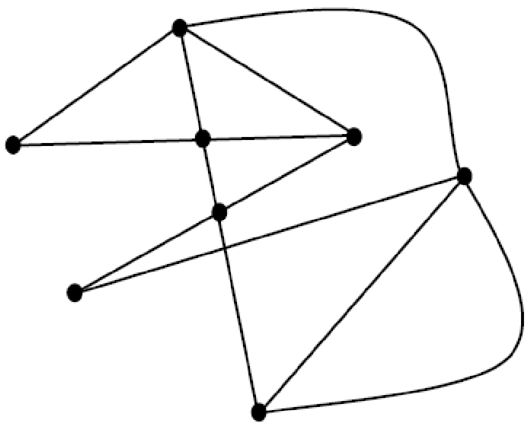
有向图和无向图

- 上面讨论的图统称为：无向图(undirected graph)。
- 如果边集E是二元*有序对*的集合，即$e \in E$都是形如$e = (u, v)$ 的形式，此时的图称为有向图(directed graph)。 u称为边e的起点，v称为边e的终点。

$$u \xrightarrow{e} v$$

- 除显示声明外，均表示无向图。

定义： 已有图G和G'，若$V(G) \subseteq V(G')$且$E(G) \subseteq E(G')$，则称G是G'的子图(subgraph) 。



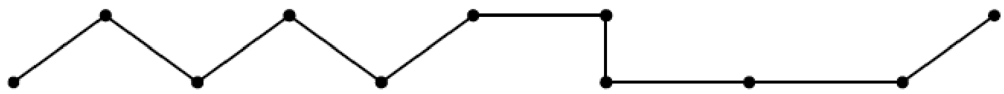
如果图H包含图G的所有顶点，则称H是G的支撑子图或生成子图。

如果图H包含了图G中所有两个端点都在V(H)中的边，则称H是G的导出子图。

图上的基本操作

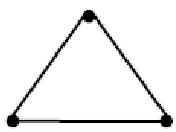
- $G \cup \{e_{ij}\}$：在G中增加边$e_{ij} = \{v_i, v_j\}$。
- $G \setminus \{e_{ij}\}$：从G中删去边$e_{ij} = \{v_i, v_j\}$。
  - 反复操作，可得到图G的任意生成子图
- $G \setminus \bar{E}$，其中$\bar{E} \subseteq E(G)$：从G中删去$\bar{E}$中的所有边。
- $G \setminus \{v\}$：从G中删去顶点v及其关联的边。
  - 反复操作，可得到图G的任意导出子图。
- $G \setminus \bar{V}$，其中$\bar{V} \subseteq V(G)$：从G中删去$\bar{V}$中的所有顶点及与这些顶点相关联的边。

- 路径图(Path P_n)
  - $V = \{0,1, \dots, n\}$,
  - $E = \{i-1, i\}: i = 1,2, \dots, n\}$.

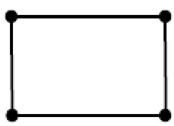


P_{11}

- 环(Cycle C_n)
  - $V = \{1,2, \dots, n\}$,
  - $E = \{i, i+1\}: i = 1,2, \dots, n-1\} \cup \{\{1, n\}\}$.



C_3

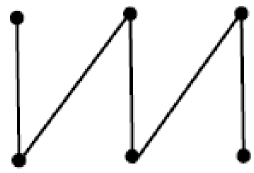


C_4

- 二分图(Bipartite graph $B_{n,m}$)
  - $V = \{u_1, \ldots, u_n\} \cup \{v_1, \ldots, v_m\}$,
  - $E \subseteq \left\{\{u_i, v_j\}: i = 1,2, \ldots, j = 1,2, \ldots, m\right\}$.

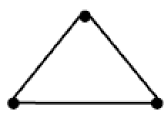
$B_{1,1}$

$B_{1,2}$

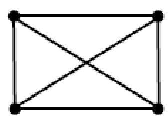


$B_{3,3}$

- 完全图(Complete graph K_n)
  - $V = \{1,2, \ldots, n\}$
  - $E = \binom{V}{2}$.



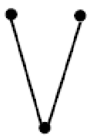
K_3



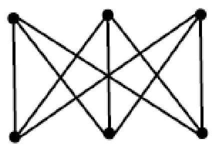
K_4

- 完全二分图(Complete bipartite graph $K_{n,m}$)
  - $V = \{u_1, \ldots, u_n\} \cup \{v_1, \ldots, v_m\}$,
  - $E = \left\{\{u_i, v_j\}: i = 1,2, \ldots, j = 1,2, \ldots, m\right\}$.

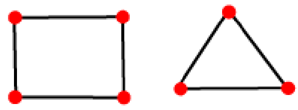
$K_{1,1}$

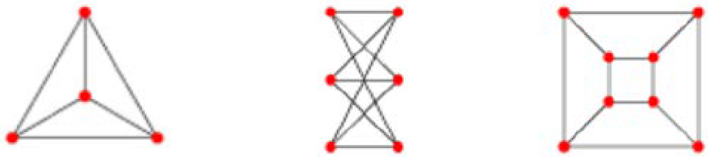


$K_{1,2}$



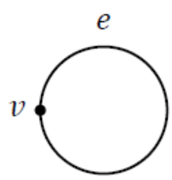
$K_{3,3}$

- 如果图中所有顶点的度数都是一个常值r，则称该图为r-正则图(r-regular graph)。
  - 0-正则图：空图 
  - 1-正则图：不相连的边（集） 
  - 2-正则图：不相交的环（集） 
  - 3-正则图：又称为立方图（cubic graph）

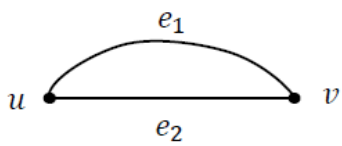


简单图

- 对无向图$G = (V, E)$
  - **自环(Loop)**：$e \in E$，如果$e = \{v, v\}$ 其中$v \in V$，则称e 是一个自环。

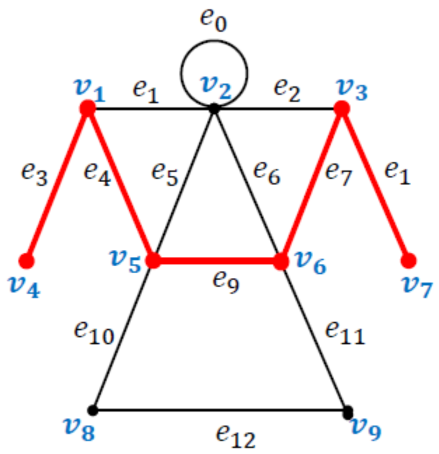


  - **重边(Multiedge)**：$e_1, e_2 \in E$ 且 $e_1 = e_2 = \{u, v\}$，其中$u, v \in V$，则称e_1, e_2是重边。



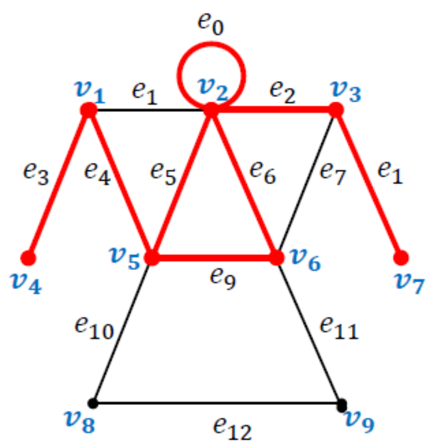
- **简单图(Simple graph)**：没有自环和重边的无向图被称为简单图。

路径与游走



- 路径(Path)：
  - 不允许环，各顶点和边至多出现一次。

$(v_4, e_3, v_1, e_4, v_5, e_9, v_6, e_7, v_3, e_1, v_7)$

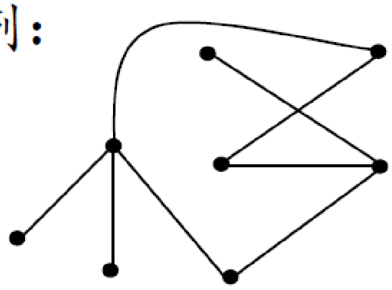


$(v_4, e_3, v_1, e_4, v_5, e_9, v_6, e_7, v_3, e_1, v_7)$

- 游走(Walk)：
  - 允许环，顶点和边可重复。

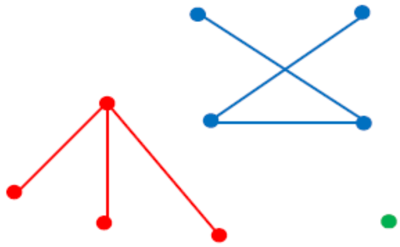
$(v_4, e_3, v_1, e_4, v_5, e_5, v_2, e_0, v_2, e_0, v_2, e_6, v_6, e_9, v_5, e_5, v_2, e_2, v_3, e_1, v_7)$

- 连通图(Connected graph): 如果图G上任意两点u, v之间都有一条路径，则称G是一个连通图。否则，称为非连通图(disconnected graph)。
- 例：



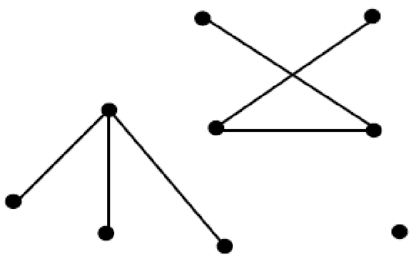
极大连通子图

- 对给定图G,定义G的**极大连通子图**：
①是原图的子图，
②是连通图，
③已经等于原图，或再扩大（增加顶点或边）则成为非连通图。



连通分支

- 连通分支(Component)：图$G=(V,E)$的极大连通子图也被称为图G的连通分支。
- 连通分支可能不唯一，图G的极大连通分支的个数用$Con(G)$表示。
- 例：

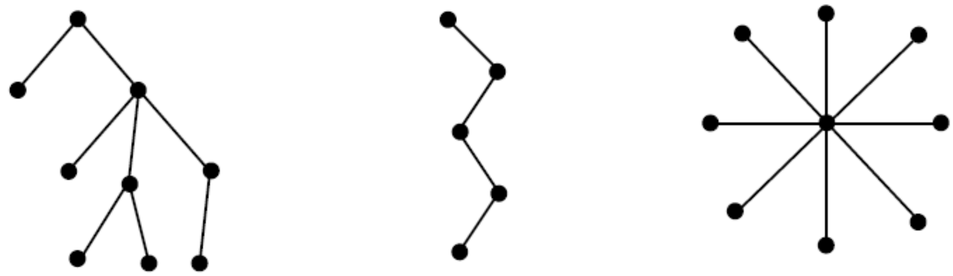


$Con(G)=3$

G

树

- 无环连通图被称为树(tree)



- 树是一类很重要的对象，在实际中有广泛应用，后面会专门讲到。
- **握手定理**(*Handshaking theorem*, Leonhard Euler 1736)：给定无向图$G = (V, E)$，以下等式成立

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

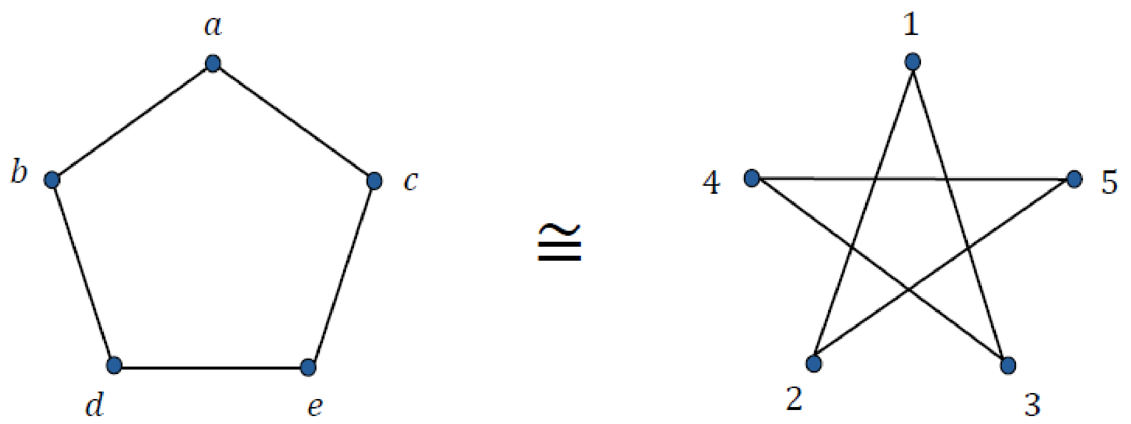
- 证明： 一条边与两个顶点相关联，在对$\deg_G(v)$做累加时，每条边被使用到两次。对边计数有类似推理。故等式成立。
- **推论**：无向图中，度数为奇数的点一定是有偶数多个。
- 证明：

Ch 05 图同构和图计数 Isomorphism and Score

图同构 graph Isomorphism

- 图同构(*Graph isomorphism*)：若对图$G = (V, E)$ 以及图$G' = (V', E')$ 存在双射函数$f: V \to V'$，满足对任意$x, y \in V$ 都有 $\{x, y\} \in E$ 当且仅当 $\{f(x), f(y)\} \in E'$ 那么我们称图G和图G'是同构的。
- 用符号图$\boldsymbol{G \cong G'}$表示图同构。
- 直观：同构的图之间，仅仅是顶点的名字不同。

例子

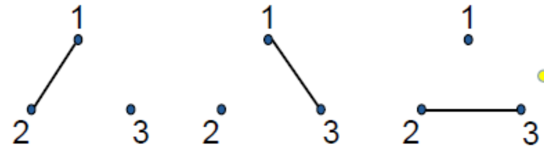


$$f:\ a \mapsto 1, b \mapsto 2, \mathrm{c} \mapsto 3, d \mapsto 5, e \mapsto 4$$

图的计数

- **问题**：以集合$V=\{1,2,\ldots,n\}$中的元素为顶点构造图，$G=(V,E)$其中$E\subseteq\binom{V}{2}$，求问能构成多少个图？
- **解**：$\left|\binom{V}{2}\right|=\binom{n}{2}$，为$K_n$的边数目。

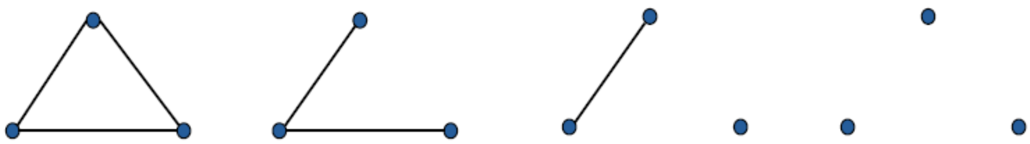
  每条边有两种可能，故以V为顶点的图共有$2^{\binom{n}{2}}$种。



非同构图的计数

上界

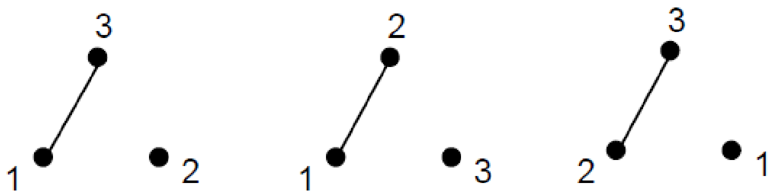
- **问题**：以集合$V=\{1,2,\ldots,n\}$中的元素为顶点构造图，$G=(V,E)$其中$E\subseteq\binom{V}{2}$，求问**彼此不同构**的图有多少个？
- 例：含三个顶点的彼此不同构的图只有以下4种：



$$4<2^{\binom{3}{2}}=8$$

下界

- 显然，（同构）图的个数不会超过所有图的个数（是$2^{\binom{n}{2}}$）。
- 与此同时，任一$G = (V, E)$至多与$n!$个V上不同的图同构。
- 例： $3! = 6$，但与第一张图同构且互不相同的图只有三种。



- **解**：设n个顶点且不同构的图有x个，则：

$$\frac{2^{\binom{n}{2}}}{n!} \le x \le 2^{\binom{n}{2}}$$

- 我们可以对上下界估值：

$$-\log_2 2^{\binom{n}{2}} = \binom{n}{2} = \frac{n^2}{2}\left(1 - \frac{1}{n}\right)$$

$$-\log_2 \frac{2^{\binom{n}{2}}}{n!} = \binom{n}{2} - \log_2 n!$$

$$\ge \binom{n}{2} - \log_2 n^n$$

$$= \frac{n^2}{2}\left(1 - \frac{1}{n} - \frac{2\log_2 n}{n}\right)$$

$$x = \Theta(2^{\frac{n^2}{2}})$$

Graph Score

概念

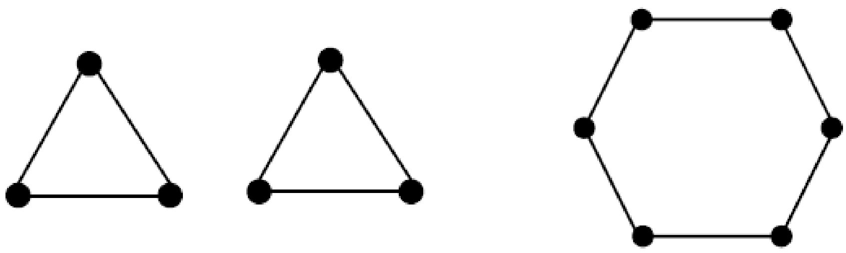
各个顶点度的序列，按照非递减的顺序写

- Let G be a graph. The vertices of G be $v_1, v_2, \dots, v_n$. The the degree sequence of G, or a score of G is:

$$(\deg_G(v_1), \deg_G(v_2), \dots, \deg_G(v_n))$$

同构一样相同score，score相同不一定同构

- Isomorphic graphs $\Longrightarrow$ The same scores.
- The same scores $\not\Longrightarrow$ Isomorphic graphs.



(2,2,2,2,2,2) (2,2,2,2,2,2)

注意：不是所有有限序列都是graph score

Score Theorem

构造D'

D为graph score 充要 D'为graph score

Let $D = (d_1, d_2, \dots, d_n)$ be a sequence of natural numbers, $n > 1$. Suppose that $d_1 \le d_2 \le \cdots \le d_n$, and let the symbol D' denote the sequence $(d_1', d_2', \dots, d_{n-1}')$, where

$$d_i' = \begin{cases} d_i & \text{if } i < n - d_n \\ d_i - 1 & \text{if } i \ge n - d_n \end{cases}$$

Then D is a graph score iff D' is a graph score.

例子

每次构造D'并进行重排

- (1,1,1,2,2,3,4,5,5)
- (1,1,1,1,1,2,3,4)
- ~~(1,1,1,0,0,1,2)~~
- (0,0,1,1,1,1,2)
- ~~(0,0,1,1,0,0)~~
- (0,0,0,0,1,1)
- (0,0,0,0,0)

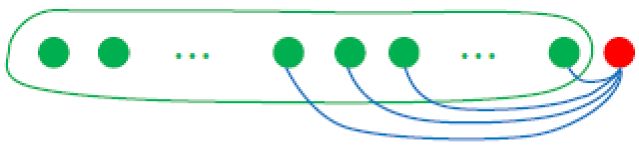
证明

正向 如果D'为graph score，D为graph score

$G' = (V', E')$, where

$V' = \{v_1, v_2, \dots, v_{n-1}\}$

New vertex v_n



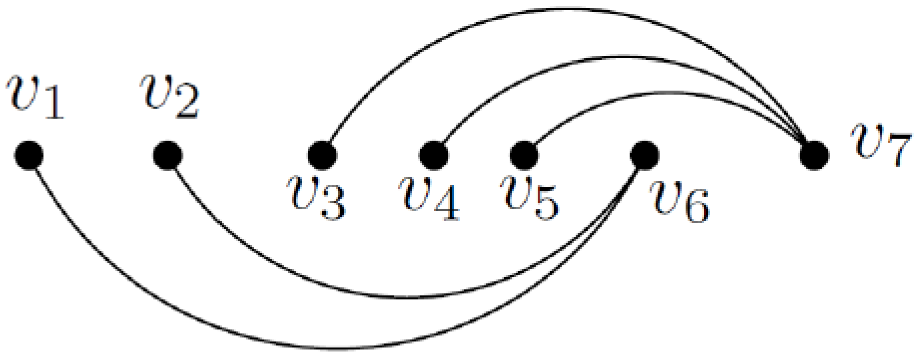
$G = (V, E)$

$V = V' \cup \{v_n\}$

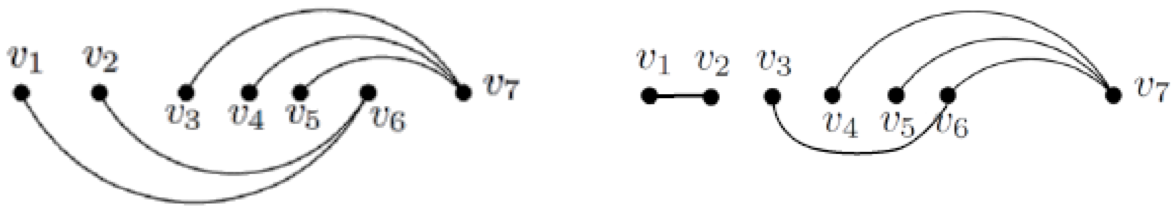
$$E = E' \cup \{\{v_i, v_n\}: i = n - d_n, n - d_n + 1, \dots, n - 1\}.$$

反向 如果D为graph score，D‘为graph score

不能直接删除



考虑转化为右图：与最大度顶点相邻的边都在其旁边



G hat 一个等价类，对一个graph score能还原的图的集合，证明其中有一个图满足右图即可

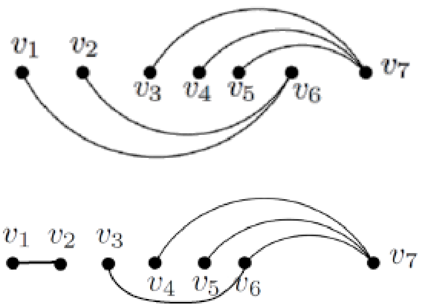
The set $\hat{G}$ of all graphs on the vertex set $\{v_1, \ldots, v_n\}$ in which the degree of each vertex v_i equals d_i. $i = 1, 2, \ldots, n$. It will be *sufficient* to prove the following claim

Claim. The set $\hat{G}$ contains a graph G_0 in which the vertex v_n is adjacent *exactly* to the *last d_n vertices*, i.e. to vertices $v_{n-d_n}, v_{n-d_n+1}, \ldots, v_{n-1}$.

证明：

引入$j(G)$为最大的与v_n不相邻点的index

- If $d_n = n - 1$, then any graph from $\hat{G}$ satisfies the claim.
- O.W. $d_n < n - 1$: $\forall G \in \hat{G}$
  - $j(G) = Max\{j \in \{1,2,\dots,n-1\} \mid \{v_j, v_n\} \notin E(G)\}$



- Let G_0 be a graph in $\hat{G}$ with *smallest* possible value of $j(G)$.
- Prove: $j(G_0) = n - d_n - 1$

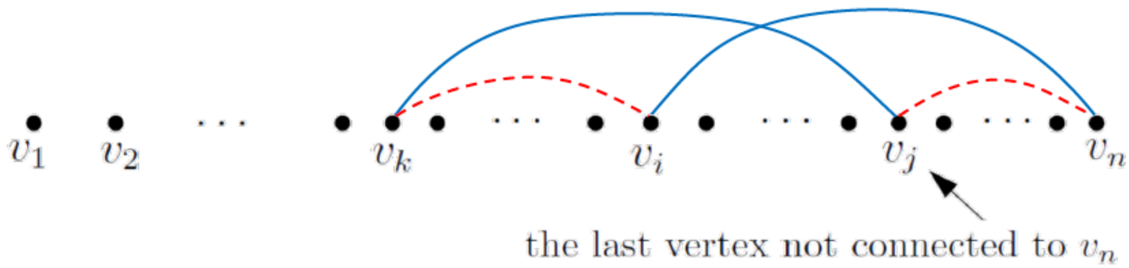
第一个图$j(G) = 6$，第二个图$j(G) = 3$

找到最小的$j(G) = n - d_n - 1$即可

G_0为$j(G)$最小的图，导出有比其更小的矛盾。

- (Proof by contradiction) Suppose

$$j = j(G_0) > n - d_n - 1$$



$G' = (V, E')$ where

$E' = \left(E(G_0) \setminus \left\{\{v_i, v_n\}, \{v_j, v_k\}\right\}\right) \cup \left\{\{v_j, v_n\}, \{v_i, v_k\}\right\}$

The score of G' and G_0 are the same. There is a contradiction as $J(G') \le J(G_0) - 1$.

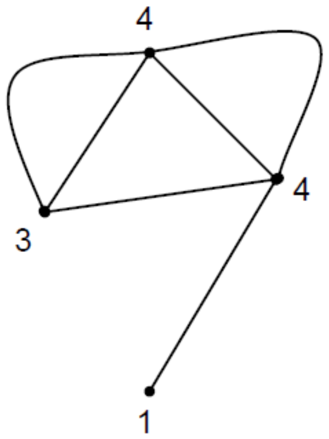
18

Ch 05 握手定理的应用 Handshake lemma

握手定理

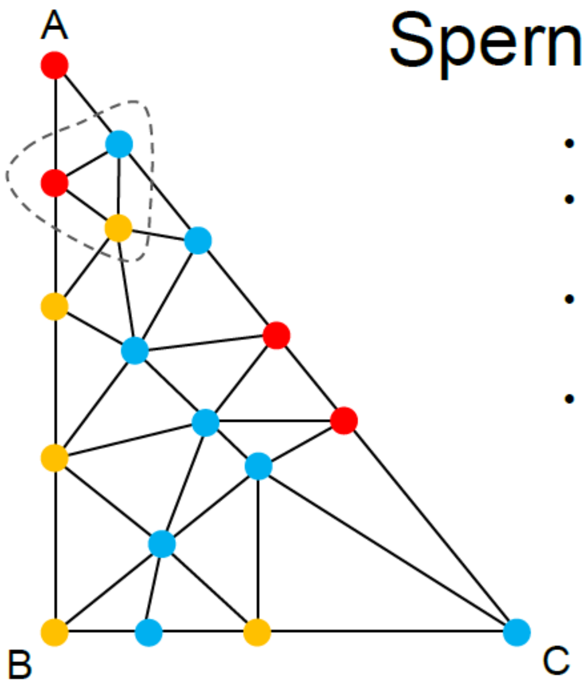
- **握手定理：** 给定无向图 $G=(V,E)$，有 $\sum_{v\in V}\deg_G(v)=2|E|$

- **推论：** 无向图中，度数为奇数的点一定是有偶数多个。



$1+3+4+4=12=2\times 6$

Sperner 引理



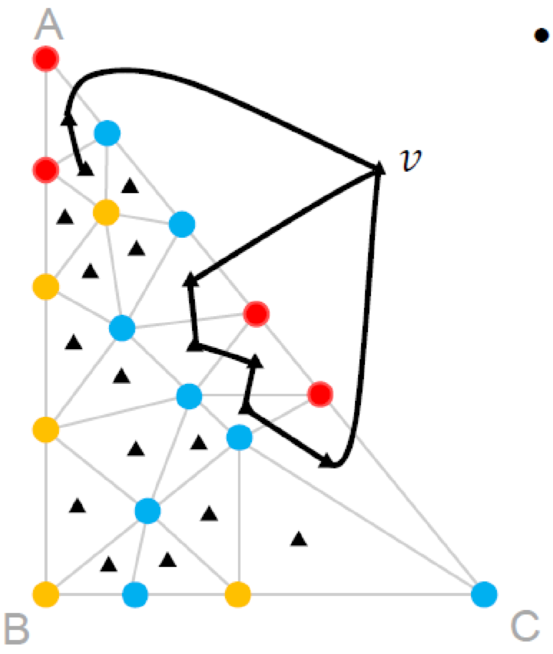
Sperner 引理

- 已知平面上的一个三角形**ABC**。
- 任意划分成若干小的不重叠三角形。
- 用●、●、●依次对**A**、**B**、**C**三个顶点着色。
- 对其余顶点着色：
  - **BC**边上的点用●色或●色
  - **AB**边上的点用●色或●色
  - **AC**边上的点用●色或●色
  - 其它内部顶点：任意着色

Sperner 引理（平面）:必然存在一个三个顶点不同色的三角形

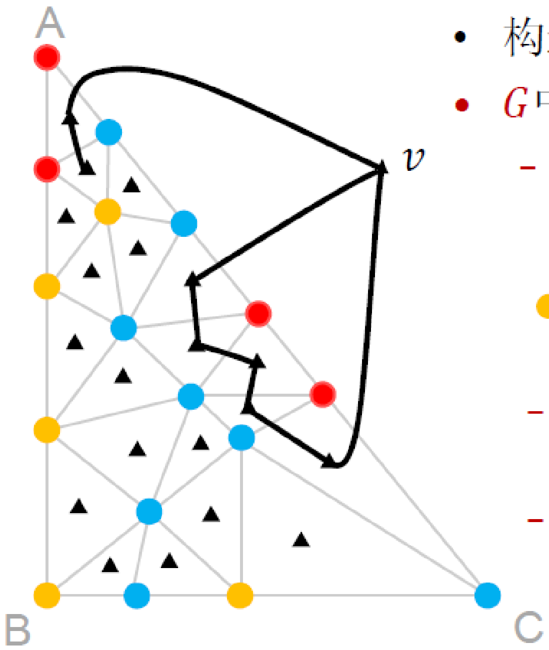
3

证明

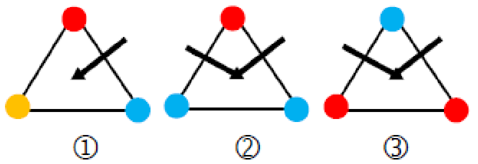


- 构造图$G=(V,E)$
  - V：每个闭合的连续平面（小三角形）抽象为一个点，外面的开放平面也抽象为一个点，用▲表示，取名为v。
  - E：两个▲之间有一条边当且仅当原对应平面相邻且邻边顶点着色为●和●。

5



- 构造图$G=(V,E)$
- G中顶点的度数：
  - V在ABC内(非v)度数非0的情况:

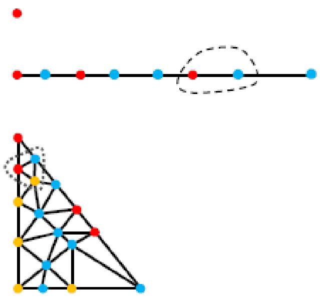


  - V在ABC内(非v)的点在其余情况下度数均为0。
  - V在ABC外的点（点v）的度数:就是AC边上的颜色改变次数，易证其必为**奇数**。
  - 根据**握手定理**，G中必还有度数为奇的点，即情况①必发生。

6

一般形式

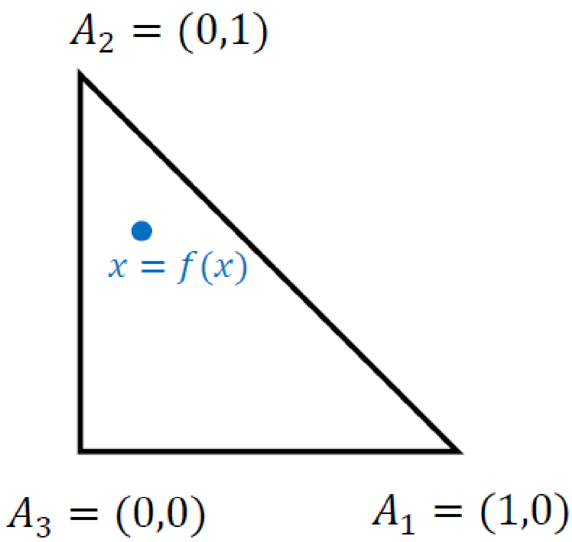
- Spernner's lemma (Sperner, 1928)：对任意n维单形体(n-simplex)进行分割并用$n+1$种颜色去着色，则任何合适的单形体分割着色方案下，都必有一个包含所有不同颜色的单元。
- 例:
  - $n=0$
  - $n=1$
  - $n=2$



  - $n=3$ 四面体
  - ……

7

拓扑应用 定点 fix point



- Δ is a triangle in the plane.
- $f:\Delta\to\Delta$ is continuous: $\forall a\in\Delta, \forall\epsilon>0, \exists\delta>0$ $(b\in\Delta\wedge dist(a,b)\le\delta \to dist(f(a),f(b))\le\epsilon.)$
- Planar Brouwer's fixed point theorem: Every continuous function $f:\Delta\to\Delta$ has a fixed point.

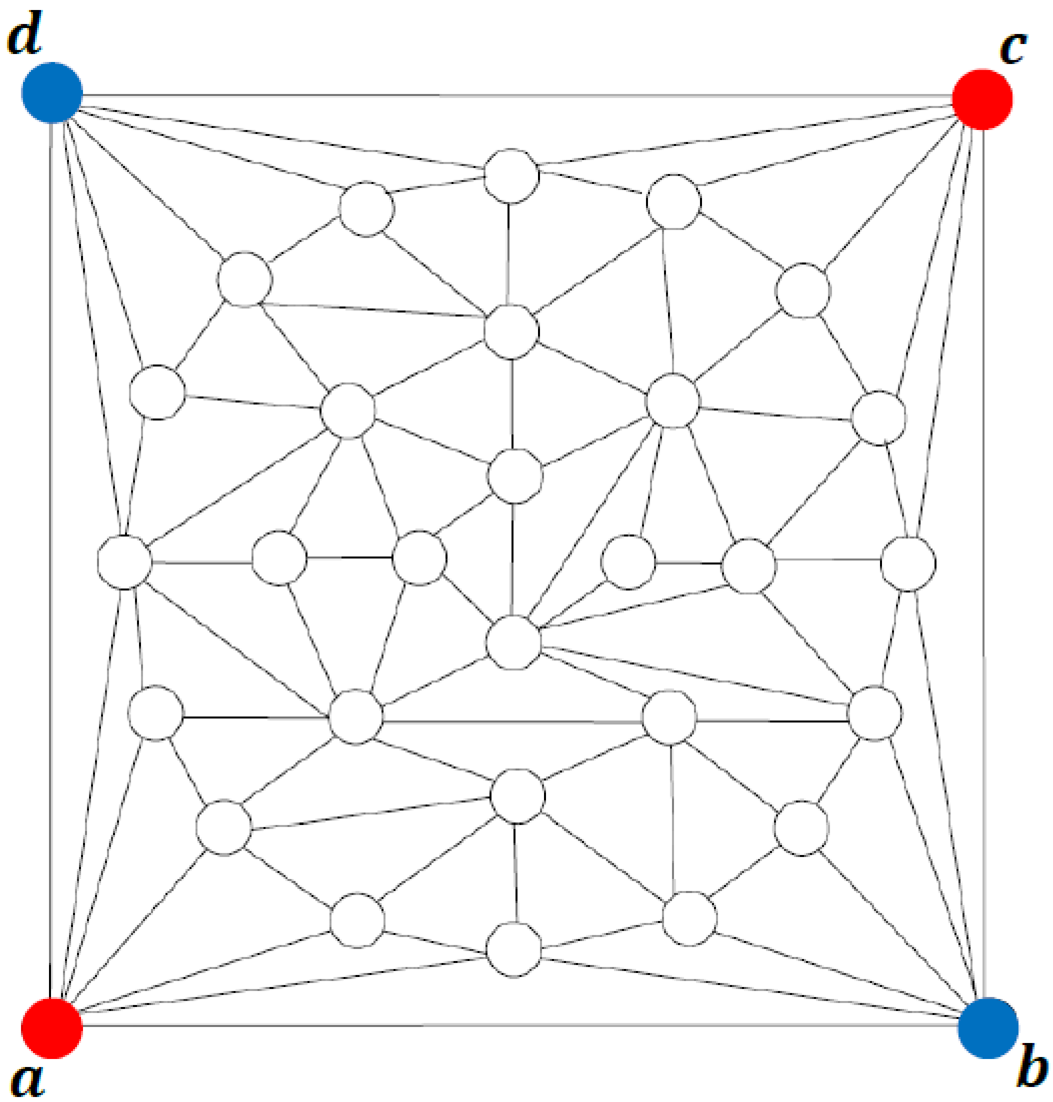
证明思路

定义
$$\begin{cases} \beta_1(a)=x \\ \beta_2(a)=y \\ \beta_3(a)=1-x-y \end{cases}$$

满足β_i的集合为M_i，证$M_1 \cap M_2 \cap M_3$不空，对三角形进行无限三角剖分，满足性质的点着色，必有三色三角形，剖分无限次后该三角形size近似为0

博弈论应用 HEX game

E



每人下一次，知道先有纯红连起ac或纯蓝连起bd

证明一定存在获胜者

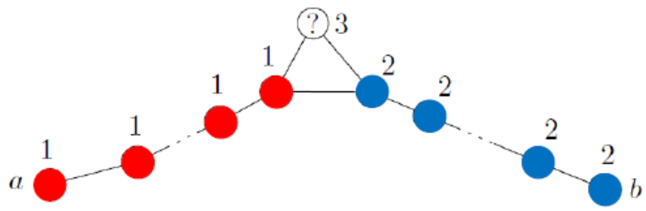
进行标记，证明不会c和d都为3即可

Labelling vertex v :

- 1： if the vertex belongs to R and there is an all-red path from a to v.
- 2： if the vertex belongs to B and there is an all-blue path from b to v.
- 3: otherwise.

Observation: If the proposition fails, then both c and d must be labelled by 3.

不存在三label三角形



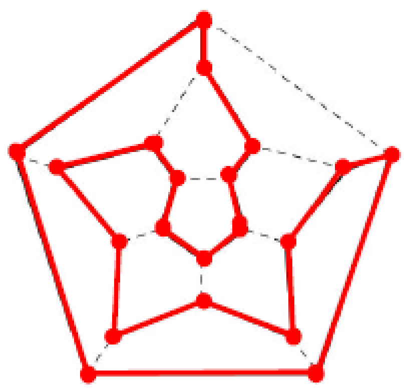
Observation: If the proposition fails, then both c and d must be labelled by 3.

- A triangle contains three different labels {1, 2, 3} will lead to contradiction.
- If both c and d have label 3, then there must be such an triangle.
- Either c is labeled 1 or d is labeled 2.
- Either RED wins or BLUE wins.

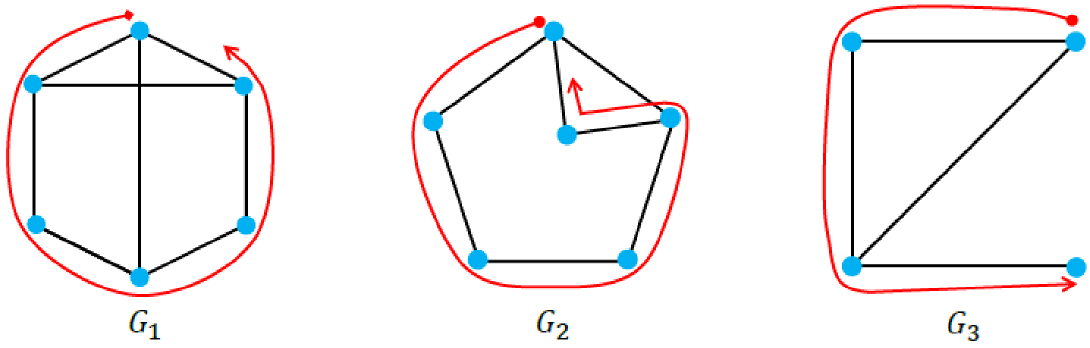
c和d都为3，可合并为一点，与a和b形成三label三角形，应用Sperner 引理，知道其中必有三label三角形，与事实矛盾。

握手定理在哈密尔顿图应用

周游所有点



- 哈密顿回路(Hamiltonian cycle)：如果一个环经过图上所有点正好一次，则此环被称为哈密顿环。
- 哈密顿图(Hamiltonian graph)：含有哈密顿环的图，被称为哈密顿图。
- 哈密顿路径(Hamiltonian path)：如果一条路径经过图上所有点正好一次，则此路径被称为哈密顿路径。
- 仅考虑简单图（无环、无重边）



- G_1, G_2, G_3 都含有哈密顿路径
- 仅G_1, G_2 含哈密顿回路，是哈密顿图

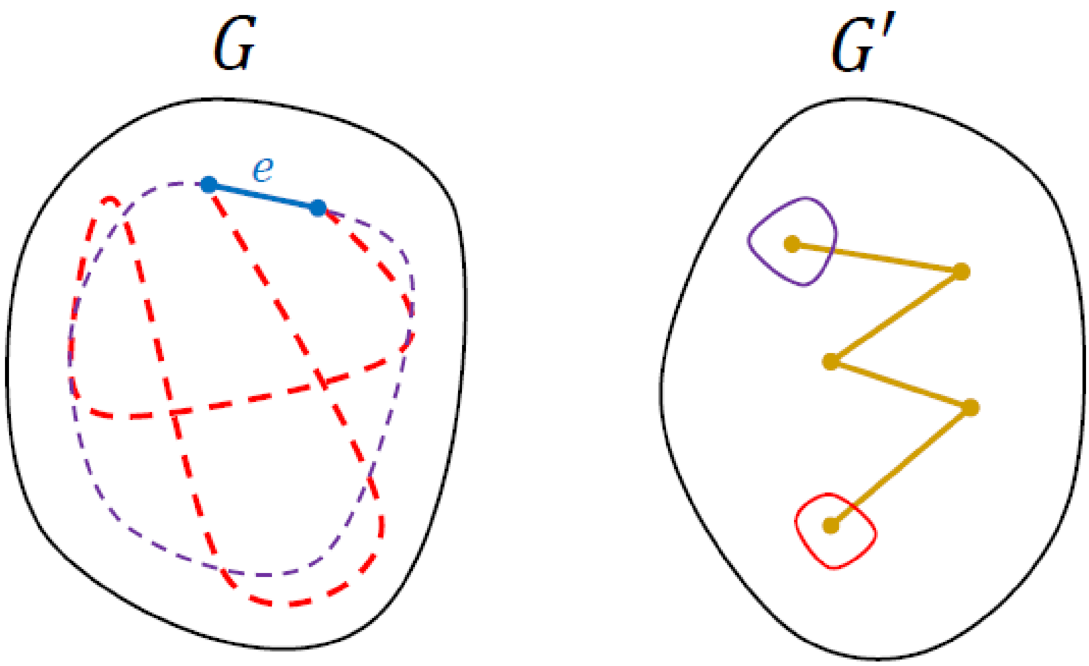
哈密顿回路 → 哈密顿路径，反之不成立。

应用握手定理

定理(Smith)：对3-正则图，包含图上任意边e的哈密顿回路必有偶数条。

证明

经过e的点映射到度数为1的点

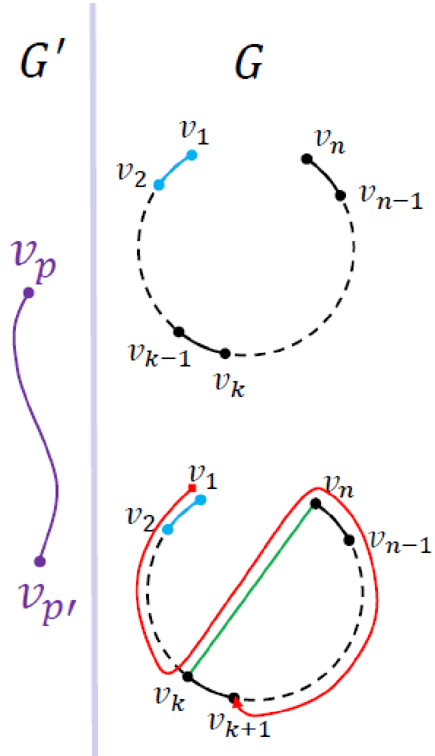


– 图G是3-正则图，$e=\{v_1,v_2\}$是一条固定的边，不失一般性，假设原图中有含有e的哈密顿回路。

– 构造图$G'=(V',E')$

- V'中的每一点，代表一条从v_1开始，以e为第一条边的哈密顿路径（由前提假设知V'非空）
- 构造E'：

- 构造E'
  - $v_p\in V'$ 代表哈密顿路径P；
  - v_n在G中度数为3，故必存在$1<k<n-1$满足$\{v_k,v_n\}\in E(G)$；
  - $P'=v_1v_2\dots v_kv_nv_{n-1}\dots v_{k+1}$是哈密顿路径。$v_{p'}\in V'$；
  - $\{v_p,v_{p'}\}\in E'$。

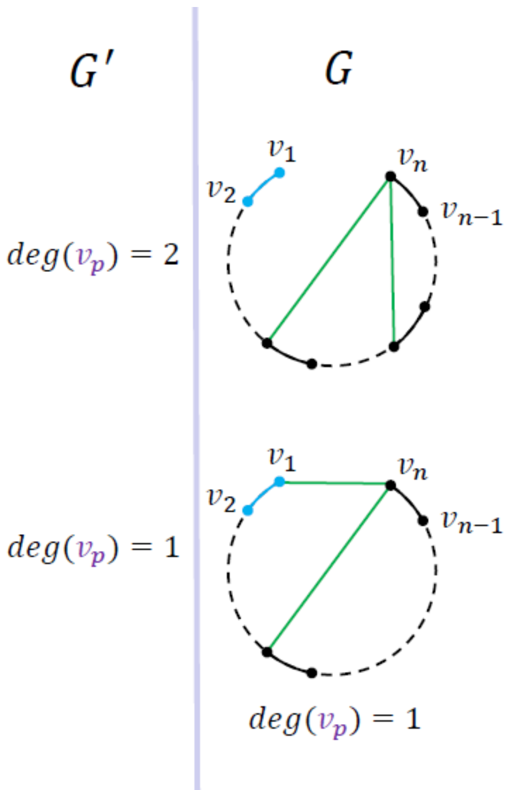


➢ E'中任意v_p的度数至多为2：

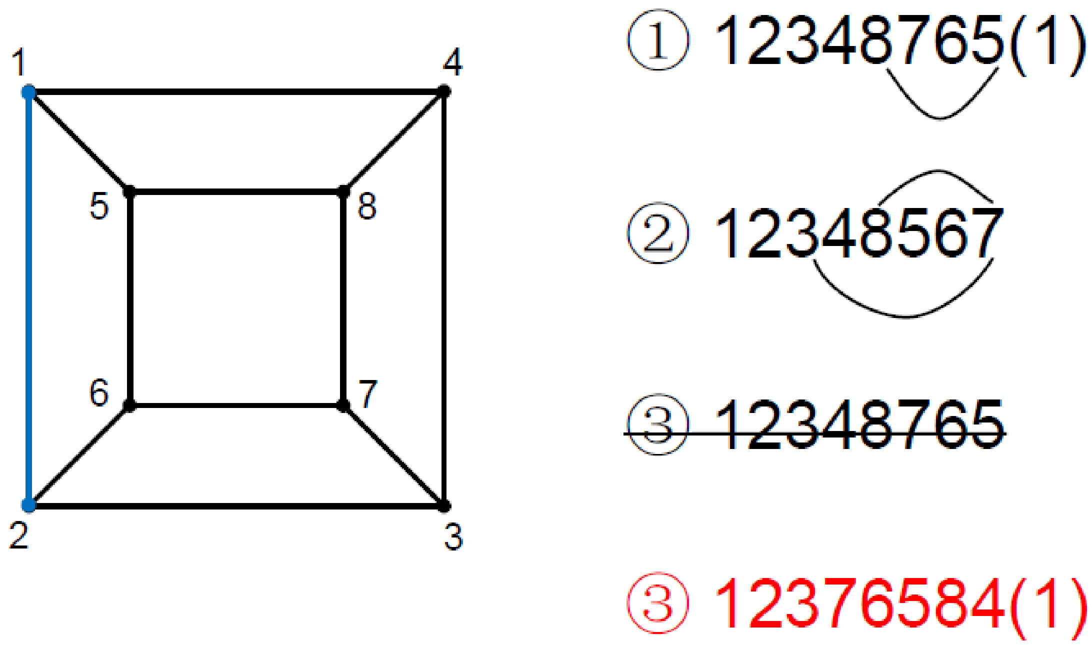
➢ $deg(v_p)=1$当且仅当原始用到的哈密顿*路径*实际上是图G中一个哈密顿*回路*。

➢ 根据握手定理，度数为奇数的点必有偶数个，故必存在另一点$deg(v_q)=1$。

➢ v_q对应图G中的另一条哈密顿回路，得证。



例子



Ch 05 生成树的个数 The number of spanning trees

树的刻画

树(Tree)：连通无环图

叶子(leaf)：图G中度数为1的顶点被称为叶子或终点(end-vertex)。

引理：对任意树T，如果$T \geq 2$，则T必含有至少两个终点。

取T中的一条极长路径P

$deg_T(v_0) = degT(v_t) = 1$

树生长引理(Tree-growing lemma)：对图G及图G上的叶子结点v而言，如下命题等价

I. 图G是树。

II. 图$G - v$是树。

连通无环图加上或减去一个度数为1的节点不会变为有环

树的等价刻画

对图$G=(V,E)$而言，以下陈述等价

I. 图G是树。

II. 路径唯一：对任意两点$u,v\in V$，存在从u到v的唯一路径。

III. 最小连通图：G是连通图，且去掉任意一条边后都成为非连通图。

IV. 最大无环图：G不含环，但增加任何一条边所得到的图$G+e$（其中$e\in\binom{V}{2}\backslash E$）中含有一个环。

V. Euler方程：G是连通图，且$|V|=|E|+1$。

树是一种特殊类型的平面图，是不包含回路且连通的无向图。在教科书中给出树的等价定义的证明很繁琐，部分内容学生理解起来有困难，不易接收。本文主要通过欧拉公式、归纳法、反证法对树的等价定义做以下证明。

定理　设树 $T=\langle V,E\rangle$，以下关于树的定义是等价的。

(1)无回路的连通图；

(2)T 无回路，且 $e=v-1$，其中 e 是树 T 中边数，v 是结点数；

(3)T 是连通图，且 $e=v-1$；

(4)T 无回路，但在 T 的任两个不相邻的结点之间添加一条边，得到一个且仅一个回路。

证明(1)⇒(2)用归纳法

(a)当 $e=1$ 时，因 T 是无回路的连通图，则 $v=2$，所以 $e=v-1$ 成立。

(b)假设 $e=k$ 时命题成立。当 $e=k+1$，由于 T 是无回路的连通图，所以新添加的第 k+1 条边和 T 中一个结点以及 T 外的一个结点联结。于是 $v_{k+1}=V_k+1$，$e_{k+1}=e_k+1$，有 $e_{k+1}=e_k+1=v_k-1+1=V_{k+1}-1$。综合以上，命题成立。

(1)⇒(2)应用欧拉公式

因 T 是无回路的连通图，故 $k=1$ 由欧拉公式 $v-e+k=2$ 得到 $e=v-1$。

(2)⇒(3)用反正法

假设 T 不是连通图，设有 $\omega(\omega>1)$个连通分支，设为 $T_1,T_2,\cdots,T_\omega$，其结点数分别为 $V_1,V_2,\cdots,V_\omega$，并且 $\sum_{i=1}^{\omega}V_i=V$，由于每个分支中都无回路，则在 T_i 中有 $e_i=V_i-1$。所以在 T 中边数 $e=\sum_{i=1}^{\omega}e_i=\sum_{i=1}^{\omega}(V_i-1)=\sum_{i=1}^{\omega}V_i-\omega=v-\omega<v-1$ 矛盾。所以 T 是连通图，且 $e=V-1$。

(3)⇒(4)用归纳法(首先证明 T 是无回路的)。

(a)当 $e=1$ 时，则有 $v=e+1=2$，显然 T 是无回路的。

(b)假设 $e=k$ 时，结论成立，当 $e=k+1$，因 $e=v-1$，所以 $v_{k+1}=e_{k+1}+1=e_k+1+1=v_k+1$. 于是，新增一条边的同时必增加一个结点，而 T 又是连通图，所以，第 k+1 条边和 T 中一个结点以及新增加的一个结点联结。故 T 是无回路的。

其次证明：如果在连通图 T 的任意两个不相邻的结点 v_i,v_j 间添加一条边(v_i,v_j)，则该边必与 T 中从 v_i 到 v_j 的原来的路径构成回路，并且该回路一定是唯一的。否则，删去边(v_i,v_j)后，在 T 中仍有回路，与题设矛盾。

(3)⇒(4)应用欧拉公式(证明 T 是无回路的)。

假设 T 中有回路，则面数 $k\geqslant2$，由欧拉公式知 $2=v-e+k\geqslant v-e+2$，即 $e\geqslant v$，而由 $e=v-1$ 知 $e<v$ 矛盾，所以 T 中无回路。

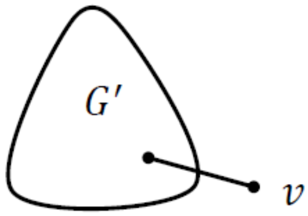
(4)⇒(1)用反证法

若图 T 不连通，则存在结点 u_i 和 u_j，在 u_i 与 u_j 之间没有路，那么在结点 u_i,u_j 之间添加一条边(u_i,u_j)，则不会产生回路，与题设矛盾，故 T 连通。

证明

- 对图$G=(V,E)$而言，以下陈述等价
  - I. 图G是树。
  - V. Euler方程：G是连通图，且$|V|=|E|+1$。

- 证明：(I.⇔V.)
  - 充分性：归纳法（用树生长引理，对顶点个数做归纳）。
  - 必要性：（归纳法）考虑连通图G满足$|V|=|E|+1\geq 2$。
    - ➢由握手定理，图G中顶点度数之和为$2|V|-2$。故图G中必存在度数小于2的顶点，且图G是连通图，任何点度数非0，故存在度数为1的点，设为v。
    - ➢考虑$G'=G-v$。易验证归纳假设条件成立，根据归纳假设G'是树。
    - ➢显然，G'是树蕴含G是树。



8

树的计数

n个不同顶点所能构成的树的个数。

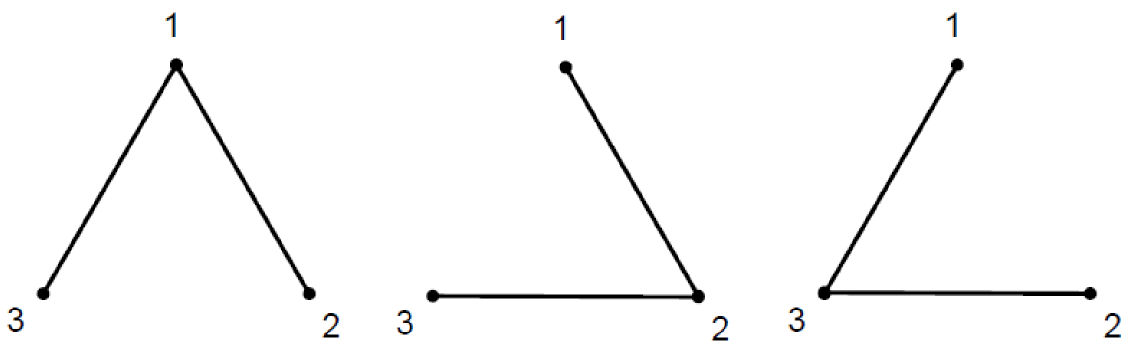
两棵树T,T'是“相等”的当且仅当树T的边集与树T'的边集相等。

生成树：生成树是包含G的所有顶点且为树的子图

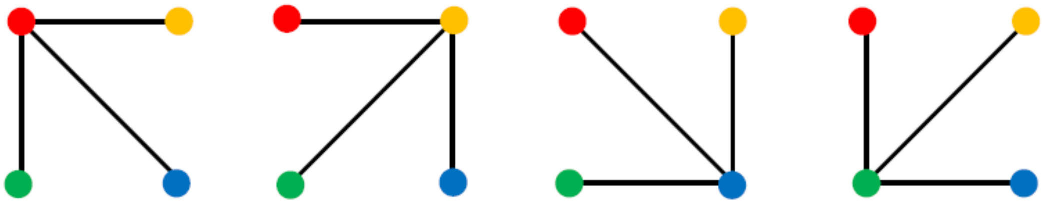
可以抽象为问K_n的生成树一共有多少种？

- $n=2$：1种

- $n=3$：3种

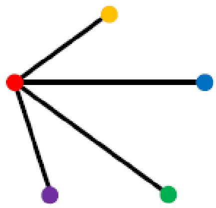


- $n = 4$： 16种
  - 星形： 4种

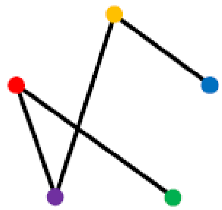


  - 路径： $\frac{4!}{2} = 12$ 种

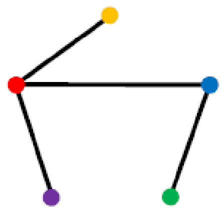
- $n = 5$： 125种
  - 星形： 5 种



  - 路径： $\frac{5!}{2} = 60$ 种

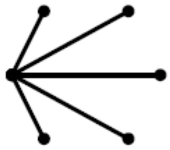


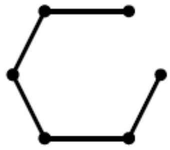
  - T形： $5 \cdot 4 \cdot 3 = 60$种



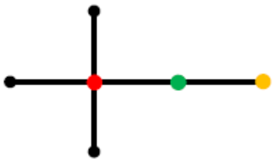
1296种

- $n=6$：?种
  - 星形：6种，路径：$\frac{6!}{2}=360$ 种

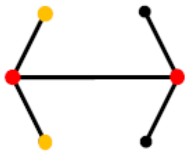




  - 十字架形：$6\times5\times4=120$ 种



  - 双箭头形：$\binom{6}{2}\times\binom{4}{2}=90$ 种



  - 单箭头形：$6\times5\times4\times3=360$ 种

  - 雨棚形：$\frac{6\times5\times4\times3\times2}{2}=360$ 种

24

顶点个数	树的种数
1	$1=1^{-1}$
2	$1=2^{0}$
3	$3=3^{1}$
4	$16=4^{2}$
5	$125=5^{3}$
6	$1296=6^{4}$

- Caley 定理(Caley's formula)：n个顶点能构成的不同树一共有n^{n-2}种。

通过score证明

给定一个score序列，可以知道对应的树的个数

Proposition. Let $d_1, d_2, \dots, d_n$ be positive integers summing up to $2n-2$. Then the number of spanning trees of the graph K_n in which the vertex i has degree exactly d_i for all $i = 1,2,\dots,n$ equals

$$\frac{(n-2)!}{(d_1-1)!\,(d_2-1)!\cdots(d_n-1)!}.$$

Proof. (By induction on n) T: the set of STs of K_n with given degrees.

- $n = 1,2$, the proposition holds trivially.
- $n > 2$: there must exist an i with $d_i = 1$. w.l.o.g. $d_n = 1$.
- For $1 \le i \le n-1$, $T_i \subseteq T$, where T_i is the STs with $\{i, n\} \in E$
- Delete v_n from each tree in T_i to get T_i': STs of K_{n-1} with degrees $d_1, d_2, \dots d_{i-1}, d_i - 1, d_{i+1}, \dots, d_{n-1}$.

- $$|T_i| = |T_i'| = \frac{(n-3)\,!}{(d_1-1)!\cdots(d_{i-1}-1)!(d_i-2)!(d_{i+1}-1)!\cdots(d_{n-1}-1)!}$$
  $$= \frac{(n-3)!(d_i-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}$$

$$|T| = \sum_{i=1}^{n} |T_i| = \sum_{i=1}^{n-1} \frac{(n-3)!\,(d_i-1)}{(d_1-1)!\,(d_2-1)!\cdots(d_{n-1}-1)!} = \cdots$$

得证

应用多项式定理

Finally

$$|T(K_n)| = \sum_{\substack{d_1,d_2,\dots,d_n \ge 1 \\ d_1+d_2+\cdots+d_n = 2n-2}} \frac{(n-2)!}{(d_1-1)!\,(d_2-1)!\cdots(d_n-1)!}$$

$$= \sum_{\substack{k_1+k_2+\cdots+k_n = n-2 \\ k_1,\dots,k_n \ge 0}} \frac{(n-2)!}{k_1!\,k_2!\cdots k_n!}$$

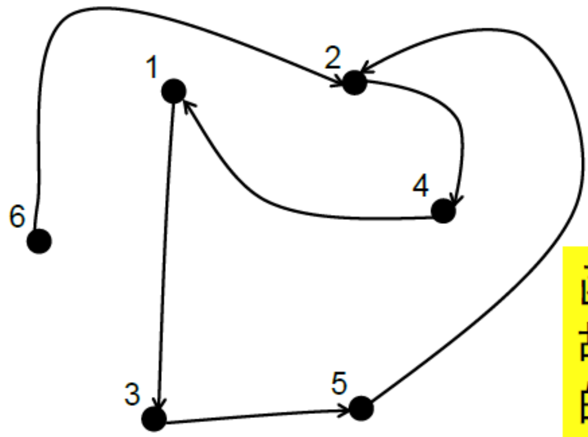
$$= \underbrace{(1+1+\cdots+1)}^{n-2} = n^{n-2}.$$

通过Vertebrates证明

函数图各顶点出度都为1

- Function graph
  $f: V \to V$

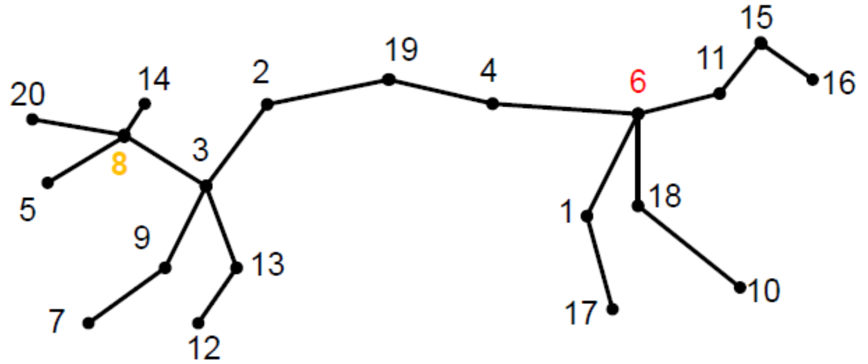
v	1	2	3	4	5	6
$f(v)$	3	4	5	1	2	2



函数图与函数一一对应。故$|V| = n$时共有n^n种不同的函数图。

树中可任取h,b，甚至hb可以重合

- 骨骼标本：三元组(T, h, b)被称为骨骼标本若其中(1) T是一棵树；(2) $h, b \in V$。h被称为颈椎骨，b被称为尾椎骨。
- 注意：h, b必须是树上的节点，除此外没有任何限制（可重合）。



① 如果$|V| = n$，用T_n表示V上的树的所有可能棵数。

② 每一棵树T对应n^2种骨骼标本(T, h, b)。

③ 骨骼标本与V上的函数图一一对应。有n^n种。

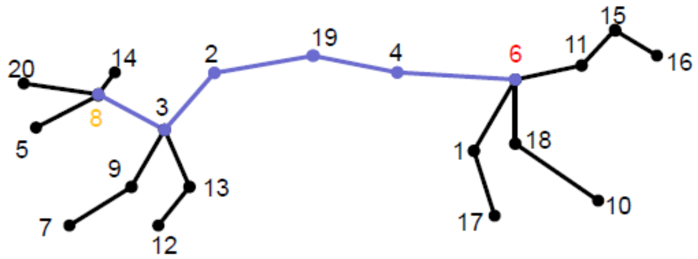
④ 根据②③： $T_n = \frac{n^n}{n^2} = n^{n-2}$

证明骨骼标本与函数图互相存在单射即可

骨骼标本对应函数图

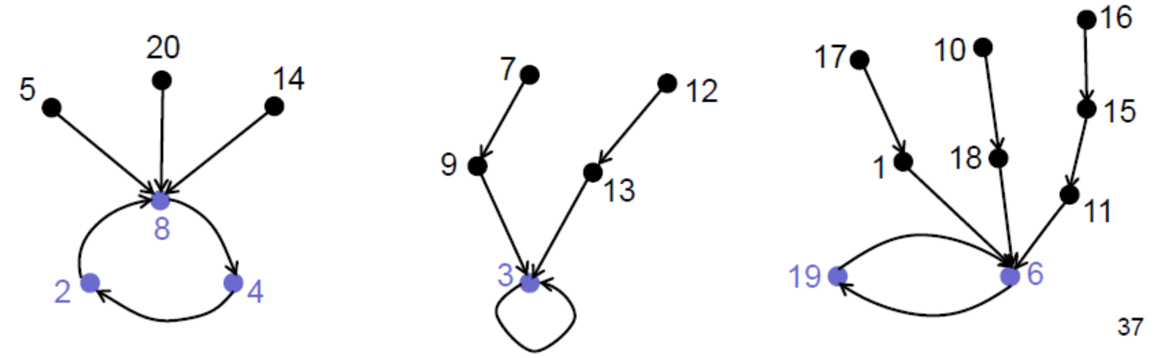
v为脊椎从小到大排序

f(v)为脊椎



• 脊椎(Spine)：出现在从颈椎骨到尾椎骨的路径上的点被称为脊椎。

v	2	3	4	6	8	19
$f(v)$	8	3	2	19	4	6

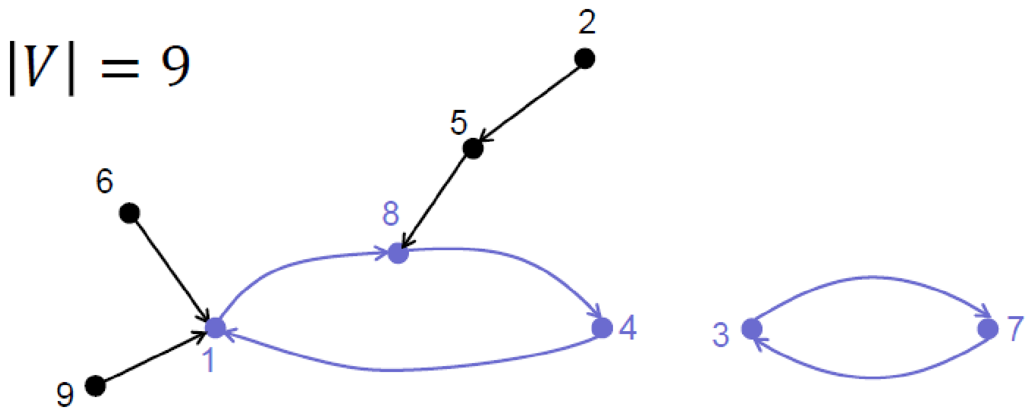


函数图对应标本

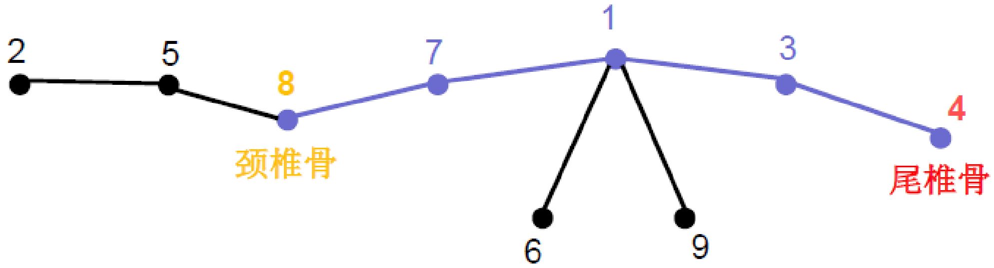
易知任何函数图都有环，将环还原为脊椎

v为脊椎从小到大排序

f(v)为脊椎函数图对应关系



v	1	3	4	7	8
$f(v)$	8	7	1	3	4



通过拉普拉斯矩阵证明

定义矩阵：

Define $n \times n$ matrix Q -- the *Laplace matrix* for G:

$$q_{ii} = \deg_G(i) \qquad i = 1,2,\dots,n$$

$$q_{ij} = \begin{cases} -1 & \{i,j\} \in E(G) \\ 0 & \text{other wise} \end{cases} \qquad i,j = 1,2,\dots,n, i \neq j.$$

去掉i行j列

$$
\begin{array}{cc}
Q = \begin{bmatrix}
\deg(1) & -1 & \cdots & 0 \\
-1 & \deg(2) & \cdots & \cdots \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & \deg(n)
\end{bmatrix}_{n\times n} & \begin{array}{c} \\ \\ i \\ \\ \end{array} \\
\qquad\qquad\qquad\qquad\qquad\quad j &
\end{array}
$$

Q_{ij} denote the $(n-1)\times(n-1)$ matrix arising from the matrix Q by deleting the ith row and jth column.

$T(G) = detQ_{11} = detQ_{ij}$

例如对于完全图有:

Application: $G = K_n$

$$
Q = \begin{bmatrix}
n-1 & -1 & \cdots & -1 \\
-1 & n-1 & \cdots & -1 \\
\vdots & \vdots & \ddots & \vdots \\
-1 & -1 & \cdots & n-1
\end{bmatrix}_{n\times n}
$$

$$
Q_{11} = \begin{bmatrix}
n-1 & -1 & \cdots & -1 \\
-1 & n-1 & \cdots & -1 \\
\vdots & \vdots & \ddots & \vdots \\
-1 & -1 & \cdots & n-1
\end{bmatrix}_{(n-1)\times(n-1)}
$$

$$
\boxed{\det(Q_{11}) = n^{n-2}}
$$

48

使用归纳法证明

定义操作:

- For an edge

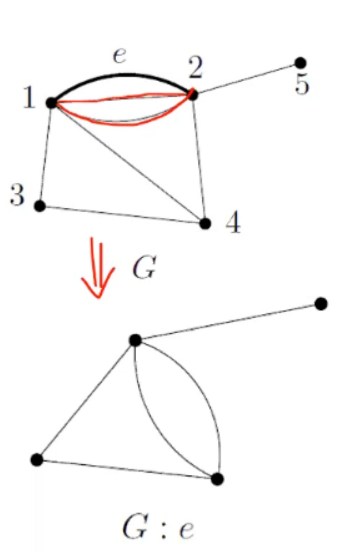
① $G-e$ Graph $(V, E\setminus\{e\})$

② $G{:}e$ contraction

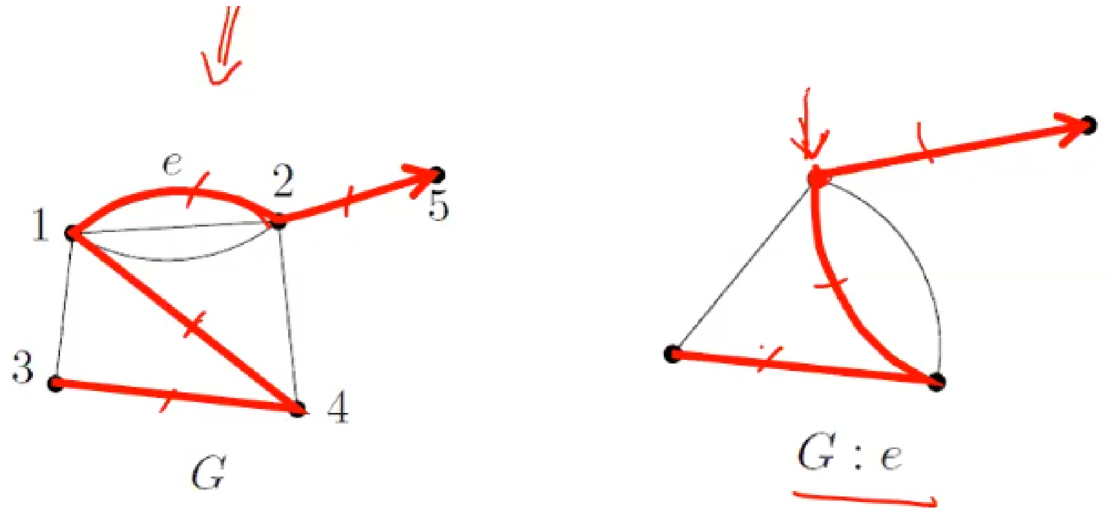
I. Remove the edge e

II. Merge the endpoints of e

III. Remove self-loops



分为没有用到e的生成树，用到e的生成树



$$T(G)=T(G-e)+T(G{:}e)$$

考虑e为{1,2}，Q'_{11}只左上角顶度数-1，$Q'_{11,22}$contraction后去掉第一行第一列相当于原行列式去掉前两行两列

$T(G) = T(G - e) + T(G : e)$ $\quad e = \{1,2\}$

Q': the Laplacian of $G - e$

Q'': the Laplacian of $G : e$

$\begin{bmatrix} deg & 0 \\ 0 & deg \end{bmatrix}$

Q'_{11} = Q_{11} except the element in the upper left corner minus 1.

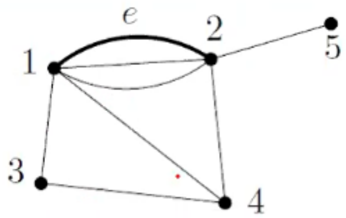
Q''_{11}= $Q_{11,22}$.

51

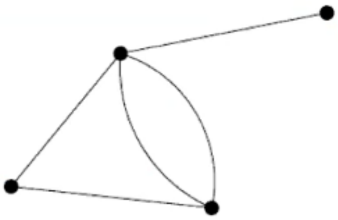
例如

Q''_{11}= $Q_{11,22}$.

G



G



$G : e$

$$Q_{11} = \begin{pmatrix} 5 & 0 & -1 & -1 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 3 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \qquad Q''_{11} = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

下面对边进行强归纳证明$T(G) = detQ_{11}$:

- Base: $m = 0$ works.
- Vertex 1 is incident to at least one edge. Fix one of them and call it e. Numbering the other end of e to be 2. By induction

(1)-e-(2)

$$\begin{aligned} T(G) &= T(G - e) + T(G : e) \\ &= \det Q'_{11} + \det Q''_{11} \\ &= \det Q'_{11} + \det Q_{11,22} \\ &= \det Q_{11} \end{aligned}$$

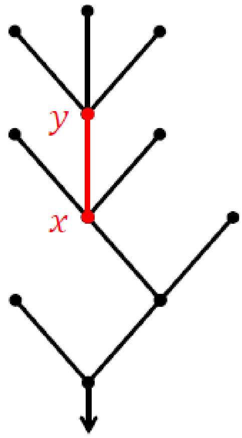
/ 2.1-1.

53

Ch 05 树同构 Tree Isomorphism

有根树(Rooted tree)

- 有根树(Rooted tree)：二元组(T, r)中T表示一棵树，$r \in V(T)$表示树上的一个特别顶点，称为根(root)。约定根用箭头标明。
- 对树上的一条边$\{x, y\} \in E(T)$，如果x是出现在从根r到y的唯一路径上，则称x是y的父亲 (father)，相应地称y是x的儿子(son)。



4

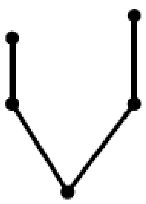
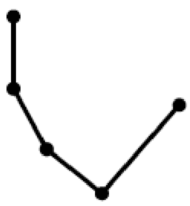
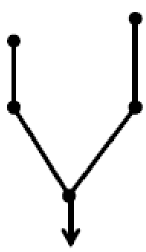
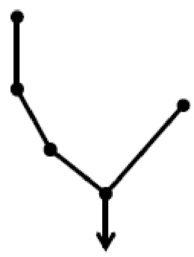
有根树之间的同构有快速算法

图之间的同构没有有效算法

有根树同构

要求同构且同一根

- **定义：** $(T, r) \cong' (T', r')$：
  - $f: V(T) \to V(T')$ 是 $T \cong T'$，
  - $f(r) = r'$。
- 例：

 $\cong$     $\ncong'$ 

$\cong'$ 关系严格地强于$\cong$关系。

判定算法

思路：将树的比较转化为字符串字典序的比较。

例：00<001 01011<0110

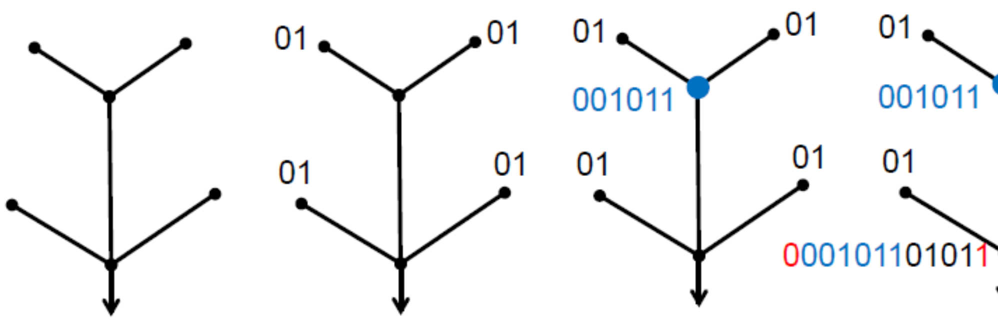
可以对树进行编码：

- 对有根树(T,r)如下编码

  R1. 所有非根叶结点都赋值为01。

  R2. 假设点v的儿子节点为$w_1,w_2,\ldots,w_k$都已各完成赋值为$A(w_i)$，且$A(w_1)\le A(w_2)\le\cdots\le A(w_k)$则对$v$节点赋值为$0A(w_1)A(w_2)\cdots A(w_k)1$。

根节点r的编码就是(T,r)的编码，用$\#(T,r)$ 表示。



8

性质： $(T,r)\cong'(T',r')$当且仅当它们具有相同的编码。

证明：

- 充分性：从有根树同构的定义和编码可证。
- 必要性：解码，从编码恢复原始的树结构。

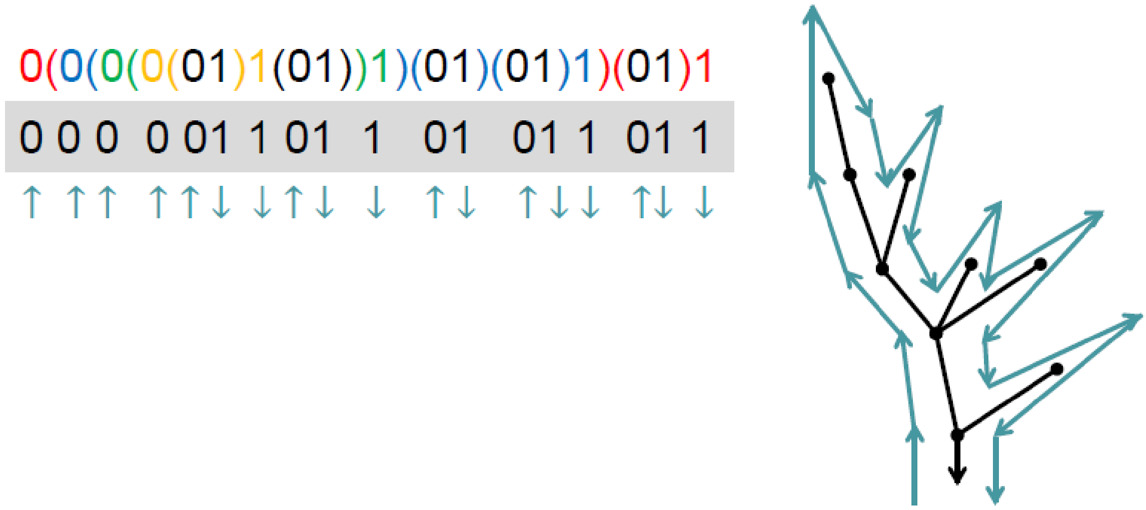
  任意有根树的编码必然有$0S1$的一般形式，其中$S=S_1S_2\ldots S_t$。

  S_1是S中0,1个数相等的最小前缀。

  S_2是第二个0,1平衡的最小前缀，等等。

  可以据此恢复出有根树，且显然这样的有根树必然是同构的。

例如

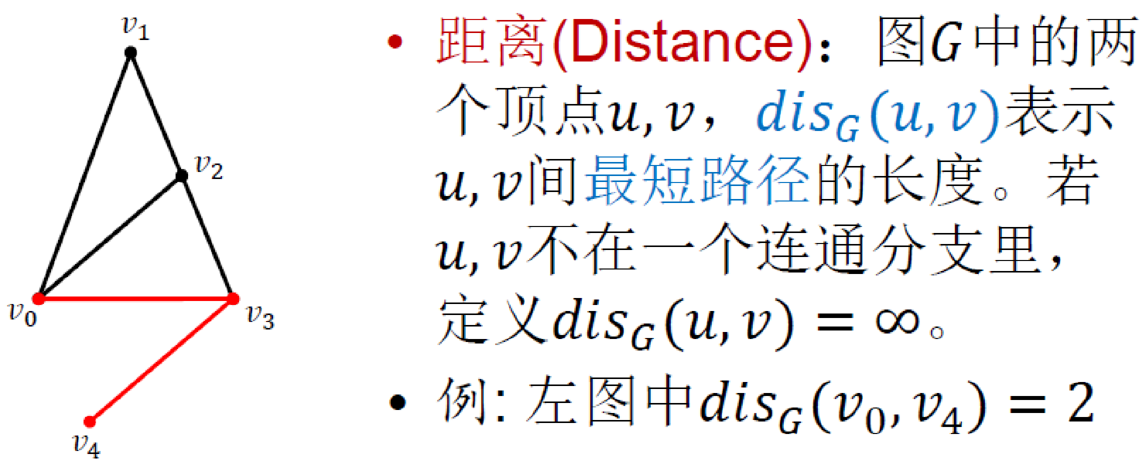


树同构

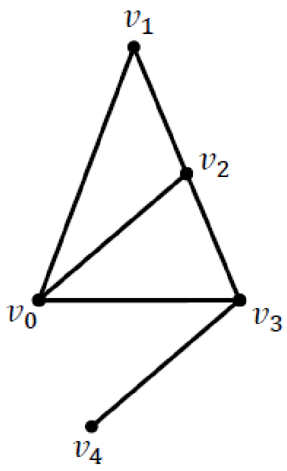
对一般树(无根树)：找到其中可以用作根的节点，且该根节点在任何同构函数下都被保持。

核心问题是选根问题

距离(Distance)



偏心率(Excentricity)



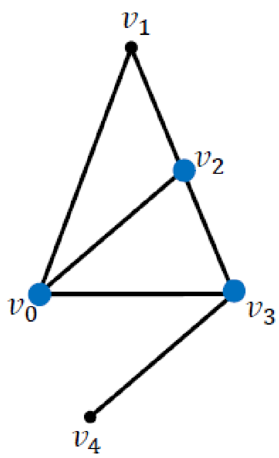
- 偏心率(Excentricity)：图G及图中的顶点v，偏心率定义为：

$$ex_G(v) = \max_{u \in G} dis_G(u, v)$$

- 例: 左图中$ex_G(v_4) = 3$

$$dis_G(v_0, v_4) = 2$$
$$dis_G(v_1, v_4) = 3$$
$$dis_G(v_2, v_4) = 2$$
$$dis_G(v_3, v_4) = 1$$

中心(Center)



- 中心(Center)：图G中偏心率最小的顶点集合叫做中心。用符号$C(G)$表示。
- 例: 左图中$C(G) = \{v_0, v_2, v_3\}$

$$ex_G(v_0) = 2$$
$$ex_G(v_1) = 3$$
$$ex_G(v_2) = 2$$
$$ex_G(v_3) = 2$$
$$ex_G(v_4) = 3$$

中心可能任意大：

– 环C_n，有$|C(C_n)| = n$

– 完全图K_n，有$|C(K_n)| = n$

为一般树找根

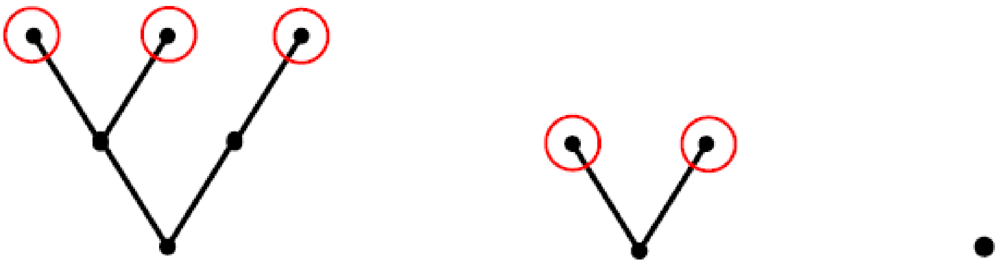
性质：对树$T=(V,E)$，$C(T)$至多含有两个顶点。且若$C(T)=\{x,y\}$，则$\{x,y\}\in E$。

证明：若$|T|\le 2$，结论显然。否则：

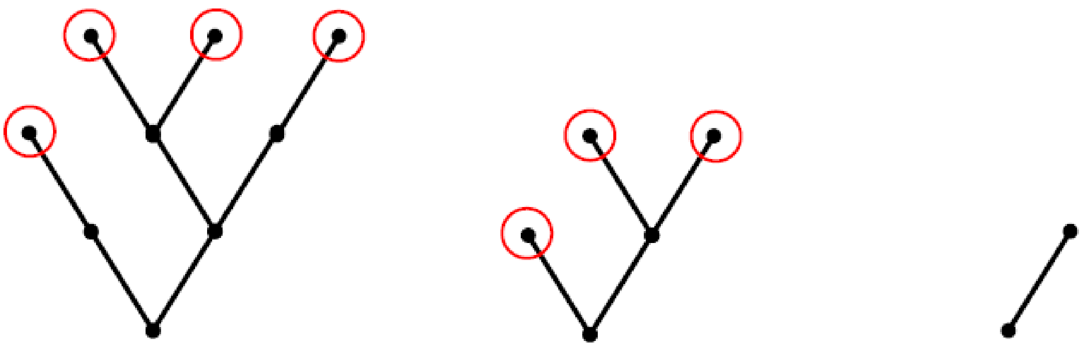
利用树的特殊性：与树上任一点v距离最远的点必然是叶子结点。

- 从T构造T'：T'是从T中删去所有叶子结点。显然对T'上的点v有 $ex_T(v)=ex_{T'}(v)+1$，进而$C(T')=C(T)$。
- 反复以上过程。直至最后剩下一个顶点（$C(T)$是一个顶点）或一条边（$C(T)$是两个顶点）。

例1：



例2：



用树的中心来完成树到有根树的转化：

- $|C(T)|=1$则中心就是根，
- $|C(T)|=2$的情形如何处理？

- $C(T)$中只含唯一顶点v：输出有根树(T,v)的编码 $\#(T,v)$ 。
- $C(T)=\{x_1,x_2\}$： $e=\{x_1,x_2\}$

$T-e$：必含有正好两个连通分支T_1,T_2。不失一般性设$x_1 \in V(T_1)$，$x_2 \in V(T_2)$。

- 计算$\#(T_1,x_1)$ 和$\#(T_2,x_2)$；
  - 如果$\#(T_1,x_1) \le \#(T_2,x_2)$，输出 $\#(T,x_1)$；
  - 否则，输出 $\#(T,x_2)$。

$\#T$ = 上述过程的输出

27

$T \cong T'$当且仅当$\#T \cong \#T'$

Ch 06 概率论 introduction The Probabilistic Method

概念

Experiment: toss a coin twice

Sample space: possible outcomes of an experiment

- Ω={HH, HT,TH,TT}

Event: a subset of possible outcomes.

- A={HH}, B={HT, TH}

Probability of an event: an number assigned to an event $\Pr(A)$

- Axiom 1: $\Pr(A) \ge 0$
- Axiom 2: $\Pr(\Omega) = 1$
- Axiom 3: For every sequence of disjoint events $\Pr(\cup_i A_i) = \sum_i \Pr(A_i)$

3

$E_1 \cap E_2$ is the event that both E_1 and E_2 happen.

$E_1 \cup E_2$ for the event that at least one of E_1 and E_2 happen.

$E_1 - E_2$ for the occurrence of an event that is in E_1 but not in E_2.

$\bar{E}$ stands for $\Omega - E$.

Lemma: for any two events E_1 and E_2:

$$\Pr(E_1 \cup E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \cap E_2)$$

Union Bound

Lemma: For any finite or countably infinite sequence of events $E_1, E_2, \ldots$

$$Pr\left(\bigcup_{i\geq 1} E_i\right) \leq \sum_{i\geq 1} \Pr(E_i).$$

Independence

相互独立mutually independent是任意子集独立

两两独立pair independent是任意两个独立

Two events A ***and*** B ***are independent*** in case

$$\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$$

A set of events $\{A_1, A_2, \ldots, A_k\}$ are **mutually independent** iff for any subset $I \subseteq [1, k]$

$$\Pr\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} \Pr(A_i)$$

可以验证1和2中ab都不独立

而2中ab是无交集的，无交集推不出独立

独立没有传递性，考虑A和B独立，B和C独立，若C=A，A当然不和A独立

Consider the experiment of tossing a coin twice

- **Example I.**
  - $A = \{HT, HH\}, B = \{HT\}$
  - Will event A independent from event B?
- **Example II.**
  - $A = \{HT\}, B = \{TH\}$
  - Will event A independent from event B?
- Disjoint $\neq$ Independence
- If A is independent from B, B is independent from C, will A be independent from C?

8

应用 概率算法

$$(x+1)(x-2)(x+3)(x-4)(x+5)(x-6) ?= x^6 - 7x^3 + 25$$

Assume $Max(Deg(G(x)), Deg\ (F(x))) = d$

Algorithm

- Choose an integer r uniformly at random in the range $\{1, \ldots, 100d\}$
- Compute $F(r)$ and $G(r)$
- If $F(r) = G(r)$ output Yes; otherwise, output No.

- E: The event that the algorithm fails.
- The algorithm may fail iff
  - $F(x) \neq G(x)$ and $F(r) = G(r)$
  - r is the solution $of\ \ H(x) = F(x) - G(x) = 0$.
  - $H(x)$ has at most d solutions.
- $\Pr(E) \leq \frac{d}{100d} = \frac{1}{100}$
- **Idea** : If it keep returning (Yes), we repeat the algorithm for k times.
  - The updated algorithm will fail iff every E_i fails for $1 \leq i \leq k$.

11

取k轮

- $$\begin{aligned}\Pr(E) &= \Pr(E_1 \cap E_2 \cap \cdots \cap E_k) \\ &= \Pr(E_1) \cdot \Pr(E_2) \cdot \cdots \cdot \Pr(E_k) \\ &\leq \left(\frac{1}{100}\right)^k\end{aligned}$$

条件概率 Conditioning

- If E and F are events with $\Pr(F) > 0$, the **conditional probability of E given F** is

$$\Pr(E|F\} = \frac{\Pr(E \cap F)}{\Pr(F)}$$

- If E and F are independent

$$\Pr(E|F) = \frac{\Pr(E \cap F)}{\Pr(F)} = \frac{\Pr(E)\Pr(F)}{\Pr(F)} = \Pr(E)$$

应用

药物测试

	Women	Men
Success	200	1800
Failure	1800	200

A = {Patient is a Women}

B = {Drug fails}

$\Pr(B|A) = ?$

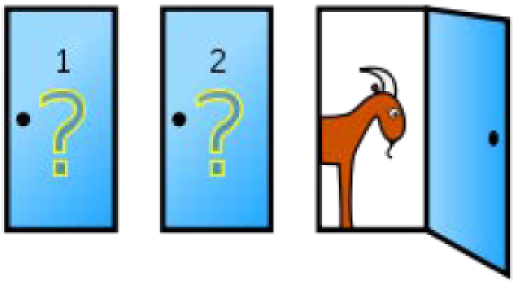
$\Pr(A|B) = ?$

Monty Hall problem

选择一扇门，主持人从另外两扇门中打开一扇山羊门，询问是否要换选另外一扇门?

换不换不一样

Suppose you're on a game show, and you're given the choice of three doors: Behind one door is a car; behind the others, goats. You pick a door, say No. 1, and the host, who knows what's behind the doors, opens another door, say No. 3, which has a goat. He then says to you, "Do you want to pick door No. 2?" Is it to your advantage to switch your choice?



Behind door 1	Behind door 2	Behind door 3	Result if staying at door #1	Result if switching to the door offered
Car	Goat	Goat	**Wins car**	Wins goat
Goat	**Car**	Goat	Wins goat	**Wins car**
Goat	Goat	**Car**	Wins goat	**Wins car**

Tuesday boy problem

两个孩子，一个是星期二男孩，另一个为男孩的概率

<boy, BTU>情况下如果boy为BTU，同<BTU, boy>重复计数

“I have two children. One is a boy born on a Tuesday. What is the probability I have two boys?”

<BTU, girl> 7
<girl, BTU> 7
<BTU, boy> 7
<boy, BTU> 7-1= 6

(7+6)/(7+7+7+6)=13/27

辛普森悖论 Simpson’s Paradox

将数据分组和将数据合并来看结果不同

	Women		Men	
	Drug I	Drug II	Drug I	Drug II
Success	200	10	19	1000
Failure	1800	190	1	1000

Drug II is better than Drug I

	Drug I	Drug II
Success	219	1010
Failure	1801	1190

A = {Using Drug I}

B = {Using Drug II}

C = {Drug succeeds}

Pr(C|A)= 219/2020 ~ 10%

Pr(C|B)=1010/2200 ~ **50%**

	Women		Men	
	Drug I	Drug II	Drug I	Drug II
Success	200	10	19	1000
Failure	1800	190	1	1000

Drug I is better than Drug II

Female Patient

A = {Using Drug I}

B = {Using Drug II}

C = {Drug succeeds}

Pr(C|A) ~ **10%**

Pr(C|B) ~ 5%

Male Patient

A = {Using Drug I}

B = {Using Drug II}

C = {Drug succeeds}

Pr(C|A) ~ **100%**

Pr(C|B) ~ 50%

女性成功率都很低，但是药物2在女性中做了少量检验；男性成功率都很高，但是药物2在男性中做了大量检验

全概率公式 Law of total probability

Let $E_1, E_2, \ldots, E_n$ be mutually disjoint events in the sample space Ω, and let $\cup_{i=1}^{n} E_i = \Omega$, then

$$\Pr(B) = \sum_{i=1}^{n} \Pr(B \cap E_i)$$

$$= \sum_{i=1}^{n} \Pr(B|E_i) \Pr(E_i)$$

条件独立 Conditional Independence

- Event A and B are ***conditionally independent given C*** in case

$$\Pr(A \cap B|C) = \Pr(A|C) \cdot \Pr(B|C)$$

Or equivalently,

$$\Pr(A|B \cap C) = \Pr(A|C)$$

例子

A和B不独立，但A和B条件独立

Example: There are three events: A, B, C

- $\Pr(A) = \Pr(B) = \Pr(C) = \frac{1}{5}$
- $\Pr(A \cap C) = \Pr(B \cap C) = \frac{1}{25}, \Pr(A \cap B) = \frac{1}{10}$
- $\Pr(A \cap B \cap C) = \frac{1}{125}$
- Whether A, B are conditionally independent given C?
- Whether A, B are independent?

贝叶斯规则 Bayes' Rule

$$\Pr(B \mid A) = \frac{\Pr(AB)}{\Pr(A)} = \frac{\Pr(A \mid B)\Pr(B)}{\Pr(A)}$$

可以用于预测

Pr(W|R)	R	¬R
W	0.7	0.4
¬W	0.3	0.6

R: It is a rainy day

W: The grass is wet

$\Pr(R|W) = ?$

$\Pr(R) = 0.8$

与全概率公式配合

Suppose that $B_1, B_2, \ldots B_k$ form a partition of S:

$$B_i \cap B_j = \varnothing; \quad \bigcup_i B_i = S$$

Suppose that $\Pr(Bi) > 0$ and $\Pr(A) > 0$. Then

$$\Pr(B_i \mid A) = \frac{\Pr(A \mid B_i)\Pr(B_i)}{\Pr(A)}$$

$$= \frac{\Pr(A \mid B_i)\Pr(B_i)}{\sum_{j=1}^{k} \Pr(AB_j)}$$

$$= \frac{\Pr(A \mid B_i)\Pr(B_i)}{\sum_{j=1}^{k} \Pr(B_j)\Pr(A \mid B_j)}$$

应用

E_i: the i^{th} coin is the biased one.

B: HHT

$\Pr(B|E_1) = \Pr(B|E_2)$

$$= \left(\frac{2}{3}\right) \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{1}{2}\right) = \frac{1}{6}$$

$$\Pr(B|E_3) = \left(\frac{1}{2}\right) \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{1}{3}\right) = \frac{1}{12}$$

$$\Pr(E_i) = \frac{1}{3}$$

- $\Pr(E_1 \mid B) = 2/5 = \dfrac{(1/6)(1/3)}{2(1/6)(1/3)+(1/12)(1/3)}$

- We have three coins
  - Two of them: fair
  - The other one: $\Pr(H) = 2/3$
- Flip them we get: HHT
- Problem: What is the probability that the first coin is the biased one?

34

离散随机变量和期望 Discrete random variables and expectation

A **random variable** X is a numerical outcomes of a random experiment

$$X: \Omega \rightarrow R$$

The **distribution** of a random variable is the collection of possible outcomes along with their probabilities:

– Discrete case:

$$\Pr(X = a) = \sum_{s \in \Omega, X(s)=a} \Pr(s)$$

投两个骰子合为4

The event $X = 4$ corresponds to the set of basic $events$ $\{(1,3), (2,2), (3,1)\}$. Hence

$$\Pr(X = 4) = \frac{3}{36} = \frac{1}{12}$$

独立随机变量

$$\Pr((X = x) \cap (Y = y)) = \Pr(X = x) \cdot \Pr(Y = y)$$

期望 Expectation

The expectation of a random variable is a weighted average of the values it assumes, where each value is weighted by the probability that the variable assumes that value.概率的加权平均

一阶刻画

A random variable $X \sim \Pr(X = x)$. Then, its expectation is

$$E[X] = \sum_x x \Pr(X = x)$$

In an empirical sample, $x_1, x_2, \ldots, x_N$,

$$E[X] = \frac{1}{N} \sum_{i=1}^{N} x_i$$

期望的线性性

没有任何前提，一定正确

$E(X)+E(Y)=E(X+Y)$

两个骰子点数和

Solution:

Let $X = X_1 + X_2$

where X_i represents the outcome of dice i for $i = 1,2$. Then

$$E(X_i) = \frac{1}{6}\sum_{j=1}^{6} j = \frac{7}{2}$$

$$E(X) = E(X_1) + E(X_2) = 7$$

$E[cX]=c \cdot E[X]$

Variance 方差

二阶刻画

The **variance** of a random variable X is the expectation of $(X - E[X])2$:

$$
\begin{aligned}
Var(X) &= E((X - E[X])^2) \\
&= E(X^2 + E[X]^2 - 2XE[X]) \\
&= E(X^2 - E[X]^2) \\
&= E[X^2] - E[X]^2
\end{aligned}
$$

概率分布

分布	符号	参数	分布律或概率密度	数学期望	方差
0 – 1 分布	$b(1, p)$	$0 < p < 1$	$P\{X = k\} = p^k(1-p)^{1-k}$, $k = 0, 1$	p	$p(1-p)$
二项分布	$B(n, p)$	$n \geq 1$, $0 < p < 1$	$P\{X = k\} = C_n^k p^k (1-p)^{n-k}$, $k = 0, 1, \cdots, n$	np	$np(1-p)$
几何分布	$P(\lambda)$	$0 < p < 1$	$P\{X = k\} = p(1-p)^{k-1}$, $k = 1, 2, \cdots$	$\frac{1}{p}$	$\frac{1-p}{p^2}$
超几何分布	$H(N, M, n)$	N, M, n, $n \leq M$	$P\{X = k\} = \frac{C_M^k C_{N-M}^{n-k}}{C_N^n}$, $k = 0, 1, \cdots, n$	$\frac{nM}{N}$	$\frac{nM}{N}\left(1 - \frac{M}{N}\right)\left(\frac{N-n}{N-1}\right)$
泊松分布	$P(\lambda)$	$\lambda > 0$	$P\{X = k\} = \frac{\lambda^k e^{-\lambda}}{k!}$, $k = 0, 1, \cdots$	λ	λ
均匀分布	$U(a, b)$	$a < b$	$f(x) = \begin{cases} \frac{1}{b-a}, & a < x < b \\ 0, & \text{其它} \end{cases}$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$
指数分布	$E(\lambda)$	$\lambda > 0$	$f(x) = \begin{cases} \lambda e^{-\lambda x}, & x > 0 \\ 0, & \text{其它} \end{cases}$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$
正态分布	$N(\mu, \sigma^2)$	μ, σ^2, $\sigma > 0$	$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$	μ	σ^2

- 伯努利分布 0-1分布 Bernoulli Distribution
- 二项分布 Binomial Distribution n次伯努利分布
- 几何分布 Geometric Distribution 反复重复实验，直到第n次成功

无记忆性: $\Pr(X = n + k \mid X > k) \;=\; \Pr(X = n)$

proof.

$$
\begin{aligned}
\Pr(X = n+k \mid X > k) &= \frac{\Pr((X = n+k) \cap (X > k))}{\Pr(X > k)} \\
&= \frac{\Pr(X = n+k)}{\Pr(X > k)} \\
&= \frac{(1-p)^{n+k-1}p}{\sum_{i=k}^{\infty}(1-p)^{i}p} \\
&= \frac{(1-p)^{n+k-1}p}{(1-p)^{k}} \\
&= (1-p)^{n-1}p \\
&= \Pr(X = n).
\end{aligned}
$$

求期望，第一次就成功+第一次失败（无记忆性）

$$E[X] = p \cdot 1 + (1-p) \cdot (E[X] + 1)$$

$$p \cdot E[X] = 1$$

$$E[X] = 1/p$$

集卡问题 Coupon Collector’s Problem

- Let X be the number of boxes bought until at least one of every type of coupon is obtained.
- X_i is the number of boxes bought while you had exactly i-1 different coupons.
- Clearly, $X=\sum_{1\le i\le n} X_i$
- X_i is a geometric random variable:
  - When exactly $i-1$ coupons have been found, the probability of obtaining a new coupon *is* $p_i = 1 - \frac{i-1}{n}$
  - $E[X_i] = \frac{1}{p_i} = \frac{n}{n-i+1}$
- By the linearity of expectations, we have

$$E[X] = E[\sum_{1\le i\le n} X_i] = \sum_{1\le i\le n} E[X_i] = \sum_{1\le i\le n} \frac{n}{n-i+1} = n \cdot \sum_{1\le i\le n} \left(\frac{1}{i}\right)$$

$$= n \cdot \ln n + \Theta(n)$$

(Where $\sum_{1\le i\le n} (\frac{1}{i})$= H(n) *harmonic number*)

马尔科夫不等式 Markov’s Inequality

Let X be a random variable that assumes only nonnegative values. Then for all $a > 0$

$$\Pr(X \geq a) \leq \frac{E[X]}{a}$$

proof.

$$E(X) \geq a \cdot \Pr(X \geq a)$$

$$\sum_{x} x \Pr(X=x) = \sum_{x<a} x \Pr(X=x) + \sum_{x \geq a} x \cdot \Pr(X=x)$$

$$\geq a \sum_{x \geq a} \Pr(X=x) = a \times \Pr(X \geq a)$$

60

例子

Bound the probability of obtaining more than $\frac{3n}{4}$ heads in a sequence of n fair coin flips. Let $X_i = 1$ if the i^{th} coin flip is head, otherwise, $X_i = 0$.

– Let $X = \sum_{1 \leq i \leq n} X_i$. It follows that $E[X] = \frac{n}{2}$

– $\Pr\left(X \geq \frac{3n}{4}\right) \leq \frac{E[X]}{\frac{3n}{4}} = 2/3$

契比雪夫不等式 Chebyshev’sInequality

$$\Pr(|X - E(X)| \geq a) \leq \frac{Var[X]}{a^2}$$

proof.

$$\Pr(|X-E(X)|^2 \geq a^2) \leq \frac{E(|X-E(X)|^2)}{a^2} = \frac{Var(X)}{a^2}$$

集卡问题 Coupon Collector’s Problem

Recall: $E[X] = n \cdot Hn$

By Markov’s inequality:

$$\Pr(X \geq 2n \cdot Hn) \leq 1/2$$

By Chebyshev’s inequality, this can be improved to

$$\Pr(X \geq 2n \cdot Hn) \leq O\left(\frac{1}{(\ln n)^2}\right)$$

Ch 06 概率方法 The Probabilistic Method

洗牌问题 Cards Shuffling

riffle洗牌

四轮洗牌可以产生所有排序吗？

不能 $\binom{52}{26}^4 < 52!$

在52个空位中选26个顺序填充左边一摞即可

n张牌需要$\frac{3\log_2 n}{2}$次riffle

布尔函数 Difficult Boolean Functions

n变元布尔函数映射到0或1

相当于数字电路

$$f:\{0,1\}^n \to \{0,1\}.$$

有2^{2^n}种：定义域n个变元有2^n种取值，都可以映射到0或1

证明：存在n变元布尔函数，其不能被少于$\frac{2^n}{\log_2(n+8)}$个symbol的formula定义

可以使用以下symbol
- Symbols: $x_1, x_2, \ldots, x_n$;
- Parenthesis：(,);
- Logical connectives: ∧, ∨, ⇒, ⇔, ¬;

The number of all Boolean functions of n variables: $= 2^{2^n}$

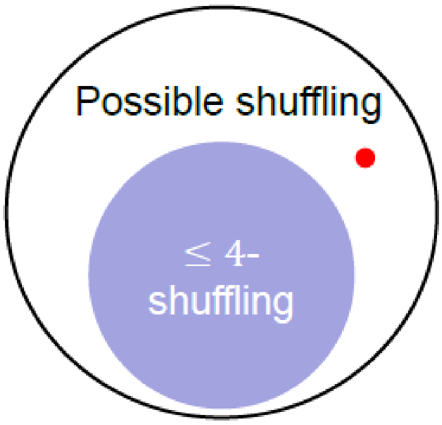
The number of formulas in n variables written by at most m symbols is: $\leq (n+8)^m$

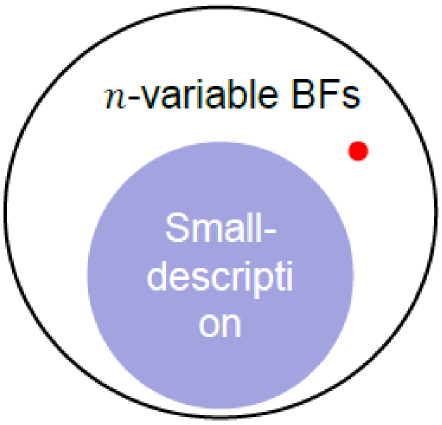
Complications will emerge when: $2^{2^n} > (n+8)^m$

$$m < 2^n / \log_2(n+8)$$

概率方法思想

紫色小于全集，存在红点



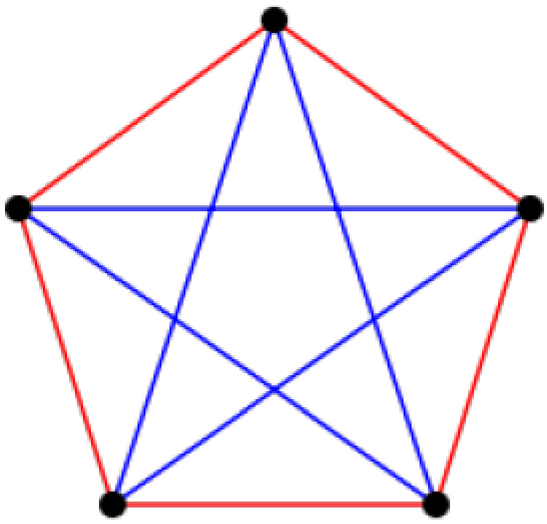


边着色 拉姆塞数 Edge Coloring Ramsey number $R(k,k)$

$R(k,k)$为最少有k个人相互认识或最少有k个人相互不认识的最小总人数

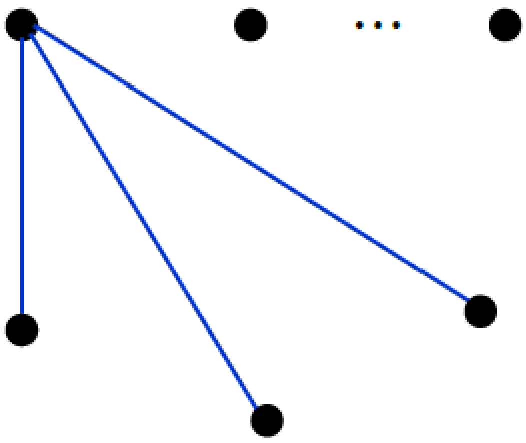
证明$R(3,3)=6$

5不成立

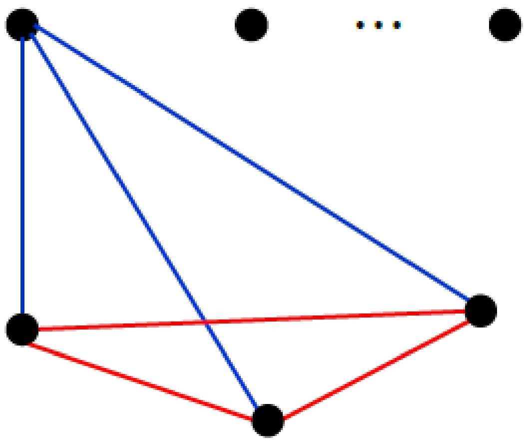


若为6：

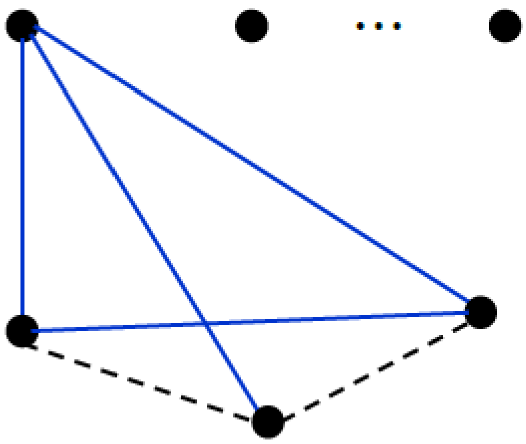
五条边一定有三条为蓝或三条为红



剩下三点连线可以全红，得证



也可以不全红，同样得证



$R(k,2)=k$

$R(s,t)\le R(s-1,t)+R(s,t-1)$

Proof. We show that $R(s,t)\le R(s-1,t)+R(s,t-1)$. To see this, let $n=R(s-1,t)+R(s,t-1)$ and consider any graph G on n vertices. Fix a vertex $v\in V$. We consider two cases:

- There are at least $R(s,t-1)$ edges incident with v. Then we apply induction on the neighbors of v, which implies that either they contain an independent set of size s, or a clique of size $t-1$. In the second case, we can extend the clique by adding v, and hence G contains either an independent set of size s or a clique of size t.
- There are at least $R(s-1,t)$ non-neighbors of v. Then we apply induction to the non-neighbors of v and we get either an independent set of size $s-1$, or a clique of size t. Again, the independent set can be extended by adding v and hence we are done.

应用概率方法

如果满足不等式，对size为n的完全图二着色，可能有一种着色方案不存在单色size为k的完全子图

Theorem. If $\binom{n}{k}2^{-\binom{k}{2}+1}<1$, then it is possible to color the edges of K_n with two colors so that it has no single-colored (monochromatic) $K_k$subgraphs.

应用union bound存在所有子图的交集<=所有存在子图概率和

- Proof.

For each $e = \{u, v\}$  $\begin{cases} \text{Head:} & f(e) = \text{RED} \\ \text{Tail:} & f(e) = \text{BLUE} \end{cases}$

A certain K_k subgraph is monochromatic: $= 2 \cdot \frac{1}{2^{\binom{k}{2}}}$

The probability that one of K_k subgraph is monochromatic: $\leq \binom{n}{k} \cdot 2 \cdot \frac{1}{2^{\binom{k}{2}}} = \binom{n}{k} 2^{-\binom{k}{2}+1}$

$< \mathbf{1}$

$k \geq 3, n = k/2, R(k,k) > 2^{k/2}$

Coloring set systems by two colors

任一子集（每个子集size都为k）都含两种颜色

- X is a finite set, $M \subseteq P(X)$.
- **Coloring function** $f: X \to \{\text{RED}, \text{BLUE}\}$
- **2-Colorability**. if there is a coloring function such that every $S \in M$ contains points of both colors. Then M is 2-colorable.

- **Example**. $X = \{1,2,3\}, M = \{\{1,2\},\{1,3\},\{2,3\}\}$ then M is not 2-colorable.

s(k)为最小的能够使得M不能二着色的集合数

证明：

任何size小于2^{k-1}的system都可能被两着色

Theorem. $s(k) \geq 2^{k-1}$, i.e. any system consisting of fewer than 2^{k-1} sets of size k admits a 2-coloring.

- Proof. $M \subseteq \binom{X}{k}$, $|M| = m$

For each $x \in X$  $\begin{cases} \text{Head:} & f(x) = \text{RED} \\ \text{Tail:} & f(x) = \text{BLUE} \end{cases}$

$S \in M$, the probability that S is single-colored is: $\frac{1}{2^k} + \frac{1}{2^k} = 2^{1-k}$

The probability that at least one of the m sets in M is *monochromatic (single-color)* is: $\leq m \cdot 2^{1-k}$

If $m < 2^{k-1}$ the probability is strictly less than 1.

Some M is 2-colorable. $\therefore s(k) \geq 2^{k-1}$.

期望 The Expectation Argument

Lemma: X

$E(X) = \mu$

then $\Pr(X \geq \mu) > 0$,

& $\Pr(X \leq \mu) > 0$.

Dense Partition

将图划分为两部分，使得两部分之间的边尽可能的多

存在划分使得至少有m/2个边在两部分之间

期望大于m/2，必有大于m/2的partition方法

Theorem. Let G be a graph with an even number, $2n$, of vertices and with $m > 0$ edges. Then the set $V = V(G)$ can be divided into two disjoint n-element subsets A and B in such a way that more than $\frac{m}{2}$ edges go between A and B.

Proof. Randomly choose n vertex to form set A.
Then $B = V \backslash A$.

For any edge $e = \{u, v\}$, the probability of e being lying 'across' A and B is: $\frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}$

$|E(G)| = m$, the expectation of the number of edges lying 'across' : $E(C(A,B)) = m \cdot \frac{n}{2n-1} > \frac{m}{2}$

There must exist a choice of A with more than half of the edges going across.

拉斯维加划分算法 A Las Vegas algorithm for finding an partition

根据上面分析，可以不断选择A集直到p发生，次数是1/p（几何分布）

Let $p = \Pr\left(C(A,B) \geq \frac{m}{2}\right)$,

$$\frac{m}{2} < E(C(A,B)) = \sum_{i \leq \frac{m}{2}-1} i \cdot \Pr(C(A,B) = i) + \sum_{i \geq \frac{m}{2}} i \cdot \Pr(C(A,B) = i)$$

$$\leq (1-p)\left(\frac{m}{2} - 1\right) + pm$$

$$\therefore\ p \geq \frac{1}{\frac{m}{2} + 1}$$

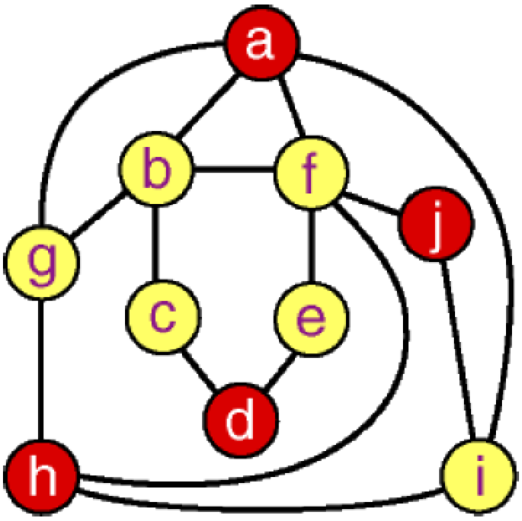
The expected number of samples before finding a cut with value at least $m/2$ is therefore just $\frac{m}{2} + 1$.

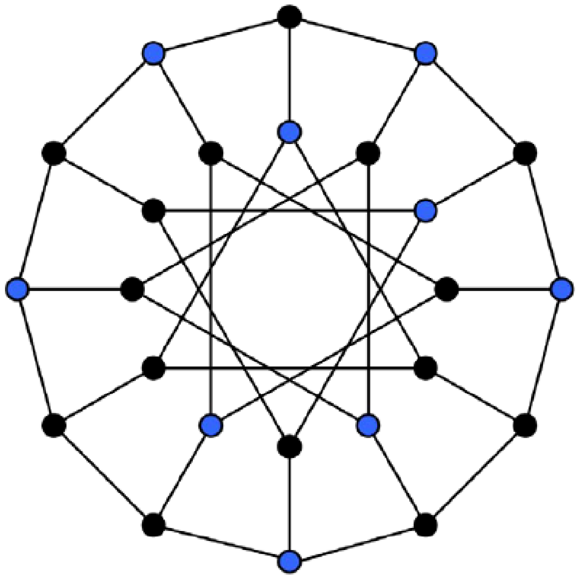
Sample and testing.

独立集 Independent set

独立集：取若干顶点，顶点之间没有边

红色点/蓝色点为独立集





找最大独立集是NPC

但可以找最大独立集的下界

Theorem. (Turàn's theorem). For any graph G on n vertices, we have $\alpha(G) \geq \frac{n^2}{2|E(G)|+n}$.
where $\alpha(G)$ denotes the size of the largest independent set of vertices in the graph G.

Lemma. For any graph G, we have

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{\deg_G(v)+1}.$$

V到V映射，找邻居都比自己大的点，这些点可组成独立集

- **Proof.** $V = \{1,2,\ldots,n\}$

  Randomly pick a permutation $\pi: \mathrm{V} \rightarrow V$,

  $M = M(\pi) \subseteq V = \{v \mid \forall u\ (\{u,v\} \in E(G) \rightarrow \pi(u) > \pi(v))\}$,

  $M(\pi)$ is an independent set in G, $\therefore$ for any π, $|M(\pi)| \leq \alpha(G)$.

  A_v: the event "$v \in M(\pi)$"

  $$P(A_v) = \frac{1}{1+|N_v|} = \frac{1}{\deg_G(v)+1}$$

  $$\alpha(G) \geq E(|M|) = \sum_{v \in V} E[I_{A_v}] = \sum_{v \in V} P(A_v) = \sum_{v \in V} \frac{1}{\deg_G(v)+1}$$

每个点度数相等时取极小值

$$\sum_{v\in V(G)} \frac{1}{\deg_G(v)+1}$$

will be minimal, when $d_1 = d_2 = \cdots = d_n = \frac{2|E(G)|}{n}$.

得证

Maximum Satisfaction 最大可满足

$$(x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee \overline{x_3}) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_4 \vee \overline{x_3}) \wedge (x_4 \vee \overline{x_1})$$

k为文字最少的子句，存在一种真值指派，最少可满足的子句数量有下界

Theorem. Given a set of m clauses, let k_i be the number of literals in the ith clause for $i = 1, \ldots, m$. Let $k = \min_{1\le i\le m} k_i$. Then there is a truth assignment that satisfies at least

$$\sum_{i=1}^{m}(1-2^{-k_i}) \geq m(1-2^{-k}).$$

- **Proof**

  Assign values independently and uniformly at random to the variables.

  The probability that the ith clause with k_i literals is satisfied is $1-2^{-k_i}$

  The expected number of satisfied clauses is $\sum_{i=1}^{m}(1-2^{-k_i}) \geq m(1-2^{-k})$.

Lovasz Local Lemma

事件间很难都相互独立，但是相互之间的dependency是limited

$E_1, E_2, \ldots, E_n$ is a set of bad events.

The probability that none of the bad events occurs is

$$\Pr\left(\bigcap_{i=1}^{n} \overline{E_i}\right)$$

相互独立和依赖图（只有相互独立的点之间无边）

一条边都没有就全部相互独立

Event F is mutually independent of the events $F_1, F_2, \dots, F_m$ if, for any subset $I \subseteq [1, n]$:

$$\Pr\left(F \mid \cap_{j \in I} F_j\right) = \Pr(F)$$

Dependency graph. for a set of events $E_1, E_2, \dots, E_n$, define graph $G = (V, E)$ such that $V = \{1,2, \dots, n\}$ and, for $i = 1, \dots, n$, event E_i is mutually independent of the events $\left\{E_j \mid (i, j) \notin E\right\}$.

每个事件发生的概率有上界

每个点都和至多d个点相互依赖

$4dp \geq 1$

所有坏事件都不发生的概率>0

Theorem[Lovasz Local Lemma]: Let $E_1, E_2, \dots, E_n$ be a set of events, and assume that the following hold:

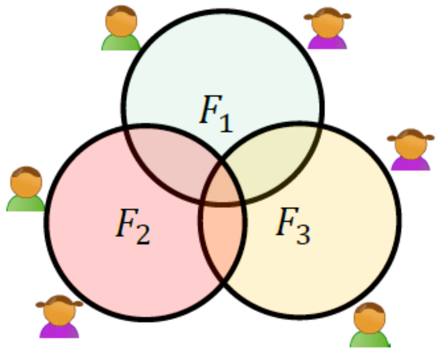
1. For all i, $\Pr(E_i) \leq p$;
2. The degree of the dependency graph given by $E_1, E_2, \dots, E_n$ is bounded by d;
3. $4dp \leq 1$.

Then $\Pr(\cap_{i=1}^{n} \bar{E}_i) > 0$.

应用 Edge-disjoint path

每对用户之间通讯链路有m条，不同对用户之间share的链路不超过k条

- Scenario
  - n pairs of users need to communicate using edge-disjoint paths on a given network.
  - Each pair $i = 1, \dots, n$ can choose a path from a collection F_i of m path (i.e. $|F_i| = m$).



Theorem: If any path in F_i shares edges with no more than k paths in F_j, where $i \neq j$ and $\frac{8nk}{m} < 1$, then there is a way to choose n edge-disjoint paths connecting the n pairs.

E_{ij}表示i对和j对用户间share了链路

E_{ij}与Eiy或E_{xj}之间有边，所以共与2n个E有边

存在一种可能所有的E都不发生，全部disjoint

Proof. Each pair i chooses a path independently and uniformly at random from F_i.

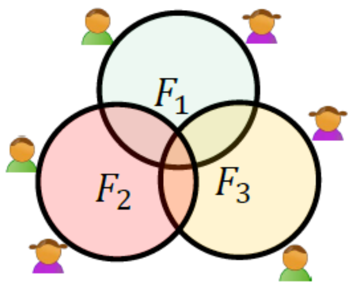
$E_{i,j}$: the event that the path chosen by pairs i and j share at least one edge.

Obviously, $p = \Pr(E_{i,j}) \leq \frac{k}{m}$,

Dependency graph, $d < 2n$.

$$4dp < \frac{8nk}{m} \leq 1$$

$\therefore$ $\Pr\left(\bigcap_{i \neq j} \overline{E_{i,j}}\right) > 0$ by Lovasz local lemma.



应用 Satisfiability

If no variable in a k −SAT formula appears in more than $T = \frac{2^k}{4k}$ clauses, then the formula has a satisfying assignment.

Proof.

- E_i: the ith clause is not satisfied.
- $p = 2^{-k}$, $d \le k \cdot T \le 2^{k-2}$

Ch 07 随机图 Introduction to Random Graphs

$G(n, p)$大小为n的顶点集，每条边的概率都为p

例子

K服从二项分布 np np(1-p)

Example: $G(n, 1/2)$

$$K = \deg(v)$$

$$\Pr(K = k) = \binom{n-1}{k}\left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^{n-k}$$

$$\approx \binom{n}{k}\left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^{n-k} = \frac{1}{2^n}\binom{n}{k}$$

$$E(K) = n/2$$

$$Var(K) = n/4$$

Independence!

Binomial Distribution

- $G(n, 1/2)$

$$\mu = n\mu' = E(K) = \frac{n}{2},$$

$$\sigma^2 = n(\sigma')^2 = Var(K) = n/4$$

中心极限定理 Central Limit Theorem

n足够大时，n个独立同分布的随机变量和能够收敛。

任意分布都能够用高斯分布来逼近，取值非常接近均值

Normal distribution (Gauss Distribution):

$X \sim N(\mu, \sigma^2)$, with density function:

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \qquad -\infty < x < +\infty$$

As long as $\{X_i\}$ is independent identically distributed with $E(X_i) = \mu$, $D(X_i) = \sigma^2$, then $\sum_{i=1}^{n} X_i$ can be approximated by normal distribution $(n\mu, n\sigma^2)$ when n is large enough.

$$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(k-n\mu)^2}{2\sigma^2}} = \frac{1}{\sqrt{\pi n/2}} e^{-\frac{(k-n/2)^2}{n/2}}$$

G(n, p)中的独立集和团集 independent set and clique

Lemma. For all integers n, k with $n \geq k \geq 2$; the probability that $G \in \boldsymbol{G}(n,p)$ has a set of k independent vertices is at most

$$\Pr(\alpha(G) \geq k) \leq \binom{n}{k}(1-p)^{\binom{k}{2}}$$

the probability that $G \in \boldsymbol{G}(n,p)$ has a set of k clique is at most

$$\Pr(\omega(G) \geq k) \leq \binom{n}{k}(p)^{\binom{k}{2}}$$

G(n, p)中的环 cycle

Lemma. The expected number of k −cycles in $G \in \boldsymbol{G}(n,p)$ is $E(x) = \frac{(n)_k}{2k} p^k$.

Proof. The expectation of certain n vertices $v_0, v_1, \cdots, v_{k-1}, v_0$ form a length k cycle is: p^k

The possible ways to choose k vertices to form a cycle C is $\frac{(n)_k}{2k}$.

The expectation of the number of all cycles:

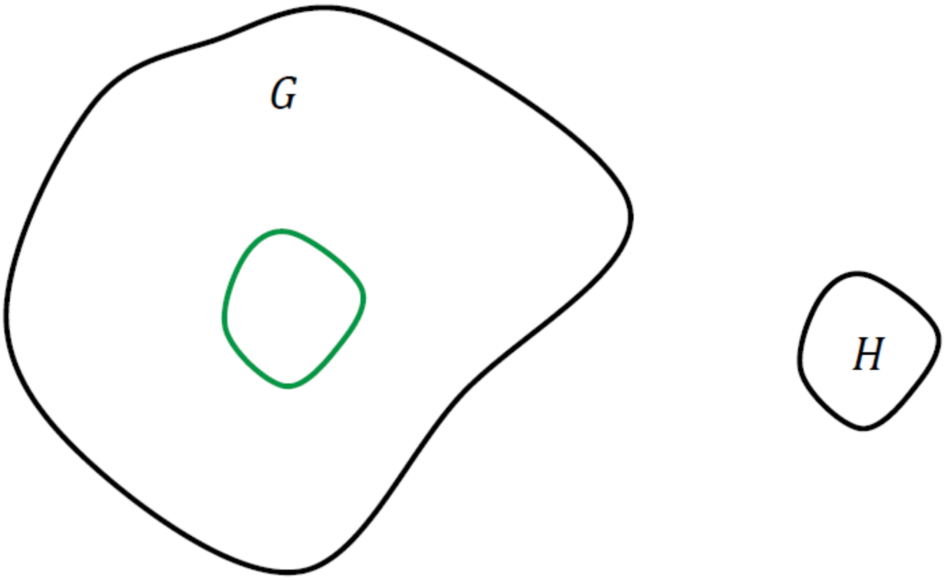
$$X = \sum_C X_C = \frac{(n)_k}{2k} p^k$$

几乎所有图都有的性质 Properties of almost all graphs

图size n无限大时，有些property发生概率近似1,；有些property发生概率近似0

Gnp size足够大时几乎一定含有一个给定子图

Proposition. For every constant $p \in (0,1)$ and every graph H, almost every $G \in \boldsymbol{G}(n,p)$ contains an induced copy of H.



Proof. $V(G) = \{v_0, v_1, \dots, v_{n-1}\}, k = |H|$

Fix some $U \in \binom{V(G)}{k}$, then $\Pr(U \cong H) = r > 0$

r depends on p, k not on n.

There are $\lfloor n/k \rfloor$ disjoint such U.

The probability that none of the $G[U]$ is isomorphic to H is: $= (1-r)^{\lfloor n/k \rfloor}$

$\Pr[\neg(H \subseteq G \text{ induced})]$: $\leq (1-r)^{\lfloor n/k \rfloor}$

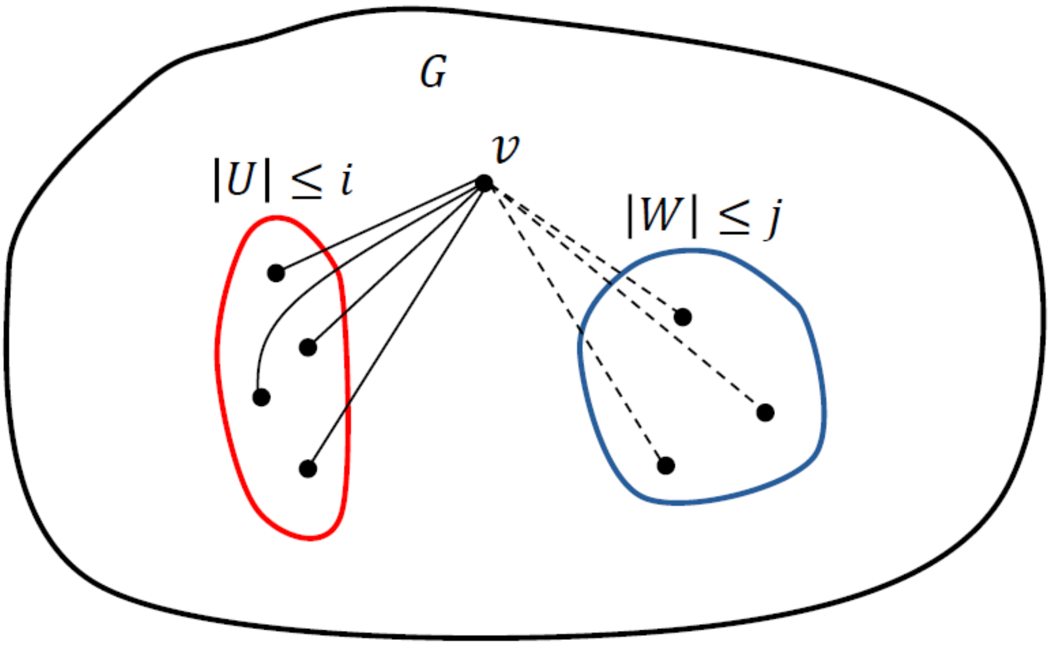
$$\Big\downarrow n \to \infty$$

$$0$$

$P_{i,j}$

能找到顶点v，可以和最多i个顶点相连，最多j个顶点不相连

Proposition. For every constant $p \in (0,1)$ and $i, j \in N$, almost every graph $G \in \boldsymbol{G}(n,p)$ has the property $P_{i,j}$.



16

指数降得比多项式快

Proof. Fix U, W and $v \in G - (U \cup W)$, $q = 1 - p$,

The probability that $P_{i,j}$ holds for v: $p^{|U|} q^{|W|} \ge p^i q^j$

The probability there's no such v for chosen U, W:

$$= \left(1 - p^{|U|} q^{|W|}\right)^{n-|U|-|W|} \le \left(1 - p^i q^j\right)^{n-i-j}$$

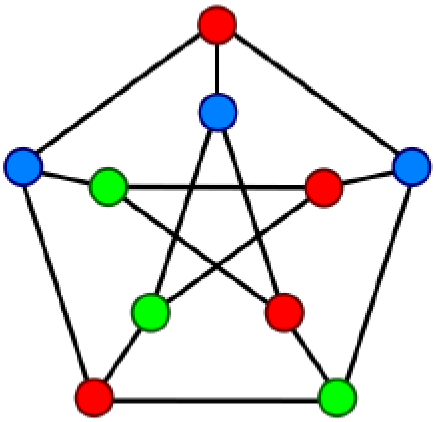
The upper bound for the number of different choice of U, W: n^{i+j}

The probability there exists some U, W without suitable v:

$$\le n^{i+j} \left(1 - p^i q^j\right)^{n-i-j} \xrightarrow{n \to \infty} 0$$

顶点着色 Colouring

给定一个图，相邻顶点不同色，求最小着色数是一个NPC



$\chi(G) = 3$

所有随机图最小着色数有下界

几乎一定不存在size超过k的独立集，没有k个顶点可以着同一颜色

Proposition. For every constant $p \in (0,1)$ and every $\epsilon > 0$, almost every graph $G \in \boldsymbol{G}(n,p)$ has chromatic number $\chi(G) > \frac{\log(1/q)}{2+\epsilon} \cdot \frac{n}{\log n}$

Proof. The size of the maximum independent set in G: $\alpha(G)$

$$\Pr(\alpha(G) \geq k) \leq \binom{n}{k} q^{\binom{k}{2}} \leq n^k q^{\binom{k}{2}}$$

$$= q^{k\frac{\log n}{\log q} + \frac{1}{2}k(k-1)} = q^{\frac{k}{2}\left(-\frac{2\log n}{\log(1/q)} + k - 1\right)}$$

(*)

Take $k = (2+\epsilon)\frac{\log n}{\log(1/q)}$ then (*) tends to ∞ with n.

$\therefore \Pr(\alpha(G) \geq k) \xrightarrow{n\to\infty} 0 \Rightarrow$ No k vertices can have the same colour.

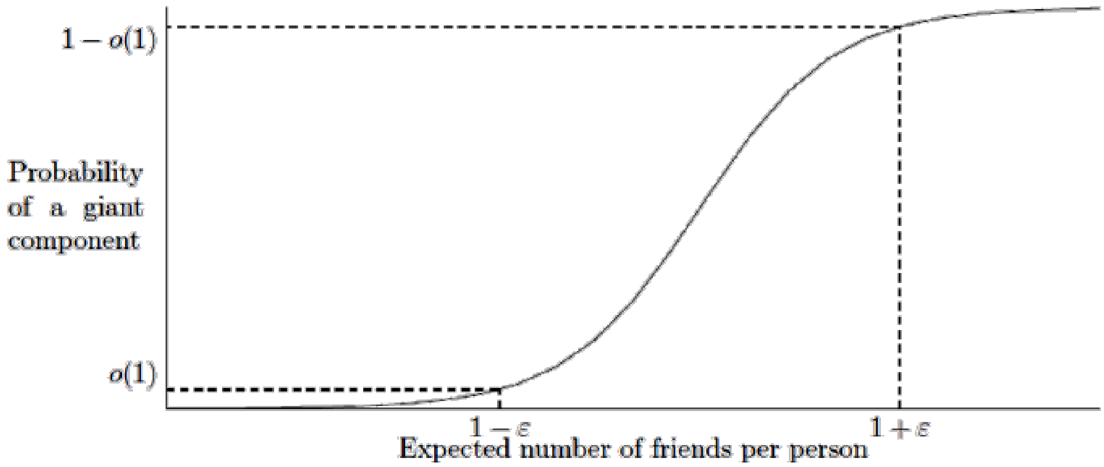
$$\therefore \chi(G) > \frac{n}{k} = \frac{\log(1/q)}{2+\epsilon} \cdot \frac{n}{\log n}$$

20

Phase transition

$G(n,p)$讨论全局性质

存在阈值现象



p(n)为阈值

Definition. If there exists a function $p(n)$ such that

– when $\lim_{n\to\infty}\left(\frac{p_1(n)}{p(n)}\right)=0$, $\boldsymbol{G}(n, p_1(n))$ almost surely does not have the property.

– when $\lim_{n\to\infty}\left(\frac{p_2(n)}{p(n)}\right)=\infty$, $\boldsymbol{G}(n, p_2(n))$ almost surely has the property.

Then we say phase transition occurs and $p(n)$ is the threshold.

Every increasing property has a threshold.

Probability	Transition
$p = o(\frac{1}{n})$	Forest of trees, no component of size greater than $O(\log n)$
$p = \frac{d}{n}, d < 1$	All components of size $O(\log n)$
$p = \frac{d}{n}, d = 1$	Components of size $O(n^{\frac{2}{3}})$
$p = \frac{d}{n}, d > 1$	Giant component plus $O(\log n)$ components
$p = \sqrt{\frac{2\ln n}{n}}$	Diameter two
$p = \frac{1}{2}\frac{\ln n}{n}$	Giant component plus isolated vertices
$p = \frac{\ln n}{n}$	Disappearance of isolated vertices Appearance of Hamilton circuit Diameter $O(\log n)$
$p = \frac{1}{2}$	Clique of size $(2-\epsilon)\ln n$

First moment method 几乎不发生

Markov's Inequality: Let x be a random variable that assumes only nonnegative values. Then for all $a > 0$

$$\Pr(x \geq a) \leq \frac{\boldsymbol{E}[x]}{a}$$

First moment method : for non-negative, integer valued variable x

$$\Pr(x > 0) = \Pr(x \geq 1) \leq \boldsymbol{E}(x)$$

$$\therefore \ \Pr(x = 0) = 1 - \Pr(x > 0) \geq 1 - \boldsymbol{E}(x)$$

期望为0，一定不发生；期望不为0，不一定发生

期望无限大，但是随机抽取到的概率仍然无限趋近于0

- If the expectation goes to 0: the property almost surely does not happen.
- If the expectation does not goes to 0:

  e.g. Expectation = $\frac{1}{n} \times n^2 + \frac{n-1}{n} \times 0 = n$

  i.e., a *vanishingly small* fraction of the sample contribute a lot to the expectation.

Second moment method 几乎一定发生

描述x不发生的概率为0

前提也可以是 $E(x^2) \leq E^2(x) \ (1 + o(1))$

Theorem. Let $x(n)$ be a random variable with $\boldsymbol{E}(x) > 0$. If

$$Var(x) = o\left(\boldsymbol{E}^2(x)\right)$$

Then x is almost surely greater than zero.

Proof. If $\boldsymbol{E}(x) > 0$, then for $x \le 0$,

$$\Pr(x \le 0) \le \Pr(|x - \boldsymbol{E}(x)| \ge \boldsymbol{E}(x))$$

$$\le \frac{Var(x)}{E^2(x)} \to 0$$

diameter two证明

diameter 任意两点之间最短距离的最大值

sharp threshold $c\,p(n) \begin{cases} c<1 \\ c>1 \end{cases}$

取1时两点之间最短距离>2

Theorem. The property that $\boldsymbol{G}(n,p)$ has diameter two has a sharp threshold at $p = \sqrt{2}\sqrt{\frac{\ln n}{n}}$

Proof. For any two different vertices $i < j$,

$$I_{ij} = \begin{cases} 1 & \{\mathrm{i,j}\} \notin E, \text{no other vertex is adjacent to both } i \text{ and } j \\ 0 & otherwise \end{cases}$$

$$x = \sum_{i<j} I_{ij}$$

If $\boldsymbol{E}(x) \xrightarrow{n\to\infty} 0$, then for large n, almost surely the diameter is at most two.

使用First moment method证明一定不发生：

$$\boldsymbol{E}(x) = \binom{n}{2}(1-p)(1-p^2)^{n-2}$$

Take $p = c\sqrt{\frac{\ln n}{n}}$, $E(x) \cong \frac{n^2}{2}\left(1 - c\sqrt{\frac{\ln n}{n}}\right)\left(1 - c^2\frac{\ln n}{n}\right)^n$

$$\cong \frac{n^2}{2}e^{-c^2 \ln n} = \frac{1}{2}n^{2-c^2}$$

$c > \sqrt{2}$，n无穷大时，期望几乎为0，一定不发生；

使用Second moment method证明一定发生：

If $Var(x) = o\left(\boldsymbol{E}^2(x)\right)$, then for large n, almost surely the diameter will be larger than two.

三种情况

$$\boldsymbol{E}(x^2) = \boldsymbol{E}\left(\sum_{i<j} I_{ij}\right)^2 = \boldsymbol{E}\left(\sum_{i<j} I_{ij} \sum_{k<l} I_{kl}\right) = \boldsymbol{E}\left(\sum_{\substack{i<j \\ k<l}} I_{ij} I_{kl}\right) = \sum_{\substack{i<j \\ k<l}} \boldsymbol{E}(I_{ij} I_{kl})$$

$$a = |\{i, j, k, l\}|$$

$$\boldsymbol{E}(x^2) = \sum_{\substack{i<j \\ k<l \\ a=4}} \boldsymbol{E}(I_{ij} I_{kl}) + \sum_{\substack{i<j \\ i<k \\ a=3}} \boldsymbol{E}(I_{ij} I_{ik}) + \sum_{\substack{i<j \\ \\ a=2}} \boldsymbol{E}(I_{ij}^2)$$

36

四个顶点完全不重合：

ij不能有边，kl不能有边，ij不能与u都相连；kl不能与u都相连（可以一条红边一条紫边）

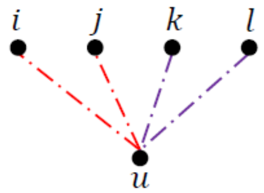
n-4表示u的取法

不考虑前两种，用<=

$$\boldsymbol{E}(x^2) = \boxed{\sum_{\substack{i<j \\ k<l \\ a=4}} \boldsymbol{E}(I_{ij} I_{kl})} + \sum_{\substack{i<j \\ i<k \\ a=3}} \boldsymbol{E}(I_{ij} I_{ik}) + \sum_{\substack{i<j \\ \\ a=2}} \boldsymbol{E}(I_{ij}^2)$$

$$\boldsymbol{E}(I_{ij} I_{kl}) \le (1-p^2)^{2(n-4)} \le \left(1 - c^2 \frac{\ln n}{n}\right)^{2n} (1+o(1)) \le n^{-2c^2}(1+o(1))$$

$$\sum_{\substack{i<j \\ k<l \\ a=4}} \boldsymbol{E}(I_{ij} I_{kl}) \le n^{4-2c^2}(1+o(1))$$



37

三个顶点：

ui存在，ju和ku都不存在；ui不存在，任意

n-3表示u的取法

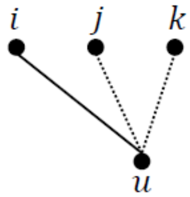
$$E(x^2) = \sum_{\substack{i<j\\k<l\\a=4}} E(I_{ij}I_{kl}) + \boxed{\sum_{\substack{i<j\\i<k\\a=3}} E(I_{ij}I_{ik})} + \sum_{\substack{i<j\\ \\a=2}} E(I_{ij}^2)$$

$$\Pr(I_{ij}I_{ik}=1) \le 1-p+p(1-p)^2 = 1-2p^2+p^3 \approx 1-2p^2$$

$$E(I_{ij}I_{ik}) \le (1-2p^2)^{n-3} = \left(1-\frac{2c^2\ln n}{n}\right)^{n-3}$$

$$\cong e^{-2c^2\ln n} = n^{-2c^2}$$

$$\sum_{\substack{i<j\\i<k}} E(I_{ij}I_{ik}) \le n^{3-2c^2}$$



39

两个顶点：

$$E(x^2) = \sum_{\substack{i<j\\k<l\\a=4}} E(I_{ij}I_{kl}) + \sum_{\substack{i<j\\i<k\\a=3}} E(I_{ij}I_{ik}) + \boxed{\sum_{\substack{i<j\\ \\a=2}} E(I_{ij}^2)}$$

$$E(I_{ij}^2) = E(I_{ij})$$

$$\sum_{ij} E(I_{ij}^2) = E(x) \cong \frac{1}{2}n^{2-c^2}$$

40

可以得到

$$E(x^2) \le E^2(x)(1+o(1))$$

应用Second moment method得到结论

Increasing property

随着边被加进来，property发生的概率变大

任何一个Increasing property都有threshold

证明：如果为Increasing property。那么边的概率增加，property概率变大

通过拆分为两个模型

q>p，那么q的边一定比p多

Lemma: If Q is an increasing property of graphs and $0 \le p \le q \le 1$, then the probability that $\boldsymbol{G}(n,q)$ has property Q is greater than or equal to the probability that $\boldsymbol{G}(n,p)$ has property Q.

Proof:

Independently generate graph $\boldsymbol{G}(n,p)$ and $\boldsymbol{G}(n,\frac{q-p}{1-p})$.

$H = \boldsymbol{G}(n,p) \cup \boldsymbol{G}(n,\frac{q-p}{1-p})$ (the union of the edge set).

Graph H has the same distribution as $\boldsymbol{G}(n,q)$:

$$\Pr(\{u,v\} \in E(H)) = p + (1-p)\frac{q-p}{1-p} = q.$$

And edges in H are independent.

The result follows naturally.

Replication

mp的property概率要大于做m-fold的property概率

m-fold replication of $\boldsymbol{G}(n,p)$:

– Independently generate m copies of $\boldsymbol{G}(n,p)$ (on the same vertex set);

– Take the union of the m copies;

The result graph H has the same distribution as $G(n,q)$, where $q = 1-(1-p)^m$.

One of the copies of $\boldsymbol{G}(n,p)$ has the increasing property

$$\downarrow$$

$G(n,q)$ has the increasing property.

As $q \le 1-(1-mp) = \boldsymbol{mp}$

$$\therefore \Pr(\boldsymbol{G}(n,\boldsymbol{mp})\text{has } Q) \ge \Pr(\boldsymbol{G}(n,q)\text{has } Q)$$

一定存在1/2的phase transition

所有increasing transition都有phase transition，即最小实数能够使得有property的概率为1/2

先证明阈值函数p(n)不是p_0的threshold

即在无限个n取值上有property的概率都大于某一常数

Theorem: Every increasing property Q of $\boldsymbol{G}(n,p)$ has a phase transition at $p(n)$, where for each n, $p(n)$ is the minimum real number a_n for which the probability that $\boldsymbol{G}(n,a_n)$ has property Q is $\frac{1}{2}$.

Proof:

First prove that for any function $p_0(n)$ with $\lim_{n\to\infty}\frac{p_0(n)}{p(n)}=0$, almost surely $\boldsymbol{G}(n,p_0)$ does not have the property Q.

Suppose otherwise: the probability that $\boldsymbol{G}(n,p_0)$ has the property Q *does not converge to 0*.

Then there exists $\epsilon>0$ for which the probability that $\boldsymbol{G}(n,p_0)$ has the property Q is $\geq \epsilon$ on an infinite set I of n. Let $m=\lceil(1/\epsilon)\rceil$ 6

做m-fold

Let $\boldsymbol{G}(n,q)$ be the m-fold replication of $\boldsymbol{G}(n,p_0)$.

For all $n\in I$, the probability that $\boldsymbol{G}(n,q)$ does not have Q : $\leq(1-\epsilon)^m\leq e^{-1}\leq 1/2$

$$\Pr(\boldsymbol{G}(n,\boldsymbol{mp_0})\text{has }Q)\geq\Pr(\boldsymbol{G}(n,q)\text{has }Q)\geq 1/2$$

As $p(n)$ is the minimum real number a_n for which $\Pr(\boldsymbol{G}(n,a_n)\text{has }Q)=\frac{1}{2}$, it follows that $\boldsymbol{mp_0(n)}\geq p(n)$.

$\therefore\ \frac{\boldsymbol{p_0(n)}}{p(n)}\geq\frac{1}{m}$ infinitely often.

Contradict to the fact that $\lim_{n\to\infty}\frac{p_0(n)}{p(n)}=0$.

7

Secondly prove that for any function $p_1(n)$ with $\lim_{n\to\infty}\frac{p(n)}{p_1(n)}=0$, almost surely $\boldsymbol{G}(n,p_1)$ almost surely has the property Q.

Ch 08 高维空间 High Dimensional Space

大数定律 Law of Large Numbers

同一试验重复了很多次，结果的均值应该接近期望

Let $x_1, x_2, \ldots, x_n$ be n independent samples of a random variable x, then

$$\Pr\left(\left|\frac{x_1 + x_2 + \cdots x_n}{n} - E(x)\right| \geq \epsilon\right) \leq \frac{Var(x)}{n\epsilon^2}$$

Proof. (Chebychev's Inequality)

$$\Pr\left(\left|\frac{x_1 + x_2 + \cdots x_n}{n} - E(x)\right| \geq \epsilon\right) \leq \frac{Var(\frac{x_1 + x_2 + \cdots x_n}{n})}{\epsilon^2} = \frac{Var(x_1 + x_2 + \cdots x_n)}{n^2\epsilon^2} = \frac{Var(x)}{n\epsilon^2}$$

6

$D(X) = E(X^2) - [E(X)]^2$

应用

高维样本模长接近于d

很难在单位球内找到样本

- $\boldsymbol{x}$ be a d −dimensional random point whose coordinates are each selected from $N\left(0, \frac{1}{2\pi}\right)$,
- i.e. $\boldsymbol{x} = [x_1, x_2, \ldots, x_d]$ with $x_i \sim N\left(0, \frac{1}{2\pi}\right)$
- By LLN: $|\boldsymbol{x}|^2 = \sum_{i=1}^{d} x_i^2 = \frac{d}{2\pi} = \Theta(d)$ with high probability.
- The probability that point $\boldsymbol{x}$ lie in the unit ball is *vanishingly small*.

任意两个随机样本，非常大的概率正交

- $\boldsymbol{x}, \boldsymbol{y}$: $[z_1, z_2, \ldots, z_d]$ with $z_i \sim N(0, 1)$
- $|\boldsymbol{x}|^2 \approx d, |\boldsymbol{y}|^2 \approx d,$
- $|\boldsymbol{x} - \boldsymbol{y}|^2 = \sum_{i=1}^{d}(x_i - y_i)^2 = 2d$

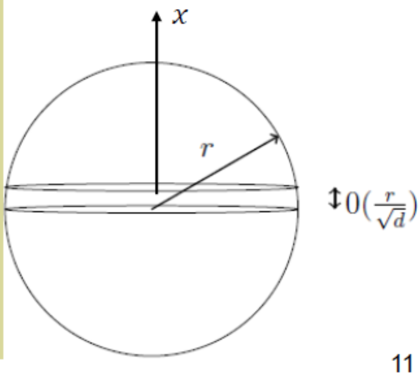
$$\boldsymbol{E}(x_i - y_i)^2 = \boldsymbol{E}(x_i^2) + \boldsymbol{E}(y_i^2) - 2\boldsymbol{E}(x_i y_i)$$
$$= 1 + 1 - 2\boldsymbol{E}(x_i)\boldsymbol{E}(y_i) = 2.$$

- $|\boldsymbol{x} - \boldsymbol{y}|^2 \approx |\boldsymbol{x}|^2 + |\boldsymbol{y}|^2$
- Pythagorean theorem ⇒ random d −dimensional $\boldsymbol{x}, \boldsymbol{y}$ are approximately orthogonal.

10

任选一个作为北极，任意数据y都非常高的概率在赤道上一个很小范围内

- $\boldsymbol{x}, \boldsymbol{y}$: $[z_1, z_2, \ldots, z_d]$ with $z_i \sim N(0, 1)$
- Pythagorean theorem ⇒ random d −dimensional $\boldsymbol{x}, \boldsymbol{y}$ are approximately orthogonal.
- If we scale these random points to be unit length and call $\boldsymbol{x}$ the North Pole, *much of the surface area of the unit ball must lie near the equator.*

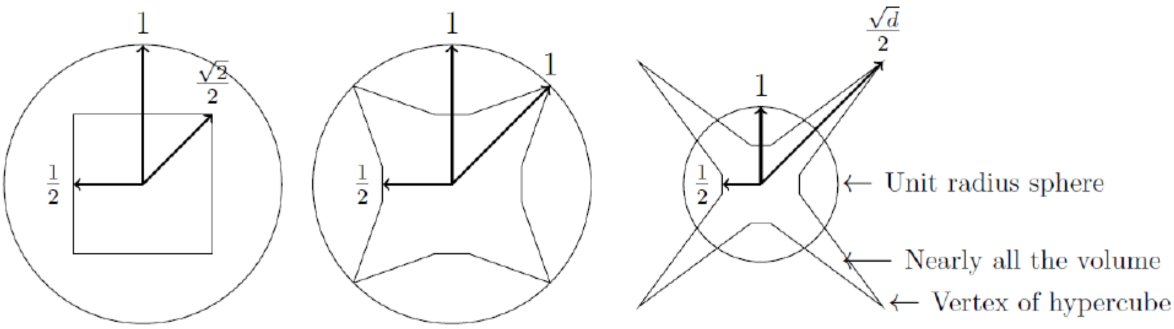


11

高维空间与单位球 Properties of High Dimensional space, unit ball

单位方：$x_i \leq 1/2$

高维下，单位方几乎所有体积都在单位球之外，任意生成一个样本，很难处于单位球内



The difference between the volume of a cube with unit-length sides and the volume of a unit-radius sphere at the dimensions: $2, 4$ and d.

高维空间几何 Geometry of High Dimensions

几乎所有样本都分布在高维空间的surface上

用无限个d维立方体去逼近体积

- Most of the volume of the high-dimensional objects is near the surface:

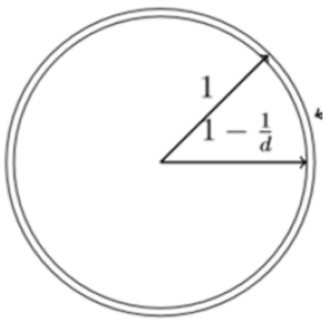
$$\frac{Volume\big((1-\epsilon)A\big)}{Volume(A)} = (1-\epsilon)^d \le e^{-\epsilon d}$$

Fix ϵ and letting $d \to \infty$, the above quantity rapidly approaches zero.

- **Application:**

S be the unit ball in d −dimensions (i.e., the set of points within distance 1 of the origin). Then $1 - e^{-\epsilon d}$ fraction of the volume is in $S \backslash (1-\epsilon)S$.

Especially, consider $\epsilon = \frac{1}{d}$.



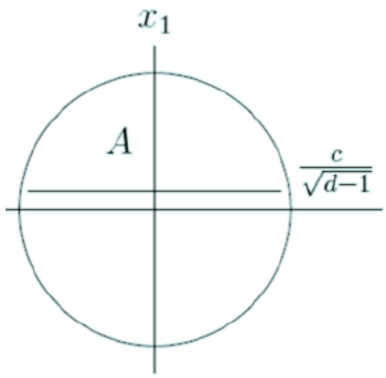
16

高维空间中的单位球 Unit ball in d−dimensions

高维空间中，单位球体积近似为0

- Surface: $A(d)=\frac{2\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}\right)}$, Volume: $V(d)=\frac{2}{d}\frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}\right)}$.
- $V(2)=\pi, V(3)=\frac{4}{3}\pi$, $\lim_{n\to\infty} V(d)=0.$
- Most of the volume of a unit ball in high dimensions is concentrated near its equator no matter which direction is defined to be the North Pole.

Theorem: For $c \geq 1$ and $d \geq 3$, at least a $1-\frac{2}{c}e^{-c^2/2}$ fraction of the volume of the d −dimensional unit ball has $|x_1| \leq \frac{c}{\sqrt{d-1}}$.



17

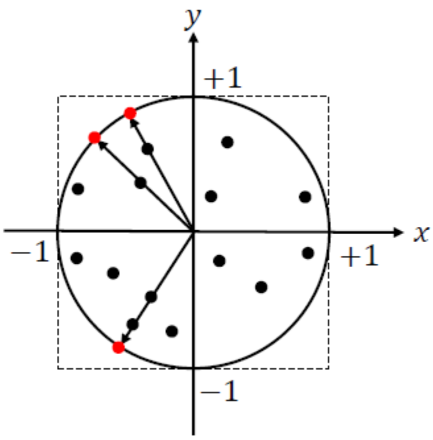
数据生成 Generating points uniformly at random from a ball

二维圆环上均匀采样

在正方形内随机生成，去掉圆外点，映射到圆环上

高维球体上无法做，因为删掉点之后内部的点几乎没有。应该用球状高斯分布然后正则化

- $d=2$
  - Generate x_i, y_i u.a.r from the interval $[-1,1]$;
  - Discard the points outside the unit circle;
  - Project the remaining points onto the circle.
- How about d is large?
  - The above strategy would fail. (why?)
  - ① Surface: Spherical normal distribution + Normalizing.
  - ② Surface+interior: Scale the point on the surface.



高维高斯分布 Gaussians in High Dimension

d维球状高斯分布 d−dimensional spherical Gaussian

每个维度都符合高斯分布，对每个维度做乘积

$$p(x) = \frac{1}{(2\pi)^{d/2}\sigma^d} exp\left(-\frac{|x|^2}{2\sigma^2}\right)$$

压缩算法 Random Projection and Johnson Lindenstrauss Lemma

寻找最近邻居问题，可以遍历，但是在高维上不可行，多项式算法维度太高

压缩算法：维度降低但是结果接近

定义投射函数

随机生成k个d维向量，与向量做内积，将d维降维k维

- Pick k vectors $\boldsymbol{u_1}, \boldsymbol{u_2}, \ldots, \boldsymbol{u_k}$, independently from the Gaussian distribution $\frac{1}{(2\pi)^{d/2}\sigma^d} exp\left(-\frac{|x|^2}{2\sigma^2}\right)$, for any vector $\boldsymbol{v}$, the projection $f: R^d \rightarrow R^k$ is:

$$f(\boldsymbol{v}) = (\boldsymbol{u_1} \cdot \boldsymbol{v}, \boldsymbol{u_2} \cdot \boldsymbol{v}, \ldots, \boldsymbol{u_k} \cdot \boldsymbol{v})$$

线性性且成正比

- $f(v_1 - v_2) = f(v_1) - f(v_2)$
- $|f(v)| \approx \sqrt{k}|v|$ w.h.p.
- To estimate $|v_1 - v_2|$, it suffices to compute $|f(v_1) - f(v_2)|$

Johnson Lindenstrass Lemma

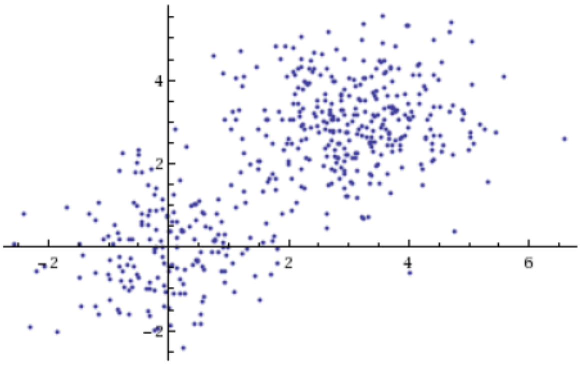
指数压缩

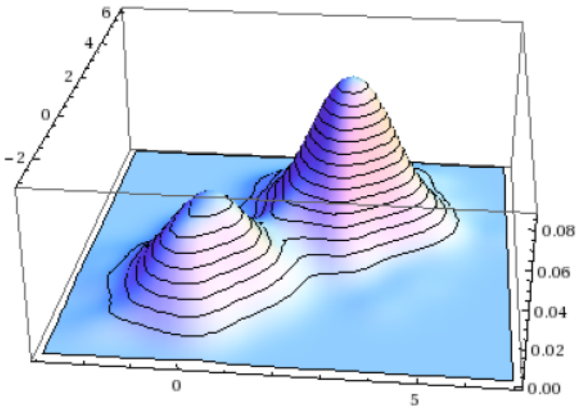
- For any $0 < \epsilon < 1$ and any integer n, let $k \geq \frac{3}{c\epsilon^2} \ln n$ for c as in the Gaussian Annulus theorem, for any set of n points in R^d, the random projection f defined above has the property that for all pairs of points v_i and v_j, with probability at least $1 - \frac{1.5}{n}$

数据分类 Separating Gaussians

估计参数

$p(x) = w1p_1(x) + w2p_2(x)$



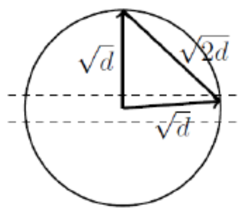


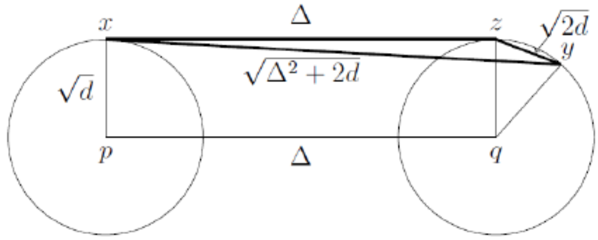
- Mixtures of Gaussians
- Parameter estimation problem

如果期望相差比较大，那么可以分开

Δ满足条件，就可以分开不同类别

When $\Delta \in \Omega(d^{1/4})$





Algorithm for separating points from two Gaussians: Calculate all pairwise distance between points. The cluster of smallest pairwise distances must come from a single Gaussian. Remove these points. The remaining points come from the second Gaussian.

Ch 09 最优子空间和SVD Best-fit subspaces and Singular Value Decomposition

最优子空间：找到给定维度的子空间，使得与原数据distance最小

特征值和特征向量 Eigenvalues & Eigenvectors

m阶矩阵至多只有m个

- **Eigenvectors** (for a square $m \times m$ matrix $\mathbf{S}$)

$$\mathbf{S}\mathbf{v} = \lambda\mathbf{v}$$

(right) eigenvector $\mathbf{v} \in \mathbb{R}^m \neq \mathbf{0}$

eigenvalue $\lambda \in \mathbb{R}$

Example

$$\begin{pmatrix} 6 & -2 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$\mathbf{S}\mathbf{v} = \lambda\mathbf{v} \iff (\mathbf{S} - \lambda\mathbf{I})\,\mathbf{v} = \mathbf{0}$$

- **How many eigenvalues** are there at most?

only has a non-zero solution if $|\mathbf{S} - \lambda\mathbf{I}| = 0$

this is a m-th order equation in λ which can have **at most m distinct solutions** (roots of the characteristic polynomial) - can be complex even though S is real.

用处

小特征值的可以舍掉，因为影响也很小

$$S = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

has eigenvalues 3, 2, 0 with corresponding eigenvectors

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

On each eigenvector, S acts as a multiple of the identity matrix: but as a different multiple on each.

Any vector (say $x=\begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix}$) can be viewed as a combination of the eigenvectors: $x = 2v_1 + 4v_2 + 6v_3$

Thus a matrix-vector multiplication such as Sx (S, x as in the previous slide) can be rewritten in terms of the eigenvalues/vectors:

$$Sx = S(2v_1 + 4v_2 + 6v_3)$$

$$Sx = 2Sv_1 + 4Sv_2 + 6Sv_3 = 2\lambda_1 v_1 + 4\lambda_2 v_2 + 6\lambda_3 v_3$$

Even though x is an arbitrary vector, the action of S on x is determined by the eigenvalues/vectors.

Suggestion: the effect of “small” eigenvalues is small.

对称矩阵的不同的特征值对应的特征向量正交

$$S\alpha_1 = \lambda_1\alpha_1$$

$$\alpha_1^T \underbrace{S^T\alpha_2}_{\substack{\| \\ S\alpha_2 \\ = \lambda_2\alpha_2}} = \lambda_1\alpha_1^T\alpha_2$$

$$\Rightarrow \lambda_2\alpha_1^T \alpha_2 = \lambda_1\alpha_1^T\alpha_2$$

$$\Rightarrow (\underline{\lambda_1 - \lambda_2})\alpha_1^T\alpha_2 = 0$$

对称矩阵特征值为实数

$$Ax = \lambda x \Rightarrow x = y + iz \Rightarrow \lambda = \frac{y^TAy + z^TAz}{y^Ty + z^Tz} \in R$$

半正定矩阵，特征值一定非负

任意向量w

$$\forall w \in \Re^n, w^T S w \geq 0, \text{ then if } Sv = \lambda v \Rightarrow \lambda \geq 0$$

例子-半正定的对称矩阵

- Let $S = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ ← Real, symmetric.

- Then

$$S - \lambda I = \begin{bmatrix} 2-\lambda & 1 \\ 1 & 2-\lambda \end{bmatrix} \Rightarrow (2-\lambda)^2 - 1 = 0.$$

- The eigenvalues are 1 and 3 (nonnegative, real).
- The eigenvectors are orthogonal (and real):

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Plug in these values and solve for eigenvectors.

特征分解 Eigen/diagonal Decomposition

U为特征向量组合成的矩阵

- Let $\mathbf{S} \in \mathbb{R}^{m \times m}$ be a **square** matrix with $\boldsymbol{m}$ **linearly independent eigenvectors** (a "non-defective" matrix)
- **Theorem**: Exists an **eigen decomposition**

$$\boxed{\mathbf{S} = \mathbf{U}\underbrace{\boldsymbol{\Lambda}}_{\text{diagonal}}\mathbf{U}^{-1}}$$

- Columns of ***U*** are **eigenvectors** of ***S***
- Diagonal elements of $\boldsymbol{\Lambda}$ are **eigenvalues** $\mathbf{S}$ of

$$\boldsymbol{\Lambda} = \mathrm{diag}(\lambda_1, \ldots, \lambda_m), \quad \lambda_i \geq \lambda_{i+1}$$

例子

Recall $S = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}; \qquad \lambda_1 = 1, \lambda_2 = 3.$

The eigenvectors $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ form $U = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$

Inverting, we have $U^{-1} = \begin{bmatrix} 1/2 & -1/2 \\ 1/2 & 1/2 \end{bmatrix}$

Recall $UU^{-1} = I$.

Then, $\boldsymbol{S=U\Lambda U^{-1}} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1/2 & -1/2 \\ 1/2 & 1/2 \end{bmatrix}$

可以做标准正交化

$$\begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$$

Symmetric Eigen Decomposition

If $\mathrm{S} \in \mathbb{R}^{m \times m}$ is a **symmetric** matrix:

Theorem: Exists a (unique) **eigen decomposition** $S = Q\Lambda Q^T$

where ***Q*** is **orthogonal:**

- $\boldsymbol{Q^{-1} = Q^T}$
- Columns of ***Q*** are normalized eigenvectors
- Columns are orthogonal.
- (everything is real)

SVD Singular vector decomposition

特征分解要求A为一个方阵，SVD分解可以针对任何矩阵，考虑$A^TA(d*d)$和$AA^T(n*n)$的特征向量和特征值

For an $m \times n$ matrix $\boldsymbol{A}$ of rank r there exists a factorization (Singular Value Decomposition = **SVD**) as follows:

$$A = \underbrace{U}_{m\times m}\underbrace{\Sigma}_{m\times n}\underbrace{V^T}_{V \text{ is } n\times n}$$

The columns of $\boldsymbol{U}$ are orthogonal eigenvectors of $\boldsymbol{AA^T}$.

The columns of $\boldsymbol{V}$ are orthogonal eigenvectors of $\boldsymbol{A^TA}$.

Eigenvalues $\lambda_1 \ldots \lambda_r$ of $\boldsymbol{AA^T}$ are the eigenvalues of $\boldsymbol{A^TA}$.

$$\sigma_i = \sqrt{\lambda_i}$$

$$\Sigma = diag(\sigma_1 \ldots \sigma_r) \longleftarrow \text{Singular values.}$$

证明A、A^TA和AA^T的秩(rank)相等

零空间一样，自由度一样，rank一样

$N(B) = \{x \mid Bx = 0\}$

$x \in N(A)$

$\to Ax = 0$

$\underline{A^TAx} = 0$

$x \in N(A^TA)$

$\Rightarrow N(A) \subseteq N(A^TA)$

$N(A^TA) \subseteq N(A)$

$y^TA^TAy = 0$

$(Ay)^T(Ay) = 0$

$\to Ay = 0$

证明A^TA和AA^T的特征值一样

更换了特征向量

$$AA^T\alpha_i = \lambda_i \alpha_i$$

$$A^TA(A^T\alpha_i) = \lambda_i (A^T\alpha_i)$$

证明A^TA和AA^T的特征值都是非负的

两者都是半正定矩阵

$$x^T(A^TA)x \geq 0$$

$$(Ax)^T(Ax)$$

证明

Lemma. $\lambda \neq 0$ be the eigenvalue of AA^T, $\alpha_1, \ldots, \alpha_k$ are pairwise orthogonal unit eigenvectors corresponds to λ, then $A^T\alpha_1, A^T\alpha_2, \ldots, A^T\alpha_k$ are pairwise orthogonal eigenvectors of A^TA, and $\sqrt{(A^T\alpha_j, A^T\alpha_j)} = \sqrt{\lambda}$.

$$(A^T\alpha_i, A^T\alpha_j) = \alpha_i^T AA^T\alpha_j = \alpha_i^T \lambda_j \alpha_j = \lambda_j \alpha_i^T \alpha_j =$$

$$= \begin{cases} i \neq j \to 0 \Leftarrow ① \\ i = j \to \lambda_j \end{cases}$$

α_i, β_i的定义

$$\left.\begin{aligned} AA^T\alpha_i &= \lambda_i \alpha_i \\ A^TA\beta_i &= \lambda_i \beta_i \end{aligned}\right\}$$

α_i is mutually $\perp$ unit vector of AA^T

$$\beta_i = \frac{1}{\sqrt{\lambda_i}} A^T\alpha_i$$

$$\vec{U} = (\alpha_1\ \alpha_2 \cdots \alpha_m) \longrightarrow V = (\beta_1\ \beta_2 \cdots \beta_n)$$

$$\underline{AV} = A[\beta_1\ \beta_2 \cdots \beta_n] = [A\beta_1 \cdots A\beta_n]$$

$$= (\sqrt{\lambda_1}\alpha_1 \cdots \sqrt{\lambda_k}\alpha_k\ 0 \cdots 0)$$

$$= (\alpha_1\ \alpha_2 \cdots \alpha_m)\begin{bmatrix}\sqrt{\lambda_1} & & & 0 \\ & \ddots & & \\ & & \sqrt{\lambda_k} & \\ 0 & & & 0\end{bmatrix} = U\Sigma.$$ 19

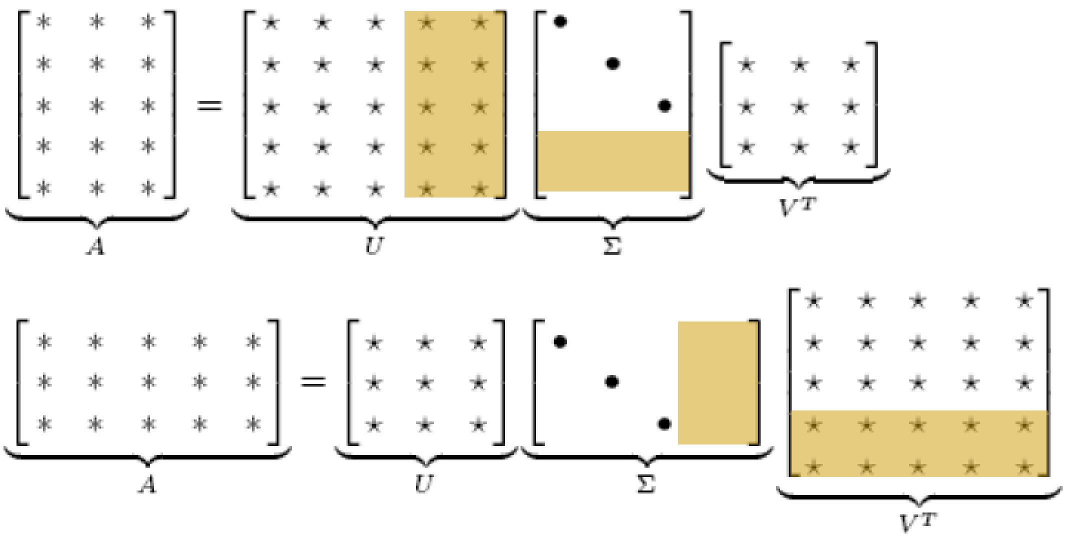
SVD应用

$$A^2 = (U\Sigma V^T)(V\Sigma U^T)$$

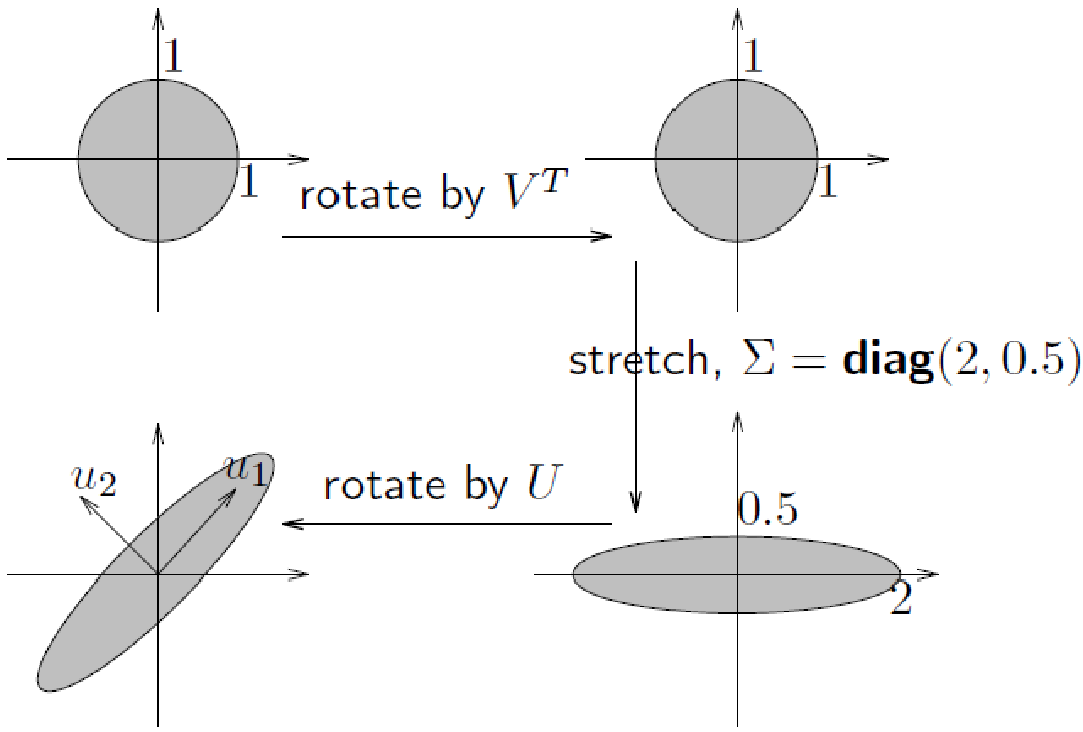
$$= U\Sigma\Sigma U^T$$

$$= U\Sigma^2 U^T$$

Illustration of SVD dimensions and sparseness



几何理解



例子

Let $$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Thus *m*=3, *n*=2. Its SVD is

$$\begin{bmatrix} 0 & 2/\sqrt{6} & 1/\sqrt{3} \\ 1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 1/\sqrt{2} & 1/\sqrt{6} & -1/\sqrt{3} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{3} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

SVD应用 低秩近似 Low-rank Approximation

寻找X的低秩近似

- Approximation problem: Find A_k of rank k such that

原始

$$A_k = \min_{X:rank(X)=k} \|A - X\|_F$$

Frobenius norm

$$\|A\|_F \equiv \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |a_{ij}|^2}.$$

A_k and X are both $m \times n$ matrices.

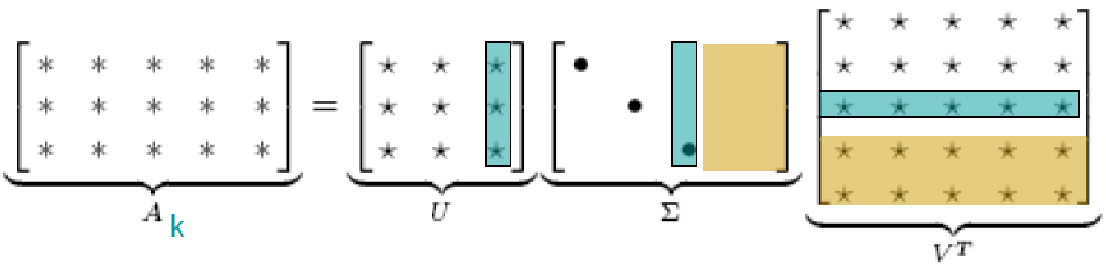
Typically, want $k << r$ = rank(X)

SVD分解

Solution via SVD

$$A_k = U \operatorname{diag}(\sigma_1, \ldots, \sigma_k, \underbrace{0, \ldots, 0}) V^T$$

set smallest r-k singular values to zero



$$A_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$$

column notation: sum of rank 1 matrices

误差

$$\min_{X:rank(X)=k} \|A - X\|_F = \|A - A_k\|_F = \sigma_{k+1}$$

SVD分解依赖数据，考虑表示整体数据的最多信息

JL分解是随机的，考虑两个数据间的distance

SVD power method

对于非常小的奇异值，认为是噪声，可以省去

通过矩阵乘法迅速找到最重要的一个奇异值

$$B = A^T A = \sum_{i=1} \delta_i^2 v_i v_i^T$$

$$B = \left(\sum_i \delta_i^2 \underline{\underline{v_i}}\, v_i^T\right)\left(\sum_j \delta_j^2 v_j \underline{\underline{v_j^T}}\right)$$

$$= \sum_{i=1}^{r} \delta_i^4 \, v_i v_i^T$$

$$\cdots \quad B^k = \sum_{i=1}^{r} \delta_i^{2k} v_i v_i^T \qquad \text{Power}$$

$$\text{if } \delta_1 >> \delta_2 .$$

$$\rightarrow \underline{\underline{\delta_1^{2k} v_1 v_1^T}}$$

$$\Downarrow$$

Estimate v_1:

B^k <u>first column</u>

+ <u>Normalize</u>.

数据很大，无法直接做乘法

可以选一个x来帮助降维

① randomly select x $\quad$ $B = A^T A$

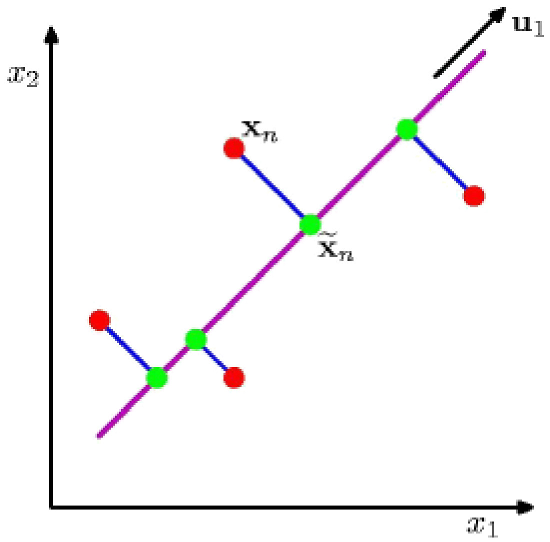
$x = \sum_{i=1}^{d} c_i v_i \quad \Leftarrow$

$B^k x \simeq (\delta_1^{2k} v_1 v_1^T) x = \delta_1^{2k} v_1 v_1^T (\sum_i c_i v_i)$

$\langle A^T A \cdots A^T A A^T A x = \delta_1^{2k} c_1 v_1 = y.$

Ch 09 主成分分析 PCA Principle component analysis

最大化紫色，最小化蓝色



协方差 Covariance

Covariance as a measure of how much each of the dimensions vary from the mean with respect to each other.

$$Cov(X, Y) = \boldsymbol{E}[(x - \boldsymbol{E}(x)(Y - \boldsymbol{E}(Y))]$$

协方差矩阵 Covariance Matrix

是对称矩阵

$$C = \begin{pmatrix} cov(x,x) & cov(x,y) & cov(x,z) \\ cov(y,x) & cov(y,y) & cov(y,z) \\ cov(z,x) & cov(z,y) & cov(z,z) \end{pmatrix}$$

协方差的正负表示正负相关，值不重要，因为单位不同

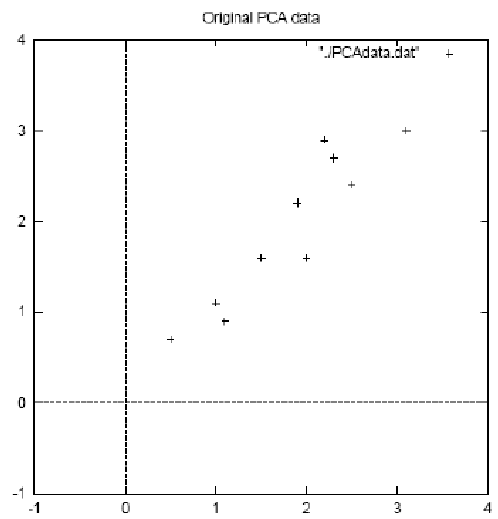
消除影响 $\rho_{xy} = \frac{cov(x,y)}{\sqrt{\delta_x}\sqrt{\delta_y}}$

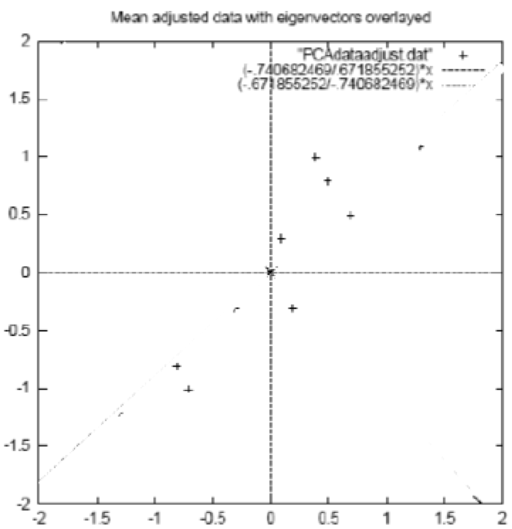
Principal Components Analysis

把数据投影到信息最大的方向上

第一步做中心化

中心放到均值上，可以简化协方差表达

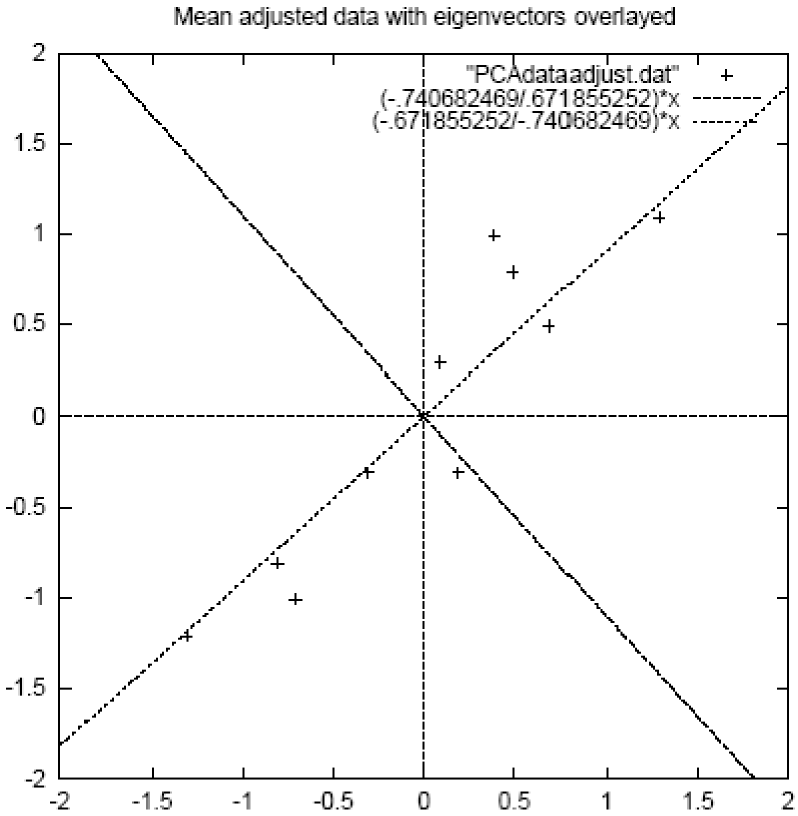




第二步计算协方差矩阵

第三步计算特征值和特征向量

做可视化，两个特征向量正交。



第四步去除不重要的特征值和特征向量

第五步向主方向做投影（进行内积）

SVD与PCA

$A_{d\times n}$.

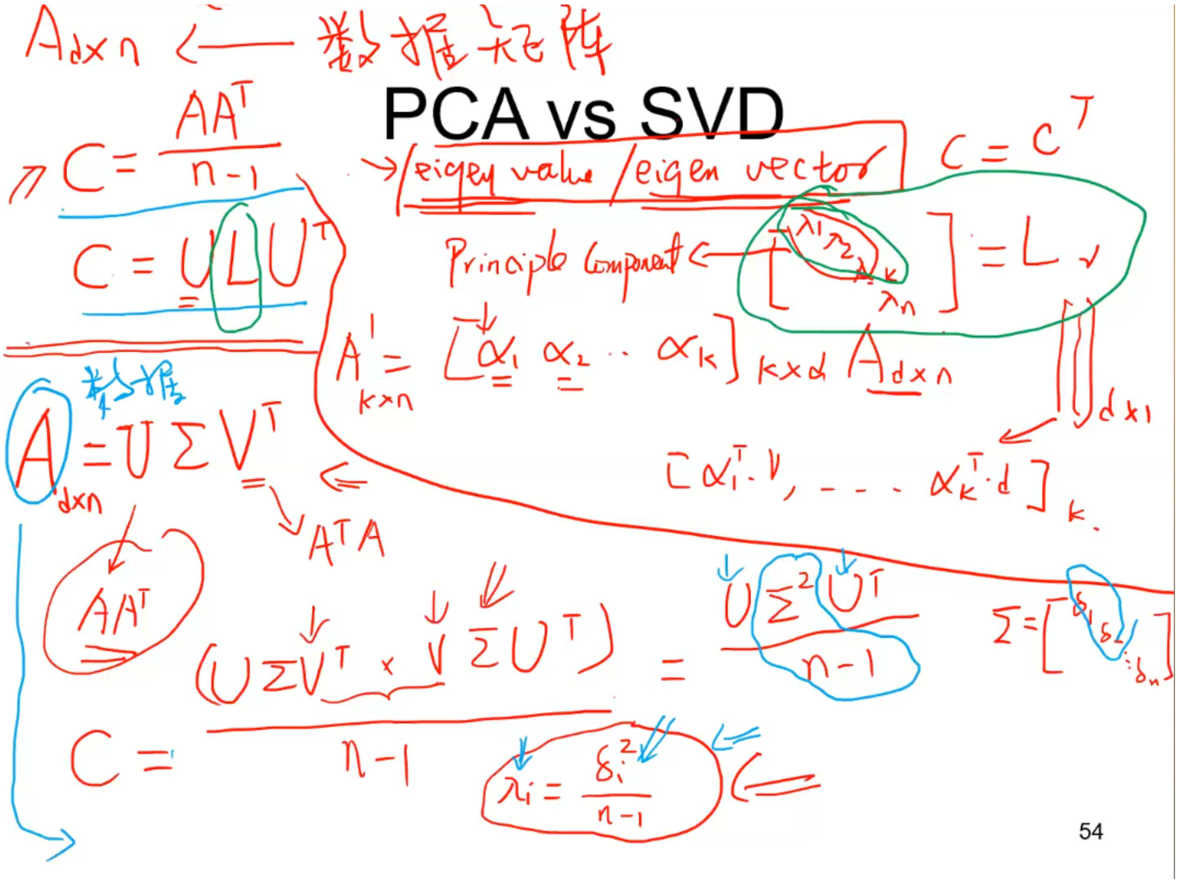
$$C_{d\times d} = \begin{array}{c c} & j \\ i & \begin{bmatrix} & & \\ & \mathrm{cov}(x_i, x_j) & \\ & & \end{bmatrix} \end{array} = \frac{AA^T}{n-1}$$

$$x_i = [x_{i1} \quad x_{i2} \quad \cdots \quad x_{in}] \qquad 1 \le i \le d$$

$$x_j = [x_{j1} \quad x_{j2} \quad \cdots \quad x_{jn}]$$

$$\mathrm{cov}(x_i, x_j) = E(x_i, x_j) = \frac{1}{n-1} \sum_{k=1}^{n} x_{ik} x_{jk}$$

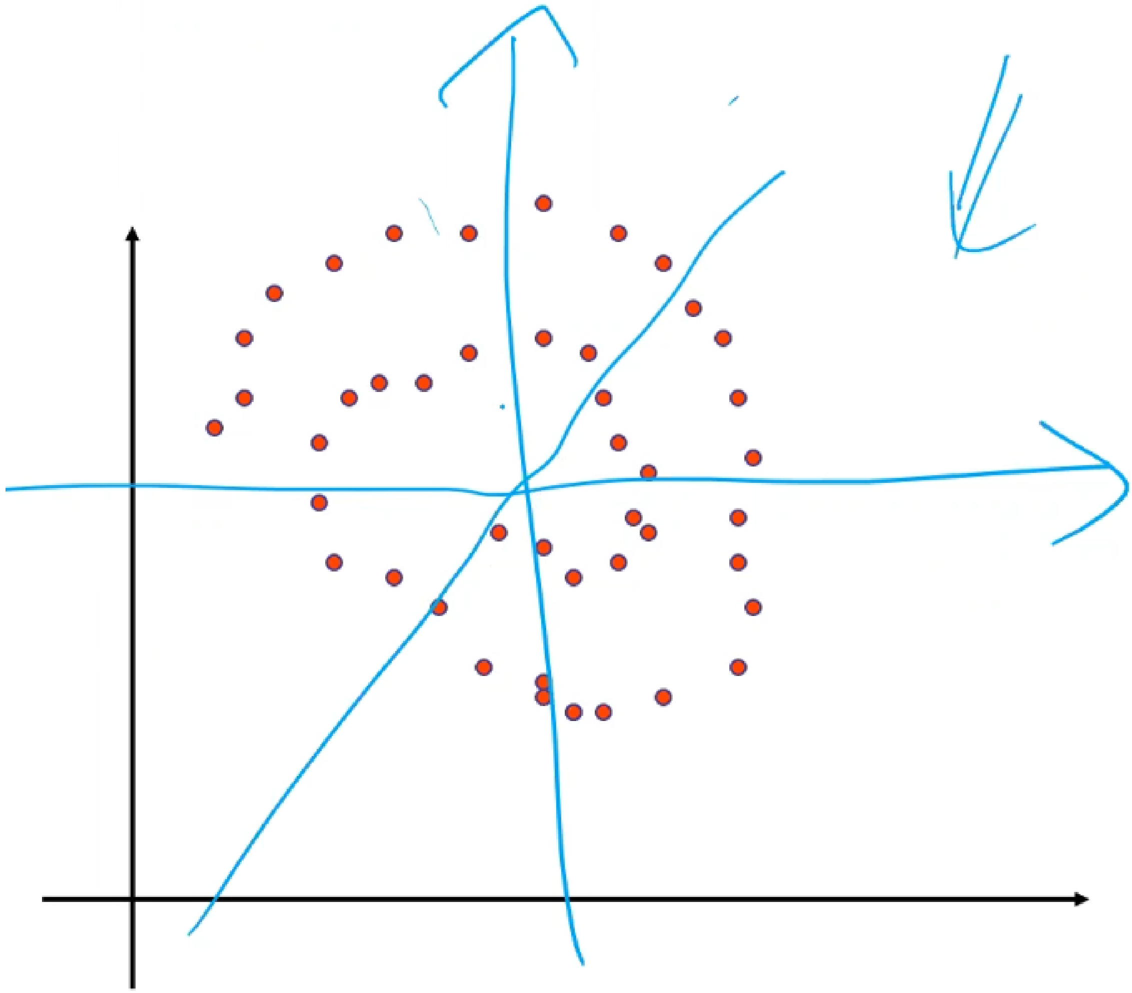
SVD奇异值=PCA特征值方/n-1



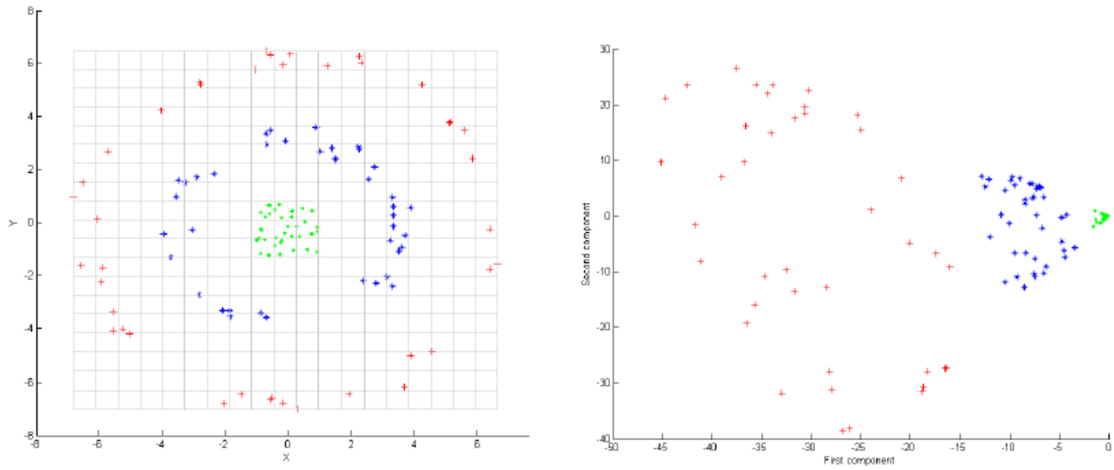
做PCA比较好，因为奇异值很小时，特征值特别特别小，计算机表示误差大

缺点

是线性降维，对非线性数据表现不好



可以用核方法，引入第三维距离



计算举例

$$A = \begin{pmatrix} 1.2 & 0.8 \\ 0.8 & 1.2 \end{pmatrix}$$

$$Ax = \lambda x$$

$$(A - \lambda E)x = 0$$

$$|A - \lambda E| = 0$$

$$\left|\begin{pmatrix} 1.2 & 0.8 \\ 0.8 & 1.2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right| = \left|\begin{pmatrix} 1.2-\lambda & 0.8 \\ 0.8 & 1.2-\lambda \end{pmatrix}\right| = 0$$

$$(1.2-\lambda)^2 - 0.64 = 0$$

$$\lambda = 2$$

$$\begin{pmatrix} 1.2 & 0.8 \\ 0.8 & 1.2 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = 2\begin{pmatrix} a \\ b \end{pmatrix}$$

$$1.2a + 0.8b = 2a$$

$$0.8b = 0.8a$$

$$a = b$$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

3. SVD计算举例

这里我们用一个简单的例子来说明矩阵是如何进行奇异值分解的。我们的矩阵A定义为：

$$\mathbf{A}=\begin{pmatrix}0&1\\1&1\\1&0\end{pmatrix}$$

首先求出 A^TA 和 AA^T

$$\mathbf{A}^{\mathbf{T}}\mathbf{A}=\begin{pmatrix}0&1&1\\1&1&0\end{pmatrix}\begin{pmatrix}0&1\\1&1\\1&0\end{pmatrix}=\begin{pmatrix}2&1\\1&2\end{pmatrix}$$

$$\mathbf{A}\mathbf{A}^{\mathbf{T}}=\begin{pmatrix}0&1\\1&1\\1&0\end{pmatrix}\begin{pmatrix}0&1&1\\1&1&0\end{pmatrix}=\begin{pmatrix}1&1&0\\1&2&1\\0&1&1\end{pmatrix}$$

进而求出 A^TA 的特征值和特征向量：

$$\lambda_1=3;v_1=\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix};\lambda_2=1;v_2=\begin{pmatrix}-1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$$

接着求出 AA^T 的特征值和特征向量：

$$\lambda_1=3;u_1=\begin{pmatrix}1/\sqrt{6}\\2/\sqrt{6}\\1/\sqrt{6}\end{pmatrix};\lambda_2=1;u_2=\begin{pmatrix}1/\sqrt{2}\\0\\-1/\sqrt{2}\end{pmatrix};\lambda_3=0;u_3=\begin{pmatrix}1/\sqrt{3}\\-1/\sqrt{3}\\1/\sqrt{3}\end{pmatrix}$$

利用 $Av_i=\sigma_iu_i,i=1,2$ 求奇异值：

$$\begin{pmatrix}0&1\\1&1\\1&0\end{pmatrix}\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}=\sigma_1\begin{pmatrix}1/\sqrt{6}\\2/\sqrt{6}\\1/\sqrt{6}\end{pmatrix}\Rightarrow\sigma_1=\sqrt{3}$$

$$\begin{pmatrix}0&1\\1&1\\1&0\end{pmatrix}\begin{pmatrix}-1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}=\sigma_2\begin{pmatrix}1/\sqrt{2}\\0\\-1/\sqrt{2}\end{pmatrix}\Rightarrow\sigma_2=1$$

也可以用 $\sigma_i=\sqrt{\lambda_i}$ 直接求出奇异值为 $\sqrt{3}$ 和1.

最终得到A的奇异值分解为：

$$A=U\Sigma V^T=\begin{pmatrix}1/\sqrt{6}&1/\sqrt{2}&1/\sqrt{3}\\2/\sqrt{6}&0&-1/\sqrt{3}\\1/\sqrt{6}&-1/\sqrt{2}&1/\sqrt{3}\end{pmatrix}\begin{pmatrix}\sqrt{3}&0\\0&1\\0&0\end{pmatrix}\begin{pmatrix}1/\sqrt{2}&1/\sqrt{2}\\-1/\sqrt{2}&1/\sqrt{2}\end{pmatrix}$$