Coursera离散数学学习笔记

前言

本笔记由chy-2003整理于上海交通大学发布于coursera的离散数学课程。讲师龙环。

不保证内容十分全面，但至少与课程内容保持一致，同时添加或删减了某些样例和引入。

定理或命题下方的块没有特殊标注即为证明。

如果发现文章内容错误，请联系 chy_2003@foxmail.com。

引言

推荐书目

Invitation to Discrete Mathematics（Oxford University Press）

Discrete Mathematics:Elementary and Beyond

函数

函数$f: X \to Y$为集合X到集合Y的一个映射。对于任意$x \in X$，都有唯一一个$y \in Y$与之对应。

单射： 对于$\forall y \in Y$最多只有一个$x \in X$与之对应。

满射： 对于$\forall y \in Y$都有至少一个$x \in X$与之对应。

双射： 同时满足单射与满射的映射。

集合运算

对于集合$A=\{1,2,3\}$，$B=\{2,4\}$，$U=\{1,2,3.4\}$:

$2^A=\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$（幂集$P(A)$）

$A\diagdown B=\{1,3\}$（$A-B$）

$A\times B=\{(1,2),(1,4),(2,2),(2,4),(3,2),(3,4)\}$

$A\oplus B=\{1,3,4\}$。

$\overline{A}=\{4\}$。

关系

对于集合A，关系$R\subseteq A\times A$，如果$(x,y)\in R$，就可以记做xRy。关系可能有以下性质：

> - 自反性：对于$\forall x\in A$，都有$xRyxRx$。
> - 对称性：对于$\forall x,y\in A$，如果xRy，就有yRx。
> - 反对称性：对于$\forall x,y\in A$，如果有xRy且yRx，那么$x=y$。
> - 传递性：对于$\forall x,y,z\in A$，如果xRy且yRz，那么xRz。

一些特殊关系：

> - 等价关系：关系R具有自反性、对称性、传递性。例如$\equiv_6\subseteq N\times N$。
> - 偏序关系：关系R具有自反性、反对称性、传递性。例如$\leqslant\subseteq N\times N$。

关系的运算

关系是一个集合，所以支持集合有关的运算。而关系还支持合成运算。我们定义$R\subseteq A\times B$，$S\subseteq B\times C$，那么合成运算$R\circ S=\{(x,z):x\in A\wedge z\in C\wedge\exists y\in B((x,y)\in R\wedge(y,z)\in S)\}$。

$R^{-1}=\{(x,y):(y,x)\in R\}$表示$R$的逆关系。

$R^n=R^{n-1}\circ R$。

等价类

有等价关系$R\subseteq A\times A$，定义$R[x]=\{y\in A:xRy\}$。$R[x]$被称为元素x在关系R下的等价类。例如对于关系$\equiv_6\subseteq N\times N$，$\equiv_6[0]=\{0,1,2,3,...\}$。

性质：

如果$R\subseteq A\times A$是等价关系，那么有

● 对于$\forall x\in A$，$R[x]$非空。

> 对于$\forall x\in A$，$x\in R[x]$。所以对于$\forall x\in A$，$R[x]$非空。

● 对于$\forall x,y\in A$，$R[x]=R[y]$或$R[x]\cap R[y]=\emptyset$。

> 若$R[x]\cap R[y]=\emptyset$，那么结论成立。
>
> 若$z\in R[x]\cap R[y]\neq\emptyset$，即$xRz$且$yRz$。那么根据对称性有$zRx$。对于$\forall x'\in R[x]$，即$xRx'$，根据传递性有$zRx'$。又根据对称性有$yRx'$。即$x'\in R[y]$。$\therefore R[x]\subseteq R[y]$。

> 同理$R[y] \subseteq R[x]$。$\therefore R[x] = R[y]$。
>
> 综上所述，结论成立。

划分

对于集合A，如果$\pi = \{B_1, B_2, \ldots, B_n\}$满足

> - 对于$\forall 1 \leqslant i \leqslant n$，有$\emptyset \neq B_i \subseteq A$。
> - 对于$\forall 1 \leqslant i < j \leqslant n$，$B_i \cap B_j = \emptyset$。（不相交性）
> - $B_1 \cup B_2 \cup \cdots \cup B_n = A$。（覆盖性）

则称π是A的一个划分。

如果$R \subseteq A \times A$是一个等价关系，则等价类集合$\Pi = \{R[x] : x \in A\}$是集合A在R关系下的划分。

练习题1.1

序的关系

偏序集

定义偏序集(S, R)，R是集合S上的偏序关系。

常用符号

偏序$\preccurlyeq, \leqslant$

严偏序$\prec, <$

逆序$\succcurlyeq, >$

线性序

如果偏序集(S, R)，$\forall x, y \in S, \Rightarrow xRy \vee yRx$，那么称$(S, R)$为线性序。

如$(N, \leqslant), (Z, \leqslant)$是线性序，$(2^A, \subseteq), (N, |)$不是。

字典序

若$(S_1, \leqslant_1), (S_2, \leqslant_2), \ldots, (S_n, \leqslant_n)$是$n$个线性序，$(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in S_1 \times S_2 \times \cdots \times S_n$。

n元字典序$(a_1, a_2, \ldots, a_n) \leqslant_{lex} (b_1, b_2, \ldots, b_n)$成立

$\Longleftrightarrow (a_1, a_2, \cdots, a_n) = (b_1, b_2, \ldots, b_n) \vee \exists i \in \{1, 2, \ldots, n\}(\forall j < i) a_j = b_j \wedge a_i <_i b_i$。

n元字典序是线性序的证明

> 部分证明，其余类似：
>
> 传递性：有n元组

> $$x = (a_1, a_2, \ldots, a_i, \ldots, a_j, \ldots, a_n)$$
> $$y = (b_1, b_2, \ldots, b_i, \ldots, b_j, \ldots, b_n)$$
> $$z = (c_1, c_2, \ldots, c_i, \ldots, c_j, \ldots, c_n)$$
>
> 设$x \leqslant_{lex} y \leqslant_{lex} z$，且$x, y$的前$i-1$项相同，$y, z$的前$j-1$项相同。对$i, j$的大小分为3类讨论：
>
> 如果$i < j$，那么$a_i <_i b_i = c_i$；如果$i = j$，那么$a_i <_i b_i <_i c_i$；如果$i > j$，那么$a_j = b_j <_j c_j$。综上，有$x \leqslant_{lex} y$。
>
> 其余部分略。

立即前元

定义：对于偏序集$(S, \preccurlyeq)$，元素x, y，若$x \prec y \wedge \neg(\exists z \in s)(x \prec z \prec y)$，那么称$x$是$y$的立即前元，记为$x \lhd y$。

性质：1、$\lhd$不具有传递性。2、多个元素可能有同一立即前元。3、一个元素可能有多个立即前元。

例：$(N, |)$。

哈斯图（Hasse diagram）

给定偏序集$(S, \preccurlyeq)$，S为有限集。只保留立即前元关系对应边。若$x \lhd y$，则代表y的点在代表x的点上方。可以通过传递闭包恢复原图。

偏序集上的极大元、极小元、最大元、最小元

> - 极大元(Maximal element) $\neg(\exists x \in S) x \succ a$。
> - 极小元(Minimal element) $\neg(\exists x \in S) x \prec a$。
> - 最大元(Largest element) $\forall x \in S, x \preccurlyeq a$。
> - 最小元(Smallest element) $\forall x \in S, a \preccurlyeq x$。

一些性质

> - 极大元、极小元可能不止一个，一个元素可能既是极大元，又是极小元。
> - 可能不存在最大元、最小元。
> - 最大元一定是极大元，最小元一定是极小元。而极小元不一定是最小元，极大元不一定是最大元。
> - 如果S是无限集，那么极大元、极小元、最大元、最小元不一定存在。
> - 如果S是有限集，那么最大元、最小元不一定存在，极大元、极小元一定存在。

S为有限集时，极小元存在性证明

> 取$\forall x_0 \in S$。如果x_0是极小元，那么证毕。如果x_0不是极小元，找到$x_1 \prec x_0$，对x_1重复以上讨论。而由于S是有限集，那么情况2在有限步后不成立，情况1成立。

线性扩充定理

线性扩充：对于有限集$(S, \preccurlyeq)$，存在一个线性序集$(S, \preccurlyeq')$，满足$x \prec y \to x \preccurlyeq' y$。

证明：

> 当$|S| = 1$时，$(S, \preccurlyeq') = (S, \preccurlyeq)$即可。当$|S| > 1$时，取$(S, \preccurlyeq)$中的一个极小元$x_0$，$S' = S \backslash \{x\}$。易证得$(S', \preccurlyeq)$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$\preccurlyeq' = \preccurlyeq'' \bigcup \{(x_0, y) : y \in S\}$。易证$(S, \preccurlyeq')$是线性序列。

一般线性扩充并不唯一。

练习题1.2

链与反链

对于有限偏序集$(S,\preccurlyeq)$，$A\subseteq S$，A被称为

> - 链（Chain）: 如果对于任意$x,y\in A,\ x\preccurlyeq y$或$y\preccurlyeq x$。
> - 反链（Antichain）: 如果对任意$x,y\in A,\ x\not\preccurlyeq y$。反链也称为独立集（Independent set）。

还可以这么定义：

> - 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。

最大独立集和最长链

给定有限偏序集$P=(S,\preccurlyeq)$。

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

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

$$t=\min\left\{k\;\middle|\;\begin{array}{c}s=A_1\cup A_2\cup\cdots\cup A_k\\ 1\leqslant i\leqslant k,A_i\text{是反链}\\ \text{任意}\ 1\leqslant i\neq j\leqslant k,A_i\cap A_j=\emptyset\end{array}\right\}$$

则$t=\omega(P)$。

> 先证明$\omega(P)\leqslant t$。
>
> $S=A_1\cup A_2\cup\cdots\cup A_t$，其中$A_1,A_2,\ldots,A_t$为不相交的反链划分。
>
> $C\subseteq S$是P中任意一条链，有$|C\cap A_i|\leqslant 1$。
>
> $|C|=|C\cap S|=|C\cap(A_1\cup A_2\cup\cdots\cup A_t)|=|(C\cap A_1)\cup(C\cap A_2)\cup\cdots\cup(C\cap A_t)|\leqslant t$。
>
> $\therefore\omega(P)\leqslant t$。
>
> 然后证明$t\leqslant\omega(P)$。
>
> 令A_1是S的极小元集合，$A_{i+1}=S\backslash(A_1\cup A_2\cup\cdots\cup A_i)$的极小元集合。
>
> 每一个A_i都是一个反链（独立集）。有限步后$A_1\cup A_2\cup\cdots\cup A_m$，由$t$的最小性，$t\leqslant m$。只需证明$m\leqslant\omega(P)$。
>
> 任取$x_m\in A_m$，由构造，得$\exists x_{m-1}\in A_{m-1}$，使得$x_{m-1}\prec x_m$。以此类推，存在序列$x_1\prec x_2\prec\cdots\prec x_m$。$\therefore m\leqslant\omega(P)$。
>
> $\therefore t\leqslant\omega(P)$。
>
> 证毕

推论1：$\alpha(P)\times\omega(P)\geqslant|S|$。

> $P=A_1\cup A_2\cup\cdots\cup A_t$，$t=\omega(P)$，$|A_i|\leqslant\alpha(P)$。
>
> $|S|=|A_1|+|A_2|+\cdots+|A_t|\leqslant\alpha(P)\times\omega(P)$。

推论2：对于任意有限偏序集$P=(S,\preccurlyeq)$，$\alpha(P)$或$\omega(P)$之一至少为$\sqrt{|S|}$。形象的，我们可以定义“宽”：$\alpha(P)$，”高“：$\omega(P)$。

Erdos-Szekeres引理：任意一个含有n^2+1个元素的实数序列$(x_1,x_2,\ldots,x_{n^2+1})$中都含有一个长度为$n+1$的单调子序列。

> 对$(x_1,\ldots,x_{n^2+1})$，设$I=1,2,\ldots,n^2+1$。
>
> 在集合I上定义关系$\preccurlyeq$：$i\preccurlyeq j\Longleftrightarrow(i\leqslant j)\wedge(x_i\leqslant x_j)$。
>
> 可以证明$(I,\preccurlyeq)$是偏序集。
>
> 由于推论2，若$\omega(I,\preccurlyeq)>n$：非递减子序列$x_{i_1}\leqslant x_{i_2}\leqslant\cdots\leqslant x_{i_m}$。若$\alpha(I,\preccurlyeq)>n$，有独立集$\{i_1,i_2,\ldots,i_m\}$。设$i_1<i_2<\cdots<i_m$，则$x_{i_1}>x_{i_2}>\ldots x_{i_m}$为非递增子序列。
>
> 证毕。

练习题1.3

组合数计数

导引：函数的计数

命题1：集合N的大小为n，集合M的大小为m，且$n\geqslant0,m\geqslant1$。从集合N到集合M所有可能的函数$f:N\to M$共有m^n个。

> 对n做数学归纳。当$n=0$时，$f=\emptyset$。f唯一。此时$m^n=1$成立。假设$n=k$时结论成立。当$n=k+1$时，取$\forall a\in N$，则$f:N\to M$可以看做如下两个部分的组合：
>
> 1、确定$f(a)\in M$即f函数在a上的值$f(a)$。$f(a)$的取值共有m中可能。
>
> 2、确定$f':M\backslash\{a\}\to M$。根据归纳假设，f'有m^{n-1}种可能。
>
> 故$f:N\to M$共有$m\times m^{n-1}=m^n$种可能。

命题2：集合N的大小为n，集合M的大小为m，且$n\geqslant0$，$m\geqslant0$。从集合N到集合M所有可能的单射函数$f:N\to M$的个数为$m\times(m-1)\times\cdots\times(m-n+1)=\prod\limits_{i=0}^{n-1}(m-i)$。

> 对n做数学归纳。当$n=0$时，$f=\emptyset$。f单射且唯一。此时公式成立。假设$n=k$时结论成立。当$n=k+1$时，取$\forall a\in N$，则$f:N\to M$可以看做如下两个部分的组合：
>
> 1、确定$f(a)\in M$即f函数在a上的值$f(a)$。$f(a)$的取值共有m中可能。
>
> 2、确定$f':M\backslash\{a\}\to M\backslash\{f(a)\}$。根据归纳假设，$f'$有$(m-1)\ldots(m-n+1)$种可能。
>
> 故$f:N\to M$共有$m\times(m-1)\times\cdots\times(m-n+1)=\prod\limits_{i=0}^{n-1}(m-i)$种可能。

练习题2.1

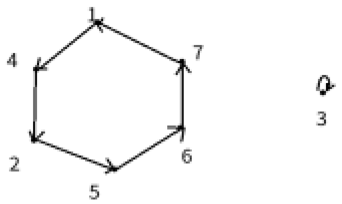
简单应用：子集计数，置换计数

命题3：集合X含有n个元素$n \geqslant 0$。则X一共有2^n个子集。

> 方法一：数学归纳法（略）
>
> 方法二：
>
> 考虑X的任意子集A，定义函数$f_A : X \to \{0,1\}$为 $f_A(X) = \begin{cases} 1 & if\ x \in A \\ 0 & if\ x \notin A \end{cases}$。$f_A$叫集合$A$的特征函数。如果可以验证（图示后显然成立）$X$的子集与函数$f_A$一一对应，那么就可以得到$X$的子集个数与从$x$到$\{0,1\}$的函数个数相等，为$2^n$个。（命题1）

置换：集合X到其自身的双射函数被称为一个置换。

置换的表示：

> - $p : X \to X$是一个双射函数。
> - 矩阵表示：如果集合X是有限集，它包含的元素$\{x_1, x_2, \ldots, x_n\}$，则函数$p$可以表示为$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ p(x_1) & p(x_2) & \ldots & p(x_n) \end{pmatrix}$。如果$x_1, x_2, \ldots, x_n$固定，那么可以用一行表示为$\begin{pmatrix} p(x_1) & p(x_2) & \ldots & p(x_n) \end{pmatrix}$。例如$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 3 & 2 & 6 & 7 & 1 \end{pmatrix}$可以表示为$p = \begin{pmatrix} 4 & 5 & 3 & 2 & 6 & 7 & 1 \end{pmatrix}$。
> - 图示法：
>
> - 环（cycles）表示：$p = ((1,4,2,5,6,7)(3))$。

可以证明对于有限集合上的任一置换：1、图示法下表达成互不相交的环（独立子环）；2、除独立子环内点的顺序不一样外，环表示唯一。

置换的计数：阶乘

集合X的大小为n（即$|X| = n$），则X上的置换一共有$n \times (n-1) \times \cdots \times 2 \times 1$个。证明：类似于命题2，略。

n的阶乘（n factorial）：$n! = n \times (n-1) \times \cdots \times 2 \times 1 = \prod_{i=1}^{n} i$。

练习题2.2

二项式定理、多项式定理

问题引入：已知集合X的大小为n（即$|X| = n$），$n \geqslant k \geqslant 0$。$X$的所有子集中正好含有$k$个元素的子集一共有多少个？例：$X = \{a,b,c\}, k = 2$。

常用符号：$\binom{X}{k}$和$|\binom{X}{k}|$。例中$\binom{X}{k} = \{\{a,b\},\{a,c\},\{b,c\}\}$，$|\binom{X}{k}| = 3$。

命题4：从含n个元素的集合X中抽取含k个元素$(n \geqslant k \geqslant 0)$的子集。所有$k$元子集的个数为

$$\left|\binom{X}{k}\right| = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$$

> 算两次：
>
> 从X中抽取k元不重复有序组，一共有$n(n-1)\dots(n-k+1)$种方法。
>
> 另一方面从任意1个X的k元子集出发，可以得到$k!$个不同的k元有序组。
>
> 二者相等，故$n(n-1)\dots(n-k+1) = k!\left|\binom{X}{k}\right|$。
>
> $$\therefore \left|\binom{X}{k}\right| = \frac{n(n-1)\dots(n-k+1)}{k!}$$

二项式系数：$|X| = n \geqslant k$均为非负整系数，定义二项式系数为

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

命题5：$m \geqslant r \geqslant 0$是满足等式$x_1 + x_2 + \dots + x_r = m$的非负$r$元整数解$(x_1, x_2, \dots, x_r)$的个数为$\binom{m+r-1}{r-1}$个。

> m个球用$r-1$个隔板隔开，方法与解$(x_1, x_2, \dots, x_r)$一一对应。就相当于在$m+r-1$个对象中，选取$r-1$个作为挡板，剩下m个为球。

性质：

> - $\binom{n}{k} = \binom{n}{n-k}$
> - $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$
> - $\sum\limits_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$

对于第三点的证明：注意到$\sum\limits_{i=0}^{n} \binom{n}{i}^2 = \sum\limits_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$。而$\binom{2n}{n}$可理解为1、直接从$2n$个元素选$n$个；2、前$n$个元素里选$i$个，后$n$个元素里选$n-i$个。

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

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

> 略

当$x=1$时，得到

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$$

当$x=-1$时，得到

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

将上面两式相加，得到

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots=2^{n-1}$$

带重复元素的排列：有来自m类的物品共n个，其中第i类物品有k_i个。即$k_1+k_2+\cdots+k_m=n$。同一类物品不可区分。那么这n个物品所组成的不同排列一共有$\frac{n!}{k_1!k_2!\ldots k_m!}$种，记作$\binom{n}{k_1,k_2,\ldots,k_m}$，被称为**多项式系数**。

> 证明思路同命题4，略。

多项式定理（Multinomial Theorem）：对任意实数$x_1,x_2,\ldots,x_m$，以及任意自然数$n\geqslant 1$，如下等式成立：

$$(x_1+x_2+\cdots+x_m)^n=\sum_{\substack{k_1+k_2+\cdots+k_m=n\\ k1,k2,\ldots,k_m\geqslant 0}}\binom{n}{k_1,k_2,\ldots,k_m}x_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}$$

> 略（归纳法）

练习题2.3

容斥原理

例：$|F\cup P|=|F|+|P|-|F\cap P|$，$|S\cup F\cup P|=|S|+|F|+|P|-|S\cap F|-|S\cap P|-|F\cap P|+|S\cap F\cap P|$。

容斥定理（Inclusion-exclusion principle）：对于任意有限集合$A_1,A_2,\ldots,A_n$，有

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

> 数学归纳法：
>
> $n=2$时成立。假设对$n-1$成立，则
>
> $$\begin{aligned}\left|\bigcup_{i=1}^{n}A_i\right|&=\left|\left(\bigcup_{i=1}^{n-1}A_i\right)\bigcup A_n\right|\\&=\left|\bigcup_{i=1}^{n-1}A_i\right|+|A_n|-\left|\left(\bigcup_{i=1}^{n-1}A_i\right)\bigcap A_n\right|\\&=\left|\bigcup_{i=1}^{n-1}A_i\right|+|A_n|-\left|\bigcup_{i=1}^{n-1}(A_i\cap A_n)\right|\end{aligned}$$
>
> 其中$\left|\bigcup_{i=1}^{n-1}A_i\right|$和$\left|\bigcup_{i=1}^{n-1}(A_i\cap A_n)\right|$可由归纳假设推出。

应用1：错排

任给一个n，求出$1,2,\ldots,n$的错排个数$D(n)$共有多少个？

> 解：用 S_n 表示所有 $\{1,2,\ldots,n\}$ 上的排列，则 $|S_n|=n!$。令 $A_i=\{\pi\in S_n:\pi(i)=i\}$，那么就有 $D(n)=n!-|A_1\cup A_2\cup\cdots\cup A_n|$。
>
> 可以发现 $|A_i|=(n-1)!$，如果 $i<j$，那么 $|A_i\cap A_j|=(n-2)!$。如果 $i_1<i_2<\cdots<i_k$，那么 $|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}|=(n-k)!$。
>
> 根据容斥原理：
>
> $$|A_1\cup A_2\cup\cdots\cup A_n|=\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)!=\sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!}$$
>
> 故$D(n)=n!(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!})$。

特别的，$\lim\limits_{n\to\infty}D_n=\frac{n!}{e}$。

应用2：欧拉函数

欧拉函数ϕ：给定自然数n，欧拉函数$\phi(n)$定义为不超过n且与n互质的自然数的个数。即

$$\phi(n)=|\{m\in\{1,2,\ldots,n\}:\gcd(n,m)=1\}|=?$$

> 解：根据整数分解定理，n可被唯一地分解成$n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$，其中$\alpha_i\geqslant 1$且$p_i$为素数，$p_1<p_2<\cdots<p_r$。
>
> 如果$1\leqslant m<n$，且m与n不互素，则必存在某个$1\leqslant i\leqslant r$有$p_i|m$。令$A_i=\{m\in\{1,2,\ldots,n\}:p_i|m\}$，则$\phi(n)=n-|A_1\cup A_2\cup\cdots\cup A_r|$。
>
> 可以发现 $|A_i|=\frac{n}{p_i}$。当 $i<j$ 时，$|A_i\cap A_j|=\frac{n}{p_ip_j}$。当 $i_1<i_2<\cdots<i_k$ 时，$|A_{i_1}\cap A_{i-2}\cap\cdots\cap A_{i_k}|=\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}$。
>
> 所以有$\phi(n)=n(1-\frac{1}{p_1})(1-frac1p_2)\ldots(1-\frac{1}{p_r})$。

练习题2.4

函数估计

大O符号

应用范围：寻找精确值困难，转而寻找可接受的估值（estimate）。

函数的渐进比较（Asymptotic comparison）

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$n\geqslant n_0$，不等式$|f(n)|\leqslant c\times g(n)$成立。

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

例子：$100000=O(1)$，$(7n^2+6n+1)(n^3+4)=O(n^5)$，$\binom{n}{2}=n(n-1)/2=\frac{1}{2}n^2+O(n)=O(n^2)$；

$0<\alpha\leqslant\beta\Rightarrow n^\alpha=O(n^\beta)$，$\forall C>0,a>1,n^n=O(a^n)$，$\forall C>0,\alpha>0,(\ln n)^C=O(n^\alpha)$。

名称	表示	条件	直观含义
大O符号	$f(n)=O(g(n))$	$\lim\limits_{n\to\infty}\frac{f(n)}{g(n)}\nrightarrow\infty$	f的增长不比g快很多
小o符号	$f(n)=o(g(n))$	$\lim\limits_{n\to\infty}\frac{f(n)}{g(n)}=0$	f的增长远远慢于g
大Ω符号	$f(n)=\Omega(g(n))$	$g(n)=O(f(n))$	f的增长至少和g一样快
大Θ符号	$f(n)=\Theta(g(n))$	$f(n)=O(g(n))$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（Harmonic number）

定义调和级数$H_n=1+\frac{1}{2}+\frac{1}{2}+\cdots+\frac{1}{n}=\sum\limits_{i=1}^{n}\frac{1}{n}$。

调和级数估值

用数列对调和级数的项做分类。

1	$\frac{1}{2},\frac{1}{3}$	$\frac{1}{4},\dots,\frac{1}{7}$	$\frac{1}{8},\dots,\frac{1}{15}$	$\frac{1}{16},\cdots$	$\dots$
$(\frac{1}{2^1},\frac{1}{2^0}]$	$(\frac{1}{2^2},\frac{1}{2^1}]$	$(\frac{1}{2^3},\frac{1}{2^2}]$	$(\frac{1}{2^4},\frac{1}{2^3}]$	$(\frac{1}{2^5},\frac{1}{2^4}]$	$\dots$
G_0	G_1	G_2	G_3	G_4	$\dots,G_t$

其中$G_k=\{\frac{1}{i}|\frac{1}{2^k}<\frac{1}{i}\leqslant\frac{1}{2^{k-1}}\}$。不难发现$|G_k|=2^{k-1}$。

同时有：

$$\sum_{x\in G_k}x\leqslant|G_k|\max G_k=2^{k-1}\times\frac{1}{2^{k-1}}=1$$
$$\sum_{x\in G_k}x\geqslant|G_k|\min G_k>2^{k-1}\times\frac{1}{2^k}=\frac{1}{2}$$

而G的最后一项G_t下表$t=\lfloor\log_2 n\rfloor+1$。

$$\left.\begin{array}{r}H_n\leqslant t\times 1\leqslant\lfloor\log_2 n\rfloor+1\\ H_n>(t-1)\times\frac{1}{2}\geqslant\frac{1}{2}\lfloor\log_2 n\rfloor\end{array}\right\}\Rightarrow H(n)=\Theta(\log_2 n)=\Theta(\ln n)$$

练习题3.1

估值初步：阶乘估值

极点估值（$n\geqslant 2$）：

$$\begin{cases} n! = \prod_{i=1}^{n} i \leqslant \prod_{i=1}^{n} n = n^n \\ n! = \prod_{i=2}^{n} i \geqslant \prod_{i=2}^{n} 2 = 2^{n-1} \end{cases}$$

进一步优化：

$$\begin{cases} n! = \prod_{i=1}^{n} i \leqslant \left(\prod_{i=1}^{\frac{n}{2}} \frac{n}{2}\right)\left(\prod_{i=\frac{n}{2}+1}^{n} n\right) = \left(\frac{n}{\sqrt{2}}\right)^n \\ n! = \prod_{i=1}^{n} i \geqslant \prod_{i=\frac{n}{2}}^{n} i > \prod_{i=\frac{n}{2}+1}^{n} \frac{n}{2} = (\frac{n}{2})^{\frac{n}{2}} = (\sqrt{\frac{n}{2}})^n \end{cases}$$

高斯估值：

算数-几何均值不等式（Arithmetic-geometric mean inequality）：

$$\sqrt{xy} \leqslant \frac{x+y}{2}(x, y \in R_+)$$

那么上界：

$$n! = \sqrt{n!n!} = \sqrt{\prod_{i=1}^{n} i(n+1-i)} = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \leqslant \prod_{i=1}^{n} \frac{n+1}{2} = (\frac{n+1}{2})^n$$

同时，我们容易验证有

$$i(n+1-i) \geqslant n$$

那么下界：

$$n! = \sqrt{n!n!} = \sqrt{\prod_{i=1}^{n} i(n+1-i)} = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \geqslant \prod_{i=1}^{n} \sqrt{n} = n^{\frac{n}{2}}$$

欧拉数（Euler number）：$e = 2.718281828\ldots$

对于$x \in R$，有$1 + x \leqslant e^x$。最终我们会得到$e(\frac{n}{e})^n \leqslant n! \leqslant en(\frac{n}{e})^n$。

> 证明：上界（归纳法）
>
> 当$n = 1$时，$1 \geqslant 1!$，结论平凡。设$n = k$时结论成立，那么当$n = k + 1$时，
>
> $n! = n(n-1)! \leqslant ne(n-1)(\frac{n-1}{e})^{n-1} = en(\frac{n}{e})^n \times e(\frac{n-1}{n})^n$。
>
> 而$e(\frac{n-1}{n})^n = e(1 - \frac{1}{n})^n \leqslant e(e^{-\frac{1}{n}})^n = 1$。所以结论成立。
>
> 证明：下界（归纳法）
>
> 当$n = 1$时，$1 \leqslant 1!$，结论平凡。设$n = k$时结论成立，那么当$n = k + 1$时，
>
> $n! = n(n-1)! \leqslant ne(n-1)(\frac{n-1}{e})^{n-1} = en(\frac{n}{e})^n \times e(\frac{n-1}{n})^{n-1}$。

> 而$e(\frac{n-1}{n})^{n-1}=e(\frac{n}{n-1})^{1-n}=e(1+\frac{1}{n-1})^{1-n}=e\left((1+\frac{1}{n-1})^{n-1}\right)^{-1}\geqslant e\left((e^{\frac{1}{n-1}})^{n-1}\right)^{-1}=e\times e^{-1}=1$。
>
> 结论成立。

Stirling公式：$n!\sim\sqrt{2\pi n}(\frac{n}{e})^n$，即$\lim\limits_{n\to\infty}\frac{\sqrt{2\pi n}(\frac{n}{e})^n}{n!}=1$。

估值初步：二项式系数估值

显然，有$\binom{n}{k}\leqslant n^k$。当$n\geqslant k>i\geqslant 0$时$\frac{n-i}{k-i}\geqslant\frac{n}{k}$，故$\binom{n}{k}=\prod\limits_{i=0}^{k-1}\frac{n-i}{k-i}\geqslant(\frac{n}{k})^k$。

二项式定理：对$n\geqslant 1,1\leqslant k\leqslant n$，取$0<x<1$，有$\binom{n}{0}+\binom{n}{1}x+\cdots+\binom{n}{n}x^n=(1+x)^n$。

显然，$\binom{n}{0}+\binom{n}{1}x+\cdots+\binom{n}{k}x^k\leqslant(1+x)^n$，故$\frac{1}{x^k}\binom{n}{0}+\frac{1}{x^{k-1}}\binom{n}{1}+\cdots+\binom{n}{k}\leqslant\frac{(1+x)^n}{x^k}$。

故$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k}\leqslant\frac{(1+x)^n}{x^k}$。取$x=\frac{k}{n}$，因为$1+x\leqslant e^x$，

有$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k}\leqslant(1+\frac{k}{n})^n(\frac{n}{k})^k\leqslant(e^{\frac{k}{n}})^n(\frac{n}{k})^k=(\frac{en}{k})^k$。

所以$\binom{n}{k}\leqslant\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k}\leqslant(\frac{en}{k})^k$。

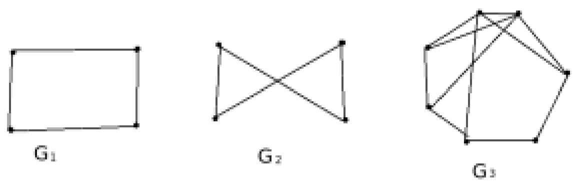
直接带入Stirling公式可以得到更好的结果。

图论导引

基本定义

图：图G是一个有序对(V,E)，其中V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，即$E\subseteq\binom{V}{2}$。为方便常用$V(G),E(G)$来分别表示"G的顶点集"和"G的边集"。

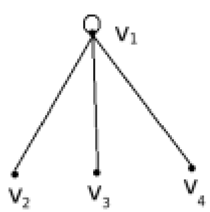
画图（drawing）：



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）**。

显然的，一条边与且仅与两个顶点相关联。

常用$N(u)$表示与顶点u相邻的点集。下图的$|G|=4,N(v_1)=\{v_1,v_2,v_3,v_4\}$。



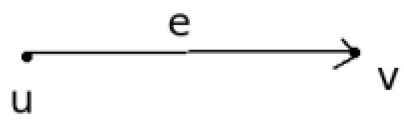
顶点的度：给定图$G=(V,E), v\in V$，定义该顶点在图G中的度（degree）为$\deg_G v = |u:\{u,v\}\in G| = |N(v)|$。一般地，$\delta(G)$表示图$G$的最小度，$\Delta(G)$表示图$G$中的最大度。显然$\deg_G(v)\leqslant |E|$。

> chy-2003注：这里的度似乎没有考虑重边，而下面提到的欧拉图考虑了重边。

上图中$\delta(G)=1$，$\Delta(G)=4$。

无向图（undirected graph）：上面讨论的都是无向图。无向图的边由集合表示$e=\{u,v\}$。

有向图（directed graph）：有向图的边由点对表示$e=(u,v)$，u称为边e的起点或**尾（tail）**，v称为边e的终点或**头（head）**。



除显式声明外，一般图为无向图。

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

若在子图基础上还有$E(G)=E(G')\cap\binom{V(G)}{2}$，则$G$是$G'$的**导出子图（induced subgraph）**。

若在子图基础上还有$V(G)=V(G')$，则G是G'的**生成子图（spanning subgraph）**。

图上基本操作：

> - $G\cup\{e_{ij}\}, G+e_{ij}$：在图$G$中增加边$e_{ij}=\{v_i,v_j\}$。
> - $G\backslash\{e_{ij}\}, G-e_{ij}$：在图$G$中删除边$e_{ij}=\{v_i,v_j\}$。不断进行这个操作可以得到任意生成子图。
> - $G\backslash\overline{E}, G-\overline{E}$，其中$\overline{E}\subseteq E(G)$：从图$G$中删去$\overline{E}$中所有的边。
> - $G\backslash\{v\}, G-v$：从图G中删去顶点v及其关联的边。不断进行这个操作可以得到任意导出子图。
> - $G\backslash\overline{V}, G-\overline{V}$，其中$\overline{V}\subseteq V(G)$：从$G$中删去$\overline{V}$中的所有顶点及与这些点相关联的边。

特殊图

路径图（path P_n）：$V=\{0,1,\ldots,n\}, E=\{\{i-1,i\}:i=1,2,\ldots,n\}$。

环（cycle C_n）：$V=\{1,2,\ldots,n\}, E=\{\{i,i+1\}:i=1,2,\ldots,n-1\}\cup\{\{1,n\}\}$。

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

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

完全二分图（Complete bipartite graph $K_{n,m}$）：

$V=\{u_1,\ldots,u_n\}\cup\{v_1,\ldots,v_n\}, E=\{\{u_i,v_j\}:i=1,\ldots,n,j=1,\ldots,m\}$

正则图：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：不相邻的边（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：

对于无向图$G=(V,E)$，**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）**：没有重边和自环的无向图。

路径（Path）：不允许环，各个顶点和边至多出现一次。

游走（Walk）：允许环，顶点和边可重复。

连通图（connected graph）：如果图G上任意两点u,v之间都有至少一条路径，则称G是一个连通图。否则称为**非连通图（disconnected graph）**。

极大连通子图：给定图G，定义G的极大联通子图：

> - 是原图的子图；
> - 是连通图；
> - 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（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。

树（tree）：无环联通图被称为树。

练习题4.1

握手定理

问题引入1：在宴会上一共有n个人，他们中一些人互相握手，已知每人握手a次，问握手总次数S为多少？$S=\frac{n\times a}{2}$

问题引入2：在宴会上一共有n个人，他们中一些人互相握手。已知握手的次数依次为$\{h_1,h_2,...,h_n\}$次。问握手总次数S为多少？$S=\frac{\sum\limits_{i=1}^{n}h_i}{2}$。

顶点的度：前面已经提到过顶点的度的概念，那么有如下几个显然的结论：

> - $\deg_G(v)\leqslant|E|$。
> - $G=P_n$，则$1\leqslant\deg_G(v)\leqslant2$。
> - $G=C_n$，则$\deg_G(v)=2$。
> - $G=K_n$，则$\deg_G(v)=n-1$。

握手定理（Handshaking theorem, Leonhard Euler 1736）：给定无向图$G=(V,E)$，以下等式成立

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

> 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。对其他边计数有类似推理。故等式成立。

推论：无向图中，度数为奇数的点一定有偶数个。

图同构（graph isomorphism）

若对图$G=(V,E)$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$G\cong G'$表示图同构。

直观地讲，同构图之间，仅仅是顶点的名字不同。

图的计数：

问题：以集合$V=\{1,2,\dots,n\}$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：$|\binom{V}{2}|=\binom{n}{2}$为$K_n$的边数。每条边可能在图中，也可能不在图中，故以$V$为顶点的图共有$2^{\binom{n}{2}}$种。

问题：以集合$V=\{1,2,\dots,n\}$中的元素为顶点构造图$G=(V,E)$，其中$E\subseteq\binom{V}{2}$。求问能构成多少个不同构的图？

例：三个顶点所组成互不同构的图共有4种。

解：显然，答案不会超过$2^{\binom{n}{2}}$。而一个n个点的图至多与$n!$个不同的图同构。于是如果记答案为X，那么有

$$\frac{2^{\binom{n}{2}}}{n!}\leqslant X\leqslant 2^{\binom{n}{2}}$$

然后对上下界进行估值：

$$\begin{aligned}\log_2 2^{\binom{n}{2}}&=\binom{n}{2}=\frac{n^2}{2}(1-\frac{1}{n})\\ \log_2\frac{2^{\binom{n}{2}}}{n!}&=\binom{n}{2}-\log_2 n\geqslant\binom{n}{2}-\log_2 n^n=\frac{n^2}{2}(1-\frac{1}{n}-\frac{2\log_2 n}{n})\end{aligned}$$

于是就有

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

练习题4.2

欧拉图

欧拉图（Eulerian graph）：如果从图$G=(V,E)$上的某一点v出发，存在沿图E中边的一个连续游走（walk），该游走覆盖所有的顶点，且用到E中每条边一次且仅一次，最后回到点v，则称G是欧拉图。其中闭合的游走被称为一条**欧拉回路（Euler tour）**。

欧拉图的判定：**欧拉图定理**：图$G=(V,E)$是欧拉图当且仅当图G是连通图，且每个顶点的度数都是偶数。

> 必要性证明：
>
> 欧拉图必然是连通的。
>
> 而每个点的度数都是偶数：由于要求是回路，那么对于一个点，进入一次必然会离开一次。
>
> 充分性证明：
>
> 考虑图G中最长的边不重复的游走方案$T=(v_0,e_1,v_1,\dots,e_m,v_m)$。由于$T$已经最大，所以所有与$v_m$相关联的边都已含在$T$中。且已知$v_m$的度数为偶数，如果$v_m$出现在游走方案中间$T=(v_0,e_1,v_1,\dots,e_i,v_m,e_{i+1},\dots,v_m)$，那么中间的每个$v_m$对$v_m$的度数贡献是2。出现在末端的$v_m$对$v_m$的度数贡献为1。而又由于$v_m$的度数为偶数，则$v_0=v_m$。也就是说$T=(v_m,e_1,v_1,\dots,e_m,v_m)$。所以$T$是回路。
>
> 若T不是欧拉回路，由于G是连通图，所以必然存在$e=\{u,v\}$，e不包含在T中，但又与T中的某个点$v=v_i$相关联。这样的话$|u,e,v_i,e_{i+1}\dots,e_i,v_i|=|T|+1$与$T$的最长性矛盾。所以$T$是欧拉回路。

进一步的问题：对图$G=(V,E)$，是否存在一个连续的游走方案，使E中的每条边e在方案中恰好出现一次。对于非欧拉图，若存在则必然不是欧拉回路，这样的游走方案被称为**欧拉道路**。

定理：图$G=(V,E)$中存在欧拉道路当且仅当图G是连通的且或者1、所有顶点度数都为偶数，或者2、除2个顶点度数为奇数外，其余顶点的度数都是偶数。且度数为奇数的两个点必为欧拉道路的起点和终点。

> 情况2的充分性证明：
>
> 设度数为奇数的两个点为u,v，在u,v之间增加边$e=\{u,v\}$，那么$G+e$就是欧拉图。这个图的欧拉路径必然会用到边e。去掉e后就得到了以u,v为起点和终点的欧拉道路。

有向欧拉图

有向图的入度（indegree）：$\deg_G^+(v)=|u:(u,v)\in E|$；

有向图的出度（outdegree）：$\deg_G^-(v)=|u:(v,u)\in E|$；

> chy-2003注：这里的定义似乎同样不能有效地表示重边。

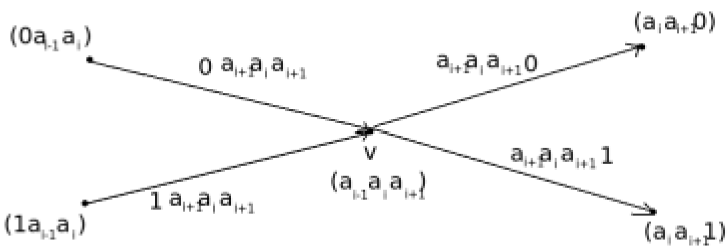
有向图的对称化（symmetrization）：给定有向图$G=(V,E)$，定义$sym(G)=(V,\overline{E})$，其中$\overline{E}=\{\{x,y\}:(x,y)\in E\vee(y,x)\in E\}$。

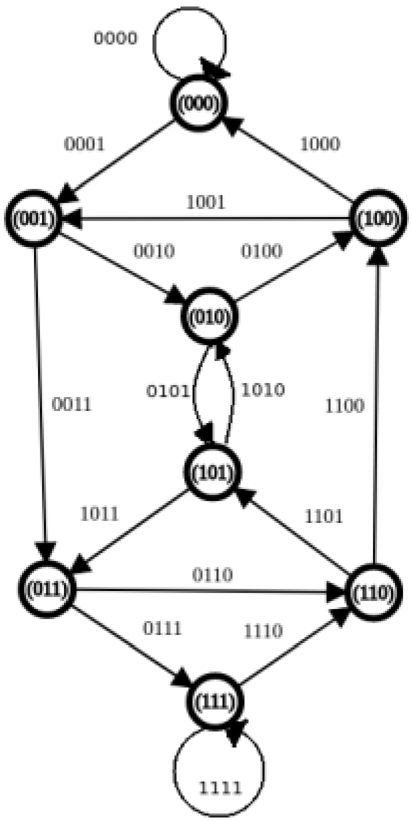
性质：有向图$G=(V,E)$含欧拉环（即依边集E的方向的一个连续游走方案，用到所有的边正好一次）的充分必要条件是$sym(G)$是连通图且对V中所有点v都有$\deg_G^+(v)=\deg_G^-(v)$。

> 证明：同无向图欧拉定理。

编码盘

问题：一个编码盘的底盘可转动且分成16个相等的扇面。每个扇面上写入0或者1，顶部四个位置的扇面可见。顺时针读取当前可见扇面的值，为一个4位二进制输出。试问底盘上的16个二进制数的序列应如何设置，使得转动编码盘底盘正好能输出所有的4为二进制编码？

> 分析：
>
> 如果当前的状态为$a_1a_2a_3a_4$，逆时针方向旋转一个扇面，那么新的输出是$a_2a_3a_4a_5$。定义如下点集和有向边：点$(a_{i-1}a_ia_{i+1}),(a_i,a_{i+1},a_{i+2})$，有向边$a_{i-1}a_ia_{i+1}a_{i+2}=((a_{i-1}a_ia_{i+1}),(a_ia_{i+1}a_{i+2}))$。
>
> 不难发现$|V|=2^3=8$，$\deg_G^+(v)=\deg_G^-(v)=2$。
>
> 
>
>
> 我们可以画出整个图



于是存在有向欧拉回路，如

$$
\begin{gathered}
0000, 0001, 0010, 0101, \\
1010, 0100, 1001, 0011, \\
0110, 1101, 1011, 0111, \\
1111, 1110, 1100, 1000
\end{gathered}
$$

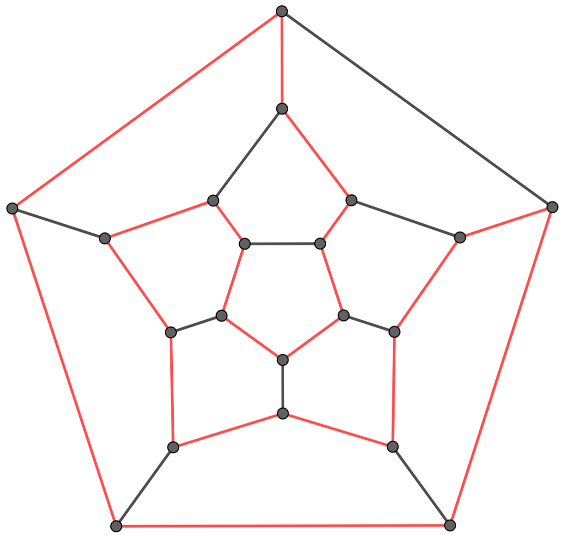
于是我们就能得到一种答案：

0000101001101111

练习题5.1

哈密顿图与Ore定理

背景：19世纪英国数学家哈密顿（Sir William Hamilton）提出问题：正凸12面体，把20个顶点比作世界上20个城市，30条棱表示这些城市间的交通路线。问，能否周游整个世界，即从某个城市出发，经过每城市一次且只一次，最后返回出发地。



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。

哈密顿道路（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道路。

注意：讨论哈密顿图相关的时候一般指简单图。因为重边和自环显然没有用。

判断哈密顿图的充分（不必要）条件：

定理[Dirac 1952]：$|G| = n \geqslant 3$，且$\delta(G) \geqslant \frac{n}{2}$，则图$G$一定是哈密顿图。

> 因为$\delta(G) \geqslant \frac{n}{2}$，图$G$必为连通图。（若不是连通图，则取顶点个数最少的连通分支G'，必有$\delta(G') < |G'| \leqslant \frac{n}{2}$。）
>
> 取G中最长路径$P = x_1 \dots x_k$。显然有$N(x_1) \subseteq P, N(x_k) \subseteq P$。
>
> 取$i \in [1, \dots, k-1]$，$k \leqslant n$，其中
>
> $$\begin{cases} |i : \{x_i, x_k\} \in E(G)| \geqslant \frac{n}{2} \\ |i : \{x_1, x_{i+1}\} \in E(G)| \geqslant \frac{n}{2} \end{cases}$$
>
> 如果记第一个集合为A，第二个集合为B，那么显然有$|A| + |B| > n$。也就是说存在一个i，使x_i与x_k相邻且x_{i+1}与x_1相邻。那么我们构造$x_1 x_{i+1} P x_k x_i P x_1$是一个环。而由于$P$的最大性，$P$经过了图$G$中所有顶点，所以图$G$是哈密顿图。（这一部分证明与欧拉图中类似，不再重复。）

注意：这个定理不是必要条件。

判断哈密顿图的充分（不必要）条件：

定理[Ore 1960]：图$G = (V, E)$，$|G| = n \geqslant 3$。对任意不同$u, v \in V$，若u, v不相邻，则$\deg_G(u) + \deg_G(v) \geqslant n$。满足以上条件的图$G$是哈密顿图。

> 证明：与上一个证明类似，略。

显然，Dirac定理是Ore定理的特例。

注意：这个定理不是必要条件。

引理：图$G=(V,E)$，$|G|=n\geqslant 3$。若存在不相邻的点$u,v\in V$且$\deg_G(u)+\deg_G(v)\geqslant n$，则$G=(V,E)$是哈密顿图当且仅当$G'=(V,E\cup\{\{u,v\}\})$是哈密顿图。

> 必要性显然。
>
> 充分性：（反证法）
>
> 若G'中有哈密顿回路而G中没有，则G'中的哈密顿回路P必经过边$e=\{u,v\}$。
>
> $P-e$是以u,v为始点和终点的哈密顿道路。接下来证明$\deg_G(u)+\deg_G(v)<n(*)$。
>
> 若$\deg_G(u)+\deg_G(v)\geqslant n$，则同Dirac定理的证明，从$P-e$可构造不含$e$的哈密顿回路，与假设矛盾。
>
> $(*)$与命题前提矛盾，故假设错误。即G为哈密顿图。

判断哈密顿图的必要（不充分）条件：

定理：如果图$G=(V,E)$是哈密顿图，则对所有非空子集$S\subseteq V$，必然有$Con(G-S)\leqslant|S|$。

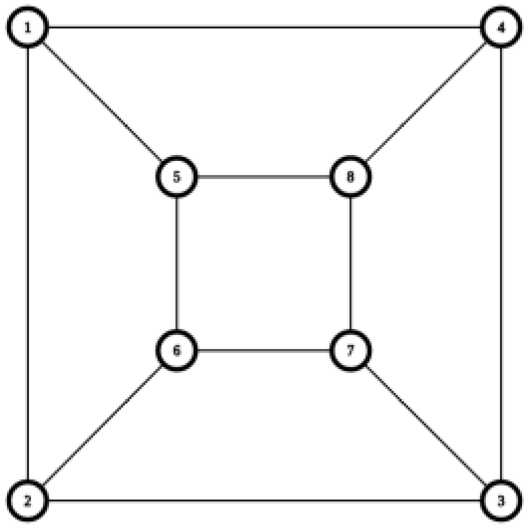
> 设C是图G中的一条哈密顿回路，易验证对于v的每个非空子集$Con(C-S)\leqslant|S|$。
>
> 而$C-S$是$G-S$的生成子图，故$Con(G-S)\leqslant Con(C-S)\leqslant|S|$。

练习题5.2

握手定理的应用（一）： Smith定理

定理（Smith）：对3正则图，包含图上任意边的哈密顿回路必有偶数条。

> 证明：（Thomason 1978）
>
> 思路：选取图G中任意一条边e，构造图G'，使图G'中的顶点的度数为1或2。当顶点度数为1时，能证明原图G中必有一条含e的哈密顿回路。由于G'受到握手定理限制，所以G'中必然存在第2个点度数为1。而因为对应关系，原始图G中必存在另一条哈密顿回路。
>
> 过程：图G是3正则图，$e=\{v_1,v_2\}$是一条固定的边。为了不失一般性，假设原图中存在含有e的哈密顿回路。
>
> 构造图$G'=(V',E')$。
>
> V'中的每一个点，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。）
>
> 接下来构造E'。$v_P\in V'$代表哈密顿路径$P=v_1,v_2,...,v_n$。由于v_n在G中度数为3，故必存在$1<k<n-1$满足$\{v_k,v_n\}\in E(G)$。于是可构造另一条路径$P'=v_1v_2\ldots v_kv_nv_{n-1}\ldots n_{k+1}$是哈密顿路径。令$\{v_P,v_{P'}\}\in E'$。
>
> G'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中的一个哈密顿回路。（因为v_n和v_1相邻，就只能构造出一个$1<k<n-1$满足$\{v_k,v_n\}\in E(G)$。反之$\deg(v_P)=2$。
>
> 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$\deg(v_Q)=1$。
>
> 例子：

> 
>
>
> 如图，假设我们固定$e=\{1,2\}$。一开始获得路径12348765(1)。8与5相邻，我们可以得到12348567。7和3, 8响铃，能得到12348765和12376584(1)。前者重复，不再考虑，而后者是另一条哈密顿回路。

握手定理的应用（二）：Sperner引理

Sperner引理（平面）：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，用红黄蓝三色依次对A、B、C三个顶点着色。然后这样对剩余顶点着色：

> - BC边上的点用黄色或者蓝色；
> - AB边上的点用红色或者黄色；
> - AC边上的点用红色或者蓝色；
> - 对余下的内部顶点任意着色。

这样必然存在一个三个顶点不同色的小三角形。

> Sperner's lemma 的证明：
>
> 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，记为v。
>
> E：两个点之间有一条边，当且仅当原对应平面相邻且相邻边顶点着色为红和蓝。
>
> 接下开考虑G中顶点的度数：
>
> V在ABC内（非点v）度数非0的情况：
>
> 1、三个顶点分别为红黄蓝；2、三个顶点两红一蓝；3、三个顶点两蓝一红。
>
> 其余情况度数均为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中必还有度数为奇数的点，即情况1必然发生。

Sperner's lemma的完整形式（sperner 1928）：对任意n维单形体（n-simplex）进行分割并用$n+1$中颜色去着色，则任何合适的单形分割着色方案下，都必有一个包含所有不同颜色的单元。$n=1$时，是两端颜色不同的线段，$n=2$就是上面所述的情况，$n=3$时是四面体……

练习题5.3

树

树的刻画

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

引理：对任意树T，如果$|T| \geqslant 2$，则T必含至少两个终点。

> 取T中的一条极长路径P，则因为T中没有环，且P极长，所以P的两端即为终点。

树的生长引理（Tree-growing lemma）：对图G及图G上的叶子节点v而言，图G是树当且仅当图$G-v$是树。

> 充分性证明：
>
> 由于G无环，那么$G-v$显然也无环。而对图G中任意不为v的点对x, y，x到y的路径不经过点v，所以$G-v$连通。
>
> 必要性证明：
>
> 由于$\deg(v) = 1$，且$G-v$无环，那么图G也无环。
>
> 假设加入的边为$\{u, v\}$，那么对于$G-v$任何点x，都有路径v到u到x可达。所以图G连通。

树的等价刻画：对于图$G = (V, E)$而言，以下称述等价：

> - 图G是树。
> - 路径唯一：对任意两点$u, v \in V$，存在从u到v的唯一路径。
> - 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。
> - 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。
> - Euler方程：G是连通图，且$|V| = |E| + 1$。

下面证明第1条和第5条等价。

> 1蕴含5：（归纳法）
>
> 连通性显然。当$|V| = 1$时，结论成立。假设当$|V| = n$时成立，当$|V| = n+1$时，根据树的生长引理，去掉一个叶子后仍是一棵树。根据归纳假设，这时结论成立。而加回这个点会使点数和边数同时增加1，所以结论假设成立。
>
> 5蕴含1：（归纳法）
>
> 当$|V| = 1$时，结论平凡。设$|V| = n$时结论平凡。当$|V| = n+1 = |E| + 1 \geqslant 2$时，根据握手定理，图$G$中顶点度数之和为$2|V| - 2$。故图$G$中必然存在度数小于2的顶点。且图$G$是连通图，任何顶点的度数非0，所以存在度数为1的点，记为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。根据树的生长定理，G也是树。

练习题6.1

有根树同构

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）。约定在节点上画向下箭头标明。

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）**。

一般的图之间，图的同构问题尚无有效的算法；而有根树之间的同构有快速算法。

定义：$(T,r)\cong' (T',r')$当且仅当$f:V(T)\to V(T')$是$T\cong T'$且$f(r)=r'$。

显然，$\cong'$关系严格强于$\cong$。

思路：将树的比较转化为字符串比较。

字符串比较：**字典序（Lexicographic order）**：对不同的序列$s=s_1s_2\dots s_n$和$t=t_1t_2\dots t_m$。如果s是t的初始序列（即$t=st_{n+1}\dots t_m$），则$s<t$；如果t是s的初始序列（即$s=ts_{m+1}\dots s_n$），则$t<s$。否则令i是$s_i\neq t_i$的最小下标，若$s_i<t_i$，则$s<t$；若$s_i>t_i$，则$s>t$。

过程：对有根树(T,r)如下编码：

> R1：所有非根叶节点都赋值为01。
>
> R2：假设点v的儿子节点为$w_1,w_2,\dots,w_k$都已各完成赋值，为$A(w_i)$，且$A(w_1)\leqslant A(w_2)\leqslant\cdots\leqslant A(w_k)$。则对$v$节点赋值为$0A(w_1)A(w_2)\dots A(w_k)1$。
>
> 根节点r的编码就是(T,r)的编码，用$\#(T,r)$表示。

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

> 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$S=S_1S_2\dots S_t$。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……可以根据此恢复出有根树，且显然这样的有根树必然是同构的。

树同构的判定

一般的树之间的同构也有快速的算法。

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

距离（Distance）：图G中的两个顶点u,v，$dis_G(u,v)$表示u,v之间的最短路径的长度。若u,v不在一个连通分支里，定义$dis_G(u,v)=\infty$。

偏心率（Excentricity）：图G及图中的顶点v，偏心率定义为：$ex_G(v)=\max\limits_{u\in G}dis_G(u,v)$。

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。中心可能任意大，例如环和完全图的$C(G)=V(G)$。

性质：对树$T=(V,E)$，$C(T)$含至多两个顶点，且若$C(T)=\{x,y\}$，则$\{x,y\}\in E$。

> 若$|T|\leqslant 2$，结论显然，否则利用树的特殊性：与树上任意一点v距离最远的点必然是叶子节点，
>
> 从T构造T'：T'是从T中删去所有叶子节点。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）。

用树的中心来完成树到有根树的转化：

> $|C(T)|=1$，则中心v就是根，输出$\#(T,v)$。

> $|C(T)|=2$，$C(T)=\{x_1,x_2\}, e=\{x_1,x_2\}$，$T-e$必然含有正好两个连通分支$T1,T2$。不失一般性，设$x_1\in V(T_1), x_2\in V(T_2)$。计算$\#(T_1,x_1),\#(T_2,x_2)$，若$\#(T_1,x_1)\leqslant\#(T_2,x_2)$，输出$\#(T,x_1)$，否则输出$\#(T,x_2)$。
>
> $\#T$为以上过程的输出。

性质：$T\cong T'$当且仅当$\#T\cong' \#T'$。

> 证明：与有根树类似。

练习题6.2

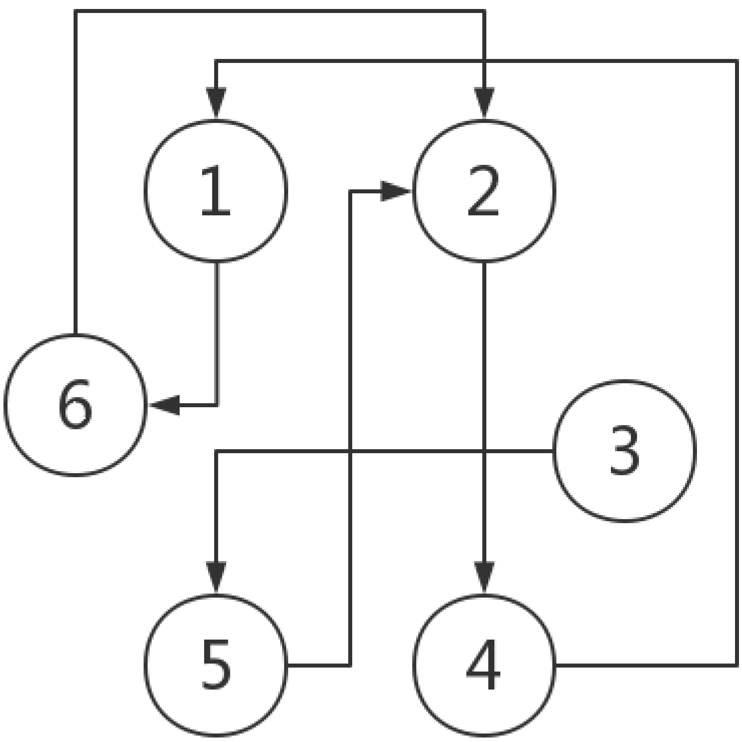
生成树计数

生成树（Spanning tree）：对连通图$G=(V,E)$，生成树是包含G中所有顶点且为树的子图。

问题：K_n的生成树共有多少种？（K_n为有n个顶点的完全图。）

特殊情况：$n=2$时，有1种生成树；$n=3$时，有3种生成树；$n=4$时，有$4+12=16$种；$n=5$时，有$5+60+60=125$种；$n=6$时，有$6+360+120+90+360+360=1296$种。

Caley定理（Caley's formula）：K_n的生成图个数是n^{n-2}个。

> - 定义1：**函数图（function graph）**：$f:V\to V$。如下面的函数：
>
> | v | **1** | **2** | **3** | **4** | **5** | **6** |
> |---|---|---|---|---|---|---|
> | $f(v)$ | 3 | 4 | 5 | 1 | 2 | 2 |
>
> 
>
>
> 不难发现函数与函数图一一对应。当$|V|=n$时共有n^n种不同的函数图。

- 定义2：**脊椎动物（Vertebrate）骨骼标本**：三元组(T,h,b)被称为骨骼标本若其中T是一棵树且$h,b\in V$。h被称为颈椎骨，v被称为尾椎骨。注意：h,b除了必须是树上节点外没有任何要求（可重合）。
- 定义3：**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。
- 证明过程：

用T_n表示$K_n=(V,E)$的生成树个数。每一棵树对应n^2种骨骼标本。我们希望证明骨骼标本与V上的函数图一一对应，有n^n种。如果如此，那么$T_n=\frac{n^n}{n^2}=n^{n-2}$。接下来证明骨骼标本与$V$上的函数图一一对应。

从骨骼标本对应到函数图：

让脊椎上的点被从小到大排序后对应位置的点指向。也就是说，如果依次有点$8,3,2,19,4,6$，那么就有如下对应关系：

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

（也就是说上面一行是下面一行排序后的结果。）这样得到了若干个环。然后再将剩余的点向环连边。如果上面的例子中还有$e_1=\{1,2\}$和$e_2=\{5,1\}$，那么$f(5)=1$，$f(1)=2$。

这样，骨骼标本就与函数图一一对应了。

接下来证明函数图与骨骼标本一一对应：

显然函数图中必然有环。我们找出所有的环，然后将环上的点如上表这般从小到大写在第一行，然后根据函数图中的对应关系写出第二行。那么第二行从左至右就是骨骼标本的颈椎骨到尾椎骨了。最后加入剩下的点，就可以得到与之对应的骨骼标本。

这样一来，我们证明了骨骼标本与函数图一一对应。所以$T_n=n^{n-2}$成立。

最小生成树

带权图（weighted graph）：$G=(V,E,w)$是带权图，其中(V,E)是无向图，w是对边的赋值的集合，即边的权重。

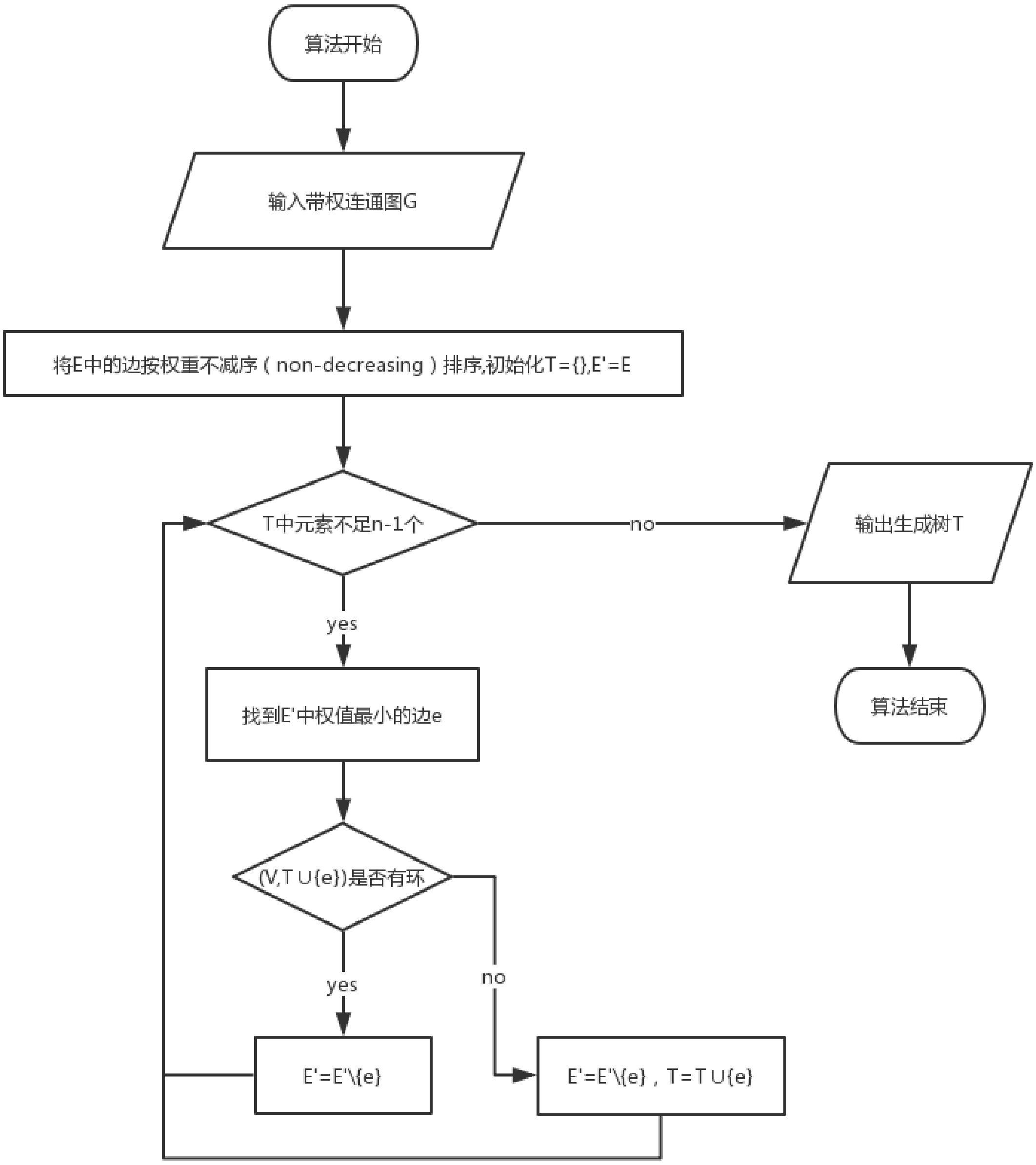
有时使用$w(G)$表示$\sum\limits_{e\in E}w(e)$。

最小生成树（Minimum spanning tree）：给定带权图G，最小生成树是(V,E)的生成树中代价最小的树。最小生成树不一定唯一。

Caley定理（Caley's formula）：n个顶点能构成的不同生成树共有n^{n-2}种。

Kruskal算法：

- 输入：连通带权图$G_w=(V,E,\alpha)$。
- 输出：最小生成树T。
- 算法流程：

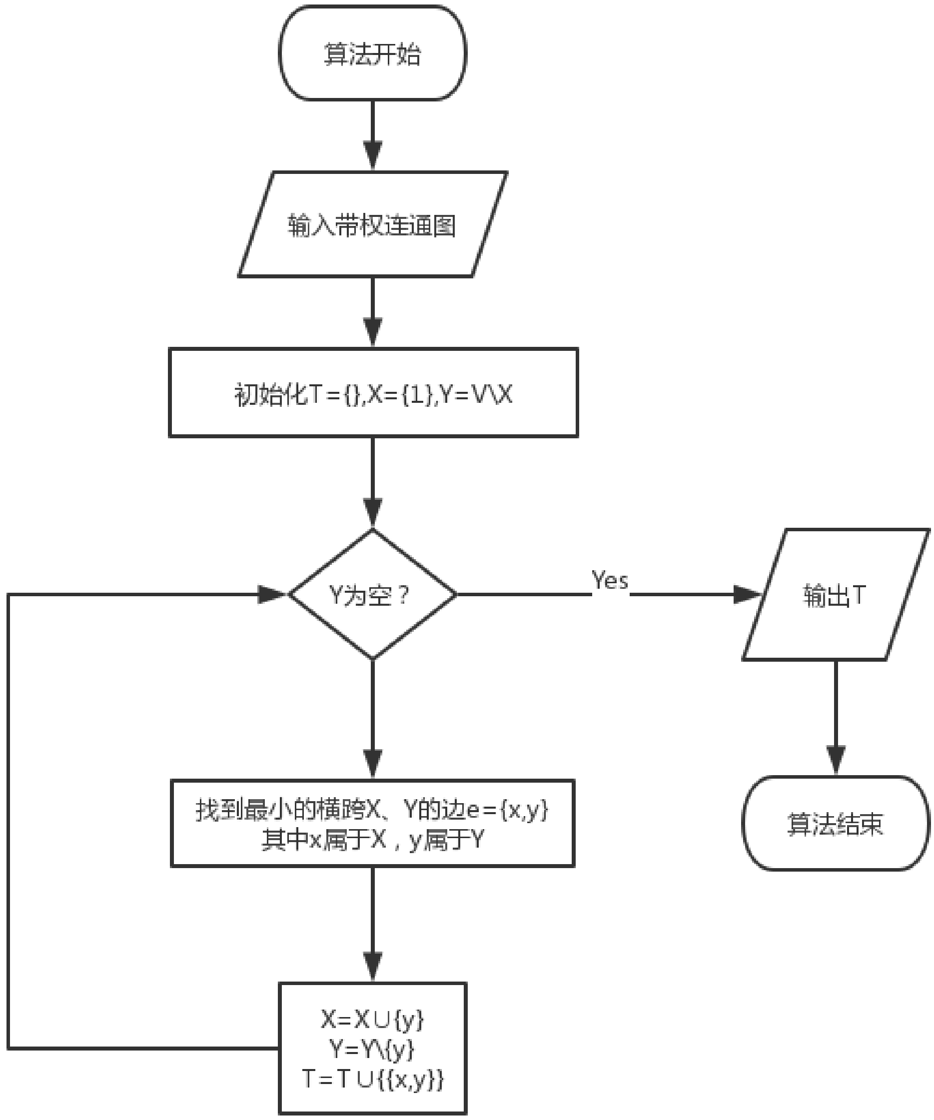


- 正确性证明：

每次加边减少一个连通分支，而原图是连通图，所以$n-1$次之后就变成了一个连通分支，算法结束。而对于任何生成树T_0^*，用$e=\{u,v\}$表示被算法加入的第一条不在T_i^*中的边。把e加入T_i^*必然产生环。T_i^*中u到v的路径上必然存在一条不在T中的边e'，且$w(e') \geqslant w(e)$。更新$T_{i+1}^* = (T_i^* \{e'\}) \cup \{e\}$。那么显然$w(T_{i+1}^*) \leqslant w(T_i^*)$，最终能得到$T \lhd T_{i+1}^*$。正确性得证。

Prim算法：

- 算法流程：



- 正确性证明：

显然算法会在有限步后结束，因为每一步我们都减少了一个连通分支。而由于每次加入的边跨两个集合，所以一定不会有环。算法的过程是在不断地生长一棵树，所以输出一定是一棵树。那么我们只需要证明这棵树是最小生成树就好了。

任何一棵原图的生成树T_0^*。用$e=\{u,v\}$表示被算法加入的第一条不在T_i^*中的边。把e加入T_i^*必然有环，T_i^*中u到v的路径上必然存在一条不在T中的边e'，且$w(e')\geqslant w(e)$。更新$T_{i+1}^*=(T_i^*\{e'\})\cup\{e\}$。那么显然$w(T_{i+1}^*)\leqslant w(T_i^*)$，最终能得到$T\lhd T_{i+1}^*$。正确性得证。

练习题6.3

网络流

基本概念

流网络（Flow network）：(G,s,t,c)，其中$G=(V,E)$是有向图，源点（Source）s，汇点（Sink）t和容量函数（Capacity function）：$\forall e\in E, c(e)\in R, c(e)>0$。

割（Cut）：顶点集V被划分为两个集合A,B，其中$s\in A, t\in B$。常用$\{A,B\}$表示割。

容量（Capacity）：从集合A到集合B的边的容量之和。$c(A,B)=\sum\limits_{u\in A,v\in B}c(u,v)$。

最小割（Min-cut）问题：寻找容量最小的割。

流（Flow）：给定流网络(G,s,t,c)，流函数$f:V\times V\to R$满足如下条件：

> - $f(u,v)\leqslant c(u,v)$**（Capacity constraint，流量限制）**；
> - $f(u,v)=-f(v,u)$**（Skew symmetry，对称性）**；
> - $\sum\limits_{v\in V}f(u,v)=0$对任意$v\in V\backslash\{s,t\}$成立**（Flow conservation，流量平衡）**；
> - 一个流的值被定义为从源点出发的流量之和$|f|=\sum\limits_{v\in V\backslash\{s\}}f(s,v)$。

最大流（Max-flow）问题：寻找值最大的流。

对流函数f，经过割$\{A,B\}$的流用$f(A,B)$表示：$f(A,B)=\sum\limits_{u\in A,v\in B}f(u,v)$。

同时，$f(u,B)\triangleq f(\{u\},B)$，$f(A,v)\triangleq f(A,\{v\})$。

性质1：对给定流网络(G,s,t,c)上的任意割$\{X,Y\}$以及流f，$|f|=f(X,Y)$。

> 证明：对$|X|$做归纳。
>
> 当$X=\{s\}$时，由流的定义，结论成立。假设对割$\{X,Y\}$结论成立。对任意$w\in Y\backslash\{t\}$，考察新割$\{X',Y'\}=\{X\cup\{w\},Y\backslash\{w\}\}$：
>
> $$\begin{aligned}f(X',Y')&=f(X,Y)+f(w,Y)-f(X,w)-f(w,w)\\&=f(X,Y)+f(w,Y)+f(w,X)-0\\&=f(X,Y)+f(w,V)\\&=f(X,Y)+0\\&=|f|\end{aligned}$$

上述结论同样说明：

$$\begin{aligned}|f|&=\sum_{v\in V\backslash\{s\}}f(s,v)\\&=f(s,V\backslash\{s\})\\&=f(V\backslash\{t\},t)\\&=\sum_{v\in V\backslash\{t\}}f(v,t)\end{aligned}$$

性质2：最大流值小于等于最小割容量。

> 证明：对流函数f，对任意$s-t$割$\{A,B\}$：
>
> $$\begin{aligned}|f| &= f(A,B)\\ &= \sum_{u\in A, v\in B} f(u,v)\\ &\leqslant \sum_{u\in A, v\in B, f(u,v)\geqslant 0} f(u,v)\\ &\leqslant \sum_{u\in A, v\in B} c(u,v)\\ &= c(A,B)\end{aligned}$$

最大流最小割定理

剩余图（Residual graph）：

> 对于流网络(G,s,t,c)，其中$G=(V,E)$。定义：
>
> - 原始边$e=\{u,v\}\in E$，剩余边（Residual edge）$e=\{v,u\}$。
> - 关于流f的剩余容量（Residual Capacity）：
>
> $$c_f(e)=\begin{cases} c(e)-f(e) & if \quad e\in E\\ f(e) & if \quad e^R\in E\end{cases}$$
>
> - 剩余图：$G_f=(V,E_f)$：关于流f的剩余流量为正的剩余边，及相应正剩余容量。
>
> 即：$E_f=\{e: f(e)<c(e)\}\cup\{e^R: f(e)>0\}$。

定义流的加法：f是G上的流，f'是关于流f的剩余图G_f上的流，对所有$u,v\in V$，定义

$(f+f')(u,v)=f(u,v)+f'(u,v)$。

性质：f是G上的流，f'是关于流f的剩余图G_f上的流，则$f+f'$也是G上的流。

> 证明：定义$g=f+f'$。
>
> 容量限制：
>
> $$\begin{aligned}g(u,v) &= f(u,v)+f'(u,v)\\ &\leqslant f(u,v)+(c(u,v)-f(u,v))\\ &= c(u,v)\end{aligned}$$
>
> 对称性：
>
> $$\begin{aligned}g(v,u) &= f(v,u)+f'(v,u)\\ &= -f(u,v)-f'(u,v)\\ &= -(f(u,v)+f'(u,v))\\ &= -g(u,v)\end{aligned}$$
>
> 流量平衡：

> 对$\forall v \in V\backslash\{s,t\}$，有$\sum\limits_{v\in V} f(u,v)=0, \sum\limits_{v\in V} f'(u,v)=0$。故
>
> $$\sum_{v\in V} g(u,v)=\sum_{v\in V}(f(u,v)+f'(u,v))=0$$

扩流路径（Augmenting Path）：对流网络G和流f，剩余图G_f中s到t的简单路径P。

流量瓶颈（Bottleneck capacity）：扩流路径P各边在G_f中的最小剩余容量值，记为b。

扩流：沿路径P扩流（$Augment(f,P)$）：对所有$e\in P$，如果$e\in E$，$f^+(e)=f(e)+b$；如果$e^R\in E$，$f^+(e)=f(e)-b$。对所有$e\notin P$，$f^+(e)=f(e)$。

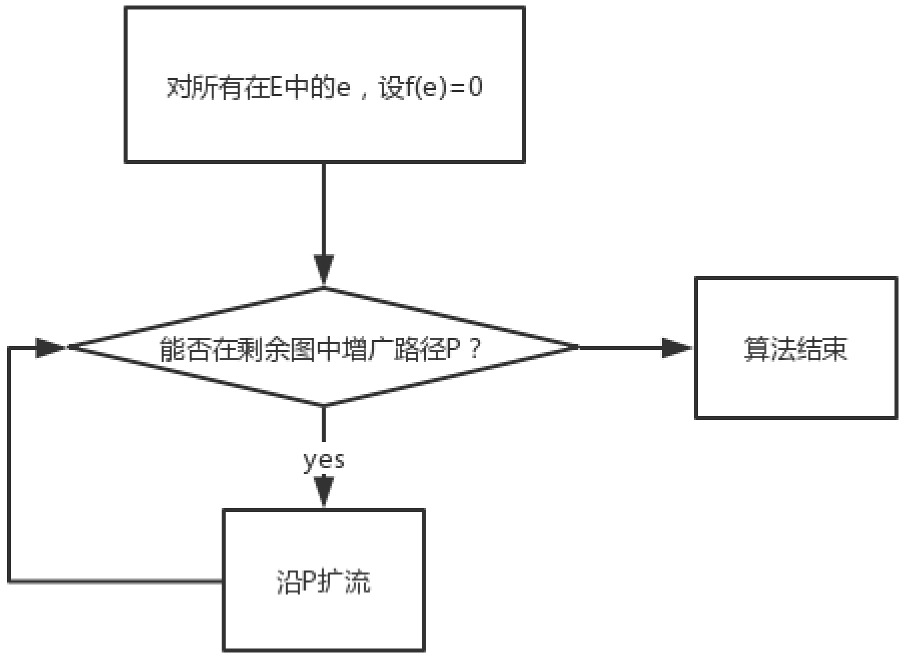
最大流最小割定理（Max-flow min-cut theorem）：对流网络(G,s,t,c)以及该网络上的流f，如下三个命题互相等价：

> 1、存在一个割$\{A,B\}$，有$c(A,B)=|f|$；
>
> 2、流f是原流网络中的一个最大流；
>
> 3、不存在相对于流f的扩流路径。

证明：

> $1\to 2$：对任意割$\{A,B\}$和流g，有$|g|\leqslant c(A,B)$。故$c(A,B)=|f|$蕴含$|g|\leqslant|f|$，即f是最大流。
>
> $2\to 3$：如果存在相对于流f的扩流路径，则可沿P扩充，得到一个值更大的流。
>
> $3\to 1$：若命题3成立，设A是从s出发沿剩余图G_f可达到的所有点，$B=V\backslash A$。则G_f中不含从A到B的路径，故原图从B到A的边的流为0。类似的，原图上从A到B的所有边e，都有$f(e)=c(e)$。此时$c(A,B)=f(A,B)=|f|$。

Ford-Fulkerson最大流算法：



> 分析：若容量函数取值为整数，设(G,s,t,c)的最大流为f^*，则Ford-Fulkerson算法运行过程中至多迭代$|f^*|$次。

改进的算法：

对(G,s,t,c)，$G=(V,E)$，$n=|V|$，$m=|E|$。

> - Edmonds-Karp Algorithm: $O(nm^2)$。要点：使用最短路径算法来选择下一条扩流路径。
> - Dinic's Algorithm: $O(n^2m)$。要点：改进Edmonds-Karp Algorithm，使用了Blocking flow（而不是Augment path）来选择扩流方案。

应用：二分图匹配（略）。

练习题6.4