1. Logic and Proof

Propersition : A statement that is either true or false

Compound Propersition : $p\ q\ r \quad \vee \wedge \neg$

$p \vee \neg p \Rightarrow$ true $\quad p \wedge \neg p \Rightarrow$ false

$\equiv$: def $P \equiv Q$ (logically equialment) if they have same truth table

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

p iff q (iff : if and only if)

Contrapositive : 逆否命题 $\neg q \to \neg p \equiv p \to q$

Converse : 逆命题 $q \to p$

$\neg(p \wedge q) \equiv \neg p \vee \neg q$

$\neg(p \vee q) \equiv \neg p \wedge \neg q$

2. Quantifier

$\neg(\forall x\, P(x)) \iff \exists x\, \neg p(x)$

$\neg(\exists x\, P(x)) \iff \forall x\, \neg p(x)$

$\neg(\forall x \exists y)(P(x,y)) \iff (\exists x \forall y)(\neg P(x,y))$

3. Proof Method

1. Direct proof $p \to q$

2. Indirect proof

- proof by contraposition $\neg q \to \neg p$

To proof $p \to q$:

Suppose $\neg q$

⋮

Therefore $\neg p$

- proof by contradiction

To proof : P

Suppose $\neg p \Rightarrow r \wedge \neg r \Rightarrow$ false

Therefore : p

Example : Prove $\sqrt{2}$ is irrational

Suppose $\sqrt{2}$ is rational : $\sqrt{2} = \frac{a}{b}$ $a, b \in \mathbb{Z}$ and a, b have no common factor

$\sqrt{2}$ is rational $\Rightarrow$ $(\sqrt{2})^2$ is rational

$\Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2 \Rightarrow$ a is even

let $a = 2k \Rightarrow 2b^2 = 4k^2 \Rightarrow b^2 = 2k^2 \Rightarrow$ b is even

$\therefore$ a, b have common factor : 2

contradiction

$\therefore \sqrt{2}$ is irrational

4. Mathmatical Induction

(1) Basis : P(1) hold

(2) IH : for $\forall k \in \mathbb{Z}$, $k > 1$ P(k) hold

(3) Inductive Step : NTS : P(k+1) hold
(Need to show)

Strong Inductive

(1) Basis

(2) IH : For $m \in \mathbb{Z}^+$ $1 \le m \le k$ p(m) hold.

(3) Inductive Step : NTS P(k+1)

当我们发现初始条件不止一项的时候，就应考虑 Strong Induction

Fundamental Theorem of Arithmetic

Every positive integer $n \ge 2$ is either prime or can be written as product of primes

Example :

Consider the following pseudocode for a recursive version of the Euclidean algorithm:

```
Euclid(a, b) // a >= b >= 0, a,b integers
if b = 0
    return a
else
    return Euclid(b, a mod b)
```

(a) (1 point) Prove: $\gcd(a, b) = \gcd(b, a - b)$.

(b) (1 point) Let r be the remainder if we divide a by b. Prove: $\gcd(a, b) = \gcd(b, r)$.

(c) Write a proof of correctness for the pseudocode above.

(a) let $\gcd(a, b) = d$

According to Bezout Theorem: $x, y \in \mathbb{Z}$. s.t.

$xa + by = d$

$d = xa - xb + xb + by$

$= x(a-b) + (x+y)b$

According to Bezout Identity

$\gcd(a-b, b) = d = \gcd(a, b)$

(b) ...

(c): Basis : $b = 0$ $Euc(a, 0) = \gcd(a, 0) = a$

IH: (Strong Induction) For any $m \in \mathbb{Z}$, $0 \le m \le k$ $(k \in \mathbb{Z})$. $Euc(a, k) = \gcd(a, k)$

Inductive: $Euc(a, k+1) = Euc(k+1, a \bmod k+1)$ ($r \le k$)

$= \gcd(k+1, a \bmod k+1) = \gcd(a, k+1)$

5. Number Theory

Divisibility : $a, b, c \in \mathbb{Z}$ $a | b \Leftrightarrow b = ac$

Properties of Divisibility

$a,b,c \in \mathbb{Z}$:

① $a|b,\ a|c \Rightarrow a|(b+c)$

② $a|b \Rightarrow a|bc$

③ $a|b,\ b|c \Rightarrow a|c$

Corollary: $a|b, a|c \Rightarrow a|mb+nc,\ m,n \in \mathbb{Z}$

Division Algorithm: $a,b \in \mathbb{Z}$. there exist unique $q,r \in \mathbb{Z}$. $0 \le r < b$

$a = bq + r$

Greatest Common Divisor (gcd)

DEF:

① $a,b,c \in \mathbb{Z}$. c is a common divisor of a,b. if $(c|a) \wedge (c|b)$

② greatest common divisor: d.

1) $d|a$ and $d|b$

2) For all $c \in \mathbb{Z}$. if $c|a$ and $c|b$ then $c|d$.

Theorem: $a = bq + r$ $\gcd(a,b) = \gcd(b,r)$

Bezout Theorem: $a,b \in \mathbb{N}^*$. $\exists$ s.t such that $sa + tb = \gcd(a,b)$ ☆

Bezout Identity

s,t ⇒ Bezout Coefficients

⇓

Insight: $\gcd(a,b) = d$ is the smallest positive integer that a,b can represent in format $xa+yb$.

6. Modular Arithetic

DEF:

$a,b \in \mathbb{Z}$. $m \in \mathbb{Z}^+$ a is congruent to b Modular M if $m|(a-b)$ i.e. $a-b = km$. $(k \in \mathbb{Z})$

Notation:

$a \equiv b \pmod m$ $a \not\equiv b \pmod m$

Theorem: $a,b \in \mathbb{Z}$. $m \in \mathbb{Z}^+$.

$a \equiv b \pmod m$ iff a & b have the same remainder when divided by m

Theorem: $a \equiv b \pmod m$ iff $a = b + km$ $(a,b,k \in \mathbb{Z}.\ m \in \mathbb{Z}^+)$

Addition Multiplication:

Theorem: $m \in \mathbb{Z}^+$

$a \equiv b \pmod m$

$c \equiv d \pmod m$ $\Rightarrow$ $\begin{cases} a+c \equiv b+d \pmod m \\ a \cdot c \equiv b \cdot d \pmod m \end{cases}$

→ Think about. Can we say $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod m$?

No: ⇒ $a = 5$

$b = 10$

$c = 2$

$m = 10$

How to deal with $a^b \pmod m$ efficiently?
(write exponent as a sum of power of 2)

Ex: $11^7 \pmod{13}$ $\quad 11^7 = 11^{4+2+1}$

$11^2 = 121 \equiv 4 \pmod{13}$

$11^4 \equiv 4^2 \equiv 16 \equiv 3 \pmod{13}$

$11^7 \equiv 4 \cdot 3 \cdot 11 \equiv 132 \equiv 2 \pmod{13}$

Multiplicative Inverse

Theorem: $a, m \in \mathbb{Z}$. $m > 1$ if $\gcd(a,m) = 1$ then a has a multiplicate inverse mod m
i.e. there is an $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod m$ $\quad (0 < b \le m$. b is unique)

Proof: $a, m \in \mathbb{Z}, \gcd(a,m) = 1 \Rightarrow sa + tm = 1 \Rightarrow sa = 1 - tm$

$sa \equiv 1 - tm \equiv 1 \pmod m$

Theorem: if p is prime and $a \not\equiv 0 \pmod p$ then a has a multiplicative inverse mod p.

Euclid Algorithm: Ex: Find an inverse of 101 modulo 4620

$\gcd(101, 4620) = 1$

每次都把 r 換掉

$4620 = 45 \cdot 101 + 75$ r

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1$

$\Rightarrow$

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$\vdots$

$= -35 \cdot 4620 + 1601 \cdot 101$

$\therefore$ 1601 is an inverse of 101 modulo 4620

Fermat's Little Theorem (FLT)

Theorem: if p is prime and $\gcd(a,p) = 1$ (p∤a) then $a^{p-1} \equiv 1 \pmod p$

Corollary: $a^p \equiv p \pmod p$ for any a, p

Can we say? $\Rightarrow$ $a^{p-1} \equiv 1 \pmod p \Rightarrow p$ is prime ? X

Chinese Remainder Theorem (CRT)

$M = m_1 \cdot m_2 \cdot m_3 \cdots m_n \Rightarrow$ (互質)

$M_i = \frac{M}{m_i}$ $\quad M_i M_i^{-1} \equiv 1 \pmod{m_i}$

$x \equiv r_i M_i M_i^{-1} \pmod m$

Ex. $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$ $\quad M = 105$

$\begin{cases} M_1 = 35 \\ M_2 = 21 \\ M_3 = 15 \end{cases} \Rightarrow \begin{cases} M_1^{-1} = 2 \\ M_2^{-1} = 1 \\ M_3^{-1} = 1 \end{cases}$

$x \equiv \sum_{i=1}^{n} M_i M_i^{-1} r_i \equiv 23 \pmod{105}$

FLT 特殊例子：p 是素数怎么办？ ⇒ FLT + CRT

Find $3^{2021} \pmod{35}$. Use Fermat's little theorem and the Chinese remainder theorem. Show all your work and explain how you arrived at your answer.

Solution: $35 = 5 \cdot 7$ 5: prime 7: prime ⇒ CRT.

let $M = 5 \times 7 = 35$ $M_1 = 7$ $M_2 = 5$

$1 = 3 \times 5 - 2 \times 7 \Rightarrow M_1^{-1} = -2$ $M_2^{-1} = 3$

$r_i \Rightarrow \begin{cases} 3^{2021} \equiv r_1 \pmod 5 \\ 3^{2021} \equiv r_2 \pmod 7 \end{cases}$ $\Rightarrow 3^4 \equiv 1 \pmod 5$ $3^{2021} = (3^4)^{505} \times 3 \equiv 3 \pmod 5$ $r_1 = 3$

$\Rightarrow 3^6 \equiv 1 \pmod 5$ $3^{2021} = (3^6)^{336} \times 3^5 \equiv 3^5 \equiv 5 \pmod 7$ $r_2 = 5$

$\Rightarrow x \equiv \sum_{i=1}^{2} M_i M_i^{-1} r_i = 33 \pmod{35}$ $\therefore 3^{2021} \equiv 33 \pmod{35}$

CRT 的特殊例子：m_i 之间不互质怎么办？

$\begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 7 \pmod{15} \end{cases} \Rightarrow$ Transfer $x \equiv 1 \pmod 6 \Leftrightarrow (x \equiv 1 \pmod 2) \wedge (x \equiv 1 \pmod 3)$ ↑include

Then: $x \equiv 7 \pmod{15} \Rightarrow x = 15k + 7 = 3(5k+2) + 1 \equiv 1 \pmod 3$

(1)

$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 7 \pmod{15} \end{cases}$ CRT ⇒ $x \equiv 7 \pmod{30}$

7. Counting

Addition:

Def: size of set Ex: $S = \{1,2,3\}$ $|S| = 3$

inclusive - exclusive Principle: $|A \cup B| = |A| + |B| - |A \cap B|$

Disjoint: A and B disjoint $\Leftrightarrow A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$

Addition Rule: A, B finite sets, $A \cap B = \emptyset$.
⇒ there are $|A| + |B|$ ways to choose an element from $|A \cup B|$

Product Rule: if an activity can be performed in t successive steps and step i can be done in n_i ways independent of the outcome of previous steps. Then the activity can be done in $n_1 \times n_2 \times \cdots \times n_t$ ways

Complementary Counting: $P(n,k) = n(n-1)\cdots(n-k+1)$

n-factorial $n! = P(n,n)$

$C(n,k) = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{(n-k)! \cdot k!} = C(n, n-k)$

Properties of Combination

① Bijective Counting: $C(n,k) = C(n,n-k)$

$S \xrightarrow{1-1} T$ and $T \xrightarrow{1-1} S$ (one to one relationship)

② Recursion Property: $\underbrace{C(n,k)}_{i} = \underbrace{C(n-1,k-1)}_{ii} + \underbrace{C(n-1,k)}_{iii}$

i: # of pick k num from n

ii: # of pick k num from n, contain person A

iii: # of pick k num from n, without person A

Binomial Theorem (Newton's Formula)

① $(a+b)^n = C(n,0)a^n b^0 + C(n,1)a^{n-1}b^1 + \cdots + C(n,n)a^0 b^n$

$= \sum_{i=1}^{n} C(n,i)\, a^{n-i} b^i$

② $a=b=1 \Rightarrow \quad C(n,0)+C(n,1)+\cdots+C(n,n) = 2^n$

Combinations with repetition (stars and bars)

Ex1: Using chocolate (c) Vanilla (v) and strawberry (s) to make 4 dessert order

⇒ cccc ccc v ccvs ···

stars and bars: n type of objects, how many different sets consisting of r objects.

$C(n+r-1, n-1) = C(n+r-1, r)$

∴ $C(3+4-1,4) = 15$ ↪ 我的理解：把 r 個完全相同的東西放入 n 個不同盒子

Ex2: How many solutions to $x_1+x_2+x_3+x_4+x_5 = 13 \quad x_i \geq 0$

把 13 個球放進 5 個盒 $C(5+13-1, 5-1) = C(17,4)$

Permutation with repitition

MAMMAL _ _ _ _ _ _ : $\frac{6!}{3!2!1!}$

general result: $\frac{n!}{n_1!\, n_2! \cdots n_k!}$ k type.

8. Discrete Probability Theory

Basic concept: 1. sample space: S ex: 2 coin toss {HH, HT, TH, TT}

2. event: subset of sample space

3. probability space:

Sample space: S Function: P

$\forall x \in S \quad p(x) > 0$

$\sum_{x \in S} p(x) = 1$

4. Axioms 公理

① $0 \leq P(A) \leq 1$ For every event A

② $P\emptyset = 0 \qquad P(S) = 1$

③ if event A is a disjoint union of A_i

$$P(A) = \sum_i P(A_i)$$

Uniform Distribution:

Uniform distribution over sample space S

$$P(x) = \frac{1}{|S|} \qquad P(A) = \frac{|A|}{|S|}$$

Theorem: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

$$P\left(\bigcup_{j=1}^{n} A_i\right) \le \sum_{i=1}^{n} P(A_i)$$ with equality holding iff A_i is pairwise disjoint

Theorem: $P(\bar{A}) = 1 - P(A)$ $\quad A \cup \bar{A} = S$

Coditional Probability:

Two events A, B. Suppose know B occured

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$ (B发生情况下 A发生的概率)

Ex: Prob of sum of 2 dice ≥ 10 when 1st dice < 6?

A: sum ≥ 10 $\quad P(A) = \frac{1}{6}$

B: 1st roll < 6 $\quad P(B) = \frac{5}{6}$

$P(A \cap B) = \frac{1}{12}$

$$P(A|B) = \frac{\frac{1}{12}}{\frac{5}{6}} = \frac{1}{10}$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \qquad P(A \cap B) = P(A|B) \cdot P(B)$$ Multiplication Law

Law of total probability

Def: Partition: A partition of S is a collection of pairwise disjoint events

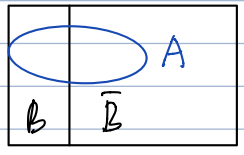
$$\begin{cases} \text{①} \ \bigcup_{j=1}^{m} B_i = S \\ \text{②} \ B_i \cap B_j = \phi \quad i \ne j \end{cases}$$

$(B, \bar{B})$ partition

Theorem:

Partition B_i of S event: A

$$P(A) = \sum_{i=1}^{m} P(A|B_i) \cdot P(B_i)$$



$$\Rightarrow P(A) = P(A \cap B) + P(A \cap \bar{B}) = P(A|B) \cdot P(B) + P(A|\bar{B}) \cdot P(\bar{B})$$

Bayes' Law

$$P(B|A) = \frac{P(A|B)\cdot P(B)}{P(A)} = \frac{P(A\cap B)}{P(A)}$$

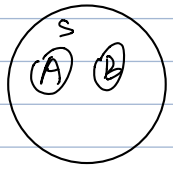
$$= \frac{P(A|B)\cdot P(B)}{P(A|B)\cdot P(B) + P(A|\bar{B})\cdot P(\bar{B})}$$

Independence:

A, B. independence => if $P(A\cap B) = P(A)\cdot P(B)$

Propersition: if A, B independence => $P(A|B) = P(A)$

$P(B|A) = P(B)$



=> A, B independ ? => No. $P(A|B) = 0$

$P(A) \neq 0$

Positively correlate => $P(A\cap B) > P(A)\cdot P(B)$

negatively correlate => $P(A\cap B) < P(A)\cdot P(B)$

Mutually Independence

$A_1, A_2, \cdots A_n$ are mutually independent if for any sub section

$A_{i1}, A_{i2}, \cdots, A_{im}$ $P(A_{i1}\cap A_{i2}\cap\cdots\cap A_{im}) = P(A_{i1})\cdot P(A_{i2})\cdots P(A_{im})$

=> check pair wise independence

Bernolli Trail (Mutually independent)

2 outcomes => { p success; 1-p failure

Prob of exact k success in n trails => $\binom{n}{k} p^k (1-p)^{n-k}$

9. Expectation

Random Variable

Def: random Variable is a function R that:

$S \xrightarrow{R} \mathbb{R}$

S: sample space; $\mathbb{R}$: real number

Def: An indicator random variable is R.V. with range {0, 1}

Def: If R is R.V. define $P(R=r) = P\{x=S: R(x)=r\}$

Def: independent: 2 R.V R_1 R_2 independent if

① $P(R_1=x_1 \mid R_2=x_2) = P(R_1=x_1)$

② $P(R_1=x_1 \wedge R_2=x_2) = P(R_1=x_1)\,P(R_2=x_2)$

To prove independent need to prove every pair of x_i, x_j

Mutually independent: $R_1, R_2, \cdots R_n$ mutually independent R.V.

if For all $r_1, r_2, \cdots, r_n \in R$ $\begin{cases} P(R_1 \wedge R_2 \cdots \wedge R_n) = P(R_1)P(R_2)\cdots P(R_n) \\ P(R_1=r_1 \wedge \cdots \wedge R_n=r_n) = P(R_1=r_1)\cdots P(R_n=r_n) \end{cases}$

Expectation

The expect value of R.V. R over S is

$$E(R) = \sum_{x \in S} R(x)\,P(x) = \sum_r r\,P(X=r)$$

Linearity of Expectation

Theorem: For any R.V. R_1 and R_2 on S, $E(R_1+R_2) = E(R_1)+E(R_2)$

Corollary: $E(R_1+R_2+\cdots+R_n) = E(R_1)+E(R_2)+\cdots+E(R_n)$

不以一相互独立

e.g. n位检查帽子是否原子取 X_i: 第i位拿到原来帽子

$E(X)$:

$$X_i = \begin{cases} 1 & \text{person } i \text{ get his hat} \\ 0 & \text{o/w.} \end{cases}$$

$$X = \sum_{i=1}^{n} X_i \quad E(X) = \sum E(X_i) = n \cdot \frac{1}{n} = 1$$

Bernoulli Trail: $E(X) = np$

Expectation of product

if R_1, R_2 indep $\Rightarrow$ $E(R_1 \cdot R_2) = E(R_1)\,E(R_2)$

Geometric R.V. 几何分布

Bernoulli $\Rightarrow$ $\begin{cases} P \\ 1-P=q \end{cases}$ $\Rightarrow$ How many trails occur before we obtain success?

Sample space $= \{S, FS, FFS, \cdots\}$

$\Rightarrow P(X=k) = q^{k-1}p$

$$E(X)=\sum_{k=1}^{\infty} p(k)\cdot k = \sum_{1}^{\infty} k\cdot(1-p)^{k-1}\cdot p = \frac{p}{q}\sum_{k=1}^{\infty} k\cdot q^k$$

10. Variance

Def: $Var(R) = E[(R-E(R))^2]$

Def: Standard deviation $\sigma(R) = \sqrt{Var(R)}$

Properties for variance

① $Var \geq 0$

② $Var(X) = E(X^2) - (E(X))^2$

③ $E(X^2) \geq (E(X))^2$

Single bernoulli trail: $\begin{cases} 1 : p \\ 0 : 1-p \end{cases}$ $E(X)=p$

$E(X)=p$

$V(X)=p(1-p)$

$V(X) = E(X^2) - (E(X))^2 = E(X) - (E(X))^2 = p(1-p)$

Linearity of Variance: R_1, R_2 indep $\Rightarrow Var(R_1+R_2) = Var(R_1) + Var(R_2)$

n bernoulli trails $\Rightarrow E(X)=np$ $Var(X)=np(1-p)$

Markov's and Chebyshev's inequality

Markov: for non-negative R.V. $S \to \mathbb{R}$ where $R(x) \geq 0$ for all $x \in S$, for any positive real number $a>0$

$$P(R \geq a) \leq \frac{E(R)}{a}$$

Ex: R: IQ score. $E(R)=100$. $a=200$ $P(R \geq 200) \leq \frac{1}{2}$

Chebyshev: Let $R: S \to \mathbb{R}$ and let $r>0$ be a positive real number

$$P(|R-E(R)| \geq r) \leq \frac{Var(R)}{r^2}$$

Ex: R: sum of roll 2 fair dice

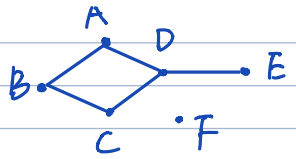
$E(R)=7$ $Var(R) = E(R^2) - (E(R))^2 = 54.833 - 49 = 5.833$

↳ $2^2\cdot\frac{1}{36} + 3^2\cdot\frac{1}{36} + \cdots + 12^2\frac{1}{36}$

题值: $P(|R-7| \geq 5) \leq \frac{5.833}{5^2} = 0.233$

实际: $P(R=2) + P(R=15) = 0.056$

11. Graph Theory



DEF: $G = (V, E)$ V : set of vertices $= \{A, B, C, D, E, F\}$

E : set of edges $= \{(A,B), (A,D), (B,C), (C,D), (D,E)\}$

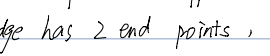
DEF: ① each $e \in E$ has 2 end-points

② B is adjacent to A ; edge (A, B) incident to A

③ Neighbour : $N(D) = \{A, C, E\}$

④ Degree : $\deg(A) = 2$ $\deg(D) = 3$ $\deg(F) = 0$

⑤ simple graph: undirected graph with no loops 自环 or multiple edges 重边



Theorem (Handshake theory)

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

proof: The degree count # of times V appeared as an endpoint in an edge. Since each edge has 2 end points, each edge contribute 2 to the sum

Corollary : An undirected graph has an even number of vertices of odd degree
无向图有偶数个奇度顶点.

proof: V_1 : even deg V_2 : odd deg

$$2m = \underbrace{\sum_{v \in V_1} \deg(v)}_{\text{偶}} + \underbrace{\sum_{v \in V_2} \deg(v)}_{\text{奇}}$$

$\Downarrow$ must even

DEF: A list of non-negative integers $d_1, d_2, \ldots, d_n$ is graphic if it is the degree sequence of a simple graph

可图化判定: Havel-Hakimi Theorem

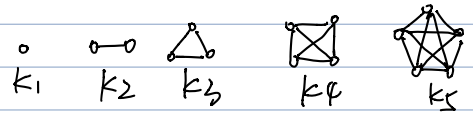
For $n > 1$, an integer d of size n is graphic iff d' is graphic where d' is obtained from d by deleting its largest element D and subtract 1 from its D-next-largest element

Ex. 1, 2, 2, 3, 3, 3, 3, 3 graphic ?

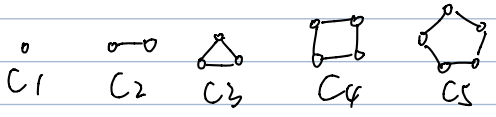
$n=8$, $D=3$: [3] 3, 3, 3, 3, 2, 2, 1 (2 2 2 3 2 2 1) ⇒ [3] 2 2 2 2 1 1 1 (1 1 1 2 2 1) ⇒ [2] 2 1 1 1 1 (1 0 1 1 1) ⇒ [1] 1 1 1 0 (0 1 1 0) ⇒ 1, 1, 0, 0 ⋮

Special kinds of graph

① complete graph $K_n = (V, E)$

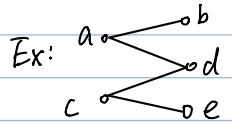


② cycle graph $C_n = (V, E)$

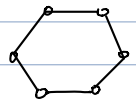
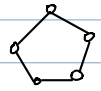


Bipartite Graph 二部圖

DEF: A Graph $G(V, E)$ is bipartite if its vertices can be partitioned into 2 disjoint subsets V_1, V_2, such that $V = V_1 \cup V_2$ and each edge connects a vertex in V_1 and a vertex in V_2. $E \subseteq \{(x,y) : x \in V_1, y \in V_2\}$

Ex: 

$V_1 = \{a, c\}$
$V_2 = \{b, d, e\}$

 ✓  X

Theorem: A graph is bipartite iff it contains no cycle of odd length

Subgraph: Def: $G' = (V', E')$ $G = (V, E)$ $V' \subseteq V$ $E' \subseteq E$ G': subgraph of G

Graph Isomorphism: 2 graph $G_1 = (V_1, E_1)$ $G_2 = (V_2, E_2)$ if $(V_1 = V_2 \wedge E_1 = E_2)$
$\Rightarrow G_1 \cong G_2$

↳ DEF: Two simple graph G_1, G_2 are isomorphic if there is bijection $f : V_1 \to V_2$ such that for all $x, y \in V_1$, there is an edge $(f(x), f(y))$ in E_2 (function preserves adjacency)

Check Isomorphism: ⇒ All ⇒ $n!$ mapping
⇒ shortcut ⇒ # vertices, # edges, degree sequence, subgraphs

path and connectivity

PATH: a finite sequence of vertices of $v_0, v_1, \ldots, v_n$ in V such that (v_{i-1}, v_i) is an edge in E for $1 \le i \le n$.

↳ path of length 0: single vertex

↳ circuit: begin and end at the same vertex

↳ simple circuit: no repeated edges (but can have repeted vertex)

↳ simple path: . . . . . .

CONNECTIVITY Undirected G: connected: if there is a path between every pair of vertices

Disconnected: o/w

Theorem: There is a simple path between every pair of vertices in connected undirected graph

Connected Component: G: simple undirected graph. A connected component of G is a connected subgraph of G that is maximal connected.

↳ This means: not a proper subgraph of any other connected subgraph

↳ connected undirected graph has 1 connected component

Theorem: Every simple undirected graph with n vertices and k edges ($k<n$) has at least $n-k$ connected component.

Proof: induction on k, #edges

Basis: $k=0$ G ⇒ n vertices, 0 edges, every vertex is a CC

There are exactly $n=n-0$ CC

Induction: IH: Assume P(k) holds

NTS: P(k+1) holds

↳ G has at least $n-(k+1)$ CC

Remove an arbitrary edge (u,v), get result G'

By IH ⇒ G' has at least $n-k$ CCs

Now add back edge (u,v)

↳ case1: if u,v in the same CC of G'

then G has same number of CCs as G'.

⇒ G has at least $n-k > n-k+1$ CC's ✓

↳ case 2: if u,v in the different CCs in G'

then these two CCs are merged, reducing the # of CCs by 1, so G has at least $n-k-1 = n-(k+1)$ CC. ✓

DEF: a complete bipartite graph $K_{l,m}$ is a bipartite graph ($V = V_1 \cup V_2$)

$l = |V_1|$ $m = |V_2|$ $n = l+m$ edge $= l \cdot m$

DEF: **Cut Edge**: (bridge) or a cut vertex of a simple graph is an edge or vertex whose deletion increases # of CC's

Distance: length of the shortest path

Diameter: max distance

Trees : connected undirected graph with no circuits

Theorem : every tree is bipartite

Properties: ① There is exactly 1 simple path between every pair of vertices
② Adding an edge between 2 vertices create a circuit
③ Removing an edge disconnected a graph
↳ every edge is a cut edge
④ $|E| = |V| - 1$

Theorem: An undirected graph is a tree iff there is a unique simple path between any two of its vertices

Euler Circuit & Path (通过所有边一次且仅一次)

Theorem: if G is a connected undirected simple graph,
the G contains a Euler Circuit iff every vertex has even degree
这种图叫欧拉图 : Eulerian (Proof 略)

Lemma: if G is a simple undirected graph in which the deg(v) at least 2.
Then G has a simple circuit

Proof: Let v any vertex of G. Construct a simple path $v_1 \to v_2 \to v_3 \to \cdots$
By choosing v_2 be any vertex adjacent to v_1 and for each $i > 1$
choose v_{i+1} to be any vertex adjacent to v_i except v_{i-1}:
The existence of such a vertex is guaranteed by our assumption
Since G has finite number of vertices we must eventually chosen
a vertex we chosen before. if v_k is 1st we have a simple
circuit. that path of the path that lies between 2 occurance of v_k is a
simple circuit.

Theorem: A connected graph G has a Euler path iff exactly 2 vertices have odd degree.

Hamilton Circuit and Path (经过所有顶点)

充分条件

Theorem: (ORE) if G is a simple graph with $n \geq 3$ vertices and if $\deg(u) + \deg(v) \geq n$ for each pair of non-adjacent vertices then G has a Hamilton circuit.

Theorem: (Dirac): 若 G is a simple graph with $n \geq 3$ vertices and if $\deg(v) \geq \frac{n}{2}$ for each vertex $v \in G$ Then G has a Ha...cir

必要条件

若 G 是 Hamilton. 对 V 的任意非空子集 S.

$$\underbrace{W(G-S)}_{\text{减去S后的连通分支数}} \leq \underbrace{|S|}_{\text{S中顶点个数}}$$