

1. Logic and Proof

Proposition : A statement that is either true or false

Compound Proposition : $P \vee Q \vee R \vee \dots$
 $P \vee \neg P \Rightarrow \text{true}$ $P \wedge \neg P \Rightarrow \text{false}$

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

$$\begin{array}{c} P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P) \\ \hline P \text{ iff } Q \quad (\text{iff: if and only if}) \end{array}$$

Contrapositive : 逆命題 $\neg q \rightarrow \neg p \equiv p \rightarrow q$

Converse : 逆命題 $q \rightarrow p$

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

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

2. Quantifier

$$\neg(\forall x P(x)) \Leftrightarrow \exists x \neg P(x)$$

$$\neg(\exists x P(x)) \Leftrightarrow \forall x \neg P(x)$$

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

3. Proof Method

1. Direct proof $p \rightarrow q$

2. Indirect proof

■ Proof by contraposition $\neg q \rightarrow \neg p$

To proof $p \rightarrow q$:

Suppose $\neg q$

:

Therefore $\neg p$

■ Proof by contradiction

To proof: p

Suppose $\neg p \Rightarrow r \wedge \neg r \Rightarrow \text{false}$

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

$\therefore \sqrt{2}$ is irrational

4 Mathematical Induction

- (1) Basis : $P(1)$ hold
- (2) IH : for $\forall k \in \mathbb{Z}, k \geq 1$ $P(k)$ hold
- (3) Inductive Step : NTS : $P(k+1)$ hold
(Need to show)

Strong Inductive

- (1) Basis's
 - (2) IH : For $m \in \mathbb{Z}^+$, $1 \leq m \leq k$ $P(m)$ hold.
 - (3) Inductive Step : NTS $P(k+1)$
-] 当我们发现证明起来不容易的时候，就应该用 Strong Induction

Fundamental Theorem of Arithmetic

Every positive integer $n \geq 2$ 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
01 if b = 0
02   return a
03 else
04   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.

(b) ..

(c) Basis : $b=0$ $\text{Fac}(a, 0) = \gcd(a, 0) = a$

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

Inductive : $\text{Fac}(a, k+1) = \text{Fac}(k+1, a \bmod k+1)$

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

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: $a|b, a|c \Rightarrow a|m(b+n)c, m, n \in \mathbb{Z}$

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

$$a = bq + r$$

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: $a = bq + r$ $\text{gcd}(a, b) = \text{gcd}(b, r)$

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

↓

Bézout Identity

$s, t \Rightarrow$ Bézout Coefficients

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



6. Modular Arithmetic

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:

$$a \equiv b \pmod{m} \quad a \not\equiv b \pmod{m}$$

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 $a = b + km \quad (a, b, k \in \mathbb{Z}, m \in \mathbb{Z}^+)$

Addition Multiplication:

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

$$\begin{aligned} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{aligned} \Rightarrow \left\{ \begin{array}{l} a+c \equiv b+d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{array} \right.$$

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

No: $\Rightarrow a=5$

$b=10$

$c=2$

$m=10$

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

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

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

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

$$11^7 \equiv 4 \cdot 3 \cdot 11 \equiv 122 \equiv 2 \pmod{13}$$

Multiplicative Inverse

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

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

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

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

$$\begin{aligned} \gcd(101, 4620) &= 1 && \text{每次都把上捨掉} \\ 4620 &= 45 \cdot 101 + 75 && | \\ 101 &= 1 \cdot 75 + 26 && | \\ 75 &= 2 \cdot 26 + 23 && \Rightarrow \quad | \\ 26 &= 1 \cdot 23 + 3 && | \\ 23 &= 7 \cdot 3 + 2 && | \\ 3 &= 2 \cdot 1 + 1 && | \\ & & & = -35 \cdot 4620 + 101 \cdot 101 \end{aligned}$$

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

Fermat's Little Theorem (FLT)

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

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

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

Chinese Remainder Theorem (CRT)

$$\begin{cases} M = m_1 \cdot m_2 \cdot m_3 \cdots m_n \Rightarrow (\exists \bar{M}) \\ M_i = \frac{M}{m_i} \quad M_i \bar{M}_i \equiv 1 \pmod{m_i} \\ x \equiv r_i M_i \bar{M}_i \pmod{m} \end{cases}$$

$$\text{Ex. } \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} M = 105 \\ M_1 = 35 \\ M_2 = 21 \\ M_3 = 15 \end{cases} \Rightarrow \begin{cases} M_1^{-1} = 2 \\ M_2^{-1} = 1 \\ M_3^{-1} = 1 \end{cases} \quad x \equiv \sum_{i=1}^n M_i M_i^{-1} r_i \equiv 23 \pmod{105}$$

FLT 特殊例子： p 不是素数或 1/n 的？ \Rightarrow 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 \Rightarrow CRT.

$$\begin{aligned} \text{let } M &= 5 \times 7 = 35 & M_1 &= 7 & M_2 &= 5 \\ 1 &= 3 \times 5 - 2 \times 7 \Rightarrow & M_1^{-1} &= -2 & M_2^{-1} &= 3 \end{aligned}$$

$$\begin{aligned} r_1 \Rightarrow \begin{cases} 3^{2021} \equiv r_1 \pmod{5} \\ 3^{2021} \equiv r_2 \pmod{7} \end{cases} &\Rightarrow 3^4 \equiv 1 \pmod{5} & 3^{2021} = (3^4)^{505} \times 3 \equiv 3 \pmod{5} & r_1 = 3 \\ &\Rightarrow 3^6 \equiv 1 \pmod{7} & 3^{2021} = (3^6)^{336} \times 3^5 \equiv 3^5 \equiv 5 \pmod{7} & r_2 = 5 \end{aligned}$$

$$\Rightarrow x \equiv \sum_{i=1}^2 M_i M_i^{-1} r_i = 23 \pmod{35} \quad \therefore 3^{2021} \equiv 23 \pmod{35}$$

CRT 的特殊例子， m_i 之间不互质怎么办？

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

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

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 7 \pmod{3} \end{cases} \stackrel{\text{CRT}}{\Rightarrow} x \equiv 7 \pmod{30}$$

7. Counting

Addition:

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

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, $A \cap B = \emptyset$.

\Rightarrow 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 $n_1 \times n_2 \times \dots \times n_t$ ways

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

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

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

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: $\underline{\frac{C(n, k)}{i}} = \underline{\frac{C(n-1, k-1)}{ii}} + \underline{\frac{C(n-1, k)}{iii}}$

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)

$$\begin{aligned} ① (a+b)^n &= C(n, 0) a^n b^0 + C(n, 1) a^{n-1} b^1 + \dots + C(n, n) a^0 b^n \\ &= \sum_{i=0}^n C(n, i) a^{n-i} b^i \end{aligned}$$

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

Combinations with repetition (stars and bars)

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

$\Rightarrow cccc \ cccv \ ccvs \dots$

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

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

$$\hookrightarrow C(3+4-1, 4) = 15 \quad \text{我的理解: 把 } r \text{ 个完全相同的东西放入 } n \text{ 个不同盒子里}$$

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

$$\text{把 } 13 \text{ 个球放进 } 5 \text{ 个盒} \quad C(5+13-1, 5-1) = C(17, 4)$$

Permutation with repetition

$$\text{M A M M A L} \quad \dots : \frac{6!}{3! 2! 1!}$$

$$\text{general result: } \frac{n!}{n_1! n_2! \dots n_k!} \quad k \text{ type.}$$

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:

$$\left\{ \begin{array}{l} \text{Sample space: } S \quad \text{Function: } P \\ \forall x \in S \quad p(x) \geq 0 \\ \sum_{x \in S} p(x) = 1 \end{array} \right.$$

4. Axioms of Probability

$$① 0 \leq p(A) \leq 1 \quad \text{For every event } A$$

$$② p(\emptyset) = 0 \quad p(S) = 1$$

② 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

$$P(X) = \frac{1}{|S|} \quad P(A) = \frac{|A|}{|S|}$$

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

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

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

Conditional Probability:

Two events A, B. Suppose know B occurred

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad (B \text{发生时} A \text{发生的概率})$$

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

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

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

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

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

$$P(A \cap B) = P(A|B) \cdot P(B)$$

Multiplication Law

Law of total probability

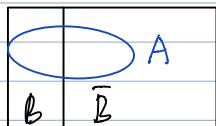
Def: Partition: A partition of S is a collection of pairwise disjoint events

$$\left\{ \begin{array}{l} \text{① } \bigcup_{i=1}^m B_i = S \\ \text{② } B_i \cap B_j = \emptyset \quad i \neq j \end{array} \right. \quad (\underbrace{B_1, B_2, \dots, B_m}_{\text{partition}})$$

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

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

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

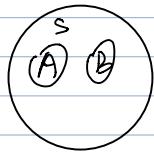
$$= \frac{P(A|B) \cdot P(B)}{P(A|B) \cdot P(B) + P(A|\bar{B}) \cdot P(\bar{B})}$$

Independence:

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

Proposition: if A, B independent $\Rightarrow P(A|B) = P(A)$

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



\Rightarrow A, B independent? \Rightarrow No. $P(A|B) = P(A) \neq 0$

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

Negatively correlate $\Rightarrow P(A \cap B) < P(A) \cdot P(B)$

Mutually Independence

A_1, A_2, \dots, A_n are mutually independent if for any subsection

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

\Rightarrow check pairwise independence

Bernoulli Trail (Mutually independent)

2 outcomes \Rightarrow $\begin{cases} p & \text{success} \\ 1-p & \text{failure} \end{cases}$

Prob of exact k success in n trials $\Rightarrow \binom{n}{k} p^k (1-p)^{n-k}$

9. Expectation

Random Variable

Def: random variable is a function that:

$$\begin{array}{ccc} S & \xrightarrow{R} & \mathbb{R} \\ \text{sample space} & & \text{real number} \end{array}$$

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

$$\textcircled{1} \quad P(R_1=x_1 | R_2=x_2) = P(R_1=x_1)$$

$$\textcircled{2} \quad P(R_1=x_1 \wedge R_2=x_2) = P(R_1=x_1) P(R_2=x_2)$$

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

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

If For all $r_1, r_2, \dots, r_n \in \mathbb{R}$, $P(R_1=r_1 \wedge R_2=r_2 \wedge \dots \wedge R_n=r_n) = P(R_1=r_1) P(R_2=r_2) \dots P(R_n=r_n)$

$$P(R_1=r_1 \wedge \dots \wedge R_n=r_n) = P(R_1=r_1) \dots P(R_n=r_n)$$

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: $E(R_1+R_2+\dots+R_n) = E(R_1)+E(R_2)+\dots+E(R_n)$
不互不相容事件

e.g. n次检查帽子是否属于自己 X_i : 第*i*次拿错后是否属于自己

$E(X_i)$:

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

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

$$= n \cdot \frac{1}{n} = 1$$

Bernoulli Trail: $E(X)=np$

Expectation of product

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

Geometric R.V. 定义

Bernoulli $\Rightarrow \begin{cases} p \\ 1-p=q \end{cases} \Rightarrow$ How many trials occur before we obtain success?
Sample space = {S, FS, FFS, ...}

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

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

10. Variance

Def: $\text{Var}(R) = E[(R - E(R))^2]$

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

Properties for variance

- ① $\text{Var} \geq 0$
- ② $\text{Var}(X) = E(X^2) - (E(X))^2$
- ③ $E(X^2) \geq (E(X))^2$

Single bernoulli trial: $\begin{cases} 1: P \\ 0: 1-P \end{cases}$ $E(X) = P$ $V(X) = E(X^2) - (E(X))^2 = E(X) - (E(X))^2 = P(1-P)$
 $V(X) = P(1-P)$

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

n bernoulli trials $\Rightarrow E(X) = np$ $\text{Var}(X) = n p(1-p)$

Markov's and Chebyshen's inequality

Markov: for non-negative R.V. $S \rightarrow \mathbb{R}$ where $R(n) \geq 0$
 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. $E(R) = 100$. $a = 200$ $P(R \geq 200) \leq \frac{1}{2}$

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

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

Ex: R : sum of roll 2 fair dice

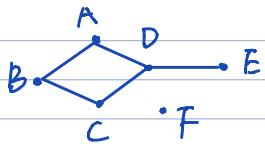
$$E(R) = 7 \quad \text{Var}(R) = E(R^2) - (E(R))^2 = 54.833 - 49 = 5.833$$

$$\hookrightarrow 2^2 \cdot \frac{1}{36} + 3^2 \cdot \frac{1}{36} + \dots + 12^2 \cdot \frac{1}{36}$$

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

$$\text{Ansatz: } P(R=2) + P(R=15) = 0.056$$

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 or multiple edges


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


Proof: V_1 : even deg V_2 : odd deg

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

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

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 graphic?

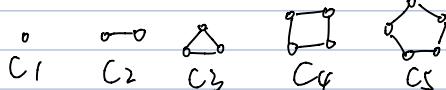
$$\begin{array}{l} n=8 \quad [3, 3, 3, 3, 2, 2, 1] \Rightarrow [3, 2, 2, 2, 2, 1] \Rightarrow [2, 2, 1, 1, 1] \Rightarrow [1, 1, 1, 0] \Rightarrow [1, 1, 0, 0] \Rightarrow \dots \\ D=3 \end{array}$$

Special kinds of graph

① complete graph $K_n = (V, E)$

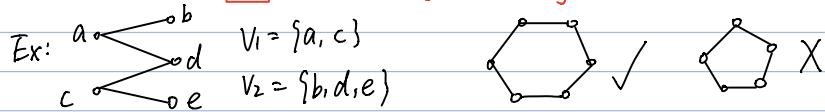


② cycle graph $C_n = (V, E)$



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 . $E \subseteq \{(x, y) : x \in V_1, y \in V_2\}$



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 graphs G_1, G_2 are isomorphic if there is a bijection $f: V_1 \rightarrow V_2$ 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 : \Rightarrow All $\Rightarrow n!$ mapping
 \Rightarrow shortcut \Rightarrow # vertices, # edges, degree sequence, subgraphs

path and connectivity

PATH : a finite sequence of vertices of V_0, V_1, \dots, V_n in V such that (V_{i-1}, V_i) is an edge in E for $1 \leq i \leq n$.

↳ path of length 0: single vertex

↳ circuit : begin and end at the same vertex

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

\hookrightarrow 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 ($k \leq n$)

has at least $n-k$ connected components.

Proof: induction on k , #edges

Basis: $k=0$ $G \Rightarrow n$ 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 $\Rightarrow G'$ has at least $n-k$ CCs

Now add back edge (u,v)

↳ case 1: if uv in the same CC of G'

then G has same number of CCs as G'

$\Rightarrow G$ has at least $n-k > n-k+1$ CC's ✓

↳ case 2: if uv 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 creates a circuit
 - ③ Removing an edge disconnects 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

这将问题转化为图论：Eulerian (Proof idea)

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 $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow \dots$

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 part of the path that lies between 2 occurrence 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 (哈密顿圈和路)

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): If 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 Hamil

必要条件

若 G 是 Hamilton. 对 v 和 任一非度零集 S .

$$\underbrace{w(G-S)}_{\text{若在 } S \text{ 后仍连通分枝}} \leq |S| \quad \begin{matrix} |S| \\ \text{若至两个} \end{matrix}$$