Mathematical Foundation of Computer Science

Notes of Class and Video

Counting (class)

$\{0,1\}^n := \{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}$
$= $ the set of all bit string of length n

$(0,0,1)$ or 001

$A_n : \{x \in \{0,1\}^n \mid x$ does not contain the pattern $11\}$
Q: Write down A_n and $|A_n|$ for $n=1,2,3,4$

$A_0 = \{\varepsilon\}$ $|A_0| = 1$
$A_1 = \{0,1\}$, $|A_1| = 2$
$A_2 = \{00, 01, 10\}$, $|A_2| = 3$
$A_3 = \{000, 001, 010, 100, 101\}$, $|A_3| = 5$
$A_4 = \{0000, 0001, 0010, 0100, 0101, 1000, 1001, 1010\}$, $|A_4| = 8$

Q: for general n?
idea:
for A_{n+2}:
add 0 to every element in A_{n+1}
add 10 to every element in A_n

Fibonacci: $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $\cdots$, $F_n = F_{n-1} + F_{n-2}$ $\forall n \geq 2$
Lemma. $|A_n| = F_{n+2}$
Proof. Induction on n
$n = 0, \cdots$
$n \geq 2$ (induction step):
$A_n = \{x \in \{0,1\}^n \mid x = 0y, y \in A_{n-1}\} \cup \{x \in \{0,1\}^n \mid x = 10z, z \in A_{n-2}\}$
$\Rightarrow |A_n| = |A_{n-1}| + |A_{n-2}|$
$= F_{n+1} + F_n = F_{n+2}$ ∎

by induction

Lemma. $F_n \le 2^{n-2} \quad \forall\, n \ge 2$

Proof 1. Induction on n

Proof 2. $F_n = |A_{n-2}| \le |\{0,1\}^{n-2}| = 2^n$ ∎

Lemma. $F_n \ge 2^{n/2-1} \quad \forall n \ge 2$

Proof 1. Induction on n

Proof 2. $B_n := \{x \in \{0,1\}^n \mid x = *0*0* \cdots\}$

$= \{x \in \{0,1\}^n \mid x_i = 0 \quad \forall i \text{ is even}\}$

$\subseteq A_n$

$\forall n \ge 0, \quad |A_n| \ge |B_n| = 2^{\lceil n/2 \rceil} \ge 2^{n/2}$

$\forall n \ge 2, \quad F_n = |A_{n-2}| \ge |B_{n-2}| = 2^{\lceil n/2-1 \rceil} \ge 2^{n/2-1}$ ∎

How fast does F_n grows: $\frac{1}{2}\sqrt{2}^n \le F_n \le \frac{1}{n} \times 2^n$

"Lemma." $F_n \le \alpha^n$, α is some number between $[\sqrt{2}, 2]$

"Proof."

$F_0 = 0 \le \alpha^0, \quad F_1 = 1 \le \alpha^1$

$F_n = F_{n-1} + F_{n-2} \le \alpha^{n-1} + \alpha^{n-2} \le \alpha^n$ "∎"

Observation. It goes through as long as $\alpha^{n-1} + \alpha^{n-2} \le \alpha^n \wedge \alpha \ge 1$

$$\begin{cases} \alpha + 1 \le \alpha^2 \\ \alpha \ge 1 \end{cases} \Rightarrow \alpha \ge \frac{1+\sqrt{5}}{2}$$

$\varphi_1 = \frac{1+\sqrt{5}}{2}$, $\varphi_2 = \frac{1-\sqrt{5}}{2}$

Lemma. $\varphi_1^{n-2} \leq F_n \leq \varphi_1^{n}$

Proof. use what's above and what's below $\square$

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} F_n + F_{n-1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$$

$$\overset{\text{def.}}{=\!=} A^1 \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \cdots = A^i \begin{pmatrix} F_{n-i+1} \\ F_{n-i} \end{pmatrix}$$

$$= A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Review.

Eigenvalue of A: $Au = \lambda u \iff (A - \lambda I)u = 0$

$$\Rightarrow \det(A - \lambda I) = 0$$

$$A - \lambda I = \begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix}$$

$$\det(A - \lambda I) = \det \begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - \lambda - 1 = 0$$

$$\Rightarrow \lambda = \varphi_1 \text{ or } \lambda = \varphi_2$$

Eigenvector

$$(A - \lambda I)u = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 - \varphi_1^2 + \varphi_1 \end{pmatrix} = \begin{pmatrix} 1-\varphi_1 & 1 \\ 1 & -\varphi_1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 \\ \varphi_1 - 1 \end{pmatrix}}$$

$$\underbrace{\varphi_1 \begin{pmatrix} 1 \\ \varphi_1 - 1 \end{pmatrix}}_{\text{also eigenvalue}} \overset{Au=\lambda u}{=\!=} A \begin{pmatrix} 1 \\ \varphi_1 - 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \varphi_1 - 1 \end{pmatrix} = \begin{pmatrix} \varphi_1 \\ 1 \end{pmatrix}$$

write $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ on the basis of eigenvector:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha \begin{pmatrix} \varphi_1 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} \varphi_2 \\ 1 \end{pmatrix}$$

$$\Rightarrow \alpha + \beta = 0$$

$$= \alpha\begin{pmatrix}\varphi_1\\1\end{pmatrix} - \alpha\begin{pmatrix}\varphi_2\\1\end{pmatrix}$$

$$= \begin{pmatrix}\alpha(\varphi_1-\varphi_2)\\0\end{pmatrix}$$

$$\Rightarrow \alpha = \frac{1}{\varphi_1-\varphi_2} = \frac{1}{\sqrt{5}}$$

$$\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix}\varphi_1\\1\end{pmatrix} - \frac{1}{\sqrt{5}}\begin{pmatrix}\varphi_2\\1\end{pmatrix}$$

$$\begin{pmatrix}F_{n+1}\\F_n\end{pmatrix} = A^n\begin{pmatrix}1\\0\end{pmatrix} = A^n\left[\frac{1}{\sqrt{5}}\begin{pmatrix}\varphi_1\\1\end{pmatrix} - \frac{1}{\sqrt{5}}\begin{pmatrix}\varphi_2\\1\end{pmatrix}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\varphi_1^n\begin{pmatrix}\varphi_1\\1\end{pmatrix} - \varphi_2^n\begin{pmatrix}\varphi_2\\1\end{pmatrix}\right]$$

Review.

$$Au = \lambda u$$

$$\Rightarrow A^n u = A^{n-1}\lambda u = \lambda A^{n-1} u = \cdots = \lambda^n u$$

$$F_n = \frac{\varphi_1^n - \varphi_2^n}{\sqrt{5}}$$

$$\frac{F_{n+1}}{F_n} = \frac{\varphi_1^{n+1} - \varphi_2^{n+1}}{\varphi_1^n - \varphi_2^n} \xrightarrow{\infty} \varphi_1 = 1.619$$

What is A^n:

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$$

$$A^n A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a+b \\ c+d \end{pmatrix}$$

$$= \begin{pmatrix} F_{n+1} + b \\ F_n + d \end{pmatrix} = \begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix}$$

$\Rightarrow b = F_n, \ d = F_{n-1}$

$$\Rightarrow A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Lemma. $F_{n+1} \times F_{n-1} = F_n^2 + (-1)^n$

Proof 1. Induction on n. $\blacksquare$

proof 2. Use formula. $\blacksquare$

proof 3. $\det(A^n) = \det \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$

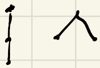
$$= \det^n(A) = (-1)^n \quad \blacksquare$$

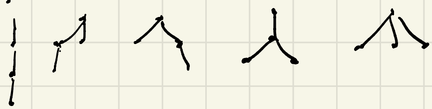
Catalan Numbers (class)

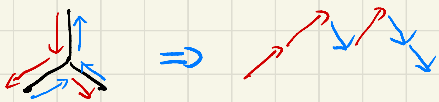
Q1: Mountain Ranges  how many possible paths?

Q2: ( )((( )))

Q3: Trees: n-edge, how many possible?

n=2:  T_2 2

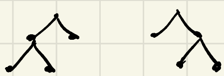
n=3:  T_3 5

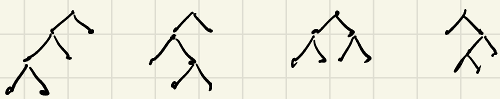


Q4: Binary Trees: Always 0 or 2 children

How many bi-trees with n

n=1  B_1 1

n=2  B_2 2

n=3  B_3 5

Q5:

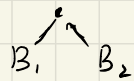
$$M_n := \left|\left\{ x \in \{+1,-1\}^{2n} \;\middle|\; \sum_{i=1}^{k} x_i \geq 0 \;\; \forall k = 1, \dots, 2n-1, \; \sum_{i=1}^{2n} x_i = 0 \right\}\right|$$

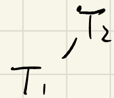
M_0 : $\{\}$ $\qquad M_0 = 0$

M_1 : $(+1, -1)$ $\qquad M_1 = 1$

M_2 : $(+1, +1, -1, -1)$, $(+1, -1, +1, -1)$, $\quad M_2 = 2$

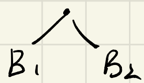
back to binary tree with n nodes (B) and n-edge tree (T)

B = • or 

T = • or 

B2T(Binary Tree B)

if B = • return •

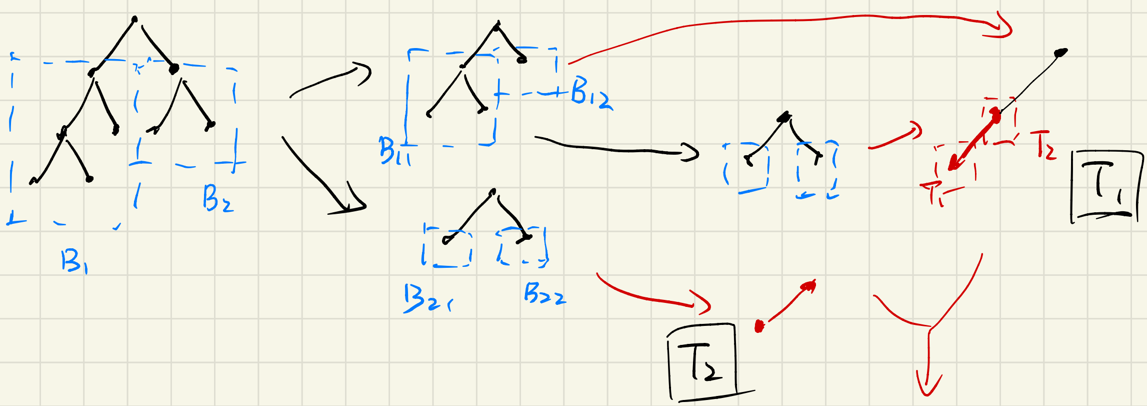
else B = 

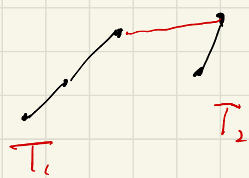
T_1 = B2T(B_1)

T_2 = B2T(B_2)

add an edge connecting the root of T_1 to the root of T_2 as left most child

e.g,

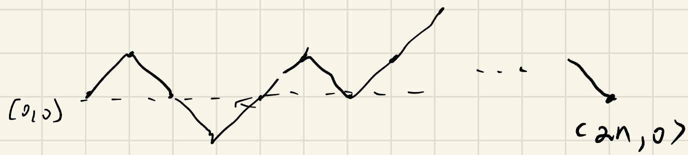




Q: ? T2B(. . .)

$M_n \leq 4^n = 2^{2n} = \left| \{+1,-1\}^{2n} \right|$

$M_n \leq \binom{2n}{n} = \left| \{ x \in \{+1,-1\}^{2n} \mid \sum x_i = 0 \} \right|$



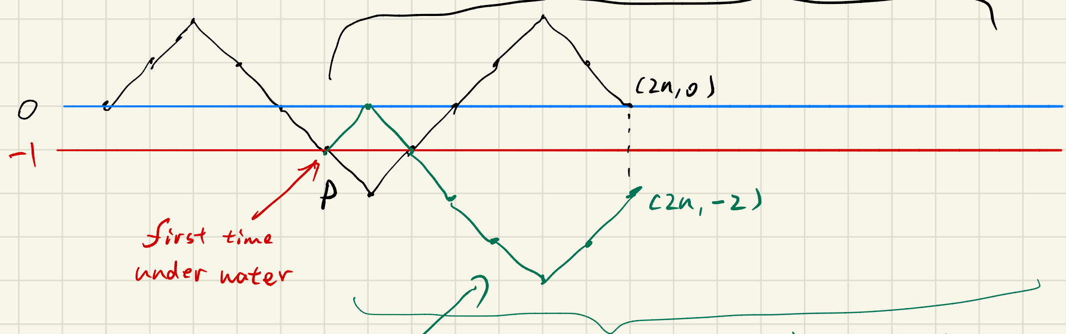
Good sequence: ≥ 0 all the time

Bad sequence: ≤ -1 at some point

$M_n = \binom{2n}{n} - \underline{\#\text{bad sequence}}$

↘ k times

↗ k+1 times



after P, exchange up and down

↘ k+1 times

↗ k times

Φ : bad sequence $\to \{ \{+1,-1\}^{2n} \mid \sum x_i = -2 \}$

Ψ : $\{ \{+1,-1\}^{2n} \mid \sum x_i = -2 \} \to$ bad sequence

Φ, Ψ are inverse of each other

Φ is a bijection

$|\text{bad sequences}| = \left| \{ \{+1,-1\}^{2n} \mid \sum x_i = -2 \} \right| = \binom{2n}{n+1} = \binom{2n}{n-1}$

n+1 times +1

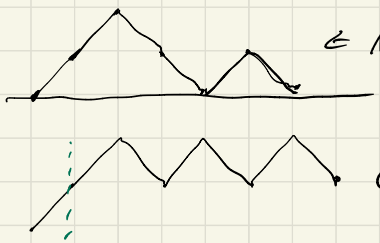
n-1 times -1

$M_n = \binom{2n}{n} - \binom{2n}{n-1}$

Another Proof.

$M_n = \{ \{+1,-1\}^{2n} \mid \cdots \}$

$D_n = \{ \{+1,-1\}^{2n+1} \mid \sum_{i=1}^{k} x_i \geq 1 \text{ for } k=1,\dots,2n, \sum_{i=1}^{2n+1} x_i = 1$



$\in M_3$

$\in D_3$

Observation: $|M_n| = |D_n|$

Proof: $x \in D_n$ iff $x = (+1, y)$, $y \in M_n$

D_n ?

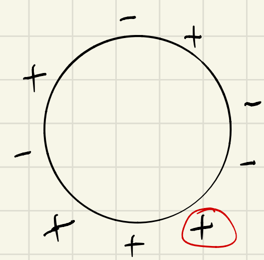
let $x \in \{ \{+1,-1\}^{2n+1} \mid \sum x_i = 1 \} =: A$

$- + - - + + + - + \quad \in A_3$

$+ - - + + + - + - \quad$ [shift $\rightarrow$]

We get $2n+1$ cyclical shifts

Claim: Exactly one of them is in D_n



proof.

1) copy the circle

2) while there is a "+" followed by "−",

- pair them up
- delete them

3) A single + will survive

Δ starting at the survivor will give you a sequence in D_n

Δ starting at somewhere else won't ∎

$x \in A_n \longrightarrow 2n+1$ cyclical shifts $\longrightarrow$ exactly one in D_n

But there are $2n+1$ ways to obtain a specific seq in D_n

$$|D_n| = \frac{|A_n|}{2n+1} = \frac{1}{2n+1}\binom{2n+1}{n+1}$$

$$= \frac{1}{2n+1} \cdot \frac{(2n+1)!}{(n+1)!\,n!} = \frac{(2n)!}{(n+1)!\,n!} = \frac{(2n)!}{(n+1)n!\,n!}$$

$$= \frac{1}{n+1}\binom{2n}{n} \qquad \blacksquare$$

two proof shows: $\frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$

Obs: Let $x \in A_n$ and

$x^{(0)}, x^{(1)}, \ldots, x^{(2n)}$ be the $2n+1$ cyclical shifts

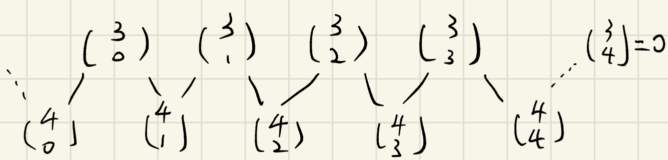
Then they are all distinct

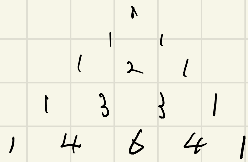
Enumerative Combinatorics (Video)

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

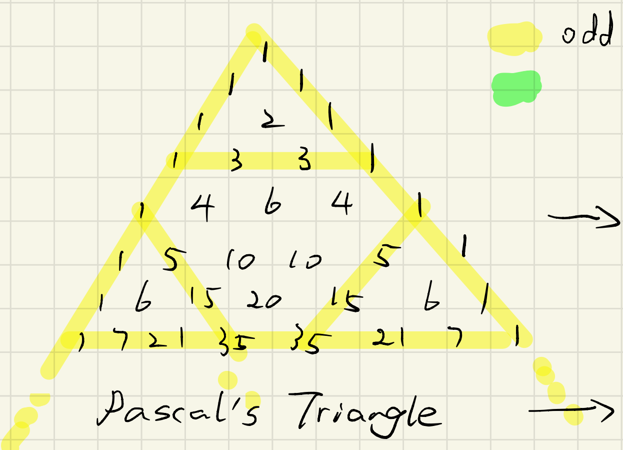
proof 1. formula

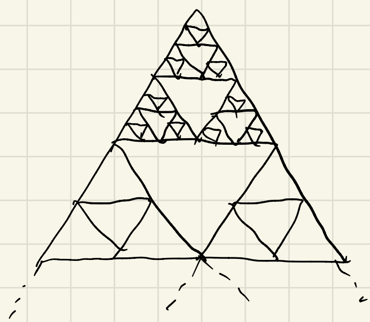
proof 2. include x or don't include x





Pascal's Triangle





Pascal's Triangle → Sierpinski Triange

Binomial Theorem $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

coefficient

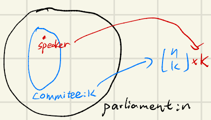
binomial

proof.1. induction on n

proof.2. sum of 2^n item

Combinatorial Identities

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



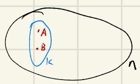
1. choose a commitee
1. choose a speaker

$\Longleftrightarrow$

1. choose a speaker (n)
2. choose a commitee (2^{n-1})

$$\sum_{k=0}^{n} k^2\binom{n}{k} = n \cdot 2^{n-1} + n^2 \cdot 2^{n-2}$$

(not so nice)



A, B could be the same one

1. choose comitee ($\sum\binom{n}{k}$)
2. choose A, B (k^2)

$\Longleftrightarrow$

1. choose A, B
2. choose the rest

} discuss if A=B !!!

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

($A \neq B$ case)

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

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

Parliament $n+1$, committe of $k+1$ members

youngest 1 2 ... s ... n $n+1$ oldest

speeker

constriant: speeker must be the oldest one in a committe

1) speek
2) committe: k more members $\sum_{s=1}^{n+1}\binom{s-1}{k} = \sum_{m=0}^{n}\binom{m}{k}$

$\Longleftrightarrow$

1) select $k+1$ members $\binom{n+1}{k+1}$
2) the oldest be the speeker 1

Def. $m^{\underline{k}} = m(m-1)\cdots(m-k+1)$, then $\binom{m}{k} = \dfrac{m^{\underline{k}}}{k!}$

then we have $\displaystyle\sum_{m=0}^{n} m^{\underline{k}} = \frac{(n+1)^{\underline{k+1}}}{k+1}$

Application: $\displaystyle\sum_{k=0}^{n} k^2 = \sum_{k=0}^{n}(k(k-1)+k) = \sum(k^{\underline{2}} + k^{\underline{1}}) = \frac{(k+1)^{\underline{3}}}{3} + \frac{(k+1)^{\underline{2}}}{2} = \cdots$

$\displaystyle\sum_{k=0}^{n} k^4 = \cdots$

Sums (class)

$$\sum_{i=1}^{n} \binom{n}{i} = 2^n$$

proof 1. Common known

proof 2. Comb proof : $\binom{n}{k}$ = # subsets of $[n]$ of size k

proof 3. $(1+1)^n = \cdots$

Lemma. $\sum_{k=0}^{n} k \binom{n}{k} = n 2^{n-1}$

Proof 1. Parliament of size n, select a committe (in the video, previously)

Proof 2. $f(x) = (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$

$f'(x) = \sum_{k=0}^{n} \binom{n}{k} k x^{k-1}$, $x=1$ is what we want

$= n(1+x)^{n-1}$. $\blacksquare$

Proof 3. $\sum k \binom{n}{k} = \sum k \cdot \frac{n!}{k!(n-k)!} = \sum \frac{n!}{(k-1)!(n-k)!} = n \sum \frac{(n-1)!}{(k-1)!(n-k)!}$

$= n \sum_{k=1}^{n} \binom{n-1}{k-1} = n \sum_{j=0}^{n-1} \binom{n-1}{j} = n \cdot 2^{n-1}$ $\blacksquare$

Q. $\sum_{k=0}^{n} k^2 \binom{n}{k} = ?$ (proved in video) $= n \cdot 2^{n-1} + n(n-1) \cdot 2^{n-2}$

Lemma. $\sum_{k=0}^{n} k(k-1) \binom{n}{k} = n(n-1) \cdot 2^{n-2}$ $\blacksquare$

proof. 1 formular

proof. 2 $f(x) = (1+x)^n = \sum \binom{n}{k} x^k$

$f''(x) = n(n-1)(1+x)^{n-2} = \sum k(k-1) \binom{n}{k} x^{k-2}$

$= \left(f(x) \frac{n}{1+x} \right)' = f'(x) \frac{n}{1+x} - f(x) \frac{n}{(1+x)^2} = f(x) \left[\frac{n^2}{(1+x)^2} - \frac{n}{(1+x)^2} \right]$

$= f(x) \frac{n(n-1)}{(1+x)^2}$, take $x=1$ $\blacksquare$

Methods of proof

A. combinational arguments
B. Calculous
C. Massaging

Q: What is $\sum_{k=1}^{n} k$, then $\sum_{k=1}^{n} k^2$, then $\sum_{k=1}^{n} k^5$?

Lemma. $\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1)$

Proof 1. induction [Problem: what if $\sum k^5$?] $\blacksquare$

Proof 2. guesswork. Answer's probably an^3+bn^2+cn+d

Plug in $n=0,1,2,3 \Rightarrow \cdots$ $\blacksquare$

Proof 3. "shifting the sum"

$$X = \sum_{k=1}^{n} k^2, \quad X+(n+1)^2 = \sum_{k=1}^{n+1} k^2 = \sum_{j=0}^{n} (j+1)^2 = X + 2\sum_{j=0}^{n} j + n+1$$

$$\Rightarrow \sum j = \frac{(\ )^2-(\ )}{2}$$

From this, we get the idea

$$Y = \sum_{k=1}^{n} k^3, \quad Y+(n+1)^3 = \sum_{j=0}^{n} (j+1)^3 = Y + 3X + \frac{3}{2} n(n+1) + n+1$$

$$\Rightarrow X = \cdots$$ $\blacksquare$

Q. change: what is $\sum_{k=1}^{n} k(k-1)$

notation: $k^{\underline{a}} = k(k-1)\cdots(k-a+1)$ [$k^{\underline{a}}$: "k to the following a"]
[k^a: "k to the a"]

Lemma. $\sum_{k=1}^{n} k^{\underline{a}} = \frac{(n+1)^{\underline{a+1}}}{a+1}$

Proof 1. induction

Proof 2. combinational proof (in video)

$1 \quad 2 \quad \cdots \quad n$

① select j
② select a numbers smaller than j

Expected Minimum (Video)

choose $A \in \binom{[n]}{k}$ uniformly at random

$X = \min(A)$, $E(X) = ?$

$1 \quad 2 \quad 3 \quad \cdots \quad i \quad i{+}1 \quad \cdots \quad n$

$$E(X) = \sum_{i=1}^{n} i \underline{\Pr(X=i)}$$

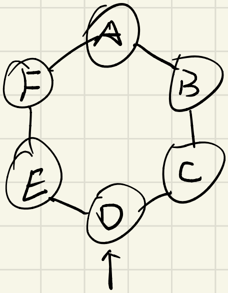
$$\frac{\#(A \in \binom{[n]}{k} : \min(A)=i)}{\binom{n}{k}} = \frac{\binom{n-i}{k-1}}{\binom{n}{k}}$$

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

Lemma: Let X be a non-negative random varible taking integer values. Then $E[X] = \sum_{i \geq 1} \Pr[X \geq i]$

Proof. $E[X] = \sum_{i=1}^{n} i \Pr[X=i] = \sum_{i=1}^{n} \Pr[X=i] \sum_{j=1}^{i} 1$

Discrete Probability (Class)



Ant starting at D and walking randomly: $\{+1,-1\}^{\infty}$

Q₁: How long on average to reach A

Q₂: $\Pr$[reach A eventually]

Lemma: $\Pr[\text{never reach } A] = 0$

proof 1. It's obvious

proof 2. $\Pr[\text{never reach } A] \le \Pr[\text{don't reach } A \text{ within } n \text{ steps}]$

$$\le \Pr[\text{never } +1+1+1+1+1 \text{ in the first } n \text{ steps}]$$

$$\le \Pr[\forall i \in \underbrace{\{0,1,\dots,\lfloor \tfrac{n}{5} \rfloor -1\}}_{\text{divid}}: (X_{5i+1}, X_{5i+2}, X_{5i+3}, X_{5i+4}, X_{5i+5}) \ne (+1,+1,+1,+1,+1)]$$

$$\le \left(\frac{31}{32}\right)^{\lfloor n/5 \rfloor -1} \quad (\text{cgt to } 0)$$

it holds for all n $\blacksquare$

proof 3. $t \in \mathbb{N}_0$ let $a^{(t)} := \Pr[\text{Ant is at } A \text{ after } t \text{ steps}]$

$b^{(t)} := \Pr[\dots B \dots t \dots]$

$\vdots$

$f^{(t)} := \Pr[\dots f \dots t \dots]$

$$x^{(t)} = (a^{(t)} \dots f^{(t)})^T$$

$$\begin{cases} b^{(t+1)} = \frac{1}{2} a^{(t)} + \frac{1}{2} c^{(t)} \\ \dots \end{cases}$$

$$\Rightarrow x^{(t+1)} = M x^{(t)}$$

$$M = \begin{pmatrix} 0 & 1/2 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 1/2 & 0 & 0 & 0 & 1/2 & 0 \end{pmatrix}$$

$$y^{(t)} = \begin{pmatrix} \Pr[\text{after } t \text{ steps we are at } B, \text{ but never been to } A] \\ \Pr[\text{ - - - - - - - - } C, \text{ - - - - - } A] \\ \vdots \\ \Pr[\text{ - - - - - - - - } F \text{ - - - - - - } A] \end{pmatrix}$$

$$y_C^{(t+1)} = \frac{1}{2} y_B^{(t)} + \frac{1}{2} y_C^{(t)}$$

- - - -

$$y^{(t+1)} = L \cdot y^{(t)}, \quad M = \begin{pmatrix} 0 & 1/2\ 0\ 0\ 0\ 0 \\ 1/2 & \\ 0 & \\ 0 & L \\ 0 & \\ 0 & \end{pmatrix}$$

$\Pr[A \text{ not reached within } t \text{ steps}]$ $\quad (\lambda_i \leq 1)$

$$= y_B^{(t)} + y_C^{(t)} + \cdots + y_F^{(t)} = \|y^{(t)}\| = \Big\|L^t \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\Big\| \longrightarrow 0$$

$\|x\| = \sqrt{\sum x_i^2}$

$\blacksquare$

Proof 4.7

$b := E[\#\text{ of steps from } B \text{ to } A]$ $\qquad b = 1 + \frac{1}{2}c$

$c := E[\#\text{ of - - - - - - } C \text{ to } A]$ $\qquad c = 1 + \frac{1}{2}b + \frac{1}{2}d$

$d :$ $\qquad d = 1 + \frac{1}{2}c + \frac{1}{2}e$

$e :$ $\qquad$ - - -

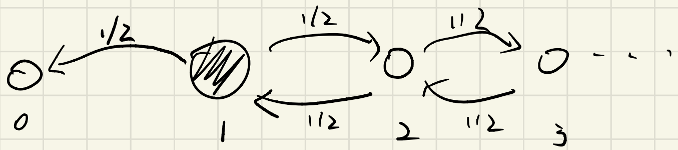
$f :$

$$\begin{pmatrix} b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + L \cdot \begin{pmatrix} b \\ c \\ d \\ e \\ f \end{pmatrix}$$

$$v = \mathbb{1} + Lv$$

$$(I_d - L)v = \mathbb{1} \qquad v = (I_d - L)^{-1}\mathbb{1}$$

The confused SJTU students : Random walk on $\mathbb{Z}$



Q: Pr[student reaches 0 eventually] ?

E[steps until 0]

$p_n := Pr$[the first time reach 0 after n steps]

$p_1 = \frac{1}{2}$, $p_2 = 0$, $p_3 = \frac{1}{8}$, $p_4 = 0$. $p_5 = \frac{2}{32} = \frac{1}{16}$

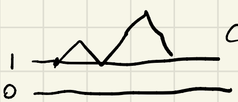
(change)

$p_n: = Pr$[··· 2n+1 steps]

$p_0 = \frac{1}{2}$, $p_1 = \frac{1}{8}$, $p_2 = \frac{1}{16}$

Pr[after 2n steps, student is at ① and never at 0 within 2n steps]

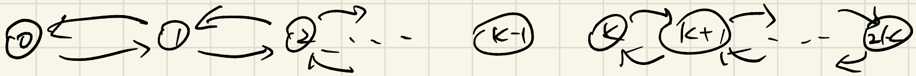
$= \frac{C_n}{4^n}$



Pr[reach 0 at some point] $= \sum_{n=0}^{\infty} \frac{C_n}{2 \cdot 4^n} = \sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{2(n+1)4^n}$

is this 1 ?

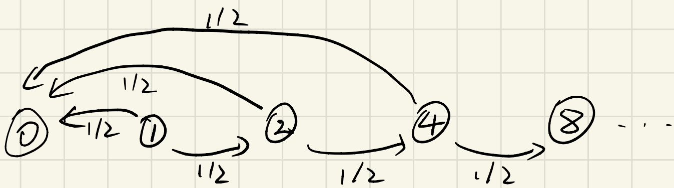
Start at k, run until you are at 0 or at $2k$



$\Pr[\text{eventually reach } 0 \text{ or } 2k] = 1$

$\Pr[2k \text{ before } 0] = 1/2$

same intuition



$\Pr[\text{student never goes to } 0] = \Pr[1 \to 2] \times \Pr[2 \to 4] \times \cdots$

$= \frac{1}{2} \times \frac{1}{2} \cdots$

$\to 0$

$X_k = E[\#\text{ steps until } 0 \text{ is reached when starting at } k]$

$X_1 = 1 + \frac{1}{2} \times 0 + \frac{1}{2} X_2$

$X_2 = 1 + \frac{1}{2} X_1 + \frac{1}{2} X_3$

$X_3 = 1 + \frac{1}{2} X_2 + \frac{1}{2} X_4$

$\vdots$

$Y_d = X_{2^d} = \text{steps from } 2^d \text{ to } 0$

$Y_d \geq 2^d + \frac{1}{2} Y_{d+1}$

claim: $Y_0 \geq d + 2^{-d} \cdot Y_d \quad \forall d$

proof: induction on d

$y_0 \geq d + 2^{-d} y_d \geq d$

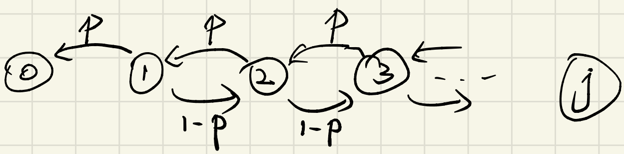
So $E[\#\text{ steps to } 0] = \infty$

$$E[X_k] = \sum_{n=0}^{\infty} (2n+1) \Pr[\#\text{steps is } 2n+1]$$

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

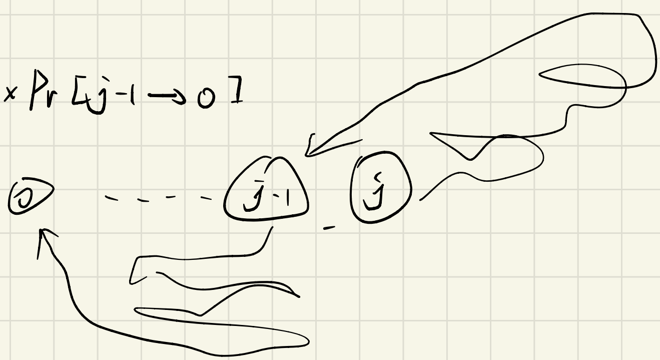
$$= \frac{1}{2} \sum \frac{1}{n+1} = \frac{1}{2} \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

Biased Random Walk



$r_j(p) = \Pr[\text{eventually reach } 0 \text{ when starting at } j]$

$$\Pr[j \to 0] = \Pr[j \to j-1] \times \Pr[j-1 \to 0]$$



$$= \Pr[1 \to 0] \times \Pr[j-1 \to 0]$$

$$= r \cdot r_{j-1} = r \cdot r \cdot r_{j-2} = \cdots = r^j \quad \Rightarrow r_j = r^j$$

Then, $r = p + (1-p) r_2 = p + (1-p) r^2$

$$\Rightarrow \underset{1-p}{\overset{1}{(1-p)}} r^2 \underset{-p}{\overset{-1}{- r + p}} = 0 \Rightarrow r = 1, \frac{p}{1-p}$$

Obs. $r(p) = 1$ or $r(p) = \frac{p}{1-p}$

(i) for $p = \frac{1}{2}$: the same, $r_1(p) = 1$

(ii) for $p > \frac{1}{2}$, $\frac{p}{1-p} > 1$, $\therefore r_1(p) = 1$

(iii) for $p < \frac{1}{2}$

[note: for $p = 0$, $r(p) = 0$]

$\Sigma_n :=$ [we reach 0 after $2n+1$ steps, starting at 1, not earlier]

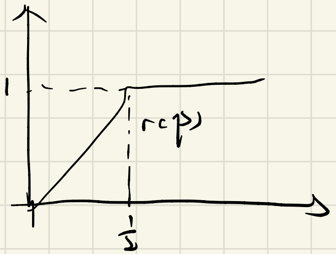
$Pr[\Sigma_n] = C_n \cdot p^{n+1}(1-p)^n$

$$r(p) = \sum_{n=0}^{\infty} C_n p^{n+1}(1-p)^n = \underbrace{p}_{<1/2} \sum_{n=0}^{\infty} C_n (\underbrace{p(1-p)}_{<1/4})^n$$

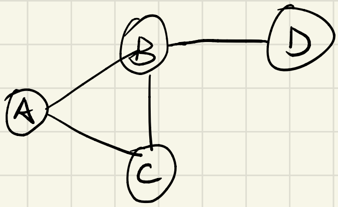
$$< \frac{1}{2} \sum C_n \left(\frac{1}{4}\right)^n = r\left(\frac{1}{2}\right) = 1$$

$\therefore r(p) < 1$

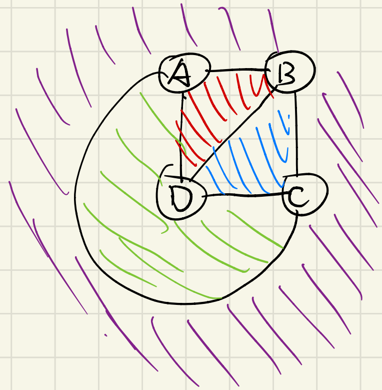
$\therefore r(p) = \frac{p}{1-p}$



The Crossing Number Inequality for Graph Diagrams



plane diagram



$n = 4$
$m = 6$
$f = 4$

Euler's Formula

In any connected plane diagram

$$n - m + f = 2$$

proof. . . . $\blacksquare$

Lemma. Connected & simple then

$m \leq 3n - 3$. If $n \geq \ldots (3)$ then $m \leq 3n-6$

Proof. $2 \cdot m = \#\text{edge-face incidences} \geq 3(f-1) = 3f - 3$

$\Rightarrow 3f \leq 2m + 3$,

also $m = n + f - 2$

$3m = 3n + 3f - 6 \leq 3n + 2m + 3 - 6 \Rightarrow m \leq 3n - 3$

D: a graph diagram

$Cr(D) :=$ the number of crossing

G is a graph on n vertices with m edges

Theorem. If $m \geq 3n-5$ then $Cr(G) = 1$.

Theorem. $Cr(G) \geqslant m - 3n + 6$

Proof. Let D be a diagram G

$c := Cr(D)$

We can remove a crossing by deleting one edge.

We can delete c edges, creating a sub-diagram D' of D.

D' is a plane diagram with n vertices and $\geqslant m-c$ edges

D': n vertices, $\geqslant m-c$ edges.

$m - c \leq 3n - 6$

$\Rightarrow c \geqslant m - 3n + 6$

$\blacksquare$

e.g. $n = 100$, $m = 3000$ $\Rightarrow$ $Cr \geqslant m - 3n + 6 = 2706$

Theorem: If $m \geq 4n$, then $Cr \geq \frac{m^3}{64n^2}$

Proof. First, two simple observations.

Edges with a common endpoint don't cross

edges cross at most once

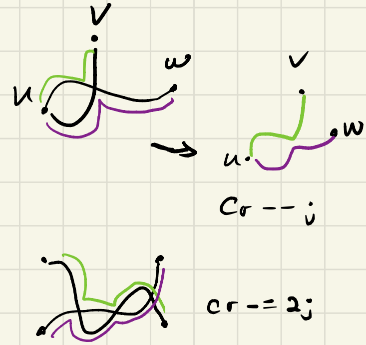
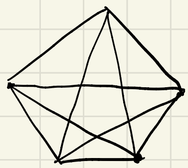


Diagram D



toss a biased coin

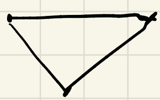
vertex survives with $Pr = p$

n vertices

m edges

c crossings

Diagram D'

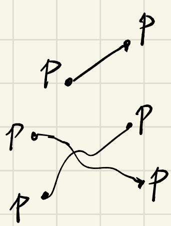


random variables $\begin{cases} n' & \text{vertices} \\ m' & \text{edges} \\ c' & \text{crossings} \end{cases}$

$E[n'] = np$

$E[m'] = p^2 m$

$E[c'] = p^4 c$



$c' \geq m' - 3n'$

$E[c'] \geq E[m'] - 3E[n']$

$p^4 c \geq p^2 m - 3pn$

$c \geq \frac{m}{p^2} - \frac{3n}{p^3} \quad \forall p \in [0,1]$

set $p = \frac{4n}{m} \leq 1$. $c \geq \dots = \frac{m^3}{64n^2}$

Technique: Generating Function

$0, 1, 1, 2, 3, 5 \quad F_0, F_1, \dots$

generating function: $f(x) = \sum_{n=0}^{\infty} F_n x^n$ (power series)

closed form for $f(x)$?

$$f(x) = \sum^{\infty} F_n x^n = F_0 + x F_1 + \sum_{n=2}^{\infty} F_n x^n$$

$$= 0 + x + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) x^n$$

$$= 0 + x + x \sum_{n=2}^{\infty} F_{n-1} x^{n-1} + x^2 \sum_{n=2}^{\infty} F_{n-2} x^{n-2}$$

$$= x + x f(x) + x^2 f(x)$$

$$\Rightarrow f(x) = \frac{x}{1 - x - x^2} \longrightarrow = x \cdot \frac{1}{1-(x+x^2)}$$

intuition: $\frac{1}{1-z} = \sum^{\infty} z^n$

(try)

$$= x \sum_{n=0}^{\infty} (x+x^2)^n = x \sum_{n=0}^{\infty} x^n (1+x)^n$$

$$= x \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{n,k=0}^{\infty} x^{n+k+1} \binom{n}{k}$$

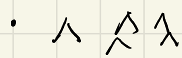
$$= \sum_{m,n,k=0}^{\infty} x^{m+1} \binom{n}{k}, \quad [m = n+k]$$

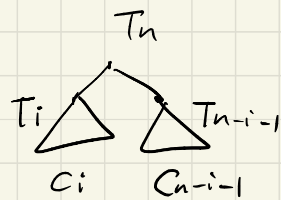
$$= \sum_{m=0}^{\infty} x^{m+1} \sum_{\substack{n,k:\\ n+k=m}} \binom{n}{k} = \sum_{m=0}^{\infty} x^{m+1} \sum_{k=0}^{m} \binom{m-k}{k}$$

$$\Rightarrow \sum_{m=0}^{\infty} x^m \cdot F_m = f(x) = \sum_{m=0}^{\infty} x^{m+1} \sum_{k=0}^{m} \binom{m-k}{k}$$

$$\boxed{\text{guess: } F_{m+1} = \sum_{k=0}^{m} \binom{m-k}{k}}$$

Catalan numbers : C_n 1   1   2   5   14





$$C_n = \sum_{i=0}^{n-1} C_i C_{n-i-1} \text{ if } n \geq 1$$

$$c(x) = \sum_{n=0}^{\infty} C_n x^n = 1 + \sum_{n=1}^{\infty} C_n x^n = 1 + \sum_{n=1}^{\infty} \sum_{i=0}^{n-1} C_i C_{n-i-1} \underline{x \cdot x^i x^{n-i-1}}$$

$$= 1 + \sum_{n=1}^{\infty} \sum_{i,j=0}^{\infty} [i+j=n-1] C_i C_j \, x x^i x^j$$

$$= 1 + x \sum_{i,j=0}^{\infty} C_i x^i C_j x^j = 1 + x \left(\sum_{i=0} C_i x^i \sum_{j=0} C_j x^j \right)$$

$$= 1 + x\, c^2(x)$$

$$\Rightarrow \quad x\, c^2(x) - c(x) + 1 = 0 \quad \Rightarrow c(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

$\sum_{n=0}^{\infty} C_n x^n$: if $x > \frac{1}{4}$

$$C_n x^n = \frac{\binom{2n}{n}}{n+1} x^n \geq \frac{4^n x^n}{(2n+1)(n+1)} = \frac{(4x)^n}{(2n+1)(n+1)} \Rightarrow \sum \text{dgt}$$

if $x \leq \frac{1}{4}$, then $\exists\, p \in [0,1],\ p(1-p) = x$

$\exists$ a unique $p \in [0, \frac{1}{2}]$ s.t. $p(1-p) = x$

$$\sum_{n=0}^{\infty} C_n x^n = \sum^{\infty} C_n p^n (1-p)^n = \frac{1}{p} \sum_{n=0}^{\infty} C_n p^{n+1} (1-p)^n$$

$$= \frac{1}{p} \cdot \underbrace{\Pr[\text{p-biased Random Walk Reach } 0]}_{[*]}$$

$$= \frac{1}{1-p}$$

$$[*] = \begin{cases} 1 & \text{if } p \geq \frac{1}{2} \\ \frac{p}{1-p} & \text{if } p \leq \frac{1}{2} \end{cases}$$ (in previous notes.)

For $c(x) = 1 + x\,c^2(x)$

$x c^2 - c + 1 = 0$, $\lim_{x \to 0} c(x) = 1$

$\sum C_n x^n \leq \sum 4^n x^n = \frac{1}{1-4x}$

Partition Number: P_n

	0	0
1	1	1
2	2	2, 1+1
3	3	3, 2+1, 1+1+1
5	4	4, 3+1, 2+2, 2+1+1, 1+1+1+1
7	5	5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1
11	6	6, 5 1, 4 2, 4 1 1, 3 3, 3 2 1, 3 1 1 1, 2 2 2, 2 2 1 1, 2 1 1 1 1, 1 1 1 1 1 1

P_n^k = # of ways to write n as $a_1+a_2+\cdots$ where $a_1 \geq a_2 \geq \cdots$ and $a_1 \leq k$

Then $P_n^n = P_n$ → Dynamic Programming

$$P_n^k = \sum_{a=1}^{k} P_{n-a}^{a} \qquad \left[P_n^1 = 1,\ P_n^0 \begin{cases} 1 & \text{if } n=0 \\ 0 & \text{else} \end{cases} \right]$$

Is there one-dimensional, linear recurrence, like $P_n = P_{n-1} + P_{n-2} + \cdots$?

$$p(x) = \sum_{n=0}^{\infty} P_n x^n = \sum_{a \in A} x^n$$

See lecture note fore details

A = the set of all sequence $(a_1, a_2, \cdots) \in \mathbb{N}_0^{\infty}$

such that all but finitely a_i are 0

Sequence represent one way to write $n = \sum_{k=0}^{\infty} k a_k$ as

sum of int

$$= \sum_{a \in A} \prod_k (x^k)^{a_k} = \sum_{(a_1, \cdots)} x^{a_1} x^{2a_2} x^{3a_3} \cdots$$

$$= \sum_{a_1} x^{a_1} \sum_{a_2} x^{2a_2} \sum_{a_3} x^{3a_3} \cdots$$

$$= (1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots)\cdots$$

$[4\,1\,1:\quad a_1 = 2,\ a_2 = 0,\ a_3 = 0,\ a_4 = 1\ ]$

$$p(x) = \prod_{k=1}^{\infty} \sum_{i=0}^{\infty} (x^k)^i = \prod_{k=1}^{\infty} \frac{1}{1-x^k} = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots}$$

$$q(x) := (1-x)(1-x^2)(1-x^3)\cdots$$

So $p(x)q(x) = 1$

intuition:

Partition numbers $\longrightarrow$ Generating function of $p(x)$

Function $q(x)$ $\longrightarrow$ Generating function of ?

$$q(x) = \sum_{n=0}^{\infty} Q_n x^n$$

if we have formula for Q_n, can we get a formula recurrence for P_n?

Suppose we "know" Q_n, $p(x)q(x) = 1$

$$\sum_{n=0}^{\infty} P_n x^n \sum_{n=0}^{\infty} Q_n x^n = 1 + 0x + 0 \cdot x^2 + 0 \cdot x^3 + \cdots$$

$$= \sum_{n,m} P_n Q_m x^{m+n} \underset{\substack{\uparrow \\ k := n+m \\ n := k-m}}{=} \sum_{k=0}^{\infty} x^k \sum_{m=0}^{k} P_{k-m} Q_m$$

$$= \sum_{n=0}^{\infty} x^n \sum_{i=0}^{n} P_{n-i} Q_i$$

$\sum_{i=0}^{n} P_{n-i} Q_i$ = coeff. of x^n in the expansion of $p(x)q(x) = \begin{cases} 1 & \text{if } n=0 \\ 0 & \text{if } n \geq 1 \end{cases}$

if $n \geq 1$, $P_n Q_0 = -Q_1 P_{n-1} - Q_2 P_{n-2} - Q_3 P_{n-3} - \cdots$

this is the recurrence!

$$r(x) = (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$$

$$= 1 + 1x^2 + 2x^3 + 2x^4 + 3x^5 + 3x^6 + \cdots$$

$0 = 0$

$1 = 1$

$2 = 2$

$3 = 3,\ 2+1$

$4 = 4,\ 3+1$

$5 = 5,\ 4+1,\ 3+2$

write n as a sum $a_1 + a_2 + \cdots + a_k$
$a_1 > a_2 > \cdots > a_k$.

R_n : = # ways to write n as a sum of distinct int.

Q_n : = # — — — — — — — . . . . . evenly many distinct

— # — — — — — . oddly many . . . .

Figure out the Q_n

Def. For $S \subseteq \mathbb{N}$, let $w(S) = \sum_{i \in S} i$, $w(\{6,7,9\}) = 22 = w(\{9,5,4,3,1\})$

obeservation. $Q_n = (\#$ sets S with $w(S) = n$ and $|S|$ even $)$

$- (\#$ — — — — — n and ... odd$)$

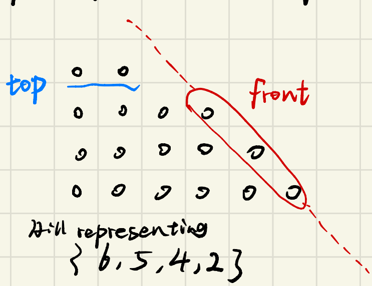
Proof idea. $(1-x)(1-x^2)\cdots(1-x^8)(1-x^9)$

Lemma. $Q_n = 0$ for all n

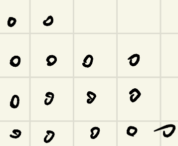
Proof. $\forall n$, there are as many enen sets S as there are odd sets S with $w(S) = n$

<u>Strategy</u>: Find a natural way to "many" the even sets with odd sets.

Def. A hill is the following way of representing a set $S \subseteq \mathbb{N}$



hill representing $\{6,5,4,2\}$

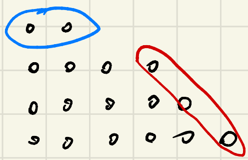


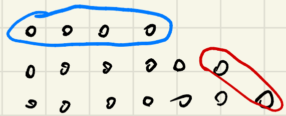
not a hill

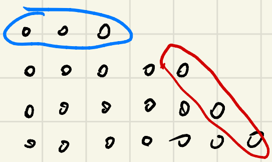
not a hill

f = size of front
t = size of top

two kinds of hills
if $t > f$, it is big-top
if $t \le f$, it is big-front







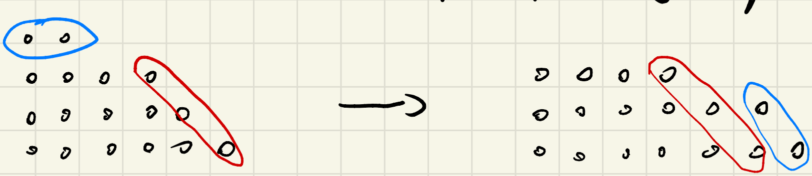
Define a transformation Φ mapping big-top hills to big-front hills and vice versa

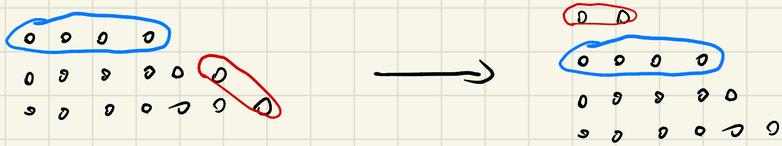
$\Phi((\Phi(s))) = s$ so it maps s back to itself when applied twice

and $\Phi(s)$ is even iff s is odd
and Φ does not change the # of $\circ$ $(w(s) = w(\Phi(s)))$

Φ works by moving top $\to$ front or front to top.

If S is big-top $(t > f)$, Φ moves front to top.
If S is big-front $(t \le f)$, Φ moves top to front.





$t > f$ big-top

Φ $\Big\downarrow$ front to top

new top $t' = f$

new frot $f' \geq f = t'$

big-front !

$t \leq f$

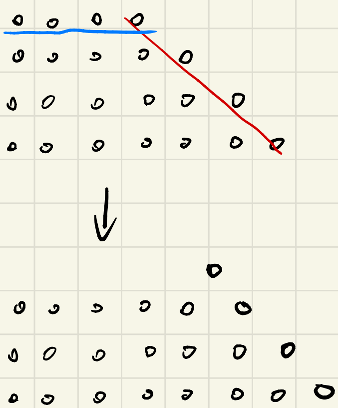
Φ $\Big\downarrow$ top to front

front f', top t'

$f' = t < t'$

big top!

Problematic Case 1

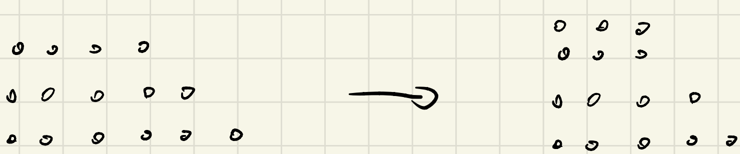


$t = f = |S|$, we get a problem !

not a hill !!

Problematic Case 2

$f = |S| = t - 1$



not a hill

Case 1: $f = t = |S|$

$$n = w(S) = t + (t+1) + \cdots + (t+f-1) = \frac{t(3t-1)}{2}$$

Case 2: $f = |S| = t-1$,

$$n = w(S) = t + (t+1) + \cdots + (t+f-1) = \frac{3f^2+f}{2}$$

$$k := -f = -|S| = \frac{k(3k-1)}{2}$$

Theorem.

$$Q_n = \begin{cases} 0 & \text{if } n \text{ is not } \frac{k(3k-1)}{2} \text{ for any } k \in \mathbb{Z} \\ (-1)^k & \text{if } n = \frac{k(3k-1)}{2} \text{ for some } k \in \mathbb{Z} \end{cases}$$

$$p_n = -Q_1 P_{n-1} - Q_2 P_{n-2} - \cdots - Q_{n-1} P_1 - Q_n P_0$$

$$= -\sum_{i=1}^{\infty} Q_i P_{n-i} = \sum_{k \in \mathbb{Z} \setminus \{0\}} (-1)^{k+1} \cdot P_{n - \frac{k(3k-1)}{2}}$$

$$= P_{n-1} + P_{n-2} - P_{n-5} - P_{n-7} + P_{n-12}$$

Graph (Video)

Graph Isomorphism

Def. ...

Degree of a Vertex

Def ...

Hand Shaking Lemma. $G=(V,E)$, $\sum_{v\in V} \deg(v) = 2|E|$

Score of a Graph

Def. ...

Graph Score Algorithm

find-graph $(d_1, \dots, d_n)$

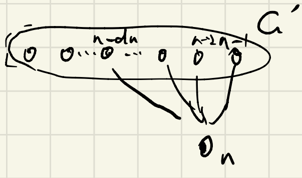
sort $(d_1, \dots, d_n)$

$$d_i' := \begin{cases} d_i - 1 & \text{for } i = n-d_n, \dots, n-1, n \\ d_i & \text{for } i = 1, \dots, n-d_n-1 \end{cases}$$

$G' :=$ find-graph $(d_1', \dots, d_{n-1}')$

if $G' =$ null return null

else $G :=$



Observation: Suppose find-score returns a graph G, then surely $\text{score}(G) = (d_1, \dots, d_n)$

Question. Suppose there is a graph G with $\text{score}(G) = (d_1, \dots, d_n)$, will find-graph return G? (YES)

or return a graph with this score

Graph Score Theorem

Theorem. $d = (d_1, \dots, d_n)$ with $d_1 \leq \dots \leq d_n$,

Define $d_i' := \begin{cases} d_i - 1 & \text{for } i = n - d_n, \dots, n-1 \\ d_i & \text{for } i = 1, \dots, n - d_n - 1 \end{cases}$

Then there exists a graph with score d if and only if there exists a graph with score d'.

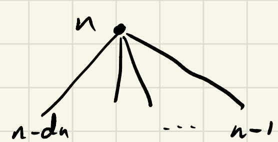
Furthermore, if $n=1$, then there exists a graph with score (d_1) if and only if $d_1 = 1$.

Proof. $d' \Rightarrow d$ ✓ (add vertice and edges)

$d \Rightarrow d'$

Claim. if $\exists\, G : \text{score}(G) = (d_1, \dots, d_n)$

then $\exists$ such G that the last vertex n with degree d_n connected to all the previous vertices.



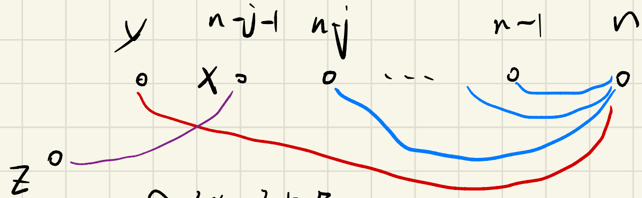
with this claim, $G - n := G'$, $\mathrm{score}(G') = d'$

proof of Claim.

Def. $j(G) :=$ the largest number j such that vertex n has an edge to $n-1, n-2, \ldots, n-j$

Theorem. If G maximize $j(G)$, then $j(G) = d_n$

Proof. Suppose not: $j(G) < d_n$



① $\{x, n\} \notin E$

② $\deg(n) = d_n$

$\Rightarrow$ ③ there must be a "y": $\{y, n\} \in E$

④ note: vertices are sorted

$\Rightarrow \deg(y) \leq \deg(x)$

and $\{y, n\} \in E$ but $\{x, n\} \notin E$

$\Rightarrow \exists\, z : \{x, z\} \in E$ but $\{y, z\} \notin E$

Now if we cancel $\{x, z\}, \{y, n\}$ and connect $\{y, z\}, \{x, n\}$

we get a graph $H := G + \{y, z\} + \{x, n\} - \{x, z\} - \{y, n\}$

observation: ① $j(H) > j(G)$

② $\mathrm{score}(H) = \mathrm{score}(G)$

However, G maximize j !!!

Graph Connectivity (Video)

Def. Subgraph. . . .

Def. A graph (V', E') is an **induced subgraph** of (V, E) if $V' \subseteq V$ and $E' = E \cap \binom{V'}{2}$

Def. Let $G = (V, E)$, $V' \subseteq V$, The **subgraph of G induced by V'** is the graph $G[V'] := (V', E \cap \binom{V'}{2})$.

Path: a specific subgraph

Def. A graph $G = (V, E)$ is **connected** if for all distinct $u, v \in V$, there is a path from u to v in G.

Lemma. Let $G = (V, E)$ be a graph. If G is not connected, then there exists a partition $V = V_1 \uplus V_2$ such that G contains no edges from V_1 to V_2.

Theorem. Let $G = (V, E)$ be a graph. Then there is a number k and a partition $V = V_1 \uplus \cdots \uplus V_k$ such that

1. each $G[V_i]$ is connected
2. G contains no edge from V_i to V_j, $\forall i \neq j$.

[connective component]

Cycles and Trees (Video)

Def. A connected, acyclic graph is called a tree.

Def. Let G be an acyclic graph. Then every CC of G is a tree, G is called a forest.

Theorem. Let G be a graph on n vertices. The following three statement are equivalent.

1. G is connected and acyclic
2. G is connected and $|E| \le n-1$
3. G is acyclic and $|E| \ge n-1$

proof. $1 \Rightarrow 2,3$. . Goal: A tree has $n-1$ edges

by induction ...

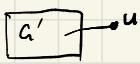
[firstly prove a tree must have a leaf u ($\deg(u)=1$)]

$2 \Rightarrow 1$ Claim. $\exists u: \deg(u)=1$

proof. Suppose not : $\sum \deg(v_i) = 2|E|$, $\sum \deg(v_i) \ge 2|V|$ $\Rightarrow |E| \ge |V| = n$. contradiction

but $|E| \le n-1$

Let $G' = G - u$, induction: G' is a tree $\Rightarrow$ G' acyclic



$\Rightarrow G$ acyclic

$\Rightarrow G$ is a tree

$3 \Rightarrow 1$ $(V_1, \dots, V_k)$ are CC.

$|V| = |V_1| + \dots + |V_k|$. $G[V_i]$ is acyclic & connected

$|E| = |E_1| + \dots + |E_k|$ $\Rightarrow G[V_i]$ is a tree, $|V_i|-1$ edge

$= |V| - k \ge n-1$ $\Rightarrow k \le 1 \Rightarrow k=1$

$\Rightarrow G$ is connected

$\Rightarrow G$ is a tree

Def. A sequence $v_0, v_1, \ldots, v_k \in V$ with $(v_i, v_{i+1}) \in E$ is called a **walk** of length k.

If $v_0 = v_k$, then it is a **closed walk**.

Observation. G contains a walk from u to v if and only if it contains a path from u to v.

Eulerian Cycle (Video)

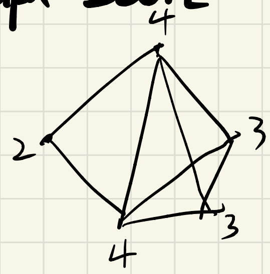
TBD...

Hamilton Cycles and Ore's Theorem (Video)

TBD...

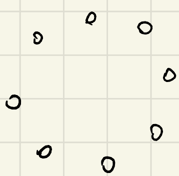
Graph (Class)

Graph Score



$(4, 4, 3, 3, 2) \longrightarrow$ score

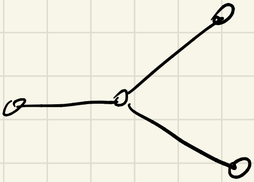
Q: Given a score 2 0 1 4 0 3 2 1, is there a graph?

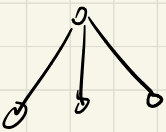


Graph Isomaphism

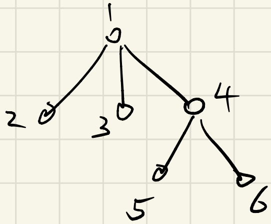
$G = (V, E)$, $H = (V', E')$

A isomaphism from G to H is a bijective function $f: V \to V'$ such that $\{u, v\} \in E \iff \{f(u), f(v)\} \in E'$

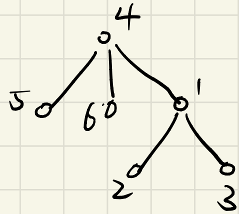




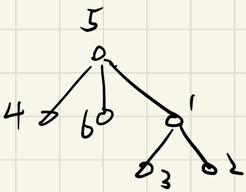
If $f: G \to G$ is an isomophism, we call f an automophism



$1 \longleftrightarrow 4$
$5 \longleftrightarrow 3$
$6 \longleftrightarrow 2$



a graph G $\xleftrightarrow{\text{automophism}}$ the same graph G drawn differently



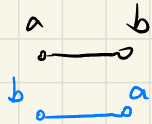
a different but isomophism

Observation: Every graph has an automophism

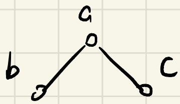
Indeed: $1 \longleftrightarrow 1$
$2 \longleftrightarrow 2$
$\cdots$
$n \longleftrightarrow n$

Def. A graph that has no automorphisms besides the identity function is called asynmetric

$n=2$

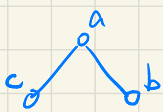


$n=3$



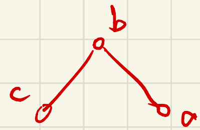
$a \to a$
$b \to c$
$c \to b$

automorphism



$a \to b$
$b \to c$
$c \to a$

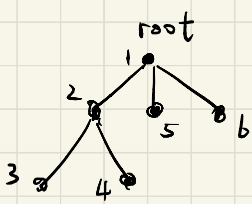
(bijective func $V \to V$)

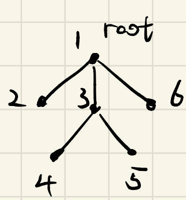


not an automorphism

rooted tree: (r, T) where $T=(V,E)$, $r \in V$

(S_1, T_1) are isomophic if $\exists$ isomophism $f\ T \to T_1$ such that $f(r) = s_1$.

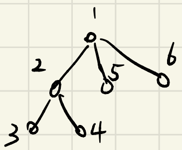




Obs. Every vertex has a set of children $\subseteq V$

If every children is linearly ordered $(<)$ from left to right,

we call it an ordered tree.



$2<5<6$

$3<4$

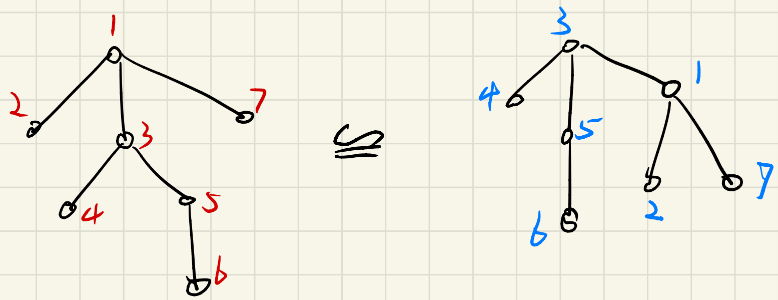
counting tree:

How many trees on $V = \{1, 2, \dots, n\}$?

Tree Isomorphism (Video)

Task: Determine whether $G \cong H$.
Maybe for some simple graph class

e.g.

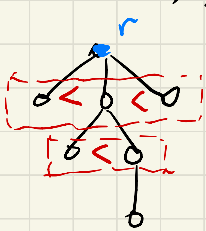


Def. A rooted tree is a pair (T, r) where T is a tree and r is a vertex in T

Def. (T_1, r_1), (T_2, r_2) are isomophic if there is a graph isomorphism $f: T_1 \to T_2$ with $f(r_1) = r_2$.

Def. An ordered tree is a rooted tree (T, r) together with, for every inner vertex, an ordering of its children.

e.g.

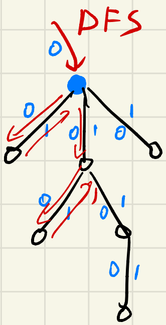


Def. Two ordered trees T_1, T_2 are isomorphic if there is an isomorphism $f: T_1 \to T_2$

1. $f(r_1) = r_2$
2. if u have children $v < w$, then $f(u)$ have children $f(v) < f(w)$

e.g.,

Encode Ordered Tree



Go "down": output 0

Go "up": output 1

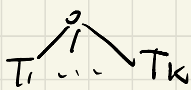
$\Rightarrow$ 0 0 1 0 0 1 0 0 1 1 1 0

"

Def. $\pi(T)$

$\pi(T)$:

  if $T =$ "o", return 0 1

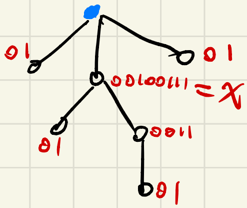
  else $T =$  return $0\,\pi(T_1)\cdots\pi(T_k)\,1$

  endif

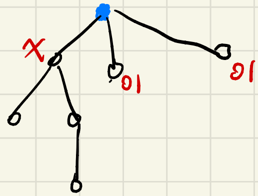
Observation. Two ordered trees T_1, T_2 are isomorphic iff $\pi(T_1) = \pi(T_2)$

Encode Rooted Tree

e.g. try



(ordered)



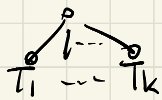
0 01 x 01 1   0 x 01 01 1

should make them the same

sort

$\pi(T)$:

if $T=$ "o" return 01

else $T=$ 

$\pi_i := \pi(T_i)$

Sort$([\pi_1, \dots, \pi_k])$

return $0\pi_1\pi_2 \cdots \pi_k 1$

endif

Observation. Two rooted trees T_1, T_2 are isomorphic iff $\pi(T_1) = \pi(T_2)$

Isomorphism of Tree(T_1, T_2):

~~for all $r_1 \in V_1$~~ Pick a r_1

forall $r_2 \in V_2$

if $\pi(T_1, r_1) = \pi(T_2, r_2)$, return true

end for

~~end for~~

return false $\Rightarrow O(n^2)$

Note: there is a linear algorithm in Text Book

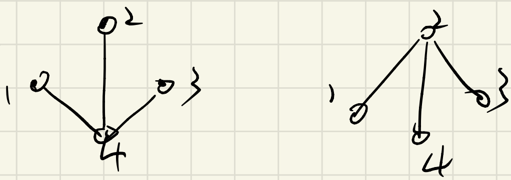
Number of Trees (Video)
[Cayley's Formula]

Q: How many trees on n vertices?

e.g. $n=3$

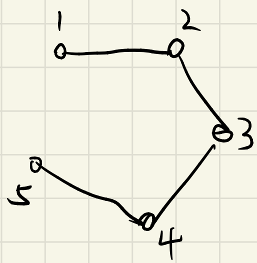
$T_3 = 3$

$n=4$



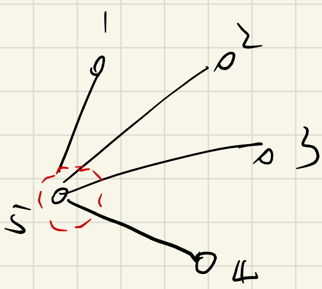
. . .

e.g. $n=5$

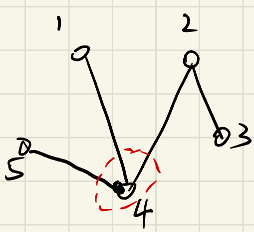


"Path": $\frac{5!}{2} = 60$

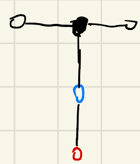
$T_5 = 125$



"star": 5



"T-shape"



$5 \times 4 \times 3 = 60$

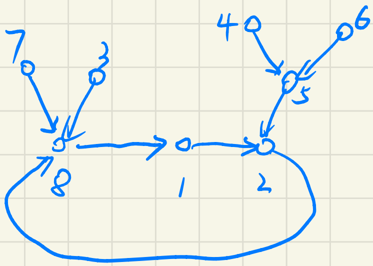
result: #vertices: 1 2 3 4 5 6 ...
#trees: 1 1 3 16 125 1296 ...

Theorem. Let $V=\{1,\dots,n\}$. There are n^{n-2} trees on V.

$\boxed{\text{Q: what is } n^n\text{? A: } \# f: V\to V}$

see a e.g. of f:

w	1	2	3	4	5	6	7	8
$f(w)$	2	8	8	5	2	5	8	1



"almost a tree"

Def. A vertebrate is a triple (T,h,b) where
(i) T is a tree on V;
(ii) $h,b\in V$.
Furthermore, h is called the head, and b the butt

$S_n := \#$vertebrates on n vertices

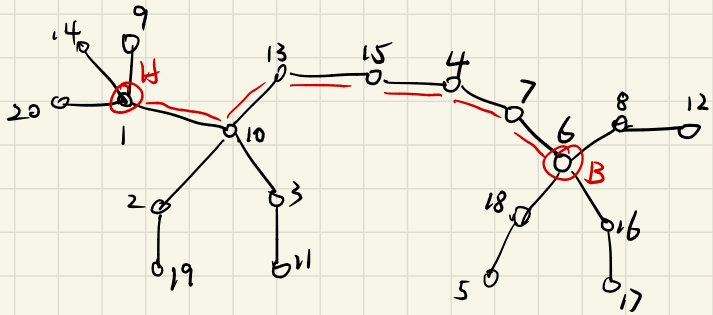
$\Rightarrow S_n = T_n\cdot n^2$ [take a tree; select head and butt]

Want to prove: $T_n = n^{n-2}$ [$\Leftrightarrow S_n = n^n$]

idea: construct $V\to V$

Def. Spine: the unique path from head to butt.

e.g.



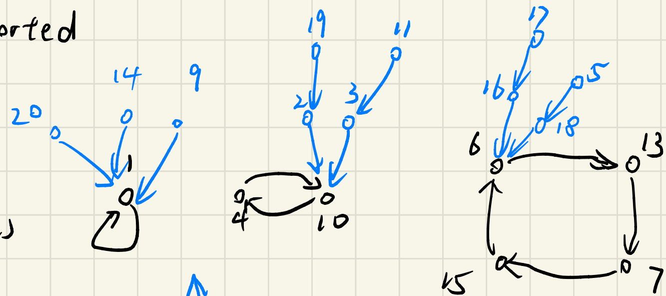
(i) write the path:

1	4	6	7	10	13	15	← x
1	10	13	15	4	7	6	← $f(x)$

spine → spine

(ii) write again, sorted

⇒ we get: (black part)

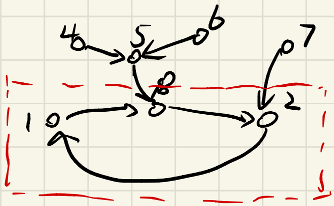


then map their neighbours: (blue part)

⇒ Vertebrate on V ⟶ function $f: V \to V$

Now: Function $f: V \to V$ ⟶ vertebrate on V ?

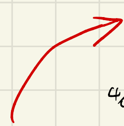
e.g.

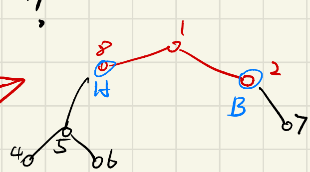


locate a cycle ⟶

1	2	8
8	1	2

H B

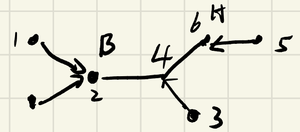




Graph. Cont. (Class)

The number of trees on n vertices $V = \{1, 2, \cdots, n\}$

(in video) Trees + head + butt = vertebrate



Proved. There is a bijection

① set of all functions from V to V

② the set of all vertebrates, i.e.,

(T, H, B), where $T = (V, E)$ is tree, $H, B \in V$

$n^n = |①| = |②| = (\#\text{tree}) \times n \times n$

$\#\text{tree} = n^{n-2}$

Advantages: Write a program that outputs a random tree.

that is, every tree on $V = \{1, \cdots, n\}$ appears the same probability

- output a random number $i \in \{1, \cdots, n\}$
- Output a random set of size 3.
- Output a random permutation (bijection $[n] \to [n]$)
- output a random function $f: [n] \to [n]$, $f(i) = ?$

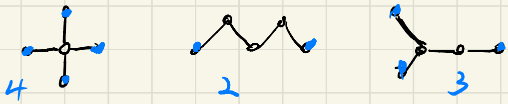
- random Tree (n):

  f: = a random function $[n] \to [n]$.

  covert f into a vertebrate (T, H, B)

  Output T.

$n=5$, 125 trees



Q: How many leaves on average?

Method. Run randomTree(n) "a million times"

count # leaves

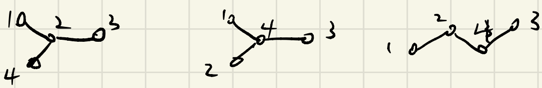
comput average.

Q: How many degree 2 vertices.

Q: If there are n^{n-2} trees on $\{1,\dots,n\}$, maybe there is a simple way to encode a tree T as a sequence $c_1,\dots,c_{n-2} \in [n]^{n-2}$?

Idea.1 Cut a leaf, write it down, go on with the remaining tree.

[Wrong]

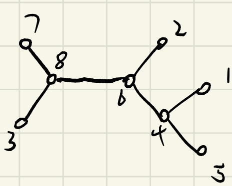


all can be encoded $\langle 1,3 \rangle$

Idea.2 Cut a leaf, write ~~it~~ down, go on with the remaining tree.

its neighbor

e.g.



cut: 1 2 3 5 4 6

write: 4 6 8 4 6 8

add a rule: cut the smallest leaf. → 4 6 8 4 6 8

e.g. if we get 4 5 2 2 2 2 when $n=8$, we know 1, 2, 3, 5, 7 are leaves. 1 is the smallest and the first leaves to cut.

decode $(V,\ c_1 c_2 \cdots c_{n-2})$

if $n \geq 3$:

$\quad l := \min V \setminus \{c_1, \cdots, c_{n-2}\}$

$\quad T' = \text{decode}(V \setminus \{l\},\ c_2, \cdots, c_{n-2})$

$\quad T := T'$ plus the edge from c_1 to l

$\quad$ return T

else if $n = 2$:

$\quad$ return the unique tree on V

Prufer Code

Expected number of leaves in a tree

$T \Longleftrightarrow c_1 c_2 \cdots c_{n-2}$

v is a leaf $\Leftrightarrow v \notin \{c_1, \cdots, c_{n-2}\}$

Random $T \Leftrightarrow$ Random $c_1 c_2 \cdots c_{n-2} =: c$

Prob space $= [n]^{n-2}$

$$\forall v,\ Pr[v \text{ is a leaf}] = Pr[v \notin \{c_1, \cdots, c_{n-2}\}]$$

$$= Pr[v \neq c_1 \wedge v \neq c_2 \wedge \cdots \wedge v \neq c_{n-2}]$$

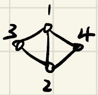
$$= \frac{n-1}{n} \times \frac{n-1}{n} \times \cdots \times \frac{n-1}{n}$$

Let $v \in [n]$

$$Pr[v \text{ is a leaf in } T] = \left(\frac{n-1}{n}\right)^{n-2} = \left(1 - \frac{1}{n}\right)^n \times \left(\frac{n}{n-1}\right)^2 \xrightarrow{n \to \infty} \frac{n}{e}$$

Claim. The number of automorphisms of a graph on n vertices divides $n!$

$\mathrm{aut}(G) \mid n!$

e.g. $\mathrm{aut}($ 

$) = 4 \mid 24$

Proof. There are $n!$ many bijections

$\pi : V \to V$

Let $G = (V, E)$ be a graph, $\pi : V \to V$ be bijection $\pi(G) = (V, \{\{\pi(u), \pi(v)\} \mid \{u, v\} \in E\})$

obs. $\pi(G)$ is isomophic to G

obs. $\pi(G) = G$ if and only if π is an automoiphism

$\pi_1, \pi_2, \ldots, \pi_{n!}$: all bijections

$\pi_1(G), \pi_2(G), \ldots, \pi_{n!}(G)$

$\quad\; \| \qquad\quad\; \| \qquad\qquad\qquad \|$

$\quad G_1 \qquad G_2 \quad , \ldots, \quad G_{n!}$

G appears $\mathrm{aut}(G)$ times in this sequence.

$a := \mathrm{aut}(G)$

$b :=$ # different graphs in the sequence $|\{G_1, G_2, \ldots, G_{n!}\}|$

Let $H \in \{G_1, \ldots, G_{n!}\}$ $\quad H \cong G$

H appears $\mathrm{aut}(H)$ times

$\qquad\qquad\quad \|$

$\qquad\quad \mathrm{aut}(G)$

Every H in $\{G_1, \ldots, G_{n!}\}$ appears a times in

$(G_1, G_2, \ldots, G_{n!})$

$\Rightarrow a \times b = n!$

$\Rightarrow a \mid n!$

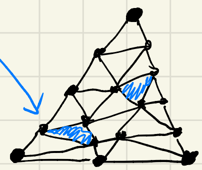
The Hand Shaking Lemma (Video)

Lemma. $G=(V,E)$, $\sum_{v\in V} \deg(v) = 2|E|$.

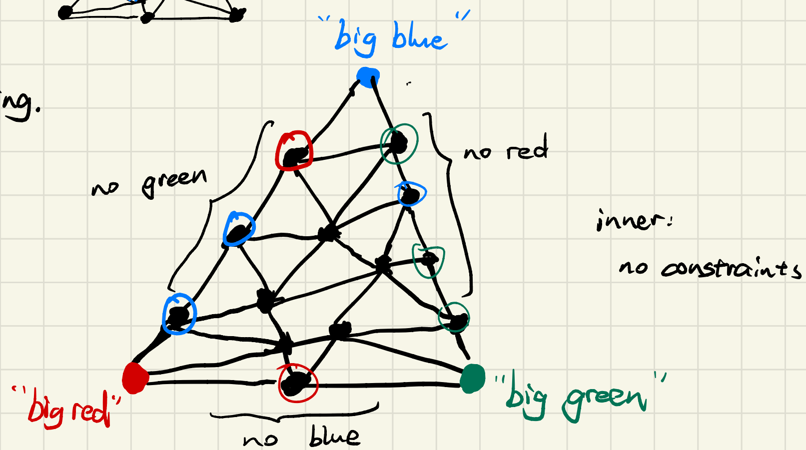
Applications.

Sperner's Lemma.

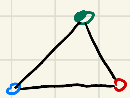
Triangulation. e.g.



Sperner Coloring.



Rainbow Triangle.



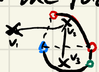
Sperner's Lemma. Every Sperner coloring of a triangulation has a rainbow triangle.

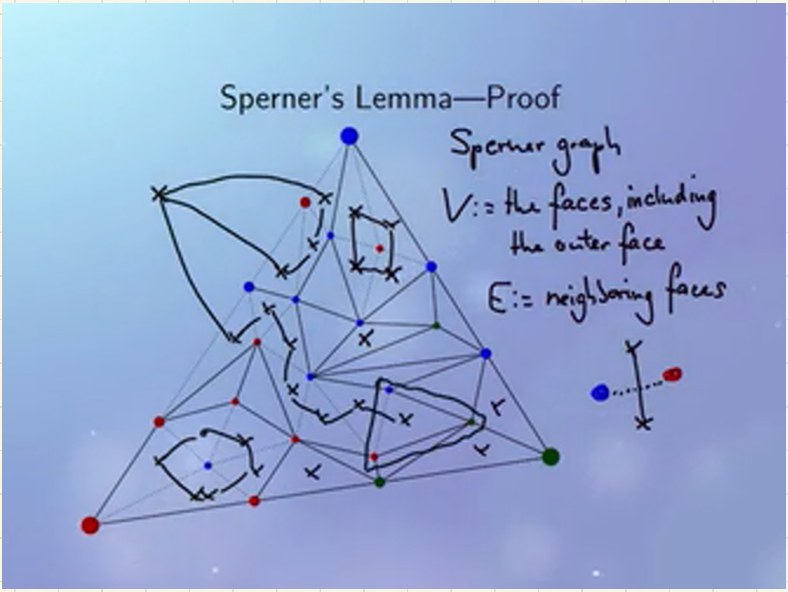
proof. Choose two colors, e.g. blue and red.

Erase edges between blue and red.

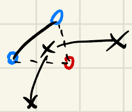
Def. Sperner graph. $V:=$ the faces, including "the outer face"

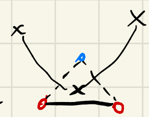
$E:=$ neighboring faces,

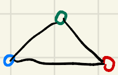




Observation: a path get stuck at a rainbow triangle.

deg() = 2

deg() = 2

deg() = 1

deg("x" in other triangle) = 0

deg(outer face) = # color changes from "big blue" to "big red"
[which is odd]

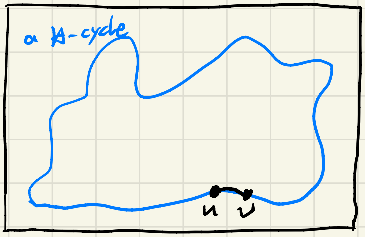
Then, #(rainbow triangles) = $\underbrace{\#(\text{odd vertices})}_{\text{even, from Hand Shaking Lemma.}} - 1$ = odd ≥ 1 ∎

Smith-Thomason Theorem on Hamilton Cycles

Def. Hamilton cycle. ...

Smith-Thomason Theorem. Let G be a graph where $\deg(v)$ is odd for all v.
If G has a Hamilton cycle, then it has at least two.

proof.

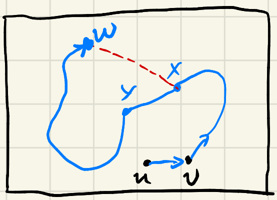


G

u-v: connected in the cycle.

Def. S: = the Hamilton path starting at (u,v). [must have (u,v)]

Def. Exchange operation / Flip on S.



G

$p \in S$

w: end point of p

$e := (x, w) \in E$

$p + e - (x,w) = p' \in S$

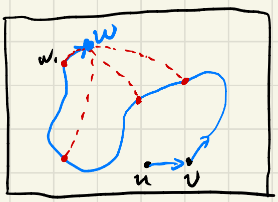
say p flips to p': $p \to p'$

also $p' \to p$ (symmetric relation)

S with this relation $(\leftrightarrow)$ is a graph H, call it the exchange graph

$p \in S$: $\deg_H(p) = \deg_G(w) - 1$ [except the vertice already connected, i.e., w_1]

odd, by def.



G

$\Rightarrow \deg_H(p)$ is even

Exception: $(w, u) \in E$, then $p - (u,v) + (u,w) = p' \notin S$,

as it doesn't connect (u,v).

Then if $(w,u) \in E$, $\deg_H(p) = \deg_G(w) - 2$

$\Rightarrow \deg_H(p)$ is odd,

while $p + (w, u)$: is a Hamilton Cycle

$\Rightarrow$ #(Hamilton Cycles containing (u,v)) = #(odd vertices in H) = even ∎

Minimum Spanning Tree (Video)

Def. Minimum Spanning Tree. ...

Def. A set $X \subseteq E$ is called **good** if there is a minimum spanning tree T such that $X \subseteq T$

Note. ϕ is good
X is good $\Rightarrow$ X is acyclic
$X' \subseteq X \Rightarrow X'$ is good

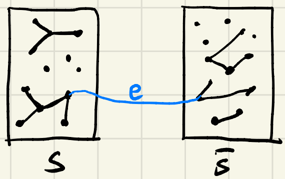
[Ref. See lecture of Matroid in Algorithm course]

Proof of Kruscal Algorithm.
Goal: show that our edge set is good in every step.

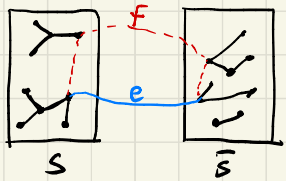
$\Uparrow$

Cut lemma. Let $X \subseteq E$ be a good set. If (V, X) is not a spanning tree, then (V, X) consists of two or more connected components.
Let $V = S \cup \bar{S}$ be a **cut** of X. [No edge from S to $\bar{S}$.]
Let $e \in E$ be an edge of minimum cost connecting two connected components of (V, X). Then $X \cup \{e\}$ is also good.

proof.



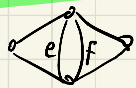
$X \subseteq E(T)$, T is M.S.T.
1. if $e \in E(T)$: $X \cup \{e\} \subseteq E(T)$
2. else $T+e$ has a cycle, crossing "gap" at least twice.



$c(f) \geq c(e)$ (weight)

$T' = T+e-f$ is a tree. [acyclic, n-1 edges]
$c(T') \leq c(T)$, while $c(T)$ is minimum.
$\Rightarrow c(T') = c(T) \Rightarrow X \cup \{e\} \subseteq E(T')$
$X \cup \{e\}$ is also good. ∎

Spanning Trees (Class)

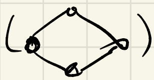
t().

$t(G)$ = # spanning trees of G

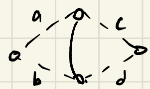
$t(K_n) = n^{n-2}$ by Cayley's Formula. [from Video]

There are n^{n-2} trees. - - - -

e.g.1. case 1: The tree uses neither e or f

$t($  $) = 4$

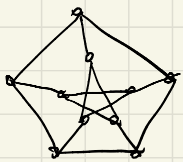
case 2: T contain e



a / b ?
c / d ?

$2 \times 2 = 4$

e.g.2



?

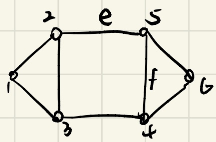
Bǎo Lì: $10^{10-2} = 10^8$

$O(n^{n-2})$?

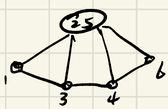
Def. Let $G = (V, E)$ be a multi graph. Then $G - e$ is $(V, E \setminus \{e\})$.

G/e : is the multi graph resulting from contracting the edge e.

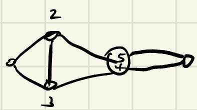
e.g. G =



$\Rightarrow$ $G/e \stackrel{\text{def.}}{=\!=}$



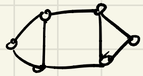
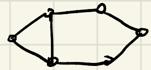
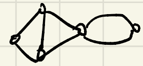
$G/f \stackrel{\text{def.}}{=\!=}$



Observation: $t(G) = t(G-e) + t(G/e)$

Proof (Informal): If $e \notin T$ then T is a spanning tree of $G-e$

If $e \in T$ then T/e is a spanning tree of G/e.

e.g. $t($  $) = t($  $) + t($  $)$

Alg. $t(G)$

  if $n=1$ return 1

  else if G not connected return 0

  else

    let e be an edge

    return $t(G-e) + t(G/e)$

Complexity.

n vertices, m edges.

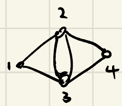
$R(n,m) \le R(n,m-1) + R(n-1,m-1)$

[compare to $\binom{a}{b} = \binom{a-1}{b} + \binom{a-1}{b-1}$]

$\le c \cdot \binom{m}{n} \le O(m^n)$

if $m = \Theta(n^2)$, then $O(n^{2n})$

G



$A_G :=$ the adjcent matrix of a graph.

$(A_G)_{u,v} =$ # edges between u and v.

$L_G :=$ the Laplacian matrix of G.

$$= \begin{pmatrix} d(1) & & & 0 \\ & d(2) & & \\ & & \ddots & \\ 0 & & & d(n) \end{pmatrix} - A_G$$

e.g.

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$L_G = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -2 & -1 \\ -1 & -2 & 4 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$$

Def. Let $M \in \mathbb{R}^{n \times n}$. Then M' is the $(n-1)\times(n-1)$ matrix resulting from M deleting the first row and first column.

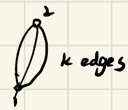
e.g. $$L_G' = \begin{pmatrix} 4 & -2 & -1 \\ -2 & 4 & -1 \\ -1 & -1 & 2 \end{pmatrix}$$

Kirchhoff's Matrix Tree Theorem

$$t(G) = \det(L'_G)$$

Proof. by induction on m.

$|V| = 2$



$L_G = \begin{pmatrix} k & -k \\ -k & k \end{pmatrix}$, $L'_G = (k)$

$\det(L'_G) = k = t(G)$

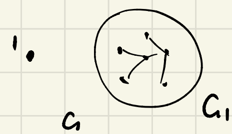
if $n \geq 2$ and $m = 0$ $\quad L_G = (0)$, $\det(L'_G) = 0 = t(G)$

induction steps:

Case 1: $\deg(1) = 0$

$$L_G = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & \boxed{L_{G_1}} & \\ 0 & & & \\ 0 & & & \end{pmatrix} \qquad L'_G = L_{G_1}$$

$t(G) = 0$



obs: let H be a graph

Then $L_H \cdot \begin{pmatrix} \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

L_H is a sigular matrix $\quad (\text{rank} < |V(H)|)$

$\Rightarrow \det(L_H) = 0$

Case 2: Vertex 1 has a neighbor v.

switch name of v and 2

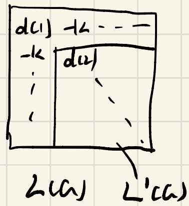
$\Rightarrow$ exchange row 2, v and column 2, v

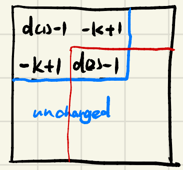
$\det = \det \times (-1)^2 = \det$!

We can assume that $e = \{1, 2\} \in E(G)$

$$t(G) = t(G-e) + t(G/e) \xrightarrow{\text{induction}} \det(L'_{G-e}) + \det(L'_{G/e})$$

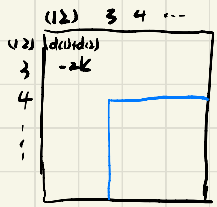
There are $k \geq 1$ edges from 1 to 2





$L_{G\cdot e}$

$$L'_{G\cdot e} = L'_G - \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}$$



$L_{G/e}$

$$\underline{L'_{G/e} = L''_G}$$

$$t(G) \overset{\text{cont.}}{=\!=} \det\left(L'_G - \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}\right) + \det(\underbrace{L''_G}_{\mathbb{R}^{(n-2)\times(n-2)}})$$

note:

$$\det\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ a_3 & & & & \\ a_4 & & L''_G & & \\ \vdots & & & & \\ a_n & & & & \end{pmatrix} = \det(L''_G)$$

whatever $a_3 \sim a_n$ are

Let: $a_i := -\#$ edges from 2 to i

$= (L_G)_{i,2}$

$$t(G) \overset{\text{cont.}}{=\!=} \det\left(L'_G - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) + \det\begin{pmatrix} 1 & 0 \; 0 \cdots 0 \; 0 \\ a_3 & \\ \vdots & L''_G \\ a_n & \end{pmatrix}$$

$$= \det\begin{pmatrix} d(2)-1 & a_3 \;\; a_4 \cdots a_n \\ a_3 & \\ \vdots & L''_G \\ a_n & \end{pmatrix} + \det\begin{pmatrix} 1 & 0 \;\; 0 \cdots 0 \\ a_3 & \\ \vdots & L''_G \\ a_n & \end{pmatrix}$$

Lemma. [Linear Algebra]

$$A = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad x_1 \cdots x_m \in \mathbb{R}^m, \quad B = \begin{bmatrix} y_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}$$

then $\det(A+B) = \det(A) + \det(B)$

$$= \det \begin{pmatrix} d(2)-1+1 & a_3+0, & \cdots, & a_n+0 \\ a_3 & & & \\ \vdots & & \boxed{L''_G} & \\ a_n & & & \end{pmatrix}$$

$$= \det(L'_G)$$

■

Alg. $t(G)$

construct L_G

construct L'_G

return $\det(L'_G)$

Partial Ordering (Video)

<u>Def.</u> Let S be a set. $R \subseteq S \times S$ be a relation.

- R is reflexive if $(x,x) \in R \ \forall x \in S$
- R is transitive if $(x,y), (y,z) \in R \Rightarrow (x,z) \in R$

$$x \longrightarrow y \longrightarrow z$$

- R is anti-symmetric if $(x,y), (y,x) \in R \Rightarrow x = y$

<u>Def.</u> A relation that is reflexive, transitive, antisymmetric is called an ordering of S.

<u>Observation</u>. A bonus property.

$(\mathbb{N}, \leq)$: $a \leq b$ or $b \leq a$.

$(\mathbb{Z}, |)$: $a \nmid b$ and $b \nmid a$ is possible

<u>Def.</u> Linear Ordering / Total Ordering.

<u>Def.</u> x is an immediate predecessor of y if

1. $x \prec y$;
2. there is no t with $x \prec t \prec y$.

Then include $x \to y$ in **Hasse Diagram**

<u>Lemma</u>. Suppose $(S, \preceq)$ is an ordering, and S is finite. Then the Hasse Diagram uniquely defines $\preceq$.

<u>Def.</u> $x \leq y$ or $y \leq x$ then x, y are **comparable**, otherwise **incomparable**.

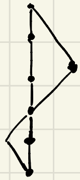
Def. $(S, \preceq)$, $C \subseteq S$, a, b is comparable $\forall a, b \in C$, then C is a **chain**.
$A \subseteq S$, a, b is incomparable $\forall a \neq b \in A$, then A is an **antichain**.

Def. x is **maximal** if $\neg \exists y \in S: x \prec y$.
minimal if $\neg \exists y \in S: y \prec x$.

Def. x is **maximum** if $y \preceq x$ $\forall y \in S$.
--- **minimum** ---

Def. height$(S) = |$largest chain$|$, width$(S) = |$largest antichain$|$

e.g.



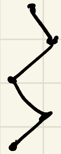
height $= 6$
width $= 2$

Mirsky's Theorem. [max size of chain = min size of partition]

height(S) is the minimum t such that we can partition S into t antichains:
$S = A_1 \cup A_2 \cup \cdots \cup A_t$

Proof. (1) Prove height$(S) \leq t$

S



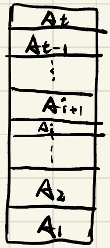
obviously: $|\text{Chain} \cap \text{Antichain}| \leq 1$
$(|C \cap A_i| \leq 1)$

$\Rightarrow |C| \leq t$

(2) Prove height$(S) \geq t$

Find $S = A_1 \cup \cdots \cup A_t$, chain C: $|C| \geq t$

S

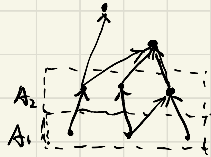


A_t : ---

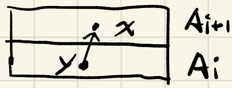
A_{i+1} : minimal of $S / (A_1 \cup \cdots \cup A_i)$

A_2 : minimal of S/A_1

A_1 : minimal of S



Lemma. $\forall x \in A_{i+1}, \exists y \in A_i : y < x$



proof. otherwise, x is minimal in $S / (A_t \cup A_{t-1} \cup \cdots \cup A_i)$

$\Rightarrow x \in A_i$, while $x \notin A_i$

Then we can find at least a chain with size of t.

Mirsky's Theorem (another description)

S can be partitioned into t antichains

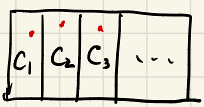
if and only if

Every chain has size at most t.

Dilworth's Theorem [max size of antichain = min size of chain partition]

width(S) is the minimum t such that we can partition S into t chains.

Proof. (1) show that $|\text{antichain}| \le |\text{chain partition}|$ [width$(S) \le t$]



$\Rightarrow |\text{antichain}| \le t$

at most one in each partition

(2) show that width$(S) \ge t$

requires more tools ... TBD.

Corollary. $\text{width}(S) \cdot \text{height}(S) \geq |S|$

proof. $\exists i : |A_i| \geq \frac{|S|}{t}$ (otherwise...)

$$= \frac{|S|}{\text{height}(S)}$$

also, $\text{width}(S) \geq |A_i|$

An Application of Mirsky's Theorem

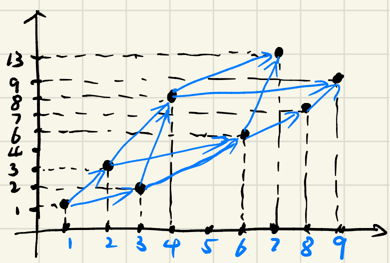
Def. 1, 3, 2, 8, 6, 4, 13, 7, 9

increasing subsequence

decreasing subsequence

Erdős-Szekeres Theorem.

Let $a_1, \ldots, a_n$ be distinct numbers.
There is an increasing subsequence of length $\geq \sqrt{n}$
or a decreasing subsequence of length $\geq \sqrt{n}$



1	3	2	8	6	4	13	7	9
1	2	3	4	5	6	7	8	9

$(\mathbb{N}^2, \leq)$

a chain: an increasing subsequence $\to$ size: height
an antichain: a decreasing subsequence $\to$ size: width

$\text{height} \cdot \text{width} \geq n$

A more gereral form.

$a_1, \cdots, a_n$: distinct numbers

If $n \geq rs+1$, then

Some increasing subsequence has size $\geq r+1$

or - - - de - — —— — — — - - $\geq s+1$

In particular, one of them must be $\geq \sqrt{n}$.

Infinite Set Theory

Def. Two sets A, B have the same size $(A \cong B)$ if there is a bijection $f: A \to B$.
If there is an injective function $f: A \to B$, we write $A \leq B$

Lemma. $N \cong N_0$ $\quad N = \{1, 2, 3, \cdots\}$
$N_0 = \{0, 1, 2, \cdots\}$

proof. $g: N \to N_0$, $x \mapsto x-1$ is bijective

Note. $N \subsetneq N_0$, yet $N \cong N_0$

Claim. $Z \cong N$ $\quad \lfloor \frac{x}{2} \rfloor \cdot (-1)^x$

Lemma. $Q \cong N$

$g: N \to Q$, $x \mapsto x$ is injective, so $N \leq Q$

$f: Q \to N$

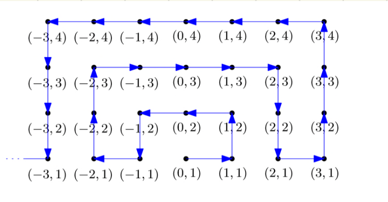
Attempt 1. Given $\frac{a}{b} \in Q$ where $\gcd(a, b) = 1$, define $f(\frac{a}{b}) = 2^a \times 3^b$

Attempt 2.

Step 1. Write down the set $Z \times N$

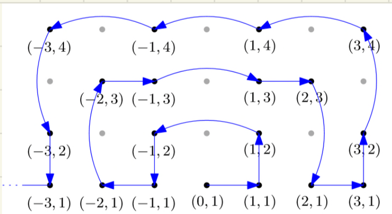
		-2	-1	0	1	2	3	4
1	$\cdots$	-2/1	-1/1	0/1	1/1	2/1	3/1	4/1
2	$\cdots$	-2/2	-1/2	0/2	1/2	2/2	3/2	4/2
3	$\cdots$	-2/3	-1/3	0/3	1/3	2/3	3/3	4/3
4	$\cdots$	-2/4	-1/4	0/4	1/4	2/4	3/4	4/4

Step 2. Remove (a,b) if $\gcd(a,b) \neq 1$

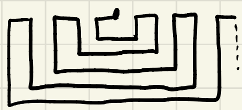


		-2	-1	0	1	2	3	4
1	---	$-2/1$	$-1/1$	$0/1$	$1/1$	$2/1$	$3/1$	$4/1$
2	---	$\cancel{-2/2}$	$-1/2$	$\cancel{0/2}$	$1/2$	$\cancel{2/2}$	$3/2$	$\cancel{4/2}$
3	---	$-2/3$	$-1/3$	$\cancel{0/3}$	$1/3$	$2/3$	$\cancel{3/3}$	$4/3$
4	---	$\cancel{-2/4}$	$-1/4$	$\cancel{0/4}$	$1/4$	$\cancel{2/4}$	$3/4$	$\cancel{4/4}$

Step 3. Build a "snake" of point, starting at $(0,1)$



		-2	-1	0	1	2	3	4
1	---	$-2/1$	$-1/1$	$\boxed{0/1}$	$1/1$	$2/1$	$3/1$	$4/1$
2	---		$-1/2$		$1/2$		$3/2$	
3	---	$-2/3$	$-1/3$		$1/3$	$2/3$		$4/3$
4	---		$-1/4$		$1/4$		$3/4$	



N:	1	2	3	4	5	6	7	8	9
Q:	0	-1	$-1/2$	$1/2$	1	2	$2/3$	$1/3$	$-1/3$

This is a bijection

Some observation about $\mathbb{R}$

① $\mathbb{R} \cong (0,1) \cong [0,1] \cong [0,1)$

② $x \in [0,1)$, $0 \leq x < 1$, $x = 0.\underbrace{1011010110 1\cdots}_{\text{infinite string of 0's and 1's}}$ in binary

$\{0,1\}^\infty$: infinite $0/1$ string

2^N : subsets of integers

$\{0,1\}^\infty \cong 2^N$

$x \in \{0,1\}^\infty$ maps to $\{n \in N \mid x_n = 1\}$

$S \subseteq N$ maps to $(x_1 x_2 \cdots)$ where $x_n = [1 \text{ if } x \in S,\ 0 \text{ if } x \notin S]$

1° $f: [0,1) \to \{0,1\}^\infty$, $x \to$ its binary representation after "."
is injective but not bijective

$\mathbb{R} \cong [0,1) \leq \{0,1\}^\infty$

e.g. $f(x) \neq 0.11111\cdots$
$f(x) \neq 0.00111\cdots$

2° $\{0,1\}^\infty \leq \mathbb{R}$ $\quad g: \{0,1\}^\infty \to \mathbb{R}$ $\quad x = (x_1, x_2, \cdots) \mapsto (0.x_1x_2x_3\cdots)_{\text{decimal}}$

$(1000\cdots) \mapsto 0.1000\cdots = 1/10$
$(01111\cdots) \mapsto 0.0111\cdots = 1/90$

<u>Def</u>. A, B sets, A^B is the set of functions $f: B \to A$
[check: if A, B are finite then $|A^B| = |A|^{|B|}$]

$\{0,1\}^N = \{f: N \to \{0,1\}\} \cong \{(f(1), f(2) \cdots) \mid \cdots\}$

$\cong \{(x_1, x_2, \cdots), x_i \in N\} = \{0,1\}^\infty$

<u>Observation</u>. $\{0,1\}^\infty \cong \{0,1\}^N \cong 2^N$

<u>Theorem</u>. **(Schröder Berstain Theorem).**

$A \leq B$, $B \leq A$ imply $A \cong B$

R^2 : the plane

Lemma. $R \cong R^2$

proof. $f: R^2 \to$ as follows

$$R \cong \{0,1\}^\infty$$

$$(x,y) \mapsto (a_1 a_2 a_3 \ldots, b_1 b_2 b_3 \ldots) \to (a_1 b_1 a_2 b_2 \cdots) \to R$$

Theorem. $N < R$

Proof.

[Cantor's First Proof.]

① $N \le R$: there is an injection $f: N \to R$. e.g. $f(x) = x$

② $N \not\cong R$. Let $f: N \to R$, we'll show that f is not a bijection.
In particular, it is not a surjection. $(\exists r \in R, \forall n \in N, f(n) \neq r)$

$r_n := f(n)$, so f "is" a sequence $r_1 r_2 \cdots \in R$

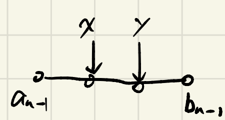
We keep an interval $I_n = [a_n, b_n]$ such that

- $r_1, r_2, \ldots, r_n \notin I_n$
- $I_1 \supseteq I_2 \supseteq \cdots$

$a_0 = 0$, $b_0 = 1$

for $n = 1, 2, 3, \cdots$

$$x = \frac{2a_{n-1} + b_{n-1}}{3}, \quad y = \frac{a_{n-1} + 2b_{n-1}}{3}$$



Set $[a_n, b_n]$ to be either $[a_{n-1}, x]$ or $[y, b_{n-1}]$,
whichever of the two does not contain r_n.
If neither contains r_n, choose the former one.

$a := \lim_{n \to \infty} a_n \qquad b := \lim_{n \to \infty} b_n$

Claim. $\forall n,\ r_n \neq a$

proof. Look at $[a_{n-1}, b_{n-1}]$

If $r_n \notin I_{n-1}$, then $r_n \neq a$;

If $r_n \in I_{n-1}$ then $r_n \notin I_n$

proof. (easier)

Observation: $r_n \notin I_n$

But $a_n \leq a \leq b_n$ so $a \in I_n$

So $r_n \neq a\ \forall n \in N$

$\Rightarrow f$ is not surjective

proof. Make an infinite matrix for $f: N \to \{0,1\}^\infty$

[see the lecture notes]

[DIAGONALIZATION]

Q: Is $R < 2^R$

Theorem. $X < 2^X$

proof. ① $X \leq 2^X$, since $f: X \to 2^X$, can be $x \to \{x\}$

② $X \neq 2^X$. Given any $f: X \to 2^X$, we show that f is not surjective by constructing a set $S \subseteq X$ s.t. $\forall x \in X: f(x) \neq S$.

Construction.

An element x is <u>white</u> if $x \in f(x)$

is <u>black</u> if $x \notin f(x)$

$S := \{x \in X \mid x \text{ is black}\}$

Claim. $\forall x \in X,\ f(x) \neq S$.

proof. If x is white, then $x \in f(x)$, $x \notin S$;

If x is black, then $x \notin f(x)$, $x \in S$.

$\Rightarrow f(x) \neq S$

Q: Is there a set X with $N < X < R$?

$\longrightarrow$ seach "Continuum Hypothesis"

[This is "independent" of the axiom of set theory.]

* Something about Computing Theory

Problem. Given an n-bit number in binary $x_1 \cdots x_n$, is it divisible by 7 ?

e.g.

```
remainder = 0 ;
for i=0 to n do
    T = remainder * 2 + x_i ;
    T = T mod 7
end for
return Yes if T=0
```

$\}$ $O(n)$

Problem. Given $x = (x_1 x_2 \cdots x_n)$ is it a perfect square ?

e.g.

```
for i=0 to (x)bin
    if i×i = (x)bin
        return Yes
```

$\}$ $O(2^n)$

e.g. l: $l \times l \leq (x)_{bin}$

u: $u \times u \geq (x)_{bin}$

$l := 0$, $u := (x)_{bin}$

while $(u - l \geq 2)$

$m := \frac{l+u}{2}$ $\longrightarrow$ $O(n * n * n)$

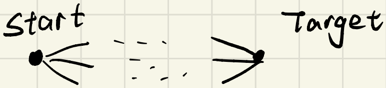
if $m \times m > (x)_{bin}$ $= O(n^3)$

$u = m$ $\rightarrow O(n^2)$

else $r = m$

Theorem. There is a computational problem that can be solved in $O(n^{20})$ but not $O(n^{19})$.

Flow (Video)



Def. The capacity of a net work is the maximum number of independent paths from Start to Target

Def. The vulerability of a network is the minimum number of edge one has to destroy in order to disconnect Start from Target.

Theorem. capacity = vulerability. [Max-flow min-cut theorem]

$G = (V, E)$

A source vertex s, a sink vertex t

Edge capacities $c: E \to R^+$

Def. Let (G, s, t, c) be a flow network. A flow is a function $f: V \times V \to R$ satisfying:

- $f(u,v) \leq c(u,v)$
- $\sum_u f(u,v) = \sum_w f(v,w) \quad \forall v \in V \setminus \{s,t\}$ [flow conservation]
- $f(u,v) = -f(v,u)$

Def. The value of a flow is $val(f) := \sum_v f(s,v)$

Lemma. Out-flow at s = in-flow at t.

$\sum_v f(s,v) = \sum_v f(v,t)$

prof. $\sum_{u,v} -f(v,u) = \underbrace{\sum_{u,v} f(u,v)}_{} = \sum_v f(s,v) + \sum_v f(t,v) + \sum_{u \in V/\{s,t\}} \underbrace{\sum_v f(u,v)}_{=0}$

$\underbrace{\sum_{v,u} f(u,v)}_{} \Rightarrow = 0 \quad = \sum_v f(s,v) - \sum f(v,t) = 0$

Def. An s-t-cut (or cut) is a set S that contains s but not t.

$$\operatorname{cap}(S) := \sum_{u\in S, v\in V\setminus S} c(u,v)$$

$$f(S) := \sum_{u\in S, v\in V\setminus S} f(u,v)$$

Lemma. $f(S) \leq \operatorname{cap}(S)$

Proof. (1) $\operatorname{val}(f) = \sum_v f(s,v) = \sum_{\substack{u\in S\\ v\in V\setminus S}} f(u,v)$ [Exercise]

$$\leq \sum_{\substack{u\in S\\ v\in V\setminus S}} c(u,v) = \operatorname{cap}(S)$$

Theorem. There is a flow f and a cut S such that

$$\underbrace{\operatorname{val}(f)}_{\textbf{Max Flow}} = \underbrace{\operatorname{cap}(S)}_{\textbf{Min Cut}}$$

Def. Let $G = (V,s,t,c)$ be a flow network and f be a flow. Then $c_f := c - f$ are the <u>residual capacities</u> and $G_f := (V,s,t,c_f)$ is the <u>residual network</u>.

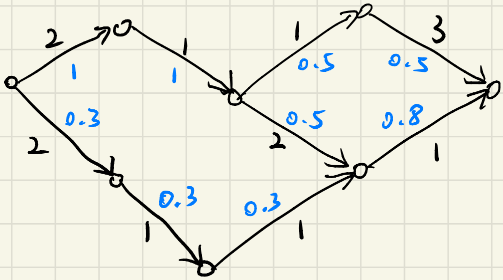
Lemma. Let f be a flow in G and f' be a flow in G_f. Then $f+f'$ is a flow in G.

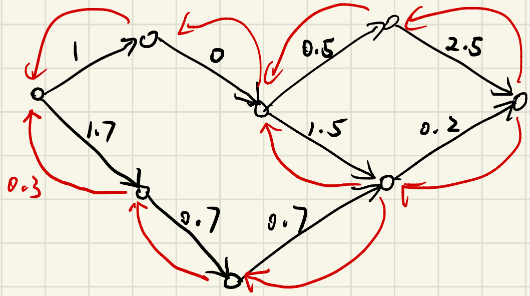
Proof. (1) $f+f' \leq c$.

Indeed $f+f' \leq f + c_f = f + c - f = c$

(2) $(f+f')(u,v) = -(f+f')(v,u)$

(3) $\sum_w (f+f')(v,w) = \sum_w f(v,w) + \sum_w f'(v,w) = 0 + 0 = 0$



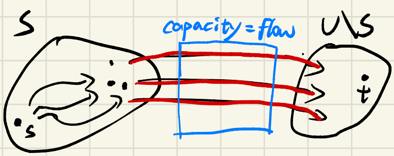


Proof. of Max-Flow Min-Cut Theorem.

1. Let f be a max flow [Assume existing ...]
2. G_f has no path $s \to t$

   if it did, $s \overset{f_p}{\rightsquigarrow}$ · $\quad val(f+f_p) > val(f)$, contradiction
3. $S := \{ v \in V \mid \exists \text{ path } s \rightsquigarrow v \text{ in } G_f \}$

   $t \notin S$, according to 2.



$\forall u \in S,\ v \in V \setminus S$:

$c_f(u,v) = 0$

$c_f = c - f \Rightarrow c(u,v) - f(u,v) = 0$

$$val(f) = \sum_{\substack{u \in S \\ v \notin S}} f(u,v) = \sum_{\substack{u \in S \\ v \notin S}} c(u,v) = cap(S)$$

An Algorithm for Maximum Flow

[Ford-Fulkerson]

maxflow(V, s, t, c):

$f := 0$ [$G_f = G$ at first]

while G_f contains a path p from s to t

$f_p :=$ maximum possible flow along p in G_f

$f := f + f_p$

end while

$S := \{ v \mid$ there is an s-v-path in $G_f \}$

return the max flow f and the min cut S.

If $c(u,v) \in \mathbb{Z}\ \forall (u,v)$:

it must terminate at some point

If $c(u,v) \in \mathbb{R}$:

fix: [Edmonds-Karp]

choose p to be the shortest s-t-path

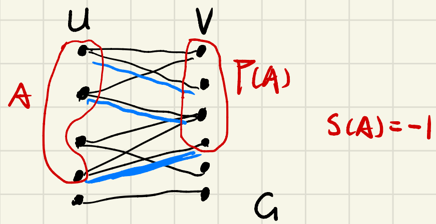
Theorem: $\leq n \cdot m$ iteration

$\Rightarrow O(n \cdot m^2)$ algorithm

Matching (Video)

Maximum Matching in Bipartite Graphs

Def. Bipartite Graphs.



Matching: $M \subseteq E$ that "don't share any point"

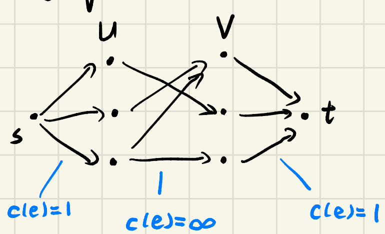
$A \subseteq U$: $\Gamma(A)$ is the neighbourhood of A

$\delta(A) := |A| - |\Gamma(A)|$

$\delta(G) := \max\limits_{A \subseteq U} \delta(A)$

Note: $\delta(G) \geq 0$, since $\delta(\varnothing) = 0 - 0 = 0$.

Algorithms for Maximum Matching [See CS214(Algorithm) Lab??]



Bipartite graph G $\longrightarrow$ Flow network G^0 $\longrightarrow$ Integral Maximum Flow

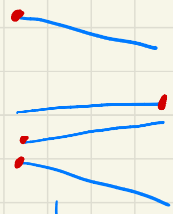
$\downarrow$

Maximum Matching

Def. Vertex Cover, ⋯ [a C: $\forall e$, $|C \cap e| \geq 1$]

König's Theorem.

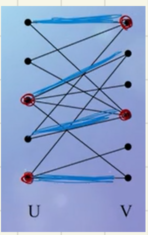
[easy part] If C is a vertex cover and M is a matching, then $|C| \geq |M|$.



4 edge of matching $\Rightarrow$ at least 4 vertices of covering

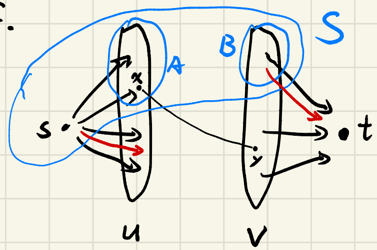
matching: disjoint

$\boxed{\text{In a bipartite graph, } \max|\text{matching}| = \min|\text{vertex cover}|}$



[hard part] There is a vertex cover C and a matching M such that $|M| = |C|$

proof.



$|M| = val(f)$

[f: maximum integral flow]

$\overset{\text{cont.}}{=} cap(S, \bar{S})$

[$S, \bar{S}$: minimum s-t-cut]

$A := S \cap U$, $B := S \cap V$

If $(x,y) \in E$, then $cap(S,\bar{S}) \geq c(x,y) \overset{\text{def.}}{=} \infty$, contradiction.

$\Rightarrow \forall x \in A, y \in V \setminus B, \{x,y\} \notin E$

In other words, $C := (U \setminus A) \cup B$ is a vertex cover.

$|C| = |U \setminus A| + |B|$

$|M| = cap(S, \bar{S}) = |U \setminus A| + |B| = |C|$

$\Gamma(A) \subseteq B$

$\Rightarrow |M| = |U| - |A| + |B|$

$\geq |U| - |A| + \Gamma(A)$ $\longrightarrow$ "Hard part" of Hall's Theorem.

$= |U| - \delta(A)$

Hall's Theorem:

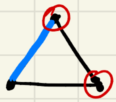
[easy part] For every $A \subseteq U$ and matching M: $|M| \leq |U| - \delta(A)$

[hard part] There is a matching M and a set $A \subseteq U$ s.t. $|M| \geq |U| - \delta(A)$

$\boxed{\text{If } G \text{ is a bipartite graph, then its maximum matching has size } |U| - \delta(G).}$

In particular, if $|\Gamma(A)| \geq |A|$ for every $A \subseteq U$,
then (and only then) there exists a matching of size $|U|$.

Note. König's Theorem fails for General Graphs.

e.g. 

$|M| = 1$

$|C| = 2$

* Matching Market

Q: ... (slides)

Given matrix $V = (V_{i,h})_{i,h}$, and price vector $p = (p_h)_h$, we define the "favorite graph" by adding edge (i, h) if $v_{i,h} - p_h = \max_{h'} (v_{i,h'} - p_{h'})$.

$\longrightarrow G_{V,p}$

Observation. If $G_{V,p}$ has a perfect matching, then assigning houses according to this perfect matching.

- is envy free
- maximizes total valuation

Algorithm. $p = (0, \dots, 0)$

while $G_{V,p}$ has no perfect matching:

- find $B \subseteq$ Buyers with $|\Gamma(B)| < |B|$
- raise p_h by 1 ($\$/¥/\dots$) for each $h \in \Gamma(B)$

end while

potential goes down by $|B|$ and up by $|\Gamma(B)|$

$$\text{potential}(V, p) := \sum_i \max_h \text{payoff}(i, h) + \sum_h p_h$$

Claim. Potential (V, p) is always ≥ 0

Proof. Buyer $1, \dots, n$, Houses $1, \dots, n$

$$\begin{aligned}
\text{Potential} &= \sum_{i=1}^{n} \max_h \text{payoff}(i, h) + \sum_h p_h \\
&\geq \sum_{i=1}^{n} \text{payoff}(i, i) + \sum_h p_h \\
&= \sum_{i=1}^{n} (V_{ii} - p_i) + \sum_h p_h \\
&= \sum_{i=1}^{n} V_{ii} \\
&\geq 0
\end{aligned}$$

Is this algorithm efficient ?

\# iterations $\leq$ initial potential

$$= \sum_i \max_h V_{i,h}$$

$n=4$, but $V_{i,h}$ can be as high as $50{,}000{,}000{,}\cdots{,}000$

TBD... ? Forgotten...