CPSC 536F Feb 8, 2022

Finish Valiant's monotone poly size majority formula

Then we'll have

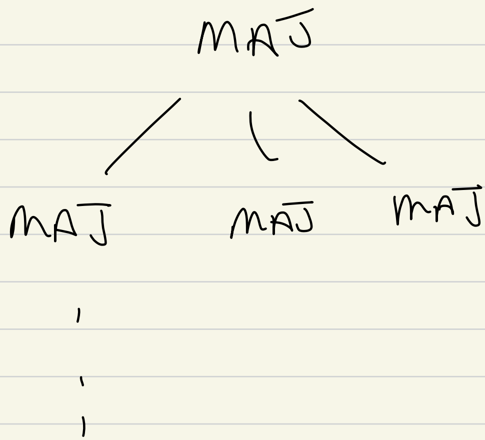
- ~~Fo~~ Boolean functions: formulas, circuits, etc. Spira's thm, - ~
- Monotone Boolean functions: similar principles
- Algebraic functions: field $\mathbb{F}$, usually $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/2\mathbb{Z}$, and $+$, $\times$: many similarities

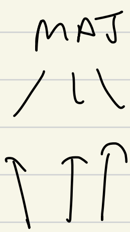
Analogue of P vs NP, easier!

Permanant: what is smallest formula ↔ determinant

"Permanent vs Determinant"

Last time:





random leaves chosen uniformly from $x_1, \ldots, x_n$

Rem: Instead of $0, 1$ could have $\{☹, ☺\}$, $\{a, b\}$...

Fixed $x_1 = 0, 1$

$\vdots$

$x_n = 0, 1$

if $MAJ(x_1, \dots, x_n) = 1$, 0

then (n odd)

prob randomly chosen leaf gives a 1 (0) has probability

$$\frac{(n+1)/2}{n} = \frac{n+1}{2n} = \frac{1}{2} + \frac{1}{2n}$$

and $\leq \frac{1}{2} - \frac{1}{2n}$ if maj are 0

If $\cancel{X}$ Y is random var $\begin{cases} 0 & \text{prob } p \\ 1 & \text{prob } 1-p, \end{cases}$

then Y_1, Y_2, Y_3 identical to Y

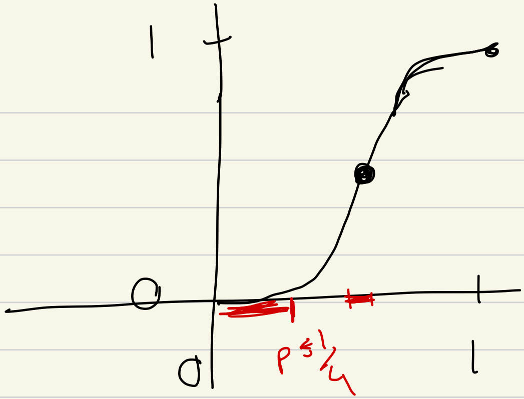
but chosen independently

$MAJ(Y_1, Y_2, Y_3) = 0$ prob

$$f(p) = p^3 + 3p^2(1-p)$$

and $= 1$ prob

$$3p(1-p)^2 + (1-p)^3$$



$f(1/2) = 1/2$

p

$$\boxed{f'(1/2) = 3/2}$$

$f(p)$, p small, $= 3p^2 + O(p^3)$

since $f(p) = 3p^2 - 2p^3$

(1) actually $f(p) \le 3p^2$.

Note:

near $p = 0$

$$f(p) \leq 3p^2$$

$$f(f(p)) \leq 3(3p^2)^2$$

$$= 3^3 p^4$$

$$f(f(f(p))) \leq 3(3^3 p^4)^2$$

$$= 3^7 p^8$$

So

$$(\underbrace{f \circ f \circ \dots \circ f}_{r})(p) \leq 3^{2^r - 1} p^{2^r}$$

$$= \frac{1}{3}(3p)^{2^r}$$

Claim: Let $p \le 1/4$

$$f^{\circ r}(p) \le \frac{1}{2} \frac{1}{2^n}$$

then this holds for $r \ge \log_2 n + \underbrace{O(1)}_{\text{absolute const}}$

Why?

$$\frac{1}{3}\left(3 \cdot \frac{1}{4}\right)^{2^r} \le \frac{1}{2} \frac{1}{2^n}$$

$$2^r \log_2 3/4 \le -n + O(1)$$

$\log_2$ again

$$r + \log_2 \log_2 3/4 \geq \log_2 n + O(1)$$

So

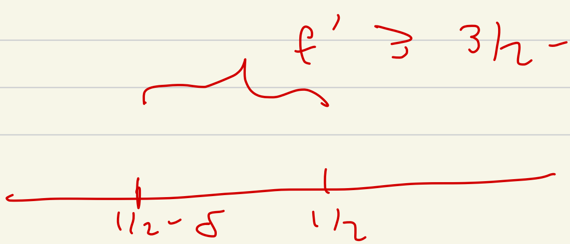
$$r \geq \log_2 n + O(1)$$

is sufficient.

Fix $\varepsilon > 0$, $f'(1/2) = 3/2$

$$f'(p) \geq 3/2 - \varepsilon \quad \text{for all}$$

$$p \geq 1/2 - \delta \quad \text{for some } \delta > 0.$$



So:

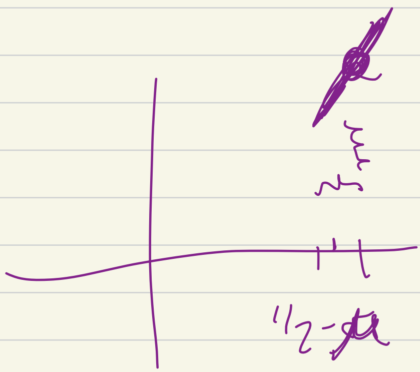
$$p_0 = \tfrac{1}{2} - \mu_1, \qquad \mu_1 = \frac{1}{2n}$$

then

$$f\left(\tfrac{1}{2} - \mu_1\right) = f\left(\tfrac{1}{2}\right) - \mu_1 f'(\xi)$$

where

$$\tfrac{1}{2} - \mu_1 \leq \xi \leq \tfrac{1}{2}$$



So

$$f\left(\tfrac{1}{2} - \mu_1\right) \leq f\left(\tfrac{1}{2}\right) - \mu_1\left(\tfrac{3}{2} - \varepsilon\right)$$

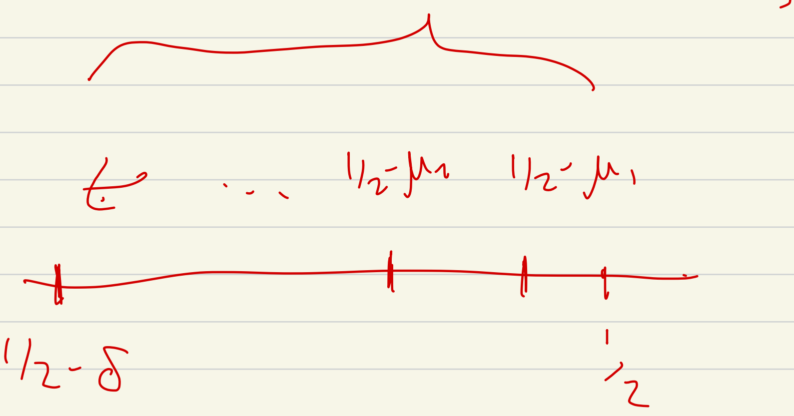
Similarly:

$$f \circ f\left(\tfrac{1}{2} - \mu_1\right) \leq$$

$$f\left(1/2 - \mu_1\left(3/2 - \varepsilon\right)\right)$$

$$\leq \underbrace{f(1/2)}_{1/2} - \mu_1\left(3/2 - \varepsilon\right)^2$$

$\longrightarrow f' \geq 3/2 - \varepsilon$



$\overbrace{\text{fc. of of}}^{r'}\left(\frac{1}{2} - \frac{1}{2n}\right)$

$$\leq \frac{1}{2} - \underbrace{\frac{1}{2n}\left(\frac{3}{2} - \varepsilon\right)^{r'}}$$

as long as $\quad \geq \delta$

we get this

$$\leq \frac{1}{2} - \delta$$

after at most r' iterations, where

$$\frac{1}{2n}\left(\frac{3}{2} - \varepsilon\right)^{r'} \geq \delta$$

$$\left(\frac{3}{2} - \varepsilon\right)^{r'} \geq 2\delta n$$

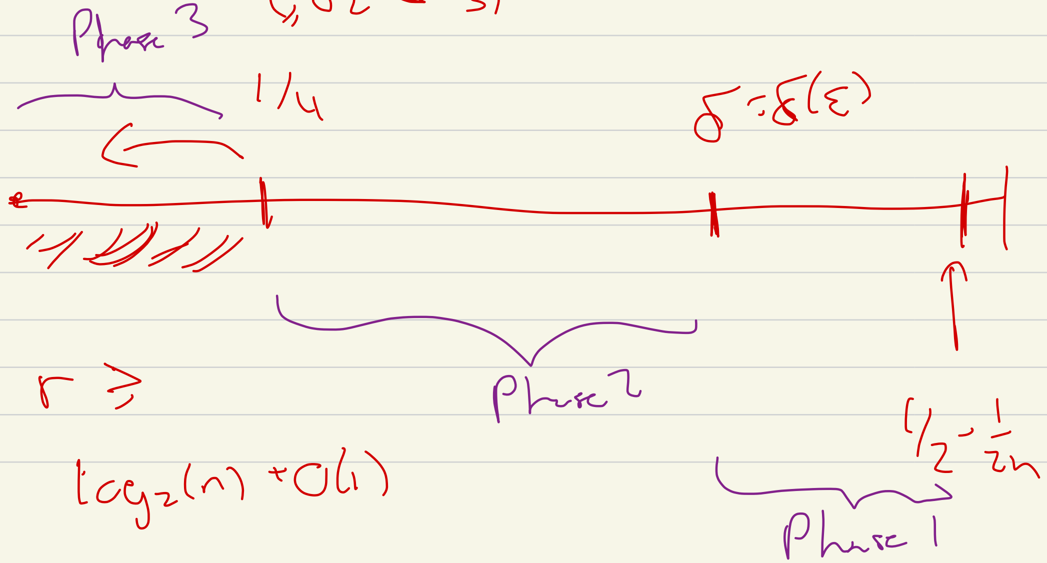
So

$$r' \log_2\left(\tfrac{3}{2} - \varepsilon\right) \geq \log_2(2\delta) + \log_2(n)$$

So

$$r' \geq \frac{\log_2(n)}{\log_2\left(\tfrac{3}{2} - \varepsilon\right)}$$

$(\delta_2 \leq 1/3)$



$r >$

$\log_2(n) + O(1)$

Phase 2:

$$\underbrace{f \circ \cdots \circ f \circ f}_{r''}\left(\frac{1}{2} - \delta\right) \leq \frac{1}{4} =: \delta_2$$

after $r'' = \text{Const} = \text{Const}(\delta, \varepsilon)$

number of iterations.

=

So after

$$\underbrace{\underbrace{r + r'}_{} + r''}_{} \text{ iterations of } f,$$

$$p \leq \frac{1}{2} - \frac{1}{2n}, \quad \overbrace{f \circ \cdots \circ f} \leq \frac{1}{2} \frac{1}{2^n}$$

with $r + r' + r'' =$

$$\log_2(n) + \frac{(\log_2 n)}{\log(\frac{3}{2}-\varepsilon)} + \underbrace{O(1)}_{\substack{\text{const} \\ \text{dep on} \\ \delta,\ \varepsilon,}}$$

$$\delta = \delta(\varepsilon)$$

So for any $\varepsilon > 0$, there is a const $C = C(\varepsilon)$ ($\to \infty$ as $\varepsilon \to 0$ ☹) s.t.

$$(\log_2 n)\left(1 + \frac{1}{\log(3/2 - \varepsilon)}\right) + C$$

iterations,

$$\frac{1}{2} - \frac{1}{2n} \longrightarrow \quad \frac{1}{2} \quad \frac{1}{2^n}$$

So there is

$$(\log_2 n)\left(1+\frac{1}{\log(3/2-\varepsilon)}\right)+O(1)$$

depth iterated MAJ

$$\begin{array}{ccc} & \mathrm{MAJ} & \\ \swarrow & \downarrow & \searrow \\ \mathrm{MAJ} & \mathrm{MAJ} & \mathrm{MAJ} \\ & \vdots & \end{array}$$

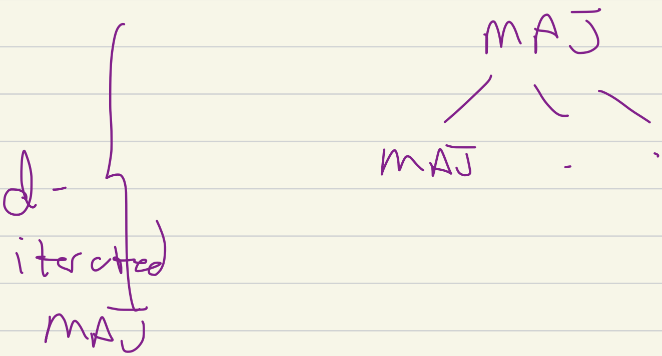
s.t. if $\mathrm{MAJ}_n(x_1, \dots, x_n) = 0$

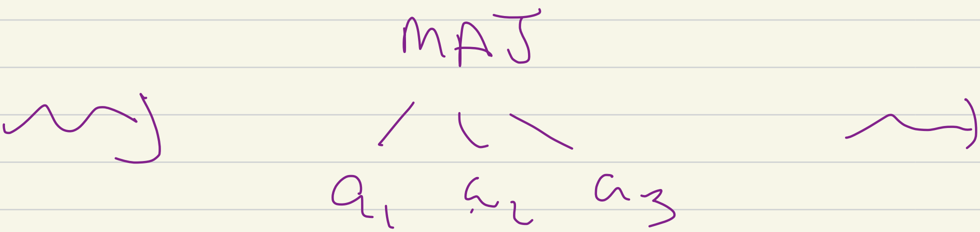
prob that above tree computes 1 instead of 0 has prob $\le 1 - \frac{1}{2}\frac{1}{2^n}$

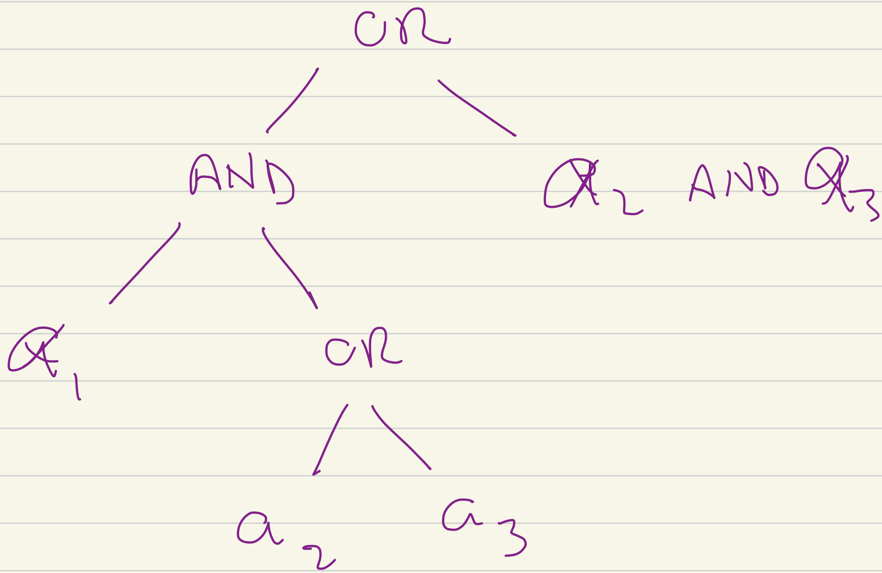
So

$MAJ(x_1, x_2, x_3)$:

$x_1 \wedge (x_2 \vee x_3)$ OR $(x_2 \wedge x_3)$

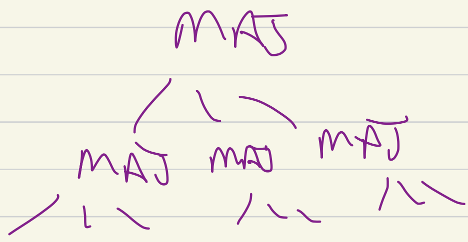






- formula $\wedge, \vee$ of size 5 for MAJ

- formula $\wedge, \vee$ of size 5^2 for



depth 2 maj

formula de Morgan $\wedge$, $\vee$

size 5^d

so $5^d = \left(2^{\log_2 5}\right)^d$

$= 2^{d \cdot \log_2 5}$

so $\left(\log_2(n) \cdot C_1 + C_2\right)$
≤ 2

$$C_1 = \left(\log_2 5\right)\left(1 + \frac{1}{\log(3/2 - \varepsilon)}\right)$$

$\simeq 6,19\ldots + \varepsilon'$

Such a formula, random leaves,
but makes a mistake on
a ~~fixed~~ $x_1, \ldots, x_n$ with prob

$$\leq \frac{1}{2} \frac{1}{2^n},$$

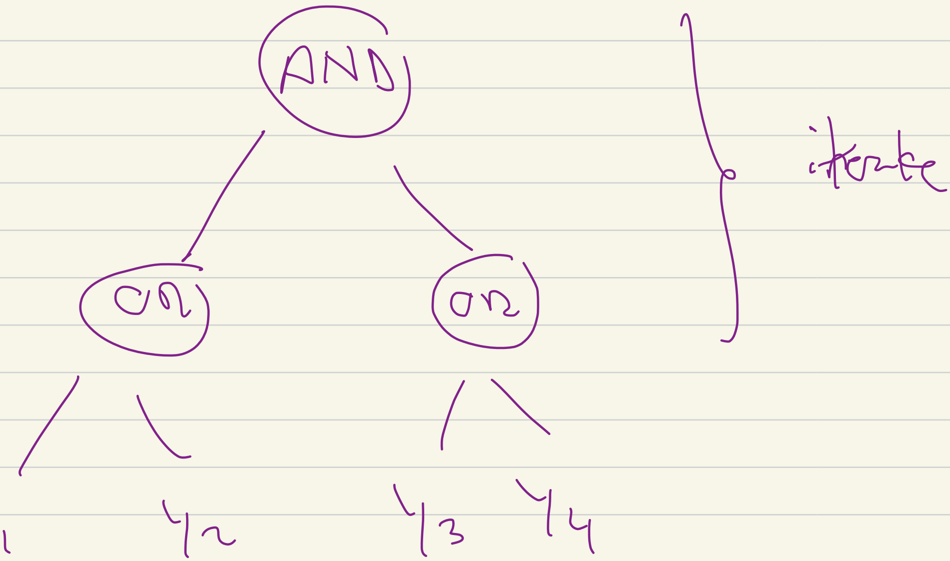
hence for any values of $x_1, \ldots, x_n$
(of which there are 2^n) with
prob $\leq \frac{1}{2}$.

Each additional iteration

$$\frac{1}{2^n} \rightarrow 3\left(\frac{1}{2^n}\right)^2 = 3 \cdot \frac{1}{4^n}$$

...

Rem: You can improve 6.16 to roughly 5.3 using



Algebraic Complexity!

Strassen, ... for matrix multiplication

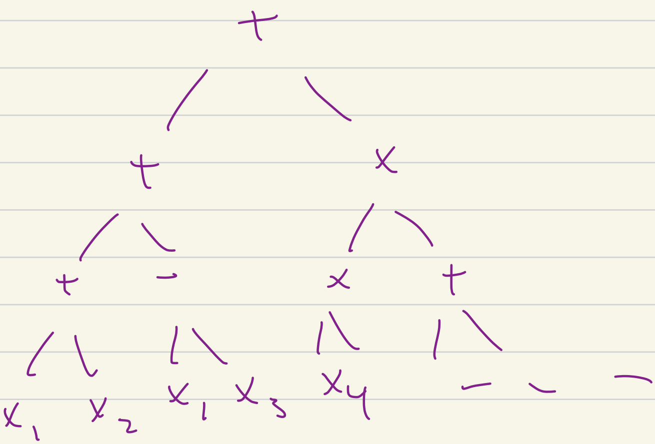
Algebraic setting:

"field of constants" $\mathbb{R}$, $\mathbb{C}$, ...

For us: $\mathbb{Z} = \{\ldots, -1, 0, 1, 2 \ldots\}$

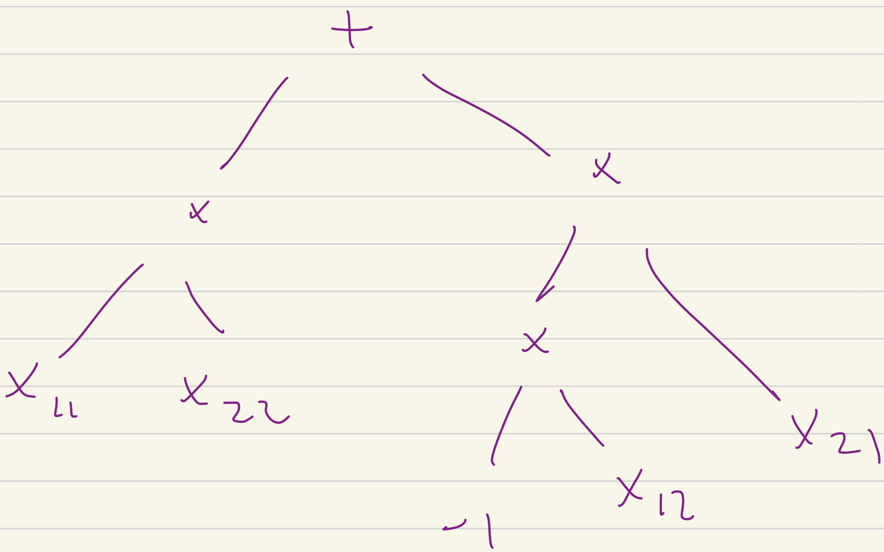
operations: $+$, $\times$

formula:



e.g. $X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$

$$\det(X) = x_{11} x_{22} + (-1)(x_{12})(x_{21})$$



rules: leaves are: variables
or integers

For complexity theory, there's a focus on Permanent:

$$\mathrm{Det}(X^{n\times n}) = \sum_{\sigma \in S_n} x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{n\sigma(n)} \cdot (-1)^{\mathrm{sign}(\sigma)}$$

$S_n = \{\text{bijections } \{1,\dots,n\} \to \{1,\dots,n\}\}$

Permanent: same w/o sign

E.g.,

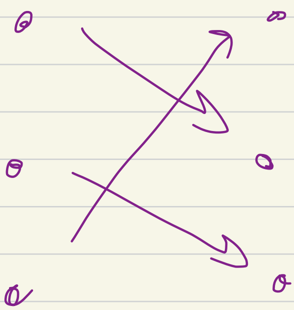
$$\mathrm{Perm}\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = x_{11}x_{22} + x_{12}x_{21}$$

Det/Perm 3×3

1

2

3



$1 = \sigma(3)$

$2 = \sigma(1)$

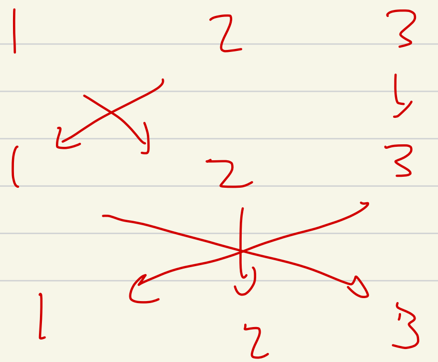
$3 = \sigma(2)$

$\sigma \in S_3$

We look at cyclic structure:

$$\begin{tikzcd}
\sigma(3) = 1 \arrow[rr] & & \sigma(1) = 2 \arrow[dl] \\
& 3 = \sigma(2) \arrow[ul] &
\end{tikzcd}$$

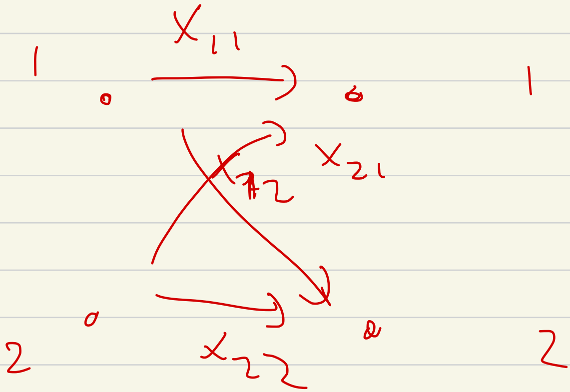
$$\operatorname{sign}(\sigma) = \#\text{ transpositions } (\text{mod } 2)$$



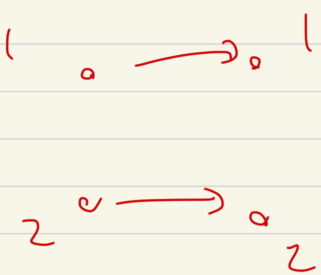
transp

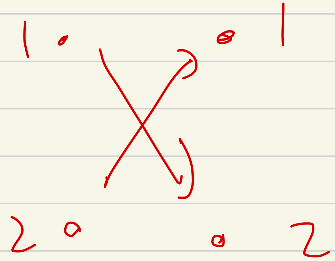
transp

Focus Perm(X)



$$\underbrace{x_{11}\, x_{22}}_{\text{perfect matching}} + x_{12}\, x_{21}$$

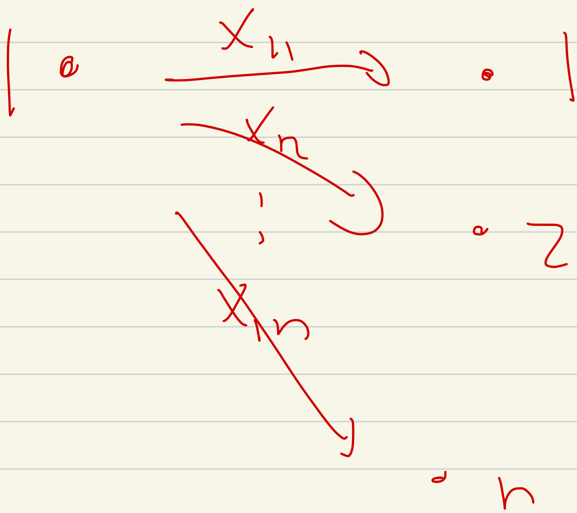




For us:

$$\mathrm{Perm}\left(X^{n \times n}\right)$$

count on a complete bipartite graph



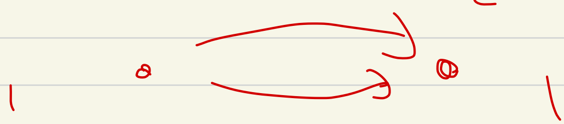
① count # perfect matchings in a bipartite graph where if each $X_{ij} = \begin{cases} 0 & \leftarrow \text{no edge} \\ 1 & \leftarrow \text{yes edge } i \to j \end{cases}$

then

$$\operatorname{Perm}(X^{n\times n}) = \#\text{ perfect matchings}$$

if $X_{11} = 2$

multiple edges



if $X_{ij} = 0, 1, 2, \ldots$

$=$

Otherwise

$\operatorname{Perm}(X^{n\times n}) =$ some polynomial in X_{ij}'s of degree n.

Next Time:

Valiant: 1979

The Complexity of Computing the Permanent:

Thm: If you can compute

$\mathrm{Perm}(X^{n\times n})$ in poly

time, with $X \in \{0,1\}^{n\times n}$

i.e. an $n \times n$ matrix $\begin{matrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \\ x_{n1} & \cdots & x_{nn} \end{matrix}$

where $x_{ij} = 0, 1$

then you have an algorithm

solves 3SAT, 3COLOUR, ...

in poly time!