Last Class.

- Gröbner Basis Computation & applications

Complexity of Gröb Basis:

Given polynomial system in 'n' variables, of max degree 'D', Gröb Basis takes at most

$$D^{2^n} \quad \text{steps.}$$

→ This is bad!
→ MANY optimizations exist.
→ Conferences & books are dedicated to this.

Question Why is $D^{2^n}$ bad?

doubly "exponential" in 'n'.

ASYMPTOTIC THINKING

CamScanner

Recall we said determinant takes

$\sim n!$ operations naively & $\sim n^3$ operations with Gauss. elim.

Why is $n^3$ better?

| | $n^3$ | $n!$ | $7n^2$ |
|---|---|---|---|
| $n=1$ | 1 | 1 ✓ | 7 |
| $n=2$ | 8 | 2 ✓ | 28 |
| $n=3$ | 27 | 6 ✓ | 63 |
| $n=4$ | 64 | 24 ✓ | 112 |
| $n=5$ | 125 | 120 ✓ | 175 |
| $n=6$ | ✓ 216 | 720 | 252 |
| $n=7$ | ✓ 343 | 5040 | 343 |
| $n=8$ | ✓ 512 | 40320 | 448 ✓✓ |
| $n=9$ | ✓ 729 | 362880 | 567 ✓✓ |
| $n=10$ | ✓ 1000 | 3628800 | 700 ✓✓ |
| $n=11$ | ✓ 1331 | 39916800 | 847 ✓✓ |

$7n^2$ better than $n^3$ only after $n=8$....

$7n^2$ better than $n!$ only after $n=6$...

You'll find similar behaviour even if you had $1000n^2$ ✱

$\Downarrow$

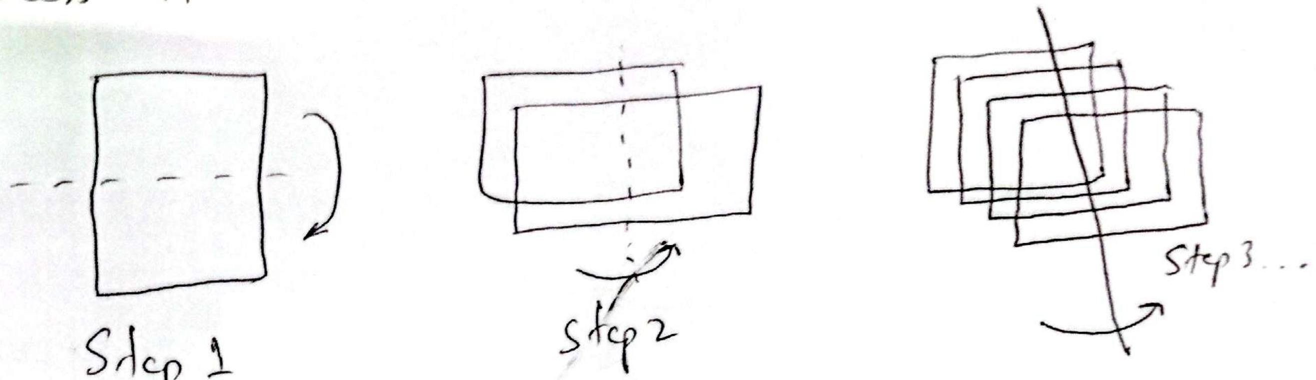
$n^3$ is better than $n!$ only after $n \geq 6$ to $\infty$

PREMISE OF ASYMPTOTICS

We care only about large values of '$n$'.

# Power of exponential.

## Process A




## Process B

10000 sheets of paper
Step 1

add 20000 sheets of paper
step 2.

add 30000 sheets of paper
step 3

| Height | Process A $\sim 2^n$ | Process B $\sim 5000n^2$ |
|---|---|---|
| toddler | 15 steps | 1 step |
| Big Ben | 21 steps | 14 steps |
| Moon. | 43 steps | 27727 steps |
| Sun | 52 steps | 547723 steps |

# Randomization

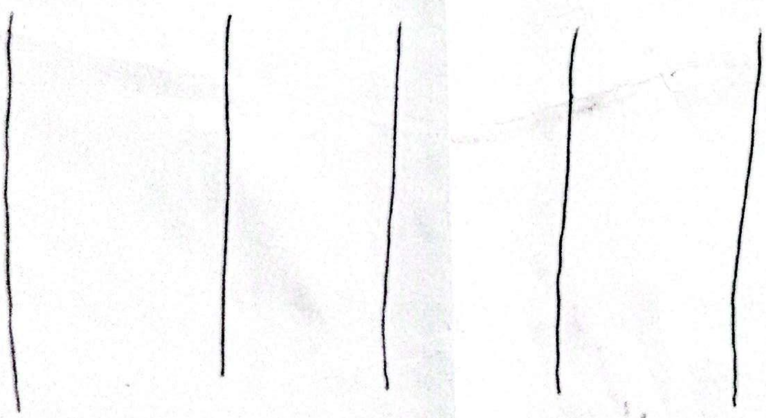
Randomization is very powerful - Used to speed up ~~to~~ Grob computations

We already saw use of randomness in Zero-Knowledge proofs

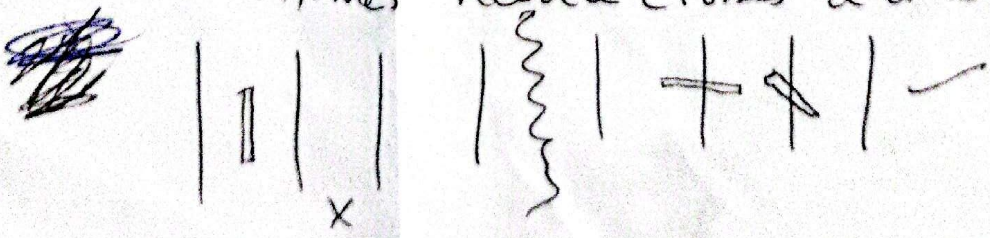
Here's another example.

BUFFON NEEDLE EXPERIMENT

1. Take a needle
2. Draw parallel lines needle length apart.



3. Randomly drop needle many times. Record no of times needle crosses a line



4. Compute $\dfrac{2 \times \text{no. of throws}}{\text{no. of times you had crossings}}$ ← Should $\sim \pi$

Quick sort:

Task given a list of numbers, sort it

Algorithm [Quicksort]

4, 3, 2, 9, 8, 5, -2, 5, 2, 8, 11

Step 1 Choose pivot.

$\boxed{4}$, 3, 2, 9, 8 . - -

Step2 Place pivot s.t everything to the left of the pivot is $\leq$ pivot & everything to the right $\geq$ pivot

3, 2, 2, 5, -2, $\boxed{4}$, 5, 8, 9, 8, 11

Step Recurse on left & right parts

CamScanner

Algorithm terminates quickly if
→ pivots are "balanced."

e.g. $\boxed{1}$ 2 3 4 5 6 7 . .

↗
Bad.

Worst Case

$n^2$ steps

→ With random shuffling, i.e.

Step 0 → randomly shuffle list.

Then average no. of steps of algorithm is at most

$$\sim n + n^{1.000001}$$

for shuffling

# Polynomial equality testing

## Question

$$(x+1)(x-2)(x+3)(x-4)(x+5)(x-6) \stackrel{?}{=} x^6 - 7x^3 + 25$$

## Algorithm 1

**Step 1** Reduce both sides to canonical form

e.g. $x^6 - 3x^5 - 41x^4 + 87x^3 + 400x^2 - 444x - 720$.

**Step 2** Compare coefficients.

requires $\sim D^2$ steps

## Algorithm 2

**Step 1** Choose random no. $\alpha$

**Step 2** evaluate both sides at $\alpha$.

Step 3 if equal, say "EQUAL"

" not , say "NOT EQUAL"

requires $\sim D$ steps.

CamScanner

e.g. Choose $x=0$

$LHS = 720$

$RHS = 25$

"NOT EQUAL"

e.g.

$(x^2-1)(x+2)(x^2+6x+9) + 14 \overset{?}{=}$ $x^5+18x^4+122x^3 + 38x^2+525x + 264$

try $x=-2$

$LHS = 14$

$RHS = 14$

"EQUAL" ← answer returned by Alg. 2

Sadly, $LHS = x^5+8x^4+20x^3+10x^2-21x-4$

$\Rightarrow$ Alg. 2 return wrong answer.

Suppose instead, we had chosen $x=1$.

$LHS = 14$
$RHS = 968$

$x = -2$ was just a bad choice

Algorithm2 modified

Try $m$ different times

Choose random. ~~[illegible]~~ no.

If LHS $\neq$ RHS

Say "NOT EQUAL

After '$m$' tries, if LHS = RHS all times,

Say "EQUAL"

→ no. of steps $\sim md$.

→ $md$ vs $d^2$

→ $md$ is ~~[illegible]~~ better when $m << d$...

~~If~~ $P(x)$ $Q(x)$

$$P(x) = Q(x) \Rightarrow P(x) - Q(x) = 0.$$

$$\Downarrow$$

$$H(x) = 0$$

~~'$d$' is a bad choice~~

☆ There are only '$d$' bad choices

Suppose you choose a no. at random from 1 to 100d.

$$\Pr[\text{bad choice}] = \frac{d}{100d} = \frac{1}{100}.$$

$$\Pr[\text{bad choice } m \text{ times}] = \left(\frac{1}{100}\right)^m$$

☆ $m = 3$ is good enough.

no. steps $\sim 3d$.

Prob. of err $< \frac{1}{1000000}$

We only did One variable.
with multiple variables, randomized algo is far better.

If you can show a non-randomized algo that's as good as randomized, you'd be solving a very important math problem.

<u>Homework</u> google P vs BPP.
(Similar to P vs NP)

# Convert words/ Sentences to numbers

Encoding func $\eta$:

e.g.

$\eta(a) = 0$

$\eta(b) = 1$

$\eta(c) = 2$

$\vdots$

$\eta(i) = 8$

encoding of

size of alphabet

$$abi = \eta(a) \times 9^0 + \eta(b) \times 9^1 + \eta(c) \times 9^2$$

$$= 0 + 9 + 2 \times 81$$

$$= 171$$

→ assign values randomly

## Decoding

Algo. Step 1:- Compute $n \% 9$ → store remainder

Step 2: $n \leftarrow \frac{(n - n\%9)}{9}$

Step 3: Repeat

e.g. given 244.

$244 \% 9 = 1 \xrightarrow{\eta^{-1}} b$

$(244-1)/9$

$= 27 \% 9 = 0 \xrightarrow{\eta^{-1}} a$

$27/9$

$= 3 \% 9 = 3 \xrightarrow{\eta^{-1}} d$

CS CamScanner

Given $(a_1, b_1)$, $(a_2, b_2)$, $(a_3, b_3)$

$f(a_1) = b_1$, $f(a_2) = b_2$, $f(a_3) = b_3$

find degree 2 poly thru these pts

$\boxed{\text{Lagrange Interpolation.}}$

$$\frac{(x-a_2)(x-a_3)}{(a_1-a_2)(a_1-a_3)} b_1 + \frac{(x-a_1)(x-a_3)}{(a_2-a_1)(a_2-a_3)} b_2$$

$$+ \frac{(x-a_1)(x-a_2)}{(a_3-a_1)(a_3-a_2)} b_3$$

Anything less than 3 pts gives infinite no. of possibilities

$\boxed{\text{Can be generalized}}$

CamScanner

You need $(n+1)$ pts to uniquely determine a degree
→ 'n' Polynomial.

→ Even with n pts, you have infinitely many possibilities

→ This and randomized polynomial equality testing is used in Cryptography

A remarkable application of randomness.

PCP Theorem → Any proof of a mathematical theorem can be written down such that a reviewer must be convinced by only looking at ~ 30 alphabets of the proof

CamScanner