CPSC 536F Feb 1, 2022

- Remarks on Andreev function and probabilistic method
- This week { Monotone formulas; Algebraic formulas }

On course website, there should be HW problems

Andreev's function: N, ℓ

consider all functions

$$\{0,1\}^N \to \{0,1\}$$

which we identify

$N = 2$

$$\{0,1\}^2 \to \{0,1\}$$

$\{0,1\}^2$

$$\left.\begin{matrix} 0\,0 \\ 0\,1 \\ 1\,0 \\ 1\,1 \end{matrix}\right\} \text{base } 2 \qquad \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix}$$

Identify

functions $\{0,1\}^N \to \{0,1\}$

with variables

$$x_0, \ldots, x_{2^N-1}$$

$$\vec{z}^1, \ldots, \vec{z}^\ell \in \{0,1\}^N$$

$$\text{Andreev}_{N,\ell}\left(f, \vec{z}^1, \ldots, \vec{z}^\ell\right)$$

$$\uparrow$$

$$x_0, \ldots, x_{2^N-1}$$

$$= f\left(\vec{z}^1 \oplus \ldots \oplus \vec{z}^\ell\right)$$

We know there exist f s.t.

$f(\vec{z})$ requires $\geq 2^N/\log N$

size formula

To use random restrictions on

$$\text{Andreev}_{N,\ell}\left(f, \vec{z}^1, \ldots, \vec{z}^\ell\right)$$

restricted $f \leftrightarrow x_0, \ldots, x_{2^N-1}$ to a hardest f to compute

random restrictions

Homework will give a proof that when you randomly restrict $\vec{z}^1, \ldots \vec{z}^\ell$

bits to describe f $= 2^N$

= # bits to describe $\vec{z}^{\,i}$ $= N\ell = \frac{n}{2}$

if you restrict ↓ randomly

from $\frac{n}{2} \to (\log n)^c$

then

$$\begin{matrix} \vec{z}^{\,1} & z^1_1 \cdots z^1_N \\ \vdots & \vdots \\ \vec{z}^{\,\ell} & z^\ell_1 \cdots z^\ell_N \end{matrix}$$

N columns, want

$$\Pr\left(\begin{array}{l}\text{Prob all } N \text{ columns still}\\ \text{has at least one rand}\\ \text{var}\end{array}\right) \geq \frac{1}{2}$$

suffices to show

$$\Pr\left(\begin{array}{l}\text{Prob a fixed colum}\\ \text{has all its rand}\\ \text{vars set to } 0/1\end{array}\right) \leq \frac{1}{2N}$$

"Union bound"

Union Bound: Consider any

{subsets / events} in a finite

probability space,

$E_1, \ldots, E_k$.

Then

$$\text{Prob}(E_1 \cup \ldots \cup E_k) \leq \text{Prob}(E_1) + \ldots + \text{Prob}(E_k)$$

(There are inclusion/exclusion principles)

e.g.

$$\text{Prob}(E_1 \cup \dots \cup E_k)$$

$$\geq \text{Prob}(E_1) + \dots + \text{Prob}(E_k)$$

$$- \text{Prob}(E_1 \cap E_2) - \text{Prob}(E_1 \cap E_3)$$

$$- \dots - \text{Prob}(E_{k-1} \cap E_k)$$

$$=$$

Talk about monotone formula + union bound.

—

Ultimately: Razborov's lower bound for circuit size for monotone formulas

A monotone formula is a formula on literals $x_1, \dots, x_n$ with only $\wedge$, $\vee$.

A monotone function on $x_1, \dots, x_n$ is

$$f : \{0,1\}^n \to \{0,1\}$$

s.t.

if $\vec{x} \leq \vec{y}$ then $f(\vec{x}) \leq f(\vec{y})$

where i.e.

$x_1 \leq y_1$ and $x_2 \leq y_2$ and ---

Eg, k-th Threshold function on n variables:

$$Th_k(x_1, \ldots, x_n) =$$

$$\begin{cases} 1 & \text{if } x_1 + \cdots + x_n \geq k \\ 0 & \text{if } x_1 + \cdots + x_n \leq k-1 \end{cases}$$

$$\text{Majority}(x_1, \ldots, x_n) = Th_{\lceil \frac{n}{2} \rceil}(x_1, \ldots, x_n)$$

e.g.

$$Th_1(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if some } x_i = 1 \\ 0 & \text{if } x_1 = \ldots = x_n = 0 \end{cases}$$

$$= x_1 \text{ OR } x_2 \text{ OR } \ldots \text{ OR } x_n$$

$=$

$$Th_2(x_1, \ldots, x_n)$$

$$= (x_1 \text{ AND } x_2) \text{ OR } (x_1 \text{ AND } x_3)$$

$$\text{OR } \ldots \text{ OR } (x_{n-1} \text{ AND } x_n)$$

$=$

$$Th_3(x_1, \ldots, x_n) = \bigvee_{i_1 < i_2 < i_3} (x_{i_1} \text{ AND } x_{i_2} \text{ AND } x_{i_3})$$

So: for $Th_k(x_1, \ldots, x_n)$

there is a formula with

$x_1, \ldots, x_n$, $\wedge$, $\vee$

$$\bigvee_{i_1 < \ldots < i_k} (x_{i_1} \wedge \ldots \wedge x_{i_k})$$

size $\binom{n}{k} \cdot k$

$k = 2$: $O(n^2)$

$k = 3$: $O(n^3)$

fixed k : $O(n^k)$

HW: There exist formulas size $2^n \cdot n$ for any monotone function on n vars.

HW: Most monotone functions require at ~~least~~ size $2^n \cdot \frac{1}{\sqrt{n}}$ + small factors.

How many monotone functions $\{0,1\}^n \to \{0,1\}$??

functions

$$\underbrace{\{0,1\}^n}_{2^n \text{ values}} \to \{0,1\} \Rightarrow 2^{2^n}$$

Remark: Consider all monotone functions $f: \{0,1\}^n \to \{0,1\}$

n even, s.t.

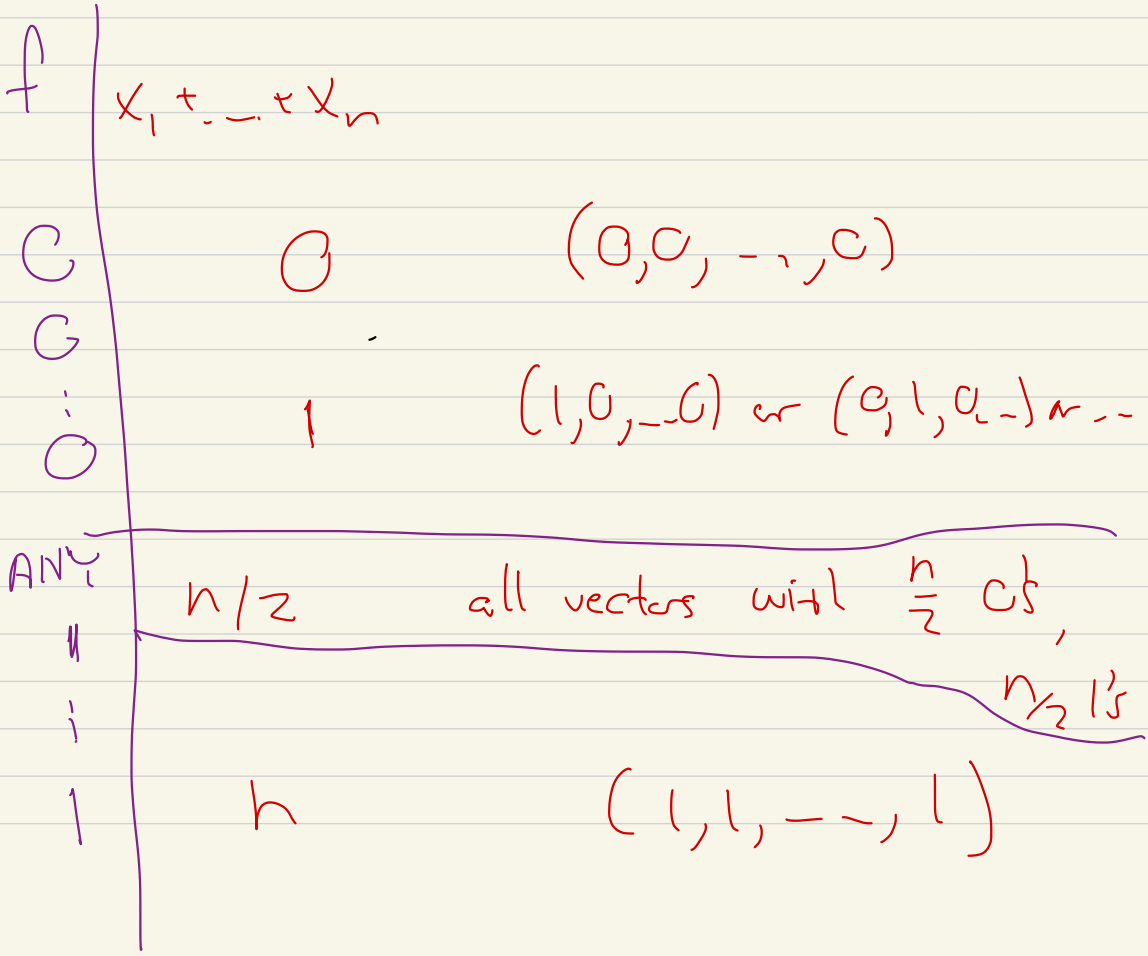
$$f(x_1, \dots, x_n)$$

(1) is 0 for $x_1 + \dots + x_n \leq \frac{n}{2} - 1$

(2) is 1 for $x_1 + \cdots + x_n \geq \frac{n}{2} + 1$

(3) is either

0, 1 for $x_1 + \cdots + x_n = \frac{n}{2}$



So such f are determined by

$$f(x_1, \ldots x_n)$$

$$\text{s.t.} \quad x_1 + \ldots + x_n = \frac{n}{2}$$

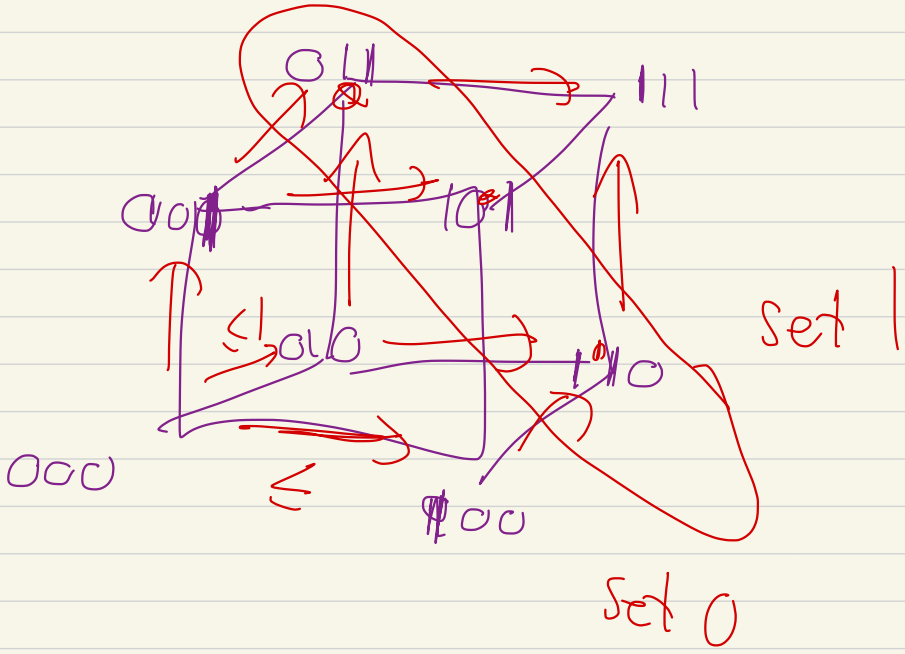
Claim: Have $\binom{n}{n/2}$ vectors of $\frac{n}{2}$ 0's, $\frac{n}{2}$ 1's. And any way of setting $\binom{n}{n/2}$ vectors to 0/1 gives a unique monotone function.

Hence

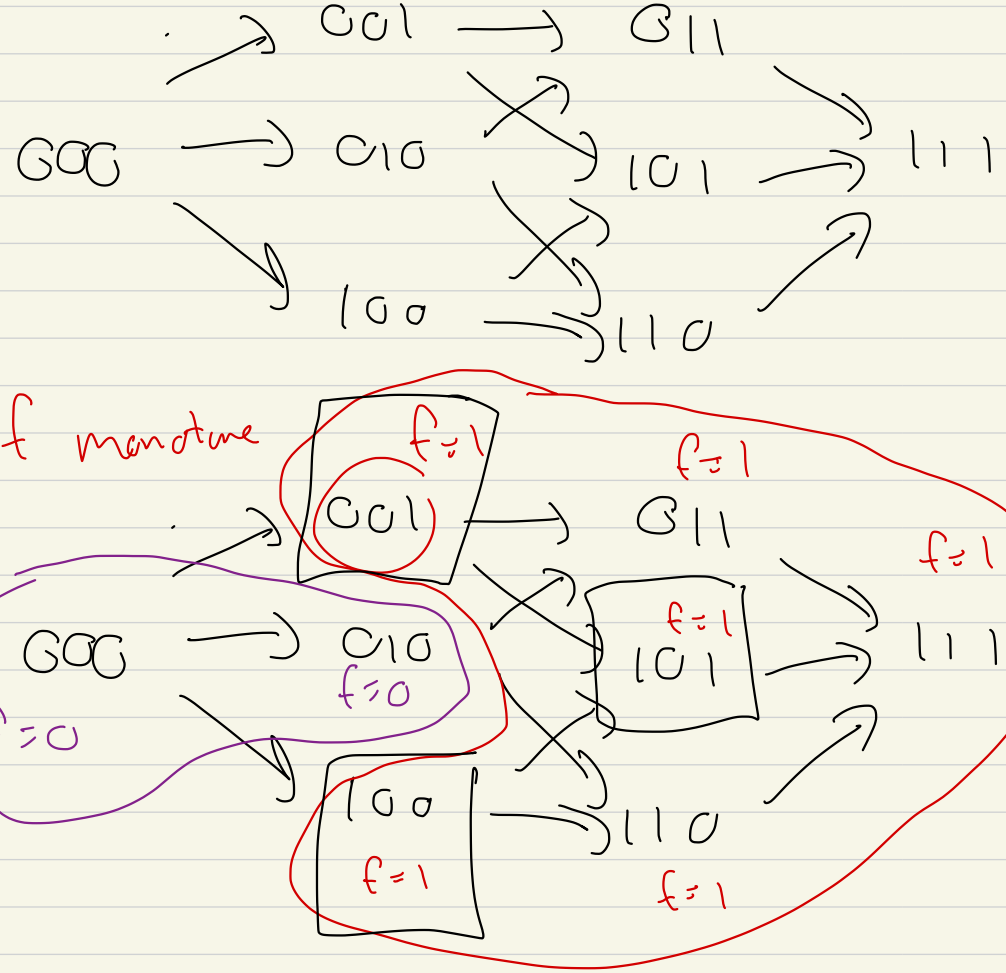
monotone functions $\geq 2^{\binom{n}{n/2}}$

$=$

poset = partially ordered set



$\rightarrow$ means $\leq$



For us:

$$\binom{n}{n/2} \approx 2^n \frac{c}{\sqrt{n}}$$

So # monotone formulas

$$2^{\left(2^n c/\sqrt{n}\right)}$$

So most monotone functions

circuit size $\rightarrow 2^n / n^{3/2}$

formula size

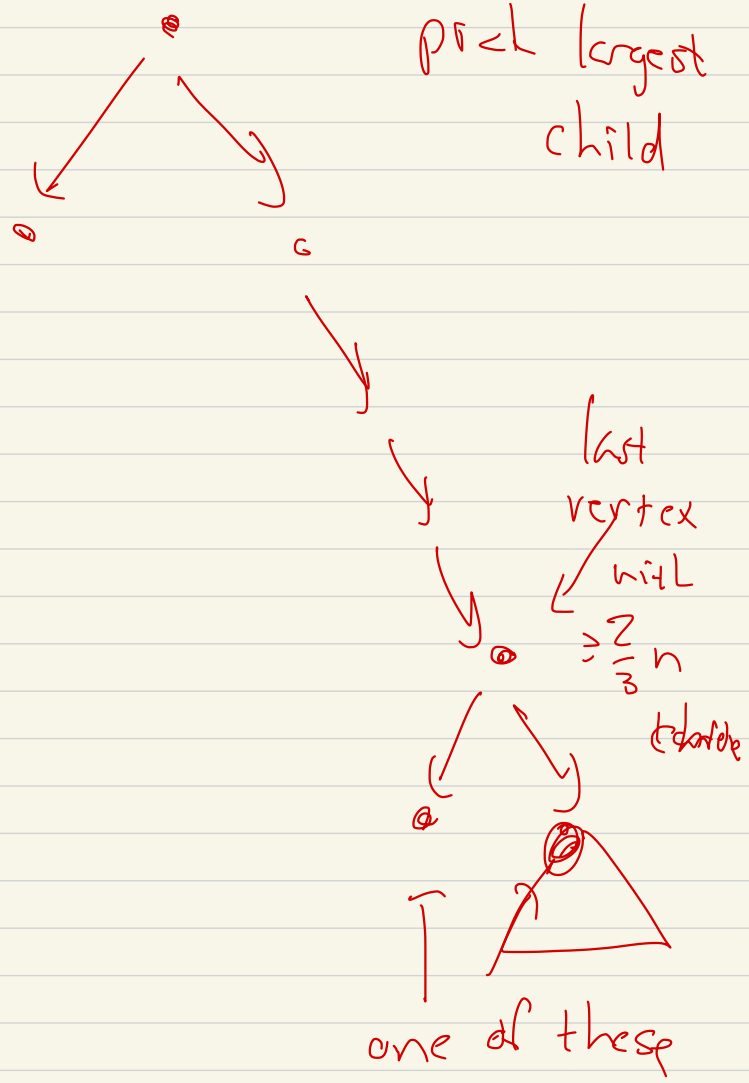
Claim (: Homework) :

Spira's lemma holds for monotone formula.

So $D(n)$ = max depth of a formula to express a monotone formula size n,

$$D(n) \leq 2 + D\left(\frac{2}{3}n\right)$$

formula tree



has $\geq \frac{n}{3}$ children

at most $2n/3$ "

Probabilistic Method!

Thm: For any fixed k, there is a formula for $Th_k(x_1, \ldots, x_n)$ of size $O_k(n \log n)$.

Thm! There is a poly size formula for $Majority(x_1, \ldots, x_n)$

Eg.

$Th_1(x_1, \ldots, x_n)$

$= x_1$ OR $\ldots$ OR x_n

$Th_2(x_1, \ldots, x_n) = \bigvee_{i_1 < i_2} (x_{i_1} \text{ AND } x_{i_2})$

$\binom{n}{2} \cdot 2$ size

$\Rightarrow$ get $O(n \log n)$

After break $Th_2(x_1, \ldots, x_n)$

$Th_3(x_1 \ldots x_n)$

Break
10:20 — 10:25

Remark: As far as I know, classes to held in-person starting next week.

Rule: divide & conquer

$Th_2(x_1, \dots x_n)$

/ or

$Th_2(x_1, \dots, x_{\frac{n}{2}})$ $Th_2(x_{\frac{n}{2}+1}, \dots, x_n)$

or

$Th_1(x_1, \dots x_{n/2})$ and $Th_1(x_{\frac{n}{2}+1}, \dots)$

$$Size(n) = 2\,Size\left(\frac{n}{2}\right) + n$$

$$= 2\left(2\,Size\left(\frac{n}{4}\right) + \frac{n}{2}\right) + n$$

$$= 4\,Size\left(\frac{n}{4}\right) + 2n$$

$$= 8\,Size\left(\frac{n}{8}\right) + 3n$$

$$\vdots$$

$$= 2^k\,Size\left(\frac{n}{2^k}\right) + kn$$

$k = \log_2 n$

$$\longrightarrow \quad n(\log_2 n)$$

Th_3!

$x_1 - - x_{\frac{n}{2}}$ $x_{\frac{n}{2}+1} - - x_n$

at least 3

OR

at least 3

OR

Th_2 and Th_1

OR

Th_1 and Th_2

$Size_3(n) = 2\,Size_3(n) + n \log n$

Rem:

$Th_k(x_1 \ldots x_n)$ this divide

& conquer roughly $n(\log n)^{k-1}$

fixed k.

$Th_{n/2} \rightsquigarrow$ large.

Th_3 in $O(n \log n)$

$Th_{n/2}$ or Maj $O(n^c)$

$0, \ldots, n-1 \qquad n = 2^N$

$\downarrow$

$\underbrace{00\ldots0}_{N} \; - - \; \underbrace{1111}_{N}$

$X_i \longleftrightarrow$ base 2 rep i

only $0 \leq i < j \leq 2^N - 1$

differ on one of their N bits.

Idea

$X_0, \ldots X_7$

X_i X_j

1st bit = 0 | 1st bit = 1

$X_0\ X_2\ X_4\ X_6$ | $X_1\ X_3\ X_5\ X_7$

$(X_0$ OR X_2 OR X_4 OR $X_6)$ AND (OR)

$= (X_0$ AND $X_1)$ OR $(X_2$ AND $X_1) \ldots$

— —

Claim!

$Th_2(x_0, \ldots x_7)$

$= (x_0\ x_2\ x_4\ x_6)$ AND $(x_1 \ldots, x_7)$

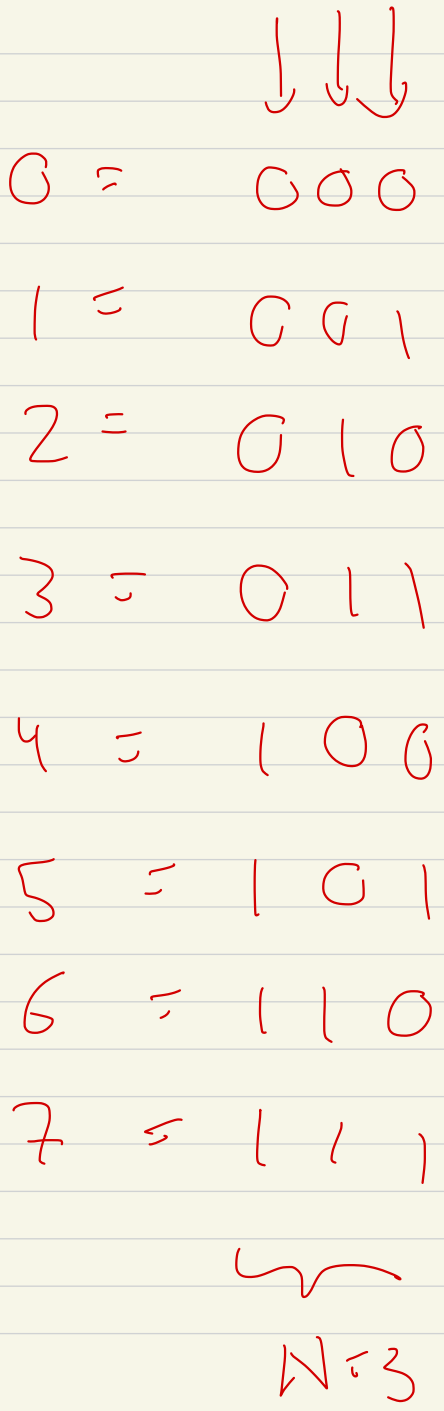
$\nearrow$ OR

OR formula x_i has 0 in 2nd bit
x_j has 1 in 2nd bit

OR

formula — — — 3rd bit
— — 3rd bit

gives $O(n \log n)$


0 = 000
1 = 001
2 = 010
3 = 011
4 = 100
5 = 101
6 = 110
7 = 111
N=3

Claim: You can partition

$\{1, \ldots, n\}$

into I_1, J_1, K_1

I_2, J_2, K_2

$\vdots$

$I_{O(\log n)}$ $J_{O(\log n)}$ $K_{O(\log n)}$

s.t. a, b, c distinct in $\{1, \ldots, n\}$

some I_r, J_r, K_r has

a, b, c falling into distinct I_r, J_r, K_r

Claim: fix $a, b, c \in \{1, \dots, n\}$ distinct. Randomly choose ℓ partitions (I_r, J_r, K_r) $r = 1, \dots, \ell$.

If $r = O(\log n)$, prob (a, b, c) do not fall into sep parts I_r, J_r, K_r

has prob $\leq \frac{1}{n^3}$.

=

Randomly choose partition

1 ⇉ put into I_r prob 1/3
- - J_r 1/3
- - K_r 1/3

1, a, b, c ... n

↳ ↳ ↳ into I_r
J_r prob 1/3
K_r

Claim: For fixed r,

Prob that a, b, c don't go into separate I_r, J_r, K_r is $\leq \frac{7}{9}$

$a \rightrightarrows I_r$, J_r, K_r goes somewhere

Say $a \to I_r$. $b \to I_r$ prob $\frac{1}{3}$; $\to J_r, K_r$ prob $\frac{2}{3}$

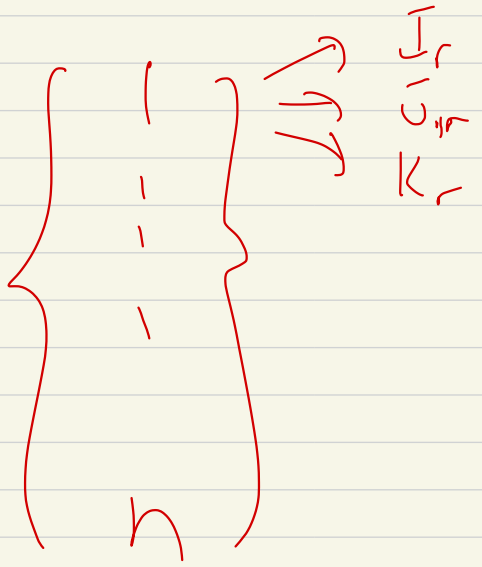
a, b distinct parts I_r J_r K_r

then c goes into last empty part

Prob $\frac{1}{3}$

So

a,
b,
c



Prob a, b, c "seperated" by I_r, J_r, K_r

$$= \frac{2}{q}$$

$$\Rightarrow \text{Prob}\left(\begin{array}{l}\text{we fail to separate} \\ a, b, c\end{array}\right) = \frac{2}{q}$$

Running ℓ independent experiments

$$\begin{array}{cccc} I_1 & & & I_\ell \\ J_1 & & & J_\ell \\ K_1 & - & - & K_\ell \end{array}$$

$$\text{Prob } a, b, c \text{ never separated} \leq \left(\frac{2}{q}\right)^{\ell}$$

Claim: $\ell = O(\log n)$

$$\left(\frac{7}{9}\right)^{\ell} \leq \frac{1}{n^3}$$

a, b, c distinct $\binom{n}{3} < \frac{1}{n^3}$

for large n.

Hence union prob < 1

that we fail to separate

a, b, c.

Class ends