Lecture 10 : PROBABILISTIC METHOD

A method to show the existence of a prescribed kind of mathematical object / structure. It works by showing that if one randomly chooses objects from a specified ensemble, the probability that the result is of prescribed kind is strictly greater than 0.

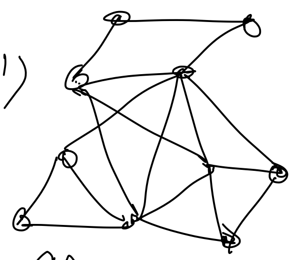
So such an object must exist.

- Even though we use probability, we conclude with certainty that an object with prescribed property exists.
- Often a non-constructive method.
- Used all over the place in mathematics & computer science
- Alon & Spencer, The Probabilistic Method, is a classic textbook

---

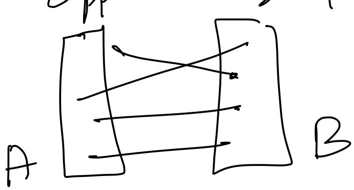
Theorem. Given any graph $G = (V, E)$, it has a bipartite subgraph with at least half the edges.

$H = (V, E')$



$$|E'| \geq \frac{|E|}{2}.$$

Pf. (You might have seen this as an approx algo for Maximum Cut problem)



$V = A \cup B$

disjoint union

$\geq 1/2$ edges go across the cut $[A : B]$

For each $v \in V$, place $v \in A$ uniformly
or $v \in B$ at random

For $e = (u,v)$ $\quad \Pr[e \text{ is cut}] = \frac{2}{4} = \frac{1}{2}$.

$\mathbb{1}_e$ = Indicator random variable for
event that edge e is cut.

$\mathbb{E}[\mathbb{1}_e] = \Pr[e \text{ is cut}] = \frac{1}{2}$

expectation

N = # edges cut by the process $= \sum_{e \in E} \mathbb{1}_e$

$$\mathbb{E}[N] = \mathbb{E}\Big[\sum_{e \in E} \mathbb{1}_e\Big]$$

$$= \sum_{e \in E} \mathbb{E}[\mathbb{1}_e] = \sum_{e \in E} \frac{1}{2} = \frac{|E|}{2}.$$

Random process gives a cut that in expectation
(aka on average) cuts 1/2 the edges

"Not everyone can be strictly below the average"

$\Rightarrow \exists$ cut $[A:B]$ s.t. $\geq \frac{|E|}{2}$ edges
cross it.

This "gives" the desired bipartite subgraph.
with $\geq \frac{|E|}{2}$ edges.

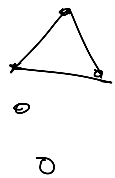
$\boxed{\text{Above is a randomized Factor } 1/2 \text{ approximation algo for Max-Cut}}$

For longest time, this was the best known approx. algorithm!

- In 1994, Goemans-Williamson gave an algo, based on <u>semidefinite</u> programming, that guaranteed a 87.8% approximation.
- This is believed to be best possible, thanks to some <u>PCP theory</u>.

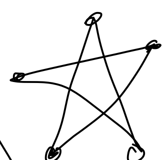
<u>Ramsey graphs</u>.

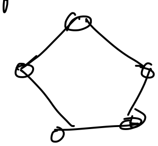
In any graph on n (big enough) vertices, there must be a triangle (K_3) or an indep. set of size 3.



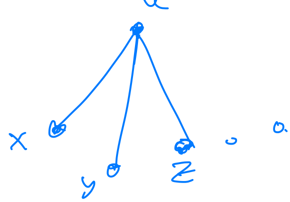
In fact $n=6$ suffices.

OTOH, for $n=5$, here's a graph with no K_3 or $\overline{K_3}$ (complement of K_3) (no clique or ind. set of 3 vertices)





<u>Pf idea</u>:



Let's say u has ≥ 3 nbrs.

Either x, y, z is an indep. set
or u and 2 of them form a triangle.

Definition : Let $k \in \mathbb{N}$.
The k^{th} Ramsey number, denoted $R(k)$
is the minimum n such that every
n-vertex graph has either a k-clique
or an indep. set of size k.

(Above : $R(3) = 6$)
$R(k)$ exists for every k, in fact

$$R(k) \leq \binom{2k-2}{k-1} \leq O\left(\frac{4^k}{\sqrt{k}}\right)$$

(proof by induction)

- $R(4) = 18$. (known)
- $R(5)$ is not known!

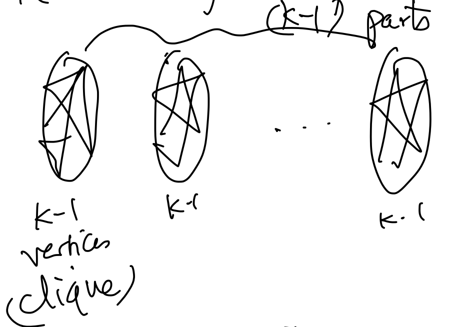
$$R(5) \in [43, 48]$$

($R(10) \in [798, 23556]$ → huge gap)

Lower bounds on $R(k)$

$R(k) > m \iff$ Existence of a graph on m vertices with no k-clique or k-indep set.

How might you construct such a graph?



Disjoint union of $(k-1)$ cliques of size $(k-1)$

Proves $R(k) \geq \Omega(k^2)$

For a while it was conjectured that $R(k) \leq O(k^2)$

Erdős (1947) $R(k) \geq \Omega(k \cdot 2^{k/2})$

($\exists$ gh on n vertices with no clique or indep set of $\approx 2 \log n$ vertices)

How to construct such a graph?

Answer: No one knows!

But Erdős showed they exist, in fact in abundance.

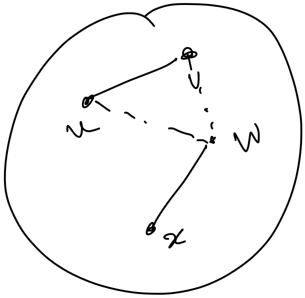
Proof: (Birth of the probabilistic method)

(alongside [Shannon 1948] proved existence of good error correction schemes)

Let's prove $R(k) > 2^{k/2}$ (for simplicity)

(define $n = 2^{k/2}$)

PICK A <u>RANDOM GRAPH</u> ON n vertices.



n vertices

For each pair $\{u, v\}$, include an edge between them with probability $1/2$. (independently for each pair)

Each possible (labeled) graph is sampled with probability $\frac{1}{2^{\binom{n}{2}}}$

Let's count the number of subsets that induce a k-clique or k-ind. set. ("bad")

$G = (V, E)$ — realization of random gh.

Fix $S \subseteq V$, $|S| = k$

$X_S = X_S(G) =$ indicator r.v that S is "bad" i.e S induces a k-clique or k-ind-set.

$$N = N(G) := \sum_{\substack{S \subseteq V \\ |S| = k}} X_S$$

N = # bad subsets that violate the desired Ramsey property.

(Would like $N = 0$)

If we prove $\mathbb{E}[N] < 1$, then that would mean, $\exists\, G$ s.t. $N(G) = 0$

("Not everybody can be strictly above average")

Such a G would be desired Ramsey graph.

$$\mathbb{E}[N] = \mathbb{E}\left[\sum_{S} X_S\right]$$

(Linearity of Expectation) $$= \sum_{\substack{S \subseteq V \\ |S| = k}} \mathbb{E}[X_S]$$

$$= \sum_{\substack{S \subseteq V \\ |S| = k}} \Pr[S \text{ induces a } k\text{-clique or a } k\text{-indep-set}]$$

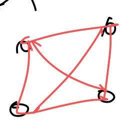
??

$$\Pr[S \text{ induces a } k\text{-clique}] + \Pr[S \text{ induces a } k\text{-ind set}]$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$\frac{1}{2^{\binom{k}{2}}} + \frac{1}{2^{\binom{k}{2}}}$$

$k=4$



$$= 2^{1-\binom{k}{2}}$$

$$\mathbb{E}[N] = \binom{n}{k} 2^{1-\binom{k}{2}}$$

$$\leq \frac{n^k}{k!} 2^{1-\frac{k(k-1)}{2}}$$

Recall $\underline{n = 2^{k/2}}$

$$= \frac{\cancel{2^{\frac{k^2}{2}}}}{k!} \cdot 2^{1 - \cancel{\frac{k^2}{2}} + \frac{k}{2}}$$

$$= \frac{2^{k/2+1}}{k!} < 1 \text{ (for } k \geq 4)$$

(infact ≈ 0 ~~ifor~~ for large k)

Want ~~obje~~ graph with $N=0$

$$\Pr[N>0] = \Pr[N \geq 1] \leq \mathbb{E}[N]$$

(Markov's inequality)

$\approx 0 \ll 1$

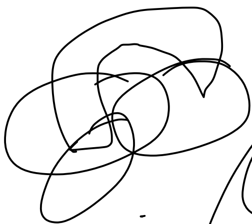
$$\Pr[N=0] > 0 \text{ (and infact } \approx 1)$$

- Lots of recent work on explicit constructions of Ramsey graphs
- Randomness extraction.

Prob. method useful to not only show existence of objects, but also to rule out certain objects (eg. in extremal combinatorics)

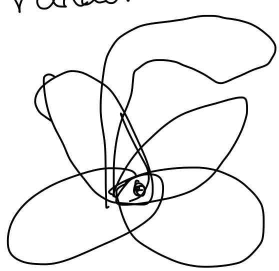
Erdös-Ko-Rado Theorem

Let $\mathcal{F}$ be a family of k-element subsets of a universe of size n. ($n \geq 2k$). Suppose every pair of sets $A, B \in \mathcal{F}$ have non-empty intersection.



Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$

(There's a very slick proof of this using prob. method, via random orderings).



$\binom{n-1}{k-1} = \#$ subsets of size k that contains a specific element.