Math 554

Hemanshu Kaul

kaul@iit.edu

The first known application of probabilistic method

Szele 1943 $\exists$ tournament on n vertices with at least $n!\,2^{-(n-1)}$ Hamiltonian paths.

→ Directed K_n

↳ path of length n

e.g.  

Proof "Create a random tournament" Exercise. ∎

- Szele conjectured max # Hamiltonian paths in a tournament on n vertices is $n!/(2-o(1))^n$
- Proved by Alon (1990) using Minc–Bregman theorem on permanents (which we will see later while studying Entropy)

Turán's Theorem answers the question

What is the maximum number of edges in an n-vertex K_k-free graph?

In the complementary form cliques change to independent sets

So, we are asking this question about graphs without large independent sets.

Caro (1979) & Wei (1981) showed that a graph with small degrees must contain large independent sets.

This result can be used to give a proof of Turán's Theorem.

independence #

Thm (Caro, Wei) For every graph G, $\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1}$

$d(v)$ = degree of v

clique #

Cor $\omega(G) \geq \sum_{v \in V(G)} \frac{1}{?}$

independence #

Thm (Caro, Wei) For every graph G, $\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1}$

$d(v)$ = degree of v

clique #

Cor $\omega(G) \geq \sum_{v \in V(G)} \frac{1}{n-d(v)}$

Cor [Turán's Thm, weaker form]
Every n-vertex K_{r+1}-free graph has at most $\left(1-\frac{1}{r}\right)\frac{n^2}{2}$ edges

Pf Fill in the details

$$r \geq \omega(G) \geq \sum_{v \in V(G)} \frac{1}{n-d(v)}$$

$$\geq \; ? \qquad \text{Think!}$$

$$= n/\left(n-\frac{2m}{n}\right), \text{ where } m = \#\text{edges}$$

Rearrange to get the needed inequality $m \leq \left(1-\frac{1}{r}\right)\frac{n^2}{2}$ ∎

Thm (Caro, Wei) For every graph G, $\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1}$

Proof

* Consider a random permutation of the vertices.
* Let I = set of vertices that appear before all its neighbors.

Thm (Caro, Wei) For every graph G, $\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1}$

Proof

* Consider a random permutation of the vertices.
* Let I = set of vertices that appear before all its neighbors.

I is an independent set.

For each v, $\mathbb{P}[v \in I] = \frac{1}{1+d(v)}$ (v appears first among $\{v\} \cup N(v)$)

$\therefore \ \mathbb{E}[|I|] = \mathbb{E}\left[\sum_{v \in V(G)} I_v\right] = \sum_{v \in V(G)} \mathbb{E}[I_v] = \sum_{v \in V(G)} \mathbb{P}[v \in I] = \sum_{v \in V(G)} \frac{1}{1+d(v)}$

$I_v = \begin{cases} 1 & \text{if } v \in I \\ 0 & \text{if } v \notin I \end{cases}$

$\blacksquare$

Ques ① Is this bound sharp?

② [DeRandomization] Can you give a deterministic algorithm that gives an independent set of this size?

In a graph $G=(V,E)$, $U \subseteq V$ is <u>dominating</u> if every vertex in $V \setminus U$ has a neighbor in U.

What is the minimum size of a dominating set?

In a graph $G=(V,E)$, $U \subseteq V$ is dominating if every vertex in $V \setminus U$ has a neighbor in U.

What is the minimum size of a dominating set?

Thm (Alon 1990) Let G be n-vertex with $\delta(G) = d > 1$. Then G has a dominating set with atmost $\left(\frac{\log(d+1)+1}{d+1}\right)n$ vertices.

Greedy algo?

In a graph $G=(V,E)$, $U \subseteq V$ is <u>dominating</u> if every vertex in $V \setminus U$ has a neighbor in U.

What is the minimum size of a dominating set?

<u>Thm (Alon 1990)</u> Let G be n-vertex with $\delta(G) = d > 1$. Then G has a dominating set with atmost $\left(\frac{\log(d+1)+1}{d+1}\right)n$ vertices.

<u>Proof</u> ① choose a random set ② Add vertices to it to ensure domination

Let $p \in [0,1]$ (to be decided later)

Let $S \subseteq V(G)$ be chosen randomly: each vertex chosen ind. w. prob. p.

In a graph $G=(V,E)$, $U \subseteq V$ is dominating if every vertex in $V \setminus U$ has a neighbor in U.

What is the minimum size of a dominating set?

Thm (Alon 1990) Let G be n-vertex with $\delta(G) = d > 1$. Then G has a dominating set with atmost $\left(\frac{\log(d+1)+1}{d+1}\right)n$ vertices.

Proof ① Choose a random set ② Add vertices to it to ensure domination

Let $p \in [0,1]$ (to be decided later)

Let $S \subseteq V(G)$ be chosen randomly: each vertex chosen ind. w. prob. p.

Let $T \subseteq V(G) \setminus S$ be the set of all vertices with no neighbors in S.

Then $S \cup T$ is a dominating set.

In a graph $G=(V,E)$, $U \subseteq V$ is dominating if every vertex in $V \setminus U$ has a neighbor in U.

What is the minimum size of a dominating set?

Thm (Alon 1990) Let G be n-vertex with $\delta(G)=d>1$. Then G has a dominating set with atmost $\left(\frac{\log(d+1)+1}{d+1}\right)n$ vertices.

Proof Let $p \in [0,1]$.
Let S = random subset of $V(G)$ with each vertex chosen ind. with prob. p.
Let $T = V(G) \setminus (S \cup N(S))$. $\therefore$ $S \cup T$ is dominating.

$$\begin{aligned}\mathbb{E}[|S \cup T|] &= \mathbb{E}[|S|+|T|] = \mathbb{E}[|S|] + \mathbb{E}[|T|] \\ &= \sum_v \mathbb{P}[v \in S] + \sum_v \mathbb{P}[v \in T] \\ &\le np + n(1-p)^{d+1} \quad \leftarrow \text{why?}\end{aligned}$$

In a graph $G=(V,E)$, $U \subseteq V$ is <u>dominating</u> if every vertex in $V \setminus U$ has a neighbor in U.

What is the minimum size of a dominating set?

<u>Thm (Alon 1990)</u> Let G be n-vertex with $\delta(G)=d>1$. Then G has a dominating set with atmost $\left(\frac{\log(d+1)+1}{d+1}\right)n$ vertices.

<u>Proof</u> Let $p \in [0,1]$.
Let S = random subset of $V(G)$ with each vertex chosen ind. with prob. p.
Let $T = V(G) \setminus (S \cup N(S))$. $\therefore$ $S \cup T$ is dominating.

$$\mathbb{E}[|S \cup T|] = \mathbb{E}[|S|+|T|] = \mathbb{E}[|S|] + \mathbb{E}[|T|]$$
$$= \sum_v \mathbb{P}[v \in S] + \sum_v \mathbb{P}[v \in T]$$
$$\leq np + n(1-p)^{d+1} \quad \leftarrow \text{why?}$$
$$\leq np + ne^{-p(d+1)} \quad \leftarrow \text{why?}$$
$$\leq n \, \frac{1+\log(1+d)}{1+d} \quad \text{for } p = \frac{\log(d+1)}{d+1}$$

Markov Inequality Let $X \geq 0$ be a random variable.
Then for every $t > 0$, $\mathbb{P}[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$.

Pf. $\mathbb{E}[X] = \sum_{k \geq 0} k\, \mathbb{P}[X=k] \geq \sum_{k \geq t} k\, \mathbb{P}[X=k] \geq t \sum_{k \geq t} \mathbb{P}[X=k] = t\, \mathbb{P}[X \geq t]$.

For us, X = counting variable (discrete r.v.)
so, " $\mathbb{E}[X] \to 0 \Rightarrow \mathbb{P}[X=0] \to 1$ "

Markov Inequality Let $X \geq 0$ be a random variable. Then for every $t > 0$, $\mathbb{P}[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$.

How is $\chi(G)$ determined?

Is it a function of $\omega(G)$? No!

A graph can be very sparse & yet have high $\chi(G)$.

Markov Inequality Let $X \geq 0$ be a random variable. Then for every $t > 0$, $\mathbb{P}[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$.

How is $\chi(G)$ determined?

Is it a function of $\omega(G)$? No!

A graph can be very sparse & yet have high $\chi(G)$.

Thm [Erdős 1959] Given $k \geq 3$, $g \geq 3$, $\exists$ graph with girth at least g and chromatic number at least k.

length of shortest cycle

Markov Inequality Let $X \geq 0$ be a random variable.
Then for every $t > 0$, $\mathbb{P}[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$.

How is $\chi(G)$ determined?
Is it a function of $\omega(G)$? No!
A graph can be very sparse & yet have high $\chi(G)$.

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$, $\exists$ graph with girth at least g and chromatic number at least k.

We want a graph with no short cycles $\longrightarrow$ girth $\geq g$
and no large independent sets $\longrightarrow$ $\chi(G) \geq \frac{n}{\alpha(G)} \geq k$

We will generate an Erdős-Renyi random graph $G(n,p)$ on n vertices & each pair of vertices is an edge independently with probability p.

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p) \leftarrow$ with n to be chosen later

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g \leftarrow$ proof looks for $\log n/n << p << n^{1/g - 1}$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

(# possible cycles of length j is ?

and all needed edges are present with probability ?)

Let X = # cycles of length $< g$

$$\mathbb{E}[X] = \sum_{j=3}^{g-1} ?$$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

(# possible cycles of length j is $\binom{n}{j}\frac{(j-1)!}{2}$. and all needed edges are present with probability p^j)

Let X = # cycles of length $< g$

$$\mathbb{E}[X] = \sum_{j=3}^{g-1} \binom{n}{j} \frac{(j-1)!}{2} p^j \leq \sum n^j p^j = \sum n^j n^{tj-j} = \sum_{j=3}^{g-1} n^{tj} < g\, n^{1-1/g}$$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

(# possible cycles of length j is $\binom{n}{j}\frac{(j-1)!}{2}$ and all needed edges are present with probability p^j)

Let X = # cycles of length $< g$

$$\mathbb{E}[X] = \sum_{j=3}^{g-1} \binom{n}{j}\frac{(j-1)!}{2}\, p^j \leq \sum n^j p^j = \sum n^j n^{tj-j} = \sum_{j=3}^{g-1} n^{tj} < g\, n^{1-1/g} = g\, n^{1/g(g-1)}$$

Since g is fixed, $\mathbb{E}[X]/n \to 0$ as $n \to \infty$, $\mathbb{E}[X] = o(n)$

so, $\exists\, n_1$ s.t. $\mathbb{E}[X] < \frac{n}{4}$ for all $n \geq n_1$.

Then, by Markov Ineq., $\mathbb{P}[X \geq \frac{n}{2}] < \frac{1}{2} < 1$.

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

For $n \geq n_1$, $\mathbb{P}[X \geq \frac{n}{2}] < 1$ where $X = \#$cycles of length $< g$

Next, we bound $\alpha(G(n,p))$. Set $\beta = \lceil \frac{3}{p} \log n \rceil$

$$\mathbb{P}[\alpha(G(n,p)) \geq \beta] \leq \binom{n}{\beta} (1-p)^{\binom{\beta}{2}} < ?$$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

For $n \geq n_1$, $\mathbb{P}[X \geq \frac{n}{2}] < 1$ where $X = \#$cycles of length $< g$

Next, we bound $\alpha(G(n,p))$. Set $\beta = \lceil \frac{3}{p} \log n \rceil$

$$\mathbb{P}[\alpha(G(n,p)) \geq \beta] \leq \binom{n}{\beta} (1-p)^{\binom{\beta}{2}} < n^{\beta} e^{-p\binom{\beta}{2}} = e^{(\log n - p\frac{(\beta-1)}{2})\beta}$$

$$\cong e^{(\log n - \frac{3}{2}\log n)\beta}$$

$$\to 0 \text{ as } n \to \infty$$

$\therefore \exists\, n_2$ s.t. $\mathbb{P}[\alpha(G(n,p)) \geq \beta] < \frac{1}{2}$ for $n \geq n_2$.

<u>Thm [Erdős 1959]</u> Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

<u>Proof</u> Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

For $n \geq n_1$, $\mathbb{P}[X \geq \frac{n}{2}] < 1$ where $X = \#$cycles of length $< g$

Next, we bound $\alpha(G(n,p))$. Set $\beta = \lceil \frac{3}{p} \log n \rceil$

$$\mathbb{P}[\alpha(G(n,p)) \geq \beta] \leq \binom{n}{\beta}(1-p)^{\binom{\beta}{2}} < n^{\beta} e^{-p\binom{\beta}{2}} = e^{(\log n - p\frac{(\beta-1)}{2})\beta}$$

$$\cong e^{(\log n - \frac{3}{2}\log n)\beta}$$

$$\to 0 \text{ as } n \to \infty$$

$\therefore \exists n_2$ s.t. $\mathbb{P}[\alpha(G(n,p)) \geq \beta] < \frac{1}{2}$ for $n \geq n_2$.

If $n \geq \max\{n_1, n_2\}$ then $\exists G$ on n-vertices with $X < \frac{n}{2}$ & $\alpha(G) < \beta$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

For $n \geq n_1$, $\mathbb{P}[X \geq \frac{n}{2}] < 1$ where $X = \#$cycles of length $< g$

Next, we bound $\alpha(G(n,p))$. Set $\beta = \lceil \frac{3}{p} \log n \rceil$

$$\mathbb{P}[\alpha(G(n,p)) \geq \beta] \leq \binom{n}{\beta} (1-p)^{\binom{\beta}{2}} < n^{\beta} e^{-p\binom{\beta}{2}} = e^{(\log n - p\frac{(\beta-1)}{2})\beta}$$

$$\cong e^{(\log n - \frac{3}{2}\log n)\beta}$$

$$\to 0 \text{ as } n \to \infty$$

$\therefore \exists n_2$ s.t. $\mathbb{P}[\alpha(G(n,p)) \geq \beta] < \frac{1}{2}$ for $n \geq n_2$.

If $n \geq \max\{n_1, n_2\}$ then $\exists G$ on n-vertices with $X < n/2$ & $\alpha(G) < \beta$

Remove a vertex from each of the X short cycles.

We get a graph G' on atleast $n/2$ vertices with girth$(G') > g$ & $\alpha(G') < \beta$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

For $n \geq n_1$, $\mathbb{P}[X \geq \frac{n}{2}] < 1$ where $X = \#$cycles of length $< g$

For $n \geq n_2$, $\mathbb{P}[\alpha(G(n,p)) \geq \beta] < \frac{1}{2}$ where $\beta = \lceil \frac{3}{p} \log n \rceil$

$\exists$ graph G' on at least $\frac{n}{2}$ vertices with girth $\geq g$ & $\alpha(G') < \beta$.

$$\Rightarrow \chi(G') \geq \frac{n/2}{\beta} > \frac{pn}{6 \log n} = \frac{n^t}{6 \log n} \longrightarrow \infty \text{ as } n \to \infty.$$

$\therefore \exists n_3$ s.t. $\chi(G') > k$ for $n \geq n_3$

Thm [Erdős 1959] Given $k \geq 3, g \geq 3$. $\exists$ graph G with girth$(G) \geq g$ and $\chi(G) \geq k$.

Proof Generate a random graph $G(n,p)$.

Let $p = n^{t-1}$ where $t < 1/g$, say $t = 1/2g$

For $n \geq n_1$, $\mathbb{P}[X \geq \frac{n}{2}] < 1$ where $X = \#$cycles of length $< g$

For $n \geq n_2$, $\mathbb{P}[\alpha(G(n,p)) \geq \beta] < \frac{1}{2}$ where $\beta = \lceil \frac{3}{p} \log n \rceil$

$\exists$ graph G' on at least $\frac{n}{2}$ vertices with girth $\geq g$ & $\alpha(G') < \beta$.

$$\Rightarrow \chi(G') \geq \frac{n/2}{\beta} > \frac{pn}{6 \log n} = \frac{n^t}{6 \log n} \longrightarrow \infty \text{ as } n \to \infty.$$

$\therefore \exists n_3$ s.t. $\chi(G') > k$ for $n \geq n_3$

So, if we choose $n \geq \max\{n_1, n_2, n_3\}$

then $\exists$ graph G with girth $\geq g$ & $\chi(G) \geq k$ ∎
(on $\geq \frac{n}{2}$ vertices)

Typical Probabilistic argument consists of defining certain "bad events" $E_1, \dots, E_k$ that we want to avoid & then showing that the probability of doing so is positive.

$\longrightarrow$ If all $\mathbb{P}[E_i]$ are small, say $\sum_i \mathbb{P}[E_i] < 1$ then O.K.

Typical Probabilistic argument consists of defining certain "bad events" $E_1, \dots, E_k$ that we want to avoid & then showing that the probability of doing so is positive.

→ If all $\mathbb{P}[E_i]$ are small, say $\sum_i \mathbb{P}[E_i] < 1$ then O.K.

→ If all E_i are independent then $\mathbb{P}[\text{none of } E_i \text{ occur}]$ is $\prod_{i=1}^{k} (1 - \mathbb{P}[E_i])$ which is > 0 if all $\mathbb{P}[E_i] < 1$

But what if E_i are dependent?

Typical Probabilistic argument consists of defining certain "bad events" $E_1, \dots, E_k$ that we want to avoid & then showing that the probability of doing so is positive.

$\rightarrow$ If all $\mathbb{P}[E_i]$ are small, say $\sum_i \mathbb{P}[E_i] < 1$ then O.K.

$\rightarrow$ If all E_i are independent then $\mathbb{P}[\text{none of } E_i \text{ occur}]$ is $\prod_{i=1}^{k} (1 - \mathbb{P}[E_i])$ which is > 0 if all $\mathbb{P}[E_i] < 1$

But what if E_i are dependent?

Lovasz Local Lemma Let $E_1, \dots, E_k$ be events with $\mathbb{P}[E_i] \le p \; \forall i$. Suppose each E_i is independent of all other E_j except for at most d of them.
Then, $ep(d+1) < 1 \Rightarrow \mathbb{P}[\text{none of } E_i \text{ occur}] > 0$

Lovasz Local Lemma Let $E_1, \ldots, E_k$ be events with $\mathbb{P}[E_i] \leq p \; \forall i$. Suppose each E_i is independent of all other E_j except for at most d of them. Then, $ep(d+1) < 1 \Rightarrow \mathbb{P}[\bigcap_{i=1}^{k} \overline{E_i}] > 0$.

Lets apply this to $R(k,k)$.

Theorem (Spencer 1977) If $e\left(\binom{k}{2}\binom{n}{k-2}+1\right)2^{1-\binom{k}{2}} < 1$ then $R(k,k) > n$.

Proof

<u>Lovasz Local Lemma</u> Let $E_1, \ldots, E_k$ be events with $\mathbb{P}[E_i] \leq p \; \forall i$. Suppose each E_i is independent of all other E_j except for at most d of them. Then, $ep(d+1) < 1 \Rightarrow \mathbb{P}[\bigcap_{i=1}^{k} \bar{E_i}] > 0$.

Lets apply this to $R(k,k)$.

<u>Theorem (Spencer 1977)</u> If $e\left(\binom{k}{2}\binom{n}{k-2}+1\right)2^{1-\binom{k}{2}} < 1$ then $R(k,k) > n$.

<u>Proof</u> Random 2-color edges of K_n (independently Red/Blue w. prob. $\frac{1}{2}$)

For each $S \in \binom{V(K_n)}{k}$, let A_S be the event S induces a monochromatic K_k.

$\mathbb{P}[A_S] = 2^{1-\binom{k}{2}} = p$.

A_S is independent of all $A_{S'}$ unless

Lovasz Local Lemma Let $E_1, \ldots, E_k$ be events with $\mathbb{P}[E_i] \leq p \; \forall i$. Suppose each E_i is independent of all other E_j except for at most d of them. Then, $ep(d+1) < 1 \Rightarrow \mathbb{P}[\bigcap_{i=1}^{k} \overline{E_i}] > 0$.

Lets apply this to $R(k,k)$.

Theorem (Spencer 1977) If $e\left(\binom{k}{2}\binom{n}{k-2}+1\right)2^{1-\binom{k}{2}} < 1$ then $R(k,k) > n$.

Proof Random 2-color edges of K_n (independently Red/Blue w. prob. $\frac{1}{2}$)

For each $S \in \binom{V(K_n)}{k}$, let A_S be the event S induces a monochromatic K_k.

$\mathbb{P}[A_S] = 2^{1-\binom{k}{2}} = p$.

A_S is independent of all $A_{S'}$ unless $|S \cap S'| \geq 2$.

For each S, there are atmost $\binom{k}{2}\binom{n}{k-2} = d$ such choices of S'.

Apply LLL to these events with p & d as above.

$\therefore$ with positive probability we have a 2-coloring of $E(K_n)$ with no monochromatic K_k ∎

Our lower bounds of $R(k,k)$

- Union Bound $\left(\frac{1}{e\sqrt{2}}+o(1)\right)k\,2^{k/2}$
- Alteration $\left(\frac{1}{e}+o(1)\right)k\,2^{k/2}$
- LLL $\left(\frac{\sqrt{2}}{e}+o(1)\right)k\,2^{k/2}$

By Optimizing the choice of n in

"$e\left(\underbrace{\binom{k}{2}\binom{n}{k-2}}_{d}+1\right)\underbrace{2^{1-\binom{k}{2}}}_{p}<1 \Rightarrow R(k,k)>n$"

Fix k, so p is fixed.

Make n small, so d is small enough.

$$d<\underbrace{\frac{k^2}{2}\left(\frac{ne}{k-2}\right)^{k-2}}<\frac{1}{ep}=\underbrace{\frac{1}{2e}2^{k/2}\left(2^{k/2}\right)^{k-2}}$$

want $n\le c\,\frac{\sqrt{2}}{e}\,k\,2^{k/2}$ where $c=\left(\frac{2}{ek^2}\right)^{1/(k-2)}\frac{k-2}{k}$

⋮

A very silly problem (& comparison)

We want to find an injective function $f : [n] \to [m]$

What is the smallest m (as a function of n) such that this is possible?

:-D

Consider a random mapping from $[n] \to [m]$ where each image is chosen independently, u.a.r.

Analyze this random construction to give an injective function using

(i) union bound,

(ii) LLL

to derive a bound on m that guarantees success.

Setup for Lovász Local Lemma:

Defn An event B is mutually independent of events $A_1, \ldots, A_k$ if $\mathbb{P}[B \mid C_{i_1} \wedge C_{i_2} \wedge \ldots \wedge C_{i_\ell}] = \mathbb{P}[B]$ $\forall \ell$ $\forall 1 \leq i_1 < i_2 < \cdots < i_\ell \leq k$.
where each C_{i_j} is either A_{i_j} or $\overline{A_{i_j}}$.

Setup for Lovász Local Lemma:

Defn An event B is mutually independent of events $A_1, \dots, A_k$ if $\mathbb{P}[B \mid C_{i_1} \wedge C_{i_2} \wedge \dots \wedge C_{i_\ell}] = \mathbb{P}[B]$ $\forall \ell$ $\forall 1 \leq i_1 < i_2 < \dots < i_\ell \leq k$.
where each C_{i_j} is either A_{i_j} or $\overline{A_{i_j}}$.

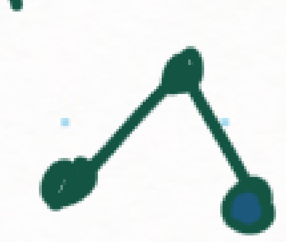
Defn G is said to be a dependency graph of events $A_1, \dots, A_n$ if $V(G) = [n]$ and for each i, A_i is mutually independent of all events A_j s.t. $ij \notin E(G)$.

Setup for Lovász Local Lemma:

Defn An event B is mutually independent of events $A_1, \ldots, A_k$ if $\mathbb{P}[B \mid C_{i_1} \wedge C_{i_2} \wedge \ldots \wedge C_{i_\ell}] = \mathbb{P}[B]$ $\forall \ell$ $\forall 1 \le i_1 < i_2 < \cdots < i_\ell \le k$.
where each C_{i_j} is either A_{i_j} or $\overline{A_{i_j}}$.

Defn G is said to be a dependency graph of events $A_1, \ldots, A_n$ if $V(G) = [n]$ and for each i, A_i is mutually independent of all events A_j s.t. $ij \notin E(G)$.

Caution! mutual independence $\neq$ pairwise independence.

e.g. Pick $x_1, x_2, x_3 \in \{0,1\}$ uniformly & independently at random.
For $i = 1, 2, 3$, let A_i be event $x_{i+1} + x_{i+2} = 0 \pmod 2$ (indices mod 3)
Then these events are pairwise independent but not mutually ind.
$\overline{K_3}$ is not a valid dep. graph, but  is a valid dep. graph.
or 

However, in many (most?) applications of LLL, the underlying probability space is a product probability space i.e., it is based on a collection of independent random experiments and each event A_i is determined by a subcollection S_i of these independent experiments.

However, in many (most?) applications of LLL, the underlying probability space is a product probability space i.e., it is based on a collection of independent random experiments and each event A_i is determined by a subcollection S_i of these independent experiments.

<u>Mutual Independence Principle</u> Let $Z_1, Z_2, \ldots, Z_m$ be independent experiments and $A_1, \ldots, A_n$ be events s.t. the occurrence of each A_i is determined by a subset S_i of $Z_1, \ldots, Z_m$. If S_i is disjoint from $S_{j_1}, \ldots, S_{j_k}$ then A_i is mutually ind. of $\{A_{j_1}, \ldots, A_{j_k}\}$

However, in many (most?) applications of LLL, the underlying probability space is a product probability space i.e., it is based on a collection of independent random experiments and each event A_i is determined by a subcollection S_i of these independent experiments.

<u>Mutual Independence Principle</u> Let $Z_1, Z_2, \ldots, Z_m$ be independent experiments and $A_1, \ldots, A_n$ be events s.t. the occurrence of each A_i is determined by a subset S_i of $Z_1, \ldots, Z_m$. If S_i is disjoint from $S_{j_1}, \ldots, S_{j_k}$ then A_i is mutually ind. of $\{A_{j_1}, \ldots, A_{j_k}\}$

In this set-up, a valid dependency graph can be formed by placing an edge $i \leftrightarrow j$ based on $|S_i \cap S_j|$.

e.g. in our application of LLL to $R(k,k)$, $Z_1, \ldots, Z_m$ are the independent "coin flips" used to color m edges of K_n. A_S is independent of all $A_{S'}$ where $|S \cap S'| \leq 1$.

Lovász Local Lemma, General Form

neighborhood in a dependency graph

Let $A_1, \ldots, A_n$ be events. For each $i \in [n]$, let $N(i) \subseteq [n]$ be such that A_i is independent of $\{A_j : j \notin \{i\} \cup N(i)\}$.

If $x_1, \ldots, x_n \in [0,1)$ satisfy

$$\mathbb{P}[A_i] \leq x_i \prod_{j \in N(i)} (1 - x_j) \quad \forall i \in [n]$$

then with probability $\geq \prod_{i=1}^{n} (1 - x_i)$, none of the events A_i occur.

Lovász Local Lemma, General Form

Let $A_1, \ldots, A_n$ be events. For each $i \in [n]$, let $N(i) \subseteq [n]$ be such that A_i is independent of $\{A_j : j \notin \{i\} \cup N(i)\}$.

If $x_1, \ldots, x_n \in [0,1)$ satisfy

$$\mathbb{P}[A_i] \leq x_i \prod_{j \in N(i)} (1 - x_j) \quad \forall i \in [n]$$

then with probability $\geq \prod_{i=1}^{n} (1 - x_i)$, none of the events A_i occur.

LLL, Symmetric Form

Let G be a dependency graph of events $A_1, \ldots, A_n$ with $\Delta(G) \leq d$ and $\mathbb{P}[A_i] \leq p \ \forall i$. Then,

$$ep(d+1) < 1 \Rightarrow \mathbb{P}\left[\bigwedge_{i=1}^{n} \overline{A_i}\right] > 0$$

Proof Set $x_i = 1/(d+1) < 1 \ \forall i$

Then $x_i \prod_{j \in N(i)} (1 - x_j) \geq \frac{1}{d+1}\left(1 - \frac{1}{d+1}\right)^d > \frac{1}{(d+1)e} \geq p$

← neighborhood in dep. graph.

Lovász Local Lemma, General Form

Let $A_1, \ldots, A_n$ be events. For each $i \in [n]$, let $N(i) \subseteq [n]$ be such that A_i is independent of $\{A_j : j \notin \{i\} \cup N(i)\}$.

If $x_1, \ldots, x_n \in [0,1)$ satisfy

$$\mathbb{P}[A_i] \leq x_i \prod_{j \in N(i)} (1 - x_j) \quad \forall i \in [n]$$

then with probability $\geq \prod_{i=1}^{n} (1 - x_i)$, none of the events A_i occur.

LLL, Symmetric Form

Let G be a dependency graph of events $A_1, \ldots, A_n$ with $\Delta(G) \leq d$ and $\mathbb{P}[A_i] \leq p \ \forall i$. Then,

$$ep(d+1) < 1 \Rightarrow \mathbb{P}\left[\bigwedge_{i=1}^{n} \overline{A_i}\right] > 0$$

e is sharp; cannot be replaced by any smaller constant

often, checking $4p(d+1) < 1$ is enough.