

# Graduate Discrete Math (21-701) Notes

Wilson Pan

February 17, 2026

## Abstract

Lecture notes based on Graduate Discrete Math (21-701)

## 1 Graphs

**Definition 1.1.** *Graph is a set of objects  $(V, E)$  and  $E \subseteq \binom{V}{2}$*

**Definition 1.2.** *Walk is a sequence of vertices*

**Definition 1.3.** *A path is a walk without repeated vertices*

**Definition 1.4.** *A proper  $K$ -coloring of a graph is a function  $c : V \rightarrow [k]$  such that  $\forall u, v \in V, u \sim v \implies c(u) \neq c(v)$*

**Theorem 1.5.** *A graph is 2 colorable if and only if there is no odd cycles in  $G$*

*Proof.* ( $\implies$ ) AFSOC there exist an odd cycle,  $C$  in  $G$ . Define the vertices of  $C$  as  $v_1, v_2, \dots, v_k$  where  $k$  is odd. Define  $c(v) = \begin{cases} \text{red} & d(v, v_1) \text{ is even} \\ \text{blue} & d(v, v_1) \text{ is odd} \end{cases}$   
Then  $c(v_1)$  and  $c(v_k)$  are both red so a contradiction.

( $\impliedby$ ) We can assume each component is connected. Choose  $v_0$  and define  $c(v) = \begin{cases} \text{red} & d(v, v_0) \text{ is even} \\ \text{blue} & d(v, v_0) \text{ is odd} \end{cases}$   
If there exist vertices  $u, v$  with  $uv$  an edge such that  $d(u, v_0) \equiv d(v, v_0) \pmod{2}$  then consider the cycle,  $C$  formed by shortest path from  $v_0 \rightarrow u$  and  $v_0 \rightarrow v$  with  $uv$ . Then  $|C| = d(u, v_0) + d(v, v_0) + 1$  is odd and we're done.  $\square$

## 2 Hypergraphs

**Definition 2.1.** *A collection  $\mathcal{H}$  of subsets of a vertex set  $V$ .*

**Definition 2.2.**  *$\mathcal{H}$  is  $k$ -uniform if  $|f| = k, \forall f \in \mathcal{H}$*

**Definition 2.3.** *A proper  $k$ -coloring of  $\mathcal{H}$  is an assignment  $c : V \rightarrow [k]$  such that  $\forall f \in \mathcal{H}, |c(f)| = k$*

**Definition 2.4.** *A rainbow coloring of  $\mathcal{H}$  is an assignment  $c : V \rightarrow [k] \forall f \in \mathcal{H}, |c(f)| = |f|$*

**Example 2.5.** *What is the least number of edges in a  $k$ -uniform graph that is not 2-colorable?*

Let this number be  $m(k)$  then  $m(1) = 0, m(2) = 3, m(3) \geq 7$

**Theorem 2.6.** *If  $\mathcal{H}$  is a 3-uniform hypergraph with less than 6 edges then  $\mathcal{H}$  is 2-colorable*

*Proof.* Using induction on  $|V|$

(Base Case) For  $n = 6$ , consider all balanced 2-colorings of  $V$  there are  $\binom{6}{3} = 20$ . Each hyperedge is incompatible with 2 of those colorings (namely those where the edges are 3 blue or 3 red). Thus, at least  $20 - 12 > 0$  of these colorings can be proper.

(Induction Hypothesis) Suppose  $n \geq 7$

**Claim 2.7.** *There are 2 vertices  $u$  and  $v$  not in any common edge.*

Each edge connects  $\binom{3}{2} = 3$  pairs of vertices. There are  $\binom{7}{2} = 21$  pairs of vertices overall. So some pair of vertices is not connected as  $21 > 18$ .

Define  $\mathcal{H}'$  by merging  $u, v$  into  $w$

**Claim 2.8.**  *$\mathcal{H}'$  is 3-uniform*

Because no edge contains both  $u$  and  $v$  the merging doesn't create a 2 set and every edge is still has size 3.

Additionally,  $||\mathcal{H}'|| \leq ||\mathcal{H}|| \leq 6$  so by induction hypothesis  $\mathcal{H}'$  is 2-colorable. Giving both  $u$  and  $v$  the same color as  $w$  and keeping the rest of the colors the same.

If an edge of  $e$  of  $\mathcal{H}$  avoids  $\{u, v\}$  then it is properly colored in  $\mathcal{H}'$ . If  $e$  contains  $u$  or  $v$  then after merging it corresponds to an edge of  $\mathcal{H}'$  containing  $w$ . If  $e$  is monochromatic in  $\mathcal{H}$  then it would be monochromatic in  $\mathcal{H}'$ . This would be a contradiction so edge is monochromatic in  $\mathcal{H}$  and thus a proper coloring.  $\square$

**Remark 2.9.** *Suppose it has 7 edges and vertices. Consider the coloring 4 red and 3 blue. Then there are  $\binom{7}{3} = 35$  such colorings. If  $\mathcal{H}$  is not 2 colorable then there are  $\binom{3}{3} + \binom{4}{3} = 5$  excluded coloring for all distinct edges. There are 4 forbidden configurations for any configurations that are not 2 colorable  $\mathcal{H}$  with  $|\mathcal{H}| = 7$  on 7 vertices*

### 3 Probabilistic Method

**Theorem 3.1.**  $m(k) \geq 2^{k-1}$

*Proof.* Color vertices of  $\mathcal{H}$  randomly red or blue. For each edge  $f$ , define  $E_f$  to be the event that  $f$  is monochromatic then  $Pr[E_f] = \frac{1}{2^{k-1}}$

$$Pr \left[ \bigcup_{f \in \mathcal{H}} E_f \right] \leq \sum_{f \in \mathcal{H}} Pr[E_f] = \frac{|\mathcal{H}|}{2^{k-1}} < 1$$

So there is non-zero probability that there exist a coloring with no monochromatic edges if  $|\mathcal{H}| < 2^{k-1}$   $\square$

**Theorem 3.2.** *Erdős-Selfridge Theorem: Given hypergraph  $\mathcal{H}$ , consider a game between a maker and breaker. The maker's goal is to color some edge all blue and breaker's goal is to prevent all blue edges.*

*If  $\mathcal{H}$  is  $k$ -uniform and  $|\mathcal{H}| < 2^{k-1}$  then the breaker has a winning strategy even as player 2.*

*Proof.* Let  $\phi(f) = \begin{cases} 0 & \text{if blocked by breaker} \\ \frac{2^{\#\text{blue} \in f}}{2^n} & \text{otherwise} \end{cases}$

be the "danger function". Define

$$\phi(\mathcal{H}) = \sum_{f \in \mathcal{H}} \phi(f)$$

Observe that if an edge is all blue, then  $\phi(\mathcal{H}) \geq 1$

At start of the game  $\phi(\mathcal{H}) = \frac{|\mathcal{H}|}{2^n}$ . The worst case for when maker moves is increasing by  $\frac{|\mathcal{H}|}{2^n}$  when the chosen vertex is in all edges. Then when breaker moves,

$$- \sum_{f \ni v_1} \phi(f).$$

When maker goes after

$$\sum_{f \ni v_2} \phi(f).$$

Notice

$$\sum_{f \ni v_1} \phi(f) > \sum_{f \ni v_2} \phi(f)$$

otherwise breaker played optimally.

So as long as  $\frac{|\mathcal{H}|}{2^{n-1}} < 1$  then breaker wins.  $\square$

**Definition 3.3.** *Incidence matrix of a hypergraph  $\mathcal{H}$  with  $|V| = n$  and  $|\mathcal{H}| = m$  is defined as*

$$I_{i,j} = \begin{cases} 1 & \text{if } v_i \in f_j \\ 0 & \text{otherwise} \end{cases}$$

**Theorem 3.4.** *Hall's Theorem*

*If  $G$  is a bipartite on  $(A, B)$  there is a complete matching if and only if*

$$\forall S \subseteq A, |\Gamma(S)| \geq |S|$$

*where  $\Gamma(S) = \{u \in B | \exists v \in S, u \sim v\}$ .*

**Theorem 3.5.** *Consider complete graph  $\mathcal{P}(X)$  where  $|X| = n$ .*

*$\mathcal{P}(X)$  has levels*

$$\binom{X}{0}, \binom{X}{1}, \dots, \binom{X}{n}$$

*$\forall k < \frac{n}{2}$ , there is an injection*

$$f_k : \binom{X}{k} \rightarrow \binom{X}{k+1}$$

*such that  $\forall S \in \binom{X}{k}, S \subseteq f_k(S)$*

*Proof.* Consider bipartite graph  $\left( \binom{X}{k}, \binom{X}{k+1} \right)$ , if  $f \in \binom{X}{k}, g \in \binom{X}{k+1}$  then we define  $f \sim g$  if  $f \subseteq g$ .

Then for some  $S \subseteq \binom{X}{k}$  then  $|\Gamma(S)| \geq \frac{|S|(n-k)}{k+1}$ .  $\square$

**Definition 3.6.** For a sperner system is a hypergraph  $\mathcal{H}$  that satisfy if

$$\forall f, g \in \mathcal{H}, f \not\subseteq g$$

**Theorem 3.7.** If  $\mathcal{H}$  is a sperner system of  $n$ -vertices then

$$|\mathcal{H}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$$

**Theorem 3.8.** LYM Inequality on a sperner family  $\mathcal{H}$ ,

$$\sum_{f \in \mathcal{H}} \frac{1}{\binom{n}{|f|}} \leq 1$$

*Proof.* Suppose  $F = \{\emptyset, \{1\}, \dots, \{1, 2, \dots, n\}\}$

Note: Any sperner family can share at most one edge with  $F$ .

Consider a random permutation  $\sigma \in S_n$  and define  $\mathcal{H}_\sigma = \{\sigma(f) | f \in \mathcal{H}\}$ .

For any  $\sigma \in S_n$ ,  $|\mathcal{H}_\sigma \cap F| \leq 1$

Now choose any  $\sigma$ , uniformly at random and define  $\mathcal{X} = |\mathcal{H}_\sigma \cap F|$  is a random variable and  $\mathcal{X} \leq 1$ .

Let  $\mathcal{X} = I_f$  where  $I_f = \begin{cases} 1 & \sigma(f) \in F \\ 0 & \text{otherwise} \end{cases}$

$$\mathbb{E}[\mathcal{X}] = \sum_{f \in \mathcal{H}} \mathbb{E}[I_f] = \sum_{f \in \mathcal{H}} \frac{1}{\binom{n}{|f|}} \leq 1$$

□

**Definition 3.9.** Define the "shadow" of  $\mathcal{H} \subseteq \binom{X}{r}$  as  $\partial\mathcal{H} \subseteq \binom{X}{r-1}$

$$\partial\mathcal{H} = \left\{ S \subseteq \binom{X}{r-1} : \exists T \in \mathcal{H}, S \subseteq T \right\}$$

**Theorem 3.10.** Let  $n = |X|$  then

$$\frac{|\mathcal{H}|}{\binom{n}{r}} \leq \frac{|\partial\mathcal{H}|}{\binom{n}{r-1}}$$

with equality only if  $\mathcal{H}$  is empty on  $\binom{X}{r}$

*Proof.* Suppose  $\mathcal{H}$  is a sperner system, not all on one level.

Write  $\mathcal{H}_i = \mathcal{H} \cap \binom{X}{i}$  then  $H = \mathcal{H}_i \cup \mathcal{H}_{i+1} \cup \dots \cup \mathcal{H}_j$  where  $i < j$  and  $\mathcal{H}_i$  nonempty.

We can instead of  $\mathcal{H}_j$  we can write  $\partial\mathcal{H}_j$  as  $\partial\mathcal{H}_j \subseteq \mathcal{H}_j$

Suppose  $\mathcal{H}$  maximizes the sum  $\sum_{f \in \mathcal{H}} \frac{1}{\binom{n}{|f|}}$  among all sperner graphs.

Let  $S \in \partial\mathcal{H}$  and  $T \subseteq \mathcal{H}$ . Define a bipartite graph from  $S \rightarrow T$  and edges if  $S \subseteq T$ .

For  $T \in \mathcal{H}$ ,  $\deg(T) = r$  for  $S \in \partial\mathcal{H}$ ,  $\deg(S) = n - (r - 1)$ .

So  $|\mathcal{H}| \cdot r = b \leq |\partial\mathcal{H}| \cdot (n - r + 1)$ .

Then  $|\mathcal{H}| \cdot r \binom{n}{r} \leq |\partial\mathcal{H}| \cdot (n - r + 1) \binom{n}{r} \implies \frac{|\mathcal{H}|}{\binom{n}{r}} \leq \frac{|\partial\mathcal{H}|}{\binom{n}{r-1}}$

□

**Definition 3.11.** An intersecting hypergraph has any 2 hyperedges intersect.

**Theorem 3.12.** For an intersecting hypergraph on  $n$ -vertices and  $r$ -uniform,

If  $r = \frac{n}{2}$  then we can fix 1 vertex and complete the remaining  $\frac{n}{2} - 1$  vertices. So  $\binom{n-1}{\frac{n}{2}-1}$

If  $r > \frac{n}{2}$  then  $2^n$ .

If  $r < \frac{n}{2}$  then  $\binom{n-1}{r-1}$ .

We'll prove the last statement

*Proof.* Assume  $n = lk$  for some  $l$  and for any  $\sigma \in S_n$  define  $\mathcal{H}_\sigma = \{\sigma(f) | f \in \mathcal{H}\}$ . Define  $\mathcal{F}$  to be a  $k$ -uniform hypergraph with  $l$  non-intersecting edges.

If  $\mathcal{H}$  is intersecting then  $|\mathcal{H}_\sigma \cap \mathcal{F}| \leq 1$ .

Let  $\mathcal{X} = |\mathcal{H}_\sigma \cap \mathcal{F}|$ . Then

$$\mathbb{E}[\mathcal{X}] = \sum_f \mathbb{E}[I_f] = |\mathcal{H}| \mathbb{P}[\sigma(f) \in \mathcal{F}] = |\mathcal{H}| \frac{l}{\binom{n}{k}} = \frac{|\mathcal{H}|}{\binom{n-1}{k-1}}$$

So  $|\mathcal{H}| \leq \binom{n-1}{k-1}$

Consider the case when  $n$  is not divisible by  $k$ . If  $n \geq 2k$  then fix a cyclic ordering  $\pi$  of the  $n$  vertices. For that ordering consider the  $n$  cyclic  $k$ -intervals for  $i = 1, 2, \dots, n$

$$I_i(\pi) = \{\pi(i), \pi(i+1), \dots, \pi(i+k-1)\}$$

indices taken modulo  $n$ .

For a given  $\pi$  define

$$\mathcal{X}_\pi := \#\{f \in \mathcal{H} | f \text{ is one of the intervals } I_i(\pi)\}$$

Any two sets counted in  $\mathcal{X}_\pi$  must intersect since  $\mathcal{H}$  is intersecting. Among the  $n$  cyclic  $k$ -intervals at most  $k$  of them can be pairwise intersecting since we can fix one vertex however  $k+1$  intervals will force two of them to be disjoint. So for every  $\pi$ ,  $\mathcal{X}_\pi \leq k$ .

So

$$\mathbb{E}[\mathcal{X}_\pi] = |\mathcal{H}| \frac{k!(n-k)!}{(n-1)!} = |\mathcal{H}| \frac{n}{\binom{n}{k}} \leq k \implies |\mathcal{H}| \leq \binom{n-1}{k-1}$$

□

We'll try constructing such a configuration.

If  $|\mathcal{H}| = \binom{n-1}{k-1}$  then  $|\mathcal{H}_\sigma \cap \mathcal{F}| = k$  for each  $\sigma \in S_n$ . Then there is an  $i$  such that  $\mathcal{I} = \begin{cases} \{i-k+1, i-k+2, \dots, i\} \\ \{i-k+2, i-k+3, \dots, i+1\} \\ \vdots \\ \{i, i+1, \dots, i+k+1\} \end{cases}$

Suppose  $a_1, \dots, a_{k-1} \in [n]$  with no  $a_j = i-k, i-k-1, \dots, i, \dots, i-k+1$

Consider a permutation  $\sigma$  sending  $a_1 \rightarrow i+1, a_2 \rightarrow i+2, \dots, a_{k-1} \rightarrow i+k-1$  and fixing  $i-k, \dots, i$ .

We know,  $|\mathcal{H}_\sigma \cap \mathcal{F}|$  includes all edges of  $\mathcal{I}$

Now let  $\sigma$  be any permutation such that  $\mathcal{H} \cap \mathcal{F}$  includes  $i$  of  $\mathcal{I}$ . It suffices to show  $\mathcal{H}_\sigma \cap \mathcal{F}$  includes all of  $\mathcal{I}$  for any transposition.

**Lemma:** Adjacent transposition generates  $S_n$ .

(Case 1) If  $j, j+1 \in \{i-k+1, 1, \dots, i+k-1\}$ , neither is  $i$  so they're both on same side of  $i$ .

Letting  $f_0 = \{i-k+1, \dots, i\}$  and  $f_1 = \{i, \dots, i+k-1\}$  then  $\tau(f_0) = f_0$  and  $\tau(f_1) = f_1$

(Case 2) If  $j = i+k-1$  and  $j+1 = i+k$  then  $\tau(f_0) = f_0$  and  $\tau(\{i-k, \dots, i-1\}) = \{i-k, \dots, i-1\}$ .

**Theorem 3.13.** Let  $\alpha_1, \dots, \alpha_n \sim \text{Ber}(p)$ , choosing numbers  $\beta_1, \dots, \beta_n$  with  $\sum \beta_i = 1$  then  $\mathbb{P}[\sum \beta_i \alpha_i \geq \frac{1}{2}] \geq p$

*Proof.* Define  $\mathcal{H}$  on  $[n]$  by  $f \in \mathcal{H}$  if  $\sum_{i \in f} a_i \geq \frac{1}{2}$ . For simplicity, assume no sum is  $\frac{1}{2}$ . Then

$$\mathbb{P}\left[\sum \beta_i \alpha_i \geq \frac{1}{2}\right] = \sum_{f \in \mathcal{H}} p^{|f|} (1-p)^{n-|f|}$$

Define  $h_k = \left| \mathcal{H} \cap \binom{[n]}{k} \right|$

$$\begin{aligned} \mathbb{P}\left[\sum \beta_i \alpha_i \geq \frac{1}{2}\right] &= \sum_k h_k p^k (1-p)^{n-k} \\ &= \sum_{k \leq \frac{n}{2}} h_k p^k (1-p)^{n-k} + h_{n-k} p^{n-k} (1-p)^k \\ &= \sum_{k \leq \frac{n}{2}} (h_k + h_n) p^{n-k} (1-p)^k - h_k (p^{n-k} (1-p)^k - p^k (1-p)^{n-k}) \end{aligned}$$

Note:  $h_k + h_{n-k} \geq \binom{n}{k}$  since it or its complement has to be in  $\mathcal{H}$

$$\begin{aligned} &\geq \sum_{k \leq \frac{n}{2}} \binom{n}{k} p^{n-k} (1-p)^k - h_k (p^{n-k} (1-p)^k - p^k (1-p)^{n-k}) \\ &= \sum_{k \leq \frac{n}{2}} \binom{n}{k} p^{n-k} (1-p)^k + \binom{n-1}{k-1} p^k (1-p)^{n-k} \\ &= p \sum_{k \leq \frac{n}{2}} \binom{n-1}{k-1} p^k (1-p)^{n-k} \\ &= p \sum_{k \leq \frac{n}{2}} \binom{n-1}{k-1} p^k (1-p)^{n-k} \\ &= p \sum_{k \leq \frac{n}{2}} \binom{n-1}{k-1} p^{k-1} (1-p)^{(n-k)-(k-1)} \\ &= p \end{aligned}$$

□

**Theorem 3.14.** If there are 10 points in the plane then they can be covered by 10 non-intersecting unit circles.

*Proof.* Given any collection  $X \subseteq \mathbb{R}^2, |X| = 10$ . Consider a random translation of the hexagonal circle pattern.

Let  $\mathcal{Z} = \#$  points in  $X$  covered then

$$\mathbb{E}[\mathcal{Z}] = \mathbb{E}[I_1] + \dots + \mathbb{E}[I_{10}] = 10 \cdot \frac{\pi}{\frac{6}{\sqrt{3}}} \approx 9.07$$

So there exist a translation such that  $\mathcal{Z} = 10$

□

**Theorem 3.15.** *Given a graph,  $G$  on  $n$  vertices and  $\frac{nd}{2}$  edges,  $d \geq 1$ . Then  $\alpha(G) \geq \frac{n}{2d}$ .*

*Proof.* Let  $S \subseteq V$  be a random subset defined by  $\mathbb{P}[v \in S] = p$ ,  $p$  to be determined. Let  $X = |S|$  and  $Y = \mathbb{E}[G|_S]$ . For each  $e = \{i, j\} \in E$ , let  $Y_e$  be indicator random variable for the event  $i, j \in S$  so that

$$Y = \sum_{e \in E} Y_e$$

For any such  $e$ ,

$$\mathbb{E}[Y_e] = \mathbb{P}[i, j \in S] = p^2$$

$$\mathbb{E}[Y] = \frac{nd}{2} p^2$$

Clearly,  $\mathbb{E}[X] = np$  so  $\mathbb{E}[X - Y] = np - \frac{nd}{2} p^2$ .

Setting  $p = \frac{1}{d}$  then  $\mathbb{E}[X - Y] = \frac{n}{2d}$ .

So there exist a  $S$  such that the number of vertices minus the number of edges is at least  $\frac{n}{2d}$ .

Create  $S^*$  from  $S$  by deleting one vertex from each edge in  $S$  and delete it and this leaves  $S^*$  with at least  $\frac{n}{2d}$  vertices. With all edges destroyed we leave  $S^*$  an independent set.  $\square$

**Theorem 3.16.** *Erdos Chromatic Number Girth Theorem*

$\forall k \in \mathbb{Z}^+, \exists$  graph of girth greater than or equal to  $k$  and chromatic number  $k$ .

*Proof.* Idea: Choose random graph  $G \sim G(n, p)$ . To show a graph satisfies both properties we need the the number of short cycles (length less than  $k$ ) to be 0 and there are no independent set of size no more than  $\frac{n}{k}$ .

For the first statement let  $X = \# \text{cycles with length} \leq k$  then

$$\mathbb{E}[X] = \sum_C \mathbb{E}[I_C] = \sum_{j=3}^k \sum_{|C|=j} \mathbb{E}[I_C] = \sum_{j=3}^k \binom{n}{j} \frac{(j-1)!}{2} p^j \leq \sum_{j=3}^k n^j p^j \leq (np)^{k+1}$$

To have  $\mathbb{E}[X] = O(1)$ , we need  $p = O\left(\frac{1}{n}\right)$

We want no independent set of size  $a \approx \frac{n}{k}$  so

$$\begin{aligned} \mathbb{P}[\alpha(G_{n,p}) \geq a] &\leq \binom{n}{a} (1-p)^{\binom{a}{2}} \\ &\leq n^a (1-p)^{a(a-1)/2} \\ &\leq n^a e^{-pa(a-1)/2} \\ &= \left( n e^{-p(a-1)/2} \right)^a \\ &= \left( e^{\ln(n) - p(a-1)/2} \right)^a \end{aligned}$$

Not possible since we need  $p \geq 5 \ln(n)/a$  but  $p = O\left(\frac{1}{n}\right)$  from previous condition.

To fix this issue consider an alteration. If  $p = \frac{n^\epsilon}{n}$  and  $0 < \epsilon < \frac{1}{k}$  then we have  $\mathbb{P}(\alpha(G_{n,p}) \geq \frac{n}{2k}) \rightarrow 0$  since  $\frac{n^\epsilon}{n} \gg \frac{5 \ln(n) - 2k}{n}$ .

To fix the short cycle issue,

$$\mathbb{E}[X] = \sum_{j=3}^k (np)^j \leq (k-3)(np)^k \leq kn^{\epsilon k}$$

By Markov's inequality

$$\mathbb{P}\left(X \geq \frac{n}{2}\right) \leq \frac{kn^{\epsilon k}}{n/2}$$

Choose  $n$  large enough such that both probabilities are greater than  $\frac{1}{2}$ . Then there exists a graph on  $n$  vertices with no independent set of size  $\frac{n}{2k}$  and less than  $\frac{n}{2}$  short cycles. Delete an vertex from each short cycle to make a graph  $G'$  with  $\frac{n}{2}$  vertices, no short cycles and no independent set of size  $\frac{n}{2k}$ . So

$$\chi(G') = \frac{n'}{\alpha(G')} \geq \frac{\frac{n}{2}}{\frac{n}{2k}} \geq k.$$

□

When does  $G_{n,p}$  have triangles?

If  $X = \# \text{triangles}$  then

$$\mathbb{E}[X] = \sum_{\text{Triangle } T \in K_n} E[I_T] = \binom{n}{3} p^3 \sim n^3 p^3 / 6 = O(1)$$

if  $p = O\left(\frac{1}{n}\right)$

Is  $G_{n,p}$  connected for  $p = \frac{c}{n}$ ?

Let  $X = \# \text{spanning trees of } G_{n,p}$  then

$$\mathbb{E}[X] = \sum_{T \in G_{n,p}} E(I_T) = n^{n-2} p^{n-1} = n^{n-2} \frac{c^{n-1}}{n^{n-1}} = \frac{c^{n-1}}{n} \rightarrow \infty.$$



Let  $Y = \#\text{isolated vertices}$  then

$$\mathbb{E}[Y] = \sum_{v \in V} \mathbb{P}(v \text{ isolated}) = n(1-p)^{n-1} \approx ne^{-p(n-1)} \approx ne^{-c}$$

For  $p = O\left(\frac{1}{n}\right)$ , let  $X = \#\text{triangles}$ . Then

$$\mathbb{E}[X] = \binom{n}{3} p^3 \rightarrow 0.$$

So  $\mathbb{P}(G_{n,p} \text{ having triangles}) \rightarrow 0$ .

**Theorem 3.17.** *Threshold of  $\mathcal{H}$  in  $G_{n,p}$ .*

*Consider  $G_{n,p}$  with  $p = p(n)$  and  $\mathcal{H}$  is fixed graph with  $k$  vertices and  $l$  edges.*

*Define  $\epsilon = \epsilon(\mathcal{H}) = \frac{l}{k}$  and  $\epsilon' = \epsilon'(\mathcal{H}) = \max_{J \subseteq \mathcal{H}} \epsilon(J)$ . If  $p^\epsilon \cdot n \rightarrow 0$  then  $\mathbb{E}[\#\mathcal{H} \text{ in } G_{n,p}] \rightarrow 0$ .*

*Proof.*  $\mathbb{E}[\#\mathcal{H} \in G_{n,p}] \leq \binom{n}{k} h p^l \leq C(n p^\epsilon)^k$  where  $h = \frac{k!}{\text{Aut}(\mathcal{H})}$

If  $p^{\epsilon'} n \rightarrow 0$ , there is some argument for densest subgraph  $J$ . □

*Now to show the other side, if  $p^{\epsilon'} n \rightarrow \infty$  (if  $p = \omega\left(\frac{1}{n^{1/\epsilon'}}\right)$  then  $G_{n,p}$  has  $\mathcal{H}$  as a subgraph with high probability.*

*Proof.* Let  $X = \#\mathcal{H}$  subgraph in  $G_{n,p}$  then by Chebyshev,

$$\mathbb{P}[X \leq 0] \leq \frac{\text{Var}[X]}{\mathbb{E}[X]^2}.$$

We can compute

$$\mathbb{E}[X^2] = \sum_{H_1, H_2 \in \mathcal{H}} \mathbb{P}[H_1, H_2 \subseteq G_{n,p}] = \sum_{t=0}^k \sum_{|H_1 \cap H_2|=t} \mathbb{P}(H_1, H_2 \subseteq G_{n,p})$$

For  $t = 0$  we have

$$\sum_{|H_1 \cap H_2|=0} \mathbb{P}(H_1 \subseteq G_{n,p}) \mathbb{P}(H_2 \subseteq G_{n,p}) \leq \mathbb{E}[X]^2$$

So

$$\mathbb{E}[X^2] - \mathbb{E}[X]^2 \leq \sum_{t=1}^k \sum_{|H_1 \cap H_2|=t} \mathbb{P}(H_1, H_2 \subseteq G) = \sum_{t=1}^k \sum_{|H_1 \cap H_2|=t} \binom{k}{t} \binom{n-k}{k-t} h p^{e(H_1 \cup H_2)}$$

By PIE,  $e(H_1 \cup H_2) \geq 2l - \epsilon' t$  since  $e(H_1 \cap H_2) \leq \epsilon' t$  as  $H_1 \cap H_2$  is a subgraph of  $H_1$

$$\begin{aligned} \sum_{t=1}^k \sum_{|H_1 \cap H_2|=t} \binom{k}{t} \binom{n-k}{k-t} h p^{e(H_1 \cup H_2)} &\leq \sum_{t=1}^k \sum_{|H_1 \cap H_2|=t} \binom{k}{t} \binom{n-k}{k-t} h p^{2l - \epsilon' t} \\ &= \sum_{t=1}^k \sum_{|H_1 \cap H_2|=t} \binom{n}{k} h \cdot h \binom{n-k}{k-t} p^{l - \epsilon' t} \\ &\quad (\sum_{H \in \mathcal{H}} p^l = \mathbb{E}[X] = \binom{n}{k} \cdot h \cdot p^l) \\ &\leq \mathbb{E}[X] \sum_{t=1}^k h \binom{k}{t} \binom{n-k}{k-t} p^{l - \epsilon' t} \\ &\leq \mathbb{E}[X] \sum_{t=1}^k h \cdot C \cdot n^k \cdot \frac{1}{n^t} \cdot p^{l - \epsilon' t} \\ &\leq \mathbb{E}[X] \sum_{t=1}^k C' \cdot h \cdot \binom{n}{k} \cdot p^l \cdot \frac{1}{(n p^{\epsilon'})^t} \\ &= \mathbb{E}[X]^2 \sum_{t=1}^k C' \left( \frac{1}{n p^{\epsilon'}} \right)^t \rightarrow 0 \end{aligned}$$

□

**Theorem 3.18. Chernoff Bound**

Suppose you had independent random values  $\zeta_1, \dots, \zeta_n$  with  $\zeta_i \in \{-1, 1\} \forall i$  and  $\mathbb{P}(\zeta_i = 1) = \mathbb{P}(\zeta_i = -1) = \frac{1}{2}$ .

Let  $X = \sum_{i=1}^n \zeta_i$

$$\begin{aligned}
 \mathbb{P}(X > a) &= \mathbb{P}(e^{tX} > e^{ta}) \\
 &\leq \frac{\mathbb{E}(e^{tX})}{e^{ta}} \\
 &= \frac{\mathbb{E}(e^{t \sum \zeta_i})}{e^{ta}} \\
 &= \frac{\prod_{i=1}^n \mathbb{E}[e^{t\zeta_i}]}{e^{ta}} \\
 &= \frac{\left(\frac{e^t + e^{-t}}{2}\right)^n}{e^{ta}} \\
 &\leq e^{nt^2/2 - ta} \\
 &= e^{a^2/2n - a^2/n} \quad (\text{for } t = \frac{a}{n}) \\
 &= e^{-\frac{a^2}{2n}}
 \end{aligned}$$

**Question:** How many vectors can I have in  $\mathbb{R}^d$  all at a common pairwise angle.

Equivalently,  $\exists \alpha, v_i \cdot v_j = \begin{cases} \alpha & \text{if } i \neq j \\ 1 & \text{otherwise} \end{cases}$

Let  $V = \begin{bmatrix} | & | & \cdots & | \\ v_1 & v_2 & \cdots & v_m \\ | & | & \cdots & | \end{bmatrix}$

Then  $V^T V = G = \begin{bmatrix} v_1 \cdot v_1 & v_1 \cdot v_2 & \cdots & v_1 \cdot v_m \\ \vdots & v_2 \cdot v_2 & \cdots & \\ \vdots & \vdots & \ddots & \end{bmatrix}$

Claim:  $\text{Rank}(G) \leq d$ .

For each  $\vec{x} \in \text{Ker}(V) \implies V\vec{x} = 0 \implies V^T V\vec{x} = 0 \implies G\vec{x} = 0$

We know  $\text{Rank}(V) \leq d$  so  $\text{Rank}(G) = \text{Rank}(V^T V) \leq d$ .

We can write  $G = \alpha J_m + (1-\alpha)I_m$  then  $J_m$  has eigenvalues  $m$  with multiplicity at least 1 and eigenvectors with multiplicity  $\geq m-1$ .

$$\begin{bmatrix} 1 \\ -1 \\ 0 \\ \vdots \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ -1 \\ \vdots \end{bmatrix} \cdots \begin{bmatrix} 1 \\ 0 \\ \vdots \\ -1 \end{bmatrix}$$

If  $\vec{x}$  is an eigenvector of  $J_m$  with eigenvalue  $\lambda$  then  $G\vec{x} = \alpha\lambda x + (1-\alpha)x = (\alpha\lambda + 1 - \alpha)x$ .

$G$  has eigenvalues  $1 - \alpha$  with multiplicity at least  $m-1$ .

So  $\text{Rank}(G) \geq m-1$  and consequently  $d \geq m-1$ .

**Question:** How many unit vectors  $v_1, \dots, v_n$  can I have in  $\mathbb{R}^d$  with all pairs approx equal angle.

Equivalently,  $\exists \alpha$  such that  $(*) v_i \cdot v_j \in (\alpha - \epsilon, \alpha + \epsilon)$  if  $i \neq j$  and 1 if  $i = j$ .

**Theorem 3.19.**  $\forall \epsilon \in (0, 1)$ , there is a  $c > 0$  such that for all sufficiently large  $d$  there is a collection  $v_1, \dots, v_m \in \mathbb{R}^d$  of vectors satisfying  $(*)$  with  $m \geq 2^{cd}$

Consider the easier problem when  $\alpha = 0$ . Choose  $m$  vectors  $v_i \in \{1, -1\}^d$  at random with  $\mathbb{P}(v_i^j = +1) = \mathbb{P}(v_i^j = -1) = \frac{1}{2}$ . We know  $v_i \cdot v_i = n$  then let  $u_i = \frac{v_i}{\sqrt{n}}$ . Then  $\mathbb{E}(u_i \cdot u_v) = 0$  as  $\zeta_{i,j,k} =$

$$\begin{cases} 1 & \text{if } v_i^k \cdot v_j^k = 1 \\ -1 & \text{if } v_i^k \cdot v_j^k = -1 \end{cases} \text{ By Chernoff,}$$

$$\mathbb{P}(v_i \cdot v_j \notin (-\epsilon n, \epsilon n)) \leq 2e^{-\epsilon^2 n/2}$$

$$\mathbb{P}(\exists i, j \text{ s.t. } u_i \cdot u_j \notin (-\epsilon n, \epsilon n)) \leq \binom{m}{2} 2e^{-\epsilon^2 n/2} \leq m^2 e^{-\epsilon^2 n/2} = m^2 \beta^{-n}$$

**Theorem 3.20.** If  $\zeta_1, \zeta_2, \dots, \zeta_n$  are independent random variables with  $\mathbb{E}(\zeta_i) = 0, |\zeta_i| \leq 1, X = \sum \zeta_i$  then

$$\mathbb{P}(X \geq a) \leq e^{-\frac{a^2}{2n}}$$

**Question:** I flip biased coins with head prob =  $\frac{1}{3}$  n times. Bound the probability # head  $\geq \frac{n}{2}$ .

Define  $\zeta_i = \begin{cases} 1 & \text{if head} \\ \frac{-p}{1-p} & \text{otherwise} \end{cases}$  (Subtract expected value and dividing by  $1-p$ ) Then  $\mathbb{E}[\zeta_i] = 0, |\zeta_i| \leq 1$  for  $p < \frac{1}{2}$ .

Let  $X = h + (n-h)\frac{-p}{1-p}$

**Theorem 3.21.** For random variables  $X, Y$

$$\begin{aligned} \mathbb{E}[XY] &= \sum_{x,y} xy \mathbb{P}(X=x, Y=y) \\ &= \sum_{x,y} xy \mathbb{P}(Y=y) \mathbb{P}(X=x|Y=y) \\ &= \sum_y y \mathbb{P}(Y=y) \sum_x x \mathbb{P}(X=x|Y=y) \\ &= \mathbb{E}(Y \mathbb{E}(X|Y)) \end{aligned}$$

**Theorem 3.22.** Let  $X$  be a random variable and  $A$  an event then

$$\mathbb{E}(X|A) = \frac{1}{\mathbb{P}(A)} \sum_{w \in A} p(w) \mathcal{X}(w)$$

**Theorem 3.23.** Let  $\zeta_1, \dots, \zeta_n$  be random variable with  $\mathbb{E}(\zeta_i) = 0$  and  $|\zeta_i| \leq 1$ .

$$\mathbb{E}(e^{t \sum \zeta_i}) \leq \left( \frac{e^t + e^{-t}}{2} \right)^n$$

*Proof.*

$$\mathbb{E}(e^{t \sum \zeta_i}) = \mathbb{E} \left( \prod_{i=1}^n e^{t \zeta_i} \right) = \mathbb{E} \left( \prod_{i=1}^{n-1} e^{t \zeta_i} \mathbb{E} \left( e^{t \zeta_n} \mid \prod_{i=1}^{n-1} e^{t \zeta_i} \right) \right)$$

We know want to upper bound  $\mathbb{E} \left( e^{t \zeta_n} \mid \prod_{i=1}^{n-1} e^{t \zeta_i} \right)$ .

By convexity,  $e^{t \zeta_i} \leq h(\zeta_i) = \frac{1}{2} [(1 - \zeta_i)e^{-t} + (1 + \zeta_i)e^t] \implies \mathbb{E}[e^{t \zeta_i}] \leq \frac{e^t + e^{-t}}{2}$

$$\mathbb{E} \left( e^{t \zeta_n} \mid \prod_{i=1}^{n-1} e^{t \zeta_i} \right) \leq \left( \frac{e^t + e^{-t}}{2} \right) \mathbb{E} \left( \prod_{i=1}^{n-1} e^{t \zeta_i} \right) \leq \left( \frac{e^t + e^{-t}}{2} \right)^n$$

□

**Definition 3.24.** Random variables  $X_0, X_1, \dots$  is a martingale if it satisfies the following properties

1.  $\mathbb{E}[|X_i|] < \infty$
2.  $\mathbb{E}[X_{i+1} | X_1, \dots, X_i] = X_i$

**Theorem 3.25.** *Azuma's Theorem: If  $X_0, X_1, \dots$  is martingale and  $|X_{i+1} - X_i| \leq 1$  then*

$$\mathbb{P}(X_n - X_0 \geq \lambda\sqrt{n}) \leq e^{-\lambda^2/2}$$

*Proof.* By Markov's Inequality we have

$$\mathbb{P}(X_n - X_0 \geq \lambda\sqrt{n}) \leq \frac{\mathbb{E}[e^{t(X_n - X_0)}]}{e^{t\lambda\sqrt{n}}}$$

We can telescope the numerator as

$$\begin{aligned} \mathbb{E}[e^{t(X_n - X_0)}] &= \mathbb{E}\left[\prod_{k=1}^n e^{t(X_k - X_{k-1})}\right] \\ &= \mathbb{E}\left[\mathbb{E}\left[e^{t(X_n - X_{n-1})} | X_0, X_1, X_2, \dots, X_{n-1}\right] \prod_{k=1}^{n-1} e^{t(X_k - X_{k-1})}\right] \end{aligned}$$

By Theorem 3.23 we have  $\mathbb{E}[e^{t(X_n - X_{n-1})} | X_1, X_2, \dots, X_{n-1}] \leq e^{t^2/2}$  so

$$\mathbb{E}\left[\mathbb{E}\left[e^{t(X_n - X_{n-1})} | X_0, X_1, X_2, \dots, X_{n-1}\right] \prod_{k=1}^n e^{t(X_k - X_{k-1})}\right] \leq e^{nt^2/2}$$

So

$$\mathbb{P}(X_n - X_0 \geq \lambda\sqrt{n}) \leq e^{nt^2/2 - t\lambda\sqrt{n}}.$$

The RHS achieves it's max at  $t = \frac{\lambda}{\sqrt{n}}$ . Thus

$$\mathbb{P}(X_n - X_0 \geq \lambda\sqrt{n}) \leq e^{-\lambda^2/2}$$

□

**Definition 3.26.** *Doob's Martingale: Let  $X$  and  $Y_1, Y_2, \dots$  be random variables with  $\mathbb{E}[|Y_i|] < \infty$ . Define  $X_i := \mathbb{E}(X | Y_1, \dots, Y_i)$  for  $i \geq 1$ . with  $X_0 = \mathbb{E}[X]$*

**Theorem 3.27.** *McDiarmid's Inequality: Let  $f : \mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n \rightarrow \mathbb{R}$  that is 1-lipschitz. If  $Y_1, Y_2, \dots, Y_n$  are independent random variables where  $Y_i \in \mathcal{Y}_i$ . For  $X := f(Y_1, \dots, Y_n)$  satisfies*

$$\mathbb{P}(X - \mathbb{E}(X) \geq \lambda\sqrt{n}) \leq e^{-2\lambda^2}.$$

**Example 3.28.** *For  $m$  balls into  $n$  bins, let  $X = \#$  empty bins then*

$$\mathbb{E}[X] = n \left(1 - \frac{1}{n}\right)^m \approx ne^{-\alpha}$$

where  $m = \alpha n$ . If we let  $Y_i = \text{pos of ball } i$  then  $f(Y_1, \dots, Y_m) = \#$  empty bins. So  $\mathbb{P}(X \geq \mathbb{E}[X] + \lambda\sqrt{n}) \leq e^{-2\lambda^2}$

**Theorem 3.29.**

$$\mathbb{P}(A | B \cap C) = \frac{\mathbb{P}(A \cap B | C)}{\mathbb{P}(B | C)}$$

**Theorem 3.30.** *Lovasz Local Lemma: Given a collection  $\mathcal{B} = \{B_1, B_2, \dots, B_n\}$  of bad events. If  $B_1, \dots, B_n$  have a dependency graph of max degree  $d$  and  $4pd \leq 1$  where  $\mathbb{P}(B_i) \leq p$  then*

$$\mathbb{P}\left(\bigcap \overline{B_i}\right) > 0.$$

*Proof.* We'll prove the statement by induction on  $k = |S|$  for  $S \subseteq [n]$ . Assume  $4pd \leq 1$  then we want to show  $\forall i, \mathbb{P}\left(B_i | \bigcap_{j \in S} \overline{B_j}\right) \leq 2p$ .

Let  $S = T \cup U$  where  $T = \{j \in S | j \sim i\}$ .

$$\begin{aligned} \mathbb{P}\left(B_i | \bigcap_{j \in T} \overline{B_j} \cap \bigcap_{j \in U} \overline{B_j}\right) &= \frac{\mathbb{P}\left(B_i \cap \bigcap_{j \in T} \overline{B_j} | \bigcap_{j \in U} \overline{B_j}\right)}{\mathbb{P}\left(\bigcap_{j \in T} \overline{B_j} | \bigcap_{j \in U} \overline{B_j}\right)} \\ &\leq \frac{p}{1 - \mathbb{P}\left(\bigcup_{j \in T} B_j | \bigcap_{j \in U} \overline{B_j}\right)} \\ &\leq \frac{p}{1 - \sum_{j \in T} \mathbb{P}(B_j | \bigcap_{k \in U} \overline{B_k})} \\ &\leq \frac{p}{1 - 2dp} \quad (\text{Induction Hypothesis}) \\ &\leq 2p \quad (\text{Assumption}) \end{aligned}$$

We're done with the induction.

Then

$$\mathbb{P}\left(\bigcap_{i=1}^n \overline{B_i}\right) = \mathbb{P}\left(\overline{B_n} | \bigcap_{i=1}^{n-1} \overline{B_i}\right) \cdot \mathbb{P}\left(\bigcap_{i=1}^{n-1} \overline{B_i}\right) \geq \frac{(1-2p)^n}{p} > 0$$

□

**Theorem 3.31. Local Lemma (General Version)** Suppose  $\mathcal{B}$  is a collection of "bad" events with some dependency graph. Suppose we can assign real number  $0 < X_A < 1$  to each  $A \in \mathcal{B}$  such that

$$\mathbb{P}(A) \leq X_A \prod_{B \sim A} (1 - X_B).$$

Then

$$\mathbb{P}\left(\bigcap_{B \in \mathcal{B}} \overline{B}\right) \geq \prod_{B \in \mathcal{B}} (1 - X_B) > 0$$

*Proof.* We can prove it by induction on  $|S|$  that if  $B_1, \dots, B_t, B_{t+1}, \dots, B_S \in \mathcal{B}$  such that  $A \sim B_1, \dots, B_t$  and  $A \not\sim B_{t+1}, \dots, B_S$  to show

$$\mathbb{P}\left(A \mid \bigcap_{i=1}^S \overline{B_i}\right) \leq X_A$$

We have

$$\begin{aligned} \mathbb{P}\left(A \mid \bigcap_{i=1}^t \overline{B_i} \cap \bigcap_{i=t+1}^S \overline{B_i}\right) &= \frac{\mathbb{P}\left(A \cap \bigcap_{i=1}^t \overline{B_i} \mid \bigcap_{i=t+1}^S \overline{B_i}\right)}{\mathbb{P}\left(\bigcap_{i=1}^t \overline{B_i} \mid \bigcap_{i=t+1}^S \overline{B_i}\right)} \\ &\leq \frac{\mathbb{P}\left(A \mid \bigcap_{i=t+1}^S \overline{B_i}\right)}{\mathbb{P}\left(\bigcap_{i=1}^t \overline{B_i} \mid \bigcap_{i=t+1}^S \overline{B_i}\right)} \\ &\leq \frac{X_A \prod_{B \sim A} (1 - X_B)}{\prod_{i=1}^t (1 - X_{B_i})} \\ &\leq X_A \end{aligned}$$

Thus we're done with induction. Using the statement

$$\mathbb{P}\left(\bigcap_{i=1}^S \overline{B_i}\right) = \mathbb{P}(\overline{B_1} \mid \overline{B_2}) \times \dots \times \mathbb{P}\left(\overline{B_n} \mid \bigcap_{i=1}^S \overline{B_i}\right) \geq \prod_{i=1}^n (1 - X_{B_i}) > 0$$

□

**Theorem 3.32. Axel's Theorem:**

$\forall \epsilon > N_\epsilon$  and an infinite binary sequence such that  $\forall n > N_\epsilon$ , any 2 consecutive block of length  $n$  differ in  $\geq (\frac{1}{2} - \epsilon)n$  places.

*Proof.* Let the bad events be  $B_{i,n}$  where for each  $i$ , intervals  $[i, \dots, i+n], [i+n+1, \dots, i+2n]$  differ by less than  $(\frac{1}{2} - \epsilon)n$

Let  $X = \#$  places where they differ then  $\mathbb{E}[X] = \frac{n}{2}$ .

By Chernoff-Hoeffding's Lemma we have

$$\mathbb{P}(X - \mathbb{E}[X] \geq -\epsilon n) = \mathbb{P}(X \geq n/2 - \epsilon n) \leq e^{-2\epsilon^2 n} \leq e^{-\epsilon^2 n/10}$$

Let  $X_{B_{i_0, n}} = e^{-\epsilon^2 n/20} \cdot \frac{1}{n^3}$  then fix  $B_{i_0, n_0}$  then we have

$$X_{B_{i_0, n_0}} = e^{-\epsilon^2 n_0/20} \cdot \frac{1}{n_0^3}$$

$$e^{-\epsilon^2 n_0/20} \cdot \frac{1}{n_0^3} \prod_{n=N_\epsilon}^T \prod_{i=i_0-2n}^{i_0+2n} \left(1 - e^{-\epsilon^2 n/20} \cdot \frac{1}{n^3}\right)^{2n+2n_0} \geq$$

□

From Homework #3

**Theorem 3.33.**  $\forall \epsilon > 0, \exists N_\epsilon, \forall T, \exists$  a binary sequence of length  $T$  such that  
 (\*)  $\forall n > N_\epsilon$  identical blocks of length  $n$  are separated by distance  $\geq (2 - \epsilon)^n$

**Theorem 3.34.** *Konig's Infinity Lemma:* Let  $G$  be a connected, locally finite, infinite graph then  $G$  contains an infinite path.

**Theorem 3.35.**  $\forall \epsilon > 0, \exists N_\epsilon, \forall T, \exists$  an infinite binary sequence such that vertices of my tree are finite binary sequences with property (\*).

Let  $\mathcal{T}$  be a complete tree of all binary sequences with all vertices and join  $S \rightarrow S'$  if  $S$  can be obtained from  $S'$  by removing last digit of  $S'$ .

We want to show  $\mathcal{T}$  is locally finite and infinite. It is locally finite as each node has at most 2 children. It is infinite because for any string that satisfy (\*), any of its prefix has to satisfy (\*). By Theorem 3.34, there must be an infinite path with property (\*)

## 4 Topology

**Definition 4.1.** A topology is a set  $X$  and a collection  $\mathcal{O}$  of open sets satisfying

1.  $\emptyset \in \mathcal{O}, X \in \mathcal{O}$
2.  $\mathcal{O}$  is closed under finite intersection
3.  $\mathcal{O}$  is closed under arbitrary union

A collection of basic open sets are closed under finite intersections.

**Definition 4.2.**  $X$  is compact if every cover has a finite subcover

**Definition 4.3.** Product topogy is

$$\prod_{\alpha \in A} \mathcal{O}_\alpha$$

where  $\mathcal{O}_\alpha \subseteq X_\alpha$  is open and  $\mathcal{O}_\alpha = X_\alpha$  except for finitely many.

**Theorem 4.4.** If  $X_\alpha$  where  $\alpha \in I$  are compact topological spaces then  $\prod_{\alpha \in I} X_\alpha$  is compact.

## 5 Ramsey Numbers

**Definition 5.1.** Ramsey number  $R(k, l) = \min_{n \geq 1} \{K_n \text{ contains a red } K_k \text{ or blue } K_l\}$   
 We can see  $R(3, 3) = 6$

**Theorem 5.2.**  $R(k, l) \leq R(k - 1, l) + R(k, l - 1)$

*Proof.* Let  $n \geq R(k - 1, l) + R(k, l - 1)$  and consider a red/blue coloring of  $K_n$ . Fix  $v_0$ . Since  $v_0$  has  $\geq R(k - 1, l) + R(k, l - 1) - 1$  edges,

(Case 1) If  $v_0$  has  $\geq R(k - 1, l)$  red edges then the induced subgraph of the neighbors,  $G'$  must have red  $K_{k-1}$  or blue  $K_l$ . If red  $K_{k-1}$  then  $G' \cup v_0$  is a  $K_k$ , otherwise we have blue  $K_l$ .

(Case 2) If  $v_0$  has  $\geq R(k, l - 1)$  blue neighbors then same argument as case 1.

Thus we're done □



**Theorem 5.3.**  $R(k, k) > (1 - O(1)) \frac{k}{e\sqrt{2}} 2^{k/2}$

*Proof.* Flip fair coins to color a  $K_n$  red or blue. Let  $X = \#$  monotonic  $K_k$  then

$$\mathbb{E}[X] = \binom{n}{k} 2^{1 - \binom{k}{2}} \leq \left(\frac{en}{k}\right)^k \cdot 2 \cdot 2^{-k(k-1)/2}$$

If  $\mathbb{E}[X] < 1$  then  $R(k, k) > n$ .

$$2^{1/k} \left(\frac{en}{k}\right) 2^{(k-1)/2} < 1$$

Thus

$$n < (1 - O(1)) \frac{k}{e\sqrt{2}} 2^{k/2}$$

Consequently,  $R(k, k) > (1 - O(1)) \frac{k}{e\sqrt{2}} 2^{k/2}$  □

**Theorem 5.4.** *Alterations: Color edges of  $K_n$  randomly red or blue. Delete an vertex from each monochromatic  $K_k$ . Let  $X = n - \#$  monochromatic cliques.*

$$\begin{aligned} \mathbb{E}[X] &= n - \binom{n}{k} 2^{1 - \binom{k}{2}} \\ &\geq n - \left(\frac{en}{k}\right)^k \cdot 2 \cdot 2^{-k(k+1)/2} \\ &= n - 2 \left(\frac{en}{k} \cdot 2^{\frac{-k-1}{2}}\right) \end{aligned}$$

Let  $n = \frac{k}{e} \cdot 2^{k/2}$  then

$$\frac{k}{e} \cdot 2^{k/2} - 2^{k/2} = (1 - o(1)) \cdot \frac{k}{e} \cdot 2^{k/2}$$

**Theorem 5.5.** *Using Lovasc Local Lemma: Given  $k$ , fix  $n$ , randomly red/blue color edges.*

*Proof.* Bad events:  $B_k$  for  $k \in \mathcal{K}$  where  $\mathcal{K}$  is the collection of  $k$ -clique.

Then  $\mathbb{P}(B_k) = 2^{1 - \binom{n}{k}}$ .

If  $K_1, K_2$  share any edges, set  $B_{K_1} \sim B_{K_2}$  in dependency graph. Then

$$D \leq \binom{k}{2} \binom{n}{k-2}$$

Consequently

$$\begin{aligned} epD &\leq e \cdot 2^{1 - \binom{n}{k}} \left( 2 \binom{k}{2} \binom{n}{k-2} \right) < 1 \\ 4e \left( \left( \frac{en}{k-2} \right)^{k-2} \binom{k}{2} \right) &< 2 \binom{k}{2} \\ \left( 2e \binom{k}{2} \right)^{\frac{1}{k-2}} \cdot \frac{en}{k-2} &< 2 \binom{k}{2}^{-\frac{1}{k-2}} = 2^{\frac{k+1}{2}} \\ (1 + o(1)) \frac{en}{k-2} &< 2^{\frac{k+1}{2}} \end{aligned}$$

So

$$n < (1 - o(1)) \frac{k\sqrt{2}}{e} 2^{k/2}$$

Thus  $R(k) > (1 - o(1)) \frac{k\sqrt{2}}{e} 2^{k/2}$  □

**Definition 5.6.** Define  $K_k^j$  as the complete  $j$  uniform hypergraph on  $n$  vertices with  $k$  vertices

**Definition 5.7.** Define  $R_j(k) = \text{minimum } n \text{ such that any red/blue coloring of } \binom{[n]}{j} \text{ has a monochromatic } K_k^j$

**Theorem 5.8.**  $R_r(k, l) \leq R_{r-1}(R_r(k-1, l), R_r(k, l-1))$

*Proof.* Let  $N = R_{r-1}(R_r(k-1, l), R_r(k, l-1)) + 1$  and fix  $v$ . There are  $N + 1$  other vertices,  $Y$ . Each edge containing  $v$  includes an  $r-1$  edge in  $Y$ . Let it inherit the color of the  $r$  edges.  
(Case 1) We have  $R_r(k-1, l)$  vertices in  $Y$  such that all  $r-1$  subsets are red. (Case 1A)  $\square$

Let  $C(k) = \text{minimum } n \text{ such that } \forall X \subseteq \mathbb{R}^2 \text{ such that } |X| = n \text{ and } X \text{ has a subset } S \text{ where } |S| = k \text{ and } S \text{ is in convex position.}$

Then  $C(1) = 1, C(2) = 2, C(3) = 3, C(4) = 5, C(5) = 9, \dots$

**Theorem 5.9.**  $C(k) \leq R_4(5, k)$

**Lemma:** If  $S \subseteq \mathbb{R}^2$  is  $k$ -points in general position such that any 4 of them are in convex position, then they all are. (Easy to see by triangulation)

Given a set  $F$  of four points color  $F$  color  $F$  red if not in convex position and blue otherwise.

Note:  $K_k^n$  is a complete  $k$ -uniform hypergraph on  $n$  vertices.

A red  $K_4^5$  is impossible as  $C(4) \leq 5$ . Since we can find a blue  $K_4^k$  and we win by lemma.

Color 3-tuples according to whether "sorted slopes" are increasing or decreasing. If  $n \geq R_3(k, k)$ , I can find  $k$  vertices all of whose 3 tuples are caps or all 3 tuples are cups.

**Definition 5.10.** Let  $CC(k, l) = \min n$  such that any  $n$  pts in general position, no two have same  $x$  coordinate, have a  $k$ -cup or an  $l$ -cap.

**Theorem 5.11.** Erdos Szekeres:  $CC(k, l) = \binom{k+l-4}{k-2} + 1$

*Proof.* I have  $k$ -cup or a  $l$ -cup. We'll show it by induction on  $k+l$ . Assume no  $l$ -cap. I do have a  $(k-1)$ -cup or  $l$  cup by induction. If I delete the last point of each  $(k-1)$ -cup. Then only  $\binom{k+l-5}{k-3}$  points remain. So I deleted  $\binom{k+l-4}{k-2} + 1 - \binom{k+l-5}{k-2} + 1$ .  $\square$

**Theorem 5.12.** For all positive integers  $k$  and  $r$ , there exists  $N$  such that any  $r$ -coloring of the numbers  $1, 2, \dots, N$  has a monochromatic  $k$ -term arithmetic progression.

**Theorem 5.13.** If  $\mathbb{N}$  is partitioned into 2 sets, one contains arbitrary long arithmetic progression.  
**Statement 1:**  $\forall k, \exists N$  such that any 2 coloring of  $[N]$  has a monochromatic  $k$ -term arithmetic progression. If such a statement is false for  $k_0$ , then for all  $n$  there is a coloring of  $[n]$  with no  $k_0$  arithmetic progression. With Konig's Lemma there exists a coloring of  $\mathbb{N}$  with no  $k_0$ -term arithmetic progression.

Statement 1 implies

**Statement 2**  $\forall r, \forall k, \exists W(k, r)$  such that any  $r$ -coloring of  $[N]$  for  $N \geq W(k, r)$  admits a  $k$ -term monochromatic A.P.

Some values of  $W(k, r)$  are  $W(k, 1) = k$ ,  $W(2, r) = r + 1$ ,  $W(2, 2) = 3$  and  $W(3, 2) = 9$ .

**Theorem 5.14.**  $W(3, 2) \leq 325$

*Note: The technique used here can be used for the general case.*

*Proof.* Consider 65 blocks of 5 spots each. Within the first 33 blocks, there must be 2 blocks of the same coloring. Let the blocks be  $b_1, b_2 \in [33]$ . Of the first block consider the first 3 spots then if it's same color then we're done, WLOG for  $a_1, a_2 \in [3]$  with  $a_1 < a_2$  say  $5b_1 + a_1, 5b_1 + a_2$  be red. Let  $a_3 = 2a_2 - a_1 \in [5]$ . If  $7b_1 + a_3$  is red then we're done as  $7b_1 + a_1, 7b_1 + a_2, 7b_1 + a_3$  is a mono A.P. So say  $7b_1 + a_3$  is blue.

Since  $b_2$  is the same coloring then let  $b_3 = 2b_2 - b_1 \in [65]$ . If  $7b_3 + a_3$  is red then we have  $7b_1 + a_1, 7b_2 + a_2, 7b_3 + a_3$ . Otherwise if blue we have  $7b_1 + a_3, 7b_2 + a_3, 7b_3 + a_3$ .

Thus we're done and  $W(3, 2) \geq 65 \cdot 5 = 325$   $\square$

**Definition 5.15.**  $WF(k, l, r) = \text{minimum } N \text{ such that any } r\text{-coloring of } [N] \text{ admits } l \text{ color focused } k\text{-term A.P. or a } k+1 \text{ term A.P.}$

**Theorem 5.16.**

$$WF(2, 2, r) \leq (2r^{2r+1} + 1)(2r + 1)$$

$$WF(2, 3, r) \leq (2r^{2r^{2r+1}+1} + 1)(2r^{2r+1} + 1)(2r + 1)$$

**Definition 5.17.** *Hales-Jewett:*  $\forall r, \forall n, \exists d$  such that in any  $r$ -coloring of  $[n]^d$  hypercube, there is a monochromatic line.

**Definition 5.18.** A combinatorial line is a set of points represented by a string in  $([n] \cup \{x\})^d \setminus [n]^d$ . The points of the line are obtained by substituting  $x = 1, 2, \dots, n$ .

**Definition 5.19.** A geometric line  $([n] \cup \{x, \bar{x}\})^d \setminus [n]^d$  obtained by substituting in  $x = 1, \dots, n$  and  $\bar{x} = n - x + 1$ .

Given an A.P-free coloring of  $[N]$  want to give a line free coloring of  $[N]^d$ . Define  $\phi : [n]^d \rightarrow (n-1)d$  by  $\phi(a_0, a_1, \dots, a_{d-1}) = a_0 + a_1 + \dots + a_{d-1}$ . Then we have

$$HJ(2, r) \leq d \iff 2^d < r \iff HJ(2, r) \leq \log_2 r$$

$HJ^c(2, r) = r$  as if we take any of  $(0, \dots, 0), (1, 0, \dots, 0), \dots$  there are  $d+1 > r \implies$  a monochromatic combinatorial line.

For  $HJ(3, 2)$ , take  $p \in [3]^d$

## Additive Combinatorics

**Definition 5.20.**

$$A + A = \{a + a' | a, a' \in A\}$$

$$A \cdot A = \{a \cdot a' | a, a' \in A\}$$

**Theorem 5.21.**  $\max(|A + A|, |A \cdot A|) \geq |A|^{1+\epsilon}$

Suppose we have a set  $A$ ,  $X = A + A, Y = A \cdot A$ . Let  $\mathcal{P} = X \times Y = (A + A) \times (A \cdot A)$ . Let  $\mathcal{L} = \{\{y | y = a(x - a')\} | a, a' \in A\}$ . Then  $|\mathcal{L}| = |A|^2$ .

Define  $i(\mathcal{L}, \mathcal{P})$  to be the number of incidences between the points and lines in  $\mathcal{P}$  and  $\mathcal{L}$ .

For any line containing  $a, a' \in A$ , the equation is  $y = a(x - a')$ . For a point  $p = (a' + a'', a \cdot a'')$  we have  $a' + a'' \in A + A$  and  $a \cdot a'' \in A \cdot A$ .

$$i(\mathcal{L}, \mathcal{P}) \geq |\mathcal{L}| \cdot |A| = |A|^3$$

Then

$$i(\mathcal{L}, \mathcal{P}) = O(|\mathcal{L}|^{2/3}|\mathcal{P}|^{2/3} + |\mathcal{L}| + |\mathcal{P}|).$$

So  $|A|^3 \leq i(\mathcal{L}, \mathcal{P}) \leq C(|A|^{4/3}(|A + A| \cdot |A \cdot A|^{2/3})$  as  $|\mathcal{L}| + |\mathcal{P}| = O(|\mathcal{L}|^{2/3}|\mathcal{P}|^{2/3})$ . We also have  $|A|^2 \leq |\mathcal{P}| \leq |A|^4$  and  $|\mathcal{P}|^{1/2} \leq |\mathcal{L}| \leq |\mathcal{P}|$ . So  $C|A|^{5/2} \leq |A \cdot A||A + A|$  and consequently

$$\max(|A + A|, |A \cdot A|) \geq \epsilon|A|^{5/4}$$

## Planar Graphs

**Theorem 5.22.** *Euler's Formula for Planar Graphs:*

$$|V| - |E| + |F| = 2$$

**Theorem 5.23.** *Suppose  $G$  is a connected planar graph with  $m \geq 3$ . Then*

$$m \leq 3n - 6$$

*Proof.* Consider the bipartite graph of  $E(G)$  and  $|F(G)|$ . For each edge there is at most 2 faces and each face is closed by at least 3 edges. So

$$2|E| \leq \sum \deg(e) = \sum \deg(f) \geq |F| \cdot 3$$

$$\text{So } n - m + f = 2 \implies n - m + \frac{2}{3}m \geq 2 \implies n - \frac{1}{3}m \geq 2 \quad \square$$

**Definition 5.24.** *Let  $Cr(G)$  is the minimum number of crossing in any drawing.*

Given  $G$ , if  $e(G) \geq 3n$ ,  $G$  is not planar  $Cr(G) \geq m - 3n$  since at least  $m - 3n$  edges must be removed to make  $G$  planar.

Consider  $G$  with  $G_p$  = graph where each vertex stays with probability  $p$ . Then  $\mathbb{E}(np) = pn$  and  $\mathbb{E}(mp) = p^2m$ . Then

$$p^4 Cr(G) \geq \mathbb{E}(Cr(G_p)) \geq \mathbb{E}(m_p - 3n_p) = \mathbb{E}(m_p) - 3\mathbb{E}(n_p) \geq p^2m - 3pn$$

So  $Cr(G) \geq \frac{m}{p^2} - \frac{3n}{p^3}$  and is maximized when  $p = \frac{4n}{m}$  only when  $4n \leq m$ . Then  $\frac{m}{p^2} - \frac{3n}{p^3} = \frac{m^3}{64n^2}$ .

**Theorem 5.25.** *For any collection  $\mathcal{L}$  of lines in  $\mathbb{R}^3$ , there are at most  $O(|\mathcal{L}|^{3/2})$  joints.*

We just have to show the following lemma to imply the theorem.

**Lemma 5.26.** *In any collection of lines with  $|J|$  joints, there exist some line in  $\leq 3|J|^{1/3}$  joints.*

Lemma 5.26  $\implies$  theorem 5.25 as we define  $J(L)$  = most joints in  $|L|$  lines.

$$J(L) \leq J(L-1) + 3J^{1/3} \leq J(L-2) + 3(J-1)^{1/3} + 3J^{1/3} \leq \dots$$

$$\text{So } J \leq 3J^{1/3}L \iff J^{2/3} \leq 3L \iff J \leq \sqrt{27}L^{3/2}$$

Given an arbitrary field,  $\text{Poly}_D(\mathbb{F}^n)$  and  $S = \{a_1, \dots, a_k\}$  for  $a_i \in \mathbb{F}^n$ . We want to find a nonzero polynomial that vanishes at  $J$ .

$$\text{Let } T : \text{Poly}_D(\mathbb{F}^n) \rightarrow \mathbb{F}^k \text{ defined as } T(p) = \begin{bmatrix} p(a_1) \\ \vdots \\ p(a_k) \end{bmatrix}$$

By rank nullity theorem,

$$\dim(\text{Im}(T)) \leq k \implies \dim(\ker(T)) \geq \dim(\text{Poly}_D(\mathbb{F}^n)) - k$$

If  $\dim(\text{Poly}_D(\mathbb{F}^n)) > k$ ,  $\exists p \in \text{Poly}_D(\mathbb{F}^n)$  vanishes at  $S$ ,  $|S| = k$ .

Let

$$\mathcal{D} = \{x_1^{d_1}, x_2^{d_2}, \dots, x_n^{d_n} \mid \sum d_i \leq D\}$$

This is a basis for  $\text{Poly}_D(\mathbb{F}^n)$ . By stars and bars we have  $|\mathcal{D}| = \binom{D+n}{n} \geq \frac{D^n}{n!} > k$ . We need  $\frac{D^3}{3!} > J$  so  $D > 3J^{1/3}$ .

AFSOC each line has more than  $D > 3J^{1/3}$  joints.

If  $p \in \text{Poly}_D(\mathbb{F})$ ,  $\forall a \in \mathbb{F}, \exists c \in \mathbb{F}$  such that  $p(x) = (x - a)q(x) + c$ . If  $a$  is a root,  $p(x) = (x - a)q(x)$ .

A line is a function  $\gamma(t) = a + bt$  for  $a, b \in \mathbb{F}^n$  then  $q(t) := p(\gamma(t))$  is a polynomial in  $\text{Poly}_D(\mathbb{F})$ .  $\deg(q)$  has to have at most the degree of  $p$  so  $\deg(q) < D$ . By our assumption the line has more than  $D$  joints so  $\deg(q) > D$ . The only way  $q(t)$  can have more than  $D$  roots is if  $q$  is the zero polynomial. So we can conclude our polynomial  $p$  must be identically 0 on the union of all lines in  $\mathcal{L}$ .

Each joint is the intersection of 3 lines and  $p$  is zero on all lines. So the direction derivative along each of the lines is 0 and as they are linearly independent we have  $\nabla p = 0$  at every joint. Consider  $p_1 = \frac{\partial p}{\partial x}$ ,  $\deg(p_1) \leq D - 1$  and  $p_1$  vanishes at every joint in  $J$  so we contradict the minimality of  $D$  so the assumption that all lines have  $> D$  joints is false.

**Lemma 5.27.** *If  $P(x_1, \dots, x_n)$  is a non-zero polynomial over  $\mathbb{F}_q$ , with total degree  $D \leq q - 1$  then  $P(x)$  cannot be zero for all  $x \in \mathbb{F}_q^n$ .*

*Proof.* We can write

$$P(x) = \sum_{k=0}^D q_k(x_1, \dots, x_{n-1})x_n^k$$

We'll show the statement by induction on  $n$ .

(**Base Case**  $n = 1$ ) AFSOC  $P(x_1)$  is nonzero and vanishes on all of  $\mathbb{F}_q$ . Since  $\deg(P) \leq q - 1$  but  $P$  has  $q$  distinct roots,  $P$  must be the zero polynomial. This is a contradiction.

(**Inductive Step**) AFSOC  $P(x) = 0$  on all  $x \in \mathbb{F}_q^n$ . We write

$$P(x) = \sum_{k=0}^D q_k(x_1, \dots, x_{n-1})x_n^k$$

Since  $P(x)$  is a nonzero polynomial, there must exist at least one  $k$  for which  $q_k(x_1, \dots, x_{n-1})$  is a non-zero polynomial.

Fix the first  $n - 1$  variables. Let  $(a_1, \dots, a_{n-1})$  be an arbitrary point in  $\mathbb{F}_q^{n-1}$ . Define

$$Q(t) := P(a_1, \dots, a_{n-1}, t)$$

We can express  $Q(t) = \sum_{k=0}^D q_k(a_1, \dots, a_{n-1})t^k$ . For this fixed  $(a_1, \dots, a_{n-1})$ , each  $q_k(a_1, \dots, a_{n-1})$  is a constant in  $\mathbb{F}_q$ . This implies  $\deg(Q) \leq D \leq q - 1$ .

By assumption,  $P(x) = 0$  everywhere, so  $Q(t) = P(a_1, \dots, a_{n-1}, t) = 0$  for all  $t \in \mathbb{F}_q$ . From our base case, a single-variable polynomial of degree  $\leq q - 1$  that has  $q$  roots must be the zero polynomial. This means all coefficients of  $Q(t)$  must be zero.

Therefore  $q_k(a_1, \dots, a_{n-1}) = 0$  for all  $k$ . Since  $(a_1, \dots, a_{n-1})$  was arbitrarily chosen, this holds for all points in  $\mathbb{F}_q^{n-1}$ .

This means each  $q_k$  is a polynomial in  $n - 1$  variables that vanishes on all of  $\mathbb{F}_q^{n-1}$ . The total degree of  $P$  is  $D = \max_k(\deg(q_k) + k)$ , which implies  $\deg(q_k) \leq D \leq q - 1$ . By our inductive hypothesis, a polynomial in  $n - 1$  variables of degree  $\leq q - 1$  that vanishes everywhere must be the zero polynomial.

Thus, each  $q_k$  is the zero polynomial. This implies  $P(x)$  is the zero polynomial, which contradicts our initial assumption that  $P(x)$  is a non-zero polynomial.  $\square$

**Theorem 5.28.** *If  $N \subseteq \mathbb{F}_q^n$  is a set with the property that for all  $x \in \mathbb{F}_q^n$ , there is a line  $L_x$  such that  $L_x \setminus \{x\} \subseteq N$ , then  $|N| \geq \epsilon_n q^n$  where  $\epsilon_n > 0$  depends only on  $n$ . (The proof shows  $\epsilon_n = (10n)^{-n}$ ).*

*Proof.* Assume for the sake of contradiction that  $|N| < \left(\frac{q}{10n}\right)^n$ .

We know from the polynomial method that there exists a non-zero polynomial  $p \in \text{Poly}_D(\mathbb{F}_q^n)$  that vanishes on  $N$ , with degree  $D \leq 2n|N|^{1/n}$ .

Using our AFSOC, we can bound this degree  $D$ :

$$D \leq 2n|N|^{1/n} < 2n \left(\frac{q}{10n}\right) = \frac{q}{5}$$

So, we have found a non-zero polynomial  $p$  with total degree  $D < q/5$ .

Now, consider any arbitrary  $x \in \mathbb{F}_q^n$ . By the theorem's premise, there is a line  $L_x$  through  $x$  such that  $L_x \setminus \{x\} \subseteq N$ . We can parametrize this line as  $\gamma(t) = x + d \cdot t$  for  $t \in \mathbb{F}_q$ , where  $d \in \mathbb{F}_q^n \setminus \{0\}$  is a direction vector. Note that  $\gamma(0) = x$ , and  $L_x \setminus \{x\} = \{\gamma(t) \mid t \in \mathbb{F}_q \setminus \{0\}\}$ .

Define a new, single-variable polynomial  $R(t) := p(\gamma(t))$ . The degree of  $R(t)$  is at most the total degree of  $p$ , so  $\deg(R) \leq D < q/5$ .

Since  $p$  vanishes on  $N$ ,  $p$  must vanish on  $L_x \setminus \{x\}$ . This means  $R(t) = p(\gamma(t)) = 0$  for all  $t \in \mathbb{F}_q \setminus \{0\}$ . The set  $\mathbb{F}_q \setminus \{0\}$  has  $q - 1$  elements, so  $R(t)$  has  $q - 1$  distinct roots.

We have a polynomial  $R(t)$  with  $\deg(R) \leq D < q/5$ . For any  $q \geq 3$ , we have  $q/5 \leq q - 2$  (since  $10 \leq 4q$ ).

Thus,  $R(t)$  is a polynomial with degree strictly less than  $q - 1$ , but it has  $q - 1$  roots. A non-zero polynomial cannot have more roots than its degree. Therefore,  $R(t)$  must be the zero polynomial.

If  $R(t)$  is the zero polynomial, it must be zero for all  $t$ , including  $t = 0$ .

$$R(0) = p(\gamma(0)) = p(x) = 0$$

Since  $x \in \mathbb{F}_q^n$  was arbitrary, we have shown  $p(x) = 0$  for all  $x \in \mathbb{F}_q^n$ . We also know  $\deg(p) = D < q/5$ , which implies  $\deg(p) \leq q - 1$ .

By Lemma 5.27, any polynomial with degree  $\leq q - 1$  that vanishes on all of  $\mathbb{F}_q^n$  must be the zero polynomial. This contradicts our choice of  $p$  as a non-zero polynomial.

Therefore, our initial assumption was false, and we must have  $|N| \geq \left(\frac{q}{10n}\right)^n$ .  $\square$

**Lemma 5.29.** *If  $p \in \text{poly}_{q-1}(\mathbb{F}_q^n)$  is nonzero,  $|\text{zero}(P)| < q^n$ .  
Maximized when  $x_1^{q-1} - 1$*

**Theorem 5.30.** *Schartz-Zippel: If nonzero  $p \in \text{poly}_D(\mathbb{F}^n)$  and  $S \subseteq \mathbb{F}$  a finite subset. For random  $s_1, \dots, s_n \in S$*

$$\mathbb{P}_{s_1, \dots, s_n}(p(s_1, \dots, s_n) = 0) \leq \frac{D}{|S|}$$

*In other words,  $|\text{zero}(p) \cap S^n| \leq D|S|^{n-1}$*

*Proof.* Let  $p \in \text{poly}_D(\mathbb{F}^n)$  be nonzero. We're done if  $n = 1$ . Do induction on  $n$ .

$$p(x_1, \dots, x_n) = \sum_{k=0}^n q_k(x_1, \dots, x_{n-1})x_n^k.$$

Choose  $k_0$  to be largest such that  $q_{k_0} \neq 0$ . By induction

$$\mathbb{P}_{s_1, \dots, s_{n-1}}(q_{k_0}(s_1, \dots, s_{n-1}) = 0) \leq \frac{D - k_0}{|S|}$$

$$\mathbb{P}_{s_1, \dots, s_n}(p(s_1, \dots, s_n) = 0) \leq \mathbb{P}_{s_1, \dots, s_n}(q_{k_0}(s_1, \dots, s_{n-1}) = 0) + \mathbb{P}_{s_1, \dots, s_n}(p(s_1, \dots, s_n) = 0 | q_{k_0}(s_1, \dots, s_{n-1}) \neq 0)$$

Note: This is just  $\mathbb{P}(B) \leq \mathbb{P}(C) + \mathbb{P}(B|\neg C) \cdot \mathbb{P}(\neg C)$

$q_{k_0}(s_1, \dots, s_{n-1}) \neq 0 \implies p(s_1, \dots, s_{n-1}, x_n)$  has degree  $k_0$ .

$$\frac{\sum_{s_1, \dots, s_{n-1}} \prod_{q(s_1, \dots, s_{n-1}) \neq 0} \frac{1}{|S|^{n-1}} \mathbb{P}(p(s_1, \dots, s_n) = 0 | q_{k_0}(s_1, \dots, s_{n-1}) \neq 0)}{\sum_{s_1, \dots, s_{n-1}} \prod_{q(s_1, \dots, s_{n-1}) \neq 0} \frac{1}{|S|^{n-1}}}$$

$$\mathbb{P}_{s_1, \dots, s_n}(q_{k_0}(s_1, \dots, s_{n-1}) \neq 0) + \mathbb{P}_{s_1, \dots, s_n}(p(s_1, \dots, s_n) = 0 | q_{k_0}(s_1, \dots, s_{n-1}) \neq 0) \leq \frac{D - k_0}{|S|} + \frac{k_0}{|S|} = \frac{D}{|S|}$$

$\square$

**Theorem 5.31.** *Extremal Schwartz-Zippel. If  $p$  nonzero of degree  $d$ ,  $p = 0$  on  $S^n$  then  $|S| \leq d$ .*

**Example 5.32.**

$$p = \prod_{s \in S} (x_i - s)$$

is 0 for all  $x \in S^n$ . This holds for  $S \times \{1\} \times \{1\} \times \dots$ .

**Example 5.33.**

$$q = \prod_{a_1 \in S_1} (x_1 - a_1) \prod_{a_2 \in S_2} (x_2 - a_2) \prod_{a_3 \in S_3} (x_3 - a_3)$$

Say  $S_1, S_2, S_3$  has size 4, 3, 2, respectively. If in a  $5 \times 4 \times 3$  box then  $q$  is definitely not zero polynomial.

**Theorem 5.34.** *Combinatorial Nullstellensatz: Suppose  $p$  is a nonzero polynomial in  $\text{Poly}_d(\mathbb{F}^n)$  of degree  $d$  and the monomial  $x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$  for  $j_1 + \cdots + j_n = d$  has nonzero coefficients then  $\forall S_1, \dots, S_n \subseteq \mathbb{F}$  with  $|S_i| \geq j_i + 1$  for all  $i$ ,  $p(x) \neq 0$  for some  $x \in S_1 \times S_2 \times \cdots \times S_n$ .*

*Proof.* We'll show it by induction on  $d$ .

Suppose  $f \equiv 0$  on  $S_1 \times S_2 \times \cdots \times S_n$  where  $S_i \subseteq \mathbb{F}$ .

WLOG  $j_i \geq 1$ ,  $\forall s \in S_1$  we have  $f(x) = (x_1 - s)q_s(x) + r(x)$  then  $\deg(q_s) = d - 1$ , moreover coefficients of  $x_1^{j_1-1}x_2^{j_2}\cdots x_n^{j_n}$ . For any  $s \in S_1, s_2 \in S_2, \dots$  we have  $f(s, s_2, \dots, s_n) = 0 \implies r_s(s, s_2, \dots, s_n) = 0 \forall s_2, \dots, s_n \implies r_s(s_1, \dots, s_n) = 0 \forall s_1 \in S_1, s_2 \in S_2, \dots$

By our assumption we have  $0 = f(s_1, \dots, s_n) = (s_1 - s)q_s(s_1, \dots, s_n)$  for all  $s, s_1 \in S_1, \dots, s_n \in S_n$ . For  $s \neq s_1$  we learn  $q_s(s_1, \dots, s_n) = 0$ . Since  $q_s$  is zero on  $S_1 \setminus \{s\} \times S_2 \times \cdots \times S_n \implies$  we must have  $|S_1 \setminus \{s\}| \leq j_1 - 1$  or for some  $i$ ,  $|S_i| \leq j_i$ . by induction hypothesis.  $\square$

**Example 5.35.**  $\chi'(G)$  list chromatic number of  $G$ . We want to find  $\chi'(C_n)$ .

Consider an assignment  $c_i$  to each vertex  $i, c_i \in \mathbb{N}$ .  $f(c_1, \dots, c_n) = (c_2 - c_1)(c_3 - c_2) \cdots (c_n - c_{n-1})(c_1 - c_n)$ . The leading term of  $f$  is  $2c_1c_2 \cdots c_n$ . For all sets  $S_1, \dots, S_n \subseteq \mathbb{N}$ , chromatic number implies  $\exists c_1 \in S_1, c_2 \in S_2, \dots, c_n \in S_n$  such that  $f(c_1, \dots, c_n) \neq 0$ .

**Example 5.36.** *Cauchy Davenport: Let  $p$  prime,  $A, B \subseteq \mathbb{Z}_p$*

$$|A + B| \geq \min(p, |A| + |B| - 1)$$

*Proof.* Case 1: If  $|A| + |B| - 1 \geq p$

Consider  $x \in \mathbb{Z}_p$  then  $|x - A| = |A|$  so  $|A - x| + |B| \geq p + 1$  and  $\exists y \in A_x \cap B \implies \exists a \in A, b \in B$  such that  $y = b, y = x - a$  so  $x = a + b$ .

Case 2: If  $|A| + |B| - 1 < p$

Consider any set  $C \subseteq \mathbb{Z}$  of size  $|C| = |A| + |B| - 2$ . We want to show  $\exists x \in A + B, x \notin C$ .

Define

$$f(a, b) = \prod_{c \in C} (a + b - c)$$

We have  $\deg(f) = |C| = |A| + |B| - 2$ , consider the monomial  $a^{|A|-1}b^{|B|-1}$  then the coefficient is  $\binom{|A|+|B|-2}{|A|-1} \neq 0$  in  $\mathbb{Z}_p$ . So for  $|A|, |B|$  we have a choice of  $a, b$  such that  $a + b \notin C$ .  $\square$

**Definition 5.37.** *Finite Kakeya: In  $\mathbb{F}_a^n, \forall a, \exists b$  such that  $\{at + b | t \in \mathbb{F}_a\} \subseteq K$ . Then  $K$  is a kakeya set.*

**Theorem 5.38.** *Chevalley–Warning theorem:*

Let  $a = p^l$  for  $f_1, \dots, f_k \in \mathbb{F}_a[x_1, \dots, x_n]$ .

If  $\sum_i \deg(f_i) < n$  then the number of common zeros is a multiple of  $p$ . In particular: if there's 1 common zero then there is more.

**Example 5.39.** *Given any  $n$  numbers  $a_1, \dots, a_n$  there is a nonempty subset that sums to 0 (mod  $n$ ).*

*Proof.* Let  $S_0 = \{\}, S_1 = \{a_1\}, \dots, S_n = \{a_1, \dots, a_n\}$  then there exists  $i, j$  such that  $S_i = S_j$  so  $\square$



**Theorem 5.40.** *Erdos-Ginzburg-Ziv Theorem:*

*How large a collection of numbers do I require to ensure that some  $n$ -subset sum to a multiple of  $n$ ?  $2n - 1$  is enough*

*Proof.* (Main Case)  $n = p$  is a prime

Given numbers  $a_1, \dots, a_{2p-1}$ , we'll give two polynomials in  $2p - 1$  variables  $x_1, \dots, x_{p-1}$

We want a polynomial such that  $x_i$  behaves like indicators for  $a_i \in S$ . So  $x_i^{p-1} \equiv 1 \pmod p$  by FLT.

$$f(x_1, \dots, x_{2p-1}) = \sum_{x_i} x_i^{p-1} = \#\{i | x_i \neq 0\}$$

$$g(x_1, \dots, x_{2p-1}) = \sum_{x_i} a_i x_i^{p-1} = \sum_{x_i \neq 0} a_i$$

We have  $2p - 2 < 2p - 1$  and the trivial solution exist so a non-trivial solution exist by Chevalley-Waring

(General Case) Induction on  $n$ ,  $a_1, \dots, a_{2n-1}$

If  $n$  not prime, let  $p$  be a prime factor of  $n$ ,  $m = \frac{n}{p}$ . Find a set  $I_i$ ,  $|I_i| = p$  such that  $\sum_{j \in I_i} a_j \equiv 0 \pmod p$  for  $i \in [2m - 1]$

Say  $\sum_{i \in I_j} a_i \equiv b_j \pmod p$

Let  $c_i = \frac{b_i}{p}$ , we can find  $c_{i_1}, c_{i_2}, \dots, c_{i_m}$  such that

$$\sum_{j=1}^m c_{i_j} = \sum_{j=1}^m \sum_{t \in I_{i_j}} t = \left( \sum_{j=1}^m c_{i_j} \right) p \equiv 0$$

□

**Theorem 5.41.** *There exist an order of at least  $d^2$  2-distance set in  $\mathbb{R}^d$ ?*

*Proof.* Suppose  $S = \{p_1, \dots, p_m\}$  has just 2 distances  $\alpha$  and  $\beta$ . Consider the polynomial,  $f \in \mathbb{R}[x_1, \dots, x_d]$  defined as

$$f_i(X) = (||X - p_i||^2 - \alpha^2)(||X - p_i||^2 - \beta^2)$$

$$f_i(X) = \begin{cases} \alpha^2 \beta^2 & \text{if } X = p_i \\ 0 & \text{otherwise} \end{cases}$$

Claim:  $f_i$ 's are independent.

Suppose  $\alpha_1 f_1 + \dots + \alpha_m f_m = 0$ ,  $\forall i$ , plug in  $p_i$  gives  $\alpha_i \alpha^2 \beta^2 = 0 \implies \alpha_i = 0$

Claim:  $x_i^{d_1} x_j^{d_2}$  with  $d_1 + d_2 \leq 4$  covers all possible terms. So there is at most  $O(d^2)$  possible choices. □

**Example 5.42.** *Eventown where each club has even size and even intersection,  $\geq 2^{\lceil n + \frac{1}{2} \rceil}$*

**Example 5.43.** *Oddtown where each club has odd size and even intersection*

Let  $v_i$  = incidence vector of club  $i$  in  $\mathbb{F}_2$ .  $v_i \cdot v_j = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{otherwise} \end{cases}$

Suppose  $\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n = \vec{0}$   
 $\vec{v}_i$  on both sides so  $\alpha_i = 0$

**Theorem 5.44.** *Every Polygon has a triangulation*

*Proof.* Choose a convex vertex of the polygon (a vertex that is a vertex of the convex hull) with neighbors  $q, r$ . If  $\overline{qr} \subset P^\circ$  then we're done. Otherwise we can move the point. □

**Definition 5.45.** *We say polygon  $P \sim Q$  by scissor congruency if we can cut up  $P$  and reassembled to be  $Q$ .*

**Lemma 5.46.** *(Any rectangle)  $\sim$  (Any Unit Size Rectangle)*  
*(Any triangle)  $\sim$  (Unit Side Rectangle)*  
*(Triangle)  $\sim$  (2 Right Triangle)*  
*(Right Triangle)  $\sim$  (Rectangle)*

**Remark 5.47.** *From this lemma we can conclude any polygon is congruent to a rectangle of  $1 \times d$*

**Theorem 5.48.** *Are equal-area polyhedra necessarily plane-dissection equivalent? This is not true.*

**Example 5.49.** *Unit cube and volume 1 reg-tetrahedron are not dissection equivalent.*

*Proof.* Dihedral angle is an irrational multiple of  $\pi$   
A list of vectors  $v_1, \dots$  is independent if for every finite sum,

$$\sum_{j=1}^k \alpha_{i_j} v_{i_j} = 0 \implies \alpha_{i_j} = 0 \forall j$$

$\text{Span}(\mathcal{L})$  is the set of vectors representable as finite linear combinations.  $\mathcal{L}$  is a basis for  $V$  if  $\mathcal{L}$  is independent and  $\text{Span}(\mathcal{L}) = V$

**Lemma 5.50.** *Zorn's Lemma:  $P$  is a poset in which every chain has an upper bound then  $P$  has a maximal element.*

Doset is a set of independent sequences, ordered by inclusion.

$$\mathcal{L}_1 \subseteq \mathcal{L}_2 \cdots \subseteq$$

Then  $\cup \mathcal{L}_i$  is still independent. By Zorn's lemma and Doset we have every vector space has a (possibly infinite) basis.

Define  $\alpha$  to be dihedral angle of tetrahedron, we'll use that  $\frac{\alpha}{\pi}$  is irrational.

In general, we can define a linear transformation  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that  $f(\pi) = 0$  and  $f(\alpha) = 1$ .

Since  $\alpha$  and  $\pi$  are independent over  $\mathbb{Q}$  extended to a basis  $\alpha, \pi, v_3, v_4, \dots$

Define  $f$  using this basis by defining  $f(\alpha) = 1, f(\pi) = 0$

If a plane goes through an angle then  $l_e = l_{e_1} = l_{e_2}$  and  $\theta_e = \theta_{e_1} + \theta_{e_2}$ .

If a plane goes through an edge then  $l_{e_1} + l_{e_2} = l_e$  and  $\theta_e = \theta_{e_1} = \theta_{e_2}$

If a plane goes through another plane and creates a new edge then  $l_{e_1} = l_{e_2}$  and  $\theta_{e_1} + \theta_{e_2} = \pi$

We can assign a real number to each polytope by

$$\sum_{e \in P} l_e \cdot f(\theta_e)$$

In the first case we would have

$$R(P) = \sum_{e \in P} l_e f(\theta_e)$$

If  $P$  is a cube then  $R(P) = 0$  as each dihedral angle is  $90^\circ$  so it's a rational multiple of  $\pi$ . However if  $P$  is a tetrahedron has irrational multiple of  $\pi$  so  $R(P) \neq 0$ .  $\square$

# Linear Algebra

**Definition 5.51.** *Adjacency Matrices:* On the vertex set  $[n]$

$$A = \begin{bmatrix} & \\ & \end{bmatrix}$$

$$A_{i,j} = \begin{cases} 1 & \text{if } i \sim j \\ 0 & \text{otherwise} \end{cases}$$

If  $f : V \rightarrow \mathbb{R}$  then  $Af = g$  and if  $Af = \lambda f$  then it's an eigen function.

**Remark 5.52.** We'll denote the  $n \times n$  matrix of all ones as  $J_n$ .

**Theorem 5.53.**  $J_n$ 's eigenvalues are  $\lambda_1 = n$  with multiplicity 1 and  $\lambda_2 = 0$  with multiplicity  $n - 1$ .

*Proof.* To show  $\lambda = 0$  has multiplicity  $n - 1$  the associated eigenvectors are

$$\begin{bmatrix} 1 \\ -1 \\ 0 \\ \vdots \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ -1 \\ \vdots \end{bmatrix}, \dots,$$

□

**Theorem 5.54.**  $K_n = J_n - I_n$  has eigenvalue  $n - 1$  with multiplicity 1 and  $-1$  with multiplicity  $n - 1$ .

**Remark 5.55.** For any regular graph with degree  $d$ ,  $d$  is an eigenvalue value with multiplicity 1.

**Lemma 5.56.** For any adjacency matrix  $A$ ,  $A^2$  has the property that  $A_{i,j}^2 = \# \text{walks of length 2 from } i \rightarrow j$ . This generalizes easily to the general case for  $A^k$

*Proof.* This is easily shown from the matrix multiplication

$$A_{i,j} = \sum_{k \in [n]} A(i,k)A(k,j)$$

□

**Lemma 5.57.** For a  $d$ -regular graph with diameter 2 graph then the maximum number of vertices is  $1 + d + d(d - 1) = d^2 + 1$  vertices.

To achieve this bound, I require  $\text{girth}(G) \geq 5$

Note: Girth is the length of a shortest cycle.

Another way to achieve this bound is the Peterson Graph

**Lemma 5.58.** Any Moore graph (regular graph whose girth is at least twice its diameter) has  $A^2 + A - (d-1)I = J$ .

*Proof.* We know  $\lambda = d$  an eigenvalue for  $f \equiv 1$ . By spectral theorem,  $A$  has an orthogonal basis of real eigenvectors. Since  $f_j \perp f_1$  for  $j \neq 1$  then  $J \cdot f_j = \vec{0}$  as  $J$  is the matrix of all ones. So

$$A^2 f_j + A f_j - (d-1)I f_j = 0 \iff \lambda_j^2 + \lambda_j - (d-1) = 0$$

We can conclude  $\lambda = \frac{-1 \pm \sqrt{4d-3}}{2}$

We need  $1 + m_2 + m_3 = n$  and  $d + m_2 \lambda_2 + m_3 \lambda_3 = 0$

So  $2d - (m_2 + m_3) + (m_2 - m_3)\sqrt{4d-3} = 0$

(Case 1) If  $\sqrt{4d+3} \notin \mathbb{Q}$  then  $m_2 = m_3$  and  $2d = d^2 \implies d = 2$

(Case 2) If  $\sqrt{4d-3} = s \in \mathbb{Z}$  then  $d = \frac{s^2+3}{4}$  then

$$2d - d^2 + (m_2 - m_3)s = 0 \iff 8 \left( \frac{s^2+3}{4} \right) - (s^2+3)^2 + 16(m_2 - m_3)s = 0$$

Expanding out we have  $as^4 + bs^3 + cs^2 + ds + 15 = 0$  then  $s|15 \implies s = 1, 3, 5, 15 \implies d = 1, 3, 7, 57$ .  $\square$

We'll be covering graph where for any 2 vertices  $u, v$  there is exactly one common neighbor of  $u, v$

**Theorem 5.59.** "There is a politician":  $\exists v_0$  such that  $\forall u, v_0 \sim u$

*Note:* This doesn't hold for infinite vertices by  $H_0 = 5$ -cycle and  $H_{i+1}$  is  $H_i$  with independent path of length 2 added between parts that don't have a common neighbor in  $H_i$ .

*Step 1* A counterexample must be regular

*Step 1A*  $u \not\sim v \implies \deg(v) \geq \deg(u)$ . By symmetry  $\deg(v) = \deg(u)$ . This is from  $w_1$  being the common neighbor of  $u, v$  and  $w_2$  being the common neighbor of  $w_1, u$  and  $z_1$  being common neighbor of  $w_1$  and  $v$ .

*Step 1B* Let  $\deg(u) = d, \forall v \neq w_i$  we get  $\deg = d$  for all  $w_2, \dots, w_d$ , we get  $\deg(w_i) = \deg(v) = d$ . All but  $w_1$  are known to be degree  $d$ . Since  $w_i$  not a politician then  $w_1$  must be the politician.

Going back to the graph with diameter 2 graph then  $n = 1 + d(d-1) = d^2 - d + 1$ . There are exactly 1 path of length 2 between  $u, v$   $\deg(u) = d \implies A^2$  is  $d$  along diagonal and 1 everywhere else.  $A^2 = J + (d-1)I$ .  $J$  has e.v.  $n$  with multiplicity 1 and 0 with multiplicity  $n-1$ . So  $A^2$  has e.v.  $n + d - 1$  with multiplicity 1 and  $d - 1$  with multiplicity  $n - 1$ .

$A$  has eigenvalues  $d$  with multiplicity 1,  $\sqrt{d-1}$  with multiplicity  $s$  and  $-\sqrt{d-1}$  with multiplicity  $t$ . Also  $s + t = n - 1$ . The trace of  $A$  is 0 so  $d + \sqrt{d-1}s - \sqrt{d-1}t = 0 \implies d + (s - t)\sqrt{d-1} = 0$ . So  $\sqrt{d-1} \in \mathbb{Q} \implies h := \sqrt{d-1} \in \mathbb{N}$ .

We have  $d = \sqrt{d-1}^2 + 1 = h^2 + 1$ . So  $d + h(s - t) = 0 \implies h^2 + 1 = h(t - s) \implies h = 1 \implies d = 2$

**Theorem 5.60.** Oddtown: Clubs have odd size and intersections are even. The clubs are less than number of people.

**Lemma 5.61** (Fisher's Inequality). Let  $\mathcal{F} = \{A_1, \dots, A_m\}$  be a family of  $m$  distinct subsets of a universe  $X$  where  $|X| = n$ . Suppose there exists a constant  $k$  such that  $|A_i \cap A_j| = k$  for all  $i \neq j$ . Furthermore, assume that  $|A_i| > k$  for all  $i$ . Then:

$$m \leq n$$

*Proof.* Let  $v_1, \dots, v_m \in \mathbb{R}^n$  be the incidence vectors of the sets  $A_1, \dots, A_m$ . That is, the  $x$ -th component of vector  $v_i$  is 1 if  $x \in A_i$  and 0 otherwise.

We aim to show that these vectors are linearly independent. Consider a linear combination of these

vectors equal to the zero vector, with coefficients  $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ :

$$\sum_{i=1}^m \alpha_i v_i = 0 \quad (1)$$

We take the squared Euclidean norm (the dot product with itself) of both sides:

$$\left\langle \sum_{i=1}^m \alpha_i v_i, \sum_{j=1}^m \alpha_j v_j \right\rangle = 0$$

Expanding using the linearity of the inner product:

$$\sum_{i=1}^m \alpha_i^2 \langle v_i, v_i \rangle + \sum_{i \neq j} \alpha_i \alpha_j \langle v_i, v_j \rangle = 0$$

We observe the following properties of the incidence vectors:

- $\langle v_i, v_i \rangle = |A_i|$
- $\langle v_i, v_j \rangle = |A_i \cap A_j| = k$  (for  $i \neq j$ )

Substituting these values into the equation:

$$\sum_{i=1}^m \alpha_i^2 |A_i| + k \sum_{i \neq j} \alpha_i \alpha_j = 0$$

To simplify the second term, we use the identity  $(\sum \alpha_i)^2 = \sum \alpha_i^2 + \sum_{i \neq j} \alpha_i \alpha_j$ . Rearranging this gives  $\sum_{i \neq j} \alpha_i \alpha_j = (\sum \alpha_i)^2 - \sum \alpha_i^2$ . We substitute this back into our equation:

$$\begin{aligned} \sum_{i=1}^m \alpha_i^2 |A_i| + k \left[ \left( \sum_{i=1}^m \alpha_i \right)^2 - \sum_{i=1}^m \alpha_i^2 \right] &= 0 \\ \sum_{i=1}^m \alpha_i^2 (|A_i| - k) + k \left( \sum_{i=1}^m \alpha_i \right)^2 &= 0 \end{aligned}$$

Since we assumed  $|A_i| > k$ , we have  $|A_i| - k > 0$ . Also, squares of real numbers are non-negative (assuming  $k > 0$  and observing  $(\sum \alpha_i)^2 \geq 0$ ). Therefore, we have a sum of non-negative terms equaling zero. This implies that every individual term must be zero. Specifically:

$$\alpha_i^2 (|A_i| - k) = 0 \quad \forall i$$

Since  $|A_i| - k \neq 0$ , it must be that  $\alpha_i = 0$  for all  $i$ .

Thus, the vectors  $v_1, \dots, v_m$  are linearly independent. Since they exist in  $\mathbb{R}^n$ , the dimension of the subspace they span cannot exceed  $n$ , implying  $m \leq n$ .  $\square$

**Theorem 5.62.**  $R(k+1) \geq \binom{k}{3} + 1$ . We can group every 3 vertices then color it red

A quadratic form/homogeneous polynomial say  $q(x, y) = x^2 + 2xy + 3y^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$ . There is an bijection between quadratic form and symmetric matrices.

We can write  $A = P^T B P$  where  $B$  is a diagonal matrix with eigenvalues

$$B = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

**Definition 5.63.** For a symmetric matrix  $A$ ,

1. Positive definite if  $\lambda_i > 0$  for all  $i$
2. Negative definite if  $\lambda_i < 0$  for all  $i$

**Theorem 5.64.** Given symmetric  $A$ ,  $q_A(X) = X^T A X$ . Let  $A$  be real, symmetric  $n \times n$ . Let  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  be the eigen values of  $A$ . We can conclude

$$\lambda_k = \max_{U \subseteq V, \dim(U)=k} \min_{X \in U} \frac{X^T A X}{X^T X}$$

**Remark 5.65.** This statement doesn't care of the magnitude of  $X$  and only the direction. We're looking for the direction of greatest change.

*Proof.* We'll first show  $\lambda_k \leq \max_U$ . For this direction suffices to exhibit one good  $u$ . For  $v_1, \dots, v_n$  orthonormal eigen basis,  $v_i$  eigenvalues for  $\lambda_i$ . Let  $U_k = \{v_1, \dots, v_k\}$  and let  $X \in \text{Span}(U_k)$  so  $X = \sum_{i=1}^k \alpha_i v_i$ . WLOG  $|X| = 1$  since the magnitude does not change the result. This implies  $\sum \alpha_i^2 = 1$ .

$$X^T A X = \left( \sum \alpha_j v_j \right)^T A \left( \sum \alpha_j v_j \right) \quad (2)$$

$$= \left( \sum \alpha_j v_j \right)^T \left( \sum \alpha_j \lambda_j v_j \right) \quad (3)$$

$$= \sum \lambda_j \alpha_j^2 \quad (4)$$

This is a weighted average of  $\lambda_1, \dots, \lambda_k$  so this is at least the  $\min(\lambda_1, \dots, \lambda_k) = \lambda_k$ .

For the other direction  $\lambda_k \geq \max_U$ . Given any  $U_k$ , we want to show  $\exists X \in U_k$  such that  $\frac{X^T A X}{X^T X} \leq \lambda_k$ . Let  $W = \text{Span}(v_k, \dots, v_n)$  then  $\dim W = n - k + 1$ . So there exist a vector  $X \neq 0, X \in W \cap U_k$ . WLOG, take  $|X| = 1$ . Since  $X \in W$ ,  $X = \sum_{j=k}^n \alpha_j v_j$  and

$$X^T A X = \sum_{j=k}^n \lambda_j \alpha_j^2 \leq \max(\lambda_k, \dots, \lambda_n) = \lambda_k$$

□

**Example 5.66.** Given a  $d$ -regular graph  $G$  with adjacency matrix  $A$  with  $\lambda_1 \geq \dots \geq \lambda_n \geq -d$ . Suppose  $I$  had a negative eigenvalue that is less than  $-d$  then any vertex when applied the adjacency matrix will be the sum of the neighboring vertices, but we can't have  $|\sum| > d^2$ . Given an independent  $S$  of size  $\alpha$ . Define a vector  $v = nI_S - \alpha I = (n - \alpha)I_S - \alpha I_{\bar{S}}$ . Then  $v \cdot I = 0$ . We know

$$\min_{X \subseteq \mathbb{R}^n} \frac{X^T A X}{X^T X} = \lambda_k$$

So we know  $\lambda_k \leq \frac{v^T A v}{v^T v}$ .

$$v^T v = (nI_S - \alpha I)(nI_S - \alpha I) = \alpha n^2 - 2\alpha^2 n + \alpha^2 n = \alpha n(n - \alpha) \quad (5)$$

$$v^T A v = (nI_S - \alpha I)A(nI_S - \alpha I) \quad (6)$$

$$= nI_S A nI_S - 2\alpha^2 I_S A I + \alpha^2 I A I \quad (7)$$

$$= 0 - 2n\alpha I_S \begin{bmatrix} d \\ d \\ \vdots \\ d \end{bmatrix} + \alpha^2 nd \quad (8)$$

$$= -n\alpha^2 d \quad (9)$$

So we have  $\frac{-n\alpha^2 d}{\alpha n(n - \alpha)} = \frac{-\alpha d}{(n - \alpha)} = \frac{d}{1 - \frac{n}{\alpha}} \geq \lambda_n$ . When we solve for  $\alpha$

**Definition 5.67.** Expander Graphs

**Definition 5.68.** Let  $G = (V, E)$  and  $|V| = n$   
Cheeger Constant

$$h(G) = \min_{S \subseteq V, |S| \leq \frac{n}{2}} \frac{e(S, \bar{S})}{|S|}$$

**Remark 5.69.**  $h(G) \leq d$  and  $h(G) = 0 \iff G$  is disconnected.

**Definition 5.70.**  $G$  bipartite on  $(L, R)$  with  $|L| = |R| = n$  is a  $(d, \alpha)$  expander if

1. every degree in  $L$  is  $d$
2. every set  $S$  of size  $\leq \frac{n}{d}$  in  $L$  has  $\alpha|S|$  neighbors (in  $R$ )

**Theorem 5.71.** Let  $d \equiv 4$ , choose  $d$  edges from each vertex in  $L$  independent and 1 and only.  
Claim: With constant probability, result is a  $(d, \frac{d}{10})$  bipartite expander.

*Proof.* Let the bad events be for sets  $S \subseteq L, T \subseteq R, |S| \leq \frac{n}{d}, |T| < \alpha|S|, E_{S,T} = \{N(S) \subseteq T\}$ . Then  
 $\mathbb{P}(E_{S,T}) = \left(\frac{|T|}{n}\right)^{d|S|}$

$$\mathbb{P}(\exists S, T, |S| \leq \frac{n}{d}, |T| = \alpha|S|, E_{S,T}) \leq \sum_{s=1}^{n/d} \binom{n}{s} \binom{n}{\alpha s} \left(\frac{\alpha s}{n}\right)^d s \quad (10)$$

$$\leq \sum_{s=1}^{n/d} \binom{n}{\alpha s}^2 \left(\frac{\alpha s}{n}\right)^d s \quad (11)$$

$$\leq \sum_{s=1}^{\infty} \left(\frac{en}{\alpha s}\right)^{2\alpha s} \left(\frac{\alpha s}{n}\right)^{ds} \quad (12)$$

$$= \sum_{s=1}^{\infty} \left(\frac{n}{d}\right)^{(2\alpha-d)s} e^{2\alpha s} s^{(d-2\alpha)s} \quad (13)$$

$$= \sum_{s=1}^{\infty} \left(\frac{n}{\alpha s}\right)^{2\alpha-d} e^{2\alpha s} \quad (14)$$

$$\leq \sum_{s=1}^{\infty} 10^{(2\alpha-d)s} e^{2\alpha s} \quad (\alpha \leq d/10)$$

$$= \sum_{s=1}^{\infty} (10^{2\alpha-d} e^{2\alpha})^s < 1 \quad (15)$$

□

**Lemma 5.72.** If  $p$  has 1 fermat witnesses, half of the  $a$ 's relatively prime to  $p$  are fermat witnesses.

**Example 5.73.** Prime Algorithm

1. Randomly choose  $a$
2. Compute  $a^p \pmod{p}$   
If  $\neq a$ , report not prime else report maybe prime

From the previous lemma if not prime, at least half the  $a$  will show it.  
We want a deterministic expander graph and on the  $L$

**Theorem 5.74.** Similar setup to theorem 5.64,

$$\lambda_k = \min_{\dim(U)=k-1} \max_{X \perp U} \frac{X^T A X}{X^T X}$$

**Theorem 5.75.** We want to relate the spectral gap to the Creeger Constant

*Proof.*  $\vec{v} = nI_S - sI = (n-s)I_S - sI_{\bar{S}}$  with  $s = |S|$   
 $G$  is a  $d$ -regular graph,  $A$  is an adjacency matrix, we have

$$\lambda_2 = \max_{x \perp I} \frac{x^T A x}{x^T x} \geq \frac{\vec{v}^T A \vec{v}}{\vec{v}^T \vec{v}}$$

Note:  $\vec{v} \cdot I = ns - ns = 0$  and  $\vec{v} \cdot \vec{v} = (n-s)^2 s + s^2(n-s) = s(n-s)n$ .  
 Since the graph is  $d$ -regular we have  $ds = 2e(S) + e(S, \bar{S})$  and  $d(n-s) = 2e(\bar{S}) + e(S, \bar{S})$ .

$$\begin{aligned} \vec{v}^T A \vec{v} &= \sum_{(i,j) \in E(G)} v_i v_j = 2e(S)(n-s)^2 - 2e(S, \bar{S})s(n-s) + 2e(\bar{S})s^2 \\ &= (ds - e(S, \bar{S}))(n-s)^2 - 2e(S, \bar{S})s(n-s) + (d(n-s)e(S, \bar{S}))s^2 \\ &= ds(n-s)n - e(S, \bar{S})[(n-s)^2 + 2s(n-s) + s^2] \\ &= ds(n-s)n - e(S, \bar{S})n^2 \end{aligned}$$

Then substituting back we have

$$\lambda_2 \geq \frac{ds(n-s)n - e(S, \bar{S})n^2}{s(n-s)n} = d - \frac{e(S, \bar{S})n}{s(n-s)}$$

$\forall S \subseteq V, |S| \leq \frac{n}{2}$  we have

$$d - \lambda_2 \leq \frac{2e(S, \bar{S})}{|S|} \implies \lambda_1 - \lambda_2 \leq 2h(G)$$

□

**Example 5.76.** Consider  $A_{K_n} = J - I$  has eigenvalues  $n-1$  with multiplicity 1 and  $-1$  with multiplicity  $n-1$ .

**Lemma 5.77.** Lower bound on  $\lambda_2$  with  $G$  is  $d$ -regular,  $A = A_G$ ,  $A^2$  has eigen values  $\lambda_1^2, \dots, \lambda_n^2$   
 $\text{Trace}(A^2) = nd = \lambda_1^2 + \dots + \lambda_n^2$

$$nd - d^2 = \sum_{k=2}^n \lambda_k^2 \leq (n-1)\lambda_*^2 \quad (\lambda_* = \max_{i \neq 1} |\lambda_i|)$$

So we have  $d - o(1) = \frac{nd-d^2}{n-1} \leq \lambda_*^2 \implies \lambda_* \geq \sqrt{d} - o(1)$



**Theorem 5.78.** Consider simple random walk on a graph  $G$ ,  $G$  has adjacency matrix  $A$  and transition matrix  $P = \begin{bmatrix} \frac{1}{\deg(v_1)} & \cdots & \\ \vdots & \ddots & \\ & & \frac{1}{\deg(v_n)} \end{bmatrix} A$

**Remark 5.79.**  $P(i, j) = \mathbb{P}(\text{next at } j | \text{now at } i)$

If  $v_1, \dots, v_n$  are orthonormal eigenbasis to eigenvalues for  $A$ , also true for  $P$ . Let corresponding eigen values be  $\lambda_1 \geq \dots \geq \lambda_n$

Consider now a stochastic vector  $x$  with  $\sum_{i=1}^n x_i = 1, x_i \geq 0$ , the product  $xP = y$  where  $y$  is a stochastic vector with the new distribution given we start at distribution  $x$ .

$$x^T = \sum \alpha_i \vec{v}_i$$

Since  $P$  is symmetric

$$xP^t = P^t(\sum \alpha_i v_i) \quad (16)$$

$$= \sum_{i=1}^n (\alpha_i \lambda_i^t v_i) \quad (17)$$

$$= \alpha_1 v_1 + \sum_{i=2}^n \lambda_i^t \alpha_i v_i \quad (18)$$

$$\leq \lambda_*^t \left( \sum \alpha_i v_i \right) \quad (19)$$

So we can conclude  $xP^t \rightarrow \frac{1}{n}I$

**Theorem 5.80.** A knight makes random knight moves: let  $\tau$  be the time to return to the bottom left corner. What is  $\mathbb{E}[X]$ ?

**Definition 5.81.**  $\rho =$  probability of returning to origin for a random walk on  $\mathbb{R}$  then a random walk is recurrent if  $\rho = 1$  and transient otherwise.

**Remark 5.82.** A random walk is recurrent on  $\Gamma$  iff  $\mathbb{E}[\text{visits to origin}]$  is  $\infty$

$$\mathbb{P}(I \text{ visit exactly } k \text{ times}) = p^{k-1}(1-p)$$

$$\mathbb{E}(\text{visits}) = \sum_{k=1}^{\infty} k p^{k-1}(1-p) = \frac{1}{1-p}$$

For our random walk on  $\mathbb{R}$ ,

$$\mathbb{E}[\text{visit}] = \sum_{n=0}^{\infty} \mathbb{E}[I_n] = \sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{2^{2n}} = \sum_{n=0}^{\infty} a_n \geq \sum_{n \geq N} \frac{1}{\sqrt{\pi n}}$$

Where  $a_n \sim \frac{1}{\sqrt{\pi n}}$  by Stirling's Formula

The expected time to return to origin is not finite.

**Theorem 5.83.** The probability starting from  $j$  we reach  $n$  before reaching 0 is  $p_j = \frac{j}{n}$ .  $p_j = \frac{1}{2}p_{j-1} + \frac{1}{2}p_{j+1}$

For a random walk on  $\mathbb{R}^2$  let  $I_n = 1$  if at 0 at  $2n$ .

$$\Pr(I_n) = \sum_n \frac{1}{4^{2n}} \sum_k \frac{(2n)!}{n!n!(n-k)!(n-k)!} = \sum_n \frac{1}{4^{2n}} \binom{2n}{n} \sum_k \binom{n}{k}^2 = \sum_n \frac{1}{4^{2n}} \binom{2n}{n}^2$$

For a random walk on  $\mathbb{R}^3$  let  $I_n = 1$  if I return after  $2n$  steps.

$$\mathbb{E}[\text{visits}] = \sum_n \frac{1}{6^{2n}} \sum_{j,k} \frac{(2n)!}{j!^2 k!^2 (n-j-k)!^2} \leq \sum_n \frac{\binom{2n}{n} \binom{n}{n/3, n/3, n/3}}{2^{2n} 3^n} \sum \frac{\binom{n}{j, k, n-j-k}}{3^n}$$

By Stirling's formula,  $\frac{n!}{(\frac{n}{3})!^3} \approx \frac{(n/e)^n}{(\frac{n}{3e})^3}$

For a random walk on a directed graph, let

$$\pi(y) = \mathbb{E}(\text{visits a random direction from } z \text{ and makes to } y \text{ before visiting } z \text{ again})$$