Author's Note

The following are notes accompanying László Babai's Spring 2014 course in Honors Combinatorics at the University of Chicago. I transcribed Prof. Babai's lectures as he spoke (i.e. typeset in real time). It is occasionally difficult to keep up with Prof. Babai's pace, so there are some significant omissions in these notes. I have placed comments in parentheses to indicate where I think there are errors (it is likely there are quite many) or omissions.

If you have any improvements to suggest, please e-mail me at `contact@johnloeber.com` and I will make corrections. Contributions are very welcome: I have tried to indicate using comments where they are most required.

I also advise reading Prof. Babai's set of lecture notes on Discrete Mathematics. Finally, a formal disclaimer: this set of notes has not been reviewed by Prof. Babai; accuracy or correctness cannot be guaranteed.

Table of Contents

(If in search of specific content: I suggest downloading this document and using the search-function of your .pdf reader.)

1 Week 1: Monday, March 31, 2014

SET, Hypergraphs, Clubtown (Oddtown/Eventown).

See puzzle problem sheet on Laci's website.
Card game: SET. Study it by next class.
How many cards can be put down without a SET? What mathematical structure do the cards form? What natural substructures are SETs? What is the number of SETs?

Formalized by the same concept, Hypergraph $H = (V, E)$. V is a set of vertices, E is a set of edges, where each *edge* is a subset of V. If $n = |V|$, and $m = |E|$, then $m \leq 2^n$ (power set rule).

Clubtown: clubs $C_1, \ldots, C_m \subseteq V$, where V is the set of residents, $|V| = n$. (Rule 0) We have that no two clubs are identical, so $m \leq 2^n$.
(Rule 1) Then we have that $\forall i, |C_i|$ is even. So $m \leq 2^{n-1}$. **Do Exercise**
(Rule 2) Then, $\forall i \neq j, |C_i \cap C_j|$ is even: then $m \geq 2^{\lfloor \frac{n}{2} \rfloor}$. How do we construct this many clubs? Then how do we prove that more clubs are not possible? **Do Exercise:** prove that $m \geq 2^{\lfloor \frac{n}{2} \rfloor}$.

Then we have the much more difficult "Eventown Theorem": $m \leq 2^{\lfloor \frac{n}{2} \rfloor}$.
We make the distinction between *maximal* and *maximum*. Maximal club system: a system of clubs such that we cannot add more clubs. The maximum club system is the system of clubs that has the greatest possible number of clubs.

Challenge problem: for eventown, the maximum number is equal to the maximal number.

Now we change rule 1: we write that $\forall i, |C_i|$ is odd. (Now we are considering "Oddtown".) Then by rule 1 and 2, rule 0 is obsolete. Every person can have their own club, so $m \geq n$. Then it is also impossible to construct a larger club. So how do we prove $m = n$? Note that if n is even, then the other solution is clubs of "all but one".

Challenge Problem: The number of possible club systems with n clubs in oddtown is 2^{n^2}.

Oddtown Theorem: maximum number of clubs in Oddtown is n, i.e. WTS $m \leq n$. However, in Oddtown, maximal $\neq$ maximum! If n is odd, we can have one club of all n members of the town. If n is even, we can make two clubs of odd membership by splitting n into 2 clubs of odd size each.

Important application of maximum and maximal: if we look at linearly independent sets in linear algebra, then a maximal set is the same as the maximum set. **Do Exercise**

First miracle of linear algebra: if $\{\overrightarrow{v_1}, \ldots, \overrightarrow{v_k}\}$ are linearly independent and all belong to $\text{span}\{\overrightarrow{w_1}, \ldots, \overrightarrow{w_l}\}$, then $k \leq l$. (Exchange Lemma.)

We will approach the oddtown theorem by way of vectors. **(Do Exercise)** Look at the incidence vector V_A of a set $A \subseteq V$, where V is the "universe". If $V = \{1, \ldots, n\}$, then the incidence vector $V_A = (\alpha_1, \ldots, \alpha_n)$ such that α_i is 1 if $i \in A$, and is 0 if $i \notin A$. So now we look for some properties of vectors to immediately imply the oddtown theorem.

Lemma: under oddtown rules, $\overrightarrow{v_1}, \ldots, \overrightarrow{v_m}$ are linearly independent.

2 Week 1: Wednesday, April 2

Asymptotic Equality, Stirling's Formula, Prime Number Theorem, Extremal Combinatorics, Generator Functions, Binomial Formula, LYM(B) Inequality.

Take sequences a_n, b_n. They're asymptotically equal ("$a_n \sim b_n$") iff $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$.

Stirling's Formula: $n! \sim (\frac{n}{e})^n \sqrt{2\pi n}$.

Prime Number Theorem
$\pi(x)$ = number of primes $\leq x$
$\pi(x) \sim \frac{x}{\ln x}$ The number e is encoded in the prime numbers!

Asymptotic equalities take an unwieldy function and approximate them with a more workable function.

Do Exercise: Show that $\binom{2n}{n} \sim a \cdot n^b \cdot c^n$, where a, b, c constants. Find a, b, c. Use Stirling's Formula.

Notation: $[n] = \{1, 2, \ldots, n\}$.

Suppose we have subsets $A_i \subseteq [n]$, s.t. A_i are pairwise not comparable: $(\forall i \neq j)(A_i \not\subseteq A_j)$. So what is the maximum number m of subsets? This area is called extremal combinatorics.

A sufficient condition for $A_i \neq A_j$ is that they're of the same size. Then $m \geq \binom{n}{k} \forall k$. Then what is $\max\limits_{0\leq k\leq n} \binom{n}{k} = \binom{n}{\frac{n}{[2]}} = \binom{n}{\frac{[n]}{2}}$? (This relates to Sperner's Theorem? Notes here are incomplete.)

Do Exercise show $\binom{n}{k} \leq \binom{n}{k+1}$ for $k < \frac{n}{2}$ and it reverses for $k > \frac{n}{2}$. (Symmetry of binomial coefficients: intuitively, see Pascal's Triangle.)

The above property is called unimodality. A sequence $a_0, \ldots, a_t$ is unimodal if:

$$a_0 \leq a_1 \leq \ldots \leq a_l \geq a_{l+1} \geq \ldots \geq a_t$$

Then a sequence $a_t > 0$ is **log-concave** if $\forall i, a_i^2 \geq a_{i-1} \cdot a_{i+1}$.

Do Show that if a sequence is log-concave, then it is unimodal. But if it is unimodal, then it is not necessarily log-concave. Hence being log-concave is a stronger property.

Do prove that $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$, the nth row of Pascal's Triangle, is log-concave.

Generator function of a sequence (finite or infinite) $a_0, a_1, a_2, \ldots$:

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

E.g. $1 = (1, 1, 1, 1, \ldots)$ and $f_1(x) = \sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$. $a_n = \frac{1}{n!}$

Or take $a_n = \frac{1}{n!}$, where the generating function is e^x. (This portion was not entirely clear to me; I feel as if some details are missing.)

Do-Exercise find a closed-form expression for the general form of the fibonacci numbers $f(x) = F_0 + F_1 x + F_2 x^2 + \ldots = \frac{p(x)}{q(x)}$ where p, q polynomials. Find roots of $q(x)$.

$\mathbb{N} = \{0, 1, 2, \ldots\}$. Notation: $\dot\cup$ is the disjoint union, i.e. union of disjoint sets. Suppose $\mathbb{N} = A_1 \dot\cup \ldots \dot\cup A_k$, and A_i are arithmetic progressions, and $k \geq 2$. One possibility is $A_0 \dot\cup A_1$, where A_0 and A_1 are the even and odd numbers, respectively. For another example, take $A_i = \{r | r \equiv i \mod m\}$.

Fact: $0|0$ since $\exists c \in \mathbb{N}$ s.t. $0c = 0$, where any $n \in N$ is admissible as c.

Do Exercise $\forall k$, find $A_1, \ldots, A_k$ with $k-1$ distinct increments such that $A_1 \dot\cup \ldots \dot\cup A_k = \mathbb{N}$.

Challenge Problem Prove for $k \geq 2$, it is impossible to have all increments distinct. Hint is the context in which this problem was stated.

Challenge Problem if $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ is the generating function of the sequence $a_0, \ldots, a_n$ and all roots of f are negative reals, then $(a_i)_{i=0}^n$ is log-concave.

Example: take $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{m}$. They have a generating function: $\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{n}x^n = (1+x)^n$. The roots of this polynomial are $n \times -1$. **Binomial Theorem. Do-Exercise.**

Back to Sperner's Theorem: if $A_1, \ldots, A_m \subseteq [n]$, pairwise not comparable, then $m \leq \binom{n}{\frac{n}{\lfloor 2 \rfloor}}$. In this context, $F = \{A_1, \ldots, A_m\}$ is called a Sperner Family, and $\sum_{i=1}^m \frac{1}{\binom{n}{|A_i|}} \leq 1$. That's called the $LYM(B)$ inequality, after its authors: Bollobas - Lubell - Yamamoto - Meshalkin: though in reality Bollobas proved this before the other three.

Do: Show $LYM(B) \Rightarrow$ Sperner's Theorem. (One-liner.)
Proof of LYM(B). Arrange $[n]$ in a random order: $(a_1, \ldots, a_n)$. There are $n!$ ways to do this. We do it with uniform probability. Then we let X be the number of prefixes (first few of $(a_1, \ldots, a_n)$) that belong to F. And we note that $X \leq 1$. and then compute $E(X)$. The **Do** exercise fills out the details.

3 Week 1: Friday, April 4

Discrete Probability, Finite Probability Spaces, Events, Random Variables, Fisher's Inequality, Graph Terminology.

Quick review of **finite probability spaces**:
$\Omega \neq \emptyset$ "sample space": set of possible outcomes of an experiment. These outcomes, or elements of the sample space, are called elementary events.

e.g. flipping n coins: $|\Omega| = 2^n$.

e.g. picking a poker hand: $|\Omega| = \binom{52}{5}$

Probability distribution: $P : \Omega \to \mathbb{R}$, in such a way that $(\forall a \in \Omega)(P(a) \geq 0)$, and $\sum_{a\in\Omega} P(a) = 1$.

An **event** is some subset of the sample space: e.g. $A \subseteq \Omega$. And the probability of some event A is just $P(A) = \sum_{a\in A} P(a)$. Then $\overline{A} = \Omega \setminus A$, and $P(\overline{A}) = 1 - P(A)$.

Do Exercise: Modular equation: $P(A \cup B) + P(A \cap B) = P(A) + P(B)$.

Finally, $P(\emptyset) = 0$, obviously, and $P(\Omega) = 1$. And P is **uniform** if $(\forall a \in \Omega)(P(a) = \frac{1}{|\Omega|}$. In this case, $P(A) = \frac{|A|}{|\Omega|}$. "Naive Probability".

Random Variable: $X : \Omega \to \mathbb{R}$.
$N = |\Omega|$: N data. (I'm unsure of what this meant.)
Expected Value or Mean Value: $E(X) = \left(\sum_{a\in\Omega} X(a) \cdot P(a)\right)$. Weighted average of values of the random variable. The weights are the elementary probabilities.

Do $\min X \leq E(X) \leq \max X$
Do $E(X) = \sum_{y\in\mathbb{R}} y \cdot P(X = y)$ where $X = y : \{a \in \Omega \mid X(a) = y\}$.
Let's look at n coin flips, biased: $P(heads) = p$, $P(tails) = 1 - p$. $X = \#$ heads. Then $P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$

Then $E(X) = \sum_{k=0}^{n} k\binom{n}{k} p^k (1-p)^{n-k}$. We also note that (recalling Pascal's Identities)

$$k\binom{n}{k} = n \cdot \binom{n-1}{k-1}$$

Then $E(X) = n\sum_{k=1}^{n} \binom{n-1}{k-1} p^k (1-p)^{n-k}$.
Then we let $l = k - 1$. Then $E(X) = np\sum_{l=0}^{n-1} \binom{n-1}{l} p^l (1-p)^{n-1-l}$.
That is simply the binomial expansion of $np(p + (1-p))^{n-1} = np$. This should not come as a surprise.

We discuss the indicator variable of A:

$$\theta_A(a) = \begin{cases} 1 \text{ if } a \in A \\ 0 \text{ if } a \notin A \end{cases}$$

Which works much like a characteristic function. So:

$$\begin{aligned} E(\theta_A) &= 1 \cdot P(\theta_A = 1) + 0 \cdot P(\theta_A = 0) \\ &= \theta_A = 1 \\ &= P(A) \end{aligned}$$

Which shows us an important distinction:
Events have probabilities
Random Variables have expected value
Not the other way around, ever.

Now back to coinflips: Let

$$x_i = \begin{cases} 1 \text{ if heads} \\ 0 \text{ otherwise} \end{cases}$$

Then $X = \sum_{i=1}^{n} x_i$, and $E(x) = \sum E(X_i) = \sum p(x_i = 1) = \sum p = np$, as expected.

We mentioned linearity of expectation. $E(\sum c_i x_i) = \sum c_i E(x_i)$, where x_is are random variables. Proving this is quite straight-forward.

Do Prove the union bound: events $A_1, \ldots, A_k \subseteq \Omega$, $P(\cup A_i) \leq \sum p(A_i)$

HW Check online lecture notes for discrete math. Read up on finite probability spaces.

HW Monday Consider a club with 2000 members. Everybody gets a membership number, and a card. They shuffle the cards and give everyone a card. Member is **lucky** if the card number is equal to their year of birth. What is E(# of lucky members) = ? Note: club serves vodka to all club members legally, so $\forall$ members, age ≥ 21.

HW Fisher's Inequality: suppose we have a set system $A_1, \ldots, A_m \subseteq [n]$; $\forall i \neq j, |A_i \cap A_j| = t$. $\forall i, |A_i| > t$. WTS $m \leq n$. Note that $t \geq 1$, and t is a constant. We want to prove this with incidence vector. Show the incidence vectors of the clubs are linearly independent, over the reals. Useful observation: take the dot product of $v, w \in F^n$, where F is a field. Take two sets. Dot product of their incidence vectors are the elements of their intersection.

A graph is a 2-uniform hypergraph, i.e. every edge has two elements. $|V| = n$, $|E| = m$, so clearly $m \leq \binom{n}{2}$. The number of graphs on a given set of n vertices is $2^{\binom{n}{2}}$. The number of graphs on n vertices with m edges is: $\binom{\binom{n}{2}}{m}$.

K_n is the complete graph on n vertices. It has all possible $\binom{n}{2}$ edges.

The complement of $G = (V, E)$ is $\overline{G} = (V, \overline{E})$, where $\overline{E}$ is all the possible edges not in E, simply the complement of E. So $|E| + |\overline{E}| = \binom{n}{2}$.

The empty graph is the complement of the complete graph. It has n vertices and 0 edges.

A cycle of length n is denoted C_n.

A Path of length $n-1$ is denoted P_n. We note that the subscripts denote how many vertices a given path/cycle has.

Subgraph: $H = (W, F)$. Then $H \subseteq G$ iff $W \subseteq V$ and $F \subseteq E$.

Note: $C_3 = K_3$, the triangle. **Do**: find the max # of edges if $K_3 \nsubseteq G$, i.e. G is a triangle-free graph. (Confused; see course homepage for clearer problem statement)

4 Week 2: Monday, April 7

Probability Spaces, Independence, Markov & Chebyshev.

A probability space has two components: (Ω, P) where P is the probability distribution. We have events $A, B \subseteq \Omega$. Then we say that they are independent if $P(A \cap B) = P(A)P(B)$. Trivial events: $\emptyset, \Omega$. They are independent of everything.

We say that events are positively correlated if $P(A \cap B) > P(A)P(B)$ and negatively correlated if $P(A \cap B) < P(A)P(B)$. If we have more than 2 events, we have to be a little careful with our definition of independence:

Events $A_1, \ldots, A_k \subseteq \Omega$ are *mutually* or *fully* independent if:

$$(\forall I \subseteq [k])(P(\cap_{i \in I} A_i) = \prod_{i \in I} P(A_i))$$

Note that this makes 2^k conditions. Also note that this is different from pairwise independence. See Wikipedia.

Random variables $X, Y : \Omega \to \mathbb{R}$. We say that X, Y are independent if:

$$(\forall x, y \in \mathbb{R})(P(X = x \wedge Y = y) = P(X = x)P(Y = y))$$

By extension, we say that $X_1, \ldots, X_k$ are independent if

$$(\forall x_1, \ldots, x_k \in \mathbb{R})(P(X_1 = x_1 \wedge \ldots \wedge X_k = x_k)) = \prod_{i=1}^{k} P(X_i = x_i)$$

Do If $X_1, \ldots, X_k$ are independent RVs then $\forall I \subseteq [k]$, $\{x_i : i \in I\}$ independent.

Do events $A_1, \ldots, A_k \subseteq \Omega$ are independent iff their indicator variables are independent.

HW For Wednesday:
(a) Construct a prob. space (Ω, P) and events A, B, C that are pairwise but not **fully** (defn above) independent.
(b) Same thing with k events: $A_1, \ldots, A_k$. s.t. they are $(k-1)$ wise independent, but nt fully independent. added condition: $\forall i, P(A_i) = \frac{1}{2}$. hint: solutions should be simple; make the sample space as small as possible.

Do If there exist nontrivial independent events $A_1, \ldots, A_k \subseteq \Omega$, then $|\Omega| \geq 2^k$.

Challenge Problem
(a) If $n = 2^k - 1$, then construct n pairwise independent events of probability $\frac{1}{2}$ each over $|\Omega| = n + 1$.
(b) If $n = 2^k$, then construct n three-wise independent events also of probability $\frac{1}{2}$ each over

$|\Omega| = 2n$.

CH If $X_1, \ldots, X_k$ are non-constant (trivial?)[1] random variables that are t-wise independent, then it follows that $|\Omega| \geq \binom{k}{\lfloor \frac{t}{2} \rfloor}$.

So, full independence is an extremely restrictive and extremely powerful distinction. The power is shown by the following exercise:

DO If $X_1, \ldots, X_k$ are independent RVs then $E(\prod X_i) = \prod E(X_i)$.

For 2 random variables, we again have a definition of correlation: Take $E(XY)$ and $E(X)E(Y)$. If $>$, then we call them positively correlated. If $=$, then uncorrelated. If $<$, then negatively correlated.

For two random variables: if they are independent, then they are uncorrelated. If they are uncorrelated, then they are not necessarily independent. (We may say that independence is a stronger condition than being uncorrelated.)
HW Construct two RVs that are uncorrelated but not independent. Again, make the sample space as small as possible.

Useful inequality: Markov's inequality. Suppose $X \geq 0$, RV. Then

$$(\forall a > 0)(P(X \geq a) \leq \frac{E(X)}{a})$$

DO: one line proof of Markov's inequality

Variance of a Random Variable X. $Var(X) = E((X - E(X))^2) = E(X^2) - E(X)^2$. Note that $Var(x) = Covar(x, x)$. Conventionally, we write covariance between two random variables as $Covar(X, Y) = E(XY) - E(X)E(Y)$.

Chebyshev's Inequality
If X is a RV and $b > 0$, then $P(|X - E(X)| \geq b) \leq \frac{Var(x)}{b^2}$.

Proof let $Z = (X - E(X))^2 \geq 0$. By Markov's Inequality, the above is the exact same as $P(Z \geq b^2)$. Then by Markov, $P(Z \geq b^2) \leq \frac{E(Z)}{b^2} = \frac{Var(x)}{b^2}$.

DO We know that $Var(X) = E((X - E(X))^2)$. Prove $Var(X) = E(X^2) - E(X)^2$. Corollary of this is that $E(X^2) \geq E(X)^2$. This is true for all RVs, and is a consequence of the Cauchy-Schwarz inequality. **DO** Prove that this is equivalent to $|\overrightarrow{x} \cdot \overrightarrow{y}| \leq ||\overrightarrow{x}|| \cdot ||\overrightarrow{y}||$. Where $\overrightarrow{x} \cdot \overrightarrow{y} = \sum x_i y_i$ and $||\overrightarrow{x}|| = \sqrt{x \cdot x}$.

In particular, $Cov(X, X) = Var(X)$. Now here's something interesting: Let $X_1, \ldots, X_k$ be RVs, with $y = \sum_{i=1}^{k} X_i$. Then **DO** prove: $Var(y) = \sum_i \sum_j Cov(X_i, X_j)$, where the

[1] Event is trivial if $P(A) = 0$ or 1

diagonals ($i = j$) are the variances.

Corollary: if $X_1, \ldots, X_k$ are pairwise independent RVs, then $Var(\sum X_i) = \sum Var(X_i)$.

Notes: $Cov(X, Y) = 0$ iff X and Y are uncorrelated. In particular, if they are independent, then $Cov(X, Y) = 0$. This gives rise to more powerful conditions... (Like what? Notes are incomplete here; I couldn't keep up.)

Illustration of the power and the weakness of Chebyshev's Inequality: let's say we have n coin flips with probabilities p, $1 - p$. This kind of coin flip is a Bernoulli trial (possibly biased coin, independent, 2 outcomes). Let X be the number of heads. We already know $E(X) = np$. Then question is what is the variance. Let the indicator variable be

$$Y_i = \begin{cases} 1 \text{ if ith coin heads} \\ 0 \; tails \end{cases}$$

Then we have $X = \sum Y_i$ and **DO**: $Var(Y_i) = p(1 - p)$.
Then $Var(X) = np(1 - p)$.
(I could not keep up here at all, and I also couldn't tell what the writing on the board was. The following is incomplete and doesn't seem quite right — particularly the writing of $\sum^2$ seems unusual.)

$$\Rightarrow P(|X - np| \geq \sum np) \leq \frac{Var(x)}{(\sum np)^2} = \frac{np(1-p)}{\sum^2 n^2 p^2} = \frac{1-p}{p} \cdot \frac{1}{\sum^2} \cdot \frac{1}{n}$$

This is related to the weak law of large numbers. And we can reach that conclusion with another condition. (What was it?)

5 Week 2: Wednesday, April 9

No notes.

I was absent today. I would be grateful if someone could submit their notes for this day.

6 Week 2: Friday, April 11

Random Permutations, Erdős-Rado Arrow Symbol, Erdős-Szekeres Theorem.

Random Permutations
A permutation is a bijection, $\pi : [n] \to [n]$.
Pictorially, one can draw a directed graph that describes a permutation (cycles). Every permutation can be decomposed into unique cycles.
Talk about random permutations: then $|\Omega| = n!$ (number of permutations of a set).
Notation: $c(i, \pi)$ is the length of the cycle containing i.
Preliminary question: what is $P(1, \pi) = 1$? it's the probability that 1 maps to itself, so it is just $\frac{1}{n}$. And what is $P(1, \pi) = n$? There are $(n-1)!$ such permutations. See the cycle: there are $n-1$ places 1 can go, then there are $n-2$ places, etc. so the probability is $\frac{(n-1)!}{n!} = \frac{1}{n}$.
So based on this scant evidence, we conjecture that $P(c(1, \pi) = k) = \frac{1}{n}$.
HW Prove the above: $\forall k, P(c(1, \pi) = k) = \frac{1}{n}$.
HW What is the expected number of cycles? Prove $E(\#cycles) \sim \ln n$.
Use some variation on indicator variables.

Theorem (Baby-Ramsey): if we color the **edges** of K_6 in red/blue, then necessarily there exists a monochromatic triangle. (This gives rise to a fun game called the Ramsey Game, where the 2 players have six vertices to alternately color red/blue, and whoever creates a triangle in their own color loses.)
Proof Take a vertex. It has five outgoing edges. Then at least three are either blue or red. WLOG assume they're blue. Then take two of these three. the connecting edge must be blue or red. if blue, then we're done. else, it's red. That's true for all three pairs of blue edges. Then we have a red triangle and we are done. (If it is not immediately clear, drawing a picture helps.)

Notation (Erdős-Rado arrow symbol): $n \to (k, l)$ means that for all red/blue colorings of K_n, it will contain either a red K_k or a blue K_l. Example: $5 \not\to (3, 3)$.

Erdős-Szekeres Theorem: $\binom{k+l}{k} \to (k+1, l+1)$
$k = l = 2$, $\binom{2+2}{2} = 6 \to (3, 3)$ (Baby Version)
$k = 1, l+1 \to (2, l+1)$. Similarly, by symmetry, for $l = 1$ and $k+1$.

We note that $\binom{k+l}{k}$ is a binomial coefficient, so we can write it using pascal's triangle, where our boundary cases are the edges of the triangle. So we can do this by induction: assume $k, l \geq 2$. So **DO:** prove the Erdős-Szekeres Theorem by induction on $k + l$.

We use Pascal's Identity:

$$\binom{k+1}{k} = \binom{k + (l-1)}{k} + \binom{(k-1) + l}{k-1}$$

DO (a) $17 \to (3,3,3)$ and $(b)\lceil k!e\rceil \to \underbrace{(3,3,\ldots,3)}_{\text{k times}}$

The most interesting case is the symmetrical case, i.e. when $k = l$. So we investigate if $\binom{2k}{k} \to (k+1, k+1)$. We also note that $4^k > \binom{2k}{k}$, because $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

Do Prove $1 < \frac{4^k}{\binom{2k}{k}} < 2k+1$, and prove that $\frac{4^k}{\binom{2k}{k}} \sim c\sqrt{k}$ and find c.

Recall that the binomial coefficients are normally distributed with standard deviation $\sqrt{n}$. (Is this right? May not have noted this correctly.)

Let's denote 4^k by n, and then we can conclude $n \to (\frac{1}{2}\log_2 n, \frac{1}{2}\log_2 n)$.

Then the question is: for what k does $n \not\to (k,k)$? For example, $n \not\to (\sqrt{n}+1, \sqrt{n}+1)$. We are looking for a graph with l^2 vertices with a clique of size at most l and independent set of size at most l.

So make an $l \times l$ matrix, and let every row be a clique. Then clearly, to pick an independent set, we pick at most only one vertex from any row. Then there are l^l independent sets of size $\leq l$.

But can we reduce this any further? This question was investigated by Paul Turán. Erdős showed that $n \not\to (2\log_2 n + 1, 2\log_2 n + 1)$. This we will prove now. We want to show that there exists a graph on n vertices without K_l, $\overline{K_l}$, $l = 1 + 2\log_2 n$. We note that $\overline{K_l}$ is the complement of the clique, thereby it is an independent set.

We are going to look at a random graph. We use $\sim$ to denote adjacency. We define a graph by $(\forall i,j)(P(i \sim j) = \frac{1}{2}$, where the probabilities are independent. Then take $A \subseteq [n]$ with $|A| = t$. Then $G[A]$ is the subgraph induced on A. Then

$$P(G[A] \text{ is a clique}) = \frac{1}{2^{\binom{t}{2}}}$$

(? Not sure if noted correctly.)

Notation: $\omega(G)$ is the size of the maximum clique $= \alpha(\overline{G})$. Remember that $\alpha(A)$ denotes the maximum size of the independent set. So then

$$P(\omega(G) \geq t) = P((\exists A \subseteq [n])(|A| = t \wedge G[A] = clique))$$

$$= P(\cup_{|A|=t} \text{“G[A] = clique”})$$

So take the union bound:

$$\leq \sum_{|A|=t} p(G[A] = clique) = \frac{\binom{n}{t}}{2^{\binom{t}{2}}}$$

Prof. Babai lectured very quickly and I couldn't note down the computational steps. In any case, we prove a lemma: if $\frac{\binom{n}{t}}{2^{\binom{t}{2}}} \leq \frac{1}{2}$ then $n \not\to (t,t)$.

Proof

$$P(\omega(G) \geq t) < \frac{\binom{n}{t}}{2^{\binom{t}{2}}}$$

$$P(\alpha(G) \geq t) < \frac{\binom{n}{t}}{2^{\binom{t}{2}}}$$

$$P(\omega \geq t \vee \alpha \geq t) < 2 \cdot \frac{\binom{n}{t}}{2^{\binom{t}{2}}} \leq 1$$

That means it is not impossible. So sometimes it will happen, which gives as a proof of existence. This is an instance of proof using the probabilistic method.

We note that in constructing a random graph, we are "flipping $\binom{n}{2}$ coins" to decide adjacency, so $|\Omega| = 2^{\binom{n}{2}}$.

Every outcome is a graph.So it follows that $(\exists G)(\omega < t \wedge \alpha < t)$. And that exactly is the statement that $n \not\to (t, t)$. And then we have to estimate the quotient $\frac{\binom{n}{t}}{2^{\binom{t}{2}}}$ to show the values for this case...? (Again, it was hard to keep up, and I'm not exactly sure what the last bit is meant to be.)

Office Hours Thursday 4:30 in Ryerson 162.

7 Week 3: Monday, April 14

Probabilistic Method, Continuation of Friday's Lecture.

Erdős-DeBruijn

Challenge: an infinite graph is k-colorable iff every finite subgraph is k-colorable. 3 proofs:

- use Zorn's Lemma
- Goedel's Completeness Theorem of First-Order logic
- Tikhonof's Compactness Theorem

Discussion about the last homework: $\pi : [n] \to [n]$, where $c(i, \pi)$ = length of the π-cycle through i. (Notes on this part have been omitted.)

Last time: we started a discussion of Erdős' Theorem: $n \not\to (1 + 2\log_2 n, 1 + 2\log_2 n)$.
Lemma: if $\frac{\binom{n}{t}}{2^{\binom{t}{2}}} \leq \frac{1}{2}$ then $n \not\to (t, t)$.

Probabilistic Method: proof of existence by showing probability of the desired case occurring is > 0. We don't need an explicit construction.

We want to use this inequality: **DO** $\binom{n}{t} \leq \frac{n^t}{t!}$
WTS

$$\frac{2\binom{n}{t}}{2^{\binom{t}{2}}} \leq 1$$

then

$$\frac{2\binom{n}{t}}{2^{\binom{t}{2}}} \leq \frac{2}{t!} \cdot \frac{n^t}{2^{\frac{t(t-1)}{2}}} = \frac{2}{t!} \cdot \left(\frac{n}{2^{\frac{t-1}{2}}}\right)^t$$

So if $n \leq 2^{\frac{t-1}{2}}$ then (box-like symbol. unclear) $? \leq \frac{2}{t!} < 1 \to 0$ which is equivalent to if $\log_2 n \leq \frac{t-1}{2}$ then $1 + 2\log_2 n \leq t$. QED. (I will fill in the details later.)

So, almost all graphs have no clique or independent set of size $\geq 1 + \log_2 n$.

But this is very hard to construct explicitly. (Why?) We do $n = \binom{k}{3} \not\to (k + 1, k + 1)$ explicitly. Construction by ZS. NAGI, college classmate of Babai.

Notation: if S is a set, and $k \geq 0$, then $\binom{S}{k}$ is a set of k subsets of S. So $|\binom{S}{k}| = \binom{|S|}{k}$

Let $V = \binom{[k]}{3}$: all triples of $[k]$. Let $A, B \subseteq V$, where $|A| = |B| = 3$. We write that $A \sim B$ (A is adjacent to B) if $|A \cap B| = 1$.

HW: Prove that this graph has no clique and no independence set of size $k + 1$.

DO Show that k is asymptotically equal to $\sqrt[3]{6n}$ (from above: $n = \binom{k}{3}$).
DO find G s.t. $\alpha(G) \cdot \chi(G) \geq cn^2$ where c is a constant > 0.

8 Week 3: Wednesday, April 16

Mantel-Turán Theorem, Girth.

Discussion of last quiz. Product of n dice, independent: $(\frac{7}{2})^n$.

Mantel-Turán Theorem: If $G \not\supset K_3$ then $m \leq \frac{n^2}{4}$

1st Proof. Induction on n. Base case: $n \leq 2$; it is clear that this holds. Inductive step: (some intermediate steps of the proof were lost, making the conclusion unclear.) let $f(n)$ be this max. Remove two adjacent vertices: $f(n) \leq f(n-2) + (n-1) \leq \frac{(n-2)^2}{4} + (n-1)$.

2nd Proof. If $x \sim y$ (adjacent) then $\deg(x) + \deg(y) \leq n$: m inequalities.
Then $\sum_{x \sim y} \deg(x) + \deg(y) \leq nm$, and $\sum_{x \in V} (\deg(x))^2 \leq nm$.
Then by Cauchy Schwartz: $\frac{1}{n}(2m)^2 = \frac{1}{n}(\sum_{x \in V} \deg(x))^2 \leq \sum_{x \in V} (\deg(x))^2 \leq nm$,
Because $\sum_{x \in V} \deg(x) = 2m$.
So then $\frac{4m^2}{n} \leq nm$, implying $m \leq \frac{n^2}{4}$ and we are done.

DO Generalize this: let $t \geq 3$, and $G = (V, E)$ where $|V| = n, |E| = m$. Assume $G \not\supset K_t$. Then prove that m is less than or equal to the number of edges of the complete $(t-1)$-partite graph with nearly equal parts, i.e. that the sizes of every pair of parts differ by at most 1.

Turán's Theorem:

The complete $(t-1)$-partite graph is the extremal graph under the condition that $G \not\supset K_t$.

HW: Monday if $G \not\supset C_4$ then $m \leq cn^{3/2}$. There exists $c > 0$. Estimate c for large n. ("Kőváry-Turán-Sós").

Challenge: prove there exists $c' > 0$ such that for every $n > 1$, there exist graphs not containing C_4 such that $m \geq c'n^{3/2}$.

DO If T is a tree, then the number of edges of T is exactly $n - 1$.

Theorem: (Erdős) $(\forall k, g)(\exists G = (V, E)$ s.t. $girth(G) \geq g$ and $\chi(G) \geq k)$.

Definition of girth: length of the shortest cycle.

Chromatic number of a tree: obviously 2. Girth of a tree: infinite.

Probabilistic Method: Erdős-Ranyi random graph model:

$$G_{n,p},\ 0 \leq p \leq 1$$

$$(\forall i, j)(P(i \sim j) = p)$$

Then $E(m) = p\binom{n}{2}$.

We create a density parameter $p = \frac{n^\zeta}{n}$. $\zeta > 0$. $E(\deg(x)) = (n-1)p \sim n^\zeta$.

We know $\alpha \cdot \chi \geq \frac{n}{\alpha}$. So if α small, then χ large. We find a lower bound on chromatic number by finding an upper bound on the independence number.

P(given set of t vertices is independent) $= (1-p)^{\binom{t}{2}}$
P(there exists a set of t vertices that is independent) $\leq \binom{n}{t}(1-p)^{\binom{t}{2}} < 1$ for some $t \geq \frac{n}{k}$.

So $\binom{n}{t} \leq \frac{n^t}{t!}(1-p)^{\binom{t}{2}} = \frac{1}{t!}(n(1-p)^{\frac{t-1}{2}})^t$ and we need: $n(1-p)^{\frac{t-1}{2}} \leq 1$.

Excellent identity: **DO** $\forall x \in \mathbb{R}, 1 + x \leq e^x$.

So $n(1-p)^{\frac{t-1}{2}} \leq n \cdot e^{\frac{-p(t-1)}{2}} \leq 1$, and $\ln n - \frac{p(t-1)}{2} \leq 0$, so $\frac{p(t-1)}{2} \geq \ln n$.

$p \geq \frac{2\ln n}{t-1} \sim \frac{2k \ln n}{n}$, so let $n^\zeta > 2k \ln n$.

Now what about short cycles? Denote the number of triangles (K_3) with $\#\triangle$.

$E(\#\triangle) = p^3\binom{n}{3} < (pn)^3$. We don't want to remove more than half the vertices, so we want $(pn)^3 < \frac{n}{2}$. So we need $p^3 < \frac{n^{-2}}{2}$, so $p < \frac{n^{1/3}}{2n}$. So we can do the same thing not with triangles, but with cycles up to length g. Then we just need $(pn)^g < \frac{n}{2}$. Then $\frac{1}{g}$ will make a good ζ. But we choose ζ such that $0 < \zeta < \frac{1}{g}$. With such ζ, the expected number of cycles of length $\leq g$ is less than $\frac{n}{20}$. Because of Markov's inequality, the probability that we get more than $\frac{n}{10}$ cycles is $\leq \frac{1}{2}$.

And $P(\alpha \geq \frac{n}{k})$ is small — call it 0.1 — it goes to zero.

Then altogether, they have combined probability < 0.51. But the we remove at most $\frac{n}{10}$ points from short cycles, and the graph is still mostly intact. So $\alpha < \frac{n}{3k}$. Then $\chi \geq \frac{0.9n}{\frac{n}{3k}} = 30.9k > k$. (Something like that — the details of the end of this proof are not clear to me. It was not easy keeping up, so the above sketch of proof probably needs some careful checking.)

9 Week 3: Friday, April 18

Hypergraphs, Graph Isomorphisms, Automorphisms, Vertex-Transitivity, Permutations & Transpositions.

$H_1 = (V_1, E_1), H_2 = (V_2, E_2)$ Hypergraphs. Isomorphism $\phi : V_1 \to V_2$ bijection such that $(\forall E \subseteq V_1)(E \in E_1 \Leftrightarrow \phi(E) \in E_2)$.

Def $H_1 \simeq H_2$ if $\exists \phi : H_1 \to H_2$ isomorphism.

Theorem: if $G_1 \not\simeq G_2$ then $\exists$ proof of length $< C^{\sqrt{n \log n}}$ of this. (What do we mean by a proof of this length? Ref. concepts from computability/complexity theory.)

Automorphism of $H : H \to H$ isomorphism, a permutation of V. Then $Aut(H)$ is the automorphism group.

S_V : the group of all permutations of V, the symmetric group on V. $|S_V| = n!$.

$Aut(H) \leqslant S_V$ where we denote subgroup with $\leqslant$. We note that $Aut(H)$ has to be closed under composition.

Def. $G \leqslant S_V$ is a transitive group if $(\forall x, y \in V)(\exists \phi \in G)(\phi(x) = y)$.

Def. H is vertex-transitive if $Aut(H)$ is a transitive group: "all vertices are alike". Examples: triangular directed graph. Example of a non-v-t graph: path on 3 vertices.

HW Find smallest regular graph that is not vertex-transitive: fewest vertices, and then fewest edges.

Large graphs have few automorphisms: almost all graphs have just one automorphism (the identity automorphism). We note that "almost all" in this context means that as we let the number of graphs we consider tend to infinity, $\frac{\text{number of graphs satisfying the property}}{\text{number of graphs we consider}} \to 0$. This can also be phrased probabilistically.

Challenge: (1) Almost all graphs have $|Aut(G)| = 1$. Prove. Stronger Version:
(2) E(Aut(G)) = $1to(1)$, where (1) $\to 0$, i.e. it is $= 1 + \epsilon \forall \epsilon > 0$.
(3) Derive from (2) that $g_n \sim \frac{2^{\binom{n}{2}}}{n!}$
DO # non-isomorphic graphs on n vertices, g_n, is $\frac{2^{\binom{n}{2}}}{n!} < g_n < 2^{\binom{n}{2}}$
DO $\log_2 g_n \sim \ln \binom{n}{2} \sim \frac{n^2}{2}$
DO number of isomorphic copies of a graph G on V is $\frac{n!}{|Aut(G)|}$.

Let Rep_n be the set of representatives of isomorphism classes of graphs with n vertices. So $|Rep_n| = g_n$.

DO Then

$$\sum_{G \in Rep_n} \frac{n!}{|Aut(G)|} = 2^{\binom{n}{2}}$$

I.e.

$$\sum_{G \in Rep_n} \frac{1}{|Aut(G)|} = \frac{2^{\binom{n}{2}}}{n!}$$

DO If G is a vertex-transitive graph (true also for hypergraphs) then $\alpha(G) \cdot \chi(G) \leq n \cdot (1 + \ln n)$. Observation made by Mario Szegedy, student of L. Babai, here, some time ago.

If we have a vertex-transitive graph, it tends to have a hamiltonian cycle (cycle that goes through every vertex, i.e. cycle of length n). So take a connected vertex-transitive graph. Does that have a hamiltonian cycle?

Babai on Hamilton: "He went around, entertaining people at social functions: "here's the dodecahedron, find a Hamiltonian cycle." So they named this thing after him. Far more significantly, he established the quaternions." (Celebrated his finding of the quaternions with an act of vandalism: went out and carved $ij = k, ji = -k$ into a wooden bridge.)

Discussion of Petersen's Graph, one of the most remarkable graphs. (Responsible for "70%" of counterexamples in graph theory.) It has too many important characteristics to list here, so I suggest looking it up on the internet, e.g. here.

DO Show Petersen's Graph is vertex-transitive.
DO+ Aut(Pet) = 128. It has 120 automorphisms. Note that the automorphism group is isomorphic to S_5.

DO+ The automorphism group of the dodecahedron has size 120. The group of orientation-preserving automorphisms is isomorphic to A_5, i.e. has size 60.

DO Every permutation can be written as the transposition of two elements. (A transposition is a permutation that just swaps two points, i.e. holds the other points fixed.) i.e. transpositions generate the symmetric group.

In fact, just the neighbor-transpositions (swapping two neighbors) will generate the symmetric group.

DO Show that identity $\neq$ an odd number of transpositions.

Definitions: Even and odd permutations. Even: the permutation is a product of an even number of transpositions. Odd: product of an odd number of transpositions.

DO *Sam Lloyd's 15 puzzle*: prove that it works for exactly $\frac{1}{2}$ of starting positions. (use

even and odd permutations).

CH F_n: fixed-point free permutations of n elements. Decide whether

$$\underbrace{|F_n \cap A_n|}_{\text{Even fixed-point free Permutation}}$$

is greater than, equal to, or less than

$$\underbrace{|F_n \setminus A_n|}_{\text{Odd Fixed-Pt Free Perms}}$$

Hint Compute the difference.

NEXT TEST: Wednesday.

We define one more concept: a **tournament** is an oriented complete graph. Every edge is directed in exactly one direction. So there are $2^{\binom{n}{2}}$ tournaments on n vertices. **DO** Prove all tournaments have a hamiltonian path.

DO If strongly connected, then $\exists$ H-cycle.

10 Week 4: Monday, April 21

Diameter of a Graph, Notes Incomplete.

distance in a graph: length of the shortest path
diameter of a graph: maximum distance(x,y) between any two vertices

d-dimensional cube has 2^d vertices. as a graph, it is regular of degree d. number of edges: $d \cdot 2^{d-1}$. We call the d-dimensional cube Q_d. $diam(Q_d) = d$. diameter of a disconnected graph: infinite.

diameter of a random graph is a random variable. (See diameter as a function, and note that a given random graph is an outcome in our sample space).

theorem: almost all graphs have diameter 2. (we don't assume that they're necessarily connected): almost all are connected. (However, the expected diameter nonetheless is infinite.)

$$\lim_{n\to\infty} p_n = 1$$

where P_n = P(random graph on n vertices has diam = 2)

we'll prove this by splitting it into lots of cases and then using the union bound

diam(G) = 1 iff G is complete, probablity of that is $\frac{1}{2^{\binom{n}{2}}}$

we show by negation: WTS: P(diam(G)$\geq$ 3) $\to$ 0. we show something stronger: $\forall x, y \exists z$ s.t. $x \sim z, y \sim z$.

(I could not take notes for the rest of class. I'd be grateful if someone could fill this in.)

11 Week 4: Wednesday, April 23

Steiner Triple Systems, Fano Plane, Affine Lines.

Steiner triple system (STS): 3-uniform hypergraph s.t. $(\forall x, y \in V)(\exists$ unique edge $E)$ such that $x, y \in E$.

Famous example: "Fano Plane".
DO $|Aut(Fano)| = 168$. Second smallest nonabelian simple group. (Simple group: no nontrivial subgroup.) Smallest: A_5, where $|A_5| = 60$. Geometric figure associated: dodecahedron.

Observation:
number of points of an STS is necessarily odd.

DOif a STS of n points exists then $n \equiv 1$ or $3 \mod 6$. **Theorem:** this is iff, not just if.

DO+ Find an STS with 13 points.

Generalize such cubes to d dimensions: so $n = 3^d$. Take $F_3 = \{0, 1, 2 \mod 3\}$. Over $\mathbb{F}_3$ we look at the d-dimensional vector space: $\mathbb{F}_3^d = \{(x_1, \ldots, x_d) \mid x_i \in \mathbb{F}_3\}$. So take the affine lines (all the one-dimensional subspaces of $\mathbb{R}$, that go through the origin, shifted).

So a line through a with directional vector v: $l(a, v) = \{a + tv \mid t \in \mathbb{F}_3\}$. Where a, v vectors. **DO** affine lines in $\mathbb{F}_3^d$ is a STS. So now we have infinitely many examples. ("Linear algebra is the n-dimensional version of geometry.")

DO: These STSes have (doubly) transitive group of automorphisms.

Back to the game SET: SET is a STS with 81 points. Such a STS is just $\mathbb{F}_3^4$ with its affine lines as edges.

In SET, we are given a number of cards, and look for how many we can put out without forming a SET. I.e. we are studying the independent set. Then we are interested in $\alpha(A(d, 3))$, where d is the dim, and 3 denotes $\mathbb{F}_3$. We write $A(d, 3) = (\mathbb{F}_3^d, L_d)$, where L_d is the set of affine lines in $\mathbb{F}_3^d$.

HW So prove that $\alpha_{k+l} \geq \alpha_k \cdot \alpha_l$.

DO: Fekete's Lemma: If $a_i > 0$, $a_{k+l} \geq \alpha_k \cdot \alpha_l$ then $\exists L = \lim a_k^{1/k} = \sup a_k^{1/k}$.

HW $2 < L \leq 3$. Give us the best lower bound you can. Is $L = 3$? Major open problem. Research is OK, just give a reference.

12 Week 4: Friday, April 25

k-Paradoxical Tournaments, Paley Tournaments.

Question from Wednesday's test: take an r-uniform hypergraph with $m \leq 2^{r-1}$ for $r \geq 2$, WTS that it is then 2-colorable. We want to color the vertices such that no edge is monochromatic. So we color each vertex red/blue at random. E = Edge. Then

$$P(E \text{ monochromatic}) = \frac{1}{2^{r-1}}$$

Let $X = \#$ of monochromatic edges. Then $X = \sum_{i=1}^{m} Y_i$ where

$$Y_i = \begin{cases} 1 \text{ ith edge monochromatic} \\ 0 \text{ otherwise} \end{cases}$$

Then $E(X) = \sum E(Y_i) = \sum P(Y_i = 1) = \frac{m}{2^{r-1}} \leq 1$. So we are done if $m < 2^{r-1}$, as then $E(X) < 1 \Rightarrow \min X < 1 \Rightarrow \min x = 0$ i.e. $\exists$ outcome s.t. $X = 0$, where an outcome is a coloring. Then take the case in which $m = 2^{r-1}$. $E(X) = 1$. (Not sure how to handle this case, lost track.) Is it possible that $X \geq 1$ always? $\Rightarrow X = 1$ always. No: $\exists$ coloring $X \geq 2$. (? Unclear. Not sure exactly what this meant.)

Previous homework problem: k-paradoxical tournaments.

k-paradoxical tournament: (V, E) with $k < n$, $(\forall A \subseteq V)(|A| = k \Rightarrow (\exists x \in V)(x \to A))$. Where the notation $x \to A$ means x beat everyone in A.

$$P(x \to A) = \frac{1}{2^k}$$

$$P(x \not\to A) = 1 - \frac{1}{2^k}$$

$$P((\forall x)(x \not\to A)) = \left(1 - \frac{1}{2^k}\right)^{n-k}$$

Union Bound:

$$P((\exists A)(|A| = k \text{ and was not beaten})) \leq \binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k}$$

Lemma if $\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} < 1$ then there exists a k-paradoxical tournament on n vertices.

Use: $\forall x, 1 + x \leq e^x$ and we estimate $\binom{n}{k}$ with $\frac{n^k}{k!}$. Then we want to know if $\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} < \frac{n^k}{k!} \cdot e^{\frac{-n-k}{2^k}} <_? 1$. Routine algebra to reduce to $n^k <_? e^{\frac{n}{2^k}}$, then $k \cdot 2^k <_? \frac{n}{\ln n}$. Then take another log, so we have $\ln k + k \ln 2 <_? \ln n - \ln \ln n$, and we can take asymptotic values:$k \ln 2 \sim \ln k + k \ln 2 <_? \ln n - \ln \ln n \sim \ln n$, because parts of this dominate as $k \to \infty$. So we have $k \ln 2 <_? \ln n$. But these inequalities are the wrong way, so that's not helpful.

So we refer to the fact that over all reals, $\frac{x}{\ln x}$ is monotonically increasing, so then there exists precisely one x such that $k \cdot 2^k = \frac{x}{\ln x}$. We take some computational steps to get to $x \sim \ln 2 \cdot k^2 \cdot 2^k$. So ($\forall k \geq k_0$(∃k-paradoxical touranment on$k^2 \cdot 2^k$ vertices).

Explicit Construction: **Paley Tournament** on p vertices where $p \equiv -1 \mod 4$. The set of vertices $V(P_p) = \mathbb{F}_p$: field of order p: $\{0, \ldots, p-1\}$ mod p. We say that $x \to y$ if $y - x$ is a quadratic residue mod p. So take $p = 7$. The modulo 7 residue classes are $0, \pm 1, \pm 2, \pm 3$, and that is all. Correspondingly, the quadratic residues are $1, 2, 4$ and the non-residues are $0, 3, 5, 6$: we don't have to check all possible values for the non-residues. Then we draw a diagram. Then what does it look like if we make 1 the vertex with outgoing edges? It's the same thing, just rotated: so it is a vertex-transitive graph.

What is the significance of $p \equiv -1 \mod 4$? Well, $p \equiv -1 \mod 4 \Rightarrow (\frac{-1}{p}) = -1$, where the division-like symbol is the Legendre Symbol.

If it was not the case that $p \equiv 1 \mod 4$, then we would have a symmetric relation (if $y \sim x$ then $x \sim y$), which would be exactly what we do not want. The Legendre symbol is multiplicative and -1 is not a quadratic residue, and this is all we need to guarantee our edge-condition.

Now we make a deterministic (non-probabilistic) construction. We want that $A = \{a_1, \ldots, a_k\} \Rightarrow (\exists x)(\forall i)((\frac{x-a_i}{p}) = 1)$ (Legendre Symbol, not division). We have a theorem: the number of such values of x is $\sim \frac{p}{2^k}$. In other words, our deterministic proof involves showing that the number of such values are asymptotically equal to what we would expect if it were random.

Def: A multiplicative character of $\mathbb{F}_p$ is $\chi : \mathbb{F}_p \to \mathbb{C}$ such that $\chi(0) = 0$, $\chi(1) = 1$, and $\chi(ab) = \chi(a)\chi(b)$. (This seems particularly related to abstract algebra.)

DO if $a \in \mathbb{F}_p^x = \mathbb{F}_p \setminus \{0\}$ then $\chi(a)$ is a $(p-1)$st root of unity.

Def: $z \in C$ is a kth root of unity if $z^k = 1$. in particular, if a number z is a kth root of unity, then $|z| = 1$.

Def: z is a primitive kth root of unity: $z^k = 1$ but $z^j \neq 1$ for $1 \leq j \leq k$, i.e. for the smallest k. This means that every kth root of unity is also a primitive root of unity for some other l, where l is a divisor of k.

Then we say that k is the order of z, i.e. $o(z) = k$.

DO $o(\frac{1}{z}) = o(z)$ and $o(z_1 z_2) | lcm(o(z_1), o(z_2))$.

If the orders of z_1 and z_2 are coprime, then $o(z_1 z_2) = o(z_1)o(z_2)$.

DO+ $\frac{lcm(o(z_1),o(z_2))}{gcd(o(z_1),o(z_2))}$

13 Week 5: Monday, April 28

Fields, Integral Domains, Linear Algebra.

Algebraic concept of a **Field** — look it up if unacquainted. These are the scalars in a vector space that enable us to do linear algebra. Some infinite fields: $\mathbb{Q}, \mathbb{C}, \mathbb{R}$. **DO:** show that $\mathbb{Q}[2] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field. The part that is not immediately clear is that it satisfies the property of multiplicative inverses. Field $Q[i]$: Gaussian Rationals.

Finite fields: first example: $\mathbb{F}_p$ field of order p, where p prime. This is also known as $\mathbb{Z}$ mod $p, \mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}$, or the modulo p residue classes.

Exercise: consider this field $\mathbb{F}_p[i] = \{a + bi \mid a, b \in \mathbb{F}_p\}$. It is a field for infinitely many primes and is not a field also for infinitely many primes. **DO** For what primes is this a field?

DO If R is a finite integral domain, then R is a field. This is an interesting property: contemplate the difference made by (in)finity.

$\mathbb{H}$: the quaternions: a non-commutative field (division ring): look it up. It is 4-dimensional over the reals. Wedderburn's (little) Theorem: a finite division ring is a field.

Take $\mathbb{F}_p[i]$. We have $|\mathbb{F}_p[i]| = p^2$ because for a, b we have p choices each.

We now discuss the Eulerian Rationals. Let $\omega^3 = 1$, and $\omega \neq 1$. Then $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, the primitive third root of unity. Then define $\mathbb{Q}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Q}\}$: the Eulerian Rationals. Look them up to see their interesting properties.

We also discuss the Eulerian Integers (look them up) and make the multiplication table for $\mathbb{F}_4 : (0, 1, \omega, \omega + 1)$.

Theorem (Galois): field of order q exists iff q is a prime power, and if it exists, it is unique up to isomorphism.

Let R be an integral domain, $a \in R$, and call n_a the smallest positive integer s.t. $n_a \cdot a = 0$, i.e. $\underbrace{a + \ldots + a}_{n_a}$. If there is no such n_a, then we define $n_a = 0$.

DO n_a is the gcd of $\{k \mid k \cdot a = 0, k \in \mathbb{Z}\}$. (This is a homogeneous definition of the notion above.)

Remark: in number theory, 0 and ∞ are frequently synonyms. This is because the 'size' of a number is not given by the $<$ relation, but rather by a hierarchy of divisibility: as 0 is a multiple of every number, 0 sits at the top of the hierarchy.

DO If R is an integral domain then:

(1) $(\forall a, b \neq 0)(n_a = n_b)$
(2) This number (the characteristic) is either 0 or prime

DO For a field $\mathbb{F}$, if $\text{char}(\mathbb{F}) = p$, then $\mathbb{F}_p$ is a subfield of $\mathbb{F}$. If $\text{char}(\mathbb{F}) = 0$, then $\mathbb{Q}$ is a subfield of $\mathbb{F}$.

If we have a field $\mathbb{F}$ which is a subfield of another field $\mathbb{G}$, then $\mathbb{G}$ is a vector space over $\mathbb{F}$. If $\dim_{\mathbb{F}} \mathbb{G} = k$ then $|G| = |F|^k$.

Implication: if $\mathbb{F}$ is a finite field of characteristic p, then $|\mathbb{F}| =$ power of p.

Terminology: finite characteristic is a characteristic p, and infinite characteristic is characteristic 0.

$\mathbb{F}_p[x]$: the polynomial over $\mathbb{F}_p$, and $\mathbb{F}_p(x)$: the polynomial fractions ("rational functions") over $\mathbb{F}_p$. Recall that $\mathbb{Q}$ is a set of **equivalence classes**.

DO: Review linear algebra. We'll be specifically interested in vector spaces over finite fields.

$\mathbb{F}$ is a field, $\mathbb{F}^d$ is a d-dimensional space over $\mathbb{F}$.

Dot Product: two vectors $x = (x_1, \ldots, x_d), y = (y_1, \ldots, y_d) \in \mathbb{F}^d$. Then $x \cdot y = \sum_{i=1} x_i y_i$
Perpendicular: if $x \cdot y = 0$. Denoted $x \perp y$.
Perp: $x^\perp = \{y \mid x \cdot y = 0\}$
Isotropic: if $x \perp x$, $x \neq 0$.

Isotropic vectors: in $\mathbb{C}^2 = (1, i)$, in $\mathbb{F}_5^2 : (1, 2)$.

DO For what p is there an isotropic vector in $\mathbb{F}_p^2$?

$U \subseteq F_p^d$ is a subspace if it is closed under linear combination. And it always necessarily contains at least 0, because the empty linear combination is 0. We denote being a subspace by $U \leqslant F_p^d$.

Let $S \subseteq F_p^d$. Then $S^\perp = \cap_{x \in S} x^\perp$.

DO Show $S^\perp \leqslant F_p^d$.
HW If $U \leqslant \mathbb{F}_p^d$, then $\dim U + \dim U^\perp = d$.
DO: use this to prove Eventown.

14 Week 5: Wednesday, April 30

Ramsey's Theorem, Weil's Character Sum Estimate, Legendre Symbol, Paley Tournament.

I was absent. These notes are adapted from Alex Dunlap's.

Ramsey's Theorem:
$K_n^{(r)}$: complete r-uniform hypergraph. $\binom{n}{r}$ edges. Color the edges, looking for sets in which all edges are the same color. $n \to (s_1, \ldots, s_n)^(r)$ if for any k-coloring $A_1, \ldots, A_k$ of the edges of $K_n^{(r)}$ we have $(\exists i)(\exists B \leq V)(\binom{B}{r} \subseteq A_i)$. (With $|B| = S_i$ and no superscript r=2).

Theorem (Ramsey): $(\forall r)(\forall k)(\forall s_1, \ldots, s_k)(\exists n)(n \to (s_1, \ldots, s_k)^{(r)})$.
DO $k = 2, k = 3$.
Multiplicative character of $\mathbb{F}_q$, where q is a prime power. $\chi : \mathbb{F}_q \to \mathbb{C}$. $\chi(0) = 0, \chi(1) = 1, \chi(ab) = \chi(a)\chi(b)$. χ_0: the principal character.

In $\mathbb{F}_p$,

$$\chi(a) = \left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \neq 0 \ QR \\ -1 \text{ if } a \neq 0 \text{not a quadratic residue} \\ 0 \text{ if } a = 0 \end{cases}$$

The order of χ is the smallest k so that $\chi^k = \chi_0 = lcm(o(\chi(a)))$. **DO** $\exists a$ s.t. $o(\chi) = o(\chi(a))$.

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x(x+10)}{p}\right) = 1$$

Andre Weil's Character Sum Estimate
$\sum_{a \in \mathbb{F}_q} \chi(f(a))$. $f(x)$: polynomial with its coefficients in $\mathbb{F}_q$. Is there cancellation? If f is a square of a polynomial, or constant times this, then we do not get cancellation. If $ord(\chi) = k$ ten $f = cg^k$ prevents cancellation.

Theorem (Weil): If $f \in \mathbb{F}_q[x]$ and f cannot be written as cg^k, $\deg f = d$, then $|\sum_{a \in \mathbb{F}_q} \chi(f(a))| \leq (d - 10\sqrt{q}$.

Paley Tournament: q-odd prime power, $q \equiv -1 \mod 4$.
DO Prove that this actually defines a tournament.
$a \to b$ if $\chi_2(b - a) = 1$.
$N = (\#x)(x \to A)$ NTS $N > 0$.
Claim $N \approx q/2^d$.

Want $\chi(x - a_1) = \ldots = \chi(x - a_d) = 1$.

$$\Leftrightarrow F((\chi(x - a_1) + 1) \ldots (\chi(x - a_d) + 1) = \begin{cases} 2^d \text{ if } x \to A \\ 0 \text{ if } \exists i \text{ s.t. } a_i \to x \\ 2^{d-1} \text{ if } x \in A \wedge x \to A \setminus \{x\} \end{cases}$$

Where the 2^{d-1} case occurs at most once.

Want to compute $\sum_{x\in\mathbb{F}_q} F(x) = 2^d N$

$F(x) = \sum_{I\subset[N]} \prod_{i\in I} \chi(x - a_i 0 = \sum_{I\subset[n]} \chi(\underbrace{\prod_{i\in I}(x-a_i)}_{=f_I(x)})$

$= \sum_{I\subset[n]} \chi(f_I(x))$

$f_\emptyset(x) = 1$. $\chi(f_\emptyset(x)) = 1$.
$\sum_{x\in\mathbb{F}_q} \chi(f_\emptyset(x)) = q$, main term.

15 Week 5: Friday, May 2

Notes currently missing — to be inserted. On Weil's Character Sum Estimate.

Notes on paper, will be inserted soon. Update August 2, 2014: I confess these may have been lost. Checking my files...

16 Week 6: Monday, May 5

Linear Algebra, Finite Projective Planes, Incidence Geometries.

Review of homework problem: proving that $\dim U + \dim U^\perp = d$. Many solutions used the Gram-Schmidt procedure or Orthonormal bases, which are not admissible. (Do they work in a general field?)

$x \perp U \Leftrightarrow x \perp$ a basis of U. So let $u_1, \ldots, u_k$ be a basis of U. We represent $x = (x_1, \ldots, x_d)$. We use this to set up a system of homogeneous linear equations:

$$\begin{aligned} x_1 u_{11} + \ldots + x_d u_{1d} &= 0 \\ \vdots \qquad\qquad & \vdots \\ x_1 u_{k1} + \ldots + x_d u_{kd} &= 0 \end{aligned}$$

$\{x \mid x \cdot A = 0\} = U^\perp \leqslant \mathbb{F}^d$: the set of solutions is $U^\perp$. (Every independent constraint reduces the number of solutions.) The rows are linearly independent, so the rank(A) is k. By the Rank-Nullity Theorem, $\dim U^\perp$ =nullity$(A) = d-$rank(A). ✓

We now discuss **Finite Projective Planes**. An **Incidence Geometry** is a set $G = (P, L, I)$, where P are points, L are lines, and I is the incidence relation. This is really just a bipartite graph $G = (P + L, I)$. We can make the Fano Plane into such a graph: a regular bipartite graph of degree 3. The "Levi Graph of Geometry".

DO dual of a projective plane is a projective plane. Notably, Dual(Fano) = Fano.

Projective plane over a field $\mathbb{F}$, finite or infinite. 1-dim subspaces of $\mathbb{F}^3$: points of a projective plane $PG = (2, \mathbb{F})$ where the 2 denotes the dimension and $\mathbb{F}$ denotes the field.

2-dimensional subspaces are lines. Each projective point has a triple of homogeneous coordinates $x = (x_1, x_2, x_3) \neq 0$. $x \sim y$ if $(\exists c)(x = cy)$. Thus, points form equivalence classes.

17 Week 6: Wednesday, May 7

Graph Theory, Finite Projective Planes, Bruck-Ryser Theorem, (Orthogonal) Latin Squares.

Review of last quiz:

Know: for almost all graphs, $\alpha(G) < 1 + 2\log_2 n$. Prove: for a.a. graphs, $\chi(G) > \omega(G)^{100}$.

$G \leftrightarrow \overline{G}$, $\alpha(G) = \omega(\overline{G})$.

Now, $\chi(G) \geq \frac{n}{\alpha(G)} \geq \frac{n}{1+2\log_2 n}$. (Second $\geq$: almost always). Then we want to know if this is greater than $(1 + 2\log n)^{100}$, which is almost always $\geq \omega(G)^{100}$. This is the case for sufficiently large n.

Then we had $\mathbb{F}_p[i] = \{a + bi \mid a, b \in \mathbb{F}_p\}$. We claim that this is a field iff $\left(\frac{-1}{p}\right) = -1$. We prove this: $\Leftarrow$. $(a + bi)(a - bi) = a^2 + b^2 \neq 0$. Brief computation in complex numbers follows. The other direction: $u \in \mathbb{F}_p$, $u^2 - 1(p)$. $(u - i)(u + i) = u^2 - i^2 = -1 - (-1) = 0$.

For the third problem, adjacency depends solely on the difference, and any automorphism doesn't change the difference. That proves that it is vertex-transitive. If we want to prove that it is edge-transitive, we realize that an automorphism is scaling by a factor that is a quadratic residue, preserving the edge.

DO Fix x. If G is vertex-transitive and σ is a random automorphism (a uniform random member of the group of automorphisms), then $\sigma(x)$ is a random vertex.

Last problem: our famous inequality, $\alpha(G) \cdot \chi(G) \geq n$ for all graphs. If G is vertex-transitive, then $\alpha(G)\chi(G) < n(1 + \ln n)$. Proof: we take A, a maximum independent set, i.e. such that $|A| = \alpha(G)$. We will pick $\sigma_1, \ldots, \sigma_t$ from $\Omega = Aut(G)$. Then the probabilities are uniform because of vertex-transitivity. So $P_{\sigma_i}(x \notin \sigma_i(A)) = P(\sigma_i^{-1}(x) \notin A) = 1 - \frac{\alpha}{n}$. So $P(x \notin \cup_{i=1}^{t} \sigma_i(A)) = \left(1 - \frac{\alpha}{n}\right)^t$ because the σ_i are independent. We use the usual trick: this is less than $e^{-\frac{\alpha t}{n}}$. Then what is the probability that x is not in this union? $P((\exists x)(x \notin (above)) \leq m\left(1 - \frac{\alpha}{n}\right)^t < ne^{\frac{-\alpha t}{n}} \leq 1$.

Lemma If $ne^{-\frac{alphat}{n}} \leq 1$ then $\chi(G) \leq t$.

Then comes the routine algebra (the combinatorics is done), so we get $n \leq e^{\alpha t/n}$ so $\ln n \leq \frac{\alpha t}{n}$ so $n \ln n \leq \alpha t$, so $t \geq \frac{n \ln n}{\alpha}$. So $\chi \leq \left(\frac{n \ln n}{\alpha}\right) \leq \frac{n(1+\ln n)}{\alpha}$.

So that was the test. Now back to finite projective planes: for what numbers do we have planes of that order? I.e. $\Pi = \{n \mid \exists$ finite projective plane of order n$\}$. We have that $\Pi \supseteq \{$prime powers$\}$. However, not all of these are Galois planes. No other number is known to belong to Π. How many other numbers do we know that do not belong to Π? This is a known result, the Bruck-Ryser Theorem: if $n \equiv 1$ or $n \equiv 2 \mod 4$ (mod 4, of course, as

always) and $n \in \Pi$ then $(\exists a, b)(n = a^2 + b^2)$. If n is not a sum of two squares, then it is not in Π. If it is the sum of two squares, then we don't know. If $n \not\equiv 1$ or 2, then we also don't know.

We make a list of numbers:
in Π: $2, 3, 4, 5, 7, 8, 9$
not in Π: $6, 10$
?: for a long time, 10, and 12. All the other numbers not taken care of by Bruck-Ryser are unknown.

Exponential Growth: *nothing* is sustainable. People don't understand exponential growth.

Latin Square A square of $n \times n$. Every row and every column contains the numbers 1 through n. Orthogonal Latin Squares: a pair of latin squares is orthogonal if when superimposed we get another pairwise latin square: e.g.

$$\begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

give the orthogonal latin square

$$\begin{bmatrix} 1,1 & 3,3 & 2,2 \\ 3,2 & 2,1 & 1,3 \\ 2,3 & 1,2 & 3,1 \end{bmatrix}$$

Interesting Proposition: **DO**: Suppose $A_1, \ldots, A_k$ are $n \times n$ orthogonal latin squares. Then want to show $(1) k \leq n - 1$, $(2) \exists k = n - 1 \iff \exists$ projective plane of order n.

18 Week 6: Friday, May 9

Kőváry-Turán-Sós Theorem, Quadratic/Arithmetic/Geometric Mean, Jensen's Inequality, Matching, Konig-Hall Theorem.

Kőváry-Turán-Sós: i $G \not\supset C_4$, then $m = O(n^{3/2})$, then there exists $c > 0$ such that $m \leq cn^{3/2}$. The key observation to solving this is that no C_4 means that $(forall x, y)$ x and y have at most 1 common neighbor. Then we count (N) the paths of length 2 in 2 ways. So then $N \leq \binom{n}{2}$, counting by (a, c). But if we count by b, then $N = \sum_{b \in V} \binom{\deg(b)}{2}$. So $\binom{n}{2} \geq \sum_{b \in V} \binom{\deg(b)}{2}$. Also note that this is trivially less than $\frac{n^2}{2}$, and note that $\sum_{b \in V} \binom{\deg(b)}{2} = \frac{1}{2} \sum_{i \in V} (d_i^2 - d_i) = \frac{1}{2}(\sum d_i^2) - \frac{1}{2} \sum d_i$, where $d_i = deg(i)$. So then $n^2 > (\sum d_i^2) - 2m$, i.e. $n^2 + 2m > \sum d_i^2$.

We distinguish between the **quadratic mean** and the **arithmetic mean**. Then it's an easy exercise that the arithmetic mean is less than or equal to the quadratic mean. This is a consequence of Cauchy-Schwarz. **DO:** Prove this directly, without reference to Cauchy-Schwarz.

Continuing: then $n^2 + 2m > \sum d_i^2 \geq \frac{1}{n}(\sum d_i)^2 = \frac{1}{n}(2m)^2$. So $n^3 + 2mn > 4m^2$. So $n^3 > 4m^2 - 2mn$ (Great confusion ensued in the next few minutes — apparently a blackboard mistake was made somewhere. Calculations have been skipped, and an n-term was dropped somewhere.) Anyway, we get $(n^3 + \frac{n^2}{4})^{1/2} > 2m - \frac{n}{2}$, yielding that $m < \frac{1}{2}(\frac{n}{2} + (n^3 + \frac{n^2}{4})^{\frac{1}{2}}) \sim \frac{1}{2} n^{3/2}$.

Another way is via **Jensen's Inequality**. Take $f(x)$ convex. If $\exists f''$ then convex $\Leftrightarrow f''(x) \geq 0$ (**Do**.) For every lambda $0 \leq \lambda \leq 1$ and $x < y$, then $f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda) f(y)$. If f is continuous, then $f(\frac{x+y}{2}) \leq \frac{f(x)+f(y)}{2}$ implies the previous condition. (**DO**.)

Jensen's inequality then states that if f is convex, $\forall x_1, \ldots, x_k$, $f(\frac{x_1, \ldots, x_k}{k}) \leq \frac{f(x_1) + \ldots + f(x_k)}{k}$. **DO.**

Moreover, **DO:** show that Jensen's inequality immediately gives that the arithmetic mean is less than or equal to the quadratic mean.

More demanding, however, is the geometric mean: $\sqrt[n]{x_1, \ldots, x_n}$ for $x_i > 0$. **DO:** show that the geometric mean is less than or equal to the arithmetic mean. (Use Jensen's Inequality.)

We have that $\binom{x}{2}$ convex (it is not restricted to integer values). So $\frac{n}{2} > \frac{\sum \binom{d_i}{2}}{n} \geq$ (Jensen) $\binom{\frac{\sum d_i}{n}}{2} = \binom{\frac{2m}{n}}{2} = \frac{1}{2} \cdot \frac{2m}{n} \cdot (\frac{2m}{n} - 1)$

This also ends up yielding, using some previous observations (inequalities), that $m < \frac{1}{2}(n^{3/2} + n)$.

Anyway, that was an old homework. Now, the new homework was to show that this bound

is on the right order of magnitude. So suppose $n = 2(q^2 + q + 1)$, where q is a prime power. So we construct a bipartite levi graph from $PG(2, q)$, with $\frac{n}{2}$ vertices in each part (one part P, the other part L). We then know that there cannot be a C_4 in this graph, as it implies two points and two lines in this cycle. So the number of edges will be $\underbrace{(q^2 + q + 1)}_{\frac{n}{2}}(q+1) > (\frac{n}{2})^{3/2}$.

Remarks on prime numbers: they are remarkably dense. If we pick a random number between 1 and n, the probability that it is a prime is $\frac{1}{\ln n}$. This yields some very high probabilities: even if we enumerate the number of elementary particles in the universe (about 2^{500}) and pick one at random, the probability that it is a prime is greater than $\frac{1}{500}$. Remarkable! **DO** Prime Number Theorem implies $p_{n+1} \sim p_n$.

Bertrand's Postulate: Proven by Chebyshev.

Prime Number Theorem: proven in 1896, $\pi(x) \sim \frac{x}{\ln x}$. 40 years previous, Chebyshev showed that $\pi(x) = \Theta(\frac{x}{\ln x})$.

Anyway, let $q = \max\{r \mid r \text{ prime }, n \geq 2(r^2 + r + 1)\}$. Then pick $r_0 : n = 2(r^2 + r + 1)$. (r_0 is a number such that this equality holds.)

Then for p prime, $\frac{r_0}{2} \leq p \leq r_0$. (This p is q.) Then $n' \geq 2(p^2 + p + 1) \geq 2(\frac{r_0^2}{4} + \frac{r_0}{2} + 1) \geq \frac{n}{4}$. Then (unsure what happened here, reference was made back to the bipartite diagram) we get that some quantity ($n = p^2 + p + 1$?) $\geq (\frac{n}{2})^{3/2}$ edges $\geq (\frac{n}{8})^{3/2}$.

In fact, we can get $m \geq_\sim (\frac{n}{2})^{3/2}$ because of PNC.

Matching: set of independent (disjoint) edges in a graph. Let $\mu(G)$ be the matching number, the maximum number of independent edges. Let $\tau(G)$ be the covering number, in CS also known as the 'hitting number', the minimum number of vertices that hit every edge.

As a matter of fact, these are concepts for hypergraphs.

DO: $\tau \geq \mu$. It should be obvious. The question is: are there interesting cases when these two are equal?

(Denes) Konig's Theorem: if G is a bipartite graph, then $\tau(G) = \mu(G)$. **DO+.** Algorithmic proof (should produce simultaneously a matching of a certain size, and a hitting set of the same size).

A particular consequence of this is the Konig-Hall Marriage Theorem:
If we take a bipartite graph (L,R), is there a bijection from the left side into the right side that is a matching?

Take $A \subseteq L$. Let $N_G(A)$ be the neighborhood of A, i.e. the set of all vertices not in A that are adjacent to some vertex in A. Then iff $\nexists A \subseteq L$ s.t. $|N_G(A)| < |A|$, i.e. iff

$\forall A \subseteq L, |A| \leq |N_G(A)|$, there exists a perfect L-R matching (a matching involving all vertices in G).

We define a K-H obstacle: a subset of L larger than the entire set of its neighbors. So either a $K - H$ obstacle exists, or there is a matching. In either case, there's a short proof (we show a K-H obstacle, or we show a matching).

HW: use marriage theorem to prove that if G is a regular nonempty bipartite graph then G has a perfect matching. (Think about this intuitively.)

19 Week 7: Monday, May 12

Friendship Graph, Erdős-Rényi-Sós Theorem, Spectral Theorem, Polarities, Projective Planes, Latin Squares & Rectangles, Baer's Theorem.

Friendship Graph: $(\forall x \neq y)(\exists z!\ x \sim z \sim y)$. Examples are graphs of triangles connected at one central vertex.

Theorem (Erdős-Rényi-Sós): There are no other friendship graphs.

Latin Rectangles: $k \times n$, $k \leq n$.

HW: prove: every Latin Rectangle can be completed (i.e. row(s) can be added) to form a Latin Square.

Hint: use previous Ex: non-empty regular bipartite graph has a perfect matching.

Steiner Triple System: for every $n \equiv 1$ or 3 modulo 6, there exists a STS. The proof of existence for all these n is inductive. We construct smaller STSes (Fano Plane, the one on 13 vertices,etc.) and then connect them to form larger ones — by this approach, we can exhaust all cases.

So imagine we have three STSes on n vertices, enumerate $1, 2, \ldots, n$. Then connect vertex i from the first STS with j from the second STS, and connect that with a_{ij} in the third STS. This implies an $n \times n$ matrix with entries $1, \ldots, n$ — a Latin Square!

So to triple the size of a STS, we construct a Latin Square. Now, the three STSes we use don't have to be the same, and we can connect them in many ways, and we can have an enormous number of STSes. (**DO**: Latin Square exists for every n)

We glue three STSes together by taking three copies such that they share a point/subsystem, edge, or by connecting three disjoint copies.

The starter cases for this construction is $n = 13, 9, 7, 3, 1$. **DO:** this set of starter cases is sufficient.

Spectral Theorem:
over $\mathbb{R}$: A is an $n \times n$ symmetric matrix: $A = A^{tr}$, then there exists an orthonormal eigenbasis. Definition of terms: basis: $b_1, \ldots, b_n$: basis of $\mathbb{R}^n$. Orthonormal:

$$b_i \cdot b_j = d_{ij} = \begin{cases} 1 \text{ if i=j: normal} \\ 0 \text{ if} i \neq j \text{ : orthogonal} \end{cases}$$

Eigenbasis: each b_i in the basis is an eigenvector. A consequence of the spectral theorem is that all the eigenvalues are real-valued: this is remarkable. Characteristic polynomial of a

matrix.

Take $A \in \mathbb{C}^{n \times n}$. Let $\lambda_1, \ldots, \lambda_k$: eigenvalues of C. **DO** $\sum \lambda_i = tr(A) = \sum a_{ii}$. Review characteristic polynomials.

Now look at a matrix associated with a hypergraph: the incidence matrix. It's a $n \times m$ matrix, representing vertices and edges, respectively.

M: incidence matrix of a finite projective plane of order n: $(n^2 + n + 1) \times (n^2 + n + 1)$. We have $(n + 1)$ ones per row. **Claim:** $(n + 1)$ is an eigenvalue of M.

For any matrix, multiplying it by the all-ones vector gives us the row summations.

We extend the spectral theorem a bit: it's not just if we have an orthonormal eigenbasis — as long as we have a set of orthonormal eigenvectors, we can extend that set to make an orthonormal eigenbasis.

Now, can we express the conditions of a Latin Square in form of a matrix equation? Note that if we have two sets and we give both of them their incidence vectors, we can find the size of the intersection by taking the dot product of their incidence vectors. We have a similar operation: $M^{tr}M = (|\ell_i \cap \ell_j|)$ gives us a matrix with $n+1$ on every cell of the diagonal, and 1 everywhere else. This is equal to MM^{tr}.

DO: MM^{tr} follows from $M^{tr}M = \ldots$.

Now the question is: suppose we have the matrix given by MM^{tr}. Suppose we have the identity matrix (I) and the J-matrix, the all-ones matrix. Then $M^{tr}M = J + nI$.

The sum of every row is $(n + 1) + 1 \cdot (n^2 + n + 1 - 1) = n^2 + 2n + 1 = (n + 1)^2$. (Could we have found that previously? Yes. $M^{tr}M1 = (n + 1)M^{tr}1 = (n + 1)^2 1$.)

So $Jb_i = 0$, for $i \geq 2$. Then $(J + nI)b_i = nb_i$. We found the eigenvectors.

Polarities: a polarity is a one-to-one correspondence between points and lines of a projective plane that preserves incidence. $p \leftrightarrow \ell = f(p)$. (So $p \in \ell \Leftrightarrow f(\ell) \in f(p)$).

DO All Galois planes have polarities.

We say that p is a fixed point of f if $p \in f(p)$. Theorem (Baer): every polarity has a fixed point. **DO.** Hint: use eigenvalues of $M^{tr}M$.

Possibly degenerate projective planes:

1. Line with two points
2. Point on two lines

3. triangle on three vertices (made from three lines)

What are the degenerate projective planes? We want infinitely many examples. Every degenerate projective plane has all points but one on one line, and one point elsewhere — all other points are connected to it by unique lines. **DO**: this is all.

Back to the **friendship theorem**. The Friendship Graph: $N(x) = \{y \mid y \sim x\}$ set of neighbors of x. **Claim:** this is a possibly degenerate p.p. There are two cases. Either it is a degenerate p.p., or it is not. If it is degenerate, then it is a starburst (flower) — the graph where all triangles meet on one vertex. Now what if it is not degenerate? Then $x \leftrightarrow N(x)$ is a fixed-point free polarity. But by Baer's theorem, there's no such thing, so that rules out the non-degenerate projective planes. So all that remains are the degenerate cases, which give us the flower-graphs. So there are no friendship graphs other than those flower-graphs. And we are done with the proof of the Erdős-Rényi-Sós Friendship Theorem.

20 Week 7: Wednesday, May 14

Hermitian Dot Product, Orthogonal & Normal Matrices, Rayleigh's Theorem.

In $\mathbb{R}^n$, we have $||x|| = \sqrt{x \cdot x}$ so $||x|| = 0$ iff $x = 0$. For the complex space, however, that's not sufficient. So for $\mathbb{C}^n$, we define the **Hermitian dot product**: $\langle x, y\rangle = \sum_{i=1}^{n} \overline{x_i} y_i$. In particular, $\langle x, x\rangle = \sum \overline{x_i} x_i = \sum |x_i|^2 \geq 0 \in \mathbb{R}$.

Operator norm of $A \in \mathbb{C}^{k\times\ell}$. $||A|| = \max \frac{||A||}{||x||}$. We have to justify the use of max rather than sup. **DO** prove the max exists.

A* = conjugate transpose. **DO** $(AB)^* = B^*A^*$.

Def. S is a unitary matrix $S \in C^{n\times n}$, if $S^*S = Id$.

DO If I have an n-by-n complex matrix S, it is unitary iff $\forall x, y \in \mathbb{C}^n$, the hermitian product $\langle S_x, S_y\rangle = \langle x, y\rangle$.

In real space, $S \in \mathbb{R}^{n\times n}$ is an **orthogonal matrix** if the same holds.

Review of Spectral Theorem.

Normal Matrix: a square matrix s.t. $AA^* = A^*A$.

For $A \in \mathbb{C}^{n\times n}$, the following are equivalent:

1. There exists an orthonormal eigenbasis: $b_i^* b_j = d_{ij}$.
2. A is normal
3. A is unitarily diagonalizable.

For the Real spectral theorem, i.e. $A \in \mathbb{R}^{n\times n}$, the following are equivalent:

1. there exists an orthonormal eigenbasis
2. $A = A^{tr}$

Examples of normal matrices: A if $A = A^*$. These are called Hermitian Matrices. Direct generalization of the real symmetric matrices. The unitary matrices are also normal, $A^{-1} = A^*$. So in particular, the real orthogonal matrices are also normal (therefore they have an orthonormal eigenbasis over the complex numbers, but typically not over the reals).

DO if A is normal, then A is Hermitian if and only if all eigenvalues are real. It is unitary if and only if all eigenvalues have absolute value equal to 1.

WTS that if we have a complex hermitian matrix, then the eigenvalues are real. Use the fact

that it is symmetric. $x^*Ax = x * (\lambda x) = \lambda x^* x = \lambda ||x||^2$, where $||x||^2 > 0 \in \mathbb{R}$. That's just a one-by-one matrix 9 a number). So $(\lambda ||x||^2)^* 0 = \overline{\lambda} ||x||^2 = (x^*Ax)^* = x^*A^*x^{**} = x^*Ax = \lambda ||x||^2$. Implies $\overline{\lambda} = \lambda$, so $\lambda \in \mathbb{R}$.

DO ♡ Compute the eigenvalues of the rotation matrix.
DO Verify geometric action. (For a standard basis.)

Rayleigh Quotient of a symmetric $\mathbb{R}$ (or a Hermitian $\mathbb{C}$) matrix A:

$$R_A(x) = \frac{x^*Ax}{x^*x}$$

So $R_A : \mathbb{C}^n \setminus \{0\} \to \mathbb{R}$.

Eigenvalues $\lambda_1 \geq \ldots \lambda_n \in \mathbb{R}$.
DO $\max_{A \in \mathbb{C}^n \setminus \{0\}} R_A(x) = \lambda_1$ (Rayleigh's Theorem)
$\min R_A(x) = \lambda_n$ (Apply max to $-A$)

DO $\lambda_i = \max_{U \leqslant \mathbb{C}^n, \dim U = i} \min_{x \in U, x \neq 0} R_A(x)$. **DO**: Courant-Fisher inequalities/theorem. Interlacing Theorem. Follows from Courant-Fisher. (Statement of theorems omitted — see course websites, likely under the exercises.)

21 Week 7: Friday, May 16

Projective Planes, Fixed Points, Polarities, Linear Algebra, Latin Squares.

Reviewing the theorem about polarity: Baer: finite projective plane has no fixed-point-free polarity. Recall: a polarity is a bijection from points to lines, $f : P \to L$, such that $p \in \ell \Rightarrow f(\ell) \in f(p)$. Fixed point: $p \in f(p)$.

If M is the incidence matrix, where the columns are the lines and the rows are the points, then

$$m_{ij} = \begin{cases} 1 \text{ if } p_i \in \ell_j \\ 0 \text{ otherwise} \end{cases}$$

Then we have $p_1, \ldots, p_N$ and $\ell_1, \ldots, \ell_N$, where $N = n^2 + n + 1$. Then $MM^{tr} = M^{tr}M = J + nI$, where J is the all-ones matrix, and we have $n+1$ in the diagonal, and 1 everywhere else. (**DO**)

Can we infer something about n itself? The incidence matrix is not uniquely assigned. We have $(N!)^2$ incidence matrices. Does a matrix tell us anything about polarities? Can we make inferences?

Suppose we have our incidence matrix M with rows $p_1, \ldots, p_N$ and columns $f(p_1), \ldots, f(p_N)$. Then f is a polarity **if and only if** M is a symmetric matrix, i.e. $M = M^{tr}$. Therefore it has **real eigenvalues**.

$(p_i \in \ell_j \Leftrightarrow p_j = f(\ell_j) \in f(p_i) = \ell_i)$.

$MM^{tr} = M^2$. Let M have eigenvalues $\mu_1, \ldots, \mu_N$. Then M^2 has eigenvalues $\mu_1^2, \ldots, \mu_N^2$. **DO** This holds for all matrices over any field.

This means that if we know the eigenvalues of the square, we almost know the eigenvalues of the original matrix. This means that the only ambiguity is the sign. So the eigenvalues of M are $(n+1)$ (given by the all-ones vector, $M \cdot 1 = (n+1)1$) and $\pm\sqrt{n}, \ldots, \pm\sqrt{n}$.

So now what can we say about the diagonals of M? $m_{ii} = 1 \Leftrightarrow p_i \in f(p_i) : p_i$ is a fixed point. So if f is fixed-point-free, then $(\forall i)(m_{ii} = 0)$. Then the trace of the matrix (sum of the diagonal elements) $= 0$. But the trace is also equal to another important quantity, the sum of the eigenvalues! So we have $Tr(M) = 0 = \sum \mu_i$. we note that we have $Tr = (n+1) + k\sqrt{n}$ for $k \in \mathbb{N}$. We note we have $n \geq 2$ because we're on a projective plane. Babai claims this sum cannot be 0.

We now have two cases: we have $n + 1 = -k\sqrt{n}$. If n is not a square: then the RHS is irrational or 0. Done. If $n = \ell^2$ is a square, Then we have $\ell^2 + 1 = -k\ell$. We have $\ell \geq 2$, and this gives rise to a contradiction.

We could also do it just by squaring both sides: $n+1 = -k\sqrt{n}$, so $(n+1)^2 = k^2 n \equiv 0 \mod n$, but $(n+1)^2 \equiv 1 \mod n$, which gives us a contradiction. (This is faster.)

We had a related, but not-quite-identical problem on the test. M incidence matrix of projective plane of order n. $M \cdot \vec{1} = (n+1)\vec{1}$. $n+1 = \lambda_i$. (Or was it λ_1?) $N = n^2 + n + 1$. We claim that for $\lambda_2, \ldots, \lambda_N \in \mathbb{C}$, we have $|\lambda_i| = \sqrt{n}$.

Normal Matrix: commutes with its conjugate transpose. $AA^* = A^*A$. M is a real matrix, so its transpose is the same as its conjugate transpose. So M is a normal matrix. It's over the complex numbers, so there exists an Orthonormal Eigenbasis in $\mathbb{C}^n$.

$$A[\underbrace{u_1, \ldots, u_N}_{\text{U}}] = [\underbrace{Au_1}_{\lambda_1 u_1}, \ldots, \underbrace{Au_N}_{\lambda_N u_N}] = UD$$

Where D is a diagonal matrix consisting only of the eigenvalues $\lambda_1, \ldots, \lambda_N$.

Then what do we know about U? $U^*U = I$. $u_i^* \cdot u_j^* = d_{ij}$. $AU = UD$. $U^{-1}AU = D$. $U^*AU = D$. Then D^*D is the matrix with $\overline{\lambda_1}\lambda_1, \ldots, \overline{\lambda_N}\lambda_N$ in the diagonal and 0 everywhere else. This is equal to the matrix with $|\lambda_1|^2, \ldots, |\lambda_N|^2$ in the diagonals and 0s everywhere else.

We have $U^*A^*UU^*AU = D^*D$, and $(U^*AU)^* = U^*A^*U^{**}$. Then $U^*A^*AU = U^*(J + nI)U$. Now, this lets us keep our eigenvalues — it just shifts the basis. So $|\lambda_1|^2 = (n+1)^2$, so $|\lambda_1|^2 = n$. ✓

DO if $AB = BA$, A, B are diagonalizable (have an eigenbasis), then A, B have a common eigenbasis.

Now back to Latin Squares: if $k < n$ and we have a $k \times n$ Latin Rectangle, then we can extend it to a $(k+1) \times n$ Latin Rectangle. This becomes a problem of finding a perfect matching in a bipartite graph.

Sketch: we will have a bipartite graph with $1, \ldots, n$ in each part. We want each vertex to have degree $n - k$. Then, for every column missing element j, we may place j in that column in row $k+1$. (Permitted to extend.) We note that for every row we add, we have to put j somewhere — so that excludes some cell in row $k+1$ from being able to store j.

Now, in how many ways can we extend a Latin Rectangle? That's the same as the number of perfect matchings, a more difficult quantity to compute.

Let $A = (a_{ij})_{n \times n}$. Then $\det(A) = \sum_{\sigma \in S_n} sgn(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)}$. We're in S_n, so there are $n!$ terms. Also note the definition of sgn: $+1$ if σ is an even permutation, -1 if σ is an odd permutation.

Now we're interested in the **Permanent** of a matrix. (This quantity is basically infeasi-

ble to compute except for special cases.)

$$\text{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

$$\text{per}(I) = 1$$

$$\text{per}(J) = n! \quad \text{(All-Ones Matrix)}$$

We define the **Stochastic Matrix:** $a_{ij} \geq 0, \sum_{j=1}^{n} a_{ij} = 1$. The **Doubly Stochastic Matrix**: $\sum_{i=1}^{n} a_{ij} = 1$.

$$\text{per}(\frac{1}{n}J) = \frac{n!}{n^n} \approx e^{-n}$$

Permanent Inequality of a doubly stochastic matrix. Then $\text{per}(A) \geq \frac{n!}{n^n}$.

DO Use this to show: if $r \geq 3$ then a regular bipartite graph of degree r has exponentially many perfect matchings (on n; r is fixed).

22 Week 8: Monday, May 19

Permanents, Latin Squares, Linear Algebra, Perfect Matchings.

CHALLENGE. If $\sigma \in S_n$, $\sigma \neq 1$, $\text{ord}(\sigma) = n^\alpha, \Rightarrow (\exists m)(\sigma^m \neq 1, \sigma^m$ fixes at least $n(1 - \frac{1}{\alpha})$ points).

DO If G is an r-regular graph of girth ≥ 5, then $n \geq r^2 + 1$. Show that $n = r^2 + 1$ is possible for $r = 1, 2, 3$.

DO Suppose $a_1, \ldots, a_n, b \in \mathbb{R}, a_i \neq 0$. Pick a subset $I \subseteq [n]$ at random. We want to find $P(\sum_{i \in I} a_i = b) \leq \frac{c}{\sqrt{n}}$. For some constant c. Estimate c. Hint: this follows from an earlier theorem in this course.

DO Show $n! \geq (\frac{n}{e})^n$. Give a 1-line proof. Stirling's formula is neither allowed nor helpful.

Count perfect matchings in an r-regular bipartite graph. We use the Permanent Inequality by Falikman-Egorychev around 1980. Before that, it was called "van der Waerden's conjecture". (See the van Lint-Wilson text.)

We say that an $n \times n$ matrix is stochastic if every entry is greater than or equal to 0, and every row sums to 1. It is doubly stochastic if the same is true for the columns. (i.e. A and A^{tr} are both stochastic.)

The permanent inequality says that if A is doubly stochastic, then $Per(A) \geq \frac{n!}{n^n} \geq \frac{1}{e^n}$. Equality holds if and only if $A = \frac{1}{n}J$.

Bipartite graph $G = (K + L, E)$ has an incidence matrix $M = (m_{ij})$.

$$m_{ij} = \begin{cases} 1 \text{ if left}_i \sim \text{right}_i \\ 0 \text{ otherwise} \end{cases}$$

(Take $i \in K, j \in L$).
deg(left i) = $\sum i^{th}$ row
deg(right j) = $\sum j^{th}$ column
If $K = L = n$, then the number of perfect matchings is equal to the permanent of M. $\frac{1}{r}M$ is doubly stochastic. (Graph is r-regular.)

$\text{per}(\frac{1}{r}M) \geq \frac{n!}{n^n} \geq \frac{1}{e^n}$. The number of perfect matchings, $\text{per}(M) = r^n \cdot \text{per}(\frac{1}{r}M) \geq \frac{r^n}{e^n} = (\frac{r}{e})^n$, $r \geq 3$.

HW Let $L(n)$ denote the number of $n \times n$ Latin Squares. Prove: $\ln L(n) \sim n^2 \ln n$.

CH Prove almost all Latin Squares have no non-identity automorphism. (You have to

define the notion of an automorphism on a Latin Square.)

We're still interested in finite projective planes of order that is not prime-power. Specifically, we're curious about the case when $n \equiv 2 \mod 4$: two orthogonal Latin Squares exist for all such n, except for one case: For the case of 6, Terry proved in 1906 that there are no two orthogonal Latin Squares of order 6.

There is a construction that relates Latin Squares, Matrices, and Affine Lines/Affine Planes/Projective Geometry. A reference will be inserted here...

(Remark: the problem with regard to 6×6 Latin Squares was actually first raised by Euler, who named it the 36 Officers Problem.)

Then, to do with incidence vectors: We have a set of points P in a space with dimension n^2+n+1. We then add another coordinate to every vector that may be 0 or 1. We call it the parity check: n^2+n is even, so n^2+n+1 is odd, so n^2+n+2 is even again. Let $v_\ell =$ incidence vector of line ℓ, we then add the parity check to construct the vector $\overline{v_\ell} \in \mathbb{F}_2^{n^2+n+2}$. Note that this vector is of course necessarily even.

Then let $U = span(\overrightarrow{v_\ell} \mid \ell \in L) \leq \mathbb{F}_2^{n^2+n+2}$.

Then **DO** if $n \equiv 2 \mod 4$, then U is a totally isotropic subspace of maximum dimension $= \frac{n^2+n+2}{2}$.

In this vein, check out McWilliams' weight enumerator identity, which connects w_u with $w_{u^\perp}$: $U \leq \mathbb{F}_q^n$, $w_u(t) = \sum_{u \in U} t^{|u|}$. $|u| = \#$ nonzero in u.

If we have a graph, then we can associate with it a symmetric real matrix called the adjacency matrix of a graph: $A = (a_{ij})$. This is an $n \times n$ matrix.

$$a_{ij} = \begin{cases} 1 \text{ if } i \sim j \\ 0 \text{ otherwise} \end{cases}$$

Easy consequence: trace of the matrix is 0. Then it follows that the sum of the eigenvalues is 0.

$A = A^{tr}$: eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$.

Then it follows that $A^2 = (b_{ij})$, and $b_{ij} = \#$ walks of length 2 from i to j.

As a special case of this statement, it is clear that $b_{ii} = \deg(i)$.

So what is $A^t = (a_{ij}^{(}t))$? Extending the above, we have $a_{ij}^{(}t) = \#$ of walks of length t from i to j.

Then what is the trace of A^2? It is the sum of the degrees; by the handshake lemma, that is $2m$, where $m = \#$ edges. This is also equal to $\sum \lambda_i^2$.

Then the trace of A^3 is 6 times the number of triangles in the graph.

Suppose I have a number of edges m. What is the maximum number of triangles? Try to create the complete subgraph, where $t = \binom{n}{3}$.

DO: Prove: $t \leq \frac{\sqrt{2}}{3} m^{3/2}$.

DO (This lemma may come in useful): if $x_1, \ldots, x_n \in \mathbb{R}$, then $(\sum x_i^2)^3 \geq (\sum x_i^3)^2$.

Note: the bound in the exercise is asymptotically tight: if $m = \binom{n}{2}$ and $t = \binom{n}{3}$ then $t \sim \frac{\sqrt{2}}{3} m^{3/2}$.

23 Week 8: May 21

Random Graphs, Chernoff Bound, Hyperbolic Functions.

Random graph G with n vertices. The expected degree of a given vertex is $\frac{n-1}{2}$. We expect the actual outcome to be quite close to the expected value:

$$P\left(\left|\deg - \frac{n-1}{2}\right| > \epsilon n\right) \to 0$$

At what rate does this go to zero? This is given by Chebyshev's inequality, which gives a rate of decay on $O_\epsilon(\frac{1}{n})$. (Law of Large Numbers.)

The weakness of Chebyshev's inequality is that it only uses pairwise independence. Using Chebyshev with the Union Bound does not give us the desired result, so we use a much stronger concentration inequality:

Chernoff Bound. $X = \sum_{i=1}^{n} Y_i$ where Y_i all independent, $|Y_i| \leq 1$, $E(Y_i) = 0$. Then $P(|X| \geq a) \leq 2e^{\frac{-a^2}{2n}}$.

DO prove: with exponential probability, all vertices have degree close to $\frac{n-1}{2}$. (Quantify these statements: what is exponential? What is close?)

Proof. Special case: $Y_i = \pm 1 \therefore P(Y_i = 1) = \frac{1}{2}$.
We know $P(X \geq a) = P(e^{tx} \geq e^{ta})$, which is true $\forall t > 0$. By Markov's inequality, $P(X \geq a) \leq \frac{E(e^{tx})}{e^{ta}}$.

So $E(e^{tx}) = E(e^{\sum tY_i}) = E(\prod e^{tY_i}) = \prod E(e^{tY_i}) \leq (\cosh t)^n \leq e^{\frac{nt^2}{2}}$. The third equality is where we use full independence.

$$E(e^{tY_i} = \frac{e^t + e^{-t}}{2} = \cosh(t) \leq e^{t^2/2}$$

DO Show that $\cosh(t) \leq e^{t^2/2}$.

$$(\forall t)(P(X \geq a) \leq \frac{e^{\frac{nt^2}{2}}}{e^{ta}}$$

Find the t to minimize the above expression. Easy, because we have $t(\frac{nt}{2} - a)$, so the zeroes are at $t = 0$ and $t = \frac{2a}{n}$.

Proof. General case: we still claim $E(e^{tY} \leq \cosh t$. We take $Y = Y_i$. Assumptions: $|Y| \leq 1, E(Y) = 0$. If under these assumptions we prove our claim, then we are done.

Let $h_t(x) = \cosh(t) + x \sinh(t)$. Then $(\forall x)(-1 \leq x \leq 1 \Rightarrow h_t(x) \geq e^{tx})$.

$e^{ty} \leq h_t(Y)$. $E(e^{ty}) \leq E(h_t(Y)) = E(\cosh t + Y \sinh t) = \cosh t + \sinh t \cdot E(Y) = \cosh t$.

The last 15 minutes were spent on the sixth quiz.

24 Week 8: Friday, May 23

Graphs, Linear Algebra.

Review of Wednesday's Test Problems.

First question: if A is doubly stochastic, then $\text{per}(A) \leq 1$. A stochastic matrix: every entry ≥ 0, and every row sum $= 1$. Doubly stochastic if $A = A^{tr}$ as well. Then derive the fact that $\prod(\sum_{j=1}^{n} a_{ij}) \geq \text{per}(A)$ whenever $a_{ij} \geq 0$. And if A is stochastic, then the left side equals 1.

Second question: Littlewood-Offord problem. Input: $a_1, \ldots, a_n, b \in \mathbb{R}$, and $\forall a_i \neq 0$. We choose a random subset $I \subseteq [n]$, i.e. a random element from the power set. WTS $P(\sum_{i \in I} a_i = b) \leq \frac{c}{\sqrt{n}}$. Suppose all $a_i > 0$ and $I \subset J$. Then $\sum_{i \in I} < \sum_{j \in J}$. Let $A = \{I \mid \sum a_i = b\}$, then A is a Sperner Family so $|A| = \binom{n}{\lfloor \frac{n}{2} \rfloor}$. So $P(A) = \frac{|A|}{2^n} \leq \frac{\binom{n}{\lfloor \frac{n}{2} \rfloor}}{2^n} \sim \sqrt{\frac{2}{A}} \cdot \frac{1}{\sqrt{n}} < \frac{c}{\sqrt{n}}$.

Now suppose $a_1, \ldots, a_{\frac{n}{2}} > 0$, and we don't know/care about the rest. Then $I = I_1 \cup I_2$. Then $I_1 \subseteq [\frac{\lceil n \rceil}{2}]$ and $I_2 \subseteq \{\frac{\lceil n \rceil}{2} + 1, \ldots, n\}$. So we fix I_2. Then we want $P_I(A \mid I \cap \{\frac{\lceil n \rceil}{2} + 1, \ldots, n\} = I_2)$. (It is now not necessary that A is a Sperner Family.) Then we want to show that $(\forall I_2)(P_I \leq \frac{c'}{\sqrt{n}})$. (Intuition: we are taking the entire set of $a_i, \ldots, a_n$. We split it down the middle, and then we take a random subset of the entire set. We then see where this random subset is split. Then we 'toss our coins' for I_2 while I_1 is still open.) Then for fixed I_2, the I_1s are a Sperner Family. So it's the exact same approach as before, but with a different set size — it follows that the new inequality bit is $\frac{c}{\sqrt{\frac{n}{2}}} = \frac{\sqrt{2} \cdot c}{\sqrt{n}}$, so $c' = c \cdot \sqrt{n}$.

The third problem was to prove that $t \leq cm^{3/2}$, where $c = \frac{\sqrt{2}}{3}$. We use A, the adjacency matrix: $\sum \lambda_i^2 = \text{tr}(A^2) = 2m$ and $\sum \lambda_i^3 = \text{tr}(A^3) = 6t$. ($m$ is the number of edges, t the number of triangles.) Note the λ_i, eigenvalues of A, are real because A is symmetric.

Nobody got the bonus problem: G graph, A adjacency matrix. We claim $\lambda_1 \geq$ average degree $= \frac{2m}{n}$.

For λ_1, we have Rayleigh's Quotient. (Computational details omitted— see earlier section on the Rayleigh Quotient.) The numerator of the Rayleigh Quotient is the quadratic form associated with A. Then if we take $1^{tr} A 1 = \sum_i \sum_j a_{ij} = 2m$. The norm of the all-ones vector squared is $||1||^2 = \sum_{i=1}^{n} 1^2 = n$.

Results that are too good to be true: some solutions to the first problem stated that $per(A) \leq \frac{n!}{n^n} \leq 1$. This is not sensible for various reasons.

With regard to the first bonus problem: when is $\lambda_1 = d$? What is the condition for equality? Take a digraph with adjacency matrix A. Because it is a digraph, the eigenvalues are not necessarily real; $\lambda_i \in \mathbb{C}$. **DO** $\forall |\lambda_i| \leq$ max outdegree.

DO Undirected graph: $\lambda_i = \deg \max$ iff there exists a connected component which is regular of max. degree. (Example: two disconnected components, both regular — see their adjacency matrix.)

DO $\lambda_1 =$average degree iff G is regular.

Undirected graphs. Recall $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$. Assume $\lambda_1 > 0$. Let's look at λ_n. We know that $\sum \lambda_i = \mathrm{tr} A = 0$.
DO $(\forall i)(|\lambda_i| \leq \lambda_1)$.

Is it possible for $\lambda_n = -\lambda_1$?

If G is connected, then the average degree $\geq 2 - \frac{2}{n}$. (**DO**.)

The smallest possible degree of a graph (given by a tree) is just $n - 1$. As a lower bound, that yields the above.

HW If G is bipartite, then $\lambda_n = -\lambda_1$, and in fact $\lambda_{n-l} = -\lambda_{1+l}$. So the entire spectrum is symmetric about 0.

DO If G is connected, and $\lambda_n = -\lambda_1$, then G is bipartite. (Probably on the next test.)

Interlacing. If G is an undirected graph with eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$, and $G_1 : G$ minus some vertex has eigenvalues $\mu_1 geq \ldots \geq \mu_{n-1}$ then $\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \ldots \geq \mu_{n-1} \geq \lambda_n$.

DO (a) Look up Chebyshev Polynomials. What are their roots? (b) Relate characteristic polynomial of a path to Chebyshev polynomial.

25 Week 9: Wednesday, May 28

Alphabets, Shannon Capacity of a Graph, Orthonormal Representation of a Graph.

I arrived 10 minutes late.

Important information about choosing a grade for the class.

Five-spoked Umbrella. $v_1, \ldots, v_5$, and $v_i \perp v_{i+2} \mod 5$. **DO** $\cos\theta = \frac{1}{5^{1/4}}$. Hint: spherical cosines theorem.

Now graphs and alphabets. Let Σ = set of vertices = alphabet. $V(G^k) = \sigma^k$, where $V(G \cdot H) = V(G) \times V(H)$. We write $a \simeq b$ to indicate that two letters are "adjacent or equal". So letters can be confused. Words $a_1 \ldots a_k \simeq b_1 \ldots b_k$ if $(\forall i)(a_i \simeq b_i)$. Question: number of pairwise not confoundable messages?

DO $\overline{K_s} \cdot \overline{K_t} = \overline{K_{st}}$.
DO $\alpha(G \cdot H) \geq \alpha(G) \cdot \alpha(H)$. In particular, $\alpha(G^{k+l}) \geq \alpha(G^k) \cdot \alpha(G^l)$.

Recall Fekete's Lemma. So the limit $\lim_{k\to\inf}(\alpha(G^k))^{1/k}$ exists. We call this $\Theta(G)$, the (zero-error) **Shannon Capacity** of G.

Obvious bounds: $\alpha(G) \leq \Theta(G) \leq n = |V(G)|$. Lower because lim = sup, and for $k = 1$ we get $\alpha(G)$. Upper: because $|V(G^k)| = n^k$.

Graph function: f: Graphs $\to$ Numbers. Domain is graphs, but isomorphic graphs give the same numerical result, i.e. $G_1 \simeq G_2 \Rightarrow f(G_1) = f(G_2)$.

Lemma. If f is graph function such that $(\forall g)(f(G) \geq \alpha(G))$ and $(\forall G, H)(f(G \cdot H) \leq f(G) \cdot f(H)))$ then $(\forall G)(\Theta(G) \leq f(G))$.

Proof. $\alpha(G^k) \leq f(G^k) \leq f(G)^k$.
$\therefore \alpha(G^k)^{1/k} \leq f(G)$.
$\therefore \lim(G^k)^{1/k} \leq f(G)$.

HW Prove that $\Theta(G) \leq \chi(\overline{G})$. The above lemma will be helpful.

Corollary: if $\chi(\overline{G}) = 2$, implying a bipartite nonempty graph, then $\Theta(G) = 2$. **DO**.

Corollary: if $\chi(\overline{G}) = \alpha(G)$ then both are equal to $\Theta(G)$. This includes all perfect graphs.

What is smallest graph that is not covered by this? Give some thought to it: it is the pentagon (C_5). The Shannon capacity of the pentagon was an open question for 30 years, but proved by Lovász.

$\alpha(C_5) = 2$.
$\alpha(C_5^2) = 5$ **DO**

Imagine each C_5 as a line with five points on it, and their product as a five-by-five board on a torus (the endpoints are connected). We draw an analogy from chess to find the largest independent set: the king, on a point, can move to any adjacent vertex. So this is the King's graph on a toroidal five-by-five chessboard. The piece that most easily evades the King is the knight — we don't repeat points or move to points adjacent to where we have already been. The king's moves correspond to moving in F_5 with slope $1/2$. Drawing this out shows that the independence set is of size at least 5.

This is just the affine lines in $\mathbb{F}_5$. Consequently $\alpha(C_5^2) \geq 5$ — it is an exercise to show that it is in fact equal. It follows that $\Theta(C_5) \geq \sqrt{5}$.

Also, $\chi(\overline{C_5}) = 3 \geq \Theta(C_5)$. The **fractional chromatic number** of C_5 is $\frac{5}{2}$. So $\sqrt{5} \leq \Theta(C_5) \leq \frac{5}{2}$. Lovász Theorem: $\Theta(C_5) = \sqrt{5}$.

An Orthonormal Representation ONR of a graph: $i \in V \to v_i \in \mathbb{R}^d, ||v_i|| = 1$ s.t. if $i \not\sim j$ then $v_i \perp v_j$.
DO if ONR exists in $\mathbb{R}^d$: $d(G) = \min$ such d.
Prove: $\Theta(G) \leq d(G)$.

Back to the umbrella. $v_1, \ldots, v_n$: ONR of G. c: any $||c|| = 1$. Imagine the c as the stem and the v_i as the spokes.

$$\vartheta(G) = \min_{v_1,\ldots,v_n} \max_i \frac{1}{(c^T v_i)^2}$$

The umbrella serves as the instance of this we need. C_7 is still open.

26 Week 9: Friday, May 30

Fractional Chromatic Numbers, Lovàsz' Theta.

Shannon Capacity of a graph G. We defined a product $V(G \cdot H) = V(G) \times V(H)$ and $(g_1, h_1) \simeq (g_2, h_2)$ if $g_1 \simeq g_2$ and $h_1 \simeq h_2$. And the Shannon Capacity, $\Theta(G) = \lim_{k\to\infty} \alpha(G^k)^{1/k} = \sup \alpha(G^k)^{1/k}$.

Lemma: if f : Graphs $\to \mathbb{R}^+$, such that $\forall G, f(G) \geq \alpha(G)$ and $(\forall G, H) f(G \cdot H) \leq f(G) \cdot f(H)$, then $(\forall G)(\Theta(G) \leq f(G))$.

The exercise was that $\chi(\overline{G}) \geq \alpha(G)$. That $\chi(\overline{G}) \geq \alpha(G)$ is obvious: $\chi(H) \geq \alpha(\overline{H}) = \omega(H)$. Then we show submultiplicativity: if $g : V(\overline{G}) \to \{colors\}$ and $h : V(\bar{H}) \to \{colors\}$ then $(g, h) : (u, w) \to (g(v), h(w))$ where $v \in V(\bar{G})$ and $w \in V(\bar{H})$. So suppose $(v_1, w_1) \sim (v_2, w_2)$ in $G \cdot H$. Then if $(v_1, w_1) \not\sim (v_2, w_2)$ in $G \cdot H$ then either $v_1 \not\sim v_2$ in G or $w_1 \not\sim w_2$ in H. $v_1 \sim v_2$ in $\bar{G}$, so $g(v_1) \neq g(v_2)$.

Moshe Rosenfeld: linear programming upper bound: fractional chromatic number. Take $C_1, \ldots, C_m$: independent sets in G. If a graph is k-colorable, then every color class is an independent set, clearly. So: G is k-colorable iff $\exists \leq k$ independent sets $C_i, \ldots, C_{i_k}$ such that $\bigcup C_{i_j} = V$.

Assign $x_1, \ldots, x_m \in \{0, 1\}$ such that $\cup_{x_j=1} C_j = V$ such that $(\forall i), \sum_{j:i\in C_j} x_j \geq 1$ and $\sum x_j \leq k$.

So:

$$\chi(G) = \min\{\sum_{j=1}^{m} x_j \mid (\forall i)(\sum_{j:i\in C_j} x_j \geq 1\}$$

This is an integer programming (IP) problem (a type of linear programming (LP)), where the latter part of the minimization is the constraint, and the objective function is the former part. We need one more constraint: $0 \leq x_j$.

Integer Programming is a Linear Programming problem in which we are only looking for integer solutions. IP is NP-Hard, whereas LP can be solved in polynomial time.

Linear relaxation: $\chi^*(G) =$ optimum over the reals. Clearly $\chi^*(G) \leq \chi(G)$.

This is still not feasible, because we have to list all the independent sets, but it is a useful (theoretical) device for some graphs.

Example: $\chi^*(G) = \frac{5}{2}$. This is optimum: let $x_{12} = \ldots = x_{51} = \frac{1}{2}$.

"I am not talking about computation, I am talking about mathematics!" The joke about the mathematician on the ground and the economist in the balloon was told.

DO: prove that $\Theta(G) \leq \chi^*(\bar{G})$.

Now, back to Lovàsz' Theta Function: (this was mentioned last class, though I don't think I mentioned it by name; it would be wise to look it up).

$$\vartheta(G) = \min_{\text{ONR of G}(v_1,\ldots,v_n)\text{stem c}} \max_{1\leq i\leq n} \frac{1}{(c^T v_i)^2}$$

Where an ONR of G is $v_1, \ldots, v_n$ s.t. $||v_i|| = 1$ and if $i \not\sim j$ then $v_i \perp v_j$. Stem: $||c|| = 1$.

DO: in Lovàsz' Theta, inf = min.

Theorem: $\Theta(G) \leq \vartheta(G)$. This is the case for all G.

Proof:
(1) $\vartheta(G) \geq \alpha(G)$. Suppose $A \subseteq V$, A independent. Then $\{v_i \mid i \in A\}$ is orthonormal.

Fact: if $b_1, \ldots, v_n$ is an orthonormal basis of $\mathbb{R}^n$, then $(\forall c)(||c||^2 = \sum (c \cdot b_i)^2$. (This is from the Pythagorean theorem in n dimensions.)

If we just have an orthonormal set of vectors, then we can extend it to an orthonormal basis. So $||c||^2 \geq \sum_{i=1}^{\alpha} (cv_i)^2 \geq \alpha \cdot \min\{(cv_i)^2\}$. Then $\alpha \leq \frac{1}{\min(cv_i)^2} = \max \frac{1}{(cv_i)^2}$.

DO $\vartheta(G \cdot H) \leq \vartheta(G)\vartheta(H)$.
Challenge+: A more difficult theorem: $\vartheta(G \cdot H) = \vartheta(G) \cdot \vartheta(H)$.

It is a helpful fact that $\Theta(G) \leq d(G) =$ min dim of ONR.

27 Week 10: Monday, June 2

k-matchings, Orthogonal Polynomials, Chebyshev Polynomials.

k-matching: a set of k independent edges. Let $m_k(G)$ be the number of k-matchings in G. This quantity is unimodal for all curve, and under rather general conditions it gives a bell curve (satisfies the central limit theorem).

Generating Functions: For a sequence $a_0, a_1, a_2, \ldots$, its generating function is $\sum_{k=0}^{\infty} a_k x^k$. Example: $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ has the generating function $(1+x)^n$.

The matching polynomial of G is $\mu_G(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \cdot m_k \cdot x^{n-2k}$.

Suppose we have two polynomials. How are their roots related? Let

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

then if we reverse the coefficients:

$$h(x) = a_n + a_{n-1} x + \ldots + a_0 x^n = x^n f\left(\frac{1}{x}\right)$$

and if we alternate signs:

$$\ell(x) = a_0 - a_1 x + a_2 x^2 - \ldots = f(-x)$$

This theory came from a 1970s paper by Heilmann & Lieb, who were Statistical Physicists.

If G s cycle-free (forest), then $\mu_G(x) = f_G(x) =$ characteristic polynomial of $G = \det(xI - A_G)$ where A_G is the adjacency matrix of G. (**DO** — not difficult if you understand the determinant).

Theory of Orthogonal Polynomials. Suppose we have a density function $\rho \geq 0$ on $\mathbb{R}$ that satisfies $(\forall k) \int_{-\infty}^{\infty} x^{2k} p(x) dx < \infty$. This defines for us an inner product on polynomials: if we have $f, g \in \mathbb{R}[x]$, then $\langle f, g \rangle = \int_{-\infty}^{\infty} f(x) g(x) \rho(x) dx$. Then we have a notion of orthogonality: two polynomials are orthogonal if their inner product is 0.

Then we take a basis of the space of polynomials: $1, x, x^2, x^3, \ldots$ and we apply Gram-Schmidt Orthogonalization to give $f_0, f_1, f_2, \ldots$ with $\deg(f_j) = j$.

Some of the more remarkable polynomials in this family:

- Chebyshev Polynomial: there are two kinds, $T_n(x)$ and $U_n(x)$. They are orthogonal polynomials with respect to one of these two weight functions: $\sqrt{1-x^2}$ and $\frac{1}{\sqrt{1-x^2}}$, both

of which are equivalent. They are everywhere in mathematics, even in combinatorics. $\cos(n\theta) = T_n(\cos\theta)$, where we remark that $\cos(n\theta)$ is always a polynomial of cosine: $\cos(2\theta) = 2(\cos\theta)^2 - 1$. We note that n turns out to be the degree. Relevant to approximation theory.

Another interesting weight function is $e^{-x^2/2}$. This yields the Gaussian ("Bell") curve. Then, if we let $p(x) = e^{-x^2/2}$, then we can define $H_n(x)$, the Hermite polynomials, which are also very interesting.

So to characterize orthogonal polynomials, we only need to define the density function.

Theorem. If $f_0, f_1, \ldots$ is a sequence of orthogonal polynomials, then (1) all roots of each f_j are real. (2) The roots interlace, i.e. between every two roots of f_n, there is a root of f_{n-1}.

Interlacing is already familiar: if f_G is the characteristic polynomial of a graph, then the roots of f_G and $f_{G/V}$ interlace. (Where G/V denotes G minus any vertex.) It was a previous exercise to derive this from Courant-Fischer via the Interlacing theorem for symmetric matrices. (Reference is made to the Rayleigh quotient — see previous section.)

Reminder: P_n is the path on $n-1$ vertices.

$\mu_{P_n}(x) = 2T_n(x)$ (Here, the Characteristic and Chebyshev polynomials are the same, because a path is a tree.)
$\mu_{C_n}(x) = U_n(x)$
$\mu_{K_n}(x) = H_n(x)$

There are even more examples of classical orthogonal polynomials that show up as the matching polynomials of specific families of graphs (e.g. the Laguerre polynomial for complete bipartite graphs).

Theorem. (H-L) The roots of $\mu_G(x)$ are real for every graph G, and they interlace with $\mu_{G/V}(x)$.

$\therefore$ all roots of $\mu'_G = \sum m_k \cdot x^k$ are negative reals. It follows that the sequence of coefficients is log-concave and unimodal. This is an extremely strong and amazingly general conclusion.

If we let X be a random variable and all of its values are ≥ 0, independently, then $f_X(t) = \sum_{k=0}^{\infty} P(X = k) \cdot t^k$. **DO:** If X, Y independent, then $f_{X+Y} = f_X \cdot f_Y$.

28 Week 10: Friday, June 6

Review of the final exam.

Reviewing the test (last class). See course homepage for copy of the test problems.

First problem: we want to find exponentially many independent sets. The idea is that we take some complete graph, and t copies of that. We note that there are $t^{n/t}$ ways to pick a vertex from each of these. We end up having that $t = 3$, so we just assemble disjoint triangles.

Second Problem: Eventown Theorem. We take incidence vectors $c_i \to v_i$. If we have $|C_i \cap C_j|$ even, then the dot product of $v_i \cdot v_j$ must be even. But we are working in $\mathbb{F}_2^n$, so the dot product must always be 0. So vectors are pairwise perpendicular. Then we can look at the span: $span(v_1, \ldots, v_m) = U$, so $U \perp U$, a totally isotropic subspace.

Now, if $U \leq \mathbb{F}_q^n$, and $\dim U = k$, then $|U| = q^k$, so as $\dim U = k$, we have $|U| = 2^k$. And we know that a totally isotropic subspace can never have dimension $\geq \frac{n}{2}$. We have that $U \perp U$, so $U^\perp \supseteq U$. We recall that $\dim U = \dim U^\perp = n$, so $k \leq n - k$, so $k \leq \frac{n}{2}$, and we're done.

(See previous notes for the proof that $\dim U + \dim U^\perp = n$ — as usual, we construct a system of homogeneous linear equations and the rank-nullity theorem.)

Third problem: if $G \not\supset C_4 \to m \leq Cn^{3/2}$. (This was a previous homework.) I.e. $\exists c > 0 (\forall n)(\exists G \not\supset C_4, m > cn^{3/2})$. So if $n = 2(q^2 + q + 1) \sim 2q^2$, we take the incidence graph of a projective plane of order q: points and lines. This yields that the number of edges is $(q+1)(q^2+q+1) \sim q^3 \sim \left(\frac{n}{2}\right)^{3/2}$.

Bonus problem: prove Chernoff's bound. We proved it in class.

Next problem: applying the Chernoff bound to rolling dice. First of all, Z is a sum $= Z_1 + \ldots + Z_n$ where

$$Z_i = \begin{cases} 1 \text{ if ith die shows a six} \\ 0 \text{ otherwise} \end{cases}$$

Clearly these are independent, but their expected value is 1/6. So we introduce $Z_i' = Z_i - \frac{1}{6}$. Then $|Z_i' \leq \frac{5}{6}$, and $E(Z_i') = 0$. And $Z' = \sum Z_i' = Z - \frac{n}{6}$. We can apply Chernoff's bound directly to this, yielding that $c = \frac{1}{2}$. We can use a trick and declare $Z_i'' = \frac{6}{5} Z_i'$, and then $c = \frac{18}{25}$, which is the best result we can get.

Next question: Shannon Capacity. Defining Shannon Capacity is clear (see previous section if necessary).

If $G \simeq \overline{G}$, then $\Theta(G) \geq \sqrt{n}$. The first observation is that $(\forall G)\alpha(G \cdot \overline{G}) \geq n$. Proof: $\{(v, v) | v \in V(G)\}$ is independent in $G \cdot \overline{G}$. (Follows from definition of adjacency.) So then

if $G \simeq \overline{G}$, $a(G^2) = \alpha(G \cdot \overline{G}) \geq n$. We know that $\Theta(G) \geq (\alpha(G^2))^{1/2}$. Then we use Fekete's Lemma to yield that $\alpha(G^2)^{1/2} = n$.

The generalization may be of interest: Theorem (Lovász): if G is self-complementary and vertex-transitive then $\theta(G) = \sqrt{n}$, and C_5 is the first member of this class of graphs. (This is a **CH*****).

Babai mentions a question that he believes is open, and not inaccessible: $(\exists k)(\forall \ell)(\exists G)$: $Theta(G) \leq k, \chi(\overline{G}) \geq \ell$. Is this true?

Next question: fractional chromatic number. We have a graph G and $C_1, \ldots, C_m$: independent sets. With each one we associate a variable $x_1, \ldots, x_m$, where $0 \leq x_i \leq 1$. For every vertex $j \in [n]$, and declare $s_j = \sum_{j \in C_i} x_i \geq 1$. These are the constraints.

Then $\chi^*(G) = \min_{constraints} \sum x_i$.

First: $\chi^* \leq \chi$, followign from the above. (The chromatic number is an instance of the fractional chromatic number.)

Next: our favorite inequality: $\chi^* \cdot \alpha \geq n$. Clearly $\sum_{j=1}^{n} s_j \geq n$, but $C = \sum x_i |C_i| = \sum_{j=1}^{n} s_j$.

But $\sum x_i \underbrace{|C_i|}_{\leq \alpha} \leq \left(\underbrace{\sum x_i}_{\chi^*} \right) \alpha$.

Next: Littlewood-Offord problem, we discussed in class.

Have a good summer and look up Lovàsz' paper on Shannon Capacity.