Math 155R, Assignment 1. Total: 20 pts.
Due on Feb 02, 2018.

Problem 1. [9pts] Let I be a non-empty set and for each $i \in I$ let $(X_i, \leq_i)$ be a poset. Define $X = \prod_{i \in I} X_i$ and on X we define the binary relation $\leq$ by

$$(x_i)_{i \in I} \leq (y_i)_{i \in I} \iff \forall i \in I, x_i \leq_i y_i.$$

(i) [3pts] Prove that $(X, \leq)$ is a poset.

(ii) [3pts] Give sufficient (and general) conditions on I and the posets $(X_i, \leq_i)$ to ensure that $(X, \leq)$ is locally finite.

(iii) [3pts] Suppose that $I = [n]$ for some $n \geq 1$ and that for each $i \in I$ we have that the poset $(X_i, \leq_i)$ is isomorphic to $([2], \leq)$ (with the usual order). Prove that $(X, \leq) \simeq (\mathcal{P}([n]), \subseteq)$.

Problem 2. [9pts] Let $u_1, \ldots, u_n$ be non-empty finite posets (we are omitting the partial order from the notation) and assume that each one is an interval. Let $u = \prod_i u_i$ be its product poset, as constructed on the previous question.

(i) [3pts] Prove that u is an interval.

(ii) [3pts] Let $\mu_i \in A[u_i]$ and $\mu \in A[u]$ be the corresponding inverses of ζ in each incidence algebra. Prove that

$$\mu(u) = \prod_{i=1}^{n} \mu_i(u_i).$$

(iii) [3pts] Deduce that if $(X, \leq) = (\mathcal{P}(R), \subseteq)$ for some finite set R, then

$$\mu[S, T] = \begin{cases} 0 & \text{if } S \text{ is not included in } T \\ (-1)^{\#T - \#S} & \text{if } S \subseteq T. \end{cases}$$

Problem 3. [2pts] Give an explicit example for a well-chosen poset X showing that, in general, the incidence algebra $A[X]$ discussed in class is not commutative.

Assignment 1

Math 155r (Combinatorics)

Due February 1st, 2018

Problem 1.

Solution. (i) To show that $(X, \preceq)$ is a poset, I'll show that $\preceq$ is indeed a binary relation that is reflexive, antisymmetric, and transitive.

Let $(x_i)_{i \in I} \in X$. Since each $(X_i, \preceq_i)$ is a poset (and consequently reflexive), we have $x_i \preceq x_i$ for all $i \in I$. Therefore, the definition of $\preceq$ implies $(x_i) \preceq (x_i)$. $\preceq$ is reflexive.

Let $(x_i)_{i \in I}, (y_i)_{i \in I} \in X$, and suppose $(x_i) \preceq (y_i)$ and $(y_i) \preceq (x_i)$. The definition of $\preceq$ implies that $x_i \preceq y_i$ for all $i \in I$. Similarly, the definition of $\preceq$ implies that $y_i \preceq x_i$ for all $i \in I$. Each $(X_i, \preceq_i)$ is a poset (and consequently antisymmetric), so $x_i \preceq y_i$ and $y_i \preceq x_i$ implies that $x_i = y_i$ for all $i \in I$. Therefore $(x_i) = (y_i)$. $\preceq$ is antisymmetric.

Let $(x_i)_{i \in I}, (y_i)_{i \in I}, (z_i)_{i \in I} \in X$, and suppose $(x_i) \preceq (y_i)$ and $(y_i) \preceq (z_i)$. The definition of $\preceq$ implies that $x_i \preceq y_i$ and $y_i \preceq z_i$ for all $i \in I$. Each $(X_i, \preceq_i)$ is a poset (and consequently transitive), so $x_i \preceq y_i$ and $y_i \preceq z_i$ imply that $x_i \preceq z_i$ for all $i \in I$. Therefore $(x_i) \preceq (z_i)$. $\preceq$ is transitive.

(ii) If I is finite, and each poset $(X_i, \preceq_i)$ is locally finite, then $(X, \preceq)$ (and its isometric class, which includes the product of X with any amount of posets that contain only one element) is locally finite.

Let $[x_1, y_1] \times ... \times [x_n, y_n]$ be some interval in X. Each $[x_i, y_i]$ is finite (since each X_i is locally finite), and there are a finite number of these intervals. Therefore the number of elements in $[x_1, y_1] \times ... \times [x_n, y_n]$ is equal to $\prod^n \#([x_i, y_i])$, which is finite (where $\#([x_i, y_i])$ is the number of elements in $[x_i, y_i]$). Therefore X is locally finite.

(iii) To prove that $(X, \preceq) \simeq (\mathcal{P}([n]), \subseteq)$, I'll define a bijection $\phi : X \to \mathcal{P}([n])$ and show that ϕ respects $\preceq$.

First, define $\phi : X \to \mathcal{P}([n])$. Since each $(X_i, \preceq_i)$ is isomorphic to $([2], \leq)$ (and is a two-element chain), there exist distinct elements $\min(X_i)$ and $\max(X_i)$. Define ϕ the following way:

$$\phi((x_i)_{i \in [n]}) = \{i \in [n] : x_i = \max(X_i)\}$$

Now I'll show ϕ is a bijection by proving it's surjective and injective.

Let $A \in \mathcal{P}([n])$. Define $(x_i)_{i \in [n]}$ so that $x_i = \begin{cases} \min(X_i) & i \notin A \\ \max(X_i) & i \in A \end{cases}$. By definition, $\phi((x_i)) = A$ so ϕ is surjective.

Let $(x_i)_{i\in[n]}, (y_i)_{i\in[n]} \in X$ such that $\phi((x_i)) = \phi((y_i))$. The definition of ϕ implies that each $x_i = y_i$ for all $i \in [n]$ so $(x_i) = (y_i)$. Therefore ϕ is injective.

Now I'll show that ϕ respects $\preceq$ (and is therefore an isomorphism) by proving that $(x_i)_{i\in[n]} \preceq (y_i)_{i\in[n]}$ implies $\phi((x_i)) \subseteq \phi((y_i))$.

Let $(x_i)_{i\in[n]}, (y_i)_{i\in[n]} \in X$, and suppose $(x_i) \preceq (y_i)$.
Suppose $a \in \phi((x_i))$. By definition of ϕ, this implies that $x_a = \max(X_a)$. The definition of $(x_i) \preceq (y_i)$ implies that $x_a \preceq y_a$. Together, $x_a = \max(X_a)$ and $x_a \preceq y_a$ imply that $y_a = \max(X_a)$. Since $y_a = \max(X_a)$, the definition of ϕ implies that $a \in \phi((y_i))$. Therefore $\phi((x_i)) \subseteq \phi((y_i))$ and ϕ is an isomorphism. Hence $(X, \preceq) \simeq (\mathcal{P}([n]), \subseteq)$. □

Problem 2.

Solution. (i) To be an interval, a poset $(X, \preceq)$ must have values $\min(X)$ and $\max(X)$. This is apparent from the definition of an interval.

I'll demonstrate the existence of $\min(u)$ and $\max(u)$. Define $(x_i)_{i\in[n]}$ such that $x_i = \min(u_i)$ (which exists because u_i is an interval). Similarly define $(y_i)_{i\in[n]}$ such that $y_i = \max(u_i)$.

For some $(z_i)_{i\in[n]} \in u$ each z_i satisfies $x_i \preceq z_i \preceq y_i$ (by the choice of x_i and y_i) so therefore $(x_i) \preceq (z_i) \preceq (y_i)$. Hence $\min(u) = (x)$ and $\max(u) = (y)$, so u is an interval.

(ii) To prove the claim $\mu(u) = \prod^n \mu_i(u_i)$, I'll proceed by induction on n.
Base Case: Suppose $n = 1$. Then for some interval $u = \prod^1 u_i = u_1$ and subinterval $[x_1, y_1] \in u$ we have

$$\mu([x_1, y_1]) = \prod^1 \mu_i([x_i, y_i]) = \mu_1([x_1, y_1])$$

Which is true since $u = u_1$ (and $A[u] = A[u_1]$). So the claim is proven for $n = 1$.

Induction Case: I'll first show, for intervals u_1, u_2 and some subinterval $([x_1, y_1], [x_2, y_2]) \in \mathcal{I}(u_1 \times u_2)$, that $\mu(([x_1, y_1], [x_2, y_2])) = \mu_1([x_1, y_1]) \cdot \mu_2([x_2, y_2])$.
Note that $\zeta(([x_1, y_1], [x_2, y_2])) = \zeta_1([x_1, y_1]) \cdot \zeta_2([x_2, y_2])$ (follows from the definition of $\preceq$ on u). Similarly note that $\delta(([x_1, y_1], [x_2, y_2])) = \delta_1([x_1, y_1]) \cdot \delta_2([x_2, y_2])$. I'll show that $\mu * \zeta = \delta$ (and by our characterization of isometries this confirms that $\zeta^{-1} = \mu$ in $A[u]$).

$$\begin{aligned}
(\mu * \zeta)(([x_1, y_1], [x_2, y_2])) &= \sum_{(x_1,x_2)\preceq(t_1,t_2)\preceq(y_1,y_2)} \mu(([x_1, t_1], [x_2, t_2])) \cdot \zeta(([t_1, y_1], [t_2, y_2])) \\
&= \sum_{(x_1,x_2)\preceq(t_1,t_2)\preceq(y_1,y_2)} \mu_1([x_1, t_1]) \cdot \mu_2([x_2, t_2]) \\
&= \sum_{x_1\preceq t_1\preceq y_1} \mu_1([x_1, t_1]) \cdot \sum_{x_2\preceq t_2\preceq y_2} \mu_2([x_2, t_2]) \\
&= \sum_{x_1\preceq t_1\preceq y_1} \mu_1([x_1, t_1]) \cdot \zeta([t_1, y_1]) \cdot \Big(\sum_{x_2\preceq t_2\preceq y_2} \mu_2([x_2, t_2]) \cdot \zeta([t_2, y_2])\Big) \\
&= (\mu_1 * \zeta_1)([x_1, y_1]) \cdot (\mu_2 * \zeta_2)([x_2, y_2]) \\
&= \delta_1(([x_1, y_1])) \cdot \delta_2(([x_2, y_2])) \\
&= \delta(([x_1, y_1], [x_2, y_2])
\end{aligned}$$

So therefore $\mu = \zeta^{-1}$. Now suppose for $u_a = \prod^n u_i$ that $\mu_a(u_a) = \prod^n \mu_i(u_i)$. For some other interval u_{n+1} and $u = u_a \times u_{n+1}$, the above argument proves $\mu(u) = \mu_a(u_a) \cdot \mu_{n+1}(u_{n+1})$. Therefore $\mu(u) = \prod^{n+1} \mu_i(u_i)$. The claim is proven for all $n \geq 1$ by induction.

(iii) Let $\#R = n$. I proved in problem 1 part (iii) that $(\mathcal{P}(R), \subseteq) \simeq (Y, \preceq)$ where $Y = \prod_i^n Y_i$, with $(Y_i, \preceq) \simeq ([2], \leq)$. This means $(\mathcal{P}(R), \subseteq) \simeq (Y, \preceq) \simeq (\prod^n [2], \leq)$. Since μ only depends on the structure of the poset (the isomorphism class), we can define μ on $\prod^n [2]$ and the definition will also hold for X. Note that each $[2]$ is an interval since $[2] = [1,2]$. By part (ii) of this problem $\mu \in A[\prod^n [2]]$ is defined

$$\mu([x,y]) = \prod_i^n \mu_i([x_i, y_i])$$

Since each poset $[2]$ has only two elements, we know the behavior of $\mu_i \in A[[2]]$ on any interval u is

$$\mu_i([x_i, y_i]) = \begin{cases} 0 & \ell([x_i, y_i]) = 0 \\ 1 & \ell([x_i, y_i]) = 1 \\ -1 & \ell([x_i, y_i]) = 2 \end{cases}$$

With this explicit definition of μ_i we can modify the definition of μ for

$$\mu([x,y]) = \begin{cases} 0 & x \npreceq y \leftrightarrow \exists i \in [n], x_i \npreceq y_i \\ (-1)^{\#\{i \in [n] : \ell([x_i, y_i]) = 2\}} & x \preceq y \end{cases}$$

With the obvious bijection ϕ as defined in problem 1, the two values $1, 2 \in [n]$ correspond to the absence or presence, respectively, of some $r_i \in R$ in $A \in \mathcal{P}(R)$. We can analyze the following expression in this new context:

$$\ell([x_i, y_i]) = \begin{cases} 0 & x_i \npreceq y_i \\ 1 & x_i = y_i.\ r_i \in \phi(x) \text{ and } r_i \in \phi(y), \text{ or alternatively } r_i \notin \phi(x) \text{ and } r_i \notin \phi(y) \\ 2 & x_i < y_i.\ r_i \notin \phi(x) \text{ and } r_i \in \phi(y) \end{cases}$$

With this analysis, it is clear that $\#\{i \in [n] : \ell([x_i, y_i]) = 2\}$ captures the number of elements that are in $\phi(y)$ but not in $\phi(x)$. Therefore, simply translating the above definition to the language of sets yields

$$\mu([S,T]) = \begin{cases} 0 & S \not\subseteq T \\ (-1)^{\#T - \#S} & S \subset T \end{cases}$$

□

Problem 3. *Solution.* Let $(X, \preceq) = ([2], \leq)$ (with the natural ordering) and let A be some commutative unitary ring. Define the function $f(u) = \begin{cases} 0 & 2 \notin u \\ 1 & 2 \in u \end{cases}$. Note that $f(\{\}) = 0$, so therefore $f \in A[X]$. However,

$$(f * \zeta)([1,2]) = \sum_{1 \leq t \leq 2} f([1,t]) \cdot \zeta([t,2]) = f([1,1]) \cdot \zeta([1,2]) + f([1,2]) \cdot \zeta([2,2]) = 1$$

$$(\zeta * f)([1,2]) = \sum_{1 \leq t \leq 2} \zeta([1,t]) \cdot f([t,2]) = \zeta([1,1]) \cdot f([1,2]) + \zeta([1,2]) \cdot f([2,2]) = 1 + 1$$

Since $f * \zeta \neq \zeta * f$ the incidence algebra $A[X]$ is not commutative. □

Math 155R, Assignment 2. Total: 20 pts.
Due on Feb 09, 2018.

Problem 1. [10pts] In this problem we consider the divisibility poset $(\mathbb{N}^*, |)$, which is locally finite. Our incidence algebra and lower convolution algebra will have coefficients in $A = \mathbb{R}$. Note that in this case elements of $\mathcal{L}(\mathbb{N}^*)$ are all functions $\phi : \mathbb{N}^* \to \mathbb{R}$ since our poset has a (unique) minimal element, namely, 1.

The function $\omega : \mathbb{N}^* \to \mathbb{R}$ is the number of *different* prime factors. A number $n \in \mathbb{N}^*$ is *squarefree* if the only square dividing n is 1.

(i) [3pts] Define the function $\mu : \mathbb{N}^* \to \mathbb{R}$ as follows:

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is squarefree} \\ 0 & \text{otherwise.} \end{cases}$$

Prove that the Möbius function $\mu' \in \mathbb{R}[\mathbb{N}^*]$ is given by

$$\mu'[m, n] = \begin{cases} \mu(n/m) & \text{if } m|n \\ 0 & \text{otherwise.} \end{cases}$$

(ii) [4pts] Define the series

$$F(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Prove that for each $s > 1$ the series $F(s)$ converges absolutely. Also, prove that

$$\lim_{s \to 1} F(s) = 0.$$

(iii) [3pts] Show that for all $n \in \mathbb{N}^*$ we have

$$\sum_{d^2|n} \mu(d) = \begin{cases} 1 & \text{if } n \text{ is squarefree} \\ 0 & \text{otherwise.} \end{cases}$$

Problem 2. [10pts] In the following problems, $p > 2$ is a prime.

(i) [3pts] Consider a polynomial $f(x) \in \mathbb{F}_p[x]$ of the form $f(x) = x^2 + c$. Prove that if $f(n)$ is a square for each $n \in \mathbb{F}_p$, then $c = 0$ (thus, f itself is a square!). Give a more general statement about other quadratic polynomials.

(ii) [3pts] Let $f \in \mathbb{F}_p[x, y]$ be a non-zero polynomial of degree $d \geq 1$. Show that

$$\#\{(\alpha, \beta) \in \mathbb{F}_p^2 : f(\alpha, \beta) = 0\} \leq dp.$$

(iii) [4pts] Use the result in the previous item (and possibly other refinements in the argument) to get better lower bounds on the size of Kakeya sets in $\mathbb{F}_p^2$.

Remark. The bound from class for $n = 2$ is $\#S \geq (2n)^{-n}p^n = p^2/16$. Beat this bound (even if your improved bound only works for large p).

Assignment 2

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* (i) I'll confirm that μ' is indeed the Möbius function by showing it matches the appropriate values for each interval $[m,n] \in \mathcal{I}(N^*)$. First note that, when m does not divide n, we have, as intended

$$\mu'([m,n]) = \mu'([]) = 0$$

Now consider the case when m divides n, and note that $[m,n] \simeq [1, \frac{n}{m}]$ with the isomorphism

$$\phi : [m,n] \to [1, \frac{n}{m}] \text{ defined as } \phi(t) = \frac{t}{m}$$

Next, suppose $\omega(\frac{n}{m}) = k$ and let

$$p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = \frac{n}{m}$$

be the prime factorization of $\frac{n}{m}$ (with each a_i the respective power of p_i in the factorization). Let

$$C_i = \{p_i^j : 0 \leq j \leq a_i\}$$

be the chain poset (that represents the divisibility structure of some number $p_i^{a_i}$) with the same relation $|$. Note that $[1, \frac{n}{m}] \simeq \prod_{i=1}^k C_i$ with the isomorphism

$$\phi : [1, \frac{n}{m}] \to \prod_{i=1}^k C_i \text{ defined by } \phi(t) = (p_i^{b_i})_{i \in [k]}$$

(where $p_1^{b_1} p_2^{b_2} \dots p_k^{b_k} = t$ is the prime factorization of t). Therefore, we have $[m,n] \simeq \prod_{i=1}^k C_i$.

I proved on the last assignment that the Möbius function of a product poset is equal to the product of the Möbius function on each individual poset. Therefore (since the Möbius function only depends on the *structure* of a poset) it suffices to demonstrate that μ' behaves on each chain C_i as the Möbius function should and that the Möbius function of the product of these chains is in fact μ'. We proved in class, where C is a chain, that the Möbius function on a chain should behave in the following way:

$$\mu_{\text{Möbius}}(C) = \begin{cases} 1 & \ell(C) = 1 \\ -1 & \ell(C) = 2 \\ 0 & \ell(C) > 2 \end{cases}$$

I've already considered the case when the interval is empty above, so we can assume each chain here has a length of at least one. Suppose $\ell(C_i) = 1$. Therefore $C_i = \{1\}$ by definition, and

$$\mu'([1,1]) = \mu(1) = (-1)^{\omega(1)} = 1$$

Suppose $\ell(C_i) = 2$. Therefore $C_i = \{1, p_i\}$ by definition, and

$$\mu'([1, p_i]) = \mu(p_i) = (-1)^{\omega(p_i)} = -1$$

Suppose $\ell(C_i) = j > 2$. Therefore $C_i = \{1, p_i, p_i^2, \ldots, p_i^{j-1}\}$ and

$$\mu'([1, p_i^{j-1}]) = \mu(p_i^{j-1}) = 0$$

since p_i^{j-1} for $j > 2$ is certainly not squarefree. Therefore μ' is the Möbius function of each chain C_i. Consequently, on the interval $[1, \frac{m}{n}] \simeq [m, n]$, we have the following Möbius function:

$$\mu_{\text{Möbius}}([1, \frac{m}{n}]) = \prod_{i=1}^{k} \mu'(C_i)$$

$$\begin{aligned}\mu'([1, \frac{m}{n}]) = \mu(\frac{m}{n}) &= \begin{cases} (-1)^{\omega(\frac{m}{n})} & \frac{m}{n} \text{ squarefree} \\ 0 & \text{otherwise} \end{cases} \\ &= \prod_{i=1}^{k} \mu'(C_i) = \mu_{\text{Möbius}}([1, \frac{m}{n}])\end{aligned}$$

Since if $\frac{m}{n}$ is not squarefree, then some C_i will have length 3 (there will be some prime with a power of 2). By definition, $\mu'(C_i) = 0$ so the entire product is 0, as expected. Similarly, if $\frac{m}{n}$ is squarefree, then $\mu_i(C_i)$ will be -1 (and 1 otherwise) only if $\ell(C_i) = 2$, which means the power of p_i in the factorization is 1. This means it is a $'$different$'$ prime factor, so the number of -1 terms multiplied is equal to $\omega(\frac{m}{n})$. Therefore $\mu_{\text{Möbius}} = \mu'$.

(ii) For each term,

$$\frac{|\mu(n)|}{n^s} \leq \frac{1}{n^s}$$

since $\mu(n) \in \{-1, 0, 1\}$. Additionally,

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

converges by the p-series test when $s > 1$. Since each term of this series has a smaller absolute value than each term of the p-series, the following series converges:

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s}$$

Hence

$$F(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

converges absolutely for every $s > 0$. Since this series converges absolutely, I am free to rearrange terms of the summation as I like. To prove that $\lim_{s\to 1+} F(s) = 0$, consider the following:

$$\begin{aligned}\sum_{d=1}^{\infty}\frac{1}{d^s}\cdot\sum_{a=1}^{\infty}\frac{\mu(a)}{a^s} &= \sum_{d=1}^{\infty}\sum_{a=1}^{\infty}\frac{\mu(a)}{(ad)^s}\\ &= \sum_{n=1}^{\infty}\sum_{a|n}\frac{\mu(a)}{n^s}\\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{a|n}\mu(a)\\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{1|a|n}\mu'([1,a])\cdot\zeta([a,n])\\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\cdot\delta([1,n])\\ &= 1\end{aligned}$$

(Since $\delta([1,a]) = 0$ for every $n \neq 1$. The second line follows: for some term $\frac{\mu(a)}{(ad)^s}$ in the original summation, the same term is counted in the second summation when $n = ad$ and $a = a$. I can rearrange the order the terms are summed because these converge absolutely.) As s approaches 1 from the right, the following series diverges:

$$\sum_{d=1}^{\infty}\frac{1}{d^s}$$

This implies that, in order for the product of these two series to exist,

$$\lim_{x\to s+} F(s) = \lim_{x\to s+}\sum_{n=1}^{\infty}\frac{\mu(n)}{n} = 0$$

(iii) Let

$$p_1^{a_1}p_2^{a_2}\dots p_k^{a_k} = n$$

be the prime factorization of n (with each a_i the respective power of p_i in the factorization). Next, define

$$m = \prod_{i=1}^{k} p_i^{b_i} \text{ where each } b_i = \left\lfloor(\frac{a_i}{2})\right\rfloor$$

(For example, if $a_i = 2$ then $b_i = 1$, or $a_i = 5$ then $b_i = 2$, etc.) This definition ensures that every value $t \in [1, m]$ satisfies $t^2|n$, and every value $d^2|n$ is present $d \in [1, m]$ (clear from the definition of m)). Since the posets $\{d : d^2|n\}$ and $[1, m]$ are in fact equal, we have

$$\sum_{d^2|n}\mu(d) = \sum_{d|m}\mu(d) = \sum_{1|d|m}\mu'([1,d])\cdot\zeta([d,m]) = \delta([1,m]) = \begin{cases}1 & m = 1\\ 0 & m \neq 1\end{cases}$$

By definition of δ. Note that if $m = 1$, then n is squarefree (since there were no primes with a power greater than 1 in the factorization of n). If $m \neq 1$, then n is not squarefree (there is some $b_i \neq 0$, hence $a_i > 1$, so p_i^2 is a factor of n). □

Problem 2. *Solution.* (i) First, I'll determine the number of squares in $\mathbb{F}_p$. Let $G = \mathbb{F}_p - \{0\}$ be a group under multiplication in $\mathbb{F}_p$. Define a group homomorphism

$$\phi : G \to G \text{ defined by } \phi(x) = x^2$$

Notice that $\ker\phi = \{1, -1\}$, since $1^2 = (-1)^2 = 1$. The First Isomorphism Theorem (which states that $\operatorname{Im}\phi \simeq G/\ker\phi$) implies that $\operatorname{Im}\phi = \frac{p-1}{2}$ (since $\#G = p - 1$). Therefore, there are only $\frac{p-1}{2}$ elements y in G such that there exists an $x \in G$ where $x^2 = y$. Including the element $0 \in \mathbb{F}_p$, we have a total of $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ squares in $\mathbb{F}_p$.

The assumption that $f(x) = x^2 + c$ is a square for every $x \in \mathbb{F}_p$ implies that, for some square y, the element $y + c$ is also a square. $0^2 = 0$ is a square, so therefore every element bc where $b \in \mathbb{F}_p$ is also a square.

Suppose, for contradiction, that $c > 0$. Let $a \in \mathbb{F}_p$ such that a is *not* a square (there exists such an element because $\frac{P+1}{2}$ is an upper bound for the number of squares and $p > 2$). Define $b = ac^{-1}$ (we know c is invertible because $c \neq 0$ and p is a prime). Since $bc = (ac^{-1})c = a$, by the above characterization of square elements, I conclude that a is a square. Contradiction, therefore $c = 0$.

Consider some general quadratic $f(x) = x^2 + bx + c$ that satisfies the condition that $f(n)$ is a square for all $n \in \mathbb{F}_p$. $'$Complete the square$'$ to yield $f(x) = (x + \frac{1}{2}b)^2 + c - \frac{1}{4}b^2$. Considering the constant $k = c - \frac{1}{4}b^2$ in the context of the previous argument implies $k = c - \frac{1}{4}b^2 = 0$. Hence any such monic quadratic which satisfies this condition can be written in the form $f(x) = (x - d)^2$.

(ii) Fix some $a \in \mathbb{F}_p$. Consider f to be a polynomial in one variable of just y. The base case proved in class implies that the polynomial vanishes at a maximum number of points

$$\#\{y \in \mathbb{F}_p : f(a, y) = 0\} \leq \deg_y f$$

Note $\deg_y f \leq \deg f$. Since there exist p possible values of a, there exist a maximum of $p \cdot \deg f$ possible points in the vanishing set of f:

$$\#\{(\alpha, \beta) \in \mathbb{F}_p^2 : F(\alpha, \beta) = 0\} \leq p \cdot \deg f$$

(iii) I'll improve this bound by adjusting the construction of the polynomial used to model the Kakeya set S (Prof. Pasten said in class this was a sufficient solution). Fix the dimension of the problem to $n = 2$.

Let K be a field and $S \in K^2$ be a nonempty set. Define $M = \#S$. I'll prove there exists a nonzero polynomial $p \in K[x, y]$ with degree $d \leq 2M^{\frac{1}{2}}$ such that $p(s) = 0$ for all $s \in S$.

Define the vector space $V_d = K[x, y]_{\leq d}$ (the space of all bivariate polynomials of total degree less then or equal to d). Notice that

$$\dim V_d = \binom{2+d}{2} = (d + 1)(d + 2)$$

(since we can count all possible monomials, which are a basis of V_d, by choosing d strokes from $d + 2$ dots). Define a linear map

$$L : V_d \to K^M \text{ defined as } L(p) = (p(s))_{s \in S}$$

I'll show the $\ker L \neq \{0\}$, hence there exists some nonzero polynomial that vanishes on every element in S. Note that

$$\dim V_d = (d+1)(d+2) > d^2$$

So if $\operatorname{Im} L = M \leq d^2$ then certainly $\dim V - \dim \operatorname{Im} L = \dim \ker L > 0$ by the rank-nullity theorem. Therefore d must be greater than or equal to $M^{\frac{1}{2}}$. Since $M \geq 1$, there exists some d' such that $M^{\frac{1}{2}} \leq d' < 2M^{\frac{1}{2}}$. Hence there exists such a polynomial with degree $d' < 2M^{\frac{1}{2}}$ that vanishes on S.

Now that I've proved this lemma, consider the following:
Claim: Every Kakeya set $S \subset F_p^2$ satisfies $\#S = M \geq c_2 p^2$ where $c_2 = (2)^{-2} = \frac{1}{4}$.

Suppose, for a contradiction, there existed such a Kakeya set $S \subset \mathbb{F}_p^2$ with $\#S = M < \frac{1}{4}p^2$

By the lemma, construct a nonzero polynomial $f \in \mathbb{F}_p^2[x, y]$ that satisfies:

$$f(s) = 0 \text{ for all } s \in S$$

$$\deg f = d \leq 2M^{\frac{1}{2}} < p$$

(By assumption $M < \frac{1}{4}p^2$ so therefore $2M^{\frac{1}{2}} < p$). Now let $h \in \mathbb{F}_p^2$ be the homogeneous part of f with the highest degree (we know h is nonzero because the lemma guarantees that f is nonzero).

Let $u \in \mathbb{F}_p^2 \setminus \{0\}$ be a direction vector. By definition of a Kakeya set, there exists some offeset/translation vector $v \in \mathbb{F}_p^2$ such that

$$\{v + \lambda u : \lambda \in \mathbb{F}_p\} \subset S$$

Consider the function

$$\phi : \mathbb{F}_p \to \mathbb{F}_p[t] \text{ defined as } \phi(t) = f(v + tu)$$

which maps some element t to a polynomial in $_p[t]$. Note that the coefficient of the monomial in $\phi(t)$ of degree d (the term with t^d) is equal to h (the homogeneous part of f). (This is because each variable in f is now expressed in terms of some expression that includes one t.) Therefore $\deg \phi(t) \leq \deg f < p$.

However, $\phi(t)$ vanishes on p points (all of $\mathbb{F}_p$) (since f vanishes on the Kakeya set S). A nonzero polynomial $\phi(t)$ of one variable cannot vanish on $p > \deg \phi(t)$ points, therefore $\phi(t)$ is the zero polynomial. This implies $h(u) = 0$ for all $u \in F_p^2 - \{0\}$ (since h is homogeneous). Finally, since h vanishes on $\mathbb{F}_p \times \mathbb{F}_p$ and $p > \deg h$, we conclude that h is the zero polynomial (by the lemma proved in class). Therefore f is the zero polynomial. Contradiction.

Hence a Kakeya set $S \subset \mathbb{F}_p^2$ has cardinality $\#S \geq \frac{1}{4}p^2$ (which beats the bound proved in class by a factor of 4). □

Math 155R, Assignment 3. Total: 20 pts.
Due on Feb 16, 2018.

Problem 1. [9pts] Let p be a prime. Let $\mathcal{I}_p(r)$ be the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of exact degree r, for $r \geq 1$.

(i) [3pts] Prove that the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree $\leq r$ is equal to the polynomial $x^{p^r} - x$.

(ii) [3pts] Prove that

$$\mathcal{I}_p(r) = \frac{1}{r}\sum_{d|r} \mu(d) p^{r/d}.$$

(iii) [3pts] Prove that

$$\mathcal{I}_p(r) = \frac{p^r}{r} + \mathcal{O}\left(\frac{p^{r/2}}{r}\right)$$

where the implicit constant is absolute (i.e. independent of p and r).

Problem 2. [3pts] Let p be a prime and let A be a non-empty subset of $\mathbb{F}_p$. Prove that

$$\#\{a+b : a, b \in A \text{ and } a \neq b\} \geq \min\{p, 2 \cdot \#A - 3\}.$$

Problem 3. [8pts] Let K be a field and let S be a set of five points in K^2 such that no three points of S are collinear.

(i) [3pts] Prove that there is a polynomial $f \in K[x, y]$ of total degree 2 vanishing at each point of S.

(ii) [3pts] Prove that the polynomial f in the previous item is unique (for this set S) up to a scalar multiple.

(iii) [2pts] Prove that given any five points in $\mathbb{R}^2$ with no three of them collinear, there is a unique smooth conic section passing through them.

Assignment 3

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* (i) The following proof is from *A Concrete Introduction to Higher Algebra.* I will only record here the first part of the proof which I understand:

Claim: If $q(x)$ is an irreducible polynomial of degree d and d divides n, then $q(x)$ divides x^{p^n}
Let $F = F_p[x]/(q(x)) = F_p[\alpha]$ be the extension of $\mathbb{F}_p$ with α a root of $q(x)$. Then $q(x)$ is the minimal polynomial over $\mathbb{F}_p$ of α. Since F is a field with p^d elements (remember d is the degree of $q(x)$) then, by Fermat's Little Theorem (which states for a prime p and any integer a that $a^p - a$ is a multiple of p, which means it equals zero in our field)

$$\alpha^{p^d} = \alpha$$

(since we are working in a finite field). Since d divides n, there exists some integer e such that $de = n$. Therefore we have

$$\alpha^{p^n} = \alpha^{p^{de}} = \alpha$$

so therefore α is a root of $x^{p^n} - x$. By assumption, $q(x)$ is irreducible in $\mathbb{F}_p[x]$ so either $q(x)$ divides $x^{p^n} - x$ or there exist polynomials $s(x), t(x) \in \mathbb{F}_p[x]$ such that

$$s(x)q(x) + t(x)(x^{p^n} - x) = 1$$

(see Wikipedia article on Bezout's identity. For a, b with greatest common factor d there exist some integers x and y such $ax + by = d$. Here, the greatest common factor of $q(x)$ and $x^{p^n} - 1$ is 1). However, if this expression were true then we could evaluate at α for

$$s(\alpha)q(\alpha) + t(\alpha)(\alpha^{p^n} - \alpha) = 0 \neq 1$$

because α is a root of $q(x)$ and $x^{p^n} - x$ as shown above. Contradiction. Therefore $q(x)$ divides x^{p^n}.

The next part of the proof involves showing that every irreducible factor of $x^{p^n} - x$ has a degree d that divides n, but it involves splitting fields and morphisms that I do not understand.

(ii) Since the product of all monic irreducible polynomials of degree d dividing r is equal to $x^{p^r} - x$, this implies that the sum of the degrees on the largest term of each monic irreducible polynomial is p^r. Therefore, we have

$$p^r = \sum_{d|r} d \cdot \mathcal{I}_p(d)$$

(This is the summation of the degree of the largest term times the number of polynomials for each class of monic irreducible polynomials of exact degree d.) If we now define

$$\Phi(r) = p^r$$

$$\phi(r) = r \cdot \mathcal{I}_p(r)$$

Then the formula for the Möbius inversion yields

$$\phi(r) = (\Phi * \mu')(r)$$

Replace the convolution expression and μ' as defined on the previous assignment for the divisibility poset $\mathbb{N}$ and observe

$$r \cdot \mathcal{I}_p(r) = \sum_{e|r} \mu'([e,r]) \cdot p^e = \sum_{e|r} \mu(\frac{r}{e}) \cdot p^e$$

Define $d = \frac{r}{e}$ and $e = \frac{r}{d}$. As the summation ranges over the values of e, it will also range over all the values of d. Therefore we can equivalently replace

$$r \cdot \mathcal{I}_p(r) = \sum_{d|r} \mu(d) \cdot p^{r/d}$$

Divide both sides by r to yield the desired result

$$\mathcal{I}_p(r) = \frac{1}{r} \sum_{d|r} \mu(d) \cdot p^{r/d}$$

(iii) To show this claim, it is necessary to demonstrate that there exists an A such that

$$|\mathcal{I}_p(r) - \frac{p^r}{r}| \leq A \frac{p^{r/2}}{r}$$

Or equivalently,

$$\frac{p^r}{r} - A\frac{p^{r/2}}{r} \leq \mathcal{I}_p(r) \leq \frac{p^r}{r} + A\frac{p^{r/2}}{r}$$

To prove the upper bound, I'll use the equation derived in the previous part:

$$p^r = \sum_{d|r} d \cdot \mathcal{I}_p(d) = r \cdot \mathcal{I}_p(r) + \sum_{d|r, d \neq r} d \cdot \mathcal{I}_p(d)$$

$$r \cdot \mathcal{I}_p(r) = p^r - \sum_{d|r, d \neq r} d \cdot \mathcal{I}_p(d)$$

Since the summation is nonnegative, this implies

$$\mathcal{I}_p(r) \leq \frac{p^r}{r}$$

To prove the lower bound, consider the following

$$\begin{aligned} p^r &= r \cdot \mathcal{I}_p(r) + \sum_{d|r, d \neq r} d \cdot \mathcal{I}_p(d) \\ &\leq r \cdot \mathcal{I}_p(r) + \sum_{d \leq \frac{r}{2}} d \cdot \mathcal{I}_p(d) \end{aligned}$$

(Since the divisibility summation will only sum on values of d less than or equal to $\frac{r}{2}$ anyway, and each summand is nonnegative.) With the upper bound of $\mathcal{I}_p(d)$ proved above, we now have

$$p^r \leq r \cdot \mathcal{I}_p(r) + \sum_{d \leq \frac{r}{2}} d \cdot \frac{p^d}{d} = r \cdot \mathcal{I}_p(r) + \sum_{d \leq \frac{r}{2}} p^d$$

The summation is now a geometric series, so we can compute

$$\sum_{d\leq \frac{r}{2}} p^d = p\frac{1-p^{r/2}}{1-p} = p\frac{p^{r/2}-1}{p-1} \leq \frac{p^{r/2+1}-1}{p-1}$$

Subtracting this value for the summation from the above inequality yields

$$p^r - \frac{p^{r/2+1}-1}{p-1} \leq r \cdot \mathcal{I}_p(r)$$

The numerator of this fraction factors into $(p-1)$ and another factor (since clearly 1 is a root of $p^{r/2+1}-1$). This other factor is asymptotically less than $2p^{r/2}$ (since the leading term of this factor is $p^{r/2}$, as it multiplies with $p-1$ to yield $p^{r/2+1}-1$). Therefore we have

$$p^r - 2p^{r/2} \leq r \cdot \mathcal{I}_p(r)$$

$$\frac{p^r}{r} - 2\frac{p^{r/2}}{r} \leq \mathcal{I}_p(r)$$

So I have proven the lower bound. We now see that an absolute constant of $A = 2$ satisfies

$$\frac{p^r}{r} - 2\frac{p^{r/2}}{r} \leq \mathcal{I}_p(r) \leq \frac{p^r}{r} + 2\frac{p^{r/2}}{r}$$

Therefore I have proven the claim.

(NB: Help with the last part of this problem from Markus Blaser and Chandan Saha's lecture on computational number theory and algebra, number 9) □

Problem 2. *Solution.* Define $\alpha = \#A$, and let

$$C = \{a + b : a, b \in A \text{ and } a \neq b\}$$

First suppose that $2\alpha - 2 > p$. I'll prove that, in such a case, $C = \mathbb{F}_p$.

By definition, $C \subseteq \mathbb{F}_p$. To show the other inclusion, let $u \in \mathbb{F}_p$. Define

$$u - A = \{u - a : a \in A\}$$

Note that

$$A \cap (u - A) \neq \emptyset$$

since $\#A = \#(u - A) = \alpha$ and $2\alpha - 2 > p$ by assumption (it is not possible to have this many different elements in $\mathbb{F}_p$). Therefore $A \cap (u - A)$ has at least two distinct elements (A and $u - A$ must overlap twice). There exist two distinct values $a_1, a_2 \in (A \cap (u - A)$ such that

$$a_1 \in u - A \text{ and } a_2 \in u - A$$

Consequently, there exist a_1' and a_2' (by definition of $u - A$) such that

$$a_1 = u - a_1' \text{ and } a_2 = u - a_2'$$

$$u = a_1 + a_1' = a_2 + a_2'$$

Since $a_1 \neq a_2$, this implies that either $a_1 \neq a_1'$ or $a_2 \neq a_2'$ (since there is only one way to divide a number u into two equal parts). Since $a_i, a_i' \in A$ and $a_i \neq a_i'$ for some i, therefore $a_i + a_i' = u \in C$. This proves the inclusion in the other direction, hence $C = \mathbb{F}_p$.

Now suppose $2\alpha - 2 \leq p$. I'll show that $\#C \geq 2\alpha - 3$.

Suppose, for a contradiction, that $\#C \leq 2\alpha - 4$. For simplicity, let C' be some set with $C \subseteq C'$ and $\#C' = 2\alpha - 4$ (I'll show that the largest possible such set still leads to contradiction, and certainly smaller sets will as well).

Define the bivariate polynomial

$$f(x,y) = (x-y) \cdot \prod_{c \in C'} (x+y-c)$$

Note that $f \in \mathbb{F}_p[x,y]$ and that $f(x,y) = 0$ for all $(x,y) \in A \times A$ (since when $x \neq y$ the term $x+y$ corresponds to some $a+b = c \in C \subset C'$ and therefore $(x+y-c) = 0$. When $x = y$, we have $(x-y) = 0$).

Additionally, observe that deg $= \#C' + 1 = 2\alpha - 3$ by construction.

First, observe that the monomial $x^{\alpha-2}y^{\alpha-2}$ appears in $\prod_{c \in C'}(x+y-c)$. This is because

$$\binom{2\alpha-4}{\alpha-2} \neq 0 \text{ in } \mathbb{F}_p$$

Since $2\alpha - 4 < 2\alpha - 2 \leq p$ (we proved a similar version of this claim in class). The factorials of numbers less than p will always be nonzero (nonzero elements cannot multiply to equal zero in a field). This means that the coefficient of $x^{\alpha-2}y^{\alpha-2}$ is nonzero. Therefore, the coefficient of $x^{\alpha-1}y^{\alpha-2}$ (or alternatively $x^{\alpha-2}y^{\alpha-1}$) in $(x-y)\prod_{c \in C'}(x+y-c)$ is also nonzero.

Finally, the monmoial $x^{\alpha-1}y^{\alpha-2}$ appears in f. Additionally observe that

$$\deg(x^{\alpha-1}y^{\alpha-2}) = 2\alpha - 3 = \deg f$$

Furthermore, $\alpha - 1 < \alpha = \#A$ and $\alpha - 2 < \alpha = \#A$. By the Combinatorial Nullstellensatz, the polynomial f cannot vanish on the product set $A \times A$. Contradiction. Hence $\#C \geq 2\alpha - 3$, so we conclude

$$\#\{a+b : a, b \in A \text{ and } a \neq b\} \geq \min\{p, 2 \cdot \#A - 3\}$$

□

Problem 3. *Solution.* (i) For some field K, let $K[x,y]_{d \leq 2}$ be the space of all bivariate polynomials of degree less than or equal to 2. Consider the linear map

$$L : K[x,y]_{d \leq 2} \to K^5 \text{ defined by } L(p) = (p(s))_{s \in S}$$

Note that the dimension of $K[x,y]_{d \leq 2}$ is 6. The explicit basis is

$$1, x, y, x^2, y^2, xy$$

This can also be seen with the stroke/dot monomial counting method, which yields

$$\binom{n+d}{d} = \binom{2+2}{2} = 6$$

Furthermore $\dim \operatorname{Im} L \leq 5$, since the dimension of the codomain K^5 is 5. Therefore, by the rank-nullity theorem, we have

$$\dim \ker L = \dim K[x,y]_{d\leq 2} - \dim \operatorname{Im} L \geq 6 - 5 = 1$$

So $\ker L$ is nonzero, which means there exists a nonzero polynomial $f \in K[x,y]_{d\leq 2}$ such that $f(s) = 0$ for all $s \in S$ (f vanishes at each point in S). Now I'll prove $\deg f = 2$. Suppose, for a contradiction, that $\deg f < 2$. Then we can write

$$f(x,y) = ax + by + c$$

(Clearly every bivariate polynomial of degree less than 2 has this form. Alternatively, note that this is just a linear combination of the basis vectors with degree less than 2.) Set $f(x,y) = 0$ for

$$0 = ax + by + c$$

However, this equation describes a line, and by assumption no three points in S are colinear, hence f cannot vanish on all of the points in S. Contradiction. Therefore $\deg f = 2$.

(ii) To prove that the polynomial f is unique, I will demonstrate that $\ker L$ is one-dimensional. Choose 4 points $p_1, p_2, p_3, p_4 \in S$. Let

$$0 = a_1x + b_1y + c_1$$

be the line that intersects p_1 and p_2 in the plane K^2 (we can always define a line between two points). Similarly, let

$$0 = a_2x + b_1y + c_2$$

be the line that intersects p_3 and p_4 in the plane K^2. By construction, the polynomial

$$g(x,y) = a_1x + b_1y + c_1$$

vanishes on p_1 and p_2, and that the polynomial

$$h(x,y) = a_2x + b_2y + c_2$$

vanishes on p_3 and p_4. Note that $\deg g \leq 1$ and $\deg h \leq 1$. The polynomial

$$(gh)(x,y) = (a_1x + b_1y + c)(a_2x + b_2y + c_2)$$

vanishes on all four points p_1, p_2, p_3, p_4 by construction. Furthermore, $\deg gh \leq 2$. Therefore $gh \in K[x,y]_{d\leq 2}$. This means I can construct a polynomial that vanishes on any four points in S, and is nonzero on the fifth (because this fifth point p_5 does not lie on the $p_1 - p_2$ line or the $p_3 - p_4$ line by assumption. Therefore $g(p_5) \neq 0$ and $h(p_5) \neq 0$ so $(gh)(p_5) \neq 0$). Consequently, there exist polynomials $q_i \in K[x,y]_{d\leq 2}$ such that

$$L(q_1) = (e_1, 0, 0, 0, 0)$$

$$L(q_2) = (0, e_2, 0, 0, 0)$$
$$L(q_3) = (0, 0, e_3, 0, 0)$$
$$L(q_4) = (0, 0, 0, e_4, 0)$$
$$L(q_5) = (0, 0, 0, 0, e_5)$$

With each $e_i \neq 0$. Since there are 5 linearly independent vectors in the image of L, we have $\dim \operatorname{Im} L = 5$. By the rank nullity theorem, this implies

$$\dim \ker L = K[x, y]_{d \leq 2} - \dim \operatorname{Im} L = 6 - 5 = 1$$

So the dimension of the kernel (which is exactly the set of polynomials that vanish on all five points) is exactly 1. Therefore $\ker L = \{\lambda f : \lambda \in K\}$, so f is unique up to a scalar multiple.

(iii) This result follows from the previous two parts. I proved above that there exists some polynomial g of degree 2 that vanishes on these five points in $\mathbb{R}^2$. Set g equal to zero for

$$g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with $a, b, c, d, e, f \in \mathbb{R}$. This is the general equation for a conic section (which is defined by any quadratic bivariate polynomial. See Wikipedia "Conic Section"). All that remains is to show that g is not a degenerate conic section. The only degenerate conic sections are intersecting lines, parallel lines, a single line, and a point (See Wikipedia "Degenerate Conic"). All four of these violate the fact that g vanishes on five distinct points, of which no three are colinear. □

Math 155R, Assignment 4. Total: 20 pts.
Due on Feb 26, 2018.

Problem 1. [6pts] Let $G = (V, E)$ be a graph.

(i) [3pts] Suppose that $v = 100$ and $e = 4852$. Prove that G is connected.

(ii) [3pts] Starting from the idea implicit in the previous item, state and prove a more general result.

Problem 2. [6pts] Let $T = (V, E)$ be a non-trivial tree.

(i) [3pts] Suppose that T has exactly two vertices of degree 1. Prove that $T \simeq P^e$.

(ii) [3pts] Suppose that T has exactly four vertices of odd degree. Prove that these degrees are $1, 1, 1, 3$ or $1, 1, 1, 1$.

Problem 3. [8pts] Prove that every tree is planar.

Assignment 4

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* (i) and (ii) Suppose, for a contradiction, that $G = (V, E)$ is not connected. This implies that

$$n := \#\pi_0(G) \geq 2$$

(There are $n \geq 2$ individual connected components of G). Let the collection

$$\{G_1, \ldots, G_n\} = \{(V_1, E_1), \ldots, (V_n, E_n)\}$$

be the set of graphs such that each G_i is connected, and each G_i is a subgraph of G. Accordingly define

$$v_i := \#V_i \text{ and } e_i := \#E_i$$

By definition

$$v = \#V = \sum_i^n v_i \text{ and } e = \#E = \sum_i^n e_i$$

Now, define the graph $G' = (V', E')$ where

$$V' = \bigsqcup_{i=2}^n V_i$$

$$E' = \bigsqcup_{i=2}^n E_i$$

Where $\sqcup$ is the disjoint union. The union is disjoint because the above collection of G_i is a partition (necessarily disjoint) by definition. Therefore we know

$$v' = \#V' = \sum_{i=2}^n v_i = v - v_1$$

$$e' = \#E' = \sum_{i=2}^n e_i = e - e_1$$

Notice that G' is a subgraph of $K^{v'}$ (where $K^{v'}$ is a complete graph with v' vertices). We know that $K^{v'}$ has $\binom{v'}{2}$ edges, since there exists an edge between every vertex. Since G' is a subgraph, we also know

$$e' \leq \binom{v'}{2}$$

Similarly notice that G_1 is a subgraph of K^{v_1}. We know K^{v_1} has $\binom{v_1}{2}$ ediges, since there exists an edge between every vertex. Since G_1 is a subgraph, we also know

$$e_1 \leq \binom{v_1}{2}$$

Combine all of the above facts for

$$e = \sum_{i=1}^{n} e_i = e_1 + \sum_{i=2}^{n} e_i = e_1 + e' \leq \binom{v_1}{2} + \binom{v'}{2} = \binom{v_1}{2} + \binom{v - v_1}{2}$$

This expression is the largest when v_1 takes the minimum possible value of 1 (a connected component must have at least one vertex). This is because the number of edges in a graph with v vertices is a maximum of

$$\binom{v}{2} = \frac{v!}{2(v-2)!} = \frac{v(v-1)}{2}$$

This expression is related quadratically to the number of vertices, so therefore the expression

$$\binom{v_1}{2} + \binom{v - v_1}{2} = \frac{v_1!}{2(v_1 - 2)!} + \frac{(v - v_1)!}{2(v - v_1 - 2)!} = \frac{v_1(v_1 - 1)}{2} + \frac{(v - v_1)(v - v_1 - 1)}{2}$$

is maximized when either $v_1 = 1$ or $v_1 = v - 1$ (the expression is symmetric in this sense). (Alternatively, since we are dealing with a finite vertex set just graph the expression to find a maximum on the interval $1 \leq x \leq v$ to determine $v_1 = x$.)

Evaluate this expression for $v = 100$ to yield

$$e \leq \binom{1}{2} + \binom{100 - 1}{2} = 0 + 4851$$

But by assumption $e = 4582$, so we have a contradiction. Therefore the original supposition (that G is not connected) is false. So G is connected.

For a more general result, observe that, for an unconnected graph with v vertices, the maximum number of edges is

$$e \leq \binom{v-1}{2}$$

(this follows from the above work). Therefore, if there are more edges than this expression in the graph, it is necessarily connected. □

Problem 2. *Solution.* (i) Let $x, y \in V$ be the two vertices with

$$\deg x = \deg y = 1$$

I will first demonstrate that, for all other $z \in V$ where $z \neq x$ and $z \neq y$, we have

$$\deg z = 2$$

Suppose, for a contradiction, that there existed such a $z \in V$ with $\deg z = k \geq 3$. Let

$$V' = \{v \in V : \{v, z\} \in E \text{ and } v \neq x \text{ and } v \neq y\}$$

(V' is the set of adjacent vertices to z excluding x and y. Our definition of a graph guarantees that there are a total of k adjacent vertices, since we forbid repeated edges and loops.) Note that

$$\#V' \geq k - 2 = 1$$

Further observe that, if there existed some vertex $v \in V'$ with $\deg v = 1$, then this would contradict the assumption that x and y are the *only* two vertices of degree 1. Hence all vertices $v \in V$ have degree $\deg v \geq 2$.

Let $v' \in V$ be some vertex. Consider the graph $F = (V, E')$, where $E' = E \setminus \{v', z\}$. Note that F is a graph (a forest) with two connected components. Furthermore, we proved in class that F is specifically a a forest that contains two trees (see the proof about the number of edges in a tree. We proved in the inductive step that deleting an edge from a tree results in a graph with two trees). Let

$$T_1 = (V_1, E_1) = C(z)$$
$$T_2 = (V_2, E_2) = C(v')$$

be the connected components of z and v respectively. T_1 is nontrivial (because z now has at least two remaining adjacent vertices) and T_2 is nontrivial (because $\deg v' \geq 2$). Apply the proposition proved in class to conclude that both T_1 and T_2 have at least two endpoints (vertices of degree 1). Observe that

$$T = (V, E) = (V_1 \cup V_2, E_1 \cup E_2 \cup \{z, v'\})$$

Since $v' \neq x$ and $v' \neq y$ by assumption (x and y have degree 1 and we chose v' with $\deg v' \geq 2$), therefore there exist at least three distinct vertices (it is possible that v' was an endpoint of T_2, so when we reconnect the graphs it is no longer an endpoint. If this is the case, however, the other endpoint of T_2 is preserved) labeled $x, y, w \in V$ such that

$$\deg x = \deg y = \deg w = 1$$

Contradiction. Hence for all $z \in V$ where $z \neq x$ and $z \neq y$, we have

$$\deg z = 2$$

Now that we know the degree sequence of T is

$$1, 1, 2, \ldots, 2, \ldots, 2$$

I'll construct an isomorphism on vertices

$$\phi : T \to P^e$$

Note that the vertex set of P^e is the set of integers $\{0, \ldots, e\}$ by definition of a path with length e. Furthermore, we proved in class that for a tree T we know $e = v - 1$, so $v = e + 1$. Therefore

$$\#V = \#\{0, \ldots, e\}$$

Recall that, for some $x, y \in V$, we know $d_T(x, y)$ is the distance between the vertices x and y, defined as the length of the shortest path between the two vertices. Let $x \in V$ be some vertex with $\deg x = 1$. Define

$$\phi(v) = d_T(x, v)$$

I'll demonstrate that ϕ is an isomorphism by proving that it is a bijective morphism. Since the domain and range of ϕ have the same cardinality (see two paragraphs above; the cardinality of both is $e+1$), it suffices to show that ϕ is injective and surjectivity follows.

Suppose, for a contradiction, that there existed $v_1, v_2 \in V$ with $v_1 \neq v_2$ such that $\phi(v_1) = \phi(v_2)$. Equivalently, this means

$$d_T(x, v_1) = d_T(x, v_2)$$

Define the two paths from x to v_i as follows

$$P_1 : x \to p_1 \to \ldots \to p_i \to \ldots \to v_1$$

$$P_2 : x \to q_1 \to \ldots \to q_i \to \ldots \to v_2$$

There exists some vertex v_1' in the path P_1 and v_2' in the path P_2 such that $v_1' \neq v_2'$ but $p_i = q_i$ for all of the vertices that come earlier in this path (since $v_1 = v_2$ the paths must diverge at some point; v_1' and v_2' are the vertices in each respective path right after this initial divergence). Observe that, if d is the vertex right before v_1' and v_2' in the two paths, then either $d = x$ or $d = p_i = q_i$ for some i.

If $d = x$, then we have a contradiction since $\deg d \geq 2$ (it is connected to v_1' and v_2') and by assumption $\deg x = 1$. If $d = p_i = q_i$ for some i then we have a contradiction since $\deg d \geq 3$ (it is connected to v_1', v_2', and the vertex $p_{i-1} = q_{i-1}$).

Either way, there is a contradiction. Therefore for every $v_1, v_2 \in V$ with $v_1 \neq v_2$, we know $\phi(v_1) \neq \phi(v_2)$, so ϕ is injective, and therefore bijective.

Recall that $T = (V, E)$. Also recall the path graph $P^e = (W, F)$, where

$$W = \{0, 1, \ldots, e\}$$

$$F \text{ is the edgeset induced by the relation } xR_F y \iff (x - y) \in \{1, -1\}$$

To show ϕ is a morphism, suppose there exist $v_1, v_2 \in V$ such that $\{v_1, v_2\} \in E$. I'll prove that this implies $\{\phi(v_1), \phi(v_2)\} \in F$.

Suppose $v_1, v_2 \in V$ such that $\{v_1, v_2\} \in E$. This implies $d_T(v_1, v_2) = 1$ (since there exists a path $P^1 : v_1 \to v_2$ of length 1 between the vertices).

Without loss of generality, suppose

$$\phi(v_1) = d_T(x, v_1) < d_T(x, v_2) = \phi(v_2)$$

(they cannot be equal because $\phi(v) = d_T(x, v)$ is injective). Let $\phi(v_1) = k$. Since this means $d_T(x, v_1) = k$, there exists a path

$$P^k : x \to p_1 \to \ldots \to p_i \to \ldots \to v_1$$

of length k that connects x and v_1. Consider the path

$$P^{k+1} : x \to p_1 \to \ldots \to p_i \to \ldots \to v_1 \to v_2$$

of length $k+1$ that connects x and v_2 (we can just append v_2 to the previous path because v_1 and v_2 are adjacent. We also know that v_2 has not appeared in the path P^k elsewhere because by assumption $d_T(x, v_1) < d_T(x, v_2)$). This implies $d_T(x, v_2) = \phi(v_2) = k+1$.

Therefore $\phi(v_1) = k$ and $\phi(v_2) = k+1$. Since $(k - (k+1)) \in \{1, -1\}$ this implies $\{k, k+1\} \in W$ (where W is the edgeset of the codomain P^e). Therefore $\{\phi(v_1), \phi(v_2)\} \in W$, so ϕ is indeed an isomorphism. Hence $T \simeq P^e$.

(ii) Let $v = \#V$. Let the degree sequence of T be the following:

$$\delta = d_1 \leq d_2 \leq \ldots \leq d_i \leq \ldots \leq d_v = \Delta$$

We proved in class that every nontrivial tree has at least 2 endpoints (vertices of degree 2). Therefore two of the odd vertices must have degree 1. Now let the other two vertices of odd degree have degree d_{v-1} and d_v. Also assume that the other vertices have the *minimum* possible degree of 2 (and there are $v-4$ such vertices). Therefore

$$\sum_i^v d_i \geq 1 + 1 + d_{v-1} + d_v + (v-4)(2) = 2v + d_{v-1} + d_v - 6$$

We know that $2e = \sum d_i$ (we proved this in class), so therefore

$$2e \geq 2v + d_{v-1} + d_v - 6$$

We proved in class that $e = v - 1$ for a tree, so this yields

$$2(v-1) = 2v - 2 \geq 2v + d_{v-1} + d_v - 6$$

$$4 \geq d_{v-1} + d_v$$

d_{v-1} and d_v are both odd by assumption and positive (because the graph is connected, and if either were zero then the graph would be disconnected). This implies that the only possible degrees of d_{v-1} and d_v are $1, 1$ and $1, 3$.

Therefore, with the two endpoints from above, the only possible degrees are $1, 1, 1, 1$ or $1, 1, 1, 3$. □

Problem 3. *Solution.* I'll prove that every tree $T = (V, E)$ is planar by induction on $v = \#V$.

For a base case, consider the trivial tree when $v = 1$. Therefore $V = \{v_1\}$ and $E = \emptyset$. Define

$$\theta : V \to \mathbb{R}^2 \text{ such that } \theta(v_1) = (x, y) \text{ for any } (x, y) \in \mathbb{R}^2$$

$$\psi : E \times [0, 1] \to \mathbb{R}^2$$

Clearly both θ and ψ are injective (since θ only maps one element and ψ maps no elements). ψ is also 'acceptable' (there are only a finite number of lines $L \in \mathbb{R}^2$ that intersect $\operatorname{Im}\psi$ on infinite points) because $\operatorname{Im}\psi = \emptyset$. The final condition, namely that $\{x, y\} \in E$ implies

$$\{\psi(\{x, y\}, 0), \psi(\{x, y\}, 1)\} = \{\theta(x), \theta(y)\}$$

holds vacuously since E is empty. Therefore the trivial tree is planar, so the base case is proven.

For the inductive step, suppose that every tree with less than or exactly v vertices is planar. Now let $T = (V, E)$ be some tree with $\#V = v + 1$. We proved in class that every nontrivial tree has at least two endpoints with degree 1 (and T is nontrivial since $\#V = v + 1 \geq 1 + 1$). Let x be such an endpoint, and suppose that $\{x, y\} \in E$ for some $y \in V$ (note that this is the only edge that contains x since $\deg x = 1$ by construction).

Now define the tree $T' = (V', E')$ with

$$V' = V \setminus \{x\}$$

$$E' = E \setminus \{x, y\}$$

Since $\#V' = v$, apply the inductive hypothesis to conclude that T' is planar with some embedding (θ', ψ') that satisfies the requisite conditions.

Now consider the local region around the vertex y. Since ψ' is acceptable, there are only a finite number of lines that intersect ψ in an infinite number of points around y (note that by this inductive step *all* the edges will be constructed as straight lines). Therefore, consider some line through y that does not intersect ψ at an infinite (and therefore at any) points. Let p be some point on this line, locally close to y. Define

$$\theta : V \to \mathbb{R}^2 \text{ such that } \theta(v) = \begin{cases} \theta'(v) & v \in V' \\ p & v = x \end{cases}$$

$$\psi : E \times [0, 1] \to \mathbb{R}^2 \text{ such that } \psi(\{a, b\}, t) = \begin{cases} \psi'(\{a, b\}, t) & \{a, b\} \in E' \\ \theta(x) + t(\theta(y) - \theta(x)) & \{a, b\} = \{x, y\} \end{cases}$$

We defined θ and ψ in terms of θ' and ψ', so to check that θ and ψ still satisfy the conditions it suffices to examine how the behave on the vertex x and the edge $\{x, y\}$, respectively.

θ is injective, because we chose p such that $p \notin \operatorname{Im} \psi'$, and therefore $p \notin \operatorname{Im} \theta'$ (since $\operatorname{Im} \theta \subset \operatorname{Im} \psi$ when the edge set is nonempty). Since $\theta(x) = p$ is not in $\operatorname{Im} \theta'$, the injectivity of θ is maintained.

Similarly, we chose p to be on a line so that the line does not intersect *any* points in $\operatorname{Im} \psi'$. Therefore, since the piecewise parametization of a line is continuous and clearly injective, we know that ψ is still injective.

ψ is still 'acceptable' because, as mentioned in class, the edge added is polygonal (it is merely a line segment).

Finally, for the added edge $\{x, y\}$, observe that

$$\{\psi(\{x, y\}, 0), \psi(\{x, y\}, 1)\} = \{\theta(x), (\theta(x) + (\theta(y) - \theta(x)))\} = \{\theta(x), \theta(y)\}$$

Therefore the embedding (θ, ψ) of T meets the requisite conditions, so T is planar. By induction, we conclude that all trees are planar. □

Math 155R, Assignment 5. Total: 20 pts.

Due on March 5, 2018.

For a connected graph G which is not a tree, we define the *girth* of G as the minimal length of a cycle in G. This is denoted by $g = g(G)$ and it is well-defined since connected graphs that are not trees do contain cycles. Moreover, $g \geq 3$.

Problem 1. [10pts] Adapt the work from class to prove the following

Theorem. *Let G be a connected graph which is not a tree. If G is planar, then*

$$e \leq \frac{g}{g-2}(v-2).$$

Problem 2. [3pts] Prove that $K^{3,3}$ is not planar.

Problem 3. [3pts] The torus $\mathcal{T}$ is the topological space obtained by identifying the top and bottom, as well as the left and right edges of the unit square $[0,1] \times [0,1]$ —think of the surface of a donut. Prove that $K^{3,3}$ can be embedded in $\mathcal{T}$. (We already worked out the case of planar graphs in a rigorous way, so, a clear drawing suffices for this problem.)

Problem 4. [4pts] Certain matrix M of size 100×100 has only 0's and 1's as entries. It is known that the entries of each row and column add up to 50. Prove that some of the 1's in M can be replaced by 0's in such a way that in the new matrix, each row and each column has exactly one non-zero entry.

Assignment 5

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* First, every edge of G is in the boundary of 1 or 2 faces (this follows from the injectivity of the embedding ψ). Therefore

$$2e \geq \sum_{A\in\mathcal{F}} \#\{\text{edges in bd}A\} \geq \sum_{A\in\mathcal{F}} \#\{\text{edges in bd}\overline{A}\}$$

(The summations are over the faces $\mathcal{F}$ of G.) Note that

$$\#\{\text{edges in bd}A\} \geq \#\{\text{edges in bd}\overline{A}\}$$

This is because, although $\overline{A}$ is *larger* than A, the boundary of $\overline{A}$ is *smaller* than the boundary of A. As we discussed in class, each bd$\overline{A}$ corresponds to a subgraph $H \preceq G$. We proved in class that H has an Euler circuit, which means that H is cyclic. Since H has a cycle, it has at least g edges (since the girth of G is g, and any subgraph H has a girth which is at least the girth of the graph G. This is because any graph embedding preserves cycles, and if there were a shorter cycle in H then this cycle would also appear in G). Therefore every bd$\overline{A}$ contains at least g edges:

$$\#\{\text{edges in bd}\overline{A}\} \geq g$$

Since the number of faces in a planar graph is given by the Euler's formula $v - e + f = 2$, the summation can be expressed as

$$2e \geq \sum_{A\in\mathcal{F}} g = (2 - v + e)g$$

$$2e \geq 2g - vg + eg$$

Rearranging terms and simplifying yields (as desired),

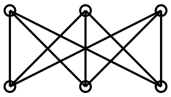
$$eg - 2e \leq vg - 2g$$

$$e(g-2) \leq g(v-2)$$

$$e \leq \frac{g}{g-2}(v-2)$$

□

Problem 2. *Solution.* This result follows immediately from the previous problem. Recall that $K^{3,3}$ is of the following form:



Observe that $K^{3,3}$ has $3(3) = 9$ edges. This graph has cycles, which are of length at least 3 by definition. Furthermore, a bipartite graph has no cycles of odd length (we proved this in class on 3/2), so the girth of $K^{3,3}$ is not 3. Let the vertex sets of $K^{3,3}$ be $\{a_1, a_2, a_3\}$ and $\{b_1, b_2, b_3\}$. We have a cycle

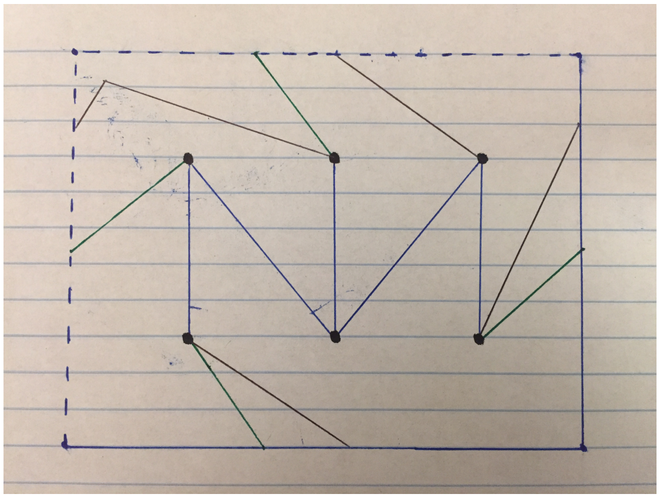
$$a_1 \to b_1 \to a_2 \to b_2 \to a_1$$

of length 4 (as every a is connected to every b). Therefore $g = 4$. Considering the inequality proved in the first problem yields

$$e = 9 \not\leq 8 = \frac{4}{4-2}(6-2) = \frac{g}{g-2}(v-2)$$

So therefore $K^{3,3}$ is not planar. □

Problem 3. *Solution.* I will show that $K^{3,3}$ is planar on a torus (which is the topological space obtained by identifying the top/bottom and left/right of a square. I can prove anything about a torus by proving the fact about this special type of 'glued' square). Consider the following diagram:



Observe that there are no edges between the vertices in the top row and no edges between the vertices in the bottom row, so the graph is bipartite. Further notice that each vertex in one row is adjacent to every vertex in the other row, so the graph is a complete bipartite graph. We already developed the theory of planar graphs formally, so this diagram (with polygonal paths/edges) suffices to demonstrate the planarity of $K^{3,3}$ on a torus. □

Problem 4. *Solution.* Let $M = (m_{ij})$. Consider the bipartite graph $G = (V, E)$ with vertex sets

$$V_1 = \{(1, i) : 1 \leq i \leq 100\}$$

$$V_2 = \{(2, j) : 1 \leq j \leq 100\}$$

Note that $V = V_1 \cup V_2$. Let V_1 represent the set of rows in the matrix M and V_2 represent the set of columns in the matrix M. Let the edge relation R_E be defined as

$$(\alpha, i) R_E (\beta, j) \iff \alpha \neq \beta \text{ and } m_{ij} = 1$$

G is indeed a bipartite graph, because R_E will never be true for a pair vertices in V_1 or a pair of vertices in V_2. Now I'll prove that G satisfies 'Hall's Condition':

Let $S \subseteq V_1$. Recall that $\Gamma(S)$ is defined

$$\Gamma(S) = \{(2, j) \in V_2 : \exists (1, i) \in S \text{ such that } (1, i) R_E (2, j)\}$$

I'll now demonstrate that $\#\Gamma(S) \geq \#S$. Either $\#S \leq 50$ or $\#S > 50$.

First suppose that $\#S \leq 50$. Since there exists at least one $(1, i) \in S$ (or else the inequality holds trivially) and by assumption each row has 50 entries equal to 1, this implies that $(1, i) R_E (2, j)$ for 50 distinct values of j. Therefore

$$\#\Gamma(S) \geq 50 \geq \#S$$

Now suppose that $\#S > 50$. Suppose, for a contradiction, that $\#\Gamma(S) < \#S$, or equivalently, that there exists the set

$$T = V_2 - \Gamma(S)$$

with $\#T > 100 - \#S$ (T is the set of vertices to which no vertex in S is connected). By definition of T, every $(2, j) \in T$ is not connected to any $(1, i) \in S$. Each $(2, j) \in V_2$ is connected to 50 distinct vertices in V_1 by assumption (this is the structure of the matrix and consequently R_E). Therefore, we know each $(2, j) \in T$ is connected to 50 distinct vertices in $V_1 - S$ (because each $(2, j)$ is not connected to any vertex in S). However, $\#S > 50$ by assumption, so there do not exist 50 distinct vertices in $V_1 - S$. Contradiction. Therefore $\#\Gamma(S) \geq \#S$, so Hall's Condition is met, and there exists a matching from V_1 (the rows of M) to V_2 (the columns of M).

Apply an identical argument (simply switching the labels V_1 and V_2) to conclude that there exists a matching from V_2 (the columns of M) to V_1 (the rows of M). Therefore, there exists a perfect matching from the columns of M to the rows of M. This means there exists some disjoint set of edges $E' \subset E$ such that for every $(1, i) \in V_1$ there is some $\{(1, i), (2, j)\} \in E'$, and for every $(2, j) \in V_2$ there is some $\{(1, i), (2, j)\} \in E'$. Consider the new matrix $M' = (m_{ij})$, defined by

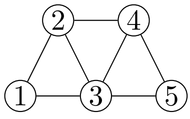
$$m'_{ij} = 1 \iff (1, i) R_{E'} (2, j)$$

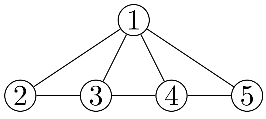
Since E' is a perfect matching, each $(1, i)$ and $(2, j)$ each appear exactly once in E', so therefore there is exactly one entry of 1 in each row and column of M' (and M' is generated by replacing 1s in M with 0s, since $E' \subset E$ by definition of a matching). □

Math 155R, Assignment 6. Total: 20 pts.

Due on March 26, 2018.

Problem 1. [6pts] Compute the chromatic polynomial $P(G,t)$ for the following graphs G:

(i) 

, (ii) 

.

Problem 2. [4pts] List all polynomials $F(t) \in \mathbb{Z}[t]$ of degree 4 that are the chromatic polynomial of some graph.

Problem 3. [2pts] For a graph G and a positive integer n, let $Q(G,n)$ be the number of colorings of G using exactly n colors, up to relabeling the colors. That is, $Q(G,n)$ is the number of vertex-surjective morphisms $\phi : G \to K^n$ counted up to automorphisms of K^n (in a sense, this is the "correct" number of n-colorings of G). Prove that for every positive integer n we have

$$P(G,n) = \sum_{j=1}^{n} j! \cdot \binom{n}{j} \cdot Q(G,j).$$

Problem 4. [8pts] Let $G = (V,E)$ be a graph. An *orientation* for G is a subset

$$D \subseteq \{(x,y) \in V^2 : x \neq y\}$$

with the property that it maps bijectively to E under the rule $(x,y) \mapsto \{x,y\}$. Intuitively, D is a choice of direction for each edge of G. We say that an orientation D for G *has a cycle* if there is some marked cycle $\phi : C^\ell \to G$ with the property that for each $j \in \mathbb{Z}/\ell\mathbb{Z}$ we have that $(\phi(j), \phi(j+1)) \in D$ (of course, if G has no cycles then in particular no orientation of G has a cycle). Prove that the number of orientations of G that do not have cycles is equal to $(-1)^v P(G,-1)$.

Remark. One can think of this last problem as an interpretation of "the number of colorings using -1 colors".

Assignment 6

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* To solve this problem, I'll simply count the number of morphisms from each graph to K^n. Observe that the following procedure works equally for both part (i) and (ii):

First consider vertex 1. There are n choices of vertices in K^n to which 1 could be mapped.
Now consider vertex 2. Since the 'color' of vertex 1 has now been fixed, there are only $(n-1)$ choices of vertices in K^n to which 2 could be mapped (since 1 and 2 are adjacent they must map to different vertices of K^n).
Now consider vertex 3. Since the color of vertices 1 and 2 has now been fixed, there are only $(n-2)$ choices of vertices in K^n to which 3 could be mapped.
Now consider vertex 4. Since the color of two vertices adjacent to 4 has now been fixed, there are only $(n-2)$ choices of vertices in K^n to which 4 could be mapped.
Now consider vertex 5. Since the color of two vertices adjacent to 5 has now been fixed, there are only $(n-2)$ choices of vertices in K^n to which 5 could be mapped.

Therefore there are n choices for 1, $(n-1)$ choices for 2, and $(n-2)$ choices for $3, 4, 5$. This yields

$$n(n-1)(n-2)^3$$

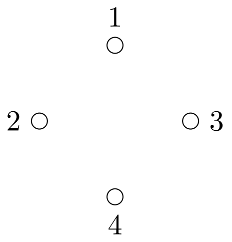
total morphisms, so $P(G,t)$ is the unique polynomial which interpolates the above expression, hence

$$P(G,t) = t(t-1)(t-2)^3$$

□

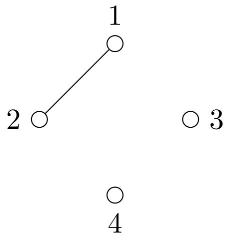
Problem 2. *Solution.* We proved in class that the degree of the chromatic polynomial is equal to the number of vertices. To find the possible chromatic polynomials of degree 4, it therefore suffices to determine the possible graphs of degree 4 and examine their chromatic polynomials. I will do this systematically, ordered by the number of edges in the graph.

1.



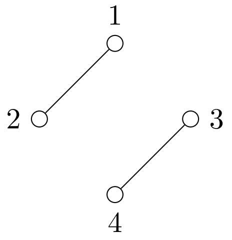
The chromatic polynomial of such a graph is t^4.

2.



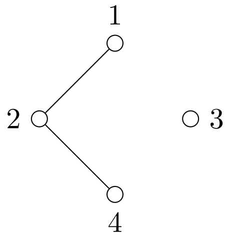
The chromatic polynomial of such a graph is $t^2(t)(t-1) = t^3(t-1)$.

3.



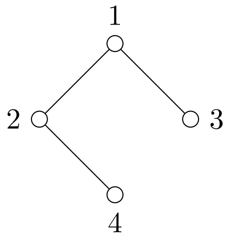
The chromatic polynomial of such a graph is $(t(t-1))^2 = t^2(t-1)^2$.

4.



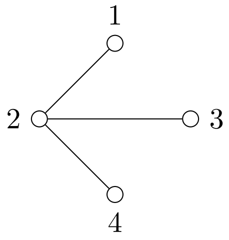
The chromatic polynomial of such a graph is $t(t)(t-1)^2 = t^2(t-1)^2$.

5.



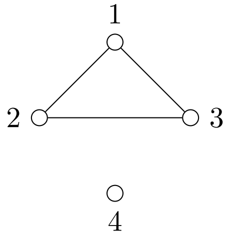
The chromatic polynomial of such a graph is $t(t-1)^3$.

6.



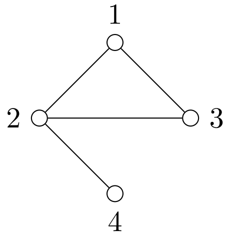
The chromatic polynomial of such a graph is $t(t-1)^3$.

7.



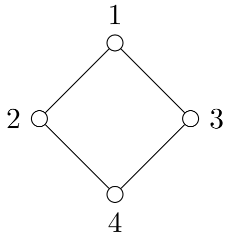
The chromatic polynomial of such a graph is $t(t)(t-1)(t-2) = t^2(t-1)(t-2)$.

8.



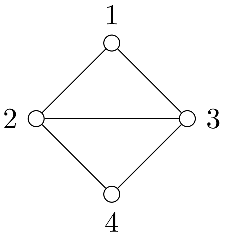
The chromatic polynomial of such a graph is $t^2(t-1)(t-2) - t(t-1)(t-2) = t(t-1)^2(t-2)$.

9.



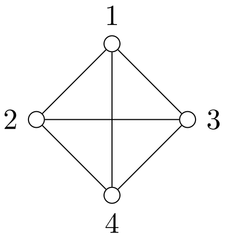
The chromatic polynomial of such a graph is $t(t-1)^3 - t(t-1)(t-2) = t(t-1)[(t-1)^2 - (t-2)] = t(t-1)(t^3 - 3t + 3)$.

10.



The chromatic polynomial of such a graph is $t(t-1)(t^3-3t+3)-t(t-1)^2 = t(t-1)(t-2)^2$.

11.



The chromatic polynomial of such a graph is $t(t-1)(t-2)(t-3)$.

Therefore, the polynomials of degree 4 which are the chromatic polynomials of some graph are

$$\begin{cases} t^4 \\ t^3(t-1) \\ t^2(t-1)^2 \\ t(t-1)^3 \\ t^2(t-1)(t-2) \\ t(t-1)^2(t-2) \\ t(t-1)(t^2-3t+3) \\ t(t-1)(t-2)^2 \\ t(t-1)(t-2)(t-3) \end{cases}$$

□

Problem 3. *Solution.* To count $P(G, K^n)$ (the number of morphisms $\phi : G \to K^n$), observe that for each morphism ϕ the image of ϕ is some subgraph of K^n. Observe that, for every ϕ, we have

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\theta"'] & K^n \\ K^j \arrow[ur, "\psi"'] & \end{tikzcd}$$

Where $\theta : G \to K^j$ is a morphism from G to K^j (the subgraph of K^n) and $\psi : K^j \to K^n$ places this subgraph in K^n.

Every morphism ϕ can be written as the composition $\psi \circ \theta$, where j is number of vertices in the image of ϕ (this j is the minimum number of vertices necessary for a particular morphism ϕ).

Since θ is a vertex surjective morphism from G to K^j, the value $Q(G,j)$ counts $\#\{\theta\}$ up to automorphism. There are $j!$ automorphisms of K^j, so therefore there are $j! \cdot Q(G,j)$ morphisms $\theta : G \to K^j$.

Now we must consider ψ. There are $\binom{n}{j}$ possible images of $\psi : K^j \to K^n$ (since we are choosing j vertices of K^n). Note that I am not counting twice morphisms that use the same vertices but in a different order. This is because the distinct morphisms generated by reordering/relabeling vertices is already counted in the argument about θ above, when I mentioned that there are $j!$ automorphisms of K^j.

Since there are $j! \cdot Q(G,j)$ choices for θ and $\binom{n}{j}$ choices for ψ, there are a total of $j! \cdot \binom{n}{j} \cdot Q(G,j)$ choices for some particular j. The j value for a morphism $\phi : G \to K^n$ satisfies $1 \leq j \leq n$, so therefore the total number of morphisms is given by

$$P(G,n) = \sum_{j=1}^{n} j! \cdot \binom{n}{j} \cdot Q(G,j)$$

□

Problem 4. *Solution.* I'll prove the claim by induction on e, the number of edges in G. Let v denote the number of vertices in G. Let the number of acyclic orientations for G be denoted $\mathcal{O}(G)$.

Base Case: Suppose $e = 0$. Then the only possible orientation is $D = \emptyset$, since $E = \emptyset$ and there must exist a bijection between D and E. This D is acyclic, so $\mathcal{O}(G)$. Furthermore, we know that $P(G,t) = t^v$ so $P(G,-1) = (-1)^v$. Therefore

$$(-1)^v P(G,-1) = (-1)^v(-1)^v = 1 = \mathcal{O}(G)$$

Inductive Case: Suppose $e \geq 1$. Then there exists an edge $\{x_0, y_0\}$ in G. I'll write $\mathcal{O}(G)$ in terms of $\mathcal{O}(G_{\text{del}})$ and $\mathcal{O}(G_{\text{con}})$, where $G_{\text{del}} = G - \{x_0, y_0\}$ and $G_{\text{con}} = G/\{x_0, y_0\}$ (the graphs obtained by deleting and contracting the edge $\{x_0, y_0\}$, respectively).

I first claim that every aylclic orientation D_{del} for G_{del} can be extended to at least one aylclic orientation for G. Let D_{del} be an acyclic orientation for G_{del}. Recall that the edge $\{x_0, y_0\}$ has been deleted from G to obtain G_{del}.

Suppose that there does not exist a path in D_{del} of the form

$$x_0 \to v_1 \to \ldots \to v_j \to y_0$$

(A path is considered to be in an orientation if every pair of vertices appears in the orientation in that order. For example $(x_0, v_1), (v_i, v_{i+1}), (v_j, y_0) \in D_{\text{del}}$.) Since there is no such path, define $D = D_{\text{del}} \cup \{(y_0, x_0)\}$. Observe that D is an orientation for G that is acyclic (because the existence of a cycle requires such a path to be present in G_{del}).

Now suppose that there does exist a minimal path in D_{del} of the form

$$x_0 \to v_1 \to \ldots \to v_j \to y_0$$

Then there cannot exist a path in D_{del} of the form

$$y_0 \to w_1 \to \ldots \to w_k \to x_0$$

If there existed both of these paths, then simply combining them

$$x_0 \to v_1 \to \ldots \to v_j \to y_0 \to w_1 \to \ldots \to w_k \to x_0$$

yields a cycle in D_{del}, contradicting the fact that this orientation is acyclic (note that this composition is in fact bijective on edges, so therefore it is a cycle. Since there is a bijection between D and E, every edge can only exist in one direction in D. So if there existed a duplicate edge (a, b), it would be in the same direction like this

$$x_0 \to \ldots \to v_i \to \ldots \to a \to b \to \ldots \to y_0$$

$$y_0 \to \ldots \to a \to b \to \ldots \to w_i \to \ldots \to x_0$$

If this were the case, it would still contradict the assumption that D_{del} is acyclic, since there exists the cycle

$$x_0 \to \ldots \to v_i \to \ldots \to a \to b \to \ldots \to w_i \to \ldots \to x_0$$

Either way results in a contradiction, so therefore there does not exist a path from y_0 to x_0 in D_{del}. Since there is no such path, define $D = D_{\text{del}} \cup \{(x_0, y_0)\}$. Observe that D is an orientation for G that is acyclic (because the existence of a cycle requires such a path to be present in G_{del}).

So every acyclic orientation for G_{del} results in at least one acyclic orientation for G (it is still possible that neither of these paths exist in which case each orientation for G_{del} results in two acyclic orientations for G).

I now claim that every acyclic orientation D_{con} for G_{con} can be extended to two acyclic orientations of G. Let D_{con} be an acyclic orientation of G_{con}. Every vertex v that is adjacent to either x_0 or y_0 is adjacent to the contracted vertex z_0. Look at the 'direction' of the edge connecting v to z_0 in D_{con}. Preserve the direction of this edge in the orientation D for G (the uncontracted graph). In other words, when uncontracting the orientation D_{con}, if there were two edges from v to x_0 and from v to y_0 in G, then preserve the direction of the edge from v to z_0 in G_{con} when constructing D.

Once we uncontract D_{con} to D, we have an orientation D that is still missing an edge from x_0 to y_0. There are two possible orientations of this last edge, which yield the acyclic orientations

$$D_1 = D \cup \{(x_0, y_0)\}$$

$$D_2 = D \cup \{(y_0, x_0)\}$$

for G. Note that both of these orientations for G are still acyclic. Since D_{con} is acyclic, simply uncontracting and adding the edge $\{x_0, y_0\}$ regardless of orientation cannot result in a cycle (as the way we inserted the collapsed edges from x_0 and y_0 ensured that there is no path from x_0 to y_0, since all of the collapsed edges from these vertices are going into them or coming out of them. There is no path from x_0 to y_0 not involving the collapsed edges either, since this would yield a cycle in D_{con} for the contracted (for which $x_0 = y_0$) graph, contradicting the fact that D_{con} is acyclic). Therefore each acyclic orientation for G_{con} can be extended to two acyclic orientations for G.

At this point, we know that $\mathcal{O}(G_{\text{del}})$ is the number of acyclic orientations which can be extended to at least one acyclic orientation of G, and $\mathcal{O}(G_{\text{con}})$ is the number of acyclic orientations which can be extended to two acyclic orientations of G. Note that $\mathcal{O}(G_{\text{del}})$ includes the extension of the acyclic orientations of G_{con} to G_{del} in the way I described. Therefore we only need to add $\mathcal{O}(G_{\text{con}})$ once in order to capture the fact that these orientations result in two acyclic orientations for G. Finally, we have

$$\mathcal{O}(G) = \mathcal{O}(G_{\text{del}}) + \mathcal{O}(G_{\text{con}})$$

Since G_{del} and G_{con} have fewer edges than G, apply the induction hypothesis for

$$\begin{aligned}\mathcal{O}(G) = \mathcal{O}(G_{\text{del}}) + \mathcal{O}(G_{\text{con}}) &= (-1)^v P(G_{\text{del}}) + (-1)^{v-1} P(G_{\text{con}}, -1)\\ &= (-1)^v (P(G_{\text{del}}, -1) - P(G_{\text{con}}, -1)) = (-1)^v P(G, -1)\end{aligned}$$

Since we know that $P(G, -1) = P(G_{\text{del}}, -1) - P(G_{\text{con}}, -1)$ by the properties of the chromatic polynomial. This completes the inductive step. □

Math 155R, Assignment 7. Total: 20 pts.
Due on Apr 02, 2018.

Problem 1. [2pts] Compute the Ramsey number $R(3, 3)$.

Problem 2. [5pts] Prove the following claim from class:
Let $2 \leq k \leq v$ and let $a_1, ..., a_k \geq 0$ be integers with $a_1 + ... + a_k = v$. Then $e(K_{a_1,...,a_k}) \leq e(T(v, k))$ and equality holds if and only if $K_{a_1,...,a_k} \simeq T(v, k)$.

Problem 3. [5pts] Let G be a graph. Prove that there is a bipartite sub-graph $H \leq G$ satisfying $e(H) \geq e(G)/2$.

Problem 4. [8pts] Prove that there is a constant $c > 0$ such that the following holds:
If G is a graph with no cycles of length 4, then $e(G) \leq c \cdot v(G)^{3/2}$.

Assignment 7

Math 155r (Combinatorics)

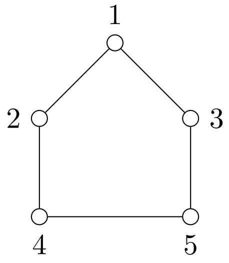
Beckham Myers

Problem 1. *Solution.* I claim that $R(3,3) = 6$. To show this, I will demonstrate:

(i) There exists a graph with 5 vertices which does not contain a clique of size 3 or an independent vertex set of size 3 ($R(3,3) > 5$).

(ii) Every graph with six vertices has either a clique of size 3 or an independent vertex set of size 3 or both ($R(3,3) \leq 6$).

To show (i), consider the graph $G = C^5$ (the cycle graph with 5 vertices). By inspection, it is clear that the following graph has no cliques or independent vertex sets of size 3:



Therefore $R(3,3) > 5$.

To show (ii), let G be a graph with 6 vertices. Further let v be a vertex in G. Then either $\deg v \leq 2$ or $\deg v \geq 3$.

First suppose that $\deg v \geq 3$. Then v at at least 3 adjacent vertices; let 3 be these be labeled x, y, z. Suppose that one of the following edges exists in G: $\{x,y\}, \{y,z\}, \{x,z\}$. Then those two vertices which are adjacent, along with v, form a 3-clique in G. If none of these three edges are present in G, then the set $\{x,y,z\}$ is independent in G. Either way, there exists a 3-clique or an independent set of vertices of size 3.

Now suppose that $\deg v \leq 2$. Consider the graph G^*, the edge-wise complement of G. The degree of v in G^* is given by $\deg v \geq 5 - 2 = 3$ (since there are 5 other vertices in G besides v). Since $\deg v \geq 3$ in G^*, the above argument implies that G^* has either a 3-clique or an independent set of vertices of size 3. Therefore G has either a 3-clique or an independent set of vertices of size 3 (since any clique in G^* becomes independent in G and any independent set in G^* becomes a clique in G).

(i) implies that $R(3,3) > 5$, and (ii) implies that $R(3,3) \leq 6$. Therefore $R(3,3) = 6$, as desired. □

Problem 2. *Solution.* We proved in class that the number of edges in a complete multi-partite graph $K_{a_1,\ldots,a_k}$ with v vertices and $\sum a_i = v$ is given by

$$e(K_{a_1,\ldots,a_k}) = \frac{1}{2}\sum_{i\neq j} a_i a_j = v^2 - \sum_i^k a_i^2$$

Further recall $T(v,k) \simeq K_{b_1,\ldots,b_k}$ where $\sum b_i = v$ and

$$\left\lfloor \frac{v}{k} \right\rfloor \leq b_1 \leq \ldots \leq b_k \leq \left\lceil \frac{v}{k} \right\rceil$$

We want to show that

$$e(K_{a_1,\ldots,a_k}) = v^2 - \sum_i^k a^2 \leq v^2 - \sum_i^k b^2 = e(T(v,k))$$

$$\sum_i^k b_i^2 \leq \sum_i^k a_i^2$$

It therefore suffices to show that the function

$$\phi(x_1,\ldots,x_k) = \sum_i^k x_i^2$$

when constrained to integer tuples $(x_1,\ldots,x_k)$ which satisfy $\sum x_i = v$ has a minimum on values of x_i which correspond to the b_i above.

Let $x = (x_1,\ldots,x_k)$ be such an integer tuple with $\sum x_i = v$. Without loss of generality, order the coordinates in increasing order:

$$x_1 \leq x_2 \leq \ldots \leq x_k$$

First suppose $x_k - x_1 \leq 1$. Then the condition that $\sum x_i = v$ and that the difference between the greatest and least terms is at most 1 uniquely define the Turan values $b_1,\ldots,b_k$ (as we discussed in class), so we have

$$K_{x_1,\ldots,x_k} \simeq T(v,k)$$

Now suppose that $x_k - x_1 > 1$. I'll show that for these values of the $x = (x_1,\ldots,x_k)$, there exist another set of values $x' = (x'_1,\ldots,x'_k)$ such that $\phi(x') < \phi(x)$ (in which case x is not the minimum of ϕ).

Let $x'_1 = x_1 + 1$ and $x'_k = x_k - 1$. Observe that we still have

$$\sum_i^k x'_i = (x_1+1) + \Big[\sum_{1<i<k} x_i\Big] + (x_k - 1) = \sum_i^k x_i = v$$

Furthermore, note that

$$\phi(x_i') = \sum_i^k x_i'^2 = (x_1+1)^2 + (x_k-1)^2 + \sum_{1<i<k} x_i^2$$

To show that $\phi(x') < \phi(x)$ it therefore suffices to demonstrate

$$(x_1+1)^2 + (x_k-1)^2 + \sum_{1<i<k} x_i^2 < \sum_i^k x_i^2$$

$$(x_1+1)^2 + (x_k-1)^2 < x_1^2 + x_k^2$$

$$x_1^2 + 2x_1 + 1 + x_k^2 - 2x_k + 1 < x_1^2 + x_k^2$$

$$2x_1 - 2x_k + 2 < 0$$

$$x_k - x_1 > 1$$

But this was exactly what we assumed in this case (see above), so we indeed have $\phi(x') < \phi(x)$. Since for every

$$x = (x_1, \dots, x_k) \not\simeq (b_1, \dots, b_k) = b$$

there exists an x' for which $\phi(x') < \phi(x)$, the minimum of ϕ cannot occur on some x which is not isomorphic to b. Therefore $e(T(v,k)) = e(K_{b_1,\dots,b_k}) \leq e(K_{a_1,\dots,a_k})$, and equality holds when $K_{a_1,\dots,a_k} \simeq T(v,k)$.

NB: Spoke with Elliot about this problem □

Problem 3. *Solution.* I will prove the claim by induction on v, the number of vertices in the graph G.

Base Case: Suppose $v = 1$. Then G is simply the graph with exactly one vertex and no edges. There exists a morphism $\phi : G \to K^2$, so therefore G is bipartite and there exists a bipartite subgraph $H \leq G$ (where $H = G$) such that

$$e(H) \geq e(G)/2$$

Inductive Case: Suppose $v \geq 2$. Let x_0 be some vertex in G. Define $G' = G - \{x_0\}$ (the graph obtained from deleting the vertex x_0 and all edges containing x_0 from G). Apply the inductive hypothese to conclude that there exists some bipartite subgraph $H' \leq G'$ such that

$$e(H') \geq e(G')/2$$

Write H' as the disjoint union of two vertex sets with no edges present within each set (definition of bipartite graphs):

$$H' = H_1' \cup H_2'$$

Now consider the vertices in H_i' which are connected to the vertex x_0 in the graph G, which I will denote $\Gamma_G(x_0) \cap H_i'$. Without loss of generality (the proof proceeds identically in the other case) suppose that

$$\#(\Gamma_G(x_0) \cap H_1') \geq \#(\Gamma_G(x_0) \cap H_2')$$

(In other words, x_0 is connected in G to a greater than or equal to number of vertices in H_1' than it is connected to in H_2'.) Then define $H_1 = H_1'$ and $H_2 = H_2' \cup \{x_0\}$. I am placing the vertex x_0 in the second vertex set because this preserves more of the edges connecting to x_0 from the original graph. Note that H_1 and H_2 are disjoint, and let H be the graph obtained by deleting the edges between vertices in H_i and retaining edges from G that contain a vertex from H_1 and a vertex from H_2. This procedure results in a bipartite graph.

Further observe that, since I am adding the vertex x_0 to the subgraph $H \leq G$ in the base case and inductive step, all the vertices of G are present in H (only edges are deleted). Therefore, taking into consideration that the H_i are disjoint,

$$\Gamma_G(x_0) = (\Gamma_G(x_0) \cap H_1) \cup (\Gamma_G(x_0) \cap H_2)$$

$$\#(\Gamma_G(x_0)) = \#(\Gamma_G(x_0) \cap H_1) + \#(\Gamma_G(x_0) \cap H_2)$$

The assumption

$$\#(\Gamma_G(x_0) \cap H_1') \geq \#(\Gamma_G(x_0) \cap H_2')$$

therefore implies that

$$\#(\Gamma_H(x_0)) = \#(\Gamma_G(x_0) \cap H_1) \geq \frac{1}{2}[\#(\Gamma_G(x_0))]$$

Since $e(G) = e(G') + \#(\Gamma_G(x_0))$, we therefore have

$$e(H) = e(H') + \#(\Gamma_G(x_0) \cap H_1) \geq \frac{1}{2}e(G') + \frac{1}{2}[\#(\Gamma_G(x_0))] = \frac{1}{2}e(G)$$

So $e(H) \geq \frac{1}{2}e(G)$ as desired, and the inductive step has been proven. □

Problem 4. *Solution.* Let G be a graph with no cycles of length 4. Further let the number of vertices in G be denoted n. I will employ a counting argument to show the bound on $e(G)$. First note that a cycle of length 4 is injective on vertices (this is not necessarily true for cycles in general, but for cycles of length 4 it is required). It is easy to see why this is the case: two or three vertices don't suffice because our definition of graph forbids repeated edges.

I will now proceed to count the number of paths of length 2 (since any such path could be 'glued' to another such path to yield a cycle of length 4 by adding edges between the first and last vertices). Such a path consists of three vertices x, y, z with the edges $\{x, y\}, \{y, z\}$ present in G. Therefore, for some vertex y, the number of 2-paths with y as the center vertex is given by the number of possible choices of two adjacent vertices, or equivalently $\binom{\deg y}{2}$. Summing over all of the vertices in G yields the total number of such paths (since every path has some vertex as its center vertex):

$$\#\{\text{paths of length 2}\} = \sum_{v \in G} \binom{\deg v}{2}$$

Now further observe that every vertex pair x, z can have only one additional vertex that is adjacent to both of them (since if y_1 and y_2 were both adjacent to both x and z then $x \to y_1 \to z \to y_2 \to x$ is a 4-cycle in G). This means that each vertex pair x, z can only be the endpoints of a maximum of one path of length 2. So the possible distinct vertex pairs is a bound on the number of paths of length 2 in G (as every path has two distinct vertices as its endpoints). Therefore we know

$$\#\{\text{paths of length 2}\} \leq \binom{n}{2}$$

Combining the above two counting arguments yields the inequality

$$\sum_{v \in G} \binom{\deg v}{2} \leq \binom{n}{2}$$

$$\sum_{v \in G} \frac{\deg v(\deg v - 1)}{2} \leq \frac{n(n-1)}{2}$$

$$\sum_{v \in G} (\deg v)^2 - \deg v \leq n(n-1)$$

The Cauchy-Schwarz inequality states that $\langle u, v \rangle^2 \leq |u| \cdot |v|$. Define the vectors u, v by

$$u = (\deg v_1, \deg v_2, \ldots, \deg v_n)$$

$$v = (1, 1, \ldots, 1)$$

Then the inequality implies

$$\big(\sum_{v \in G} \deg v\big)^2 \leq \sum_{v \in G} (\deg v)^2 \cdot \sum_{1}^{n} 1^2$$

Therefore we know

$$\frac{1}{n}\big(\sum_{v \in G} \deg v\big)^2 \leq \sum_{v \in G} (\deg v)^2$$

So therefore combining the two above inequalities yields

$$\frac{1}{n}\big(\sum_{v \in G} \deg v\big)^2 - \sum_{v \in G} \deg v \leq n(n-1)$$

$$\frac{1}{n}\big(\sum_{v \in G} \deg v\big)^2 - \sum_{v \in G} \deg v - (n^2 - n) \leq 0$$

Solving the quadratic $\frac{1}{n}x^2 + x - (n^2 - n) = 0$ for x yields

$$x = \frac{1 \pm \sqrt{1 + 4(n^2 - n)(\frac{1}{n})}}{\frac{2}{n}}$$

It's clear that as x becomes large the quadratic will be positive, so the values of x between the zeroes of the polynomial when replaced for $\sum \deg v$ will satisfy the inequality above. Therefore we have

$$\sum_{v \in G} \deg v \leq x = \frac{n + n\sqrt{1 + 4(n-1)}}{2} = \frac{1}{2}(n + n\sqrt{4n - 3})$$

Since $\sum \deg v = 2e(G)$, this yields

$$e(G) \leq \frac{1}{4}n(1 + \sqrt{4n - 3})$$

It's clear that this upper bound is asymptotically $\mathcal{O}(n^{3/2})$. Therefore we can choose some c, (such as $c = 1$) to satisfy

$$\frac{1}{4}n(1 + \sqrt{4n - 3}) \leq n^{\frac{3}{2}}$$

Therefore for all graphs G without cycles of length 4 we have

$$e(G) \leq c \cdot v(G)^{\frac{3}{2}}$$

NB: Proof idea from Clapham 1989. □

Math 155R, Assignment 8. Total: 20 pts.

Due on Apr 09, 2018.

Problem 1. [9pts] Let $v \geq r \geq 2$. Consider G a random sub-graph of K^v, where each of the $\binom{v}{2}$ edges of K^v might be used with probability $1/2$ (independently).

(i) Take a fixed set S of r vertices of K^v. What is the probability that S is a clique of G? What is the probability that S is an independent set of G?

(ii) Show that the probability that G contains an r-clique or an r-independent set, is at most

$$2 \cdot \binom{v}{r} \cdot 2^{-\binom{r}{2}}.$$

(iii) Conclude that the Ramsey number $R(r, r)$ grows exponentially on r. (Hint: if v is not too big, then the previous probability is < 1, and one should correctly interpret the meaning of that.)

Problem 2. [5pts] Compute the optimal value of $W(2, 3)$.

Problem 3. [6pts] Using the van der Waerden theorem, prove the following:

Let $a_1 < a_2 < ...$ be an infinite sequence of positive integers. Suppose that for some B we have that $a_{j+1} \leq a_j + B$ for each $j \geq 1$. Then the set $X = \{a_j : j \geq 1\}$ contains arbitrarily long arithmetic progressions.

Assignment 8

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* (i) If S is a clique of G, then every possible edge between the r vertices in S is connected by an edge. There are $\binom{r}{2}$ possible edges between r vertices. Since each edge independently has a probability of $\frac{1}{2}$ of appearing, the probability of all $\binom{r}{2}$ edges appearing is

$$(\frac{1}{2})(\frac{1}{2})\dots(\frac{1}{2}) = (\frac{1}{2})^{\binom{r}{2}} = 2^{-\binom{r}{2}}$$

Similarly, if S is an independent set of G, then every possible edge between the r vertices in S does *not* appear. Since each of the $\binom{r}{}$ edges independently has a probability of $\frac{1}{2}$ of not appearing, the probability of all $\binom{r}{2}$ edges being absent is

$$(\frac{1}{2})(\frac{1}{2})\dots(\frac{1}{2}) = (\frac{1}{2})^{\binom{r}{2}} = 2^{-\binom{r}{2}}$$

(ii) Let the sample space U be the set of all possible subgraphs $G \leq K^v$ (where G has v vertices). Let $X_S \subset U$ be the subset of these graphs for which the vertex set S is a clique or an independent set in G. Note that the probability of the vertex set S being a clique or an independent set in G is then given by

$$\frac{\#X_S}{\#U}$$

Let $S_1, \dots, S_\ell$ be all the possible sets of r vertices, namely $\#S_i = r$. Since there are v vertices, $\ell = \binom{v}{r}$. Now I'll define the set X as the set of all possible subgraphs for which there exists *some* vertex set S of size r that is a clique or independent vertex set:

$$X = X_{S_1} \cup \dots \cup X_{S_\ell} = \bigcup_{i}^{\ell=\binom{v}{r}} X_{S_i}$$

(We have the inclusion $\subseteq$ because any subgraph in X has a clique/independent set, so it must have this clique or independent set on some S. Therefore this subgraph is in some X_{S_i}. We have the inclusion $\supseteq$ because any subgraph which has a clique/independent set on a particular S_i has a clique/independent set in general.)

We seek to find the probability of randomly generating a subgraph $G \in X$, which is given by $\frac{\#X}{\#U}$. By the definition of union, we know that

$$\#X = \#\Big(\bigcup_{i}^{\ell=\binom{v}{r}} X_{S_i}\Big) \leq \sum_{i}^{\ell=\binom{v}{r}} \#X_{S_i}$$

Equality holds when the X_{S_i} are disjoint (which, as a side remark, will not happen in this problem), and the right hand side will overcount any subgraphs that appear in multiple X_{S_i} sets. Therefore we have

$$\frac{\#X}{\#U} \leq \sum_{i}^{\ell=\binom{v}{r}} \frac{\#X_{S_i}}{\#U}$$

Now we must determine $\frac{\#X_{S_i}}{\#U}$, the probability of a particular vertex set S of size r being a clique or an independent vertex set.

I proved in (i) that the probability of S being a clique is $2^{-\binom{r}{2}}$. Therefore, the probability that S is not a clique is $1 - 2^{-\binom{r}{2}}$. Similarly, the probability of S not being an independent set is $1 - 2^{-\binom{r}{2}}$. Therefore the probability of being neither a clique nor an independent set is $(1 - 2^{-\binom{r}{2}})^2$. This means that the probability of being either a clique or an independent set is

$$\frac{\#X_S}{\#U} = 1 - (1 - 2^{-\binom{r}{2}})^2 = 1 - (1 - 2 \cdot 2^{-\binom{r}{2}} + (2^{-\binom{r}{2}})^2) = 2 \cdot 2^{-\binom{r}{2}} - 2^{-2\binom{r}{2}}$$

However, $2^{-2\binom{r}{2}}$ is always positive so we have

$$\frac{\#X_S}{\#U} = 2 \cdot 2^{-\binom{r}{2}} - 2^{-2\binom{r}{2}} \leq 2 \cdot 2^{-\binom{r}{2}}$$

Applying this to the inequality at the top of the page yields

$$\frac{\#X}{\#U} \leq \sum_{i}^{\ell=\binom{v}{r}} \frac{\#X_{S_i}}{\#U} \leq \sum_{i}^{\ell=\binom{v}{r}} 2 \cdot 2^{-\binom{r}{2}} = \binom{v}{r} \cdot (2 \cdot 2^{-\binom{r}{2}})$$

So the probability that G contains an r-clique or an r-independent set is at most

$$2 \cdot \binom{v}{r} \cdot 2^{-\binom{r}{2}}$$

(iii) If $v = R(r,r)$, then the probability of choosing a subgraph $G \leq K^{R(r,r)}$ that contains a r-clique or an r-independent set is 1. Therefore, by part (ii), we have

$$1 \leq 2 \cdot \binom{v}{r} \cdot 2^{-\binom{r}{2}}$$

(If the probability calculated in (ii) were less than one, then the true probability of G being a subgraph with an r-clique or an r-independent set is less than one as well. If this were the case, then there would exist subgraphs for which there were no r-cliques or r-independent sets, contradicting the definition of a Ramsey number.) Let's see how increasing r by 1 places new demands on v:

$$1 \leq 2 \cdot \binom{v}{r+1} \cdot 2^{-\binom{r+1}{2}} = 2 \cdot \frac{v!}{(r+1)!(v-r-1)!} \cdot 2^{-\frac{r(r+1)}{2}}$$

$$1 \leq 2 \cdot \frac{(v-r)}{r+1} \cdot \frac{v!}{r!(v-r)!} \cdot 2^{-\frac{r^2+r-2r+2r}{2}} = 2 \cdot \frac{(v-r)}{r+1} \cdot \binom{v}{r} \cdot 2^{-\frac{r(r-1)}{2}-r}$$

$$1 \leq 2 \cdot \binom{v}{r} \cdot 2^{-\binom{r}{2}} \cdot \left[\frac{(v-r)}{r+1} \cdot 2^{-r}\right] = 2 \cdot \binom{v}{r} \cdot 2^{-\binom{r}{2}} \cdot \left[(\frac{v}{r+1} - \frac{r}{r+1}) \cdot 2^{-r}\right]$$

As $r \to \infty$ the term $\frac{r}{r+1}$ becomes 1, so we have

$$1 \leq 2 \cdot \binom{v}{r} \cdot 2^{-\binom{r}{2}} \left[(\frac{v}{r+1} - 1) \cdot 2^{-r} \right]$$

Since we know that the terms outside of the brackets are already greater than or equal to 1, it is necessary to show formulate a lower bound on v such that the terms inside the brackets do not cause the entire expression to become less than 1. The binomial coefficient has a polynomial rate of growth with respect to v (specifically an r degree polynomial). This is clear from the definition of the binomial coefficient:

$$\binom{v}{r} = \frac{v!}{r!(v-r)!} = \frac{v(v-1)(v-2)\dots(v-r+1)}{r!}$$

The other terms 2 and $2^{-\binom{r}{2}}$ are constant with respect to v. Therefore, when moving from $R(r,r)$ to $R(r+1,r+1)$, the term $(\frac{v}{r+1} - 1) \cdot 2^{-r} \simeq \frac{v}{r+1} \cdot 2^{-r}$ cannot become too small (meaning it cannot become small so fast such that $\frac{1}{\frac{v}{r+1} \cdot 2^{-r}}$ is more than polynomial growth). This implies that $\frac{v}{2^r}$ doesn't decrease exponenentially, which means that $v = R(r+1,r+1)$ does increase exponenetially. □

Problem 2. *Solution.* I claim that $W(2,3) = 9$. To show this, I will demonstrate:

(i) There exists a 2-coloring of $[1,8]$ with no monochromatic arithmetic progression of length 3 ($W(2,3) > 8$).

(ii) Every 2-coloring of [1,9] has a monochromatic arithmetic progression of length 3 ($W(2,3) \leq 9$).

To show (i), consider the coloring $\phi : [1,8] \to [1,2]$ given by

$$\phi(i) = (1,1,2,2,1,1,2,2)_i$$

(My notation is such that i indexes into the 8-tuple, which describes all the values that ϕ takes for each $i \in [1,8]$. For example $\phi(1) = 1$ and $\phi(3) = 2$.) It is evident by inspection that there is no monochromatic arithmetic progression in $[1,8]$ for this particular ϕ, so therefore $W(2,3) > 8$.

To show (ii), let $\phi : [1,9] \to [1,2]$ be a coloring given by

$$\phi(i) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9)_i$$

First note that at least 5 numbers must have the same color (since x_i can only be two values and there are 9 such x_i). Without loss of generality, suppose that 1 appears at least 5 times in this tuple (the proof proceeds identically if it is 2 that appears at least 5 times).

I'll show that there exists a monochromatic progression when 1 appears exactly 5 times (and certainly there will be such a progression when 1 appears more than 5 times). It suffices to consider *all* such 9-tuples and confirm that there exists a monochromatic arithmetic progression of length 3 for each one. To do this, I wrote a computer program and printed out the results on the next page (the indices to the right of each tuple correspond to the indices of the desired progression).

Therefore, every 2-coloring of [1,9] has a monochromatic arithmetic of length 3. (i) implies that $W(2,3) > 8$ and (ii) implies that $W(2,3) \leq 9$. Therefore $W(2,3) = 9$ as desired.

$$\left\{\begin{array}{ll}
(1,1,1,1,1,2,2,2,2) & 1\ 2\ 3 \\
(1,1,1,1,2,1,2,2,2) & 1\ 2\ 3 \\
(1,1,1,1,2,2,1,2,2) & 1\ 2\ 3 \\
(1,1,1,1,2,2,2,1,2) & 1\ 2\ 3 \\
(1,1,1,1,2,2,2,2,1) & 1\ 2\ 3 \\
(1,1,1,2,1,1,2,2,2) & 1\ 2\ 3 \\
(1,1,1,2,1,2,1,2,2) & 1\ 2\ 3 \\
(1,1,1,2,1,2,2,1,2) & 1\ 2\ 3 \\
(1,1,1,2,1,2,2,2,1) & 1\ 2\ 3 \\
(1,1,1,2,2,1,1,2,2) & 1\ 2\ 3 \\
(1,1,1,2,2,1,2,1,2) & 1\ 2\ 3 \\
(1,1,1,2,2,1,2,2,1) & 1\ 2\ 3 \\
(1,1,1,2,2,2,1,1,2) & 1\ 2\ 3 \\
(1,1,1,2,2,2,1,2,1) & 1\ 2\ 3 \\
(1,1,1,2,2,2,2,1,1) & 1\ 2\ 3 \\
(1,1,2,1,1,1,2,2,2) & 4\ 5\ 6 \\
(1,1,2,1,1,2,1,2,2) & 1\ 4\ 7 \\
(1,1,2,1,1,2,2,1,2) & 2\ 5\ 8 \\
(1,1,2,1,1,2,2,2,1) & 6\ 7\ 8 \\
(1,1,2,1,2,1,1,2,2) & 2\ 4\ 6 \\
(1,1,2,1,2,1,2,1,2) & 2\ 4\ 6 \\
(1,1,2,1,2,1,2,2,1) & 2\ 4\ 6 \\
(1,1,2,1,2,2,1,1,2) & 1\ 4\ 7 \\
(1,1,2,1,2,2,1,2,1) & 1\ 4\ 7 \\
(1,1,2,1,2,2,2,1,1) & 5\ 6\ 7 \\
(1,1,2,2,1,1,1,2,2) & 5\ 6\ 7 \\
(1,1,2,2,1,1,2,1,2) & 2\ 5\ 8 \\
(1,1,2,2,1,1,2,2,1) & 1\ 5\ 9 \\
(1,1,2,2,1,2,1,1,2) & 2\ 5\ 8 \\
(1,1,2,2,1,2,1,2,1) & 4\ 6\ 8 \\
(1,1,2,2,1,2,2,1,1) & 2\ 5\ 8 \\
(1,1,2,2,2,1,1,1,2) & 3\ 4\ 5 \\
(1,1,2,2,2,1,1,2,1) & 3\ 4\ 5 \\
(1,1,2,2,2,1,2,1,1) & 3\ 4\ 5 \\
(1,1,2,2,2,2,1,1,1) & 3\ 4\ 5 \\
(1,2,1,1,1,1,2,2,2) & 3\ 4\ 5 \\
(1,2,1,1,1,2,1,2,2) & 3\ 4\ 5 \\
(1,2,1,1,1,2,2,1,2) & 3\ 4\ 5 \\
(1,2,1,1,1,2,2,2,1) & 3\ 4\ 5 \\
(1,2,1,1,2,1,1,2,2) & 1\ 4\ 7 \\
(1,2,1,1,2,1,2,1,2) & 4\ 6\ 8 \\
(1,2,1,1,2,1,2,2,1) & 2\ 5\ 8
\end{array}\right.$$

$$\left\{\begin{array}{ll}
(1,2,1,1,2,2,1,1,2) & 1\ 4\ 7 \\
(1,2,1,1,2,2,1,2,1) & 1\ 4\ 7 \\
(1,2,1,1,2,2,2,1,1) & 5\ 6\ 7 \\
(1,2,1,2,1,1,1,2,2) & 5\ 6\ 7 \\
(1,2,1,2,1,1,2,1,2) & 1\ 3\ 5 \\
(1,2,1,2,1,1,2,2,1) & 1\ 3\ 5 \\
(1,2,1,2,1,2,1,1,2) & 1\ 3\ 5 \\
(1,2,1,2,1,2,1,2,1) & 1\ 3\ 5 \\
(1,2,1,2,1,2,2,1,1) & 1\ 3\ 5 \\
(1,2,1,2,2,1,1,1,2) & 6\ 7\ 8 \\
(1,2,1,2,2,1,1,2,1) & 2\ 5\ 8 \\
(1,2,1,2,2,1,2,1,1) & 3\ 6\ 9 \\
(1,2,1,2,2,2,1,1,1) & 4\ 5\ 6 \\
(1,2,2,1,1,1,1,2,2) & 4\ 5\ 6 \\
(1,2,2,1,1,1,2,1,2) & 4\ 5\ 6 \\
(1,2,2,1,1,1,2,2,1) & 4\ 5\ 6 \\
(1,2,2,1,1,2,1,1,2) & 1\ 4\ 7 \\
(1,2,2,1,1,2,1,2,1) & 5\ 7\ 9 \\
(1,2,2,1,1,2,2,1,1) & 1\ 5\ 9 \\
(1,2,2,1,2,1,1,1,2) & 6\ 7\ 8 \\
(1,2,2,1,2,1,1,2,1) & 1\ 4\ 7 \\
(1,2,2,1,2,1,2,1,1) & 3\ 5\ 7 \\
(1,2,2,1,2,2,1,1,1) & 7\ 8\ 9 \\
(1,2,2,2,1,1,1,1,2) & 2\ 3\ 4 \\
(1,2,2,2,1,1,1,2,1) & 2\ 3\ 4 \\
(1,2,2,2,1,1,2,1,1) & 2\ 3\ 4 \\
(1,2,2,2,1,2,1,1,1) & 2\ 3\ 4 \\
(1,2,2,2,2,1,1,1,1) & 2\ 3\ 4 \\
(2,1,1,1,1,1,2,2,2) & 2\ 3\ 4 \\
(2,1,1,1,1,2,1,2,2) & 2\ 3\ 4 \\
(2,1,1,1,1,2,2,1,2) & 2\ 3\ 4 \\
(2,1,1,1,1,2,2,2,1) & 2\ 3\ 4 \\
(2,1,1,1,2,1,1,2,2) & 2\ 3\ 4 \\
(2,1,1,1,2,1,2,1,2) & 2\ 3\ 4 \\
(2,1,1,1,2,1,2,2,1) & 2\ 3\ 4 \\
(2,1,1,1,2,2,1,1,2) & 2\ 3\ 4 \\
(2,1,1,1,2,2,1,2,1) & 2\ 3\ 4 \\
(2,1,1,1,2,2,2,1,1) & 2\ 3\ 4 \\
(2,1,1,2,1,1,1,2,2) & 5\ 6\ 7 \\
(2,1,1,2,1,1,2,1,2) & 1\ 4\ 7 \\
(2,1,1,2,1,1,2,2,1) & 1\ 4\ 7 \\
(2,1,1,2,1,2,1,1,2) & 3\ 5\ 7
\end{array}\right.$$

$$\left\{\begin{array}{ll}
(2,1,1,2,1,2,1,2,1) & 3\ 5\ 7 \\
(2,1,1,2,1,2,2,1,1) & 1\ 4\ 7 \\
(2,1,1,2,2,1,1,1,2) & 6\ 7\ 8 \\
(2,1,1,2,2,1,1,2,1) & 3\ 6\ 9 \\
(2,1,1,2,2,1,2,1,1) & 1\ 4\ 7 \\
(2,1,1,2,2,2,1,1,1) & 4\ 5\ 6 \\
(2,1,2,1,1,1,1,2,2) & 4\ 5\ 6 \\
(2,1,2,1,1,1,2,1,2) & 4\ 5\ 6 \\
(2,1,2,1,1,1,2,2,1) & 4\ 5\ 6 \\
(2,1,2,1,1,2,1,1,2) & 2\ 5\ 8 \\
(2,1,2,1,1,2,1,2,1) & 5\ 7\ 9 \\
(2,1,2,1,1,2,2,1,1) & 2\ 5\ 8 \\
(2,1,2,1,2,1,1,1,2) & 6\ 7\ 8 \\
(2,1,2,1,2,1,1,2,1) & 1\ 3\ 5 \\
(2,1,2,1,2,1,2,1,1) & 1\ 3\ 5 \\
(2,1,2,1,2,2,1,1,1) & 7\ 8\ 9 \\
(2,1,2,2,1,1,1,1,2) & 5\ 6\ 7 \\
(2,1,2,2,1,1,1,2,1) & 5\ 6\ 7 \\
(2,1,2,2,1,1,2,1,1) & 1\ 4\ 7 \\
(2,1,2,2,1,2,1,1,1) & 7\ 8\ 9 \\
(2,1,2,2,2,1,1,1,1) & 3\ 4\ 5 \\
(2,2,1,1,1,1,1,2,2) & 3\ 4\ 5 \\
(2,2,1,1,1,1,2,1,2) & 3\ 4\ 5 \\
(2,2,1,1,1,1,2,2,1) & 3\ 4\ 5 \\
(2,2,1,1,1,2,1,1,2) & 3\ 4\ 5 \\
(2,2,1,1,1,2,1,2,1) & 3\ 4\ 5 \\
(2,2,1,1,1,2,2,1,1) & 3\ 4\ 5 \\
(2,2,1,1,2,1,1,1,2) & 6\ 7\ 8 \\
(2,2,1,1,2,1,1,2,1) & 2\ 5\ 8 \\
(2,2,1,1,2,1,2,1,1) & 4\ 6\ 8 \\
(2,2,1,1,2,2,1,1,1) & 7\ 8\ 9 \\
(2,2,1,2,1,1,1,1,2) & 5\ 6\ 7 \\
(2,2,1,2,1,1,1,2,1) & 5\ 6\ 7 \\
(2,2,1,2,1,1,2,1,1) & 1\ 4\ 7 \\
(2,2,1,2,1,2,1,1,1) & 7\ 8\ 9 \\
(2,2,1,2,2,1,1,1,1) & 6\ 7\ 8 \\
(2,2,2,1,1,1,1,1,2) & 1\ 2\ 3 \\
(2,2,2,1,1,1,1,2,1) & 1\ 2\ 3 \\
(2,2,2,1,1,1,2,1,1) & 1\ 2\ 3 \\
(2,2,2,1,1,2,1,1,1) & 1\ 2\ 3 \\
(2,2,2,1,2,1,1,1,1) & 1\ 2\ 3 \\
(2,2,2,2,1,1,1,1,1) & 1\ 2\ 3
\end{array}\right.$$

□

Problem 3. *Solution.* Define the set

$$X' := X - a_1 = \{a_j - a_1 : j \geq 1\}$$

X' contains the values in X 'shifted' so that the sequence of integers begins at 0. Suppose that we are looking for an arithmetic sequence of length k. Van der Waerden's theorem implies that there exists a number $N \geq W(B,k)$ (where B is the bound on $a_{j+1} - a_j$ for all $j \geq 1$) such that for all

$$\phi : [N] \to [B]$$

there exists an arithmetic sequence in $[N]$ of length k on which ϕ is constant. Consider the following such ϕ defined by

$$\phi(x) = x - a'_\ell$$

where $a'_\ell \in X'$ is the greatest member of X' less than or equal to x. Since the difference between consecutive a' terms is less than or equal to B, ϕ will indeed assign a unique value to each x that is in $[B]$. Since ϕ is defined from $[N]$ where $N \geq W(B,k)$, van der Waerden's theorem implies that there exists an arithmetic sequence

$$\{x_1, x_2, \ldots, x_k\} \subset [N]$$

such that $\phi(x_1) = \phi(x_2) = \ldots = \phi(x_k)$. By definition of ϕ, this implies that

$$x_1 - a'_{\ell_1} = x_2 - a'_{\ell_2} = \ldots = x_k - a'_{\ell_k}$$

$$a'_{\ell_1} - x_1 = a'_{\ell_2} - x_2 = \ldots = a'_{\ell_k} - x_k$$

where each a'_{ℓ_i} is the greatest member of X' less than or equal to x_i. Furthermore, since the x_i terms are an arithmetic sequence we know

$$x_k = x_{k-1} + r = x_{k-2} + 2r = \ldots = x_1 + (k-1)r$$

Adding this equation to

$$a'_{\ell_k} - x_k = a'_{\ell_{k-1}} - x_{k-1} = \ldots = a'_{\ell_1} - x_1$$

(which comes from above) yields

$$a'_{\ell_k} - x_k + x_k = a'_{\ell_{k-1}} - x_{k-1} + x_{k-1} + r = \ldots = a'_{\ell_1} - x_1 + x_1 + (k-1)r$$

$$a'_{\ell_k} = a'_{\ell_{k-1}} + r = \ldots = a'_{\ell_1} + (k-1)r$$

which implies that $\{a'_{\ell_1}, a'_{\ell_2}, \ldots, a'_{\ell_k}\}$ is an arithmetic sequence of length k. Therefore

$$\{a'_{\ell_1} + a_1, a'_{\ell_2} + a_1, \ldots, a'_{\ell_k} + a_1\} = \{a_{\ell_1}, a_{\ell_2}, \ldots, a_{\ell_k}\} \subset X$$

is an arithmetic sequence of length k as well. □

Math 155R, Assignment 9. Total: 20 pts.
Due on Apr 16, 2018.

Problem 1. [5pts] Let $(K, |-|)$ be a field with a non-archimedean absolute value. Suppose that for a suitable positive real constant θ we have $\theta \cdot \log |K^\times| = \mathbb{Z}$. Furthermore, suppose that K is complete for this absolute value. Let $A = \mathcal{O}_K$. Let $F(x) \in A[x]$ be a polynomial, let $\alpha \in A$ and assume that

- $|F(\alpha)| < 1$, and
- $|F'(\alpha)| = 1$.

Prove that there is $\beta \in A$ such that $|\beta - \alpha| < 1$ and $F(\beta) = 0$.

Problem 2. [4pts] Suppose that k is a field of characteristic different from 2. Prove that $1 + t$ is a square in $k[[t]]$.

Problem 3. [6pts] For $n \geq 0$ define A_n as the number of ways in which n left parentheses and n right parenthesis can be correctly written. For instance, $A_0 = 1$. A more interesting example: If $n = 2$ we only have the following possible arrangements:

$$(()) \quad \text{and} \quad ()()$$

while something like)(() is not permitted. Thus, $A_2 = 2$.

(i) Prove that for all $n \geq 0$ we have $A_{n+1} = \sum_{j=0}^{n} A_j A_{n-j}$.

(ii) Using the method of generating series, give a simple closed formula for A_n.

Problem 4. [5pts] Let k be a field. Prove that the power series

$$f = t + t^2 + t^6 + t^{24} + ... = \sum_{n \geq 1} t^{n!} \in k[[t]]$$

is transcendental over $k(t)$ (that is, it is not algebraic).

Assignment 9

Math 155r (Combinatorics)

Beckham Myers

Problem 1. *Solution.* Since K is complete with respect to $|\cdot|$, it suffices to demonstrate that there exists a Cauchy sequence which converges to β, with $F(\beta) = 0$. I will do this by applying Newton's Method to generate guesses which are successively closer and converge to the root β. Let $\alpha_0 = \alpha$. By assumption $|F(\alpha_0)| < 1$ and $|F'(\alpha_0)| = 1$. Define $\alpha_1 = \alpha_0 - \frac{F(\alpha_0)}{F'(\alpha_0)}$.

First observe that $\alpha_1 \in A$. This follows from the strong triangle inequality:

$$|\alpha_1| = |\alpha_0 - \frac{F(\alpha_0)}{F'(\alpha_0)}| \leq \max\{|\alpha_0|, |\frac{F(\alpha_0)}{F'(\alpha_0}|\} = \max\{|a_0|, \frac{|F(\alpha_0)|}{|F'(\alpha_0)|}\} < 1$$

Since $|\alpha_0| < 1$ by assumption, and $|F(\alpha_0)| < 1$ while $|F'(\alpha_0)| = 1$. The proof involves iterating this process to generate a sequence of $\alpha_0, \alpha_1, \ldots$ such that $|F(\alpha_{i+1})| < |F(\alpha_i)|$. Since $|\cdot|$ is non-archimedean, this implies that the sequence is Cauchy, in which case it converges in K. □

Problem 2. *Solution.* For an element $f = a_0 + a_1 t + a_2 t^2 + \ldots \in k[[t]]$, recall that if we write

$$f^2 = (a_0 + a_1 t + a_2 t^2 + \ldots)^2 = b_0 + b_1 t + b_2 t^2 + \ldots$$

The values for each b_n are given by

$$b_n = \sum_{k+\ell=n} a_k a_\ell$$

This is by definition of multiplication in $k[[t]]$. To show that $1 + t$ is a square in $k[[t]]$, we want to show there exists some f for which the first equation above for f^2 yields $b_0 = 1$, $b_1 = 1$, and $b_j = 0$ for all other $j > 1$. The second equation above yields

$$b_0 = 1 = \sum_{k+\ell=0} a_k a_\ell = a_0^2$$

This implies that $a_0 = 1$. Now consider

$$b_1 = 1 = \sum_{k+\ell=1} a_k a_\ell = a_0 a_1 + a_1 a_0 = 2a_1$$

So we have $1 = 2a_1$. Since k is a field that does not have characteristic 2, we know that the element $1 + 1 = 2 \neq 0$. So 2 is invertible and we have $a_1 = 2^{-1}$. In general, for some $n > 1$, observe that

$$b_n = 0 = \sum_{k+\ell=n} a_k a_\ell = 2a_n a_0 + \sum_{k+\ell=n, k>0, \ell>0} a_k a_\ell = 2a_n + \sum_{0<k<n} a_k a_{n-k}$$

So therefore the coefficient a_n is given by

$$a_n = -2^{-1} \sum_{0<k<n} a_k a_{n-k}$$

We can always calculate this summation, so therefore the function

$$f = a_0 + a_1 t + a_t^2 + \ldots = 1 + 2^{-1} t + \sum_{n \geq 2} \Bigg(-2^{-1} \cdot \sum_{0<k<n} a_k a_{n-k} \Bigg) t^n$$

is a square root of $1+t$, so $1+t$ is indeed a square in $k[[t]]$. □

Problem 3. *Solution.* (a) I'll prove the claim by induction. Note that we have $A_0 = A_1 = 1$. For $n+1 = 1$, we have

$$A_1 = \sum_0^0 A_j A_{n-j} = A_0^2 = 1$$

so the base case is proven.

Now, I'll demonstrate that the claim holds when $n+1 > 1$. For any proper arrangement of $n+1$ pairs parentheses, we must start with a left parenthesis. This parenthesis must have a matching right parenthesis somewhere in the arrangement. Now note that there could be a total of j possible pairs of parentheses between the initial left parenthesis and its matching right parenthesis, where $0 \leq j \leq n$.

For each j such that $0 \leq j \leq n$, note that there are j pairs between the initial left parenthesis and its matching right parenthesis, and $n-j$ pairs after the matching right parenthesis. So for each j, there are A_j ways of arranging the first group of nested parentheses, and A_{n-j} ways of arranging the second group of nested parentheses (these must be arranged independently. When arranging parentheses, once the matching right parenthesis for the first left parenthesis is closed, all of the pairs inside of it must be closed as well). Therefore there are a total of $A_j A_{n-j}$ ways of arranging the parentheses for a given j. So summing over j yields

$$A_{n+1} = \sum_{j=0}^{n} A_j A_{n-j}$$

(b) Define the power series $f = A_0 + A_1 t + A_2 t^2 + \ldots \in k[[t]]$. Observe that

$$\begin{aligned}
f &= A_0 + A_1 t + A_2 t^2 + \ldots \\
f^2 &= A_0^2 + (A_0 A_1 + A_1 A_0) t + (A_0 A_2 + A_1 A_1 + A_2 A_0) t^2 + \ldots \\
f^2 &= A_0^2 + A_2 t + A_3 t^2 + \ldots \\
f^2 &= 1 + A_2 t + A_3 t^2 + \ldots \\
t f^2 &= A_1 t + A_2 t^2 + A_3 t^3 + \ldots \\
t f^2 &= f - 1
\end{aligned}$$

Which gives the quadratic $tf^2 - f + 1 = 0$. Applying the quadratic formula to solve for f yields

$$f = \frac{1 \pm \sqrt{1-4t}}{2t}$$

Recall that $A_0 = 1$, so therefore $\lim_{t\to 0} f(t) = A_0 = 1$. Note that

$$\lim_{t\to 0} \frac{1+\sqrt{1-4t}}{2t} = \pm\infty$$

$$\lim_{t\to 0} \frac{1-\sqrt{1-4t}}{2t} = \lim_{t\to 0} \frac{\left(\frac{2}{\sqrt{1-4t}}\right)}{2} = \frac{2}{2} = 1$$

The second line is by L'Hopital's rule. This implies that

$$f = \frac{1-\sqrt{1-4t}}{2t}$$

I proved in Problem 2 that $1+u$ is a square in $k[[t]]$. The Binomial Series (see Wikipedia) states that we have

$$(1+u)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k$$

where $\binom{\alpha}{k}$ is defined

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$$

Therefore, applying this to $\sqrt{1-4x}$ yields

$$\sqrt{1-4t} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} \cdot (-4t)^k = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} (-1)^k \cdot 4^k \cdot t^k$$

The definition of $\binom{\frac{1}{2}}{k}$ gives

$$\begin{aligned}
\binom{\frac{1}{2}}{k} &= \frac{1}{k!} \cdot (\frac{1}{2}) \cdot (-\frac{1}{2}) \cdot (-\frac{3}{2}) \cdots (-\frac{2k-3}{2}) \\
&= \frac{(-1)^{k-1}}{k! \cdot 2^k} \cdot 1 \cdot 1 \cdot 3 \cdot \ldots \cdot (2k-3) \\
&= \frac{(-1)^{k-1}}{k! \cdot 2^k} \cdot \frac{1}{2 \cdot 4 \cdot \ldots \cdot (2k-2) \cdot 2n} \cdot \frac{1}{(2k-1)} \cdot (2k)! \\
&= \frac{(-1)^{k-1}}{k! \cdot 2^k} \cdot \frac{1}{2^k(1 \cdot 2 \cdot \ldots \cdot n)} \cdot \frac{1}{(2k-1)} \cdot (2k)! \\
&= \frac{(-1)^{k-1} \cdot (2k)!}{k! \cdot 4^k \cdot k! \cdot (2k-1)} = \frac{(-1)^{k-1}}{4^k \cdot (2k-1)} \cdot \binom{2k}{k}
\end{aligned}$$

Replacing this term in the expansion for $\sqrt{1-4t}$ yields

$$\sqrt{1-4t} = \sum_{k=0}^{\infty} \frac{(-1)^{2k-1}}{2k-1} \cdot \binom{2k}{k} \cdot t^k = -\sum_{k=0}^{\infty} \frac{1}{2k-1} \cdot \binom{2k}{k} \cdot t^k$$

Therefore

$$\begin{aligned}
f &= \frac{1}{2t}(1-\sqrt{1-4t}) \\
&= \frac{1}{2t}\left[1 + \sum_{k=0}^{\infty} \frac{1}{2k-1} \cdot \binom{2k}{k} \cdot t^k\right]
\end{aligned}$$

Therefore A_n, which is the coefficient of the monomial t^n by construction of f, is

$$A_n = \frac{1}{2} \cdot \frac{1}{2(n+1)-1} \cdot \binom{2(n+1)}{n+1} = \frac{1}{2} \cdot \frac{1}{2n+1} \cdot \frac{(2n+2)(2n+1)}{(n+1)^2} \cdot \binom{2n}{n} = \frac{1}{n+1} \cdot \binom{2n}{n}$$

So therefore

$$A_n = \frac{1}{n+1} \cdot \binom{2n}{n}$$

□

Problem 4. *Solution.* Suppose, for contradiction, that the power series

$$f = t + t^2 + t^6 + \ldots = \sum_{n=0}^{\infty} t^{n!} \in k[[t]]$$

were not transcentendental. Then it is algebraic, and there exists a polynomial $P \in k(t)[X]$ such that $P(f) = 0$. Let $d = \deg_X P$ be minimal (meaning P is a vanishing polynomial with the lowest degree). This implies that $1, f, f^2, \ldots, f^d$ are linearly dependent. Consider the linear combination

$$0 = \sum_{i=0}^{d} \alpha_i f^i$$

Each α_i is a rational function in $k(t)$. Multiply the entire equation by all of the denominators of the α_i functions to yield

$$0 = \sum_{i=0}^{d} \alpha_i' f^i$$

where each α_i' is now a polynomial in $k[t]$. Since d is minimal, this implies $\alpha_d' \neq 0$. Now I'll examine the $\alpha_d' + df^d$ term closer. Define

$$p = \max\{\deg_t(\alpha_i) : 1 \leq i \leq d\}$$

(p is the maximum degree of t in any of the α_i' coefficient functions). Now let $n > d+p$ (remember d is the degree of the polynomial P in the X variable). I'll show that the monomial $t^{dn!}$ does not vanish. Recall that in the expansion of

$$f^d = (t + t^2 + t^6 + \ldots)^d$$

the coefficient of $t^{dn!}$, which I will call λ, is given by the equation

$$\lambda = \sum_{a_1! + a_2! + \ldots + a_d! = dn!} 1$$

(The condition on the summation corresponds to the monomials $t^{a_1!}, t^{a_2!}, \ldots, t^{a_d!}$ being multiplied in the expansion of f^d). I claim that the only term in this summation is when $a_1 = \ldots = a_d = n$. Clearly when $a_1 = \ldots = a_d = n$ the condition on the summation is satisfied.

Let $a_1, \ldots, a_d$ be such that $a_1! + a_2! + \ldots + a_d! = dn!$. Further suppose for contradiction that there existed an j such that $a_j \neq n$. Then for some k we have $a_k > n$. (If $a_j > n$ then $k = j$. If

$a_j < n$ then the summation condition guarantees that another a_k value must be larger than n to make up for the smaller a_j term). But observe that

$$a_1! + \ldots + a_k! + \ldots + a_j! + \ldots + a_d! \geq a_k! \geq (n+1)! = (n+1)n! > dn!$$

Since by construction $n > d + p$. This is a contradiction, since we assumed $a_1! + \ldots + a_d! = dn!$. Therefore the only set of a_i values that work are when $a_1 = \ldots = a_d = n$. So we have $\lambda = 1$. This means that the term $t^{dn!}$ in the expansion of f^d is monic (it does not vanish). The f^d term is multiplied by α'_d. Since $\alpha'_d \neq 0$ (as the degree of the polynomial is minimal), there exists some term t^m, not necessarily monic, in $\alpha'_d f^d$ where $dn! \leq m \leq dn! + p$. (This is because the degree of this term could vary from exactly $dn!$, when it is multiplied by a constant in α'_d, to $dn! + p$, when α'_d contains a t^p term, and anywhere in between).

Now I'll examine the terms $\alpha'_i f^i$ for when $i < d$. Since the term t^m appears in $\alpha'_d f^d$ with $dn! \leq m \leq dn! + p$, I will show that there are no terms in any $\alpha'_i f^i$ with degree in this rangle. Since α' has a maximum degree p, it suffices to demonstrate that there are no terms in f^i with degree x where $dn! - p \leq x \leq dn!$.

Fix some $\ell < d$. A term in the expansion of f^ℓ with degree x must satisfy the following equation:

$$a_1! + a_2! + \ldots + a_\ell! = x$$

(This condition corresponds to the monomials $t^{a_1!}, \ldots, t^{a_\ell!}$ being multiplied in the expansion of f^ℓ.) Either the maximum a_i value is less than or equal to n or it is greater than n. First suppose that the maximum a_i value is less than or equal to n. Then we have

$$a_1! + \ldots + a_\ell! \leq n! + \ldots + n! = \ell n! \leq dn! - n!$$

The last inequality comes from the fact that $\ell < d$ by assumption. Furthermore, since we set $n > d + p$, this implies $n! > p$ as well. Using this in the above inquality yields

$$x = a_1! + \ldots + a_\ell! \leq dn! - n! < dn! - p$$

$$x < dn! - p$$

So therefore when the maximum a_i value is less than or equal to n we know that the degree of the corresponding term in the expansion of f^ℓ must be less than $dn! - p$. Now suppose that the maximum a_i value is greater than n. This implies

$$x = a_1! + \ldots + a_\ell! \geq (n+1)! = (n+1)n! > dn!$$

Since $n > d + p$ by construction. So therefore when the maximum a_i value is greater than n we know that the degree of the corresponding term in the expansion of f^ℓ must be greater than $dn!$.

Either way, when we multiply the expansion f^ℓ by α'_ℓ, since $\deg \alpha'_i \leq p$, the above bounds on the degree x of a term in the expansion of f^ℓ imply that any term in $\alpha'_i f^\ell$ satisfies either $x < dn!$ or $x > dn! + p$. However, there exists a term t^m with a nonzero coefficient which satisfies $dn! \leq m \leq dn! + p$ that comes from the expansion of $\alpha_d f^d$. Therefore this term does not vanish. This contradicts the assumption that $P(f) = 0$. Therefore f cannot be algebraic, so f is transcendental over $k(t)$. □