CS201A:Mathematics for Computer Science - I
Assignment 3

Anuj Singhal
Roll No. 210166

October 2022

1 [2+2+4 points]

1.1 Recall the complete graph K_n. How many subgraphs does K_n have?

We know, number of edges in a complete graph on n vertices = $\binom{n}{2} = \frac{n(n-1)}{2}$
Now every subset of $E(K_n)$ defines the edge set of a unique subgraph of K_n
So the number of subgraphs of $K_n = \#$ subsets of $E(K_n)$
i.e. number of subgraphs of $K_n = 2^{|E(K_n)|} = 2^{\frac{n(n-1)}{2}}$

1.2 When will K_n have an Eulerian circuit?

We use a theorem derived in class that states:
A graph has a Eulerian circuit iff every vertex has even degree
Now, since in a complete graph all vertices have equal degree, each equal to $(n-1)$, we can immediately conclude from above theorem that:
A complete graph K_n has an Eulerian circuit iff $n-1$ is even i.e n is odd.
$\implies$ **K_n will have an Eulerian circuit iff n is odd.**

1.3 What are the eigenvalues of the adjacency matrix of K_n?

We can write the adjacency matrix A of K_n as:

$$K_n = J_n - I_n$$

where J_n is $n \times n$ matrix of all 1's and I_n is identity matrix, i.e.

$$K_n = \begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \vdots & & \ddots & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix}$$

For calculating the eigenvalues of K_n, we find the roots of equation

$$|K_n - \lambda I_n| = 0$$

$$\implies \begin{vmatrix} -\lambda & 1 & \dots & 1 \\ 1 & -\lambda & \dots & 1 \\ \vdots & & \ddots & 1 \\ 1 & \dots & 1 & -\lambda \end{vmatrix} = 0$$

Now we replace the 1st row by sum of all rows:

$$\begin{vmatrix} -\lambda & 1 & \dots & 1 \\ 1 & -\lambda & \dots & 1 \\ \vdots & & \ddots & 1 \\ 1 & \dots & 1 & -\lambda \end{vmatrix} = \begin{vmatrix} (n-1)-\lambda & (n-1)-\lambda & \dots & (n-1)-\lambda \\ 1 & -\lambda & \dots & 1 \\ \vdots & & \ddots & 1 \\ 1 & \dots & 1 & -\lambda \end{vmatrix}$$

$$i.e.\ ((n-1)-\lambda) \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & -\lambda & \dots & 1 \\ \vdots & & \ddots & 1 \\ 1 & \dots & 1 & -\lambda \end{vmatrix} = 0$$

Now subtracting 1st column from all other columns, we get:

$$i.e.\ ((n-1)-\lambda) \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & -1-\lambda & 0 & \dots & 0 \\ \vdots & 0 & -1-\lambda & 0 & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ 1 & 0 & \dots & 0 & -1-\lambda \end{vmatrix} = 0$$

$$\implies ((n-1)-\lambda)(-1-\lambda)^{n-1} = 0$$

i.e $\lambda = n-1$ *or* $\lambda = -1$ ($n-1$ times repeated root)

2 [5+4 points]

Let G be a graph, A be its adjacency matrix, and d be its maximum degree.

2.1 Show that the maximum eigenvalue of A is atmost d.

Let d be the maximum degree of all vertices and λ be an eigenvalue of the adjacency matrix $A = [a_{ij}]$.
Also let b be an eigenvector corresponding to eigenvalue λ such that $|b| = 1$,
$\implies Ab = \lambda b$

$$\implies \sum_{j=1}^{n} a_{ij} b_j = \lambda b_i$$

$$\implies |\sum_{j=1}^{n} a_{ij} b_j| = |\lambda b_i|$$

$$\implies \sum_{j=1}^{n} |a_{ij} b_j| \geq |\lambda b_i|$$

Thus,

$$\sum_{j=1}^{n} |a_{ij}| \geq |\lambda|$$

Hence,

$$d \geq |\lambda|$$

$$d \geq \lambda$$

So, the maximum eigenvalue can be atmost d.
hence proved.

2.2 Show that the minimum eigenvalue of A is atleast $-d$.

Using the exactly same result that we have obtained from part 1

$$d \geq |\lambda|$$

It immediately follows that

$$-d \leq \lambda$$

So, the minimum eigenvalue is atleast -d.
hence proved.

3 [5 points]

Show that the number of walks of length m between vertex i and vertex j is the $(i, j) - th$ entry of A^m

We will try to apply induction to prove that #walks of length m between vertex i and $j = (i, j) - th$ entry of A^m
First, base case is for m = 1 can be proved by the definition of adjacency matrix itself.
Now for the induction step, consider that the theorem holds for $m - 1$ i.e.
Consider any pair (i, j) then every walk of length m from i to j can be represented as a walk of length 1 from i to one of its adjacent vertex say v and a walk of length $m - 1$ from v to j.
So, if we define $\phi(i, j, m)$ to denote the number of walks from any vertex i to j of length m, then we can formally write

$$\phi(i, j, m) = \sum_{v=1}^{n} \phi(i, v, 1) \times \phi(v, j, m - 1)$$

Now, $\phi(i, v, 1)$ is basically the number of edges from vertex i to v which is the $(i, v) - th$ entry of A from the definition of adjacency matrix. i,e $A_{i,v}$
Also, from the induction step, we can assume for all v,

$$\phi(v, j, m - 1) = A_{v,j}^{m-1}$$

$$\implies \phi(i, j, m) = \sum_{v=1}^{n} \phi(i, v, 1) \times \phi(v, j, m - 1) = \sum_{v=1}^{n} A_{i,v} A_{v,j}^{m-1}$$

Which by definition of matrix multiplication is:

$$\implies \phi(i,j,m) = \sum_{v=1}^{n} A_{i,v}A_{v,j}^{m-1} = (A \times A^{m-1})_{i,j} = A_{i,j}^{m}$$

Hence we have proved inductively that the number of walks of length m from i to j is equal to the $(i,j)-th$ entry of A^m Hence proved.

4 [12 points]

Define graph product of G_1 and G_2, on vertex set $V_1 \times V_2$, as the graph $G_1 \hat{\otimes} G_2$ as follows:
$((u,i),(v,j))$ is an edge in $G_1 \hat{\otimes} G_2$ if,
$(u = v$ and $(i,j) \in E(G_2))$ or $((u,v) \in E(G_1)$ and $i = j)$.
Show that $\chi(G) \leq t$ iff $\alpha(G \hat{\otimes} K_t) = |V(G)|$.
(Note: $\chi(\cdot)$ is the chromatic number and $\alpha(\cdot)$ is the stability number.)

5 [2+5 points]

5.1 What is the chromatic number of a bipartite graph?

Consider a bipartite graph $G(X \bigsqcup Y, E)$
Our claim is that we can always have a valid coloring with 2 different colors.
Proof: We color the vertices from set X with color c_1 and from set Y with color c_2 then by the property of bipartite graph, all the edges are between a vertex from X and a vertex from Y i.e. between vertices of different colors c_1 and c_2.
Hence, any bipartite graph can be colored with 2 colors.
Now, if the graph has zero edges, then the graph can also be colored with only 1 color. In which case the chromatic number is 1.
Hence proved that the chromatic number of a bipartite graph is $\chi(G) \leq 2$

5.2 Show that a regular bipartite graph has a perfect matching.

Consider a bipartite graph $G(X \bigsqcup Y, E)$ which is d-regular
Then each vertex has degree d.
We know that the count of edges in the graph will be the count of edges from to X to Y.
Now the number of edges going out from $X = d|X|$ Similarly the number of edges entering $Y = d|Y|$

$$\implies d|X| = d|Y| \implies |X| = |Y|$$

Now since $|X| = |Y|$, any complete matching will be a perfect matching.
Let us assume the opposite that there does not exist a complete matching, then for a subset $S \subseteq X$, by Hall's marriage theorem (using converse of it)

$$|S| > N(|S|)$$

where $N(|S|)$ denotes the neighbourhood of S
Also, number of edges arising from $S = d|S|$ (regular bipartite graph)
Consider a function $\phi(v)$ such that $\phi(v) = \#$number of edges from a vertex v to set S.
So the number of edges arising from S can be written in terms of number of edges coming to S from its neighbourhood, i.e.

$$d|S| = \sum_{i=1}^{|N(S)|} \phi(v_i)$$

Consider $\phi(v_o)$ to be the maximum of $\phi(v)\ \forall\ v \in\ N(S)$, then

$$d|S| \leq |N(S)|\phi(v_o)$$

By our assumption, $|S| > N(|S|)$

$$\implies \phi(v_o) > d$$

This is a contradiction as the maximum no. of edges from any vertex to S has to be upper bounded by its degree, d.
Hence our assumption was wrong, so by contradiction,

$$|S| < |N(S)|\ \forall\ S \subseteq X$$

Hence, by Hall's marriage theorem, there exist a complete matching, which will be a perfect matching because we earlier proved that $|X| = |Y|$
Hence proved.

6 [4+4 points]

Consider a quadratic equation $X^2 + aX + b = 0 \ mod \ p$, where p is a prime, and $a, b \ \in Z$. Formulate a condition on $a, \ b, \ p$ that tells us whether the equation has zero, one or two solutions.
Can there be three, or more, solutions?

7 [5+6 points]

Let $n \in N$. Prove that, for every composite $n > 4$, $(n-1)! \ = 0 \ mod \ n$.

Case 1: n is a prime power. Here we assume that n is a power a prime number say p. i.e.

$$n = p^\alpha \ for \ \alpha > 1 \ and \ prime \ p$$

In this case, we further consider 2 cases
when $\alpha = 2$, we can have 2 integers p and $2p$ and since $n > 4$, these 2 integers will be strictly less than n, so they will be present in the product of $(n-1)!$ and their product is $2n$ so we say that $n|(n-1)!$
Otherwise if $\alpha > 2$ then we can take 2 distinct integers p and $p^{\alpha-1}$ such that both of them have to be less than n so they will be present in $(n-1)!$ and hence again $p^\alpha|(n-1)! \implies n|(n-1)!$
Hence proved.
Case 2: n is not a prime power. By Fundamental Theorem of Arithmetic, we can represent n in its prime factorisation.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \ ; \ k > 1$$

Here we can simply take the set of integers $\{p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}\}$
Since each of these terms are distinct and every term is present in the product $(n-)!$ so $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}|(n-1)! \implies n|(n-1)!$
Hence proved.

More interestingly, show that for any $n > 1$,
n is prime iff $(n-1)! \ = -1 \ mod \ n$.
(This is known as Wilson's primality criterion.)

We have already proved one part of the required equivalent statement, that is p is not prime, then $(p-1)! \ \neq -1 \ mod \ n$. Now we just need to prove the remaining part that if p is prime then $(p-1)! \ = -1 \ mod \ p$

Clearly, if $p = 2 \ or \ 3$ the congruence is easily verified. Thus we may assume that $p \geq 5$.
Suppose that $1 \leq a \leq p-1$. Then $(a,p) = 1$ so there will exist a unique inverse (a^{-1}) of a mod p.
So, all the integers from 1 to $p-1$ and their inverses exist in the product $(n-1)!$.
However, there are some x such that $x = x^{-1}$, which will not be cancelled in the product.
For them we need to prove another lemma, that:
If p is prime then $x^2 \equiv 1 \ (mod \ p)$ iff $x \equiv \pm 1 \ (mod \ p)$
Proof: We can rearrange the equation as:

$$x^2 \equiv 1 \ (mod \ p) \iff (x-1)(x+1) \equiv 0 \ (mod \ p) \iff p|(x-1) \ or \ p|(x+1)$$

$$\implies x \equiv 1 \ (mod \ p) \ or \ x \equiv -1 \ (mod \ p)$$

Hence the lemma is proved.
Now we use this lemma to claim that only 1 and $p-1$ are the cases where $x = x^{-1}$, so we handle them separately and write the result only for all $2 \leq x \leq p-2$

$$\implies (p-1)! \equiv (1)(1)(p-1) \ (mod \ p) \equiv -1 \ (mod \ p)$$

Hence proved.

Acknowledgements

1. Class notes.

2. An Introduction to The Theory of Numbers by Ivan Niven