Graphs, Modular Arithmetic, Bijections, RSA 2

Computer Science Mentors 70

February 6 to 10, 2017

1 Graph Theory

1.1 Introduction

1. Let $G = (V, E)$ be an undirected graph. Match the term with the definition.

Walk	Cycle	Tour	Path

________________Walk that starts and ends at the same node
________________Sequence of edges.
________________Sequences of edges with possibly repeated vertex or edge.
________________Sequence of edges that starts and ends on the same vertex and does not repeat vertices (except the first and last)

2. What is a tournament?

3. What is a simple path?

1.2 Questions

1. Given a graph G with n vertices, where n is even, prove that if every vertex has degree $\frac{n}{2}+1$, then G must contain a 3-cycle.

2. Every tournament has a Hamiltonian path. (Recall that a Hamiltonian path is a path that visits each vertex exactly once)

3. What is wrong with the following proof?

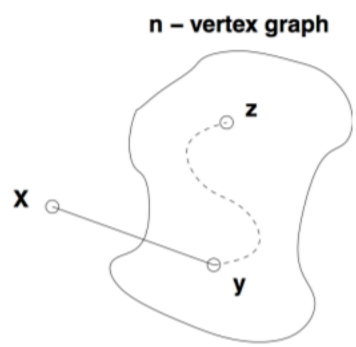
False Claim: If every vertex in an undirected graph has degree at least 1, then the graph is connected.

Proof. We use induction on the number of vertices $n \geq 1$.

Base case: There is only one graph with a single vertex and it has degree 0. Therefore, the base case is vacuously true, since the if-part is false.

Inductive Hypothesis: Assume the claim is true for some $n \geq 1$.

Inductive Step: We prove the claim is also true for $n+1$. Consider an undirected graph on n vertices in which every vertex has degree at least 1. By the inductive hypothesis, this graph is connected. Now add one more vertex x to obtain a graph on $(n+1)$ vertices, as shown below.



All that remains is to check that there is a path from x to every other vertex z. Since x has degree at least 1, there is an edge from x to some other vertex; call it y. Thus, we can obtain a path from x to z by adjoining the edge x, y to the path from y to z. This proves the claim for $n+1$. □

2 Eulerian Tour

2.1 Introduction

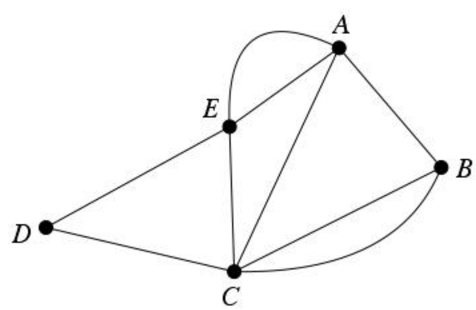
An **Eulerian path** is a path that uses every edge exactly once.

An **Eulerian tour** is a path that uses each edge exactly once and starts and ends at the same vertex.

Eulers Theorem: An undirected graph $G = (V, E)$ has an Eulerian tour if and only if G is even degree and connected (except possibly for isolated vertices).

2.2 Questions

1. Is there an Eulerian Tour? If so, find one. Repeat for an Eulerian Path.



2. If every node has even degree except two nodes that have odd degree, prove that the graph has a Eulerian path.

3 Trees

3.1 Introduction

If complete graphs are maximally connected, then trees are the opposite: Removing just a single edge disconnects the graph! Formally, there are a number of equivalent definitions for identifying a graph $G = (V, E)$ as a tree.

Assume G is connected. There are 3 other properties we can use to define it as a tree.

1. G contains __________cycles.

2. G has __________edges.

3. Removing any additional edge will __________________

One additional definition:

4. G is a tree if it has no cycles and ______________________________

Theorem: G is connected and contains no cycles if and only if G is connected and has $n - 1$ edges.

3.2 Questions

1. We saw in the notes on page 8 that 1 and 2 above were saying the same thing- that is, stated rigorously, 1 $\Leftrightarrow$ 2. We will now prove that 1 $\Leftrightarrow$ 3:

2. Prove the following properties of trees.

   a Any pair of vertices in a tree are connected by exactly one (simple) path.

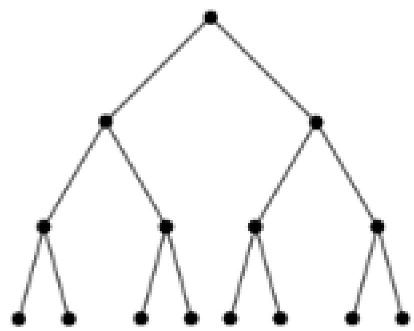
   b Adding any edge to a tree creates a simple cycle.

3. Now show that if a graph satisfies either of these two properties then it must be a tree:

   a If for every pair of vertices in a graph they are connected by exactly one simple path, then the graph must be a tree.

   b If the graph has no simple cycles but has the property that the addition of any single edge (not already in the graph) will create a simple cycle, then the graph is a tree.

4. Recall from the notes that a **rooted tree** is a tree with a particular node designated as the root, and the other nodes arranged in levels, growing down from the root. An alternative, recursive, definition of rooted tree is the following: A rooted tree consists of a single node, the root, together with zero or more branches, each of which is itself a rooted tree. The root of the larger tree is connected to the root of each branch.



Prove that given any tree, selecting any node to be the root produces a rooted tree according to the definition above.

5. A **spanning tree** of a graph G is a subgraph of G that contains all the vertices of G and is a tree.
Prove that a graph $G = (V, E)$ if connected if and only if it contains a spanning tree.

6. Show that the edges of a complete graph on n vertices for even n can be partitioned into $\frac{n}{2}$ edge disjoint spanning trees.
   Hint: Recall that a complete graph is an undirected graph with an edge between every pair of vertices. The complete graph has $\frac{n*(n-1)}{2}$ edges. A spanning tree is a tree on all n vertices – so it has $n-1$ edges. So the complete graph has enough edges (for even n) to create exactly $\frac{n}{2}$ edge disjoint spanning trees (i.e. each edge participates in exactly one spanning tree). You have to show that this is always possible.

7. How many distinct spanning trees does K_3 have? How many does K_4 have?

4 Hypercubes

4.1 Introduction

What is an n dimensional hypercube?

Bit definition: Two __________ x and y are __________ and only if ____ and ____ differ in ______________________ bit position.

Recursive definition: Define the 0-__________ as the $(n-1)$ dimensional __________

with vertices labeled 0x (x is an element of ______________ (hint: how many remaining bits are there?). Do the same for the 1-__________ with vertices labeled _______. Then an n dimensional __________ is created by placing an edge between _______ and _______ in the _____________ and _____________

respectively.

4.2 Questions

1. How many vertices does an n dimensional hypercube have?

2. How many edges does an n dimensional hypercube have?

3. How many edges do you need to cut from a hypercube to isolate one vertex in an n-dimensional hypercube?

4. Prove that any cycle in an n-dimensional hypercube must have even length.

5. **Coloring Hypercubes**
   Let $G = (V, E)$ be an undirected graph. G is said to be k-vertex-colorable if it is possible to assign one of k colors to each vertex of G so that no two adjacent vertices receive the same color. G is k-edge-colorable if it is possible to assign one of k colors to each edge of G so that no two edges incident on the same vertex receive the same color.
   Show that the n-dimensional hypercube is 2-vertex-colorable for every n.

5 Extra Practice

5.1 Questions

1. Let v be an odd degree node. Consider the longest walk starting at v that does not repeat any edges (though it may omit some). Let w be the final node of the walk . Show that $v \neq w$.

2. Prove that undirected connected graph with $|V| \geq 2$, 2 nodes have same degree

3. Prove that every undirected finite graph where every vertex has degree of at least 2 has a cycle.

4. Prove that every undirected finite graph where every vertex has degree of at least 3 has a cycle of even length.

6 Bijections

6.1 Questions

1. Draw an example of each of the following situations

One to one AND NOT onto (injective but not surjective)	Onto AND NOT one to one (surjective but not injective)	One to one AND onto (bijection, i.e. injective AND surjective)

2. Are the following functions **injections** from Z_{12} to Z_{24}?

   a. $f(x) = 2x$

   b. $f(x) = 6x$

c. $f(x) = 2x + 4$

3. Are the following functions **surjections** from Z_{12} to Z_6? (Note: that $\lfloor x \rfloor$ is the floor operation on x)

   a. $f(x) = \lfloor \frac{x}{2} \rfloor$

   b. $f(x) = x$

   c. $f(x) = \lfloor \frac{x}{4} \rfloor$

4. Are the following functions **bijections** from Z_{12} to Z_{12}?

   a. $f(x) = 7x$

   b. $f(x) = 3x$

   c. $f(x) = x - 6$

7 RSA

7.1 Questions

1. **How does RSA work?**

   a. Alice wants to send Bob a message $m = 5$ using his public key ($n = 26$, $e = 11$). What cipher text E(m) will Alice send?

b. What is the value of d (Bobs private key) in this scheme? Note that traditional RSA schemes use much larger prime numbers, so its harder to break n down into its prime factors than it is in this problem.

2. In RSA, if Alice wants to send a confidential message to Bob, she uses Bobs public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$. And then Bob chose $e = 3$ so his public key is (3, 77). And then Bob chose $d = 26$ so his private key is (26, 77).
   Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.