CS 70 Homework #3

Sundry

caleb - cyro@berkeley.edu

Question 1: Planarity and Graph Complementary

a) max number of edges in simple graph (undirected)

↳ $\frac{n(n-1)}{2}$; n = vertices

↳ $\bar{E} = \frac{n(n-1)}{2} - |E|$; edges in $\bar{G}$

$|E|$ = # edges in G

B) Theorem: If $|V| \leq 15$, prove G being planar implies that G is nonplanar

<u>Direct Proof</u>

Assume G is planar, undirected graph

↳ Graph G must follow Eulers formula with (e) edges and (v) vertices ≥ 3 to be planar

$$e \leq 3(v) - 6$$

↳ from part A, we found $\bar{E} = \frac{n(n-1)}{2} - |E|$

⟶ plug parts together

$$\frac{n(n-1)}{2} - |E| \leq 3(v) - 6 \quad ; \; v = n$$

↳ $\frac{n(n-1)}{2} - (3(n) - 6) \leq 3(n-6)$

↳ $n(n-1) \leq 12(n-2)$

↳ $n^2 - n - 12n \leq -24$

↳ $n^2 - 13n \leq -24$

↳ $n \leq 10.7$ ⟶ Since $n \leq 10.7$, G possibly can fail Eulers formula for a planar graph

↳ Therefore, Theorem is True

c) converse of part B

Theorem: if $\bar{G}$ is non-planar then G is planar
vertices ≥ 15

<u>Direct Proof</u>

Assume: $\bar{G}$ is non-planar because it contains a cons
of K_5

↳ K_5: 5 vertices, 10 edges → fails $|\bar{E}| \leq 3|\bar{V}| - 6$

↳ Since we know $\bar{G}$ contains K_5, we can use
subdivision in order to increase # vertices and edges

→ subdivide K_5 10 times to get 15 vertices and 20 edges

↳ $\bar{G} = (V, \bar{E})$; $|\bar{V}| = 15$ and $|\bar{E}| = 20$

$$|E| = \frac{(15)(15-1)}{2} - 20 = 85 \text{ edges and } 15 \text{ vertices}$$

↳ Kuratowski's theorem on graph $\bar{G}$

$85 \leq 3(15) - 6 \rightarrow 85 \leq 39$ False

→ therefore G can not/still be non-planar

↳ Theory is False

2) Touring Hypercube

a) Theorem: hypercube has an Eulerian tour if and only if n is even

looking at 2 arbitrary vertices in n-cube

$x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$

↳ Since it's a hypercube, then 2 vertices joined by path which traverses vertices in the same!

$x_1, x_2, \ldots, x_n$

$y_1, x_2, \ldots, x_n$

$y_1, y_2, \ldots, x_n$

until it reaches

$y_1, y_2, \ldots, y_n$

→ Since each vertex in n-cube is next to exactly n other vertices, with flipping one n bits of the vertex

↳ Since our hypercube is even ~~#~~ of vertices, we can say that the graph is connected since every vertex has an even degree

h) theorem: Show that every hypercube has a Hamiltonian tour

Proof by induction

BC ($n=1$): A 1-cube is essentially 2 vertices connected by an edge. This fulfills our definition of a Hamiltonian tour

IH: Assume theorem is true for n and $n=k$

IS: $(k+1)$ cube will have 2 subgraphs corresponding $(k+1)$ to the k cube with vertices joined by its edges

↳ This tells us that our subdivision will have a Hamiltonian tour in one subgraph and a corresponding Hamiltonian cycle in an other, denoted by HC_n and HC_n'.

↳ In order to prove that the entirety is a Hamiltonian cycle, further, we can remove any arbitrary edge (v_1, v_2) from both HC_n and HC_n' and putting these two edges together creates a Hamiltonian cycle in $(k+1)$ cube, which proves the theorem

↳ By Induction, the theorem is true

3) Binary Trees

a) def of binary tree (height > 0) : Tree with 1 vertex (root) which has a degree of 2.

def of binary tree (height = 0) : only a vertex which is both a root and leaf

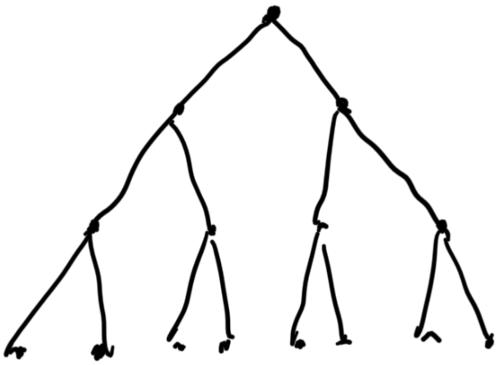
↳ What this tells us is that a tree (h > 0) will start with a root and have two different edges or branches that will start expanding the tree. Without the root, we are left with 2 vertices that can be considered as a root, which each can be used to fulfill the definition of a binary tree (causing 2 binary trees) Both them L and R with roots a and c

def of height : max length of path between root and leaf

↳ By proving that our main tree (T) can be expressed as 2 different binary trees (L and R) if the root of T is removed, we can find the height by looking for the largest of either L and R and adding 1 to that value which represents the root of T. or in other terms

↳ $h(T) = \max(h(L), h(R)) + 1$

h) Consider the graph theoretic def of a binary tree



visual	totals	difference	height
	1		0
		$> 2^1$	
	3		1
		$> 2^2$	
	7		2
		$> 2^3$	
	15		3

↳ From this, we see with $h+1$, the difference increases by 2^{h+1} of the total number of vertices. This is due to the def of binary tree where we stating that the degree of a non leaf and non root can only be 3. This means that a vertex enough extends by 2 branches or just stays a leaf. However we must account for the 1st instance of the binary tree, or the root, with a degree one lower than a non leaf / non root. This leaves us with an equation to calculate the max vertices of a binary tree with height (h).

↳ $2^{h+1} - 1$ vertices

c) theorem: all binary trees with n leaves will have 2n-1 vertices

Induction proof

BC (n=0): 2(1) - 1 = 1 True ✓

I H: Assume theorem is true for n leaves, taking into account that max number of vertices = $2^{h+1} - 1$ from part B

I S (n+1): Using part B, we can look at the difference between difference between h and h+1. the difference = 2^h which also conveniently equals the number of leaves for h+1. or in other words 2n.

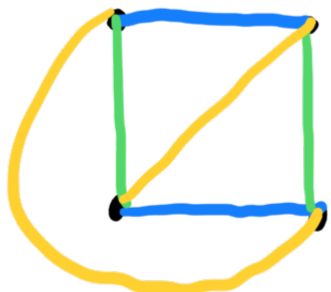
Since 2^{h+1} is equal to the number of vertices - root and 2n is equal to the number of leaves times 2 or necessary for the difference of h and h+1 which essentially means it is equal to the number of vertices - root we can substitute 2^{h+1} with 2n

2n-1 = vertices

By induction, this theorem is true

4) Edge coloring

a)



color 1: Blue

color 2: Green

color 3: Yellow

b) Theorem: any graph with max degree $d \geq 1$ can be edge colored with $2d-1$ colors

Proof by Induction

BC ($d=1$): $2(1)-1 = 1$ ✓

IH: Assume theorem is true for d and $d=k$

IS: for Graph G, create new graph G' where
$(k+1)$ $G' = G - \{u,v\}$

↳ v_{degree} in $G \leq d$
v_{degree} in $G' \leq d-1$
v's edges use $d-1$ colors

↳ u_{degree} in $G \leq d$
u_{degree} in $G' \leq d-1$
u's edges use $d-1$ colors

$d-1+d-1 = 2d-2$ coloring

↳ adding $\{u,v\}$ doesn't interfere any more, allows IH to be true for $k+1$

⇒ By Induction, the proof is true

c) Theorem: a tree can be edge colored with d colors where d is the max degree of any vertex

Base case ($d=0$): True ✓

IH: Assume theorem is true for d until $d=k$

IS: like what B ! $G' = G - V$ where

(k+1)

↳ u's degree in G $\leq d$ colors

↳ u's degree in $G-V$ $\leq d-1$ colors

↳ IH applies to G'

↳ G' d' colored where $d' \leq d$ and G' can be d colored if u is added back into the equation, allowing $\{u, v\}$ to be colored

↳ By induction, this proof is true

5) Modular Practice

a) $9x + 5 \equiv 7 \pmod{13}$

$\quad -5 \quad -5$

↳ $\frac{9x}{9} = \frac{2}{9} \pmod{13}$

↳ $x = \frac{2}{9} \pmod{13}$; since fraction cannot exist in a modulo, need to do inverse

↳ $\gcd(9, 13) \rightarrow 1$; inverse exists

→ Bezout's theorem: $\gcd(a, b) = sa + tb$

↳ $(9, 13) = 1 \rightarrow 1 = 9s + 13t$

$d = \gcd(x, y) = as + by$

$d = \gcd(9, 13) = 9s + 13t$

$1 = \gcd(13, 9) = 9s + 13t$

↳ Euclid algorithm! $\gcd(9, 13) = 1$

→ $\underset{\text{largest \#}}{\underline{13}} : \underset{\text{multiple}}{\underline{1}} \cdot \underset{\text{small \#}}{\underline{9}} + \underset{\text{remainder}}{\underline{4}}$

↳ $9 = 2 \cdot 4 + 1$ → $4 = 4 \cdot 1 + 0$

↳ 1 is remainder GCD has to be 1

→ $1 = 9 - 2 \cdot 4$ → $4 = 13 - 1 \cdot 9$

solve in terms of N and mod

$1 = 9 - 2(13 - 1 \cdot 9)$ → $3 \cdot 9 - 2 \cdot 13$

↳ $1 = 9 - 2(13 - 1 \cdot 9)$

↳ $(1 \cdot 9) = -(2 \cdot 13) - (2 \cdot 9)$

↳ $(3 \cdot 9) = (2 \cdot 13)$

Bezouts results in $1 = 9 \cdot 3 - 13 \cdot 2$

↳ $9x + 5 \equiv 7 \mod 13$ → $9x \equiv 2 \mod 13$

↳ $3(9x) \equiv 3(2 \mod 13)$ → $27x \equiv 6 \pmod{13}$

↳ $x \equiv 6 \pmod{13}$

b) $3x+12 \equiv 4 \pmod{21}$

↳ $3x \equiv -8 \pmod{21}$; $21-8=13$

↳ $x \equiv 13/3 \bmod 21$

However...

$\gcd(3, 21) = \underline{3}$

↳ this means that there are no solutions since an inverse doesn't exist and it's relatively prime.

c) $5x+4y \equiv 0 \pmod 7$ and $2x+y \equiv 4 \pmod 7$

↳ $5x+4y \equiv 0 \bmod 7$

$-8x-4y \equiv 0 \bmod 7$

↳ $-3x \equiv -16 \pmod 7$

↳ $-3x \equiv (-3 \bmod 7)(x \bmod 7)$

↳ $-3+7=4$

$-16 \bmod 7 \rightarrow -9 \rightarrow -2 \rightarrow 5$

$+7 \quad +7 \quad +7$

$$\hookrightarrow \frac{1}{4}\cdot 4x \equiv 5 \bmod 7 \cdot \frac{1}{4}$$

$$x \equiv \frac{5}{4} \bmod 7 \rightarrow (4, 7)$$

$$\hookrightarrow 7 = 1\cdot 4 + 3$$

$$4 = 1\cdot 3 + 1$$

$$1 = 4 - 1\cdot 3 = 4 - 1(7 - 1\cdot 4)$$

$$\hookrightarrow 3 = 7 - 1\cdot 4 = 4 - 1\cdot 7 + 1\cdot 4 = 2\cdot 4 - 1\cdot 7$$

$$\hookrightarrow 8x \equiv 10 \bmod 7 \rightarrow 8 \bmod 7 \equiv 1 \bmod 7$$

$$\hookrightarrow (8 \,(\bmod 7))\, x\, (x \bmod 7)$$

$$\hookrightarrow x \bmod 7 \equiv 3 \rightarrow x \equiv 3 \bmod 7$$

$$\hookrightarrow 5(3) + 4y \equiv 0 \bmod 7$$

$$\hookrightarrow 15 + 4y \equiv 0 \bmod 7$$

$$\hookrightarrow 4y \equiv -15 \bmod 7 \;;\quad -15 \xrightarrow{+7} -8 \xrightarrow{+7} -1 \xrightarrow{+7} 6$$

$$\hookrightarrow 4y \equiv 6 \bmod 7 \rightarrow y \equiv 12 \bmod 7 \equiv 5 \bmod 7$$

d) $13^{2023} = x \pmod{12}$

b) Fermat Little theorem: $a^{p-1} \equiv 1 \pmod n$

$\rightarrow 13^{2023} = 13^{11(18)} = (\underbrace{13^{11}})^{18}$

$\hookrightarrow 13^{11} \equiv 1 \pmod{12}$; FLT

$\hookrightarrow (13^{11})^{183} \cdot 13^{10}$

$\hookrightarrow 1^{183} \cdot 13^{10} \pmod{12}$

$\hookrightarrow 1 \cdot 13^{10} \pmod{12}$

$\hookrightarrow x = 13^{10}$

e) $7^{62} \equiv x \pmod{11}$

↳ $7^{62} \to 7^{(10\cdot 6)+2} \to (7^{10})^6 \cdot 7^2$

↳ $7^{10} \equiv 1 \pmod{11}$

↳ $(1 \pmod{11})^6$

↳ $1^6 \cdot 7^2 \pmod{11}$

↳ $1 \cdot 49 \pmod{11}$

↳ $49 \xrightarrow[-11]{} 38 \xrightarrow[-11]{} 27 \xrightarrow[-11]{} 16 \xrightarrow[-11]{} 5$

↳ $5 \bmod 11 = x$

6) Non Trivial Solution

a) The only possible cubic values for mod 7 are $\pm 1, 0$.

b) Fermat's Little Law

$\rightarrow 0 \equiv n^7 - n = n(n^3-1)(n^3+1) \pmod 7$

* $(-1)^3, 0^3, 1^3$ give correct values

b) -1 can mean $+6$

b) $x^3 + 2y^3 \equiv 0 \pmod 7$ $x \equiv y \equiv 0 \pmod 7$

Proof by contraposition

$\neg Q$ $x, y \not\equiv 0 \pmod 7$ not multiples of 7

x^3 and y^3 cannot be 0

↳ mod 7 is 1 or 8

→ $P \to x^3 + 2y^3 \equiv 0 \pmod 7$

↳ $1 + 2 \equiv 0$ no

$6 + 12 \equiv 0$ no

$1 + 12 \equiv 0$ no

$6 + 2 \equiv 0$ no

proven $\neg P$

↳ By contrapositive, this theorem is true

c) $x^3 + 2y^3 = 2x^2y$

Proof by contradiction

has nontrivial solution

$x = 0$ $y =$ non zero

↳ $x^3 + 2y^3 = 2x^2y \pmod 2$

Constrains 2 · 2 mod 2 would be 0

↳ $x^3 + 2y^3 = 0$

↳ proof is proven this

↳ By contradiction, this theorem is true

7) <u>Wilson's theorem</u> : $(p-1)! \equiv -1 \pmod p$

prove theorem for both directions

a) p is prime if $(p-1)! \equiv -1 \pmod p$

* if p isn't prime, then will exist a value that can divide p ; $k \mid p$, so $k \mid (p-1)!$ and $q \equiv 1 \bmod p$ this means that p must be prime.

b) $(p-1)! \equiv -1 \pmod p$ if p is prime

* Since integers mod p interact with a group when each element isn't congruent 0 can [illegible] have a multiplicative inverse, we can assume that p cannot be divided by a prime k n, or pn is the first product after 0 n [illegible] in n defined by prime factorization theorem. this informs me that this direction can only be true if p is prime.