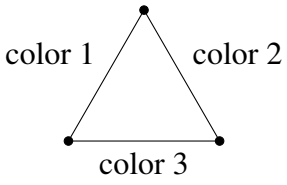
CS 70 Discrete Mathematics and Probability Theory
Spring 2025 Rao

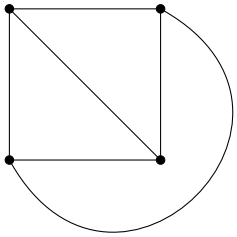
HW 03

1 Edge Colorings

Note 5

An edge coloring of a graph is an assignment of colors to edges in a graph where any two edges incident to the same vertex have different colors. An example is shown on the left.





(a) Show that the 4 vertex complete graph above can be 3 edge colored. (You may use the numbers $1,2,3$ for colors. A figure is shown on the right.)

(b) Prove that any graph with maximum degree $d \geq 1$ can be edge colored with $2d-1$ colors.

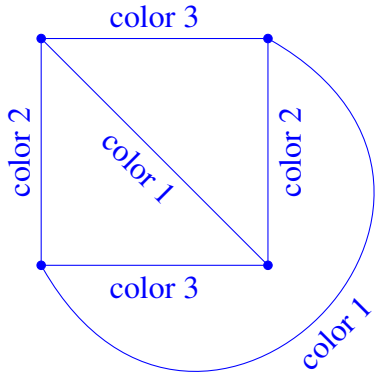
(c) Prove that a tree can be edge colored with d colors where d is the maximum degree of any vertex.

Solution:

(a) Three color a triangle u_1, u_2, u_3 where (u_1, u_2) is colored 1, (u_2, u_3) is colored 2, and (u_3, u_1) is colored 3. This is a valid 3 coloring as the edges are all colored differently.

Consider adding a fourth vertex v, the incident edges must be colored differently and each incident edge (v, u_i) needs to be colored differently from the edges incident to u_i. That is, one can color (v, u_1) with 2 as it is not incident to the edge colored 2 and that color is avalaible. Similarly one can color edge (v, u_2) with color 3 and (v, u_3) with color 1.

Another proof is simply provide a coloring which is below.



(b) We will use induction on the number of edges n in the graph to prove the statement: If a graph G has $n \geq 0$ edges and the maximum degree of any vertex is d, then G can be colored with $2d-1$ colors.

Base case ($n = 0$). If there are no edges in the graph, then there is nothing to be colored and the statement holds trivially.

Inductive hypothesis. Suppose for $n = k \geq 0$, the statement holds.

Inductive step. Consider a graph G with $n = k+1$ edges. Remove an edge of your choice, say e from G. Note that in the resulting graph the maximum degree of any vertex is $d' \leq d$. By the inductive hypothesis, we can color this graph using $2d'-1$ colors and hence with $2d-1$ colors too. The removed edge is incident to two vertices each of which is incident to at most $d-1$ other edges, and thus at most $2(d-1) = 2d-2$ colors are unavailable for edge e. Thus, we can color edge e without any conflicts. This proves the statement for $n = k+1$ and hence by induction we get that the statement holds for all $n \geq 0$.

(c) We will use induction on the number of vertices n in the tree to prove the statement: For a tree with $n \geq 1$ vertices, if the maximum degree of any vertex is d, then the tree can be colored with d colors.

Base case ($n = 1$). If there is only one vertex, then there are no edges to color, and thus can be colored with 0 colors.

Inductive hypothesis. Suppose the statement holds for $n = k \geq 1$.

Inductive Step. Remove any leaf v of your choice from the tree. We can then color the remaining tree with d colors by the inductive hypothesis. For any neighboring vertex u of vertex v, the degree of u is at most $d-1$ since we removed the edge $\{u,v\}$ along with the vertex v. Thus its incident edges use at most $d-1$ colors and there is a color available for coloring the edge $\{u,v\}$. This completes the inductive step and by induction we have that the statement holds for all $n \geq 1$.

2 Touring Hypercube

Note 5

In the lecture, you have seen that if G is a hypercube of dimension n, then

- The vertices of G are the binary strings of length n.
- u and v are connected by an edge if they differ in exactly one bit location.

A *Hamiltonian tour* of a graph (with $n \geq 2$ vertices) is a tour that visits every vertex exactly once.

(a) Prove that a hypercube has an Eulerian tour if and only if n is even.

(b) Prove that every hypercube has a Hamiltonian tour.

Solution:

(a) In the n-dimensional hypercube, every vertex has degree n. If n is odd, then by Euler's Theorem there can be no Eulerian tour. On the other hand, the hypercube is connected: we can get from any one bit-string x to any other y by flipping the bits they differ in one at a time. Therefore, when n is even, since every vertex has even degree and the graph is connected, there is an Eulerian tour.

(b) By induction on n. When $n = 1$, there are two vertices connected by an edge; we can form a Hamiltonian tour by walking from one to the other and then back.

Let $n \geq 1$ and suppose the n-dimensional hypercube has a Hamiltonian tour. Let H be the $n+1$-dimensional hypercube, and let H_b be the n-dimensional subcube consisting of those strings with initial bit b.

By the inductive hypothesis, there is some Hamiltonian tour T on the n-dimensional hypercube. Now consider the following tour in H. Start at an arbitrary vertex x_0 in H_0, and follow the tour T except for the very last step to vertex y_0 (so that the next step would bring us back to x_0). Next take the edge from y_0 to y_1 to enter cube H_1. Next, follow the tour T in H_1 backwards from y_1, except the very last step, to arrive at x_1. Finally, take the step from x_1 to x_0 to complete the tour. By assumption, the tour T visits each vertex in each subcube exactly once, so our complete tour visits each vertex in the whole cube exactly once.

To build some intuition, here are the first few cases:

- $n = 1$: 0, 1
- $n = 2$: 00, 01, 11, 10

  [Take the $n = 1$ tour in the 0-subcube (vertices with a 0 in front), move to the 1-subcube (vertices with 1 in front), then take the tour backwards. We know 10 connects to 00 to complete the tour.]

- $n = 3$: 000, 001, 011, 010, 110, 111, 101, 100

  [Take the $n = 2$ tour in the 0-subcube, move to the 1-subcube, then take the tour backwards. We know 100 connects to 000 to complete the tour.]

The sequence produced with this method is known as a Gray code.

3 Planarity and Graph Complements

Note 5

Let $G = (V, E)$ be an undirected graph. We define the complement of G as $\overline{G} = (V, \overline{E})$ where $\overline{E} = \{(i, j) \mid i, j \in V, i \neq j\} - E$; that is, $\overline{G}$ has the same set of vertices as G, but an edge e exists is $\overline{G}$ if and only if it does not exist in G.

(a) Suppose G has v vertices and e edges. How many edges does $\overline{G}$ have?

(b) Prove that for any graph with at least 13 vertices, G being planar implies that $\overline{G}$ is non-planar.

(c) Now consider the converse of the previous part, i.e., for any graph G with at least 13 vertices, if $\overline{G}$ is non-planar, then G is planar. Construct a counterexample to show that the converse

does not hold.

Hint: Recall that if a graph contains a copy of K_5, then it is non-planar. Can this fact be used to construct a counterexample?

Solution:

(a) If G has v vertices, then there are a total of $\frac{v(v-1)}{2}$ edges that could possibly exist in the graph. Since e of them appear in G, we know that the remaining $\frac{v(v-1)}{2} - e$ must appear in $\overline{G}$.

(b) Since G is planar, we know that $e \leq 3v-6$. Plugging this in to the answer from the previous part, we have that $\overline{G}$ has at least $\frac{v(v-1)}{2} - (3v-6)$ edges. Since v is at least 13, we have that $\frac{v(v-1)}{2} \geq \frac{v \cdot 12}{2} = 6v$, so $\overline{G}$ has at least $6v - 3v + 6 = 3v + 6$ edges. Since this is strictly more than the $3v-6$ edges allowed in a planar graph, we have that $\overline{G}$ must not be planar.

(c) The converse is not necessarily true. As a counterexample, suppose that G has exactly 13 vertices, of which five are all connected to each other and the remaining ten have no edges incident to them. This means that G is non-planar, since it contains a copy of K_5. However, $\overline{G}$ also contains a copy of K_5 (take any 5 of the 8 vertices that were isolated in G), so $\overline{G}$ is also non-planar. Thus, it is possible for both G and $\overline{G}$ to be non-planar.

4 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y. For each subpart, show your work and justify your answers.

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

(b) Prove that $3x + 12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x + 4y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

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

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{13}.$$

Now since $\gcd(9,13) = 1$, 9 has a (unique) inverse mod 13, and since $9 \times 3 = 27 \equiv 1 \pmod{13}$ the inverse is 3. So multiply both sides by $9^{-1} \equiv 3 \pmod{13}$ to get:

$$x \equiv 6 \pmod{13}.$$

(b) Notice that any number $y \equiv 4 \pmod{21}$ can be written as $y = 4 + 21k$ (for some integer k). Evaluating y mod 3, we get $y \equiv 1 \pmod{3}$.

Since the right side of the equation is $1 \pmod 3$, the left side must be as well. However, $3x+12$ will never be $1 \pmod 3$ for any value of x. Thus, there is no possible solution.

(c) First, subtract the first equation from four times the second equation to get:

$$\begin{aligned} 4(2x+y)-(5x+4y) &\equiv 4(4)-0 \pmod 7 \\ 8x+4y-5x-4y &\equiv 16 \pmod 7 \\ 3x &\equiv 2 \pmod 7 \end{aligned}$$

Multiplying by $3^{-1} \equiv 5 \pmod 7$, we have $x \equiv 10 \equiv 3 \pmod 7$.

Plugging this into the second equation, we have

$$2(3)+y \equiv 4 \pmod 7,$$

so the system has the solution $x \equiv 3 \pmod 7$, $y \equiv 5 \pmod 7$.

(d) We use the fact that $13 \equiv 1 \pmod{12}$. Thus, we can rewrite the equation as

$$x \equiv 13^{2023} \equiv 1^{2023} \equiv 1 \pmod{12}.$$

(e) One way to solve exponentiation problems is to test values until one identifies a pattern.

$$\begin{aligned} 7^1 &\equiv 7 \pmod{11} \\ 7^2 &\equiv 49 \equiv 5 \pmod{11} \\ 7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 5 \equiv 2 \pmod{11} \\ 7^4 &= 7 \cdot 7^3 \equiv 7 \cdot 2 \equiv 3 \pmod{11} \\ 7^5 &= 7 \cdot 7^4 \equiv 7 \cdot 3 \equiv 10 \equiv -1 \pmod{11} \end{aligned}$$

We theoretically could continue this until we the sequence starts repeating. However, notice that if $7^5 \equiv -1 \implies 7^{10} = (7^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}$.

Similarly, $7^{60} = (7^{10})^6 \equiv 1^6 \equiv 1 \pmod{11}$. As a final step, we have $7^{62} = 7^2 \cdot 7^{60} \equiv 7^2 \cdot 1 = 49 \equiv 5 \pmod{11}$.

5 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod p.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod q$?

Solution:

Direction 1: If p is prime, then the statement holds.

For the integers $1, \cdots, p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod{p}$, or when $p \mid x^2 - 1 = (x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod{p}$, as desired.

Direction 2: The expression holds *only if* p is prime (contrapositive: if p isn't prime, then it doesn't hold).

We will prove by contradiction that if some number p is composite, then $(p-1)! \not\equiv -1 \pmod{p}$. Suppose for contradiction that $(p-1)! \equiv -1 \pmod{p}$. Note that this means we can write $(p-1)!$ as $p \cdot k - 1$ for some integer k.

Since p isn't prime, it has some prime factor q where $2 \leq q \leq n-2$, and we can write $p = q \cdot r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p-1)! \equiv -1 \pmod{q}$. However, we know q is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod{q}$. Since $0 \not\equiv -1 \pmod{q}$, we have reached our contradiction.

6 How Many Solutions?

Note 6

Consider the equation $ax \equiv b \pmod{p}$ for prime p. In the below three parts, when we discuss solutions, we mean a solution x in the range $\{0, 1, \ldots p-1\}$. In addition, include justification for your answers to all the subparts of this problem.

(a) For how many pairs (a, b) does the equation have a unique solution?

(b) For how many pairs (a, b) does the equation have no solution?

(c) For how many pairs (a, b) does the equation have p solutions?

Now, consider the equation $ax \equiv b \pmod{pq}$ for distinct primes p, q. In the below three parts, when we discuss solutions, we mean a solution x in the range $\{0, 1, \ldots pq-1\}$.

(d) If $\gcd(a, pq) = p$, show that there exists a solution if and only if $b = 0 \pmod{p}$.

(e) If $\gcd(a, pq) = p$ and there is a solution x, show that there are exactly p solutions. (Hint: consider how you can generate another solution $x +$ ___)

(f) For how many pairs (a, b) are there exactly p solutions?

Solution:

(a) As long as a and p are coprime, then there is a unique solution $x = a^{-1}b \pmod{p}$. All $p-1$ values of a besides $a = 0$ are coprime to p, and any values of b will suffice. Thus, there are $(p-1)p$ pairs of values.

(b) If $a = 0$ but $b \neq 0$, then there are no solutions. There are $p-1$ such pairs.

(c) If $a = 0, b = 0$, then any value of x is a solution. Note that the previous two parts already used up $(p-1)p + (p-1) = p^2 - 1$ pairs, so there is only 1 pair left.

(d) First, note that $\gcd(a, pq) = p$ means that a is a nonzero multiple of p in $\pmod{pq}$.

Only if direction: The original equation tells us that $ax = b + kpq$, and we assume there is a solution x. If a is a multiple of p, then so is ax, and thus $b + kpq$ must be as well. In order for this to be true, b must therefore also be a multiple of p, and thus $b \mod p = 0$.

If direction: Assuming that both a, b are multiples of p, then we have the equation $\frac{a}{p}x = \frac{b}{p} + kq$. Looking at this equation in $\mod q$ tells us that $\frac{a}{p}x \equiv \frac{b}{p} \pmod{q}$ which has a unique solution x as long as $\frac{a}{p}$ is coprime to q. We know this is satisfied, because $\frac{a}{p}$ can neither be 0 nor q, due to $a \neq 0 \pmod{pq}$.

(e) Note that any number of the form $x + iq \pmod{pq}$ for $i \in \{0, 1, \ldots, p-1\}$ will generate a different, valid solution. This is because $a(x+iq) = ax + aiq = ax + kipq = ax = b \pmod{pq}$. There are p possible values for i that give us unique numbers in $\pmod{pq}$.

Now, we will show that any other number cannot be a valid solution. If we consider other numbers of the form $x + z$ where $z \neq iq \pmod{pq}$, then notice that z is not a multiple of q, and a is also not a multiple of q, so az cannot be a multiple of q and therefore neither is a multiple of pq, and thus $az \neq 0 \pmod{pq}$. Then, $a(x+z) = ax + az = b + az \neq b \pmod{pq}$.

(f) Let's consider the cases. If a is a nonzero multiple of p (for which there are $q-1$ values), then the previous parts tell us that there are exactly p solutions iff $b = 0 \pmod{p}$ (for which there are q values). There are thus $q(q-1)$ pairs in this case.

If a is a nonzero multiple of q, then analogous reasoning tells us that there is a solution iff $b = 0 \pmod{q}$, and there will be q solutions, not p.

The only remaining case is that $a = 0$ (which is equivalent to saying that a is a multiple of both p and q). Then, if $b = 0$ then any value of x is a solution, and if $b \neq 0$ then there are no solutions.

Thus, only the first case yields any solutions, for which there are $q(q-1)$ such pairs.