CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Koushik Sen and Satish Rao

HW 03

1 Planarity and Graph Complements

Let $G = (V, E)$ be an undirected graph. We define the complement of G as $\overline{G} = (V, \overline{E})$ where $\overline{E} = \{(i, j) | i, j \in V, i \neq j\} - E$; 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 thirteen vertices, of which five are all connected to each other and the remaining eight 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.

2 Touring Hypercube

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 is a sequence of vertices $v_0, v_1, \ldots, v_k$ such that:

- Each vertex appears exactly once in the sequence.
- Each pair of consecutive vertices is connected by an edge.
- v_0 and v_k are connected by an edge.

(a) Show that a hypercube has an Eulerian tour if and only if n is even. (*Hint: Euler's theorem*)

(b) Show 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 Connectivity

Consider the following claims regarding connectivity:

(a) Prove: If G is a graph with n vertices such that for any two non-adjacent vertices u and v, it holds that $\deg u + \deg v \geq n-1$, then G is connected.

[*Hint:* Show something more specific: for any two non-adjacent vertices u and v, there must be a vertex w such that u and v are both adjacent to w.]

(b) Give an example to show that if the condition $\deg u + \deg v \geq n-1$ is replaced with $\deg u + \deg v \geq n-2$, then G is not necessarily connected.

(c) Prove: For a graph G with n vertices, if the degree of each vertex is at least $n/2$, then G is connected.

(d) Prove: If there are exactly two vertices with odd degrees in a graph, then they must be in the same connected component (meaning, there is a path connecting these two vertices).

[*Hint:* Proof by contradiction.]

Solution:

(a) If u and v are two adjacent vertices, they are connected by definition. Then, consider non-adjacent u and v. Then, there must be a vertex w such that u and v are both adjacent to w. To see why, suppose this is not the case. Then, the set of neighbors of u and v has $n-1$ elements, but there are only $n-2$ other vertices. (This is the Pigeonhole Principle.) We have proven that for any non-adjacent u and v, there is a path $u \to w \to v$, and thus G is connected.

(b) Consider the graph formed by two disconnected copies of K_2. For non-adjacent u, v, it holds that $\deg u + \deg v = 2 = 4-2 = n-2$, but the graph is not connected.

(c) If each vertex's degree is at least $n/2$, then for any two non-adjacent vertices u, v,

$$\deg u + \deg v \geq \frac{n}{2} + \frac{n}{2} = n > n-1.$$

Then by part (a), the graph is connected.

(d) Suppose that they are not connected to each other. Then they must belong to two different connected components, say G_1 and G_2. Each of them will only have one vertex with odd degree. This leads to a contradiction since the sum of all degrees should be an even number.

4 Graph Coloring

Prove that a graph with maximum degree at most k is $(k+1)$-colorable.

Solution:

The natural way to try to prove this theorem is to use induction on the graph's maximum degree, k. Unfortunately, this approach is extremely difficult because covering all possible types of graphs when maximum degree changes requires extreme caution. You might be envisioning a certain graph as you write your proof, but your argument will likely not generalize. In graphs, typical good choices for the induction parameter are n, the number of nodes, or e, the number of edges. We typically shy away from inducting on degree.

We use induction on the number of vertices in the graph, which we denote by n. Let $P(n)$ be the proposition that an n-vertex graph with maximum degree at most k is $(k+1)$-colorable.

Base Case $n = 1$*:* A 1-vertex graph has maximum degree 0 and is 1-colorable, so $P(1)$ is true.

Inductive Step: Now assume that $P(n)$ is true, and let G be an $(n+1)$-vertex graph with maximum degree at most k. Remove a vertex v (and all edges incident to it), leaving an n-vertex subgraph,H. The maximum degree of H is at most k, and so H is $(k+1)$-colorable by our assumption $P(n)$. Now add back vertex v. We can assign v a color (from the set of $k+1$ colors) that is different from all its adjacent vertices, since there are at most k vertices adjacent to v and so at least one of the $k+1$ colors is still available. Therefore, G is $(k+1)$-colorable. This completes the inductive step, and the theorem follows by induction.

5 Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x+5 \equiv 7 \pmod{11}$.

(b) Show that $3x+15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x+2y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

(e) $7^{21} \equiv x \pmod{11}$.

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{11}.$$

Now since $\gcd(9,11) = 1$, 9 has a (unique) inverse mod 11, and since $9 \times 5 = 45 \equiv 1 \pmod{11}$ the inverse is 5. So multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get:

$$x \equiv 10 \pmod{11}.$$

(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, $3x+15$ will never be $1 \pmod{3}$ for any value of x. Thus, there is no possible solution.

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

$$2(2x+y)-(3x+2y) \equiv x \equiv 1 \pmod 7.$$

Now plug into the second equation.

$$2+y \equiv 4 \pmod 7,$$

so the system has the solution $x \equiv 1 \pmod 7$, $y \equiv 2 \pmod 7$.

(d) We use the fact that

$$13 \equiv 1 \pmod{12}$$

Thus, we can rewrite the equation as $x \equiv 13^{2019} \equiv 1^{2019} \equiv 1 \pmod{12}$.

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

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

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, $7^{20} = (7^{10})^2 \equiv 1^2 \equiv 1 \pmod{11}$. As a final step, we have $7^{21} = 7 \cdot 7^{20} \equiv 7 \cdot 1 = 7 \pmod{11}$.

6 Nontrivial Modular Solutions

(a) What are all the possible perfect cubes modulo 7?

(b) Show that any solution to $a^3 + 2b^3 \equiv 0 \pmod 7$ must satisfy $a \equiv b \equiv 0 \pmod 7$.

(c) Using part (b), prove that $a^3 + 2b^3 = 7a^2b$ has no non-trivial solutions (a,b) in the integers. In other words, there are no integers a and b, that satisfy this equation, except the trivial solution $a = b = 0$.

[*Hint:* Consider some nontrivial solution (a,b) with the smallest value for $|a|$ (why are we allowed to consider this?). Then arrive at a contradiction by finding another solution (a',b') with $|a'| < |a|$.]

Solution:

(a) Checking by hand, the only perfect cubes modulo 7 are 0, 1, and $6 \equiv -1$:

$$0^3 \equiv 0 \pmod 7 \qquad 4^3 \equiv 1 \pmod 7$$
$$1^3 \equiv 1 \pmod 7 \qquad 5^3 \equiv -1 \pmod 7$$
$$2^3 \equiv 1 \pmod 7 \qquad 6^3 \equiv -1 \pmod 7$$
$$3^3 \equiv -1 \pmod 7$$

(b) Considering the equation $a^3 + 2b^3 \equiv 0 \pmod 7$ and considering all cases for a^3 and b^3, the only way that $a^3 + 2b^3 \equiv 0 \pmod 7$ is if $a^3 \equiv b^3 \equiv 0 \pmod 7$. Thus $a \equiv b \equiv 0 \pmod 7$.

(c) We first show that if (a,b) is a solution to $a^3 + b^3 = 7a^2b$, then $a = 0$ implies that $b = 0$. In other words, if $a = 0$, then the solution must be trivial. To see why this is the case, suppose that $a = 0$. Then $b^3 = 0$, and so $b = 0$. Thus, any nontrivial solution must have $a \neq 0$, or equivalently, $|a| > 0$.

If (a,b) is a solution to the original equation, then this is also a solution to

$$a^3 + 2b^3 \equiv 0 \pmod 7.$$

From Part (b), we know that a, b are all divisible by 7, which in turn means that a^3, b^3 are divisible by 7^3. Thus, we can divide the entire original equation by 7^3, to see that

$$\left(\frac{a}{7}\right)^3 + 2\left(\frac{b}{7}\right)^3 = 7\left(\frac{a}{7}\right)^2\left(\frac{b}{7}\right).$$

Indeed, $(a/7, b/7)$ is another solution where all the values are integers, and $|a/7| < |a|$ (as $|a| > 0$). We've reached a contradiction to our initial assumption, which was that (a,b) was the solution with the least value of $|a|$. (This is a valid assumption since the $|a|$ are positive integers, and a non-empty set of positive integers has a minimum.) Thus, there does not exist a nontrivial solution to $a^3 + 2b^3 = 7a^2b$.

7 Check Digits: ISBN

In this problem, we'll look at a real-world applications of check-digits.

International Standard Book Numbers (ISBNs) are 10-digit codes $(d_1 d_2 \ldots d_{10})$ which are assigned by the publisher. These 10 digits contain information about the language, the publisher, and the number assigned to the book by the publisher. Additionally, the last digit d_{10} is a "check digit" selected so that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \pmod{11}$. (*Note that the letter X is used to represent the number 10 in the check digit.*)

(a) Suppose you have a very worn copy of the (recommended) textbook for this class. You want to list it for sale online but you can only read the first nine digits: 0-07-288008-? (the dashes are only there for readability). What is the last digit? Show your work.

(b) Wikipedia says that you can determine the check digit by computing $\sum_{i=1}^{9} i \cdot d_i \pmod{11}$. Show that Wikipedia's description is equivalent to the above description.

(c) Prove that changing any single digit of the ISBN will render the ISBN invalid. That is, the check digit allows you to *detect* a single-digit substitution error.

(d) Can we ever switch two distinct digits in an ISBN number and get another valid ISBN number? For example, could 012345678X and 015342678X both be valid ISBNs? Explain.

Solution:

(a) $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 + 10 \cdot d_{10} = 189 + 10d_{10} \equiv 2 + 10d_{10} \pmod{11}$. From the definition of the check digit, we know that $2 + 10d_{10} \equiv 0 \pmod{11}$ so $10d_{10} \equiv 9 \pmod{11}$. From here, we can quickly see that $d_{10} = 2$.

(b) It is sufficient to show that $d_{10} \equiv \sum_{i=1}^{9} i \cdot d_i \pmod{11}$ is a valid check digit (that is, that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \pmod{11}$). To see this, we note that

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot d_i &= \sum_{i=1}^{9} i \cdot d_i + 10 \cdot d_{10} \\
&= \sum_{i=1}^{9} i \cdot d_i + 10 \cdot \sum_{i=1}^{9} i \cdot d_i \\
&= (1 + 10) \cdot \sum_{i=1}^{9} i \cdot d_i \\
&\equiv 0 \pmod{11}
\end{aligned}$$

(c) Suppose that the correct digits are d_i (for $1 \leq i \leq 10$) and that the new digits are f_i. Since the question asks about a single substitution error, we will assume without loss of generality that the kth digit has been changed, i.e. $f_k \neq d_k$.

We proceed by proof by contradiction. Assume that the new ISBN is the same as previous one. Hence, we can write:

$$\sum_{i=1}^{10} i \cdot d_i \equiv \sum_{i=1}^{10} i \cdot f_i \pmod{11}$$

Since only for the kth digit $f_k \neq d_k$, then

$$k \cdot d_k \equiv k \cdot f_k \pmod{11}$$

Since 11 is prime and $1 \leq k \leq 10$, k has a (unique) inverse mod 11. We multiply the above equation by $k^{-1} \pmod{10}$.

$$d_k \equiv f_k \pmod{11}$$

Since $1 \leq d_k \leq 10$ and $1 \leq f_k \leq 10$, then

$$d_k = f_k$$

This is a contradiction, since at the beginning we assumed $f_k \neq d_k$. Hence, the the new ISBN is not the same as previous one and the error will be detected.

(d) Let's suppose that digits k and m are switched and all of the rest are left unchanged. We will write

$$f_i = \begin{cases} d_k, & i = m \\ d_m, & i = k \\ d_i, & \text{otherwise} \end{cases}$$

where $d_k \neq d_m$ (if they are equal, it's as if you never switched them so of course it will still be valid). Then we can write:

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot f_i &= k \cdot d_m + m \cdot d_k + \sum_{i \neq k,m} i \cdot d_i \\
&= (k-m+m)d_m + (m-k+k)d_k + \sum_{i \neq k,m} i \cdot d_i && \text{note that } k-m+m=k \\
&= (k-m) \cdot d_m + (m-k) \cdot d_k + \sum_{i=1}^{10} i \cdot d_i && \text{bring like terms into the summation} \\
&= (k-m) \cdot d_m - (k-m) \cdot d_k + \sum_{i=1}^{10} i \cdot d_i \\
&= (k-m) \cdot (d_m - d_k) + \sum_{i=1}^{10} i \cdot d_i && \text{combine like terms} \\
&\equiv (k-m) \cdot (d_m - d_k) \pmod{11} && \text{by the definition of the check digit}
\end{aligned}$$

Since we know that $-9 \leq k-m \leq 9$, $k-m \neq 0$, $d_m - d_k \neq 0$, and 11 is prime, we know that this will not be equivalent to 0 mod 11, thus an error will be detected.

8 Wilson's Theorem

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 $(p-1)! = 1 \cdot 2 \ldots \cdot p-1$ 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 $(p-1)! \not\equiv -1 \pmod{p}$; Hypothetically assume 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.