CS 70 Discrete Mathematics and Probability Theory
Spring 2021

HW 3

1 Planarity

(a) Prove that $K_{3,3}$ is nonplanar.

(b) Consider graphs with the property T: For every three distinct vertices v_1, v_2, v_3 of graph G, there are at least two edges among them. Use a proof by contradiction to show that if G is a graph on ≥ 7 vertices, and G has property T, then G is nonplanar.

Solution:

(a) Assume toward contradiction that $K_{3,3}$ were planar. In $K_{3,3}$, there are $v = 6$ vertices and $e = 9$ edges. If $K_{3,3}$ were planar, from Euler's formula we would have $v - e + f = 2 \Rightarrow f = 5$. On the other hand, each region is bounded by at least four edges, so $4f \leq 2e$, i.e., $20 \leq 18$, which is a contradiction. Thus, $K_{3,3}$ is not planar.

(b) In this problem, we use proof by contradiction. Assume G is planar. Select any five vertices out of the seven. Consider the subgraph formed by these five vertices. They cannot form K_5, since G is planar. So some pair of vertices amongst these five has no edge between them. Label these vertices v_1 and v_2. The remaining five vertices of G besides v_1 and v_2 cannot form K_5 either, so there is a second pair of vertices amongst these new five that has no edge between them. Label these v_3 and v_4. Label the remaining three vertices v_5, v_6 nd v_7. Since v_1v_2 is not an edge, by property T (which states any three vertices must have at least two edges between them)it must be that $\{v_1, v\}$ and $\{v_2, v\}$ are edges, where $v \in \{v_3, v_4, v_5, v_6, v_7\}$. Similarly for v_3, v_4 we have that $\{v_3, v\}$ and $\{v_4, v\}$ are edges, where $v \in \{v_1, v_2, v_5, v_6, v_7\}$. Now consider the subgraph induced by $\{v_1, v_2, v_3, v_5, v_6, v_7\}$. With the three vertices $\{v_1, v_2, v_3\}$ on one side and $\{v_5, v_6, v_7\}$ on the other, we observe that $K_{3,3}$ is a subgraph of this induced graph. This contradicts the fact that G is planar.

The above shows that any graph with 7 vertices and property T is non-planar. Any graph with greater than 7 vertices and property T will also be non-planar because it will contain a subgraph with 7 vertices and property T.

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 $v_0, v_1, \dots, v_k$ 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 Hamiltonian cycle in a dense graph.

A *Hamiltonian cycle* is a cycle where each vertex appears exactly once.

We will show that a simple graph with $n \geq 3$ vertices and where every vertex has degree strictly greater than $n/2$ has an Hamiltonian cycle.

We will do a proof by induction, but it is a bit different from what we are used to.

The idea is to say there is no smallest counterexample. That is, we assume we have a graph $G = (V,E)$ where adding any edge produces a graph with a Hamiltonian cycle.

Consider two vertices u and v that are non-adjacent and thus adding edge (u,v) implies that $G + (u,v)$ has a Hamiltonian cycle. Now G does not have any Hamiltonian cycles so every Hamiltonian cycle in $G + (u,v)$ uses edge (u,v).

This implies that there is a path, $u, v_1, \ldots, v_{n-2}, v$, in G that visits every vertex once and whose endpoints are u and v.

Argue that G has a Hamiltonian cycle. This contradicts the assumption that G did not have a Hamlitonian cycle and completes a proof of the claim since this means there is no smallest counterexample to the claim.

(Hint: Use the fact the u and v have high degree to argue that there is v_i on the path $v_2, \ldots, v_{n-2}$ where $(u, v_i) \in E$ and $(v, v_{i-1}) \in E$.)

Solution:

We have the path $u, v_1, \ldots, v_{n-2}, v$, in G. Let $U = \{v_i : (u, v_i) \in E \text{ and } i \in [2, n-2]\}$ and $V = \{v_i : (v_{i-1}, v) \text{ and } i \in [2, n-2]\}$. Look closely at V, these are not neighbors of v, but one over from neighbors of v along the path.

Notice $|U|, |V| > n/2 - 1$ since the degree of u and v are at least $n/2$ and they don't participate in an edge. The minus 1 is due to v_1 not being allowed in either set. The sum of their sizes is then strictly greater than $n-2$ which means that $U \cap V$ is non-empty since there are only $n-2$ vertices in $[2, n-2]$.

Lets take $i \in U \cap V$. That is, (u, v_i) and (v, v_{i-1}) are edges in G.

The cycle formed by $v_1, \ldots, v_{i-1}, v, v_{n-2}, v_{n-3}, \ldots, v_i, u$ is a Hamlitonian cycle.

5 Modular Practice

(a) Calculate 72^{316} mod 7.

(b) Solve the following system for x:

$$\begin{aligned} 3x &\equiv 4 + y \pmod 5 \\ 2(x-1) &\equiv 2y \pmod 5 \end{aligned}$$

(c) If it exists, find the multiplicative inverse of 31 mod 23 and 23 mod 31.

(d) Let n, x be positive integers. Prove that x has a multiplicative inverse modulo n if and only if $\gcd(n,x) = 1$. (Hint: Remember an iff needs to be proven both directions. The gcd cannot be 0 or negative.)

Solution:

(a) Notice that $72 \equiv 2 \pmod 7$. Also notice that $2^3 = 8 \equiv 1 \pmod 7$. Then

$$72^{316} \equiv 2^{316} \equiv 2 \cdot 2^{315} \equiv 2 \cdot (2^3)^{105} \equiv 2 \cdot 1^{105} \equiv 2 \pmod 7$$

(b) Solving the system we get $2x \equiv 3 \pmod 5$. At this point, the student must remember that he/she cannot divide by 2 and must find the inverse. We can multiply both sides by $2^{-1} \pmod 5$. Since $2 * 3 \equiv 1 \pmod 5$, we multiply 3 on both sides of the second equation to get $x - 1 \equiv 6y \pmod 5$, which can be simplified to $x - 1 \equiv y \pmod 5$. (Note that division by 2 in normal arithmetic is the same as multiplying by 2^{-1} in modular arithmetic.) Our final solution is $x = 4$.

(c)

31	23	-20	27	1
23	8	7	-20	1
8	7	-6	7	1
7	1	1	-6	1
1	0	1	1	1

The table above is running egcd algorithm. First apply the gcd on the left two columns. After confirming that the gcd is 1, we then start the process of finding the multiplicative inverse by using the egcd algorithm explained in the notes. (Remember that finding the multiplicative inverse for $a \pmod b$ is to find an x to fulfill $a * x \equiv 1 \mod b$.) Using this tabular form will speed up your process (compared to writing out equations each time).

$$31^{-1} \bmod 23 = 3 = -20$$
$$23^{-1} \bmod 31 = 27$$

(d) If x has a multiplicative inverse modulo n, then $\gcd(n,x) = 1$.

Given that x has a multiplicative inverse modulo n, we can proceed as follows:

Assume for the sake of contradiction that the gcd, d, is greater than 1.

$$xa \equiv 1 \pmod n$$
$$xa = bn + 1$$
$$\frac{xa}{d} = \frac{bn+1}{d}$$
$$\frac{xa}{d} = \frac{bn}{d} + \frac{1}{d}$$

We've reached a contradiction because xa/d and bn/d must both be integers, however, $1/d$ is not. Therefore we've reached a contradiction, and because the gcd cannot be 0 or negative, it must be 1.

If $\gcd(n,x) = 1$, then x has a multiplicative inverse modulo n. The proof is as follows:

We know $\exists\, a, b \in \mathbb{Z}$ such that

$$an + bx = 1,$$
$$bx \equiv 1 \pmod n.$$

Thus, x has a multiplicative inverse b.

6 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of a modulo m**.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

Solution:

(a) No, because $3 \cdot 5 = 15 \equiv 5 \pmod{10}$.

(b) Yes, because $3 \cdot 5 = 15 \equiv 1 \pmod{14}$.

(c) Yes, because $(3 + 14n) \cdot 5 = 15 + 14 \cdot 5n \equiv 15 \equiv 1 \pmod{14}$.

(d) No. For contradiction, assume $x \in \mathbb{Z}$ is an inverse of 4 modulo 8. Then $4x \equiv 1 \pmod{8}$. Then $8 \mid 4x - 1$, which is impossible.

(e) No. We have $xa \equiv x'a \equiv 1 \pmod{m}$. So

$$xa - x'a = a(x - x') \equiv 0 \pmod{m}.$$

Multiply both sides by x, we get

$$xa(x - x') \equiv 0 \cdot x \pmod{m}$$
$$\implies x - x' \equiv 0 \pmod{m}.$$
$$\implies x \equiv x' \pmod{m}$$

7 Just Can't Wait

Joel lives in Berkeley. He mainly commutes by public transport, i.e., bus and BART. He hates waiting while transferring, and he usually plans his trip so that he can get on his next vehicle immediately after he gets off the previous one (zero transfer time, i.e. if he gets off his previous vehicle at 7:00am he gets on his next vehicle at 7:00am). Tomorrow, Joel needs to take an AC Transit bus from his home stop to the Downtown Berkeley BART station, then take BART into San Francisco.

(a) The bus arrives at Joel's home stop every 22 minutes from 6:05am onwards, and it takes 10 minutes to get to the Downtown Berkeley BART station. The train arrives at the station every 8 minutes from 4:25am onwards. What time is the earliest bus he can take to be able to transfer to the train immediately? Show your work. (Find the answer without listing all the schedules. Hint: derive an equation relating the bus number and train number and then work in modular arithmetic to get rid of one of the variables to give a set of possible train numbers.)

(b) Joel has to take a Muni bus after he gets off the train in San Francisco. The commute time on BART is 33 minutes, and the Muni bus arrives at the San Francisco BART station every 17 minutes from 7:12am onwards. What time is the earliest bus he could take from Berkeley to ensure zero transfer time for both transfers? If all bus/BART services stop just before midnight, is it the only bus he can take that day? Show your work.

Solution:

(a) The earliest AC Transit bus Joel can take is at 7:11am, from which he can transfer to BART immediately after he gets off the bus at 7:21am.

Let the x^{th} bus (zero-based) be the bus Joel can take with zero transfer time, and let the y^{th} train (zero-based) be the train that he will connect to. Taking the time the BART starts running (4:25am) as a reference point, let t be the time in minutes from 4:25am to the transfer time to the y^{th} train [1]. Figure 1 shows the timeline.

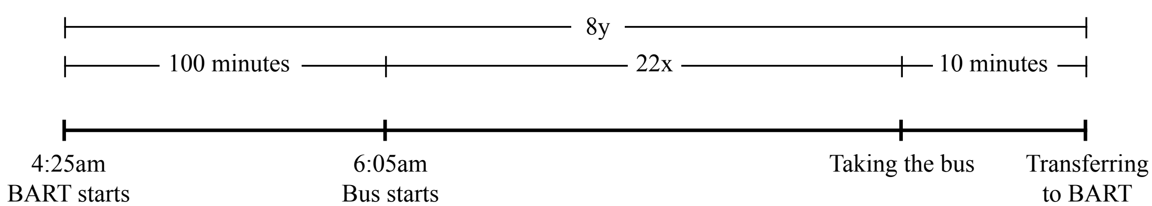

Figure 1: Timeline

From the timeline, we see the relation between x, y, and t,

$$
\begin{aligned}
t = 100 + 22x + 10 &= 8y \\
8y - 22x &= 110 \\
4y - 11x &= 55 \qquad (1)
\end{aligned}
$$

We modulo both sides of Equation (1) with 11 to eliminate x,

$$
\begin{aligned}
&\text{Left-hand side: } (4y - 11x) \equiv 4y, \pmod{11}, \\
&\text{Right-hand side: } 55 \equiv 0 \pmod{11},
\end{aligned}
$$

[1] Using any other time as a reference point works too, i.e., midnight, 7:00am (and find the BART departure after 7:00am), etc.

and form a congruence,

$$4y \equiv 0 \pmod{11}. \tag{2}$$

Since 3 is the multiplicative inverse of 4 modulo 11. Multiplying both sides of the congruence (2) by 3 gives us y,

$$\begin{aligned} 3 \cdot 4y &\equiv 3 \cdot 0 \pmod{11} \\ y &\equiv 0 \pmod{11}, \\ y &\in \{\dots, 0, 11, 22, 33, \dots\}. \end{aligned}$$

Since the bus hasn't started running when the 0^{th} and 11^{th} trains run, the 22^{th} train is the first train to connect to. The 22^{th} train departs at 4:25am + 8(22) minutes = 4:25am + 2:56 hours = 7:21am. The bus that arrives the BART station at 7:21am departs Joel's home stop at 7:21am - 10 minutes = 7:11am.

(b) The first AC Transit bus Joel can take is at 11:35am, from which he can connect to BART at 11:45am, and then Muni bus at 12:18pm. This is the only bus of the day that he can avoid waiting for both transfers.

From part a, we know that the soonest time Joel can arrive the San Francisco BART station is 7:21am + 33 minutes = 7:54am, and that he can choose to arrive every 88 minutes after that, since it is the interval AC Transit bus and BART coincides again. Let x be the number of times this 88-minute interval occurs after 7:54am (x starts from 0), and y^{th} bus (zero-based) be the Muni bus that Joel can transfer to with zero transfer time. Taking the time the Muni bus starts running (7:12am) as a reference point, let t be the time in minutes from 7:12am to the transfer time from BART to the y^{th} Muni bus. Figure 2 shows the timeline.

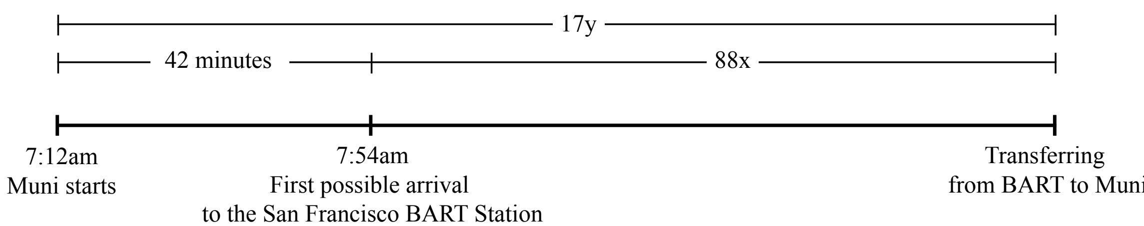

Figure 2: Timeline

Again, we write a relation between x, y, and t.

$$\begin{aligned} t = 42 + 88x &= 17y \\ 17y - 88x &= 42 \end{aligned} \tag{3}$$

The rest is quite similar to part a.

We modulo both sides of Equation (3) with 88 to eliminate x and form a congruence,

$$17y \equiv 42 \pmod{88}. \tag{4}$$

We have $17 \times 5 = 85 \equiv -3 \pmod{88}$. Let's mutiply both sides by 5:

$$-3y \equiv 210 \equiv 34 \pmod{88}. \tag{5}$$

We have $3 \times 29 = 87 \equiv -1 \pmod{88}$. Let's mutiply both sides by 29:

$$y \equiv 34 \times 29 = 986 \equiv 18 \pmod{88}, \tag{6}$$

$$y \in \{\ldots, -70, 18, 106, \ldots\}. \tag{7}$$

The first Muni bus Joel can take with zero transfer time is the 18^{th} Muni bus at 7:12am + 17(18) minutes = 7:12am + 5:06 hours = 12:18pm. Subtracting the 33 minutes BART transit time, the BART departure time is 12:18pm - 33 minutes = 11:45am. Subtracting the 10 minutes AC Transit travel time, the AC Transit bus departure time is 11:45am - 10 minutes = 11:35am.

Because the Least Common Multiple of 88 and 17 is $88 \times 17 = 1496$, it will take 1,496 minutes = 24 hours 56 minutes for all three buses and BART to coincide again. Since all services stop just before midnight and restart at their respective times the next day, all three buses and BART coincide only once a day, and what we found is the only bus Joel can take that day. □