CS 70 Discrete Mathematics and Probability Theory
Spring 2020 **HW 3**

1 A Better Stable Pairing

In this problem we examine a simple way to *merge* two different solutions to a stable matching problem. Let R, R' be two distinct stable pairings. Define the new pairing $R \wedge R'$ as follows:

> For every job j, j's partner in $R \wedge R'$ is whichever is better (according to j's preference list) of their partners in R and R'.

Also, we will say that a job/candidate *prefers* a pairing R to a pairing R' if they prefers their partner in R to their partner in R'. We will use the following example:

jobs	preferences	candidates	preferences
A	1>2>3>4	1	D>C>B>A
B	2>1>4>3	2	C>D>A>B
C	3>4>1>2	3	B>A>D>C
D	4>3>2>1	4	A>B>D>C

(a) $R = \{(A,4),(B,3),(C,1),(D,2)\}$ and $R' = \{(A,3),(B,4),(C,2),(D,1)\}$ are stable pairings for the example given above. Calculate $R \wedge R'$ and show that it is also stable.

(b) Prove that, for any pairings R, R', no job prefers R or R' to $R \wedge R'$.

(c) Prove that, for any stable pairings R, R' where j and c are partners in R but not in R', one of the following holds:

- j prefers R to R' and c prefers R' to R; or
- j prefers R' to R and c prefers R to R'.

[*Hint*: Let J and C denote the sets of jobs and candidates respectively that prefer R to R', and J' and C' the sets of jobs and candidates that prefer R' to R. Note that $|J|+|J'| = |C|+|C'|$. (Why is this?) Show that $|J| \leq |C'|$ and that $|J'| \leq |C|$. Deduce that $|J'| = |C|$ and $|J| = |C'|$. The claim should now follow quite easily.]

(You may assume this result in the next part even if you don't prove it here.)

(d) Prove an interesting result: for any stable pairings R, R', (i) $R \wedge R'$ is a pairing [*Hint*: use the results from (c)], and (ii) it is also stable.

Solution:

(a) $R \wedge R' = \{(A,3),(B,4),(C,1),(D,2)\}$. This pairing can be seen to be stable by considering the different combinations of jobs and candidates. For instance, A prefers 2 to their current partner 3. However, 2 prefers her current partner D to A. Similarly, A prefers 1 the most, but 1 prefers her current partner C to A. We can prove the stability of this pairing by considering the remaining pairs like this.

(b) Let j be a job, and let their partners in R and R' be c and c' respectively, and without loss of generality, let $c > c'$ in j's list. Then their partner in $R \wedge R'$ is c, whom they prefer over c'. However, for j to prefer R or R' over $R \wedge R'$, j must prefer c or c' over c, which is not possible (since $c > c'$ in their list).

(c) Let J and C denote the sets of jobs and candidates respectively that prefer R to R', and J' and C' the sets of jobs and candidates that prefer R' to R. Note that $|J| + |J'| = |C| + |C'|$, since the left-hand side is the number of jobs who have different partners in the two pairings, and the right-hand side is the number of candidates who have different partners.

Now, in R there cannot be a pair (j,c) such that $j \in J$ and $c \in C$, since this will be a rogue couple in R'. Hence the partner in R of every jobs in J must lie in C', and hence $|J| \leq |C'|$. A similar argument shows that every jobs in J' must have a partner in R' who lies in C, and hence $|J'| \leq |C|$.

Since $|J| + |J'| = |C| + |C'|$, both these inequalities must actually be tight, and hence we have $|J'| = |C|$ and $|J| = |C'|$. The result is now immediate: if the jobs j is partners with the candidate c in one but not both pairings, then

- either $j \in J$ and $c \in C'$, i.e., j prefers R to R' and c prefers R' to R,
- or $j \in J'$ and $c \in C$, i.e., j prefers R' to R and c prefers R to R'.

(d) (i) If $R \wedge R'$ is not a pairing, then it is because two jobs get the same candidate, or two candidates get the same job. Without loss of generality, assume it is the former case, with $(j,c) \in R$ and $(j',c) \in R'$ causing the problem. Hence j prefers R to R', and j' prefers R' to R. Using the results of the previous part would imply that c would prefer R' over R, and R over R' respectively, which is a contradiction.

(ii) Now suppose $R \wedge R'$ has a rogue couple (j,c). Then j strictly prefers c to their partners in both R and R'. Further, c prefers j to her partner in $R \wedge R'$. Let c's partners in R and R' be j_1 and j_2. If she is finally matched to j_1, then (j,c) is a rogue couple in R; on the other hand, if she is matched to j_2, then (m,w) is a rogue couple in R'. Since these are the only two choices for c's partner, we have a contradiction in either case.

2 Pairing Up

Prove that for every even $n \geq 2$, there exists an instance of the stable matching problem with n jobs and n candidates such that the instance has at least $2^{n/2}$ distinct stable matchings.

Solution:

To prove that there exists such a stable matching instance for any even $n \geq 2$, we just need to show how to construct such an instance.

The idea here is that we can create pairs of jobs and pairs of candidates: pair up job $2k-1$ and $2k$ into a pair and candidate $2k-1$ and $2k$ into a pair, for $1 \leq k \leq n/2$ (you might come to this idea since we are asked to prove this for *even* n).

For n, we have $n/2$ pairs. Choose the preference lists such that the kth pair of jobs rank the kth pair of candidates just higher than the $(k+1)$th pair of candidates (the pairs wrap around from the last pair to the first pair), and the kth pair of candidates rank the kth pair of jobs just higher than the $(k+1)$th pair of jobs. Within each pair of pairs (j, j') and (c, c'), let j prefer c, let j' prefer c', let c prefer j', and let c' prefer j.

Each match will have jobs in the kth pair paired to candidates in the kth pair for $1 \leq k \leq n/2$.

A job j in pair k will never form a rogue couple with any candidate c in pair $m \neq k$. If $m > k$, then c prefers her current partner in the kth pair to j. If $m < k$, then j prefers its current partner in the kth pair to c. Then a rogue couple could only exist in the same pair - but this is impossible since exactly one of either j or c must be matched to their preferred choice in the pair.

Since each job in pair k can be stably matched to either candidate in pair k, and there are $n/2$ total pairs, the number of stable matchings is $2^{n/2}$.

3 Well-Ordering Principle

In this question we walk you through one possible method to prove the well-ordering principle using induction. Recall that the well-ordering principle can be stated as follows:

For every non-empty subset S of the set of natural numbers $\mathbb{N}$, there is a smallest element $x \in S$; i.e.

$$\exists x : \forall y \in S : x \leq y.$$

We break this problem into cases depending on whether S is finite or not.

(a) Prove the well-ordering principle for finite sets S by induction on the size of the set.

(b) Prove that a set S containing only elements less than or equal to n must have size at most $n+1$, by induction on the maximal element of S.

(c) Use the previous part to prove the well-ordering principle for infinite sets S. (*Hint*: Choose an arbitrary element $x \in S$ and split S into two sets - one with all elements which are at most x and one with all elements larger than x.)

Solution:

(a) **Base case**: All sets of size one have a least element - namely, the lone element.

Inductive hypothesis: Assume for some arbitrary $k \geq 1$ that all sets of size k have a least element.

Inductive step: Let set S have $k+1$ elements. Consider some arbitrary element $x \in S$. Define the set $S' = S \setminus \{x\}$. By the inductive hypothesis, S' has a least element - call it x'. Now if $x' < x$ then x' is also the least element of S. If $x < x'$ then x is the least element of S, since all elements of S' are larger than x', which is larger than x. Either way, S has a least element.

(b) **Base case**: If the maximal element of S is 0, then $|S| = 1$, since 0 is the only natural number less than or equal to 0.

Inductive hypothesis: Assume that for all natural numbers $0 \leq x \leq k$ that if the maximal element of set S is x, then $|S| \leq x+1$.

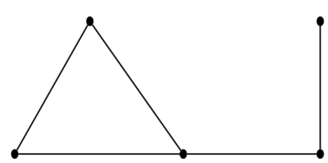
Inductive step: Consider a set S which has maximal element $k+1$. Define $S' = S \setminus \{k+1\}$. Then the maximal element of S' must be between 0 and k, inclusive, meaning that the number of elements in S' is $k+1$ by the inductive hypothesis. Adding back the element $k+1$, we then see that S must have size at most $(k+1)+1 = k+2$ elements.

(c) Choose an arbitrary element $x' \in S$. Consider the two sets $S_1 = \{x \mid x \in S,\ x \leq x'\}$ and $S_2 = \{x \mid x \in S,\ x > x'\}$. Note that $S_1 \cup S_2 = S$, so if we show that there is an element in S which is less than all elements of both S_1 and S_2, then we will have shown that S has a least element.

By part (b), since all elements of S_1 are at most x', S_1 has at most $x'+1$ elements in it, i.e. S_1 has finite size. So by part (a), S_1 has a least element, call it x_{min}. By definition, all elements in S_1 are greater than or equal to x_{min}. Also, all elements in S_2 are greater than x', which is greater than or equal to x_{min}. This completes the proof.

4 Degree Sequences

The *degree sequence* of a graph is the sequence of the degrees of the vertices, arranged in descending order, with repetitions as needed. For example, the degree sequence of the following graph is $(3,2,2,2,1)$.



For each of the parts below, determine if there exists a simple undirected graph G (i.e. a graph without self-loops and multiple-edges) having the given degree sequence. Justify your claim.

(a) $(3,3,2,2)$

(b) $(3,2,2,2,2,1,1)$

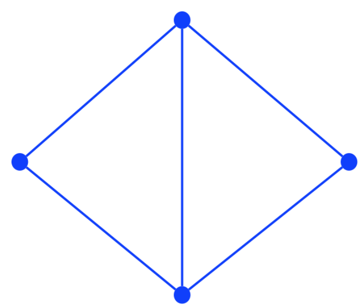
(c) $(6,2,2,2)$

(d) $(4,4,3,2,1)$

Solution:

(a) **Yes**

The following graph has degree sequence $(3,3,2,2)$.



(b) **No**

For any graph G, the number of vertices that have odd degree is even. The given degree sequence has 3 odd degree vertices.

(c) **No**

The total number of vertices is 4. Hence there cannot be a vertex with degree 6.

(d) **No**

The total number of vertices is 5. Hence, any degree 4 vertex must have an edge with every other vertex. Since there are two degree 4 vertices, there cannot be a vertex with degree 1.

5 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.

6 Trees and Components

(a) Bob removed a degree 3 node from an n-vertex tree. How many connected components are there in the resulting graph? Please provide an explanation.

(b) Given an n-vertex tree, Bob added 10 edges to it and then Alice removed 5 edges. If the resulting graph has 3 connected components, how many edges must be removed in order to remove all cycles from the resulting graph? Please provide an explanation.

Solution:

(a) **3.**

Let the original graph be denoted by $G = (V, E)$ and the resulting graph after Bob removes the node be denoted by $G' = (V', E')$. Let $|V| = n$ and hence $|E| = n - 1$ by the Theorem proved in class. Also, $|V'| = n - 1$ and $|E'| = n - 4$. Let k denote the number of connected components in G'. Since removing vertices and edges should not give rise to cycles, we know that the graph G' is acyclic. Hence each of the connected components is a tree. Let $n_1, n_2, \ldots, n_k$ denote the number of nodes in each of the k connected components respectively. Again by the Theorem proved in class, we have that each of the component consists of $n_1 - 1, n_2 - 1, \ldots, n_k - 1$ edges respectively. Thus the total number of edges in G' is

$$n - 4 = |E'| = \sum_{i=1}^{k} (n_i - 1) = (\sum_{i=1}^{k} n_i) - k = (n-1) - k.$$

Hence $k = 3$.

Alternate Solution. Here we use the fact that removing an edge from a forest (i.e an acyclic graph) increases the number of components by exactly 1. If we remove the three edges incident on the vertex removed by Bob, we get 4 components. However, Bob has also removed the degree 3 vertex which itself is one of the four connected components. Hence we are left with 3 connected components.

(b) **7.**

We first note that in any connected graph if we remove an edge belonging to a cycle, then the resulting graph is still connected. Hence for any connected graph, we can repeatedly remove edges belonging to cycles, until no more cycles remain. This process will give rise to a connected acyclic graph, i.e., a tree.

Since the final graph we wish to obtain is acyclic, each of its connected component must be a tree. Thus the components should have $n_1 - 1$, $n_2 - 1$ and $n_3 - 1$ edges each, where n_1, n_2, n_3 are the number of vertices in each of these components. Let n denote the total number of vertices and hence $n = n_1 + n_2 + n_3$. As a result, the total number of edges in the final graph is $n - 3$. The total number of edges after Bob and Alice did their work was $n - 1 + 10 - 5 = n + 4$. Thus one needs to remove 7 edges.

7 Bipartite Graphs

An undirected graph is bipartite if its vertices can be partitioned into two disjoint sets L, R such that each edge connects a vertex in L to a vertex in R (so there does not exist an edge that connects two vertices in L or two vertices in R).

(a) Suppose that a graph G is bipartite, with L and R being a bipartite partition of the vertices. Prove that $\sum_{v \in L} \deg(v) = \sum_{v \in R} \deg(v)$.

(b) Suppose that a graph G is bipartite, with L and R being a bipartite partition of the vertices. Let s and t denote the average degree of vertices in L and R respectively. Prove that $s/t = |R|/|L|$.

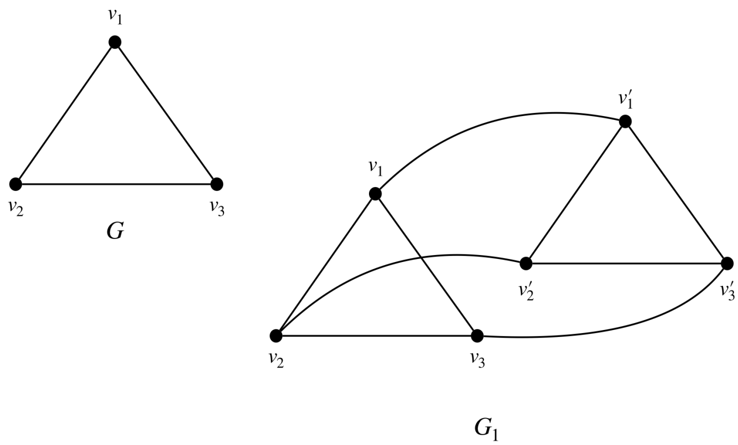
(c) The *double* of a graph G consists of two copies of G with edges joining the corresponding "mirror" vertices. More precisely, if $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_n\}$ is the set of vertices and E the set of edges, then the double of the graph G is given by $G_1 = (V_1, E_1)$, where

$$V_1 = \{v_1, v_2, \ldots, v_n, v'_1, v'_2, \ldots, v'_n\},$$

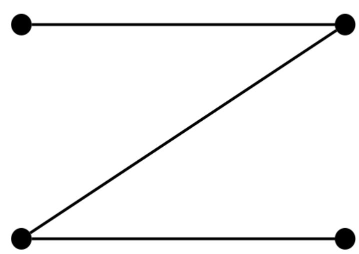
and

$$E_1 = E \cup \{(v'_i, v'_j) | (v_i, v_j) \in E\} \cup \{(v_i, v'_i), \forall i\}.$$

Here is an example,



Draw the double of the following graph:



(d) Now suppose that G_1 is a bipartite graph, G_2 is the double of G_1, G_3 is the double of G_2, and so on. (Each G_{i+1} has twice as many vertices as G_i). Show that $\forall n \geq 1$, G_n is bipartite.

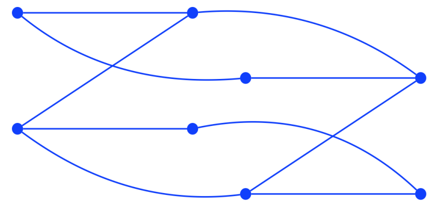
Hint: Use induction on n.

Solution:

(a) Since G is bipartite, each edge connects one vertex in L with a vertex in R. Since each edge contributes equally to $\sum_{v \in L} \deg(v)$ and $\sum_{v \in R} \deg(v)$, we see that these two values must be equal.

(b) By part (a), we know that $\sum_{v \in L} \deg(v) = \sum_{v \in R} \deg(v)$. Thus $|L| \cdot s = |R| \cdot t$. A little algebra gives us the desired result.

(c) The double of the graph in part (c) is as shown below:



(d) We use induction. Let $P(n)$ be the proposition that G_n is bipartite. The base case is when $n = 1$. We see that $P(1)$ must be true since G_1 is bipartite by assumption. Now suppose that for $k \geq 1$, $P(k)$ holds. We see that the graph G_{k+1} consists of two subgraphs, each having the same structure as G_k, except the edges joining the corresponding vertices of the two subgraphs. Ignore these extra edges, i.e, the edges joining the corresponding vertices of the two subgraphs. Since $P(k)$ is true, we can label the two subgraphs into disjoint sets $\{L_1, R_1\}$ and $\{L_2, R_2\}$. Then we can define new sets $L = \{L_1, R_2\}$ and $R = \{R_1, L_2\}$ that are disjoint. Every edge connects a vertex from L_1 to R_1 and from L_2 to R_2, so it connects from L to R. Now considering the extra edges that we ignored, we see that each such edge connects a vertex from L_1 to a vertex in L_2 and a vertex in R_1 to a vertex in R_2. Hence, every edge connects from L to R. Thus, the graph G_{k+1} is bipartite.

8 The Last Digit

In each case show your work and justify your answers.

(a) If $9k+5$ and $2k+1$ have the same last digit for some natural number k, find the last digit of k.

(b) If $S = \sum_{i=1}^{19} i!$, then find the last digit of S^2.

(c) Denote the last digit of a natural number a by b. Show that the last digit of a^n is the same as the last digit of b^n where is $n \geq 1$ is a natural number.

(d) Inspired by part (c), show that the last digit of a^{4k+1} for all natural numbers k is the same as the last digit of a. [Euler's Theorem is not allowed.]

Solution:

(a) We have

$$9k+5 \equiv 2k+1 \pmod{10},$$
$$7k \equiv -4 \pmod{10},$$
$$7k \equiv 6 \pmod{10}.$$

Now since gcd(7,10)=1, 7 has a (unique) inverse mod 10, and since $7 \times 3 = 21 \equiv 1 \pmod{10}$ the inverse is 3. We multiply both sides of $7k \equiv 6 \pmod{10}$ by 3:

$$k \equiv 18 \equiv 8 \pmod{10}.$$

Hence, the last digit of k is 8.

(b) Note that for $n \geq 5$:

$$n! = \left(\prod_{i=6}^{n} i\right) \times 5! = \left(\prod_{i=6}^{n} i\right) \times 120 \equiv 0 \pmod{10}.$$

So we have:

$$S = \sum_{i=1}^{19} i! = 1! + 2! + 3! + 4! + \sum_{i=5}^{19} i! = 1 + 2 + 6 + 24 + 0 \equiv 3 + 0 \pmod{10}.$$

Then, for S^2:

$$S^2 \equiv 9 \pmod{10}.$$

Hence, the last digit of S^2 is 9.

(c) By definition we have:

$$a \equiv b \pmod{10}.$$

From Theorem 6.1 we have: $a \times a \equiv b \times b \pmod{m}$. If we repeat this $n-1$ times then we get:

$$a^n \equiv b^n \pmod{10}.$$

Thus, the last digit of a^n is the same as the last digit of b^n.

(d) Since we only need the last digit of a to determine the last digit of a^n, we investigate this for all possible last digits of b, i.e. $\{0,1,2,3,4,5,6,7,8,9\}$, when they are raised to the power n.

b	0	1	2	3	4	5	6	7	8	9
$b^2 \pmod{10}$	0	1	4	9	6	5	6	9	4	1
$b^3 \pmod{10}$	0	1	8	7	4	5	6	3	2	9
$b^4 \pmod{10}$	0	1	6	1	6	5	6	1	6	1
$b^5 \pmod{10}$	0	1	2	3	4	5	6	7	8	9

As we can see for b^5 we get the same last digit as b. As a result, b^6 is the same as b^2, b^7 is the same as b^3, and so on.

Hence, for any natural number k, and $0 \leq \ell \leq 3$, $b^{4k+\ell} \equiv b^{\ell} \pmod{10}$.

So for $\ell = 1$:

$$b \equiv b^{4k+1} \pmod{10}.$$

And from part (c) we conclude:

$$a \equiv a^{4k+1} \pmod{10},$$

where b is the last digit of a.

9 Can You Invert It?

State whether each of the following functions f have a well-defined inverse or not. Recall that a function has an inverse if, for every element in the codomain, there exists exactly one element in the domain that maps to it; that is, the function is onto (surjective) and one-to-one (injective). If it does, provide the inverse function f^{-1}. If it does not, explain if it violates the onto condition, one-on-one condition, or both, and justify your response.

(a) $f : \mathbb{R} \to \mathbb{R},\ f(x) = 3x - 12$

(b) $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2 + 1$

(c) $f : \mathbb{R} \to \mathbb{R},\ f(x) = 3x^3 - 12x$

(d) $f : \mathbb{R}^+ \to \mathbb{R}^+,\ f(x) = \sqrt{x+1}$, where $\mathbb{R}^+$ denotes the positive reals

(e) $f : \mathbb{R}^+ \to \mathbb{N},\ f(x) = \lfloor x \rfloor$

(f) $f : \mathbb{R}^3 \to \mathbb{R}^3,\ f(x) = Ax$, where $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

(g) $f : \mathbb{R}^3 \to \mathbb{R}^3,\ f(x) = Ax$, where $A = \begin{bmatrix} 5 & 2 & 4 \\ 1 & 0 & 2 \\ 3 & 2 & 0 \end{bmatrix}$

Solution:

(a) Has an inverse. $f^{-1}(x) = (1/3)x + 4$

(b) No inverse. Violates onto condition: e.g. no real number maps to 0. Violates one-to-one condition: e.g. 2 is mapped to by both 1 and -1.

(c) No inverse. f is onto, but violates one-to-one condition: e.g. f has three zeros.

(d) No inverse. f is one-to-one, but violates onto condition: no positive real number maps to any real number less than 1.

(e) No inverse. f is onto but violates one-to-one condition: e.g. both 1.1 and 1.2 map to 1.

(f) Has an inverse (note that this is just a permutation matrix). Inverse function is exactly same as original function, i.e. $f^{-1} = f$.

(g) No inverse. Violates onto condition: anything not in the span of the columns of A is not mapped to, e.g. the vector $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^T$. Violates one-to-one condition: e.g. anything of the form $k \cdot \begin{bmatrix} 2 & -3 & 0 \end{bmatrix}^T$ maps to 0.

10 Make Your Own Question

You must make your own question on this week's material and solve it.

11 Homework Process and Study Group

You must describe your homework process and study group in order to receive credit for this question.