PROBLEM 1

Prove that, for all $n \in \mathbb{N}$,

$$2903^n - 803^n - 464^n + 261^n \text{ is divisible by } 1897$$

Claim: $\forall n \in \mathbb{N}$ $\; 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Claim: $\forall n \in \mathbb{N}$ $\quad 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Observe : $\quad 1897 = 7 \times 271 \quad$ prime

Claim: $\forall n \in \mathbb{N}$ $\quad 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Observe : $\quad 1897 = 7 \times 271$ $\quad$ prime

$$2903 \equiv 5 \pmod 7 \qquad\qquad 2903 \equiv 193 \pmod{271}$$
$$803 \equiv 5 \pmod 7 \qquad\qquad 803 \equiv 261 \pmod{271}$$
$$464 \equiv 2 \pmod 7 \qquad\qquad 464 \equiv 193 \pmod{271}$$
$$261 \equiv 2 \pmod 7 \qquad\qquad 261 \equiv 261 \pmod{271}$$

Claim: $\forall n \in \mathbb{N}$ $\quad 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Observe : $\quad 1897 = 7 \times 271$

prime

$$2903 \equiv 5 \pmod 7 \qquad\qquad 2903 \equiv 193 \pmod{271}$$
$$803 \equiv 5 \pmod 7 \qquad\qquad 803 \equiv 261 \pmod{271}$$
$$464 \equiv 2 \pmod 7 \qquad\qquad 464 \equiv 193 \pmod{271}$$
$$261 \equiv 2 \pmod 7 \qquad\qquad 261 \equiv 261 \pmod{271}$$

Claim: $\forall n \in \mathbb{N}$ $\quad 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Observe : $\quad 1897 = 7 \times 271$ prime

$$2903^n \equiv 5^n \pmod{7} \qquad\qquad 2903^n \equiv 193^n \pmod{271}$$
$$803^n \equiv 5^n \pmod{7} \qquad\qquad 803^n \equiv 261^n \pmod{271}$$
$$464^n \equiv 2^n \pmod{7} \qquad\qquad 464^n \equiv 193^n \pmod{271}$$
$$261^n \equiv 2^n \pmod{7} \qquad\qquad 261^n \equiv 261^n \pmod{271}$$

Claim: $\forall n \in \mathbb{N}$ $\quad 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Observe : $\quad 1897 = 7 \times 271$

prime

$$\underbrace{\begin{aligned} 2903^n &\equiv 5^n \pmod 7 \\ 803^n &\equiv 5^n \pmod 7 \\ 464^n &\equiv 2^n \pmod 7 \\ 261^n &\equiv 2^n \pmod 7 \end{aligned}}$$

$$\Downarrow$$

$$7 \mid 2903^n - 803^n - 464^n + 261^n$$

$$\underbrace{\begin{aligned} 2903^n &\equiv 193^n \pmod{271} \\ 803^n &\equiv 261^n \pmod{271} \\ 464^n &\equiv 193^n \pmod{271} \\ 261^n &\equiv 261^n \pmod{271} \end{aligned}}$$

$$\Downarrow$$

$$271 \mid 2903^n - 803^n - 464^n + 261^n$$

Claim: $\forall n \in \mathbb{N}$ $\quad 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

Proof: (by modular arithmetic)

Observe : $\quad 1897 = 7 \times 271$ $\quad$ prime

$$2903^n \equiv 5^n \pmod 7 \qquad\qquad 2903^n \equiv 193^n \pmod{271}$$

$$803^n \equiv 5^n \pmod 7 \qquad\qquad 803^n \equiv 261^n \pmod{271}$$

$$464^n \equiv 2^n \pmod 7 \qquad\qquad 464^n \equiv 193^n \pmod{271}$$

$$261^n \equiv 2^n \pmod 7 \qquad\qquad 261^n \equiv 261^n \pmod{271}$$

$$\Longrightarrow \quad 7 \times 271 \mid 2903^n - 803^n - 464^n + 261^n . \qquad \blacksquare$$

PROBLEM 1 [15 points]

Identifying the application of congruence — 3 pts

Identifying the need for $1897 = 271 \times 7$ — 4 pts

Correctly computing congruences — 4 pts

__________ n^{th} power of congruences — 1 pts

Adding congruences and finishing the proof — 3 pts

PROBLEM 2

For all $n \geq 2$

$$n \text{ is prime} \iff (n-1)! \equiv -1 \pmod{n}$$

Wilson's Theorem

Claim: $\forall n \geq 2$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Claim : $\forall n \geq 2 \quad n$ is prime $\iff (n-1)! \equiv -1 \pmod{n}$

$n = 2 \qquad (2-1)! \equiv -1 \pmod{2}$ is true

$n = 3 \qquad (3-1)! \equiv -1 \pmod{3}$ is true

So, let's assume $n \geq 4$.

Claim: $\forall n \geq 4$ n is prime $\iff (n-1)! \equiv -1 \pmod{n}$

Claim: $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Suppose n is prime.

Claim: $\forall n \geq 4$ n is prime $\iff (n-1)! \equiv -1 \pmod{n}$

Suppose n is prime.

Idea: $(n-1)! = 1 \times 2 \times 3 \times \cdots \times (n-2) \times (n-1)$

each of these has a unique inverse $(\bmod\ n)$ in $\{2, 3, \ldots, n-2\}$

Claim : $\forall n \geq 4$ n is prime $\iff (n-1)! \equiv -1 \pmod{n}$

Suppose n is prime.

Idea: $(n-1)! = 1 \times 2 \times 3 \times \cdots \times (n-2) \times (n-1)$

each of these has a unique inverse $\pmod{n}$ in $\{2, 3, \ldots, n-2\}$

Then, $\underbrace{1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-2)}_{\text{pair up with inverses}} \cdot (n-1) \equiv n-1 \pmod{n}$

$\equiv -1 \pmod{n}.$

Claim: $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \dots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \dots, (n-2)\}$ if n is prime.

Claim: $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \cdots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \cdots, (n-2)\}$ if n is prime.

Proof of Lemma: $\gcd(r, n) = 1 \Longrightarrow$ inverse exists

$\Rightarrow \exists\, r'$ s.t. $rr' \equiv 1 \pmod{n}$

Claim: $\forall n \geq 4$ $\quad n$ is prime $\iff (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \cdots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \cdots, (n-2)\}$ if n is prime.

Proof of Lemma: $\gcd(r, n) = 1 \implies$ inverse exists

$\implies \exists\, r'$ s.t. $\quad rr' \equiv 1 \pmod{n}$

Then, $r' \pmod{n} \in \{2, 3, \cdots, (n-2)\}$ is the desired inverse.

from division theorem

Claim: $\forall n \geq 4$ n is prime $\iff (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \dots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \dots, (n-2)\}$ if n is prime.

Proof of Lemma: $\gcd(r, n) = 1 \implies$ inverse exists

$\implies \exists\, r'$ s.t. $rr' \equiv 1 \pmod{n}$

Then, $r' \pmod{n} \in \{2, 3, \dots, (n-2)\}$ is the desired inverse.

from division theorem

Note: $r' \pmod{n} \neq 1$ and $r' \pmod{n} \neq n-1$.

Claim: $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \cdots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \cdots, (n-2)\}$ if n is prime.

Proof of Lemma: Why unique?

Claim: $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \cdots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \cdots, (n-2)\}$ if n is prime.

Proof of Lemma: Why unique?

If $\exists$ distinct $r', r'' \in \{1, 2, \cdots, (n-1)\}$ that are inverses $\pmod{n}$ of r, then

$$r \cdot r' \equiv 1 \pmod{n} \quad \text{and}$$

$$r \cdot r'' \equiv 1 \pmod{n}$$

$$\Rightarrow \quad r \cdot (r' - r'') \equiv 0 \pmod{n}$$

Claim : $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

Lemma: Each $r \in \{2, 3, \cdots, (n-2)\}$ has a unique inverse $\pmod{n}$ in $\{2, 3, \cdots, (n-2)\}$ if n is prime.

Proof of Lemma: Why unique?

If $\exists$ distinct $r', r'' \in \{1, 2, \cdots, (n-1)\}$ that are inverses $\pmod{n}$ of r, then

$$r \cdot r' \equiv 1 \pmod{n}$$ and
$$r \cdot r'' \equiv 1 \pmod{n}$$

$$\Rightarrow \quad r \cdot (r' - r'') \equiv 0 \pmod{n}$$

Not possible for prime n

$\blacksquare$

Claim : $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

If n is not prime

Then, $\exists\, q \in \{2, 3, \dots, (n-2)\}$ such that $q \mid n$.

Claim: $\forall n \geq 4$ n is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

If n is not prime

Then, $\exists\ q \in \{2, 3, \dots, (n-2)\}$ such that $q \mid n$.

Suppose, for contradiction, that $(n-1)! \equiv -1 \pmod{n}$.

$$\Rightarrow n \mid (n-1)! + 1$$

$$\Rightarrow q \mid (n-1)! + 1$$

Claim : $\forall n \geq 4 \quad n$ is prime $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

If n is not prime

Then, $\exists\, q \in \{2, 3, \dots, (n-2)\}$ such that $q \mid n$.

Suppose, for contradiction, that $(n-1)! \equiv -1 \pmod{n}$.

$$\Rightarrow n \mid (n-1)! + 1$$

$$\Rightarrow q \mid (n-1)! + 1$$

Contradiction

However, $\quad q \mid (n-1)!$

$\blacksquare$

PROBLEM 2 [15 points]

Pairing argument for prime n ——— 8 pts

Using pairing lemma to prove theorem ——— 3 pts

Proof for non-prime n ——— 4 pts

PROBLEM 3

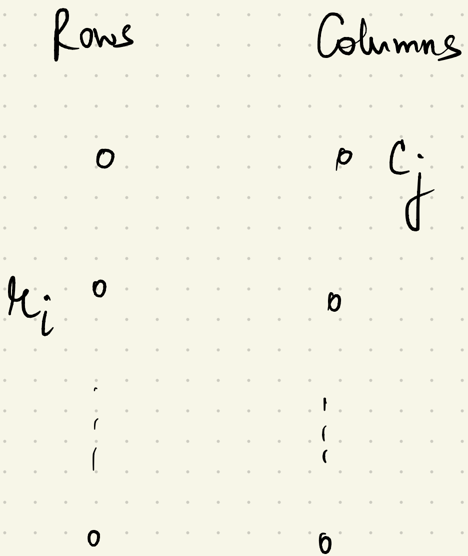
Every doubly stochastic matrix is a convex combination of permutation matrices.

Birkhoff - von Neumann Theorem

Let A be any doubly stochastic matrix.

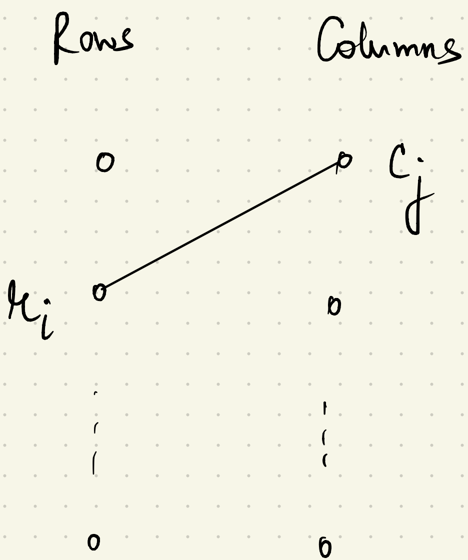
Let A be any doubly stochastic matrix.

Construct a bipartite graph $G = (R \cup C, E)$



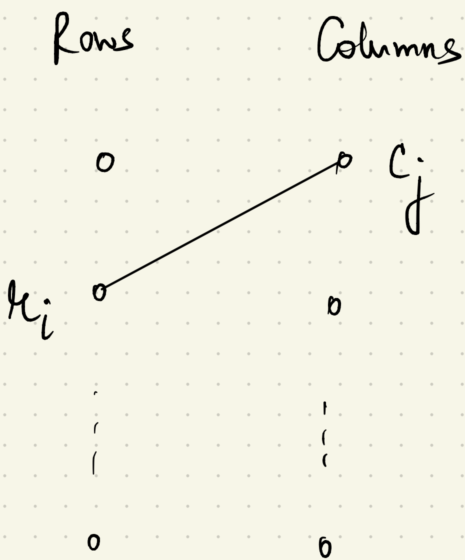
Let A be any doubly stochastic matrix.

Construct a bipartite graph $G = (R \cup C, E)$



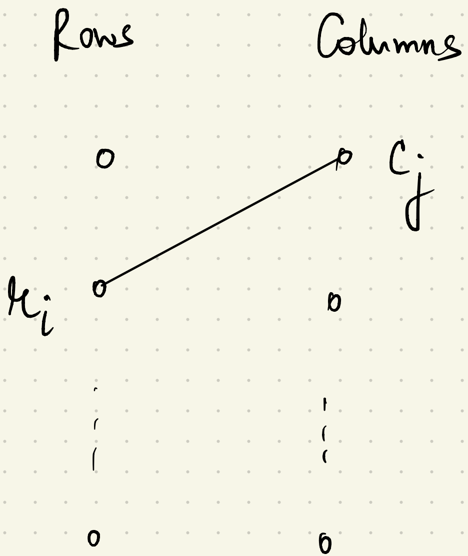
Edge (r_i, c_j) exists if $A_{ij} > 0$.

Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.



Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.

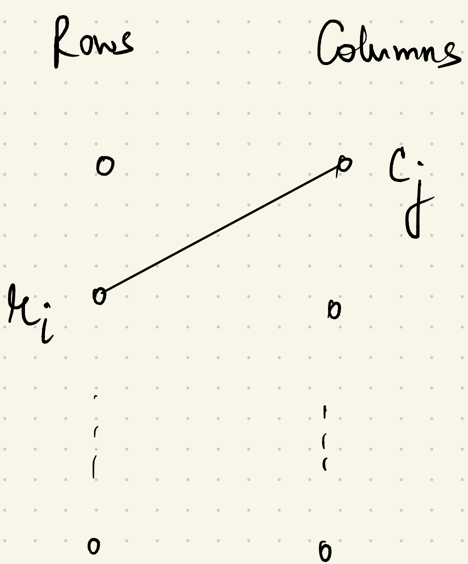
Proof of claim: Using Hall's theorem.



Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.

Proof of claim: Using Hall's theorem.

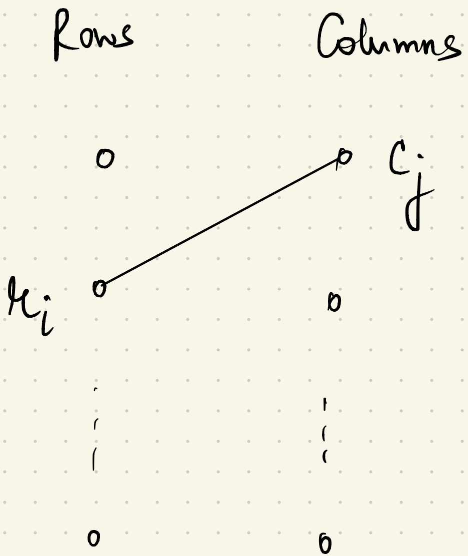
Consider any subset S of rows.



Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.

Proof of claim: Using Hall's theorem.

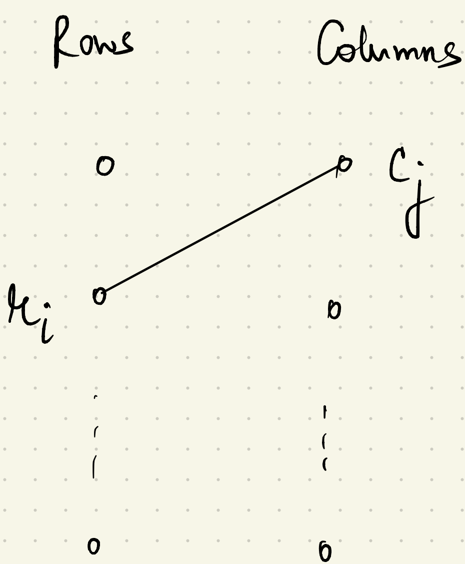
Consider any subset S of rows.



Sum of non zero entries of A across all rows in S $= |S|$

Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.

Proof of claim: Using Hall's theorem.



Consider any subset S of rows.

Sum of nonzero entries of A across all rows in S $= |S|$

If $|N(S)| < |S|$, then

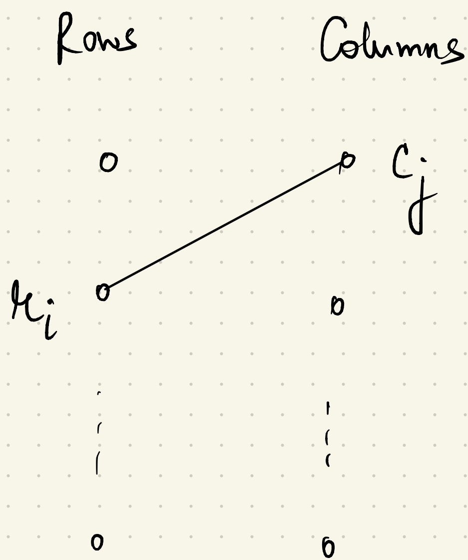
Sum of nonzero entries of A across all column in $N(S) < |S|$

Contradiction.

Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.

Proof of claim: Using Hall's theorem.

Consider any subset S of rows.



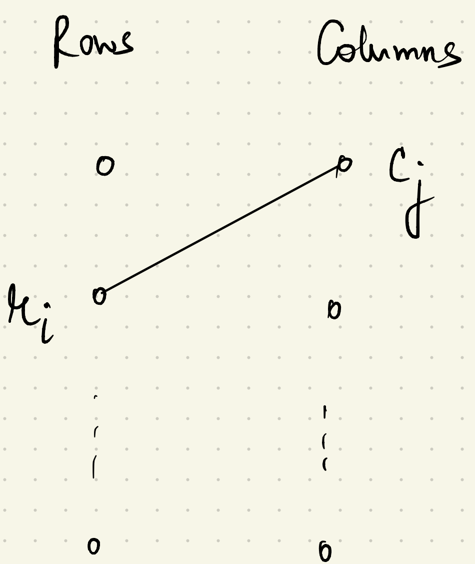
$$|N(S)| \geq |S|.$$

$\Rightarrow$ Perfect matching exists

Claim: Graph $G = (R \cup C, E)$ admits a perfect matching.

Proof of claim: Using Hall's theorem.

Consider any subset S of rows.



$$|N(S)| \geq |S|.$$

$\Longrightarrow$ Perfect matching exists

$\Updownarrow$

Permutation matrix

Let

λ = smallest nonzero entry in A

P = permutation matrix guaranteed by claim

$A' = A - \lambda P$ ("peeling off" P)

Let λ = smallest non zero entry in A

P = permutation matrix guaranteed by claim

$A' = A - \lambda P$ ("peeling off" P)

Observe: (1) A' has equal row and column sums

(2) Hall's theorem can still be applied to A'

(3) # zero entries in A' > # zero entries in A.

Let λ = smallest nonzero entry in A

P = permutation matrix guaranteed by claim

$A' = A - \lambda P$ ("peeling off" P)

Observe: ① A' has equal row and column sums

② Hall's theorem can still be applied to A'

③ # zero entries in A' > # zero entries in A.

The "peeling off" procedure must terminate in $\leq n^2$ steps. ∎

PROBLEM 3 [15 points]

Construction of bipartite graph ——— 2 pts

Proving existence of perfect matching ——— 5 pts

Explaining the "peeling off" procedure ——— 3 pts

Showing that Hall's theorem still applies on the remaining matrix ——— 2 pts

Arguing Termination of this procedure ——— 3 pts

PROBLEM 4

(a) Given distinct stable matchings P, Q.

If all men weakly prefer P, then all women weakly prefer Q.

(b) If each man points to his more preferred partner and each woman points to her less preferred partner, then if m points at w, then w points at m

(c) Show that a woman can strategically manipulate under the men-proposing DA algorithm.

Claim: If all men weakly prefer P, then all women weakly prefer Q.

Claim: If all men weakly prefer P, then all women weakly prefer Q.

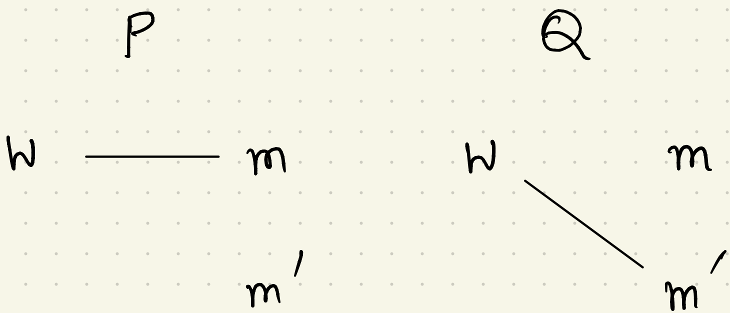
Proof: (by contradiction)

Suppose woman w strictly prefers P over Q.

Claim: If all men weakly prefer P, then all women weakly prefer Q.

Proof: (by contradiction)

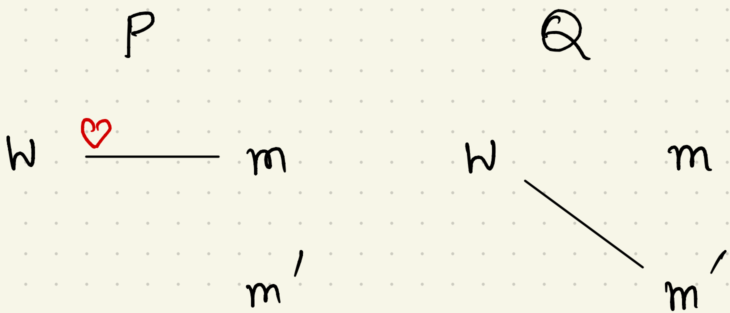
Suppose woman w strictly prefers P over Q.



Claim: If all men weakly prefer P, then all women weakly prefer Q.

Proof: (by contradiction)

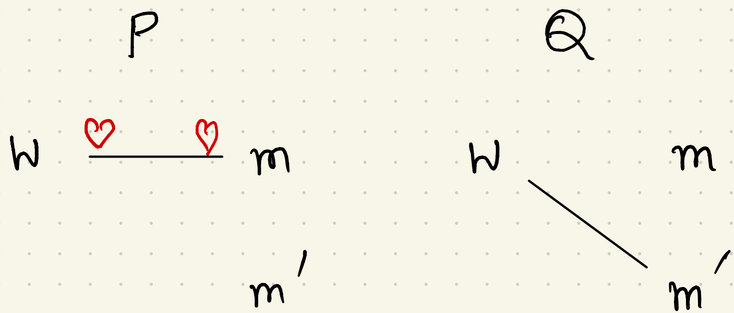
Suppose woman w strictly prefers P over Q.



Claim: If all men weakly prefer P, then all women weakly prefer Q.

Proof: (by contradiction)

Suppose woman w strictly prefers P over Q.

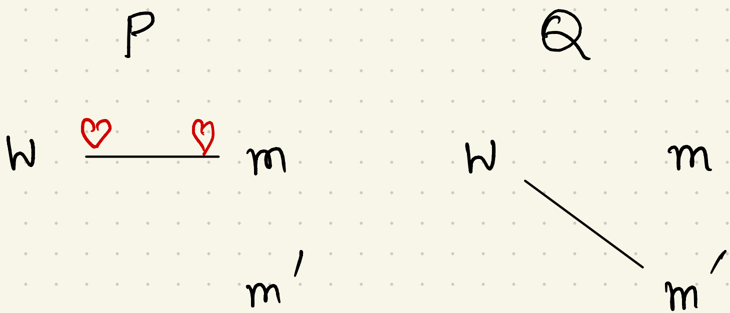


m must strictly prefer P over Q

Claim: If all men weakly prefer P, then all women weakly prefer Q.

Proof: (by contradiction)

Suppose woman w strictly prefers P over Q.



m must strictly prefer P over Q

$\Rightarrow$ (m, w) block Q.

$\blacksquare$

PROBLEM 4(a) [5 points]

Identifying proof by contradiction. —— 1 pt

Identifying the correct conditions for P and Q ← 3 pts

Identifying the blocking pair —— 1 pt

Claim: Men point to more preferable partner between P and Q.
Women " less " " "

Then, if m points to w, then w points to m.

Claim: Men point to more preferable partner between P and Q.
Women " less " " "
Then, if m points to w, then w points to m.

Proof: Only need to consider men/women with different partners in P and Q.

Claim: Men point to more preferable partner between P and Q.
Women " less " " "
Then, if m points to w, then w points to m.

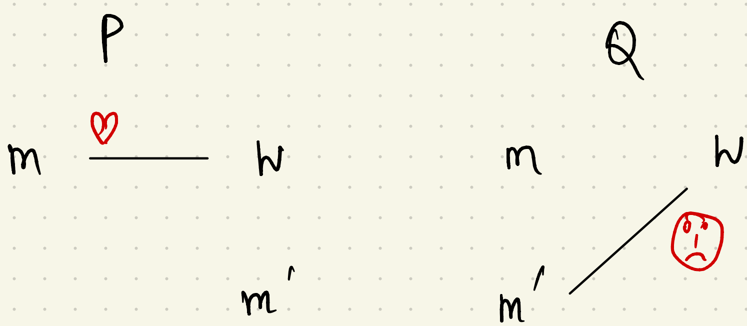
Proof: Only need to consider men/women with different partners in P and Q.

Suppose $m \rightarrow w$ but $w \rightarrow m'$.

Claim: Men point to more preferable partner between P and Q.
Women " less " " "
Then, if m points to w, then w points to m.

Proof: Only need to consider men/women with different partners in P and Q.

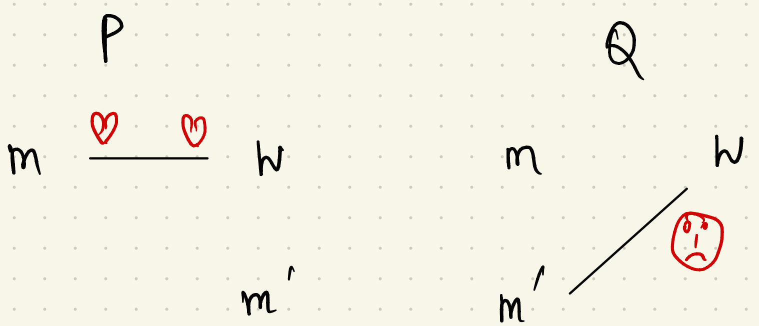
Suppose $m \longrightarrow w$ but $w \longrightarrow m'$.



Claim: Men point to more preferable partner between P and Q.
Women " less " " "
Then, if m points to w, then w points to m.

Proof: Only need to consider men/women with different partners in P and Q.

Suppose $m \to w$ but $w \to m'$.



$\Rightarrow (m, w)$ block Q.

∎

PROBLEM 4(b) [5 points]

Identifying proof by contradiction —————— 1 pt

Identifying the correct conditions for P and Q — 3 pts

Identifying the blocking pair —————— 1 pt

Claim: Strategic manipulation is possible under DA algorithm.

Claim: Strategic manipulation is possible under DA algorithm.

Proof:

$w_3 \succ w_1 \succ w_2$ m_1 $\qquad$ w_1 : $m_1 \succ m_2 \succ m_3$

$w_1 \succ w_3 \succ w_2$ m_2 $\qquad$ w_2 $m_1 \succ m_2 \succ m_3$

$w_1 \succ w_2 \succ w_3$ m_3 $\qquad$ w_3 $m_2 \succ m_1 \succ m_3$

DA matching for original preferences: $(m_1, w_3), (m_2, w_1), (m_3, w_2)$

Claim: Strategic manipulation is possible under DA algorithm.

Proof:

$w_3 \succ w_1 \succ w_2$ m_1 w_1: $\cancel{m_1 \succ m_2 \succ m_3}$ $m_1 \succ m_3 \succ m_2$

$w_1 \succ w_3 \succ w_2$ m_2 w_2 $m_1 \succ m_2 \succ m_3$

$w_1 \succ w_2 \succ w_3$ m_3 w_3 $m_2 \succ m_1 \succ m_3$

DA matching for original preferences: $(m_1, w_3), (m_2, w_1), (m_3, w_2)$

——— modified ———: $(m_1, w_1), (m_2, w_3), (m_3, w_2)$

PROBLEM 4(c) [5 points]

Construction of original and modified instances — 4 pts

Explaining how the modified instance is better — 1 pt