# COL 202: DISCRETE MATHEMATICAL STRUCTURES

## MAJOR EXAM SOLUTIONS

# PROBLEM 1(a)

(a) **[5 points]** Prove or disprove: Every graph $G = (V, E)$ has a bipartite subgraph with at least $|E|/2$ edges.

Proof by probabilistic argument

Assign each vertex to the "left" set w.p. $1/2$ and "right" w.p. $1/2$. independently of other vertices.

Fix any edge $e = \{u, v\}$.

Define $X_e = \begin{cases} 1 & \text{if edge } e \text{ is crossing} \\ 0 & \text{o/w} \end{cases}$

# PROBLEM 1(a)

(a) **[5 points]** Prove or disprove: Every graph $G = (V, E)$ has a bipartite subgraph with at least $|E|/2$ edges.

$\Pr(X_e = 1) = \Pr(u \text{ on left and } v \text{ on right or vice versa})$

disjoint events $= \Pr(u \text{ left}, v \text{ right}) + \Pr(u \text{ right}, v \text{ left})$

independence $= \Pr(u \text{ left}) \cdot \Pr(v \text{ right}) + \Pr(u \text{ right}) \cdot \Pr(v \text{ left})$

$= \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}.$

Define $X = \sum_{e \in E} X_e$

Then $\mathbb{E}[X]$ is expected number of crossing edges.

# PROBLEM 1(a)

(a) **[5 points]** Prove or disprove: Every graph $G = (V, E)$ has a bipartite subgraph with at least $|E|/2$ edges.

By linearity of expectation:

$$\mathbb{E}[X] = \sum_e \mathbb{E}[X_e]$$

$$= \frac{|E|}{2}.$$

$X$ is a random variable whose expectation is $\frac{|E|}{2}$.

$\Rightarrow \Pr\left(X \geq \frac{|E|}{2}\right) > 0$ ← probabilistic method

$\Rightarrow \exists$ a vertex partition with at least $\frac{|E|}{2}$ crossing edges. $\blacksquare$

# PROBLEM 1(b)

(b) [**10 points**] Prove or disprove: Every graph $G = (V, E)$ where $|V|$ is even and $|E| > 0$ has a bipartite subgraph with strictly more than $|E|/2$ edges.

Proof by probabilistic argument.

Let $|V| = 2n$.

We will divide $V$ into two sets, say $A$ and $B$, of size $n$ each

No. of equipartitions $= {}^{2n}C_n$.

Fix an edge $e = \{u, v\}$.

# PROBLEM 1 (b)

(b) **[10 points]** Prove or disprove: Every graph $G = (V, E)$ where $|V|$ is even and $|E| > 0$ has a bipartite subgraph with strictly more than $|E|/2$ edges.

Let us count the number of partitions in which $e$ is crossing

(I) If $u \in A$ and $v \in B$

picking $n-1$ vertices other than $u$ in the set $A$

The number of such partitions is ${}^{2n-2}C_{n-1}$.

(II) If $u \in B$ and $v \in A$

The number of such partitions is ${}^{2n-2}C_{n-1}$.

# PROBLEM 1(b)

(b) **[10 points]** Prove or disprove: Every graph $G = (V, E)$ where $|V|$ is even and $|E| > 0$ has a bipartite subgraph with strictly more than $|E|/2$ edges.

Define $X_e$ as in part (a).

Suppose each equipartition is chosen uniformly at random.

$$\Pr(X_e = 1) = \frac{2 \cdot {}^{2n-2}C_{n-1}}{{}^{2n}C_n} = \frac{n}{2n-1} > \frac{1}{2}.$$

Desired bipartite subgraph exists by the same argument as in part (a).

$\boxed{\text{Ly}}$

# PROBLEM 1(a) [5 pts]

* Mention "We will prove the statement." ——— 0.5 pts
* Mention proof technique. ——— 0.5 pts
* Mention the experiment (random partitioning) ——— 0.5 pts
* Correctly define indicator random variables and their sum ——— 1 pt
* Correctly compute expected values ——— 1 pt
* Apply probabilistic method to finish the proof ——— 1.5 pts

# PROBLEM 1(b) [10 pts]

* Mention "We will prove the statement." ——— 1 pt
* Mention proof technique. ——— 1 pt
* Mention the experiment (random partitioning) ——— 1 pt
* Correctly define indicator random variables and their sum ——— 1 pt
* Correctly compute expected values ——— 4 pts

  (should be <u>strictly more</u> than $|E|/2$)
* Apply probabilistic method to finish the proof ——— 2 pts

# PROBLEM 2 (a)

**Problem 2 [6+4+5=15 points]**
For any $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, \ldots, n\}$. We will assume that $n \geqslant 3$.

A permutation $\sigma$ of $[n]$ is said to be *concave* if, for every $i \in \{2, 3, \ldots, n-1\}$, $\sigma(i) \geqslant \frac{\sigma(i-1)+\sigma(i+1)}{2}$. For example, when $n = 4$, the permutation $(1, 2, 3, 4)$ is concave but the permutation $(4, 1, 3, 2)$ is not.

A permutation $\sigma$ of $[n]$ is said to be *bitonic* if there exists some $i \in [n]$ such that

- for all $j \in [n-1]$ such that $j < i$, $\sigma(j) < \sigma(j+1)$, and
- for all $k \in [n-1]$ such that $k \geqslant i$, $\sigma(k) > \sigma(k+1)$.

For example, when $n = 4$, the permutation $(1, 2, 3, 4)$ is bitonic but the permutation $(4, 1, 3, 2)$ is not.

# PROBLEM 2 (a)

(a) **[6 points]** Prove or disprove: Every concave permutation is bitonic.

Proof by contradiction.

Let $\sigma$ be any concave permutation of $[n]$.

Let $i^* \in [n]$ be such that $\sigma(i^*) = n$.

Suppose, for contradiction, that $\sigma$ is not bitonic. Then,

(i) either $\exists\, j < i^*$ such that $\sigma(j) > \sigma(j+1)$

(ii) or $\exists\, k \geq i^*$ such that $\sigma(k) < \sigma(k+1)$.

# PROBLEM 2 (a)

(a) **[6 points]** Prove or disprove: Every concave permutation is bitonic.

(i) $\exists\, j < i^*$ such that $\sigma(j) > \sigma(j+1)$

Let $j^*$ be the closest index to $i^*$ that satisfies case (i).

Observe that $j^* \neq i^* - 1$; thus $j^* < i^* - 1$.

Then, $\sigma(j^*) > \sigma(j^*+1)$ and $\sigma(j^*+1) < \sigma(j^*+2)$.

well-defined

$\Longrightarrow$ Concavity violated at $j^*+1$.

Contradiction!

# PROBLEM 2 (a)

(a) **[6 points]** Prove or disprove: Every concave permutation is bitonic.

(ii) $\exists\, k \geq i^*$ such that $\sigma(k) < \sigma(k+1)$.

Let $k^*$ be the index closest to $i^*$ that satisfies case (ii).

Then, $k^* \neq i^*$, and thus $k^* > i^*$.

We have $\sigma(k^*) < \sigma(k^*+1)$ and $\sigma(k^*) < \sigma(k^*-1)$

well-defined

$\Rightarrow$ concavity violated at $k^*$.

Contradiction.

Therefore, $\sigma$ must be bitonic.

$\boxtimes$

# PROBLEM 2 (b)

(b) [**4 points**] Identify all concave permutations of the set [5]. No explanation is required.

| | |
|---|---|
| 1 2 3 4 5 | 5 4 3 2 1 |
| 1 3 4 5 2 | 2 5 4 3 1 |
| 1 3 5 4 2 | 2 4 5 3 1 |
| 1 5 4 3 2 | 2 3 4 5 1 |

# PROBLEM 2 (c)

(c) [**5 points**] How many bitonic permutations of $[n]$ are there? Explain your reasoning.

There are $2^{n-1}$ bitonic permutations

Observe:

① 1 must always be at one of extremes of any bitonic permutation

② After eliminating 1, the remaining permutation of $\{2, 3, \ldots, n\}$ is also bitonic.

Recurrence: $f(n) = 2 f(n-1) \implies f(n) = 2^{n-1}$.

Verify by induction using above observations.

# PROBLEM 2(a) [6 pts]

* Mention "We will prove the statement." ——— 1 pt
* Mention proof technique. ——— 1 pt
* Correctly derive contradiction for the left of the peak ——— 2 pts
* Correctly derive contradiction for the right of the peak ——— 2 pts

# PROBLEM 2(b) [4 pts]

0.5 pt for each correct answer

− 0.5 pt for each incorrect answer

Minimum marks : 0/4.

(even if the solution consists of more incorrect answers than correct ones)

# PROBLEM 2(C) [5 pts]

* Mention the correct answer ———— 1 pt
* Making the relevant observations ———— 1 pt
* Correct recurrence ———— 2 pts
* Verify via induction ———— 1 pt

# PROBLEM 3 (a)

(a) **[2 points]** Prove that for any non-negative random variable $X$,

$$\Pr(X \geqslant 1) \leqslant \mathbf{E}[X].$$

This result is a special case of what's called Markov's inequality: $\mathbb{P}r\,(X \geq k) \leq \frac{\mathbb{E}[X]}{k}$

For any $k \geq 0$,

if $\mathbb{P}r\,(X \geq k) = p$, then $\mathbb{E}[X] \geq k \cdot p$.

The desired inequality follows when $k=1$.

$\blacksquare$

# PROBLEM 3 (b)

(b) **[13 points]** Given any $n \in \mathbb{N}$, consider a *random graph* $G = (V, E)$ on $n$ vertices in which for any pair of vertices $u, v \in V$, the edge $\{u, v\}$ exists with probability $1/2$ independently of any other pair of vertices.

An *independent set* of a graph is a subset of vertices in which no two vertices are adjacent.

Show that the probability that the largest independent set of the random graph $G$ is larger than $\lceil 3\log_2 n + 1\rceil$ is $o\left(n^{-\log_2 n}\right)$, where $o(.)$ stands for little-o notation.

Fix $k = \lceil 3 \log_2 n + 1 \rceil$.

Fix any subset of vertices $S \subseteq V$ such that $|S| = k$

$$\mathbb{P}(S \text{ is independent}) = \mathbb{P}(\text{no edge between any of the } {}^kC_2 \text{ pairs of vertices in } S)$$

$$= \left(\frac{1}{2}\right)^{{}^kC_2} \quad \text{——} \quad 1$$

# PROBLEM 3 (b)

(b) **[13 points]** Given any $n \in \mathbb{N}$, consider a *random graph* $G = (V, E)$ on $n$ vertices in which for any pair of vertices $u, v \in V$, the edge $\{u, v\}$ exists with probability $1/2$ independently of any other pair of vertices.

An *independent set* of a graph is a subset of vertices in which no two vertices are adjacent.

Show that the probability that the largest independent set of the random graph $G$ is larger than $\lceil 3 \log_2 n + 1 \rceil$ is $o\left(n^{-\log_2 n}\right)$, where $o(.)$ stands for little-o notation.

Let $S_1, S_2, \ldots, S_{{}^nC_k}$ be all $k$-sized subsets of vertices.

Let $X_i = \begin{cases} 1 & \text{if } S_i \text{ is independent} \\ 0 & \end{cases}$

Let $X = \sum_{i=1}^{{}^nC_k} X_i$

Then $\mathbb{E}[X] \underset{\substack{\downarrow \\ \text{by linearity of expectation}}}{=} \sum_i \mathbb{E}[X_i] = \sum_i \Pr(X_i = 1) \underset{\substack{\downarrow \\ \text{using (1)}}}{=} {}^nC_k \cdot \left(\frac{1}{2}\right)^{{}^kC_2}$

# PROBLEM 3 (b)

(b) **[13 points]** Given any $n \in \mathbb{N}$, consider a *random graph* $G = (V, E)$ on $n$ vertices in which for any pair of vertices $u, v \in V$, the edge $\{u, v\}$ exists with probability $1/2$ independently of any other pair of vertices.

An *independent set* of a graph is a subset of vertices in which no two vertices are adjacent.

Show that the probability that the largest independent set of the random graph $G$ is larger than $\lceil 3\log_2 n + 1 \rceil$ is $o\left(n^{-\log_2 n}\right)$, where $o(.)$ stands for little-o notation.

$$\mathbb{E}[X] = {}^nC_k \cdot \left(\tfrac{1}{2}\right)^{{}^kC_2}$$

$$\leq n^k \cdot \left(\left(\tfrac{1}{2}\right)^{(k-1)/2}\right)^k \qquad \text{since } {}^nC_k \leq n^k$$

$$\leq \left[n \cdot \left(\tfrac{1}{2}\right)^{\frac{3}{2}\log_2 n}\right]^k \qquad \text{since } k \geq 3\log_2 n$$

$$= \left[n \cdot n^{-3/2}\right]^k \leq n^{-k/2} \quad \text{——— } (2)$$

# PROBLEM 3 (b)

(b) **[13 points]** Given any $n \in \mathbb{N}$, consider a *random graph* $G = (V, E)$ on $n$ vertices in which for any pair of vertices $u, v \in V$, the edge $\{u, v\}$ exists with probability $1/2$ independently of any other pair of vertices.

An *independent set* of a graph is a subset of vertices in which no two vertices are adjacent.

Show that the probability that the largest independent set of the random graph $G$ is larger than $\lceil 3\log_2 n + 1 \rceil$ is $o\left(n^{-\log_2 n}\right)$, where $o(.)$ stands for little-o notation.

From part (a), we have $\Pr(X \geq 1) \leq \mathbb{E}[X]$.

$$\Rightarrow \Pr(X \geq 1) \leq n^{-k/2} \quad \left(\text{from } 2\right)$$

$$= o\left(n^{-\log_2 n}\right). \quad \text{———} \quad 3$$

# PROBLEM 3(b)

(b) **[13 points]** Given any $n \in \mathbb{N}$, consider a *random graph* $G = (V, E)$ on $n$ vertices in which for any pair of vertices $u, v \in V$, the edge $\{u, v\}$ exists with probability $1/2$ independently of any other pair of vertices.

An *independent set* of a graph is a subset of vertices in which no two vertices are adjacent.

Show that the probability that the largest independent set of the random graph $G$ is larger than $\lceil 3\log_2 n + 1 \rceil$ is $o\left(n^{-\log_2 n}\right)$, where $o(.)$ stands for little-o notation.

$\Pr$(size of largest independent set $\geq k$)

same events

$= \Pr$(there exists an independent set of size $\geq k$)

$\leq \Pr$( " " " " $= k$)

(using $A \subseteq B \Rightarrow \Pr(A) \leq \Pr(B)$)

$= \Pr(X \geq 1)$

$= o\left(n^{-\log_2 n}\right)$ from 3 as desired.

# PROBLEM 3 (a) [2 pts]

* Proving the inequality for all $K \geq 0$ ———— 1.5 pt

* Substituting $K=1$ ———— 0.5 pt

# PROBLEM 3 (b) [13 pts]

* Computing expected value of indicator variables ——— 3 pts

* Deriving $o\left(\frac{1}{n^{\lg_2 n}}\right)$ bound on $\Pr(X \geq 1)$ ——— 8 pts

* Finishing the proof by observing that the bound on $\Pr(X \geq 1)$ gives a bound on the desired probability ——— 2 pts

# PROBLEM 4 (a)

(a) **[5 points]** Let $a$, $b$, $c$, $d$, and $m$ be positive integers. Prove or disprove: If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, and $\gcd(c, m) = 1$, then $a \cdot c^{-1} \equiv b \cdot d^{-1} \pmod{m}$, where $c^{-1}$ and $d^{-1}$ are the multiplicative inverses $\pmod{m}$ of $c$ and $d$, respectively.

Proof by using standard properties of congruence.

Observe :

① $\gcd(c, m) = 1$ and $c \equiv d \pmod{m} \Rightarrow \gcd(d, m) = 1$.

② By ①, $c^{-1}$ and $d^{-1}$ are well-defined.

Then,
$$c.(ac^{-1} - bd^{-1}) \pmod{m}$$
$$\equiv acc^{-1} - bcd^{-1} \pmod{m}$$
$$\equiv a.1 - b.1 \pmod{m}$$
$$\equiv a - b \pmod{m}$$

[Note : $c \equiv d \pmod{m}$ and $dd^{-1} \equiv 1 \pmod{m}$
$\Rightarrow cd^{-1} \equiv 1 \pmod{m}$]

# PROBLEM 4 (a)

(a) **[5 points]** Let $a$, $b$, $c$, $d$, and $m$ be positive integers. Prove or disprove: If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, and $\gcd(c, m) = 1$, then $a \cdot c^{-1} \equiv b \cdot d^{-1} \pmod{m}$, where $c^{-1}$ and $d^{-1}$ are the multiplicative inverses $\pmod{m}$ of $c$ and $d$, respectively.

Thus, $c \cdot (ac^{-1} - bd^{-1}) \pmod{m} \equiv a - b \pmod{m} \equiv 0 \pmod{m}$

Since $c$ and $m$ are relatively prime

we have $ac^{-1} - bd^{-1} \equiv 0 \pmod{m}$ as desired.

$\boxtimes$

# PROBLEM 4 (b)

(b) [**5 points**] Let $a$, $b$, $c$, $d$, and $m$ be positive integers such that $b$ and $m$ are relatively prime. Prove or disprove: If $b^a \equiv 1 \pmod{m}$, $b^c \equiv 1 \pmod{m}$, and $d = \gcd(a,c)$, then $b^d \equiv 1 \pmod{m}$. How does your answer change if you are not given that $b$ and $m$ are relatively prime?

Proof by using gcd - spc equivalence and part (a).

$d = \gcd(a,c) \Rightarrow \exists$ integers $\alpha, \beta$ such that $d = \alpha a + \beta c$.

Without loss of generality, $\alpha \geq 0$ (can achieve by adding enough copies of 'a')

Thus, we must have that $\beta \leq 0$.

$$b^a \equiv 1 \pmod{m} \Rightarrow b^{\alpha a} \equiv 1 \pmod{m} \text{ ——— } (1)$$

$$b^c \equiv 1 \pmod{m} \Rightarrow b^{-\beta c} \equiv 1 \pmod{m} \text{ ——— } (2)$$

# PROBLEM 4 (b)

(b) [**5 points**] Let $a$, $b$, $c$, $d$, and $m$ be positive integers such that $b$ and $m$ are relatively prime. Prove or disprove: If $b^a \equiv 1 \pmod{m}$, $b^c \equiv 1 \pmod{m}$, and $d = \gcd(a, c)$, then $b^d \equiv 1 \pmod{m}$. How does your answer change if you are not given that $b$ and $m$ are relatively prime?

Observe that $\gcd(b^{-\beta c}, m) = 1$. This is because

$b^{-\beta c} \equiv 1 \pmod{m}$ and $\gcd(1, m) = 1$. (Do not need to assume that $b, m$ are rel. prime)

By applying part (a), we can divide ① by ② to get

$$b^{\alpha a + \beta c} \equiv 1 \pmod{m}$$

or $b^d \equiv 1 \pmod{m}$ as desired. $\blacksquare$

# PROBLEM 4 (c)

(c) **[5 points]** Let $b$, $p$, and $n$ be positive integers. Prove or disprove: If $p$ is a prime such that $p|(b^n - 1)$, then:

- either $p|(b^d - 1)$ for some proper divisor $d$ of $n$ (a proper divisor of $n$ is any positive divisor of $n$ excluding $n$ itself),
- or $p \equiv 1 \pmod{n}$.

Proof by using Euler's theorem and part (b).

$p$ is prime $\Rightarrow$ $b^{p-1} \equiv 1 \pmod{p}$ by Euler's thm since $\phi(p) = p-1$.

Given $b^n \equiv 1 \pmod{p}$.

Let $d = \gcd(n, p-1)$.

By part (b), $b^d \equiv 1 \pmod{p}$

# PROBLEM 4 (c)

(c) [**5 points**] Let $b$, $p$, and $n$ be positive integers. Prove or disprove: If $p$ is a prime such that $p|(b^n - 1)$, then:

- either $p|(b^d - 1)$ for some proper divisor $d$ of $n$ (a proper divisor of $n$ is any positive divisor of $n$ excluding $n$ itself),
- or $p \equiv 1 \pmod{n}$.

If $d = n$, then $\gcd(n, p-1) = n \Rightarrow n \mid p-1$

$\Rightarrow p \equiv 1 \pmod{n}$.

If $d < n$, $p \mid b^d - 1$ for some divisor $d < n$ of $n$

proper divisor.

$\blacksquare$

# PROBLEM 4 (a) [5 pts]

* Mentioning "We will prove the statement" ——— 0.5 pt
* Observing that $c^{-1}$ and $d^{-1}$ are well-defined ——— 1 pt
* Observing that $c \cdot (ac^{-1} - bd^{-1}) \equiv 0 \pmod{m}$ ——— 2.5 pts
* Using relative primality of $c$ and $m$ to finish the proof ——— 1 pt

# PROBLEM 4 (b) [5 pts]

* Mentioning "We will prove the statement" —— 0.5 pt
* Invoking gcd-spc equivalence and observing that $\alpha \geq 0$ and $\beta \leq 0$ —— 2 pts
* Observing that part (a) can be used to divide the congruences in ① and ② —— 1.5 pts
* Stating that relative primality of $b$ and $m$ is not needed. —— 1 pts

# PROBLEM 4 (c) [5 pts]

* Mentioning "We will prove the statement" —— 0.5 pt

* Using Euler's theorem —— 1 pt

* Using part (b) —— 1.5 pts

* Case analysis for $d=n$ and $d<n$ —— 2 pts