Problem 1 (3 points)

Suppose we have two functions: $f(n) = n^{\sqrt{n}}, g(n) = 2^{n^{2/3}}$. Choose the correct option(s). Explain why.

(a) $f(n) = o(g(n))$, (b) $f(n) = \omega(g(n))$, (c) $f(n) = \Theta(g(n))$, (d) $f(n) = O(g(n))$, (e) $f(n) = \Omega(g(n))$.

(a) $f(n) = o(g(n))$ and (d) $f(n) = O(g(n))$ are both correct.

From a theorem in class, to show $f(n) = o(g(n))$, it is sufficient to show $\log(f(n)) = o(\log(g(n)))$. Observe

$$\frac{\log f(n)}{\log g(n)} = \frac{\log n^{\sqrt{n}}}{\log 2^{n^{2/3}}} = \frac{\sqrt{n}\log n}{n^{2/3}\log 2}$$

$$= \frac{n^{1/2}\log n}{n^{1/2} n^{1/6}} = \frac{\log n}{n^{1/6}}$$

Using this with L'Hopital we have

$$\lim_{n\to\infty} \frac{\log(f(n))}{\log(g(n))} = \lim_{n\to\infty} \frac{\log n}{n^{1/6}} = \lim_{n\to\infty} \frac{1/n}{\frac{1}{6}n^{-5/6}}$$

$$= \lim_{n\to\infty} \frac{1}{\frac{1}{6} n^{1/6}} = 0$$

It follows that $f(n) = o(g(n))$ as claimed.
Furthermore, $f(n) = o(g(n))$ implies $f(n) = O(g(n))$.

Problem 2 (3 points)

What is the reminder when you divide 3^{132} by 26?

Note $3^3 = 27 = 26 + 1 \equiv 1 \mod 26$

Hence
$$\begin{aligned} 3^{132} \bmod 26 &\equiv (3^3)^{44} \bmod 26 \\ &\equiv (3^3 \bmod 26)^{44} \\ &\equiv (1 \bmod 26)^{44} \\ &\equiv 1 \bmod 26. \end{aligned}$$

So the remainder is 1.

Problem 3 (4 points)

Let a_n be a sequence defined by $a_1 = 1$, $a_2 = 8$, $a_n = a_{n-1} + 2a_{n-2}$ $(n \geq 3)$. Prove that $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ for all $n \geq 1$.

Let $P(n)$ be the predicate that $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$. We first prove the base cases $n=1$ and $n=2$.

We have

$P(1)$: $3 \cdot 2^{1-1} + 2(-1)^1 = 3-2 = 1 = a_1$.

$P(2)$: $3 \cdot 2^{2-1} + 2(-1)^2 = 3 \cdot 2 + 2 = 8 = a_2$.

So $P(1)$ and $P(2)$ are true.

Now, for $n \geq 3$ we assume $P(n)$ and $P(n-1)$ are true a will show $P(n+1)$ is true. We then have

$$
\begin{aligned}
a_{n+1} &= a_n + 2a_{n-1} \\
&= 3 \cdot 2^{n-1} + 2(-1)^n + 2(3 \cdot 2^{n-2} + 2(-1)^{n-1}) \quad \text{by I.H} \\
&= 3 \cdot 2^{n-1} + 2(-1)^n + 3 \cdot 2^{n-1} + 2(-1)^{n-1} + 2(-1)^{n-1} \\
&= 2(3 \cdot 2^{n-1}) + 2((-1)^n + (-1)^{n-1}) + 2(-1)^{n-1} \\
&= 3 \cdot 2^n + 2(-1)^{n-1} \\
&= 3 \cdot 2^n + 2(-1)^{n+1}
\end{aligned}
$$

There fore $P(n+1)$ is true. This completee the proof by induction

Problem 4 (5 points)

Consider a random ordering (permutation) of the numbers $1, 2, \ldots, n$ (each of the $n!$ orderings are equally likely). A pair i, j is out of order if $i < j$ but i occurs after j in the random ordering.

(i) Given a pair i, j (such that $i < j$), what is the probability that i, j is out of order? **(2 points)**

(ii) Suppose E_{ij} is the event that pair i, j is out of order. Are the events $\{E_{ij} | 1 \leq i < j \leq n\}$ mutually independent? (You only need to give a short justification). **(1 point)**

(iii) What is the expected number of pairs that are out of order? Suppose p^* is the answer for part (i). The answer can be expressed in term of p^*. **(2 points)**
Hint: Define appropriate Bernoulli random variables X_{ij} for each pair i, j, and express the random variable X that captures the number of pairs out of order in terms of $\{X_{ij}\}$.

(i) The probability is $\frac{1}{2}$.

(ii) No they are not mutually independent. For example, if $E_{12}, E_{23}, \ldots, E_{n-1,n}$ all occur, then the permutation must be $1, 2, 3, \ldots n-1, n$ hence all other E_{ij} occur in this case

(iii) Define $X_{ij} = \begin{cases} 1 & \text{if } E_{ij} \text{ occurs} \\ 0 & \text{otherwise} \end{cases}$

Then $X = \sum_{1 \leq i < j \leq n} X_{ij}$.

It follows that

$$\mathbb{E}[X] = \mathbb{E}\Big[\sum_{1\le i<j\le n} X_{ij}\Big] = \sum_{1\le i<j\le n} \mathbb{E}[X_{ij}]$$

$$= \sum_{1\le i<j\le n} 1\cdot \Pr[X_{ij}=1] + 0\cdot \Pr[X_{ij}=0]$$

$$= \sum_{1\le i<j\le n} 1\cdot \frac{1}{2} = \sum_{1\le i<j\le n} \frac{1}{2}$$

Note that the total # of pairs $1\le i<j\le n$ is $\binom{n}{2} = \frac{n(n-1)}{2}$

Thus $\mathbb{E}[X] = \frac{1}{2}\cdot\frac{n(n-1)}{2} = \frac{n(n-1)}{4}$

Problem 5 (4 points)

Let A and B be two events with $A \subset B$ and $0 < P(A) < P(B) < 1$. Which of the following are true statements. You **do not** need to justify your answer.

(a) $P(A \cup B) = P(A) + P(B)$
(b) $P(A \cup \overline{B}) = P(A) + P(\overline{B})$
(c) $P(A|\overline{B}) > P(A)$
(d) $P(\overline{B}|A) > P(B)$

Only (b) is true.

Note: While a justification is not needed, one is given since this is a practice final

(a) Note $P(A\cup B) = P(A) + P(B) - P(A\cap B)$.

However $A\cap B = A$ since $A \subseteq B$.

So $P(A\cup B) = P(B) \neq P(A) + P(B)$ unless $P(A)=0$.

Thus a) is not true.

(b) Since $A \subseteq B$ we have $A\cap \bar{B} = \emptyset$

thus $P(A\cup \bar{B}) = P(A) + P(\bar{B}) + P(A\cap\bar{B})$

$= P(A) + P(\bar{B}) + P(\emptyset)$

$= P(A) + P(\bar{B})$

(c), (d) Since $A\cap\bar{B} = \emptyset$ we have

$P(A|\bar{B}) = P(\bar{B}|A) = 0$.

So (c), (d) are not true

Problem 6 (5 points)

Consider a graph $G(V, E)$ on n vertices. A subset $S \subseteq V$ is called a vertex cover of G if and only if for every edge $(u, v) \in E$, either $u \in S$ or $v \in S$, or both $u, v \in S$ i.e., for every edge, at least one of its endpoints must be in the vertex cover S. The minimum vertex cover of G is the vertex cover of G with the fewest number of vertices.

(i) Let G^c represent the graph complement of G. Prove that S is a vertex cover if and only if $V \setminus S$ is a clique in G^c. **(3 points)**

(ii) Let k be the size of the largest clique in G^c. Is the size of the vertex cover of smallest size $n - k$? If yes, prove this. If not, give a counter-example. **(2 points)**

Write $G=(V,E)$ and $G^c=(V,E^c)$.

(i) Suppose S is a vertex cover in V. Assume toward a contradiction that $V\setminus S$ is not a clique. Then there exists vertices $u,v \in V\setminus S$ such that $(u,v)\notin E^c$. Thus $(u,v)\in E$. However $u,v\notin S$ since $u,v\in V\setminus S$, contradicting that S is a cover. We conclude that If S is a cover, then G is a Clique.

To prove that G is a clique implies S is a cover, we will proceed by contrapositive.

Assume that S is not a cover. Then there exists some edge $(u,v)\in E$ such that $u,v\notin S$. But then $u,v\in V\setminus S$ and $(u,v)\notin E^c$ so $V\setminus S$ is not a clique. This shows that if S is not a cover, then $V\setminus S$

is not a clique. We conclude that if $V \setminus S$ is a clique, then S is a cover.

(ii) Yes. To prove this, suppose towards a contradiction that there is a cover S of size $s < n-k$. Then $V \setminus S$ is a clique in G^c by part (i). However, $|V \setminus S| = |V| - |S| = n - s > n-(n-k) = k$. Hence G^c has a clique of size larger than k. However this contradicts the assumption that the largest clique in G^c has size k. Thus S cannot have a cover of size less than $n-k$.

To see that S has a cover of size $n-k$, let S' be a clique of k in G, and set $S = V \setminus S'$. Then $S' = V \setminus S$ so it follows from part (i) that S is a cover in G. Furthermore $|S| = |V \setminus S'| = |V| - |S'| = n-k$

Problem 7 (9 points)

Identify whether the follows proofs are correct, and if there are any mistakes, identify them.

1. Consider a drunken ant that follows the following random process to go along a straight-line path from a point A to a point B. In each second, it takes *one* step in the forward direction with probability 4/5, and with probability 1/5 it takes *three* steps in the backward direction.

   Claim: Pr[*The ant has covered* $3n/5$ *steps after* n *seconds*] $\leq 1/3$.

   Proof. Let X_i be the number of steps taken by the ant in the ith second, and let X be the random variable representing the total number of steps taken after n seconds. From the problem description,

   $$X_i = \begin{cases} 1 & \text{with probability } 4/5 \\ -3 & \text{with probability } 1/5 \end{cases}.$$

   Hence, for each $i \in [n]$, $\mathrm{E}[X_i] = \frac{4}{5} - \frac{3}{5} = 1/5$. Hence by linearity of expectation, $\mathrm{E}[X] = \sum_{i=1}^{n} \mathrm{E}[X_i] = n/5$. Since $\mathrm{E}[X] \geq 0$, by applying Markov's inequality, we have

   $$\Pr[X \geq 3n/5] \leq \frac{\mathrm{E}[X]}{3n/5} = \frac{n/5}{3n/5} \leq 1/3.$$

   $\square$

   Is the above proof correct? If not, identify the incorrect step(s). **(3 points)**

The proof is incorrect. One cannot apply Markov since X is not non-negative.

Instructor's Note: The above answer is sufficient. However to highlight the importance of nonnegativity to Markov, observe that if $n=1$, then $X = X_1$ and $\Pr\{X_1 \geq 3/5\} = 4/5$ so the claimed inequality doesn't hold.

2. There is a murder in the town of Braavos which has a population of $N = 40000$, and anyone could be the culprit with equal probability. The forensics team has a finger-print test that for a given person says there is a match with probability 0.4 if the person is guilty, and with probability 10^{-4} if the person is not guilty. The finger-print test outputs a match with a certain Mr. Jack in Evanstown. The prosecutor argues that Mr. Jack is guilty since the probability that Mr. Jack is guilty is at least 0.9975 using the following proof

Proof. Let I be the event that Jack is innocent, and G be the event that Jack is guilty. Let T be the event that the test returns positive, and F be the event that the test returns negative.

$$\Pr[\text{ Jack is innocent }] = \Pr[I] = \frac{\Pr[I|T]}{\Pr[I|T] + \Pr[G|T]} = \frac{10^{-4}}{0.4 + 10^{-4}} = \frac{0.0001}{0.4001} = \frac{1}{4000} \leq 0.0025$$

Hence the probability that Jack is guilty is at least 0.9975. □ □

Is the above proof correct? If not, how what is the correct calculation for Pr[Jack is innocent] (you don't need to simplify the numeric expressions)? **(3 points)**

The proof is incorrect. Baye's rule is not used correctly

3. Let M be an $n \times n$ matrix.

Claim. We have $\sum_{i,j=1}^{n} M(i,j)^2 = \sum_{\ell} \lambda_\ell^2$, *where the* $\lambda_1, \lambda_2, \ldots$ *are the eigenvalues of the matrix* M, *and* $M(i,j)$ *is the* (i,j)*th entry of* M.

Proof. From the spectral theorem, we know that

$$M = \sum_{\ell=1}^{n} \lambda_\ell e_\ell e_\ell^T, \text{ and } M(i,j) = \sum_{\ell} \lambda_\ell e_\ell(i) e_\ell(j).$$

Hence,

$$\begin{aligned}
\sum_{i=1}^{n}\sum_{j=1}^{n} M(i,j)^2 &= \sum_{i=1}^{n}\sum_{j=1}^{n} \Big(\sum_{\ell} \lambda_\ell e_\ell(i) e_\ell(j)\Big)^2 \\
&= \sum_{i}\sum_{j}\sum_{\ell_1}\sum_{\ell_2} \lambda_{\ell_1}\lambda_{\ell_2} e_{\ell_1}(i) e_{\ell_1}(j) e_{\ell_2}(i) e_{\ell_2}(j) \\
&= \sum_{\ell_1}\sum_{\ell_2} \lambda_{\ell_1}\lambda_{\ell_2} \sum_{i} e_{\ell_1}(i) e_{\ell_2}(i) \sum_{j} e_{\ell_1}(j) e_{\ell_2}(j) \\
&= \sum_{\ell_1}\sum_{\ell_2} \lambda_{\ell_1}\lambda_{\ell_2} (\langle e_{\ell_1}, e_{\ell_2}\rangle)^2.
\end{aligned}$$

But note that by the orthogonality of eigenvectors, $\langle e_{\ell_1}, e_{\ell_2}\rangle = \sum_i e_{\ell_1}(i) e_{\ell_2}(i)$ is 0 when $\ell_1 \neq \ell_2$ and 1 when $\ell_1 = \ell_2$. Hence,

$$\sum_{i=1}^{n}\sum_{j=1}^{n} M(i,j)^2 = \sum_{\ell_1} \lambda_{\ell_1}^2 \langle e_{\ell_1}, e_{\ell_1}\rangle^2 = \sum_{\ell_1} \lambda_{\ell_1}^2.$$

$\square$

The proof is not correct.
We cannot apply the spectral theorem since M is not necessarily symmetric.