Problem 1

Warmup:

-

Proof: By the fundamental theorem of arithmetic, every integer greater than 1 can be uniquely expressed as a product of prime numbers. Therefore, we may express $n \in [1, 200]$ as

$$n = 2^{r_2} \cdot 3^{r_3} \cdot \dots = 2^r \cdot m$$

where m is an odd integer that contains all prime factors greater than 2, and r is the number of times 2 divides n. Since $n \leq 200$, we have $m \leq \frac{200}{2^r} \leq 200$. Since m is odd, it can at most take on 100 values, which are $1, 3, 5, \dots, 199$. Since we are choosing 101 different numbers, by the pigeonhole principle, at least two of them must have an odd part m that is the same. Therefore, we have $n_1 = 2^{r_1} \cdot m$ and $n_2 = 2^{r_2} \cdot m$ for some r_1, r_2. WLOG, let $r_1 < r_2$ (equality is impossible since n_1 and n_2 are distinct), so $r_2 - r_1$ is a positive integer. Then,

$$\frac{n_2}{n_1} = \frac{2^{r_2}}{2^{r_1}} = 2^{r_2 - r_1} \in \mathbb{N}_+ \Rightarrow n_1 \mid n_2$$

■

Problem 2

Proof: Assume, to the contrary, that there exists two longest paths P, Q of length n in the graph G, and that they do not share any vertices. Select 2 vertices, $u \in P, v \in Q$ such that the shortest path R between u, v is the shortest among all possible choices of u, v.

We first prove that R does not intersect P or Q. Assume, to the contrary (WLOG), that R intersects P at vertex x. Then, we can construct a new path R' by replacing the segment of P from u to x with the segment of R from x to v, which is shorter than R. This contradicts the assumption that the selection u, v gives the shortest R. Therefore, R does not intersect P or Q.

Next, we construct a path longer than P (and Q). Consider the path $P' + R + Q'$, where

- P' is the segment of P from one end of P to u. Denote $P = P' + P''$, where P'' is the segment of P from u to the other end of P. Let P' be the longer of the two segments. Therefore, since $|P| = |P'| + |P''|$, we have $|P'| \geq \lceil \frac{|P|}{2} \rceil = \lceil \frac{n}{2} \rceil$.
- R is the shortest path from u to v. It must have length $|R| \geq 1$.
- Q' is the segment of Q from v to one end of Q, defined in an analogous way to P'. $|Q'| \geq \lceil \frac{n}{2} \rceil$.

Therefore, $|P' + R + Q'| = \lceil \frac{n}{2} \rceil + 1 + \lceil \frac{n}{2} \rceil \geq n + 1 > |P| = |Q|$, which contradicts the assumption that P, Q are longest paths in G.

Thus, we conclude that P and Q must share at least one vertex.

■

Problem 3

3.a

Proof: Defining terms mathematically, we wish to prove the statement

$$f \in O(g) \wedge g \in O(h) \Leftrightarrow f \in O(h)$$

This may be shown by simply expanding the definition of both sides.

$$f \in O(g) \Leftrightarrow \exists c, n_0 \in \mathbb{N}_+ \text{ st } \forall n \geq n_0, f(n) \leq cg(n)$$
$$g \in O(h) \Leftrightarrow \exists d, m_0 \in \mathbb{N}_+ \text{ st } \forall m \geq m_0, g(m) \leq dh(m)$$

Let $k = \max(n_0, m_0)$. Then, we have $\forall n \geq k, f(n) \leq cg(n) \leq cdh(n)$, where cd is a constant. Therefore, we have $f \in O(h)$.

■

3.b

Proof: By definition of monotonicity, if $a > b, a, b \in \mathbb{Z}_+$, then $f(a) > f(b), g(a) > g(b)$. Since the ranges of f and g are both in $\mathbb{Z}_+$, we have $f(n) > 0, g(m) > 0$ for all $n, m \in \mathbb{Z}_+$. Therefore,

$$\begin{aligned} f(a) + g(a) &> f(a) + g(a) + (g(b) - g(a)) \\ &= f(a) + g(b) \\ &> f(a) + (f(b) - f(a)) + g(b) \\ &= f(b) + g(b) \end{aligned}$$

Therefore, $f + g$ is monotone increasing.

Similarly, if $a > b, a, b \in \mathbb{Z}_+$, then $g(a) > g(b)$ and $g(a), g(b) \in \mathbb{Z}_+$ (in the domain of f), so we have $f(g(a)) > f(g(b))$ from the monotonicity of f. Therefore, $f \circ g$ is also monotone increasing.

■

3.c

Proof: By definition, $T(n) \in n^{O(1)} \Leftrightarrow \exists N, c : T(n) \leq n^c, \forall n > N \Leftrightarrow T(n) \in O(n^c)$

■

3.d

Proof:

$$n! = \prod_{i=1}^{n} i < \left(\prod_{i=1}^{n} i\right) \cdot \left(\prod_{i=1}^{n} \frac{n}{i}\right) = \prod_{i=1}^{n} n = n^n$$

Therefore, for all $n > 0$, we have $n! < n^n$. Since log is a monotone increasing function, we have $\log(n!) < \log(n^n) = n\log(n)$. Therefore, we have for $c = 1, N = 0$, $\log(n!) \leq cn\log(n) \forall n > N$. Therefore, $\log(n!) \in O(n\log(n))$.

■

Problem 4

4.a

Proof: Define the set

$$S = \mathbb{Z}_+ \cap \left(\bigcup_{\substack{i=1 \\ i \text{ is odd}}} [a_i, 2a_i) \right)$$

where $a_i = 2^i$. Since $2a_i = 2^{i+1} < 2^{i+2} = a_{i+2}$, S is a disjoint union of intervals. Therefore, if $n \in S$, then it must be in exactly one of the intervals $[a_i, 2a_i)$.

Since $4a_i = a_{i+2}$, we must have

$$S' = \mathbb{Z}_+ \setminus S = \mathbb{Z}_+ \cap \left(\bigcup_{\substack{i=1 \\ i \text{ is odd}}} [2a_i, 4a_i) \right)$$

Similarly, S' is a disjoint union of intervals. If $n \in S'$, then it must be in exactly one of the intervals $[2a_i, 4a_i)$.

Define the functions f and g as follows:

$$f(n) = \begin{cases} e^{a_i} + (n - a_i) \text{ if } n \in [a_i, 2a_i) \\ e^n \text{ if } n \notin S \end{cases}$$

$$g(n) = \begin{cases} e^n \text{ if } n \in S \\ e^{2a_i} + (n - 2a_i) \text{ if } n \in [2a_i, 4a_i) \end{cases}$$

We first show that both f and g are monotone increasing. We will show that for any consecutive pair of integers $n, n+1$, $f(n) \le f(n+1)$ and $g(n) \le g(n+1)$.

Let $n, n+1 \in S$. Then, $f(n) = e^{a_i} + (n - a_i), f(n+1) = e^{a_i} + (n + 1 - a_i) > f(n)$. $g(n) = e^n, g(n+1) = e^{n+1} > g(n)$.

Similarly, if $n, n+1 \in S'$, the same argument applies.

If $n \in S$ and $n+1 \in S'$, it must be that $n + 1 = 2a_i$ for some i (for all other n, we would have $n + 1 \in S$ since S is a union of intervals).

- For $f(n)$: $f(n) = e^{a_i} + (n - a_i), f(n+1) = e^{2a_i}$. Therefore, $f(n+1) - f(n) = e^{a_i} - (2a_i - 1 - a_i) = e^{a_i} - a_i + 1$. Using the Taylor expansion of e^x, we have $e^x - x + 1 = \left(1 + x + \frac{x^2}{2} + \cdots\right) - x + 1 = 2 + \frac{x^2}{2} + \cdots > 0$, so $f(n+1) > f(n)$.
- For $g(n)$: $g(n) = e^n, g(n+1) = e^{n+1} + (2a_i - 2a_i) = e^{n+1} > g(n)$.

Lastly, if $n \in S'$ and $n + 1 \in S$, it must be that $n + 1 = a_i$ for some i.

- For $f(n)$: $f(n) = e^n, f(n+1) = e^{a_i} + (a_i - a_i) = e^{a_i} > f(n)$.
- For $g(n)$: $g(n) = e^{2a_{i-2}} + (n - 2a_{i-2}), g(n+1) = e^{a_i} = e^{4a_{i-2}}$. With a similar argument as above, we have $g(n+1) > g(n)$.

We then show that these two functions satisfy $f \notin O(g)$ and $g \notin O(f)$.

Assume, to the contrary, that $f \in O(g)$. Then, we have $f(n) \le cg(n)$ for some $c > 0, N > 0$ and all $n > N$. Let $n = 4a_i - 1$ for some i. Therefore,

$$\begin{aligned} f(n) - cg(n) &= e^{4a_i - 1} - c\left(e^{2a_i} + (n - 2a_i)\right) \\ &= e^{2a_i}\left(e^{2a_i - 1} - c\right) - c(2a_i - 1) \\ &\ge e^{2a_i}\left(e^{2a_i - 1} - c\right) - ce^{2a_i} \\ &\ge e^{2a_i}\left(e^{2a_i - 1} - 2c\right) \end{aligned}$$

Since $2c$ is a constant, we can choose i such that $e^{2a_i - 1} - 2c > 0$ (an explicit formula would be $i > \log_2\left(\frac{\ln(2c)+1}{2}\right)$), so $f(n) > cg(n)$, which contradicts the assumption that $f \in O(g)$.

Assume, to the contrary, that $g \in O(f)$. Then, we have $g(n) \le cf(n)$ for some $c > 0, N > 0$ and all $n > N$. Let $n = 2a_i - 1$ for some i. Therefore,

$$\begin{aligned} g(n) - cf(n) &= e^{2a_i - 1} - c(e^{a_i} + (n - a_i)) \\ &= e^{a_i}(e^{a_i - 1} - c) - c(a_i - 1) \\ &\geq e^{a_i}(e^{a_i - 1} - c) - ce^{a_i} \\ &\geq e^{a_i}(e^{a_i - 1} - 2c) \end{aligned}$$

Since $2c$ is a constant, we can choose i such that $e^{a_i - 1} - 2c > 0$, which contradicts the assumption that $g \in O(f)$. Therefore, we conclude that $f \notin O(g)$ and $g \notin O(f)$.

■

4.b

Proof: We shall prove the statement.

Let $g(n) = \max\{f_1(n), ..., f_k(n)\} = f_{a_n}(n)$. By definition, $g(n) \geq f_i(n)\ \forall i \in [1, k], n \in \mathbb{Z}_+$. Therefore, $f_i \in O(g)\ \forall i$. Let g' be a function such that $f_i \in O(g')\ \forall i$. Then, by definition, $\exists c_i, N_i : f_i(n) \leq g'(n)\ \forall n > N_i, \forall i$. Let $N = \max\{N_1, ..., N_k\}$, $c = \max\{c_1, ..., c_k\}$. Then, we have

$$g(n) = f_{a_n}(n) \leq c_{a_n} g'(n) \leq cg'(n)\ \forall n > N$$

Therefore, $g(n) \in O(g')$.

■

Collaborators: Gio Huh