CS5800 PS1 - Aditya Shanmugham (NUID : 002738073)

Problem 1: Asymptotics

In order to solve this problem, I am comparing equations in a set of 2, strategically

1) **Comparing** $g01 = n^{101/100}$ **and** $g02 = n * 2^{(n+1)}$**:**

$n^{101/100}$ Applying log on both sides: $log(n^{(101/100)})$ $(101/100) * log(n)$ $log(n) + (1/100) * log(n)$ Ignoring log(n) on both sides and applying log: $log(1/100) + log^{2}(n)$ **- (1)**	$n * 2^{(n+1)}$ $log(n * 2^{(n+1)})$ $log(n) + (n + 1) * log(2)$ $log(n) + (n + 1) * log(2)$ $log(n + 1) + log^{2}(2)$ **- (2)**

Here (2) is greater than (1)

- $g01 = n^{101/100}$ **<** $g02 = n * 2^{(n+1)}$

2) **Comparing** $g03 = n * (log(n)^{3})$ **and** $g04 = n^{log(log(n))}$**:**

$n * log(n)^{3}$ $n * log(n)^{3}$ Applying log on both sides: $log(n) + log(log(n)^{3})$ $log(n) + 3 * log^{2}(n)$	$n^{log(log(n))}$ $n^{log(log(n))}$ $[log^{2}(n)] * log(n)$ $[log^{2}(n)] * log(n)$

$log(n)\ +\ 3\ *\ log^{2}(n)$ **- (1)**	$log^{2}(n)\ *\ log(n)$ **- (2)**

Here (2) is greater than (1)

- $g03\ =\ n\ *\ (log(n)^{3})$ **>** $g04\ =\ n^{log(log(n))}$

3) Comparing $g11\ =\ 2^{(log(n^{0.5})}$ **and** $g12\ =\ n^{0.5^{log(n)}}$ **:**

$2^{(log(n^{0.5})}$ Applying log on both sides: $log(2^{log(n^{0.5})})$ $log(n^{0.5})\ *\ log(2)$ $log(n^{0.5})\ *\ log(2)$ $0.5\ *\ log(n)\ *\ log(2)$ **- (1)**	$n^{0.5^{log(n)}}$ $log(2^{0.5^{logn}})$ $log(n)\ *\ log(2^{0.5})$ $log(n)\ *\ log(2^{0.5})$ $log(n)\ *\ 0.5\ *\ log(2)$ **- (2)**

Here (1) is equal to (1):

- $2^{(log(n^{0.5})}$ = $n^{0.5^{log(n)}}$

4) Comparing $g07\ =\ 2^{(log(n)^{0.5})}$ **and** $g08\ =\ 2^{2^{n+1}}$ **:**

$2^{(log(n)^{0.5})}$ $2^{(log(n)^{0.5})}$ Applying log on both sides: $log(2^{log(n)^{0.5}})$ $log(n)^{0.5}\ *\ log(2)$	$2^{2^{n+1}}$ 4^{n+1} $log(4^{n+1})$ $(n\ +\ 1)\ *\ log(4)$

Applying log on both sides: $log[log(n)^{0.5} * log(2)]$ $log(log(n)^{0.5} + log^2(2))$ $0.5 * log^2(n) + log^2(2)$ **- (1)**	$log(n) * 0.5 * log(2)$ $log[(n + 1) * log(4)]$ $log(n + 1) * log^2(4)$ $log(n + 1) + log^2(4)$ **- (2)**

Here (2) is greater than (1)

- $g07 = 2^{(log(n)^{0.5})}$ < $g08 = 2^{2^{n+1}}$

5) Comparing $g07 = 2^{(log(n)^{0.5})}$ and $g03 = n * (log(n)^3)$:

$2^{(log(n)^{0.5})}$ Applying log on both sides: $log(2^{log(n)^{0.5}})$ $log(n)^{0.5} * log(2)$ **- (1)**	$n * (log(n)^3)$ $log(n * log(n)^3)$ $log(n) + 3 * log^2(n)$ **- (2)**

Here (2) is greater than (1)

- $g07 = 2^{(log(n)^{0.5})}$ < $g03 = n * (log(n)^3)$

6) Comparing $g07 = 2^{(log(n)^{0.5})}$ and $g11 = 2^{(log(n^{0.5})}$:

$2^{(log(n)^{0.5})}$ $2^{(log(n)^{0.5})}$ Applying log on both sides: $log(n)^{0.5} * log(2)$	$2^{(log(n^{0.5})}$ $2^{0.5*log(n)}$ $0.5 * log(n) * log(2)$

Applying log on both sides: $0.5 * log(n) \ + log^{2}(2)$ **- (1)**	$log(0.5) + log^{2}(n) + log^{2}(2)$ **- (2)**

Here (2) is greater than (1)

- $g07 = 2^{(log(n)^{0.5})}$ < $g11 = 2^{(log(n^{0.5})}$

7) **Comparing** $g08 = 2^{2^{n+1}}$ **and** $g11 = 2^{(log(n^{0.5})}$:

$2^{2^{n+1}}$ 4^{n+1} Applying log on both sides: $log(4^{n+1})$ $(n + 1) * log(4)$ $(n + 1) * log(4)$ Applying log on both sides: $log(n + 1) \ + log^{2}(4)$ **- (1)**	$2^{(log(n^{0.5})}$ $2^{(log(n^{0.5})}$ $log(2^{(log(n^{0.5})})$ $(log(n^{0.5}) * log(2)$ $0.5 * log(n) * log(2)$ $log(0.5) + log^{2}(n) + log^{2}(2)$ **- (2)**

Here (1) is greater than (2)

- $g08 = 2^{2^{n+1}}$ > $g11 = 2^{(log(n^{0.5})}$

8) **Compare** $g03 = n * (log(n)^{3})$ **and** $g01 = n^{101/100}$

$n * (log(n)^{3})$ Applying log on both sides: $log(n * log(n)^{3})$	$n^{101/100}$ $log(n^{(101/100)})$

$log(n) + log(log(n)^3)$ $(n + 1) * log(4)$ $log(n) + 3 * log^2(n)$ **- (1)**	$(101/100) * log(n)$ $0.5 * log(n) * log(2)$ $log(n) + (0.01) * log(n)$ **- (2)**

Here (1) is greater than (2)

- $g03 = n * (log(n)^3) > g01 = n^{101/100}$

9) Compare $g03 = n * (log(n)^3)$ and $g02 = n * 2^{(n+1)}$:

$n * (log(n)^3)$ Applying log on both sides: $log(n * log(n)^3)$ $log(n) + log(log(n)^3)$ $log(n) + 3 * log^2(n)$ **- (1)**	$n * 2^{(n+1)}$ $log(n * 2^{n+1})$ $log(n) + log(2^{n+1})$ $log(n) + (n + 1) * log(2)$ **- (2)**

Here (2) is greater than (1)

- $g03 = n * (log(n)^3) < g02 = n * 2^{(n+1)}$

10) Compare $g04 = n^{log(log(n))}$ and $g01 = n^{101/100}$:

$n^{log(log(n))}$ $n^{log^2(n)}$ Applying log on both sides: $log(n^{log^2(n)})$	$n^{101/100}$ $n^{(101/100)}$ $log(n^{(101/100)})$

$log^2(n) * log(n)$ Applying log on both sides: $log^3(n) + log^2(n)$ **- (1)**	$(101/100) * log(n)$ $log(101/100) + log^2(n)$ **- (2)**

Here (1) is greater than (2)

- $g04 = n^{log(log(n))}$ > $g01 = n^{101/100}$

11) Compare $g01 = n^{101/100}$ and $g11 = 2^{(log(n^{0.5})}$

$n^{101/100}$ Applying log on both sides: $log(n^{(101/100)})$ $(101/100) * log(n)$ $(101/100) * log(n)$ Applying log on both sides: $log(101/101) + log^2(n)$ **- (1)**	$2^{(log(n^{0.5})}$ $log(2^{log(n^{0.5})})$ $log(n^{0.5}) * log(2)$ $0.5 * log(n) * log(2)$ $log(0.5) + log^2(n) + log^2(2)$ **- (2)**

Here (1) is greater than (2)

- $g01 = n^{101/100}$ > $g11 = 2^{(log(n^{0.5})}$

12) Compare $g08 = 2^{2^{n+1}}$ and $g02 = n * 2^{(n+1)}$:

$2^{2^{(n+1)}}$ $4^{(n+1)}$	$n * 2^{(n+1)}$ $n * (2^{n+1})$

Applying log on both sides: $(n + 1) * log(4)$ $(n + 1) * log(2) * log(2)$ **- (1)**	$log(n) + (n + 1) * log(2)$ $log(n) + (n + 1) * log(2)$ **- (2)**

Here (1) is greater than (2)

- $g08 = 2^{2^{n+1}}$ > $g02 = n * 2^{(n+1)}$

13) Compare $g05 = log(n^{2n})$ **and** $g03 = n * (log(n)^{3})$**:**

$log(n^{2n})$ $2n * log(n)$ Applying log on both sides: $log(2n * log(n))$ $log(2n) + log^{2}(n)$ $log(2n) + log^{2}(n)$ $log(2n) * log^{2}(n)$ **- (1)**	$n * (log(n))^{3}$ $n * log(n)^{3}$ $log(n * log(n)^{3})$ $log(n) + log(log(n)^{3})$ $log(n) + 3 * log(log(n))$ $log(n) + 3 * log^{2}(n)$ **- (2)**

Here (1) is greater than (2)

- $g05 = log(n^{2n})$ < $g03 = n * (log(n)^{3})$

14) **Compare** $g05 = log(n^{2n})$ **and** $g04 = n^{log(log(n))}$:

$log(n^{2n})$ $2n * log(n)$ Applying log on both sides: $log(2n) * log^2(n)$ **- (1)**	$n^{log^2(n)}$ $n^{log^2(n)}$ $log^2(n) * log\ (n)$ **- (2)**

Here (1) is greater than (2)

- $g05 = log(n^{2n})$ > $g04 = n^{log(log(n))}$

15) Compare $g06 = n!$ **and** $g08 = 2^{2^{n+1}}$ **:**

$n!$. Applying log on both sides: $= log(n!)$ Using Sterling Approximation: $= n * log(n) - n$ **- (1)**	$2^{2^{n+1}}$ $= 4^{n+1}$ $(n + 1) * log(4)$ $(n + 1) * log(4)$ **- (2)**

Here (1) is greater than (2). But when we plot the g06 and g08 in a graph, initially g06 seems slower than g08 until it converges and surpasses g08 at 10^{25}

- $g06 = n!$ **>** $g08 = 2^{2^{n+1}}$

16) Compare $g09 = log(n!)$ **and** $g10 = ceil(log(n)!)$**:**

$log(n!)$	$ceil(log(n)!)$
$= log(n * (n - 1) * (n - 2)..).$ $= log(n) + log(n - 1) + log(n - 2)..$ <= $log(n) * log(n) * log(n) *$..... = $O(log(n) * n)$ **- (1)**	$log(x) * (log(x) - 1) * (log(x) - 2)$... <= $log(x) * log(x) * log(x)$.... = $O(log(x)^{x})$ **- (2)**

Here (2) is greater than (1)

- $g09 = log(n!)$ < $g10 = ceil(log(n)!)$

17) **Compare** $g05 = log(n^{2n})$ **and** $g09 = log(n!)$:

$log(n^{2n})$	$log(n!)$
= $2n * log(n)$ **- (1)**	From comparison no (16): $log(n!)$ = $O(log(n) * n)$ **- (2)**

Here (1) is greater than (2)

- $g05 = log(n^{2n})$ > $g09 = log(n!)$

18) Compare $g03 = n * (log(n)^{3})$ **and** $g10 = ceil(log(n)!)$**:**

$n * log(n)^{3}$	$ceil(log(n)!)$
Applying log: $log(n * log(n))$ $log(n)$ + $log(log(n))$ $log(n) + 3 * log^{2}(n)$ **- (1)**	From comparison no (16): $ceil(log(n)!)$ = $O(log(x)^{x})$ $log(log(x)^{x})$ $x * log(log(x))$ $x * log^{2}(x)$ **- (2)**

Here (2) is greater than (1)

- $g03 = n * (log(n)^3) < g10 = ceil(log(n)!)$

Based on the above comparisons:

The order :

$$\boxed{g06 > g08 > g02 > g10 > g03 > g05 > g09 > g04 > g01 > g11 = g12 > g07}$$

Problem 2: More Asymptotics

1) If $f(n) = \Omega(g(n))$ and $g(n) = \Omega(f(n))$, then $f(n) = \theta(g(n))$:

-> $f(n) = \Omega(g(n))$ - (1)

then,

$g(n) = O(f(n))$ *as per Transpose Property (a)*

-> $g(n) = O(f(n))$ - (2)

Using property (b) on (1) and (2):

-> $g(n) = \Theta(f(n))$ - (3)

Using symmetry property (c) on (3)

-> $f(n) = \Theta(g(n))$

Properties used in this solution:

(a) Transpose Property :

If $f(n) = O(g(n))$ then $g(n) = \Omega(f(n))$

(b) If $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ then $f(n) = \Theta(g(n))$

(c) Symmetry Property:

If $f(n) = \Theta(g(n))$ then $g(n) = \Theta(f(n))$

The equality provided in the question is **True.**

2) $f(n) = o(g(n))$ then $g(n)\ not \in O(f(n))$

-> $f(n) = o(g(n))$ - (1)

(1). Can be written as:

$f(n) < g(n) * c$, where 'c' is a constant - (2)

From the question : $g(n) = O(f(n))$ - (3)

(3). Can be written as:

$g(n) <= f(n) * c$, where 'c' is a constant - (4)

In order for (2) to be equal to (4), the equation should be:

$f(n) * c < (g(n)) * c <= f(n) * c$ - (5)

Where (5) is impossible.

Hence, $g(n)\ not \in O(f(n))$.

The equality provided in the question is **True.**

3) If $f(n) = O(h(n))$ and $g(n) = O(h(n))$, then $f(n) + g(n) = O(h(n))$:

-> $f(n) = O(h(n))$ - (1)
-> $g(n) = O(h(n))$ - (2)

Using Property (a) on (1) and (2):

$f(n) + g(n) = O(h(n) + h(n))$

$f(n) + g(n) = O(2 * h(n))$

$f(n) + g(n) = 2 * O(h(n))$

$0.5 * (f(n) + g(n)) = O(h(n))$ - (3)

Using Property (b) on (3):

$f(n) + g(n) = O(h(n))$

Properties used in this solution:
(a) If $f(n) = O(d(n))$ and $g(n) = O(e(n))$ then $f(n) + g(n) = O(d(n) + e(n))$
(b) If $f(n) = O(g(n))$ then $c * f(n) = O(g(n))$

The equality provided in the question is **True.**

4) If $f(n) = O(h(n))$ and $g(n) = O(h(n))$, then $f(n) * g(n) = O(h(n))$

-> $f(n) = O(h(n))$ - (1)
-> $g(n) = O(h(n))$ - (2)

Using Property (a) on (1) and (2):

$f(n) * g(n) = O(h(n) * h(n))$

$f(n) * g(n) = O(h^2(n))$

Properties used in this solution:
(a) If $f(n) = O(d(n))$ and $g(n) = O(e(n))$ then $f(n) * g(n) = O(d(n) * e(n))$

The equality provided in the question is **False.**

5) If $f(n) = O(g(n))$ then $2^{f(n)} = O(2^{g(n)})$

-> $f(n) = O(g(n))$ - (1)

Raising to the power of 2:

-> $2^{f(n)} <= \ 2^{g(n)*c}$

-> $2^{f(n)} <= \ 2^{g(n)^c}$ - (2)

If c>1 in (2) then $2^{g(n)}$ won't be constant time. Hence, the equality is not true.

We can also prove it using log

Applying log on (1)

-> $f(n)\ *\ log(2)\ \ <=\ g(n)\ *\ log(2)\ +\ log(c)$ - (3)

The equation (3) is valid only from c>1. If c = 0 then the log(c) reaches - infinity thereby breaking the inequality.

The equality provided in the question is **False.**

Problem 3: Modular Arithmetic Computations

1) **Compute $3^{1500}\ mod\ 11$:**

1500 to binary = (1011 1011 100)

Initialise *a=3* and *out=1*

Bits	a	out
0	3	1
0	(3*3) mod11 = 9	1
1	(3*9) mod 11 = 5	(9*1) mod 11 = 9
1	(3*5) mod 11 = 4	(9*5) mod 11 = 1
1	(3*4) mod 11 = 1	(1*4) mod 11 = 4
0	(3*1) mod 11 = 3	4
1	(3*3) mod 11 = 9	(4*3) mod 11 = 1
1	(3*9) mod 11 = 5	(1*9) mod 11 = 9
1	(3*5) mod 11 = 4	(9*5) mod 11 = 1
0	(3*4) mod 11 = 1	1

Bits	a	out
1	(3*1) mod 11 = 3	**(1*1) mod 11 = 1**

The answer is **1.**

2) Compute $5^{4358}\ mod\ 10$

4358 to binary = (1000 1000 0011 0)

Initialise *a=5 and out=1*

Bits	a	out
0	5	1
1	(5*5) mod 10 = 5	(1*5) mod 10 = 5
1	(5*5) mod 10 = 5	(5*5) mod 10 = 5
0	(5*5) mod 10 = 5	5
0	(5*5) mod 10 = 5	5
0	(5*5) mod 10 = 5	5
0	(5*5) mod 10 = 5	5
0	(5*5) mod 10 = 5	5
1	(5*5) mod 10 = 5	(5*5) mod 10 = 5
0	(5*5) mod 10 = 5	5
0	(5*5) mod 10 = 5	5
0	(5*5) mod 10 = 5	5
1	(5*5) mod 10 = 5	**(5*5) mod 10 = 5**

The answer is **5.**

3) Compute $6^{22345}\ mod\ 7$

22345 to binary = (1010 1110 1001 001)

Initialise *a=6 and out=1*

Bits	a	out
1	6	6
0	(6*6) mod 7 = 1	6
0	(6*1) mod 7 = 6	6
1	(6*6) mod 7 = 1	(6*6) mod 7 = 1
0	(6*1) mod 7 = 6	1
0	(6*6) mod 7 = 1	1
1	(6*1) mod 7 = 6	(1*1) mod 7 = 1
0	(6*6) mod 7 = 1	1
1	(6*1) mod 7 = 6	(1*1) mod 7 = 1
1	(6*6) mod 7 = 1	(1*6) mod 7 = 6
1	(6*1) mod 7 = 6	(6*1) mod 7 = 6
0	(6*6) mod 7 = 1	6
1	(6*1) mod 7 = 6	(6*1) mod 7 = 6
0	(6*6) mod 7 = 1	6
1	(6*1) mod 7 = 6	**(6*1) mod 7 = 6**

The answer is **6.**

4) **Compute GCD(648,124)**

Using Euclid Algorithm:

= GCD(648, 124) = GCD(124, 648 mod 124) = GCD(124, 28)
= GCD(124, 28) = GCD(28, 124 mod 28) = GCD(28, 12)
= GCD(28, 12) = GCD(12, 28 mod 12) = GCD(12, 4)
= GCD(12, 4) = GCD(4, 12 mod 4) = GCD(4, 0)

The answer is **4.**

5) **Compute GCD(123456789, 123456788)**

Using Euclid Algorithm:

= GCD(123456789, 123456788) = GCD(123456788, 123456789 mod 123456788) = GCD(123456788, 1)

= GCD(123456788, 1) = GCD(1, 123456788 mod 1) = GCD(1, 0)

The answer is **1.**

6) **Compute GCD(**$10^{117}, 2^{200}$**) :**

GCD of the number are:

10^{117} = $2^{117} * 5^{117}$

$2^{200} = 2^{117} * 2^{83}$

$GCD(10^{117}, 2^{200}) = GCD(5^{117} * 2^{117}, 2^{200})$ = $2^{!17}$; since there are no more factors left (2 and 5 are coprime).

The answer is 2^{117}**.**