

[illegible]

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for  
this examination are my own work.

I understand that sanctions will be  
imposed, if I am found to have violated the  
University regulations governing academic  
integrity.

Student's Name: \_\_\_\_\_

Student's Signature: \_\_\_\_\_

**Problem 1:** [8 pts] For each of the following predicates, decide whether it is true or false. If it is true, prove it. If it is false, state it is false; you do not have to prove it.

- (a) (Random variable  $X$ ; positive integer  $n$ ;  $V(\cdot)$  is variance)

$$\forall X \forall n (V(nX) \geq nV(X))$$

- (b) (Prime number  $p$ ;  $x, y, z$  in  $\mathbb{Z}_p$ ;  $y \neq 0$ )

$$\forall x \forall y \exists z (x + yz \equiv 0 \pmod{p})$$

- (c) (Sets  $S, T, U$ )

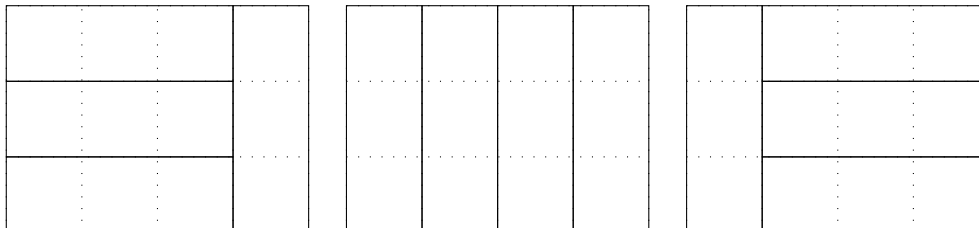
$$\forall S \forall T \forall U (|S \cup T \cup U| \geq |S| + |T| + |U| - |S \cap T| - |S \cap U| - |T \cap U|)$$

- (d) (Real numbers  $x, y, z$ )

$$\forall x \exists y \forall z (x^2 + y - \log_{10} z > 0)$$

- Solution:**
- (a) True. We know that  $V(nX) = n^2V(X)$ , variance is non-negative, and  $n^2 \geq n$ .
  - (b) True. The inverse of  $y$  must exist in  $\mathbb{Z}_p$ , so we can set  $z \equiv -y^{-1}x \pmod{p}$  to satisfy the equation for any  $x$  and  $y$ .
  - (c) True. By the inclusion-exclusion principle,  $|S \cup T \cup U| = |S| + |T| + |U| - |S \cap T| - |S \cap U| - |T \cap U| + |S \cap T \cap U|$ , so it is greater than the right hand side.
  - (d) False.

**Problem 2:** [7 pts] Let  $E_n$  be the number of ways in which you can tile a 3-by- $n$  board with 1-by-3 pieces. For example, when  $n = 4$  the board is 3-by-4 and  $E_4 = 3$ . The 3 ways are shown as follows:



- Calculate  $E_1$ ,  $E_2$ , and  $E_3$ .
- Show that  $E_n = E_{n-1} + E_{n-3}$ . (Hint: You may use a counting argument.)
- Let  $F_n$  be the Fibonacci numbers. Prove that  $E_n \leq F_n$  for all  $n \geq 1$  using induction. You may use the result of (b).

**Solution:** (a) 1, 1, 2.

- Consider the top-rightmost tile of a 3-by- $n$  board. If it is vertical, the remaining board is 3-by- $(n - 1)$ , so there are  $E_{n-1}$  ways to tile it. If it is horizontal, it must be followed by two more horizontal tiles below it, so there are  $E_{n-3}$  ways to tile it. Therefore  $E_n = E_{n-1} + E_{n-3}$ .
- We prove this statement  $P(n)$  using induction on three base cases. Observe that  $E_1 = F_1$  ( $P(1)$ ),  $E_2 = F_2$  ( $P(2)$ ), and  $E_3 = F_3$  ( $P(3)$ ). For the inductive step, suppose that  $P(k - 1)$ ,  $P(k - 2)$ , and  $P(k - 3)$  are true. Then  $E_n = E_{n-1} + E_{n-3} \leq F_{n-1} + F_{n-3} \leq F_{n-1} + F_{n-2} = F_n$ . (For the last inequality, we use the fact that the Fibonacci sequence is non-decreasing.) So  $P(k)$  is true, thus proving the statement  $P(n)$  by induction.

**Problem 3:** [7 pts]  $S$ , a set of integers, is recursively defined as follows:

*Basis:* 4914 and 3588 are in  $S$ .

*Recursive step:* If  $x, y \in S$ , then  $x - y \in S$ .

(Note that  $x$  and  $y$  may be the same.)

- (a) Let  $P(n)$  be the statement “for any integer  $a$ , if  $a \in S$  then  $an \in S$  and  $-an \in S$ .” Prove  $P(n)$  is true for all positive integers  $n$  by induction.
- (b) Let  $A_m$  be the set of all multiples of some integer  $m$ . Find the integer  $m$  such that  $S = A_m$ , and provide a complete proof of this equality, showing all steps.

**Solution:**

- (a)  $P(0)$  is true because if  $a \in S$ , applying the recursive step,  $a - a = 0 \in S$ .  $P(1)$  is true since  $a \in S$  and  $0 - a = -a \in S$ . Suppose  $P(1)$  and  $P(k)$  are true. Then  $P(k+1)$  is true because, applying the recursive step,  $-an - a = -(a+1)n \in S$  and  $an - (-a) = (a+1)n \in S$ .
- (b) Part (a) shows that  $4914s \in S$  and  $3588t \in S$  for all  $s, t$ , so  $\gcd(4914, 3588) \in S$ . Therefore

$$\begin{aligned} \gcd(4914, 3588) &= \gcd(3588, 1326) = \gcd(1326, 936) = \gcd(936, 390) \\ &= \gcd(390, 156) = \gcd(156, 78) = 78 \in S \end{aligned}$$

$A_{78} \subseteq S$ : Using part (a) directly, since  $78 \in S$ , then  $78n \in S$  for any integer  $n$ .

$S \subseteq A_{78}$ : 4914 and 3588 are multiples of 78. Suppose  $x$  and  $y$  are multiples of 78. Then clearly  $x - y$  is a multiple of 78. By structural induction,  $S \subseteq A_{78}$ .

**Problem 4:** [6 pts] For this question, no proof is required.

- (a) Fill in the following recursive definition so that  $X$  is the set of all positive integers.

*Basis:* \_\_\_\_\_  $\in X$ .

*Recursive step:* If  $a \in X$ , then  $a + 3 \in X$ .

- (b) Fill in the following recursive definition so that  $f(n) = \binom{n}{m}$ , the binomial coefficient for fixed  $m$ .

$$\begin{aligned} f(m) &= 1 \\ f(k+1) &= f(k) \end{aligned}$$

- (c) Fill in the following recursive definition so that  $S$  is the set of complete graphs.

*Basis:* \_\_\_\_\_ is in  $S$ .

*Recursive step:* Suppose that  $G = (V, E)$  is in  $S$ , where  $V = \{v_1, v_2, \dots, v_n\}$ . Then  $G' = (V', E')$  is in  $S$ , where  $V' = \{v_1, v_2, \dots, v_n, v_{n+1}\}$ , and:

$$E' = \underline{\hspace{10cm}}$$

**Solution:** (a)  $\{1, 2, 3\} \in X$ .

(b)  $f(k+1) = f(k) \cdot \frac{k+1}{k+1-m}$

- (c) Basis: The graph with one vertex and no edges is a complete graph.  
Recursive step:  $E' = E \cup \{e'_1, e'_2, \dots, e'_n\}$ , where  $e'_i$  is the edge between vertex  $i$  and  $n+1$ .

**Problem 5:** [6 pts]

- (a) For what values of  $n$  will a complete graph  $K_n$  be bipartite?
- (b) For what values of  $m, n$  will a complete bipartite graph  $K_{m,n}$  have an Euler path but not an Euler circuit?

Explain your answers.

- Solution:** (a) Only when  $n = 2$ . If  $n \geq 3$ , then consider any vertex colored blue; all of its neighbors will be colored red, and they are neighbors of each other, violating two-coloring. (We do not penalize saying  $n = 1$  is bipartite because it is an unclear edge case.)
- (b) Only when one of  $m$  or  $n$  is 2 and the other is odd. In a complete bipartite graph, each of the  $m$  vertices have degree  $n$  and each of the  $n$  vertices have degree  $m$ , and we must have exactly two vertices of odd degree.

**Problem 6:** [6 pts]

In this question, we consider simple graphs  $G = (V, E)$  with  $|V| \geq 3$  where all vertices satisfy  $\deg(v) \geq 2$ . Let us call them *two-dense* graphs.

Consider the following statement:

All two-dense graphs have a triangle subgraph (a cycle of length 3).

Here is an inductive proof of the statement.

Proof. Let the proposition  $P(n)$  be the above statement for  $|V| = n$ . We will prove  $P(n)$  is true for  $n \geq 3$ .

Base case ( $P(3)$ ): For the two-dense graph  $G$  with three vertices, each vertex has a degree of 2, so  $G$  is simply a triangle and has itself as a subgraph.

Inductive step: Suppose  $P(k)$  is true, i.e. any two-dense graph with  $K$  vertices has a triangle subgraph. Extend any such graph  $G$  to obtain  $G' = (V', E')$  by adding one vertex and at least two edges from the new vertex to any different vertices in  $|V|$ .  $G'$  is a simple graph with  $k + 1$  vertices and all vertices satisfy  $\deg(v) \geq 2$ , so  $G'$  is two-dense.  $G'$  contains  $G$  as a subgraph, so using the inductive assumption,  $G'$  also has a triangle subgraph. Therefore,  $P(k + 1)$  is true.

- (a) Give a counterexample to show that the statement is wrong.
- (b) Since the statement is wrong, the proof must be wrong as well. Choose one of the following statements to explain why the proof is wrong, and explain it.
  1. There is an error in the base case.
  2. The proof requires another base case, which has not been proven.
  3. In the inductive step,  $G'$  is wrongly constructed: sometimes it is not a two-dense graph.
  4. In the inductive step,  $G'$  may not always have a triangle subgraph.
  5. In the inductive step,  $G'$  is correct and always has a triangle subgraph, but this does not mean  $P(k + 1)$  is true.



[WORK SPACE FOR QUESTION 6]

- Solution:**
- (a) Any cycle  $C_n$  with  $n \geq 4$ .
  - (b) The correct choice is (5). Not all graphs with  $k + 1$  vertices satisfying  $\deg(v) \geq 2$  can be constructed using the procedure in the inductive step. However,  $P(k + 1)$  is a statement on all such graphs. Therefore,  $P(k + 1)$  being true does not follow from  $G'$  containing a triangle.

**Problem 7:** [6 pts] There are two bags that contain balls. The first bag contains 1 red ball and 9 blue balls and the second bag contains 9 red balls and 1 blue ball. Consider the following two scenarios:

1. You randomly choose one ball from the first bag and then put it back. Then you randomly chose another ball again from the first bag. Let  $E_1$  be the event that the first ball chosen is red, and  $E_2$  the event that the second ball chosen is red.
2. You randomly choose one of the bags, you randomly choose one ball from that bag and then you put it back. Then you randomly choose another ball from the same bag. Let  $E_1$  be the event that the first ball chosen is red, and  $E_2$  the event that the second ball chosen is red.

For both scenarios, calculate  $P(E_1)$ ,  $P(E_2)$ , and  $P(E_2|E_1)$ . Show the steps of your calculations.

**Solution:**

1. Because there are 1 red ball and 9 blue balls in the first bag,  $P(E_1) = 1/10$ .

Because the ball is placed back in the bag, there are also 1 red ball and 9 blue balls in the first bag for the second choice. So,  $P(E_2) = \frac{1}{10}$ .  
 $P(E_2|E_1) = P(E_2 \cap E_1)/P(E_1) = P(E_2)P(E_1)/P(E_1) = \frac{1}{10} \times \frac{1}{10} / \frac{1}{10} = 1/10$ .

2. Let  $B_1$  be the event that the first bag is chosen, and  $B_2$  the event that the second bag is chosen. We have

$$P(E_1) = P(B_1)P(E_1|B_1) + P(B_2)P(E_1|B_2) = \frac{1}{2} \times \frac{1}{10} + \frac{1}{2} \times \frac{9}{10} = \frac{1}{2}.$$

Because the ball is placed back in the bag, the same holds for the second choice. So,  $P(E_2) = \frac{1}{2}$ .

Next consider  $P(E_2 \cap E_1)$ :

$$P(E_2 \cap E_1) = P(B_1)P(E_2 \cap E_1|B_1) + P(B_2)P(E_2 \cap E_1|B_2)$$

The probability  $P(E_2 \cap E_1|B_1)$  is  $1/10 \cdot 1/10$  and  $P(E_2 \cap E_1|B_2)$  is  $9/10 \cdot 9/10$ , therefore

$$\begin{aligned} P(E_2 \cap E_1) &= \frac{1}{2} \times \frac{1}{10} \times \frac{1}{10} + \frac{1}{2} \times \frac{9}{10} \times \frac{9}{10} \\ &= \frac{82}{200}. \end{aligned}$$

So,

$$P(E_2|E_1) = P(E_2 \cap E_1)/P(E_1) = \frac{82}{200} / \frac{1}{2} = \frac{82}{100}.$$

It is interesting to note that, in this case,  $P(E_2|E_1) \neq P(E_2)$ .

**Problem 8:** [8 pts] Consider throwing  $m$  balls into  $n$  boxes at random. The probability that a ball ends up in any given box is  $\frac{1}{n}$ . After all balls have been thrown, let  $X$  be the number of balls in the first box and  $Y$  be the number of boxes that are empty.

- a) What is  $E(X)$ ?
- b) What is  $V(X)$ ?
- c) What is  $E(Y)$ ?

Show the steps of your calculations.

**Solution:** 1.  $E(X)$ : Each ball assignment is a Bernoulli trial with probability  $\frac{1}{n}$  of success, and there are  $m$  trials. Therefore,  $X$  follows the Binomial distribution for which we know  $E(X) = m \left( \frac{1}{n} \right) = \frac{m}{n}$

Alternative solution:

Let  $X_i$  be the indicator random variable such that  $X_i = 1$  if the  $i$ -th ball is in the first box,  $X_i = 0$  otherwise. Obviously,  $X = \sum_{i=1}^m X_i$ . For

$$1 \leq i \leq m, E(X_i) = P(\text{ball } i \text{ in the first box}) = \frac{1}{n}.$$

Therefore,

$$E(X) = E\left(\sum_{i=1}^m X_i\right) = \sum_{i=1}^m E(X_i) = \sum_{i=1}^m \frac{1}{n} = \frac{m}{n}$$

2.  $V(X)$ : Each ball assignment is a Bernoulli trial with probability  $\frac{1}{n}$  of success, and there are  $m$  trials. Therefore,  $X$  follows the Binomial distribution for which we know  $V(X) = m \left( \frac{1}{n} \right) \left( 1 - \frac{1}{n} \right) = \frac{m(n-1)}{n^2}$ .

Alternative solution:

$V(X) = V\left(\sum_{i=1}^m X_i\right) = \sum_{i=1}^m V(X_i)$  since  $X_i$  and  $X_j$  are independent for  $i \neq j$ .

$$\text{For } 1 \leq i \leq m, V(X_i) = (0 - E(X_i))^2 \left( \frac{n-1}{n} \right) + (1 - E(X_i))^2 \left( \frac{1}{n} \right) = \frac{n-1}{n^3} + \frac{(n-1)^2}{n^3} = \frac{n(n-1)}{n^3} = \frac{n-1}{n^2}$$

$$\text{Therefore, } V(X) = \sum_{i=1}^m \frac{n-1}{n^2} = \frac{m(n-1)}{n^2}$$

3.  $E(Y)$ : Let  $Y_i$  be the indicator random variable such that  $Y_i = 1$  if box  $i$  is empty,  $Y_i = 0$  otherwise. Obviously,  $Y = \sum_{i=1}^n Y_i$ .

For  $1 \leq i \leq n$ ,  $E(Y_i) = P(\text{box } i \text{ is empty}) = \left(\frac{n-1}{n}\right)^m$ .

Therefore,

$$E(Y) = E\left(\sum_{i=1}^n Y_i\right) = \sum_{i=1}^n E(Y_i) = \sum_{i=1}^n \left(\frac{n-1}{n}\right)^m = n \left(\frac{n-1}{n}\right)^m$$

**Problem 9:** [6 pts] (a) How many elements in  $\mathbb{Z}_{70}$  have multiplicative inverses? Explain your answer.

(b) Let  $\mathbb{Z}_n$  be the set of all integers modulo  $n$ . If  $n = pq$  where  $p, q$  are prime integers, prove that exactly  $(p - 1)(q - 1)$  elements from  $\mathbb{Z}_n$  have multiplicative inverses.

**Solution:** (a) We can write  $70 = 2 \cdot 5 \cdot 7$ .

$$M_7 = \{0, 7, 14, 21, 28, 35, 42, 49, 56, 63\}$$

$$M_5 = \{0, 5, 10, 15, 20, \dots, 65\}$$

$$M_2 = \{0, 2, 4, 6, \dots, 68\}$$

The integers that do not have an inverse are those that are not relatively prime with 70, i.e., all the multiples of 7, 5, 2, i.e.,  $M_7 \cup M_5 \cup M_2$ . Note that  $|M_7| = 10$ ,  $|M_5| = 14$ ,  $|M_2| = 35$ . Moreover,  $|M_7 \cap M_5| = 2$ ,  $|M_7 \cap M_2| = 5$ , and  $|M_5 \cap M_2| = 7$ . Finally,  $|M_7 \cap M_5 \cap M_2| = 1$ .

By the inclusion exclusion principle,  $|M_7 \cup M_5 \cup M_2| = 10 + 14 + 35 - 2 - 5 - 7 + 1 = 36$ . Therefore, the number of elements that have an inverse is  $70 - 36 = 24$ .

(b) Integer  $a$  has a multiplicative inverse modulo  $n = pq$ , if and only if  $\gcd(a, pq) = 1$ . Any  $a$  that is divisible by  $p$  has  $\gcd(a, pq) = p \neq 1$  and there are exactly  $q$  such values in  $\mathbb{Z}_n$ , i.e.,  $(0 \cdot p), (1 \cdot p), \dots, ((q - 1) \cdot p)$ . Likewise, any  $a$  that is divisible by  $q$  has  $\gcd(a, pq) = q \neq 1$  and there are exactly  $p$  such values in  $\mathbb{Z}_n$ , i.e.,  $(0 \cdot q), (1 \cdot q), \dots, ((p - 1) \cdot q)$ .

Since  $p, q$  are primes, if  $\gcd(a, pq) \neq 1$  then it is either  $p$  or  $q$  and these are exactly the elements  $a$  that do not have an inverse. The total number of them is  $p + q - 1$  since  $0 \cdot p = 0 \cdot q$  should not be counted twice. The total number of elements that have an inverse are thus  $pq - (p + q - 1) = (p - 1)(q - 1)$ .

**Problem 10:** [8 pts] Given a  $n \times p$  matrix  $A$  and a  $p \times m$  matrix  $B$ , the following algorithm computes the  $n \times m$  product matrix  $C = A \cdot B$ .

```

MATRIX-MULT( $A, B$ )
for  $i = 1$  to  $n$  do
    for  $j = 1$  to  $m$  do
         $C[i, j] = 0$ 
        for  $k = 1$  to  $p$  do
             $C[i, j] = C[i, j] + A[i, k] \cdot B[k, j]$ 
        end for
    end for
end for
return  $C$ 

```

a) Compute the output of the algorithm for input:

$$A = \begin{pmatrix} -1 & 1 \\ 5 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 1 & 2 \\ 0 & 1 & 4 \end{pmatrix}$$

- b) What is the  $O(\cdot)$  asymptotic complexity of the algorithm when given two matrices both of which are of size  $n \times n$ ?
- c) Express the total number of multiplications that the algorithm does, expressed as a function of  $n, m, p$ .
- d) Assume you are given three matrices  $M_1, M_2, M_3$  where  $M_1$  is  $50 \times 60$ ,  $M_2$  is  $60 \times 25$ , and  $M_3$  is  $25 \times 8$ . You want to compute the product  $M_1 \cdot M_2 \cdot M_3$ . In which order will you do the pairwise matrix multiplications, if you want to minimize the total number of multiplications?

[WORK SPACE FOR QUESTION 10]

**Answer:** a)

$$C = \begin{pmatrix} -3 & 0 & 2 \\ 15 & 5 & 10 \end{pmatrix}$$

b)  $O(n^3)$ .

c) The first loop is executed  $n$  times, therefore the second is executed  $nm$  times, and the third  $nmp$  times. At every iteration of the innermost loop a multiplication is executed, therefore the answer is  $nmp$ .

d) There are two ways to do the multiplication. Either  $M_1 \cdot M_2$  and then multiply the result with  $M_3$  from the right, or  $M_2 \cdot M_3$  and then multiply the result with  $M_1$  from the left.

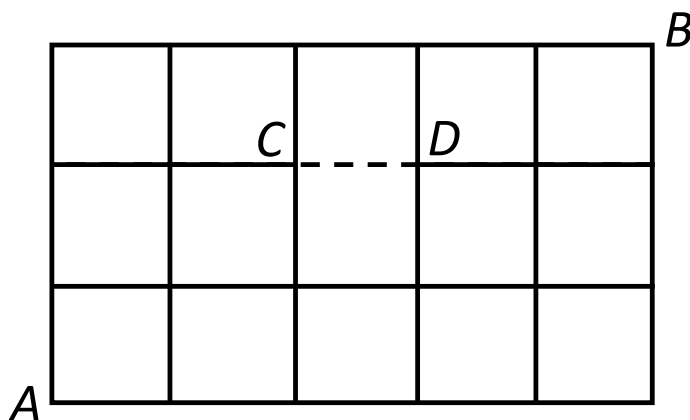
For the first case, to multiply  $M_1 \cdot M_2$  we need  $50 \cdot 60 \cdot 25$  multiplications and the result is of size  $50 \times 25$ . Multiplying this with  $M_3$  takes  $50 \cdot 25 \cdot 8$  multiplications. Total multiplications is 85000.

For the second case, to multiply  $M_2 \cdot M_3$  we need  $60 \cdot 25 \cdot 8$  multiplications and the result is of size  $60 \times 8$ . Multiplying this with  $M_1$  takes  $50 \cdot 60 \cdot 8$  multiplications. Total multiplications is 36000.

Clearly, the second approach is much faster.

**Problem 11:** [6 pts] In the following shape, consider paths that start from  $A$  and finish at  $B$  following the lines. Every path may only have steps going *up* or *right*. E.g., one path would be  $\{\uparrow, \uparrow, \uparrow, \rightarrow, \rightarrow, \rightarrow, \rightarrow, \rightarrow\}$ . How many distinct such paths are there if:

- All lines in the rectangle are possible?
- The line from  $C$  to  $D$  (the dashed line in the figure below) is missing, so paths cannot pass between  $C$  and  $D$ ?



- Answer:**
- The distance from  $A$  to  $B$  is 8 steps, 5 right, and 3 up. The answer is  $C(8, 5) = 56$ .
  - Having removed this edge, it is no longer possible to reach  $D$  from  $C$ , since down movements are not possible. Therefore, we need to subtract from the total number of paths, those that go through both  $C$  and  $D$ . There are  $C(4, 2) = 6$  paths from  $A$  to  $C$ , 1 path from  $C$  to  $D$ , and  $C(3, 2)$  from  $D$  to  $B$ , which means there are  $6 \times 1 \times 3$  paths from  $A$  to  $B$  that pass through  $C$  and  $D$ . So there are  $56 - 18 = 38$  from  $A$  to  $B$  that don't pass between use the edge between  $C$  and  $D$ .



**Problem 12:** [6 pts] For each of the following statements, prove whether it is true or false. If it is false, you can use a counterexample as a proof.

- a) Let  $f_1(x), f_2(x), g(x)$  be functions from the set of real numbers to the set of positive real numbers. If  $f_1(x)$  and  $f_2(x)$  are both  $\Theta(g(x))$ , then  $f_1(x) + f_2(x)$  is also  $\Theta(g(x))$ .
- b) Let  $f(x), g(x)$  be functions from the set of real numbers to the set of positive real numbers, If  $f(x)$  is  $O(g(x))$  then  $2^{f(x)}$  is  $O(2^{g(x)})$ .

**Answer:** a) This is true. There exist positive constraints  $C_1, C'_1, C_2, C'_2, k_1, k'_1, k_2, k'_2$ , such that  $f_1(x) \geq C_1 g(x)$  for all  $x > k_1$ ,  $f_1(x) \leq C'_1 g(x)$  for all  $x > k'_1$ ,  $f_2(x) \geq C_2 g(x)$  for all  $x > k_2$ , and  $f_2(x) \leq C'_2 g(x)$  for all  $x > k'_2$ .

Adding the first and third inequality, we get that  $f_1(x) + f_2(x) \geq (C_1 + C_2)g(x)$  for all  $x > \max\{k_1, k_2\}$ .

Adding the second and fourth inequality, we get that  $f_1(x) + f_2(x) \leq (C'_1 + C'_2)g(x)$  for all  $x > \max\{k'_1, k'_2\}$ .

Hence  $f_1(x) + f_2(x)$  is  $\Theta(g(x))$  with constraints  $(C_1 + C_2), (C'_1 + C'_2), \max\{k_1, k_2\}, \max\{k'_1, k'_2\}$ .

- b) This is false. Consider  $f(x) = 2x$  and  $g(x) = x$ . Clearly  $f(x)$  is  $O(g(x))$ . Then  $2^{f(x)} = 2^{2x} = 4^x$ , whereas  $2^{g(x)} = 2^x$ . So  $2^{f(x)}/2^{g(x)} = 2^x$ , i.e., the ratio of the two functions is not bound by any constant  $C$ , therefore  $2^{f(x)}$  is not  $O(2^{g(x)})$ .