

Assignment 1

1. Correctness of bubble sort

Bubble sort pseudo code:

BUBBLESORT(A)

1. **for** $i = 1$ **to** $A.length - 1$
2. **for** $j = A.length$ **down to** $i + 1$
3. **If** $A[j] < A[j - 1]$
4. **exchange** $A[j]$ **with** $A[j - 1]$

- a. We need to show that elements in every instance of A' form a permutation of the elements of A and in each iteration it moves the smallest element in the selected sub-array to its left most position, accumulating all the smaller elements sorted to the left part of the array until it reaches the end. This is how the above mentioned bubble sort code sorts the entire array.

b. Loop invariant for lines 2-4

Loop invariant: At the beginning of each iteration of the for loop, $A[j]$ = minimum element of the subarray $A[j..n]$ and the subarray $A[j..n]$ is a permutation of the values that were in subarray $A[j..n]$ at the time of the loop start.

Initialization: Initially, $j = n$ and the subarray $A[j..n]$ contains only a single element $A[n]$. Since the array has only one element and the element present is considered the smallest one, the loop invariant condition holds.

Maintenance: By the loop invariant, $A[j]$ is the smallest element in subarray $A[j..n]$. At the code execution lines 3-4, swap $A[j]$ and $A[j - 1]$ if $A[j]$ is less than $A[j - 1]$, which makes $A[j - 1]$ the smallest element in subarray $A[j - 1..n]$ then onwards. Since the only change to the subarray $A[j - 1..n]$ is the swap of elements, and the subarray $A[j..n]$ is a permutation of the values that were in $A[j..n]$ at the time of the loop start, we see that subarray $A[j - 1..n]$ is also a permutation of the values that were in subarray $A[j - 1..n]$ at the

time of the loop start. Gradually decrementing j for the next iteration maintains the loop invariant condition.

Termination: The loop terminates when j gradually decreases and reaches i . From the above loop invariant condition, $A[i]$ = minimum element in the subarray $A[i..n]$ and subarray $A[i..n]$ is a permutation of the values that were in subarray $A[i..n]$ at the time of the loop start.

c. Loop invariant for lines 1-4

Loop invariant: At the beginning of each iteration of the outer for loop at lines 1-4, the subarray $A[1..i-1]$ consists of the $(i-1)$ smallest elements in array $A[1..n]$ in sorted order, and the subarray $A[i..n]$ consists of the remaining $(n-i+1)$ values same as in original array $A[1..n]$.

Initialization: Initially before the execution starts, $i = 1$. The subarray $A[1..i-1]$ is empty, and since there is no element, we can simply say that the loop invariant condition holds.

Maintenance: For a given value of i in each iteration, from the above loop invariant condition, the subarray $A[1..i-1]$ consists of the i smallest values in the array $A[1..n]$ in sorted order. The above question (b) showed that after executing the for loop of lines 2-4, $A[i]$ is the smallest value in subarray $A[i..n]$, and subarray $A[1..i]$ is now the i smallest values originally in array $A[1..n]$ in sorted order. Even after the for loop at lines 2-4 permutes the subarray $A[i..n]$, the subarray $A[i+1..n]$ still consists of the $n-i$ remaining elements, same as in the original array $A[1..n]$. This process happens for each iteration of i and maintains the loop invariant condition.

Termination: When $i = n+1$, the for loop at lines 1-4 terminates so that $i-1 = n$. From the above loop invariant condition, the subarray $A[1..i-1]$ is the entire array $A[1..n]$, and it consists of the original array $A[1..n]$ elements, in sorted order. Hence on the termination of the outer for loop the entire array is sorted.

- d. The running time depends on the number of times the loops are being executed in the above code. For each value of i in the outer loop at lines 1-4, the inner loop at lines 2-4 executes $n - i$ iterations, and i takes on the values $1, 2, \dots, n - 1$. The total number of iterations in the inner loop correspondingly are as follows:

{Formula used for below summation: Sum of first n integers starting from 1 = $n * (n+1)/2$ }

$$(n - 1) + (n - 2) + \dots + 3 + 2 + 1 = n * (n - 1)/2 \\ = n^2/2 - n/2.$$

Thus the running time of bubble sort is $\Theta(n^2)$ in all cases (best, worst and average). So, the worst-case running time of bubble sort is the same as that of insertion sort worst-case running time.

2.Counting Basic Operations and Analyzing Algorithms

Algorithm

1. $l=0$
2. $k=0$
3. for $i=1$ to n do
4. $l=l + i*3$
5. if $k<n$ do
6. $k=4*i*i$
7. return (k,l)

a.

n	1	2	3	4	5
Return value (k)	4	4	4	4	16
Return value (l)	3	9	18	30	45
# multiplications ("*")	3	4	5	6	9

b. Value of $k = f(n) = 4 * (\text{ceil}(\text{sqrt}(\text{ceil}(n/4))))^2$.

Justification:

From the above code it is evident that the algorithm executes for 1 to n times for a given value of n. And based on the condition present at line-5 it enters into the if block and updates the value of 'k'.

Number of times k is updated = Number of times the condition at line-5 is satisfied.

Condition at line-5 is $(k < n)$. We can replace k with $(4 * i * i)$ since it is the value being updated in it at line-6.

$$\Rightarrow 4 * i * i < n$$

$$\Rightarrow i^2 < n/4$$

$$\Rightarrow i < \sqrt{n/4}$$

Since the initial value of k is 0, it will directly enter into the if block in line-5 initially. So we can modify the above condition as follows

$$\Rightarrow i = \sqrt{n/4}$$

And this will work for all the numbers exactly divisible by 4. But for the numbers which are not divisible by 4 we get decimal values. So in order to avoid them and to get the closest possible integer we place a ceiling.

$$\Rightarrow i = \text{ceil}(\sqrt{\text{ceil}(n/4)}) \rightarrow (\text{Equation: 1})$$

Now from code line-6 $k = 4*i*i$. Replace i with the above value

$$\Rightarrow k = 4 * (\text{ceil}(\sqrt{\text{ceil}(n/4)}))^2$$

Let us verify the same with some examples.

(i) $n = 64$ (which is divisible by 4)

The expected k value is 64. From the above formula $k = 4 * (\text{ceil}(\sqrt{\text{ceil}(n/4)})^2)$

$$\begin{aligned} \Rightarrow k &= 4 * (\text{ceil}(\sqrt{\text{ceil}(n/4)})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(\sqrt{\text{ceil}(64/4)})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(\sqrt{\text{ceil}(16)})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(\sqrt{16})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(4)^2) \\ \Rightarrow k &= 4 * (4^2) \\ \Rightarrow k &= 4 * 4 * 4 \\ \Rightarrow k &= 64. \end{aligned}$$

From the above expected = actual. Hence proved.

(ii) $n = 97$ (which is not divisible by 4)

The expected k value is 100. From the above formula $k = 4 * (\text{ceil}(\sqrt{\text{ceil}(n/4)})^2)$

$$\begin{aligned} \Rightarrow k &= 4 * (\text{ceil}(\sqrt{\text{ceil}(n/4)})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(\sqrt{\text{ceil}(97/4)})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(\sqrt{\text{ceil}(24.25)})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(\sqrt{25})^2) \\ \Rightarrow k &= 4 * (\text{ceil}(5)^2) \\ \Rightarrow k &= 4 * 5 * 5 \\ \Rightarrow k &= 100. \end{aligned}$$

From the above expected = actual. Hence proved.

c. Value of $I = f(n) = 3/2 * (n * (n+1))$.

Justification:

From the above code we can conclude that the for loop at line 3-6 executes 1 to n times for a given n. The value of I is being updated at line-4 where it is basically adding up all the values of $(3*i)$ where $(1 \leq i \leq n)$.

$$\begin{aligned}
\Rightarrow I &= \sum_{i=1}^n (3 * i) \\
\Rightarrow I &= 3 * \sum_{i=1}^n (i) \\
\Rightarrow I &= 3 * (n * (n+1))/2 \\
\Rightarrow I &= 3/2 * (n * (n+1))
\end{aligned}$$

Let us verify the same with some examples.

(i) $n = 75$

The expected value is $I = 8550$. From the above formula $I = 3/2 * (n * (n+1))$

$$\begin{aligned}
\Rightarrow 3/2 * (75 * (76)) \\
\Rightarrow 8550.
\end{aligned}$$

From the above expected = actual. Hence proved.

(ii) $n = 86$

The expected value is $I = 11223$. From the above formula $I = 3/2 * (n * (n+1))$

$$\begin{aligned}
\Rightarrow 3/2 * (86 * (87)) \\
\Rightarrow 11223.
\end{aligned}$$

From the above expected = actual. Hence proved.

d. Number of Multiplications = $f(n) = n + \text{ceil}(\text{sqrt}(\text{ceil}(n/4))) * 2$.

Justification:

From the above code, in total we have multiplications at 3 places. One at line-4 and two at line-6.

Let Number of multiplications = mul

Let Number of times line-4 executed = x

Let Number of times line-6 executed = y

$$\Rightarrow \text{mul} = x + (2 * y) \rightarrow (\text{Equation: 1})$$

From above question(b) (Equation: 1) line-6 is executed for $\text{ceil}(\sqrt{\text{ceil}(n/4)})$ times.

$$\Rightarrow y = \text{ceil}(\sqrt{\text{ceil}(n/4)}).$$

From above question(c) line-4 is executed for n times.

$$\Rightarrow x = n.$$

Substitute x and y values in (Equation: 1)

$$\Rightarrow \text{mul} = n + (2 * \text{ceil}(\sqrt{\text{ceil}(n/4)})).$$

Let us verify the same with some examples.

(i) n = 11

The expected value is mul = 15. From the above formula $\text{mul} = n + (2 * \text{ceil}(\sqrt{\text{ceil}(n/4)}))$.

$$\Rightarrow \text{mul} = 11 + (2 * \text{ceil}(\sqrt{\text{ceil}(11/4)}))$$

$$\Rightarrow \text{mul} = 11 + (2 * \text{ceil}(\sqrt{3}))$$

$$\Rightarrow \text{mul} = 11 + (2 * 2)$$

$$\Rightarrow \text{mul} = 15.$$

From the above expected = actual. Hence proved.

(ii) n = 60

The expected value is mul = 68. From the above formula $\text{mul} = n + (2 * \text{ceil}(\sqrt{\text{ceil}(n/4)}))$.

$$\Rightarrow \text{mul} = 60 + (2 * \text{ceil}(\sqrt{\text{ceil}(60/4)}))$$

$$\Rightarrow \text{mul} = 60 + (2 * \text{ceil}(\sqrt{15}))$$

$$\Rightarrow \text{mul} = 60 + (2 * 4)$$

$$\Rightarrow \text{mul} = 68.$$

From the above expected = actual. Hence proved.

3. Practice working with asymptotic notation.

The decreasing order of the functions by their asymptotic growth is as follows.

$$1) 2\sqrt{n^3} \text{ is order of } \sqrt{n^3}$$

$$\Rightarrow 2\sqrt{n^3}$$

$$\Rightarrow \sqrt{n^3}.$$

$$2) 7 * \log(n!) \text{ is the order of } n * \log(n)$$

$$\Rightarrow n * \log(n) - (n * \log e) + O(\log n) \text{ (Using stirling's approximation for factorials)}$$

$$\Rightarrow n * \log(n).$$

$$3) 5 * e^{\ln(n)} \text{ is the order of } n ("*").$$

$$\Rightarrow 5 * e^{\log_e(n)}$$

$$\Rightarrow 5 * n.$$

$$4) n/4 \text{ is the order of } n ("*").$$

$$5) 4 * \sqrt{n} \text{ is the order of } \sqrt{n}.$$

$$6) 6 * \ln(n^2) \text{ is the order of } \log(n).$$

$$7) 3 * 2^{-2n} \text{ is the order of } 1/2^n$$

$$\Rightarrow 3 / 2^{(2*n)}$$

$$\Rightarrow (3 / 4) * (1/2^n).$$

From all the above $(5 * e^{\ln(n)})$ and $(n/4)$ are asymptotically equal.

Justification:

- Comparing (1) and (2). By applying the limits:

$$\Rightarrow \lim_{n \rightarrow \infty} (2 * n^{3/2}) / (7 * \log(n!))$$

$$\Rightarrow \lim_{n \rightarrow \infty} (2 * n^{3/2}) / (7 * n * \log(n)) \text{ (Using stirling's}$$

$$\text{approximation } \log(n!) = n * \log(n) - (n * \log e) + O(\log(n)) = (n * \log(n)) \text{ approximately) (Applying L'Hopital's Rule on top of it)}$$

$$\Rightarrow \lim_{n \rightarrow \infty} (3 * n^{1/2}) / (7 * (\log(n)+1))$$

$$\Rightarrow \lim_{n \rightarrow \infty} (3/2 * n^{-1/2}) / (7/n)$$

$$\Rightarrow \lim_{n \rightarrow \infty} ((3 * \sqrt{n}) / 14)$$

$$\Rightarrow \infty \text{ (i.e. } f(n) \in \omega(g(n)) \text{)}$$

From the formal definition $f(n) \in \omega(g(n))$ for all $c, n_0 > 0$

then $f(n) > c \cdot (g(n)) \geq 0$ for all $n \geq n_0$. (Since it is satisfying strictly greater than condition that means it will also satisfy equal to case $f(n) \geq c \cdot (g(n)) \geq 0$, i.e. $f(n) \in \Omega(g(n))$)

Therefore $2\sqrt{n^3} > (7 * \log(n!))$.

- Comparing (2) and (3):

$$\Rightarrow \lim_{n \rightarrow \infty} (7 * \log(n!)) / (5 * e^{\ln(n)})$$

$$\Rightarrow \lim_{n \rightarrow \infty} (7 * n * \log(n)) / (5 * e^{\log_e(n)}) \text{ (Using stirling's}$$

approximation $\log(n!) = n * \log(n) - (n * \log e) + O(\log(n)) = (n * \log(n))$ approximately)

$$\Rightarrow \lim_{n \rightarrow \infty} (7 * n * \log(n)) / (5 * n)$$

$$\Rightarrow \lim_{n \rightarrow \infty} (7 * \log(n)) / (5)$$

$$\Rightarrow \infty \text{ (i.e. } f(n) \in \omega(g(n)) \text{)}$$

From the formal definition $f(n) \in \omega(g(n))$ for all $c, n_0 > 0$

then $f(n) > c \cdot (g(n)) \geq 0$ for all $n \geq n_0$. (Since it is satisfying strictly greater than condition that means it will also satisfy equal to case $f(n) \geq c \cdot (g(n)) \geq 0$, i.e. $f(n) \in \Omega(g(n))$)

Therefore $(7 * \log(n!)) > (5 * e^{\ln(n)})$.

- Comparing (3) and (4):

$$\Rightarrow \lim_{n \rightarrow \infty} (5 * e^{\ln(n)}) / (n/4)$$

$$\Rightarrow \lim_{n \rightarrow \infty} (5 * e^{\log_e(n)}) / (n/4)$$

$$\Rightarrow \lim_{n \rightarrow \infty} (5 * n) / (n/4)$$

$$\Rightarrow 20 > 0 \text{ (i.e. } f(n) \in \theta(g(n)) \text{)}$$

From the formal definition $\theta(g(n)) = O(g(n)) \cap \Omega(g(n))$

Therefore $(5 * e^{\ln(n)})$ and $(n/4)$ are asymptotically equal.

- Comparing (4) and (5):

$$\Rightarrow \lim_{n \rightarrow \infty} (n/4) / (4 * \sqrt{n})$$

$$\Rightarrow \lim_{n \rightarrow \infty} (\sqrt{n}) / (4 * 4)$$

$$\Rightarrow \lim_{n \rightarrow \infty} (\sqrt{n} / 16)$$

$$\Rightarrow \infty \text{ (i.e. } f(n) \in \omega(g(n)) \text{)}$$

From the formal definition $f(n) \in \omega(g(n))$ for all $c, n_0 > 0$

then $f(n) > c \cdot g(n) > 0$ for all $n \geq n_0$. (Since it is satisfying strictly greater than condition that means it will also satisfy equal to case $f(n) \geq c \cdot g(n) > 0$, i.e. $f(n) \in \Omega(g(n))$)

Therefore $(n/4) > (4 * \sqrt{n})$.

- Comparing (5) and (6). By applying the limits:

$$\Rightarrow \lim_{n \rightarrow \infty} (4 * \sqrt{n}) / (6 * \ln(n^2))$$

$$\Rightarrow \lim_{n \rightarrow \infty} (4 * \sqrt{n}) / (6 * \log(n^2) / \log(e))$$

$$\Rightarrow \lim_{n \rightarrow \infty} (4 * \sqrt{n} * \log(e)) / (6 * \log(n^2)) \text{ (Applying L'Hopital's$$

Rule)

$$\Rightarrow \lim_{n \rightarrow \infty} (n^{-1/2} * \log(e) * n) / (3 * 2)$$

$$\Rightarrow \lim_{n \rightarrow \infty} (\sqrt{n} * \log(e)) / 6$$

$$\Rightarrow \infty \text{ (i.e. } f(n) \in \omega(g(n)) \text{)}$$

From the formal definition $f(n) \in \omega(g(n))$ for all $c, n_0 > 0$

then $f(n) > c \cdot g(n) > 0$ for all $n \geq n_0$. (Since it is satisfying strictly greater than condition that means it will also satisfy equal to case $f(n) \geq c \cdot g(n) > 0$, i.e. $f(n) \in \Omega(g(n))$)

Therefore $(4 * \sqrt{n}) > (6 * \ln(n^2))$.

- Comparing (6) and (7):

$$\Rightarrow \lim_{n \rightarrow \infty} (6 * \ln(n^2)) / (3 * 2^{-2n})$$

$$\Rightarrow \lim_{n \rightarrow \infty} (6 * \log(n^2) / \log(e)) / ((3 / 4^n))$$

$$\Rightarrow \lim_{n \rightarrow \infty} (6 * \log(n^2) * 4^n) / (3 * \log(e))$$

$$\Rightarrow \lim_{n \rightarrow \infty} (2 * \log(n^2) * 4^n) / (\log(e))$$

$$\Rightarrow \infty \text{ (i.e. } f(n) \in \omega(g(n)) \text{)}$$

From the formal definition $f(n) \in \omega(g(n))$ for all $c, n_0 > 0$

then $f(n) > c \cdot (g(n)) \geq 0$ for all $n \geq n_0$. (Since it is satisfying strictly greater than condition that means it will also satisfy equal to case $f(n) \geq c \cdot (g(n)) \geq 0$, i.e. $f(n) \in \Omega(g(n))$)

Therefore $(6 * \ln(n^2)) > (3 * 2^{-2n})$.

4. Prove or disprove rigorously.

a. $n^3 - 2n^2 + 3n \in \Omega(n^2)$

Proof:

$$f(n) = n^3 - 2n^2 + 3n$$

$$g(n) = n^2$$

$$\Rightarrow n^3 - 2n^2 + 3n \geq 0 \text{ (for all } n \geq 0 \text{)}$$

$$\Rightarrow n^3 - 2n^2 + 3n \geq -2n^2 + 3n \text{ (for all } n \geq 0 \text{)}$$

$$\Rightarrow n^3 - 2n^2 + 3n \geq -2n^2 + 3n^2 \text{ (for all } n \geq 0 \text{)}$$

$$\Rightarrow n^3 - 2n^2 + 3n \geq n^2 \text{ (for all } n \geq 0 \text{)}$$

From the formal definition $f(n) \in \Omega(g(n))$ for all $c, n_0 > 0$

then $f(n) \geq c \cdot (g(n)) \geq 0$ for all $n \geq n_0$.

Therefore we choose $n_0 = 1$, and $c = 1$.

b. $4n^2 - n - n \log(n) - \log(n) \in \omega(n^2)$

Proof:

$$f(n) = 4n^2 - n - n \log(n) - \log(n)$$

$$g(n) = n^2$$

$$\Rightarrow 4n^2 - n - n \log(n) - \log(n) \geq 0 \text{ (for all } n \geq 0 \text{)}$$

$$\Rightarrow 4n^2 - n - n \log(n) - \log(n) > 4n^2 - n - n \log(n) - n^2 \text{ (for all } n > 0 \text{)}$$

$$\Rightarrow 4n^2 - n - n \log(n) - \log(n) > 3n^2 - n^2 - n \log(n) \text{ (for all } n > 0 \text{)}$$

$$\Rightarrow 4n^2 - n - n \log(n) - \log(n) > 2n^2 - n \log(n) \text{ (for all } n > 0 \text{)}$$

$$\Rightarrow 4n^2 - n - n \log(n) - \log(n) > 2n^2 - n^2 \text{ (for all } n > 0 \text{)}$$

$$\Rightarrow 4n^2 - n - n \log(n) - \log(n) > n^2 \text{ (for all } n > 0 \text{)}$$

From the formal definition $f(n) \in \omega(g(n))$ for all $c, n_0 > 0$
then $f(n) > c \cdot g(n) > 0$ for all $n \geq n_0$.
Therefore we choose $n_0 = 1$, and $c = 1$.

c. $\sum_{i=1}^n i^{3/2} \in O(n^{5/2})$

Proof:

$$f(n) = \sum_{i=1}^n i^{3/2}$$

$$g(n) = O(n^{5/2})$$

$$\Rightarrow 0 \leq 1^{3/2} + 2^{3/2} + 3^{3/2} + \dots + n^{3/2} \text{ (for all } n \geq 0)$$

$$\Rightarrow 1^{3/2} + 2^{3/2} + 3^{3/2} + \dots + n^{3/2} \leq n^{3/2} + n^{3/2} + n^{3/2} + \dots +$$

$n^{3/2}$

$$\Rightarrow 1^{3/2} + 2^{3/2} + 3^{3/2} + \dots + n^{3/2} \leq n \cdot n^{3/2} \text{ (for all } n > 0)$$

$$\Rightarrow 1^{3/2} + 2^{3/2} + 3^{3/2} + \dots + n^{3/2} \leq n^{5/2} \text{ (for all } n > 0).$$

From the formal definition $f(n) \in O(g(n))$ for all $c, n_0 > 0$
then $0 \leq f(n) \leq c \cdot g(n)$ for all $n \geq n_0$.
Therefore we choose $n_0 = 1$, and $c = 1$.

5. Design, Analyse and communicate algorithms.

Algorithm

// Method to perform matrix multiplication.

1. matrixMultiply(A, B)

2. C = {{0,0}, {0,0}}

3. for i=0 to A.length do

4. for j=0 to B.length do

5. for k=0 to C.length do

6. C[i][j] += A[i][k] * B[k][j]

7. return C

// Method to calculate A to power of n using divide and conquer.

8. multiply(A, n)

9. if(n < 1) do

10. return {{1,0}, {0,1}}

11. else if(n%2 == 0) do

12. return multiply(matrixMultiply(A, A), n/2)

```

13.  else do
14.      return matrixMultiply(A,
multiply(matrixMultiply(A, A), (n-1)/2))

```

Textual Explanation:

If n is less than 1:
 return identity matrix

Else:

If n is odd:

A * recursive call with parameters(A^2 , (n-1)/2)

Else:

recursive call with parameters(A^2 , n/2)

(In the recursive call with parameters, the first argument is multiplying A with itself which will be used for computing A^n while popping off from the stack and the second argument is n/2 in case of even 'n' and (n-1)/2 in case of odd 'n' which basically reduces 'n' by half to perform a Divide and Conquer).

Example:

$A = \{\{2, 0\}, \{0, 2\}\}$

Calculate A^5

In the below explanation $\text{matrixMultiply}(A^i, A^j)$ will be written as A^{i+j} For example $\text{matrixMultiply}(A, A)$ is A^2 .

In order to calculate A to the power of 5. We make a function call $\text{multiply}(A, 5)$.

- Step 1: Initially when $\text{multiply}(A, 5)$ is called the execution enters into the condition block at lines 13-14 and again a function call ($A * \text{multiply}(A^2, 2)$) is called.

- Step 2: Now in this function call $\text{multiply}(A^2, 2)$ the execution enters into the condition block at lines 11-12 and again a function call $\text{multiply}(A^4, 1)$ is called.
- Step 3: Now in this function call $\text{multiply}(A^4, 1)$ the execution enters into the condition block at lines 13-14 and again a function call $(A * \text{multiply}(A^8, 0))$ is called.
Now at this point of time we have all these calls in the recursion stack.

$\text{multiply}(A, 5) \rightarrow \text{multiply}(A^2, 2) \rightarrow \text{multiply}(A^4, 1) \rightarrow \text{multiply}(A^8, 0)$

Now from the next steps onwards we keep track of this stack and the return value of each function.

- Step 4: Now in this function call $\text{multiply}(A^8, 0)$ the execution enters into the condition block at lines 9-10 and returns $\{\{1,0\}, \{0,1\}\}$. From here onwards we start popping from the stack.
- Step 5:
stack: $\text{multiply}(A, 5) \rightarrow \text{multiply}(A^2, 2) \rightarrow \text{multiply}(A^4, 1)$
Return Value from previous function call: $\{\{1,0\}, \{0,1\}\}$

Now in this function call $\text{multiply}(A^4, 1)$ according to the Step 3 we compute $A^4 * \{\{1,0\}, \{0,1\}\}$ which is $\{\{16,0\}, \{0,16\}\}$ and return it.

- Step 6:
stack: $\text{multiply}(A, 5) \rightarrow \text{multiply}(A^2, 2)$
Return Value from previous function call: $\{\{16,0\}, \{0,16\}\}$

Now in this function call $\text{multiply}(A^2, 2)$ according to Step 2 we simply return $\{\{16,0\}, \{0,16\}\}$ as the output.

- Step 7:

stack: multiply(A, 5)

Return Value from previous function call: $\{\{16,0\}, \{0,16\}\}$

Now in this function call multiply(A, 5) according to Step 1 we simply return $A * \{\{16,0\}, \{0,16\}\}$ which is $\{\{32,0\}, \{0,32\}\}$ and return it as the final output.

This is how the above algorithm works to calculate A^n for a square matrix.

Asymptotic runtime of the algorithm:

$$\begin{array}{ll} T(n) = 1 & \text{if } n < 1 \\ T(n) = T(n/2) + 1 & \text{Otherwise} \end{array}$$

For example $n = 4^k$

$$\begin{aligned} \text{Then applying log on both sides } &=> \log(n) = \log(4^k) \\ &=> \log(n) = \log(2^{2k}) \\ &=> \log(n) = 2k \\ &=> k = \log(n)/2. \text{ (Equation: 1)} \end{aligned}$$

$$T(0) = 1$$

$$T(4^0) = T(1) = T(0) + 1 = 1 + 1 = 2$$

$$T(2) = T(1) + 1 = 2 + 1 = 3$$

$$T(4^1) = T(4) = T(2) + 1 = 4$$

$$T(8) = T(4) + 1 = 5$$

$$T(4^2) = T(16) = T(8) + 1 = 6$$

$$T(32) = T(16) + 1 = 7$$

$$T(4^3) = T(64) = T(32) + 1 = 8$$

$$T(128) = T(64) + 1 = 9$$

$$T(4^4) = T(256) = T(128) + 1 = 10$$

.
.
.

$$\begin{aligned}
 T(4^k) &= (2*k) + 2 = (2 * \log(n)/2) + 2 \text{ (from Equation: 1)} \\
 &= \mathbf{\log(n) + 2}
 \end{aligned}$$

There the asymptotic runtime of the above algorithm is **$\log(n)$** .

Correctness of the Algorithm:

Recursion invariant condition: At each recursive call in the execution, multiply(A,n) always returns A^k where $k \leq n$.

Initialization (Base Condition): When the divide and conquer is reached to the lowest granular level where $n = 0$, the multiply(A, n) returns the Identity matrix $(I) = \{\{1,0\},\{0,1\}\}$. Because in the lowest granular level $n = 0$ and anything to the power of 0 should be 1 which basically represents identity in case of number, similarly in case of matrices we are defining identity as the identity matrix. Hence $A^0 = I$ where $I = \{\{1,0\}, \{0,1\}\}$.

Maintenance: The main control logic of our code deals with two cases. When n is even, then the algorithm at lines 11-12 reduces n to $n/2$, until n approaches to 0 and once the recursion stack starts popping out the function calls, the algorithm then returns $A^{k/2} * A^{k/2} = A^k$ where $k \leq n$. And when n is odd, then the algorithm at lines 13-14 reduces n to $(n - 1)/2$, until n approaches to 0 and once the recursion stack starts popping out the function calls, the algorithm then returns $A * A^{(k-1)/2} * A^{(k-1)/2} = A^k$ where $k \leq n$. Thus, the recursion invariant condition is maintained.

Termination: When the last function call in the stack is popped off, multiply(A, n) gives A^n , which is the final solution to the problem. Hence proved.