My name and student number: Joseph Siu, 1010085701. Sanchit Manchanda, Ali Zaki Rashid.

Claim of Question 1. After $\mathrm{AUX}(\mathrm{A}, 4)$ is terminated, A remains the same as the initial $A = [2, 1, 4, 3]$.

We will use L1, L2 to represent "line 1, line 2" and so on for simplicity.

Proof of Question 1.

First, call $\mathrm{AUX}(\mathrm{A}, 4)$.

$(\mathrm{AUX}(\mathrm{A}[1..4], 4))$. On L1 since $4 > 2$, we enter L2. On L2 and L3 we swap the values of A[2] and A[3]. Now we have $A = [2, 4, 1, 3]$. After that, on L4 we call $\mathrm{AUX}(\mathrm{A}[1..2], 2)$, to avoid ambiguity, let $\mathrm{A}'[1..2] = \mathrm{A}[1..2]$ be the alias array passed into $\mathrm{AUX}(\mathrm{A}[1..2], 2)$. By alias we mean that swaps performed on, e.g., $\mathrm{A}'[1..2]$ will also affect A[1..2].

$(\mathrm{AUX}(\mathrm{A}[1..4], 4) \to \mathrm{AUX}(\mathrm{A}'[1..2], 2))$. Since $\mathrm{NOT}(2 > 2)$, we jump to L7. Since $\mathrm{NOT}(A'[1] > A'[2])$, no swap has performed from $\mathrm{AUX}(\mathrm{A}'[1..2], 2)$. We terminates our $\mathrm{AUX}(\mathrm{A}'[1..2], 2)$ after this.

$(\mathrm{AUX}(\mathrm{A}[1..4], 4))$. On L5 we call $\mathrm{AUX}(\mathrm{A}[3..4], 2)$, to avoid ambiguity, let $\mathrm{A}''[1..2] = \mathrm{A}[3..4]$ be the alias array passed into $\mathrm{AUX}(\mathrm{A}[3..4], 2)$.

$(\mathrm{AUX}(\mathrm{A}[1..4], 4) \to \mathrm{AUX}(\mathrm{A}''[1..2], 2))$. Since $\mathrm{NOT}(2 > 2)$, we jump to L7. Since $\mathrm{NOT}(A''[1] > A''[2])$, no swap has performed from $\mathrm{AUX}(\mathrm{A}''[1..2], 2)$. We terminates our $\mathrm{AUX}(\mathrm{A}''[1..2], 2)$ after this.

$(\mathrm{AUX}(\mathrm{A}[1..4], 4))$. On L6 we call $\mathrm{AUX}(\mathrm{A}[2..3], 2)$, to avoid ambiguity, let $\mathrm{A}'''[1..2] = \mathrm{A}[2..3]$ be the alias array passed into $\mathrm{AUX}(\mathrm{A}[2..3], 2)$.

$(\mathrm{AUX}(\mathrm{A}[1..4], 4) \to \mathrm{AUX}(\mathrm{A}'''[1..2], 2))$. Since $\mathrm{NOT}(2 > 2)$, we jump to L7. Since $4 > 1$, that is, $\mathrm{A}'''[1] > \mathrm{A}'''[2]$, we enter L8 and swap the values of $\mathrm{A}'''[1]$ and $\mathrm{A}'''[2]$. Now we have $\mathrm{A}''' = [1, 4]$. We terminates our $\mathrm{AUX}(\mathrm{A}'''[1..2], 2)$ after this. Now we have $\mathrm{A} = [2, 1, 4, 3]$.

$(\mathrm{AUX}(\mathrm{A}[1..4], 4))$. After L6 has performed, we terminate our call of $\mathrm{AUX}(\mathrm{A}[1..4], 4)$. Now we have $\mathrm{A} = [2, 1, 4, 3]$, which justifies our claim.

Define the set $S = \{2^a \mid a \in \mathbb{Z}^+\}$, since $S \subseteq \mathbb{N}$, it has a total order.

Claim of Question 2. $\mathrm{AUX}(\mathrm{A}[1..n], n)$ satisfies the following specifications:

Preconditions:

1. $n \in S$, the elements $\mathrm{A}[1..n]$ are from the same totally ordered set.
2. $\mathrm{A}[1..\frac{n}{2}]$ and $\mathrm{A}[\left(\frac{n}{2}+1\right)..n]$ are sorted in non-decreasing order. Namely $\forall i \in \mathbb{Z}^+.\forall j \in \mathbb{Z}^+.\left[\left(1 \le i < j \le \frac{n}{2}\right) \text{ IMPLIES } (\mathrm{A}[i] \le \mathrm{A}[j])\right]$, and $\forall i \in \mathbb{Z}^+.\forall j \in \mathbb{Z}^+.\left[\left(\frac{n}{2}+1 \le i < j \le n\right) \text{ IMPLIES } (\mathrm{A}[i] \le \mathrm{A}[j])\right]$.

Postconditions:

1. n and the multiset of elements in $\mathrm{A}[1..n]$ are not changed.
2. $\mathrm{A}[1..n]$ is sorted in non-decreasing order: $\forall i \in \mathbb{Z}^+.\forall j \in \mathbb{Z}^+.\left[(1 \le i < j \le n) \text{ IMPLIES } (\mathrm{A}[i] \le \mathrm{A}[j])\right]$.

Termination: The algorithm terminates.

Justification. First, from question n must be a power of 2, and to compare the first 2 elements of $\mathrm{A}[1..n]$ we n has to be at least 2^1, this is precisely how we defined our S. Moreover, to compare the elements $\mathrm{A}[1..n]$ they need to be in the same totally ordered domain. Furthermore, the algorithm should terminate whenever it is executed to be correct, and at that time our given n should not be changed. Also, since this is the auxillary function of a sorting algorithm, the multiset of $\mathrm{A}[1..n]$ should not be changed, and $\mathrm{A}[1..n]$ should be sorted in non-decreasing order since we are swaping the larger elements from beginning to end (right).

Proof of Question 3 by induction on S.

For $n \in S$, let $P(n) =$ "for all array $\mathrm{A}[1..n]$ with elements from a totally ordered set and $\mathrm{A}[1..\frac{n}{2}]$ and $\mathrm{A}[\left(\frac{n}{2}+1\right)..n]$ are sorted in non-decreasing order, if $\mathrm{AUX}(\mathrm{A}[1..n], n)$ is performed, then it eventually halts, at which time $\mathrm{A}[1..n]$ is sorted in non-decreasing order, n and the multiset of elements in $\mathrm{A}[1..n]$ are unchanged".

To prove $\forall n \in S.P(n)$, it is equivalent to prove $\forall n \in \mathbb{Z}^+.P(2^n)$ by our definition of S. That is, we will first show $P(2^1)$ holds as the base case, then for arbitrary $n \in \mathbb{Z}^+$, we will assume $P(2^n)$ and show $P(2^{n+1})$.

Base Case: $n = 1$.

Let A[1..2^1] be arbitrary array with elements from a totally ordered set, and A[1..1] and A[2..2] are sorted in non-decreasing order (which are trivially sorted in non-decreasing order for all array when $n = 1$).

Assume AUX(A[1..2], 2) is called.

Since NOT($2 > 2$), we jump to L7:

Case 1. $A[1] > A[2]$.

We enter L8 and swap the values of A[1] and A[2]. Now A[1..2] is sorted in non-decreasing order, and the multiset of elements in A[1..2] is unchanged. We terminates our AUX(A[1..2], 2) after this. No assignment to n thus n is unchanged.

For Case 1 we have shown the call halts and at that time $A[1..2]$ is sorted in non-decreasing order, n and the multiset of elements in A[1..2] are unchanged.

Case 2. NOT($A[1] > A[2]$).

Since NOT($A[1] > A[2]$), which is equivalent to $A[1] \leq A[2]$, this already shows that A[1..2] is sorted in non-decreasing order, and the multiset of elements A[1..2] is trivially unchanged. We terminates our AUX(A[1..2], 2) after this. No assignment to n thus n is unchanged.

For Case 2 we have shown the call halts and at that time $A[1..2]$ is sorted in non-decreasing order, n and the multiset of elements in A[1..2] are unchanged.

For all cases we have shown the call halts and at that time A[1..2] is sorted in non-decreasing order, n and the multiset of elements in A[1..2] are unchanged. Thus we conclude the call halts and at that time A[1..2] is sorted in non-decreasing order, n and the multiset of elements in A[1..2] are unchanged.

By direct proof, we have shown if AUX(A[1..2], 2) is performed, then it eventually halts, at which time A[1..2] is sorted in non-decreasing order, n and the multiset of elements in A[1..2] are unchanged.

Since $A[1..2^1]$ is arbitrary, by definition we have shown $P(2^1)$.

Let $n \in \mathbb{Z}^+$ be arbitrary;

Assume $P(2^n)$.

Let A[1..2^{n+1}] be arbitrary array with elements from a totally ordered set, and A[1..2^n] and A[$(2^n + 1)$ ..2^{n+1}] are sorted in non-decreasing order.

Assume AUX(A[1..2^{n+1}], 2^{n+1}) is called.

Since $n \geq 1$, this implies $n + 1 \geq 2$ and so $2^{n+1} \geq 2^2 = 4$. Thus $2^{n+1} > 2$ and we enter L2.

Because $2^n \geq 2$, A[1..2^n] and A[($2^n + 1$)..2^{n+1}] both contain at least 2 and an even number of elements respectively, so this means we are allowed to split the arrays equally (w.r.t. the size) respectively so that there is no empty array or invalid index. For the sake of clarification: let B[1..2^{n-1}] = B (that is, let B[1..2^{n-1}], where we will also use B to represent such array), C[1..2^{n-1}] = C, D[1..2^{n-1}] = D, E[1..2^{n-1}] = E be a copy, which will not be changed, (for simplicity, we will assume our array copies throughout this proof will not be changed when the original array has been modified) of the original array A[1..2^{n-1}], A[$\left(2^{n-1} + 1\right)$ ..2^n], A[$2^n + 1$.. $\left(2^n + 2^{n-1}\right)$], A[$\left(2^n + 2^{n-1} + 1\right)$ ..2^{n+1}] respectively. We will also denote A for A[1..2^{n+1}].

For simplicity, we will simply say sorted instead of sorted in decreasing order throughout this proof.

At the start of L2, by our construction, we have now A = B · C · D · E (concatenation of arrays).

Since we assumed A[1..2^n] = B · C and A[$(2^n + 1)$ ..2^{n+1}] = D · E are sorted, we have B, C, D, E are also sorted.

Now, on L2 and L3, we swap the values of $\mathrm{A}[i+2^{n+1-2}]$ and $\mathrm{A}[i+2^{n+1-1}]$ for $i \in [2^{n+1-2}]$ (set of integers from 1 to 2^{n+1-2} as introduced in assignment 6). After this, we have $\mathrm{A} = \mathrm{B} \cdot \mathrm{D} \cdot \mathrm{C} \cdot \mathrm{E}$, so we can see the multiset of elements in A is unchanged compared to the initial $\mathrm{A}[1..n]$ which was passed from the call (for simplicity we will simply say "unchanged" instead of "unchanged compared to the initial $\mathrm{A}[1..n]$ which was passed from the call").

On L4, we call $\mathrm{AUX}(\mathrm{A}[1..2^n, 2^n)$. Since we assumed $P(2^n)$, by specialization and modus ponens, we have $\mathrm{AUX}(\mathrm{A}[1..2^n, 2^n)$ terminates and at that time $\mathrm{A}[1..2^n]$ is sorted. Also, the multiset of elements in $\mathrm{A}[1..2^n]$ is unchanged, thus, the multiset of elements in A is also unchanged.

Now, let $B'[1..2^{n-1}] = B', D'[1..2^{n-1}] = D'$ be a copy of $\mathrm{A}[1..2^{n-1}], \mathrm{A}[\left(2^{n-1}+1\right)..2^n]$ respectively. After L4 we have $\mathrm{A} = \mathrm{B}' \cdot \mathrm{D}' \cdot \mathrm{C} \cdot \mathrm{E}$, and B', D', $\mathrm{B}' \cdot \mathrm{D}'$ are sorted respectively.

On L5, we call $\mathrm{AUX}(\mathrm{A}[(2^n+1)..2^{n+1}], 2^n)$. Since we assumed $P(2^n)$, by specialization and modus ponens, we have $\mathrm{AUX}(\mathrm{A}[(2^n+1)..2^{n+1}], 2^n)$ terminates and at that time $\mathrm{A}[(2^n+1)..2^{n+1}]$ is sorted. Also, the multiset of elements in $\mathrm{A}[(2^n+1)..2^{n+1}]$ is unchanged, thus, the multiset of elements in A is also unchanged.

Now, let $\mathrm{C}'[1..2^{n-1}] = \mathrm{C}', \mathrm{E}'[1..2^{n-1}] = \mathrm{E}'$ be a copy of $\mathrm{A}[(2^n+1), \left(2^n+2^{n-1}\right)], \mathrm{A}[\left(2^n+2^{n-1}+1\right)..2^{n+1}]$ respectively. After L5 we have $\mathrm{A} = \mathrm{B}' \cdot \mathrm{D}' \cdot \mathrm{C}' \cdot \mathrm{E}'$, and C', E', $\mathrm{C}' \cdot \mathrm{E}'$ are sorted respectively.

On L6, we call $\mathrm{AUX}(\mathrm{A}[\left(2^{n-1}+1\right)..\left(2^n+2^{n-1}\right)], 2^n)$. Since we assumed $P(2^n)$, by specialization and modus ponens, we have $\mathrm{AUX}(\mathrm{A}[\left(2^{n-1}+1\right)..\left(2^n+2^{n-1}\right)], 2^n)$ terminates and at that time $\mathrm{A}[\left(2^{n-1}+1\right)..\left(2^n+2^{n-1}\right)]$ is sorted. Also, the multiset of elements in $\mathrm{A}[\left(2^{n-1}+1\right)..\left(2^n+2^{n-1}\right)]$ is unchanged, thus, the multiset of elements in A is also unchanged.

Now, let $\mathrm{D}''[1..2^{n-1}] = \mathrm{D}''$, $\mathrm{C}''[1..2^{n-1}] = \mathrm{C}''$ be a copy of $\mathrm{A}[\left(2^{n-1}+1\right)..(2^n)]$ and $\mathrm{A}[(2^n+1)..\left(2^n+2^{n-1}\right)]$ respectively. After L6 we have $\mathrm{A} = \mathrm{B}' \cdot \mathrm{D}'' \cdot \mathrm{C}'' \cdot \mathrm{E}'$, and D'', C'' are sorted respectively.

After L6 has performed, we are about to terminate our call of $\mathrm{AUX}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$, thus we have shown $\mathrm{AUX}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$ eventually halts.

Since for all lines the multiset of elements in A is unchanged, we conclude the multiset of elements in A immediately before halts (and thus when it halts) is also unchanged. Also, there is no assignment to n thus n is unchanged.

Now we show that $\mathrm{A} = \mathrm{B}' \cdot \mathrm{D}'' \cdot \mathrm{C}'' \cdot \mathrm{E}'$ immediately before halts (and thus when it halts) is sorted.

To this end, we will first prove some lemmas.

Let $\mathrm{A}'[1..2^{n+1}] = \mathrm{A}'$ be the sorted permutation of A, since the multiset of A is unchanged, this means A' is also the sorted permutation of our initial A which was passed from the call $\mathrm{AUX}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$.

Lemma 1. $\mathrm{B}' = \mathrm{A}'[1..2^{n-1}]$, that is, B' is the array containing 2^{n-1} smallest elements in A.

Proof of Lemma 1.

To prove Lemma 1, since by construction of B' we know B' is the array containing 2^{n-1} smallest elements in $\mathrm{B} \cdot \mathrm{D}$, so it is equivalent to show that all 2^{n-1} smallest elements in A are also in $\mathrm{B} \cdot \mathrm{D}$. In other words, there does not exists $a \in \mathrm{C} \cdot \mathrm{E}$ such that a is strictly smaller than the largest element in B'.

To obtain a contradiction, assume there exists $a \in \mathrm{C} \cdot \mathrm{E}$ such that a is strictly smaller than the largest element in B'. Instantiate such a.

By definition of array concatenation, this implies $a \in \mathrm{C}$ or $a \in \mathrm{E}$.

Case 1. $a \in \mathrm{C}$.

Since $\mathrm{B} \cdot \mathrm{C}$ is sorted, and the size of B is 2^{n-1}, this shows there are at least 2^{n-1} elements in (B and thus in) $\mathrm{B} \cdot \mathrm{D}$ that are at most a.

Also, by assumption a is strictly smaller than the largest element in B', where the size of B' is also 2^{n-1}, this implies there exists an element $b \in \mathrm{B}'$ such that $b > a$. Instantiate such b.

However, on the other hand, there exists at least 2^{n-1} elements in $\mathrm{B} \cdot \mathrm{D}$ that are at most a thus strictly less than b. This contradicts the definition of B': $b \in \mathrm{B}'$ implies b is one of the first 2^{n-1} smallest elements in A.

Hence we obtained a contradiction in Case 1.

Case 2. $a \in \mathrm{E}$.

Since $\mathrm{D} \cdot \mathrm{E}$ is sorted, and the size of D is 2^{n-1}, this shows there are at least 2^{n-1} elements in (D and thus in) $\mathrm{B} \cdot \mathrm{D}$ that are at most a.

Also, by assumption a is strictly smaller than the largest element in B', where the size of B' is also 2^{n-1}, this implies there exists an element $b \in \mathrm{B}'$ such that $b > a$. Instantiate such b.

However, on the other hand, there exists at least 2^{n-1} elements in $\mathrm{B} \cdot \mathrm{D}$ that are at most a thus strictly less than b. This contradicts the definition of B': $b \in \mathrm{B}'$ implies b is one of the first 2^{n-1} smallest elements in A.

Hence we obtained a contradiction in Case 2.

For all cases we obtained contradiction, thus we conclude this is a contradiction.

By contradiction, we have shown that all 2^{n-1} smallest elements in A are also in $\mathrm{B} \cdot \mathrm{D}$ (and thus in B' by construction), so $\mathrm{B}' = \mathrm{A}'[1..2^{n-1}]$. Hence we conclude Lemma 1.

Lemma 2. $\mathrm{E}' = \mathrm{A}'\left[\left(2^n + 2^{n-1} + 1\right) ..2^{n+1}\right]$, that is, E' is the array containing 2^{n-1} largest elements in A.

Proof of Lemma 2.

We will follow similar steps as in the proof of Lemma 1. To prove Lemma 2, since by construction of E' we know E' is the array containing 2^{n-1} largest elmeents in $\mathrm{C} \cdot \mathrm{E}$, so it is equivalent to show that all 2^{n-1} largest elements in A are also in $\mathrm{C} \cdot \mathrm{E}$. In other words, there does not exists $a \in \mathrm{B} \cdot \mathrm{D}$ such that a is strictly larger than the smallest element in E'.

To obtain a contradiction, assume there exists $a \in \mathrm{B} \cdot \mathrm{D}$ such that a is strictly larger than the smallest element in E'. Instantiate such a.

By definition of array concatenation, this implies $a \in \mathrm{B}$ or $a \in \mathrm{D}$.

Case 1. $a \in \mathrm{B}$.

Since $\mathrm{B} \cdot \mathrm{C}$ is sorted, and the size of C is 2^{n-1}, this shows there are at least 2^{n-1} elements in (C and thus in) $\mathrm{C} \cdot \mathrm{E}$ that are at least a.

Also, by assumption a is strictly larger than the smallest element in E', where the size of E' is also 2^{n-1}, this implies there exists an element $b \in \mathrm{E}'$ such that $b < a$. Instantiate such b.

However, on the other hand, there exists at least 2^{n-1} elements in $\mathrm{C} \cdot \mathrm{E}$ that are at least a thus strictly greater than b. This contradicts the definition of E': $b \in \mathrm{E}'$ implies b is one of the last 2^{n-1} largest elements in A.

Hence we obtained a contradiction in Case 1.

Case 2. $a \in \mathrm{D}$.

Since $\mathrm{D} \cdot \mathrm{E}$ is sorted, and the size of E is 2^{n-1}, this shows there are at least 2^{n-1} elements in (E and thus in) $\mathrm{C} \cdot \mathrm{E}$ that are at least a.

Also, by assumption a is strictly larger than the smallest element in E', where the size of E' is also 2^{n-1}, this implies there exists an element $b \in \mathrm{E}'$ such that $b < a$. Instantiate such b.

However, on the other hand, there exists at least 2^{n-1} elements in $\mathrm{C} \cdot \mathrm{E}$ that are at least a thus strictly greater than b. This contradicts the definition of E': $b \in \mathrm{E}'$ implies b is one of the last 2^{n-1} largest elements in A.

Hence we obtained a contradiction in Case 2.

For all cases we obtained contradiction, thus we conclude this is a contradiction.

By contradiction, we have shown that all 2^{n-1} largest elements in A are also in $\mathrm{C} \cdot \mathrm{E}$ (and thus in E' by construction), so $\mathrm{E}' = \mathrm{A}'[\left(2^n + 2^{n-1} + 1\right) ..2^{n+1}]$. Hence we conclude Lemma 2.

Lemma 3. If B', $\mathrm{D}'' \cdot \mathrm{C}''$, and E' are sorted respectively, and $\mathrm{B}'[2^{n-1}] \leq \mathrm{D}''[1]$ and $\mathrm{C}''[2^{n-1}] \leq \mathrm{E}'[1]$, then $\mathrm{B}' \cdot \mathrm{D}'' \cdot \mathrm{C}'' \cdot \mathrm{E}' = \mathrm{A}$ is sorted.

Proof of Lemma 3. See below.

So, by Lemma 1, 2, 3 and modus ponens we conclude $\mathrm{B}' \cdot \mathrm{D}'' \cdot \mathrm{C}'' \cdot \mathrm{E}' = \mathrm{A}$ is also sorted, thus by the uniqueness of sorted permutation $\mathrm{A} = \mathrm{A}'$.

By proof of conjunction, $\mathrm{AUX}(\mathrm{A}[1..n], n)$ eventually halts, at which time $\mathrm{A}[1..n]$ is sorted in non-decreasing order, n and the multiset of elements in $\mathrm{A}[1..n]$ are unchanged.

By direct proof, if $\mathrm{AUX}(\mathrm{A}[1..n], n)$ is performed, then it eventually halts, at which time $\mathrm{A}[1..n]$ is sorted in non-decreasing order, n and the multiset of elements in $\mathrm{A}[1..n]$ are unchanged.

Since $\mathrm{A}[1..2^{n+1}]$ is arbitrary, by generalization we have shown $P(2^{n+1})$.

By induction, we have $\forall n \in S.P(n)$. So, $\mathrm{AUX}(\mathrm{A}[1..n], n)$ satisfies the specifications as in our Question 2.

Proof of Lemma 3.

Assume B', $\mathrm{D}'' \cdot \mathrm{C}''$, and E' are sorted respectively, and $\mathrm{B}'[2^{n-1}] \leq \mathrm{D}''[1]$ and $\mathrm{C}''[2^{n-1}] \leq \mathrm{E}'[1]$.

Let $i \in \mathbb{Z}^+$ be arbitrary;

Let $j \in \mathbb{Z}^+$ be arbitrary;

Assume $(1 \leq i < j \leq 2^{n+1})$.

Case 1. $k2^{n-1} + 1 \leq i < j \leq (k+1)2^{n-1}$ for $k \in \{0, 1, 2, 3\}$.

Then since B', $\mathrm{D}'' \cdot \mathrm{C}''$, and E' are sorted, (by specialization and modus ponens) $\mathrm{A}[i] \leq \mathrm{A}[j]$.

For Case 1 $\mathrm{A}[i] \leq \mathrm{A}[j]$.

Case 2. $1 \leq i \leq 2^{n-1}$, $k2^{n-1} + 1 \leq j \leq (k+1)2^{n-1}$ for $k \in \{1, 2\}$.

Then $\mathrm{A}[i] \leq \mathrm{B}'[2^{n-1}] \leq \mathrm{D}''[1] \leq \mathrm{A}[j]$.

For Case 2 $\mathrm{A}[i] \leq \mathrm{A}[j]$.

Case 3. $1 \leq i \leq 2^{n-1}$, $3 \cdot 2^{n-1} + 1 \leq j \leq 2^{n+1}$.

Then $\mathrm{A}[i] \leq \mathrm{B}'[2^{n-1}] \leq \mathrm{D}''[1] \leq \mathrm{C}''[2^{n-1}] \leq \mathrm{E}'[1] \leq \mathrm{A}[j]$.

For Case 3 $\mathrm{A}[i] \leq \mathrm{A}[j]$.

Case 4. $2^{n-1} \leq i < j \leq 3 \cdot 2^{n-1}$.

Then since $\mathrm{D}'' \cdot \mathrm{C}''$ is sorted, (by specialization and modus ponens) $\mathrm{A}[i] \leq \mathrm{A}[j]$.

For Case 4 $\mathrm{A}[i] \leq \mathrm{A}[j]$.

Case 5. $2^{n-1} \leq i \leq 3 \cdot 2^{n-1}, 3 \cdot 2^{n-1} + 1 \leq j \leq 2^{n+1}$.

Then $\mathrm{A}[i] \leq \mathrm{C}''[2^{n-1}] \leq \mathrm{E}'[1] \leq \mathrm{A}[j]$.

For Case 5 $\mathrm{A}[i] \leq \mathrm{A}[j]$.

For all cases $\mathrm{A}[i] \leq \mathrm{A}[j]$, thus $\mathrm{A}[i] \leq \mathrm{A}[j]$.

By direct proof, $(1 \leq i < j \leq 2^{n+1})$ IMPLIES $(\mathrm{A}[i] \leq \mathrm{A}[j])$.

Since $j \in \mathbb{Z}^+$ is arbitrary, $\forall j \in \mathbb{Z}^+.(1 \leq i < j \leq 2^{n+1})$ IMPLIES $(\mathrm{A}[i] \leq \mathrm{A}[j])$.

Since $i \in \mathbb{Z}^+$ is arbitrary, $\forall i \in \mathbb{Z}^+.\forall j \in \mathbb{Z}^+.\left[(1 \leq i < j \leq 2^{n+1}) \text{ IMPLIES } (\mathrm{A}[i] \leq \mathrm{A}[j])\right]$.

By direct proof, we conclude If B', $\mathrm{D}'' \cdot \mathrm{C}''$, and E' are sorted respectively, and $\mathrm{B}'[2^{n-1}] \leq \mathrm{D}''[1]$ and $\mathrm{C}''[2^{n-1}] \leq \mathrm{E}'[1]$, then $\mathrm{B}' \cdot \mathrm{D}'' \cdot \mathrm{C}'' \cdot \mathrm{E}' = \mathrm{A}$ is sorted.

Define the set $S' = \{2^a \mid a \in \mathbb{N}\}$, since $S' \subseteq \mathbb{N}$, it has a total order.

Proof of Question 4 by induction on S'.

Consider the specifications of $\mathrm{SRT}(\mathrm{A}[1..n], n)$:

Precondition: $n \in S'$, the elements $\mathrm{A}[1..n]$ are from the same totally ordered set.

Postcondition: n and multiset of elements in $\mathrm{A}[1..n]$ are unchanged. $\mathrm{A}[1..n]$ sorted in nondecreasing order.

Termination: The algorithm terminates.

For $n \in S'$, let $Q(n) =$ "for all array $\mathrm{A}[1..n]$ with elements from a totally ordered set, if $\mathrm{SRT}(\mathrm{A}[1..n], n)$ is performed, then it eventually halts, at which time $\mathrm{A}[1..n]$ is sorted in non-decreasing order, n and the multiset of elements in $\mathrm{A}[1..n]$ are unchanged". We will prove $\forall n \in S'.Q(n)$, equivalently $\forall n \in \mathbb{N}.Q(2^n)$.

Base Case: $n = 0$.

Let $\mathrm{A}[1..2^0]$ be arbitrary array with elements from a totally ordered set.

Assume $\mathrm{SRT}(\mathrm{A}[1..1], 1)$ is called.

Since $\mathrm{NOT}(1 > 1)$, we halts, $\mathrm{A}[1..1]$ is trivially sorted in non-decreasing order, n and the multiset of elements in $\mathrm{A}[1..1]$ are trivially unchanged.

By proof of conjunction and direct proof, we have shown if $\mathrm{SRT}(\mathrm{A}[1..1], 1)$ is performed, then it eventually halts, at which time $\mathrm{A}[1..1]$ is sorted in non-decreasing order, n and the multiset of elements in $\mathrm{A}[1..1]$ are unchanged.

Since $\mathrm{A}[1..2^0]$ is arbitrary, by definition we have shown $Q(2^0)$.

Let $n \in \mathbb{N}$ be arbitrary;

Assume $Q(2^n)$.

Let $\mathrm{A}[1..2^{n+1}]$ be arbitrary array with elements from a totally ordered set. Assume $\mathrm{SRT}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$ is called. Then $n + 1 \geq 1$ implies $2^{n+1} \geq 2$, so $2^{n+1} > 2$ and we enter L1 to L2.

On L2, by inductive hypothesis $Q(2^n)$, so by specialization and modus ponens on $Q(2^n)$ we have $\mathrm{AUX}(\mathrm{A}[1..2^n], 2^n)$ terminates and at that time $\mathrm{A}[1..2^n]$ is sorted in non-decreasing order, 2^n and the multiset of elements in $\mathrm{A}[1..2^n]$ are unchanged.

On L3, by inductive hypothesis $Q(2^n)$, so by specialization and modus ponens on $Q(2^n)$ we have $\mathrm{AUX}(\mathrm{A}[(2^n + 1)\,..2^{n+1}], 2^n)$ terminates and at that time $\mathrm{A}[(2^n + 1)\,..2^{n+1}]$ is sorted in non-decreasing order, 2^n and the multiset of elements in $\mathrm{A}[(2^n + 1)\,..2^{n+1}]$ are unchanged.

Now, since the array $\mathrm{A}[1..2^{n+1}]$ and 2^{n+1} have met the preconditions of $\mathrm{AUX}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$, on L4 we call $\mathrm{AUX}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$. By Question 3, we have shown $\mathrm{AUX}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$ eventually halts, at which time $\mathrm{A}[1..2^{n+1}]$ is sorted in non-decreasing order, 2^{n+1} and the multiset of elements in $\mathrm{A}[1..2^{n+1}]$ are unchanged. After L4 we halt $\mathrm{SRT}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$.

So, by proof of conjunction and direct proof, we have if $\mathrm{SRT}(\mathrm{A}[1..2^{n+1}], 2^{n+1})$ is performed, then it halts, and that time $\mathrm{A}[1..2^{n+1}]$ is sorted in non-decreasing order, 2^{n+1} and the multiset of elements in $\mathrm{A}[1..2^{n+1}]$ are unchanged.

Since $\mathrm{A}[1..2^{n+1}]$ is arbitrary, by generalization we have shown $Q(2^{n+1})$.

By induction, we have shown $\forall n \in \mathbb{N}.Q(2^n)$, equivalently $\forall n \in S'.Q(n)$, that is, SRT is correct for all possible input.