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

Assume n is a power of 2. Consider the algorithm SRT that sorts an array $A[1..n]$ into nondecreasing order. Note that the algorithm SRT calls an auxiliary function AUX.

Question 1.

For all $i \in \mathbb{Z}^+$, let $n' = 2^i$ where $n' \in \mathbb{Z}^+$. Define

$$U : \{2^i \mid i \in \mathbb{Z}^+\} \to \mathbb{N}, U(2^i) = U(n') = \begin{cases} 2 & \text{if } i = 1, \\ \frac{n'}{4} + 3 \cdot U\left(\frac{n'}{2}\right) & \text{if } i > 1. \end{cases},$$

and

$$L : \{2^i \mid i \in \mathbb{Z}^+\} \to \mathbb{N}, L(2^i) = L(n') = \begin{cases} 1 & \text{if } i = 1, \\ \frac{n'}{4} + 3 \cdot L\left(\frac{n'}{2}\right) & \text{if } i > 1. \end{cases}.$$

Here the domains for U and L are $\{2^i \mid i \in \mathbb{Z}^+\}$ (are all powers of 2 except 2^0). Since AUX is an auxilliary function of SRT, and within SRT, AUX will be called only when $n' > 1$, that is, $n' \geq 2^1$, and our comparison $A[1] > A[2]$ when $n' \leq 2$ only makes sense when $n' \geq 2 = 2^1$. Moreover, since we assumed n is a power of 2, this implies our domain covers all possible values of the calls of AUX with respect to SRT.

> **Claim 1**
>
> The functions U and L are well defined.   ♀

Let B denote the set where $B = \{2^i \mid i \in \mathbb{Z}^+\}$. Since B is a subset of $\mathbb{Z}^+$, this implies B has a well ordering, and where we can apply induction on $i \in \mathbb{Z}^+$ to show $n' = 2^i \in B$ hold for all $i \in \mathbb{Z}^+$.

Proof of Claim 1 by strong induction on $i \in \mathbb{Z}^+$.
For all $n' \in B$ where $n' = 2^i$ for some $i \in \mathbb{Z}^+$, define the predicate $S(n') =$ "$U(n') \in \mathbb{N}$ and $L(n') \in \mathbb{N}$."
Now, to show the functions U and L are well defined, it suffices to show $\forall n' \in B.S(n')$ as we have verified the domains of U and L are well defined. This is equivalent to show $\forall i \in \mathbb{Z}^+.S(2^i)$.
Base Case: $i = 1$.
　　Then $U(2^1) = 2 \in \mathbb{N}$ and $L(2^1) = 1 \in \mathbb{N}$ are well defined.
So, $S(2^1)$ holds.
Inductive Step:
　　Let $i \in \mathbb{Z}^+$ be arbitrary;
　　　　Assume $\forall j \in \mathbb{Z}^+.(j \leq i)$ IMPLIES $S(2^i)$, that is, $\forall j \in \mathbb{Z}^+.(j \leq i)$ IMPLIES $(U(2^j) \in \mathbb{N}$ AND $L(2^j) \in \mathbb{N})$.
　　　　Case 1. $i = 1$.
　　　　　　Then $U(2^2) = \frac{2^2}{4} + 3 \cdot U\left(\frac{2^2}{2}\right) = 1 + 3 \cdot U(2^1) = 1 + 3 \cdot 2 = 7 \in \mathbb{N}$ and
　　　　　　$L(2^2) = \frac{2^2}{4} + 3 \cdot L\left(\frac{2^2}{2}\right) = 1 + 3 \cdot L(2^1) = 1 + 3 \cdot 1 = 4 \in \mathbb{N}$.
　　　　For Case 1 $U(2^2)$ and $L(2^2)$ are well defined.
　　　　Case 2. $i \geq 2$.
　　　　　　Then since $U(2^i) \in \mathbb{N}$ and $L(2^i) \in \mathbb{N}$ by inductive hypothesis (specialization and modus ponens, and definition of S), we have $U(2^{i+1}) = \frac{2^{i+1}}{4} + 3 \cdot U\left(\frac{2^{i+1}}{2}\right) = \frac{2^{i+1}}{4} + 3 \cdot U(2^i) \in \mathbb{N}$ and $L(2^{i+1}) = \frac{2^{i+1}}{4} + 3 \cdot L\left(\frac{2^{i+1}}{2}\right) = \frac{2^{i+1}}{4} + 3 \cdot L(2^i) \in \mathbb{N}$. Here $\frac{2^{i+1}}{4} \in \mathbb{N}$ since $i \geq 2$ implies $i - 1 \geq 1$ and so $i - 1 \in \mathbb{N}$ and $\frac{2^{i+1}}{4} = 2^{i+1-2} = 2^{i-1} \in \mathbb{N}$.
　　　　For Case 2 $U(2^2)$ and $L(2^2)$ are well defined.
　　　　For all cases $S(2^{i+1})$, thus $S(2^{i+1})$.
　　By strong induction, we have shown $\forall n' \in B.S(n')$.

QUOD
ERAT
DEM∎

Justification.

For $i \in \mathbb{Z}^+$, for array A, define the predicate $Q(i, A) =$"If A is well defined on index from 1 to 2^i where such elements are from a totally ordered domain, then $U(2^i)$ is an upper bound on the worst case number of steps performed by AUX($A[1..2^i], 2^i$) and $L(2^i)$ is a lower bound on the worst case number of steps performed by AUX($A[1..2^i], 2^i$), where steps are array element comparisons and swap operations."

For $i \in \mathbb{Z}^+$, define $P(i) = $ "For all array A. $Q(i, A)$."

> **Lemma 1**
>
> $\forall i \in \mathbb{Z}^+, P(i)$.   🖊

Proof of Lemma 1 by strong induction on $i \in \mathbb{Z}^+$.
Base Case: $i = 1$.
    Let array A be arbitrary;
        Assume A is well defined on index from 1 to $2^1 = 2$ and all such elements are from a totally ordered domain.
        Consider AUX($A[1..2^1], 2$). In this case since NOT($2 > 2$), we will execute line 7 after line 1. First we compare $A[1]$ and $A[2]$, if $A[1] < A[2]$, then the execution is terminated, which gives the lower bound of 1 step for the execution of AUX($A[1..2^i], 2^i$). If $A[1] > A[2]$, then we move into line 8 and swap the values of $A[1]$ and $A[2]$, then terminate the call, which gives the upper bound of $1 + 1 = 2$ steps for the execution of AUX($A[1..2^i], 2^i$).
    By direct proof, we have shown $Q(1, A)$.
    Since A is arbitrary, we have shown $P(1)$.
Inductive Step:
    Let $i \in \mathbb{Z}^+$ be arbitrary;
        Assume $\forall j \in \mathbb{Z}^+.(j \leq i)$ IMPLIES $P(j)$.
        Let array A be arbitrary;
            Assume A is well defined on index from 1 to 2^{i+1} where such elements are from a totally ordered domain.
            $i \in \mathbb{Z}^+$ implies $i + 1 \geq 2$ and so $2^{i+1} \geq 4$.
            Consider AUX($A[1..2^{i+1}], 2^{i+1}$). In this case since $2^{i+1} > 2$, we will execute into line 2. From line 2 and 3, there are precisely $\frac{2^{i+1}}{4}$ steps performed, here $\frac{2^{i+1}}{4}$ must be a positive integer since $\frac{2^{i+1}}{4} = \frac{2^{i+1}}{2^2} = 2^{i+1-2} = 2^{i-1}$ and $i \in \mathbb{Z}^+$ implies $i - 1 \geq 0$ and for all $j \in \mathbb{N}, 2^j \in \mathbb{Z}^+$.
            Since $\frac{2^{i+1}}{2} = 2^i$. By inductive hypothesis (specialization and modus ponens) $P(i)$.
            By specialization, we have $Q(i, A)$. That is, $U(2^i)$ is an upper bound and $L(2^i)$ is a lower bound on the worst case number of steps performed by AUX($A[1..2^i], 2^i$) (we ignore our definition of steps, as they are defined previously).
            So, on line 4, 5, and 6, a minimum of $L(2^i)$ steps and a maximum of $U(2^i)$ steps are performed respectively. So, from line 4 to line 6, a minimum of $3 \cdot L(2^i)$ steps and a maximum of $3 \cdot U(2^i)$ steps are performed.
            Hence, from line 2 to line 6, a minimum of $\frac{2^{i+1}}{4} + 3L(2^i)$ steps and a maximum of $\frac{2^{i+1}}{4} + 3 \cdot U(2^i)$ steps are performed. Since the execution terminates right after line 6, we conclude that the number of steps performed by AUX($A[1..2^{i+1}], 2^{i+1}$) is bounded below by $\frac{2^{i+1}}{4} + 3 \cdot L(2^i)$ and bounded above by $\frac{2^{i+1}}{4} + 3U(2^i)$.
        By definition of U and L and indirect proof, we have shown $Q(i + 1, A)$.

<div align="right">
Quod
Erat
Dem■
</div>

Since A is arbitrary, we have shown $P(i+1)$.

By strong induction, we have shown $\forall i \in \mathbb{Z}^+, P(i)$.

Therefore, by Lemma 1 we have shown that U and L are indeed the upper and lower bounds on the worst case number of steps performed by $\mathrm{AUX}(A[1..n'], n')$ respectively where $n' = 2^i$ for some $i \in \mathbb{Z}^+$.

Moreover, for the sake of simplicity and 'good', we have chosen the above definitions, and they are also not trivial bounds since our base definition and recursion definition are chosen accordingly to the procedure.

Question 2.

We first solve the recurrence $U(n')$ using the method of repeated substitution.

For $U(n')$ where $n' = 2^i$ for some $i \in \mathbb{Z}^+$:

Case 1. $i = 1$. Then $U(n') = U(2^1) = 2$ is already defined explicitely.

Case 2. $i \geq 2$. Then we have

$$U(n) = U(2^i) = \frac{2^i}{4} + 3 \cdot U\left(\frac{2^i}{2}\right)$$

$$= \frac{2^i}{4} + 3\left[\frac{2^{i-1}}{4} + 3U\left(\frac{2^{i-1}}{2}\right)\right]$$

$$= \frac{2^i}{4} + \frac{3 \cdot 2^i}{8} + 9 \cdot U\left(\frac{2^{i-2}}{2}\right)$$

$$= \frac{2^i}{4}\left[\sum_{j=0}^{1}\left(\frac{3}{2}\right)^j\right] + 3^2 \cdot U\left(\frac{2^{i-2}}{2}\right)$$

$$\frac{2^i}{4} + \frac{3 \cdot 2^i}{8} + 9 \cdot U\left(\frac{2^{i-2}}{2}\right) = \frac{2^i}{4} + \frac{3 \cdot 2^i}{8} + 9\left[\frac{2^{i-2}}{4} + 3 \cdot U\left(\frac{2^{i-2}}{2}\right)\right]$$

$$= \frac{2^i}{4} + \frac{3 \cdot 2^i}{8} + \frac{9 \cdot 2^{i-2}}{4} + 27 \cdot U\left(\frac{2^{i-2}}{2}\right)$$

$$= \frac{2^i}{4}\left[\sum_{j=0}^{2}\left(\frac{3}{2}\right)^j\right] + 3^3 \cdot U\left(\frac{2^{i-3}}{2}\right)$$

$$\vdots$$

$$= \frac{2^i}{4}\left[\sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^j\right] + 3^{i-1} \cdot U\left(\frac{2^2}{2}\right)$$

$$= \frac{2^i}{4}\left[\sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^j\right] + 3^{i-1} \cdot U\left(2^1\right)$$

$$= \frac{2^i}{4}\left[\sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^j\right] + 3^{i-1} \cdot 2$$

where the summation and the exponentiations are well defined since $i \geq 2$ implies $i - 2 \geq 0$ and $i - 1 \geq 1$.

We now verify the explicite form using induction.

Claim 2

For $U(n')$ where $n' \in B$, that is, $n' = 2^i$ for some $i \in \mathbb{Z}^+$, $U(n')$ has the explicite form

$$U(n') = U(2^i) = \begin{cases} 2 & \text{if } i = 1, \\ \frac{2^i}{4}\left[\sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^j\right] + 3^{i-1} \cdot 2 & \text{if } i > 1. \end{cases}$$

♀

Proof of Claim 2 by induction.
For $i \in \mathbb{Z}^+$, define the predicate $R(i) =$"$U(2^i)$ has the explicite form as in Claim 2."
Base Case: $i = 1$. Then $U(2^1) = 2$ which matches the explicite form. So $R(1)$ holds.
Inductive Step:

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

Assume $R(i)$.

Case 1. $i = 1$.

Then $\frac{2^2}{4}\left[\sum_{j=0}^{2-2}\left(\frac{3}{2}\right)^j\right] + 3^{2-1} \cdot 2 = 1 + 3 \cdot 2 = 7$ which matches $U(2^2) = \frac{2^2}{4} + 3 \cdot U\left(2^{2-1}\right) = 1 + 3 \cdot 2 = 7$. So $R(2)$ holds.

For Case 1 we have shown $R(i + 1)$.

Case 2. $i \geq 2$.

By definition of U we have

$$U(2^{i+1}) = \frac{2^{i+1}}{4} + 3 \cdot U(2^i)$$
$$= \frac{2^{i+1}}{4} + 3 \cdot U(2^i),$$

since $i \geq 2$ and we assumed $R(i)$, we have

$$= \frac{2^{i+1}}{4} + 3 \cdot \left(\frac{2^i}{4}\left[\sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^j\right] + 3^{i-1} \cdot 2\right)$$

$$= \frac{2^{i+1}}{4}\left[1 + \frac{3}{2}\sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^j\right] + 3^{(i+1)-1} \cdot 2$$

$$= \frac{2^{i+1}}{4}\left[1 + \sum_{j=0}^{i-2}\left(\frac{3}{2}\right)^{j+1}\right] + 3^{(i+1)-1} \cdot 2$$

$$= \frac{2^{i+1}}{4}\left[\left(\frac{3}{2}\right)^0 + \sum_{j=1}^{(i+1)-2}\left(\frac{3}{2}\right)^j\right] + 3^{(i+1)-1} \cdot 2$$

$$= \frac{2^{i+1}}{4}\left[\sum_{j=0}^{(i+1)-2}\left(\frac{3}{2}\right)^j\right] + 3^{(i+1)-1} \cdot 2$$

For Case 2 we have shown $R(i + 1)$.

For all cases $R(i + 1)$, thus $R(i + 1)$.

By induction, we have shown $\forall i \in \mathbb{Z}^+, R(i)$.

Q<small>UOD</small>
E<small>RAT</small>
D<small>EM</small>∎

Question 3.

Define the set $C = \{2^i \mid i \in \mathbb{N}\}$. Since C is a subset of $\mathbb{N}$, thus C has a well ordering. So we may apply induction on $i \in \mathbb{N}$ to show $n = 2^i \in C$ holds for all $i \in \mathbb{N}$.

Claim 3

For $n \in \mathbb{Z}^+$ where $n \in C$, that is, $n = 2^i$ for some $i \in \mathbb{N}$, define

$$T : C \to \mathbb{N}, T(n) = T(2^i) = \begin{cases} 0 & \text{if } i = 0, \\ 2 \cdot T(2^{i-1}) + U(2^i) & \text{if } i > 0. \end{cases}$$

Then, our $T(n)$ is well defined and represents a good upper bound on the worst case number of steps performed by $\text{SRT}(A[1..n], n)$ for any array A that is well defined on index from 1 to n where such elements are from a totally ordered domain. ♀

Claim 4

The function $T(n)$ is well defined. ♀

Proof of Claim 4.
First we can see the domain of T is well defined according to the question.
Now we show the codomain is well defined. To this end, for $n \in C$ where $n = 2^i$ for some $i \in \mathbb{N}$, define the predicate $W(n) = W(2^i) = \text{``}T(2^i) \in \mathbb{N}.\text{''}$
Now we show $\forall i \in \mathbb{N}.W(2^i)$.
Base Case: $i = 0$.
    Then $T(2^0) = 0 \in \mathbb{N}$.
So, $W(2^0)$ holds.
Inductive Step:
    Let $i \in \mathbb{N}$ be arbitrary;
        Assume $\forall j \in \mathbb{N}.(j \leq i)$ IMPLIES $W(2^j)$.
        Case 1. $i = 0$.
            Then $T(2^1) = 2 \cdot T(2^0) + U(2^1) = 2 \cdot 0 + 2 = 2 \in \mathbb{N}$.
        For Case 1 $W(2^{i+1})$ holds.
        Case 2. $i \geq 1$.
            Then $T(2^{i+1}) = 2 \cdot T(2^i) + U(2^{i+1}) = 2 \cdot T(2^i) + U(2^{i+1})$. By inductive hypothesis
            $T(2^i) \in \mathbb{N}$, and from our previous claim $U(2^{i+1}) \in \mathbb{N}$, so $T(2^{i+1}) \in \mathbb{N}$.
        For Case 2 $W(2^{i+1})$ holds.
        For all cases $W(2^i)$, thus $W(2^i)$.
    By induction, we have shown $\forall n \in C.W(n)$.
    Therefore, we conclude that $T(n)$ is well defined.

QUOD
ERAT
DEM∎

Now, we show that $T(n)$ is indeed an upper bound (during the proof we can also see why it is a 'good' upper bound).

For $i \in \mathbb{N}$, for array A, define the predicate $V(i, A) = \text{``If } A$ is well defined on index from 1 to 2^i where such elements are from a totally ordered domain, then $T(2^i)$ is an upper bound on the worst case number of steps performed by $\text{SRT}(A[1..2^i], 2^i)$, where steps are array element comparisons and swap operations.''

For $i \in \mathbb{N}$, define $X(i) = \text{``For all array } A. \ V(i, A).\text{''}$

Lemma 2

$\forall i \in \mathbb{N}, X(i).$

Proof of Lemma 2 by strong induction on $i \in \mathbb{N}$.
Base Case: $i = 0$.
    Let array A be arbitrary;
        Assume A is well defined on index from 1 to $2^0 = 1$ and all such elements are from a totally ordered domain.
        Consider $\mathrm{SRT}(A[1..1], 1)$. In this case since $\mathrm{NOT}(1 > 1)$, no step has been executed. So the number of steps performed by $\mathrm{SRT}(A[1..1], 1)$ is 0. Since $T(2^0) = 0$, we have $T(2^0)$ is an upper bound on the worst case number of steps performed by $\mathrm{SRT}(A[1..1], 1)$.
    By direct proof, we have shown $V(0, A)$.
Since A is arbitrary, we have shown $X(0)$.
    Let $i \in \mathbb{N}$ be arbitrary;
        Assume $\forall j \in \mathbb{N}.(j \leq i)$ IMPLIES $X(j)$.
            Let array A be arbitrary;
                Assume A is well defined on index from 1 to 2^{i+1} where such elements are from a totally ordered domain.
                Consider $\mathrm{SRT}(A[1..2^{i+1}], 2^{i+1})$. In this case since $2^{i+1} > 1$, we will execute into line 2. On line 2 and 3, their steps are bounded by $T(2^i)$ respectively by inductive hypothesis (specialization and modus ponens), and from our previous claim $U(2^{i+1})$ is an upper bound on the worst case number of steps performed by $\mathrm{AUX}(A[1..2^{i+1}], 2^{i+1})$. So, the number of steps performed by $\mathrm{SRT}(A[1..2^{i+1}], 2^{i+1})$ is bounded above by $2 \cdot T(2^i) + U(2^{i+1}) = T(2^{i+1})$.
            By definition of T and direct proof, we have shown $V(i+1, A)$.
        Since A is arbitrary, we have shown $X(i+1)$.
By strong induction, we have shown $\forall i \in \mathbb{N}, X(i)$.

Quod Erat Dem■

Question 4.

Similar to Question 2, we repeatly substitute our recursive definition and we can see that: For $n \in \mathbb{N}$ where $n \in C$, that is, $n = 2^i$ for some $i \in \mathbb{N}$, define

$$T'(n) = T'(2^i) = \begin{cases} 0 & \text{if } i = 0, \\ \sum_{j=1}^{i}(2^{i-j} \cdot U(2^j)) & \text{if } i > 0. \end{cases}$$

We now prove this by strong induction:

Claim 5

For all $n \in C$. $T(n) = T'(n)$.

Proof of Claim 5 by strong induction on $i \in \mathbb{N}$.
For $n \in C$, that is, $n = 2^i$ for some $i \in \mathbb{N}$, define the predicate $Y(n) = Y(2^i) = $"$T(2^i) = T'(2^i)$."
Now we show $\forall i \in \mathbb{N}.Y(2^i)$.
Base Case: $i = 0$.
    Then $T(2^0) = 0$ and $T'(2^0) = 0$.
So, $Y(2^0)$ holds.

Inductive Step:

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

        Assume $\forall j \in \mathbb{N}.(j \leq i)$ IMPLIES $Y(2^j)$.

        Case 1. $i = 0$.

            Then $T(2^1) = 2 \cdot T(2^0) + U(2^1) = 2 \cdot 0 + 2 = 2$ and $T'(2^1) = \sum_{j=1}^{1}(2^{1-j} \cdot U(2^j)) = 1 \cdot U(2^1) = 2$.

        For Case 1 $Y(2^{i+1})$ holds.

        Case 2. $i \geq 1$.

            Then $T'(2^{i+1}) = \sum_{j=1}^{i+1}(2^{(i+1)-j} \cdot U(2^j)) = \sum_{j=1}^{i}(2^{(i+1)-j} \cdot U(2^j)) + (U(2^{i+1})) = 2\sum_{j=1}^{i}(2^{i-j} \cdot U(2^j)) + (U(2^{i+1}))$. By inductive hypothesis (specialization and modus ponens) $T(2^i) = T'(2^i)$, so by substitution and definition of T', T, we have $T'(2^{i+1}) = 2\sum_{j=1}^{i}(2^{i-j} \cdot U(2^j)) + (U(2^{i+1})) = 2 \cdot T'(2^i) + U(2^{i+1}) = 2 \cdot T(2^i) + U(2^{i+1}) = 2 \cdot T(2^{i+1})$.

        For Case 2 $Y(2^{i+1})$ holds.

        For all cases $Y(2^i)$, thus $Y(2^i)$.

    By strong induction, we have shown $\forall n \in C.Y(n)$.

<div align="right">QUOD
ERAT
DEM■</div>

Therefore, by Claim 5 we can see T' is the equivalent explicit formula of T, as required.

In conclusion, we have succesfully solved the good upper bounds for the worst case number of steps performed by AUX and SRT, and we have verified our solutions using inductions. Despite there might exists some more tighten bounds to this question, for the sake of simplicity and verification, we have chosen the above definitions.

Also, for Question 4's repeating substitutions, since it is precisely following the same procedure as in Question 2, we simply ommited the steps, however as we have verified the correctness of the explicite formulas, we can be confident that the repeated substitutions are correct.