

CSED332 Assignment 4

Gwon Minjae

Problem 1

Consider the following program to find the maximum value in an array. Write a Hoare logic proof (decorated program) to prove the given Hoare triple.

$\{0 < N\}$

```
int m = A[0];
int i = 1;
while (i < N){
    if (A[i] > m)
        m = A[i];
    else
        skip;
    i = i + 1;
}
```

$\{m = \max(A[0], A[1], \dots, A[N-1])\}$

Proof.

$\{0 < N\}$

```
int m = A[0];
int i = 1;
```

$\{i = 1 \wedge m = \max(A[0], \dots, A[i-1])\}$

```
while (i < N){
```

$\{1 \leq i < N \wedge m = \max(A[0], \dots, A[i-1])\} \implies$

$\{1 \leq i+1 \leq N \wedge m = \max(A[0], \dots, A[i-1])\}$

```
    if (A[i] > m)
        m = A[i];
```

```
    else
        skip;
```

$\{1 \leq i+1 \leq N \wedge m = \max(A[0], \dots, A[i])\}$

```
    i = i + 1;
```

$\{1 \leq i \leq N \wedge m = \max(A[0], \dots, A[i-1])\}$

```
}
```

$\{1 \leq i \leq N \wedge m = \max(A[0], \dots, A[i-1]) \wedge i \geq N\} \implies$

$\{i = N \wedge m = \max(A[0], \dots, A[i-1])\} \implies$

$\{m = \max(A[0], A[1], \dots, A[N-1])\}$

Problem 2

Write a Hoare logic proof (decorated program) to show that the given Hoare triple holds and the program always terminates (hint: what is a ranking function?).

$$\{x \geq 0 \wedge y > 0\}$$

```
int r = x;
int q = 0;
while (y <= r) {
    r = r - y;
    q = q + 1;
}
```

$$\{x = qy + r \wedge 0 \leq r < y\}$$

Proof.

$$\{x \geq 0 \wedge y > 0\}$$

```
int r = x;
int q = 0;
```

$$\{x \geq 0 \wedge y > 0 \wedge x = qy + r\}$$

```
while (y <= r) {
```

$$\{x \geq 0 \wedge y > 0 \wedge x = qy + r \wedge y \leq r\} \implies$$

$$\{x \geq 0 \wedge y > 0 \wedge x = (q + 1)y + (r - y) \wedge y \leq r\}$$

```
    r = r - y;
```

$$\{x \geq 0 \wedge y > 0 \wedge x = (q + 1)y + r \wedge 0 \leq r\}$$

```
    q = q + 1;
```

$$\{x \geq 0 \wedge y > 0 \wedge x = qy + r \wedge 0 \leq r\}$$

```
}
```

$$\{x \geq 0 \wedge y > 0 \wedge x = qy + r \wedge 0 \leq r \wedge r < y\} \implies$$

$$\{x = qy + r \wedge 0 \leq r < y\}$$

Problem 3

Consider the following program for sorting an array. Write a Hoare logic proof to prove the given Hoare triple, where $sorted(a_1, a_2, \dots, a_k)$ means $a_1 \leq a_2 \leq \dots \leq a_k$.

$$\{0 \leq N\}$$

```

int i = 1;
while (i < N) {
    int j = i;
    while (j > 0 && A[j-1] > A[j]) {
        int t = A[j-1];
        A[j-1] = A[j];
        A[j] = t;
        j = j - 1;
    }
    i = i + 1;
}
{sorted(A[0], A[1], A[2], ..., A[N-1])}

```

Prerequisite.

$$\begin{aligned}
 S(a, b) &= \begin{cases} \text{sorted}(A[a], \dots, A[b]), & \text{if } 0 \leq a \leq b < N \\ \{\}, & \text{otherwise.} \end{cases} \\
 L(a, b) &= \begin{cases} \{A[a], \dots, A[b]\}, & \text{if } 0 \leq a \leq b < N \\ \{\}, & \text{otherwise.} \end{cases} \\
 R &= (\text{WLOG}) \text{ Remaining part of } A
 \end{aligned}$$

Proof.

$$\{0 \leq N\}$$

```
int i = 1;
```

$$\{0 \leq N \wedge i \geq 1 \wedge A = \text{sorted}(A[0]) + \{A[1], \dots, A[N-1]\} \implies$$

$$\{0 \leq N \wedge i \geq 1 \wedge A = \text{sorted}(A[0], \dots, A[i-1]) + \{A[i], \dots, A[N-1]\} \implies$$

```
while (i < N) {
```

$$\{0 \leq N \wedge i \geq 1 \wedge A = \text{sorted}(A[0], \dots, A[i-1]) + \{A[i], \dots, A[N-1]\} \wedge i < N \implies$$

$$\{0 \leq N \wedge 1 \leq i < N \wedge A = \text{sorted}(A[0], \dots, A[i-1]) + \{A[i], \dots, A[N-1]\} \implies$$

$$\{0 \leq N \wedge 1 \leq i+1 \leq N \wedge A = \text{sorted}(A[0], \dots, A[(i+1)-2]) + \{A[(i+1)-1], \dots, A[N-1]\} \implies$$

```
int j = i;
```

$$\{0 \leq N \wedge 1 \leq i+1 \leq N \wedge A = \text{sorted}(A[0], \dots, A[(i+1)-2]) + \{A[(i+1)-1], \dots, A[N-1]\} \wedge j \leq i \implies$$

$$\{0 \leq N \wedge 1 \leq i+1 \leq N \wedge A = S(0, j-2) + L(j-1, j) + S(j+1, i-1) + R \wedge j \leq i\}$$

```
while (j > 0 && A[j-1] > A[j]) {
```

$$\begin{aligned}
 \{0 \leq N \wedge 1 \leq i+1 \leq N \wedge A = S(0, j-2) + L(j-1, j) + S(j+1, i-1) + R \wedge j \leq i \\
 \wedge j > 0 \wedge A[j-1] > A[j]\} \implies
 \end{aligned}$$

$$\begin{aligned}
 \{0 \leq N \wedge 1 \leq i+1 \leq N \wedge A = S(0, j-2) + L(j-1, j) + S(j+1, i-1) + R \\
 \wedge 0 \leq j-1 \leq i \wedge A[j-1] > A[j]\}
 \end{aligned}$$

```
int t = A[j-1];
```

```
A[j-1] = A[j];
```

```
A[j] = t;
```

$$\begin{aligned}
 \{0 \leq N \wedge 1 \leq i+1 \leq N \wedge A = S(0, (j-1)-2) + L((j-1)-1, j-1) + S((j-1)+1, i-1) + R \\
 \wedge 0 \leq j-1 \leq i \wedge A[j-1] \leq A[j]\}
 \end{aligned}$$

```
j = j - 1;
```

$$\{0 \leq N \wedge 1 \leq i + 1 \leq N \wedge A = S(0, j - 2) + L(j - 1, j) + S(j + 1, i - 1) + R \\ \wedge 0 \leq j \leq i \wedge A[j] \leq A[j + 1]\}$$

}

$$\{0 \leq N \wedge 1 \leq i + 1 \leq N \wedge A = S(0, j - 2) + L(j - 1, j) + S(j + 1, i - 1) + R \\ \wedge 0 \leq j \leq i \wedge A[j] \leq A[j + 1] \wedge (j \leq 0 \vee A[j - 1] \leq A[j])\} \implies$$

$$\{0 \leq N \wedge 1 \leq i + 1 \leq N \wedge A = \text{sorted}(A[0], \dots, A[i]) + \{A[(i + 1)], \dots, A[N - 1]\}\} \implies$$

$$\{0 \leq N \wedge 1 \leq i + 1 \leq N \wedge A = \text{sorted}(A[0], \dots, A[(i + 1) - 1]) + \{A[(i + 1)], \dots, A[N - 1]\}\}$$

i = i + 1;

$$\{0 \leq N \wedge 1 \leq i \leq N \wedge A = \text{sorted}(A[0], \dots, A[i - 1]) + \{A[i], A[i + 1], \dots, A[N - 1]\}\}$$

}

$$\{0 \leq N \wedge 1 \leq i \leq N \wedge A = \text{sorted}(A[0], \dots, A[i - 1]) + \{A[i], A[i + 1], \dots, A[N - 1]\} \wedge i \geq N\} \implies$$

$$\{0 \leq N \wedge i = N \wedge A = \text{sorted}(A[0], \dots, A[i - 1]) + \{A[i], A[i + 1], \dots, A[N - 1]\}\} \implies$$

$$\{0 \leq N \wedge i = N \wedge A = \text{sorted}(A[0], \dots, A[N - 1])\} \implies$$

$$\{\text{sorted}(A[0], A[1], A[2], \dots, A[N - 1])\}$$