Program Verification:
Reversing an Array

HE Mingxin, Max

CS104: program07 @ yeah.net

CS108: mxhe1 @ yeah.net

I2ML(H) Spring 2023 (CS104|CS108)

Outline

- Program Verification: Reversing an Array
  - Key Points
  - Introducing the array assignment rule
  - Summary

Key Points

Key points to learn:

Partial correctness for array assignments

- Prove that a Hoare triple is satisfied under partial correctness for a program containing array assignment statements.

The array assignment inference rule

Let A be an array of n integers.

First, write down the sequence of changes.
Resolve all of the changes when we prove the implied's.

$(\!|\, Q[A\{e1 \leftarrow e2\}/A] \,|\!)$
A[e1] = e2;
$(\!|\, Q \,|\!)$ array assignment

- A is the original array.
- $A\{e1 \leftarrow e2\}$ is the new array, which is identical to array A except that the $e1^{th}$ element is $e2$.

The array re-assignment notation

The array reassignment notation:

$$A\{e1 \leftarrow e2\}[i] = \begin{cases} e2, & \text{if } i = e1 \\ A[i], & \text{if } i \neq e1 \end{cases}$$

Note that $e1$ is an index whereas $e2$ is an array element.

We apply assignments from left to right.

Examples:

- $A\{1 \leftarrow 3\}[1] = 3$
- $A\{1 \leftarrow 3\}\{1 \leftarrow 4\}[1] = 4$

Reversing an array

Consider an array R of n integers, $R[1], R[2], ..., R[n]$.

We want to reverse the order of its elements.

Our algorithm:

For each $1 \leq j \leq \lfloor n/2 \rfloor$,
we will swap $R[j]$ with $R[n+1-j]$.

Reversing an array

R is an array of n integers, $R[1], R[2], ..., R[n]$. Prove that the following triple is satisfied under partial correctness.

$$\llparenthesis\, (\forall x\, ((1 \leq x \leq n) \rightarrow (R[x] = r_x)))\, \rrparenthesis$$

```
j = 1;
while (2 * j <= n) {
   t = R[j];
   R[j] = R[n+1-j];
   R[n+1-j] = t;
   j = j + 1;
}
```

$$\llparenthesis\, (\forall x\, ((1 \leq x \leq n) \rightarrow (R[x] = r_{n+1-x})))\, \rrparenthesis$$

Reversing an array

R is an array of n integers, $R[1], R[2], ..., R[n]$. Prove that the following triple is satisfied under partial correctness.

Let $Inv(j)$ denote our invariant.

$(\!|\ (\forall x\ ((1 \leq x \leq n) \to (R[x] = r_x)))\ |\!)$

```
j = 1;
while (2 * j <= n) {
  t = R[j];
  R[j] = R[n+1-j];
  R[n+1-j] = t;
  j = j + 1;
}
```

$(\!|\ (\forall x\ ((1 \leq x \leq n) \to (R[x] = r_{n+1-x})))\ |\!)$

CQ 1 Reversing an array

CQ 1: Consider **the premise of implied (A)**.
Which of the following is an accurate description of the formula?

(A) No swap has occurred.

(B) Elements in $[1, j-1]$ have been swapped, and elements in $[j, (n+1)/2]$ have NOT been swapped.

(C) Elements in $[1, j]$ have been swapped, and elements in $[j+1, (n+1)/2]$ have NOT been swapped.

(D) All swaps have been completed.

(E) None of the above

CQ 2 Reversing an array

CQ 2: Consider **the conclusion of implied (A)**.
Which of the following is an accurate description of the formula?

(A) No swap has occurred.

(B) Elements in $[1, j-1]$ have been swapped, and elements in $[j, (n+1)/2]$ have NOT been swapped.

(C) Elements in $[1, j]$ have been swapped, and elements in $[j+1, (n+1)/2]$ have NOT been swapped.

(D) All swaps have been completed.

(E) None of the above

CQ 3 Reversing an array

CQ 3: Consider **the premise of implied (C)**.
Which of the following is an accurate description of the formula?

(A) No swap has occurred.

(B) Elements in $[1, j-1]$ have been swapped, and elements in $[j, (n+1)/2]$ have NOT been swapped.

(C) Elements in $[1, j]$ have been swapped, and elements in $[j+1, (n+1)/2]$ have NOT been swapped.

(D) All swaps have been completed.

(E) None of the above

CQ 4 Reversing an array

CQ 4: Consider **the conclusion of implied (C)**.
Which of the following is an accurate description of the formula?

(A) No swap has occurred.

(B) Elements in $[1, j-1]$ have been swapped, and elements in $[j, (n+1)/2]$ have NOT been swapped.

(C) Elements in $[1, j]$ have been swapped, and elements in $[j+1, (n+1)/2]$ have NOT been swapped.

(D) All swaps have been completed.

(E) None of the above

CQ 5 Reversing an array

CQ 5: Consider **the premise of implied (B)**.
Which of the following is an accurate description of the formula?

(A) No swap has occurred.

(B) Elements in $[1, j-1]$ have been swapped, and elements in $[j, (n+1)/2]$ have NOT been swapped.

(C) Elements in $[1, j]$ have been swapped, and elements in $[j+1, (n+1)/2]$ have NOT been swapped.

(D) All swaps have been completed.

(E) None of the above

CQ 6 Reversing an array

CQ 6: Consider **the conclusion of implied (B)**.
Which of the following is an accurate description of the formula?

(A) No swap has occurred.

(B) Elements in $[1, j-1]$ have been swapped, and elements in $[j, (n+1)/2]$ have NOT been swapped.

(C) Elements in $[1, j]$ have been swapped, and elements in $[j+1, (n+1)/2]$ have NOT been swapped.

(D) All swaps have been completed.

(E) None of the above

Summary

Key points learnt:

Partial correctness for array assignments

- Prove that a Hoare triple is satisfied under partial correctness for a program containing array assignment statements.