

# Program Verification: Array Assignments

HE Mingxin, Max

CS104: program07 @ yeah.net

CS108: mxhe1 @ yeah.net

I2ML(H) Spring 2023 (CS104|CS108)

# Outline

## Program Verification: Array Assignments

### Key Points

Introducing the array assignment rule

An example using 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.

Consider the following triple. What should the precondition be?

$\langle \text{???} \rangle$

$A[x] = 1;$

$\langle A[y] = 0 \rangle$

array assignment

- ▶ If  $x = y$ , the precondition should be ...?
- ▶ If  $x \neq y$ , the precondition should be ...?

We are using variables as indices into arrays. We must consider multiple cases for all possible values of the variables.

# 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.

$\langle Q[A\{e1 \leftarrow e2\}/A] \rangle$

$A[e1] = e2;$

$\langle Q \rangle$                       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:

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

## CQ 1 Applying the array assignment rule

**CQ 1:** What is the precondition derived using the array assignment inference rule?

$\langle ??? \rangle$   
 $A[1] = 2;$   
 $\langle A[x] = y_0 \rangle$     array assignment

- (A)  $A\{1 \leftarrow 1\}[x] = y_0$
- (B)  $A\{1 \leftarrow 2\}[x] = y_0$
- (C)  $A\{2 \leftarrow 1\}[x] = y_0$
- (D)  $A\{2 \leftarrow 2\}[x] = y_0$
- (E) None of the above

## CQ 2 Applying the array assignment rule

**CQ 2:** What is the precondition derived using the array assignment inference rule?

$\langle \text{???} \rangle$   
 $A[1] = 2;$   
 $\langle A\{3 \leftarrow 4\}[x] = y \rangle$     array assignment

(A)  $A\{1 \leftarrow 2\}\{3 \leftarrow 4\}[x] = y$

(B)  $A\{3 \leftarrow 4\}\{1 \leftarrow 2\}[x] = y$

(C) None of the above



## CQ 3 Applying the array assignment rule

**CQ 3:** What is the precondition derived using the array assignment inference rule?

$\langle \text{???} \rangle$

$A[1] = 2;$

$\langle A\{3 \leftarrow A[y]\}[x] = y0 \rangle$      array assignment

(A)  $A\{1 \leftarrow 2\}\{3 \leftarrow A[y]\}[x] = y0$

(B)  $A\{1 \leftarrow 2\}\{3 \leftarrow A\{1 \leftarrow 2\}[y]\}[x] = y0$

(C) None of the above

## Example of the array assignment rule

### Example:

Prove that the following triple is satisfied under partial correctness.

$$\{((A[x] = x_0) \wedge (A[y] = y_0))\}$$

$$t = A[x];$$

$$A[x] = A[y];$$

$$A[y] = t;$$

$$\{((A[x] = y_0) \wedge (A[y] = x_0))\}$$

## Reversing an array

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

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,  $R[1], R[2], \dots, R[n]$ . Prove that the following triple is satisfied under partial correctness.

$$\{ (\forall x ((1 \leq x \leq n) \rightarrow (R[x] = r_x))) \}$$
$$j = 1;$$
$$\mathbf{while} \ (2 * j \leq n) \ \{$$
$$t = R[j];$$
$$R[j] = R[n+1-j];$$
$$R[n+1-j] = t;$$
$$j = j + 1;$$
$$\}$$
$$\{ (\forall x ((1 \leq x \leq n) \rightarrow (R[x] = r_{n+1-x}))) \}$$

## Reversing an array

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

Let  $Inv(j)$  denote our invariant.

$$\begin{aligned} & \langle (\forall x ((1 \leq x \leq n) \rightarrow (R[x] = r_x))) \rangle \\ & j = 1; \\ & \mathbf{while} \ (2 * j \leq n) \ \{ \\ & \quad t = R[j]; \\ & \quad R[j] = R[n+1-j]; \\ & \quad R[n+1-j] = t; \\ & \quad j = j + 1; \\ & \} \\ & \langle (\forall x ((1 \leq x \leq n) \rightarrow (R[x] = r_{n+1-x}))) \rangle \end{aligned}$$

# 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.