- Assertions (including preconditions and postconditions) are used to think logically about programs and to show that program do as they are expected to do.

- To show that a program does what is expected of it(i.e. to show that it is correct) follow the following steps:

  - 1: split the program into smaller program segments, e.g. blocks of assignment statements, loops etc...

  - 2: establish pre- and postconditions for each program segment

  - 3: show that with these conditions the program segment is correct

  - 4: show that the postcondition for one program segment and the precondition for the next piece are compatible(explained later)

- continued from previous slide:
  - 5: show compatibility with the pre-condition and postcondition for the whole program

- Example

- not concerned about declarations, don't change state of the program. Type of variables should be obvious

- Enclose pre and postconditions in { and } as with all assertions

- if C is a program segment, $\{P\}$ is a precondition, $\{Q\}$ is a postcondition then $\{P\}C\{Q\}$ is a Hoare triple

- $\{true\}x = y\{x = y\}$

- $\{\}x = y\{x = y\}$

- $\{z \neq 0\}x = 1/z\{x = 1/z\}$

- $\{1 \leq z \leq 20\}x = 1/z\{x = 1/z\}$

- Find a precondition P such that $\{P\}i = 2 * i\{i < 6\}$ is correct.

- Consider the statement $y = x * x$ and let $y \geq 1$ be the postcondition. What condition (precondition) must hold before statement is executed for postcondition to hold after statement has been executed?

- Preconditions and postconditions can be changed according to certain rules:
  - A precondition can be strengthened: $x > 5$ is stronger than $x > 2$
  - A postcondition can be weakened: $x < 10$ is weaker than $x < 5$

- If $\{a > 0\}a = a + 5\{a > 5\}$ is correct then
  - $\{a > 7\}a = a + 5\{a > 5\}$ is correct (has stronger precondition)
  - $\{a > 0\}a = a + 5\{a > 4\}$ is correct (has weaker postcondition)

- Specification: Write a program segment which swaps the values associated with 2 variables

- Attempt 1:

- x=y; y=x;

- Correct??

- Determine the precondition and postcondition from the specification

- Let x_0 be the value that is associated with variable x initially

- Let y_0 be the value that is associated with variable y initially

- Precondition $(x = x_0) \wedge (y = y_0)$

- Postcondition: (values are swapped)
  $(x = y_0) \wedge (y = x_0)$

- The initial state satisfies the precondition

- Execute the first assignment statement. What state do the variables satisfy?

- What state do the variables satisfy after execution of the combined statements?

- Is this equivalent to the postcondition??

- Now consider the program segment:
  $temp = x$; $x = y$; $y = temp$
  Is this correct??

- The precondition or postcondition hasn't changed.

- The Hoare triple for the whole program segment is:
  $\{(x = x_0) \wedge (y = y_0)\}$ $temp = x$; $x = y$;
  $y = temp$; $\{(x = y_0) \wedge (y = x_0)\}$

- $\{P\}C\{Q\}$. Program segment is partially correct if the final state satisfies $\{Q\}$ after executing C for any initial state satisfying $\{P\}$

- $\{true\}\ a = b\ \{a = b\}$
  $\{\}\ x = 3\ \{x = 3\}$
  $\{\}\ a = b; x = 3\ (a = b) \wedge (x = 3)$

- Any assertion that is at the same time a precondition and a postcondition of a program segment is called an invariant

- Show that $\{a = b\}$ is an invariant of $a+ = 2; b+ = 2$