BITS Pilani
Pilani Campus

innovate achieve lead

CS/IS F214
Logic in Computer Science

MODULE: PROGRAM VERIFICATION

Floyd-Hoare Logic: Correctness of Conditionals

Floyd-Hoare Logic: Conditionals

- Example C1:

  /* Pre: ? */

  if (x > y) then { m = x }

  else { m = y }

  /* Post: $(m >= x \wedge m >= y) \wedge (m=x \vee m=y)$ */

Floyd-Hoare Logic: Conditionals – Approach.

- Ex C1:

  /* Pre: ? */

  if (x > y) then { m = x }

  else { m = y }

  /* Post: (m >= x $\wedge$ m >= y) $\wedge$ (m=x $\vee$ m=y) */

- Approach:

  1. Derive the pre-condition, say ϕ_1, for the "then" case, which should include "*the test condition being true*"
  2. Derive the pre-condition , say ϕ_2, for the "else" case, which should include "*the test condition being false*"
  3. Derive the pre-condition for the if-then-else statement which should be the common part of ϕ_1 and ϕ_2

Verifying Conditionals: Example

- Example C1: Steps:

1. Pre-condition for the "then" case

   /* $(x>=x \wedge x>=y) \wedge (x=x \vee x=y)$ i.e. $(x>=y)$

   $(x>=y)$ is implied by $(x>y)$

   So, Precondition is: **$(x > y)$** */

   Why is this correct?

   m = x

   /* $(m>=x \wedge m>=y) \wedge (m=x \vee m=y)$ */

2. Derive the pre-condition for the "else" case
3. Apply the rule for Conditionals and derive the pre-condition for the if-then-else statement.

Verifying Conditionals: Example

- Example C1: Steps:

1. Pre-condition for the "then" case

   /* (x>y) */

   m = x

   /* (m>=x ∧ m>=y) ∧ (m=x ∨ m=y) */

2. Derive the pre-condition for the "else" case

   /* (y>=x ∧ y>=y) ∧ (y=x ∨ y=y) i.e. (x <= y)

   So, Precondition is: **(x <= y)** */

   m = y

   /* (m>=x ∧ m>=y) ∧ (m=x ∨ m=y) */

3. Apply the rule for Conditionals and derive the pre-condition for the if-then-else statement

Verifying Conditionals: Example

- Example C1: Steps:
  1. *then* case

     /* (x>y) */

     m = x

     /* (m>=x ∧ m>=y) ∧ (m=x ∨ m=y) */
  2. *else* case

     /* (x<=y) */

     m = y

     /* (m>=x ∧ m>=y) ∧ (m=x ∨ m=y) */
  3. Apply the rule for Conditionals:
     - Precondition for *then* case: TRUE ∧ x>y (i.e. $\phi \wedge B$)
     - Precondition for *else* case: TRUE ∧ x<=y (i.e. $\phi \wedge \neg B$)
     - Precondition for the if-statement: TRUE (i.e. *an empty pre-condition*)

Floyd-Hoare Logic: Rule for Conditionals

- Rule for if-statement:

$$\frac{< \phi \wedge B, \text{S1}, > \quad < \phi \wedge \neg B, \text{S2}, \psi >}{< \phi, \ \text{if B then S1 else S2}, \psi >}$$

Conditional

- Alternatively:

```
/* ϕ */  if B
           then { /* ϕ∧B */    S1     /* ψ */ }
           else { /* ϕ∧¬B */    S2     /* ψ */ }
/* ψ */
```