BITS Pilani
Pilani Campus

CS/IS F214
Logic in Computer Science

MODULE: PROGRAM VERIFICATION

Floyd-Hoare Logic: Pragmatics

Floyd-Hoare Logic: Pragmatics: Example

- Verify the correctness of this sequence of statements :

```
/*Pre: ? */
disc = b*b – 4*a*c;
rt = (-b + sqrt(disc))/(2*a)
/*Post:  a*rt*rt + b*rt + c = 0 */
```

Floyd-Hoare Logic: Pragmatics: Function Call

- Verify the correctness of this sequence of statements:

/*Pre: ? */

disc = b*b – 4*a*c;

/* $\underbrace{a*(-b+sqrt(disc))^2/(4*a^2) + b*(-b+sqrt(disc))/(2*a) + c = 0}$ */

rt = (-b + sqrt(disc))/(2*a)

/*a*rt*rt + b*rt + c = 0 */

Verifying this requires knowledge of correctness of ***sqrt***!

Floyd-Hoare Logic: Pragmatics: Function Call

/* $a*(-b+sqrt(disc))^2/(4*a^2) + b*(-b+sqrt(disc))/(2*a) + c = 0$ */

rt = (-b + sqrt(disc))/(2*a)

/*a*rt*rt + b*rt + c = 0 */

Assume that ***sqrt*** *has the following contract:*

/* Pre: x > 0 */

sqrt(x) { … }

/* Post: sqrt(x)*sqrt(x) = x */

Then

/* (disc>0 --> $(disc - b^2)/(4*a) + c = 0$) */

rt = (-b + sqrt(disc))/(2*a)

/*a*rt*rt + b*rt + c = 0 */

Floyd-Hoare Logic: Pragmatics: Function Call

- Precondition for solving a quadratic equation:

/* (b*b>4*a*c) */

disc = b*b – 4*a*c;

/* disc>0 --> (disc – b^2) /(4*a) + c = 0 */

rt = (-b + sqrt(disc))/(2*a)

/*a*rt*rt + b*rt + c = 0 */

Question: *Is there a difference between functions and built-in operations*?

Floyd-Hoare Logic: Pragmatics: Function Call

- Precondition for solving a quadratic equation:

/* (b*b>4*a*c) $\wedge\neg$(a=0) */

disc = b*b – 4*a*c;

/* (disc>0)$\wedge\neg$(a=0) --> (disc – b^2)/(4*a) + c = 0 */

rt = (-b + sqrt(disc))/(2*a)

/*a*rt*rt + b*rt + c = 0 */

Is this a realistic (*no pun intended!*) post-condition ?