CMSC 21

FUNDAMENTALS OF PROGRAMMING

Kristine Bernadette P. Pelaez

Institute of Computer Science
University of the Philippines Los Baños

program correctness

When can you say that a program is correct?

When can you say that a program is correct?

there are
NO syntax errors

When can you say that a program is correct?

given some test data,
the program yields the correct output

When can you say that a program is correct?

code is bug and error free

But!!!

Sometimes...

debugging takes
too much time
than coding

But!!!

Sometimes...

debugging
is harder
than coding

So, how can you prove that your program is correct?

Usual Solution #1

generate LOTS of
TEST DATA and
test it on your program

Usual Solution #1

however.
this **might still miss**
some errors in
the program

Usual Solution #2

pen and paper
tracing!

Usual Solution #2

but it might also
miss some errors
and is VERY TEDIOUS

U(nu)sual Solution #3

use the power of
MATHEMATICAL
LOGIC*

*specifically,
Hoare's Logic

Mathematical Logic

$\{P\}C\{Q\}$

$$\{P\}\underset{\substack{\uparrow \\ \text{your program}}}{C}\{Q\}$$

$$\{P\}C\{Q\}$$

the **precondition**

a boolean statement that must
be true before the program runs

$$\{P\}C\{Q\}$$

the **postcondition**

a boolean statement that must
be true after the program runs

{P}C{Q}

if C starts and P is satisfied,
then it is guaranteed that C will
terminate, after some time,
in a state that satisfies Q.

Example

Assign the quotient of `a/b` to `c`. given that `b>0`.

Example

Swap the values
of two variables, **a** and **b**.

Loop Invariants

Loop Invariant

the relationship
between variables
that is **true**
before, during, & after
the execution of a loop

Example

```
int i,j=N; //N>0
for(i=0;i<N;i++)
    j--;
```

Loop Invariant?

Example

```
int i,j=N; //N>0
for(i=0;i<N;i++)
    j--;
```

Loop Invariant?

```
    i + j == N
```

Loop Invariant

when the terminating condition is reached. the invariant must still be satisfied. and the goal must have been reached

Loop Invariant

that is,

$$I \wedge !B = Q$$

where I is the invariant,

B is the terminating condition, &

Q is the postcondition.

Example

```
int i,j=N; //N>0
for(i=0;i<N;i++)
    j--;
```

Loop Invariant?

```
    i + j == N
```

Example

```
int a=X,b=Y; //a>0 ^ b>0
int c=0;
for(;a>0;a--)
   c = c+b;
```

Loop Invariant?

CMSC 21

FUNDAMENTALS OF PROGRAMMING

Kristine Bernadette P. Pelaez

Institute of Computer Science
University of the Philippines Los Baños