Program Verification
Assignments and Conditionals

Alice Gao

Lecture 19

Based on work by J. Buss, L. Kari, A. Lubiw, B. Bonakdarpour, D. Maftuleac, C. Roberts, R. Trefler, and P. Van Beek

Outline

Learning Goals

By the end of this lecture, you should be able to:

- Prove that a Hoare triple is satisfied under total correctness for a program containing assignment and conditional statements.

Proving Partial and Total Correctness

- Both problems are undecidable. No algorithm can solve them in all situations.
- Different techniques for proving partial and total correctness.
- For proving partial correctness, we will construct formal proofs using inference rules.
- For proving total correctness, we will prove partial correctness and termination separately.

Proving Partial Correctness

```
(| precondition |)
(| ... |)                    <justification>
y = 1;
(| ... |)                    <justification>
z = 0;
(| ... |)                    <justification>
while (z != x) {
   (| ... |)                 <justification>
   (| ... |)                 <justification>
   z = z + 1;
   (| ... |)                 <justification>
   y = y * z;
   (| ... |)                 <justification>
}
(| postcondition |)          <justification>
```

The Assignment Inference Rule

$(\!| Q[E/x] |\!)$
x = E;
$(\!| Q |\!)$ assignment

- Q is a predicate formula.
- x is a variable in Q.
- E is a term.

Example:

$(\!| ??? |\!)$
x = 2;
$(\!| x = 2 |\!)$ assignment

The Assignment Inference Rule

- We often work backwards from the postcondition. Sometimes, we call this pushing the formula up.
- Treat E as one expression and do not worry about what's inside.
- If there is an equality in $Q[E/x]$, do not switch the two sides of an inequality.
- Do not simplify $Q[E/x]$ in any way.

Revisiting the learning goals

By the end of this lecture, you should be able to:

- Prove that a Hoare triple is satisfied under total correctness for a program containing assignment and conditional statements.