Lecture 10

Monday, February 24, 2020 4:50 PM

- Change of plans
  - Discussion of SMT postponed to next class

- Today's plan

3 - Introduce clause learning

1 - Tutorial on Homework 1

2 - Invariants v/s inductive invariants.

Homework 1'

$$
\begin{aligned}
C ::= \; & v := AExp \\
\mid \; & C_1 \,;\, C_2 \\
\mid \; & \text{if}\,(BExp)\ \{C_1\}\ \text{else}\ \{C_2\} \\
\mid \; & \text{while}\,(BExp)\ \{C_1\}
\end{aligned}
$$

Our goal: Prove $\{P\}\, C\, \{Q\}$ for some P, C, Q.

Theorem H1: $\dfrac{}{\{Q[e/v]\}\ v := e\ \{Q\}}$

For all assignment statements $v := e$

if the proposition Q holds after, then $Q[e/v]$ must have held before.

Theorem H2: $\dfrac{\{P\}\, C_1\, \{Q\} \qquad \{Q\}\, C_2\, \{R\}}{\{P\}\, C_1 ; C_2\, \{R\}}$

For all P, Q, R, ...

$$\{P\}\ C_1 ; C_2\ \{R\}$$

For all P, Q, R, C_1, C_2,

if $\{P\}\ C_1\ \{Q\}$ holds &

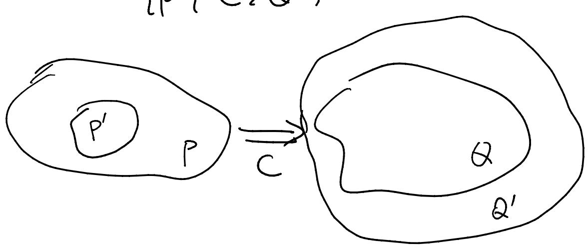
if $\{Q\}\ C_2\ \{R\}$ holds,

then $\{P\}\ C_1 ; C_2\ \{R\}$ holds.

Theorem H3: $$\frac{\{P \wedge b\}\ C_1\ \{Q\} \qquad \{P \wedge \bar{b}\}\ C_2\ \{Q\}}{\{P\}\ \text{if}(b)\ \{C_1\}\ \text{else}\ \{C_2\}\ \{Q\}}$$

Theorem H4: $$\frac{P \Rightarrow I \qquad \{I \wedge b\}\ C\ \{I\} \qquad I \wedge \bar{b} \Rightarrow Q.}{\{P\}\ \text{while}\ (b)\ \{C\}\ \{Q\}}$$

Theorem H5: $$\frac{P' \Rightarrow P \qquad \{P\}\ C\ \{Q\} \qquad Q \Rightarrow Q'}{\{P'\}\ C\ \{Q'\}}$$



Input: array a of integers (non-empty)

$\{|a| > 0\}$ ← Precondition

```
r := a[0];                      C1
i := 0;                         C3
while (i < |a|) {
    if (a[i] < r) {             C6
        r := a[i]               C8
    };                          C5
    i := i+1                    C7
}                               C4
```

C_2

i := i+1

}

<u>Output</u>: v. Minimum element which occurs in a.

Post condition

$$(\forall i \quad 0 \leq i < |a| \Rightarrow v \leq a[i]) \text{ and}$$
$$(\exists i \quad 0 \leq i < |a| \text{ and } v = a[i])$$

$\{Inv\}\ b\ \ c\ \ \{Inv\}\ b\ \ c\ \ \{Inv\}\ b\ c \ldots\ \ \{Inv\}\ \bar{b}$

Condition

body

Conceptual execution of the loop.

---

① We want to apply Theorem H2.

I.e. "invent" Q s.t.

$\{Pre\}\ C_1\ \{Q\} \qquad \{Q\}\ C_2\ \{Post\}$

<u>Proposal</u>: $Q = Pre \text{ and } v = a[0]$.

<u>Subgoal 1</u>: $\{Pre\}\ v := a[0]\ \ \{Pre \text{ and } v = a[0]\}$

<u>Proposal</u>: Trivial.

<u>Proposal'</u>: <u>Assignment rule</u>.

$\{Pre\} \Rightarrow \{Pre \text{ and } a[0] = a[0]\}$

$v := a[0]$

$\{Pre \text{ and } v = a[0]\}$

Subgoal 2: $\{Pre \text{ and } v = a[0]\}\ C_2\ \{Post\}$

Subgoal 2: {Pre and v=a[0]} C_2 {Post}

Q'

$\downarrow$

$C_2 = C_3 ; C_4$

$Q' = \{$ Pre and v= a[0] and i = 0 $\}$

Subgoal 2.2: {Pre and v=a[0] and i=0}

C_4 $\leftarrow$ The while loop.

{Post}

Q

P Pre = |a|>0

Use theorem H4.

$$\frac{P \Rightarrow I \qquad \{I \wedge b\}\ c\ \{I\} \qquad I \wedge \overline{b} \Rightarrow Q}{\{P\}\ \text{while}\ (b)\ \{I\}\ \{Q\}}$$

Invariant
i <= |a| and
forall j, 0 <= j < i ==> v <= a[j] and
i == 0 ==> v == a[0] and
i > 0 ==> exists j: int :: 0 <= j < i && v == a[j]

How does one prove $P \Rightarrow Q \wedge R$?

$\forall x : \mathbb{N}$, if x is divisible by 6,

then x is divisible by 2 and
x is divisible by 3.

Part 1 : Show that $P \Rightarrow Q$.

Part 2 : Show that $P \Rightarrow R$.

Subgoal 2.2.1 : $P \Rightarrow I$

$(\text{Pre and } i = 0 \text{ and } v = a[0]) \Rightarrow I$.

$\_ \text{ and } \_ \text{ and } \_ \text{ and } \_$

Subgoal 2.2.2 : To show : $\{I \wedge b\}\ C_5\ \{I\}$

Subgoal 2.2.3 : $I \wedge \overline{b} \Rightarrow \text{Post}$

$(\_ \text{ and } \_ \text{ and } \_ \text{ and } \_) \text{ and } (\text{not } i < |a|)$

$\Downarrow$

$(\forall j \_\_) \text{ and } (\exists j \_\_)$