cs.cornell.edu/Courses/cs4160/2019sp/tersel.pdf/Hoare.6ta

More on the assignment rule.

$$\overline{\{A[e/x]\}\ x := e\ \{A\}}$$

also

$$\overline{\{Q[X \mapsto a]\}\ X := a\ \{Q\}}.$$

Easy example:

$\{Y = 1\}\ X := Y\ \{X = 1\}$

I-ness transferred from Y to X.

also: $\{Y + Z = 1\}\ X := Y + Z\ \{X = 1\}$

or for any arithmetic expression a,

$\{a = 1\}\ X := a\ \{X = 1\}$

Lets read the general rule:

$\{Q[X \mapsto a]\}\ X := a\ \{Q\}$

precondition ~~assumption~~: Q, but with X replaced by a (or where a is substituted for X).

post condition: Q

more examples:

$\{(X \leq 5)[X \mapsto X+1]\}\ X := X+1\ \{X \leq 5\}$

ie $X+1 \leq 5$

$\{(X = 3)[X \mapsto 3]\}\ X := 3\ \{X = 3\}$

ie $3 = 3$

$\{(0 \leq X \wedge X \leq 5)[X \mapsto 3]\}\ X := 3\ \{0 \leq X \wedge X \leq 5\}$

ie $0 \leq 3 \wedge 3 \leq 5$

Rule of consequence.

Want

$\{X < 4\}\ X := X + 1\ \{X < 5\}$

not quite in right form.

$\{X + 1 < 5\}\ X := X + 1\ \{X < 5\}$

but $X < 4 \iff X + 1 < 5$, hence

$\{X < 4\}\ X := X + 1\ \{X < 5\}$ is valid

Conditional. Want $\{true\}$ if $y \leq 0$ then $x := 1$ else $x := y$ $\{x > 0\}$

How?

$$\frac{true \wedge y \leq 0 \Rightarrow 1 > 0 \quad \{1 > 0\}\ x := 1\ \{x > 0\}}{\{true \wedge y \leq 0\}\ x := 1\ \{x > 0\}} \qquad \frac{true \wedge y > 0 \Rightarrow y > 0 \quad \{y > 0\}\ x := y\ \{x > 0\}}{\{true \wedge y > 0\}\ x := y\ \{x > 0\}}$$

$$\{true\}\ \text{if } y \leq 0 \text{ then } x := 1 \text{ else } x := y\ \{x > 0\}$$

Alt. Rules $\vdash \{true\}\ x := e\ \{x = e\}$

Can we show something bogus?

$\{true\}\ x := x + 1\ \{x = x + 1\}$

$0 = 1$ not true!

Loop Invariants

$\{x \leq 0\}$ while $x \leq 5$ do $x := x+1$ $\{x = 6\}$

use I: $x \leq 6$.

$$\frac{x \leq 6 \wedge x \leq 5 \Rightarrow x+1 \leq 6 \qquad \{x+1 \leq 6\}\ x := x+1\ \{x \leq 6\}}{\{x \leq 6 \wedge x \leq 5\}\ x := x+1\ \{x \leq 6\}}$$

$$\{x \leq 6\}\ \text{while } x \leq 5 \text{ do } x := x+1\ \{x \leq 6 \wedge x > 5\}$$

Rule of consequence:

$$\frac{x \leq 0 \Rightarrow x \leq 6 \qquad x \leq 6 \wedge x > 5 \Rightarrow x = 6 \qquad \{x \leq 6\}\ \text{while } \ldots}{\{x \leq 0\}\ \text{while} \ldots\ \{x = 6\}}$$

//

Loop invariant: try bogus $x := 0$ invariant.

//

Product Example.

$\{n \geq 0\}$
$p := 0;$
$x := 0;$
while $x < n$ do
  $x := x + 1;$
  $p := p + m$
$\{p = n * m\}$

— $p = x \cdot m$ is an invariant but not ~~safe~~ safe.

$x \geq n \quad p = x \cdot m \quad p \geq n \cdot m$

try $p = x \cdot m \wedge x = n$ not nice enough!
try $p = x \cdot m \wedge x \leq n$ that works.

i. sequential composition

$$\frac{\{A\}\ c_1\ \{C\} \qquad \{C\}\ c_2\ \{B\}}{\{A\}\ c_1; c_2\ \{B\}}$$

$$\frac{\{n \geq 0\}\ p := 0; x := 0\ \{C\} \qquad \{C\}\ \text{while} \ldots \{p = n * m\}}{\{n \geq 0\}\ p := 0; x := 0; \text{while} \ldots \{p = n * m\}}$$

A c_1 c_2 B

2. Then use while rule. $I = C$. But need to use rule of consequence

$$\frac{\{I \wedge b\}\ c\ \{I\}}{\{I\}\ \text{while } b \text{ do } c\ \{I \wedge \neg b\}}$$

$\{I \wedge \neg b\} \Rightarrow \{p = n * m\}$

Rule of consequence

$$\frac{A' \Rightarrow A \qquad \{A\}\ c'\ \{B\} \qquad B \Rightarrow B'}{\{A'\}\ c'\ \{B'\}}$$

$I = A = A' = C$
$B = I \wedge \neg B$
$B' = p = n * m.$

Etc.