Hoare Logic 2

slides by Chris Osborn

Hoare Triple

P { …code…} Q

$$\frac{}{P[e/x]\ \{\ x := e\ \}\ P}$$

$$\frac{P\ \{\ C_1\ \}\ R \qquad R\ \{\ C_2\ \}\ Q}{P\ \{\ C_1;\ C_2\ \}\ Q}$$

$$\frac{P \wedge b\ \{\ C_1\ \}\ Q \qquad P \wedge \neg b\ \{\ C_2\ \}\ Q}{P\ \{\ \text{if } b \text{ then } C_1 \text{ else } C_2\ \}\ Q}$$

While Rule

$$\frac{P \wedge b \; \{\, C \,\} \; P}{P \; \{\text{While } b \; C\} \; P \wedge \neg b}$$

(P is a **loop invariant**)

Rule of Consequence

$$\frac{P \rightarrow P' \qquad P' \; \{\, C \,\} \; Q' \qquad Q' \rightarrow Q}{P \; \{\, C \,\} \; Q}$$

Sample Proofs

- sum of n
- fibonacci
- list append
- list reverse
- termination

Sum of n

$x = 0$ & $y = 0$

$P \equiv x = 1 + \ldots + y \wedge y \leq n$

```
{
  While y < n
    y := y + 1;
    x := x + y
}
```

$x = 1 + \ldots + n$

$x = 0 \wedge y = 0 \Rightarrow x = 1 + \ldots + y \wedge y \le n$ ✓

$x = 1 + \ldots + y \wedge y \le n \wedge \neg(y < n) \Rightarrow x = 1 + \ldots + n$ ✓

$x = 1 + \ldots + y \wedge y \le n \wedge y < n \Rightarrow$? ✓

$\boxed{x + y + 1 = (1 + \ldots + (y + 1)) \wedge y + 1 \le n}$

$\{y := y + 1\}$ $x + y = 1 + \ldots + y \wedge y \le n$

$\{x := x + y\}$ $x = 1 + \ldots + y \wedge y \le n$

? $\{y := y + 1; x := x + y\}$ $x = 1 + \ldots + y \wedge y \le n$

$x = 1 + \ldots + y \wedge y \le n \wedge y < n$ $\{y := y + 1; x := x + y\}$ $x = 1 + \ldots + y \wedge y \le n$

$x = 1 + \ldots + y \wedge y \le n$ $\{\text{While } y < n \ldots\}$ $x = 1 + \ldots + y \wedge y \le n \wedge \neg(y < n)$

$x = 0 \wedge y = 0$ $\{\text{While} \ldots\}$ $x = 1 + \ldots + n$

Fibonacci

$x = 0$ & $y = 1$ & $z = 1$ & $1 \leq n$

```
{
  While z < n
    y := x + y;
    x := y – x;
    z := z + 1
}
```

$y = \text{fib } n$

$P \equiv y = \text{fib } z \wedge x = \text{fib } (z-1)$
$\wedge\, z \leq n$

$x = 0 \wedge y = 1 \wedge z = 0 \wedge 1 \leq n \Rightarrow y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n$ ✓

$y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n \wedge \neg(z < n) \Rightarrow y = \text{fib } n$ ✓

$y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n \wedge z < n \Rightarrow$? ✓

$\boxed{x\text{+}y = \text{fib } (z\text{+}1) \wedge x\text{+}y\text{-}x = \text{fib } (z\text{+}1\text{-}1) \wedge z + 1 \leq n}$

$\{y := x + y\}$ $y = \text{fib } (z\text{+}1) \wedge y\text{-}x = \text{fib } (z\text{+}1\text{-}1) \wedge z + 1 \leq n$

$\{x := y - x\}$ $y = \text{fib } (z\text{+}1) \wedge x = \text{fib } (z\text{+}1\text{-}1) \wedge z + 1 \leq n$

$\{z := z + 1\}$ $y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n$

? $\{y := x + y;\ x := y - x;\ z := z + 1\}$ $y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n$

$y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n \wedge z < n$ $\{y := x + y;\ x := y - x;\ z := z + 1\}$ $y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n$

$y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n$ $\{\text{While } z < n \ldots\}$ $y = \text{fib } z \wedge x = \text{fib } (z\text{-}1) \wedge z \leq n \wedge \neg(z < n)$

$x = 0 \wedge y = 1 \wedge z = 0 \wedge 1 \leq n$ $\{\text{While} \ldots\}$ $y = \text{fib } n$

List length

$P \equiv \text{len lst} = y + \text{len } x$

```
x = lst & y = 0
{
  While x ≠ []
    x := tl x;
    y := y + 1
}
y = len lst
```

$$x = \mathrm{lst} \wedge y = 0 \Rightarrow \mathrm{len\ lst} = y + \mathrm{len}\ x \qquad ✓$$

$$\mathrm{len\ lst} = y + \mathrm{len}\ x \wedge \neg(x \neq []) \Rightarrow y = \mathrm{len\ lst} \qquad ✓$$

$$\mathrm{len\ lst} = y + \mathrm{len}\ x \wedge x \neq [] \Rightarrow \quad ? \qquad ✓$$

$$\boxed{\mathrm{len\ lst} = y + 1 + \mathrm{len(tl}\ x)}$$

$$\{x := \mathrm{tl}\ x\} \qquad \mathrm{len\ lst} = y + 1 + \mathrm{len}\ x$$

$$\{y := y + 1\} \qquad \mathrm{len\ lst} = y + \mathrm{len}\ x$$

$$? \qquad \{x := \mathrm{tl}\ x;\ y := y + 1\} \qquad \mathrm{len\ lst} = y + \mathrm{len}\ x$$

$$\mathrm{len\ lst} = y + \mathrm{len}\ x \wedge x \neq [] \qquad \{x := \mathrm{tl}\ x;\ y := y + 1\} \qquad \mathrm{len\ lst} = y + \mathrm{len}\ x$$

$$\mathrm{len\ lst} = y + \mathrm{len}\ x \qquad \{\mathrm{While}\ x \neq []\ \ldots\} \qquad \mathrm{len\ lst} = y + \mathrm{len}\ x \wedge \neg(x \neq [])$$

$$x = \mathrm{lst} \wedge y = 0 \qquad \{\mathrm{While}\ \ldots\} \qquad y = \mathrm{len\ lst}$$

List reverse

$x = lst$ & $y = []$

$P \equiv lst = rev\ y\ @\ x$

```
{
  While x ≠ []
    y := hd x :: y;
    x := tl x
}
```

$y = rev\ lst$

$$\mathit{x = lst} \wedge \mathit{y} = [\,] \Rightarrow \mathit{lst = rev\ y\ @\ x} \quad ✓$$

$$\mathit{lst = rev\ y\ @\ x} \wedge \neg(\mathit{x} \neq [\,]) \Rightarrow \mathit{y = rev\ lst} \quad ✓$$

$$\mathit{lst = rev\ y\ @\ x} \wedge \mathit{x} \neq [\,] \Rightarrow \ ? \quad ✓$$

$$\boxed{\mathit{lst = rev\ (hd\ x\ @\ y)\ @\ (tl\ x)}}$$

$$\{\mathit{y := hd\ x\ @\ y}\} \quad \mathit{lst = rev\ y\ @\ (tl\ x)}$$

$$\{\mathit{x := tl\ x}\} \quad \mathit{lst = rev\ y\ @\ x}$$

$$? \quad \{\mathit{y := hd\ x\ @\ y;\ x := tl\ x}\} \quad \mathit{lst = rev\ y\ @\ x}$$

$$\mathit{lst = rev\ y\ @\ x} \wedge \mathit{x} \neq [\,] \quad \{\mathit{y := hd\ x\ @\ y;\ x := tl\ x}\} \quad \mathit{lst = rev\ y\ @\ x}$$

$$\mathit{lst = rev\ y\ @\ x} \quad \{\mathit{While}\ \mathit{x} \neq [\,]\ \ldots\} \quad \mathit{lst = rev\ y\ @\ x} \wedge \neg(\mathit{x} \neq [\,])$$

$$\mathit{x = lst} \wedge \mathit{y} = [\,] \quad \{\mathit{While}\ \ldots\} \quad \mathit{y = rev\ lst}$$