

Hoare Logic 2

slides by Chris Osborn

Hoare Triple

$$P \{ \dots \text{code} \dots \} Q$$
$$\frac{}{P[e/x] \{ x := e \} P}$$
$$\frac{P \{ C_1 \} R \quad R \{ C_2 \} Q}{P \{ C_1; C_2 \} Q}$$
$$\frac{P \wedge b \{ C_1 \} Q \quad P \wedge \neg b \{ C_2 \} Q}{P \{ \text{if } b \text{ then } C_1 \text{ else } C_2 \} Q}$$

While Rule

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

(P is a **loop invariant**)

Rule of Consequence

$$\frac{P \rightarrow P' \quad P' \{ C \} Q' \quad Q' \rightarrow Q}{P \{ C \} Q}$$

Sample Proofs

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

Sum of n

$x = 0 \ \& \ y = 0$ $P \equiv x = 1 + \dots + y \ \wedge \ y \leq n$
 {
 While $y < n$
 $y := y + 1;$
 $x := x + y$
 }
 $x = 1 + \dots + n$

$x = 0 \ \& \ y = 0 \rightarrow x = 1 + \dots + y \ \wedge \ y \leq n$	✓
$x = 1 + \dots + y \ \wedge \ y \leq n \ \& \ \neg(y < n) \rightarrow x = 1 + \dots + n$	✓
$x = 1 + \dots + y \ \wedge \ y \leq n \ \& \ y < n \rightarrow ?$	✓

$x + y + 1 = 1 + \dots + y + 1 \ \wedge \ y + 1 \leq n$
 { $y := y + 1$ } $x + y = 1 + \dots + y \ \wedge \ y \leq n$
 { $x := x + y$ } $x = 1 + \dots + y \ \wedge \ y \leq n$

? { $y := y + 1; x := x + y$ } $x = 1 + \dots + y \ \wedge \ y \leq n$

$x = 1 + \dots + y \ \wedge \ y \leq n \ \& \ y < n$ { $y := y + 1; x := x + y$ } $x = 1 + \dots + y \ \wedge \ y \leq n$

$x = 1 + \dots + y \ \wedge \ y \leq n$ {While $y < n \dots$ } $x = 1 + \dots + y \ \wedge \ y \leq n \ \& \ \neg(y < n)$

$x = 0 \ \& \ y = 0$ {While ...} $x = 1 + \dots + n$

Fibonacci

$x = 0 \ \& \ y = 1 \ \& \ z = 1 \ \& \ 1 \leq n$
 {
 While $z < n$ $P \equiv y = \text{fib } z \ \& \ x = \text{fib } (z-1) \ \& \ z \leq n$
 $y := x + y;$
 $x := y - x;$
 $z := z + 1$
 }
 $y = \text{fib } n$

$x = 0 \ \& \ y = 1 \ \& \ z = 0 \ \& \ 1 \leq n \rightarrow y = \text{fib } z \ \& \ x = \text{fib } (z-1) \ \& \ z \leq n$	✓
$y = \text{fib } z \ \& \ x = \text{fib } (z-1) \ \& \ z \leq n \ \& \ \neg(z < n) \rightarrow y = \text{fib } n$	✓
$y = \text{fib } z \ \& \ x = \text{fib } (z-1) \ \& \ z \leq n \ \& \ z < n \rightarrow ?$	✓

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

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

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

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

$x = 0 \ \& \ y = 1 \ \& \ z = 0 \ \& \ 1 \leq n$ {While ...} $y = \text{fib } n$

List length

$x = \text{lst} \ \& \ y = 0$ $P \equiv \text{len lst} = y + \text{len } x$
 {
 While $x \neq []$
 $x := \text{tl } x;$
 $y := y + 1$
 }
 $y = \text{len lst}$

$x = \text{lst} \ \& \ y = 0 \rightarrow \text{len lst} = y + \text{len } x$	✓
$\text{len lst} = y + \text{len } x \ \& \ \neg(x \neq []) \rightarrow y = \text{len lst}$	✓
$\text{len lst} = y + \text{len } x \ \& \ x \neq [] \rightarrow ?$	✓

$\text{len lst} = y + 1 + \text{len } (\text{tl } x)$
 { $x := \text{tl } x$ } $\text{len lst} = y + 1 + \text{len } x$
 { $y := y + 1$ } $\text{len lst} = y + \text{len } x$

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

$\text{len lst} = y + \text{len } x \ \& \ x \neq []$ { $x := \text{tl } x; y := y + 1$ } $\text{len lst} = y + \text{len } x$

$\text{len lst} = y + \text{len } x$ {While $x \neq [] \dots$ } $\text{len lst} = y + \text{len } x \ \& \ \neg(x \neq [])$

$x = \text{lst} \ \& \ y = 0$ {While ...} $y = \text{len lst}$

List reverse

```

x = lst & y = []      P ≡ lst = rev y @ x
{
  While x ≠ []
    y := hd x :: y;
    x := tl x
}
y = rev lst
  
```

$x = \text{lst} \wedge y = [] \rightarrow \text{lst} = \text{rev } y @ x$	✓
$\text{lst} = \text{rev } y @ x \wedge \neg(x \neq []) \rightarrow y = \text{rev lst}$	✓
$\text{lst} = \text{rev } y @ x \wedge x \neq [] \rightarrow ?$	✓

$\boxed{\text{lst} = \text{rev}(\text{hd } x @ y) @ (\text{tl } x)}$
 $\{y := \text{hd } x @ y; \text{lst} = \text{rev } y @ (\text{tl } x)\}$
 $\{x := \text{tl } x; \text{lst} = \text{rev } y @ x\}$

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

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

$\text{lst} = \text{rev } y @ x$ $\{\text{While } x \neq [] \dots\}$ $\text{lst} = \text{rev } y @ x \wedge \neg(x \neq [])$

$x = \text{lst} \wedge y = []$ $\{\text{While } \dots\}$ $y = \text{rev lst}$