Exercises on Hoare's Logic

Andrea Simonetto*
(simonett@cs.unibo.it)

February 7, 2009

*Università degli Studi di Bologna

HL Rules

- $\vdash \{p[E/x]\} \quad x := E \quad \{p\}$

- $\dfrac{\{p\} \quad S \quad \{q\} \qquad \{q\} \quad T \quad \{r\}}{\{p\} \quad S;T \quad \{r\}}$

- $\dfrac{\{p \wedge B\} \quad S \quad \{q\} \qquad \{p \wedge \neg B\} \quad T \quad \{q\}}{\{p\} \quad \text{if } \underline{B} \text{ then } S \text{ else } T \text{ fi} \quad \{q\}}$

- $\dfrac{\{p \wedge B\} \quad S \quad \{p\}}{\{p\} \quad \text{while } \underline{B} \text{ do } S \text{ od} \quad \{p \wedge \neg B\}}$

- $\dfrac{p \Rightarrow p' \qquad \{p'\} \quad S \quad \{q'\} \qquad q' \Rightarrow q}{\{p\} \quad S \quad \{q\}}$

1 Max

Let $\underline{Max(x, y)}$ be defined as follows:

```
if(x >= y) then
   z := x
else
   z := y
fi
```

Definition 1 *The MAX function is defined as follow:*

$$MAX(x, y) = \begin{cases} x & \textit{if } x \geq y \\ y & \textit{if } y < x \end{cases}$$

Lemma 1 (Max)

$$\vdash \{tt\} \quad \underline{Max(x, y)} \quad \{z = MAX(x, y)\}$$

Proof.

$$\frac{\{x \geq y\} \quad z := x \quad \{z = MAX(x, y)\} \qquad \{x < y\} \quad z := y \quad \{z = MAX(x, y)\}}{\{tt\} \quad \underline{Max(x, y)} \quad \{z = MAX(x, y)\}}$$

□

2 Swap

Let $\underline{Swap(x,y)}$ be defined as follows:

```
t := x;
x := y;
y := t
```

Lemma 2 (Swap) *Let* t *be a fresh variable. Then, for each property* P *on* x *and* y*:*

$$\vdash \{P(x,y)\} \quad \underline{Swap(x,y)} \quad \{P(y,x)\}$$

Proof.

$$\cfrac{\{P(x,y)\} \quad t := x \quad \{P(t,y)\} \qquad \cfrac{\{P(t,y)\} \quad x := y \quad \{P(t,x)\} \qquad \{P(t,x)\} \quad y := t \quad \{P(y,x)\}}{\{P(t,y)\} \quad x := y; y := t \quad \{P(y,x)\}}}{\{P(x,y)\} \quad \underline{Swap(x,y)} \quad \{P(y,x)\}}$$

□

3 Integer division

Let $\underline{Div(x,y)}$ be defined as follows:

```
a := 0;
b := x;
while(b >= y) do
   b := b - y;
   a := a + 1
od
```

Lemma 3 (Integer division)

$$\vdash \{x \geq 0 \land y \geq 0\} \quad \underline{Div(x,y)} \quad \{x = y \cdot a + b \land 0 \leq b < y\}$$

Proof.

1. $\vdash \{x = y \cdot 0 + x \land x \geq 0 \land y \geq 0\} \quad a := 0 \quad \{x = y \cdot a + x \land x \geq 0 \land y \geq 0\}$
2. $\vdash \{x = y \cdot a + x \land x \geq 0 \land y \geq 0\} \quad b := x \quad \{x = y \cdot a + b \land b \geq 0 \land y \geq 0\}$
3. $\dfrac{(1) \qquad (2)}{\{x = y \cdot 0 + x \land x \geq 0 \land y \geq 0\} \quad a := 0; b := x \quad \{x = y \cdot a + b \land b \geq 0 \land y \geq 0\}}$
4. $\vdash \{x = y \cdot (a+1) + b - y \land b \geq 0 \land y \geq 0 \land b \geq y\} \quad b := b - y \quad \{x = y \cdot (a+1) + b \land b \geq 0 \land y \geq 0\}$
5. $\vdash \{x = y \cdot (a+1) + b \land b \geq 0 \land y \geq 0\} \quad a := a + 1 \quad \{x = y \cdot a + b \land b \geq 0 \land y \geq 0\}$
6. $\dfrac{\dfrac{(4) \qquad (5)}{\{x = y \cdot a + b \land b \geq 0 \land y \geq 0 \land b \geq y\} \quad b := b - y; a := a + 1 \quad \{x = y \cdot a + b \land b \geq 0 \land y \geq 0\}}}{\{x = y \cdot a + b \land b \geq 0 \land y \geq 0\} \quad \text{while(b>=y) do ... od} \quad \{x = y \cdot a + b \land b \geq 0 \land y \geq 0 \land b < y\}}$
7. $\dfrac{\dfrac{(3) \qquad (6)}{\{x \geq 0 \land y \geq 0\} \quad \underline{Div(x,y)} \quad \{x = y \cdot a + b \land b \geq 0 \land y \geq 0 \land b < y\}} \qquad x = y \cdot a + b \land b \geq 0 \land y \geq 0 \land b < y \Rightarrow x = y \cdot a + b \land 0 \leq b < y}{\{x \geq 0 \land y \geq 0\} \quad \underline{Div(x,y)} \quad \{x = y \cdot a + b \land 0 \leq b < y\}}$

□

4 Exponential

Let $\underline{Exp(x,y)}$ be defined as follows:

```
b := y;
z := 1;
while(b != 0) do
   b := b - 1;
   z := z * x
od
```

Lemma 4 (Exponential)

$$\vdash \{tt\} \quad \underline{Exp(x,y)} \quad \{z = x^y\}$$

Proof.

1. $$\frac{\{tt\} \quad b := y \quad \{1 = x^{y-b}\} \qquad \{1 = x^{y-b}\} \quad z := 1 \quad \{z = x^{y-b}\}}{\{tt\} \quad b := y; z := 1 \quad \{z = x^{y-b}\}}$$

2. $$\cfrac{\cfrac{\cfrac{\{b \neq 0 \wedge z = x^{y-b}\} \quad b := b-1 \quad \{b \neq -1 \wedge z = x^{y-b-1}\} \qquad b \neq -1 \wedge z = x^{y-b-1} \Rightarrow z = x^{y-b-1}}{\{b \neq 0 \wedge z = x^{y-b}\} \quad b := b-1 \quad \{z = x^{y-b-1}\}} \qquad \{z = x^{y-b-1}\} \quad z := z * x \quad \{z = x^{y-b}\}}{\{b \neq 0 \wedge z = x^{y-b}\} \quad b := b-1; z := z * x1 \quad \{z = x^{y-b}\}}}{\{z = x^{y-b}\} \quad \text{while(b!=0) ...} \quad \{z = x^y\}}$$

3. $$\frac{(1) \qquad (2)}{\{tt\} \quad \underline{Exp(x,y)} \quad \{z = x^y\}}$$

□

5 Factorial

Let $\underline{Fact(x)}$ be defined as follows:

```
y := 1;
z := 0;
while(z != x) do
   z := z + 1;
   y := y * z
od
```

Lemma 5 (Factorial)

$$\vdash \{tt\} \quad \underline{Fact(x)} \quad \{y = x!\}$$

Proof.

1. $\vdash \{y \cdot (z+1) = (z+1)!\} \quad z := z+1 \quad \{y \cdot z = z!\}$

2. $\vdash \{y \cdot z = z!\} \quad y := y * z \quad \{y = z!\}$

3. $$\dfrac{\dfrac{z \neq x \wedge y = z! \Rightarrow y \cdot (z+1) = (z+1)! \qquad \dfrac{(1) \qquad (2)}{\{y \cdot (z+1) = (z+1)!\} \quad z := z+1; y := y * z \quad \{y = z!\}}}{\{z \neq x \wedge y = z!\} \quad z := z+1; y := y * z \quad \{y = z!\}}}{\{y = z!\} \quad while(z! = x)...od \quad \{y = x!\}}$$

4. $$\dfrac{\dfrac{\{tt\} \quad y := 1 \quad \{y = 1\} \qquad \{y = 1\} \quad z := 0 \quad \{y = z!\}}{\{tt\} \quad y := 1; z := 0 \quad \{y = z!\}} \qquad (3)}{\{tt\} \quad \underline{Fact(x)} \quad \{y = x!\}}$$

□

6 Square of a number

Let $\underline{Square(n)}$ be defined as follows:

```
x := n;
y := 0;
while(x > 0) do
   y := y + 2 * x - 1;
   x := x - 1
od
```

Lemma 6 (Square)

$$\vdash \{n \geq 0\} \quad \underline{Square(n)} \quad \{y = n^2\}$$

Proof.

1. $$\frac{\{n \geq 0\} \quad x := n \quad \{x \geq 0 \land 0 = n^2 - x^2\} \qquad \{x \geq 0 \land 0 = n^2 - x^2\} \quad y := 0 \quad \{x \geq 0 \land y = n^2 - x^2\}}{\{n \geq 0\} \quad x := n; y := 0 \quad \{x \geq 0 \land y = n^2 - x^2\}}$$

2. $$\frac{\{x > 0 \land y = n^2 - x^2\} \quad y := y + 2 * x - 1 \quad \{x > 0 \land y = n^2 - (x-1)^2\} \qquad \{x > 0 \land y = n^2 - (x-1)^2\} \quad x := x - 1 \quad \{x \geq 0 \land y = n^2 - x^2\}}{\{x > 0 \land y = n^2 - x^2\} \quad y := y + 2 * x - 1; x := x - 1 \quad \{x \geq 0 \land y = n^2 - x^2\}}$$

3. $$\cfrac{(1) \qquad \cfrac{\cfrac{x > 0 \land x \geq 0 \land y = n^2 - x^2 \Rightarrow x > 0 \land y = n^2 - x^2 \qquad (2)}{\{x > 0 \land x \geq 0 \land y = n^2 - x^2\} \quad y := y + 2 * x - 1; x := x - 1 \quad \{x \geq 0 \land y = n^2 - x^2\}}}{\{x \geq 0 \land y = n^2 - x^2\} \quad \text{while(x>0) ... od} \quad \{y = n^2\}}}{\{n \geq 0\} \quad \underline{Square(n)} \quad \{y = n^2\}}$$

$\square$

7 Fibonacci

Let $\underline{Fibo(n)}$ be defined as follows:

```
y := 1;
a := 0;
i := 2;
while(i <= n) do
   t := a + y;
   a := y;
   y := t;
   i := i + 1
od
```

Definition 2

$$FIBO(n) = \begin{cases} 0 & \textit{if } n = 0 \\ 1 & \textit{if } n = 1 \\ FIBO(n-1) + FIBO(n-2) & \textit{if } n \geq 2 \end{cases}$$

Lemma 7 (Fibonacci)

$$\vdash \{n > 0\} \quad \underline{Fibo(n)} \quad \{y = FIBO(n)\}$$

Proof.

1. $\dfrac{\{n > 0\} \quad y := 1 \quad \{n > 0 \wedge y = FIBO(1)\} \qquad \{n > 0 \wedge y = FIBO(1)\} \quad a := 0 \quad \{n > 0 \wedge y = FIBO(1) \wedge a = FIBO(0)\}}{\{n > 0\} \quad y := 1; a := 0 \quad \{n > 0 \wedge y = FIBO(1) \wedge a = FIBO(0)\}}$

2. $\dfrac{(1) \qquad \{n > 0 \wedge y = FIBO(1) \wedge a = FIBO(0)\} \quad i := 2 \quad \{i \leq n + 1 \wedge y = FIBO(i-1) \wedge a = FIBO(i-2)\}}{\{n > 0\} \quad y := 1; a := 0; i := 2 \quad \{i \leq n + 1 \wedge y = FIBO(i-1) \wedge a = FIBO(i-2)\}}$

3. $\vdash \{i \leq n \wedge a = FIBO(i-2) \wedge y = FIBO(i-1)\} \quad t := a + y \quad \{i \leq n \wedge t = FIBO(i) \wedge y = FIBO(i-1)\}$

4. $\vdash \{i \leq n \wedge t = FIBO(i) \wedge y = FIBO(i-1)\} \quad a := y \quad \{i \leq n \wedge t = FIBO(i) \wedge a = FIBO(i-1)\}$

5. $$\frac{(3) \qquad (4)}{\{i \leq n \wedge a = FIBO(i-2) \wedge y = FIBO(i-1)\} \quad t := a+y; a := y \quad \{i \leq n \wedge t = FIBO(i) \wedge a = FIBO(i-1)\}}$$

6. $$\frac{(5) \qquad \{i \leq n \wedge t = FIBO(i) \wedge a = FIBO(i-1)\} \quad y := t \quad \{i \leq n \wedge y = FIBO(i) \wedge a = FIBO(i-1)\}}{\{i \leq n \wedge a = FIBO(i-2) \wedge y = FIBO(i-1)\} \quad t := a+y; a := y; y := t \quad \{i \leq n \wedge y = FIBO(i) \wedge a = FIBO(i-1)\}}$$

7. $$\frac{(6) \qquad \{i \leq n \wedge y = FIBO(i) \wedge a = FIBO(i-1)\} \quad i := i+1 \quad \{i \leq n+1 \wedge y = FIBO(i-1) \wedge a = FIBO(i-2)\}}{\{i \leq n \wedge a = FIBO(i-2) \wedge y = FIBO(i-1)\} \quad t := a+y; a := y; y := t; i := i+1 \quad \{i \leq n+1 \wedge y = FIBO(i-1) \wedge a = FIBO(i-2)\}}$$

8. $$\frac{\dfrac{i \leq n \wedge i \leq n+1 \wedge a = FIBO(i-2) \wedge y = FIBO(i-1) \Rightarrow i \leq n \wedge a = FIBO(i-2) \wedge y = FIBO(i-1) \qquad (7)}{\{i \leq n \wedge i \leq n+1 \wedge a = FIBO(i-2) \wedge y = FIBO(i-1)\} \quad t := a+y; a := y; y := t; i := i+1 \quad \{i \leq n+1 \wedge y = FIBO(i-1) \wedge a = FIBO(i-2)\}}}{\{i \leq n+1 \wedge a = FIBO(i-2) \wedge y = FIBO(i-1)\} \quad \text{while(i<=n) do ... od} \quad \{a = FIBO(n-1) \wedge y = FIBO(n)\}}$$

9. $$\frac{\dfrac{(2) \qquad (8)}{\{n > 0\} \quad \underline{Fibo(n)} \quad \{a = FIBO(n-1) \wedge y = FIBO(n)\}} \qquad a = FIBO(n-1) \wedge y = FIBO(n) \Rightarrow y = FIBO(n)}{\{n > 0\} \quad \underline{Fibo(n)} \quad \{y = FIBO(n)\}}$$

□

8 Sum of power of two

Let $\underline{SumPow2(x)}$ be defined as follows:

```
while(m >= 0) do
   s := s + n;
   n := 2 * n;
   m := m - 1
od
```

Lemma 8 (Sum of power of two)

$$\vdash \{m \geq 0 \land n = 1 \land s = 0 \land x = m\} \quad \underline{SumPow2(x)} \quad \{s = \sum_{i=0}^{x} 2^i\}$$

Proof.

1. $\vdash \{m \geq 0 \land s = 2n - 1 \land n = 2^{x-m}\} \quad n := 2 * n \quad \{m \geq 0 \land s = n - 1 \land n = 2^{x-m+1}\}$

2. $\vdash \{m \geq 0 \land s = n - 1 \land n = 2^{x-m+1}\} \quad m := m - 1 \quad \{m \geq -1 \land s = n - 1 \land n = 2^{x-m}\}$

3. $$\frac{(1) \qquad (2)}{\{m \geq 0 \land s = 2n - 1 \land n = 2^{x-m}\} \quad n := 2 * n; m := m - 1 \quad \{m \geq -1 \land s = n - 1 \land n = 2^{x-m}\}}$$

4. $$\frac{\{m \geq 0 \land s = n - 1 \land n = 2^{x-m}\} \quad s := s + n \quad \{m \geq 0 \land s = 2n - 1 \land n = 2^{x-m}\} \qquad (3)}{\{m \geq 0 \land s = n - 1 \land n = 2^{x-m}\} \quad s := s + n; n := 2 * n; m := m - 1 \quad \{m \geq -1 \land s = n - 1 \land n = 2^{x-m}\}}$$

5. $$\frac{\dfrac{m \geq 0 \land m \geq -1 \land s = n - 1 \land n = 2^{x-m} \Rightarrow m \geq 0 \land s = n - 1 \land n = 2^{x-m} \qquad (4)}{\{m \geq 0 \land m \geq -1 \land s = n - 1 \land n = 2^{x-m}\} \quad s := s + n; n := 2 * n; m := m - 1 \quad \{m \geq -1 \land s = n - 1 \land n = 2^{x-m}\}}}{\{m \geq -1 \land s = n - 1 \land n = 2^{x-m}\} \quad \text{while(m>=0) do ... od} \quad \{m < 0 \land m \geq -1 \land s = n - 1 \land n = 2^{x-m}\}}$$

6. $$\frac{m \geq 0 \land n = 1 \land s = 0 \land x = m \Rightarrow m \geq -1 \land s = n - 1 \land n = 2^{x-m} \qquad (5) \qquad m < 0 \land m \geq -1 \land s = n - 1 \land n = 2^{x-m} \Rightarrow s = \sum_{i=0}^{x} 2^i}{\{m \geq 0 \land n = 1 \land s = 0 \land x = m\} \quad \underline{SumPow2(x)} \quad \{s = \sum_{i=0}^{x} 2^i\}}$$

□