Exercises 3

March 11, 2011

Relations, wp, sp

Recall the definitions of

Hoare triple $\{P\}\ r\ \{Q\}$ is
$$\forall s, s' \in S. s \in P \land (s, s') \in r \rightarrow s' \in Q$$

strongest postcondition
$$sp(P, r) = \{s' \mid \exists s. s \in P \land (s, s') \in r\}$$

weakest precondition
$$wp(r, Q) = \{s \mid \forall s'. (s, s') \in r \rightarrow s' \in Q\}$$

Exercise 1 - Relations

Prove the following or give a counterexample.

1. $(r \cup s) \circ t = (r \circ t) \cup (s \circ t)$
2. $(r \cap s) \circ t = (r \circ t) \cap (s \circ t)$

Exercise 2 - Characterization of sp

Prove

1. $sp(P, r)$ is the the smallest set Q such that $\{P\}r\{Q\}$, that is:
   - $\{P\}r\{sp(P, r)\}$
   - $\forall Q \subseteq S.\ \{P\}r\{Q\} \rightarrow sp(P, r) \subseteq Q$
2. If P_0 satisfies
   - $\{P_0\}r\{Q\}$
   - $\forall P \subseteq S.\ \{P\}r\{Q\} \rightarrow P \subseteq P_0$

   then $P_0 = wp(r, Q)$.

Exercise 3 - Conjunctivity of wp

Show that

1. $wp(r, Q_1 \cap Q_2) = wp(r, Q_1) \cap wp(r, Q_2)$
2. $wp(r_1 \cup r_2, Q) = wp(r_1, Q) \cap wp(r_2, Q)$

Exercise 4 - Postcondition of inverse versus wp

Using definitions of Hoare triple, sp, wp in Hoare logic, prove the following: If instead of good states we look at the completement set of error states, then *wp* corresponds to doing *sp* backwards. In other words, we have the following:

$$S \setminus wp(r, Q) = sp(S \setminus Q, r^{-1})$$

1 Hoare logic syntactically

Warm-up

Use your intuition to determine which of these Hoare triples are valid. All variables are assumed to be integers.

```
1)  {j = a} j:=j+1 {a = j + 1}
2)  {i = j} i:=j+i {i > j}
3)  {j = a + b} i:=b; j:=a {j = 2 * a}
4)  {i > j} j:=i+1; i:=j+1 {i > j}
5)  {i != j} if i>j then m:=i-j else m:=j-i {m > 0}
6)  {i = 3 * j} if i>j then m:=i-j else m:=j-i {m - 2 * j = 0}
7)  {x = b} while x>a do x:=x-1 {b = a}
```

Assignment axiom

$$\frac{}{\{Q[x := e]\}\ (x = e)\ \{Q\}} \tag{1}$$

Precondition strenghtening

$$\frac{\models P_1 \to P_2 \quad \{P_2\}c\{Q\}}{\{P_1\}c\{Q\}} \tag{2}$$

Postcondition weakening

$$\frac{\{P\}c\{Q_1\} \quad \models Q_1 \to Q_2}{\{P\}c\{Q_2\}} \tag{3}$$

if-then-else

$$\frac{\{P \land B\}c_1\{Q\} \quad \{P \land \neg B\}c_2\{Q\}}{\{P\}\text{if } (B)\ c_1 \text{ else } c_2\{Q\}} \tag{4}$$

loop

$$\frac{\{I\}c\{I\}}{\{I\}\ (c)^*\ \{I\}} \tag{5}$$

while loop Try yourself!

$$\frac{(\models P \to ?);\ \{?\}c\{?\};\ (\models ? \to Q)}{\{P\}\ \mathit{while}\{I\}(F)(c)\ \{Q\}} \tag{6}$$

For a sequential program $c_1, c_2, c_3, ..., c_n$ we can then apply these rules by writing

```
assert(P)
c1;
assert(Q)
c2;
assert(R)
```

meaning that we expect that these Hoare triples hold

```
{P} c1 {Q}
{Q} c2 {R}
```

Easy example

Use the proof rules to show that the following holds:

```
assert( x == x0 && y == y0)
z = x
x = y
y = z
assert (y ==  x0 && x == y0)
```

Some more examples

Prove the following:

1. $\{a > b\}$ `m:= 1; n:= a - b` $\{m * n > 0\}$
2. $\{s = 2^i\}$ `i := i + 1; s := s*2` $\{s = 2^i\}$
3. $\{True\}$ `if i < j then min := i else min := j` $\{(min \leq i) \wedge (min \leq j)\}$
4. $\{i > 0 \wedge j > 0\}$ `if i<j then min:=i else min:=j` $\{min > 0\}$
5. $\{s = 2^i\}$ `while i<n do i:=i+1; s:=s*2` $\{s = 2^i\}$

Complete example

Give a complete Hoare logic proof for the following code

```
{P: x >= 0}
a = x;
y = 0;
while (a > 0) {
  y = y + 1;
  a = a - 1;
}
{Q: x = y}
```