Sads Hw4

Atabak Hafeez

March 30, 2017

1 Verification

1.1 Euclidean Algorithm

Function Specification

Pre-condition:

$$P(m,n) := m > 0, n > 0$$

Post-condition:

$$Q(m,n,x) := x == EuclideanAlgorithm(m,n)$$

Loop invariants

$$I = EuclideanAlgorithm(x,y) == EuclideanAlgorithm(m,n)$$

Termination ordering

For the while loop in the algorithm, the termination ordering is:

$$x + y$$

1.2 Factorial

Function Specification

Pre-condition:

$$P(n) := n > 0$$

Post-condition:

$$P(n, product) := n! == product$$

Loop invariants

$$I := product == (factor - 1)!$$

Termination ordering

For the while loop in the algorithm, the termination ordering is:

$$n - factor$$

2 Dynamic Logic: Practice

See screenshots. I have run the example code for factorial which contains two implementations for it with the proof of correctness using why3 - both terminal and gui.

3 Dynamic Logic: Theory

For these proofs we need that :

1. $[P]F$: F holds in all successor state of s reachable by evaluating P. (section 9.4.1 in the notes)
2. Definition 11.3 (Theorem). A pure term t : bool is a theorem if it is true in every state.
3. Definition 11.4 (Soundness). A set of rules is sound if all provable formulas are theorems.
4. The rules for if and while from sections 11.1.2 and 11.1.3 respectively

3.1 If

The proof for if is simple. There are two possibilities for the branching. Given that C is pure, there is branching for $\neg C$ and C. If C, if evaluates to $[t]F$, which is true from number 1 above. Else if $\neg C$, the same hold i.e. $[t']F$ is true. Hence, $[t]F$ and $[t']F$ are theorems $\Rightarrow$ **if** is sound.

3.2 while

The while rule has three rules which need to shown are theorems. The first rule is just I which is obviously a theorem as it is the loop invariant assumption before the while loop starts. The second rule is the definition of the loop invariant itself. Assume I and C, then, $[t]I$ is a theorem by the same reason as above, using number 1 from above. The third rule is also a theorem because at the this point $\neg C$ becomes true and we already assumed I, and finally we get F from where we can continue the proof. Hence, **while** is sound.