CS 310, Assignment 6

Due on 10 April in class

This is a somehow more substantial assignment and so will be marked out of 15 rather than the usual 10 marks.

1. Verify the validity of the following correctness statements by adding all the intermediate assertions and so producing the proof tableau. State all the mathematical facts used. All variables are of type `int`.

```
ASSERT(x == x0)
int sign = -1;
if (x >= 0) sign = 1;
x = x * sign;
ASSERT(abs(x) == abs(x0) && x >= 0)
```

   `abs(x)` refers to the absolute value of `x`. This is surprisingly tricky for such a small and obviously correct code fragment, but still it is very satisfying to try it out on your own, so stop here and attempt it. If on the other hand you need a few hints, then read on.

   Hints: The tricky part is the missing else branch, which will force you to keep strengthening the post-condition until you find something that will match what you get from the then branch. The problem with this is that `sign` is free floating there, so you will need to strengthen its range. `sign >= 0` is sufficient to infer the negated loop condition but is not enough. Do not be afraid to further restrict the range as much as you want; if it works to the end then you are all set, and if it does not work then you can always come back and modify the range.

2. Assume a declarative interface where `n` and `max` are constant integers, and `A` is an array of integers of size `max`. Consider the following correctness statement:

```
ASSERT( 1 < n <= max )
int i;
i = n-1;
A[n-1] = 1;
while( i >= 1 ) {
    A[i-1] = A[i] + n - i + 1;
    i = i-1;
}
ASSERT( ForAll(k = 0; k < n) A[k] == (n-k)*(n-k+1)/2 )
```

(a) Give a complete proof tableau for the above correctness statement by adding all the intermediate assertions. State all the mathematical facts that are used in the proof.

Hints: As our discussion in class will also emphasize the following two assertions are obvious tautologies:

```
Forall (k=i; k<j) P(k)  <=>  P(i) && Forall (k=i+1; k<j) P(k)
Forall (k=i; k<j) P(k)  <=>  P(j-1) && Forall (k=i; k<j-1) P(k)
```

That is, we can always separate as an extra conjunctive term an "end" of the range in a universally quantified property. Also note that this time the loop goes backward. This might be intimidating but actually that does not make much of a difference.

(b) Provide a formal argument for the total correctness of the statement.

3. A machine makes screws and nuts using a tap (for the nuts) and a die (for the screws). The tool (tap or die) has to be changed between screws and nuts. Let such a machine be specified by the following CSP process where the actions screw and nut represent the process of manufacturing a screw or a nut, respectively. The action check verifies that the right tool is being used for the next part and changes the tool if necessary (from tap to die or the other way around as appropriate).

$$\begin{array}{lcl} \text{NUT} & = & \text{check} \rightarrow \text{nut} \rightarrow \text{NUT} \\ \text{SCREW} & = & \text{screw} \rightarrow \text{check} \rightarrow \text{SCREW} \\ \text{MACHINE} & = & \text{NUT} \,||\, \text{SCREW} \end{array}$$

(a) Draw the transition graph of the process MACHINE.

(b) Obviously the tool needs to be checked (and changed) between making nuts and making screws. Is this requirement always observed by MACHINE? Explain why or why not as the case might be.

Make sure you review the submission guidelines posted on the course's Web site before handing in your answers.