CS 310, Assignment 7

Due on 8 April in class

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

```
ASSERT(0 <= n <= max)
int i;
i = n;
A[i] = 1;
while (i > 0) {
    A[i-1] = A[i]/2;
    i--;
}
ASSERT(∑_{k=0}^{n} A[k] = 2 − 1/2^n)
```

   (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.

   This is a relatively challenging proof, but will become easier with a few hints. Note first that the loop moves backward. There is nothing magical about that, just notice that at the end `i` will reach `0` rather than the typical maximum value. You will have to be creative (and it may take a few trial end errors) to introduce that `i` in the post-condition, mainly because the `0` it replaces appears a single time in the assertion but will have to be replaced two times (hint: `n == n-0`).

   Once this is done, try to proceed as usual by strengthening the post-condition with the negated loop condition and a range for the loop variables. You should be able to proceed uneventfully up to the top of the loop body. . . where your proof will bog down. Fear not, your time was not wasted. Instead, this is a sign that the post-condition (and loop invariant) need to be strengthened further. Think about what additional assertions would you need go continue. Go back and strengthen your post-condition by adding these assertions. Carry these additional assertions up through the existing proof. You will be done in no time.

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

2. Consider the following specification of a shop handling raw and cooked meat. The actions of handling raw meat, handling cooked meat and washing hands are represented by the CSP actions raw, cooked, and wash, respectively.

$$\begin{array}{lcl} \text{RAW} & = & \text{raw} \rightarrow \text{wash} \rightarrow \text{RAW} \\ \text{COOKED} & = & \text{wash} \rightarrow \text{cooked} \rightarrow \text{COOKED} \\ \text{SHOP} & = & \text{RAW} \parallel \text{COOKED} \end{array}$$

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

(b) Give the set traces(SHOP) and explain how you computed it.

(c) A common hygiene requirement while handling meat is that hands must be washed between handling raw and cooked meat. Does SHOP meet this requirement? Explain why or why not by computing and analyzing the set of traces of SHOP.

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