Formal Methods in Software Development
Exercise 2 (May 10)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.uni-linz.ac.at

March 30, 2007

The result is to me submitted to me by **May 10** (hard deadline) as an email that includes as attachments

- the declarations file and the proof directory (as a .zip or .tgz file) generated by the RISC ProofNavigator, and
- the Java/JML file together with the outputs of `jml` and `escjava2`.

1 Inserting an Element (Verification, 10 Points)

Verify with the help of the RISC ProofNavigator the partial correctness of the following Hoare triple for a program fragment that places into array b a copy of array a with element x inserted at position p.

$\{olda = a \land oldp = p \land oldx = x \land oldn = n \land 0 \leq p < n\}$

```
i = 0;
while i < n+1 do
  if i < p then
    b[i] := a[i]
  else if i = p then
    b[i] := x
  else
    b[i] := a[i-1];
  end
  i := i+1;
end
```

$$\{a = olda \land p = oldp \land x = oldx \land n = oldn \land \\ (\forall i : 0 \leq i < p \Rightarrow a[i] = b[i]) \;\land\; x = b[p] \;\land\; (\forall i : p \leq i < n \Rightarrow a[i] = b[i+1])\}$$

2 Inserting an Element (JML, 5 Points)

Write a JML header specification for the method

```
class Arrays
{
  // returns a copy of a with x at position p inserted
  static int[] insert(int[] a, int x, int p)
  {
    int n = a.length;
    int[] b = new int[n+1];
    for (int i=0; i<n+1; i++)
    {
      if (i < p)
        b[i] = a[i];
      else if (i == p)
        b[i] = x;
      else
        b[i] = a[i-1];
    }
    return b;
  }
}
```

Make this specification as strong as possible using the Hoare triple from the previous exercise as a hint (but also think about extra problems that might arise in the Java method).

Run your specification through `jml` and `escjava2` and include the output of these runs in the result of this exercise.