Formal Methods in Software Development
Exercise 2 (April 27)

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

March 21, 2006

The result is to me submitted to me by **April 27** (hard deadline) as a paper (handed out to me in class) or as a single PDF file (sent to me per email), in both cases with a cover sheet that contains your name and "Matrikelnummer".

1 Sorting Three Values

The command `SWAP` a b exchanges the values of two variables a and b; its weakest precondition is defined as:

$$\mathrm{wp}(\texttt{SWAP}\ a\ b,\ Q) = Q[a/b, b/a]$$

Use this information to formally verify the following Hoare triple:

$\{\ \}$

```
if b < a then
  if c < b then
    SWAP a c
  else
    SWAP a b;
    if c < b then SWAP b c
else if c < b then
  SWAP b c;
  if b < a then SWAP a b
```

$\{a \leq b \leq c\}$

2 Inserting an Element into an Array

Verify formally (by manual proof) 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.

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

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

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