Formal Methods in Software Development
Exercise 2 (May 10)

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

April 15, 2005

The exercise is to be submitted by **May 10** (hard deadline)

1. either as a single paper report (cover page with full name and Matrikelnummer, pages stapled) which is handed out to me in class,
2. or as a single PDF file sent to me per email.

Questions can be asked per email or in the class on April 28.

1 Sorting three Values

The command `SWAP` a b exchanges the values of two variables a and b i.e.

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

Use this information to formally verify the following Hoare triple:

$\{\ \}$

```
if (b < a)
{
  if (c < b)
    SWAP a c;
  else
  {
    SWAP a b;
    if (c < b) SWAP b c;
  }
}
else if (c < b)
{
  SWAP b c;
  if (b < a) SWAP a b;
}
```

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

2 Horner's Scheme

Verify formally the total correctness (partial correctness, termination, and non-abortion) of the following Hoare triple.

$\{s = 0 \land i = 0 \land n = \text{length}(a)\}$

```
while (i < n)
{
  s = 10*s;
  if (a[i] >= 0)
    s = s + a[i];
  else
    s = s - a[i];
  i = i+1;
}
```

$\{s = \sum_{i=0}^{n-1} |a_i| \cdot 10^{n-1-i}\}$

We know $\forall x : (x \geq 0 \Rightarrow |x| = x) \land (x < 0 \Rightarrow |x| = -x)$.