Formal Methods in Software Development
Sample Exam

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

January 11, 2012

Last Name:

First Name:

Matrikelnummer:

Studienkennzahl:

KV3 (questions 1-4):	85 points total.
KV4 (questions 1-5):	100 points total.

1. (25 points) Write a JML specification for the following method of the Java library (the specification shall be as expressive as possible).

```
public static void fill(int[] a, int fromIndex, int toIndex, int val)

    Assigns the specified int value to each element of the specified range
    of the specified array of ints. The range to be filled extends from index
    fromIndex, inclusive, to index toIndex, exclusive. (If fromIndex==toIndex,
    the range to be filled is empty.)

    Parameters:
        a - the array to be filled
        fromIndex - the index of the first element (inclusive) to be filled
                    with the specified value
        toIndex - the index of the last element (exclusive) to be filled
                  with the specified value
        val - the value to be stored in all elements of the array
    Throws:
        IllegalArgumentException - if fromIndex > toIndex
        ArrayIndexOutOfBoundsException - if fromIndex < 0 or toIndex > a.length
```

2. (15 points) Derive the weakest precondition of the following code

```
if (i < 10)
{
  i = i+1;
  a[i] = a[i]+3;
}
```

for postcondition $a[2] = 7$ (ignoring any “index out ouf bound” violations). Show all derivation steps and finally simplify the derived precondition as far as possible.

3. (20 points) Take the following program which is supposed to compute for given $n \in \mathbb{N}$ the result $s := n^2$:

   $\{n = oldn\}$

   ```
   s = 0; i = 1;
   while (i <= n)
   {
     s = s+2*i-1;
     i = i+1;
   }
   ```

   $\{s = n^2 \land n = oldn\}$

   First, assume you are given a suitable invariant I and termination term T for the loop. Using I and T, state all verification conditions that have to be proved for verifying the total correctness of this loop.

   Second, construct for $n = 5$ a table for the values of the variables after each loop iteration.

   Finally, using this table as a hint, give suitable definitions for I and T and perform the verification.

4. (25 points) Take the following asynchronous composition of two processes operating on shared variables x, y, i, j:

```
initially x = y = i = 0 and j = 1
loop          ||   loop
  x = x+j;    ||     wait i > 0;
  i = 1-i;    ||     y = y+i;
              ||     j = 1-j;
```

(a) (10 points) Give a formal model of the system (using the interleaving assumption for asynchronous composition); do not forget to model the program counters of the two processes.

(b) (5 points) Formalize in LTL the property "if at any time i becomes greater than zero, then later on also y will become greater than zero".

(c) (10 points) Is this property true for above system? If yes, explain why. If not, show an execution trace that violates the property. In the second case, if there exists an additional assumption for the system execution, under which the property holds, state this assumption (in detail).

5. (15 Points) Let S be the system described by the pseudo-code

```
initially i,j in {0,1,2} such that i < j
while i < j || while i < j
  i = i+1   ||   j = j-1
```

(checking the loop condition and performing the assignment are considered together as a single transition).

Model-check S for the correctness of the property $P :\Leftrightarrow \diamond(i = j)$ by constructing (in graphical form) the automaton for S, the automaton for the negation of P, and the product of the two automata. Based on the product automaton, argue whether P holds in S or not.