Prof. Bernd Finkbeiner, Ph.D.
Martin Zimmermann, Ph.D.
Leander Tentrup, B.Sc.

Summer term 2013
Problem Set 7
September 17, 2013

Verification

Problem 1: LTL warm-up [4 Points]

Express the following informal Linear Time Properties over $AP = \{a, b, c\}$ as LTL formulas and provide a justification.

1. There is no a before the first b
2. If there are infinitely many occurrences of a followed by b in the next step, there must be only finitely many c's
3. Every b is eventually followed by a non-empty sequence of a's that is terminated by a c
4. There are infinitely many a's and every a is followed by a, b or c

Problem 2: LTL equivalences [6 Points]

Prove or disprove the following equivalences of LTL–formulas:

$$\Box\varphi \rightarrow \Diamond\psi \equiv \varphi\, \mathcal{U}(\psi \vee \neg\varphi) \qquad \Box\Diamond\varphi \rightarrow \Box\Diamond\psi \equiv \Box(\varphi \rightarrow \Diamond\psi) \qquad \Diamond\,(\varphi\, \mathcal{U}\psi) \equiv \Diamond\psi$$

For disproving, a counterexample for one direction of the equivalence suffices. For proving, show both directions by applying already known equivalences for LTL or giving an argument using the LTL semantics.

The following exercises belong to the afternoon session.

Problem 3: Communication channels with SPIN [10 Points]

There is an easy solution to the mutual exclusion problem if one can communicate via channels instead of using shared memory.

a) Develop a Promela model of a mutual exclusion protocol for two processes, uses just one channel and no shared variables. [4 Points]

b) Use SPIN to check whether your protocol satisfies mutual exclusion. [2 Point]

c) Does your protocol avoid starvation? Give an informal argument why it does or a human readable counter example why it doesn't. [2 Points]

d) Assume you have four processes and a shared ressource that can be accessed by two processes at once, say a quadcore processor where only two cores at a time can read the RAM. Adopt your model from a) to this scenario. [2 Points]

Be prepared to demo your verification runs in the morning discussion slot on wednesday, either on your own laptop or by sending us all necessary files.