RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL FÜR INFORMATIK II
RWTH Aachen · D-52056 Aachen
http://www-i2.informatik.rwth-aachen.de/

Prof. Dr. Ir. J.-P. Katoen
M. Neuhäußer

Introduction to Model Checking
Summer term 2007

– Series 3 –

Hand in on April 27 before the exercise class.

Exercise 1 (3 points)

Give an algorithm (in pseudo–code) for invariant checking such that in case the invariant is refuted, a *minimal* counterexample, i.e. a counterexample of minimal length, is provided as error indication.

Exercise 2 (4 + 1 points)

a) Let P be an LT property. Prove that $\mathit{pref}(\mathit{closure}(P)) = \mathit{pref}(P)$.

b) Consider LT–properties P and P' to be equivalent (denoted by $P \simeq P'$) if and only if $\mathit{pref}(P) = \mathit{pref}(P')$. Prove or disprove

$$P \simeq P' \quad \text{if and only if} \quad \mathit{closure}(P) = \mathit{closure}(P').$$

Exercise 3 (3 points)

Let $AP = \{a, b\}$ and let P be the LT property of all infinite words $\sigma = A_0 A_1 A_2 \cdots \in \left(2^{AP}\right)^\omega$ such that there exists $n \geq 0$ with $a \in A_i$ for $0 \leq i < n$, $\{a, b\} = A_n$ and $b \in A_j$ for infinitely many $j \geq 0$. Provide a decomposition $P = P_{safe} \cap P_{live}$ into a safety and into a liveness property.

Exercise 4 (3 + 3 points)

In the lecture it was shown that every LT-property P over a set AP of atomic propositions can be split into a safety property P_{safe} and a liveness property P_{live} such that

$$P = P_{safe} \cap P_{live}.$$

Prove the proposition of Lemma 3.38 which states that the decomposition

$$P = \mathit{closure}(P) \cap \Big(P \cup \Big(\left(2^{AP}\right)^\omega \setminus \mathit{closure}(P)\Big)\Big)$$

is the "sharpest" one for P, i.e. for any decomposition $P = P_{safe} \cap P_{live}$ we have

a) $\mathit{closure}(P) \subseteq P_{safe}$

b) $P_{live} \subseteq P \cup \left(\left(2^{AP}\right)^\omega \setminus \mathit{closure}(P)\right)$