RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL FÜR INFORMATIK 2
RWTH Aachen · D-52056 Aachen · GERMANY
http://www-i2.informatik.rwth-aachen.de/

Prof. Dr. Ir. J.-P. Katoen
F. Gretz & F. Sher

Introduction to Model Checking
Winter term 2011/2012

– Series 3 –

Hand in on November 9th before the exercise class.

Exercise 1 (3 points)

Consider the set AP of atomic propositions defined by $AP = \{ x = 0, x > 1 \}$ and consider a nonterminating sequential computer program P that manipulates the variable x. Formulate the following informally stated properties as LT properties:

(a) false

(b) initially x is equal to zero

(c) initially x differs from zero

(d) initially x is equal to zero, but at some point x exceeds one

(e) x exceeds one only finitely many times

(f) x exceeds one infinitely often

(g) the value of x alternates between zero and two

(h) true

Determine which of the provided LT properties are safety properties. Justify your answers.

Exercise 2 (2 points)

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

Exercise 3 (4 points)

Recall the definition of AP-deterministic transition systems (cf. Series 1, Exercise 1). Let T and T′ be transition systems with the same set of atomic propositions AP. Prove the following relationship between trace inclusion and finite trace inclusion:

(a) For AP-deterministic T and T′:

$$\mathit{Traces}(\mathrm{T}) = \mathit{Traces}(\mathrm{T}') \text{ if and only if } \mathit{Traces}_{\mathit{fin}}(\mathrm{T}) = \mathit{Traces}_{\mathit{fin}}(\mathrm{T}').$$

(b) Give concrete examples of T and T′ where at least one of the transition systems is not AP-deterministic, and

$$\mathit{Traces}(\mathrm{T}) \not\subseteq \mathit{Traces}(\mathrm{T}') \quad \text{and} \quad \mathit{Traces}_{\mathit{fin}}(\mathrm{T}) = \mathit{Traces}_{\mathit{fin}}(\mathrm{T}').$$