Assignment 2: Specification and verification

INTRODUCTION

This second assignment is about specifying correctness criteria for the elevator control unit and verifying your UPPAAL model, that is, proving that the model satisfies the criteria. Correctness criteria will be defined as formulas in temporal logics. The UPPAAL model-checker will be used for verification.

This part consists of three tasks. Each task ends with a description of what you should hand in for that task. Each of the tasks contains several actions. Actions are labelled as follows:

▷ Read this assignment.
Each action is followed by further explanation.

1 Informal properties

We informally describe a set of properties. These can be seen as requirements of the elevator system.

Property 1 *The elevator control unit is deadlock-free.*

Property 2 *The elevator never travels with its door open.*

Property 3 *The amount of requests can reach the threshold value (in the description of Task 1 the value is 5) when the elevator is on the ground floor.*

Property 4 *Each floor (except the ground floor) can be reached, and only by the correct elevator.*

Property 5 *All floor requests are eventually served, i.e., the elevator reaches its destination.*

Property 6 *Whenever a request is served, the passengers will be able to leave the cabin.*

Property 7 *The time needed to serve a request is bounded by the product of the distance in number of floors by the time needed to travel the distance of one floor plus twice the time it takes to open or close the door. More formally the property is defined as follows. Let p be the time to open or close the door. Let t be the time needed to cover the distance between two floors. Let s be the service time. Let d be the distance in number of floors. Then, the property is expressed as:*

$$s \leq d \cdot t + 2 \cdot p$$

2 Tasks for Part II (15 hours)

Task 2.1. Verification (10 hours)

▷ Formalise all the aforementioned informal properties in UPPAALs' TCTL.

▷ Use UPPAAL to check if your model satisfies all the properties.

Note that:

- a good way of handling this task, is to execute these two actions *per* property and in the given order.
- you should – for now – set the number of floors to 3 (including the ground floor) and the number of elevators to 2, reducing the complexity.
- some of these informal properties may be formalised by several TCTL formulas.
- some properties require you to modify the model. It might very well be that some of the properties currently do not hold and your model must be improved. Also, Property 7 requires changes to your model before it can be verified. You may thus use different models for different properties!
- You can use the comment section of UPPAAL's verifier to add explanations where necessary.
- If you are not able to verify all properties, you can still get a "pass". You should, however, at least verify one safety and one liveness property.
- The use of the UPPAAL operators **forall** and **exists** is strongly discouraged (as discussed during the lecture). Instead of quantifying, formulate the property for some interesting values.

For Task 2.1, you should deliver UPPAAL .xml files and their associated .q files. All formalized properties should hold.

Task 2.2. Validation (2 hours)

▷ Validate your model.

You should argue why your model is realistic and why it is a good model. In a *short* report, validate your model by arguing that it is a good model in the sense of Vaandrager (see the reader on YouLearn). Your report should maximally be 1 page.

Task 2.3. Scale your model (3 hours)

Trying to scale is important. Verifying models with 3 floors and 2 elevators will not be sufficient in practice.

▷ Write a short report, answering the following questions:

1. What is the largest configuration – in number of floors and elevators – that you could verify? Answer this question for both one safety and one liveness property.
2. In order to scale to larger systems, what modifications would you suggest? Why are these modifications sound?

▷ Scale your model for Property 1.

Execute the proposed modifications and check whether indeed you can achieve better scalability on Property 1. Add the results (How much faster was your modification? Are there additional modifications possible that you did not try?) to your report. Note that the time scheduled for it is only 3 hours. Do not spend more time on it. If you cannot get your model to scale, leave it and hand it in as it is.

For Task 2.3, you should deliver this report and – if you have made any modifications – UPPAAL .xml files and their associated .q files.