Sokendai lectures 2019–2020
物理情報システムのための形式手法

Timed model checking

Project

Étienne André

Version: May 23, 2019

The answer to this project will be in the form of two documents:

1. a document containing a (short) answer to each question (a screenshot from Uppaal is allowed);
2. an Uppaal source file containing the model and the properties.

The documents must be sent by email (to sokendai(at)lipn13.fr) by **June 16th, 2019**. An acknowledgement will be sent to you (if it is not, please consider resending your email).

Exercise 1: A coal power plant

We consider a coal power plant with the following behavior:

- At first, the plant is in normal mode.
- Suddenly, it may start to heat (action startHeating).
- At that point, a timer is set; after 2 time units, the timer will trigger an alarm (action alarm).
- Then, 5 time units later, a watering system (action watering) starts.
- This watering system lasts for at most 15 time units, after which the plant is cool again (action cool) and goes back to the normal mode.
- However, 20 time units after the plant starts to heat, the plant may explode at any time (action boom)—unless of course it is cool again.

Question 1: Design a TA modeling this system according to the specification.

Question 2: Express in TCTL the following property: "it is possible that the plant explodes".

Question 3: Express in TCTL the following property: "it is impossible that the plant explodes".

Question 4: Express in TCTL the following property: "whatever happens in the future, the plant always eventually explodes".

Question 5: Express in TCTL the following property: "at any time, there is always a possibility that the plant explodes within 12 time units".

Question 6: Using the Uppaal model checker, input the model, and verify the aforementioned properties (if the Uppaal syntax does not allow you to verify a property, explain why).