Prof. Dr. Rüdiger Ehlers TU Clausthal

Model Checking and Games 2019 – Assignment Sheet 5

Due: Monday, 9th September 2019, before the lecture

Please indicate your **name**. You can work in **groups** of up to **three** students. Only one submission per group is necessary. However, in the tutorials every group member must be able to present the solutions to each problem solved by your group.

Please submit your solutions by e-mail to `ruediger.ehlers@tu-clausthal.de` or hand them in in paper form right before the lecture.

Note that you will need 50% of the points on all exercise sheets in order to take the exam. You may be asked to present your solutions in the tutorial, especially if you work in a group. We aim for asking everyone taking part in the course to present at least once during the block course.

Exercise 1: Negation Normal Form (15 pts.)

Translate the following LTL formulas into negation normal form:

- $\neg F(a \vee \mathsf{X}b)$
- $a \vee (b \wedge \neg(\mathsf{X}c \,\mathcal{R}\, \mathsf{X}\neg d))$
- $\neg\mathsf{GF}(x \vee y \,\mathcal{U}\, z)$

Exercise 2: Modelling in Promela (85 pts.)

We want to model an interesting scenario in `Promela` and verify with `Spin` that the model satisfies the specification.

Consider a motor running on battery power, where we want to model the **motor**, the **motor controller**, the **motor speed setting unit**, and the **battery** as individual processes.

- Motor and battery communicate using a shared variable that the motor can set and reset to whether it draws some power. It should draw power if and only if the `target speed value` is > 0.
- The battery has some initial capacity of 50 Wh, and it can non-deterministically decrease this capacity (in steps of 1) by one whenever the motor is drawing power. Once the value reached is 0, then it stays at 0. The battery sets a `depleted` signal whenever this is the case.

- The motor always has a `current speed value`, which is an integer between 0 and 20 (including both 0 and 20). It communicates with the controller using a `target speed value`. Whenever the two speed values differ, the motor can increase or decrease the `current speed value` by one in every step of its execution to get closer to the target speed value, except if the battery is depleted.
- When the battery is depleted, the motor can non-deterministically reduce the current speed value by 1 in each time step.
- The motor speed setting unit can set a `desired speed value` to arbitrary integers between 0 and 20 (including both 0 and 20).
- The motor controller reads the `desired speed value` and writes the `target speed value`. It should, whenever it executes a step, set the target speed value closer to the desired speed value, but the target speed value can only ever be set to the value `current speed value` plus or minus at most 2.

Model the following properties and model check that your model satisfies them using `spin` (or the graphical user interface `iSpin`:

- If the battery charge ever reaches 0, then it stays at 0.
- If the motor has a speed < 10 and the battery charge is 0, then the motor speed never becomes > 10 again.
- **25 bonus points:** If the motor infinitely often executes the step of getting the actual speed closer to the `target speed value` and the motor controller infinitely often executes the step of getting the `target speed value` closer to the `desired speed value` and the `desired speed value` does not change any more at some point, then eventually either (1) the battery will be depleted, or (2) the `desired speed value` will be the same as the `current speed value`.

Use simulation to validate that you built a correct model.