15-414/614 spring 2014 Bug Catching: Final Exam Due by 11:59pm May 4th 2014

15414/614 TA
15414sta@gmail.com

May 2, 2014

1 Temporal Logics (30 points)

1.1 Well-formed LTL and CTL formulae (10 points)

Given the following set of formulae, tell which are syntactic well-formed LTL formulae, and which are syntactic well-formed CTL formulae. Also explain the reason.

- $AX(p\neg \rightarrow q)$
- $p \rightarrow (q \vee r)$
- $EF(p \rightarrow A(qUr))$
- $pU(q \rightarrow r)$
- $FA(p \wedge q)$
- $EX(\neg p) \wedge AFG(p)$

where p, q, and r are propositional atoms.

1.2 LTL vs. CTL (20 points)

Let ϕ_{CTL} is a well-formed CTL formula, ϕ_{LTL} is the corresponding LTL formula obtained by eliminating all the path quantifiers in ϕ_{CTL}.

We say that the LTL formula ϕ_{LTL} and the CTL formula ϕ_{CTL} (both over the same AP) are equivalent, denoted as $\phi_{LTL} \equiv \phi_{CTL}$, if and only if for **any**

transition system M (over AP), we have that, $(M, s_0 \models_M \phi_{LTL}) \Leftrightarrow (M, s_0 \models_M \phi_{CTL})$, where s_0 is the initial state of the transition system.

For instance, given $\phi_{CTL} = AGp$, we have the corresponding LTL formula ϕ_{LTL} as Gp. They are equivalent to each other. However, this equivalence does not hold for all CTL and LTL formulae.

Now, considering the following CTL formulae, for each of them, if you think that it is equivalent to its corresponding LTL formula, explain the reason. If you believe that they are not equivalent, give at least one transition system which can satisfy only one of them.

- $EX(AG(p))$
- $AFAX(p \rightarrow q)$
- $AG(p \vee q) \wedge AGr$
- $AFAG(E(pUq))$

where p, q, and r are propositional atoms.

2 Nuclear Reactor (70 points)

You are to use **SPIN** to model and verify a nuclear reactor controller.

2.1 How a Nuclear Reactor Works

Figure 1 describes how a simplified nuclear power plant works[1].

Inside the nuclear reactor, we have fuel rods which contains nuclear materials such as uranium-235 or plutonium-239. The reactor is filled with water, which is heated by the thermal energy released from nuclear fission. The reactor is under extremely high pressure so that the boiling point of the water inside is above 100°C (212°F).

The nuclear chain reaction is controlled by "control rods" which are made of a neutron and used to absorb neutrons. Absorbing more neutrons in a control rod means that there are fewer neutrons available to cause fission. Pushing the control rods deeper into the reactor reduces its power output and extracting the control rod increases it.

The water heated in the reactor circulates to the steam generator. Then the generated steam moves the turbines in the generator to produce electricity.

[1] `http://www.flatworldknowledge.com/pub/introductory-chemistry/412765`

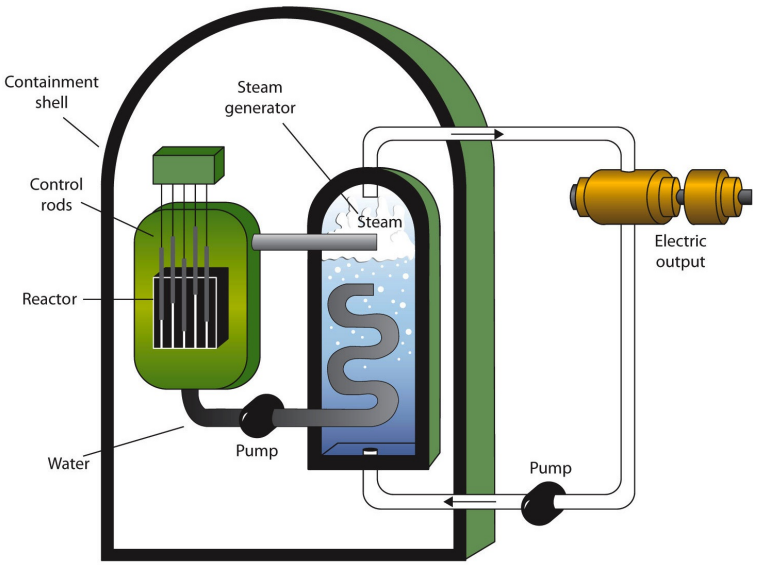

Figure 1: Nuclear Power Plant

2.2 Controller

2.2.1 Temperature

In this model, the temperature of nuclear reactor is controlled by the levels of three control rods. Each level of a control rod contributes to the temperature change (ΔT) as follows.

$$\Delta T = l_1 + l_2 + l_3 + C_{\text{NonDet}}$$
$$C_{\text{NonDet}} : \{-2, -1, 0, 1, 2\}$$
$$\text{where } l_i \text{ is level of rod } i \ (-2 \leq l_i \leq 2)$$

The non-deterministic error term C_{NonDet} is an integer value ranging between -2 to 2.

For example, in figure 2, we have the control rod 1 at level 0, the control rod 2 at level -1, and the control rod 3 at level -2. Therefore, the temperature change ΔT is

$$0 + -1 + -2 + C_{\text{NonDet}}$$
$$= -3 + C_{\text{NonDet}}.$$

If the current temperature is 255°C, then next temperature will be 252°C + C_{NonDet}, which could be a value between 250°C and 254°C.

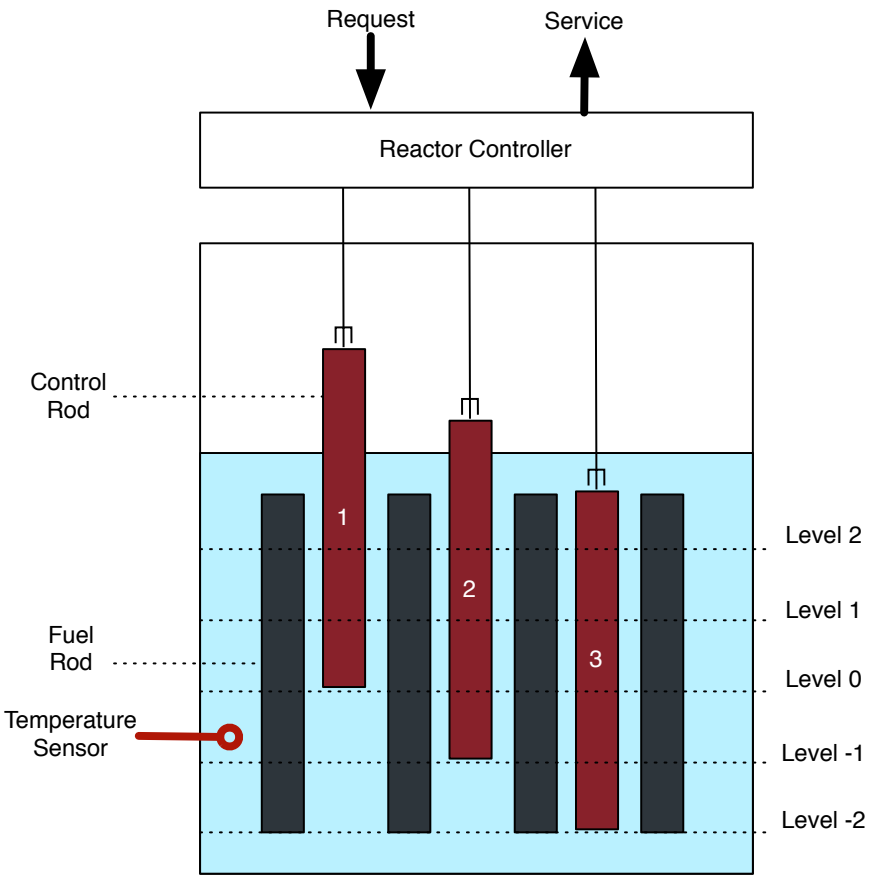

Figure 2: Reactor temperature is controlled by the levels of control rods.

For safety reasons, the reactor temperature must be maintained between 246°C and 284°C at all times.

2.3 Request

The nuclear power plant is connected with an electricity company which requests the plant to generate a certain amount of power. The power requests R are a multiple of 500 MW between 500MW and 2000MW:

$$R : \{500\ \text{MW}, 1000\ \text{MW}, 1500\ \text{MW}, 2000\ \text{MW}\}.$$

The production of power by the plant is dependent on the temperature

of the reactor (Figure 3).

Production (MW)	Temperature (°C)
2000	280
1500	270
1000	260
500	250

Figure 3: Power Production and Temperature

The company makes a request to the plant and waits until the request is served before it makes a new request.

2.4 Service

A power request is serviced if the current power production is greater or equal than the requested power for three time units. Otherwise, the controller must raise the reactor temperature to increase power generation. For example, consider the case where the current reactor temperature is 270°C and the plant generates 1500 MW, and the company requests 2000 MW. In this case, the plant has to increase the reactor temperature to at least 280°C to meet the request.

2.5 Model Requirement

Your model should satisfy these conditions:

2.5.1 Plant Policy

1. The reactor temperature should be maintained between 246°C and 284°C.
2. All requests are eventually satisfied.

2.5.2 Government Policy

1. If the requested power is smaller than current power production, the plant must lower the reactor temperature to save the nuclear fuel.
2. The plant must increase/decrease the reactor temperature as quickly as possible if the gap between the current temperature and the target temperature is greater than 10°C.

3. The department of energy orders "shutdown" to the plant if its monitoring system detects when the density of radiation around the plant exceeds the given threshold. The plant should take the following actions for the shutdown.

   (a) After getting the shutdown signal, the reactor should switch to the cool-down mode immediately.
   (b) The reactor temperature should be lowered to 250°C at the end of this cooling process.
   (c) During this cooling process, no request is serviced regardless of the current power production.

   Once the plant is cooled down, the DoE takes control of the plant and runs it until the plant serves three requests. The DoE will not signal another shutdown during this period. After this period, the plant regains its control over the plant.

   (a) Once the reactor reaches 250°C, it should switch to the DoE mode immediately.
   (b) Once the reactor enters to the DoE mode, it always serves exactly three requests and then switches to the normal operation mode .

For each specification, describe its meaning in English, and provide temporal logic formalization. Ensure that properties are not satisfied vacuously.

2.6 Submission

You are required to use the SPIN model checker to implement both the model and properties. You have to submit the following items for each part.

- Implementation (Model + Specification)
- Report : It should include
  - Assumptions made about the environment
  - Modeling decisions
  - Additional properties you have provided
  - Verification time for the properties

Please email your files together with your solution to problem 1 to:
`15414sta@gmail.com`