

CS745/ECE725 Fall 2013

Homework 4 (CTL Model Checking)

In this assignment, you will verify the correctness of a simple fault-tolerant distributed *token ring* protocol due to Beauquier et al. The problem specification is as follows:

N processes are organized in a ring and the token is circulated along the ring in a fixed direction. Each process, say p , maintains a variable x_p with domain $\{0 \cdots m_N - 1\}$, where m_N is the smallest integer not dividing N . A process p has the token if

$$x_p \neq (x_{pred_p} + 1) \mod m_N$$

where $pred_p$ denotes the predecessor process of p . A process that has the token can pass the token by executing the following statement:

$$x_p := (x_{pred_p} + 1) \mod m_N$$

Faults can perturb the state of this system from any state to any state (equivalently, the initial state of the protocol can be any arbitrary state in its state space).

You are to model this protocol in the model checker SMV and report the correctness of the following CTL properties:

$$\phi_1 = \mathbf{A} \Diamond Q$$

$$\phi_2 = \mathbf{E} \Diamond Q$$

where Q is the set of states in which at most one process holds the token.

Deliverable. You are expected to submit SMV source file through email by **11:59am on Friday, November 22**, for at least 4 processes. Write in comments which of the above properties hold.