

ECE725/CS745 Winter 2011

Homework 3 (LTL Model Checking)

In this assignment, you will verify the correctness of a simple *token ring* protocol. The problem specification is as follows:

In a token ring protocol for solving distributed mutual exclusion, processes $0 \dots N$ are organized in a ring and the token is circulated along the ring in a fixed direction. Each process, say p where $p \in \{0 \dots N\}$, maintains a variable x_p with domain $\{0, 1, \perp\}$, where $\perp$ denotes a corrupted value. Process p , $0 \leq p \leq N - 1$, has the token and can enter the critical section if and only if x_p differs from its successor x_{p+1} and process N has the token if and only if x_N is the same as its successor x_0 . A process receives the token from its predecessor process, if the predecessor owns the token and x of the predecessor is not $\perp$. Faults can corrupt the value of x of a process, if there exist at least two processes with uncorrupted values.

You are to model this protocol in Promela and verify the correctness of the following property:

$$\Box \Diamond Q,$$

where Q is a predicate that satisfies the following regular expression on the value of all x variables $0^l 1^{(N+1-l)} \cup 1^l 0^{(N+1-l)}$.

Extra credit. Increase the number of processes up to the point that Spin is unable to perform a complete exhaustive search and report this number.

Deliverable. You are expected to submit .pml file through email by **8:30am on Thursday February 17.**