Temporal Logic of Actions

Garlan Homework 14 Due: 1 December 1997

Problem 1.

Revise the message passing example from class to provide a fixed size (circular) buffer; after putting messages in each slot of the buffer, wrap around and insert new messages into the front of the buffer. You should assume that this message passing environment is going to be used long enough for integer overflow to occur – i.e.,

$$\Box(\Box\Diamond nummessages' = nummessages + 1 \Rightarrow \Diamond nummessages' = 0)$$

Don't go overboard – this doesn't need to be fault tolerant or compileable, just correct enough to get the ideas and algorithm correct so that you can use it in problems 2 and 3.

Problem 2.

Modify the TLA specification of the program to reflect your changes. In other words, define $Init_\Pi$, $\mathcal{N}_\Pi$, and L_Π and define Π with respect to these.

Problem 3.

Write the following claims in TLA and outline their proofs. If invariants are needed in order to perform the proof, write the invariants both in English and in TLA. Do **not** do a complete formal proof of the properties.

1. The receiver won't outrun the sender.
2. Messages will be processed in the order sent
3. We will process every message