Verification Techniques 2010, Homework 3

The homework til **Tuesd, Feb. 16** is to hand in solutions to the following exercises.

1.

Since. Consider the new binary temporal operator S , pronounced "since". Intuitively, since is the "backwards" analogue of (strong) until. That is, $\phi_1 \mathcal{S} \phi_2$ means that the last occurrence of ϕ_2 was followed by a period of ϕ_1 up to the present from the state after that where ϕ_2 held. The formal semantics can be described as

- $(\sigma, i) \models \phi_1 \mathcal{S} \phi_2$ iff $\exists j \leq i \ : \ (\sigma, j) \models \phi_2$ and $\forall k : j < k \leq i \ (\sigma, k) \models \phi_1$

Your problem is the following:

a) Express $\Box\,(p \implies p \,\mathcal{S}\, q)$ as a formula containing p, q, and the other temporal operators that we have used ($\circ$, $\Box$, $\Diamond$, $\mathcal{U}$, $\mathcal{W}$).

b) Draw a Büchi automaton that accepts the language that satisfies $\Box\,(p \implies p \,\mathcal{S}\, q)$.

c) Make a `never`-claim in PROMELA that will check whether a program satisfies $\Box\,(p \implies p \,\mathcal{S}\, q)$.

2.

This problem is based on a published note (enclosed), which describes several corrections to an implementation of counting semaphores. A counting semaphore should roughly synchronize accesses in a way that one wants in producer-consumer type problems: at any point there should have been at most as many completed P operations as V operations.

The algorithms describe implementations of counting semaphores by means of binary semaphores. As a clarification: I believe that the change by Hemmendinger, which is define on pabe 6, line 7 from bottom just moves the four letters `else` after the `end` in the P operation, to the line before the `VB(s.mutex)` operation.

The problem is to model three algorithms in Promela:

- the one in Figure 1,
- The modification by Hemmendinger explained on page 6,
- the one in Figure 3. (i.e., you can ignore Figure 2).

You should add checks and make suitable configurations, so make SPIN discover the problem for each of them. You should also suggest and make SPIN check a correction of the Algorithm in Figure 3.

On purpose, I have cut out the explanation (on page 9) of the problem with Figure 3. and the suggested correction.

Please make readable Promela models, and make suitable configuration(s) (concerning, e.g., number of processes) in the analysis runs.