Tutorial – Chapter 7

1) Use the LTSA to obtain an action trace that violates the following safety property:

> **property** PS = (a -> (b-> PS | a -> PS) | b -> a -> PS).

Can you think of a different trace that also violates the property?

2) A lift has a maximum capacity of ten people. In the model of the lift control system, passengers entering the lift are signalled by an *enter* action and passengers leaving the lift are signalled by an *exit* action. Specify a safety property in FSP which, when composed with the lift, will check that the system never allows the lift that it controls to have more than ten occupants.

3) For the following FSP model of the car park problem of Chapter 5:

```
CARPARKCONTROL(N=4) = SPACES[N],
SPACES[i:0..N]= ( when(i>0) arrive->SPACES[i-1]
                 | when(i<N) depart->SPACES[i+1]
                 ).

ARRIVALS   = (arrive->ARRIVALS).
DEPARTURES = (depart->DEPARTURES).

||CARPARK = (ARRIVALS||CARPARKCONTROL(4)||DEPARTURES).
```

i) specify and check a safety property OVERFLOW(N=4) which asserts that the car park does not overflow. Now check the carpark against property OVERFLOW(3). What happens in this case?

ii) specify a progress property, which asserts that cars eventually enter the car park. Which situation is reflected if we make car departure lower priority than car arrival? Do we get starvation as a result?