

## Temporal Specification – Exercises

[ Questions from previous exams ]

1. This question concerns the relationship between temporal logic and programs.

a)  $\text{if } (x > 2) \text{ then } x := 1 \text{ else } x := x + 2; \text{ end}$

$(x > 2) \Rightarrow O(x := 1 \wedge \text{other}) /$

$(x \leq 2) \Rightarrow \exists w. w = x / O(x = w + 2 \wedge \text{other})$

b)  $\square x \leq 5 \wedge \Diamond x < 5$  it's a liveness property.  
it's a safety property.

Des: Comms is a formula which captures the information transferred between different components.

c) Des: Comms is a temporal formula which describes the propagation changes for communicating between components.

$\text{Spec}_A = \square [\text{start} / O p]$

$\text{Spec}_B = \square [\text{start} / O O q]$

Comms:  $\square [P1 / O P2] / \square [P2 / O P1] / \square [P1 / O P2]$

is. Give examples of three possible types of formulae that might be used as Comms and explain what constraints these three represent.

2.

a)  $p \rightarrow q \rightarrow p \rightarrow q \rightarrow p$   
send msg      receive

the  $[M, i] \models \text{send\_msg}$   
while  $i = 2n+1$  ( $n > 1$ )

b)  $\square [ \dots ]$  is Comms

c)  $\square [\text{send\_msg} \Rightarrow \Diamond \text{recv\_msg}]$

2. Below is a temporal specification for a simple message-passing system consisting of two components, A and B.

$$\text{Spec}_A: \square \left[ \begin{array}{l} \text{true} \Rightarrow \neg(p \wedge q) \\ \text{start} \Rightarrow p \\ \wedge p \Rightarrow \bigcirc q \\ \wedge q \Rightarrow \bigcirc p \\ \wedge q \Rightarrow \bigcirc \text{send\_msg} \end{array} \right] \quad \text{Spec}_B: \square \left[ \begin{array}{l} \text{recv\_msg} \Rightarrow \bigcirc g \\ \wedge f \Rightarrow \bigcirc g \\ \wedge g \Rightarrow \bigcirc f \end{array} \right]$$

- (a) What is the behaviour of  $\text{Spec}_A$ , i.e. how often is  $\text{send\_msg}$  made true?

(b) In

$$\text{Spec}_A \wedge \text{Spec}_B \wedge \square[\text{send\_msg} \Rightarrow \text{recv\_msg}]$$

Specifying comm function types.  
what is the last formula meant to specify?

- (c) If we wish to specify that a message send will be followed, at some time in the future, by a message receipt, what formula should we modify in the above specification and what should it be changed to?