Program Correctness
Exercises 1

A. Silva M. Bonsangue

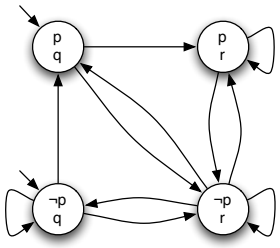
14th February 2008

Exercise 1 $\star$

Express each of the following properties (stated in English) as an LTL formula. Assume p, q, r are atomic propositions.

1. If p occurs, q never occurs in the future.
2. Always if p occurs, then eventually q occurs followed immediately by r.
3. Any occurrence of p is followed eventually by an occurence of q. Furthermore, r never occurs between p and q.

Exercise 2 $\star$



1. Do the properties $\mathbf{G}\ (p \rightarrow\ \mathbf{F}\ r)$ and $\neg(p\ \mathbf{U}\ \neg r)$ hold for all initial states of this model?
2. If not, present a path that invalidates the formula.

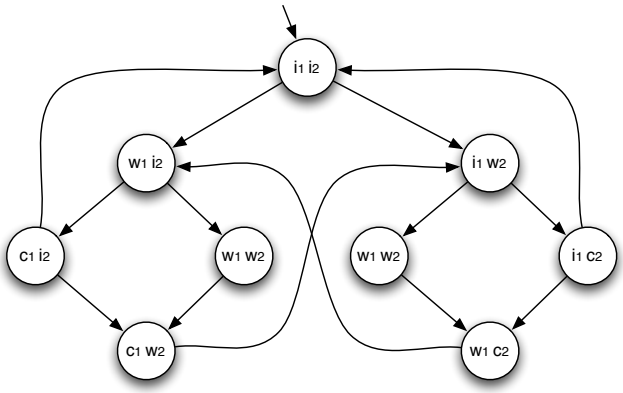
Exercise 3 $\star$

Establish the following equalities in LTL

1. $\mathbf{G}\ \phi \equiv \mathit{false}\ \mathbf{R}\ \phi$
2. $\mathbf{F}\ \phi \equiv \phi \vee\ \mathbf{X}\ \ \mathbf{F}\ \phi$
3. $\phi\ \mathbf{U}\ \psi \equiv \psi \vee (\phi \wedge\ \mathbf{X}\ (\phi\ \mathbf{U}\ \psi))$

4. $\phi \mathbf{R} \psi \equiv \neg(\neg\phi \mathbf{U} \neg\psi)$

Exercise 4 $\star$



1. Show that this model satisfies the properties of safety (mutual exclusion), liveness and non-blocking. The atomic propositions i_k, w_k and c_k represent respectively *process k is idle*, *process k is waiting* and *process k is accessing critical section*.

Exercise 5

Express the following in LTL:

Along any path, a state satisfying p occurs at most once.

Exercise 6

Consider a resource allocation protocol where n processes $P_1, P_2, \ldots P_n$ are contending for exclusive access of a shared resource. Access to this shared resource is controlled by an arbiter process. The atomic proposition req_i is true only when P_i explicitly send an access request to the arbiter. The atomic proposition gnt_i is true only when the arbiter grants access to P_j. Now suppose that the following LTL formula holds for our resource allocation protocol.

$$G(req_i \Rightarrow Fgnt_i)$$

1. Explain what this property means. Is this a desirable property?

2. Suppose that the resource allocation protocol has a distributed implementation so that each process is implemented in a different site. Does the LTL property affect the communication overheads among the processes in any way?