

# Program Correctness

## Exercises 1

A. Silva      M. Bonsangue

February 16, 2009

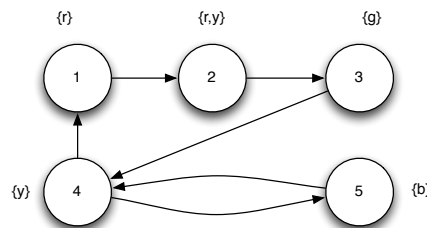
### Exercise 1 ★

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 occurrence of  $q$ . Furthermore,  $r$  never occurs between  $p$  and  $q$ .

### Exercise 2 ★

Consider the following transition system.

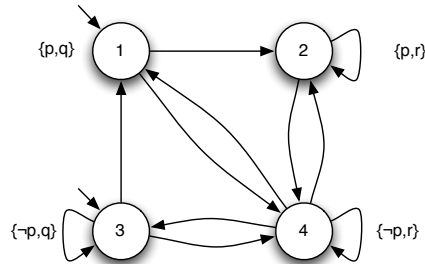


The following atomic propositions are used:  $r$ (red),  $y$ (yellow),  $g$ (green) and  $b$ (black). Indicate for each of the following LTL-formulae the set of states for which these formulae are valid.

1.  $\mathbf{XX}b$
2.  $r \mathbf{U} g$
3.  $\mathbf{GF}y$
4.  $\mathbf{F}g$

5.  $\neg r \mathbf{U} g$
6.  $r \mathbf{U} y$
7.  $\mathbf{F} \neg b$
8.  $r \Rightarrow \mathbf{X} \neg g$
9.  $(g \vee y) \Rightarrow \mathbf{F} r$
10.  $\mathbf{GF}r \Rightarrow \mathbf{F} g$

**Exercise 3** ★



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 4** ★

Consider an elevator system that services  $n$  floors numbered 0 through  $n - 1$ . There is an elevator door at each floor with a call-button and an indicator light that signals whether or not the elevator has been called for. In the elevator cabin there are  $n$  request-buttons (one per floor) and  $n$  indicator lights that inform which floor(s) are requested to be visited. For simplicity, consider  $n = 3$ . Suppose we have the following atomic propositions at our disposal (where  $i \in \{0 \dots n - 1\}$ ):

- $at(i)$ : the elevator cabin is at floor  $i$
- $open(i)$ : the elevator door at floor  $i$  is open
- $request(i)$ : there is a request for floor  $i$

Consequently, there are  $3 \times n = 9$  atomic propositions. Using these atomic propositions, specify in LTL the following properties:

1. The doors are safe, i.e., an elevator door is never open if the elevator cabin is not present at the given floor.

2. A request at a certain floor will eventually be served.
3. Again and again the elevator will return to floor 0.
4. When the top floor is requested for, the elevator will serve it immediately and will not stop on the way there.
5. The elevator cabin is motionless unless there is some request.

It is not permitted to define and use additional atomic propositions.

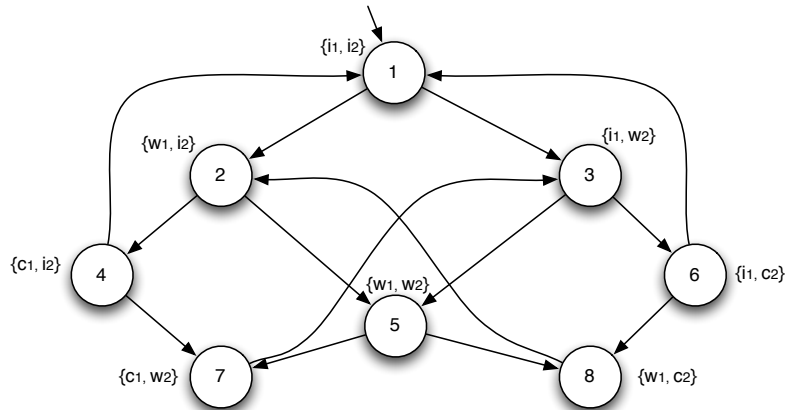
**Exercise 5** ★

Establish the following equalities in LTL

1.  $\mathbf{G} \phi \equiv \text{false} \mathbf{R} \phi$
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 6** ★

Consider the following transition system.



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 7**

Express the following in LTL:

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

### Exercise 8

Consider a resource allocation protocol where  $n$  processes  $P_1, P_2, \dots, P_n$  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  $P_i$ . 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?