McMaster University
Department of Computing and Software
Dr. W. Kahl

CAS 701
Fall 2007
Exercise Sheet 3

CAS 701 — Logic and Discrete Mathematics in Software Engineering

26 November 2007

1 LTL Formalisations

Formalise in LTL using **F**, **G**, **X**, and **U** the following derived temporal operators:

(a) **S** q: "q stops", i.e., q holds now, but not in the next step.

(b) p **B** q: before q holds, p holds at least once.

(c) p **A** q: every time q stops to hold, p holds at least once before q holds again.

2 LTL Formalisations

Formalise the following statements as well as possible in LTL, introducing appropriate atomic propositions:

(a) While process 1 keeps file F open for reading, process 2 cannot open it for writing.

(b) When process 2 becomes ready to open file F for writing, it will eventually be able to open it.

(c) When process 2 becomes ready to open file F for writing, process 1 will close F if it is keeping F open for reading.

(d) File F is normally closed.

3 The Alternating Bit Protocol

On the course page, you find the file abp.smv from [Huth, Ryan] (pp. 203–207).

(a) How many bits does a state have? How many states are therefore in the state set?

(b) Draw the state transition graph of the states reachable from the initial state in abp.smv, while abstracting from the contents of the message.

Hint: Only a fraction of the states is reachable, and this is further reduced by the abstraction!

(c) What is, in general, the difference between one fairness condition $\phi_1 \wedge \phi_2$, and two fairness conditions ϕ_1 and ϕ_2?

Write an SMV program with a fairness condition $\phi_1 \wedge \phi_2$ that is not equivalent to the two fairness conditions ϕ_1 and ϕ_2.

Hint: Solvable in four lines.

4 Elevator Control

An elevator is to be built for a building with n floors. The following requirements for the elevator control have already been collected:

- The elevator can reach each of the floors $1 \ldots n$. In each floor, there is a door through which people can enter or exit the elevator. This door is not open unless the elevator is at its floor.
- The elevator also carries a door, which is not open unless the elevator is at some floor.
- Inside the elevator there is one button for each floor, and each of these buttons has a control lamp which goes on when the button is pressed, and stays on until the repectiv floor is reached. Pressing of a button also notifies the elevator control of the desired floor.
- Inside the elevator is a direction display indication in which direction (up or down) the elevator will move.
- On each floor, there are two request buttons, one for going up, and one for going down. Each of these has a control lamp that lights up when pressed, and remains on until the elevator reaches its floor and will next move into the respective direction. The lowest floor has no "down" button, and the highest floor has no "up" button.
- The elevator door is either open or closed.

Error states, for example that the door cannot be opened or closed, or that the elevator gets stuck while moving, or power outages need not be considered.

(a) Write down further requirements for the elevator control. Consider in particular fairness and liveness conditions.

(b) Produce a formal specification using temporal logic.

Hint: Use appropriate atoms, e.g. $elevatorAtLevel(i)$ describes that the elevator is at the i-th floor, for $1 \leq i \leq n$.

(c) Implement an appropriate model in the SMV modelling language, and verify your specifications using NuSMV.