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

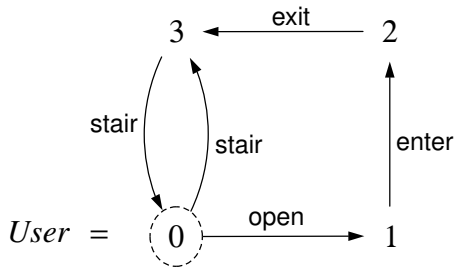
SFWR ENG 3BB4
Exercise Sheet 3

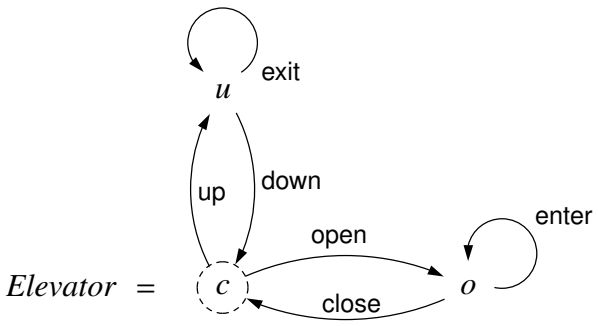
SFWR ENG 3BB4 — Software Design III — Concurrent System Design

27 February 2007

Exercise 3.1: Labelled Transition Systems — Elevator (extended from Midterm 2, 2004)

Let the following two labelled transition systems be given:





(a) Draw the reachable part of the composed LTS *Elevator* $\|$ *User*.

(b) In the system *Elevator* $\|$ *User*, what "goes wrong" relative to common sense?
Clearly define the property you find **violated** as a property of traces. Is this a **safety property** or a **liveness property**? **Justify!**

(c) For each of the following questions, if the answer is yes, supply a trace; if no, explain. Does the statement reflect a **safety property** or a **liveness property**? Reformulate the property involved as a statement about traces.

- Is it possible that after an enter event happend in the system *Elevator* $\|$ *User*, no exit will happen anymore?
- Is it possible that after an enter event happend in the system *Elevator* $\|$ *User* an up or a down event happens before the next close event?

Exercise 3.2: Modelling Car Keys (Adapted from Midterm 1, 2002)

You are to model certain aspects of locking a car that, for the sake of simplicity, is assumed to have only **one** door and **one** key, and **no** other parts (e.g. windows or roofs) that might be open or opened.

It is possible to lock and unlock the **door** no matter whether it is open or closed, but the door can only be opened while it is unlocked.

The **key** can be inserted into the ignition and removed from it, and while the key is *not* in the ignition, it can lock and unlock the door.

The **driver** can use the door to get into and out of the car. If the driver is outside the car and the door is closed, then the driver can use the key to lock and unlock the door; otherwise it is only possible to use a button to lock and unlock the door. If the driver is inside the car and the door is closed, then the driver can insert the key into the ignition and remove it.

(a) Draw an LTS for the behaviour of the **door**, starting in a closed and locked state.

(b) Draw an LTS for the behaviour of the **key**, starting outside the ignition.

(c) Draw an LTS for the behaviour of the **driver**, starting outside the closed car.

(d) Use parallel composition (and other operators as appropriate) to assemble the three components together into a single LTS process *CARKEY*.

(e) We call a state *desperate* if the driver is outside the vehicle, the door is closed and locked, and the key inside the ignition. Is it possible that the process *CARKEY* reaches a desperate state? If yes, exhibit a trace; if no, explain.

(f) Are desparate states deadlock states? Explain!

(g) Is the absence of desparate states a safety condition or a liveness condition? Explain!

(h) *Infinitely many uses* of the car are documented by traces in which both unlocking by key and insertion of the key into the ignition have infinitely many occurrences.

Are infinitely many uses of the car still possible if the locking button breaks? Explain in terms of traces! What kind of property is this?