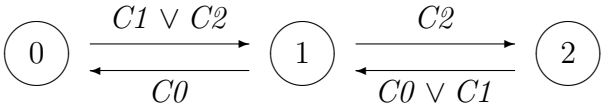
COMPUTER SCIENCE TRIPOS Part II – 2018 – Paper 7

7 Hoare Logic and Model Checking (AM)

(a) Give a formal definition of a Kripke structure, as a 3- or 4-tuple, briefly explaining the roles of its components. What might a Kripke structure model? [4 marks]

(b) A lift controller manages a lift moving between floors 0, 1 and 2. There are three 'call' input buttons (*C0*, *C1*, *C2*) within the lift requesting the lift to move to the corresponding floor. These are duplicated at each floor to avoid the need for a separate 'call' button. They are internally latched as usual—a call button-press stays active until reaching the associated floor, but can be immediately reactivated (e.g. useful when one realises the lift is setting off in the wrong direction!). The controller is (rather informally) specified by a hardware-style state transition diagram with three inputs and three states as in the diagram:



Give a Kripke-structure model for the controller, explaining any necessary changes or clarifications you make. You need not model the internal structure of the call buttons, it suffices to treat them as (a) non-deterministically becoming active and (b) deactivated on arrival at the corresponding floor. [*Hint:* Two possible answers have 12 and 24 states in the Kripke structure.] [6 marks]

(c) Give formulae (in a temporal logic of your choice, but which you should name) corresponding to

(i) If I press button *C0* the lift will eventually arrive at floor 0

(ii) If I press button *C1* the lift will eventually arrive at floor 1

(iii) If I press button *C2* the lift will eventually arrive at floor 2

[*Hint:* You might wish to check your Kripke model above defines any predicates you use in your answers.] [4 marks]

(d) Which of your formulae in Part (c) are valid in your Kripke model? [2 marks]

(e) Improve the state transition diagram in Part (b) to fix any problems you discover in Part (d). It is not necessary to give a Kripke model. [4 marks]