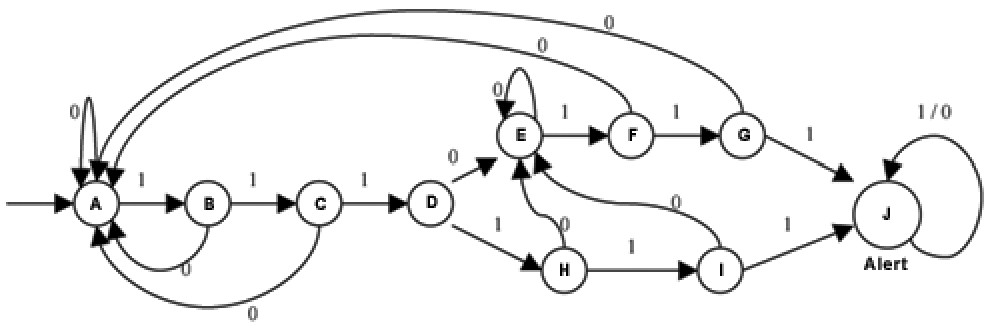
CSEP590 - Model Checking and Software Verification
Summer 2003
Solution Set 2

1. Automata

a) Design automaton M, give a graphical schematic and a formal definition
Solution:

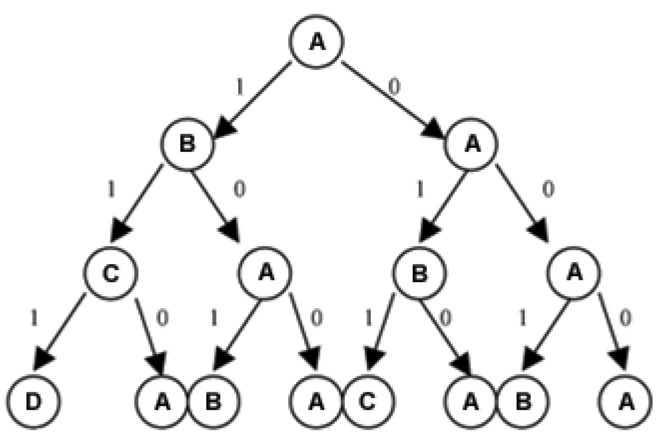
Graphical Schematic:



Formal Definition:
Let $M = (Q, E, T, q_0, l)$, where

$Q = \{A, B, C, D, E, F, G, H, I, J\}$
$E = \{1, 0\}$
$T = \{(A1B), (A0A), (B1C), (B0A), (C1D), (C0A), (D1H), (D0E), (E1F),$
$(E0E), (F1G), (F0A), (G1J), (G0A), (H1I), (H0E), (I1J), (I0E)\}$
$q_0 = \{A\}$
$l = \{J \mid \rightarrow \text{“Alert”}\}$

b) First 4 levels of complete execution tree
Solution:



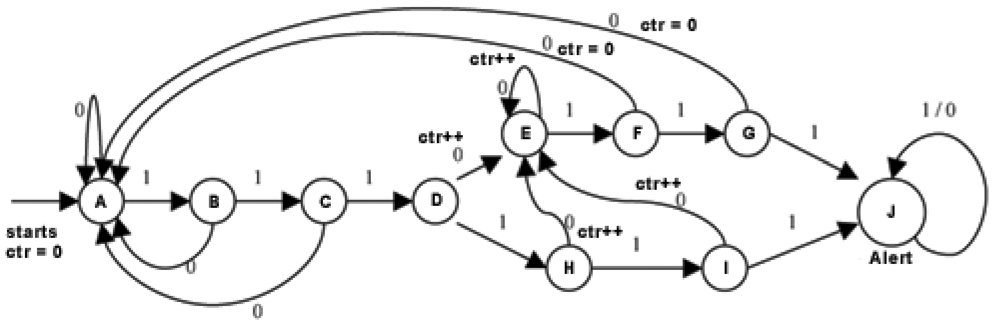
An infinite execution tree

c) One possible length-12 partial execution of M
Solution:
(A1B),(B1C),(C1D),(D1H),(H1I),(I0E),(E0E),(E0E),(E0E),(E1F),(F1G),(G0A),(A0A)

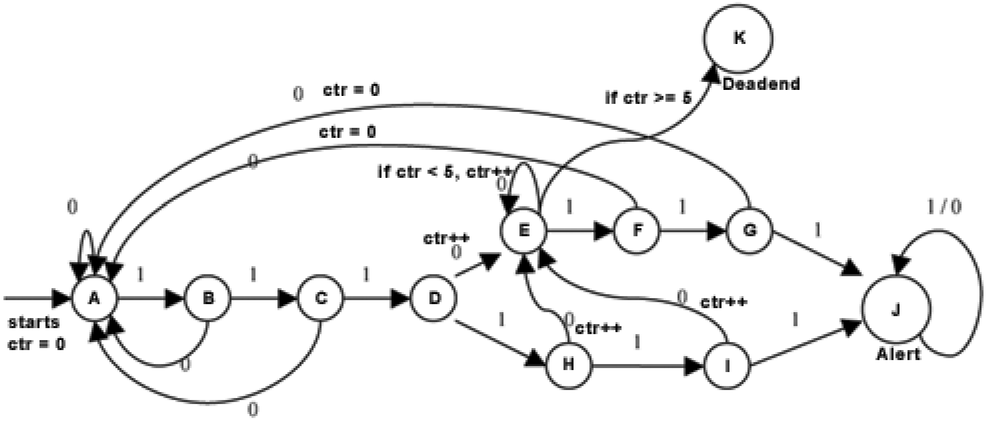
d) Adding variable “ctr”
Solution:

The transitions that should update/change the value of counter are:

Starting at state A, ctr = 0
The following transitions increment ctr: {(D0E), (E0E), (H0E), (I0E)}
The following transitions reset ctr: {(F0A), (G0A)}



e) Adding guards and a deadend state
Solution:



f) Count unfolded states
Solution:
Do not unfold states A, B, C, D, H, I (6 states)
4 unfolded states (ctr = 1, ctr = 2, ctr = 3, ctr = 4) for E, F, G (12 states)
5 unfolded states (ctr = 0, ctr = 1, ctr = 2, ctr = 3, ctr = 4) for J (5 states)
No unfolded state for K (since we always have ctr > 4) (1 state)
Total = 6 + 12 + 5 + 1 = 24 states

2. Modeling a digital circuit as a Kripke structure
a) Update equations using only NAND
Solution:
$b_1' = ([(b_1 \mid b_1) \mid (b_3 \mid b_3)] \mid b_2) \mid ([(b_1 \mid b_1) \mid (b_3 \mid b_3)] \mid b_2)$
$b_2' = ((b_2 \mid b_2) \mid b_3) \mid ((b_2 \mid b_2) \mid b_3)$
$b_3' = (b_1 \mid [b_2 \mid (b_3 \mid b_3)]) \mid (b_1 \mid [b_2 \mid (b_3 \mid b_3)])$

b) System variables, domain of variables, initial states, and transitions
Solution:
System variables $V = \{b_1, b_2, b_3)$
Domain $D = \{0, 1\}$
Initial States $S_0(V) = (b_1 = 1 \wedge b_2 = 1 \wedge b_3 = 0) \vee (b_1 = 0 \wedge b_2 = 1 \wedge b_3 = 0)$
Transitions $R(V,V') = [b_1' = ([(b_1 \mid b_1) \mid (b_3 \mid b_3)] \mid b_2) \mid ([(b_1 \mid b_1) \mid (b_3 \mid b_3)] \mid b_2)]$
$\wedge [b_2' = ((b_2 \mid b_2) \mid b_3) \mid ((b_2 \mid b_2) \mid b_3)]$
$\wedge [b_3' = (b_1 \mid [b_2 \mid (b_3 \mid b_3)]) \mid (b_1 \mid [b_2 \mid (b_3 \mid b_3)])]$

c) Define Kripke structure $K = (S, S_0, R, L)$
Solution:
$S = D \times D \times D$
$S_0 = \{(1,1,0), (0,1,0)\}$
$R = \{((1,1,0),(1,0,0)), ((1,0,0),(0,0,1)), ((0,0,1),(0,1,0)), ((0,1,0),(0,0,0))$
$((0,0,0),(0,0,0)), ((0,1,1),(1,0,0)), ((1,0,1)(0,1,1)), ((1,1,1),(1,0,1))\}$
$L((0,0,0)) = \{b_1 = 0, b_2 = 0, b_3 = 0\}$,
$L((0,0,1)) = \{b_1 = 0, b_2 = 0, b_3 = 1\}$,
$L((0,1,0)) = \{b_1 = 0, b_2 = 1, b_3 = 0\}$,
…
$L((1,1,1)) = \{b_1 = 1, b_2 = 1, b_3 = 1\}$

3. Modeling an elevator as a Kripke structure
Solution:
The idea is to have three variables, one for the floor number (1,…,5), one for the up button (0 or 1), and one for the down button (0 or 1).
The transitions are then determined by the state of the buttons and the floor.
The label function asserts the proposition "The bell rings" in the state where the elevator is on floor 1.

The Kripke structure is then:

$K = (S, S_0, R, L)$
$S = \{1,2,3,4,5\} \times \{0,1\} \times \{0,1\}$
$S_0(f,u,d) = f = 0 \wedge u = 0 \wedge d = 1$
$R = \{ ((1,1,0),(1,0,0)), ((1,0,1),(2,0,0)), ((1,0,0),(1,0,0)), ((1,1,1),(1,0,0)),$
$((2,1,0),(1,0,0)), ((2,0,1),(3,0,0)), ((2,0,0),(2,0,0)), ((2,1,1),(2,0,0)),$

$((3,1,0),(2,0,0))$, $((3,0,1),(4,0,0))$, $((3,0,0),(3,0,0))$, $((3,1,1),(3,0,0))$,
$((4,1,0),(3,0,0))$, $((4,0,1),(5,0,0))$, $((4,0,0),(4,0,0))$, $((4,1,1),(4,0,0))$,
$((5,1,0),(4,0,0))$, $((5,0,1),(5,0,0))$, $((5,0,0),(5,0,0))$, $((5,1,1),(5,0,0))$ }

$L(1,0,0)$ = *"The bell rings"*