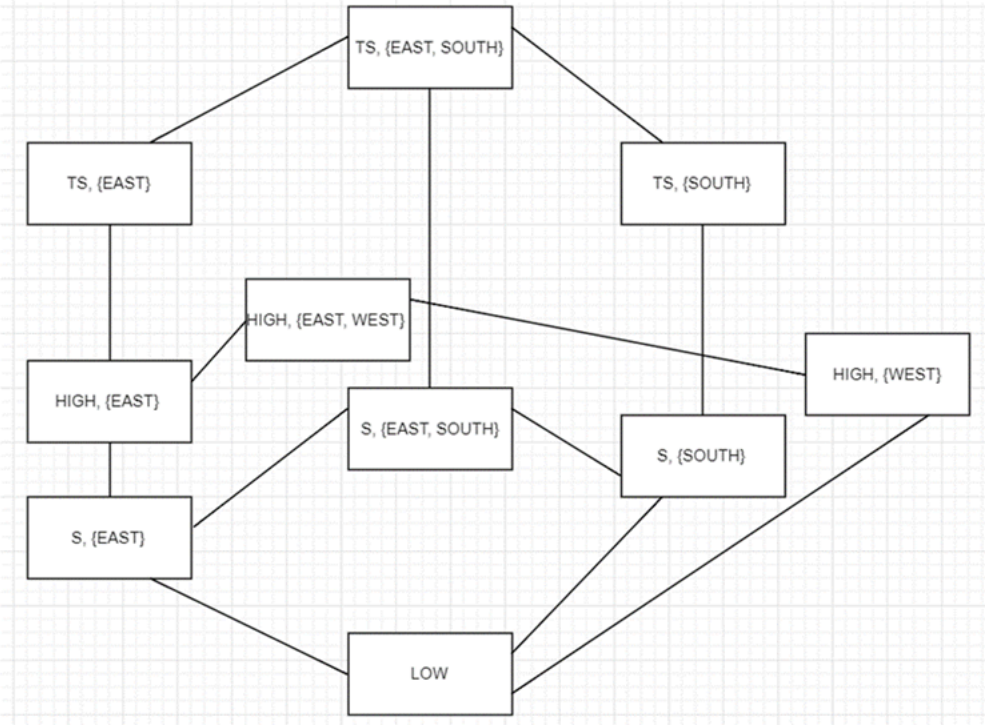


ex2

不用看

ex3

不用看

ex4

Consider a modification of the 2-bit machine of Classwork Exercise 1 (Week 3), where Holly can only alter the H bit and Lucy only the L bit. (Assume that the projection function for Lucy only shows the outputs she is supposed to see, and therefore has length equal to the number of commands issued by her.) Draw the corresponding state machine. Is this system secure? If yes, explain why. If not, show a counter example.

Answer:

Assuming:

S= {Holly, Lucy}

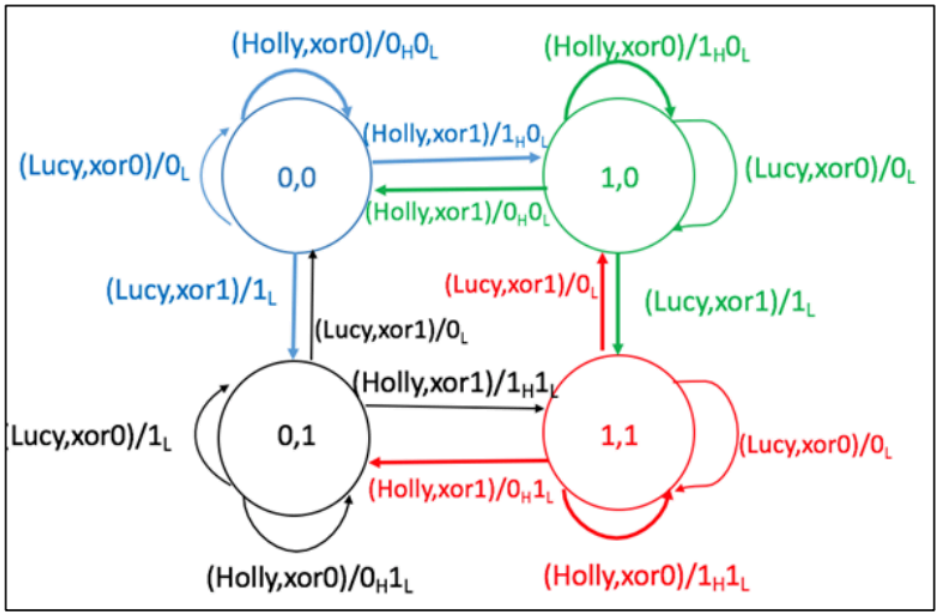
$\sum = \{(0,0), (0,1), (1,0), (1,1)\}$

$C = \{xor0, xor1\}$

The state transition function diagram is:

Commands	Input states (*H*, *L*)			
	(0, 0)	(0, 1)	(1, 0)	(1, 1)
xor0	(0, 0)	(0, 1)	(1, 0)	(1, 1)
xor1	(1, 1)	(1, 0)	(0, 1)	(0, 0)

The Finite State Machine is: (do note that Holly has the security clearance to read both H and L bits while Lucy can only ready L bits).



The above is one way to strengthen the security of this system which is to modify the commands so that Holly can alter only the high bits and Lucy only the low bits. Using the same 2-bit machine and consider the sequence c_S = (Holly, xor0), (Lucy, xor1), (Holly, xor1). Given an initial state of (0,0), the output is $0_H1_L1_H$ which correspond to Holly's and Lucy's command sequence (where the subscripts indicate the security level of the output).

Applying Definition 8-4 (from Bishop's), we use G = {Holly}, G' = {Lucy}, and A = Ø. Then $\pi_{Holly}(c_S)$ = (Lucy, xor1), so proj(Lucy, $\pi_{Holly}(c_S)$, σ_0) = (1). Now we have proj(Lucy, c_S, σ_0) = proj(Lucy, $\pi_{Holly}(c_S)$, σ_0), and therefore { Holly } :| { Lucy } holds. In other words, subjects Holly and Lucy cannot interfere each other during the execution of the commands.

The system is therefore secured under this condition because the command made by Holly and her inputs and outputs are not accessible to Lucy. As a result, Lucy is unable to deduce any information about Holly.

ex-6
待定