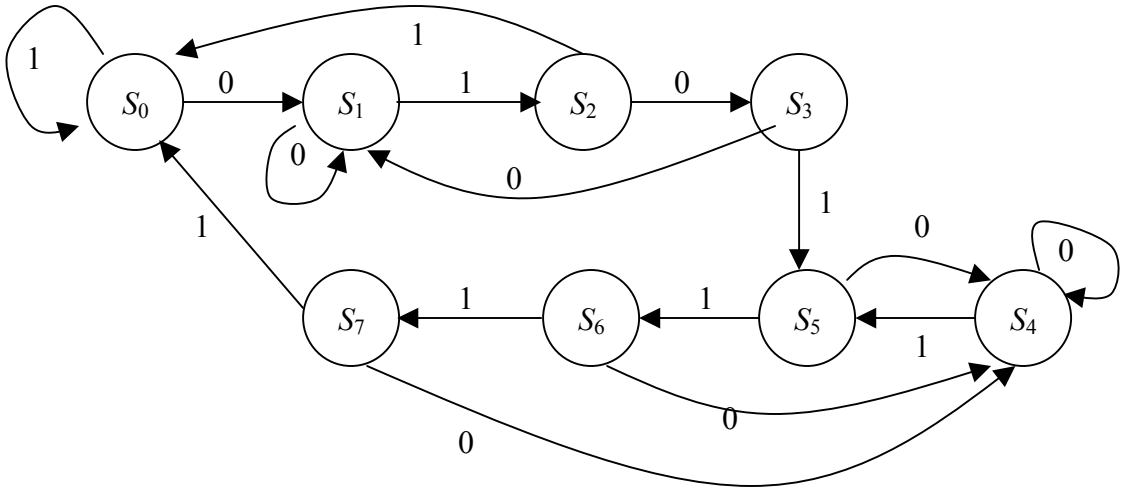
Problem Set 3 Solution
COS111 Spring 2002

Part 1

A straight-forward approach is to use 4 bits memory, 1 bit for state of the lock and 3 bits for the last 3 bits input. Then we have 16 states and a big transition diagram. The following approach has 8 states, but the initial state must be S_0 or S_4.



Part 2

Since we have 8 states, we need 3 bits:

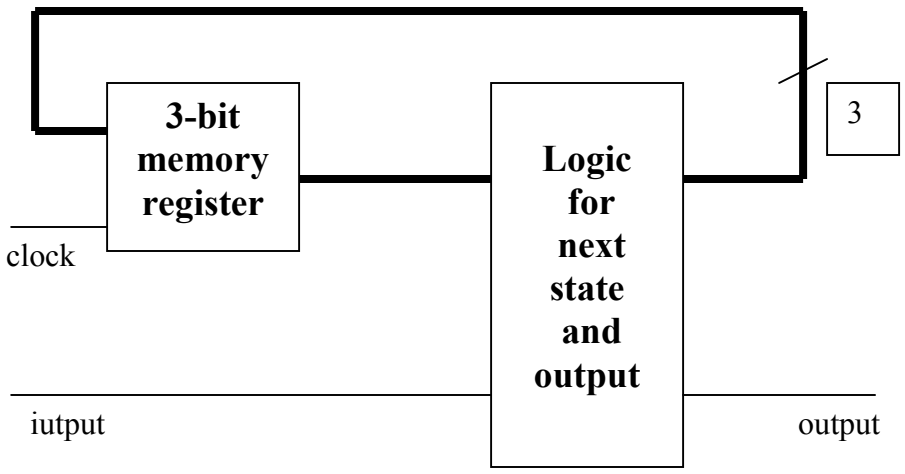
State	Representation
S_0	000
S_1	001
S_2	010
S_3	011
S_4	100
S_5	101
S_6	110
S_7	111

Part 3

The truth table is:

Current State	Input	Next State	Output
S_0	0	S_1	0
S_0	1	S_0	0
S_1	0	S_1	0
S_1	1	S_2	0
S_2	0	S_3	0
S_2	1	S_0	0
S_3	0	S_1	0
S_3	1	S_5	1
S_4	0	S_4	1
S_4	1	S_5	1
S_5	0	S_4	1
S_5	1	S_6	1
S_6	0	S_4	1
S_6	1	S_7	1
S_7	0	S_4	1
S_7	1	S_0	0

Part 4



Numeracy Exercise

(a) From problem set 1, we know that a 900 MHz computer can execute 4.05 x 10^{12} instructions during a 75-minute lecture. And from problem set 2, we know that using such computer we can crack 4.04 x 10^{6} passwords per lecture. Thus, to crack 45424 passwords, we need:

$$\frac{45424\,passwords}{4.05\times10^{6}\,passwords/lecture} = 0.0112 lectures = 0.841\,\text{min} = 50.5\,\text{sec}$$

(b) With 8-digits, we can have 10^{8} passwords. To crack a 8-digit password, we need:

$$\frac{10^{8}\,passwords}{4.05\times10^{6}\,passwords/lecture} = 24.7 lectures$$

(c) If we have 40 students cracking passwords, we can crack:

$$40\times25\times4.05\times10^{6} = 4.05\times10^{9}\,passwords$$

during 25 lectures.