HW7 Solution, CS330 Discrete Structures, Spring 2015

Instructor: Professor Edward M. Reingold
TA: Taeho Jung

April 28, 2015

1 FSM for a combination lock

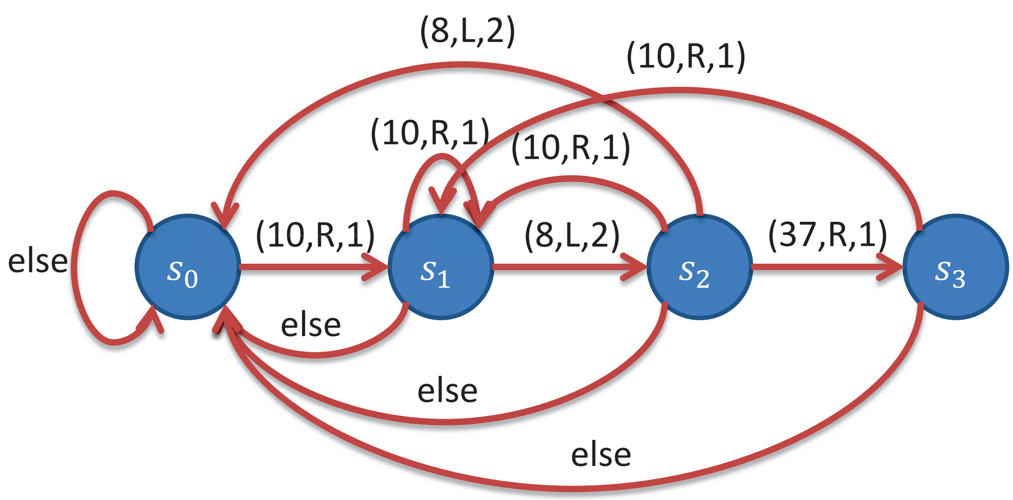

Figure 1: Finite State Machine for the Combination Lock

s_0 is the starting state, and s_3 is the final state where the lock is opened. The triple (10,R,1) means 10 right once, (8,L,2) means 8 left twice and (37,R,1) means 37 right once. 'else' means any operation except the above three.

2 FSM for bit strings having even number of '1's

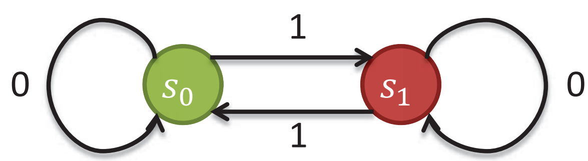

Figure 2: Finite State Machine to recognize the bit strings having an even number of 1s

3 Regular sets

a) It belongs to the set. $1011 = 10^1 1^2$

b) It belongs to the set. $1011 = 0^0 (10)^1 (11)^1$

c) It belongs to the set. $1011 = 1(01)^1 1^1$.

d) It belongs to the set. $1011 = 1^1 01(1)$.

e) It belongs to the set. $1011 = (10)^1 (11)^1$.

f) It does not belong to the set.

g) It belongs to the set. $1011 = (10)^0 1011$.

h) It belongs to the set. $(1)(01)1^1$.

4 Proof using pumping lemma.

We prove this by contradiction. Firstly, assume that the set $\{1^{n^2} | n = 0, 1, 2, \cdots\}$ is regular, i.e., the string 1^{n^2} is recognized by $FSM(S, I, f, s_0, F)$.

Let $x = 1^{n_0^2}$ for some $n_0 \geq \sqrt{|S|}$, then according to the pumping lemma in Exercise 22 (or lecture note on April 20), we can re-write the x as $x = wvu$ with a non-empty v such that $wv^k u$ is in the set of FSM for all k.

Since $x = 1^{n_0^2}$, x only has '1's in it. Therefore, $w = 1^a$, $v = 1^b$, $u = 1^c$ where a, c are non-negative integers and b is a positive integer (since v should be non-empty). Then, $x = wv^k u = 1^a (1^b)^k (1^c) = 1^{a+c+bk}$. Since $x = 1^{a+c+bk}$ is in the set of FSM, it should be in the format 1^{n^2}, which implies that $a + c + bk$ should be a perfect square for all k, which is a contradiction since a perfect square has a quadratic growth while $a + c + bk$ has a linear growth.

Therefore, our assumption that the set is regular is wrong, which means the set is not regular.

5 Extra-credit problems

1.(a)

Base Case: easily verified, thus omitted.
Assumption:

Assume $\varphi^{2i}(a) = H_{2i}a, \varphi^{2i+1}(a) = H_{2i+1}\bar{c}$.
Step:

$$\varphi^{2i+2}(a) = \varphi^{2i}(a)\varphi^2(a) = H_{2i}aH_2a = H_{2i+2}a$$

$$\varphi^{2i+3}(a) = \varphi^{2i}(a)\varphi^3(a) = H_{2i}\bar{a}H_3\bar{c} = H_{2i+3}\bar{c}$$

In conclusion, $\varphi^{2i}(a) = H_{2i}a, \varphi^{2i+1}(a) = H_{2i+1}\bar{c}$ for $i \geq 1$.

1.(b)

When N is even:

$$\lim_{N\to\infty} \varphi^N(a) = \lim_{N\to\infty} H_N a = \lim_{N\to\infty} H_N = H$$

When N is odd:

$$\lim_{N\to\infty} \varphi^N(a) = \lim_{N\to\infty} H_N \bar{c} = \lim_{N\to\infty} H_N = H$$

2.

The proof follows by the induction below.

$$H_{2N+1} = (aCbAcB)^{\frac{2^{2N+1}-2}{6}}a, \text{ for } N \geq 0$$

$$H_{2N} = (aCbAcB)^{\frac{2^{2N}-4}{6}}aCb, \text{ for } N \geq 1$$

3.

$$\varphi(\sigma(a)) = \varphi(b) = c\bar{b} = \sigma^{-1}(a\bar{c}) = \sigma^{-1}(\varphi(a))$$

$$\varphi(\sigma^{-1}(a)) = \varphi(c) = b\bar{a} = \sigma(a\bar{c}) = \sigma(\varphi(a))$$

Similarly, it can be shown that the equations hold for every letter in Σ. Then, because of the linearity of the functions, the equations hold for all strings in Σ.

4.(a)

Base case: easily verified, thus omitted.
Assumption:

$$\varphi(H_{2i})a = H_{2i+1}, \varphi(H_{2i+1})b = H_{2i+2}$$

Step:

$$
\begin{aligned}
\varphi(H_{2i+2})a &= \varphi(H_{2i+1}\bar{c}\sigma(H_{2i+1}))a \\
&= \varphi(H_{2i+1})ba\varphi(\sigma(H_{2i+1}))a \\
&= \varphi(H_{2i+1})ba\sigma^{-1}(\varphi(H_{2i+1})b) \\
&= H_{2i+2}a\sigma^{-1}(H_{2i+2}) \\
&= H_{2i+1}
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
\varphi(H_{2i+3})a &= \varphi(H_{2i+2}a\sigma^{-1}(H_{2i+2}))b \\
&= \varphi(H_{2i+2})a\bar{c}\varphi(\sigma^{-1}(H_{2i+2}))b \\
&= \varphi(H_{2i+2})a\bar{c}\sigma(\varphi(H_{2i+2})a) \\
&= H_{2i+3}\bar{c}\sigma(H_{2i+3}) \\
&= H_{2i+4}
\end{aligned}
$$

In conclusion, the following is true for all $i > 0$.

$$\varphi(H_{2i})a = H_{2i+1}, \varphi(H_{2i+1})b = H_{2i+2}$$

4.(b)

$\varphi(H_{2i})$ is a prefix of length $2^{2i+1} - 2$ of H_{2i+1}, therefore, H_{2i} is mapped to a longer prefix of H. Also, $\varphi(H_{2i+1})$ is a prefix of length $2^{2N} - 4$ of H_{2i+2}, and H_{2i+1} is also mapped to a longer prefix of H. Both combined, we have the conclusion that $\phi(H)$ has to be equal to H.

5.

Table 1: Verification for 10 state transitions

Current state x	$\varphi(x)$	State for 0	State for 1
a	$a\bar{c}$	a	$\bar{c}$
b	$c\bar{b}$	c	$\bar{b}$
c	$b\bar{a}$	b	$\bar{a}$
$\bar{b}$	cb	c	b
$\bar{c}$	ba	b	a