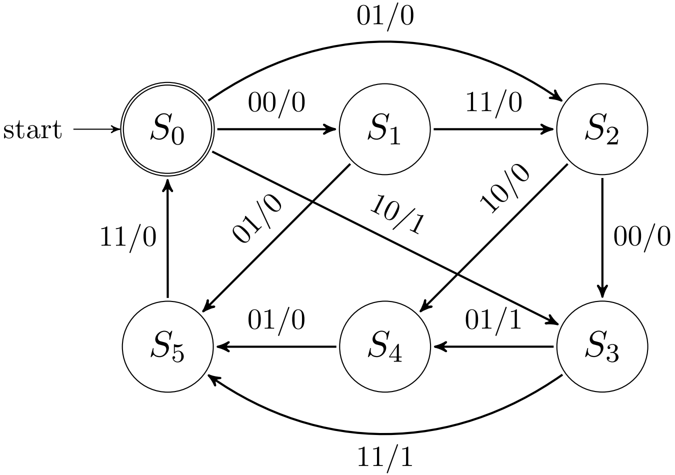
Watermarking-based Intellectual Property Core Protection Scheme

Li-Wei Chen, Shan-Yuan Zheng, Guan-Yu Chen
Supervised by C.M. Li

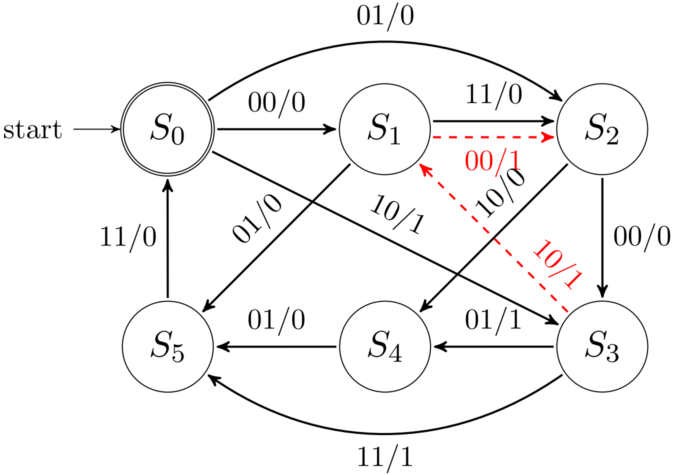
National Taiwan University

June 05, 2018

Project Description



Project Description



Algorithm

Given the input/output bit string $b_1 b_2 \cdots b_n$, where b_i is the i^{th} input/output pair and a the FSM $(\Sigma, S, s_0, \delta, F)$, we first compute the maximum length one may go from each $s \in S$ with the input and output relation specified by $b_i b_{i+1} \cdots b_n$.

The unspecified transition will not be taken into consideration, and the maximum length is recorded if there is no path to satisfy the input bit string. We also add a constraint, if the one candidate stops at b_j, the terminate state for the it must have a unspecified transition for b_{j+1} to be the maximum length path, expect for when the last input is b_n.

Algorithm

If their are multiple states that holds the same length, we choose the one that has the most free transitions. If they also have the same number, we randomly pick one to be the next state.

Then we use a greedy strategy, starting from b_0, we first choose the maximum length state as the first state, then if the maximum path stops at b_i, we then choose the maximum length state for b_{i+2} as the second state. Using b_j as the augmented trasition from the first state to the second state.

Algorithm

A new state is inserted if all the states has zero maximum length and the required input is already specified for all states. Suppose the next input/output pair is b_i, then we use b_i as transition to the new state, and b_{i+1} as the new input/output pair(transition) and continue the algorithm.

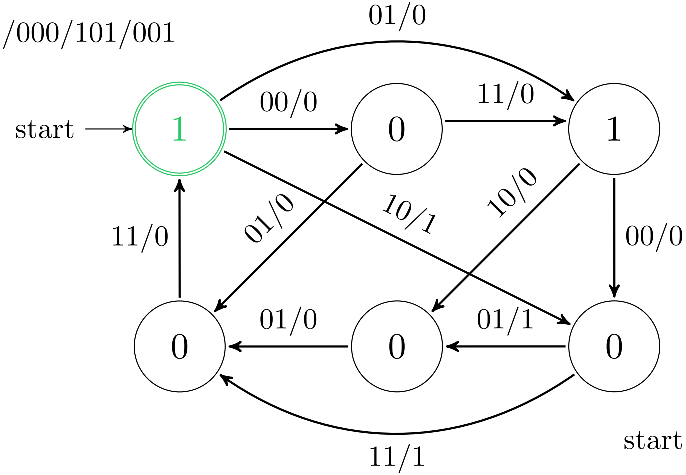
Once a new transition or state is add to the graph, they have no difference from the predefined ones. That is, the algorithm will also take them into consideration.

CSFSM Detection

The detection of CSFSM is after the data is loaded and the graph is constructed, we run over each state the check if the out transitions span the whole possible inputs. If yes, the program will report that a CSFSM is detected.

Situation—New Transition

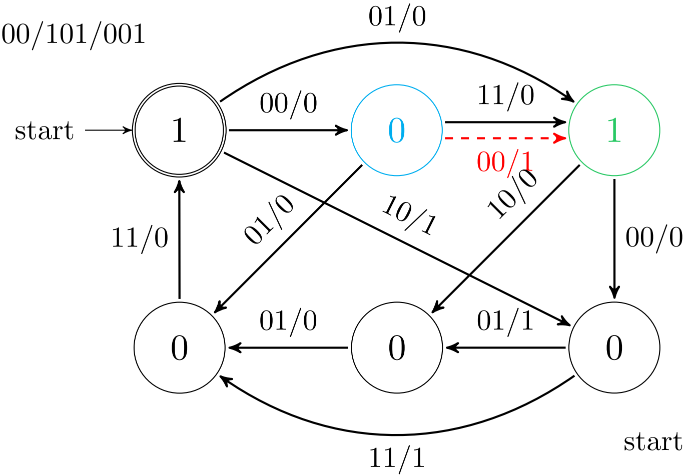
000/001/000/101/001



start at b_0 choose S_0

Situation—New Transition

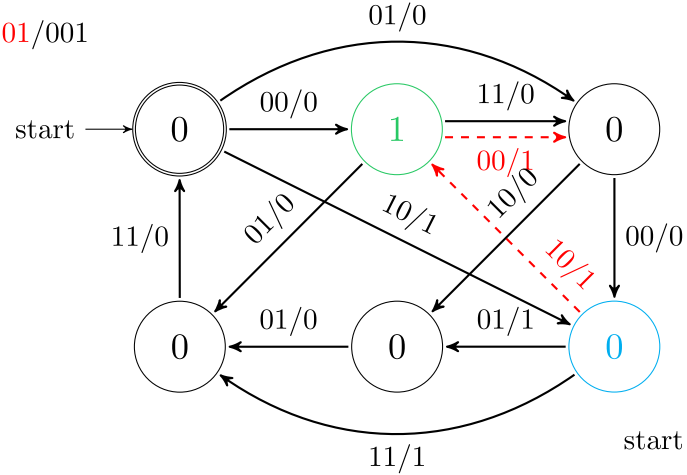
001/000/101/001



start at b_2 choose S_2

Situation—New Transition

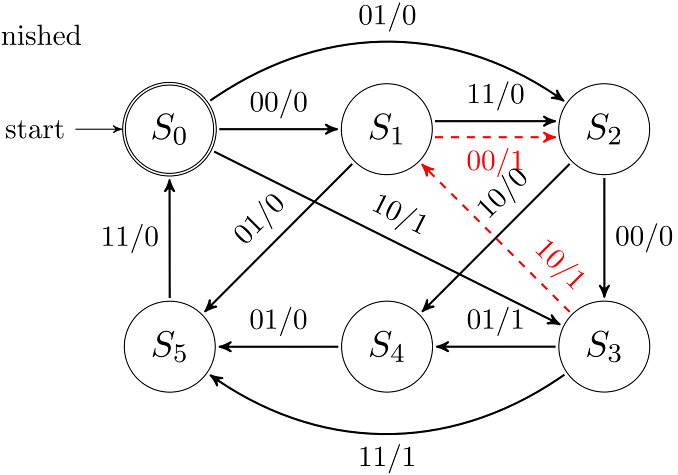
101/001



start at b_4 choose S_1

Situation—New Transition

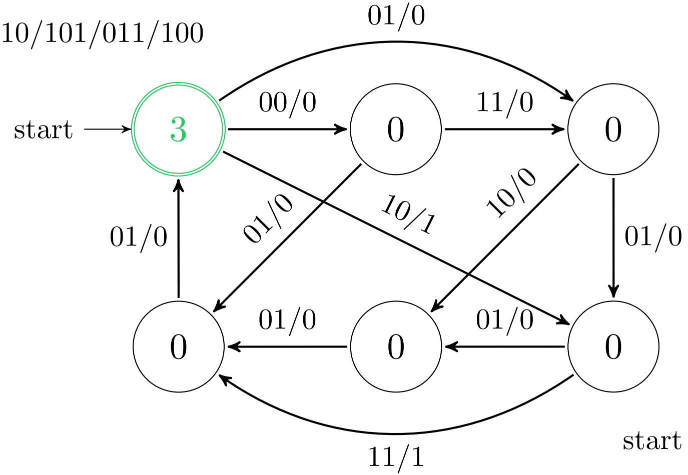
Finished



Cost $= 2$

Situation—New State

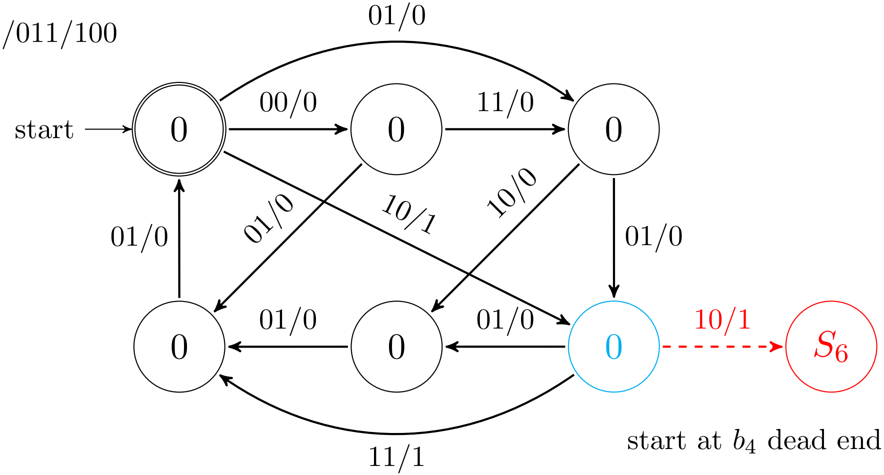
000/110/010/101/011/100



start at b_0 choose S_0

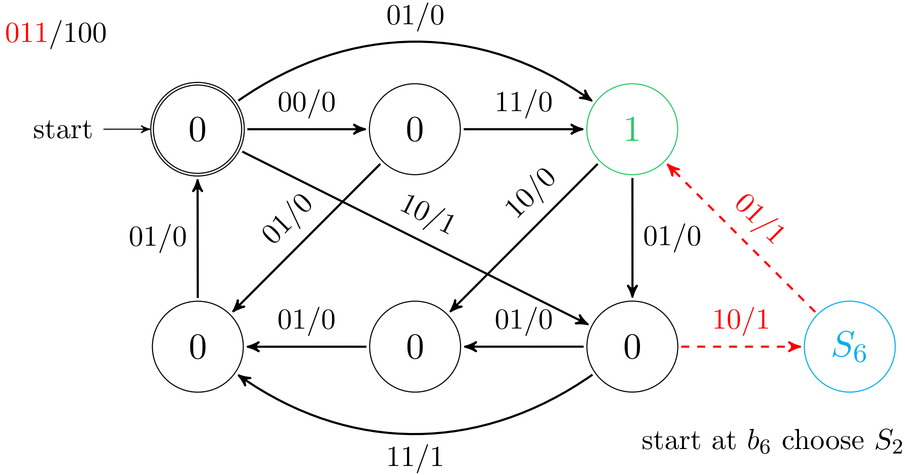
Situation—New State

101/011/100



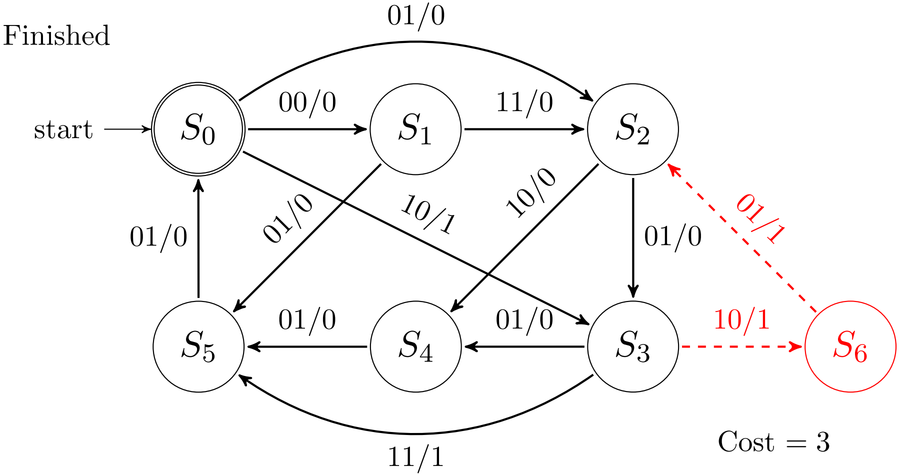
start at b_4 dead end

Situation—New State



start at b_6 choose S_2

Situation—New State



Cost $= 3$

Progress

Difficulties