# Sequential Circuits: Verification

Virendra Singh
Professor
Computer Architecture and Dependable Systems Lab
Department of Electrical Engineering
Indian Institute of Technology Bombay
http://www.ee.iitb.ac.in/~viren/
E-mail: viren@ee.iitb.ac.in

*CS-226: Digital Logic Design*

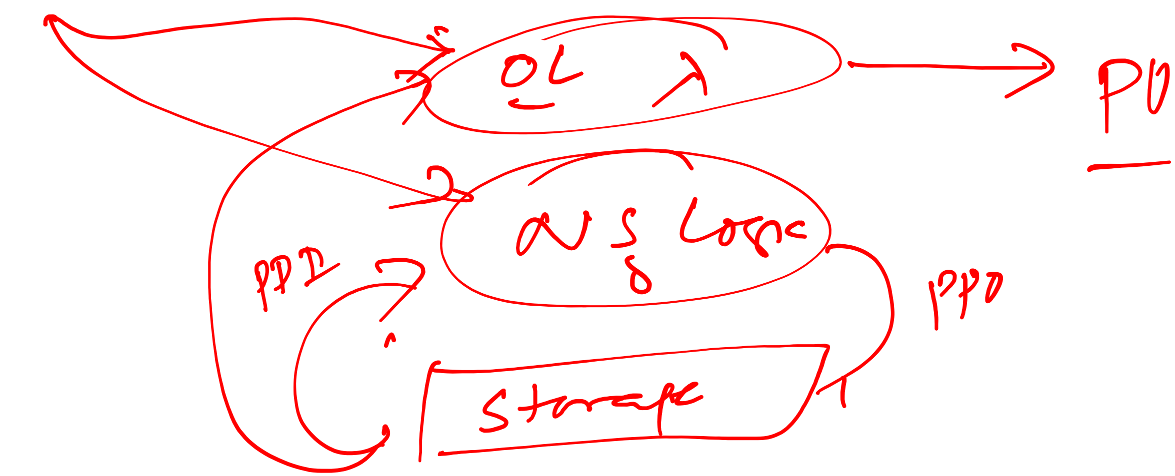
*Lecture 27: 08 April 2021*

CADSL

# Finite State Machine

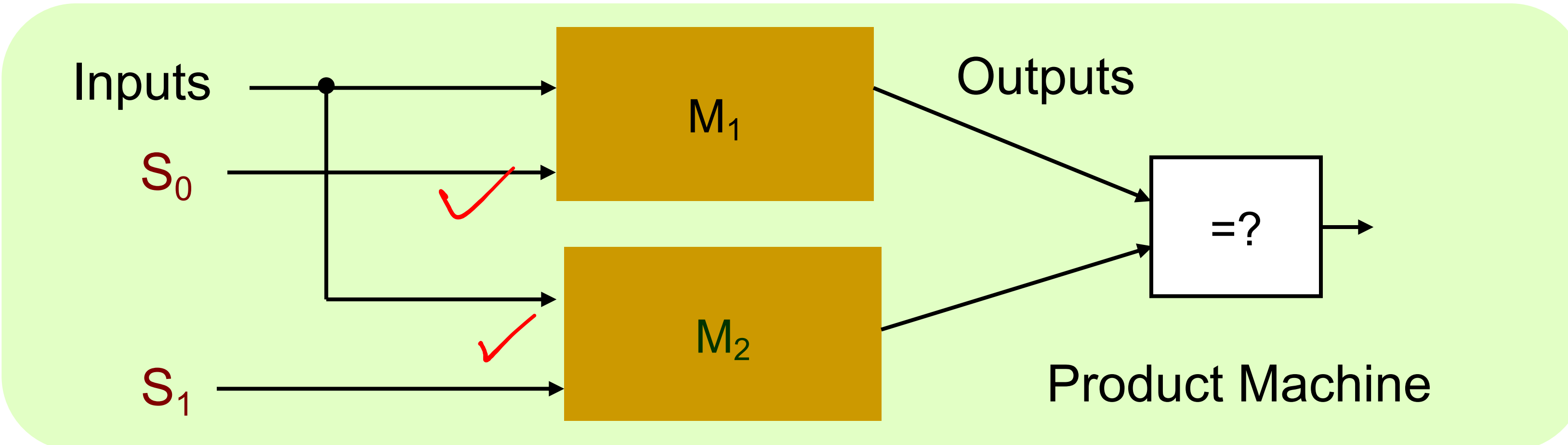
PI

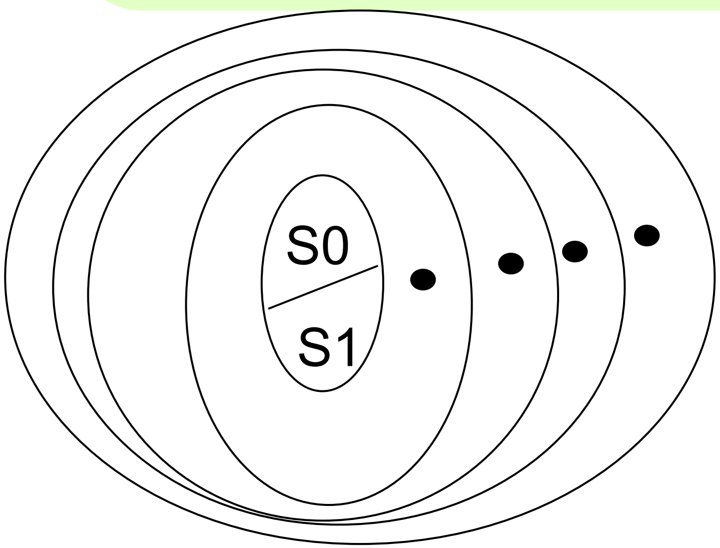
$M \; (I, O, S, \underline{\underline{S_0}}, \underline{\delta, \lambda})$



# Reachability-Based Equivalence Checking

Approach 3: Symbolic Traversal Based Reachability Analysis



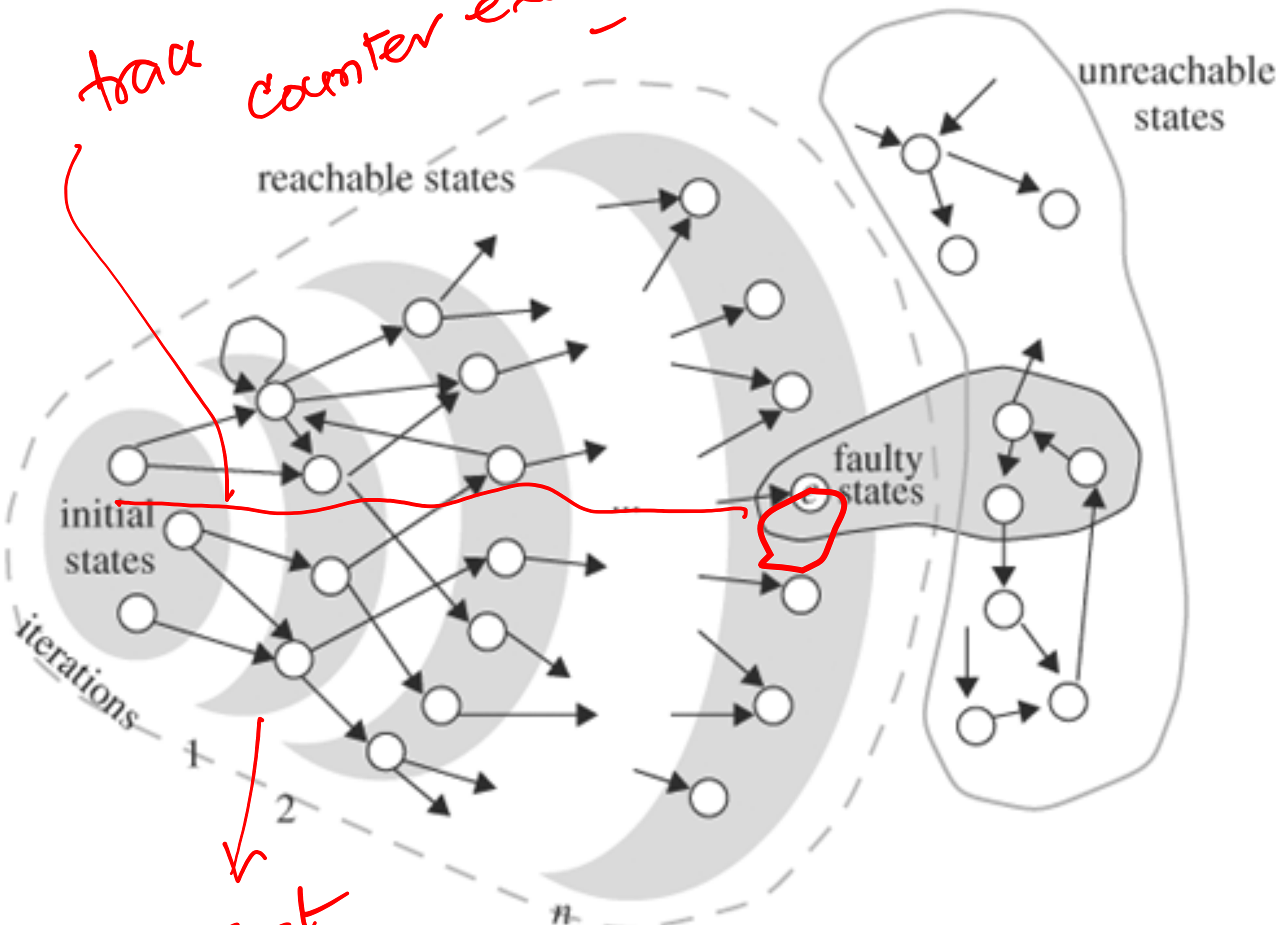




- Build product machine of $M_1$ and $M_2$
- Traverse state-space of product machine starting from reset states ($S_0$, $S_1$)
- Test equivalence of outputs in each state
- Can use any state-space traversal technique

# Forward Reachability

counter examples (cex)

trace

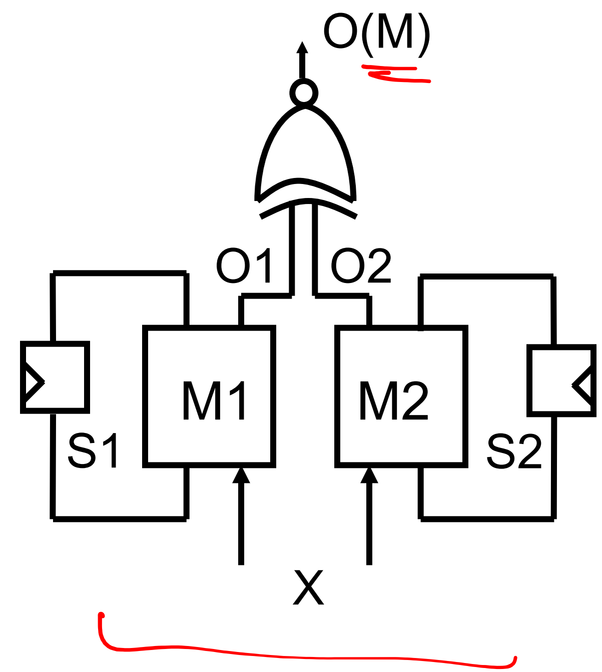



next

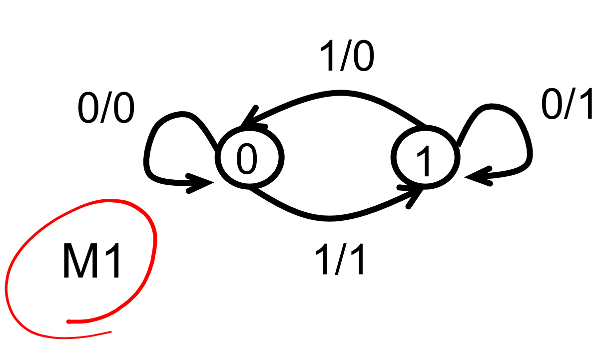
# Sequential Verification

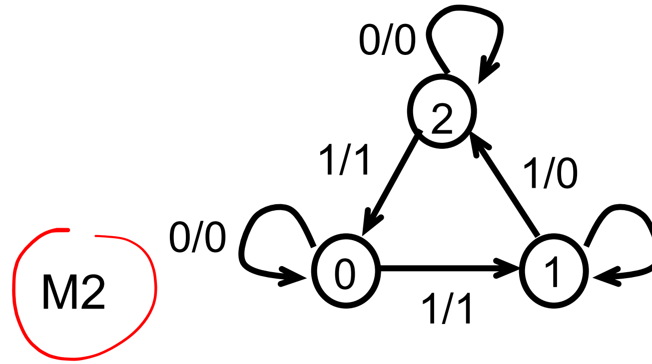
- Symbolic FSM traversal of the product machine

- Given two FSMs: $M_1(X,S_1, \delta_1, \lambda_1,O_1)$, $M_2(X,S_2, \delta_2, \lambda_2,O_2)$
- Create a product FSM: $M = M_1 \mathbf{x} M_2$
  - traverse the states of M and check its output for each transition
  - the output O(M) =1, if outputs $O_1 = O_2$
  - if all outputs of M are 1, $M_1$ and $M_2$ are *equivalent*
  - otherwise, an *error state* is reached
  - *error trace* is produced to show: $M_1 \neq M_2$



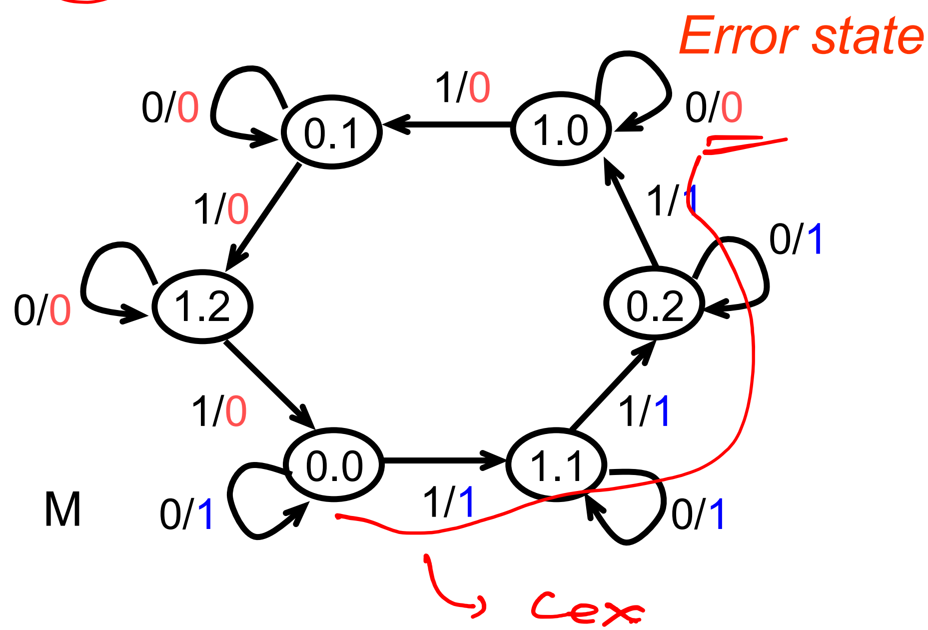
# FSM Traversal in Action




Initiall states: $s_1$=0, $s_2$=0, s=(0.0)

| State reached | Out(M) x=0 | x=1 |
|---|---|---|
| • *New* $^0$ = (0.0) | 1 | 1 |
| • *New* $^1$ = (1.1) | 1 | 1 |
| • *New* $^2$ = (0.2) | 1 | 1 |
| • *New* $^3$ = (1.0) | 0 | 0 |




- STOP - backtrack to initial state to get *error trace:* *x*={1,1,1,0}

# FSM Traversal - Algorithm

- Traverse the product machine $M(X,S,S_0,\delta,\lambda,O)$
  - start at an initial state $S_0$
  - iteratively compute symbolic image $Img(S_0,R)$ (set of *next states*):

$$\mathrm{Im}\,g(S_0,R) = \exists_x \exists_s S_0(s).R(x,s,t)$$

$$R = \prod_i R_i = \prod_i (t_i \equiv \delta_i(s,x))$$

until an *error state* is reached

  - transition relation $R_i$ for each next state variable $t_i$ can be computed as $t_i = (t \otimes \delta(s,x))$

(this is an alternative way to compute transition relation, when design is specified at gate level)

# How to Represent TF ?

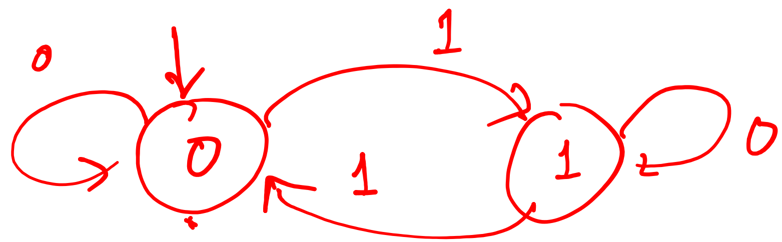
- Given a deterministic transition function (s,x) the corresponding transition relation is defined by
  - $$T(s,x,t) = \prod (t_i = \delta_i(s,x))$$
- T(s,x,t) = 1 denotes a set of encoded tripples (s,x,t) , each representing a transition in the FST of a given FSM
- Straight forward to compute image
- Need new boolean operation
  - Existential Abstraction
  - $$\exists_{xi} .f = f_{xi} + f_{\overline{xi}}$$
  - $f_{xi}$- smallest (fewest minterm) function that contains all minterms of f and independent of xi

# How to Traverse?

$x, \delta$

$S = \{0, 1\}$

$s$ $\quad t$




| $s \backslash x$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$\delta = \bar{s}x + s\bar{x}$$

$$R(s, x, t) = (t \equiv \delta)$$

$$R = (t \equiv \bar{s}x + s\bar{x}) = (t \odot (\bar{s}x + s\bar{x}))$$

$$= t \cdot (\bar{s}x + s\bar{x}) + \bar{t}\,(\overline{\bar{s}x + s\bar{x}})$$

$$= t\bar{s}x + ts\bar{x} + \bar{t}\,(\overline{\bar{s}x} \cdot \overline{s\bar{x}})$$

$$= t\bar{s}x + ts\bar{x} + \bar{t}\,((s + \bar{x}) \cdot (\bar{s} + x))$$

$$= t\bar{s}x + ts\bar{x} + \bar{t}\bar{s}\bar{x} + \bar{t}sx.$$

# How to Traverse?

$$R(x,s,t) = \underbrace{t s x + t s \bar{x} + \bar{t} \cancel{s} \bar{x} + \bar{t} s x}$$

initial $\quad 0 \quad \bar{s}$

$$f(x,s,t) = (t \bar{s} x + t s \bar{x} + \bar{t} \bar{s} \bar{x} + \bar{t} s x) \cdot \bar{s}$$

$$f(x,s,t) = \underline{t \bar{s} x + \bar{t} \bar{s} \bar{x}}$$

$f_x = t \bar{s}$

$f_{\bar{x}} = \bar{t} \bar{s}$

$f(s,t) = t \bar{s} + \bar{t} \bar{s} = \bar{s}$

$f(1,1) = \bar{s}$

$f_s = 0$

$f_{\bar{s}} = 1$

$f(t) = 0 + 1 = 1$

$\{0, 1\}$.

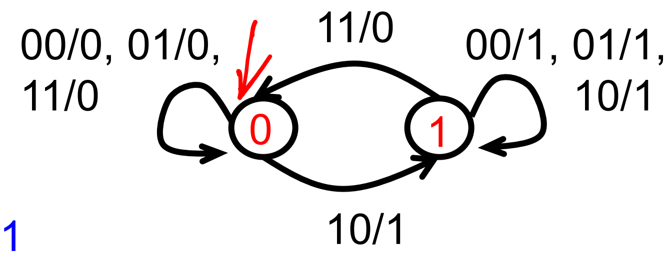
# How to Represent TF ?

- Given $f(s,x) = f(s, .. s_n, x_1, ...x_m)$ the existential abstraction w.r.t a set of variables is defined as
  - $$\exists_x .f(s,x) = \exists_{x1}(\exists_{x2}(\ldots\exists_{xm}(f(s,x)))$$

$\lambda = \lambda_1 \oplus \lambda_2$

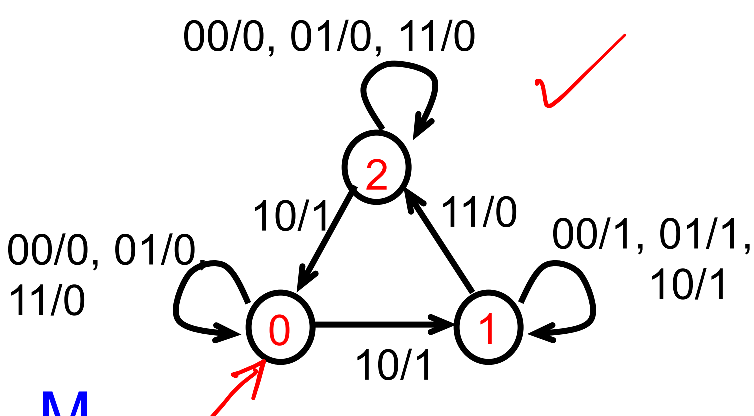
- **Procedure**
  - Compute TF, T(s,x,t)
  - Compute conjunction of T and C
  - Existentially abstract all s variable and all x variable - provides f(t)
  - f(t) is the smallest function independent of s and x which contains all the tripples in f(s,x,t)

# State Reachability in Product FSM




$M_1$

- $t_1 = \delta^1{}_1 = x_1x_2' + s_1x'_1$
- $\lambda^1 = \delta^1{}_1$



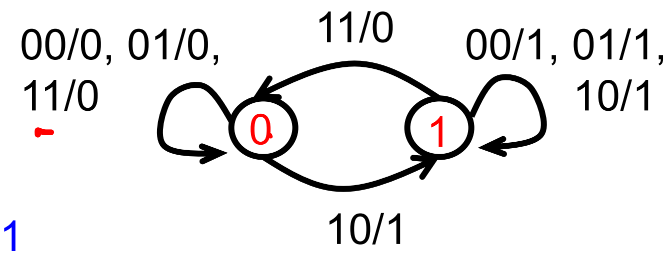

$M_2$

- 0=00, 1=01, 2 =10
- $t_2 = \delta^2{}_2 = s_3x_1x_2 + s_2(x'_1 + x_2)$
- $t_3 = \delta^2{}_3 = s'_2x_1x'_2 + s_3x'_1$
- $\lambda^2 = s_3x'_1 + x_1x'_2$

# State Reachability in Product FSM

$x_1 x_2$

$s_1$




$M_1$

- $t_1 = \delta^1{}_1 = x_1x_2' + s_1.x'_1$
- $\lambda^1 = \delta^1{}_1$ $= x_1\bar{x}_2 + s_1\bar{x}_1$

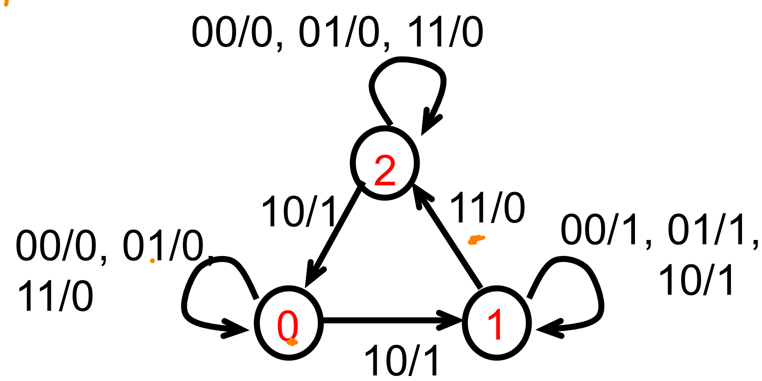
| $s$ \ $x_1x_2$ | 00 | 01 | 11 | 10 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 |

$x_1\bar{x}_2$

$s\bar{x}_1$

$\delta^1_1 = x_1\bar{x}_2 + s\bar{x}_1$

# State Reachability in Product FSM




$M_2$

- 0=00, 1=01, 2 =10
- $t_2 = \delta^2{}_2 = s_3x_1x_2 + s_2(x'_1 + x_2)$

$\delta^2_2$

$\delta^2_3$

$x_1x_2$

$s_2 s_3$

| $s_2s_3$ \ $x_1x_2$ | 00 | 01 | 11 | 10 |
|---|---|---|---|---|
| 00 | 0 | 0 | 0 | 0 |
| 01 | 0 | 0 | 1 | 0 |
| 11 | X | X | X | X |
| 10 | 1 | 1 | 1 | 0 |

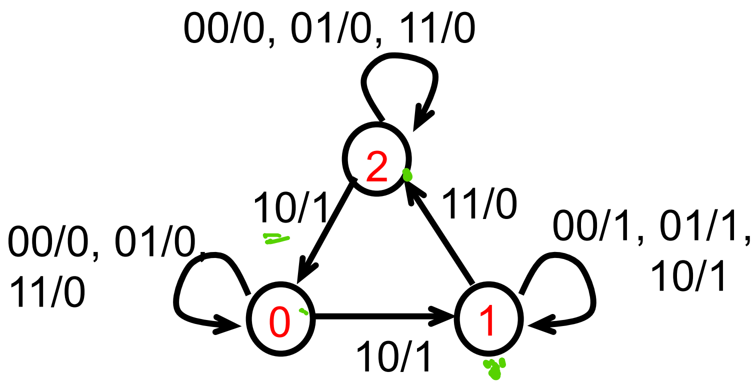
$s_3x_1x_2$

$s_2\bar{x}_1$

$s_2x_2$

$\delta^2_2 = s_2\bar{x}_1 + s_2x_2 + s_3x_1x_2$

# State Reachability in Product FSM




$M_2$

- 0=00, 1=01, 2 =10
- $t_2 = \delta^2_2 = s_3x_1x_2 + s_2(x'_1 + x_2)$
- $t_3 = \delta^2_3 = s'_2x_1x'_2 + s_3x'_1$
- $\lambda^2 = s_3x'_1 + x_1x'_2$

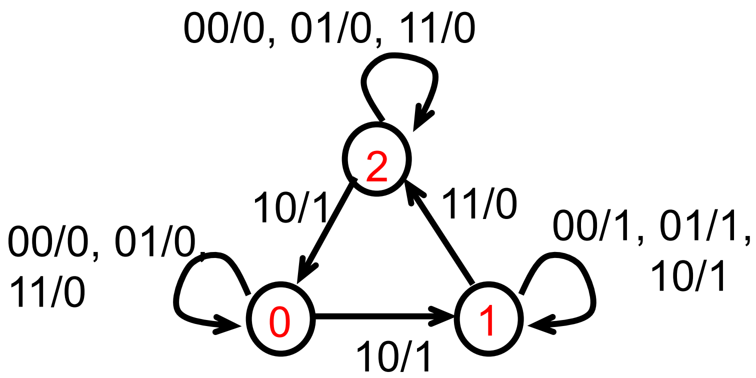
| $s_2s_3$ \ $x_1x_2$ | 00 | 01 | 11 | 10 |
|---|---|---|---|---|
| 00 | 0 | 0 | 0 | 1 |
| 01 | 1 | 1 | 0 | 1 |
| 11 | x | x | x | x |
| 10 | 0 | 0 | 0 | 0 |

$s_3\bar{x}_1$

$s_2x_1\bar{x}_1$

$$\delta^2_3 = s_3\bar{x}_1 + s_2x_1\bar{x}_2$$

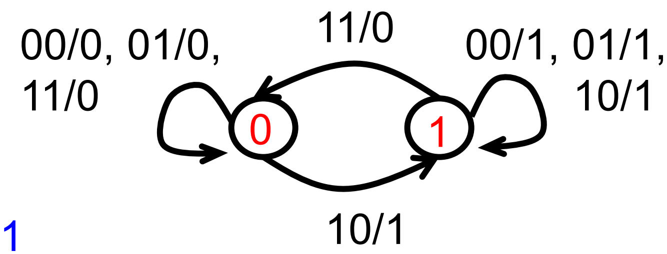
# State Reachability in Product FSM




$M_2$

- 0=00, 1=01, 2 =10
- $\lambda^2 = s_3x'_1 + x_1x'_2$

# State Reachability in Product FSM




$M_1$

- $t_1 = \delta^1{}_1 = x_1 x_2' + s_1 x'_1$
- $\lambda^1 = \delta^1{}_1$

$\delta^1_1$ $s_1$

$\delta^2_2$ $s_2$

$\delta^2_3$ $s_3$

$\delta_1 \cdot \delta_2 \delta_3$  000 → 0·0

$t_1 \cdot t_2 t_3$

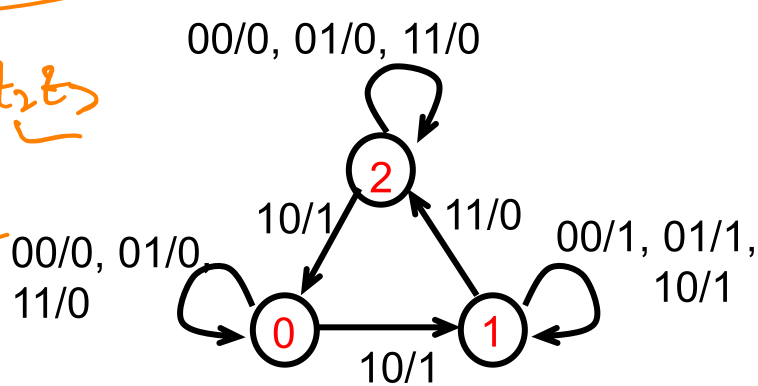
↓

101

↓

1·1

- 0=00, 1=01, 2 =10




$M_2$

- $t_2 = \delta^2{}_2 = s_3 x_1 x_2 + s_2(x'_1 + x_2)$
- $t_3 = \delta^2{}_3 = s'_2 x_1 x'_2 + s_3 x'_1$
- $\lambda^2 = s_3 x'_1 + x_1 x'_2$

# Symbolic FSM Traversal

Transition relation of the product machine

- $T(s, x, t) = (t_1 \equiv \delta^1{}_1).\ (t_2 \equiv \delta^2{}_2).\ (t_3 \equiv \delta^2{}_3)$

$T(s, x, t) = (t_1 \equiv x_1x_2' + s_1x'_1).\ (t_2 \equiv s_3x_1x_2 + s_2(x'_1 + x_2)).(t_3 \equiv s'_2x_1x'_2 + s_3x'_1)$

# Symbolic FSM Traversal

## Transition relation of the product machine

- $T(s, x, t) = (t_1 \equiv \delta^1{}_1).\ (t_2 \equiv \delta^2{}_2).\ (t_3 \equiv \delta^2{}_3)$
- Initial State is $s'_1 s'_2 s'_3$
- $T(s,x,t).C(s) = T(s,x,t).s'_1 s'_2 s'_3$

  $= (t_1 \equiv s'_1 x_1 x_2).(t_2 \equiv 0).(t_3 \equiv s'_2 x_1 x'_2).\ s'_1 s'_2 s'_3$

f

$\cancel{T}(s, x, t) = (t_1 \equiv x_1 x_2' + s_1 x'_1).\ (t_2 \equiv s_3 x_1 x_2 + s_2(x'_1 + x_2)).(t_3 \equiv s'_2 x_1 x'_2 + s_3 x'_1)\ .\ s'_1 s'_2 s'_3$

- Since this conjunction evaluate to 1 for just one s-minterm $(s'_1 s'_2 s'_3)$

# Symbolic FSM Traversal

## Transition relation of the product machine

- $T(s, x, t) = (t_1 \equiv \delta^1{}_1).\ (t_2 \equiv \delta^2{}_2).\ (t_3 \equiv \delta^2{}_3)$
- Initial State is $s'_1 s'_2 s'_3$

$$T(s, x, t) = (t_1 \equiv x_1x_2' + s_1x'_1).\ (t_2 \equiv s_3x_1x_2 + s_2(x'_1 + x_2)).(t_3 \equiv s'_2x_1x'_2 + s_3x'_1)\ .\ s'_1s'_2s'_3$$

$$G(x,t) = \exists_s (T(s,x,t).C(s))$$

$(t_1 \equiv x_1\bar{x}_2)\ (t_2 = 0)(t_3 \equiv x_1\bar{x}_2$

$$= (t_1 \equiv x_1x'_2).(t_2 \equiv 0).(t_3 \equiv x_1x'_2)$$

$\exists_s f(x,s,t)$

# Symbolic FSM Traversal

$G(x,t) = \exists_s (T(s,x,t).C(s))$

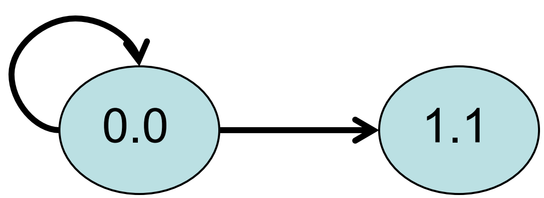
$= (t_1 \equiv x_1x'_2).(t_2 \equiv 0).(t_3 \equiv x_1x'_2)$

| | $t_1$ | $t_2$ | $t_3$ |
|---|---|---|---|
| 00 | 0 | 0 | 0 |
| 01 | 0 | 0 | 0 |
| 10 | 1 | 0 | 1 |
| 11 | 0 | 0 | 0 |

- Since this conjunction evaluate to 1 for just one s-minterm $(s'_1s'_2s'_3)$
- $g_{x1x'2} = (t_1 \equiv 1).(t_2 \equiv 0).(t_3 \equiv 1)$
- $g_{x'1x2} = g_{x'1x'2} = g_{x1x2} = (t_1 \equiv 0).(t_2 \equiv 0).(t_3 \equiv 0)$
- $\text{Img}(T,C) = g(x,t) = t'_1t'_2t'_3 + t_1t'_2t_3$

(000) 0.00 (0.0)

(101) 1.01




$C(s) = \bar{s}_1\bar{s}_2\bar{s}_3$

$C_{new}(s) = \bar{s}_1\bar{s}_2 s_3 + s_1\bar{s}_2 s_3$ (1.1)

$\lambda = \lambda_1 \oplus \lambda_2$

$\bar{s}_2(\bar{s}_1\bar{s}_3 + s_1 s_3)$

$C_{new}'(s) = C_{old}(s)$

0, 1 {0, 1}

# Forward Reachability

- BDD is used

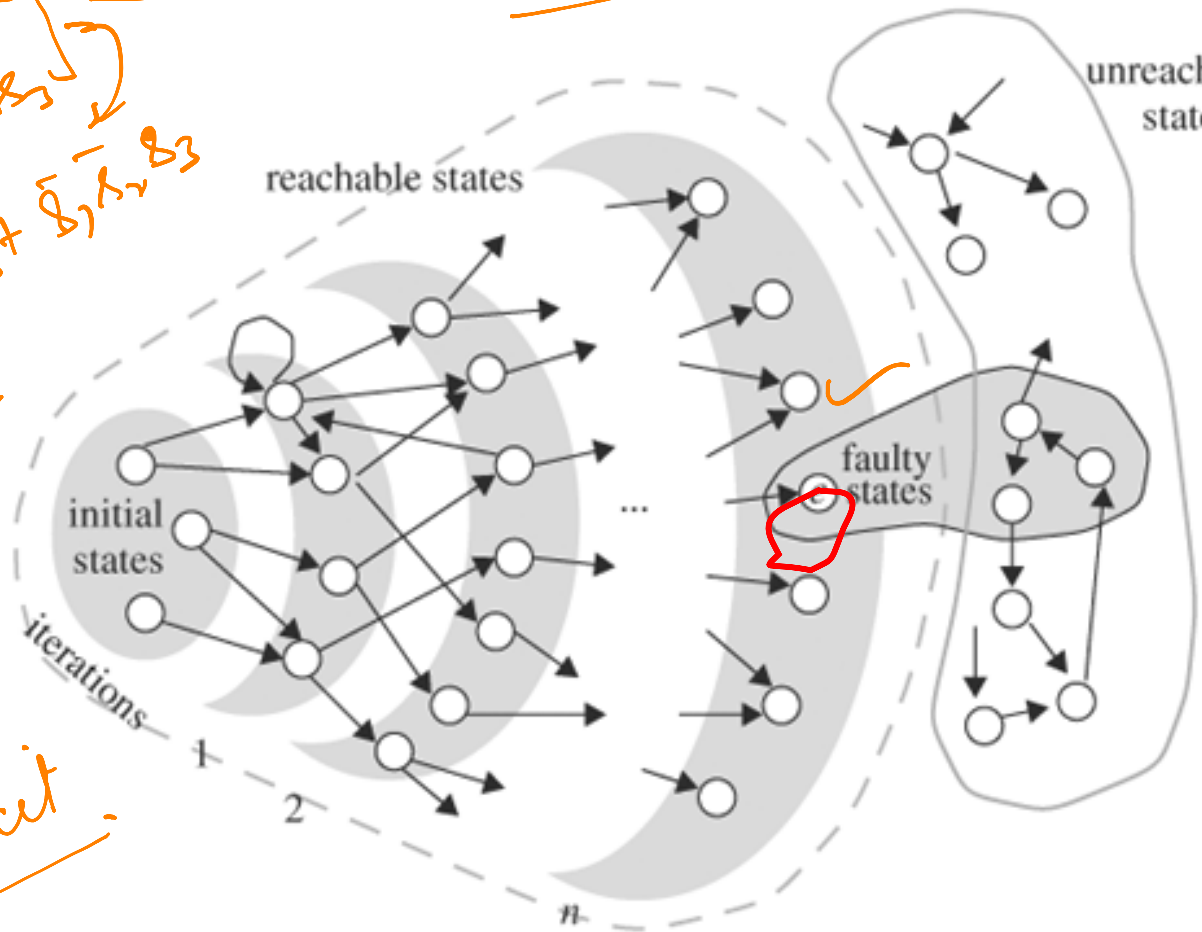
ROBDD

$\bar{s}_1 \bar{s}_2 s_3$

$\bar{s}_1 \bar{s}_2 s_3$

$\bar{s}_1 \bar{s}_2 s_3 + \bar{s}_1 \bar{s}_2 s_3$

$\bar{s}_1 \bar{s}_2$




Reachability

C(S)

Implicit

# Thank You