



# fFSM

- MPSoC

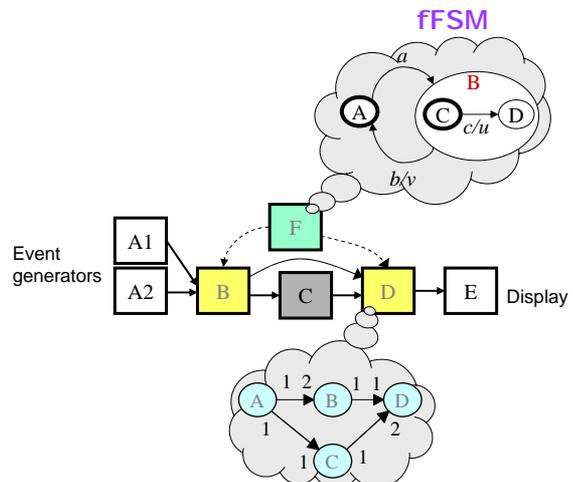
- 
- 

- -

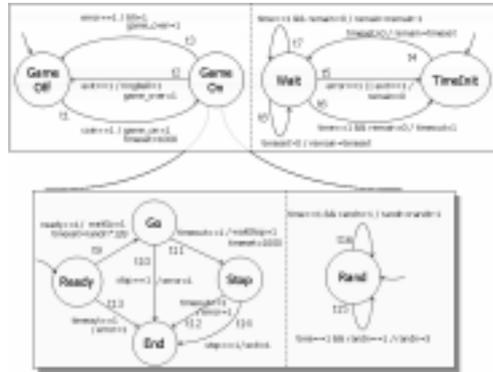
- 

- 

- 
- 
- 



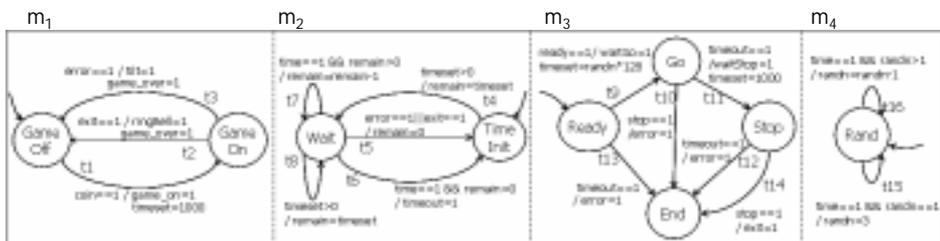
- 
- fFSM
- 
- 
- 
- 
- 
- 
- 



3

- 
- 
- 
- 
- 

(compositional)



4

# fFSM

$$fFSM = (I, O, IT, M, \gamma, V)$$

$$I \cup O \cup IT = \{e_1, \dots, e_n\}$$

$$M = \{m_1, \dots, m_n\}$$

$$\gamma: \Sigma \rightarrow 2^M$$

$$V = \{v_1, \dots, v_n\}$$

$$m_i = (S_i, s_i^0, T_i, scr_i)$$

$$S_i = \{s_i^0, s_i^1, \dots, s_i^n\}$$

$$s_i^0$$

$$t \in T_i, t = (s, g, A, s')$$

$$scr_i: S_i \rightarrow 2^{Script}$$

$$\Sigma = \prod_{i=1}^n S_i$$

$$sub: \Sigma \rightarrow 2^\Sigma$$

$$sub(s) = \{s' \mid M_i \in \gamma(s) \wedge s' \in S_i\}$$

5

# 가

$$G ::= true \mid \neg G \mid G_1 \wedge G_2 \mid e < Exp \mid e = Exp \mid v < Exp \mid v = Exp$$

$$Exp ::= n \mid v \mid Exp_1 \bullet Exp_2$$

$$\bullet \in \{+, -, \times, / \}, \quad v \in V$$

6

t

$source(t) = s$

$target(t) = s'$

$guard(t) = g$

$action(t) = A$

A

$a ::= v := Exp \mid e(p)$

$signal(A) = \{e(p) \mid \exists e \in IT. e(p) \in A\}$

$update(A) = \{v := Exp \mid \exists v \in V. (v := Exp) \in A\}$

$output(A) = \{e(p) \mid \exists e \in O. e(p) \in A\}$

7

## (Configuration)

:

$\Delta = \{\{s_1, \dots, s_n\} \mid \exists s_i \in S_i, 0 < i \leq n\}$

$\delta \in \Delta$

$\delta_0 = \{s_1^0, K, s_n^0\}$

8

$$\begin{aligned}
\langle \delta, E \rangle \models \text{true} & \quad \text{iff} \quad \text{true} \\
\langle \delta, E \rangle \models \neg G & \quad \text{iff} \quad \text{not } \langle \delta, E \rangle \models G \\
\langle \delta, E \rangle \models G_1 \wedge G_2 & \quad \text{iff} \quad \langle \delta, E \rangle \models G_1 \text{ and } \langle \delta, E \rangle \models G_2 \\
\langle \delta, E \rangle \models e < \text{Exp} & \quad \text{iff} \quad e \in E \text{ and } \text{val}(e) < \text{val}(\text{Exp}) \\
\langle \delta, E \rangle \models e = \text{Exp} & \quad \text{iff} \quad e \in E \text{ and } \text{val}(e) = \text{val}(\text{Exp}) \\
\langle \delta, E \rangle \models v < \text{Exp} & \quad \text{iff} \quad \text{val}(v) < \text{val}(\text{Exp}) \\
\langle \delta, E \rangle \models v = \text{Exp} & \quad \text{iff} \quad \text{val}(v) = \text{val}(\text{Exp}) \\
\text{val}(n) & = n \\
\text{val}(e) & \text{ val}(v) \\
\text{val}(\text{Exp}_1 \bullet \text{Exp}_2) & = \text{val}(\text{Exp}_1) \bullet \text{val}(\text{Exp}_2)
\end{aligned}$$

9

$$\delta \models s \quad \text{iff} \quad \forall s' \in \Sigma. s \in \text{sub}^*(s') \Rightarrow s' \in \delta$$

$$ET = \{t \mid \forall i \in \{1, \dots, n\}. t \in T_i \wedge \langle \delta, E \rangle \models \text{guard}(t) \wedge \delta \models \text{source}(t)\}$$

$$XT = \{t \in ET \mid \neg \exists t' \in ET. \text{source}(t) \in \text{sub}^+(\text{source}(t'))\}$$

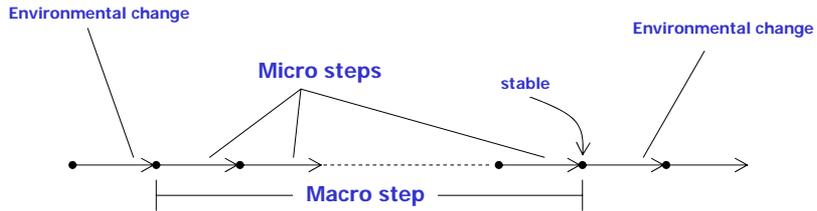
fFSM

$$\forall m_i \in M. |XT \cap T_i| \leq 1$$

10

# fFSM

- - 
  - 가
  -



11

# LKS(Labeled Kripke Structure)

$$LKS = (Q, q_0, R, L)$$

$$Q = \{q_0, \dots, q_n\} \quad \text{LKS}$$

$$q_0 = (\delta_0, \emptyset, c_0)$$

$$R \subseteq Q \times 2^{Act} \times Q$$

$$L: Q \rightarrow 2^{Script}, \quad L(q_i) = \prod_{\forall s=\delta} scr(s)$$

12

$$(\delta, E, c) \xrightarrow{Act} (\delta', E', c')$$

$$Act = \prod_{\forall t \in XT} output(action(t)) \cup \prod_{\forall t \in XT} update(action(t))$$

$$\delta' = \{s' \mid \forall s \in \delta. \exists t \in XT. (s = source(t) \Rightarrow s' = target(t)) \\ \vee (s \in sub^+(source(t)) \Rightarrow s' = reset(s)) \\ \vee (s \notin sub^*(source(t)) \Rightarrow s' = s)\}$$

$$\text{where } reset(s) = s_i^0, s \in sub(s'') \wedge m_i \in \gamma(s'') \wedge s \in S_i$$

$$E' = \prod_{\forall t \in XT} signal(action(t))$$

$$c' = L(q')$$

13

$$(\delta_i, E_i, c_i) \xrightarrow{Exe_i} (\delta_{i+1}, \emptyset, c_{i+1})$$

iff

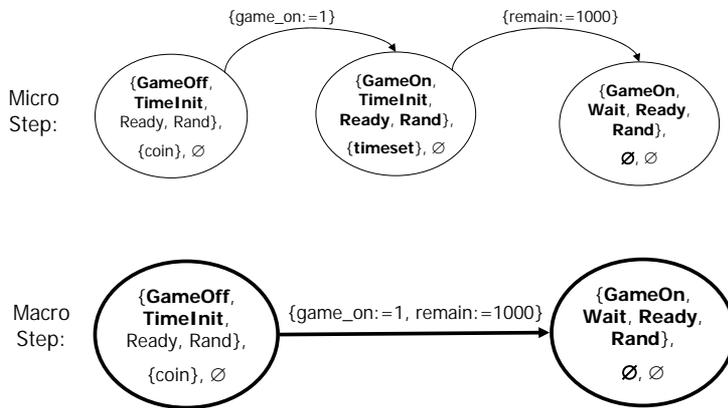
$$(\delta_i, E_i, c_i) = (\delta_{i,1}, E_{i,1}, c_{i,1}) \xrightarrow{Act_1} \Lambda \xrightarrow{Act_{k-1}} (\delta_{i,k}, \emptyset, c_{i,k}) = (\delta_{i+1}, \emptyset, c_{i+1})$$

$$k > 1 \quad E_{i,k} \quad \emptyset \quad k$$

$$Exe_i = \prod_{\forall 0 < j < k} Act_j$$

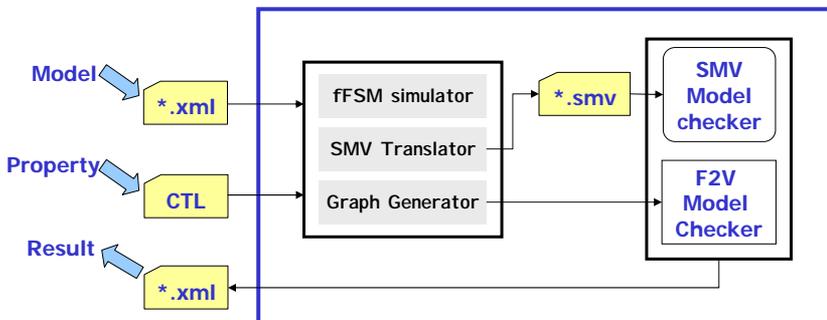
$$q \xrightarrow{Exe} q'$$

14



15

## Stepper: fFSM



Formal fFSM Verifier (F2V)

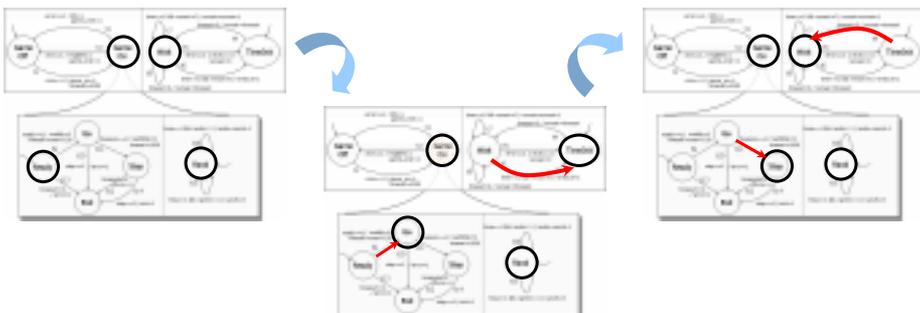
16

- - EF  $component_1 \wedge \dots \wedge EF\ component_n$
  - $\vdots$
- 가
  - EF  $(s_i \wedge EX\ s_j)$ ,  $guard(t) = g$ ,  $source(t) = s_i$ ,  $target(t) = s_j$
- (ambiguous transition)
  - AG  $\neg((t_1 \wedge t_2) \vee (t_2 \wedge t_3) \vee (t_1 \wedge t_3))$ , where  $\{t_1, t_2, t_3\}$  is a set of outgoing transitions from the same state.
- - $\neg EFAG\ deadlock$ , where  $deadlock$  is  $\neg(t_1 \vee \dots \vee t_n)$
- (circular transition)
  - AG  $(\neg stable \Rightarrow A[\neg stable\ U\ stable])$
- (Race condition violation)
  - AG  $(\neg stable \wedge update \Rightarrow AX\ A[\neg update\ U\ stable])$

17

- Race condition violation

events	Configuration	Actions
{time, ready}	{GameOn, Wait, Ready, Rand}	{waitGo:=1, remain:=0}
{timeset, timeout}	{GameOn, TimeInit, Go, Rand}	{waitStop:=1, remain:=randn*128}
{timeset}	{GameOn, Wait, Stop, Rand}	{ remain:=1000}
$\emptyset$	{GameOn, Wait, Stop, Rand}	-

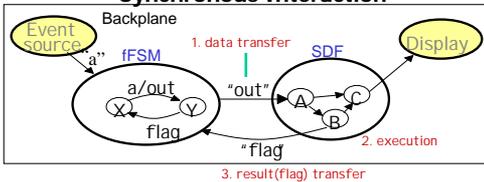


18



- - fFSM
  -
- - 
  -

### Synchronous Interaction



### Asynchronous Interaction

