CSE 591: Theoretical Aspects of CPS

Control
Reference: Tabuada Ch 6

Instructor: Georgios E. Fainekos

School of Computing, Informatics and Decision System Engineering

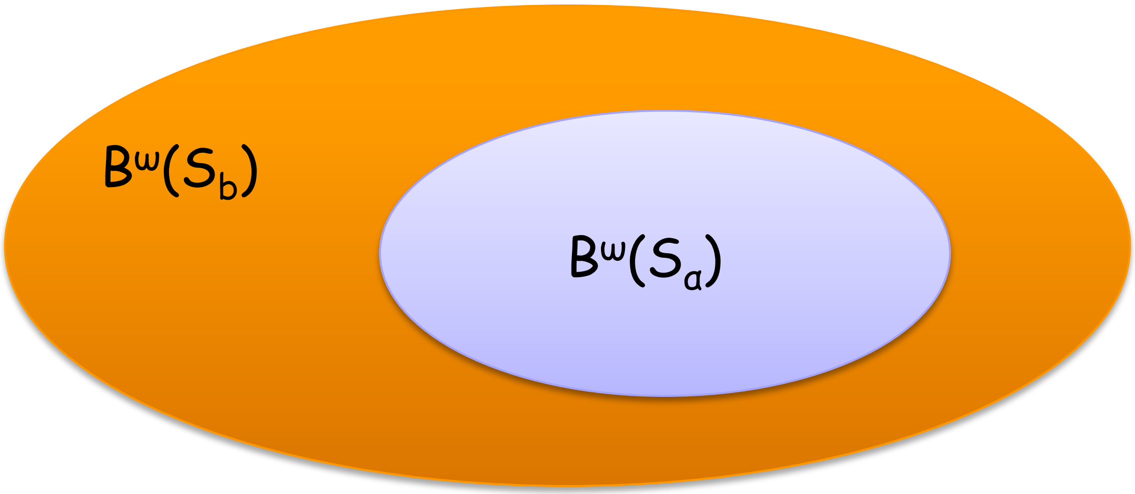
Arizona State University

fainekos at asu edu

http://www.public.asu.edu/~gfaineko

Last class: Verification

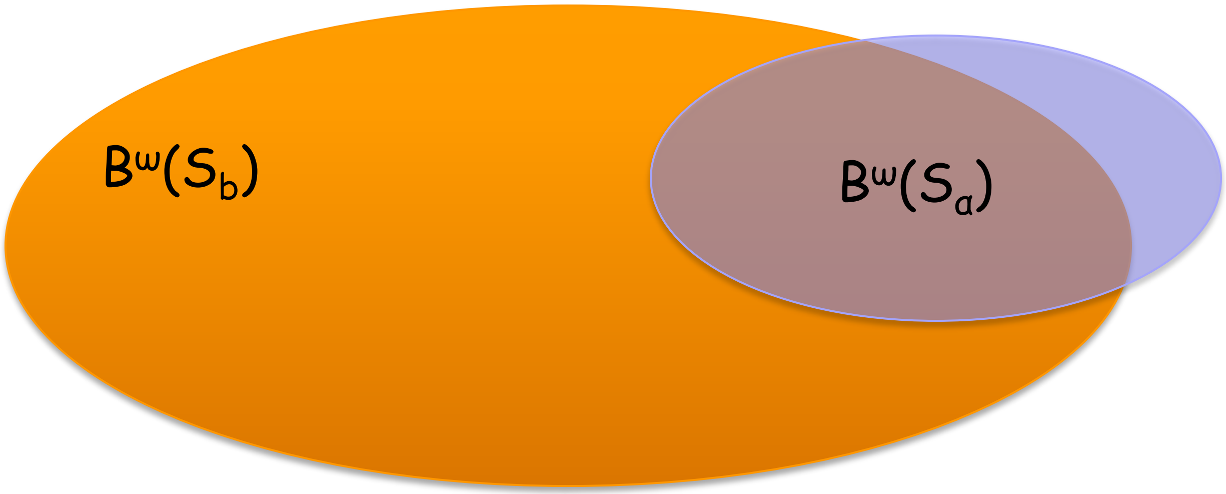
- Given a system S_a, find whether S_a satisfies the specification S_b



i.e. $S_a \preceq_B S_b$?

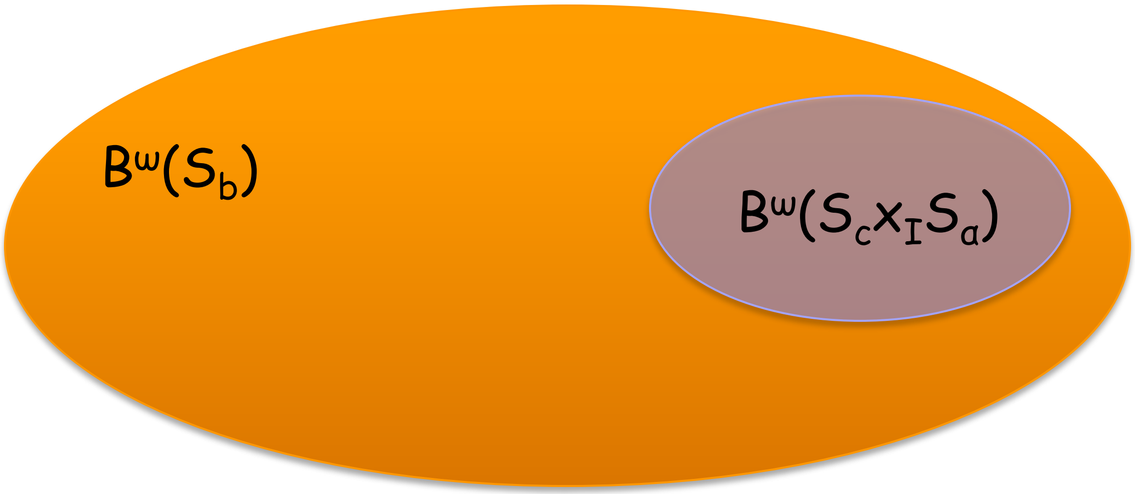
Verification

- What happens if $B^{\omega}(S_a) \not\subseteq B^{\omega}(S_b)$



Control

- Can we find a controller S_c such that $S_c x_I S_a \preceq S_b$



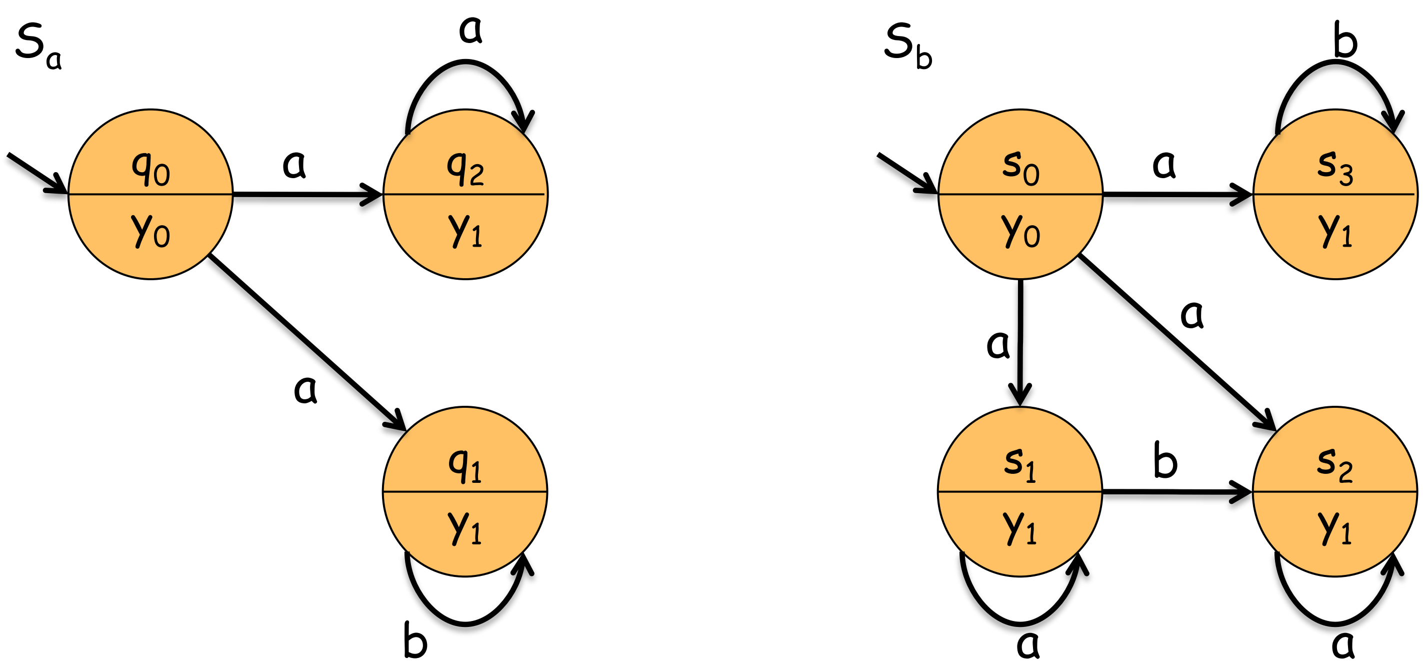
Review: Alternating Simulation

- Def. Let S_a, S_b with Y_a=Y_b. A relation $R \subseteq X_a x X_b$ is an **alternating simulation relation** from S_a to S_b if
  1. $\forall x_{a0} \in X_{a0}$. $\exists x_{b0} \in X_{b0}$. $(x_{a0}, x_{b0}) \in R$
  2. $\forall (x_a, x_b) \in R$. $H_a(x_a) = H_b(x_b)$
  3. $\forall (x_a, x_b) \in R$.
     $\forall u_a \in U_a(x_a)$. $\exists u_b \in U_b(x_b)$.
     $\forall x_b' \in Post_{ub}(x_b)$. $\exists x_a' \in Post_{ua}(x_a)$. $(x_a', x_b') \in R$

- Let R be an alternating simulation relation between S_a and S_b. The **extended alternating simulation relation** $R^e \subseteq X_a x X_b x U_a x U_b$ associated with R is defined by all $(x_a, x_b, u_a, u_b) \in X_a x X_b x U_a x U_b$ such that
  1. $(x_a, x_b) \in R$
  2. $u_a \in U_a(x_a)$
  3. $u_b \in U_b(x_b)$ and $\forall x_b' \in Post_{ub}(x_b)$. $\exists x_a' \in Post_{ua}(x_a)$. $(x_a', x_b') \in R$

Example 4.21

Alternating Simulation R' = $\{(q_0,s_0), (q_1,s_1), (q_1,s_2), (q_1,s_3)\}$



Feedback composition

- A system S_c is said to be feedback composable with a system S_a if there exists an alternating simulation relation R from S_c to S_a.

- When S_c is feedback composable with S_a, the feedback composition of S_c and S_a with interconnection relation

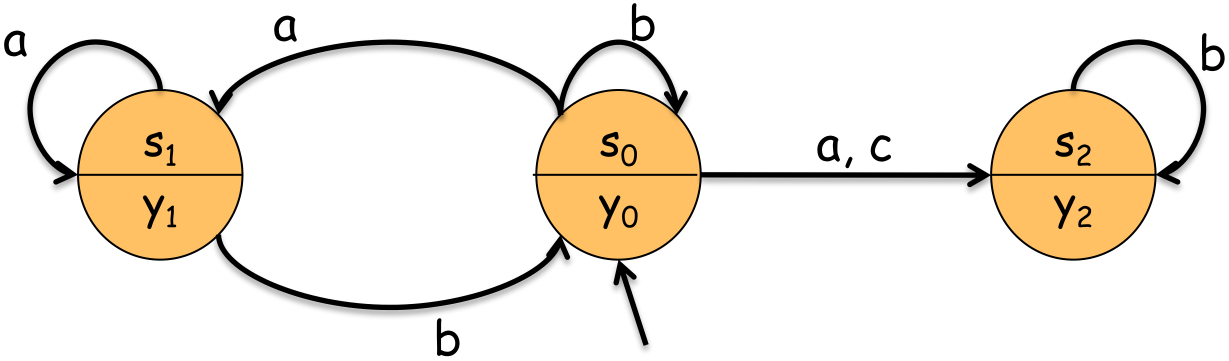
$$F = R^e$$

is given by

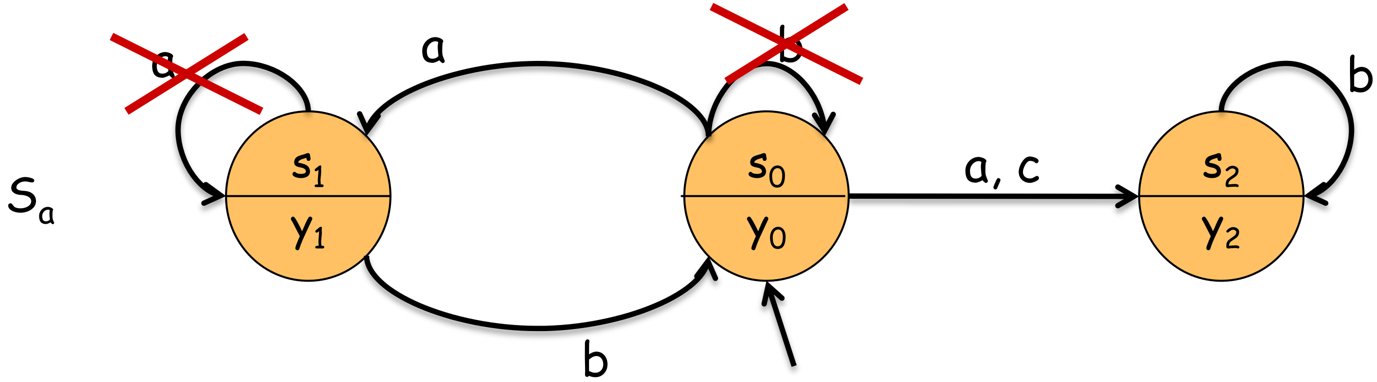
$$S_c x_F S_a$$

Example 6.2

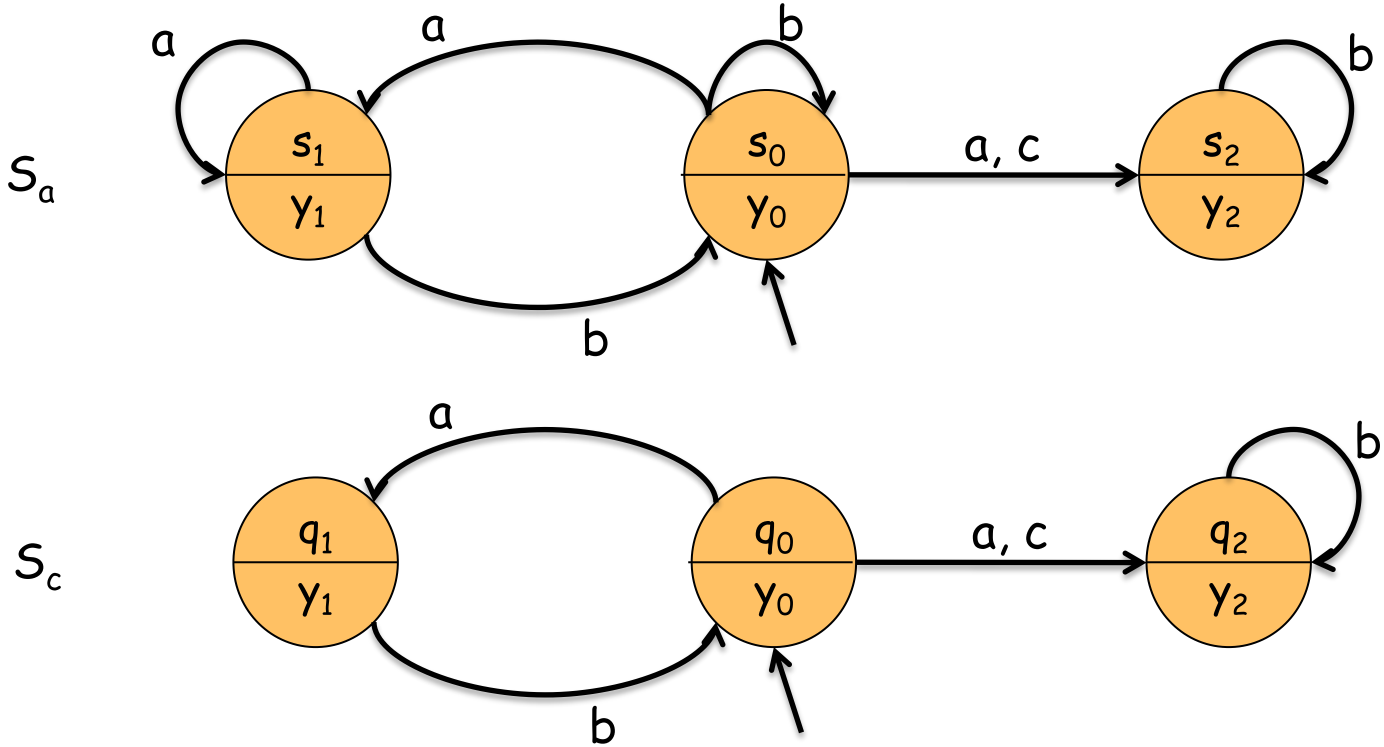
S_a



Example 6.2



Example 6.2



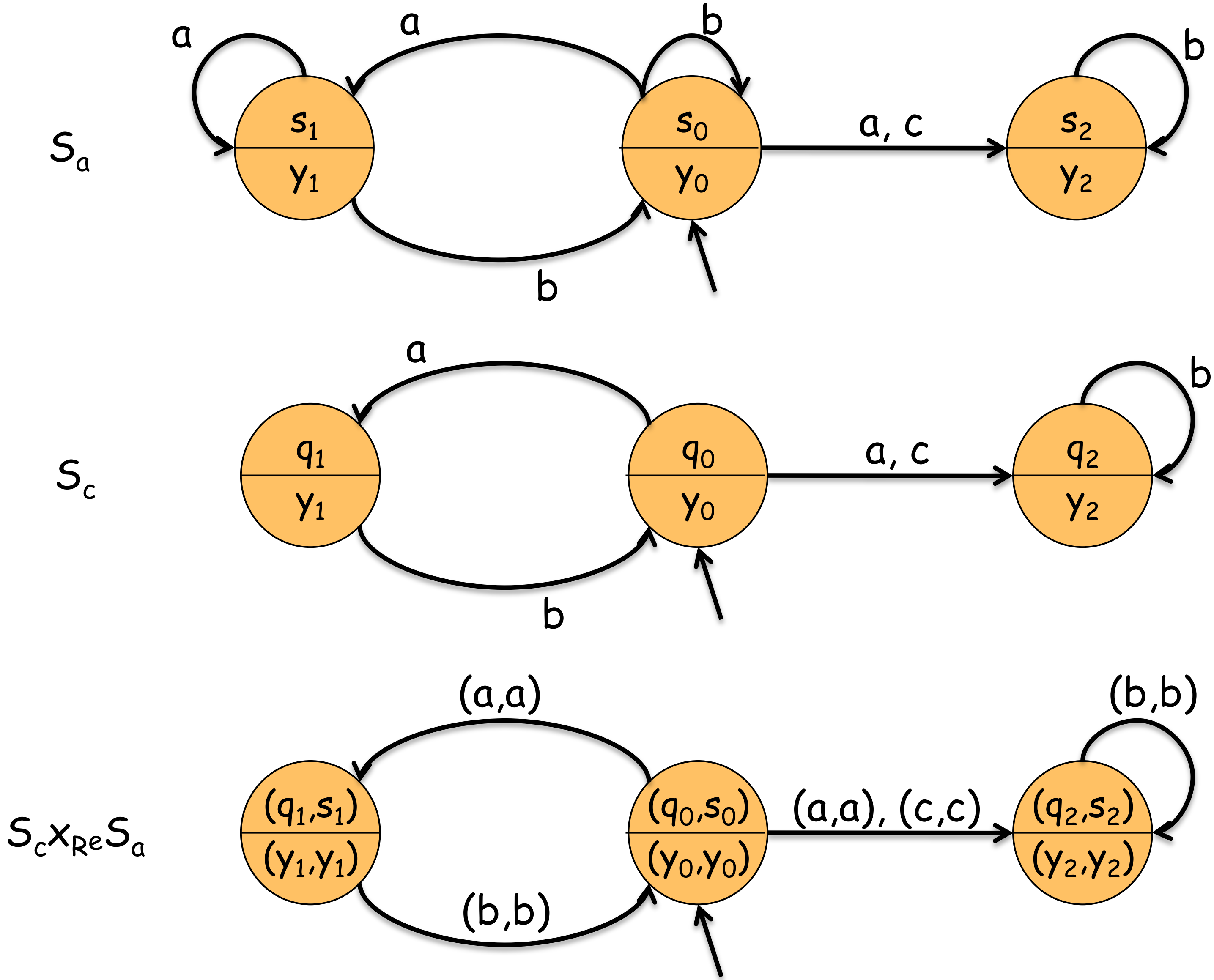
Alternating Simulation $R = \{(q_0,s_0), (q_1,s_1), (q_2,s_2)\}$

Extended: $R^e = \{(q_0,s_0,a,a), (q_0,s_0,c,c), (q_1,s_1,b,b), (q_2,s_2,b,b)\}$

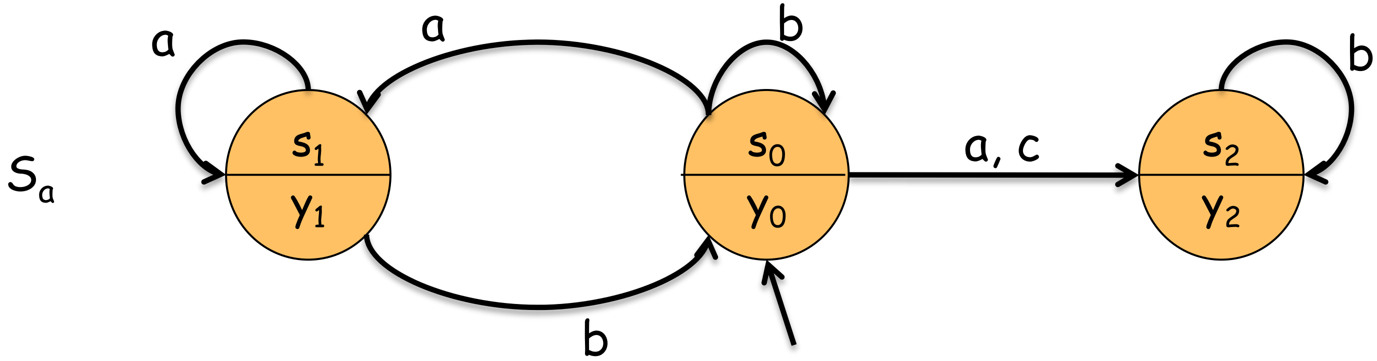
Review Composition

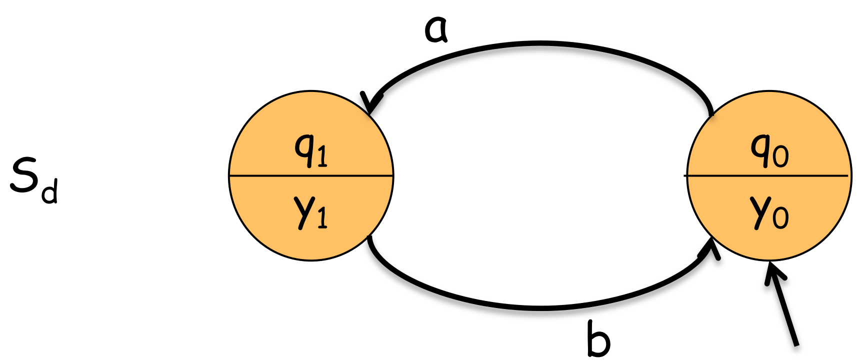
- **Def. II:** Let S_a, S_b and $I \subseteq X_a x X_b x U_a x U_b$. Then $S_a x_I S_b$
  1. $X_{ab} = \pi_X(I)$
  2. $X_{ab0} = X_{ab} \cap (X_{a0} \times X_{b0})$
  3. $U_{ab} = U_a \times U_b$
  4. $$(x_a, x_b) \xrightarrow[ab]{(u_a, u_b)} (x_a', x_b')$$
     1. $$x_a \xrightarrow[a]{u_a} x_a'$$
     2. $$x_b \xrightarrow[b]{u_b} x_b'$$
     3. $(x_a, x_b, u_a, u_b) \in I$
  5. $Y_{ab} = Y_a \times Y_b$
  6. $H_{ab}(x_a, x_b) = (H_a(x_a), H_b(x_b))$

Example 6.2


S_a
a
a
b
b
a, c
b
s_1
y_1
s_0
y_0
s_2
y_2
S_c
a
b
a, c
b
q_1
y_1
q_0
y_0
q_2
y_2
S_c x_Re S_a
(a,a)
(b,b)
(a,a), (c,c)
(b,b)
(q_1,s_1)
(y_1,y_1)
(q_0,s_0)
(y_0,y_0)
(q_2,s_2)
(y_2,y_2)

Example 6.2

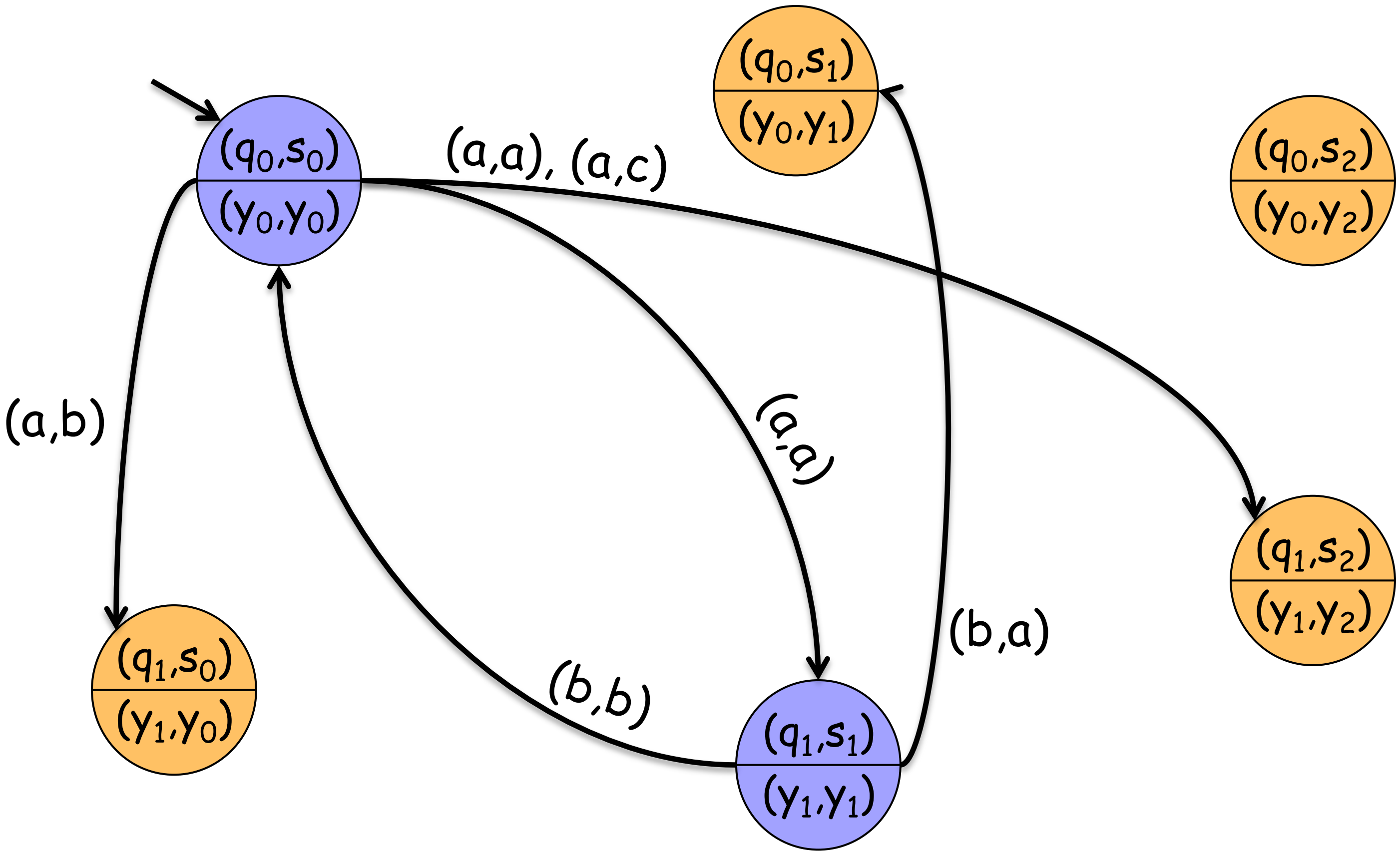




Simulation $R = \{(q_0,s_0), (q_1,s_1)\}$

$I = \{(x_d,x_a,u_d,u_a) \in X_c x X_a x U_c x U_a \mid (x_d,x_a) \in R\}$

Example 6.2



(q0,s0)
(y0,y0)
(a,a), (a,c)
(q0,s1)
(y0,y1)
(q0,s2)
(y0,y2)
(a,b)
(a,a)
(q1,s2)
(y1,y2)
(b,a)
(q1,s0)
(y1,y0)
(b,b)
(q1,s1)
(y1,y1)

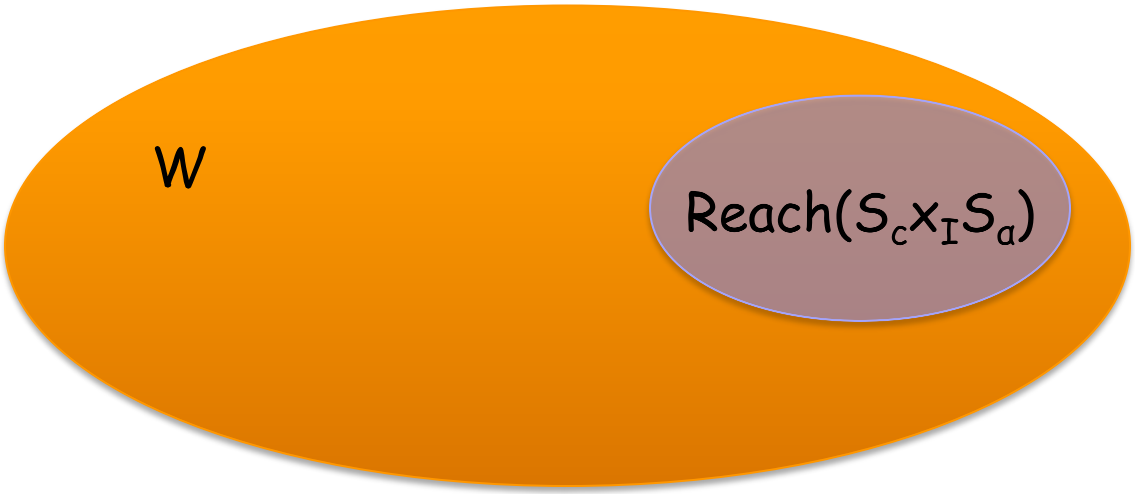
Simulation

- **Def:** Let S_a, S_b with $Y_a=Y_b$. A relation $R \subseteq X_a x X_b$ is a **simulation relation** from S_a to S_b if
  1. $\forall x_{a0} \in X_{a0} \,.\, \exists x_{b0} \in X_{b0} \,.\, (x_{a0}, x_{b0}) \in R$
  2. $\forall (x_a, x_b) \in R \,.\, H_a(x_a)=H_b(x_b)$
  3. $\forall (x_a, x_b) \in R \,.$

$$\mathbf{x_a} \xrightarrow[a]{u_a} \mathbf{x_a'} \text{ implies } \mathbf{x_b} \xrightarrow[b]{u_b} \mathbf{x_b'} \quad \text{satisfying } (x_a', x_b') \in R$$

Safety games

- Can we find a controler S_c such that
  1. $S_c x_F S_a$ is nonblocking
  2. $Reach(S_c x_F S_a) \subseteq W$



Safety game

- Lat S_a with $Y_a = X_a$ and $H_a = 1_{Xa}$ and $W \subseteq X_a$ be the set of safe states. Does it exist controller S_c s.t.
  1. S_c is feedback composable with S_a
  2. $S_c x_F S_a$ is nonblocking
  3. $\emptyset \neq B^\omega(S_c x_F S_a) \subseteq W^\omega$

- A safety game is solvable when S_c exists

Safety game

- Fixed-point operator $F_W : 2^X \to 2^X$:
  $F_W(Z) = \{x \in Z \mid x \in W \text{ and } \exists u \in U(x).\emptyset \neq Post_u(x) \subseteq Z\}$

- Proposition 6.5
  - F_W is order preserving
  - If the safety game is solvable, then any fixed-point $Z \neq \emptyset$ of F_W satisfies $Z \cap X_0 \neq \emptyset$

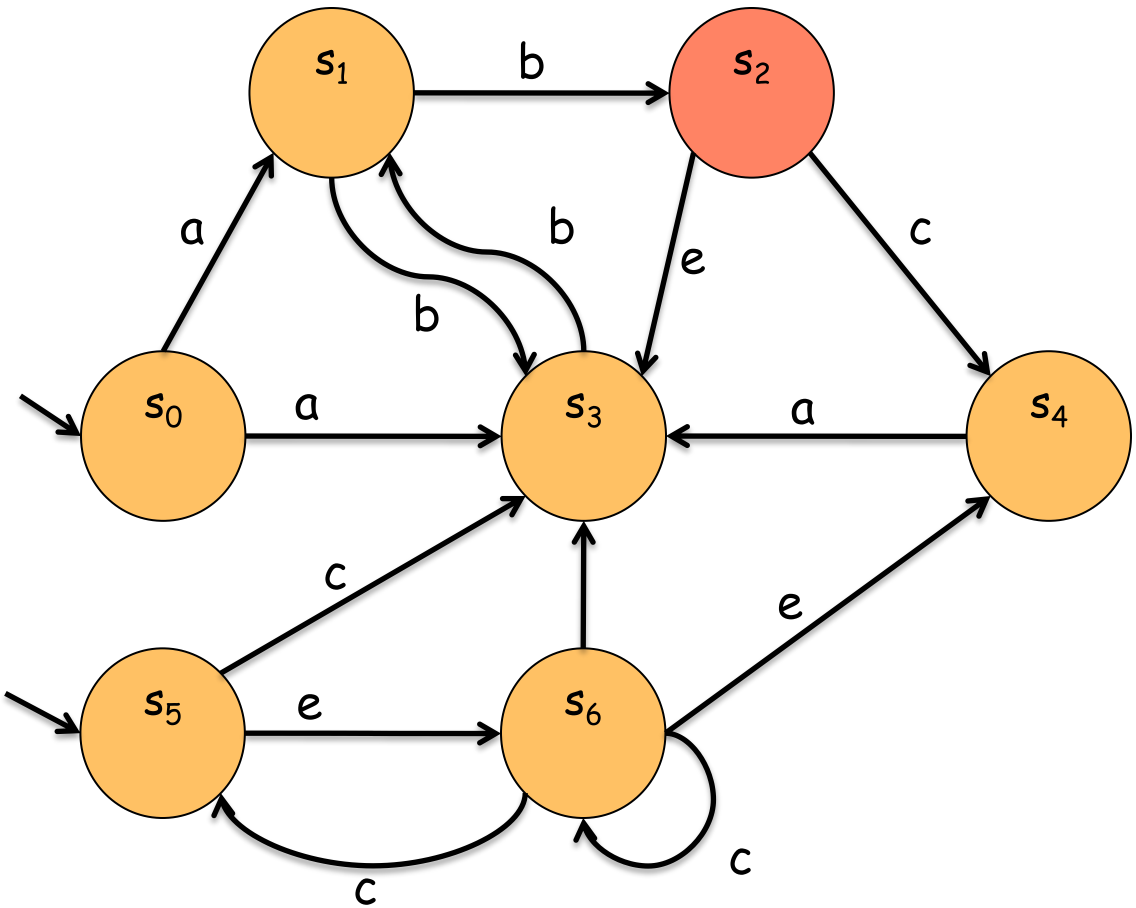
- Given a fixed-point Z of F_W, we can construct a controller

- Theorem 6.5
  A safety game with safe set W is solvable iff the greatest fixed-point Z of F_W satisfies $Z \cap X_0 \neq \emptyset$

$$Z = \lim_{i \to \infty} F^i_W(X)$$

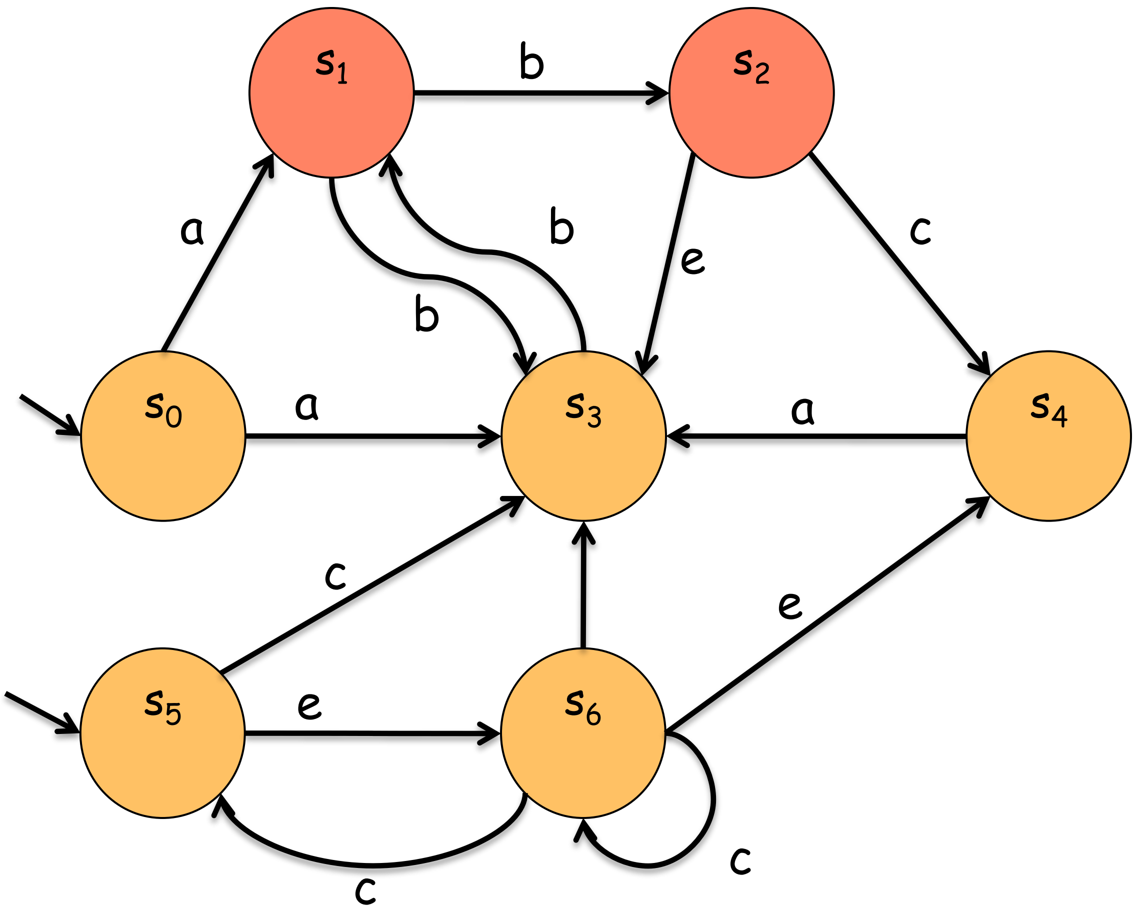
Example 6.7 - W = X_a-{s_2}

$F_W(X_a)$



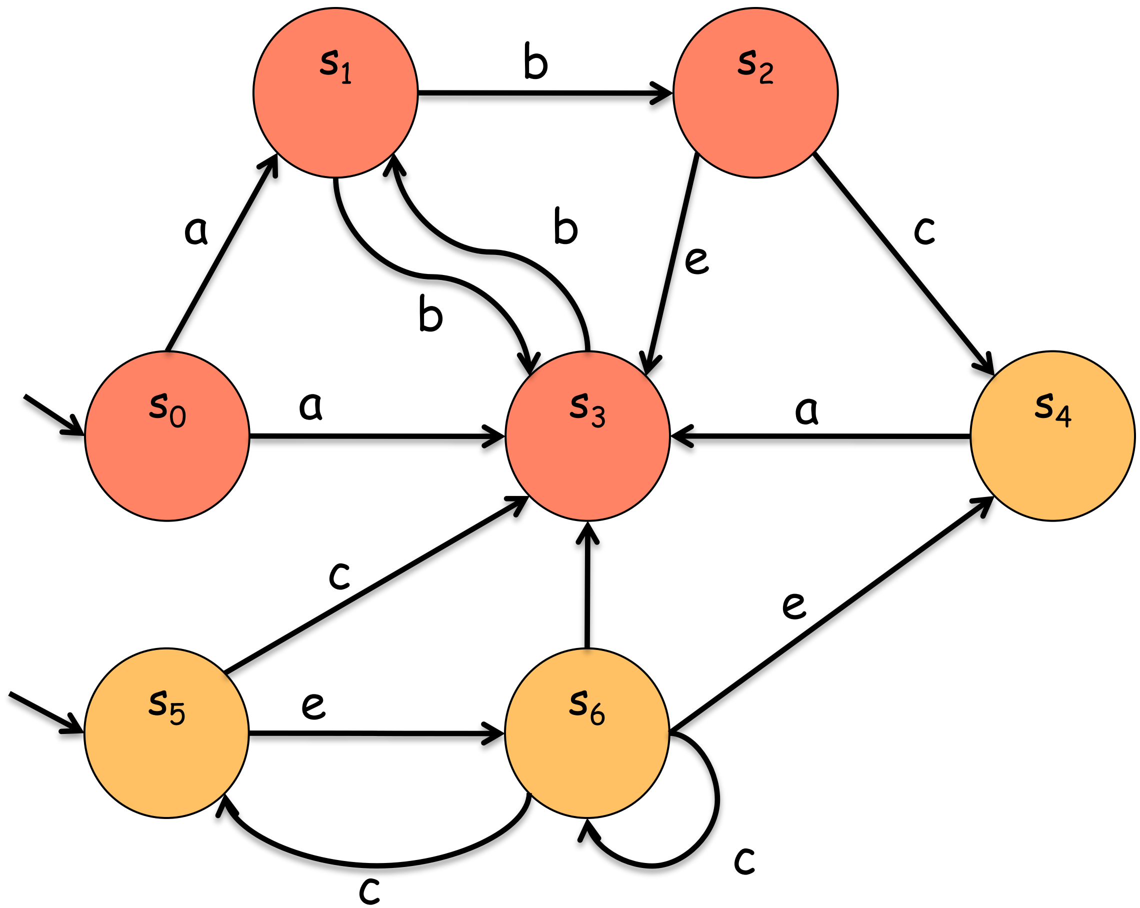
Example 6.7 - $W = X_a - \{s_2\}$

$F_W^2(X_a)$



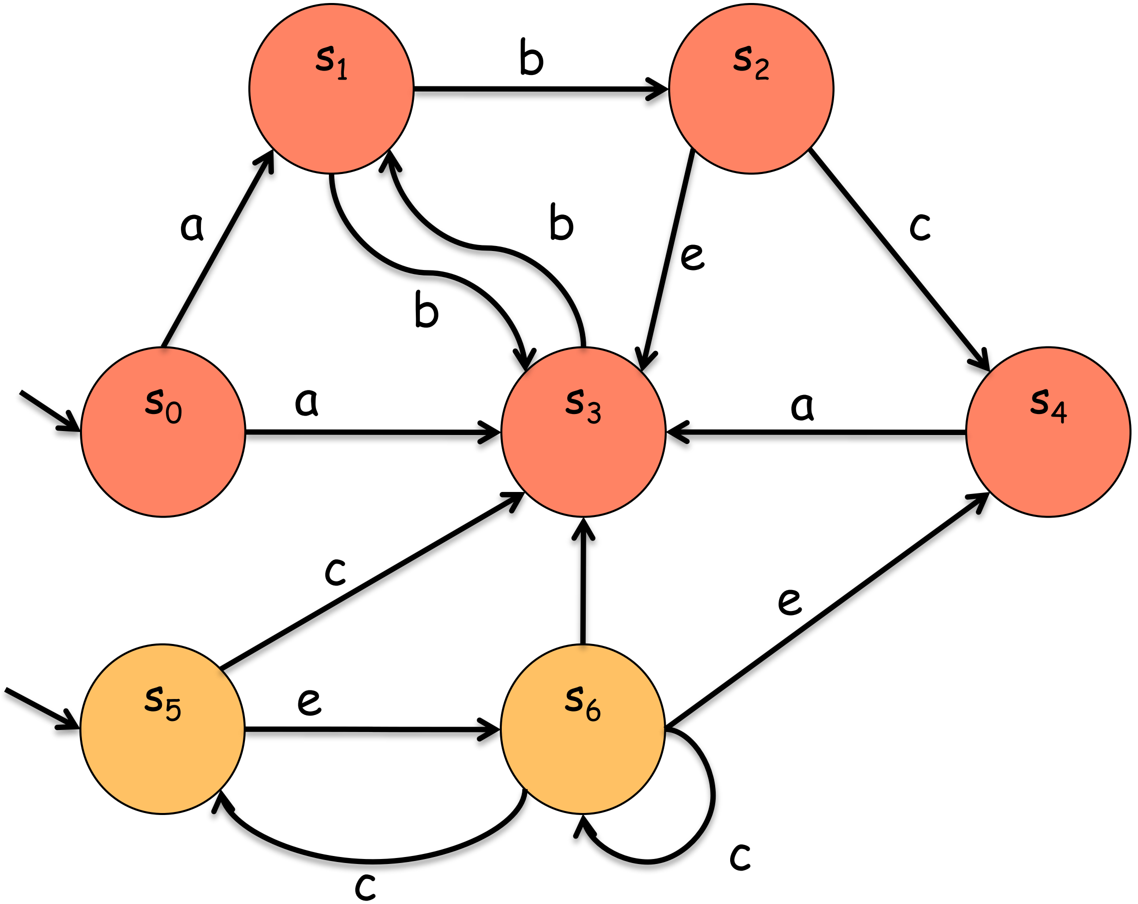
Example 6.7 - W = $X_a - \{s_2\}$

$F_W^3(X_a)$



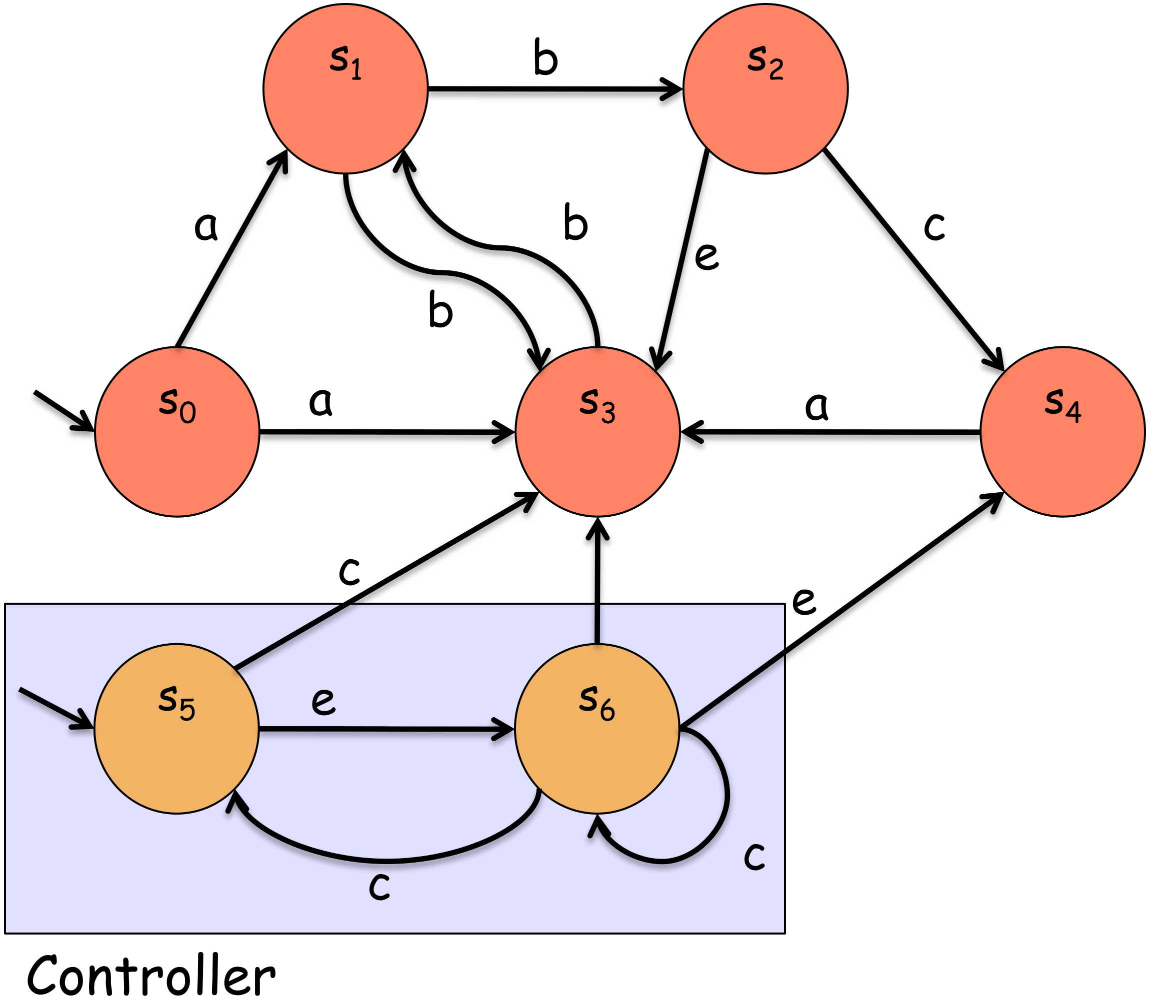
Example 6.7 - W = {s_2}

$F_W^4(X_a)$



Example 6.7 - W = X_a-{s_2}

$F_W^5(X_a)$



Final remarks

- Proposition 6.8:
  The controller determined by the greatest fixed-point is the least restrictive controller

- If S cannot be initialized, then we can replace $Z \cap X_0 \neq \emptyset$ with $X_0 \subseteq Z$

- If $Y \neq X$ and $H \neq 1_X$, then we can use as safe set $W' = H^{-1}(W)$

What is S_c for $W = X_a - \{s_0\}$?