# CSE 591: Theoretical Aspects of CPS

## Verification
## Reference: Tabuada Ch 5, Appendix A

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

# In the previous class

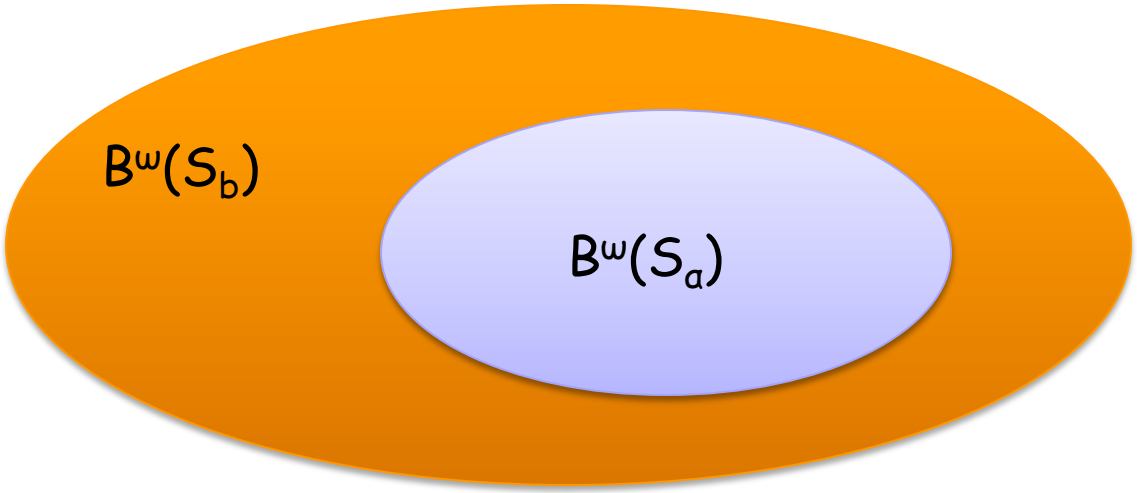


- Exact system relationships
  - Behavioral
  - Similarity
  - Alternating similarity

# This class: Verification



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




i.e. $S_a \preceq_B S_b$ ?

# How do we compute simulations?



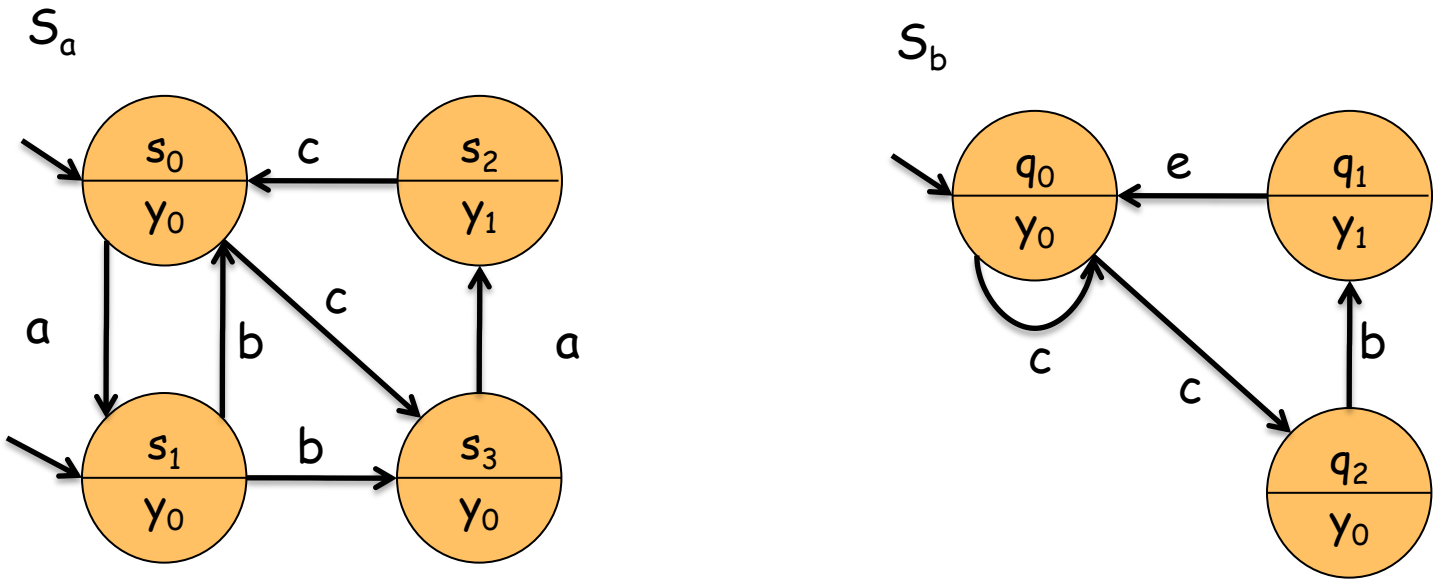
- **Def I:** Let $S_a$, $S_b$ with $Y_a=Y_b$. A relation $R \subseteq X_a \times X_b$ is a **simulation relation** from $S_a$ to $S_b$ if
  1. $\forall x_{a0} \in X_{a0} \,.\, \exists x_{b0} \in X_{b0} \,.\, (x_{a0}, x_{b0}) \in R$
  2. $\forall (x_a, x_b) \in R \,.\, H_a(x_a) = H_b(x_b)$
  3. $\forall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

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

- **Alg. I:** Let $S_a$, $S_b$ with $Y_a=Y_b$. Compute a sequence of relations $R_0$, $R_1$, $R_2$, … on $X_a \times X_b$ as
  i. $(x_a, x_b) \in R_0$ iff $H_a(x_a) = H_b(x_b)$
  ii. $(x_a, x_b) \in R_{n+1}$ iff
     a) $(x_a, x_b) \in R_n$
     b) For all $x_a \xrightarrow[a]{u_a} x_a'$ there exists $x_b \xrightarrow[b]{u_b} x_b'$ satisfying $(x_a', x_b') \in R_n$

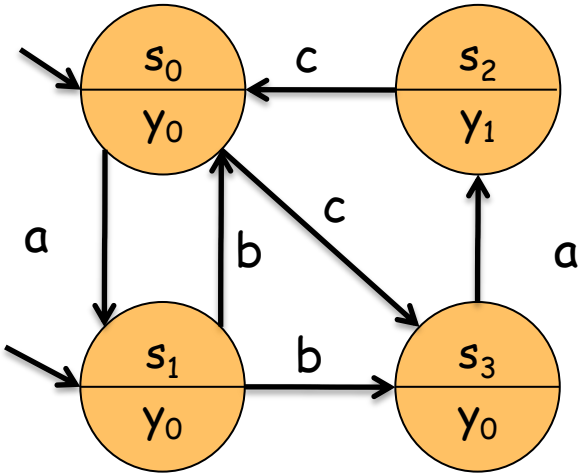
# Example 4.15

Bisimulation R = $\{(s_0,q_0), (s_1,q_0), (s_2,q_1), (s_3,q_2)\}$

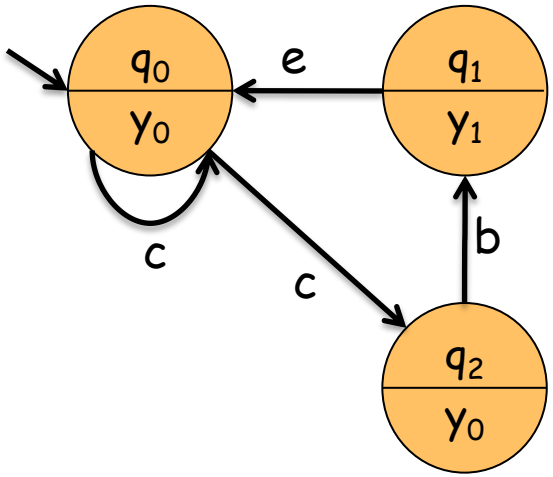


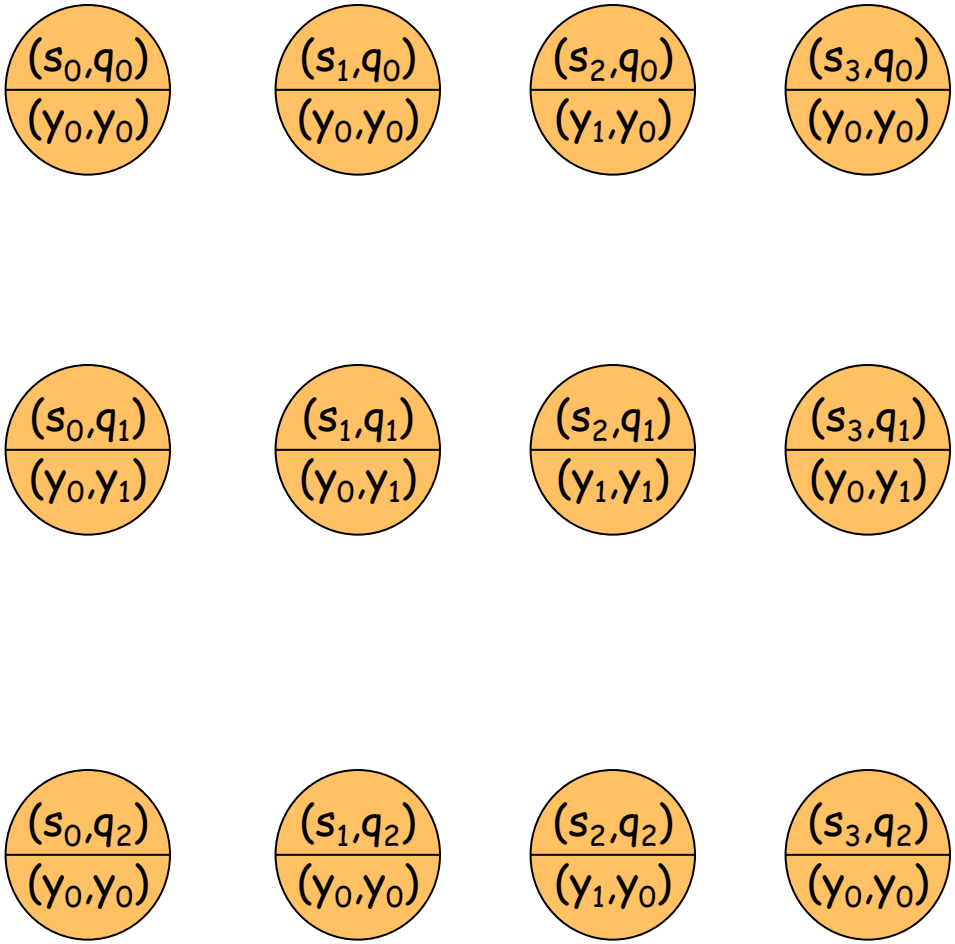
# Example 5.4 - $X_a \times X_b$

$S_a$



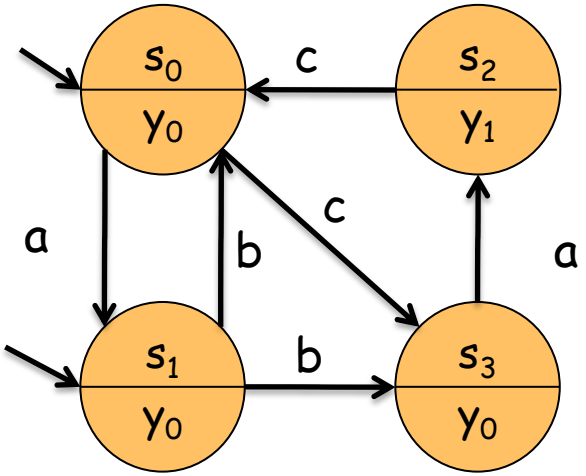

$S_b$



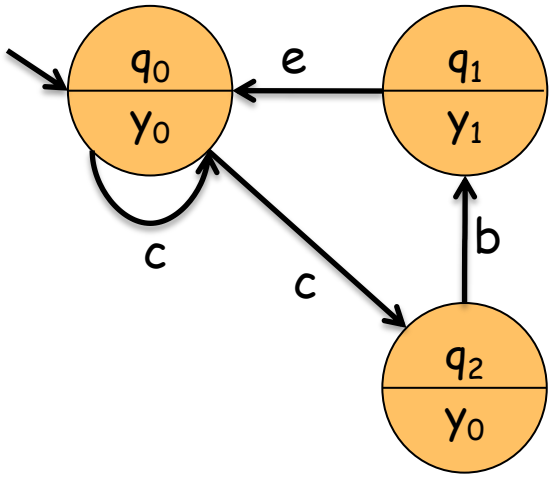



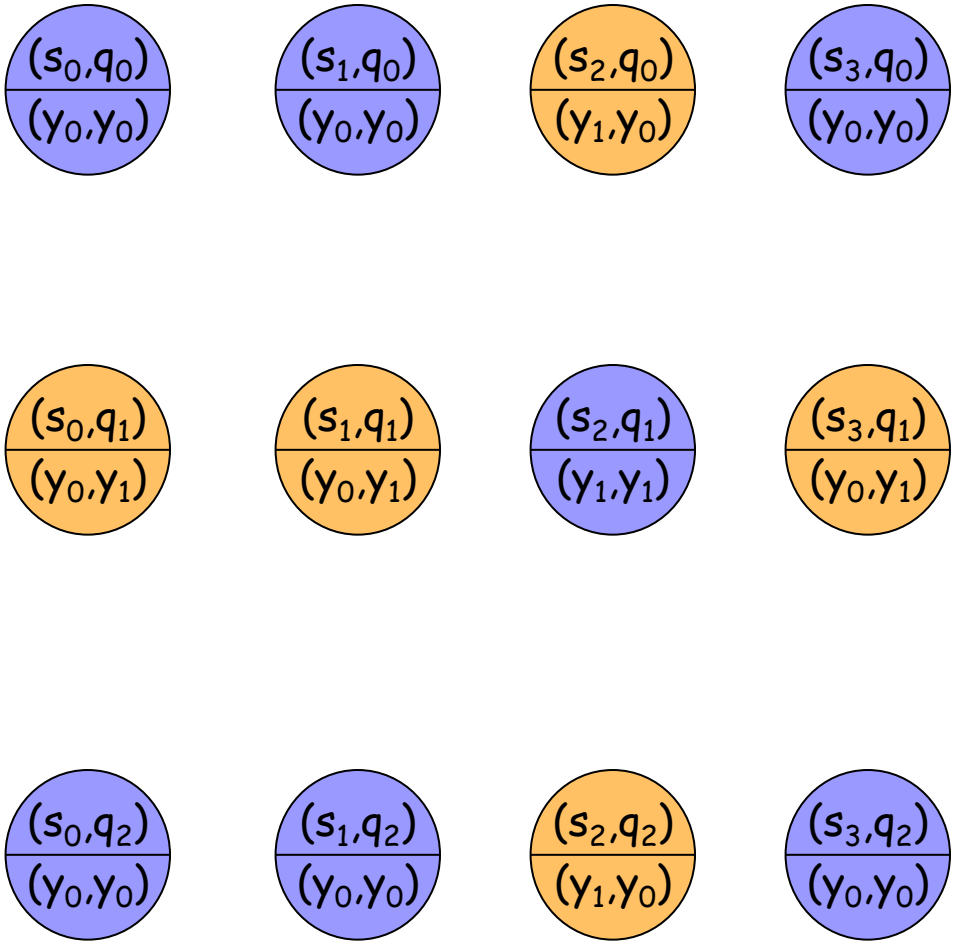
# $R_0$

$S_a$


s0
y0
c
s2
y1
a
b
c
a
s1
y0
b
s3
y0

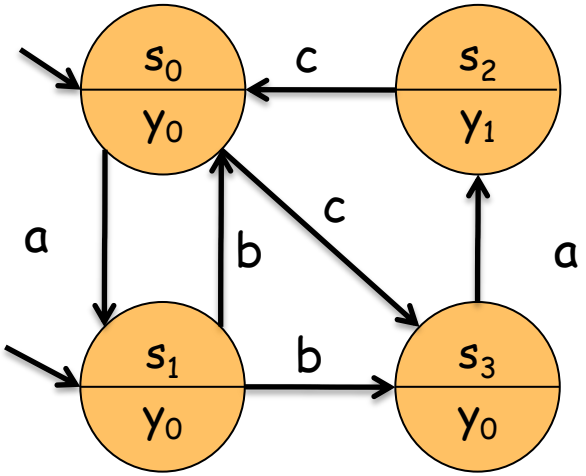
$S_b$


q0
y0
e
q1
y1
c
c
b
q2
y0

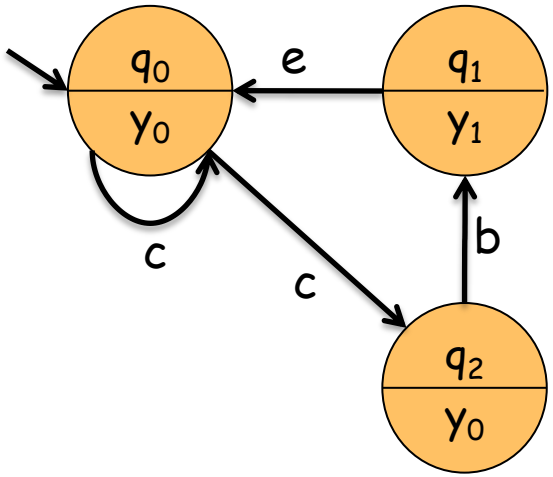

(s0,q0)
(y0,y0)
(s1,q0)
(y0,y0)
(s2,q0)
(y1,y0)
(s3,q0)
(y0,y0)
(s0,q1)
(y0,y1)
(s1,q1)
(y0,y1)
(s2,q1)
(y1,y1)
(s3,q1)
(y0,y1)
(s0,q2)
(y0,y0)
(s1,q2)
(y0,y0)
(s2,q2)
(y1,y0)
(s3,q2)
(y0,y0)

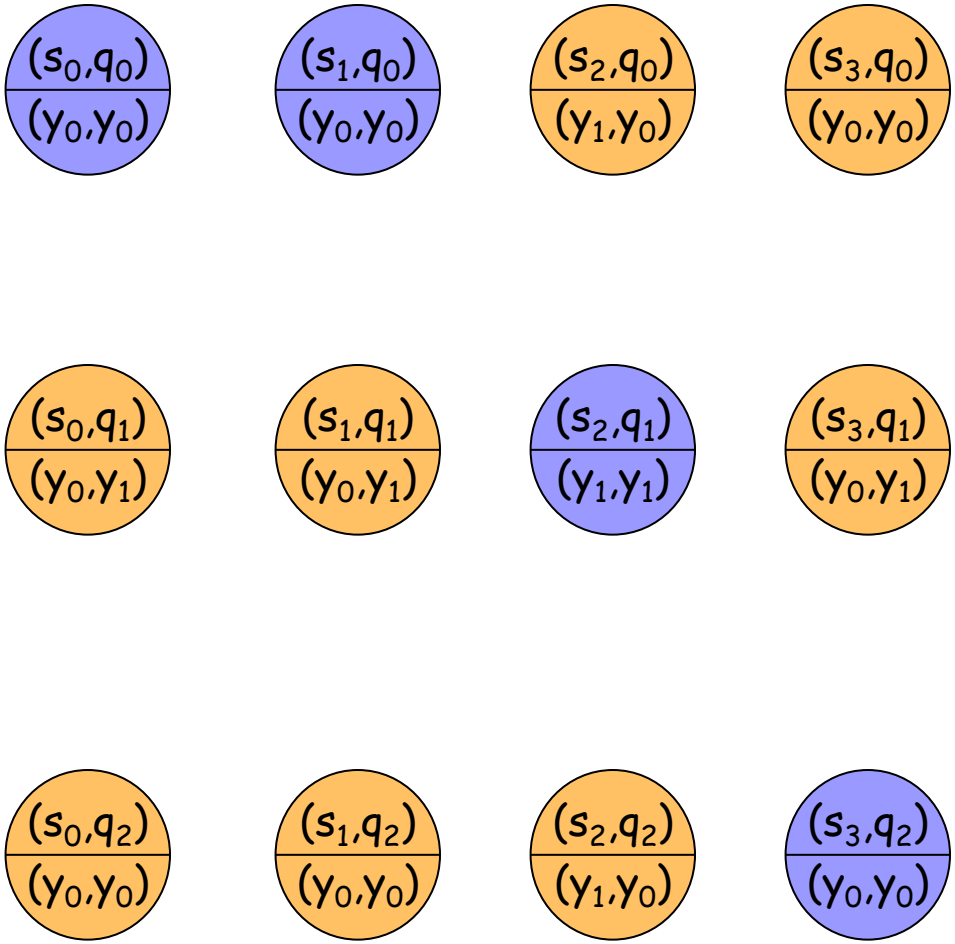
# $R_1$

$S_a$


s0
y0
c
s2
y1
a
b
c
a
s1
y0
b
s3
y0

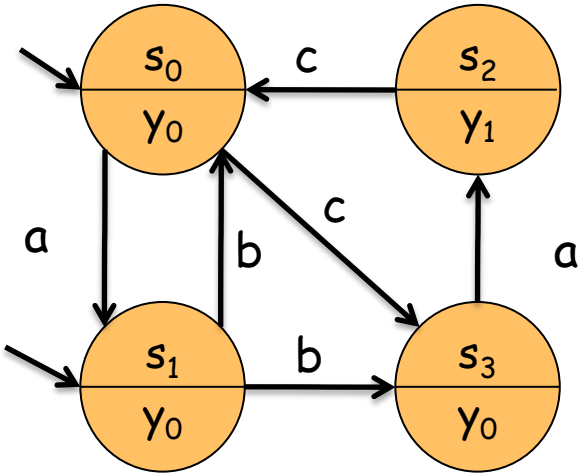
$S_b$


q0
y0
e
q1
y1
c
c
b
q2
y0

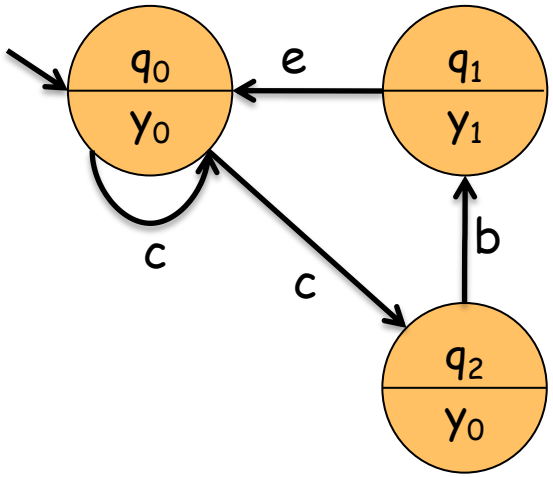

(s0,q0)
(y0,y0)
(s1,q0)
(y0,y0)
(s2,q0)
(y1,y0)
(s3,q0)
(y0,y0)
(s0,q1)
(y0,y1)
(s1,q1)
(y0,y1)
(s2,q1)
(y1,y1)
(s3,q1)
(y0,y1)
(s0,q2)
(y0,y0)
(s1,q2)
(y0,y0)
(s2,q2)
(y1,y0)
(s3,q2)
(y0,y0)

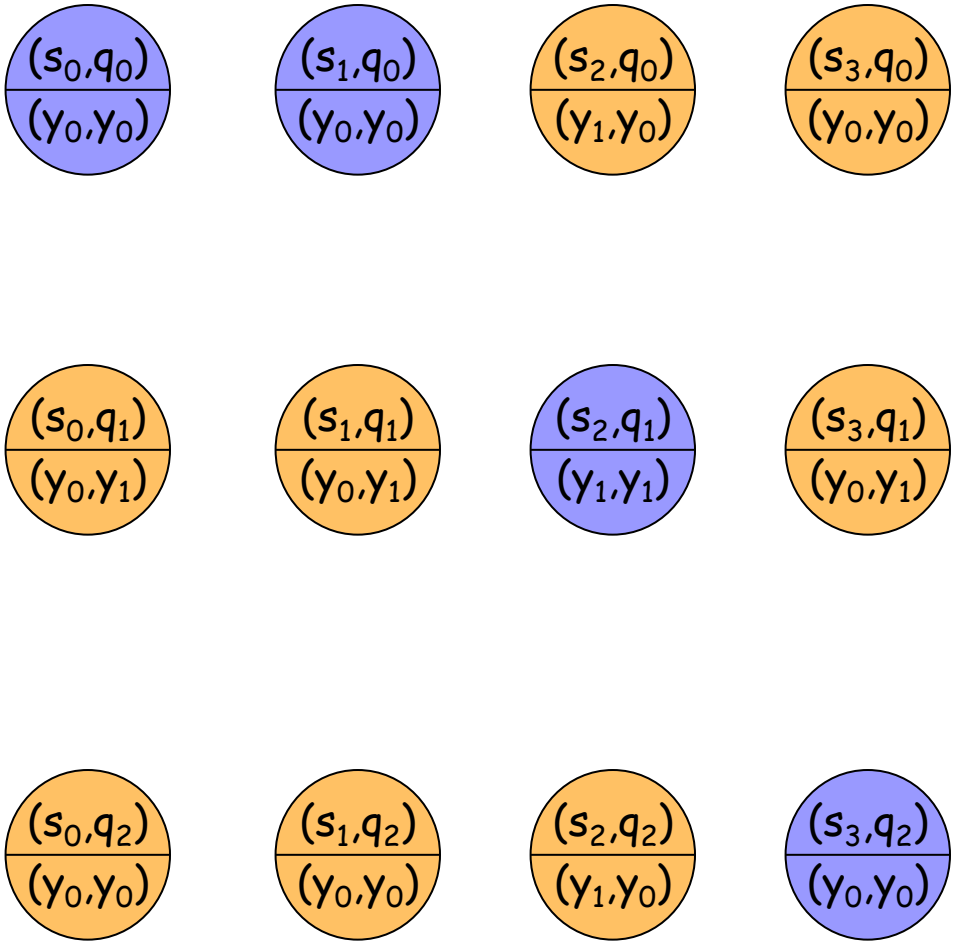
# $R_2$

$S_a$


s0
y0
c
s2
y1
a
b
c
a
s1
y0
b
s3
y0

$S_b$


q0
y0
e
q1
y1
c
c
b
q2
y0


(s0,q0)
(y0,y0)
(s1,q0)
(y0,y0)
(s2,q0)
(y1,y0)
(s3,q0)
(y0,y0)
(s0,q1)
(y0,y1)
(s1,q1)
(y0,y1)
(s2,q1)
(y1,y1)
(s3,q1)
(y0,y1)
(s0,q2)
(y0,y0)
(s1,q2)
(y0,y0)
(s2,q2)
(y1,y0)
(s3,q2)
(y0,y0)

# Bisimulation



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

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

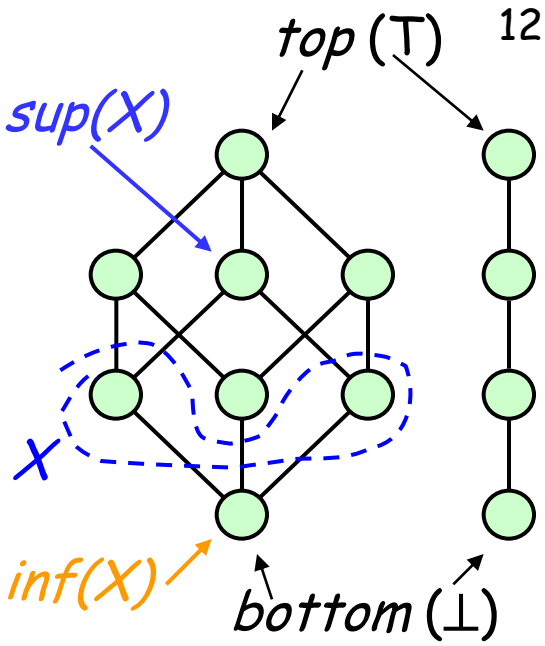
$$x_b \xrightarrow[b]{u_b} x_b' \text{ implies } x_a \xrightarrow[a]{u_a} x_a' \text{ satisfying } (x_a', x_b') \in R$$

# How do we compute bisimulations?

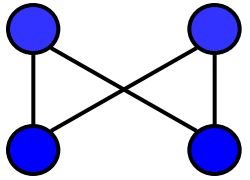


- **Alg II:** Let $S_a$, $S_b$ with $Y_a=Y_b$. Compute a sequence of relations $R_0, R_1, R_2, \ldots$ on $X_a \times X_b$ as
  - i. $(x_a,x_b)\in R_0$ iff $H_a(x_a)=H_b(x_b)$
  - ii. $(x_a,x_b)\in R_{n+1}$ iff
    - a) $(x_a,x_b)\in R_n$
    - b) For all $x_a \xrightarrow[a]{u_a} x_a'$ there exists $x_b \xrightarrow[b]{u_b} x_b'$ satisfying $(x_a',x_b')\in R_n$
    - c) For all $x_b \xrightarrow[b]{u_b} x_b'$ there exists $x_a \xrightarrow[a]{u_a} x_a'$ satisfying $(x_a',x_b')\in R_n$

# Ordering objects

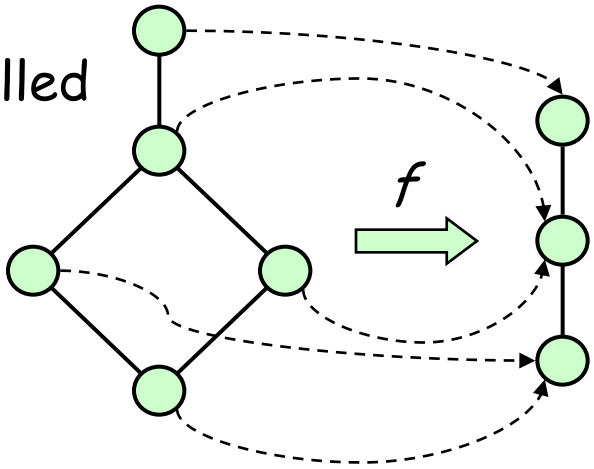



- A **partial-order** is a binary relation $\sqsubseteq$ such that for all $x,y,z \in S$ the following properties hold:
  - Reflexivity $x \sqsubseteq x$
  - Transitivity $x \sqsubseteq y$ and $y \sqsubseteq z$ imply $x \sqsubseteq z$
  - Antisymmetry $x \sqsubseteq y$ and $y \sqsubseteq x$ imply $x = y$
- A **poset** is the pair: $S=(S,\sqsubseteq)$
- In a **linear order** all the elements are comparable.



- Let $\mathcal{X}, \mathcal{Y}$ be posets, then a map $f : \mathcal{X} \to \mathcal{Y}$ is called **order-preserving** if:

$$(\forall x_1, x_2 \in X).(x_1 \sqsubseteq_X x_2 \rightarrow f(x_1) \sqsubseteq_Y f(x_2))$$



# Lattices

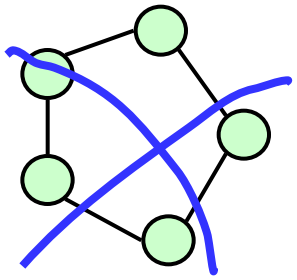
- Define **join** $\sqcup$ and **meet** $\sqcap$ as:

$$x \sqcup y := \sup(\{x, y\}) \text{ and } x \sqcap y := \inf(\{x, y\})$$

- **Lattice** $\mathcal{L}$ is a poset $(L, \sqsubseteq)$ where for all $x,y \in L$, $x \sqcap y$ and $x \sqcup y$ exist

- **Complete lattice** is a lattice where for all $X \subseteq L$, $\sqcap X$ and $\sqcup X$ exist

- **c-complete lattice** is a complete lattice with complement operator ~ such that $\sim\top = \bot$ and $\sim\bot = \top$



- A lattice is **distributive** iff it satisfies the distributive law

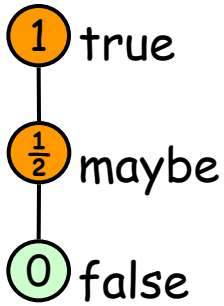
$$(\forall x, y, z \in L).(x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z))$$

- Let $\mathcal{X}, \mathcal{Y}$ be posets, then a map $f : \mathcal{X} \to \mathcal{Y}$ is called **continuous function** if for all non-empty directed sets $Z \subseteq X$:

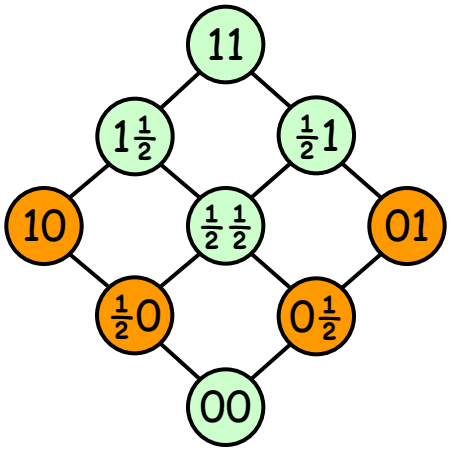
$$\sqcup f(Z) = f(\sqcup Z)$$

# Examples of lattices

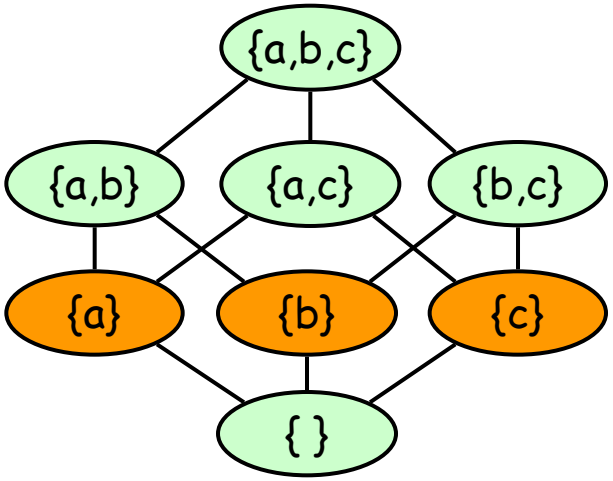
$\mathcal{B}_3=(\{0,\frac{1}{2},1\},\leq)$

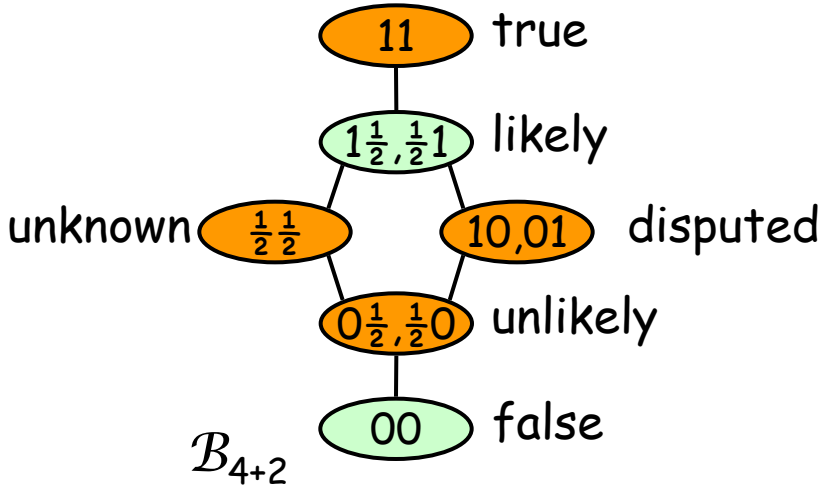



$\mathcal{B}_{3,3}=\mathcal{B}_3\times\mathcal{B}_3$

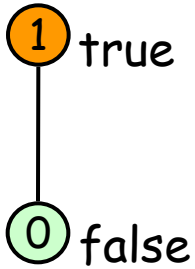



$B_S=(2^S,\subseteq)$, S={a,b,c}

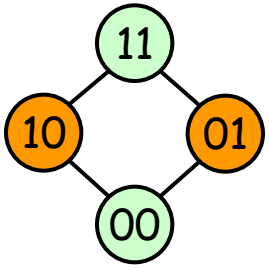



$B_2=(\{0,1\},\leq)$



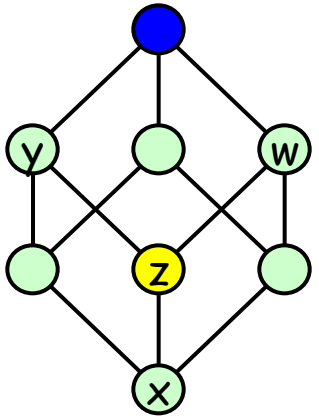

$B_{2,2}=B_2\times B_2$



# Some important lemmas

- The *join* and *meet* are order preserving functions, i.e. for all $x,y,z,w \in L$

$$x \sqsubseteq y \text{ and } z \sqsubseteq w \text{ imply } x \sqcup z \sqsubseteq y \sqcup w$$




- The connecting lemma, for $x,y \in L$

$$x \sqsubseteq y \text{ iff } x \sqcup y = y \text{ iff } x \sqcap y = x$$

- Every finite lattice is complete

- Every continuous function is order preserving

- If $\mathcal{X}, \mathcal{Y}$ are finite posets and $f: \mathcal{X} \to \mathcal{Y}$ is order preserving, then $f$ is continuous

# Tarski-Knaster Fixpoint Theorem

- Let L be a complete lattice and f : L → L be an order-preserving function, then f has fixpoints, i.e. f(x) = x. The least and greatest fixpoints are characterized as follows:

$$\mu x.f(x) = \bigsqcap\{x \in L \mid f(x) = x\} = \bigsqcap\{x \in L \mid f(x) \sqsubseteq x\}$$

$$\nu x.f(x) = \bigsqcup\{x \in L \mid f(x) = x\} = \bigsqcup\{x \in L \mid x \sqsubseteq f(x)\}$$

- Let y, z in L such that $y \sqsubseteq f(y)$, $y \sqsubseteq \mu x.f(x)$, $f(z) \sqsubseteq z$, $\nu x.f(x) \sqsubseteq z$ and, let f to be continuous, then the iteration:

$y_i$ defined as $y_0 := y$ and $y_{i+1} := f(y_i)$ converges to $\mu x.f(x)$
$z_i$ defined as $z_0 := z$ and $z_{i+1} := f(z_i)$ converges to $\nu x.f(x)$

# Proposition 5.2

- The operator $F : 2^{Xa \times Xb} \rightarrow 2^{Xa \times Xb}$ satisfies:
  1. $Z \subseteq Z' \Longrightarrow F(Z) \subseteq F(Z')$ i.e. F is order preserving
  2. $R \subseteq X_a \times X_b$ is a simulation relation from $S_a$ to $S_b$ iff $R \; F(R)$ and $X_{a0} \subseteq \pi_a(R \cap (X_{a0} \times X_{b0}))$

- (Theorem 5.3) Since F is order preserving and $2^{Xa \times Xb}$ is a finite complete lattice by the Tarski-Knaster Fixpoint Theorem has a least and a greatest fixpoint.