Formal methods in software developmen

a.y.2017/2018

Prof. Anna Labella

Partially ordered sets

A binary relation $\sqsubseteq$ on a set D is a *partial order* iff it is

reflexive: $\forall d \in D.\ d \sqsubseteq d$

transitive: $\forall d, d', d'' \in D.\ d \sqsubseteq d' \sqsubseteq d'' \Rightarrow d \sqsubseteq d''$

anti-symmetric: $\forall d, d' \in D.\ d \sqsubseteq d' \sqsubseteq d \Rightarrow d = d'$.

Such a pair $(D, \sqsubseteq)$ is called a *partially ordered set*, or *poset*.

see dens.pdf

Cpo's and domains

A *chain complete poset*, or *cpo* for short, is a poset $(D, \sqsubseteq)$ in which all countable increasing chains $d_0 \sqsubseteq d_1 \sqsubseteq d_2 \sqsubseteq \ldots$ have least upper bounds, $\bigsqcup_{n \geq 0} d_n$:

(lub1) $$\forall m \geq 0 \,.\, d_m \sqsubseteq \bigsqcup_{n \geq 0} d_n$$

(lub2) $$\forall d \in D \,.\, (\forall m \geq 0 \,.\, d_m \sqsubseteq d) \Rightarrow \bigsqcup_{n \geq 0} d_n \sqsubseteq d.$$

A *domain* is a cpo that possesses a least element, $\bot$:

$$\forall d \in D \,.\, \bot \sqsubseteq d.$$

Domain of partial functions, $X \rightharpoonup Y$

Underlying set: all partial functions, f, with domain of definition $dom(f) \subseteq X$ and taking values in Y.

Partial order: $f \sqsubseteq g$ iff $dom(f) \subseteq dom(g)$ and $\forall x \in dom(f).\ f(x) = g(x)$.

Lub of chain $f_0 \sqsubseteq f_1 \sqsubseteq f_2 \sqsubseteq \ldots$ is the partial function f with $dom(f) = \bigcup_{n \geq 0} dom(f_n)$ and

$$f(x) = \begin{cases} f_n(x) & \text{if } x \in dom(f_n), \text{ some } n \\ \text{undefined} & \text{otherwise} \end{cases}$$

Least element $\perp$ is the totally undefined partial function.

Monotonicity, continuity, strictness

- A function $f : D \to E$ between posets is *monotone* iff $\forall d, d' \in D.\ d \sqsubseteq d' \Rightarrow f(d) \sqsubseteq f(d')$.
- If D and E are cpo's, the function f is *continuous* iff it is monotone and preserves lubs of chains, i.e. for all chains $d_0 \sqsubseteq d_1 \sqsubseteq \ldots$ in D, it is the case that

$$f(\bigsqcup_{n\geq 0} d_n) = \bigsqcup_{n\geq 0} f(d_n) \quad \text{in } E.$$

- If D and E have least elements, then the function f is *strict* iff $f(\bot) = \bot$.

Least pre-fixed points

Let D be a poset and $f : D \to D$ be a function.

An element $d \in D$ is a *pre-fixed point of* f if it satisfies $f(d) \sqsubseteq d$.

The least pre-fixed point of f, if it exists, will be written

$$\boxed{fix(f)}$$

It is thus (uniquely) specified by the two properties:

(lfp1) $\quad f(fix(f)) \sqsubseteq fix(f)$

(lfp2) $\quad \forall d \in D.\ f(d) \sqsubseteq d \ \Rightarrow\ fix(f) \sqsubseteq d.$

Proposition 2.2.1. *Suppose D is a poset and $f : D \to D$ is a function possessing a least pre-fixed point, $fix(f)$* Provided f is monotone, $fix(f)$ *is in particular a fixed point for f (and hence is the least element of the set of fixed points for f).*

Proof. By definition, $fix(f)$ satisfies property (lfp1) If f is monotone we can apply f to both sides of (lfp1) to conclude that

$$f(f(fix(f))) \sqsubseteq f(fix(f)).$$

Then applying property (lfp2) with $d = f(fix(f))$, we get that

$$fix(f) \sqsubseteq f(fix(f)).$$

Combining this with (lfp1) and the anti-symmetry property of the partial order $\sqsubseteq$, we get $f(fix(f)) = fix(f)$, as required. $\square$

Tarski's Fixed Point Theorem

Let $f : D \to D$ be a continuous function on a domain D. Then

- f possesses a least pre-fixed point, given by

$$\mathit{fix}(f) = \bigsqcup_{n \geq 0} f^n(\bot).$$

- Moreover, $\mathit{fix}(f)$ is a fixed point of f, i.e. satisfies $f(\mathit{fix}(f)) = \mathit{fix}(f)$, and hence is the *least fixed point* of f.

Tarski's Fixed Point Theorem

Let $f : D \rightarrow D$ be a continuous function on a domain D. Then

- f possesses a least pre-fixed point, given by

$$\mathit{fix}(f) = \bigsqcup_{n \geq 0} f^n(\perp).$$

- Moreover, $\mathit{fix}(f)$ is a fixed point of f, i.e. satisfies $f(\mathit{fix}(f)) = \mathit{fix}(f)$, and hence is the *least fixed point* of f.

Proof

$$\perp \subseteq f(\perp) \subseteq f^2(\perp) \subseteq f^3(\perp) \ldots\ldots\ldots\ldots \bigcup f^i(\perp)$$

$$f\left(\bigcup f^i(\perp)\right) = \bigcup f^{i+1}(\perp)$$

Given another fixpoint g, we have the constant chain

$$\subseteq g \subseteq g \subseteq g \ldots\ldots\ldots\ldots \bigcup g = g$$

greater than the first one step by step, hence

$$\bigcup f^i(\perp) \subseteq g$$

- We could start from the maximum and compute the maximal fixpoint using the duality of order

- We can use minimum/ maximum fixed point to solve recursive equations like

Ex: $x = ax + b$

If we do not have inverse operations, we have to use approximation as we do in the case of formal languages

$\emptyset$

$\{b\}$

$\{ab, b\}$

$\{a^2b, ab, b\}$.....

Fixed point theorem: an example

- A fixed point x for a function f: $\wp(S) \rightarrow \wp(S)$ is an element of $\wp(S)$ such that $f(x) = x$

- We will give an interpretation of CTL operators using fixed points

Fixed point theorem: an example

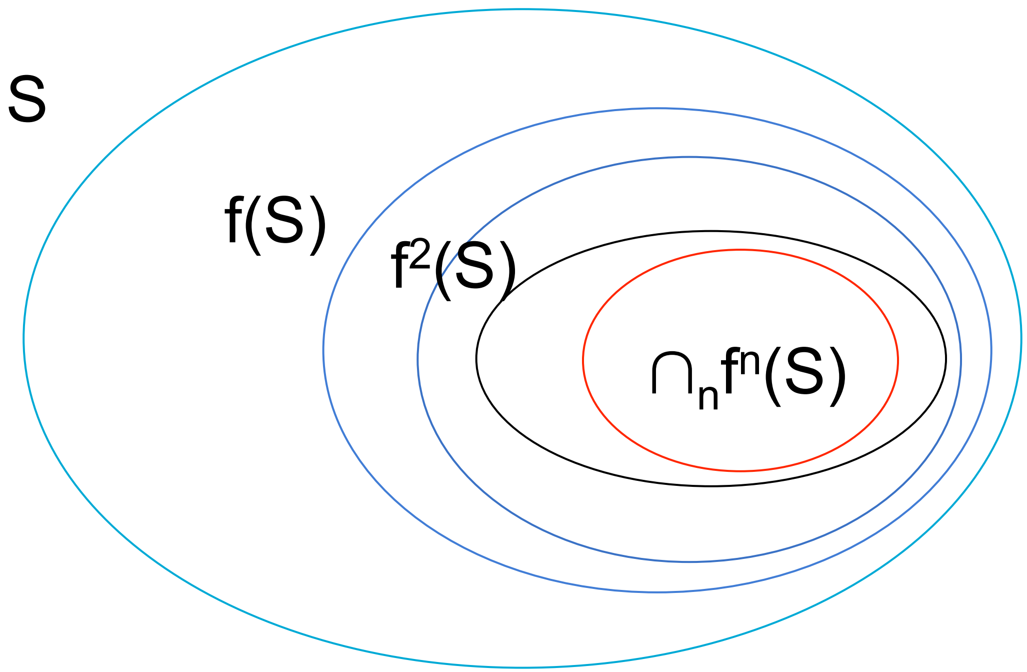
- Let S be a set (of states) of a transition system K and

f: $\wp(S) \rightarrow \wp(S)$ a monotonic function w.r.t. $\subseteq$, then f has a minimal and a maximal fixpoint

$\cup_n f^n(\emptyset)$ and $\cap_n f^n(S)$, respectively

Fixed point theorem (Tarski)

Let S be a set (of states) and
f: $\wp$(S)$\rightarrow$ $\wp$(S) a monotonic function w.r.t. $\subseteq$,
Starting from S the maximal fixpoint of f is:

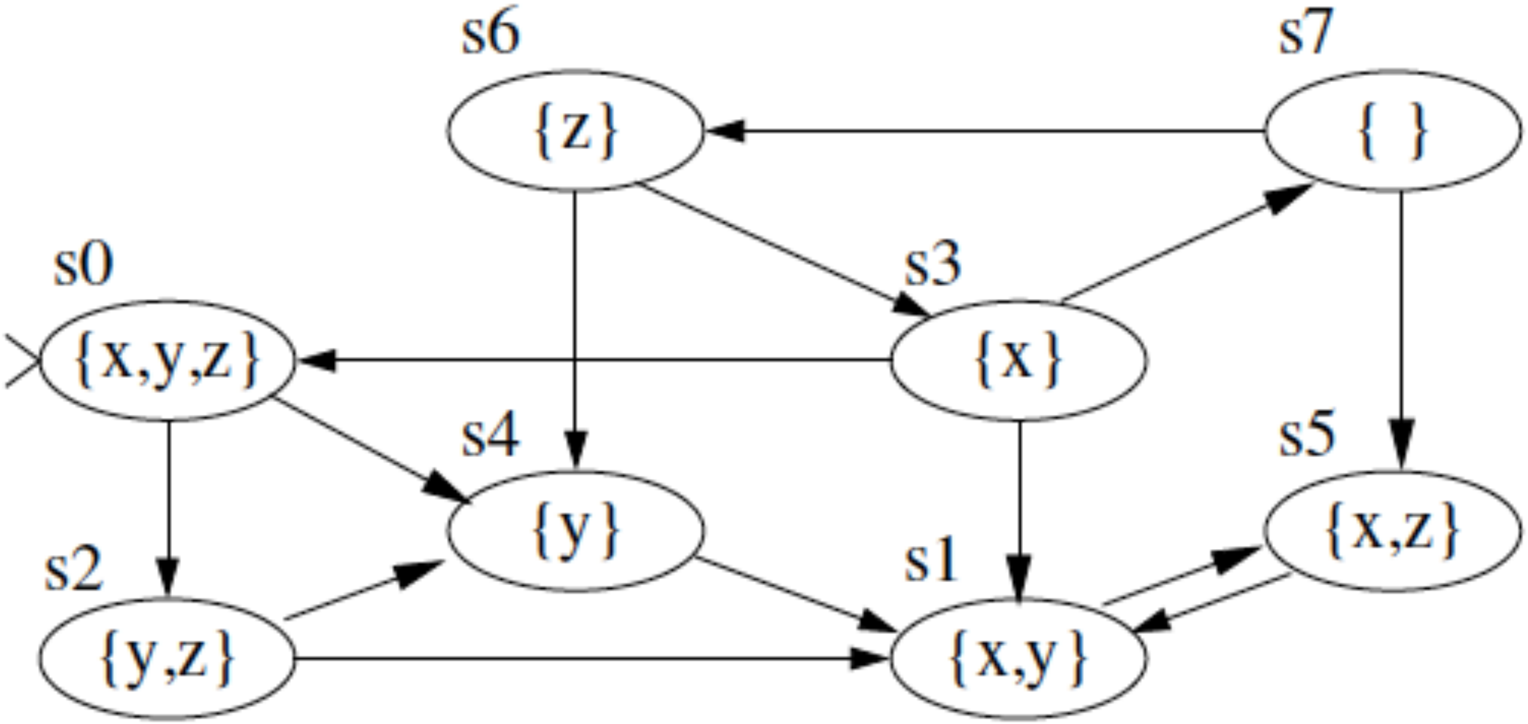


Looking for a semantic for CTL

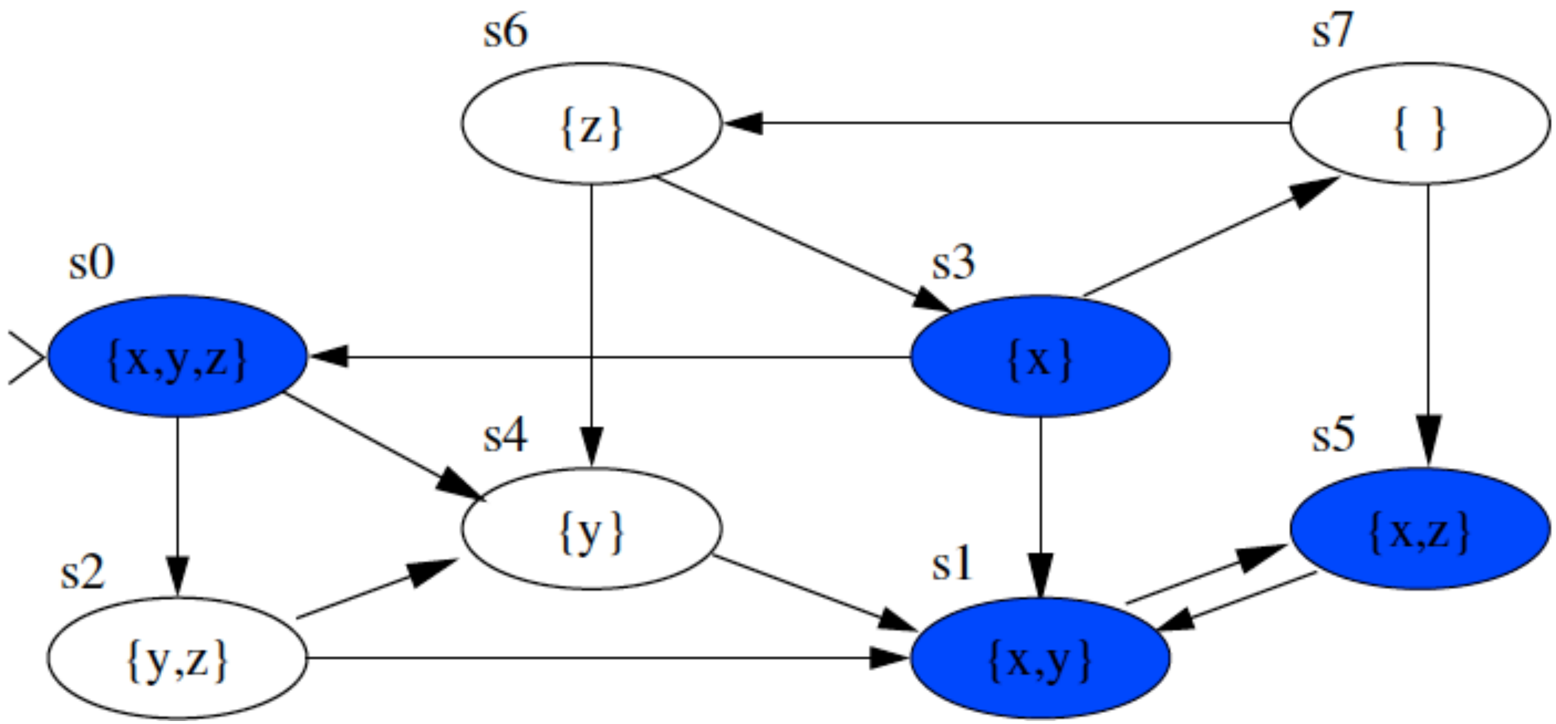
We have to find the set of states satisfying a formula φ, symbolically, $S_K(\phi)$ or $\|[\phi]\|$.

Let us start with a simple example:

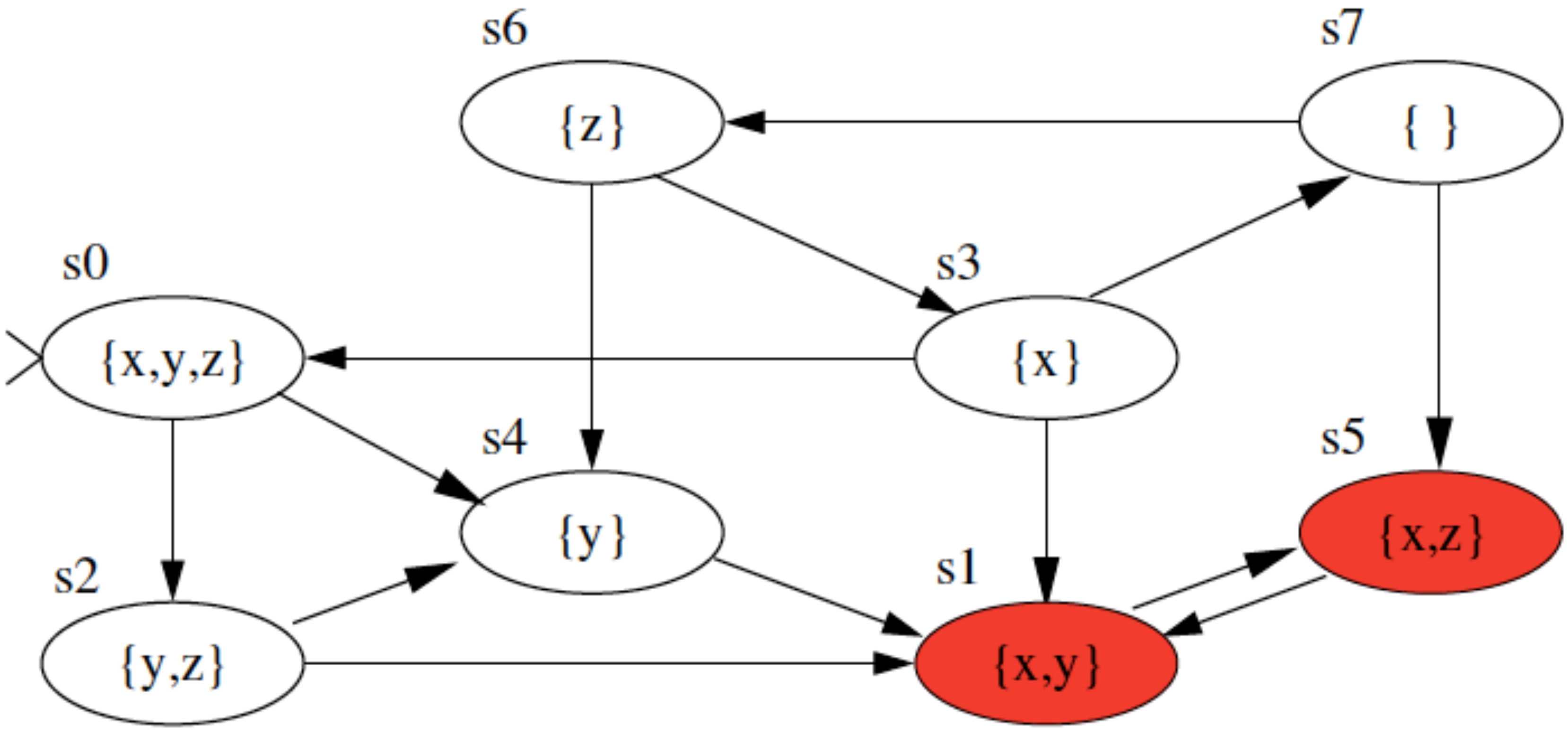
we are given with a transition system K


s6
{z}
s7
{ }
s0
{x,y,z}
s3
{x}
s4
{y}
s5
{x,z}
s2
{y,z}
s1
{x,y}

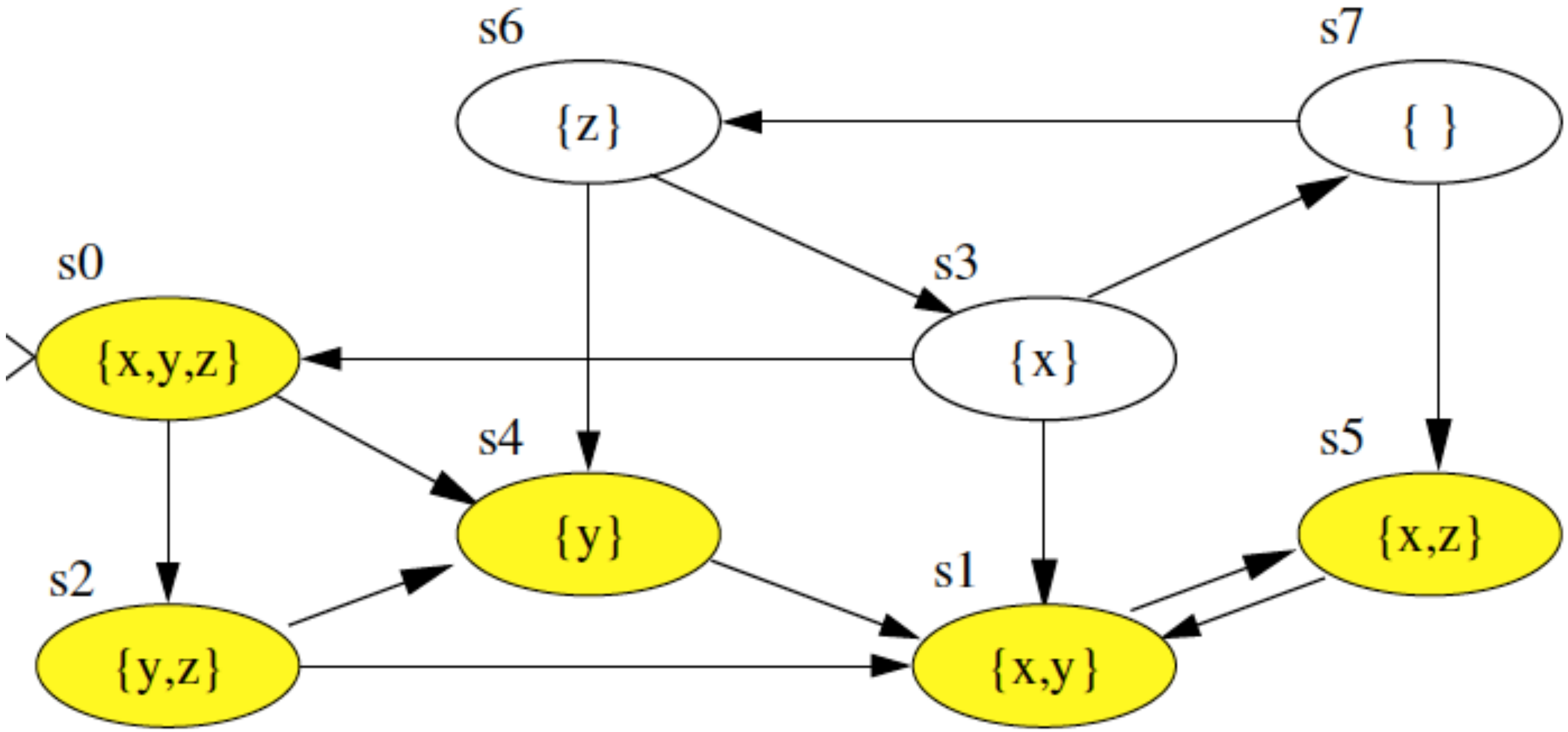
Compute ⟦*x*⟧



Compute $[\![\mathrm{AG}\ x]\!]$



Compute $[\![\mathrm{AF\ AG}\ x]\!]$



Recursively defined operators

$$AG\,\phi \equiv \phi \wedge AXAG\,\phi$$

$$EG\,\phi \equiv \phi \wedge EXEG\,\phi$$

$$AF\,\phi \equiv \phi \vee AXAF\,\phi$$

$$EF\,\phi \equiv \phi \vee EXEF\,\phi$$

$$A[\phi\ U\ \psi] \equiv \psi \vee (\phi \wedge AXA[\phi\ U\ \psi])$$

$$E[\phi\ U\ \psi] \equiv \psi \vee (\phi \wedge EXE[\phi\ U\ \psi])$$

The example again

- We want to define the set of states where EG*x* is the greatest solution of the recursive equation $x = x \wedge \mathrm{EX}(x)$
- i.e. as the maximal fixpoint of the operator $\pi = (\ ) \wedge \mathrm{EX}(\ ) : \wp(S) \rightarrow \wp(S)$
- We start from the greatest subset S and define *pre*(S’) as the subset of states such that there is for them a successor state in S’

Illustration for *EG y*

Initially, $\pi^0(S) = (all)\ S$

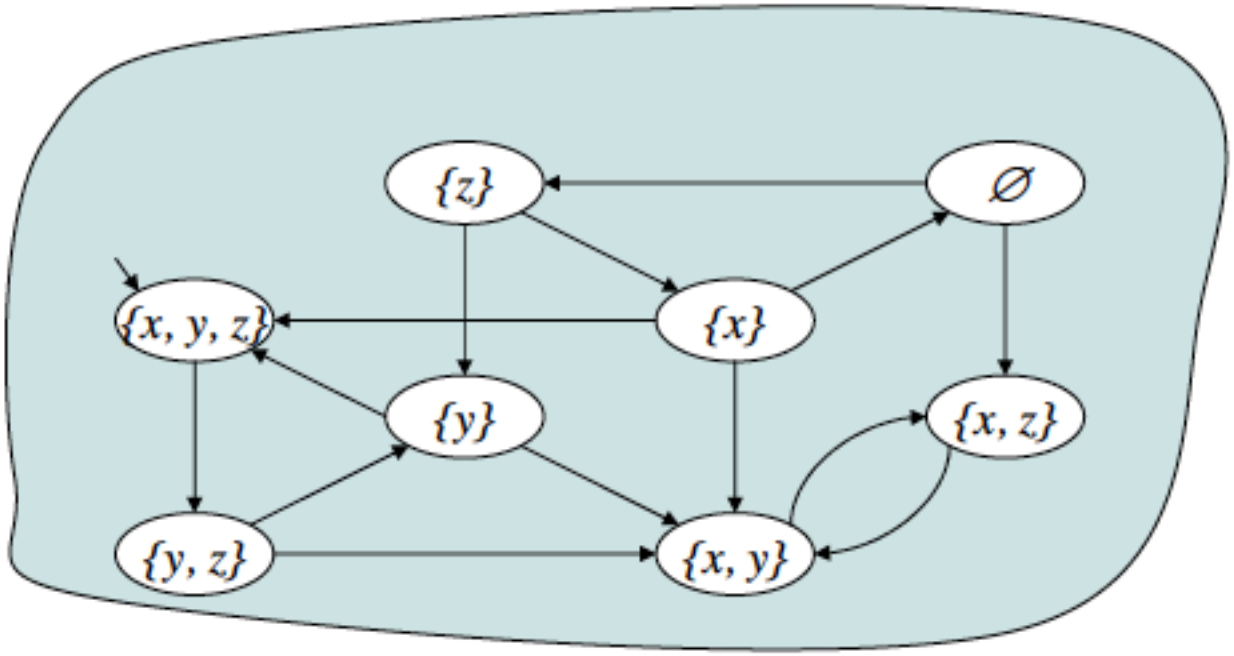
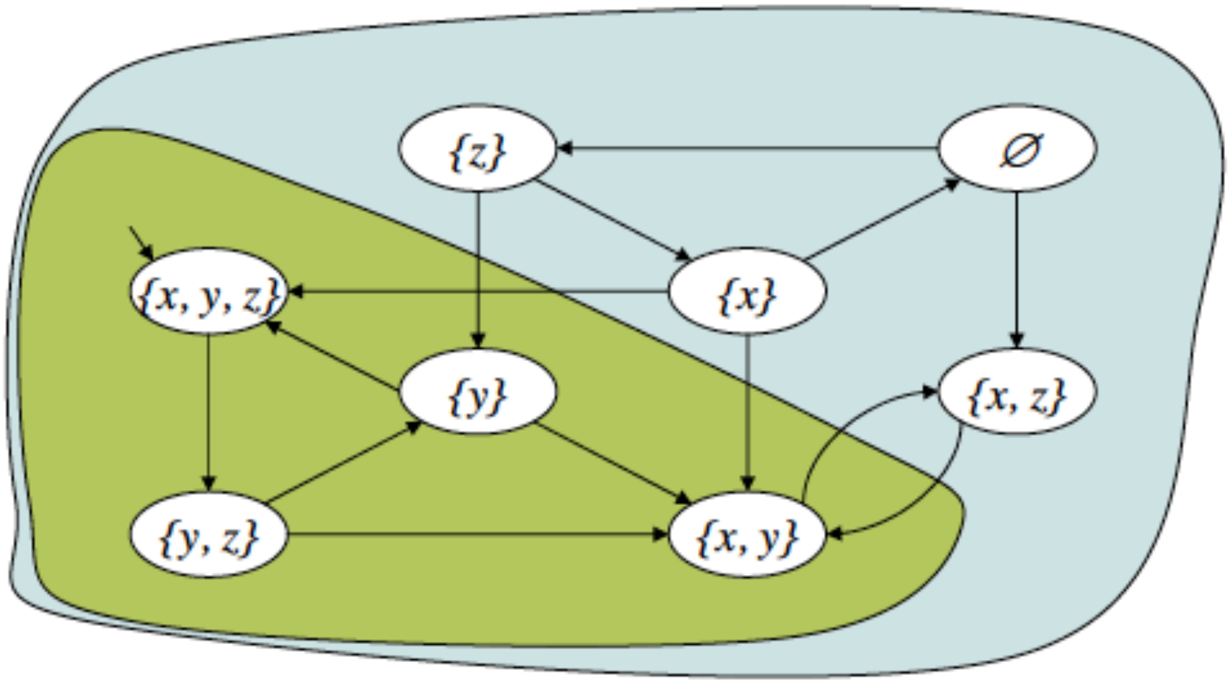


Illustration for *EG* y

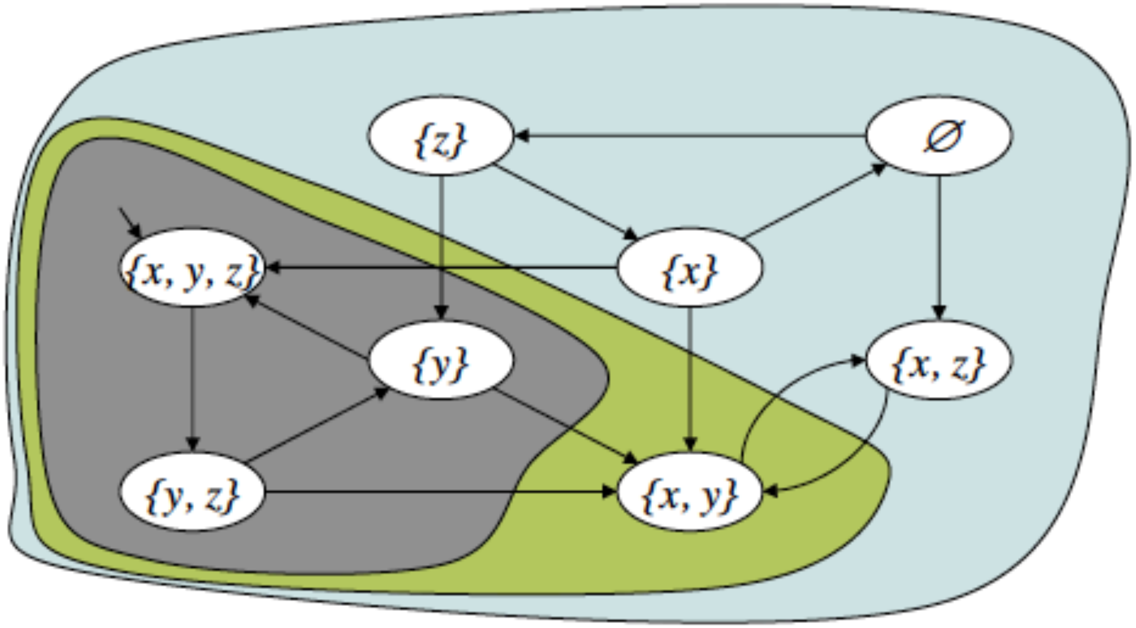
Then, $\pi^1(S) = S_K(y) \cap pre(S)$



States not satisfying y are excluded

Illustration for *EG y*

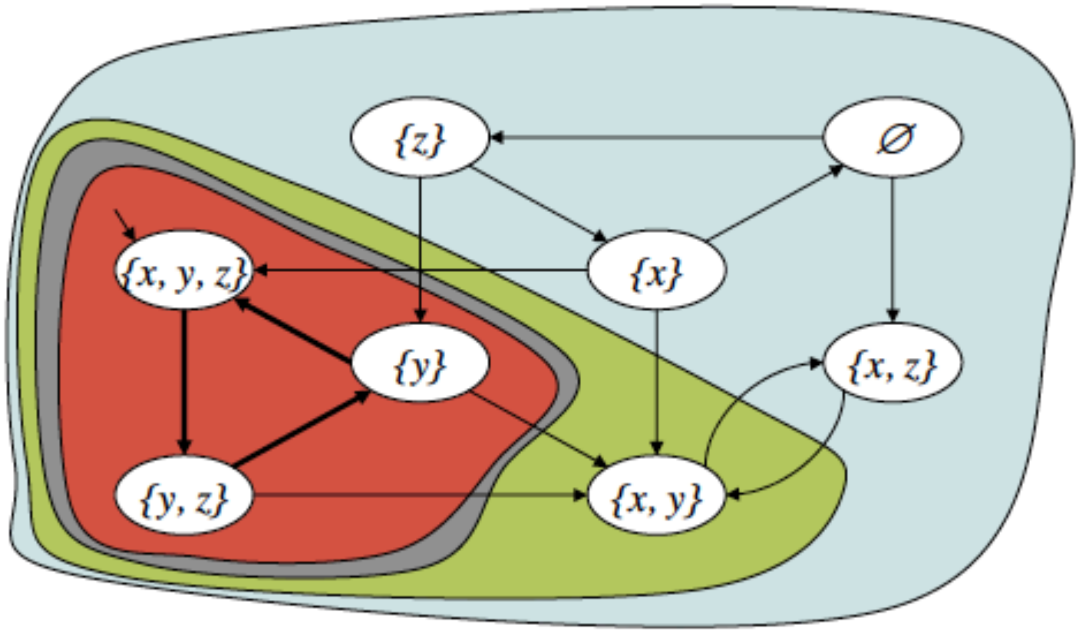
$$\pi^2(S) = S_K(y) \cap pre(\pi^1(S))$$



States having all its successors outside π^1 are excluded

Illustration for *EG* y

$$\pi^3(S) = S_K(y) \cap pre(\pi^2(S))$$



The fixed point is now reached

An example again

- We want to define the set of states where E(xU*y*) is the smallest solution of the recursive equation <x,y> = y $\vee$ ($x \wedge$ EX (x,y))
- i.e. as the minimal fixpoint of the operator

$$\xi = (\ ) \wedge EX(\ ) : \wp(S) \rightarrow \wp(S)$$

- We start from the smallest subset of S, namely Ø

Illustration for z *EU* y

Initially, $\xi^0(\varnothing) = \varnothing$

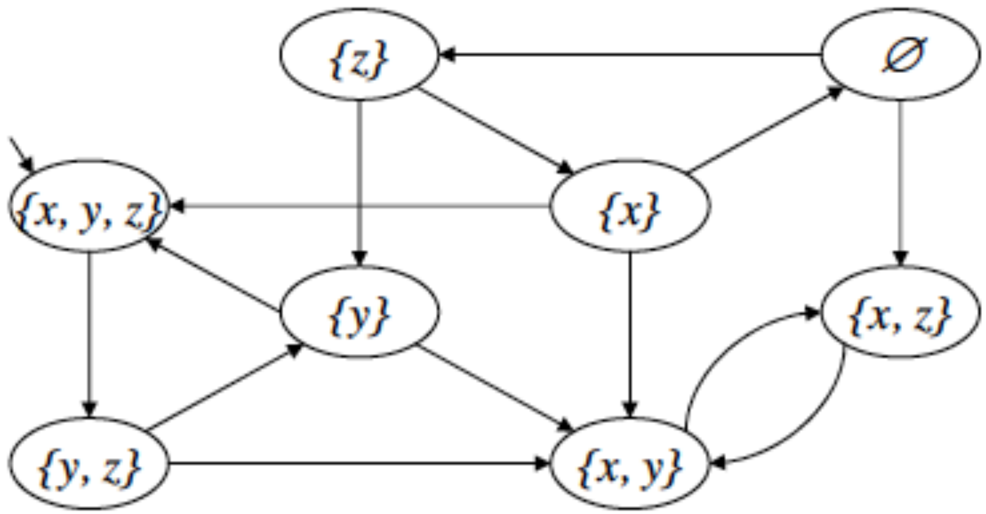
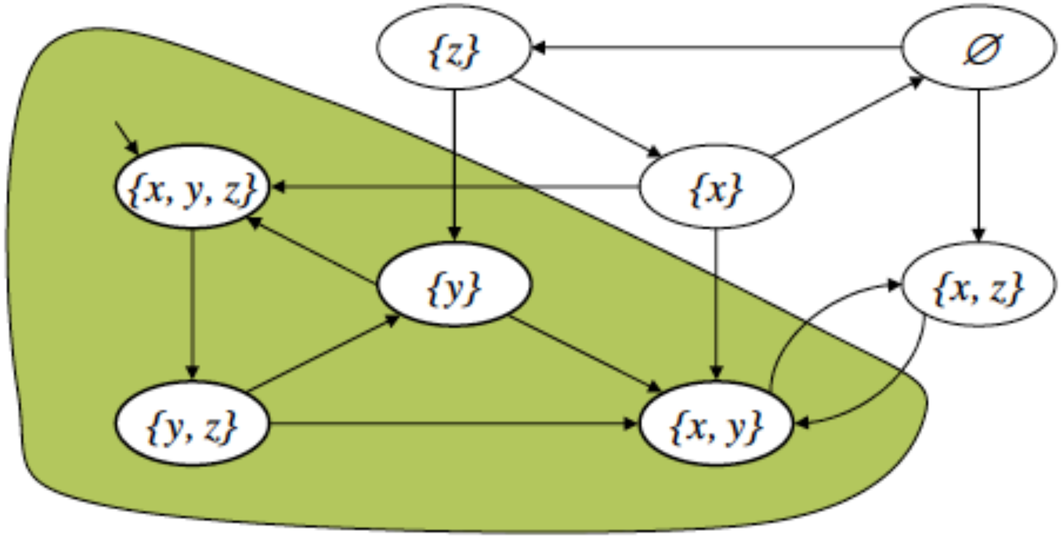


Illustration for z *EU* y

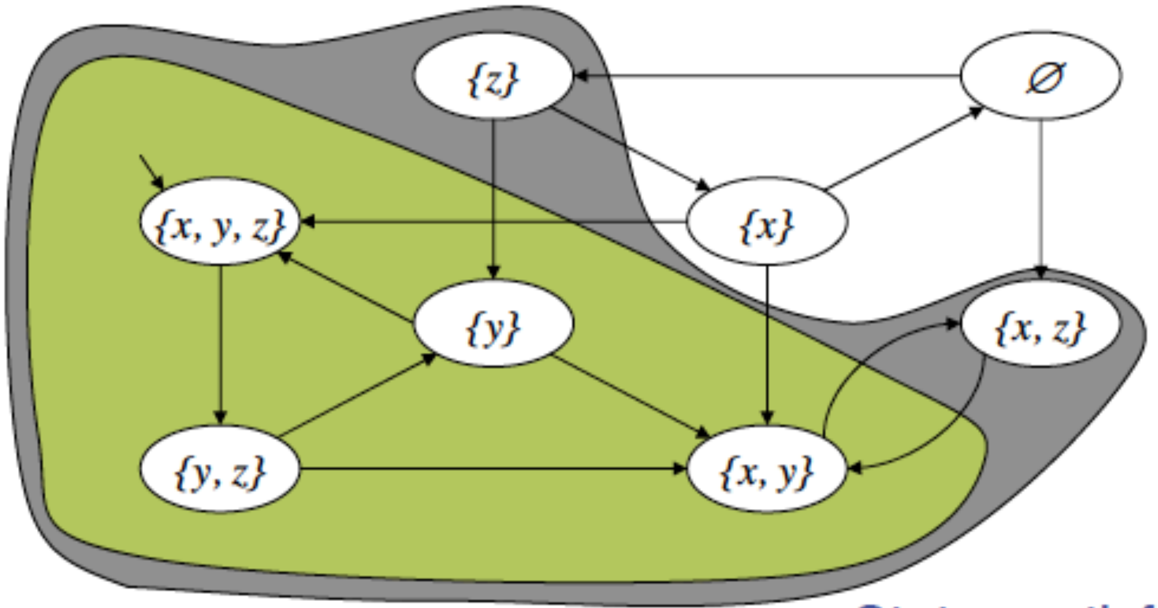
Then, $\xi^1(\varnothing) = S_K(y) \cup (S_K(z) \cap pre(\xi^0(\varnothing)))$



States satisfying y are added

Illustration for z *EU* y

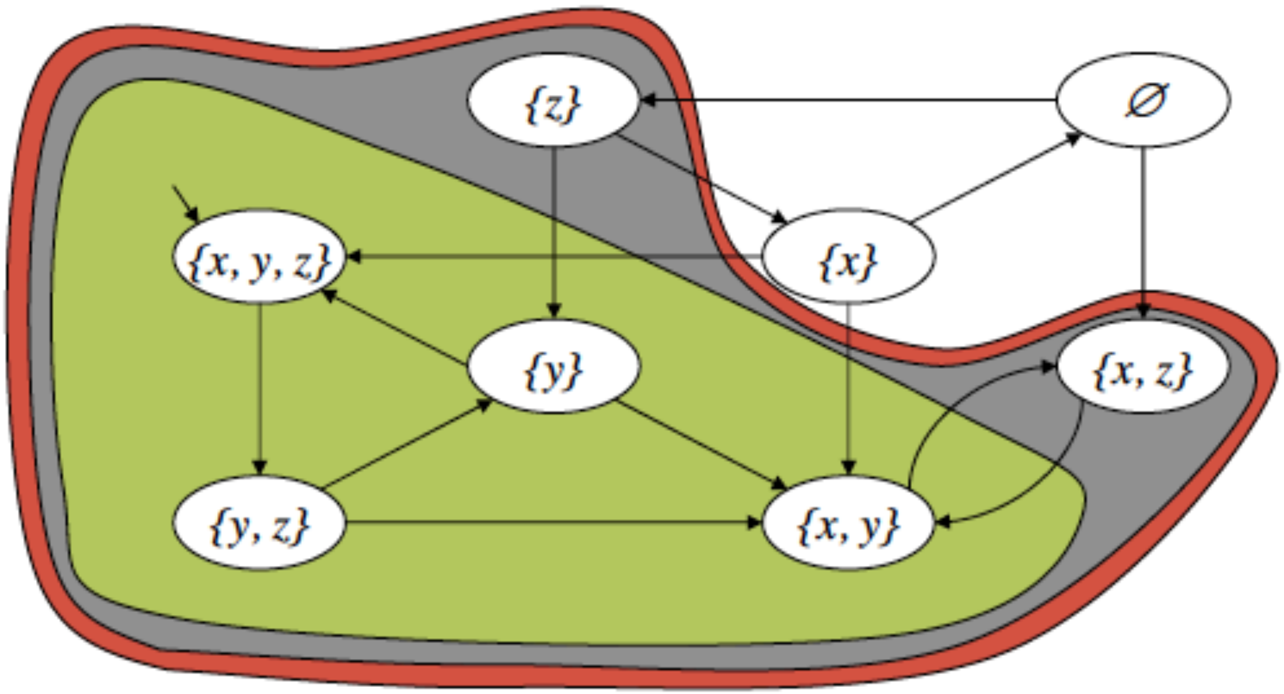
Then, $\xi^2(\emptyset) = S_K(y) \cup (S_K(z) \cap pre(\xi^1(\emptyset)))$



States satisfying z and having at least a successor in ξ^1 are added

Illustration for z *EU* y

Then, $\xi^3(\emptyset) = S_K(y) \cup (S_K(z) \cap pre(\xi^2(\emptyset)))$



The fixed point
is now reached.