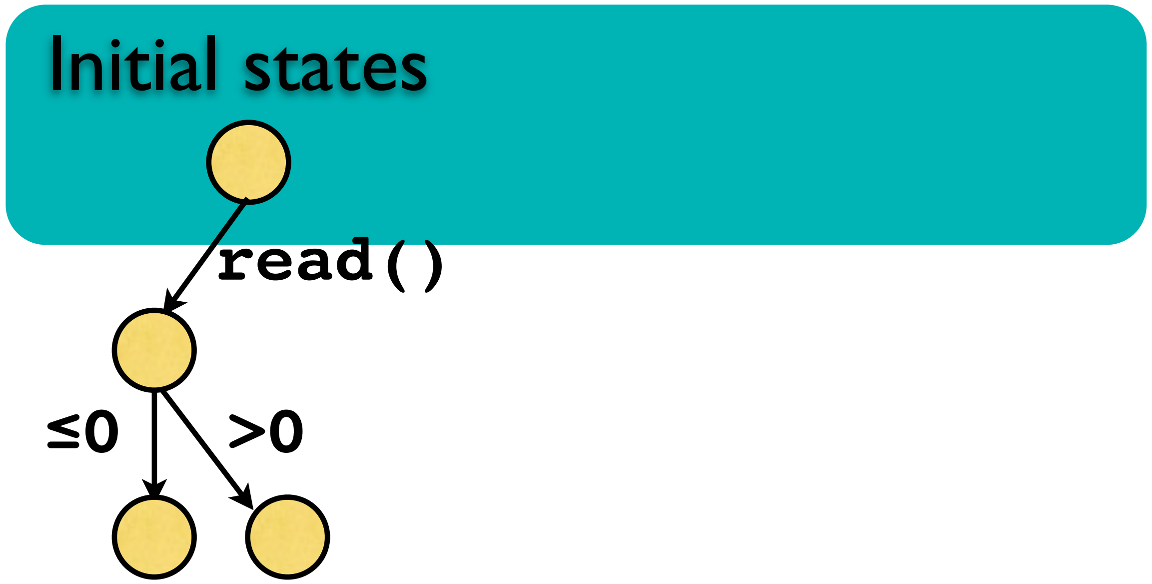
Reasoning about nondeterminism in software

High Confidence Software and Systems 2012

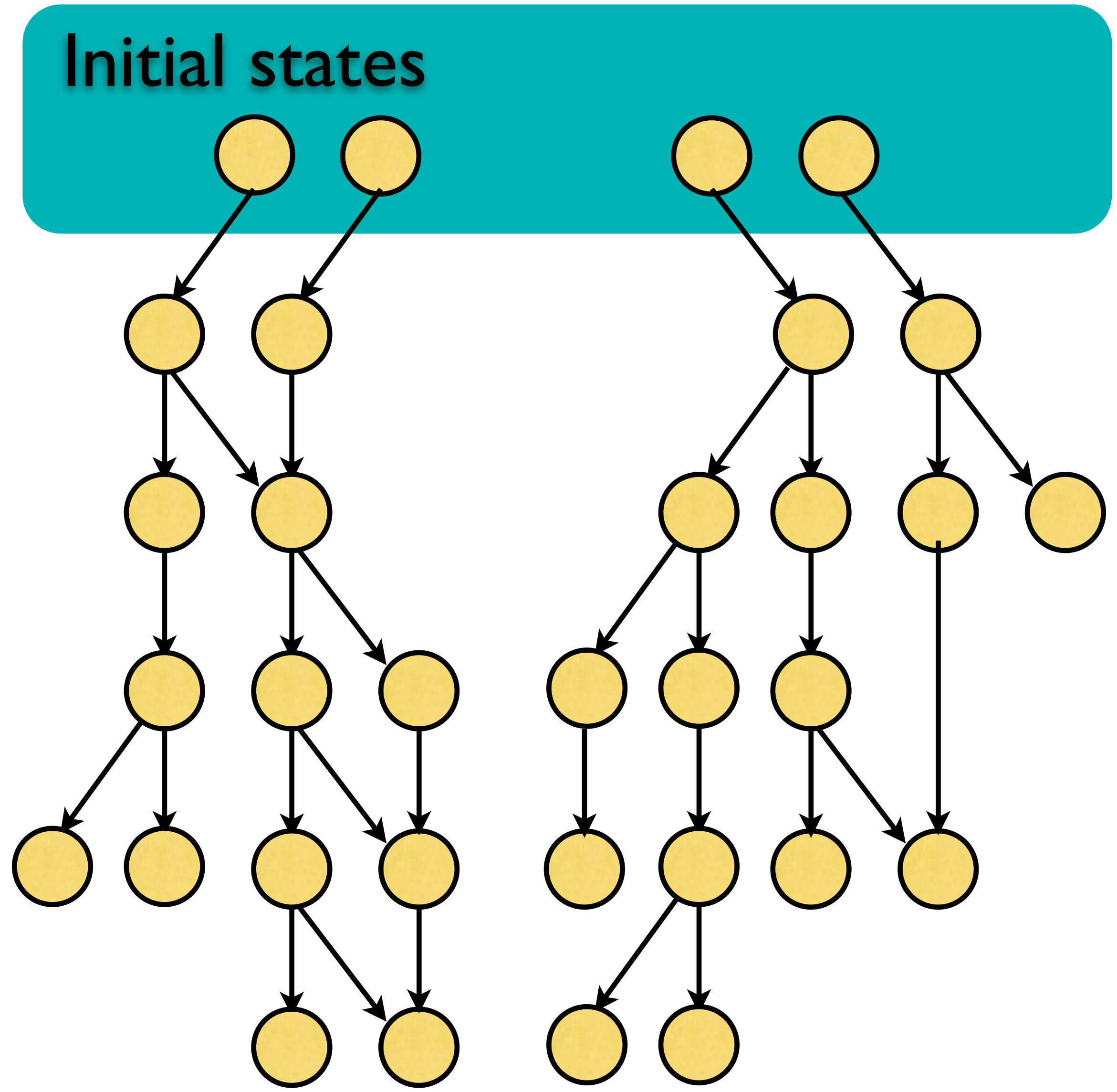
Eric Koskinen
Research Scientist and Principal Investigator
New York University
ejk@cims.nyu.edu

The behavior of software is often nondeterministic

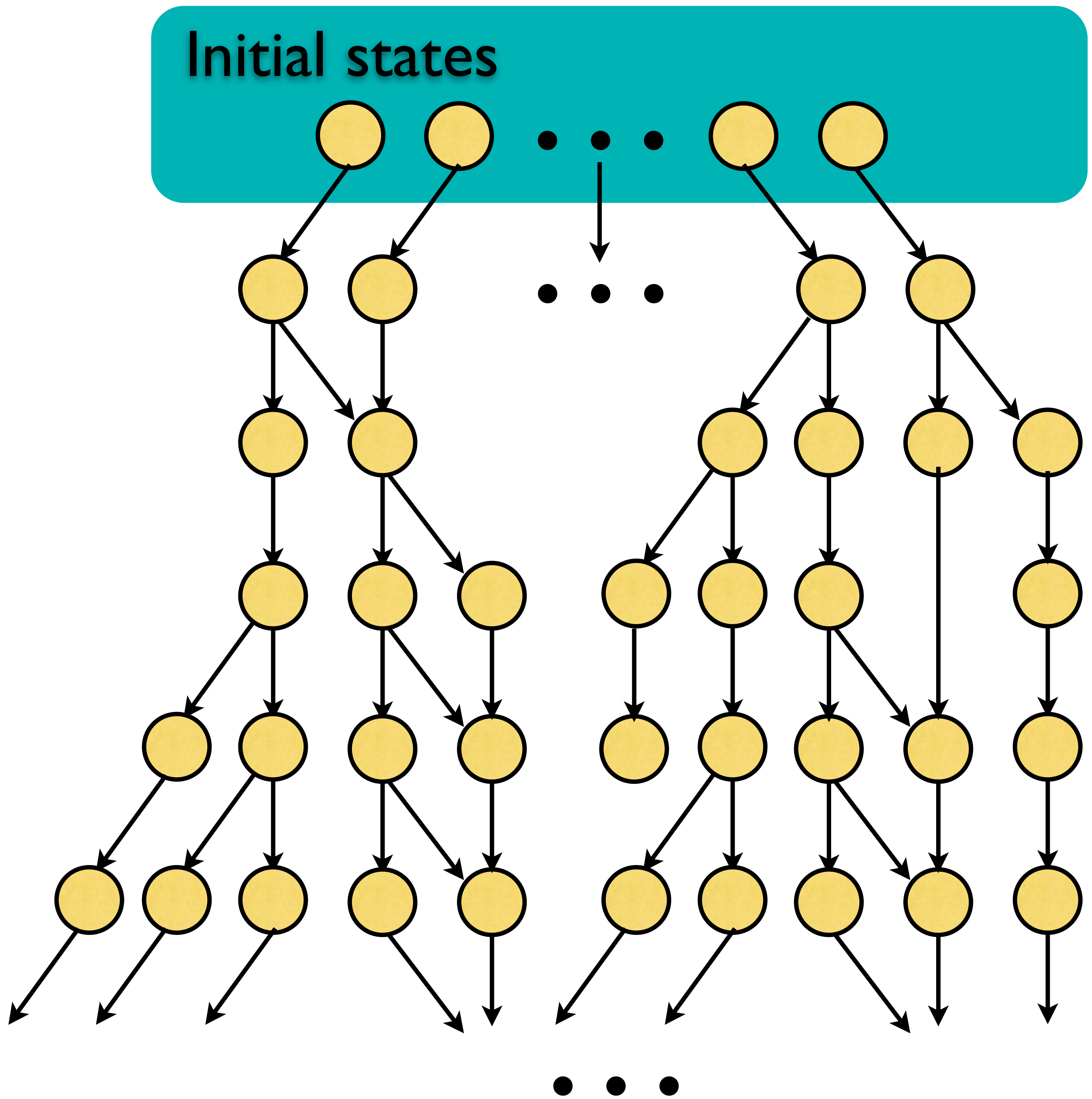
```
if (read(&buf)) {
  computeA();
else {
  computeB();
}
```



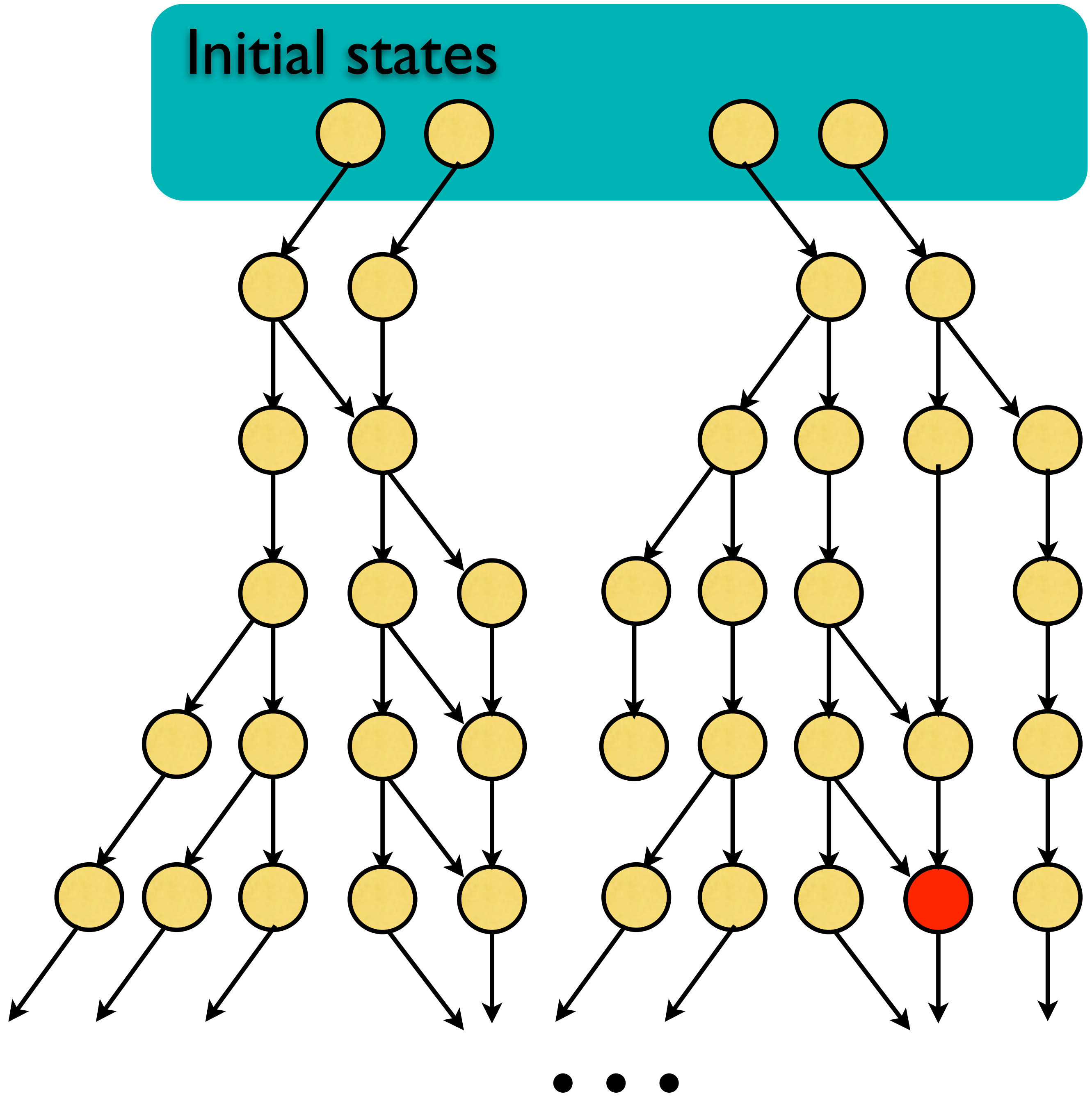
Modern software systems have elaborate control-flow.



... and infinite state spaces!

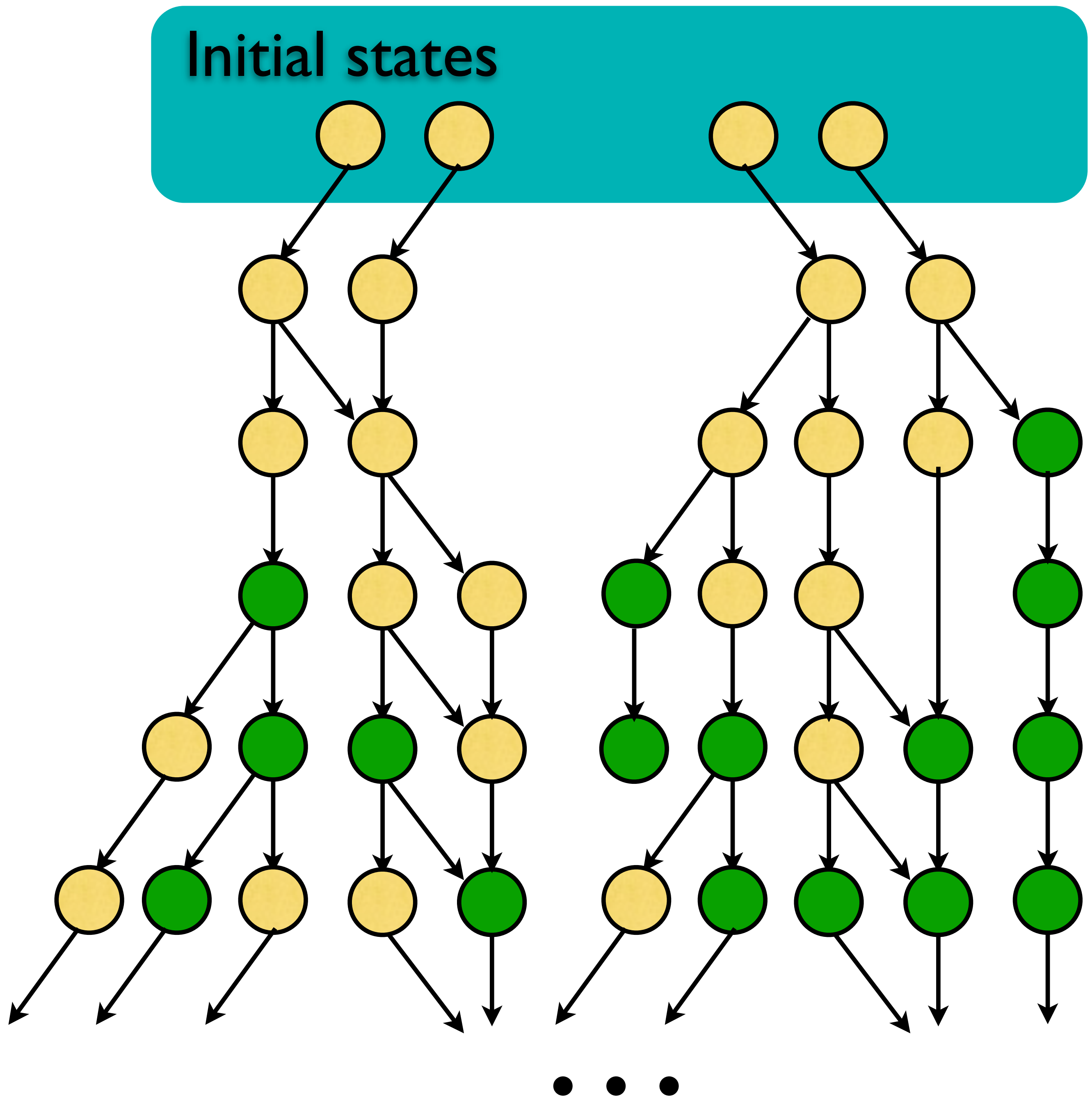


Many important properties involve the ***branching*** *behaviors of a program*



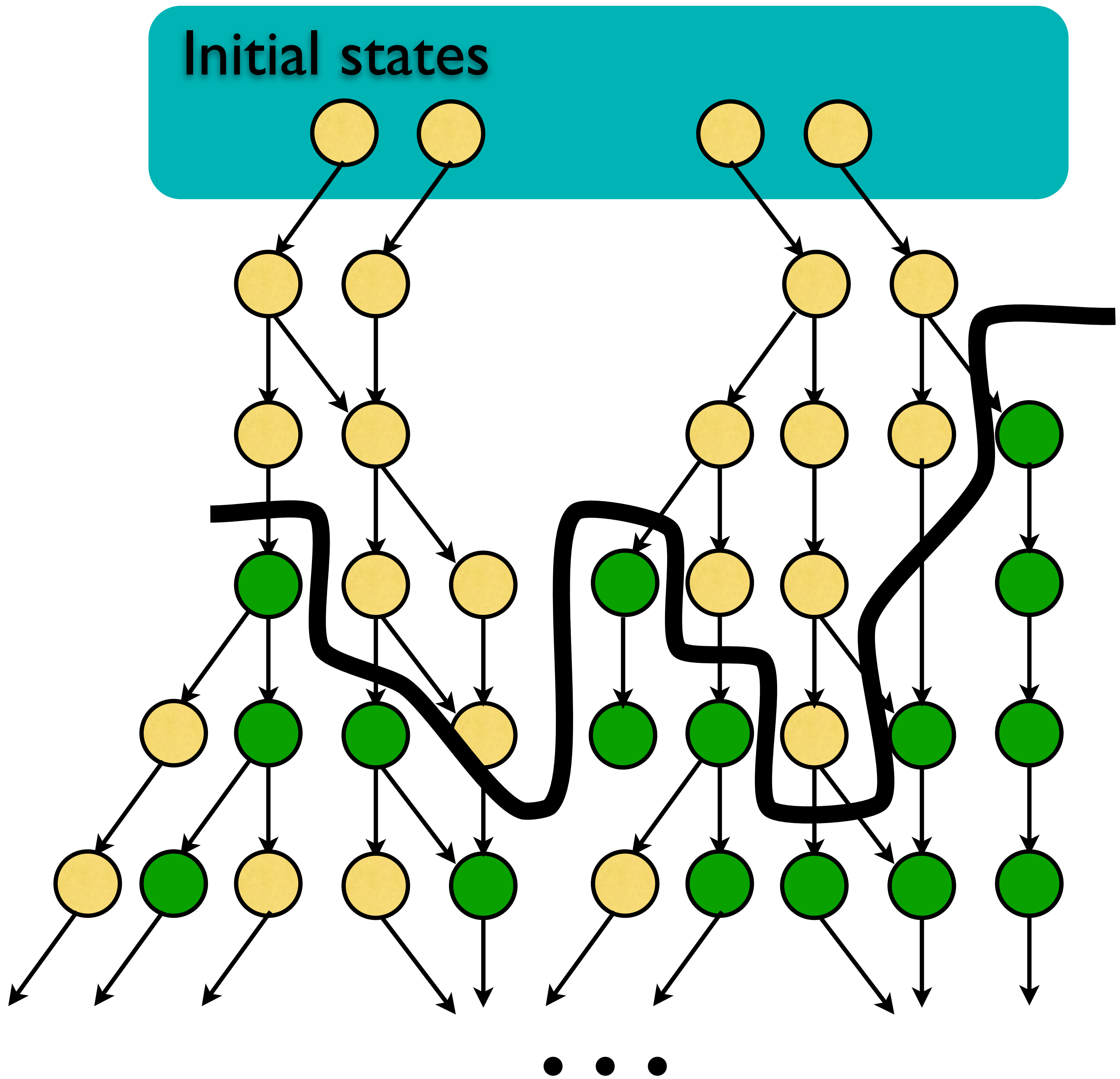
Example: *does there exist a way to reach a red state?* EF red

Many important properties involve the ***branching*** *behaviors of a program*



Example: *are you assured you will always reach a state from which point you can always be in a green state?* AF (EG green)

Many important properties involve the ***branching*** *behaviors of a program*



Example: *are you assured you will always reach a state from which point you can always be in a green state?* AF (EG green)

branching

Branching properties can be found in many temporal logics.

branching

CTL

Computation Tree Logic [Clarke 1986]

AFp	Across all paths, eventually reach *p*
EFp	There is a path that eventually reaches *p*
AGp	Across all paths, *p* always holds
EGp	There is a path along which *p* always holds

branching

CTL

Computation Tree Logic [Clarke 1986]

AFp	Across all paths, eventually reach *p*
EFp	There is a path that eventually reaches *p*
AGp	Across all paths, *p* always holds
EGp	There is a path along which *p* always holds

branching

CTL

Computation T...

AFp	Across all path...
EFp	There is a path...
AGp	Across all path...
EGp	There is a path...

Temporal property verification as a program analysis task

Byron Cook[1], Eric Koskinen[2], and Moshe Vardi[3]

[1] Microsoft Research and Queen Mary University of London
[2] University of Cambridge
[3] Rice University

Abstract. We describe a reduction from temporal property verification to a program analysis problem. We produce an encoding which, with the use of recursion and nondeterminism, enables off-the-shelf program analysis tools to naturally perform the reasoning necessary for proving temporal properties (*e.g.* backtracking, eventuality checking, tree counterexamples for branching-time properties, abstraction refinement, etc.). Using examples drawn from the PostgreSQL database server, Apache web server, and Windows OS kernel, we demonstrate the practical viability of our work.

1 Introduction

We describe a method of proving temporal properties of (possibly infinite-state) transition systems. We observe that, with subtle use of recursion and nondeterminism, temporal reasoning can be encoded as a program ana... of the tasks necessary for reasoning about temporal propertie... search, backtracking, eventuality checking, tree counterexamp... time, etc.) are then naturally performed by off-the-shelf progra...

CAV'11

branching

Program	Property	Traditional Time(s)
Example from Sec. 2	AFAGp	2.32
Example from Fig. 8 of [15]	AG(p⇒AFq)	209.64
Toy acq/rel	AG(p⇒AFq)	103.48
Toy lin. arith. 1	p⇒AFq	126.86
Toy lin. arith. 2	p⇒AFq	**timeout**
PostgreSQL strsrv	AG(p⇒AFAGq)	**timeout**
PostgreSQL strsrv+bug	AG(p⇒AFAGq)	87.31
PostgreSQL pgarch	AFAGp	31.50
PostgreSQL dropbuf	AGp	**timeout**
PostgreSQL dropbuf	AG(p⇒AFq)	53.99
Apache child	AG(p⇒AGAFq)	**timeout**
Apache child `accept` liveness	AG(p⇒(AFa ∨ AFb))	685.34
Windows frag. 1	AG(p⇒AFq)	901.81
Windows frag. 2	AFAGp	16.47
Windows frag. 2+bug	AFAGp	26.15
Windows frag. 3	AFAGp	4.21
Windows frag. 4	AG(p⇒AFq)	**timeout**
Windows frag. 4	(AFp) ∨ (AFq)	1,223.96
Windows frag. 5	AG(p⇒AFq)	**timeout**
Windows frag. 6	AFAGp	149.41
Windows frag. 6+bug	AFAGp	6.06
Windows frag. 7	AGAFp	**timeout**
Windows frag. 8	FGp	**timeout**

branching

Program	Property	Traditional Time(s)	Our Approach Time(s)
Example from Sec. 2	AFAGp	2.32	1.98
Example from Fig. 8 of [15]	AG(p⇒AFq)	209.64	27.94
Toy acq/rel	AG(p⇒AFq)	103.48	14.18
Toy lin. arith. 1	p⇒AFq	126.86	34.51
Toy lin. arith. 2	p⇒AFq	**timeout**	6.74
PostgreSQL strsrv	AG(p⇒AFAGq)	**timeout**	9.56
PostgreSQL strsrv+bug	AG(p⇒AFAGq)	87.31	47.16
PostgreSQL pgarch	AFAGp	31.50	15.20
PostgreSQL dropbuf	AGp	**timeout**	1.14
PostgreSQL dropbuf	AG(p⇒AFq)	53.99	27.54
Apache child	AG(p⇒AGAFq)	**timeout**	197.41
Apache child `accept` liveness	AG(p⇒(AFa ∨ AFb))	685.34	684.24
Windows frag. 1	AG(p⇒AFq)	901.81	539.00
Windows frag. 2	AFAGp	16.47	52.10
Windows frag. 2+bug	AFAGp	26.15	30.37
Windows frag. 3	AFAGp	4.21	15.75
Windows frag. 4	AG(p⇒AFq)	**timeout**	1,114.18
Windows frag. 4	(AFp) ∨ (AFq)	1,223.96	100.68
Windows frag. 5	AG(p⇒AFq)	**timeout**	**timeout**
Windows frag. 6	AFAGp	149.41	59.56
Windows frag. 6+bug	AFAGp	6.06	22.12
Windows frag. 7	AGAFp	**timeout**	55.77
Windows frag. 8	FGp	**timeout**	5.24

all “A” properties

branching

Program	Property	Traditional Time(s)	Our Approach Time(s)
Example from Sec. 2	AFAGp	2.32	1.98
Example from Fig. 8 of [15]	AG(p⇒AFq)	209.64	27.94
Toy acq/rel	AG(p⇒AFq)	103.48	14.18
Toy lin. arith. 1	p⇒AFq	126.86	34.51
Toy lin. arith. 2	p⇒AFq	**timeout**	6.74
PostgreSQL strsrv	AG(p⇒AFAGq)	**timeout**	9.56
PostgreSQL strsrv+bug	AG(p⇒AFAGq)	87.31	47.16
PostgreSQL pgarch	AFAGp	31.50	15.20
PostgreSQL dropbuf	AGp	**timeout**	1.14
PostgreSQL dropbuf	AG(p⇒AFq)	53.99	27.54
Apache child	AG(p⇒AGAFq)	**timeout**	197.41
Apache child `accept` liveness	AG(p⇒(AFa ∨ AFb))	685.34	684.24
Windows frag. 1	AG(p⇒AFq)	901.81	539.00
Windows frag. 2	AFAGp	16.47	52.10
Windows frag. 2+bug	AFAGp	26.15	30.37
Windows frag. 3	AFAGp	4.21	15.75
Windows frag. 4	AG(p⇒AFq)	**timeout**	1,114.18
Windows frag. 4	(AFp) ∨ (AFq)	1,223.96	100.68
Windows frag. 5	AG(p⇒AFq)	**timeout**	**timeout**
Windows frag. 6	AFAGp	149.41	59.56
Windows frag. 6+bug	AFAGp	6.06	22.12
Windows frag. 7	AGAFp	**timeout**	55.77
Windows frag. 8	FGp	**timeout**	5.24

branching

all “A” properties

Program	Property	Traditional Time(s)	Our Approach Time(s)
Example from Sec. 2	AFAGp	2.32	1.98
Example from Fig. 8 of [15]	AG(p⇒AFq)	209.64	27.94
Toy acq/rel	AG(p⇒AFq)	103.48	14.18
Toy lin. arith. 1	p⇒AFq	126.86	34.51
Toy lin. arith. 2	p⇒AFq	timeout	6.74
PostgreSQL strsrv	AG(p⇒AFAGq)	timeout	9.56
PostgreSQL strsrv+bug	AG(p⇒AFAGq)	87.31	47.16
PostgreS[illegible]	[illegible]	[illegible]	15.20
PostgreSQL dropbuf	AGp	timeout	1.14
PostgreSQL dropbuf	[illegible]	[illegible]99	27.54
Apache child	AG(p⇒AGAFq)	timeout	197.41
Apache child `accept` liveness	AG(p⇒(AFa ∨ AFb))	685.34	684.24
Windows frag. 1	AG(p⇒AFq)	901.81	539.00
Windows frag. 2	AFAGp	16.47	52.10
Windows frag. 2+bug	AFAGp	26.15	30.37
Windows frag. 3	AFAGp	4.21	15.75
Windows frag. 4	AG(p⇒AFq)	timeout	1,114.18
Windows frag. 4	(AFp) ∨ (AFq)	1,223.96	100.68
Windows frag. 5	AG(p⇒AFq)	timeout	timeout
Windows frag. 6	AFAGp	149.41	59.56
Windows frag. 6+bug	AFAGp	6.06	22.12
Windows frag. 7	AGAFp	timeout	55.77

Extend beyond the universal fragment, include existential properties . . .

branching

existential and universal

- Planning
  Is there a position I can move to such that escape is possible?
  At any point system *could* terminate and when it does *p* holds.

branching

existential and universal

- Planning
  Is there a position I can move to such that escape is possible?
  At any point system *could* terminate and when it does *p* holds.
- Games
  Are there choices that I can make (“exists”) such that I will always outwit every move (“universal”) my opponent makes?

branching

existential and universal

- Planning
  Is there a position I can move to such that escape is possible?
  At any point system *could* terminate and when it does *p* holds.
- Games
  Are there choices that I can make ("exists") such that I will always outwit every move ("universal") my opponent makes?
- Security
  Can the system eventually repair itself after an intrusion?
  Is is possible that, no matter what inputs an attacker enters, the system can escape being compromised.

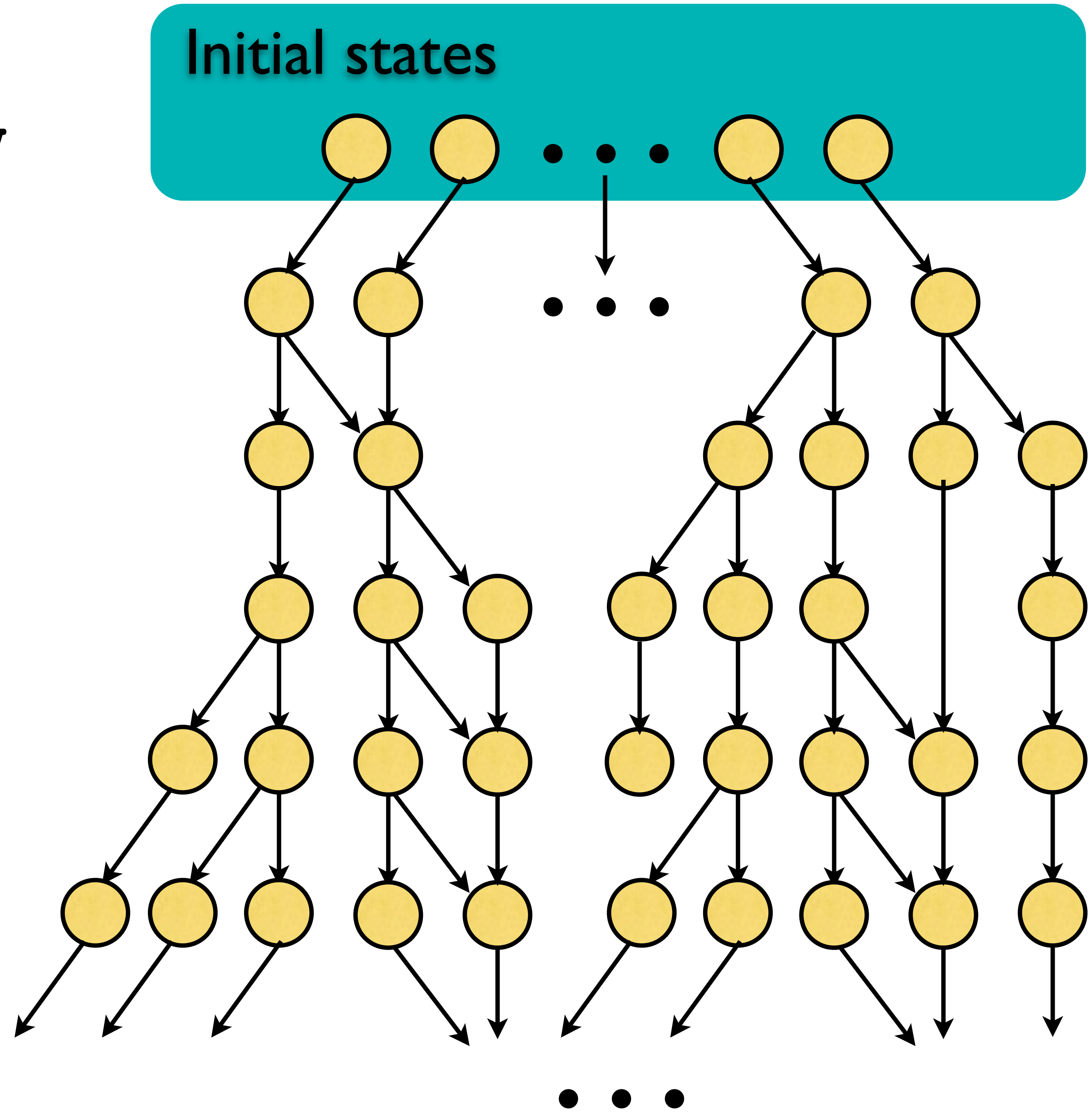
branching

existential and universal

Can be treated similarly

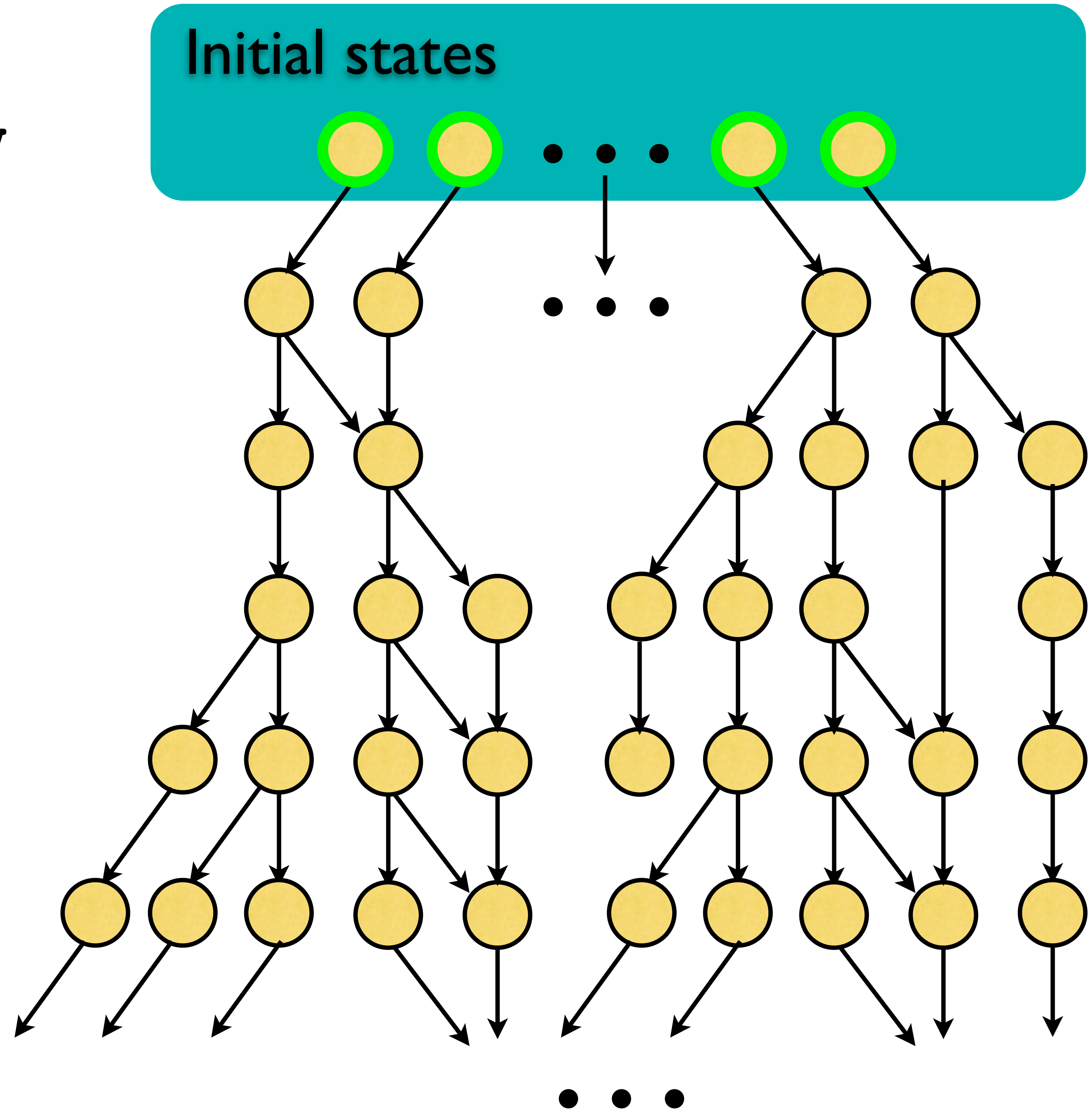
AG and EG (reachability)

AG `yellow`



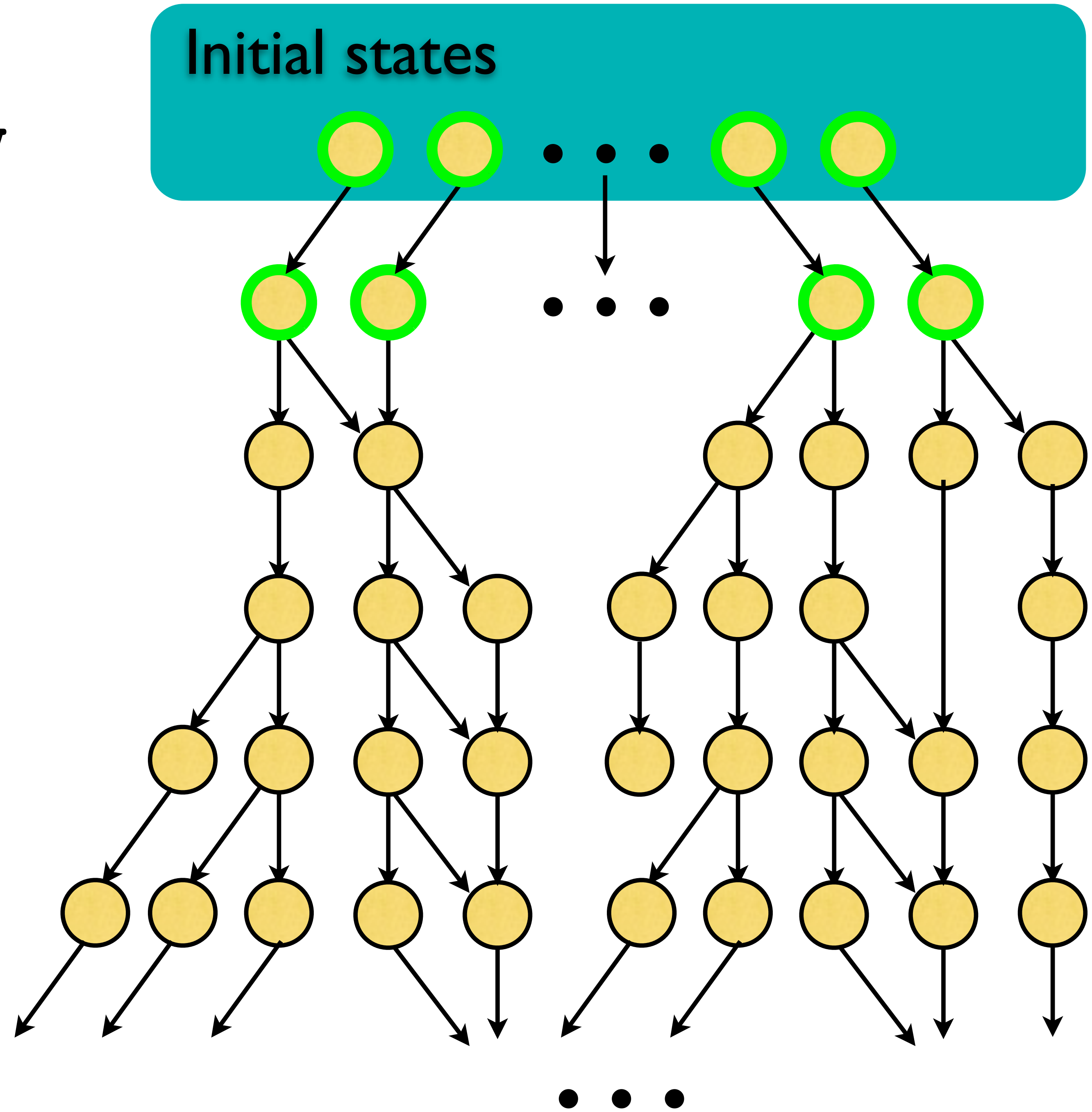
AG and EG (reachability)

AG `yellow`



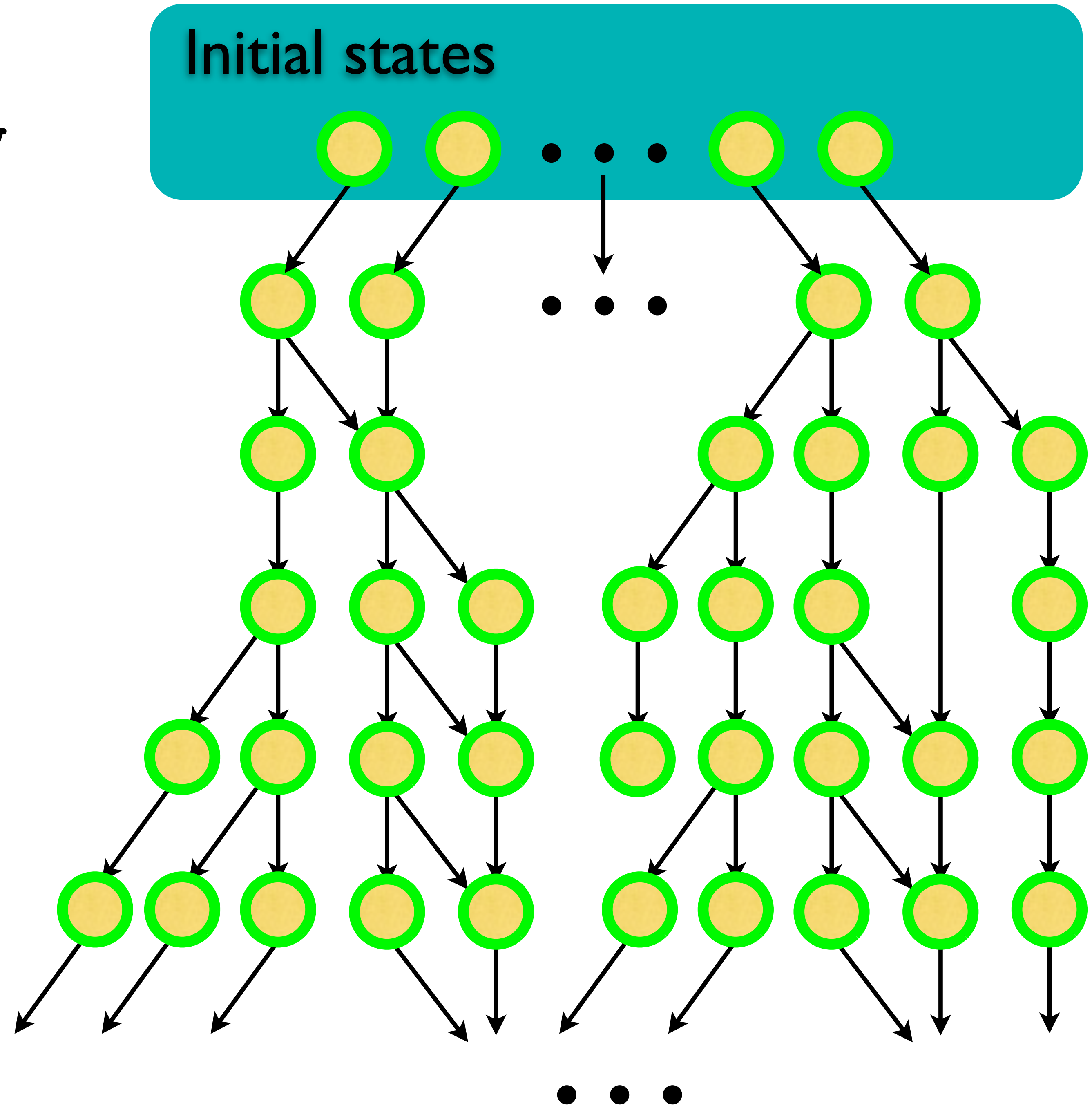
AG and EG (reachability)

AG `yellow`



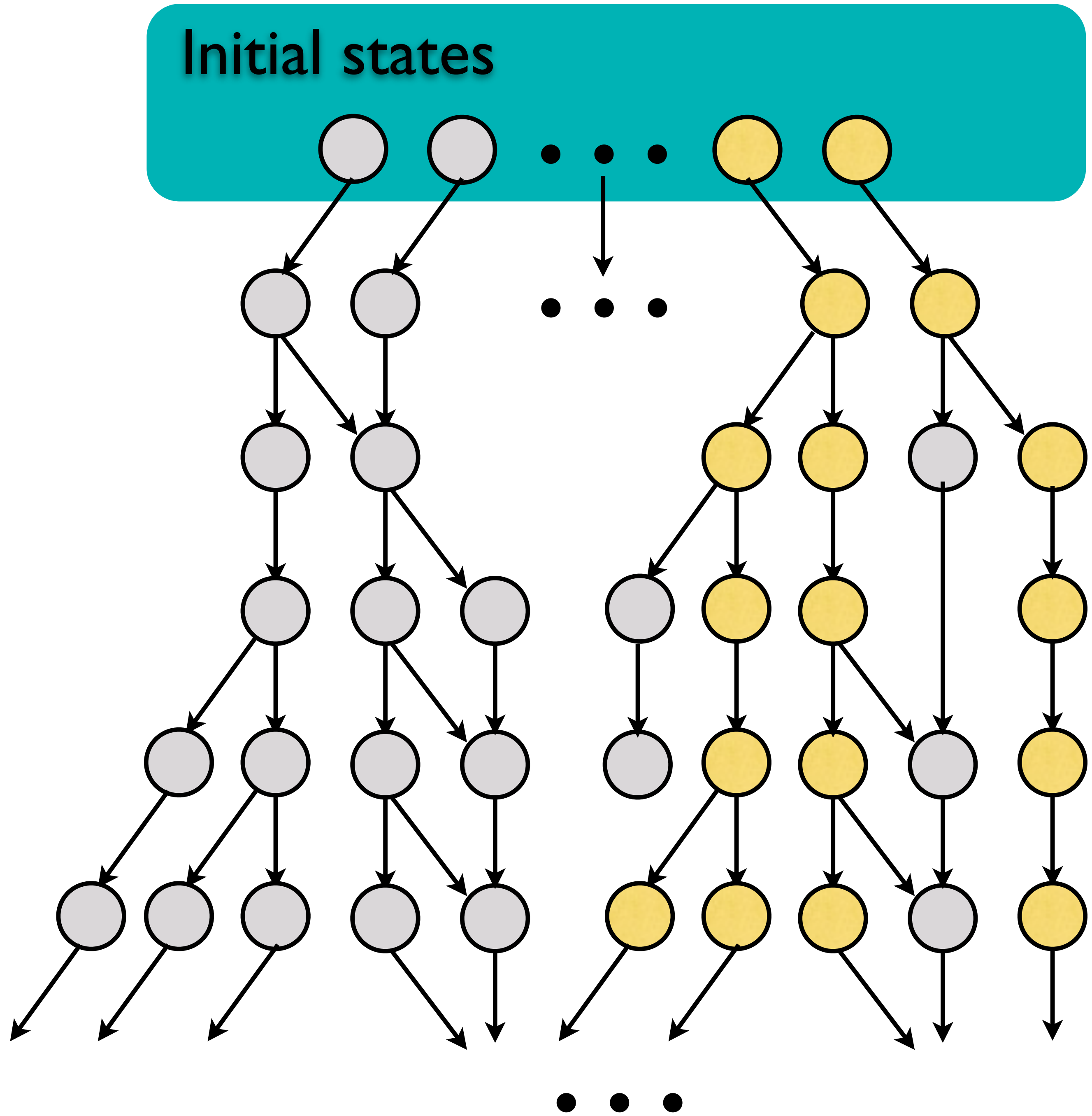
AG and EG (reachability)

AG `yellow`



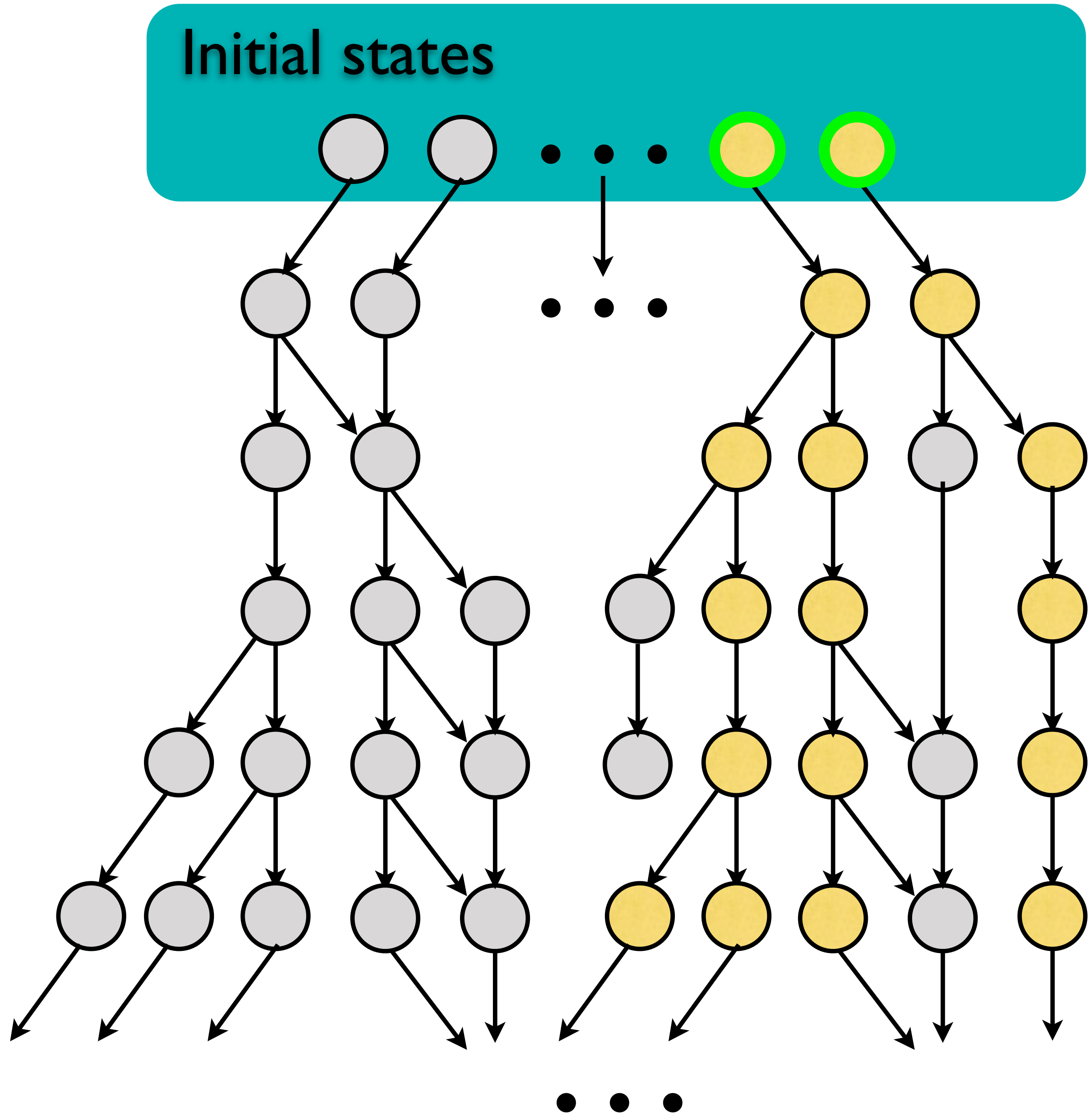
AG and EG (reachability)

EG `yellow`



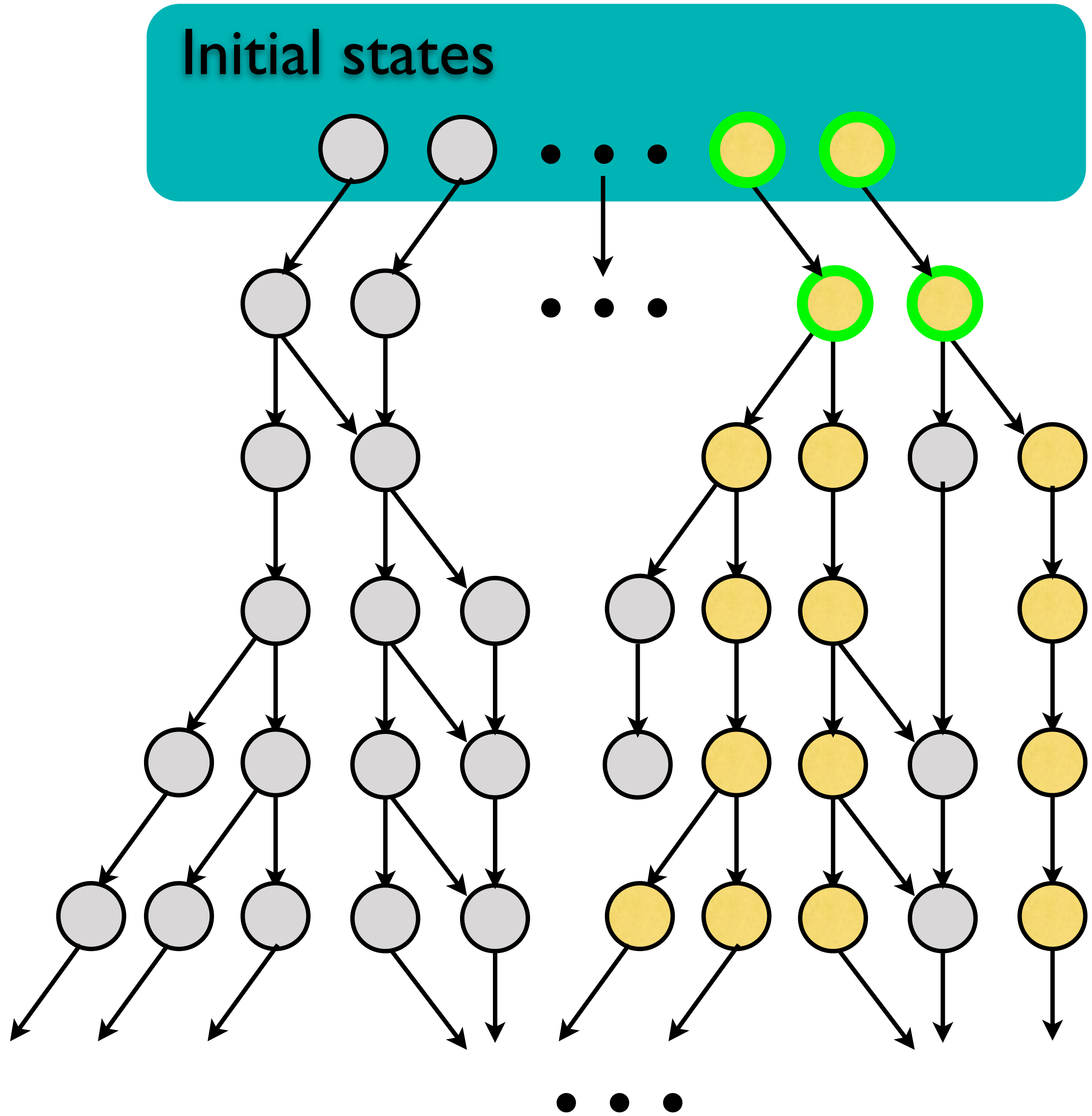
AG and EG (reachability)

EG `yellow`



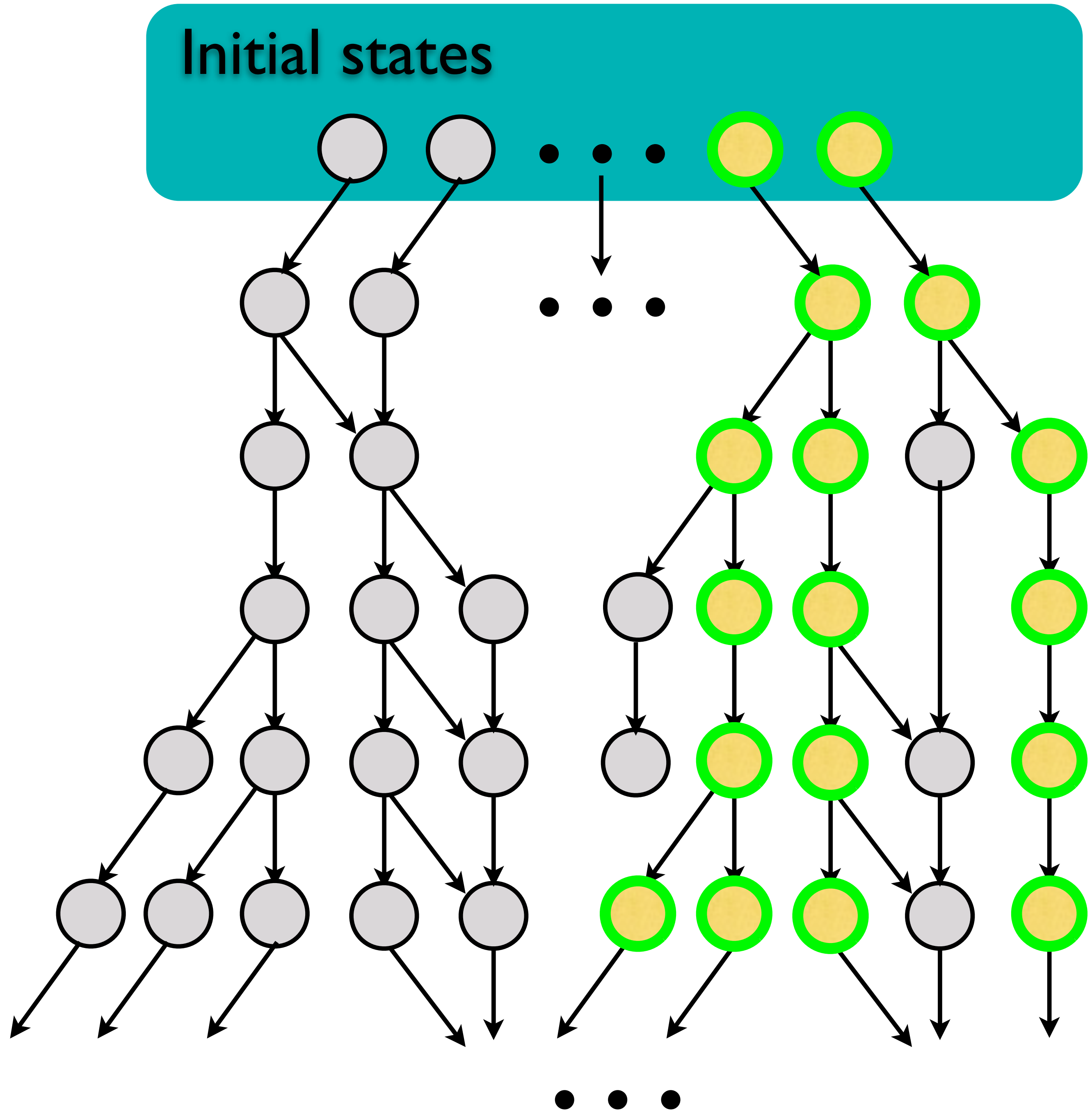
AG and EG (reachability)

EG `yellow`



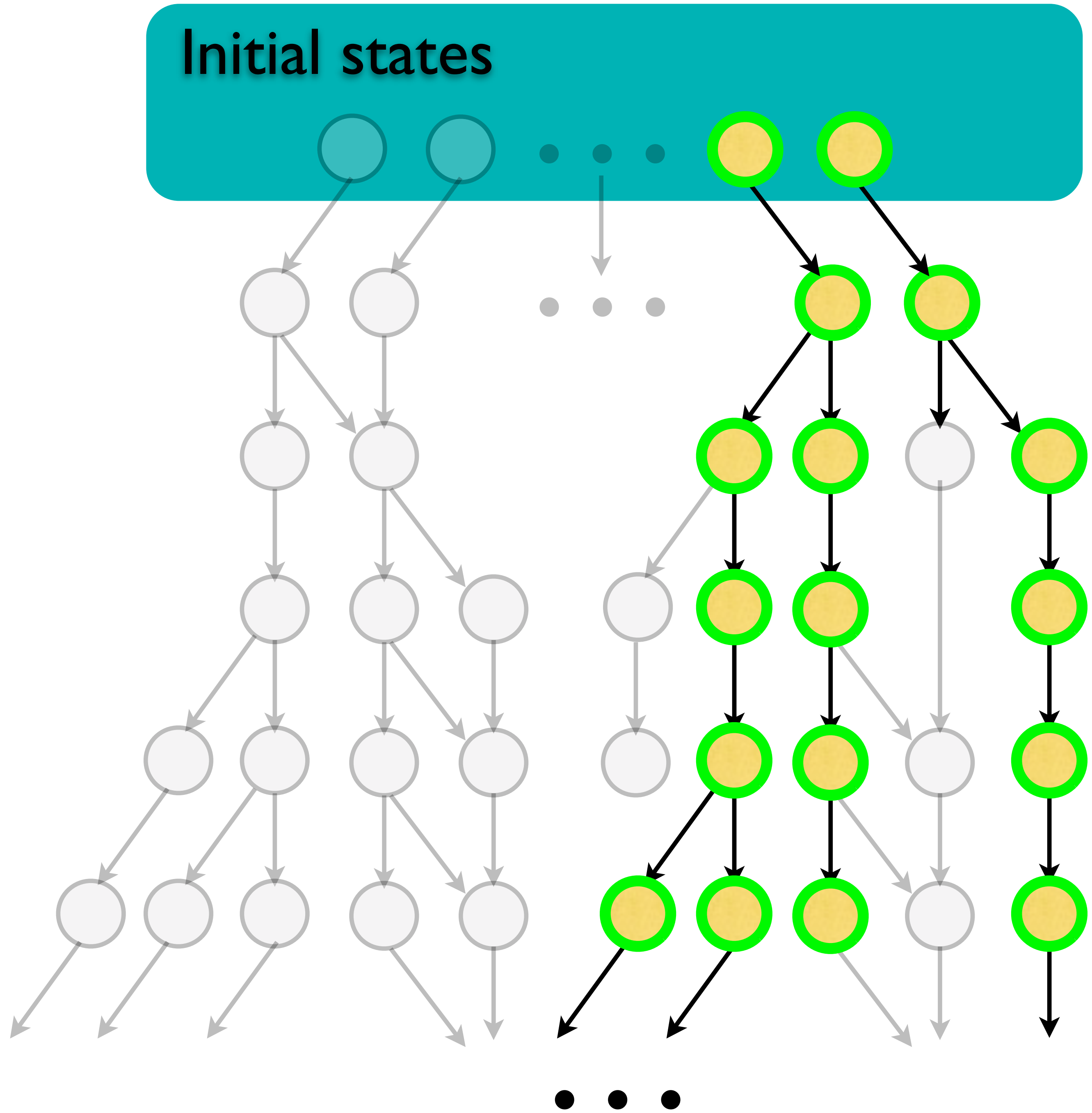
AG and EG (reachability)

EG `yellow`



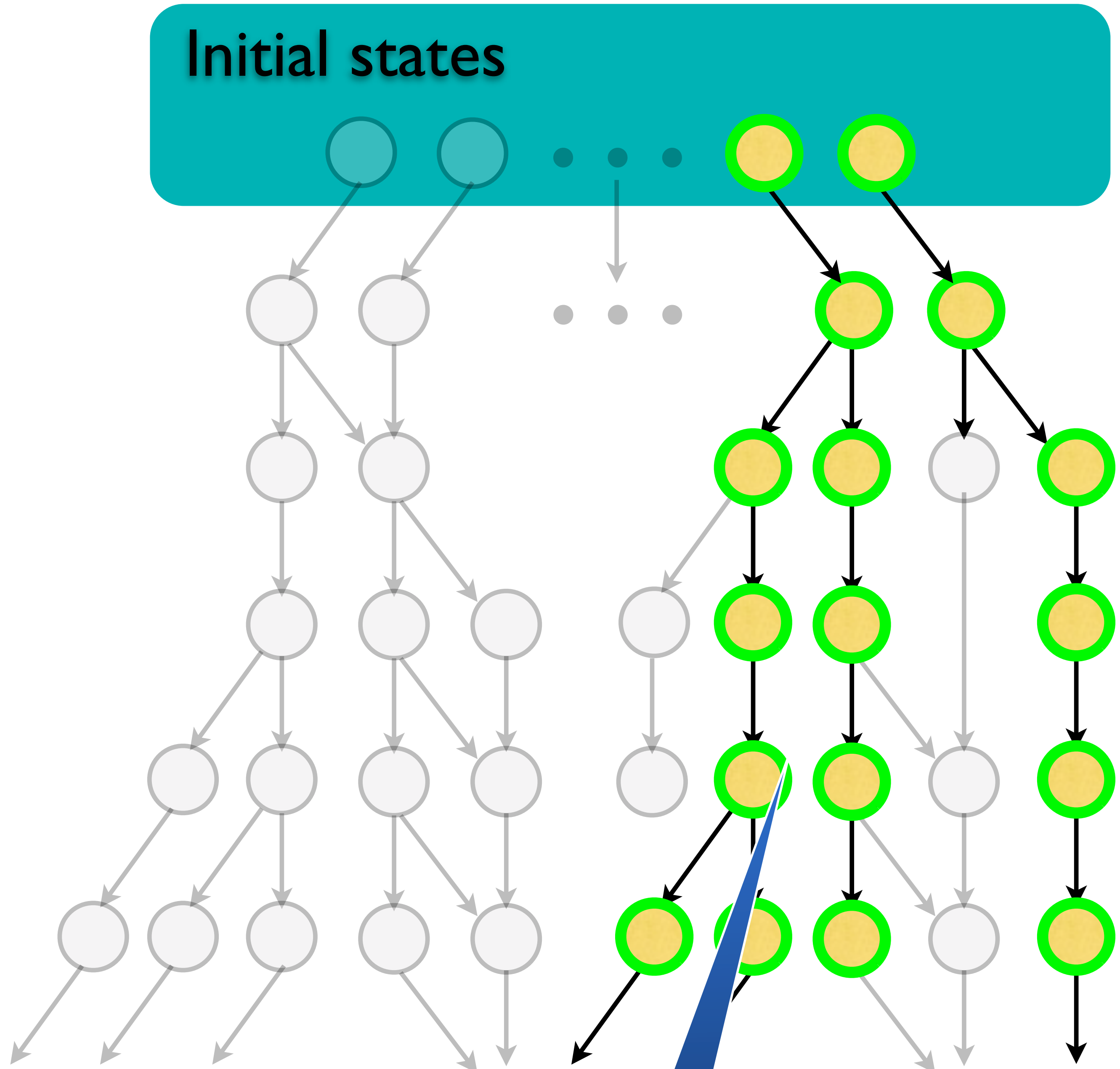
AG and EG (reachability)

EG `yellow`



AG and EG (reachability)

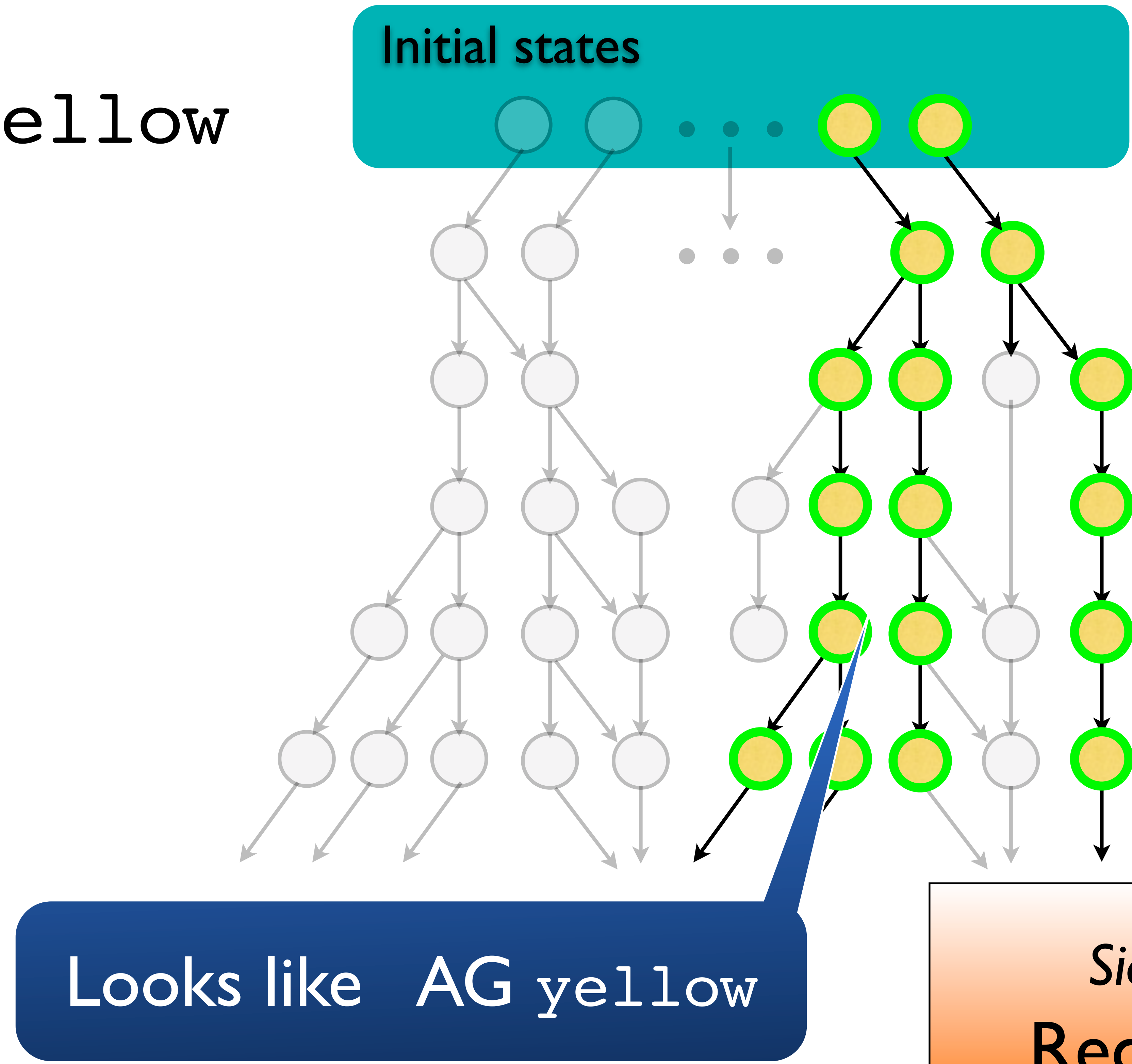
EG `yellow`



Looks like AG `yellow`

AG and EG (reachability)

EG `yellow`

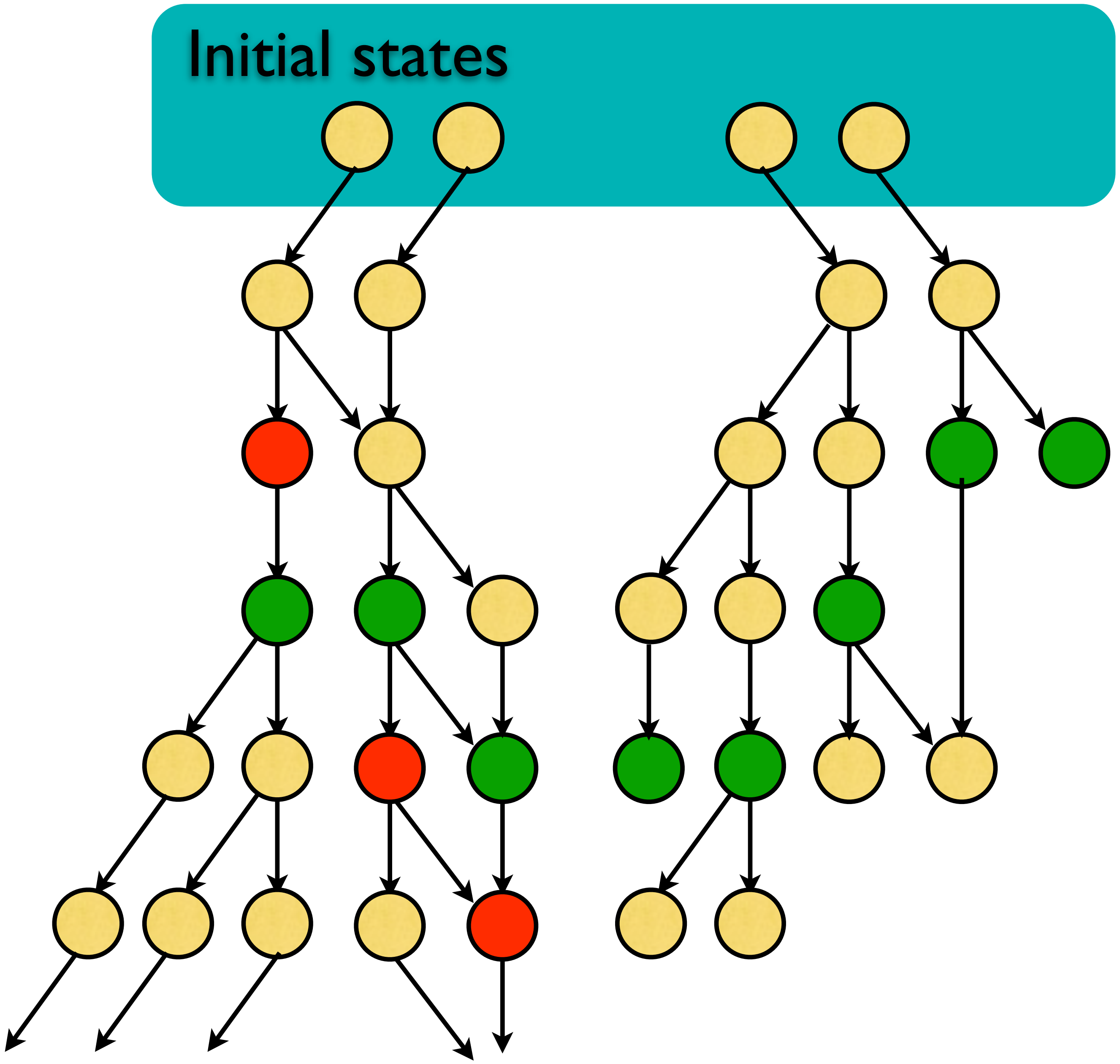


Side Condition:

Recurrent set?

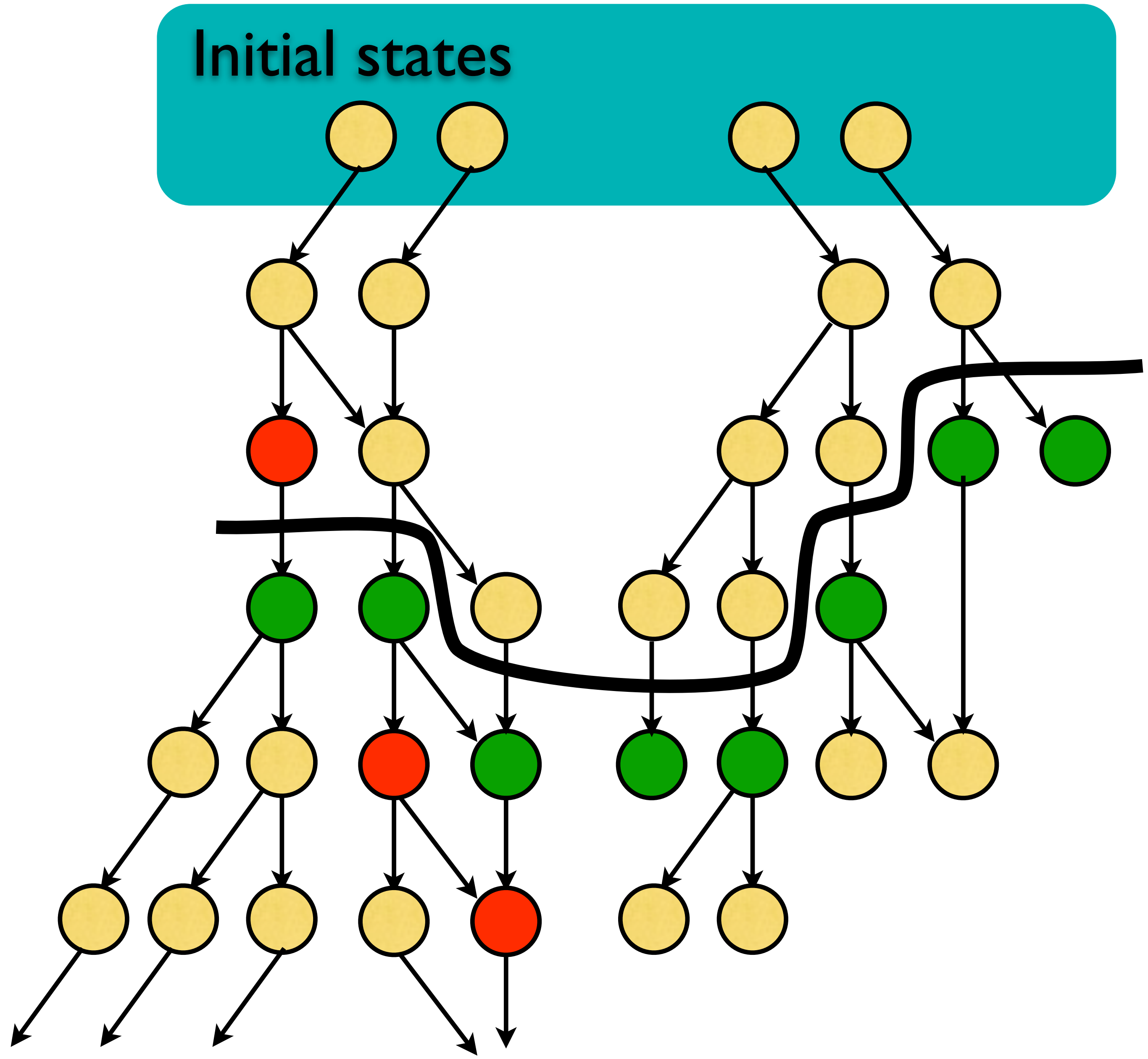
AF and EF (termination)

AF `green`



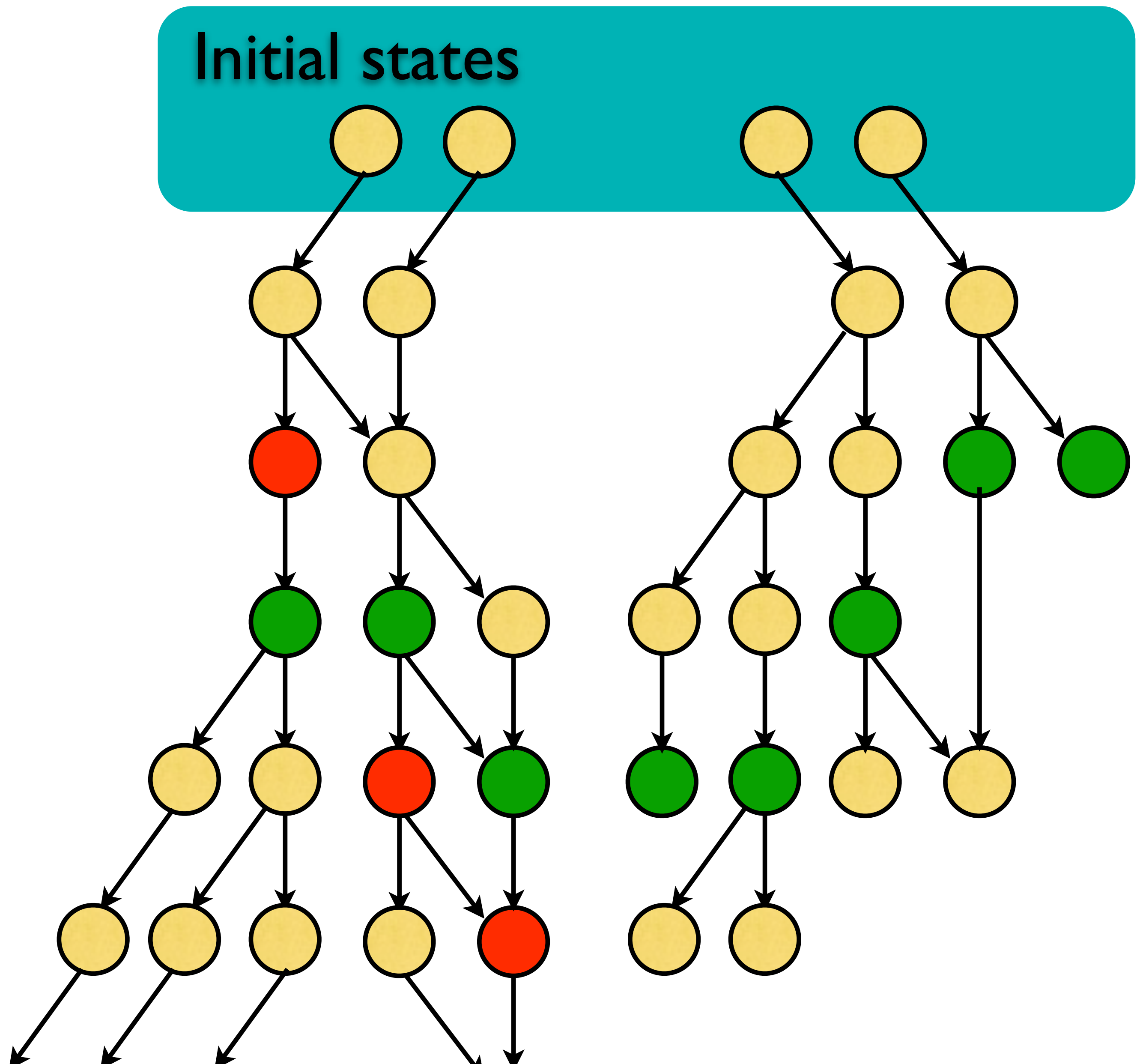
AF and EF (termination)

AF `green`



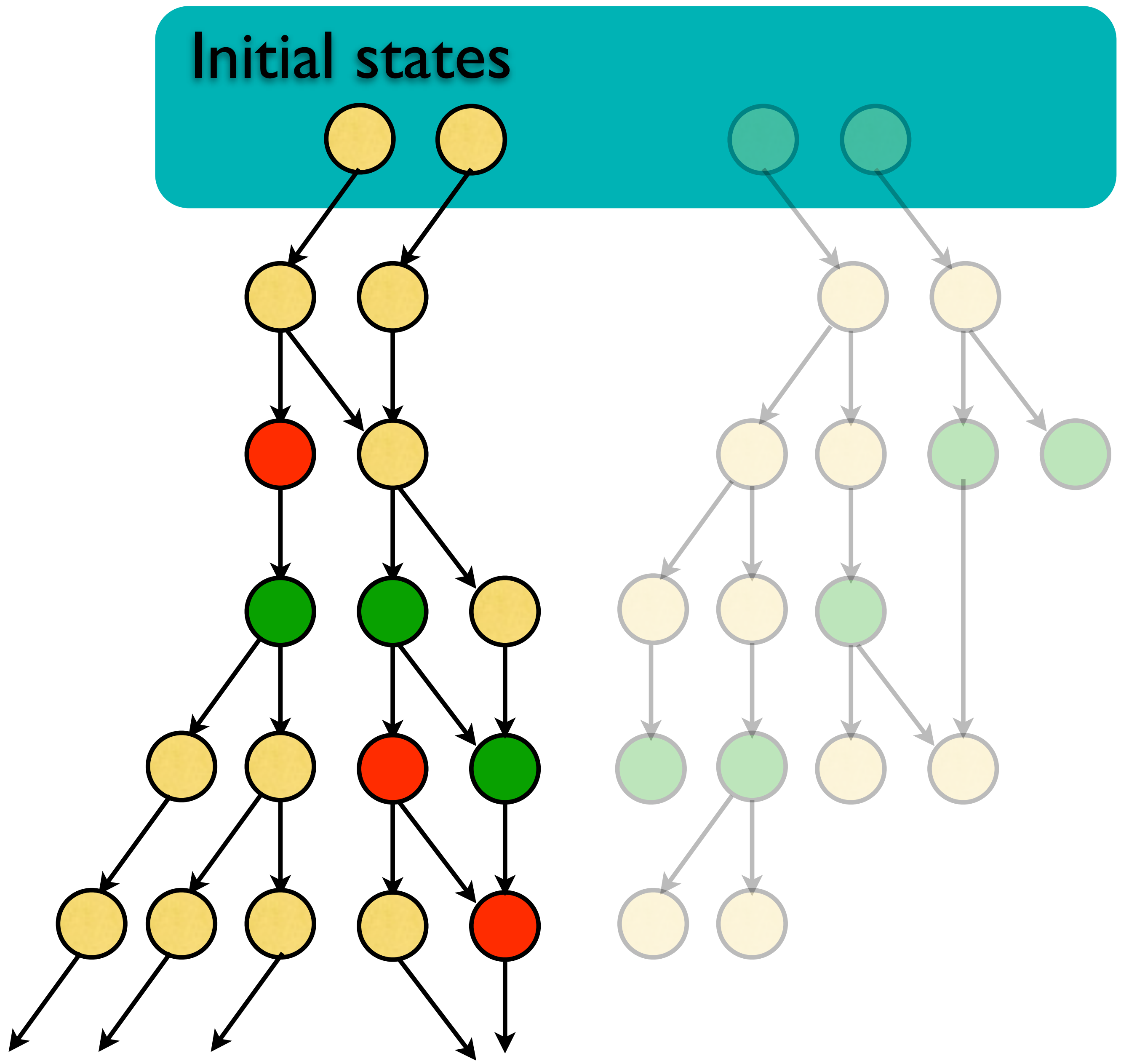
AF and EF (termination)

EF `red`



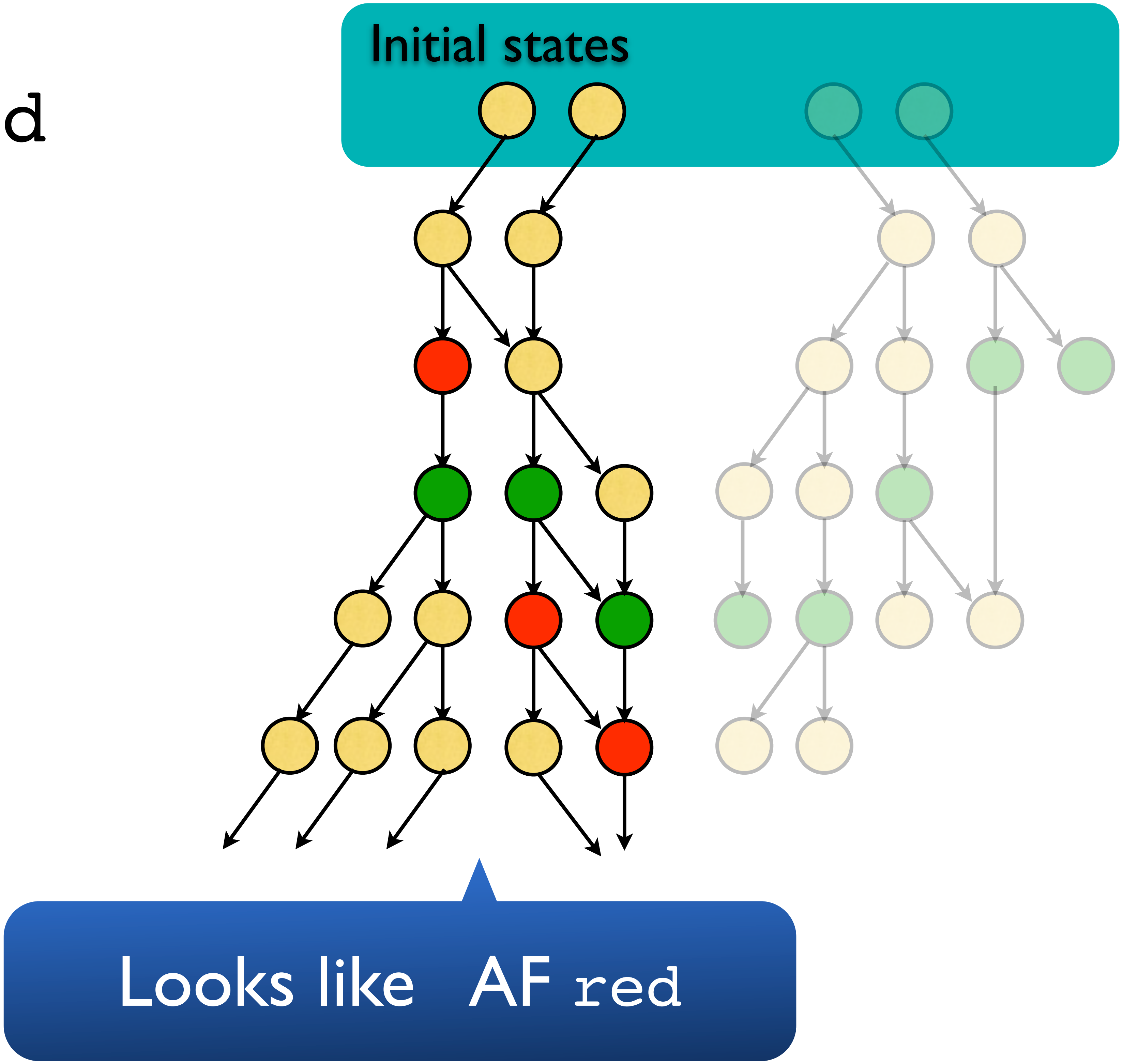
AF and EF (termination)

EF `red`



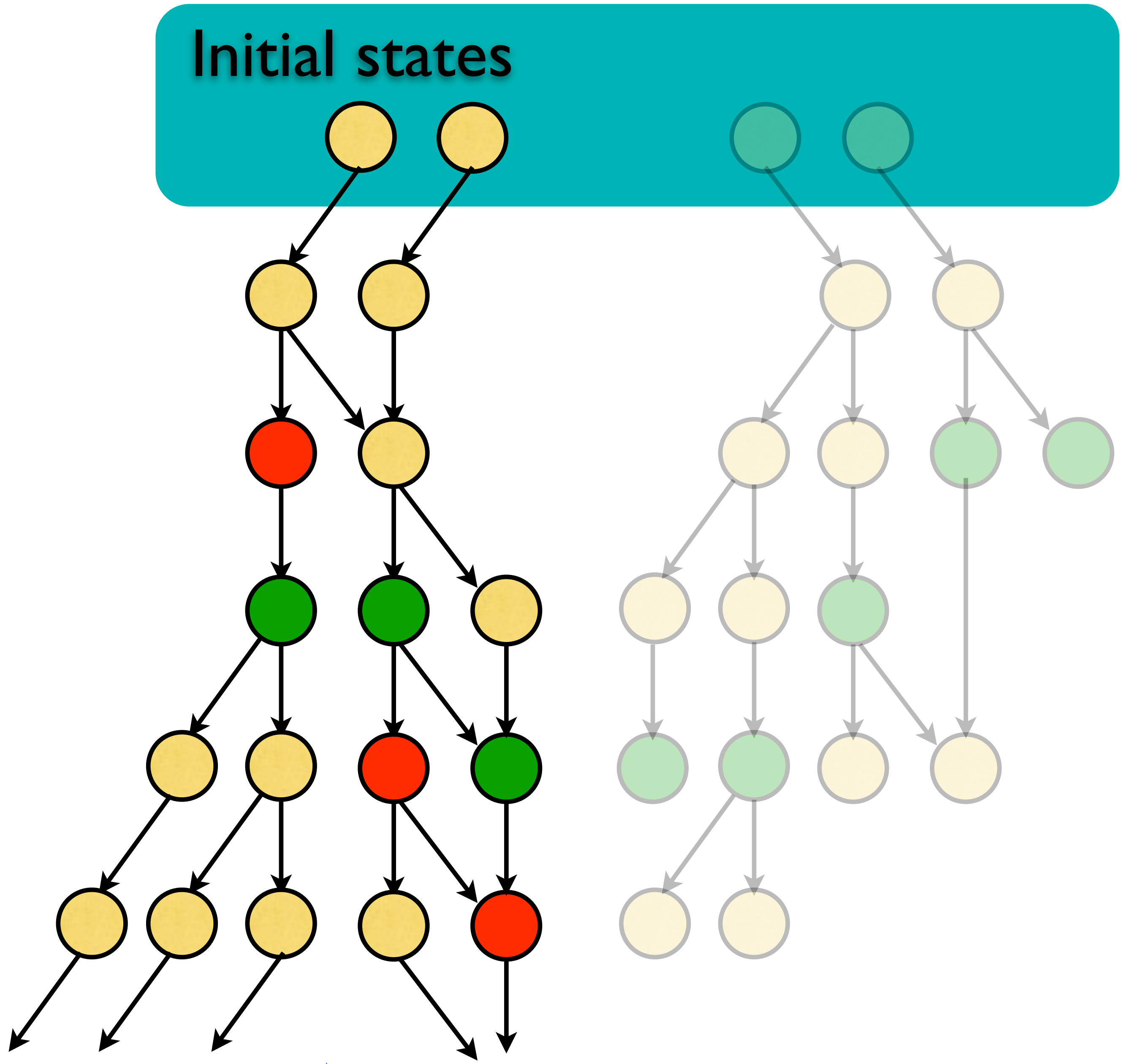
AF and EF (termination)

EF `red`



AF and EF (termination)

EF `red`



Looks like AF `red`

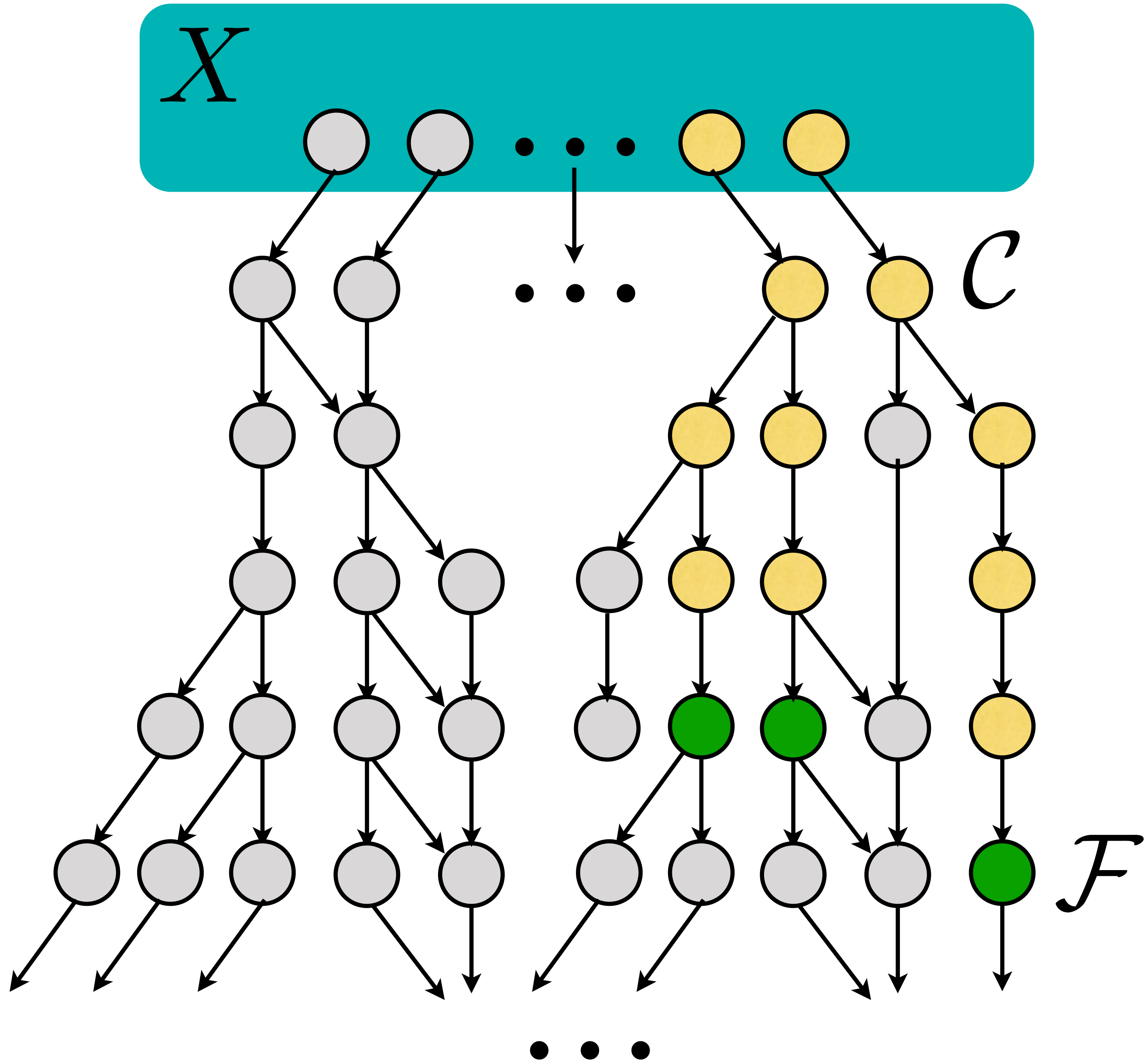
Side Condition:

Recurrent set?

*Treat **universal** and **existential** fragments similarly …*

*Treat **universal** and **existential** fragments similarly ...*

EF `green`

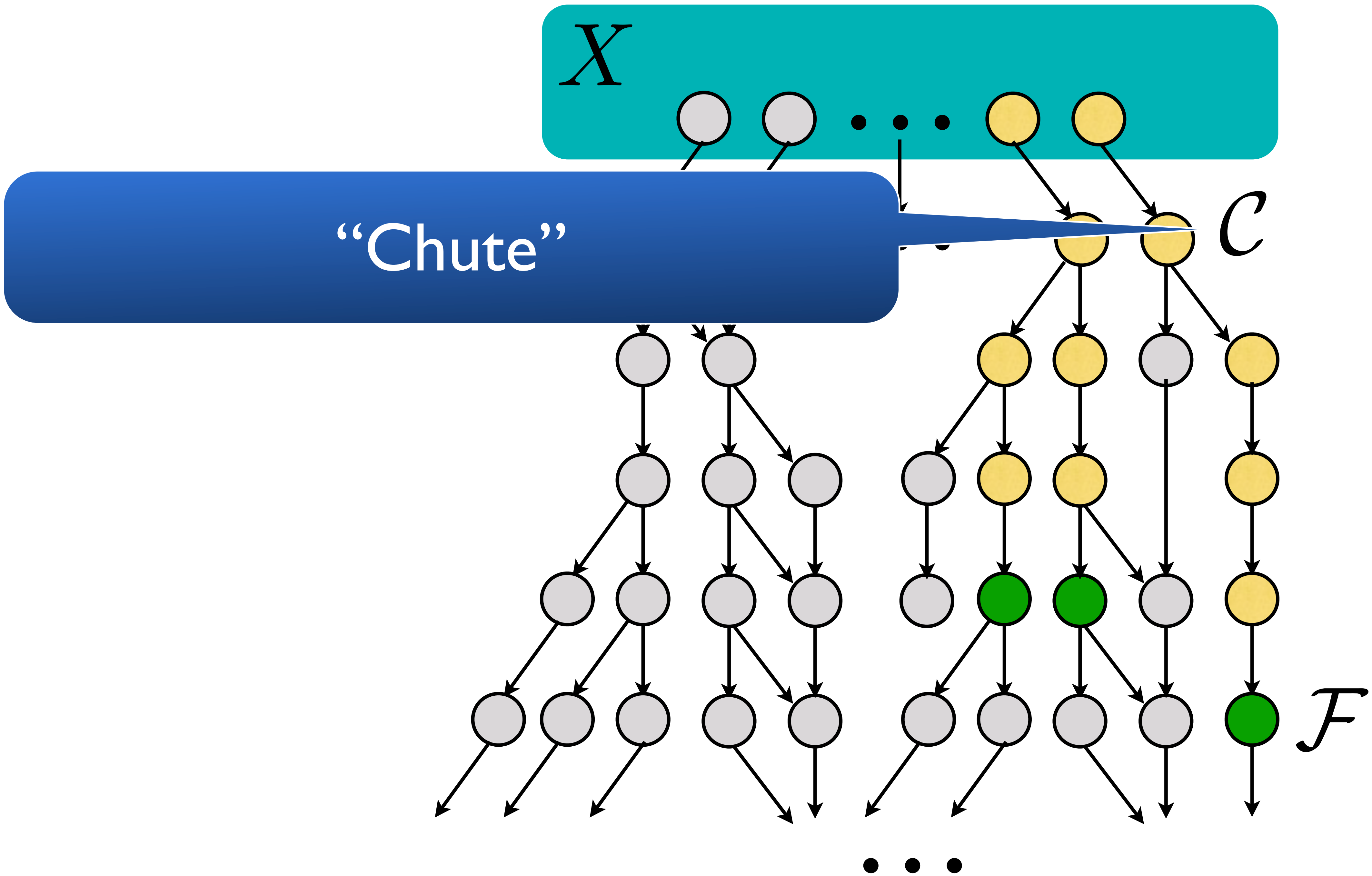


$\mathcal{C} \equiv \{s \mid color(s) = \text{yellow}\}$

$\mathcal{F} \equiv \{s \mid color(s) = \text{green}\}$

*Treat **universal** and **existential** fragments similarly . . .*

EF `green`

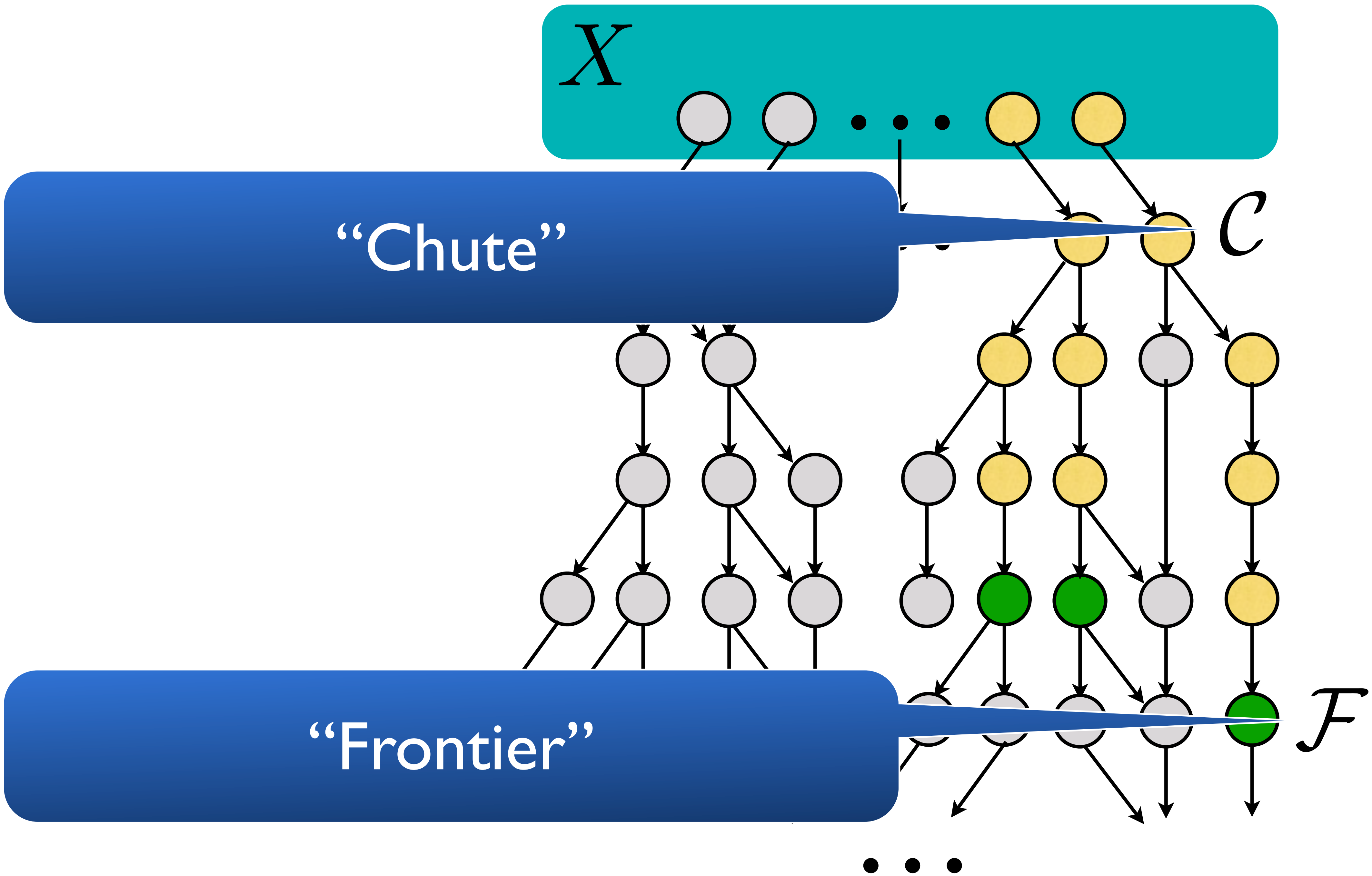


$\mathcal{C} \equiv \{s \mid color(s) = \text{yellow}\}$

$\mathcal{F} \equiv \{s \mid color(s) = \text{green}\}$

*Treat **universal** and **existential** fragments similarly ...*

EF `green`

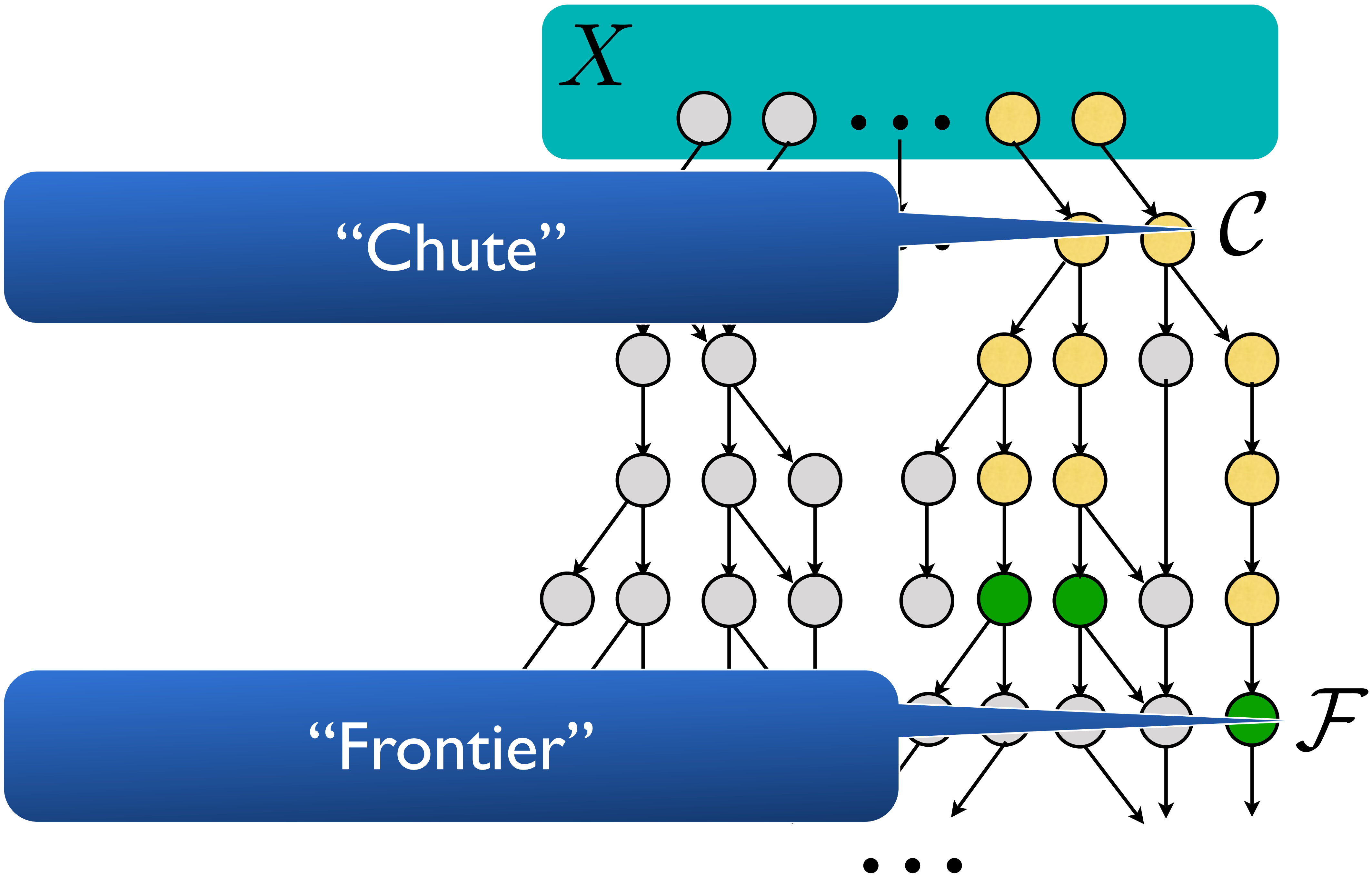


$\mathcal{C} \equiv \{s \mid color(s) = \text{yellow}\}$

$\mathcal{F} \equiv \{s \mid color(s) = \text{green}\}$

*Treat **universal** and **existential** fragments similarly . . .*

EF `green`



$\mathcal{C} \equiv \{s \mid color(s) = \text{yellow}\}$

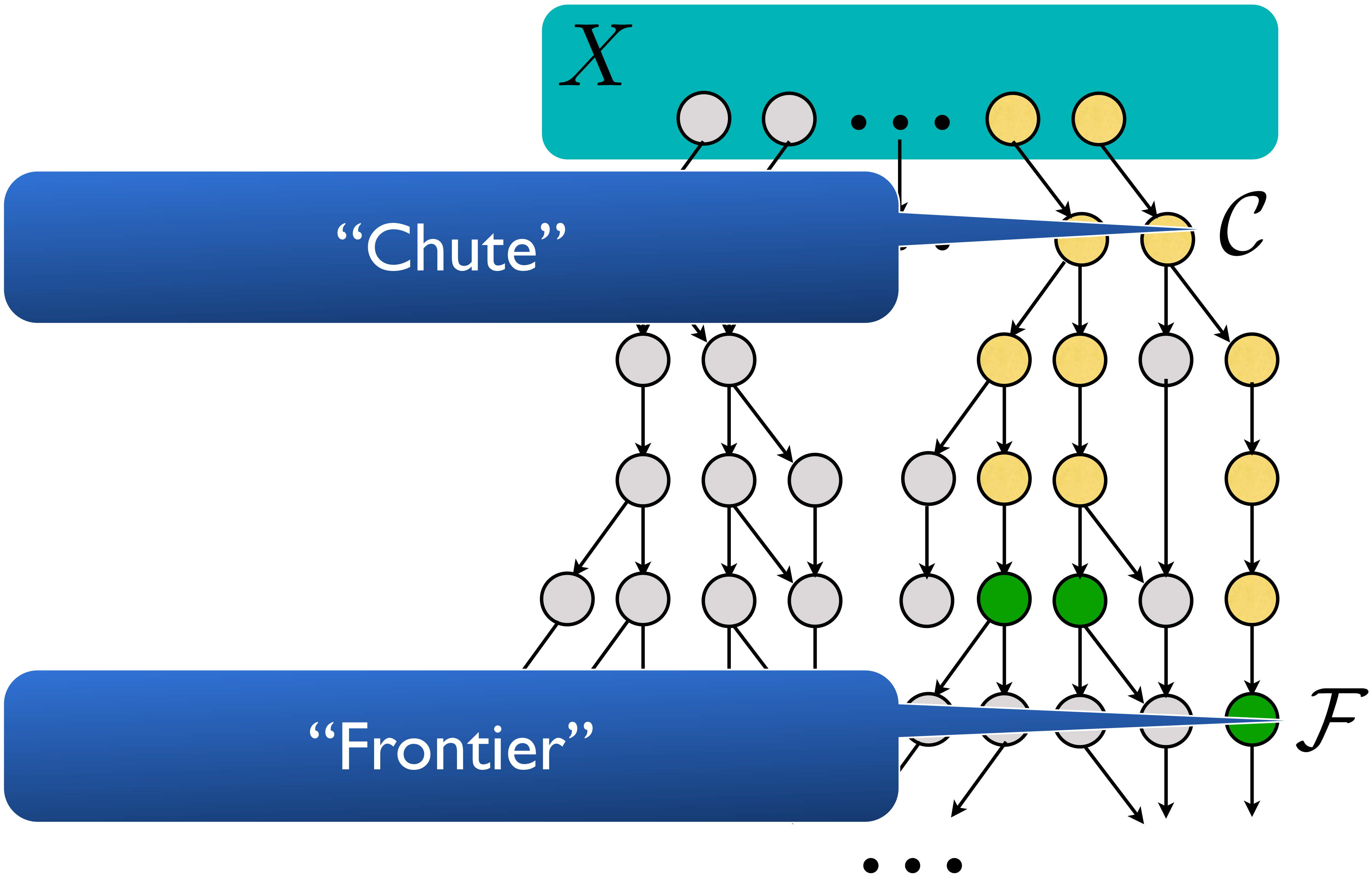
$\mathcal{F} \equiv \{s \mid color(s) = \text{green}\}$

For AFp, chute is simply S

*Treat **universal** and **existential** fragments similarly . . .*

EF `green`

Characterization for CTL . . .



$\mathcal{C} \equiv \{s \mid color(s) = \text{yellow}\}$

$\mathcal{F} \equiv \{s \mid color(s) = \text{green}\}$

For AFp, chute is simply S

Treat ***universal*** *and* ***existential*** *fragments similarly …*

$$X \vdash \Phi$$

*Treat **universal** and **existential** fragments similarly ...*

$X \vdash \Phi$

Set of states

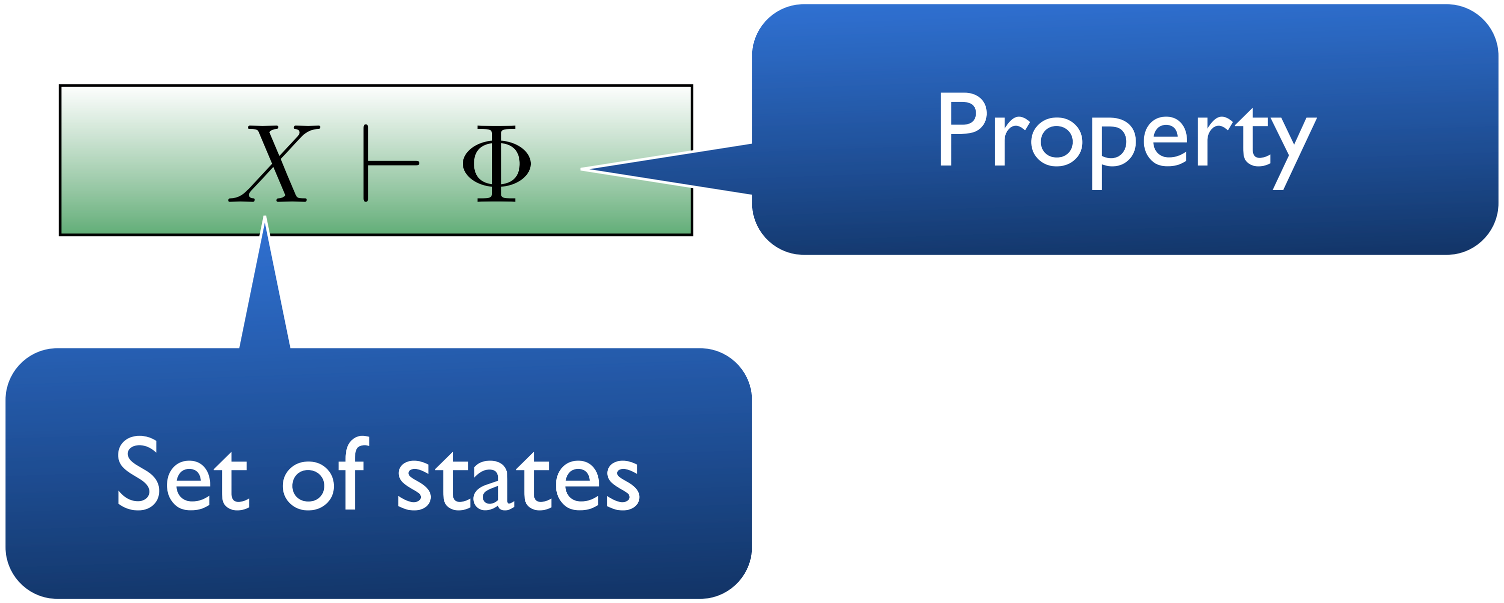
*Treat **universal** and **existential** fragments similarly ...*

$X \vdash \Phi$

Property

Set of states

Treat ***universal*** *and* ***existential*** *fragments similarly …*



Standard CTL semantics

$$
\begin{array}{rcl}
R, s \models \alpha & \iff & s \in [\![\alpha]\!]^{S} \\
R, s \models \Phi_1 \wedge \Phi_2 & \iff & R, s \models \Phi_1 \;\text{ and }\; R, s \models \Phi_2 \\
R, s \models \Phi_1 \vee \Phi_2 & \iff & R, s \models \Phi_1 \;\text{ or }\; R, s \models \Phi_2 \\
R, s \models \mathsf{AF}\Phi & \iff & \forall (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ \exists i \geq 0.\ R, s_i \models \Phi \\
R, s \models \mathsf{EF}\Phi & \iff & \exists (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ \exists i \geq 0.\ R, s_i \models \Phi \\
R, s \models \mathsf{A}[\Phi_1 \;\mathsf{W}\; \Phi_2] & \iff & \forall (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ (\forall i \geq 0.\ R, s_i \models \Phi_1) \vee (\exists j \geq 0.\ R, s \\
R, s \models \mathsf{E}[\Phi_1 \;\mathsf{W}\; \Phi_2] & \iff & \exists (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ (\forall i \geq 0.\ R, s_i \models \Phi_1) \vee (\exists j \geq 0.\ R, s
\end{array}
$$

*Treat **universal** and **existential** fragments similarly …*

$X \vdash \Phi$

Property

Set of states

$$I \vdash \Phi \quad \Longleftrightarrow \quad \forall s \in I.\ s \models \Phi$$

Standard CTL semantics

$$R, s \models \alpha \iff s \in [\![\alpha]\!]^S$$

$$R, s \models \Phi_1 \wedge \Phi_2 \iff R, s \models \Phi_1 \text{ and } R, s \models \Phi_2$$

$$R, s \models \Phi_1 \vee \Phi_2 \iff R, s \models \Phi_1 \text{ or } R, s \models \Phi_2$$

$$R, s \models \mathsf{AF}\Phi \iff \forall (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ \exists i \geq 0.\ R, s_i \models \Phi$$

$$R, s \models \mathsf{EF}\Phi \iff \exists (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ \exists i \geq 0.\ R, s_i \models \Phi$$

$$R, s \models \mathsf{A}[\Phi_1 \ \mathsf{W} \ \Phi_2] \iff \forall (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ (\forall i \geq 0.\ R, s_i \models \Phi_1) \vee (\exists j \geq 0.\ R, s$$

$$R, s \models \mathsf{E}[\Phi_1 \ \mathsf{W} \ \Phi_2] \iff \exists (s_0, s_1, \ldots) \in \Pi(S, R, \{s\}).\ (\forall i \geq 0.\ R, s_i \models \Phi_1) \vee (\exists j \geq 0.\ R, s$$

*Treat **universal** and **existential** fragments similarly …*

$$X \vdash \Phi$$

*Treat **universal** and **existential** fragments similarly ...*

$$X \vdash \Phi$$

$$\frac{X \subseteq [\![\alpha]\!]^{\mathsf{S}}}{X \vdash \alpha}$$

*Treat **universal** and **existential** fragments similarly . . .*

$$X \vdash \Phi$$

$$\frac{X \subseteq [\![\alpha]\!]^{\mathsf{S}}}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2}$$

*Treat **universal** and **existential** fragments similarly …*

$$X \vdash \Phi$$

$$\frac{X \subseteq [\![\alpha]\!]^{\mathsf{S}}}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2}$$

$$\frac{X = X_1 \cup X_2 \quad X_1 \vdash \Phi_1 \quad X_2 \vdash \Phi_2}{X \vdash \Phi_1 \vee \Phi_2}$$

*Treat **universal** and **existential** fragments similarly . . .*

$X \vdash \Phi$

$$\frac{X \subseteq [\![\alpha]\!]^{\mathsf{S}}}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad X = X$$

Decompose temporal operators:

$$\begin{array}{lll} \gamma & ::= & \mathsf{F}\Phi \mid [\Phi\ \mathsf{W}\ \Phi] \\ \Phi & ::= & \alpha \mid \Phi \vee \Phi \mid \Phi \wedge \Phi \mid \mathsf{A}\gamma \mid \mathsf{E}\gamma \end{array}$$

*Similar to CTL**

*Treat **universal** and **existential** fragments similarly ...*

$X \vdash \Phi$

$$\frac{X \subseteq [\![\alpha]\!]^S}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad \frac{X = X}{}$$

$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$

Second kind of judgement

Decompose temporal operators:

$$\gamma ::= \mathsf{F}\Phi \mid [\Phi\ \mathsf{W}\ \Phi]$$
$$\Phi ::= \alpha \mid \Phi \vee \Phi \mid \Phi \wedge \Phi \mid \mathsf{A}\gamma \mid \mathsf{E}\gamma$$

*Similar to CTL**

Treat ***universal*** *and* ***existential*** *fragments similarly …*

$$X \vdash \Phi$$

$$\frac{X \subseteq [\![\alpha]\!]^{\mathsf{S}}}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad \frac{X = X \ldots}{}$$

$$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$$

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

Treat ***universal*** *and* ***existential*** *fragments similarly ...*

$$X \vdash \Phi$$

$$\frac{X \subseteq [\![\alpha]\!]^S}{X \vdash \alpha}$$

$$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$$

Side Condition:

Recurrent set?

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

Treat **universal** and **existential** fragments similarly …

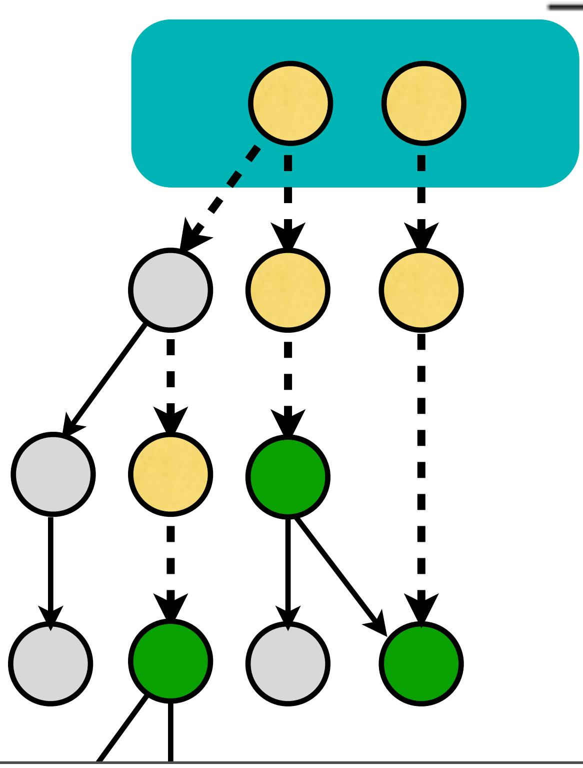
$X \vdash \Phi$

$$\frac{X \subseteq [\![\alpha]\!]^S}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad \frac{X = X}{}$$

$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \quad \mathcal{F} \vdash \Phi}{X, \mathcal{C}, \mathcal{F} \Vdash \mathsf{F}\Phi}$$



Walk

$$\frac{s \in X \quad (s,t) \in R \quad s \notin \mathcal{F} \quad s,t \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t)}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t) \quad (t,u) \in R \quad t \notin \mathcal{F} \quad u \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(t,u)}$$

*Treat **universal** and **existential** fragments similarly ...*

$$X \vdash \Phi$$

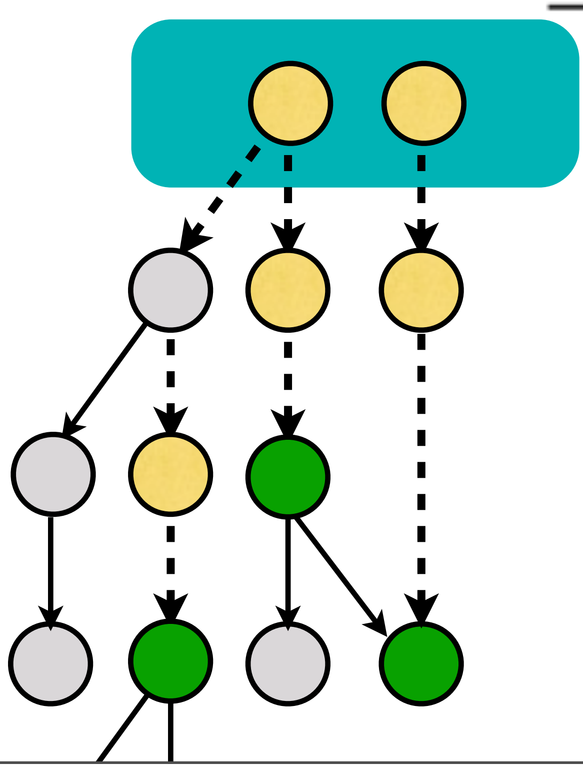
$$\frac{X \subseteq [\![\alpha]\!]^S}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad \frac{X = X}{}$$

$$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$$

Termination

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \quad \mathcal{F} \vdash \Phi}{X, \mathcal{C}, \mathcal{F} \Vdash \mathsf{F}\Phi}$$



Walk

$$\frac{s \in X \quad (s,t) \in R \quad s \notin \mathcal{F} \quad s,t \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t)}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t) \quad (t,u) \in R \quad t \notin \mathcal{F} \quad u \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(t,u)}$$

*Treat **universal** and **existential** fragments similarly …*

$X \vdash \Phi$

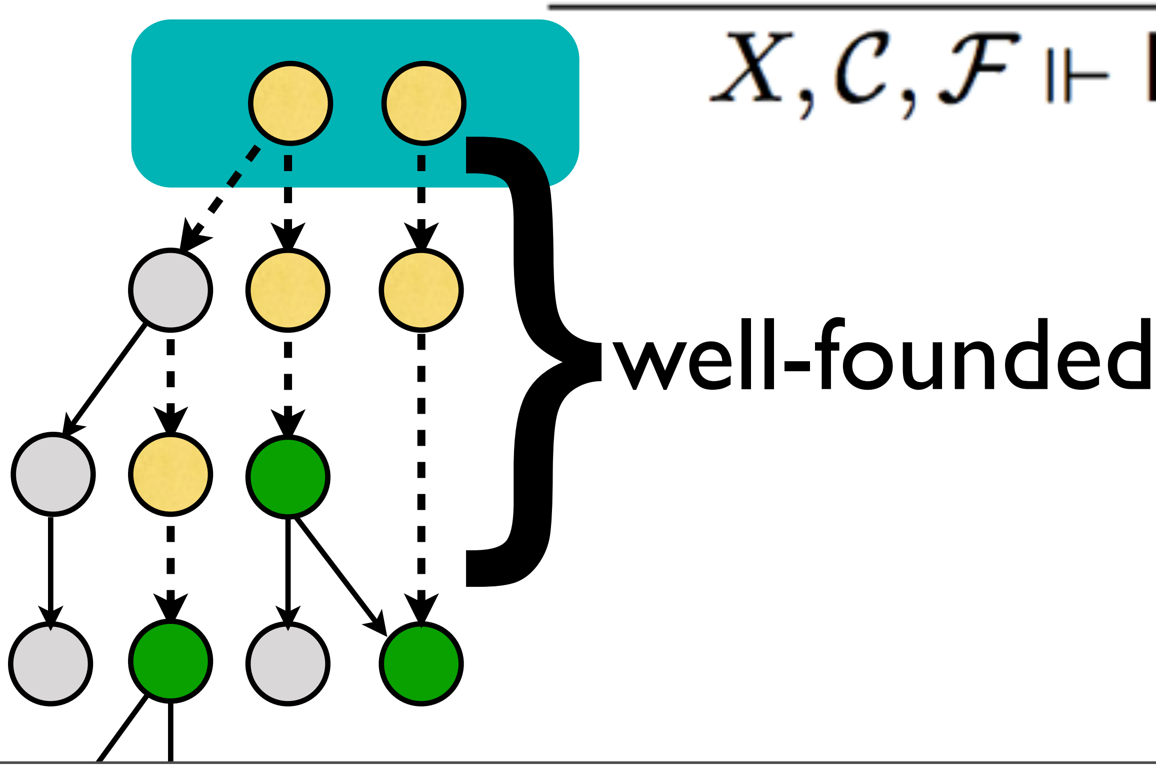
$$\frac{X \subseteq [\![\alpha]\!]^S}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad X = X$$

$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$

Termination

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \quad \mathcal{F} \vdash \Phi}{X, \mathcal{C}, \mathcal{F} \Vdash \mathsf{F}\Phi}$$



Walk

$$\frac{s \in X \quad (s,t) \in R \quad s \notin \mathcal{F} \quad s,t \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t)}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t) \quad (t,u) \in R \quad t \notin \mathcal{F} \quad u \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(t,u)}$$

*Treat **universal** and **existential** fragments similarly ...*

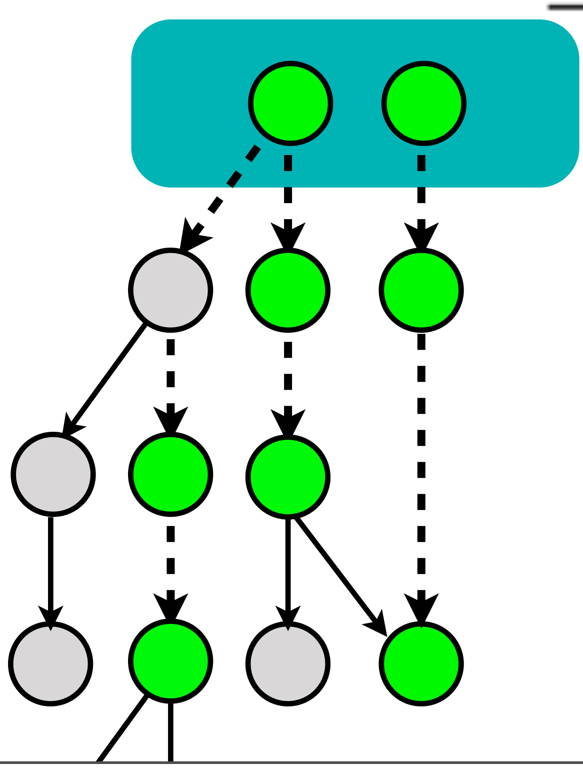
$X \vdash \Phi$

$$\frac{X \subseteq [\![\alpha]\!]^S}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad \frac{X = X}{}$$

$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \quad \mathcal{F} \vdash \Phi}{X, \mathcal{C}, \mathcal{F} \Vdash \mathsf{F}\Phi} \qquad \frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}|_1 \vdash \Phi_1 \quad \mathcal{F} \vdash \Phi_2}{X, \mathcal{C}, \mathcal{F} \Vdash [\Phi_1 \ \mathsf{W} \ \Phi_2]}$$



Walk

$$\frac{s \in X \quad (s,t) \in R \quad s \notin \mathcal{F} \quad s,t \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t)}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t) \quad (t,u) \in R \quad t \notin \mathcal{F} \quad u \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(t,u)}$$

*Treat **universal** and **existential** fragments similarly ...*

$$X \vdash \Phi$$

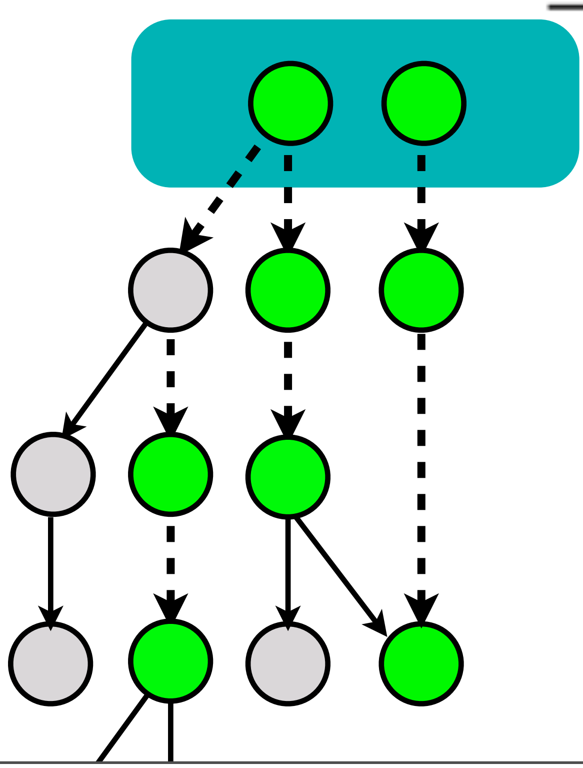
$$\frac{X \subseteq [\![\alpha]\!]^{S}}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2} \qquad \frac{X = X}{}$$

$$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$$

Safety

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rc}\ldots \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \quad \mathcal{F} \vdash \Phi}{X, \mathcal{C}, \mathcal{F} \Vdash \mathsf{F}\Phi} \qquad \frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}|_1 \vdash \Phi_1 \quad \mathcal{F} \vdash \Phi_2}{X, \mathcal{C}, \mathcal{F} \Vdash [\Phi_1 \ \mathsf{W} \ \Phi_2]}$$



$$\frac{s \in X \quad (s,t) \in R \quad s \notin \mathcal{F} \quad s,t \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t)}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(s,t) \quad (t,u) \in R \quad t \notin \mathcal{F} \quad u \in \mathcal{C}}{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}(t,u)}$$

Walk

Treat ***universal*** *and* ***existential*** *fragments similarly …*

$X \vdash \Phi$

$$\frac{X \subseteq [\![\alpha]\!]^{\mathsf{S}}}{X \vdash \alpha} \qquad \frac{X \vdash \Phi_1 \quad X \vdash \Phi_2}{X \vdash \Phi_1 \wedge \Phi_2}$$

$$\frac{X = X_1 \cup X_2 \quad X_1 \vdash \Phi_1 \quad X_2 \vdash \Phi_2}{X \vdash \Phi_1 \vee \Phi_2}$$

$$\frac{X, S, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{A}\gamma} \qquad \frac{(X, \mathcal{C}, \mathcal{F}) \text{ is rcr} \quad X, \mathcal{C}, \mathcal{F} \Vdash \gamma}{X \vdash \mathsf{E}\gamma}$$

$$\frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \quad \mathcal{F} \vdash \Phi}{X, \mathcal{C}, \mathcal{F} \Vdash \mathsf{F}\Phi} \qquad \frac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}}|_1 \vdash \Phi_1 \quad \mathcal{F} \vdash \Phi_2}{X, \mathcal{C}, \mathcal{F} \Vdash [\Phi_1 \ \mathsf{W}\ \Phi_2]}$$

Soundness and Completeness

Proof System

$I \vdash \Phi$

$\Longleftrightarrow$

CTL semantics

$\forall s \in I.\ s \models \Phi$

*Treat **universal** and **existential** fragments similarly …*

$$X \vdash \Phi$$

$$X, \mathcal{C}, \mathcal{F} \Vdash \gamma$$

- *Sets-of-states* rather than singleton states
- Works well for infinite state spaces
- *Partition* rather than *enumerate* states
- Symbolic representations/overapproximations
- *We believe it will work well in practice...*

Side Condition:

Recurrent set?

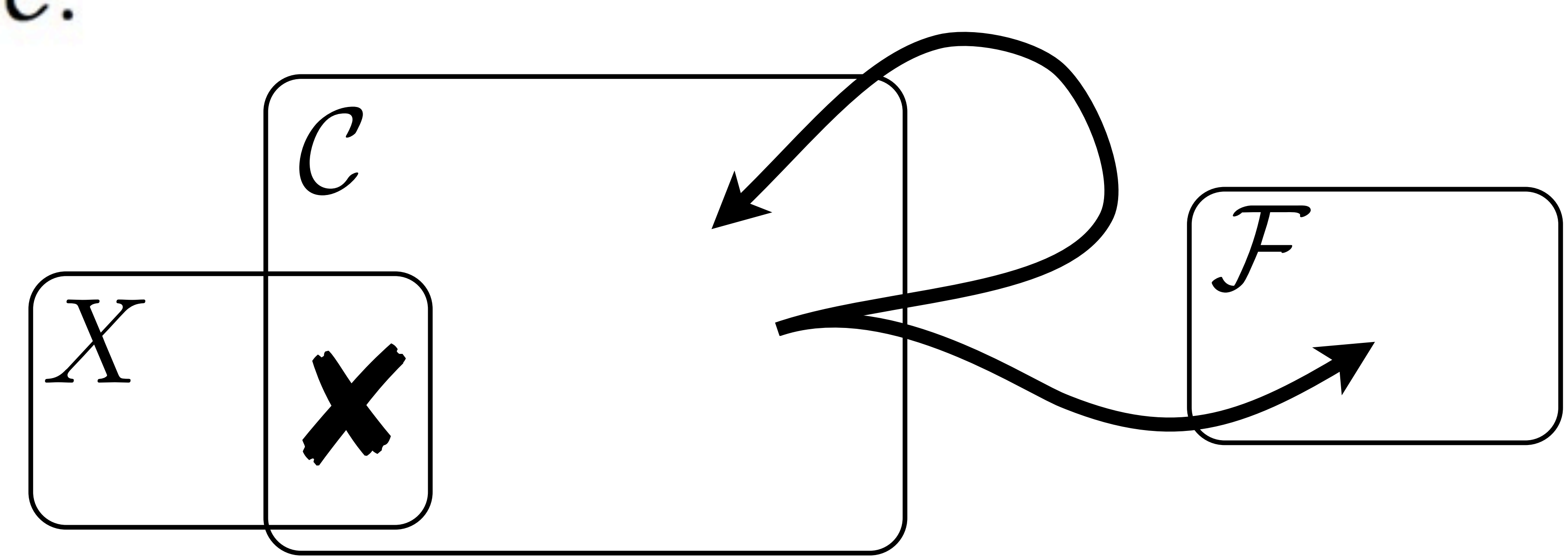
Recurrence set. For sets of states $X, \mathcal{C}, \mathcal{F}$ and transition relation R, we say that $\mathcal{C}$ is a *recurrence set* with respect to X and $\mathcal{F}$ (denoted $(X, \mathcal{C}, \mathcal{F})$ is rcr) provided either $X \cap \mathcal{F} \neq \varnothing$ or both:

1. $X \cap \mathcal{C} \neq \varnothing$
2. For every $x \in \mathcal{C}$, there exists x' such that $(x, x') \in R$ and $x' \in \mathcal{F} \vee x' \in \mathcal{C}$.

Side Condition:
Recurrent set?

Recurrence set. For sets of states $X, \mathcal{C}, \mathcal{F}$ and transition relation R, we say that $\mathcal{C}$ is a *recurrence set* with respect to X and $\mathcal{F}$ (denoted $(X, \mathcal{C}, \mathcal{F})$ is rcr) provided either $X \cap \mathcal{F} \neq \varnothing$ or both:

1. $X \cap \mathcal{C} \neq \varnothing$
2. For every $x \in \mathcal{C}$, there exists x' such that $(x, x') \in R$ and $x' \in \mathcal{F} \vee x' \in \mathcal{C}$.



Side Condition:

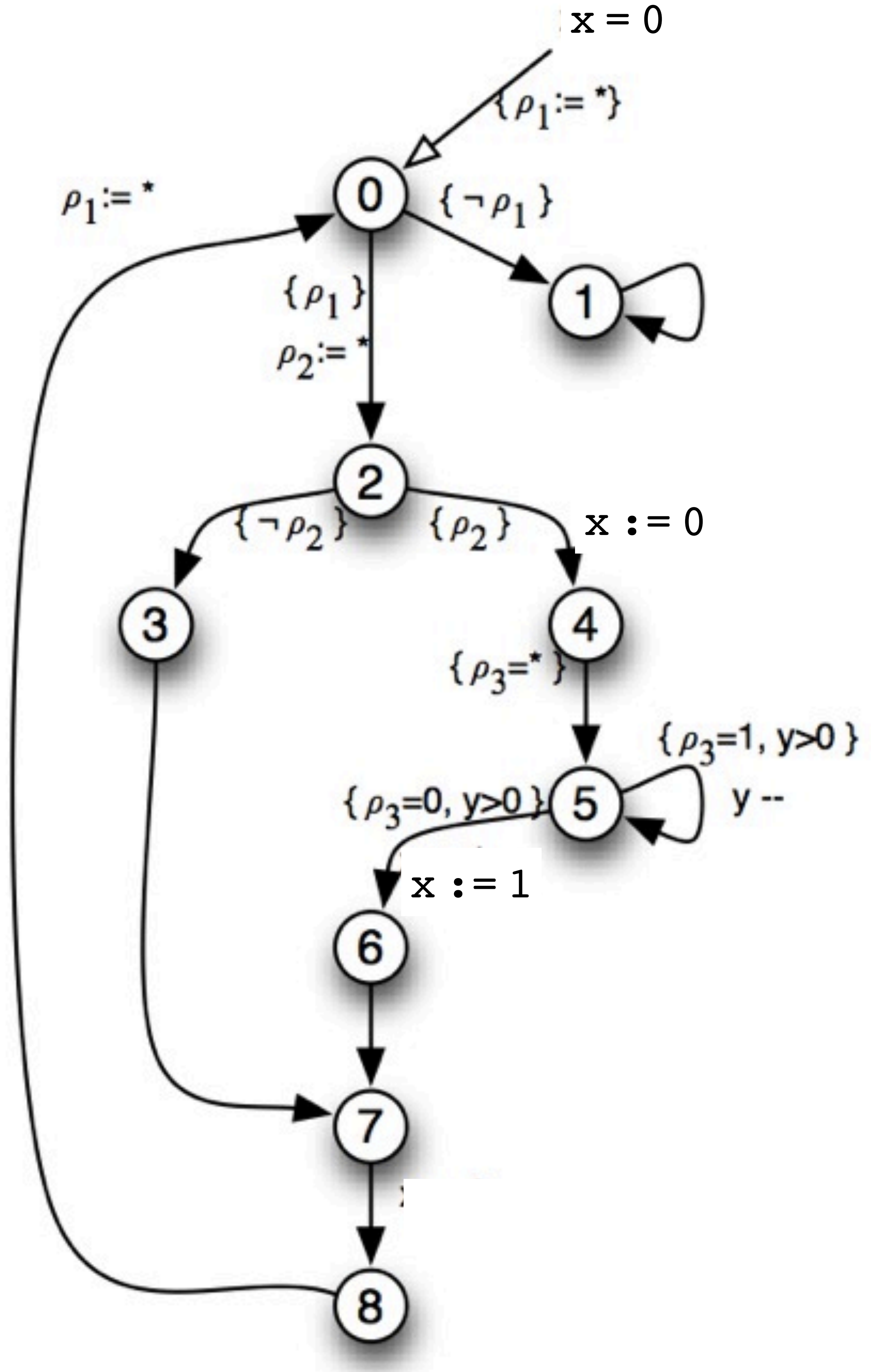
Recurrent set?

Recurrence set. For sets of states $X, \mathcal{C}, \mathcal{F}$ and transition relation R, we say that $\mathcal{C}$ is a *recurrence set* with respect to X and $\mathcal{F}$ (denoted $(X, \mathcal{C}, \mathcal{F})$ is rcr) provided either $X \cap \mathcal{F} \neq \emptyset$ or both:

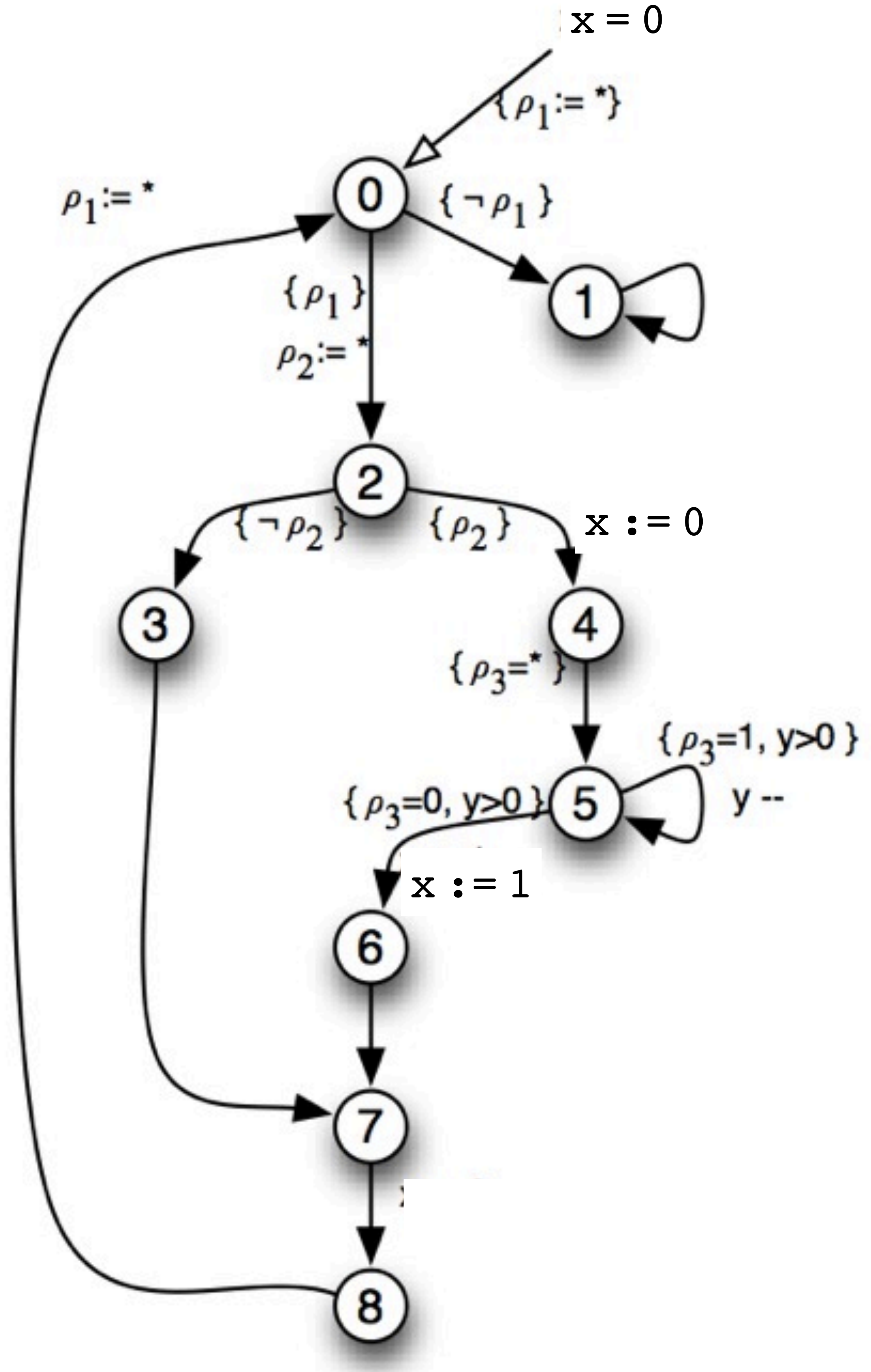
1. $X \cap \mathcal{C} \neq \emptyset$
2. For every $x \in \mathcal{C}$, there exists x' such that $(x, x') \in R$ and $x' \in \mathcal{F} \vee x' \in \mathcal{C}$.

In practice,

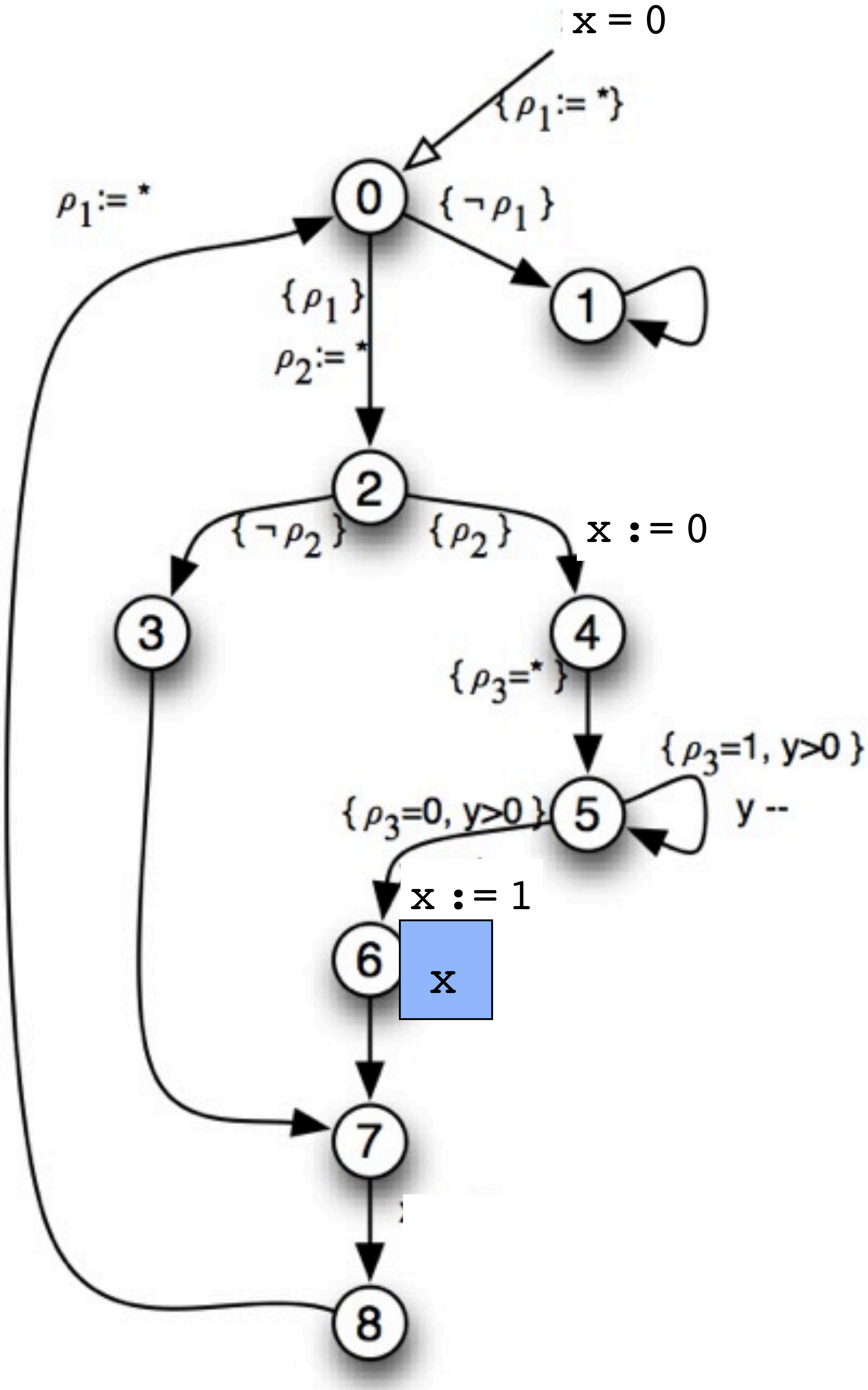
1. Guess an invariant I for chute C (using, e.g., Octagon)
2. Check that I is recurrent set (using an SMT solver)



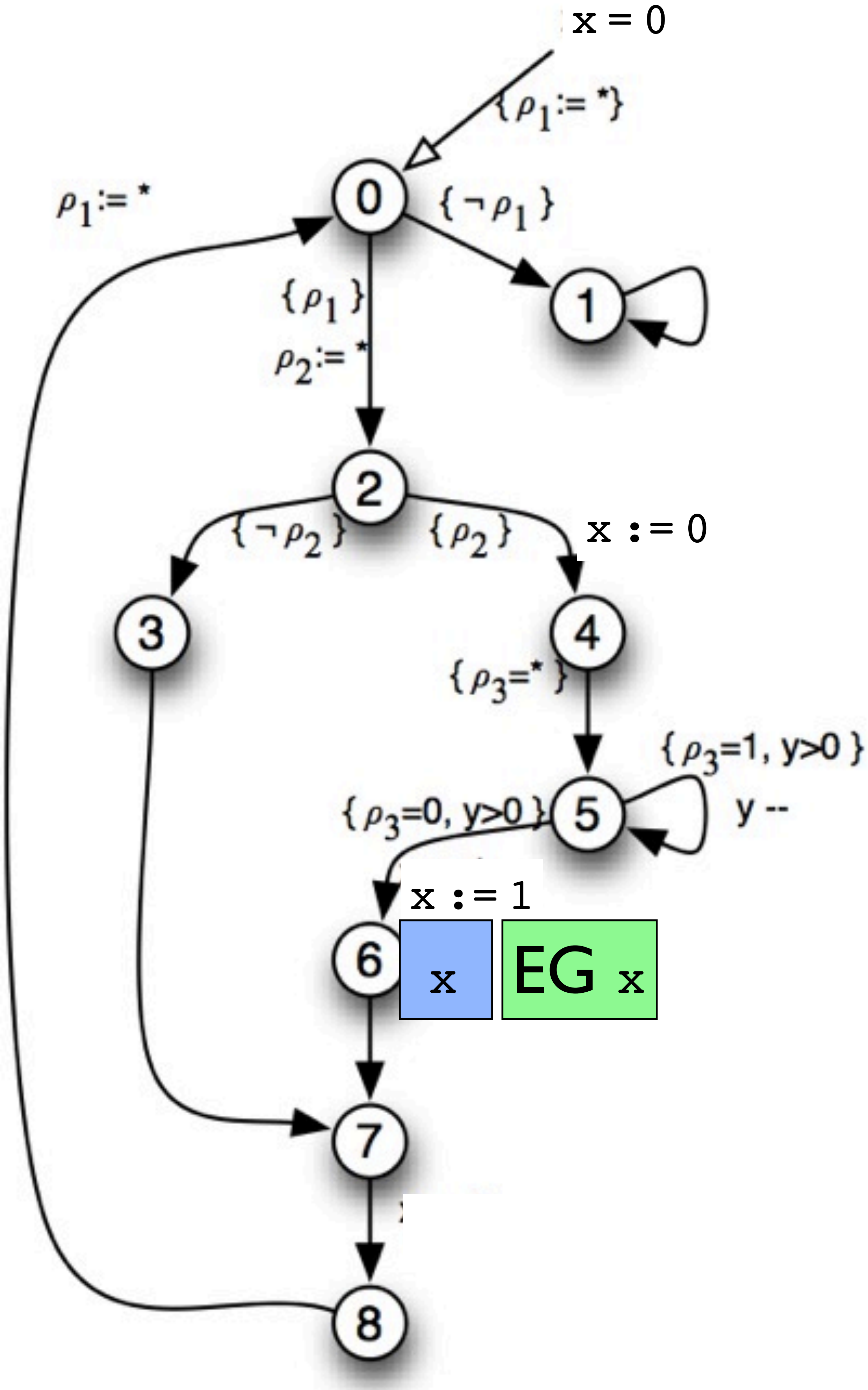
EF (AF (EG x))



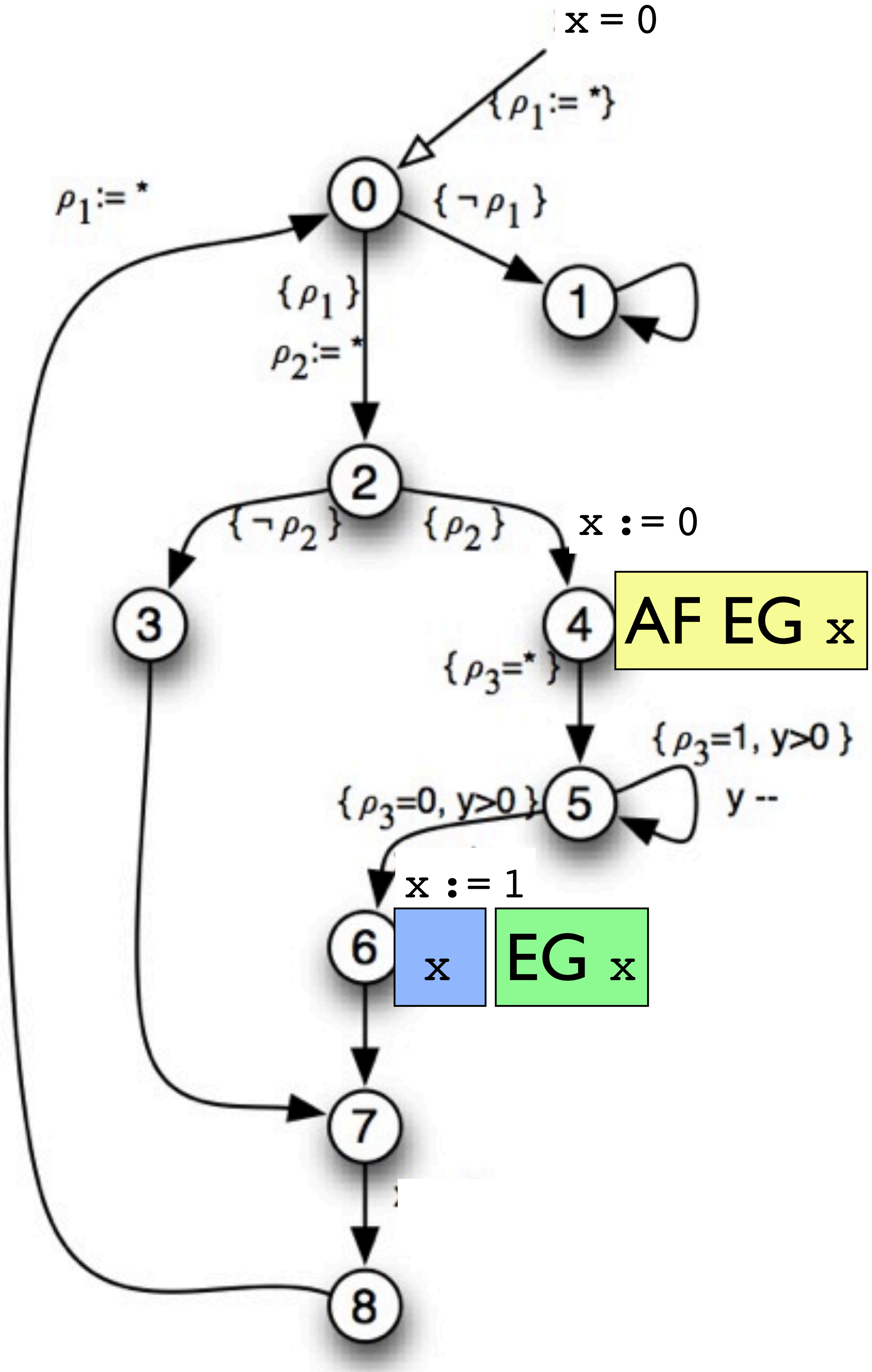
EF (AF (EG x))



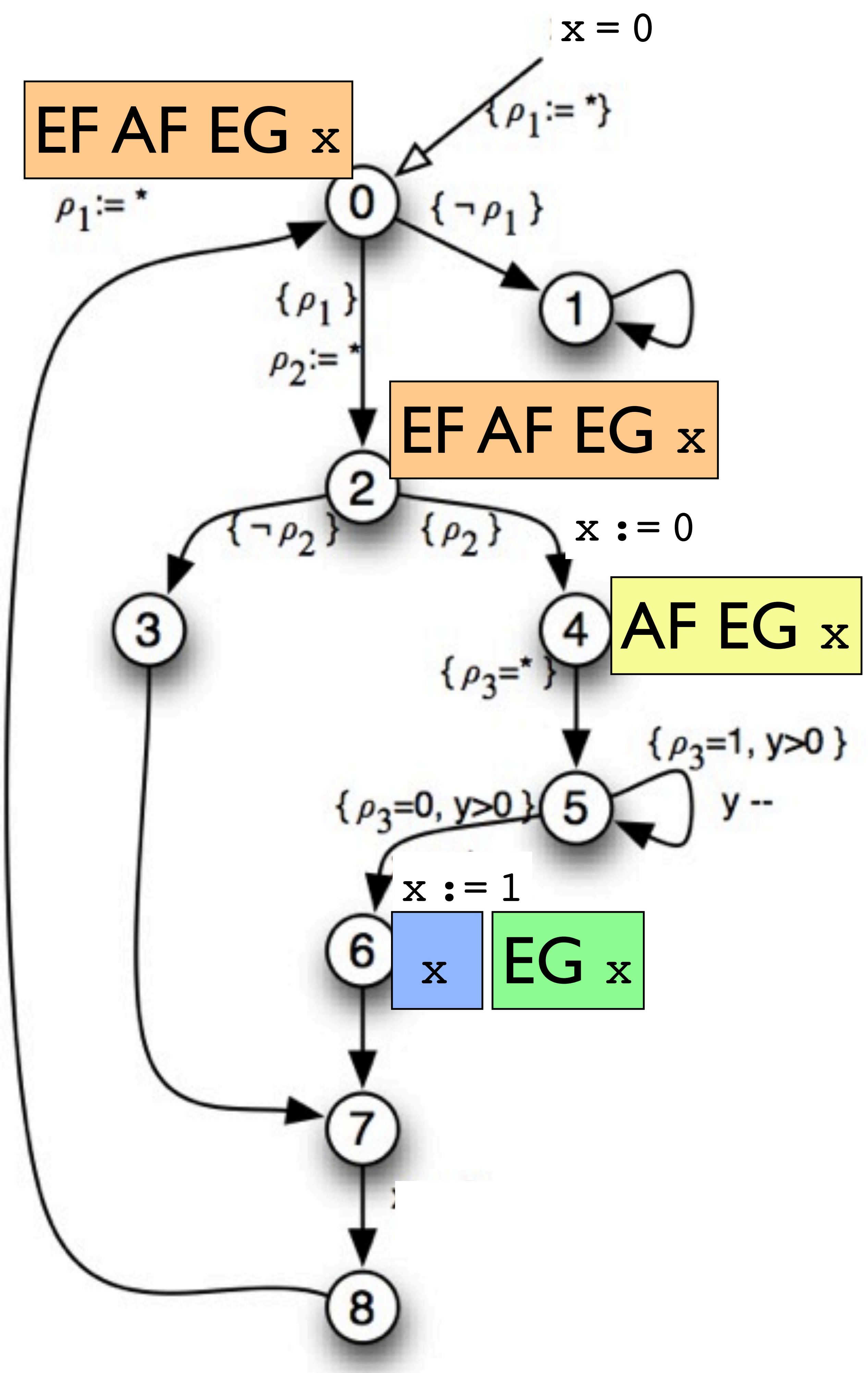
EF (AF (EG x))



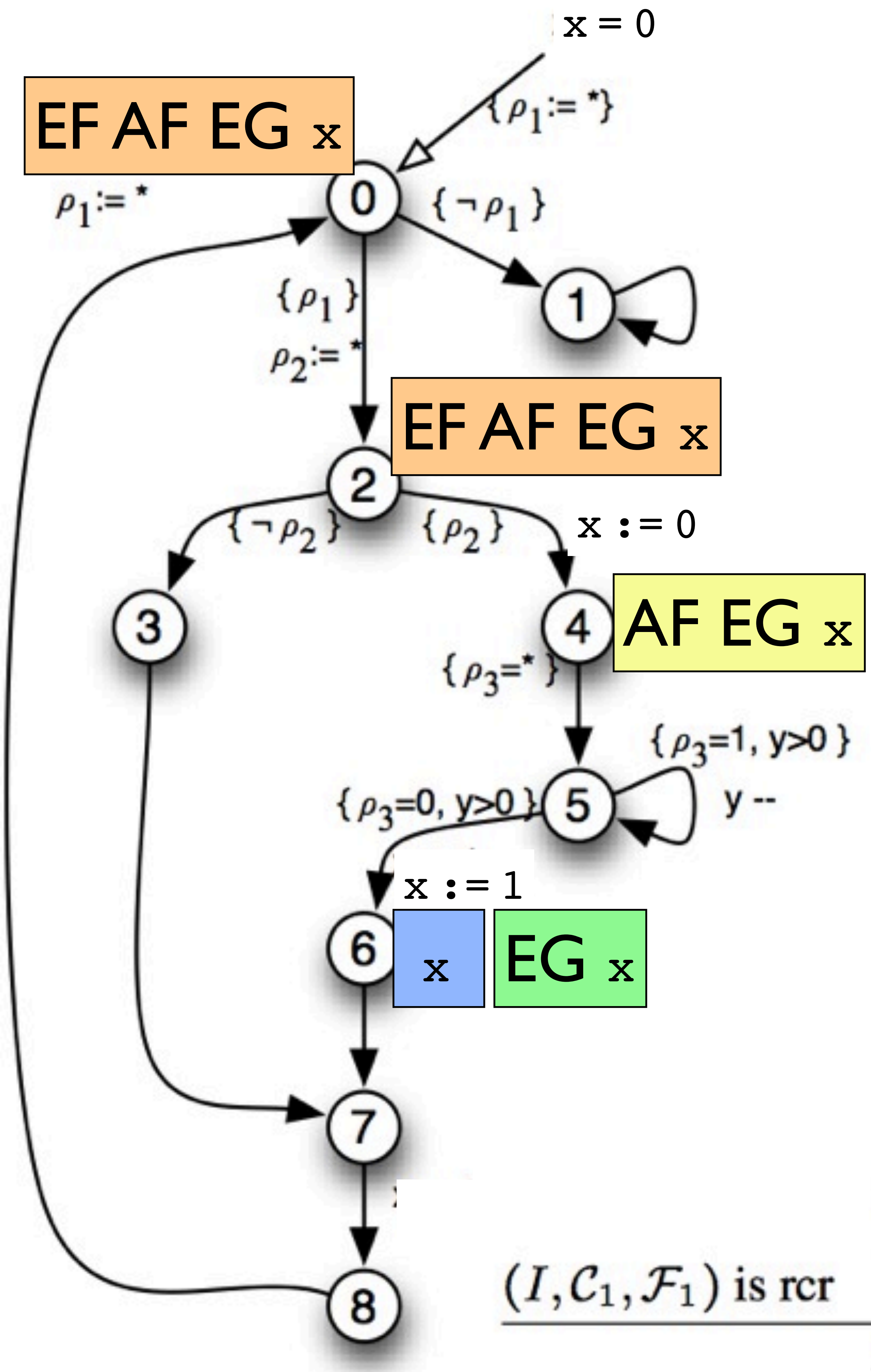
EF (AF (EG x))



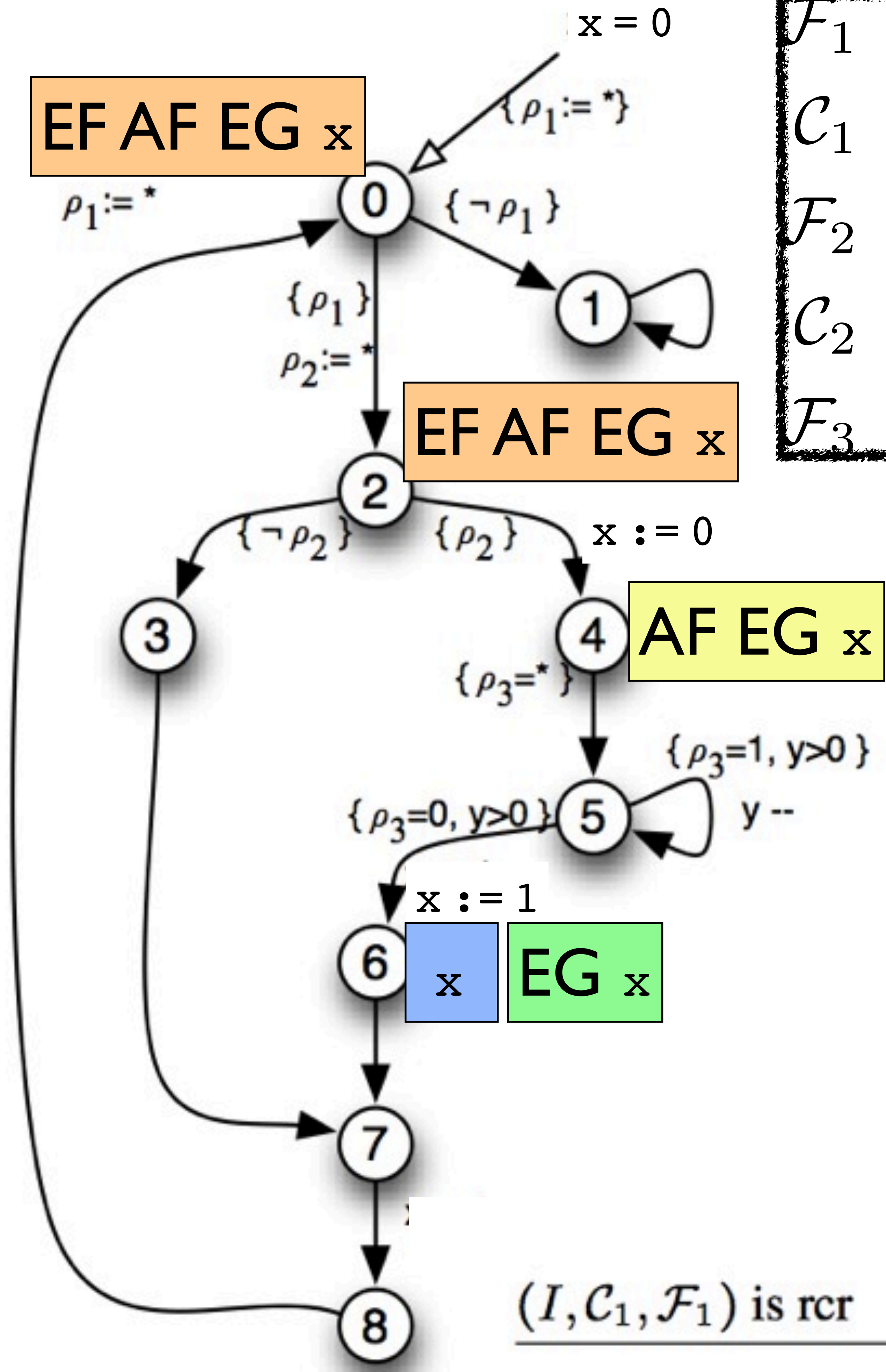
EF (AF (EG x))


x = 0
{ρ1:= *}
EF AF EG x
ρ1:= *
0
{¬ρ1}
1
{ρ1}
ρ2:= *
EF AF EG x
2
{¬ρ2}
{ρ2}
x := 0
3
4
AF EG x
{ρ3=* }
{ρ3=1, y>0 }
y --
{ρ3=0, y>0 }
5
x := 1
6
x
EG x
7
8

EF (AF (EG x))

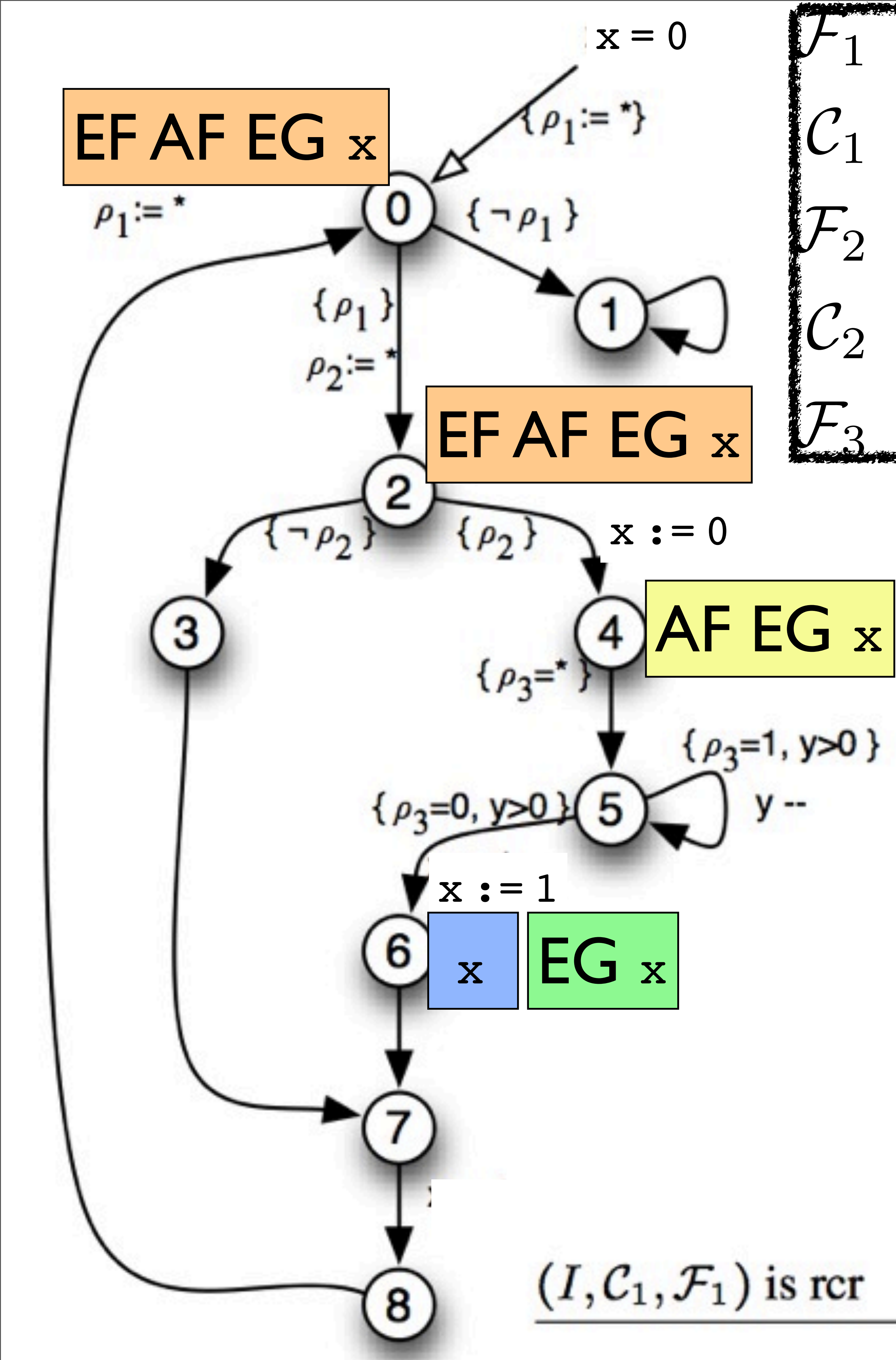


$$
\dfrac{(I,\mathcal{C}_1,\mathcal{F}_1)\ \text{is rcr} \qquad \dfrac{\mathbf{W}_{I}^{\mathcal{F}_1,\mathcal{C}_1}\ \text{is w.f.} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_1}^{\mathcal{F}_2,S}\ \text{is w.f.} \qquad \dfrac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3)\ \text{is rcr} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3,\mathcal{C}_2}|_1 \subseteq [\![p]\!]^{\mathsf{S}}}{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3,\mathcal{C}_2}|_1 \vdash p}}{\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}}{\mathcal{F}_1,S,\mathcal{F}_2 \Vdash \mathsf{FEG}p}}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}{I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{I \vdash \mathsf{EFAFEG}p}
$$



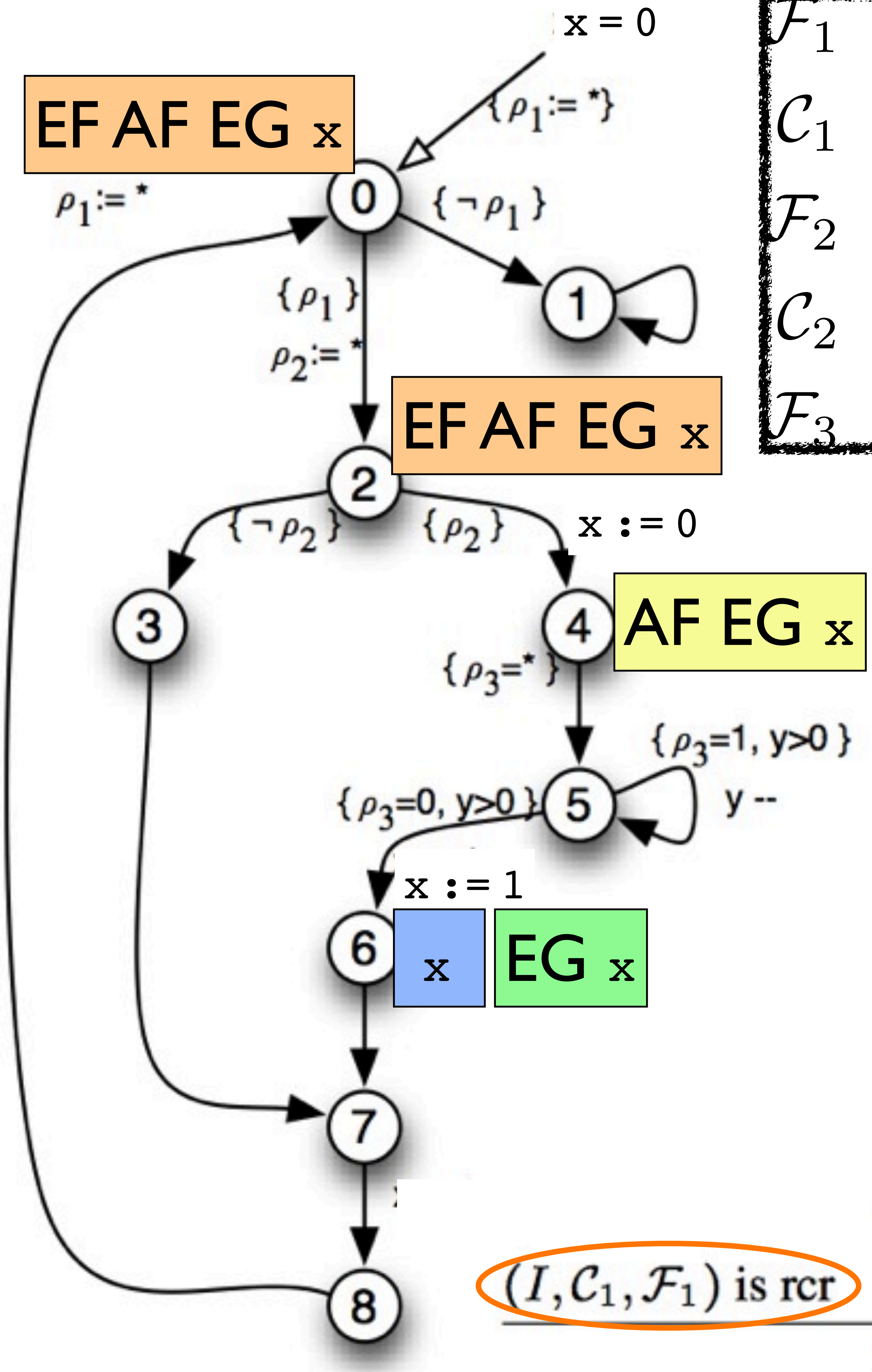
$$\mathcal{F}_1 \equiv \mathsf{pc} = 4$$
$$\mathcal{C}_1 \equiv \mathsf{pc} = 0 \Rightarrow \rho_1 \;\wedge\; \mathsf{pc} = 2 \Rightarrow \rho_2$$
$$\mathcal{F}_2 \equiv \mathsf{pc} = 6$$
$$\mathcal{C}_2 \equiv \mathsf{pc} = 2 \Rightarrow \neg\rho_2$$
$$\mathcal{F}_3 \equiv \mathsf{true}$$

$$\dfrac{\dfrac{\mathbf{W}_{I}^{\mathcal{F}_1,\mathcal{C}_1} \text{ is w.f.} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_1}^{\mathcal{F}_2,S} \text{ is w.f.} \qquad \dfrac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3) \text{ is rcr} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3,\mathcal{C}_2}|_1 \subseteq [\![p]\!]^{\mathsf{S}}}{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3,\mathcal{C}_2}|_1 \vdash p}}{\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}}{\mathcal{F}_1, S, \mathcal{F}_2 \Vdash \mathsf{FEG}p}}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}{(I,\mathcal{C}_1,\mathcal{F}_1) \text{ is rcr} \qquad I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{I \vdash \mathsf{EFAFEG}p}$$



$$\mathcal{F}_1 \equiv \mathsf{pc} = 4$$
$$\mathcal{C}_1 \equiv \mathsf{pc} = 0 \Rightarrow \rho_1 \;\wedge\; \mathsf{pc} = 2 \Rightarrow \rho_2$$
$$\mathcal{F}_2 \equiv \mathsf{pc} = 6$$
$$\mathcal{C}_2 \equiv \mathsf{pc} = 2 \Rightarrow \neg\rho_2$$
$$\mathcal{F}_3 \equiv \mathsf{true}$$

$$\dfrac{(\mathcal{I},\mathcal{C}_1,\mathcal{F}_1) \text{ is rcr} \quad \dfrac{\mathbf{W}^{\mathcal{F}_1,\mathcal{C}_1}_{\mathcal{I}} \text{ is w.f.} \quad \dfrac{\dfrac{\mathbf{W}^{\mathcal{F}_2,S}_{\mathcal{F}_1} \text{ is w.f.} \quad \dfrac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3) \text{ is rcr} \quad \dfrac{\dfrac{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \subseteq [\![p]\!]^S}{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \vdash p}}{\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}}{\mathcal{F}_1, S, \mathcal{F}_2 \Vdash \mathsf{FEG}p}}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}{\mathcal{I},\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{\mathcal{I} \vdash \mathsf{EFAFEG}p}$$



$$\mathcal{F}_1 \equiv \mathsf{pc} = 4$$
$$\mathcal{C}_1 \equiv \mathsf{pc} = 0 \Rightarrow \rho_1 \ \wedge\ \mathsf{pc} = 2 \Rightarrow \rho_2$$
$$\mathcal{F}_2 \equiv \mathsf{pc} = 6$$
$$\mathcal{C}_2 \equiv \mathsf{pc} = 2 \Rightarrow \neg\rho_2$$
$$\mathcal{F}_3 \equiv \mathsf{true}$$

$$\frac{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \subseteq [\![p]\!]^S}{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \vdash p}$$

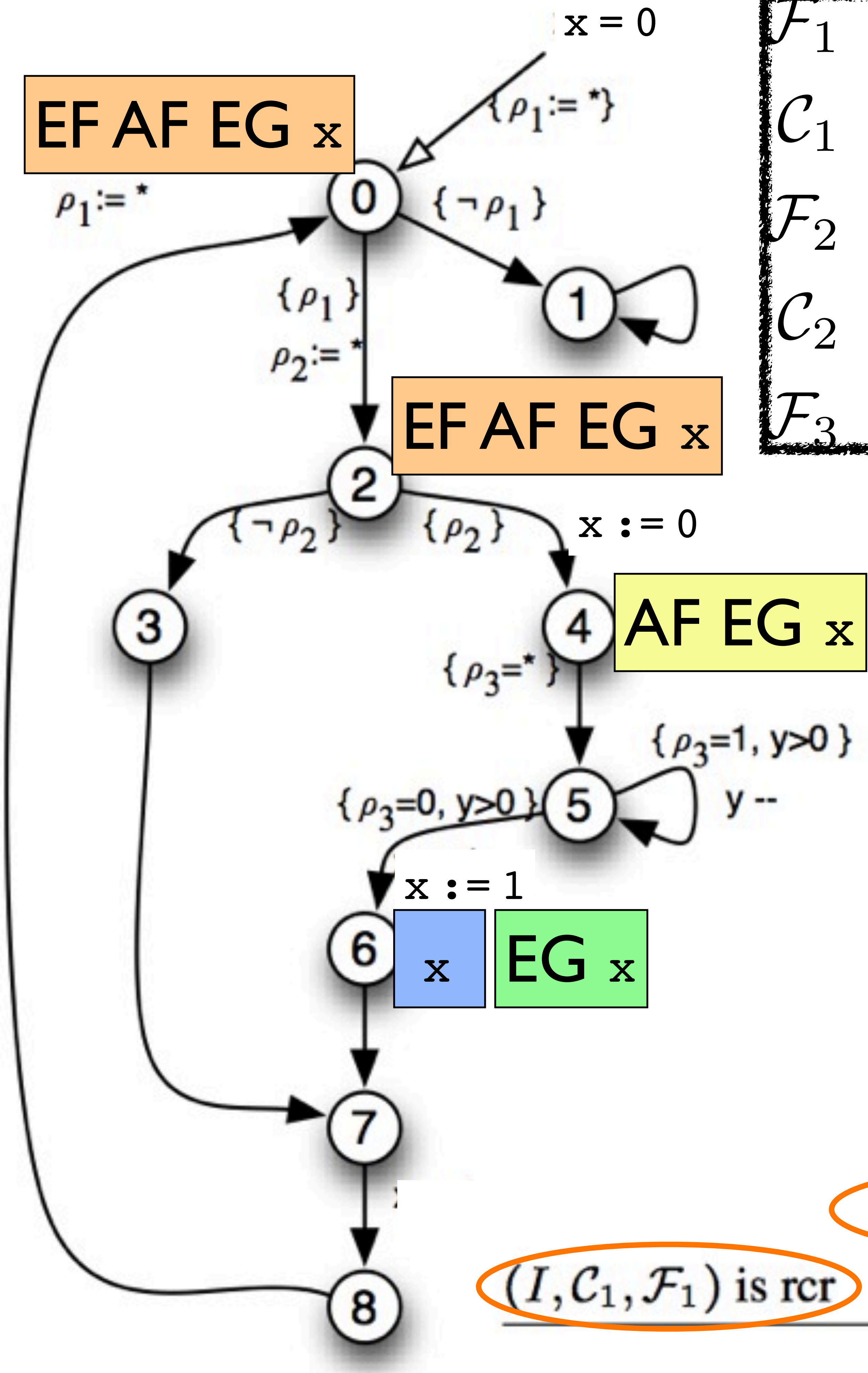
$$\frac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3) \text{ is rcr} \qquad \mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}{\mathcal{F}_2 \vdash \mathsf{EG}p}$$

$$\frac{\mathbf{W}^{\mathcal{F}_2,S}_{\mathcal{F}_1} \text{ is w.f.} \qquad \mathcal{F}_2 \vdash \mathsf{EG}p}{\mathcal{F}_1, S, \mathcal{F}_2 \Vdash \mathsf{FEG}p}$$

$$\frac{\mathcal{F}_1, S, \mathcal{F}_2 \Vdash \mathsf{FEG}p}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}$$

$$\frac{\mathbf{W}^{\mathcal{F}_1,\mathcal{C}_1}_{I} \text{ is w.f.} \qquad \mathcal{F}_1 \vdash \mathsf{AFEG}p}{I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}$$

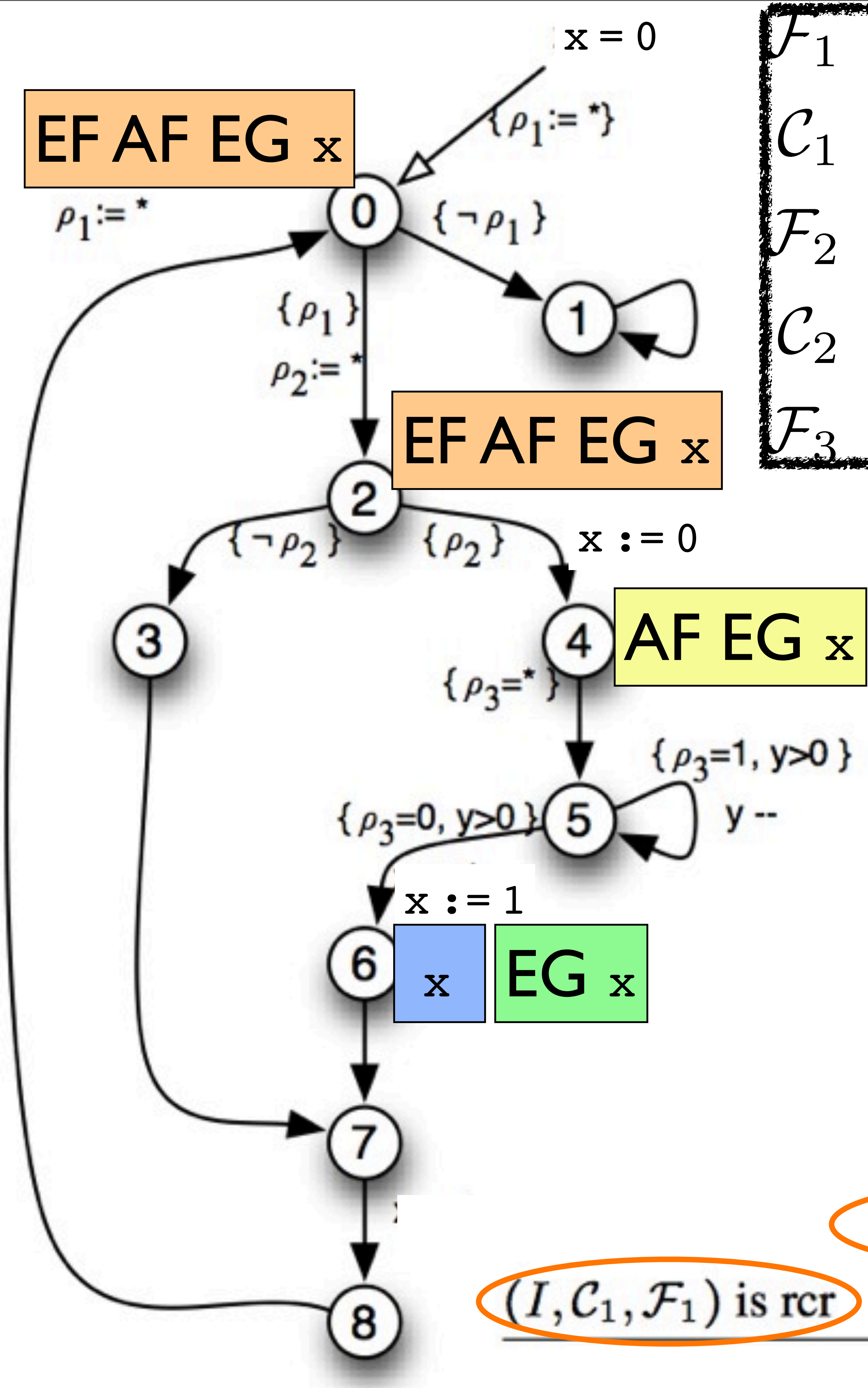
$$\frac{(I,\mathcal{C}_1,\mathcal{F}_1) \text{ is rcr} \qquad I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}{I \vdash \mathsf{EFAFEG}p}$$



$$
\begin{array}{lcl}
\mathcal{F}_1 & \equiv & \mathsf{pc} = 4 \\
\mathcal{C}_1 & \equiv & \mathsf{pc} = 0 \Rightarrow \rho_1 \ \wedge \ \mathsf{pc} = 2 \Rightarrow \rho_2 \\
\mathcal{F}_2 & \equiv & \mathsf{pc} = 6 \\
\mathcal{C}_2 & \equiv & \mathsf{pc} = 2 \Rightarrow \neg\rho_2 \\
\mathcal{F}_3 & \equiv & \mathsf{true}
\end{array}
$$

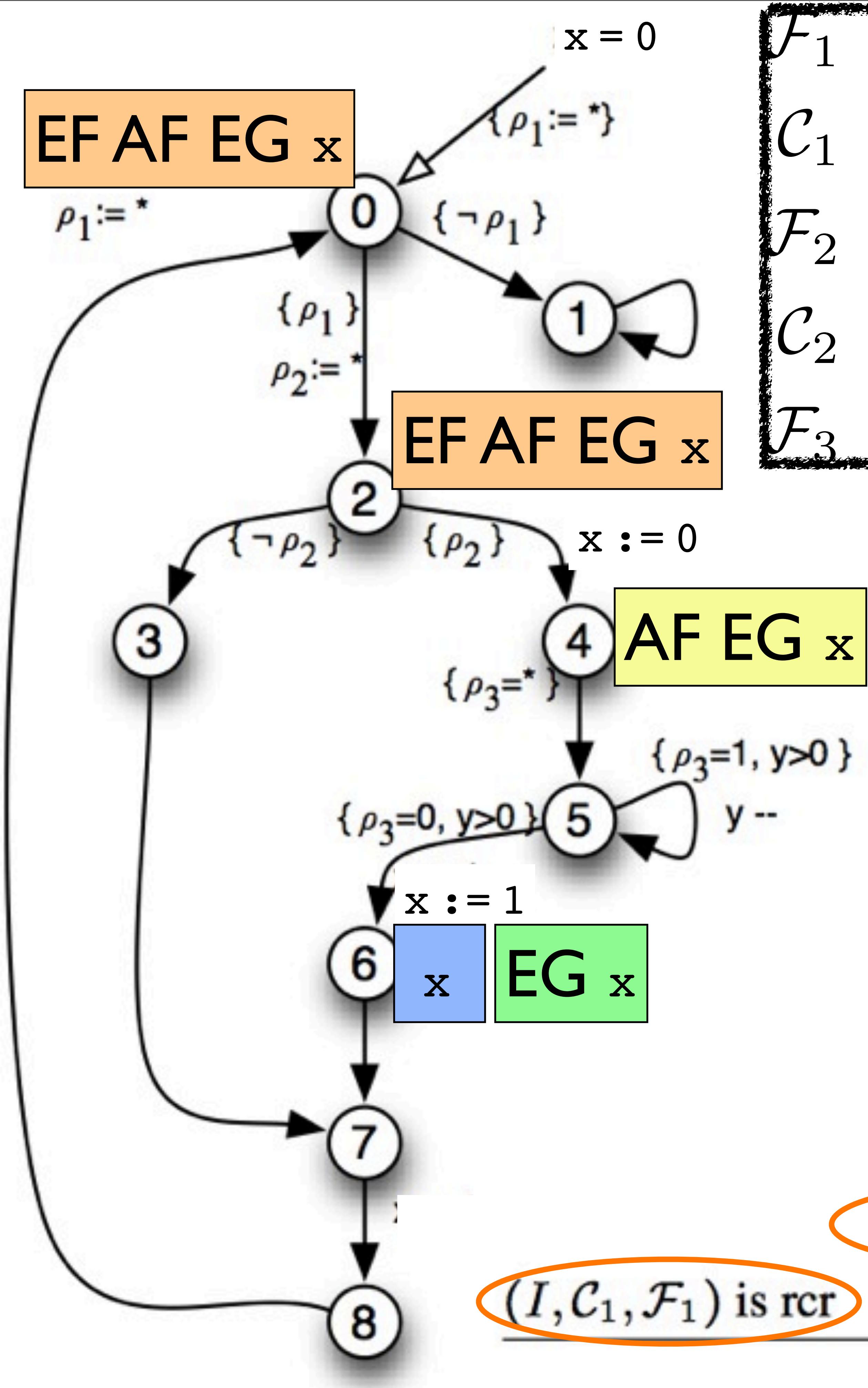
$$
\dfrac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3)\text{ is rcr} \qquad \dfrac{\dfrac{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \subseteq [\![p]\!]^{\mathsf{S}}}{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \vdash p}}{\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}
$$

$$
\dfrac{(I,\mathcal{C}_1,\mathcal{F}_1)\text{ is rcr} \qquad \dfrac{\mathbf{W}^{\mathcal{F}_1,\mathcal{C}_1}_{I}\text{ is w.f.} \qquad \dfrac{\dfrac{\mathbf{W}^{\mathcal{F}_2,S}_{\mathcal{F}_1}\text{ is w.f.} \qquad \mathcal{F}_2 \vdash \mathsf{EG}p}{\mathcal{F}_1,S,\mathcal{F}_2 \Vdash \mathsf{FEG}p}}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}{I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{I \vdash \mathsf{EFAFEG}p}
$$



$$\mathcal{F}_1 \equiv \mathsf{pc} = 4$$
$$\mathcal{C}_1 \equiv \mathsf{pc} = 0 \Rightarrow \rho_1 \ \wedge \ \mathsf{pc} = 2 \Rightarrow \rho_2$$
$$\mathcal{F}_2 \equiv \mathsf{pc} = 6$$
$$\mathcal{C}_2 \equiv \mathsf{pc} = 2 \Rightarrow \neg\rho_2$$
$$\mathcal{F}_3 \equiv \mathsf{true}$$

$$\dfrac{\dfrac{(I, \mathcal{C}_1, \mathcal{F}_1) \text{ is rcr} \qquad \dfrac{\mathbf{W}_{I}^{\mathcal{F}_1, \mathcal{C}_1} \text{ is w.f.} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_1}^{\mathcal{F}_2, S} \text{ is w.f.} \qquad \dfrac{(\mathcal{F}_2, \mathcal{C}_2, \mathcal{F}_3) \text{ is rcr} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3, \mathcal{C}_2}|_1 \subseteq [\![p]\!]^{S}}{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3, \mathcal{C}_2}|_1 \vdash p}}{\mathcal{F}_2, \mathcal{C}_2, \mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}}{\mathcal{F}_1, S, \mathcal{F}_2 \Vdash \mathsf{FEG}p}}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}{I, \mathcal{C}_1, \mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{I \vdash \mathsf{EFAFEG}p}$$



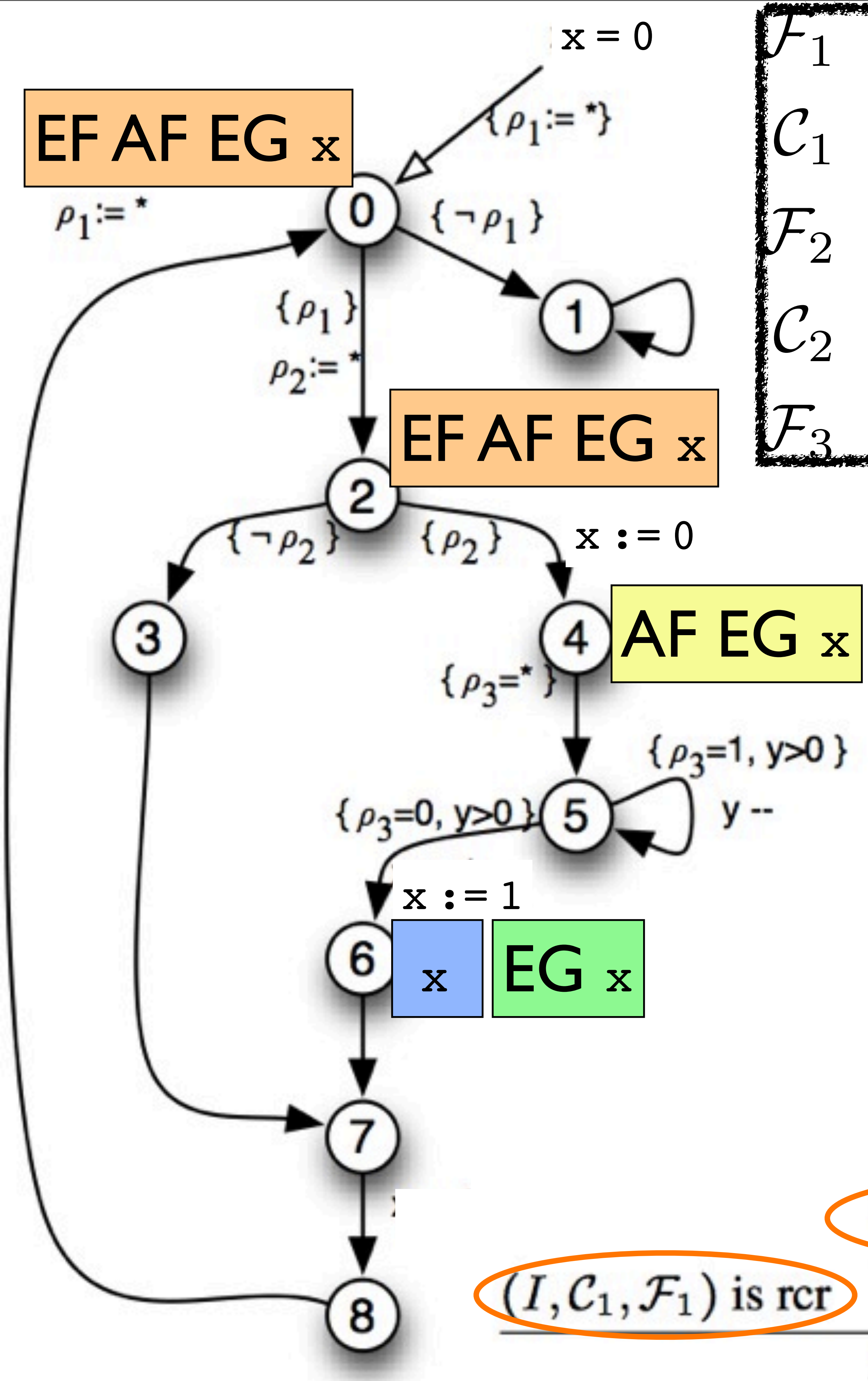
$$\mathcal{F}_1 \equiv \mathsf{pc} = 4$$
$$\mathcal{C}_1 \equiv \mathsf{pc} = 0 \Rightarrow \rho_1 \ \wedge \ \mathsf{pc} = 2 \Rightarrow \rho_2$$
$$\mathcal{F}_2 \equiv \mathsf{pc} = 6$$
$$\mathcal{C}_2 \equiv \mathsf{pc} = 2 \Rightarrow \neg\rho_2$$
$$\mathcal{F}_3 \equiv \mathsf{true}$$

$$\frac{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \subseteq [\![p]\!]^S}{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \vdash p}$$

$$\frac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3) \text{ is rcr} \qquad \dfrac{\mathbf{W}^{\mathcal{F}_3,\mathcal{C}_2}_{\mathcal{F}_2}|_1 \vdash p}{\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}$$

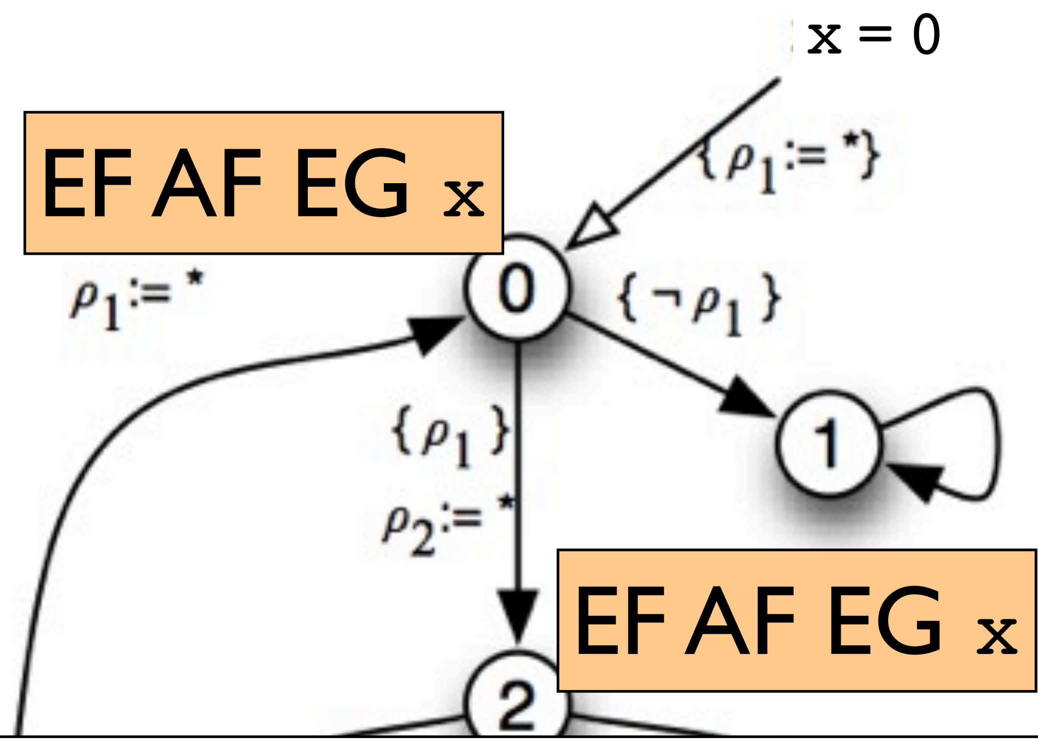
$$\frac{\mathbf{W}^{\mathcal{F}_2,S}_{\mathcal{F}_1} \text{ is w.f.} \qquad \mathcal{F}_2 \vdash \mathsf{EG}p}{\dfrac{\mathcal{F}_1,S,\mathcal{F}_2 \Vdash \mathsf{FEG}p}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}$$

$$\frac{(I,\mathcal{C}_1,\mathcal{F}_1) \text{ is rcr} \qquad \dfrac{\mathbf{W}^{\mathcal{F}_1,\mathcal{C}_1}_{I} \text{ is w.f.} \qquad \mathcal{F}_1 \vdash \mathsf{AFEG}p}{I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{I \vdash \mathsf{EFAFEG}p}$$



$$
\begin{aligned}
\mathcal{F}_1 &\equiv \text{pc} = 4\\
\mathcal{C}_1 &\equiv \text{pc} = 0 \Rightarrow \rho_1 \ \wedge\ \text{pc} = 2 \Rightarrow \rho_2\\
\mathcal{F}_2 &\equiv \text{pc} = 6\\
\mathcal{C}_2 &\equiv \text{pc} = 2 \Rightarrow \neg\rho_2\\
\mathcal{F}_3 &\equiv \text{true}
\end{aligned}
$$

$$
\dfrac{(I,\mathcal{C}_1,\mathcal{F}_1)\text{ is rcr} \qquad \dfrac{\mathbf{W}_{I}^{\mathcal{F}_1,\mathcal{C}_1}\text{ is w.f.} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_1}^{\mathcal{F}_2,S}\text{ is w.f.} \qquad \dfrac{(\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3)\text{ is rcr} \qquad \dfrac{\dfrac{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3,\mathcal{C}_2}|_1 \subseteq [\![p]\!]^S}{\mathbf{W}_{\mathcal{F}_2}^{\mathcal{F}_3,\mathcal{C}_2}|_1 \vdash p}}{\mathcal{F}_2,\mathcal{C}_2,\mathcal{F}_3 \Vdash \mathsf{G}p}}{\mathcal{F}_2 \vdash \mathsf{EG}p}}{\mathcal{F}_1,S,\mathcal{F}_2 \Vdash \mathsf{FEG}p}}{\mathcal{F}_1 \vdash \mathsf{AFEG}p}}{I,\mathcal{C}_1,\mathcal{F}_1 \Vdash \mathsf{FAFEG}p}}{I \vdash \mathsf{EFAFEG}p}
$$

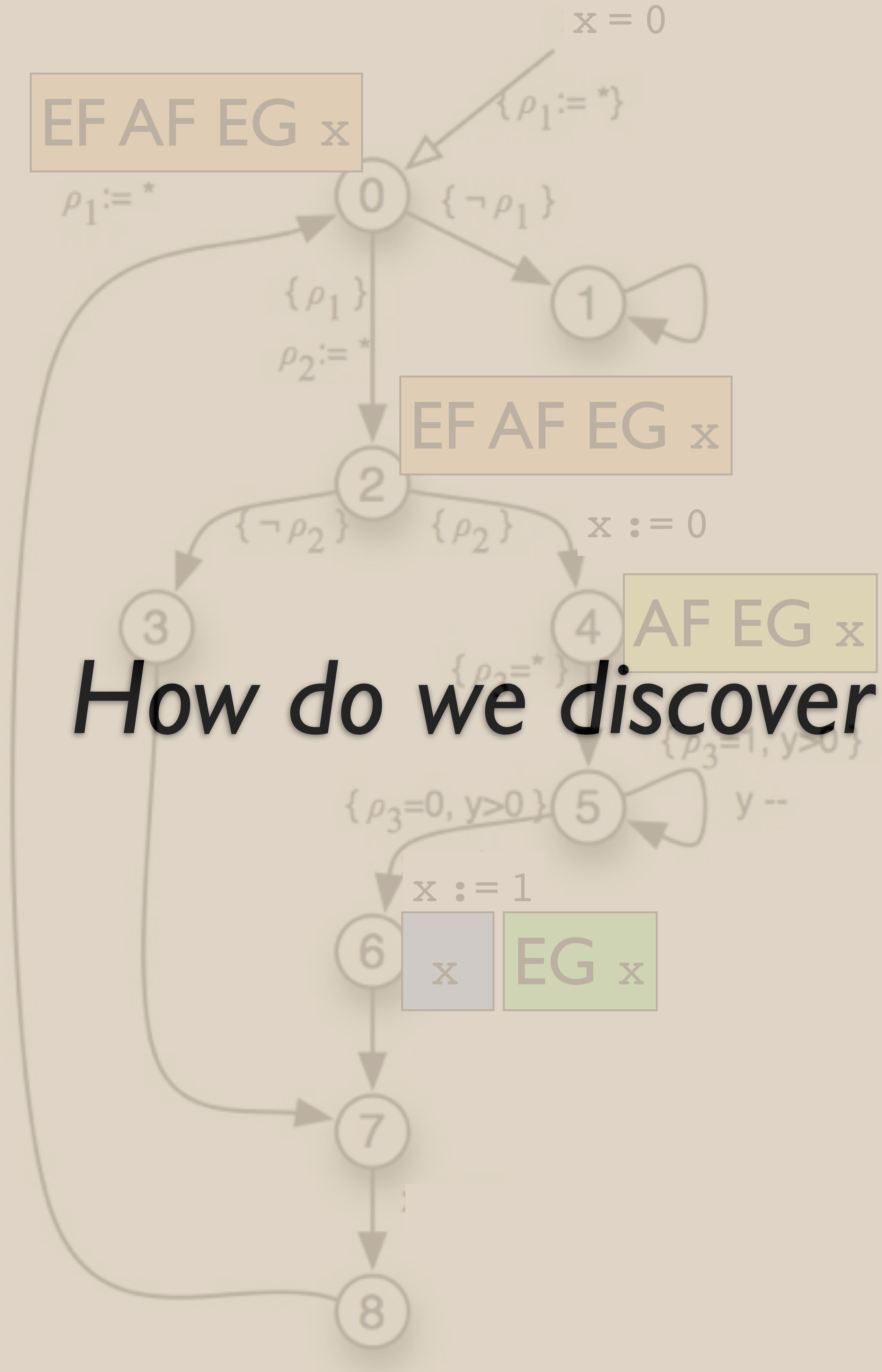


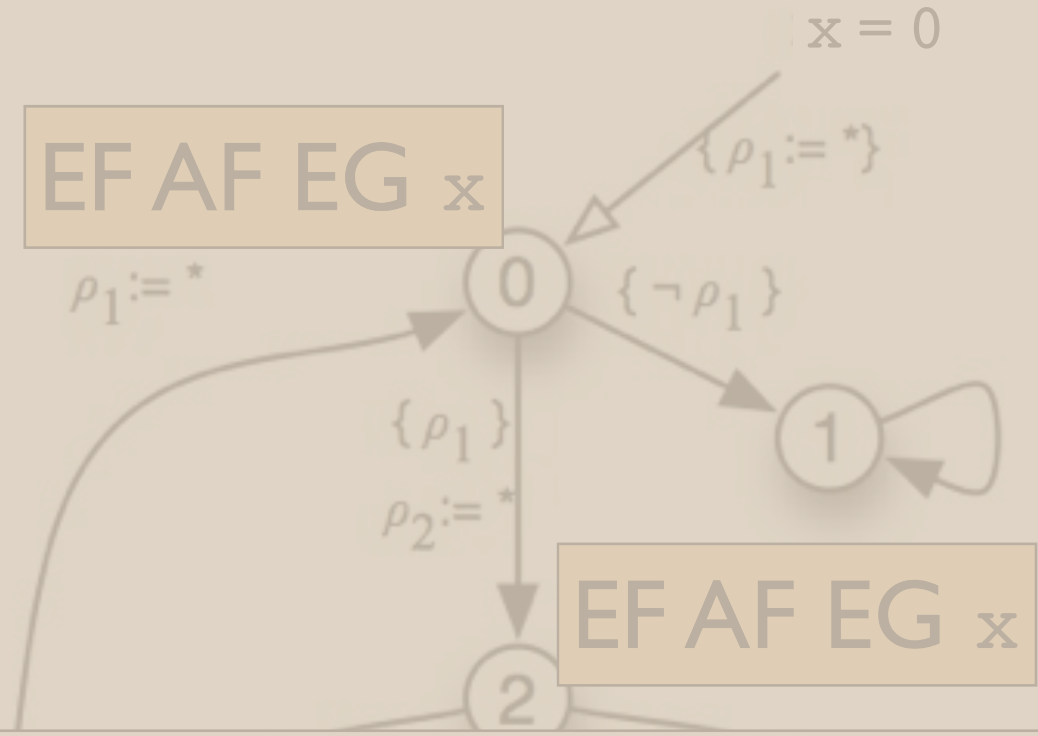
$$\mathcal{F}_1 \equiv \text{pc} = 4$$
$$\mathcal{C}_1 \equiv \text{pc} = 0 \Rightarrow \rho_1 \wedge \text{pc} = 2 \Rightarrow \rho_2$$
$$\mathcal{F}_2 \equiv \text{pc} = 6$$
$$\mathcal{C}_2 \equiv \text{pc} = 2 \Rightarrow \neg\rho_2$$
$$\mathcal{F}_3 \equiv \text{true}$$

- (Finite) derivation despite infinite state spaces
- *Partition* rather than *enumerate* states
- Symbolic representations/overapproximations
- *We believe it will work well in practice...*

$$\frac{(I, \mathcal{C}_1, \mathcal{F}_1) \text{ is rcr} \qquad I, \mathcal{C}_1, \mathcal{F}_1 \Vdash \text{FAFEG}p}{I \vdash \text{EFAFEG}p}$$

How do we discover Frontiers and Chutes?





$\equiv \quad pc = 4$

$\equiv \quad pc = 0 \Rightarrow \rho_1 \;\wedge\; pc = 2 \Rightarrow \rho_2$

$\equiv \quad pc = 6$

$\equiv \quad pc = 2 \Rightarrow \neg\rho_2$

$\equiv \quad$ true

How do we discover Frontiers and Chutes?

- *Partition* rather than *enumerate* states
- Symbolic representations/overapproximations
- *We believe it will work well in practice...*

Automation

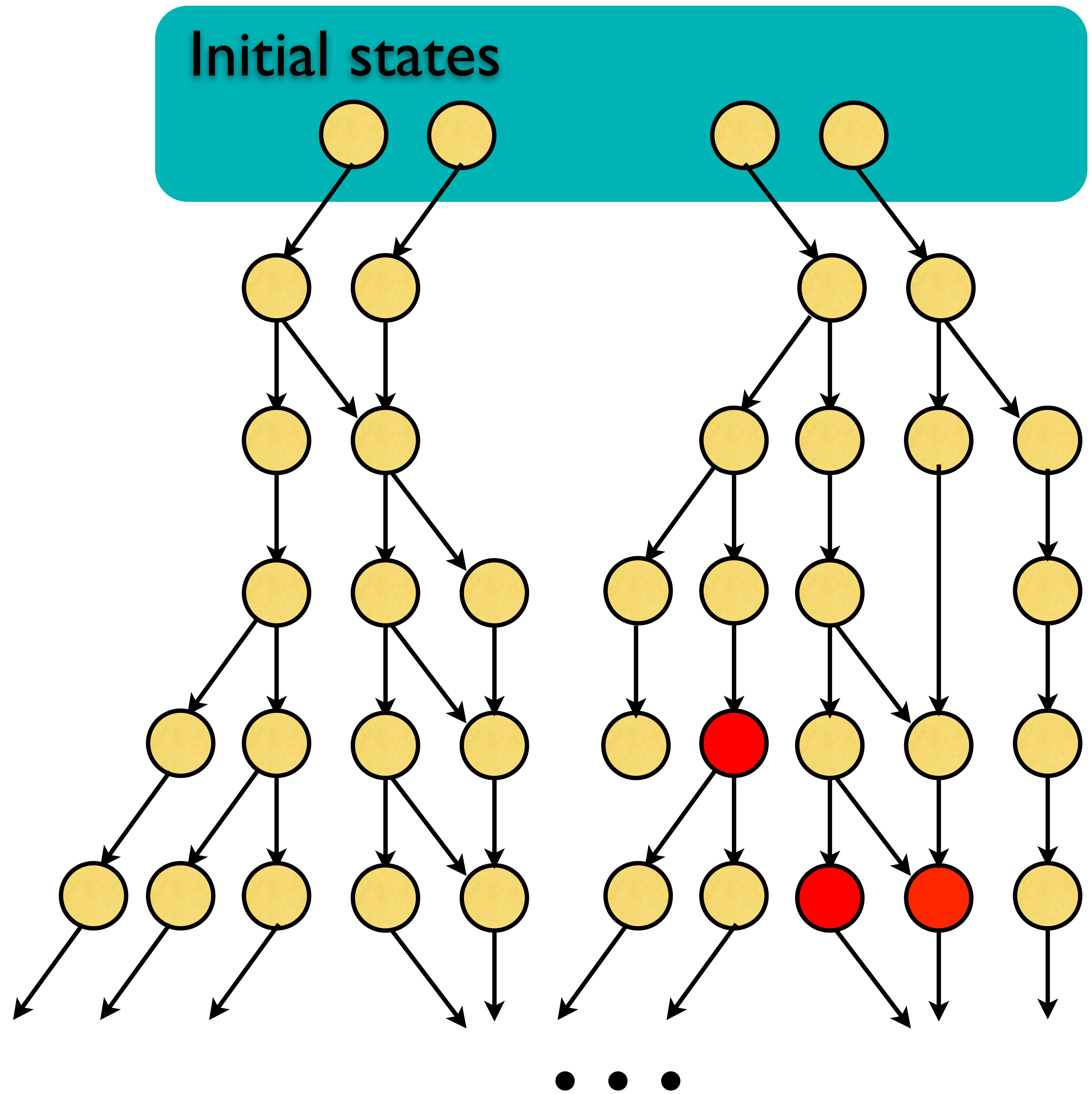
How do we discover ***frontiers***?

(see our work in CAV 2011)

Automation

How do we discover ***chutes***?

EF `red`

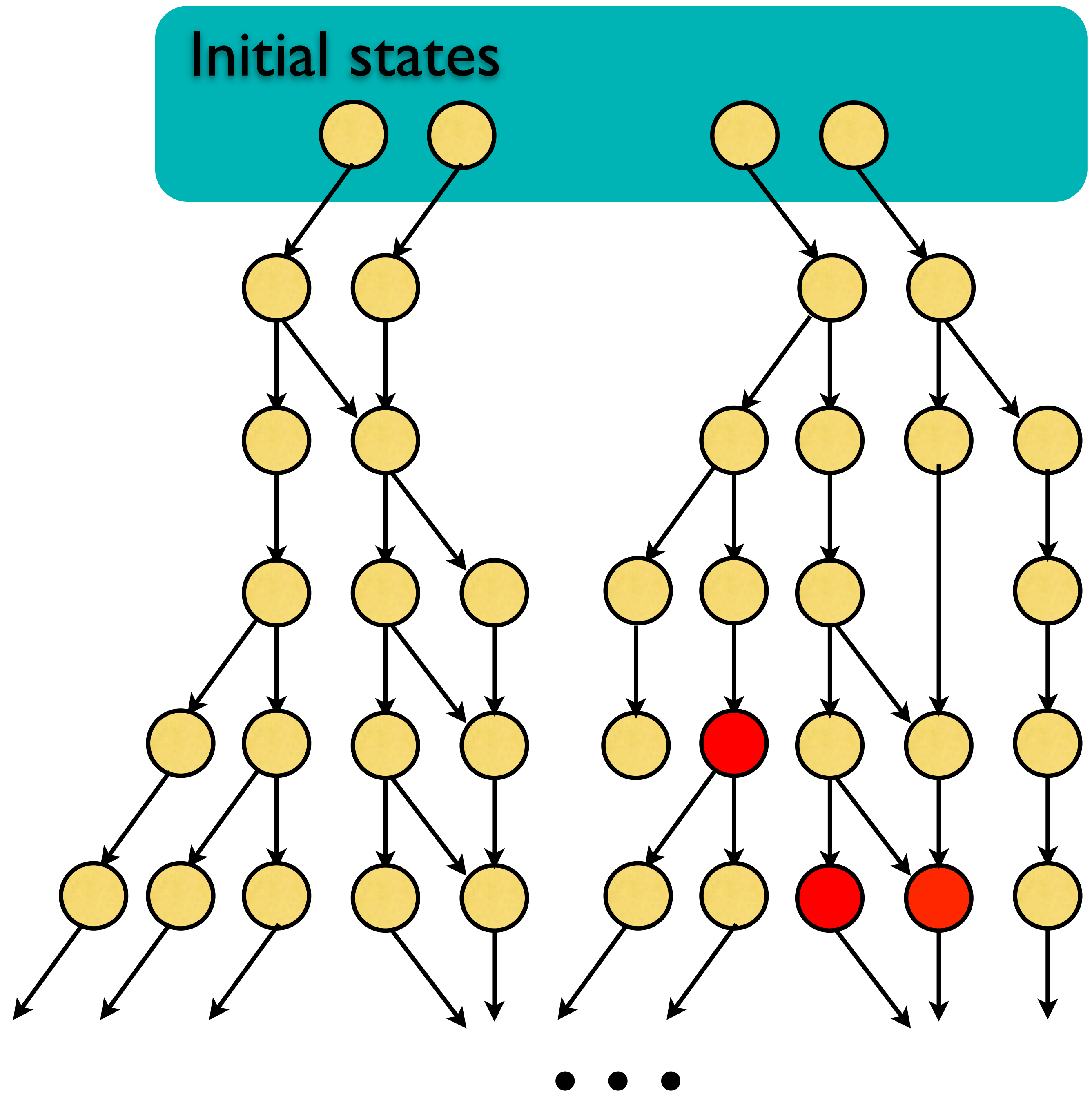


Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`

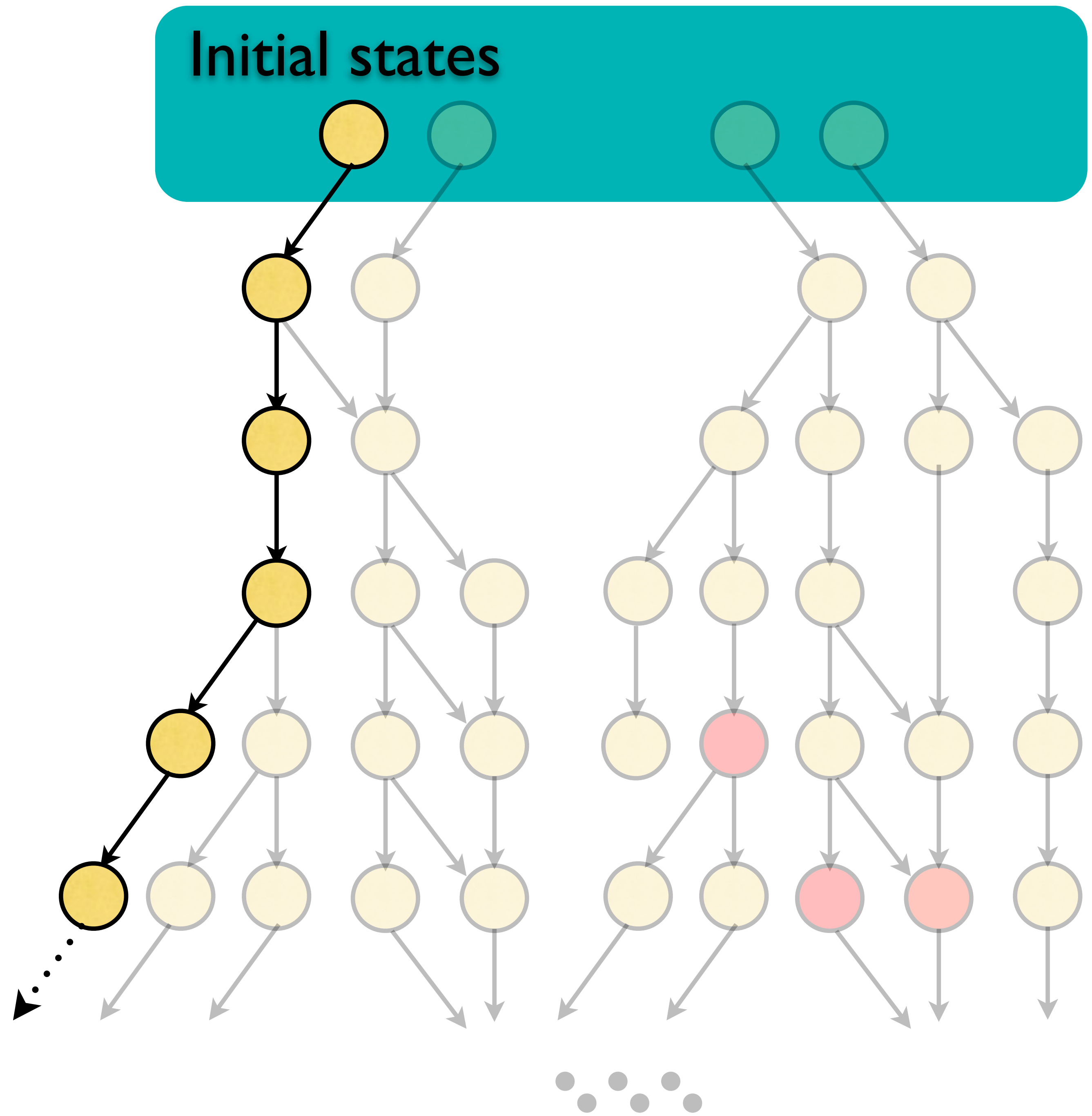


Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`

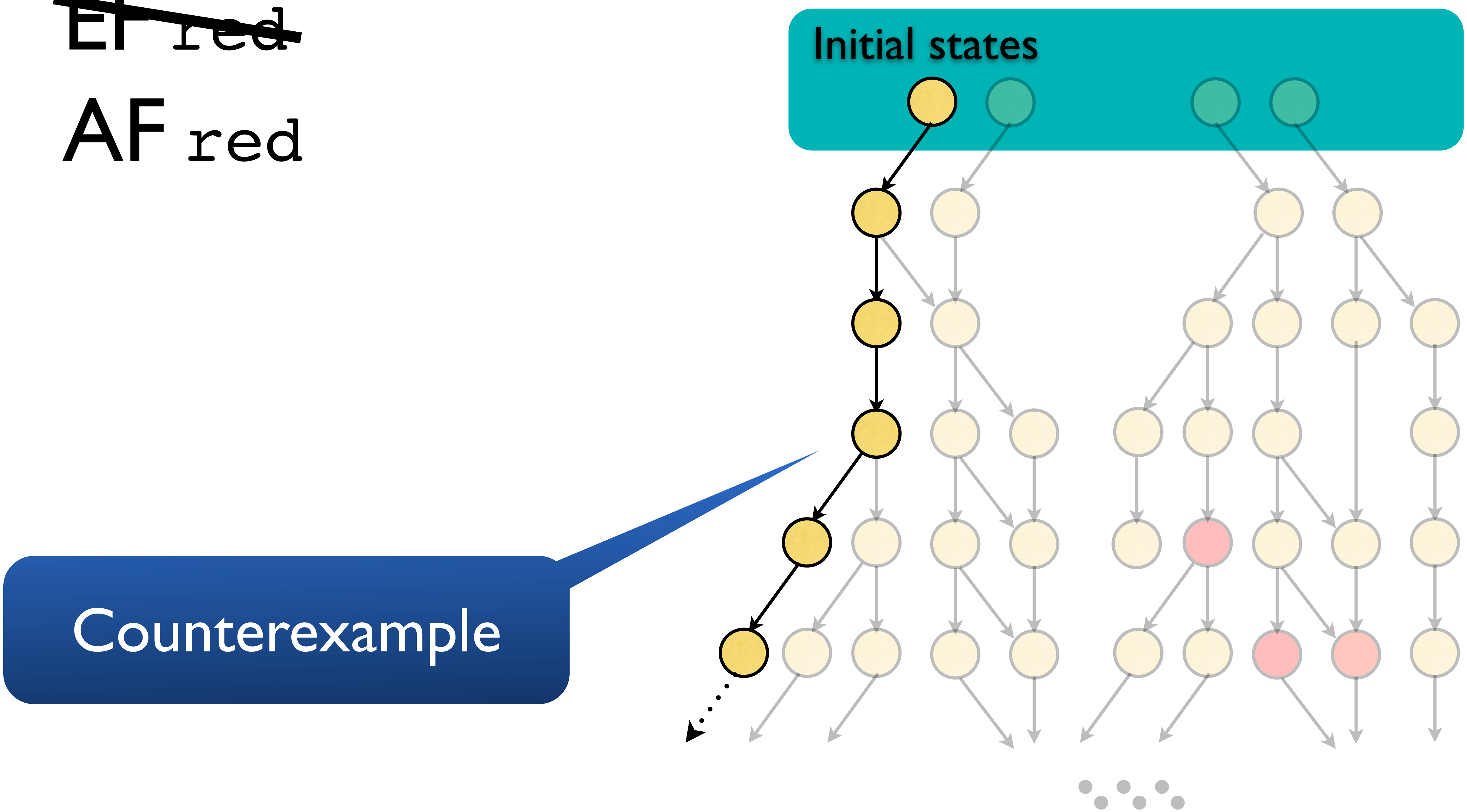


Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`

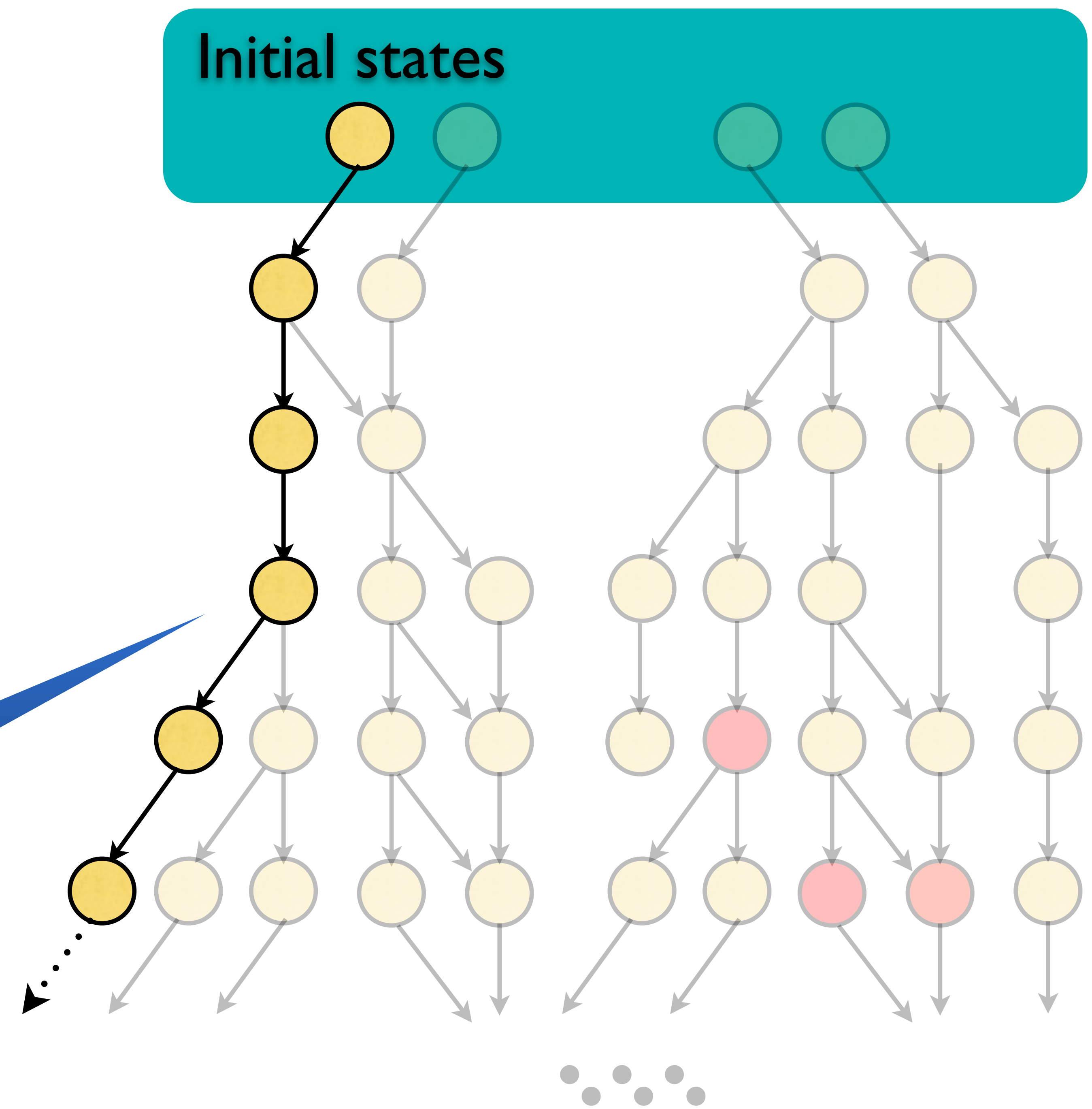


Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`



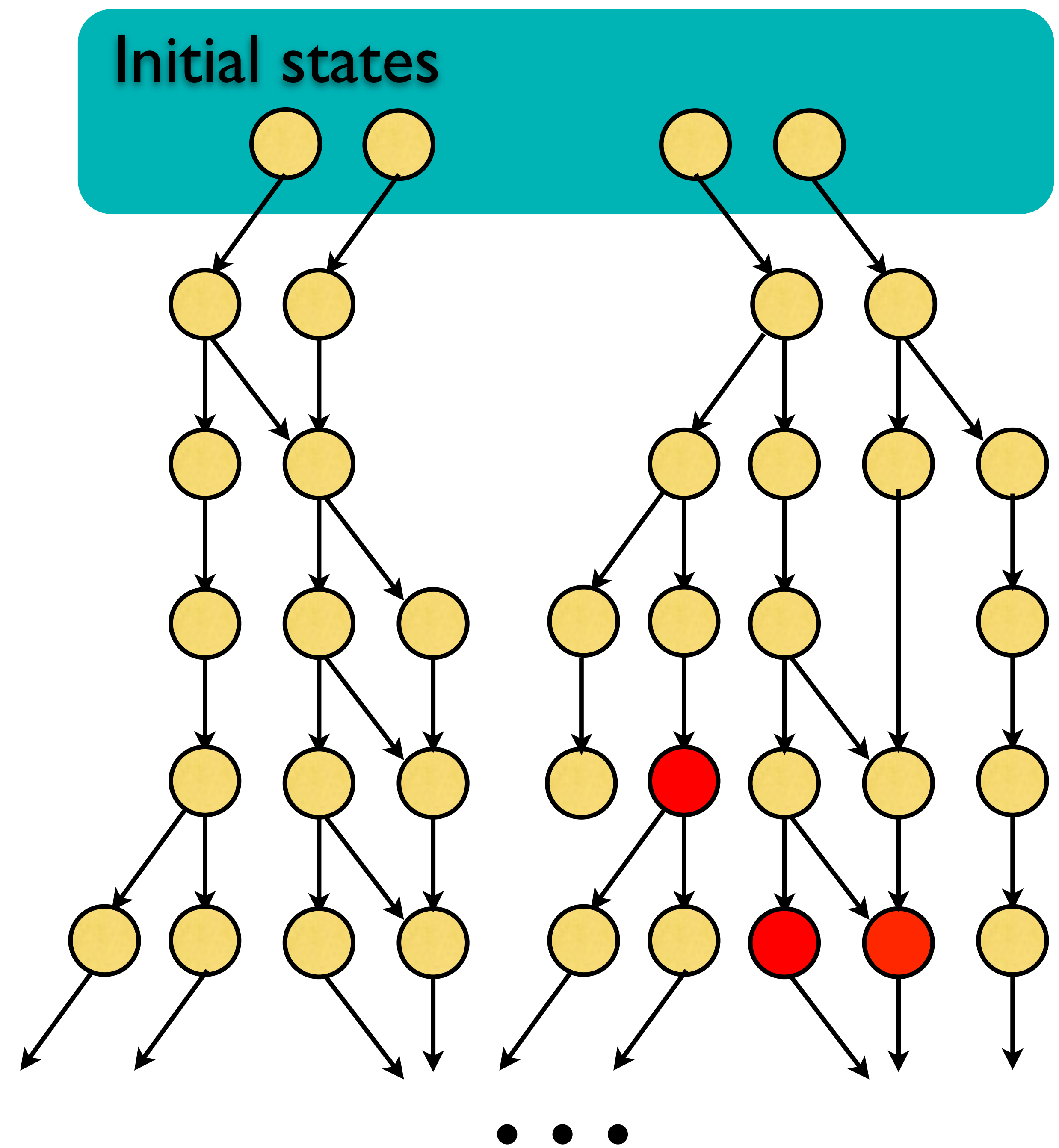
Counterexample

Remove this behavior!

Automation

How do we discover ***chutes***?

EF `red`

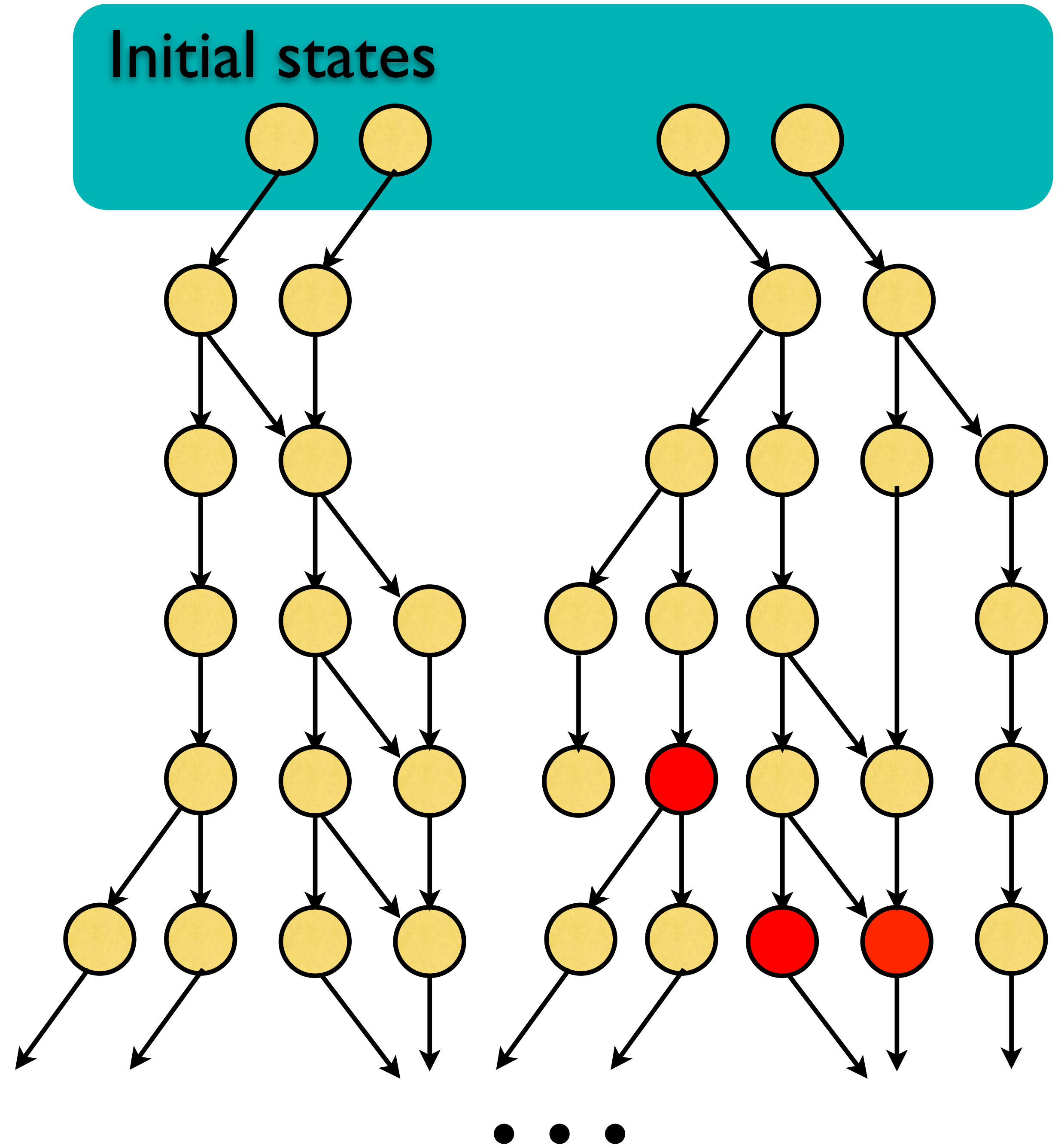


Automation

How do we discover ***chutes***?

~~EF `red`~~

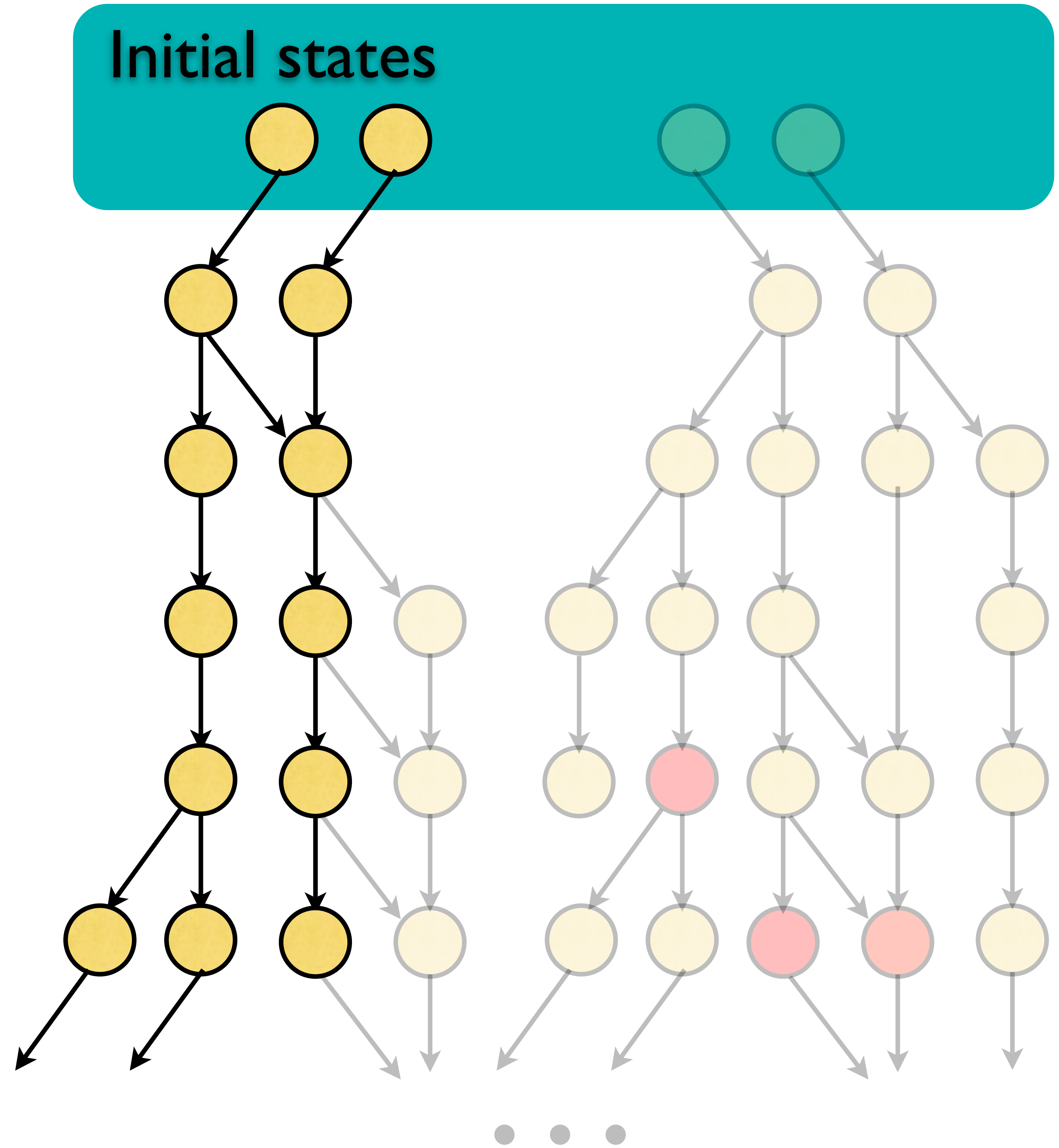
AF `red`



Automation

How do we discover ***chutes***?

EF `red`

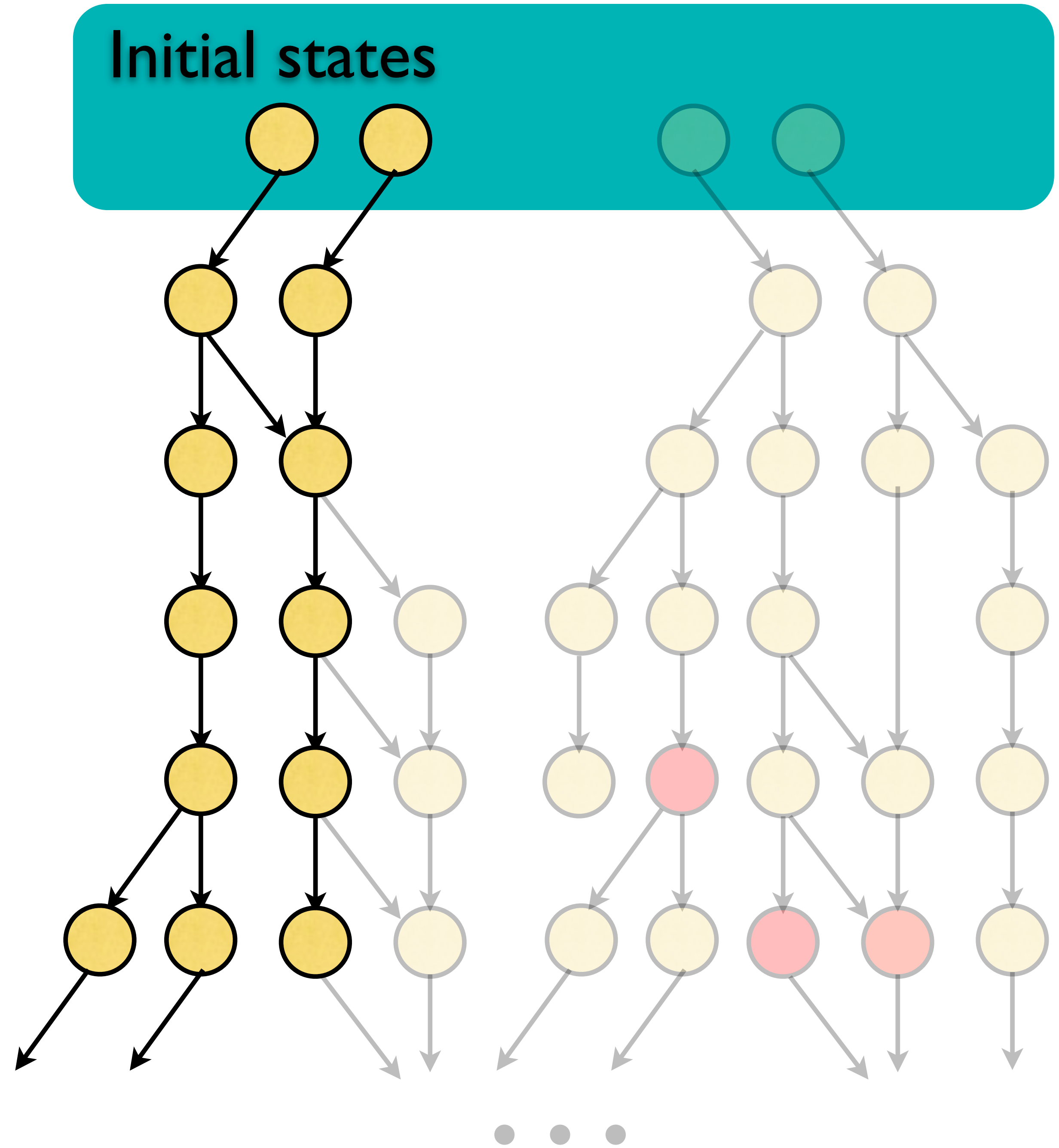


Automation

How do we discover ***chutes***?

~~EF `red`~~

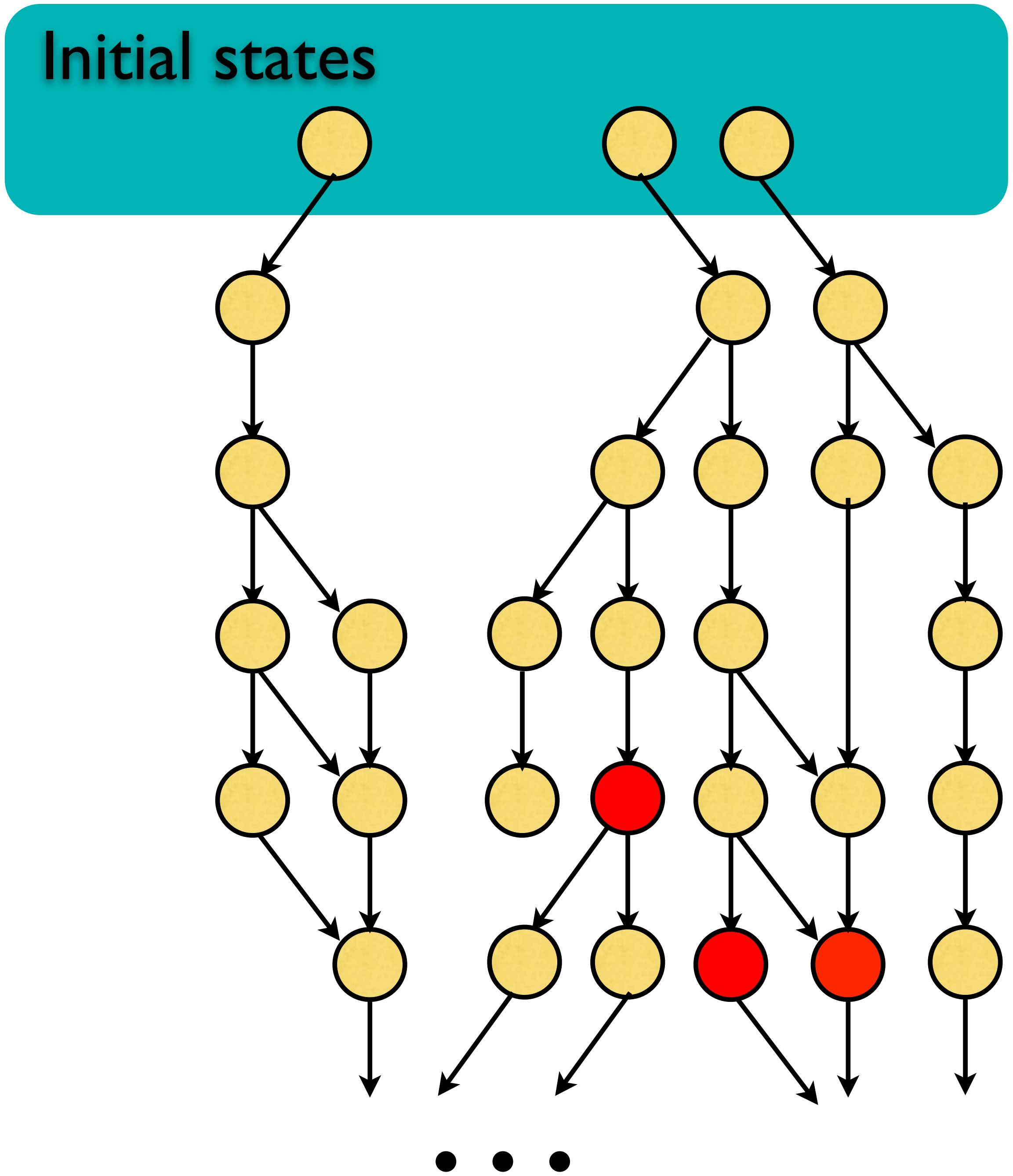
AF `red`



Automation

How do we discover ***chutes***?

EF `red`

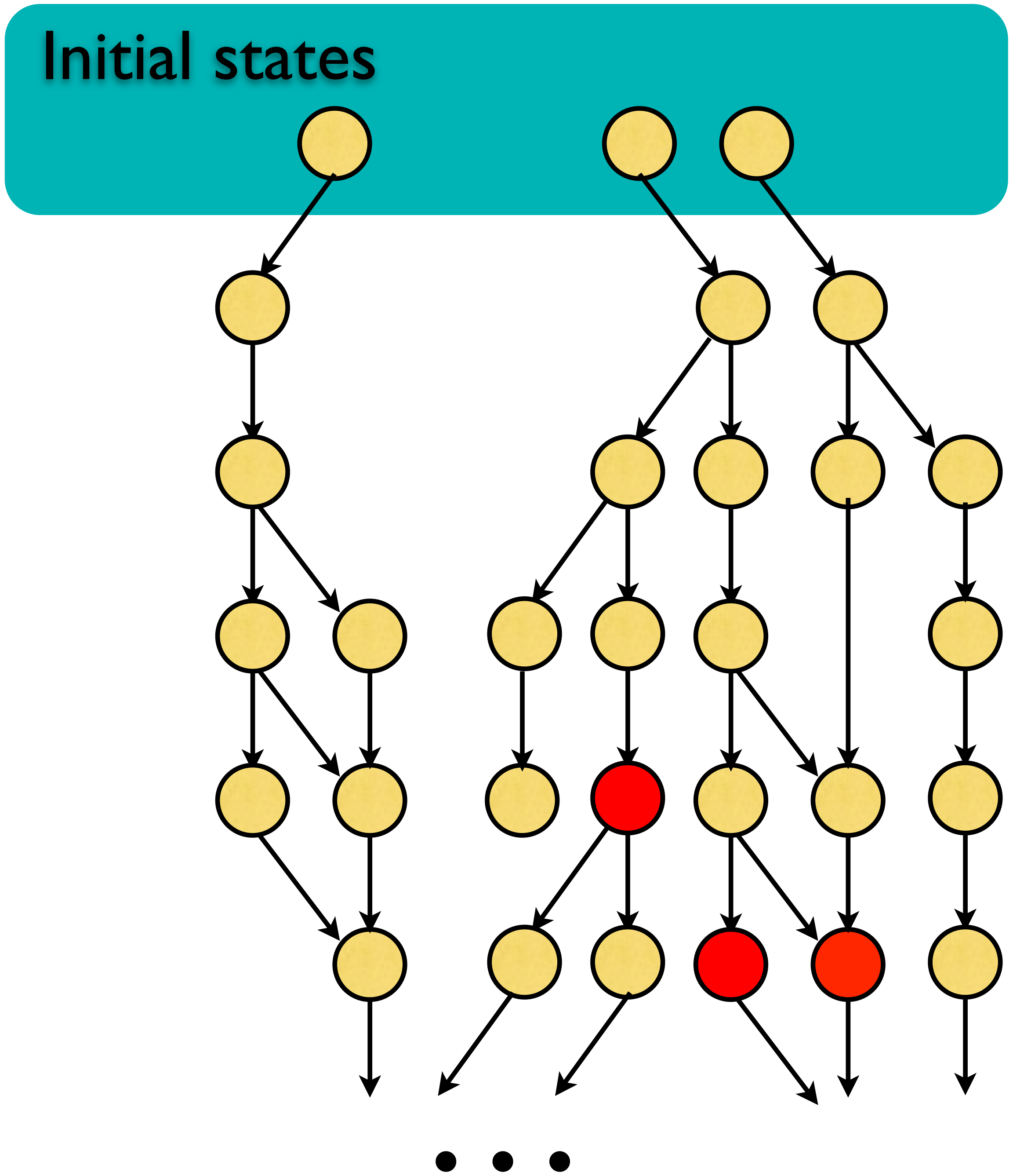


Automation

How do we discover ***chutes***?

~~EF `red`~~

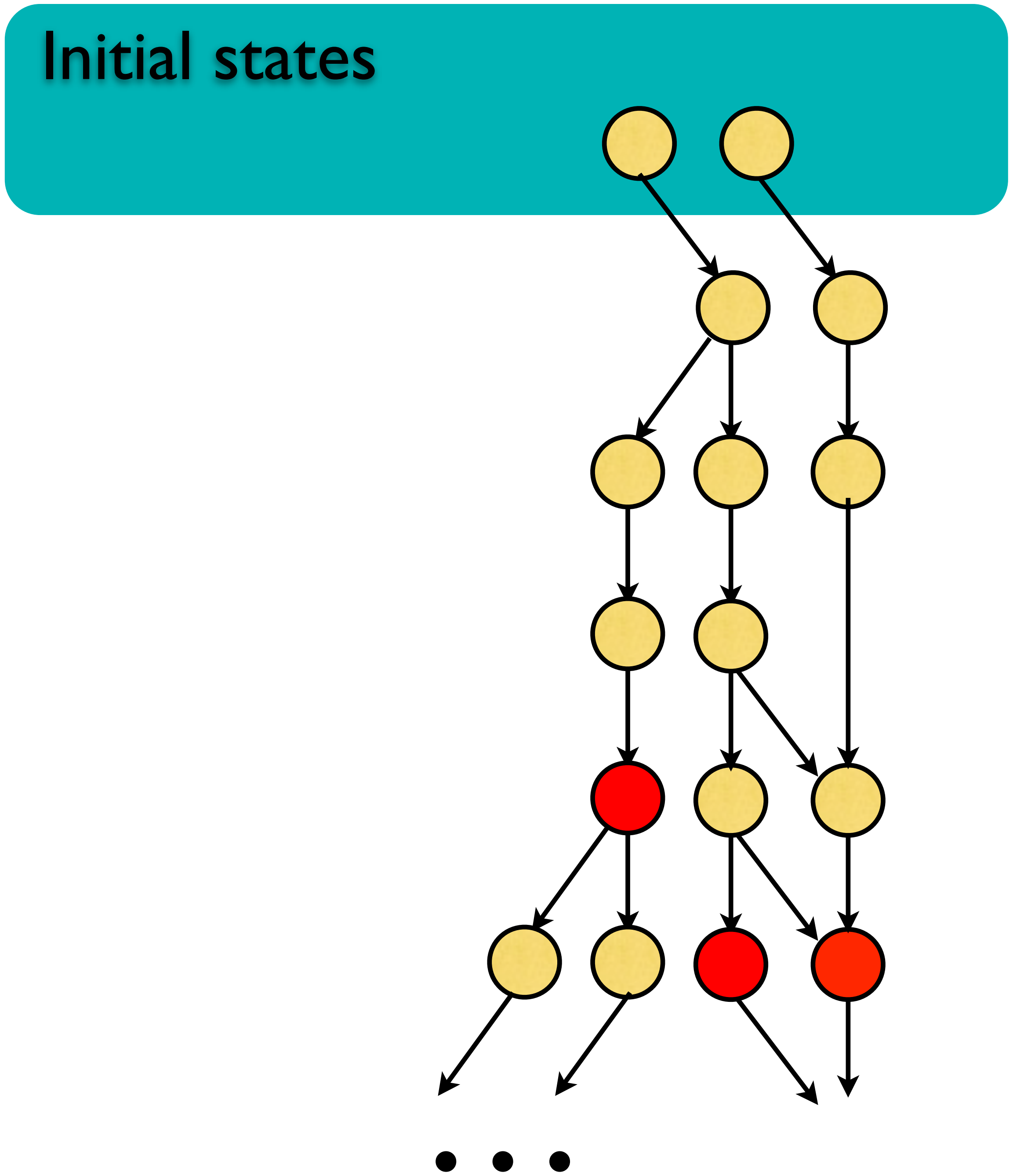
AF `red`



Automation

How do we discover ***chutes***?

EF `red`

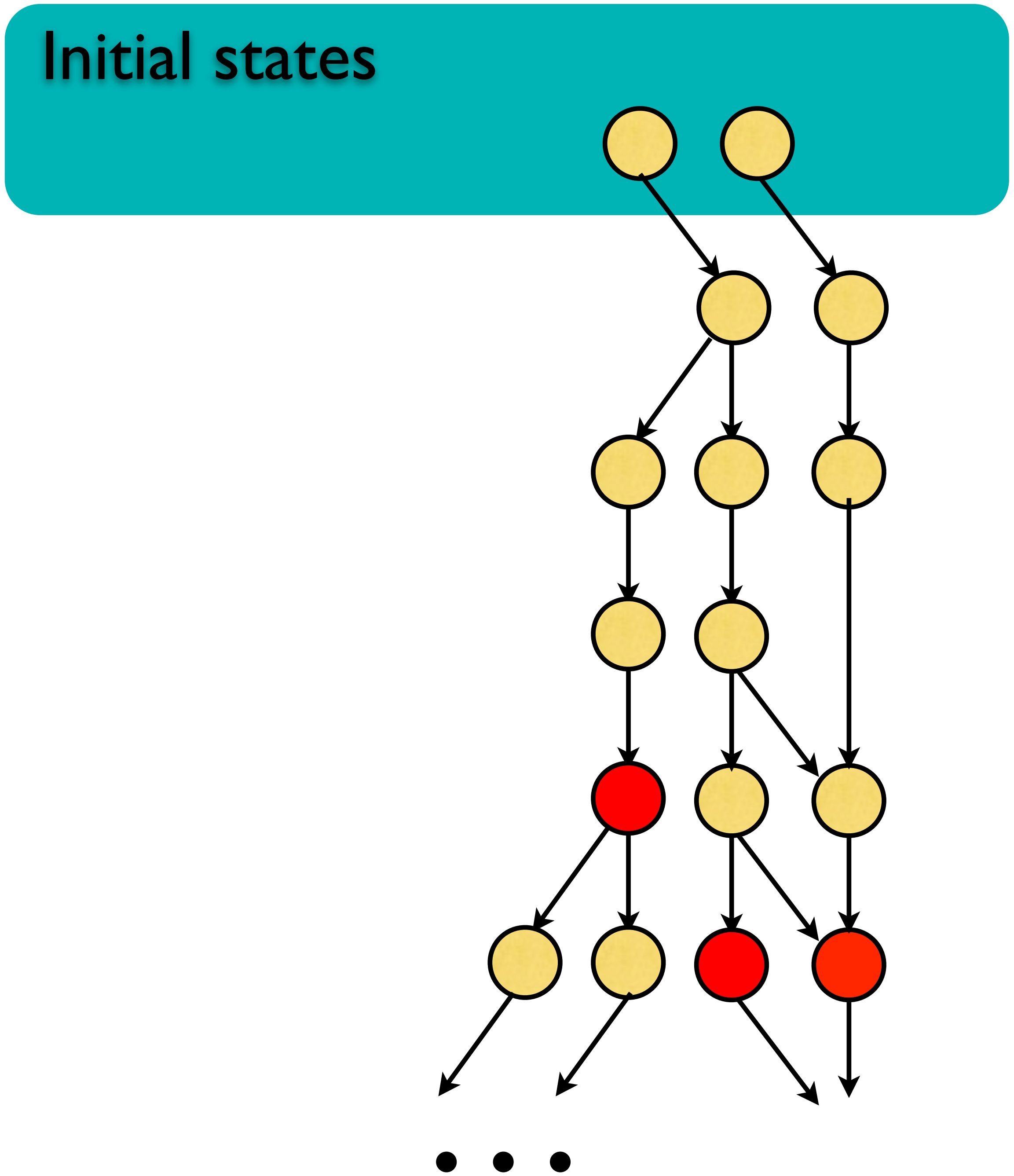


Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`



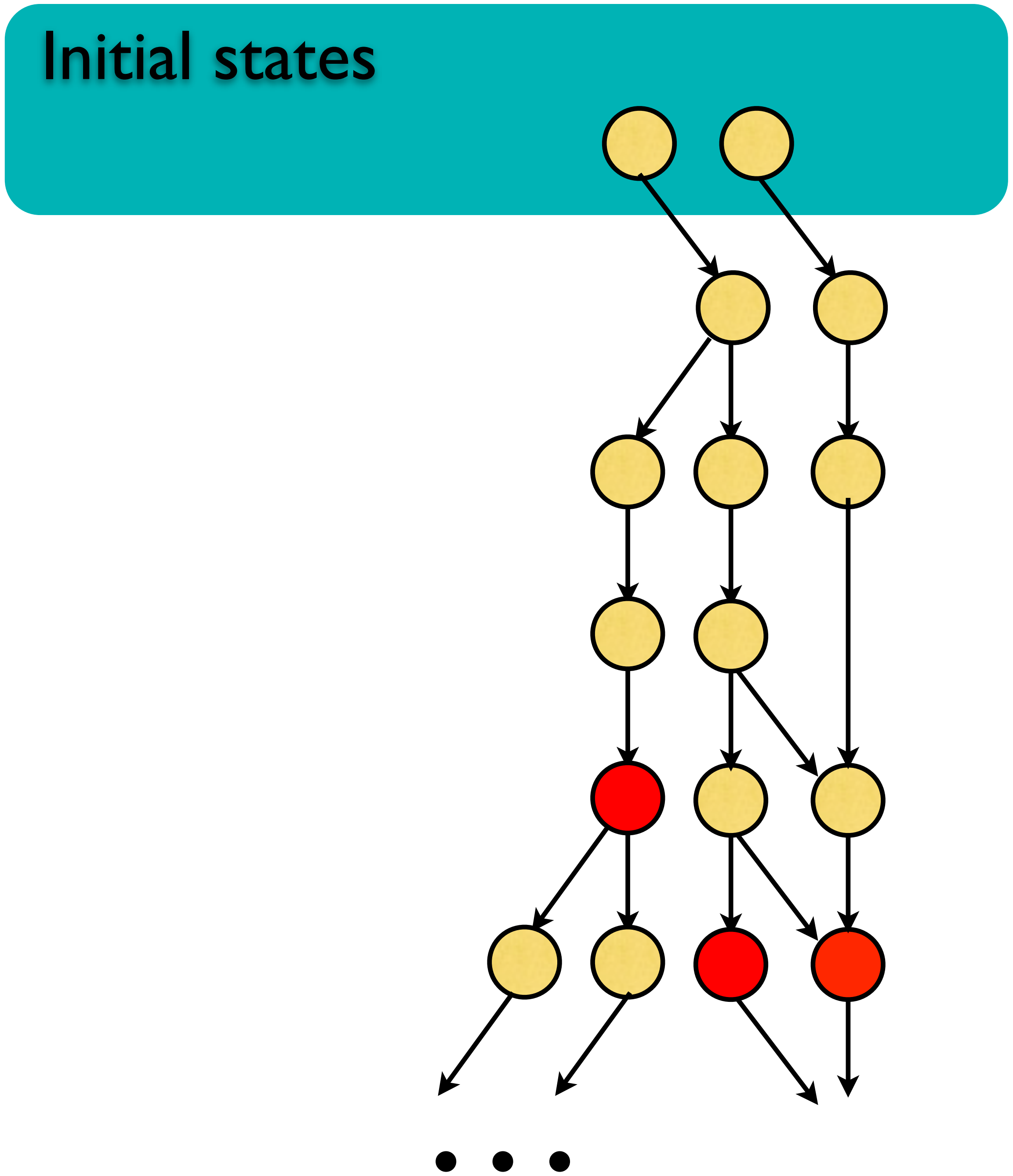
Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`

AF `red` holds!



Automation

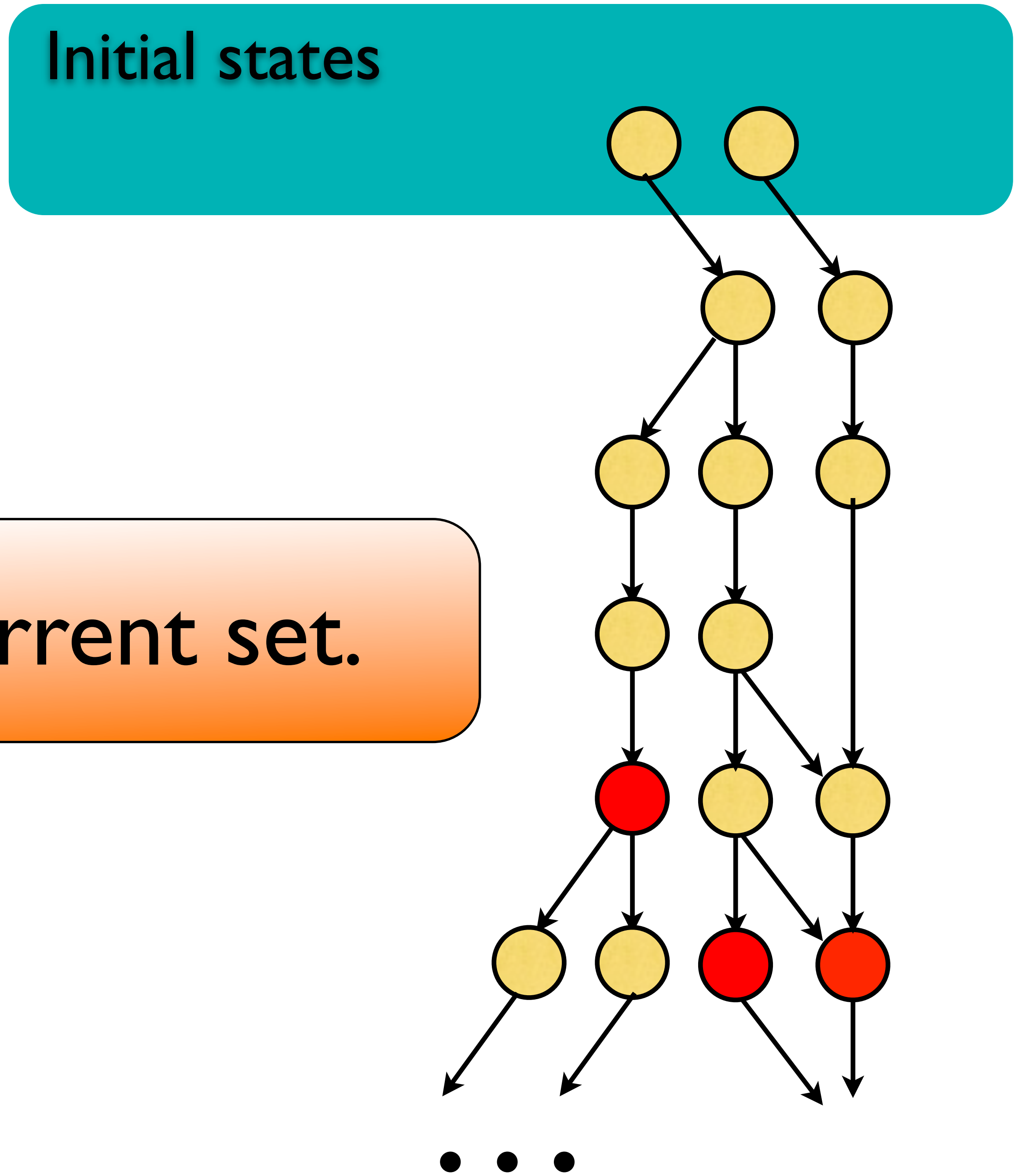
How do we discover ***chutes***?

~~EF `red`~~

AF `red`

AF `red` holds!

Recurrent set.

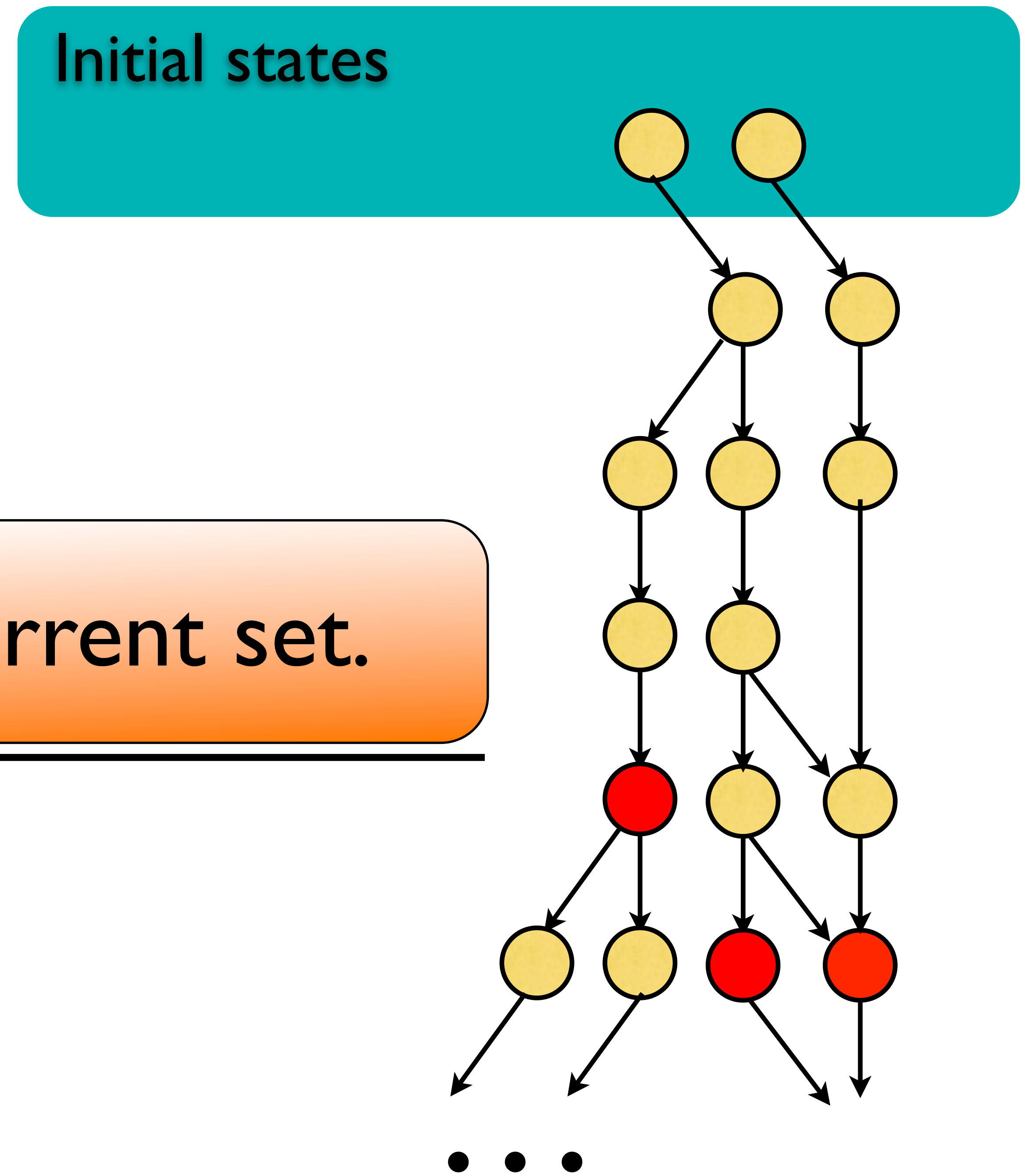


Automation

How do we discover ***chutes***?

~~EF `red`~~

AF `red`



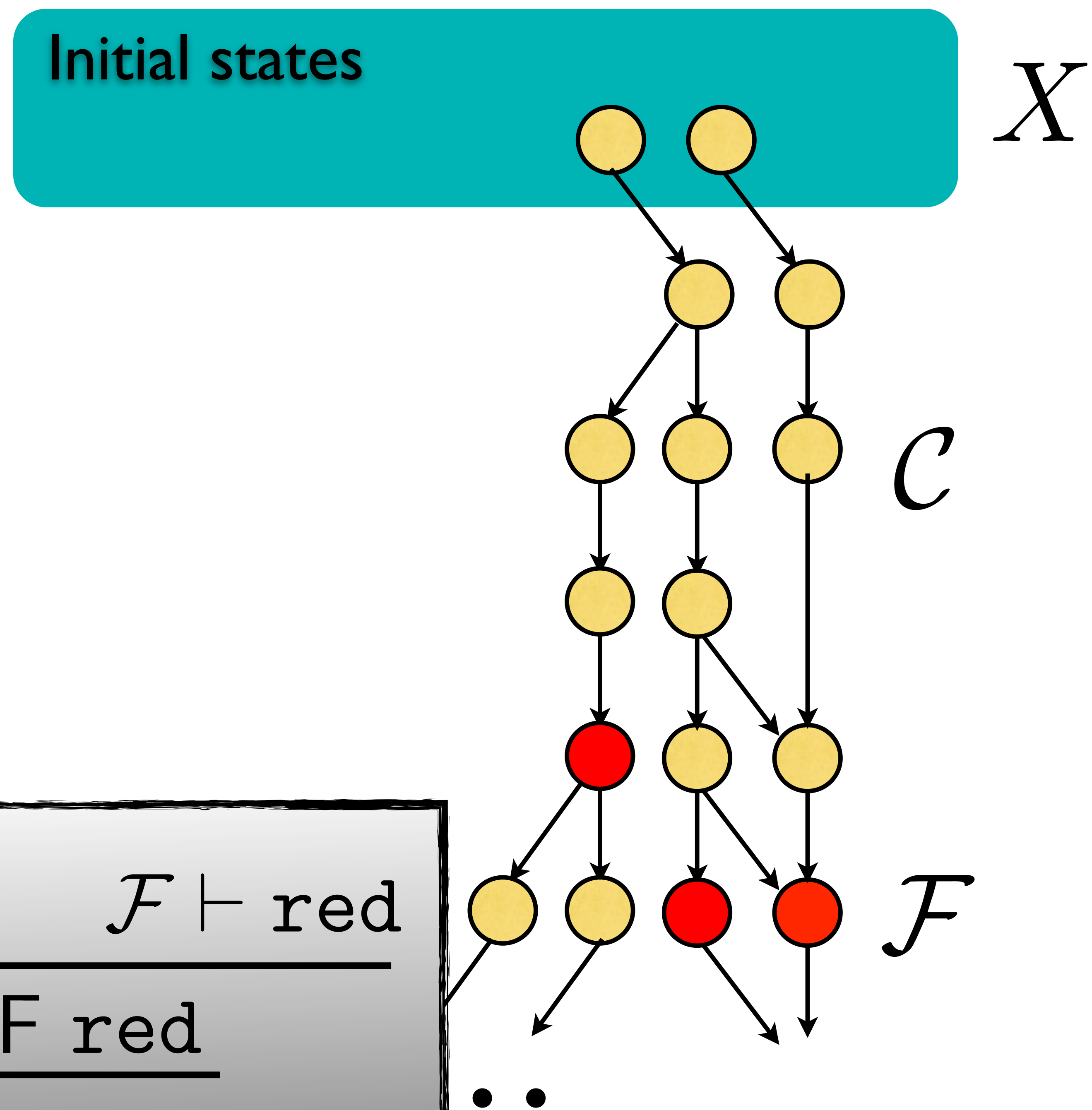
AF `red` holds! | **Recurrent set.**

EF `red`

Automation

How do we discover ***chutes***?

EF `red`



$$\dfrac{(X,\mathcal{C},\mathcal{F}) \text{ is rcr} \qquad \dfrac{\mathbf{W}_X^{\mathcal{C},\mathcal{F}} \text{ is w.f.} \qquad \mathcal{F} \vdash \texttt{red}}{X,\mathcal{C},\mathcal{F} \Vdash \mathsf{F}\ \texttt{red}}}{X \vdash \mathsf{EF}\ \texttt{red}}$$

Automation

Iterated refinement Algorithm

Prove(P, Φ) :

let Φ' = Φ where replace "E" with "A" **in**

loop

match ($P \vdash_{\forall} \Phi$) **with**

| Fail χ in EG or EF → eliminate χ

| Fail χ in AG or AF → **return** Fail

| Succeed →

if C's are recurrent, **return** Succeed

else return Fail

Implementation

- *Input*: C program, CTL property
- CIL front-end, generate the CAV'11 encoding
- *Safety*: prove encoding "cannot return false" (SLAM or BLAST)
- *Termination (AF/EF)*:
  term. argument refinement via Terminator/ARMC
- *Recurrent sets (EF/EG)*: Octagon and SMT solver

Implementation

- *Input*: C program, CTL property
- CIL front-end, generate the CAV'11 encoding
- *Safety*: prove encoding "cannot return false" (SLAM or BLAST)
- *Termination (AF/EF)*: term. argument refinement via Terminator/ARMC
- *Recurrent sets (EF/EG)*: Octagon and SMT solver

Work in progress . . .

End of talk :-)

More about me

Biography

Research Scientist, Principal Investigator, Courant Institute (NYU)

PhD from University of Cambridge (Byron Cook, Mike Gordon)

ScM from Brown University (Maurice Herlihy)

Software Engineer at Amazon.com

Research

Thesis: Temporal verification [CAV'11,POPL'11,FMSD'12]

Depth-bounded systems, Bound analysis [PLDI'09]

Concur: Transactional Memory [PPoPP08,SPAA08i, SPAA08ii]

Systems: Req Tracing [EuroSys08]