# COL:750

## Foundations of Automatic Verification

Instructor: Priyanka Golia

Course Webpage

https://priyanka-golia.github.io/teaching/COL-750/index.html

# Model Checking Algorithm — so far

$$M, s \vDash F?$$

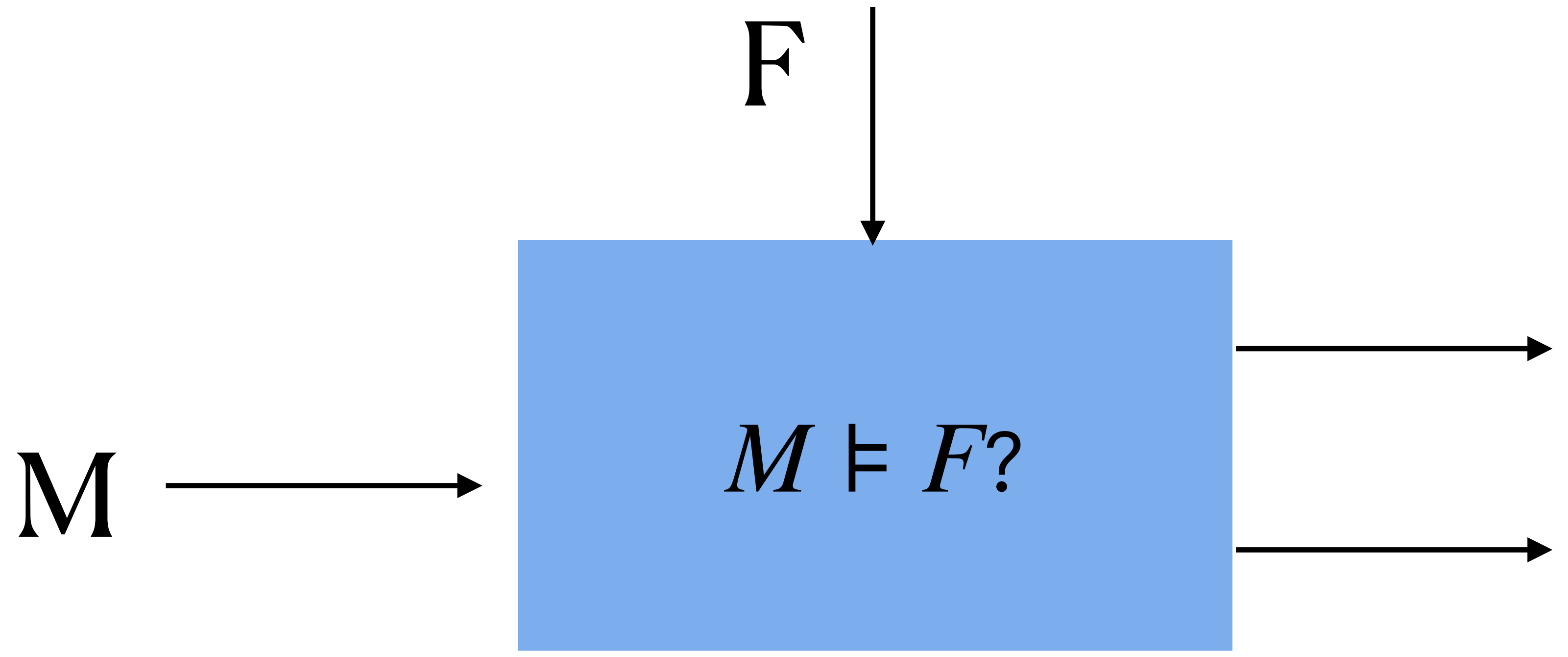

$S' \quad s.t. S' \subseteq S$, and $M, s \vDash F \ \forall s \in S'$

All states s of the model M that satisfy F

Note that not necessarily $I \subseteq S'$

# Model Checking Algorithm

$M, s \models F?$




Yes, if $M, s \models F, \forall s \in I$

No, if $\exists s \in I \; s.t. \; M, s \not\models F$,

A path of the system M demonstrating that M can't satisfy F

Bounded Model Checking with SAT (BMC)

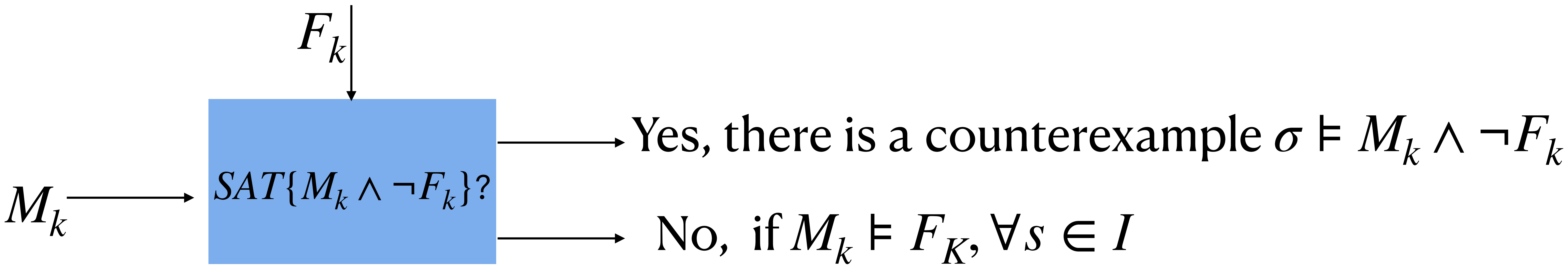
Given: Transition system M, Temporal logic formula F, and a user-supplied time bound k

Output: UNSAT, if $M$ unrolled upto $k$ satisfies F

A counterexample if $M$ unrolled upto $k$ don't satisfy F

# Model Checking Algorithm

$M, s \vDash F?$




Bounded Model Checking with SAT (BMC)

Given: Transition system M, Temporal logic formula F, and a user-supplied time bound k

Output: UNSAT, if $M$ unrolled upto $k$ satisfies F

A counterexample if if $M$ unrolled upto $k$ don't satisfy F

# Bounded Model Checking with SAT (BMC)

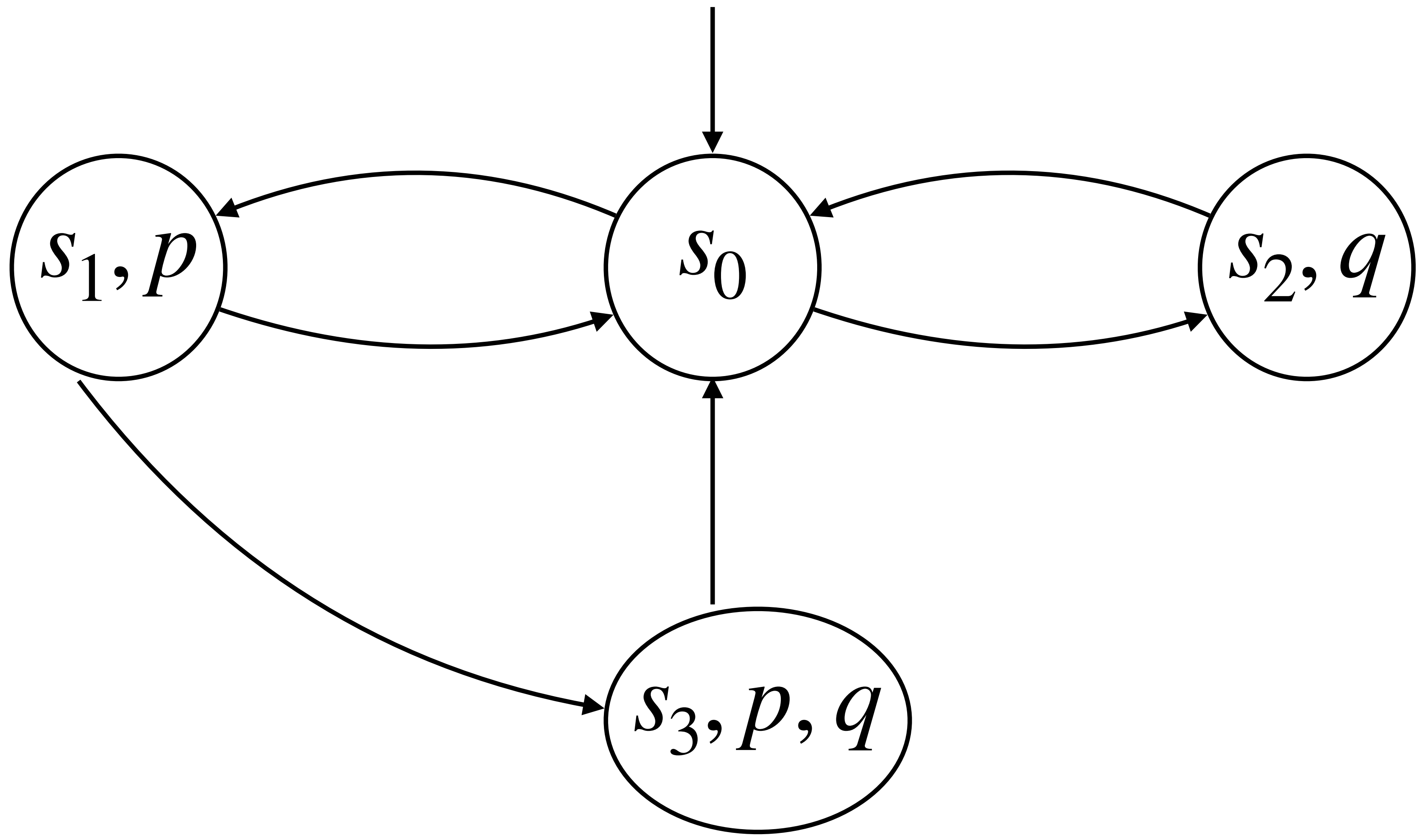
General idea:

1. Convert transition system to propositional encoding — unroll for path length k
2. Convert temporal formula along the states to propositional encoding for *k* length.
3. Using SAT Solvers look for counterexamples

# Bounded Model Checking with SAT (BMC)

Given two processes P and Q which share a resource R.

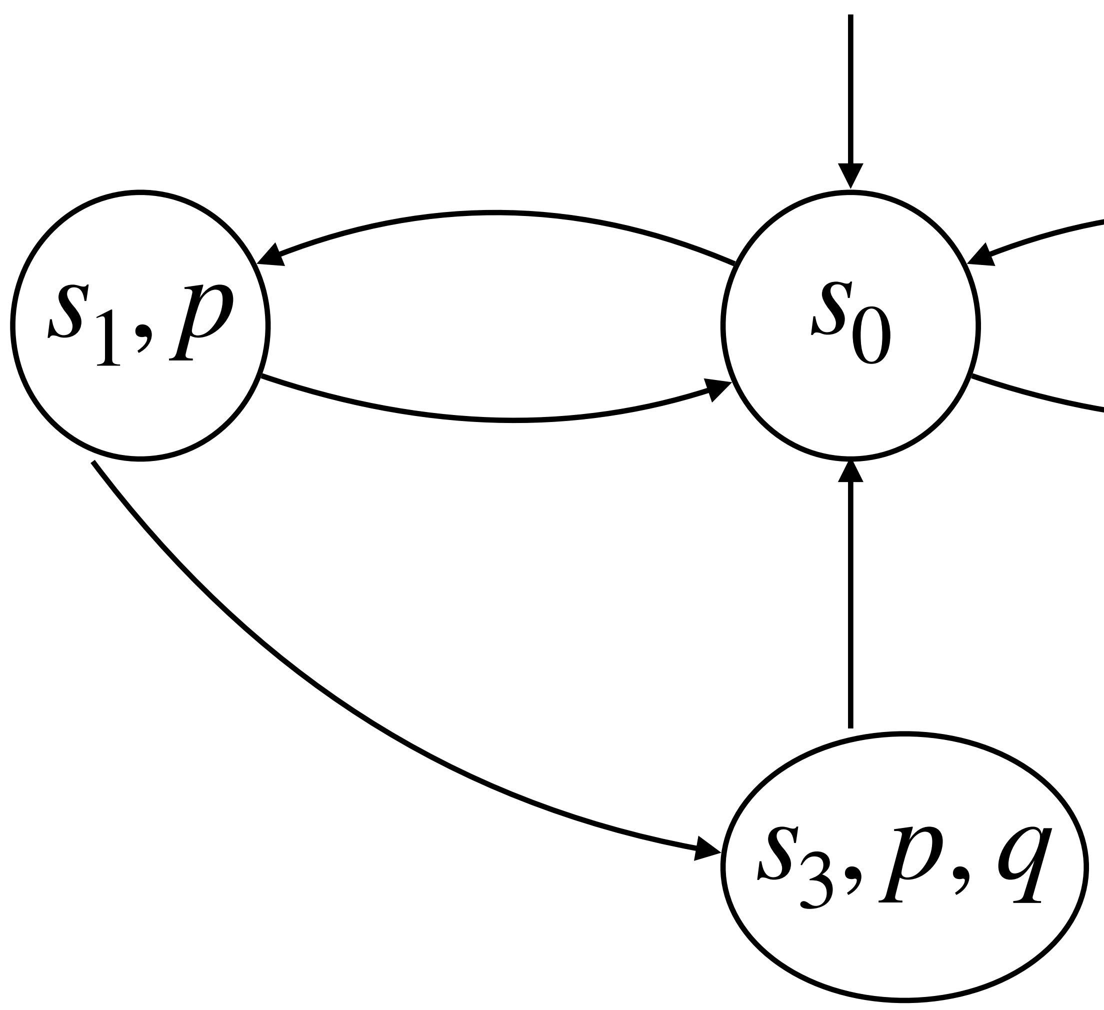
1. If R is accessed by P, then property p is True.
2. If R is accessed by Q, then property q is True.




Does $\forall \Box \neg(p \wedge q)$

K = 1

# Bounded Model Checking with SAT (BMC)




Does $\forall \Box \neg(p \wedge q)$

K = 1

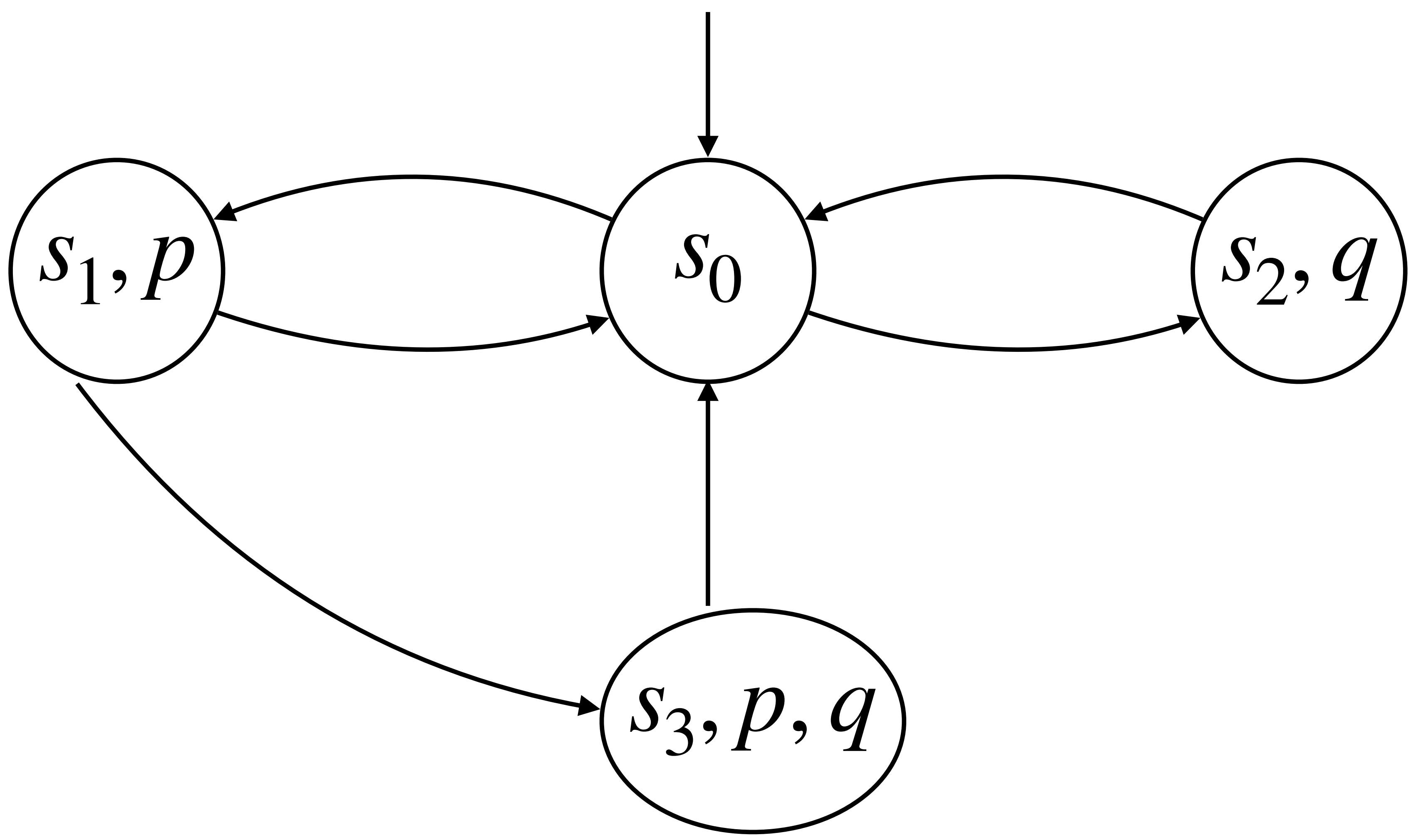
$$M_k = (\neg p_0 \wedge \neg q_0) \wedge ((\neg p_0 \wedge \neg q_0 \wedge p_1 \wedge \neg q_1) \vee (\neg p_0 \wedge \neg q_0 \wedge \neg p_1 \wedge q_1))$$

K = 1

$$\neg F_k = p_1 \wedge q_1$$

$SAT\{M_k \wedge \neg F_k\}$ $\longrightarrow$ UNSAT, $M_{k=1} \models F_{k=1}$

# Bounded Model Checking with SAT (BMC)




Does $\forall \Box \neg(p \land q)$

K = 2

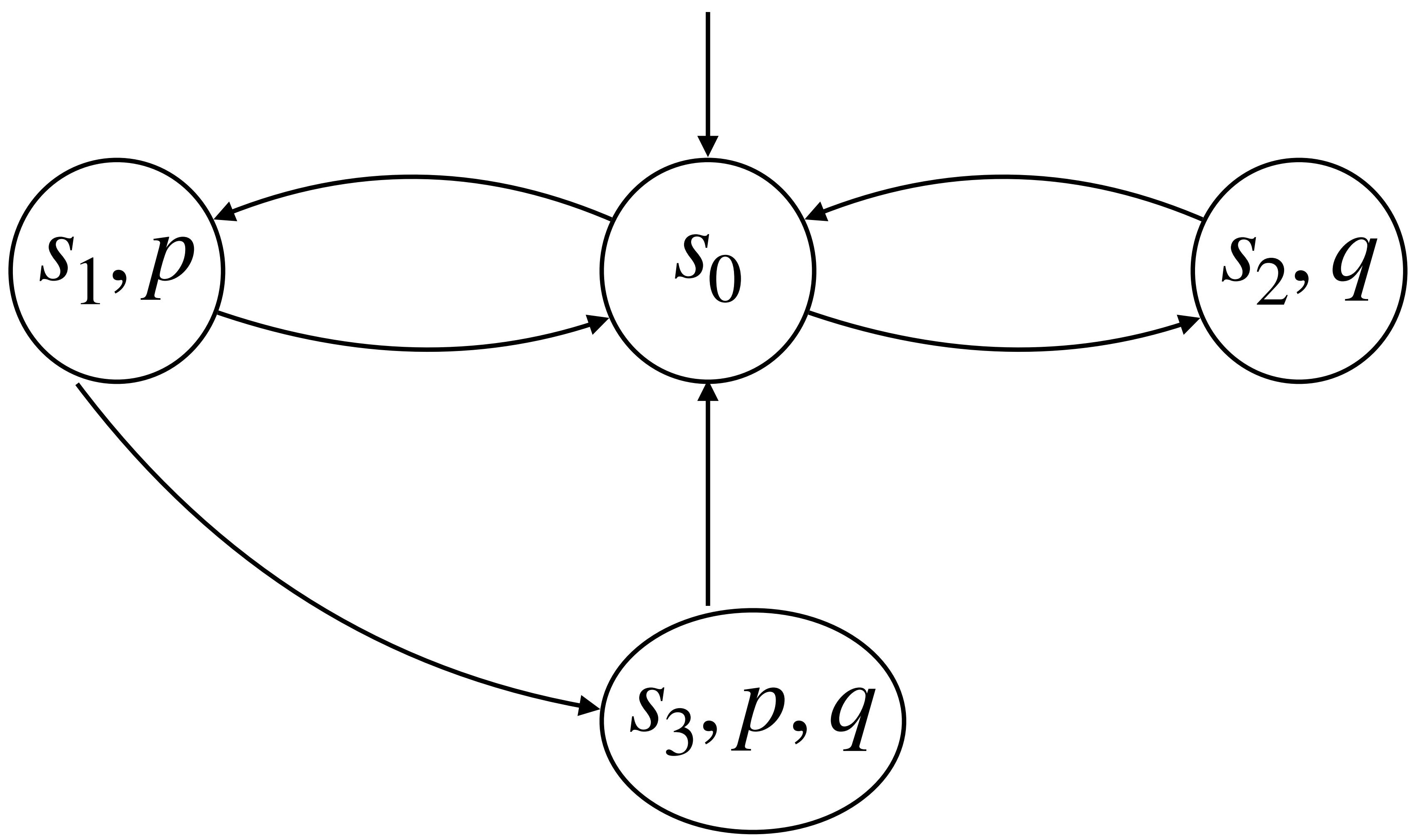
$$M_k = (\neg p_0 \land \neg q_0) \land ((\neg p_0 \land \neg q_0 \land p_1 \land \neg q_1) \lor (\neg p_0 \land \neg q_0 \land \neg p_1 \land q_1))$$

K = 1

$$M_k = (\neg p_0 \land \neg q_0) \land ((\neg p_0 \land \neg q_0 \land p_1 \land \neg q_1) \lor (\neg p_0 \land \neg q_0 \land \neg p_1 \land q_1))$$
$$\land (((p_1 \land \neg q_1 \land p_2 \land q_2) \lor (p_1 \land \neg q_1 \land \neg p_2 \land \neg q_2)) \lor (\neg p_1 \land q_1 \land \neg p_2 \land \neg q_2)))$$

K = 2

# Bounded Model Checking with SAT (BMC)




Does $\forall \square \neg(p \wedge q)$

K = 2

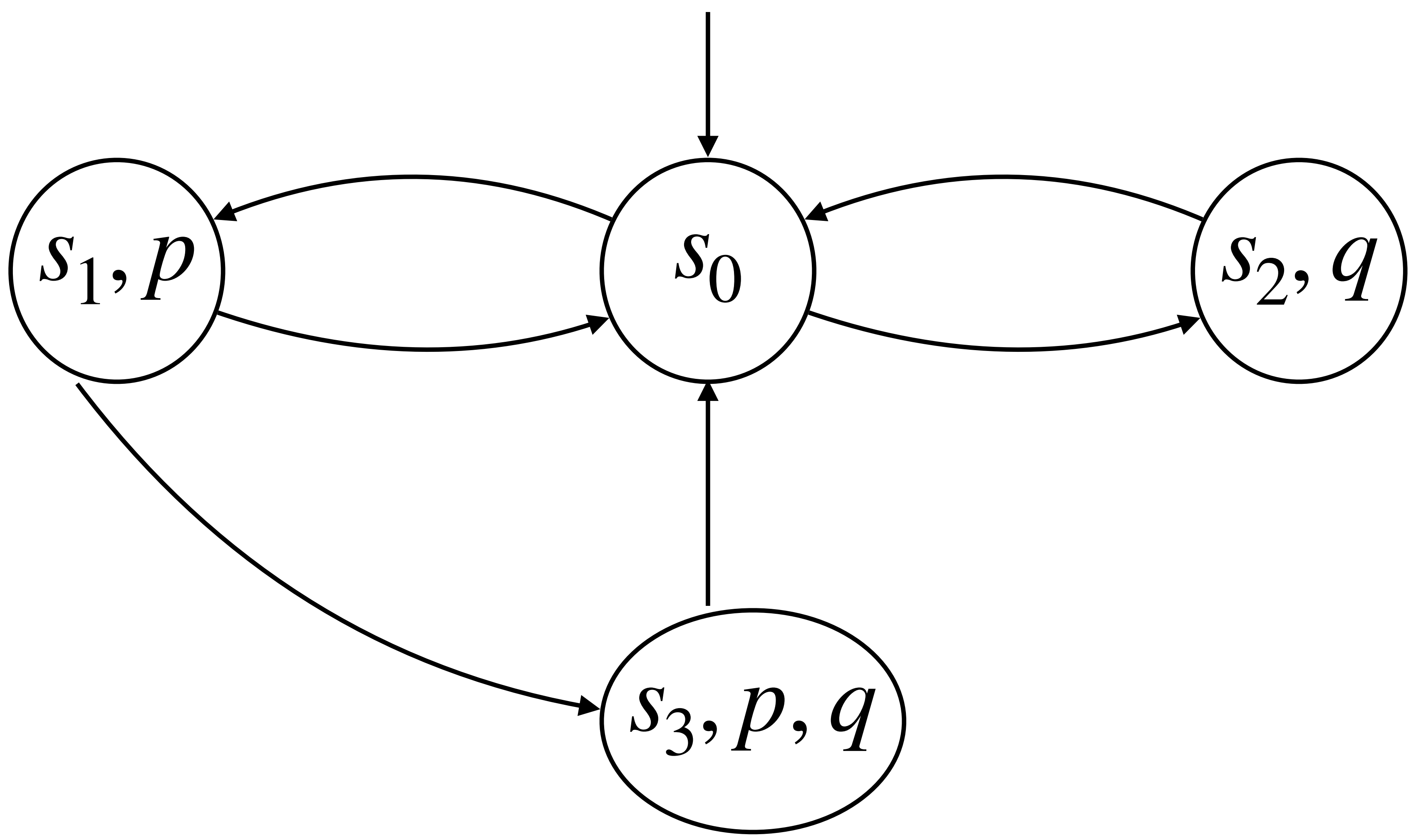
$$M_k = (\neg p_0 \wedge \neg q_0) \wedge ((\neg p_0 \wedge \neg q_0 \wedge p_1 \wedge \neg q_1) \vee (\neg p_0 \wedge \neg q_0 \wedge \neg p_1 \wedge q_1))$$
$$\wedge (((p_1 \wedge \neg q_1 \wedge p_2 \wedge q_2) \vee (p_1 \wedge \neg q_1 \wedge \neg p_2 \wedge \neg q_2)) \vee (\neg p_1 \wedge q_1 \wedge \neg p_2 \wedge \neg q_2)))$$

K = 2

$\neg F = \exists \Diamond (p \wedge q)$ $\quad \neg F_k = p_2 \wedge q_2$

$SAT\{M_k \wedge \neg F_k\}$

# Bounded Model Checking with SAT (BMC)




Does $\forall \Box \neg (p \wedge q)$

K = 2

$$M_k = (\neg p_0 \wedge \neg q_0) \wedge ((\neg p_0 \wedge \neg q_0 \wedge p_1 \wedge \neg q_1) \vee (\neg p_0 \wedge \neg q_0 \wedge \neg p_1 \wedge q_1))$$
$$\wedge (((p_1 \wedge \neg q_1 \wedge p_2 \wedge q_2) \vee (p_1 \wedge \neg q_1 \wedge \neg p_2 \wedge \neg q_2)) \vee (\neg p_1 \wedge q_1 \wedge \neg p_2 \wedge \neg q_2)))$$

K = 2

$\neg F_k = p_2 \wedge q_2$

$SAT\{M_k \wedge \neg F_k\}$

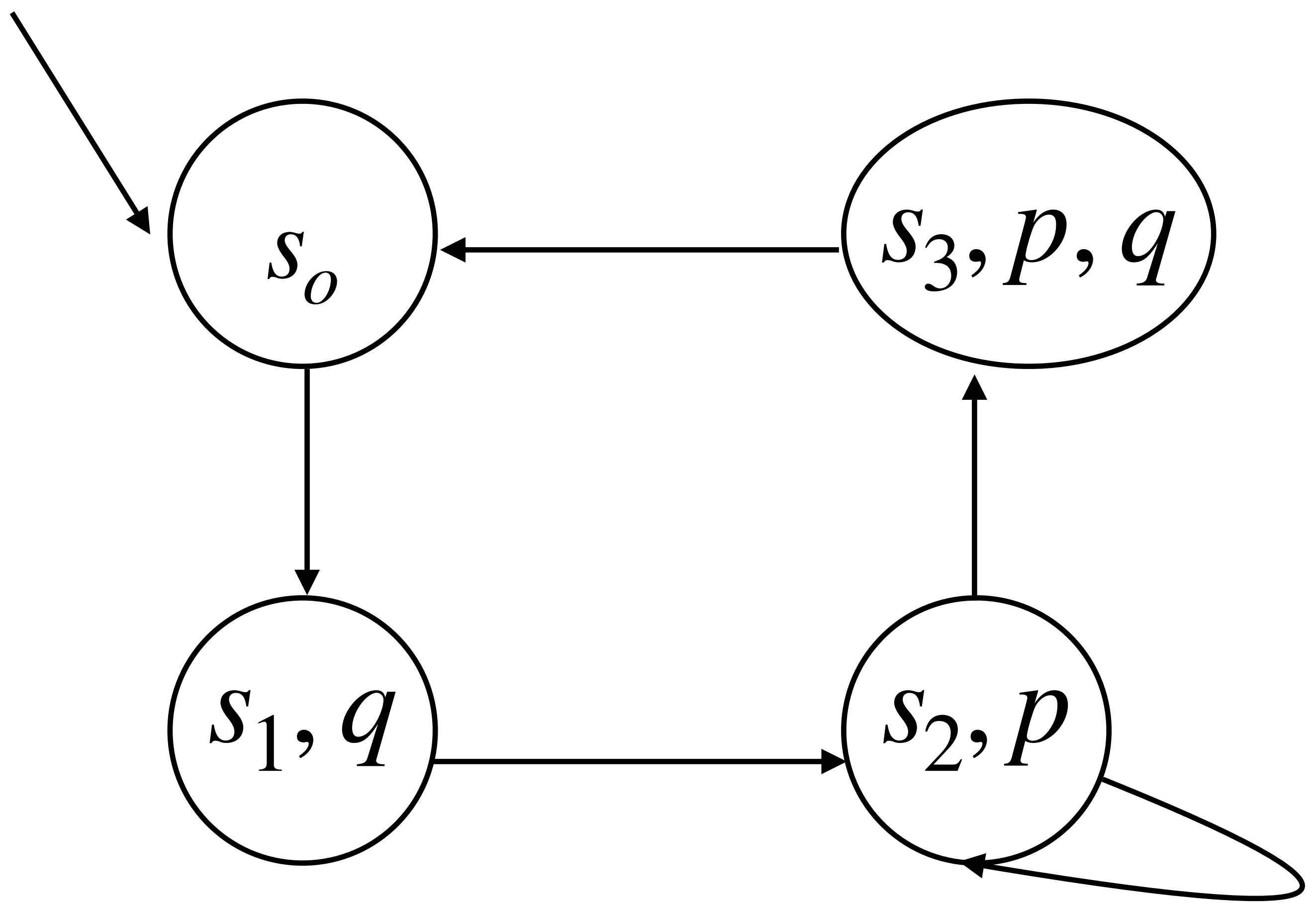
$\sigma = \langle p_0 = 0, q_0 = 0, p_1 = 1, q_1 = 0, p_2 = 1, q_2 = 1 \rangle$

$M_k \nvDash F_k$

$s_o, s_1, s_3$

# Bounded Model Checking with SAT (BMC)

Two-bit counter




$$F = \forall \Diamond (p \wedge q) \quad \neg F = \exists \Box \neg p \vee \neg q$$

K = 3

$$M_k = (\neg p_o \wedge \neg q_o) \wedge (\neg p_o \wedge \neg q_o \wedge \neg p_1 \wedge q_1) \wedge (\neg p_1 \wedge q_1 \wedge p_2 \wedge \neg q_2) \wedge ((p_2 \wedge \neg q_2 \wedge p_3 \wedge \neg q_3) \vee (p_2 \wedge \neg q_2 \wedge p_3 \wedge q_3))$$

$$\neg F_k = (\neg p_o \vee \neg q_o) \wedge (\neg p_1 \vee \neg q_1) \wedge (\neg p_2 \vee \neg q_2) \wedge (\neg p_3 \vee \neg q_3)$$

$M_k \wedge \neg F_k$ $\quad$ $SAT\{M_k \wedge \neg F_k\}$

What happens for K= 2?

$$\sigma = \langle p_0 = 0, q_0 = 0, p_1 = 0, q_1 = 1, p_2 = 1, q_2 = 0, p_3 = 1, q_3 = 0 \rangle$$

$M_k \nvDash F_k$ $\quad$ $s_o, s_1, s_2, s_2$

# Bounded Model Checking with SAT (BMC)

Property - $\forall \Diamond p$ Every path in M includes a state in which p is True.

$\exists \Box \neg p$ An infinite path in which all states satisfy $\neg p$. A loop is needed!

Lasso: A lasso is a finite path that consists of:

A prefix: a finite sequence of transitions from the initial state.

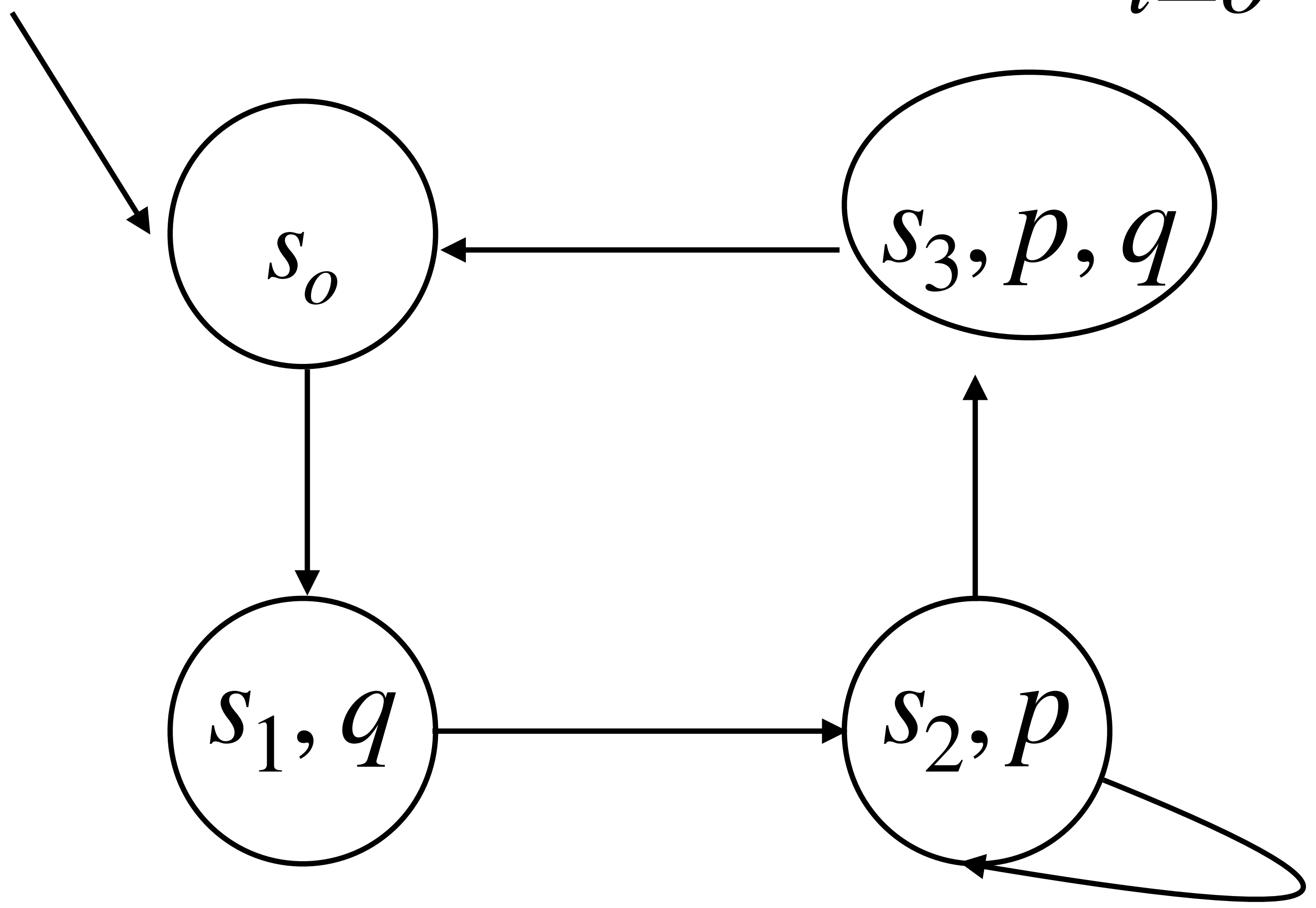
A loop: a back edge that loops from the last state back to some earlier state.

$$Lasso_k(s_o, \ldots, s_k) := \bigvee_{i=o}^{k} T(s_k, s_i)$$

$$M_k \models (\exists \Box \neg p)_k := M_k \wedge (Lasso_i(s_o, \ldots, s_k) \wedge \bigwedge_{i=o}^{k} \neg p(s_i)$$

# Bounded Model Checking with SAT (BMC)

$$Lasso_k(s_o, \ldots, s_k) := \bigvee_{i=o}^{k} T(s_k, s_i) \qquad M_k \vDash (\exists \Box \neg p)_k := M_k \wedge (Lasso_i(s_o, \ldots, s_k) \wedge \bigwedge_{i=o}^{k} \neg p(s_i)$$




$$M \overset{?}{\vDash} \forall \Diamond (p \wedge q)$$

K =2

$$M_2 \vDash (\exists \Box \neg p \vee \neg q)_2 :=$$

$$M_k \wedge (T(s_2, s_0) \vee T(s_2, s_1) \vee T(s_2, s_2)) \wedge (\neg p_o \vee \neg q_o) \wedge (\neg p_1 \vee \neg q_1) \wedge (\neg p_2 \vee \neg q_2))$$

# Bounded Model Checking with SAT (BMC)

How big should be K?

For every model $M$ and formula (LTL/CTL) F, there exists k, such that

$$M \models_K F \rightarrow M \models F$$

The minimal such k is the Completeness Threshold (CT).

# Bounded Model Checking with SAT (BMC)

How big should be K?

For every model $M$ and formula (LTL/CTL) F, there exists k, such that

$$M \vDash_K F \rightarrow M \vDash F$$

The minimal such k is the Completeness Threshold (CT).

Diameter of M

The diameter of a Kripke structure is the longest shortest path between any two reachable states. Formally:

$$\text{Diameter(M)} = \underset{\forall s, s' \in T}{Max} \; ShortestPathLength(s, s')$$

# Bounded Model Checking with SAT (BMC)

Diameter of M

The diameter of a Kripke structure is the longest shortest path between any two **reachable states**. Formally:

$$\text{Diameter(M)} = \underset{\forall s, s' \in T}{Max}\ ShortestPathLength(s, s')$$

It measures how far apart any two states can be.

It gives a worst case bound on how many steps are required to reach any states from another states.

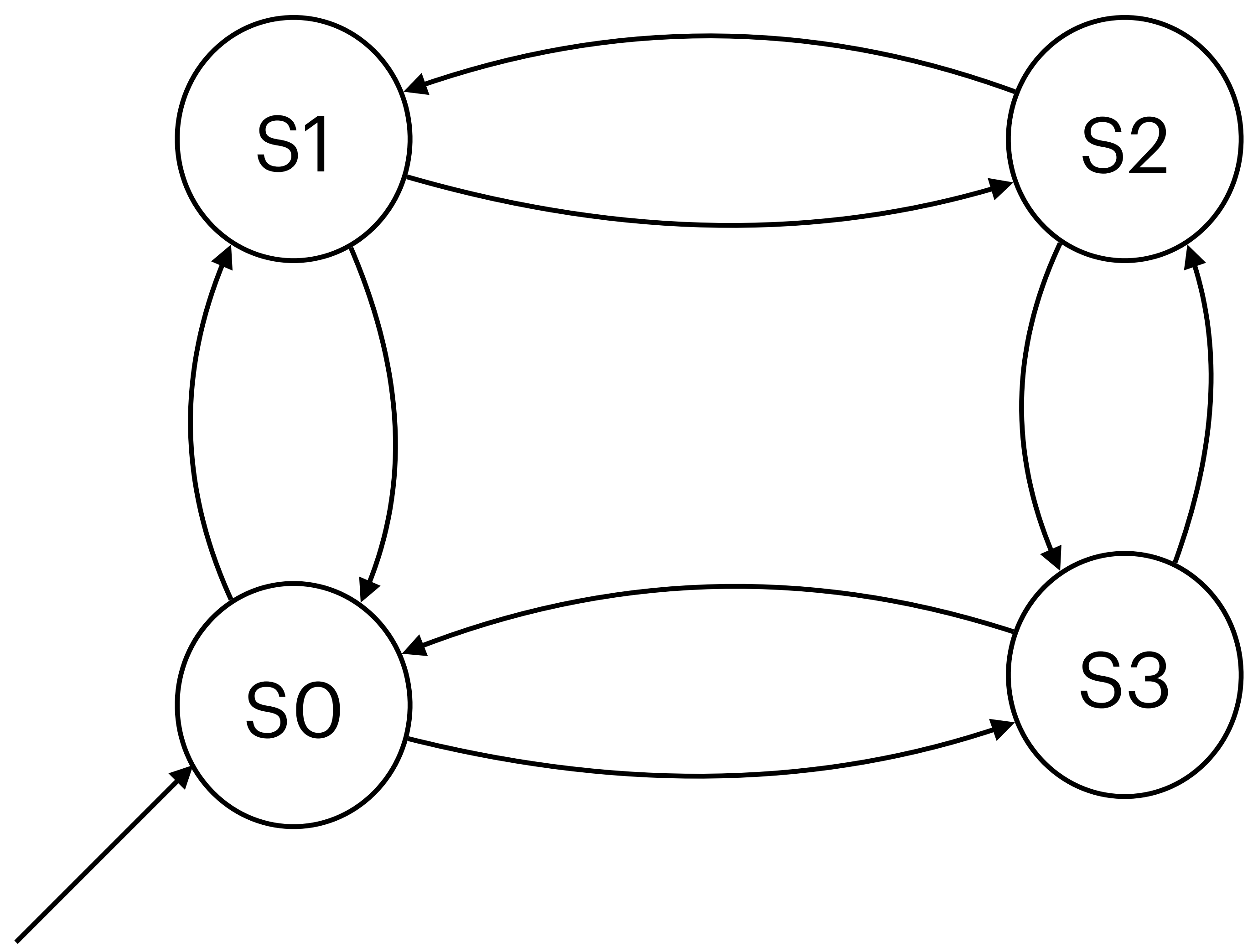
# Bounded Model Checking with SAT (BMC)

Diameter of M

What is the smallest k such that every state is reachable within k transitions?

The diameter of a Kripke structure is the longest shortest path between any two reachable states. Formally:

$$\text{Diameter(M)} = \underset{\forall s, s' \in T}{Max}\ ShortestPathLength(s, s')$$




Diameter is 2.

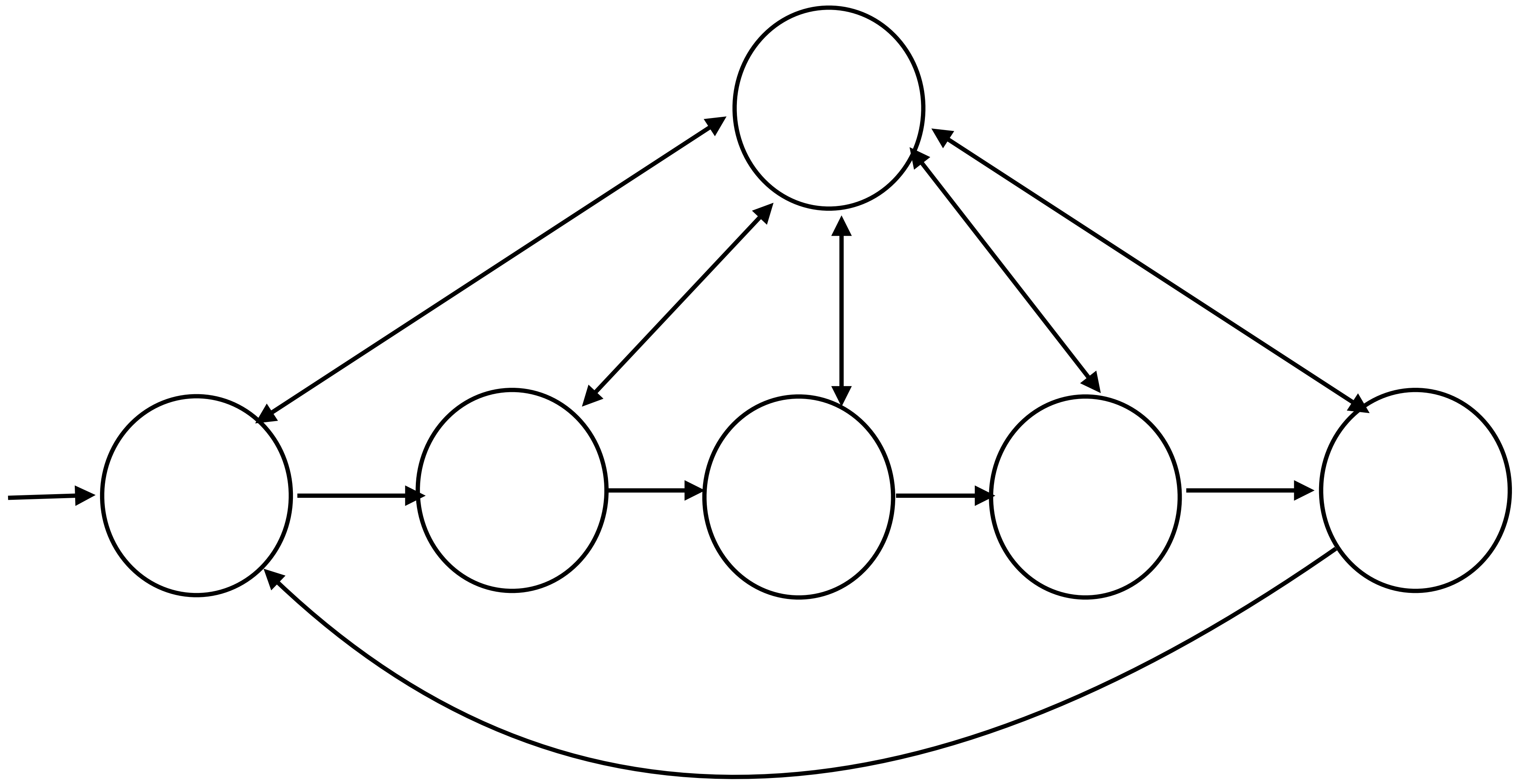
# Bounded Model Checking with SAT (BMC)

Diameter of M

What is the smallest k such that every state is reachable within k transitions?

The diameter of a Kripke structure is the longest shortest path between any two reachable states. Formally:

$$\text{Diameter(M)} = \underset{\forall s, s' \in T}{Max}\ ShortestPathLength(s, s')$$



Diameter is 2.

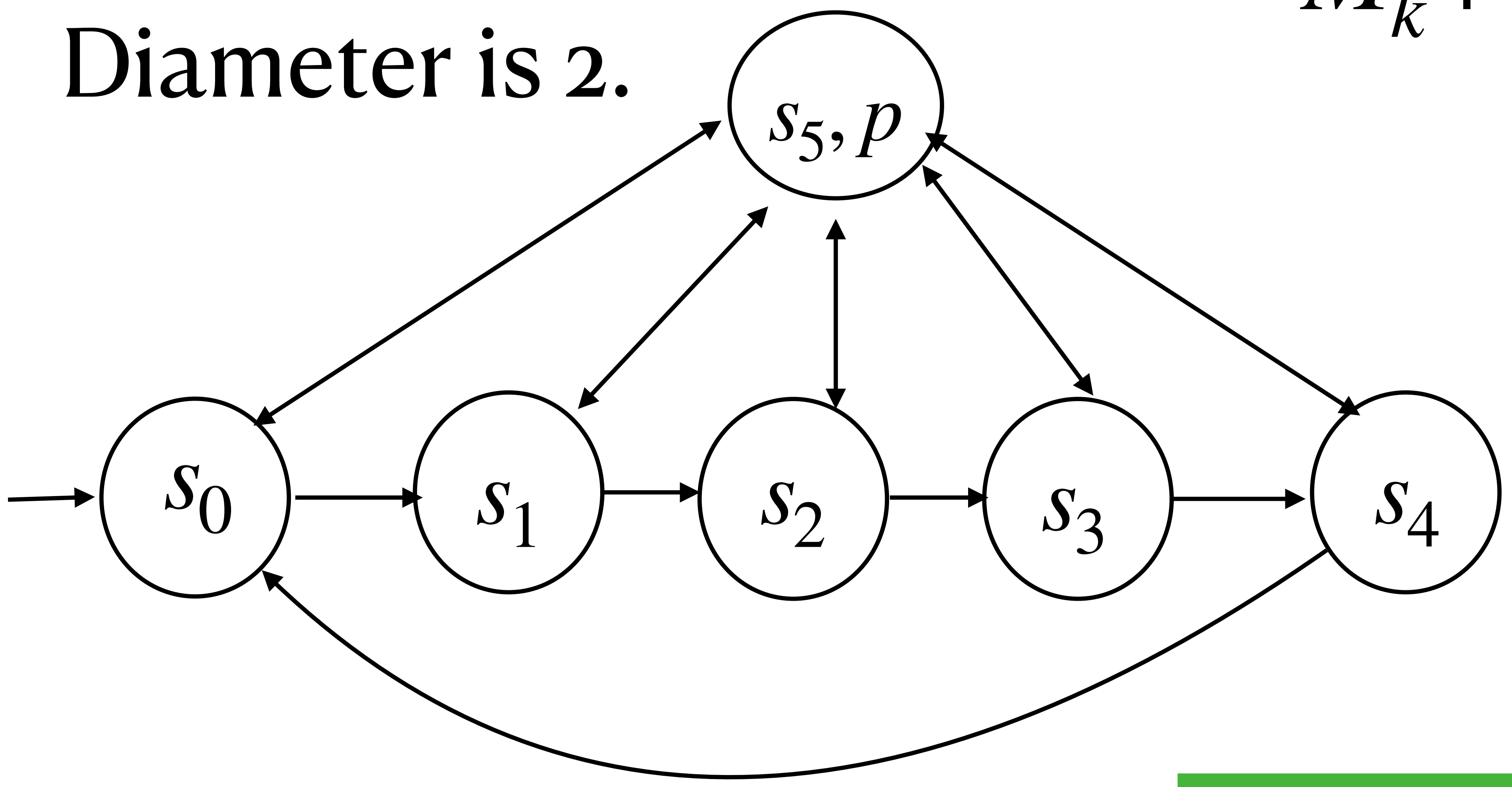
# Bounded Model Checking with SAT (BMC)

Observe that Diameter is not a completeness threshold for arbitrary properties.

Minimum k required for finding a counterexample for $\forall \Diamond p$ ?

$$M_k \vDash (\exists \Box \neg p)_k := M_k \wedge (Lasso_i(s_o, \ldots, s_k) \wedge \bigwedge_{i=o}^{k} \neg p(s_i)$$

Diameter is 2.




Shortest counterexample requires K=5

If F is a liveness property (something that must eventually hold, or hold infinitely, the Diameter is not a completeness threshold

# Bounded Model Checking with SAT (BMC)

Diameter of M

Given a model M, the diameter of M is a completeness threshold for any property of the form $\forall \Box p$

Safety properties — something always holding.

Counterexample — ($\exists \Diamond \neg p$) can we find a bad state in k step?

For Safety property, d is a completeness threshold.

# Bounded Model Checking with SAT (BMC)

Diameter of M

The diameter of a Kripke structure is the longest shortest path between any two reachable states. Formally:

$$\text{Diameter(M)} = \underset{\forall s, s' \in T}{Max}\ ShortestPathLength(s, s')$$

How to check if $K \overset{?}{\geq} d$?

State s is reachable in j steps:

$$R_j(s) = \exists s_o, \ldots, s_j\ s.t.\ s_j \wedge I(s_o) \wedge \bigwedge_{i=o}^{j-1} T(s_i, s_{i+1})$$

K is greater than or equal to Diameter d if

$$\forall s : R_{k+1}(s) \rightarrow \exists j \leq k\ R_j(s)$$

For all states, does there exists a path of length at most k?

Computationally hard problem — requires QBF calls.

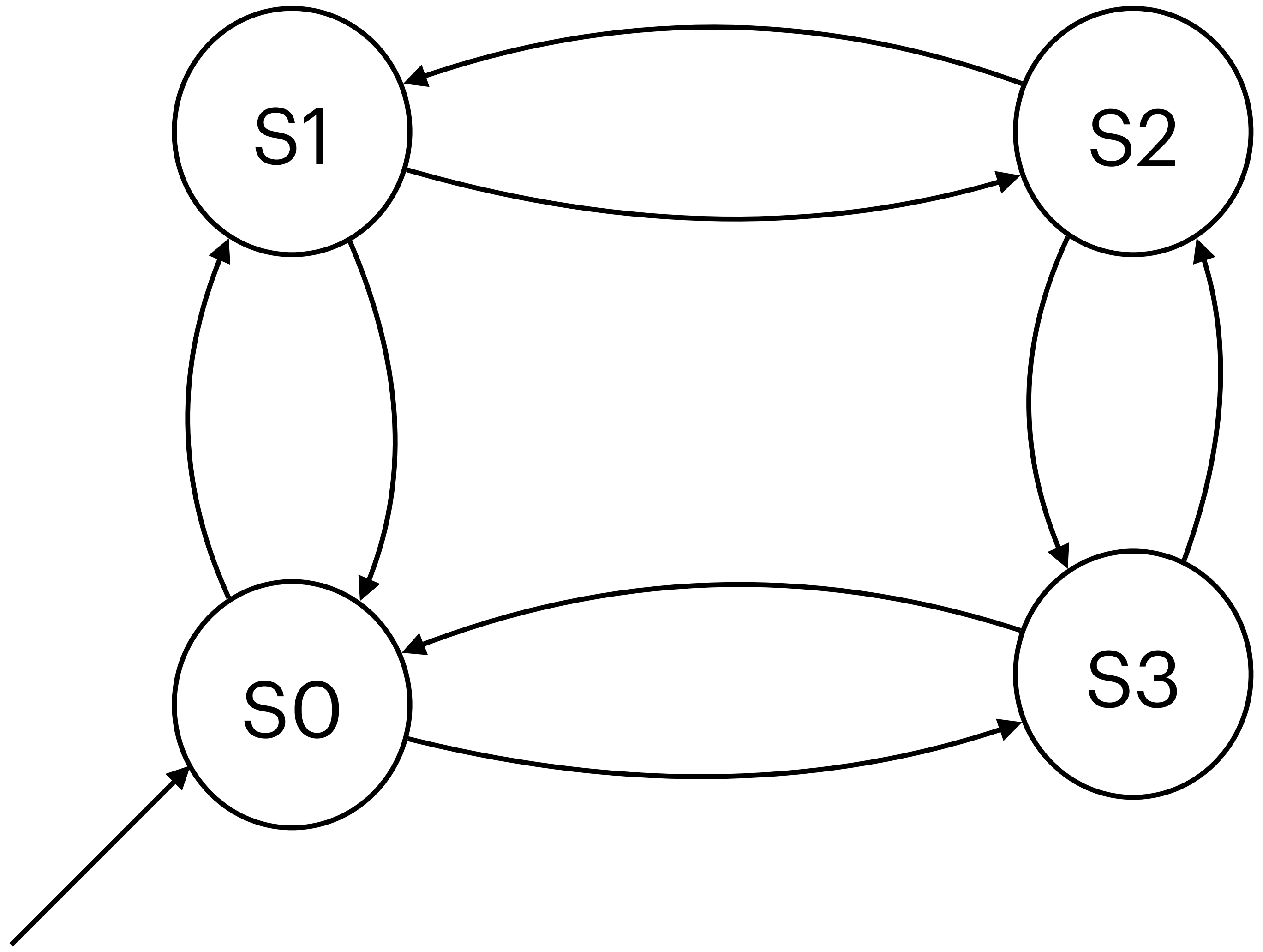
# Bounded Model Checking with SAT (BMC)

Recurrence Diameter: Least number of steps n such that all valid paths of length n have at least one cycle.

$rd$ is the longest loop-free path in M.

Recurrence Diameter $(rd)$ is an upper bound for the diameter d.

$d = 2 \quad rd = 4$




This means that after $rd$ steps, either:

All reachable states have been visited.

Any further steps must repeat a previously visited state.

# Bounded Model Checking with SAT (BMC)

General idea:

Fix a K

1. Convert transition system to propositional encoding — unroll for path length k

2. Convert temporal formula along the states to propositional encoding for k length

3. Using SAT Solvers look for counterexamples

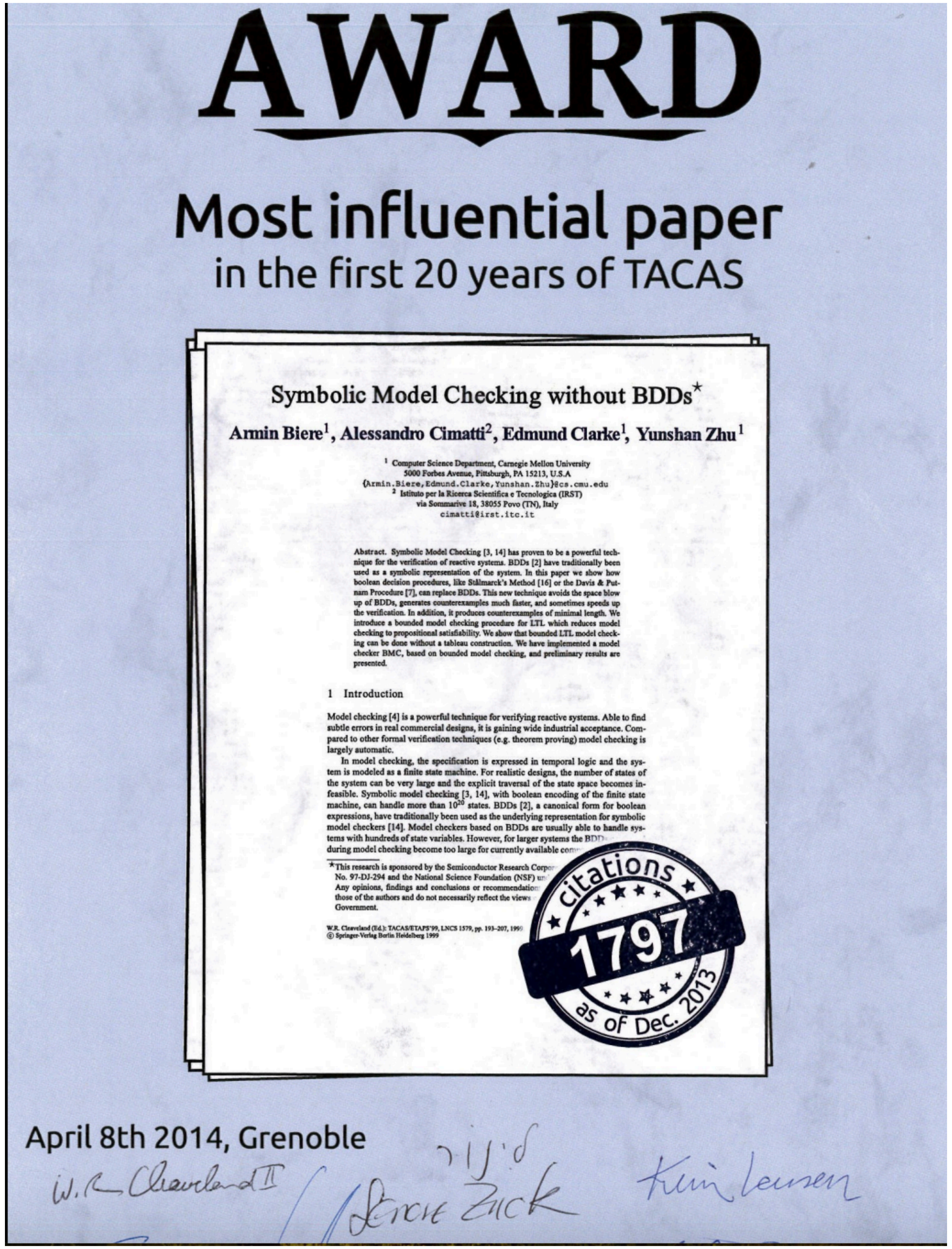
4. Found a counterexample :

   Return counterexample

5. Else:

   K= K+1

6. At some point, check if $K \overset{?}{\geq} rd$ Return True, Else: K = K+1 For safety property.




## extensions to completeness

diameter checking,

k-induction,

interpolation –

SAT based model checking without unrolling: IC3