COL:750

Foundations of Automatic Verification

Instructor: Priyanka Golia

Course Webpage 

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

CTL Model Checking Algorithm —Symbolic Model Checking

Problems with BDD:

1. BDDs are canonical representation — often become too large.
2. Variable ordering must be uniform along paths.
3. Selecting right variable ordering for small BDDs.
    1. This itself is an open problem, and can consume too much time to predict a right ordering for given instance.
    2. Sometime, no space efficient variable ordering exists.

Bounded Model Checking with SAT (BMC)

- Method used by most “industrial” model checkers.
- BMC uses SAT procedure instead of BDDs.
    - Uses Boolean encoding for transitions and set of states.
- Can handle much larger design.

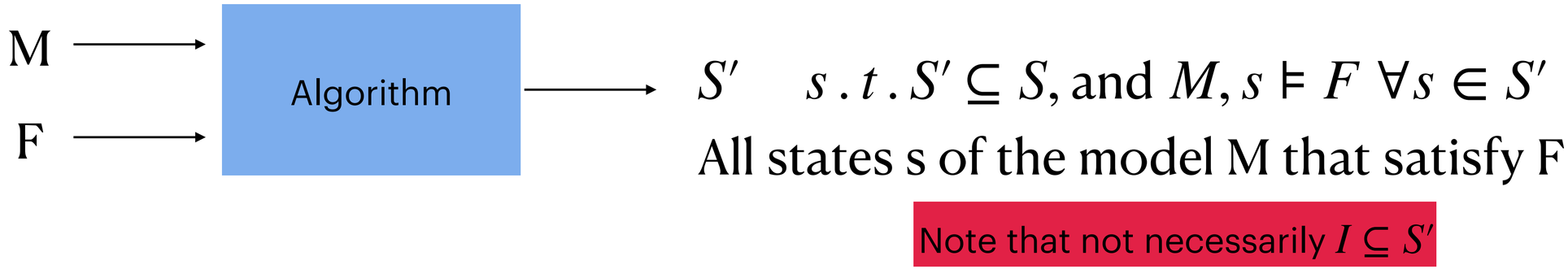
Can we reach a desired state in k steps?

Verification of safety properties — can we find a bad state in k steps?

Verification — can we find a counterexample in k steps?

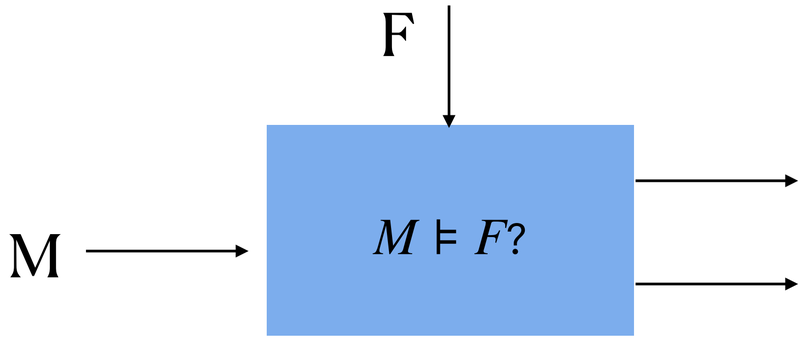
Model Checking Algorithm — so far

$$M, s \models F?$$



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)

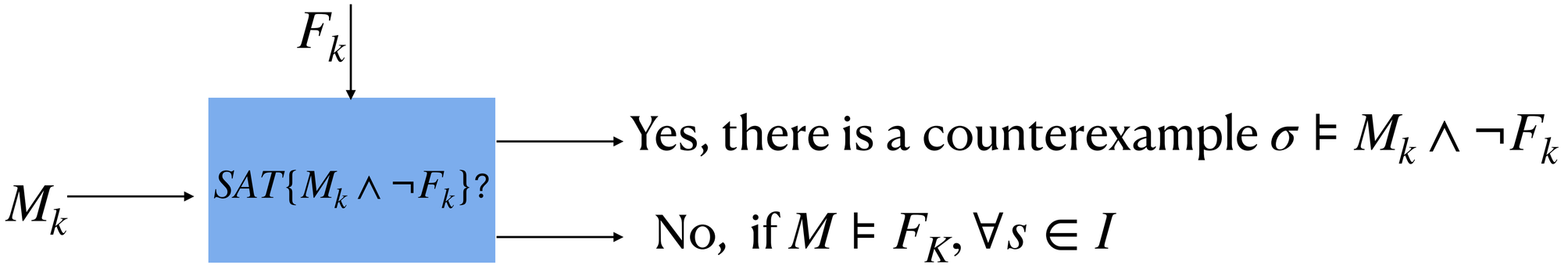
Given: Transition system M, Temporal logic formula F, and a user-supplied time bound k

Output: UNSAT, if M unrolled upto k satisfies F

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

Model Checking Algorithm

$M, s \models F?$



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

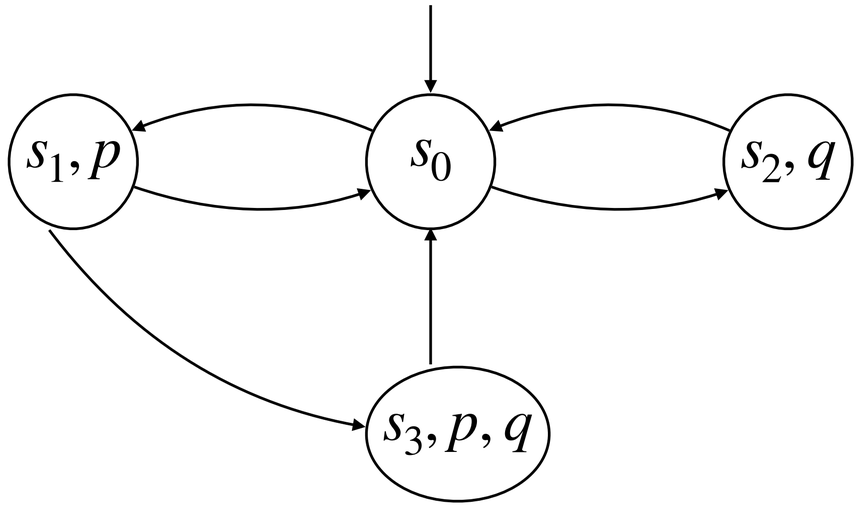
A counterexample if if M unrolled upto k don't satisfy F

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

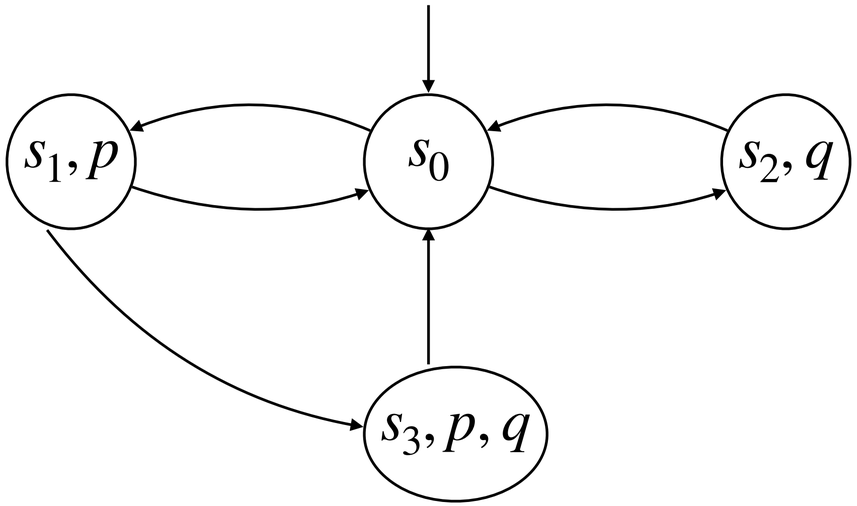
Bounded Model Checking with SAT (BMC)



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

K = 2

Bounded Model Checking with SAT (BMC)



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

K = 2

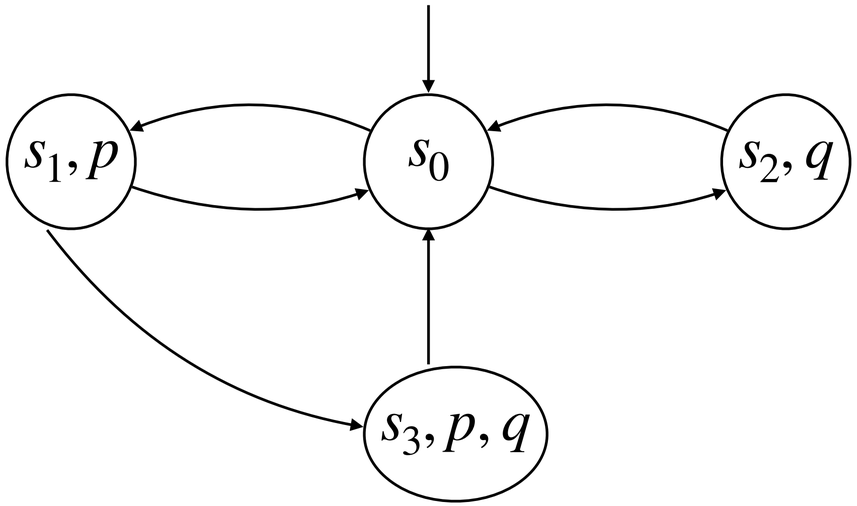
$$M_k = (\neg p_0 \wedge \neg q_0) \wedge ((\neg p_0 \wedge \neg q_0 \wedge p_1 \wedge \neg q_1) \vee (\neg p_0 \wedge \neg q_0 \wedge \neg p_1 \wedge q_1))$$

K = 1

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

K = 2

Bounded Model Checking with SAT (BMC)



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

K = 2

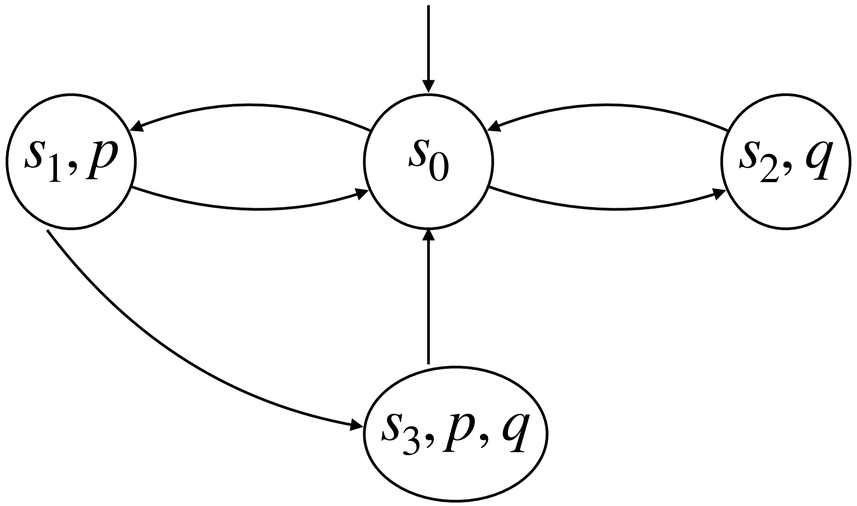
$$M_k = (\neg p_0 \wedge \neg q_0) \wedge ((\neg p_0 \wedge \neg q_0 \wedge p_1 \wedge \neg q_1) \vee (\neg p_0 \wedge \neg q_0 \wedge \neg p_1 \wedge q_1))$$
$$\wedge (((p_1 \wedge \neg q_1 \wedge p_2 \wedge q_2) \vee (p_1 \wedge \neg q_1 \wedge \neg p_2 \wedge \neg q_2)) \vee (\neg p_1 \wedge q_1 \wedge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

K = 2

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

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

Bounded Model Checking with SAT (BMC)



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

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

$$\neg F_k = p_2 \wedge q_2$$

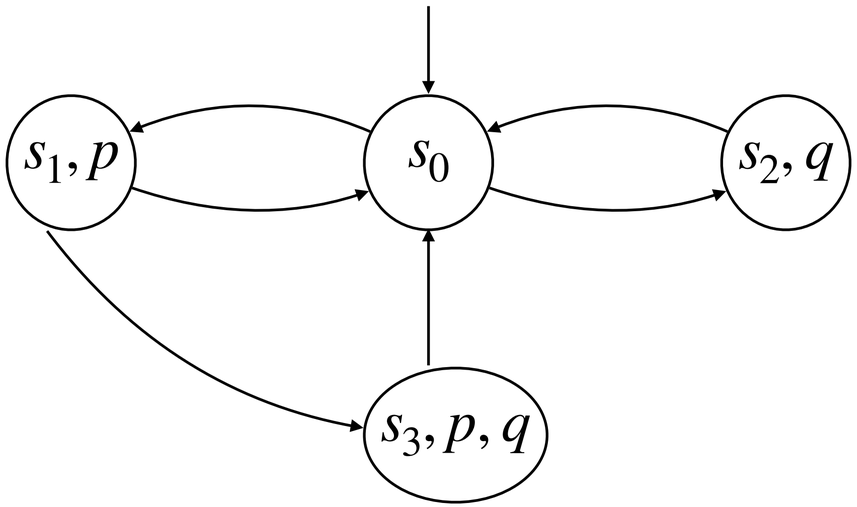
$SAT\{M_k \wedge \neg F_k\}$

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

$M_k \not\models F_k$

s_o, s_1, s_3

Bounded Model Checking with SAT (BMC)



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

K = 1

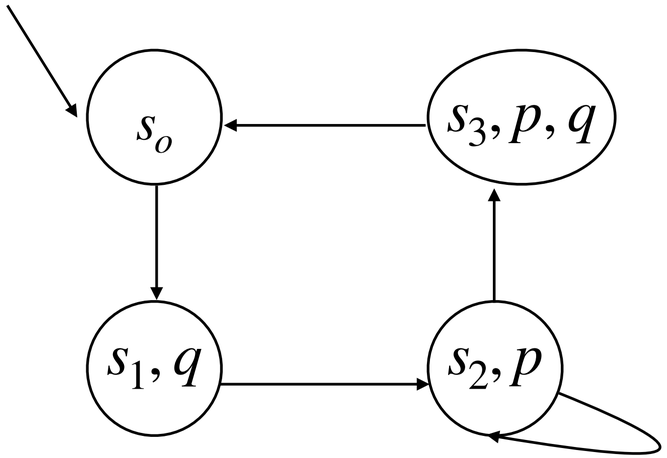
$$M_k = (\neg p_0 \wedge \neg q_0) \wedge ((\neg p_0 \wedge \neg q_0 \wedge p_1 \wedge \neg q_1) \vee (\neg p_0 \wedge \neg q_0 \wedge \neg p_1 \wedge q_1))$$

K = 1

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

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

Bounded Model Checking with SAT (BMC)



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

K = 1

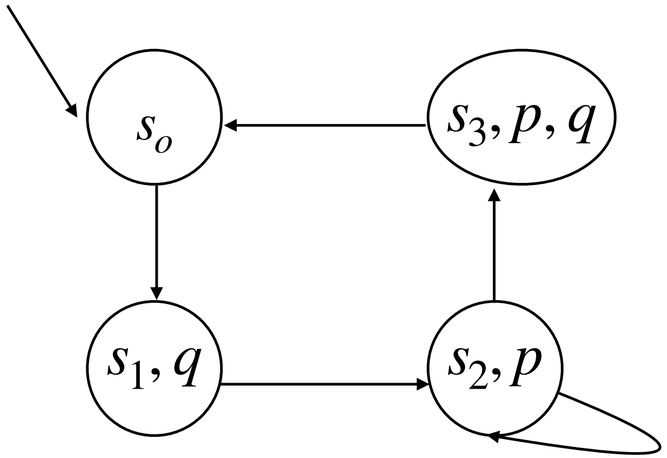
$$M_k = (\neg p_o \wedge \neg q_o) \wedge (\neg p_o \wedge \neg q_o \wedge \neg p_1 \wedge q_1)$$

$$\neg F_k = (\neg p_1 \vee \neg q_1)$$

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

$$\sigma = \langle p_0 = 0, q_0 = 0, p_1 = 0, q_1 = 1 \rangle$$ $M_k \not\models F_k$ s_o, s_1

Bounded Model Checking with SAT (BMC)



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

K = 2

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

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

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

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

$M_k \not\models F_k$ s_o, s_1, 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.

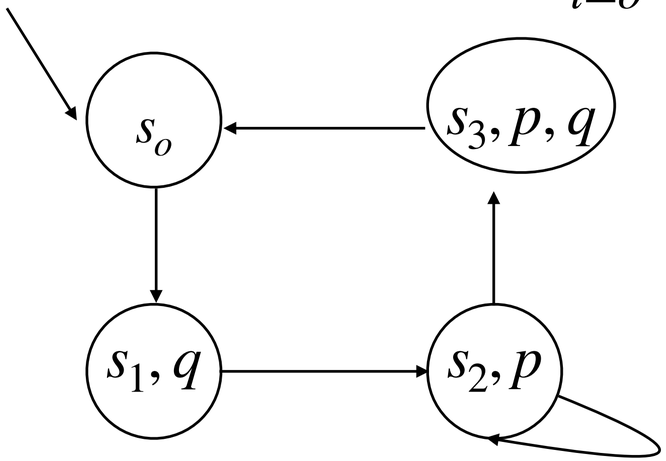
A loop: a back edge that loops from the last state back to some earlier state.

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

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

Bounded Model Checking with SAT (BMC)

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



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

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

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

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.

We should fix the source as initial states.

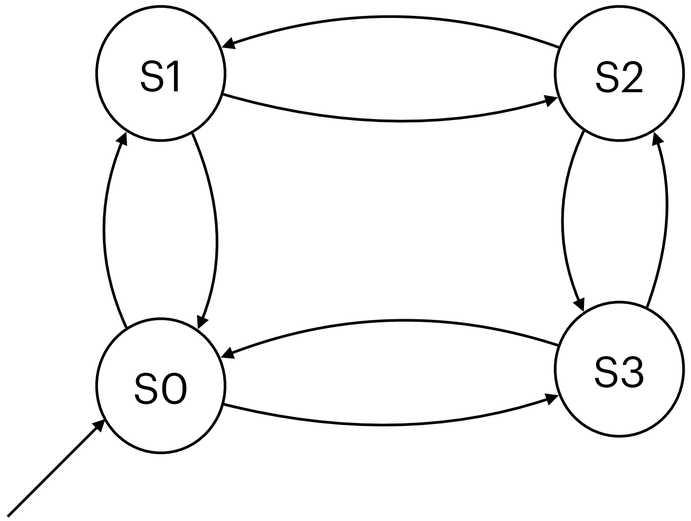
$$\text{Diameter(M)} = \underset{\forall s,s' \in T; s \in I}{Max}\ ShortestPathLength(s, s')$$

Bounded Model Checking with SAT (BMC)

Diameter of M

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

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



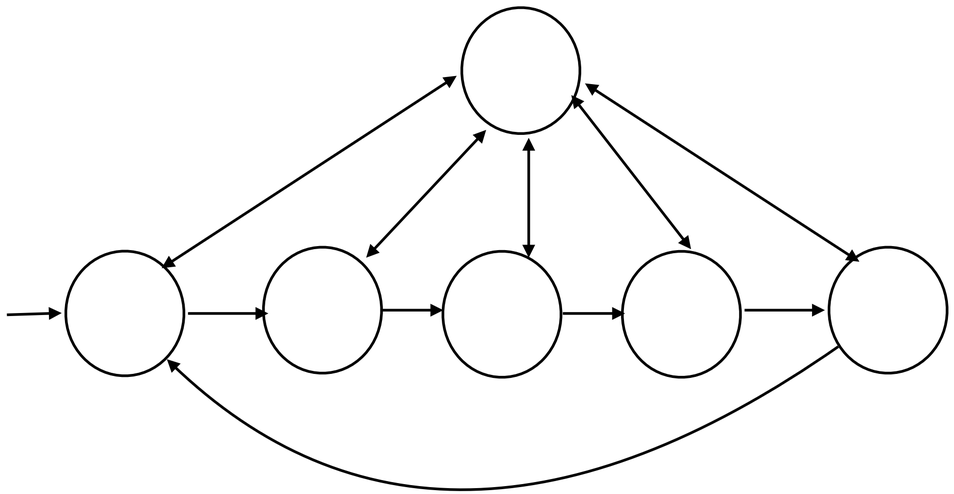
Diameter is 2.

Bounded Model Checking with SAT (BMC)

Diameter of M

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

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



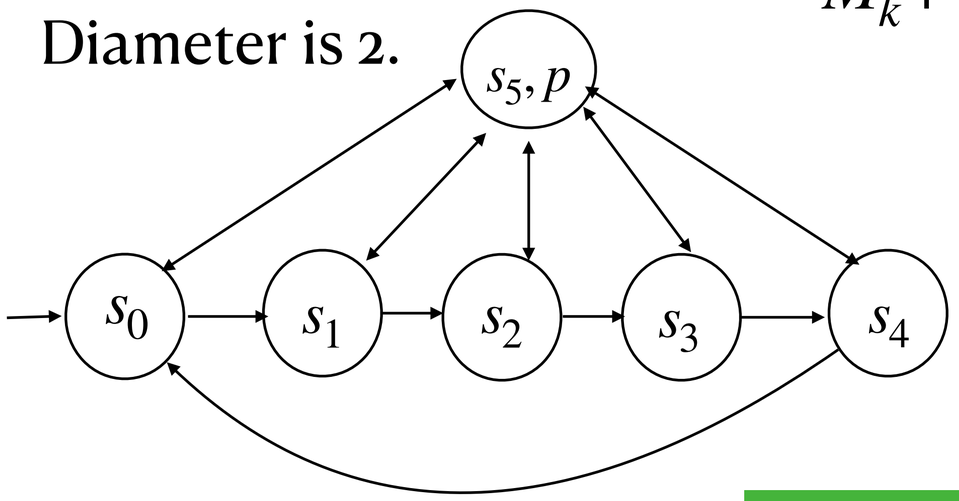
Diameter is 2.

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 $\forall \Diamond p$?

Diameter is 2.



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

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.