# Scalability: Induction, Interpolation, Property Directed Reachability


**PALLAB DASGUPTA**
**FNAE, FASc, FIETE,**
**Professor,**
**Dept of Computer Science & Engineering**
**Indian Institute of Technology Kharagpur**
Email: pallab@cse.iitkgp.ac.in
Web: http://cse.iitkgp.ac.in/~pallab

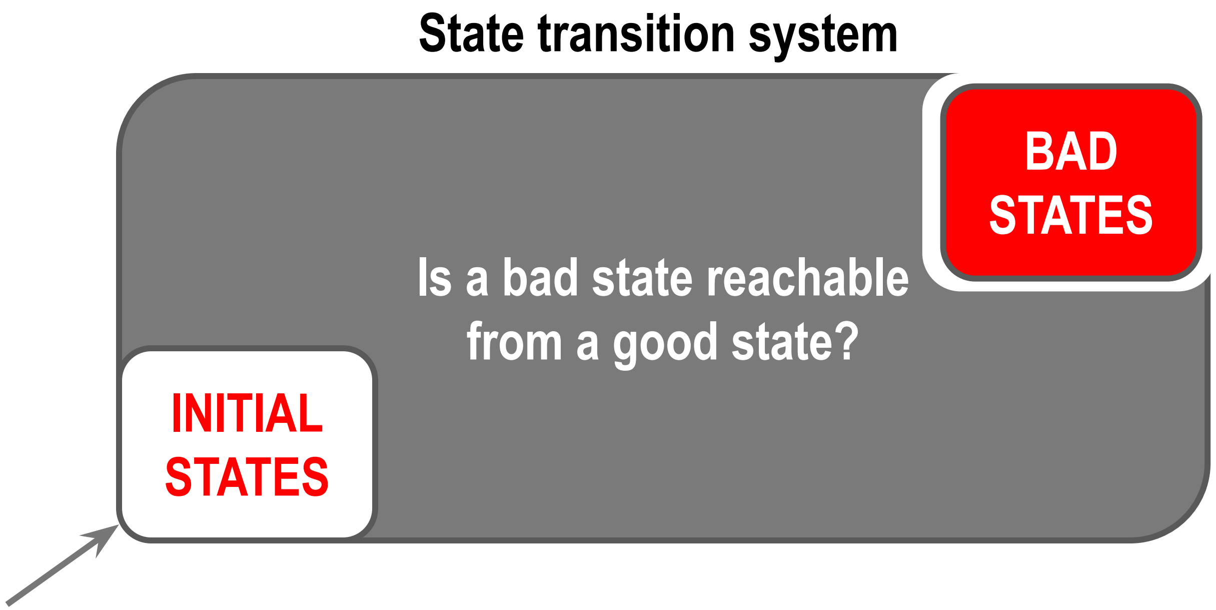


INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

FMSAFE
FORMAL METHODS FOR SAFETY CRITICAL SYSTEMS

# INDUCTION

# The intuitive basis for induction




**Suppose we prove the following:**

- All initial states are good, and
- The transition relation does not allow any transition from a good state to a bad state

**Then inductively, we are safe**

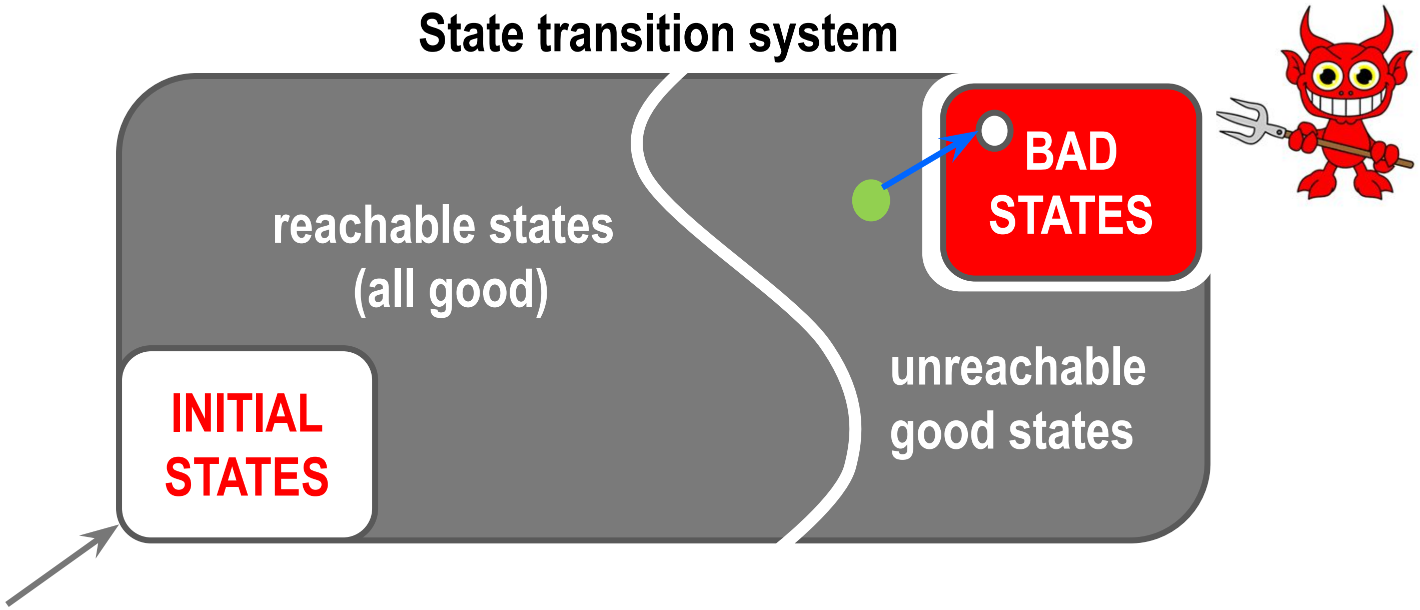
Let $P(x)$ be the formula representing good states, $T(i, x, x')$ represent the transition relation, and $I(x)$ represent the set of initial states.

Then we check:

1. Basis: $I(x) \Rightarrow P(x)$ *all initial states are good*
2. Induction: $P(x) \wedge T(i, x, x') \Rightarrow P(x')$ *successors of good states are good*

Then, by induction, no bad state is reachable.

# Deeper induction




In general the basic induction fails.

- For example, the green state is a good state having a bad successor, but it is not reachable from the initial states. The property holds on all reachable states.
  - Conclusion: The failure of basic induction does not mean that bad states are reachable.

We shall define a deeper form of induction with a depth bound *k.* We shall call it *k*-induction

# *k*-induction

A property $P(x)$ is called a ***k-invariant*** if it overapproximates all states reachable up to *k* steps. That is:

$$\forall 0 \leq N \leq k. \left( (I(x_0) \wedge \bigwedge_{j=0}^{N-1} T(i_j, x_j, x_{j+1}) \right) \Rightarrow P(x_N)$$

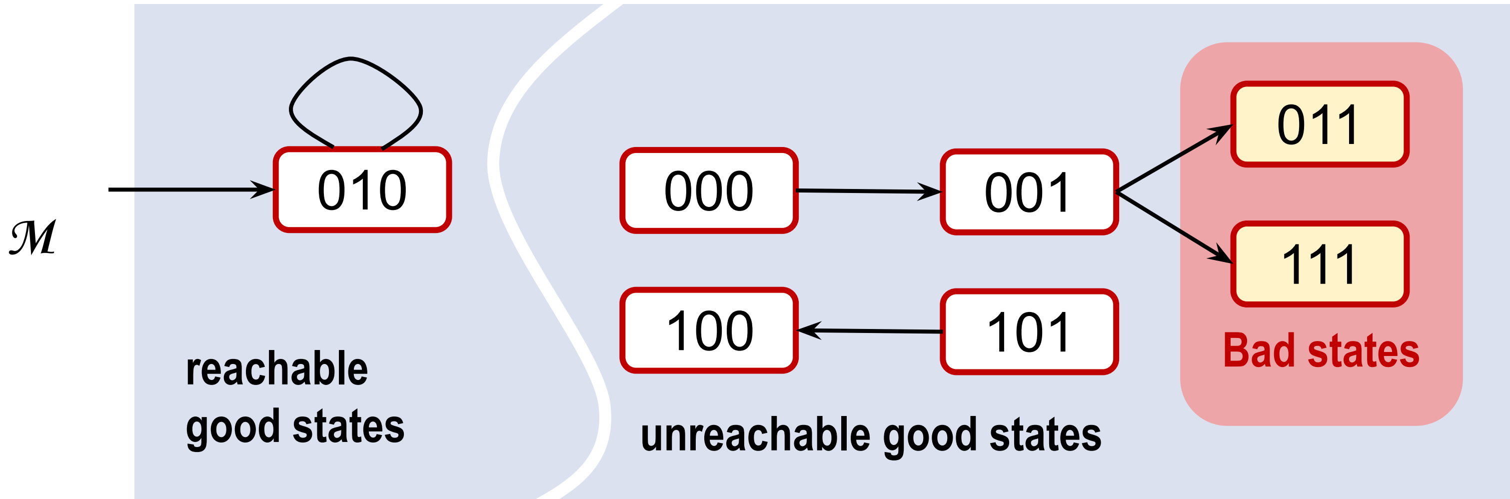
A formula $P(x)$ is called a ***k-inductive invariant*** if it is *k-invariant* and:

$$\left( \bigwedge_{j=0}^{k} P(x_j) \wedge T(i_j, x_j, x_{j+1}) \right) \Rightarrow P(x_{k+1})$$

This means that $P(x)$ is ***k-inductive invariant*** if all states reachable within *k* steps satisfy $P(x)$ and any sequence of *k* states satisfying $P(x)$ guarantees that the $(k+1)^{st}$ state also satisfies $P(x)$

This happens when there are no good state sequences of length more than *k* leading to a bad state

# Example




$P(x) = \neg x_2 \vee \neg x_3$ Therefore Bad = { 011, 111 }

*P* (*x*) is *3*-inductive in $\mathcal{M}$

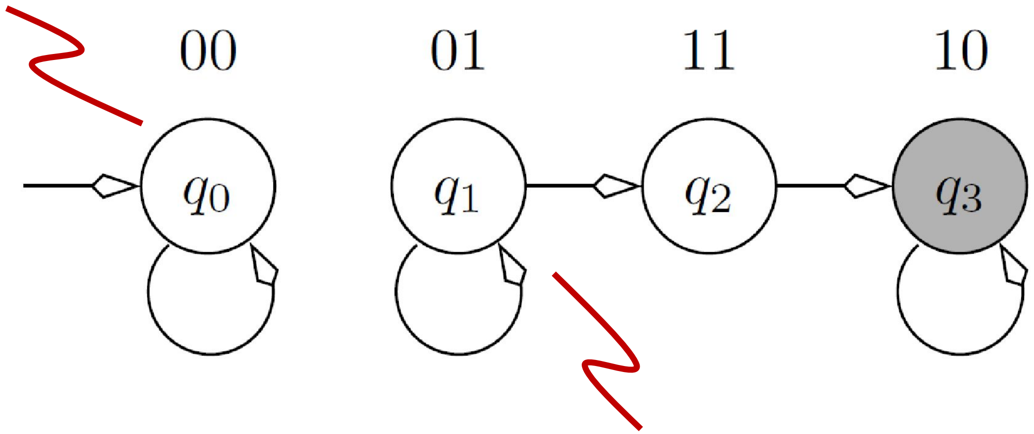
**Why is it not 1-inductive or 2-inductive?**

# *k*-induction is not complete

$$\forall 0 \le N \le k.\left( (I(x_0) \wedge \bigwedge_{j=0}^{N-1} T(i_j, x_j, x_{j+1}) \right) \Rightarrow P(x_N)$$

Here, $P(x) = \neg ( x_1 \wedge \neg x_2 ) = \neg x_1 \vee x_2$
and therefore, Bad = { $q_3$ }

Because of the loop at $q_0$, property $P(x)$ is *k-invariant* for all values of *k*.

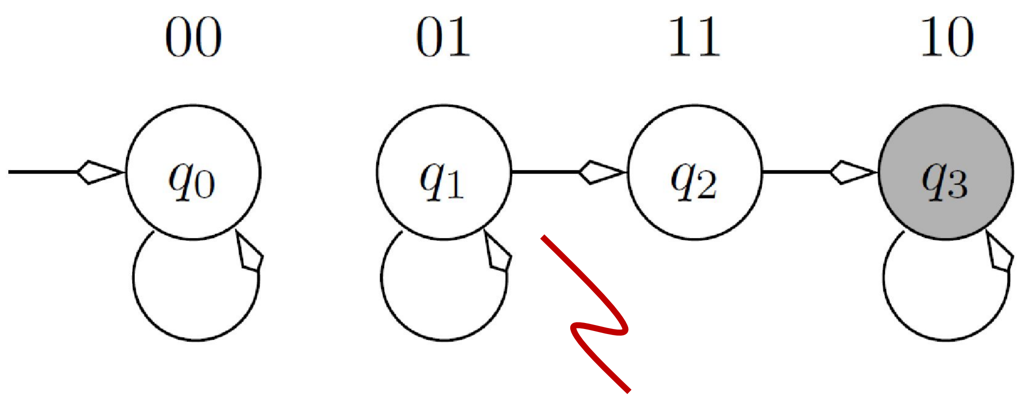



Because of the loop at $q_1$, formula $P(x)$ is not *k-inductive invariant,* even if *k* is arbitrarily large.

$$\left( \bigwedge_{j=0}^{k} P(x_j) \wedge T(i_j, x_j, x_{j+1}) \right) \Rightarrow P(x_{k+1})$$

*In this case k-induction will not converge*

# $k$-induction with loop detection




Here, $P(x) = \neg(x_1 \wedge \neg x_2) = \neg x_1 \vee x_2$ and therefore, Bad = { $q_3$ }

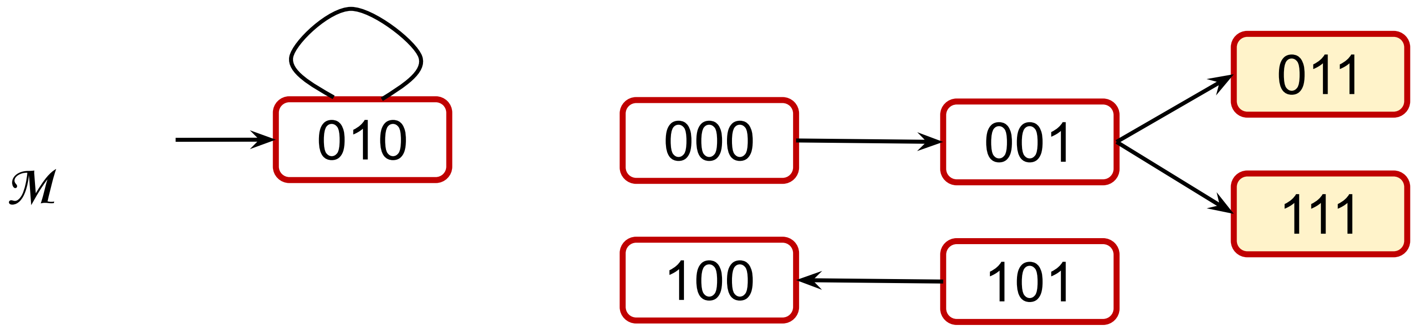
Because of the loop at $q_1$, formula $\phi$ is not *k-inductive invariant,* even if *k* is arbitrarily large.

*k-induction* can be made complete by adding a test for repetition of states.

Thereby, we test whether there are no non-repeating state sequences of length more than k leading to a bad state.

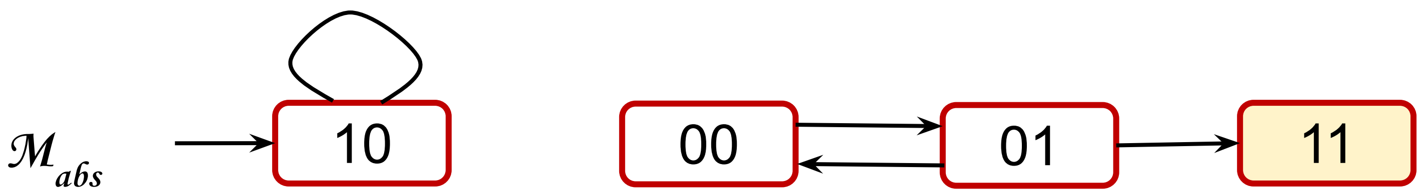
However, if $P(x)$ is *k-inductive* for large *k*, then we have many rounds of unfolding of the transition relation, T

# Abstraction can affect *k*-induction




$P(x) = \neg x_2 \vee \neg x_3$ **Therefore Bad = { 011, 111 }** **P(x) is *3*-inductive in $\mathcal{M}$**

**Suppose we abstract $\mathcal{M}$ by dropping $x_1$**




**$P(x)$ is not *k*-inductive in $\mathcal{M}_{abs}$**

**Can abstraction affect single step induction? No, as long as all variables of $P(x)$ are retained**