COL:750

Foundations of Automatic Verification

Instructor: Priyanka Golia

Course Webpage

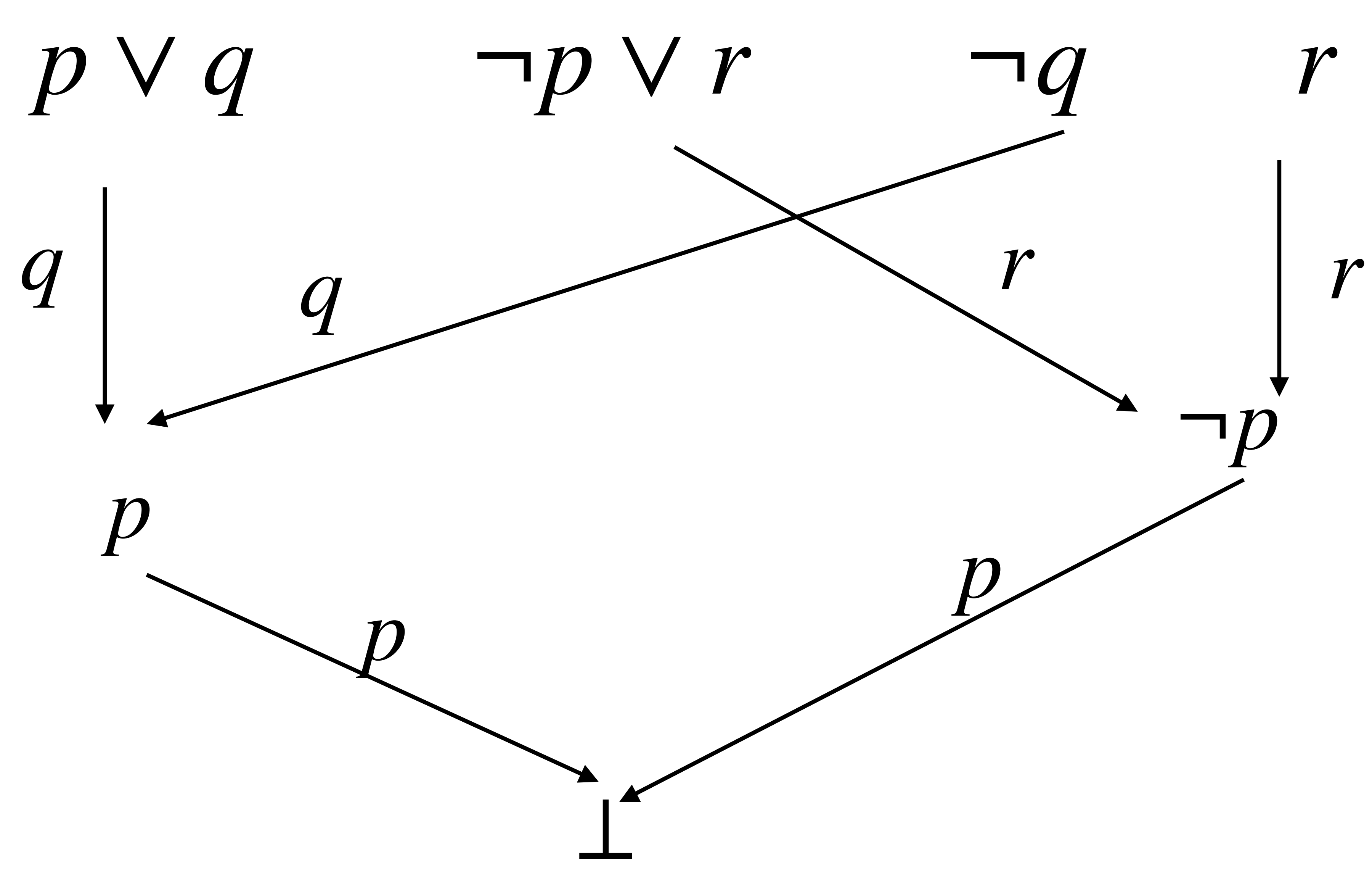
https://priyanka-golia.github.io/teaching/COL-750/index.html

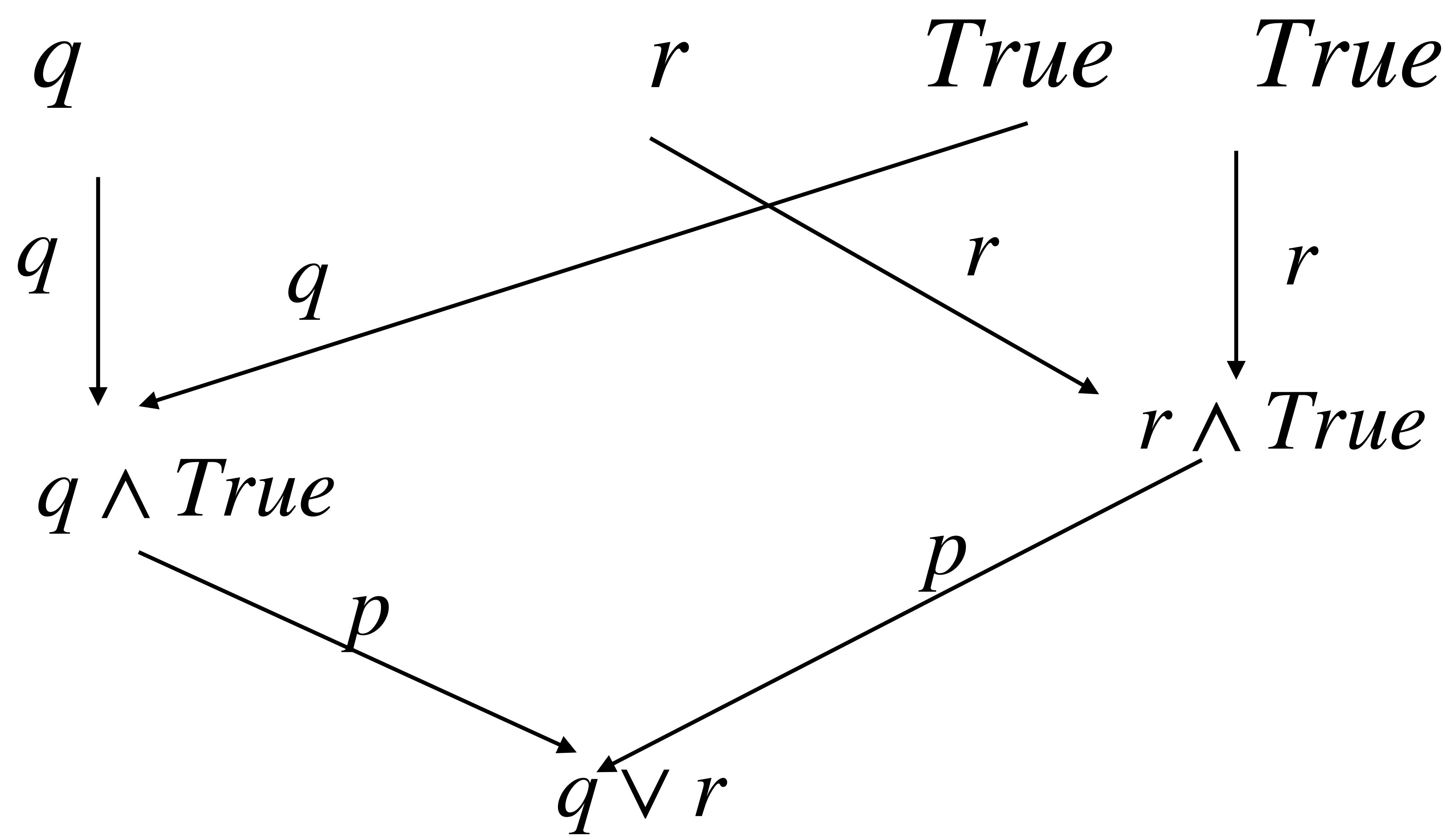
Compute Interpolants

$$A = (p \vee q) \wedge (\neg p \vee r) \qquad B = \neg q \wedge \neg r$$

Compute Interpolants

$$A = (p \vee q) \wedge (\neg p \vee r) \qquad B = \neg q \wedge \neg r$$





Model Checking using Interpolants

Inductive Invariants

Post-image (Q) = $\{s' \mid \exists s \in Q \,.\, T(s, s')\}$

Inductive invariant (I_s) for $\forall \Box p$

1. I_s must include the set of initial states, $I \subseteq I_s$
2. I_s must not include a state that is labeled with $\neg p$, $\forall s \in I_s, s \vDash p$
3. I_s must be closed under transition relation, post-image(I_s) $\subseteq I_s$ holds.

If there exists a inductive invariant for $\forall \Box P$, then $M \vDash \forall \Box p$

Model Checking using Interpolants

Can you use interplants to compute inductive invariants?

Model Checking using Interpolants

Can you use interplants to compute inductive invariants?

1. Constructs an over-approximation of the reachable states
2. Terminates when it finds an inductive invariant or a counterexample

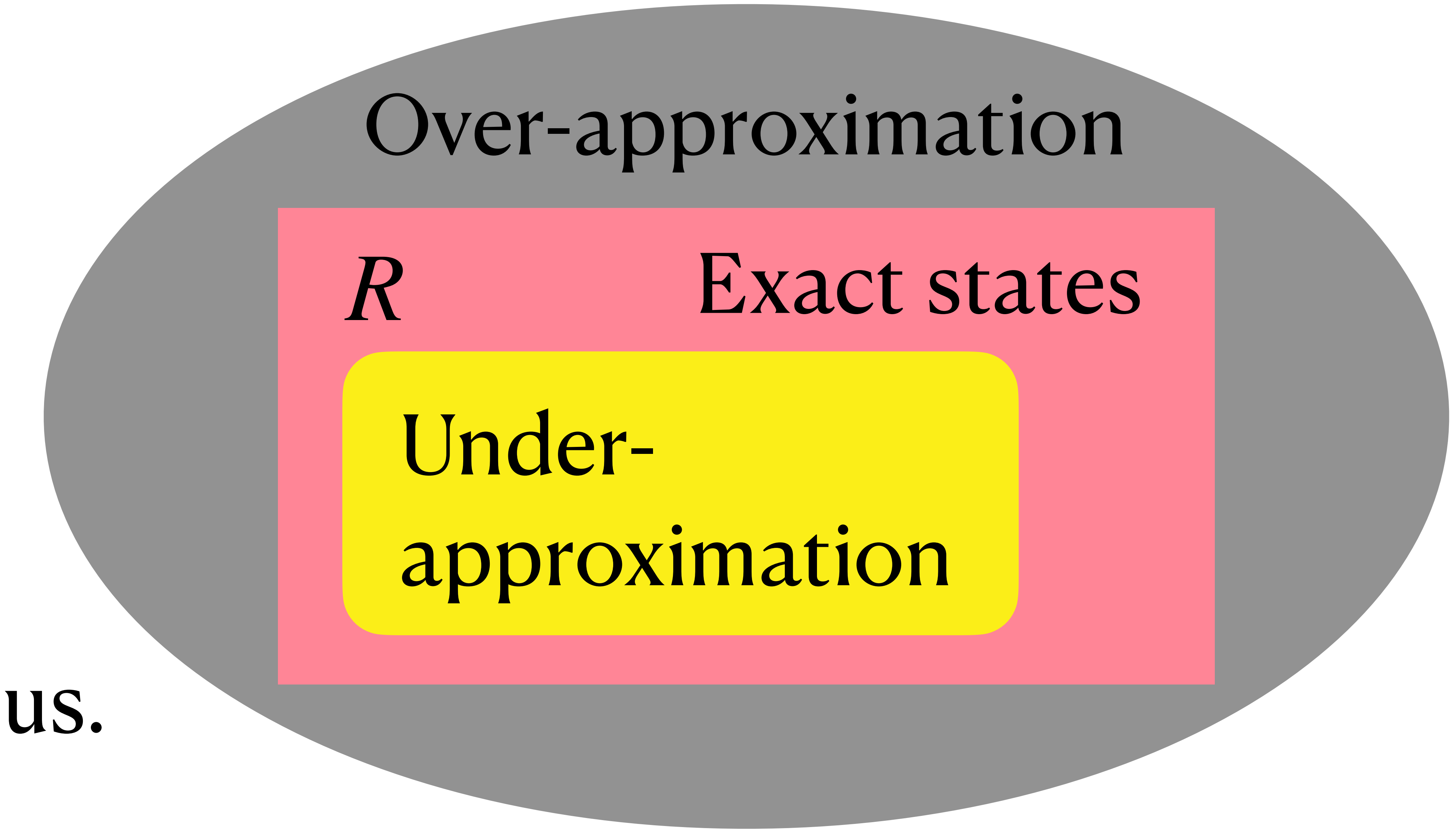
Actual reachable set: R

Over-approximation (O_p): $R \rightarrow O_p$

1. Proofs on over-approximation holds.
2. Counterexample can be spurious.

Under-approximation (U_p): $U_p \rightarrow R$

1. Proofs on over-approximation can be spurious.
2. Counterexample holds



Model Checking using Interpolants

General idea:

1. Perform BMC

2. If BMC is UNSAT:

    Iteratively compute and refine an over-approximation of states reachable in K steps.

3. If BMC is SAT:

    Check if over-approximation is same as initial states

    otherwise increase K.

Model Checking using Interpolants

General idea:

1. Perform BMC

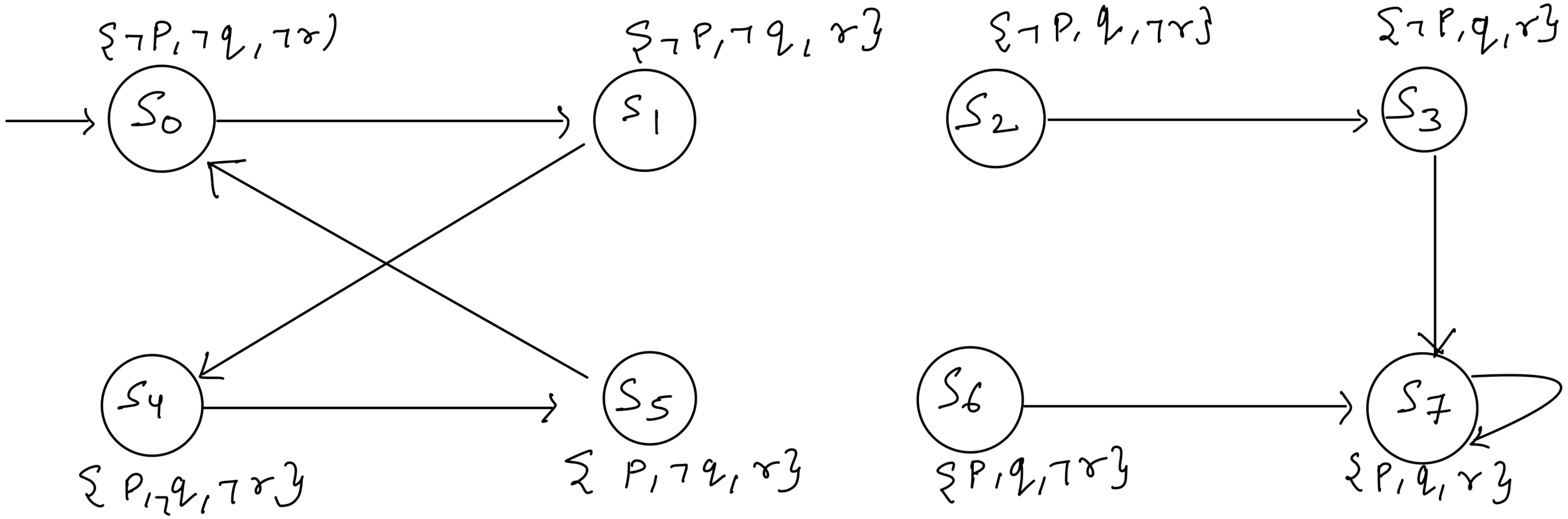
2. If BMC is UNSAT:

    Iteratively compute and refine an over-approximation of states reachable in K steps.

```
Compute Interpolant as over-approximation.
If interpolant is inductive
        Return True.
else
      use  interpolant to over-approximate.
```

3. If BMC is SAT:

    Check if over-approximation is same as initial states
    otherwise increase K.



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg(p \wedge q \wedge r)$.

Only Bad state is S_7

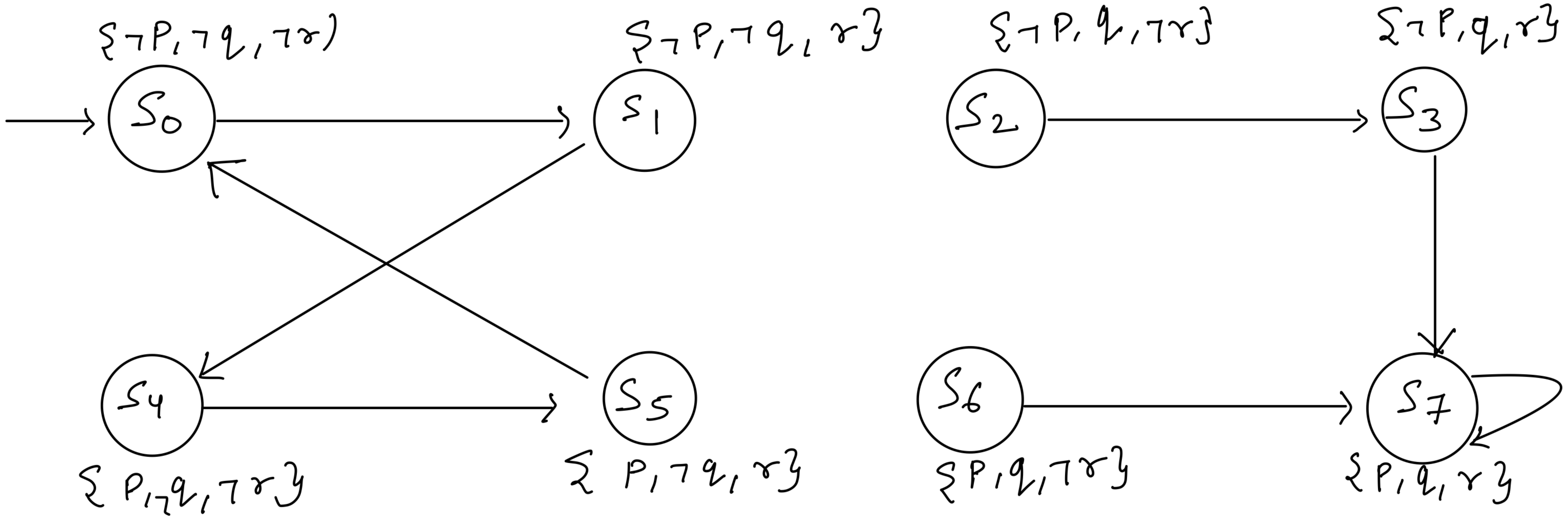
Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

1. Does initial state is a bad state?

$$CheckSAT\{s_o \wedge p_o\}$$

$$(\neg p_o \wedge \neg q_o \wedge \neg r_o) \wedge (p_o \wedge q_o \wedge r_o)$$

UNSAT — good to go!



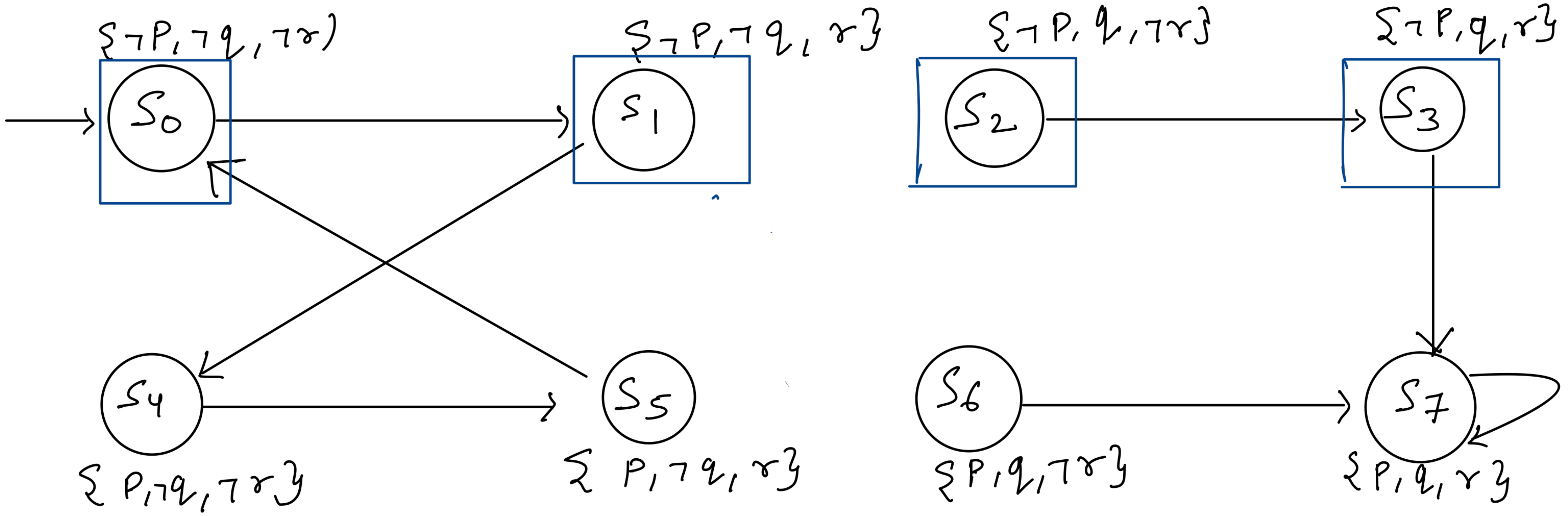
Let us consider the above example: Look carefully at the labelling function.

$F = \forall \square \neg(p \wedge q \wedge r).$ Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$\underbrace{Q(s_o) \wedge T(s_o, s_1)}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B} \qquad Q = \{s_o\} \quad \mathrm{K} = 1$$

$$\underbrace{(\neg p_o \wedge \neg q_o \wedge \neg r_o) \wedge (\neg p_1 \wedge \neg q_1 \wedge r_1)}_{A} \wedge \underbrace{(p_1 \wedge q_1 \wedge r_1)}_{B} \qquad \text{UNSAT}$$



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg(p \wedge q \wedge r).$ Only Bad state is S_7

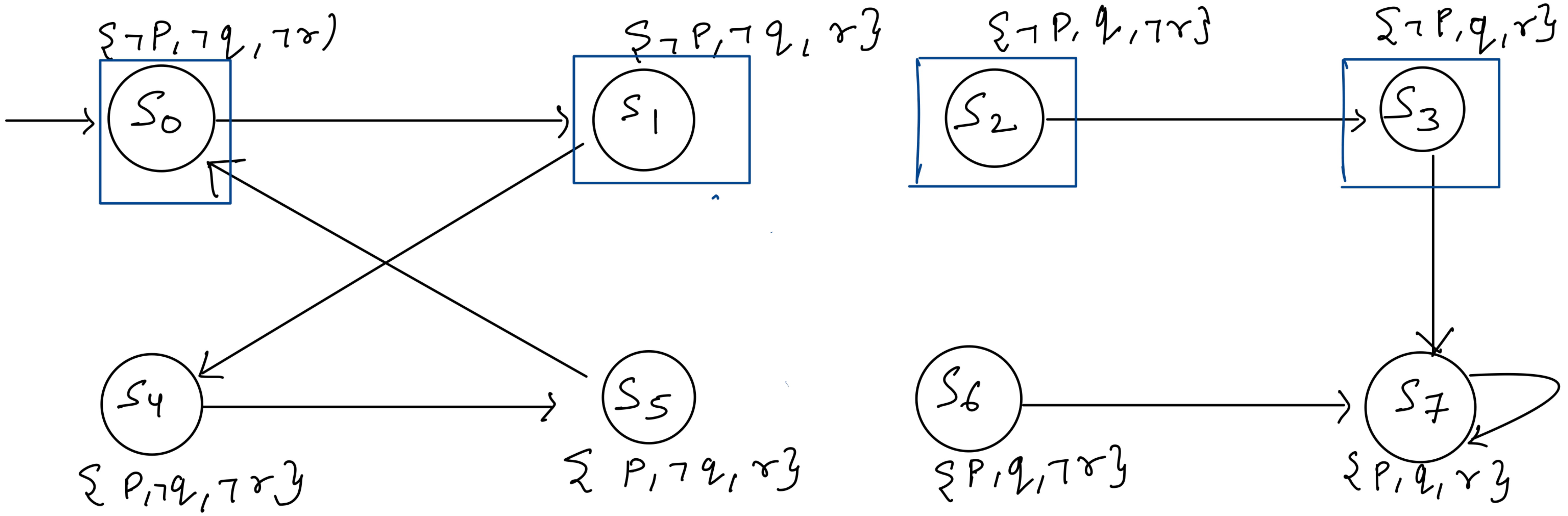
Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$\underbrace{(\neg p_o \wedge \neg q_o \wedge \neg r_o) \wedge (\neg p_1 \wedge \neg q_1 \wedge r_1)}_{A} \quad \wedge \underbrace{(p_1 \wedge q_1 \wedge r_1)}_{B} \qquad \text{UNSAT}$$

Interpolant := $\neg p_1$

$I_S = \{s_o, s_1, s_2, s_3\}$ $I_s : \{s \mid I \in L(s)\}$ $Q = Q \cup I_s$

Check the reachability with Over-approximate set



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg (p \wedge q \wedge r).$

Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$\underbrace{(\neg p_o \wedge \neg q_o \wedge \neg r_o) \wedge (\neg p_1 \wedge \neg q_1 \wedge r_1)}_{A} \quad \underbrace{\wedge (p_1 \wedge q_1 \wedge r_1)}_{B} \qquad \text{UNSAT}$$

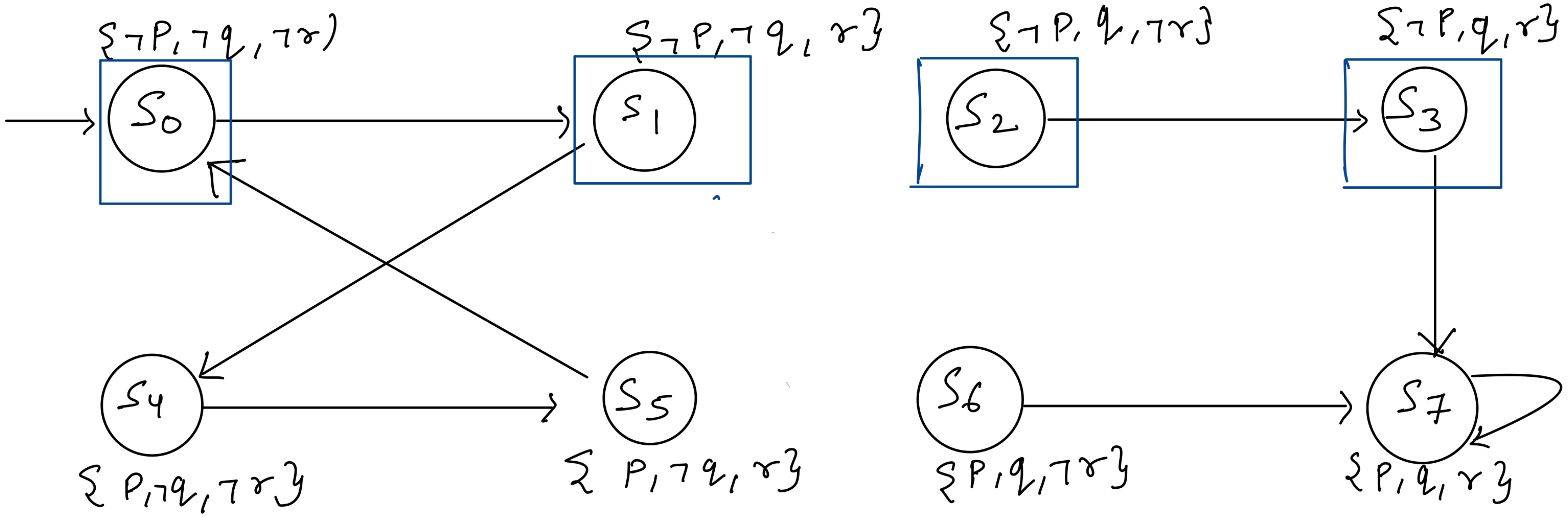
Interpolant := $\neg p_1$

$I_S = \{s_o, s_1, s_2, s_3\}$

$I_s : \{s \mid I \in L(s)\}$

$Q = Q \cup I_s$

Check the reachability with Over-approximate set



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \square \neg (p \wedge q \wedge r).$

Only Bad state is S_7

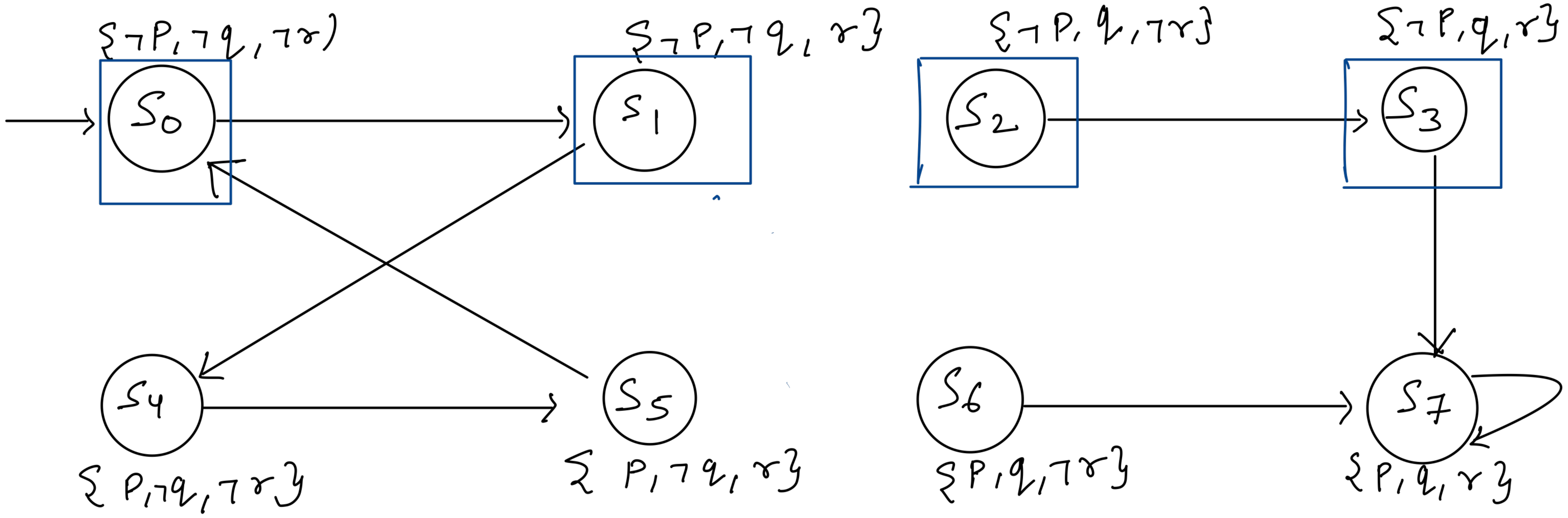
Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$Q = Q \cup I_s$

Check the reachability with Over-approximate set

$Q = \{s_o, s_1, s_2, s_3\}$

Is Q an inductive invariant ? No! post-image$(s_1) \notin Q$



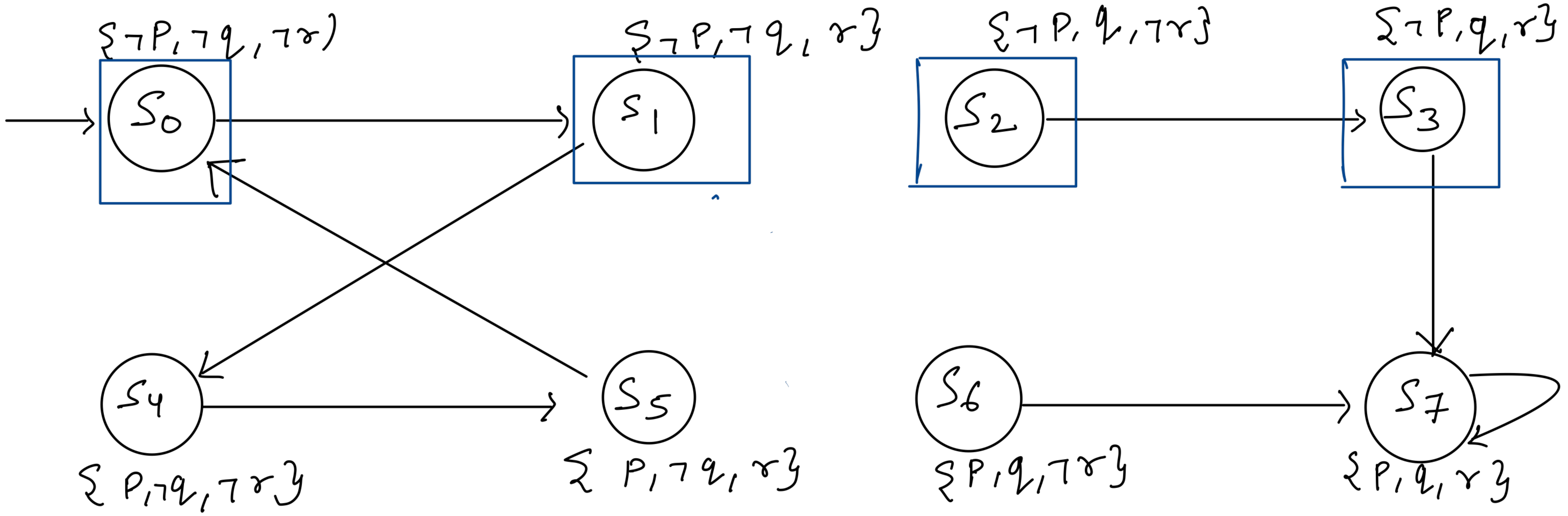
Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg(p \wedge q \wedge r).$ Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$Q = \{s_o, s_1, s_2, s_3\}$

$$\underbrace{Q(s_o) \wedge T(s_o, s_1)}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B}$$



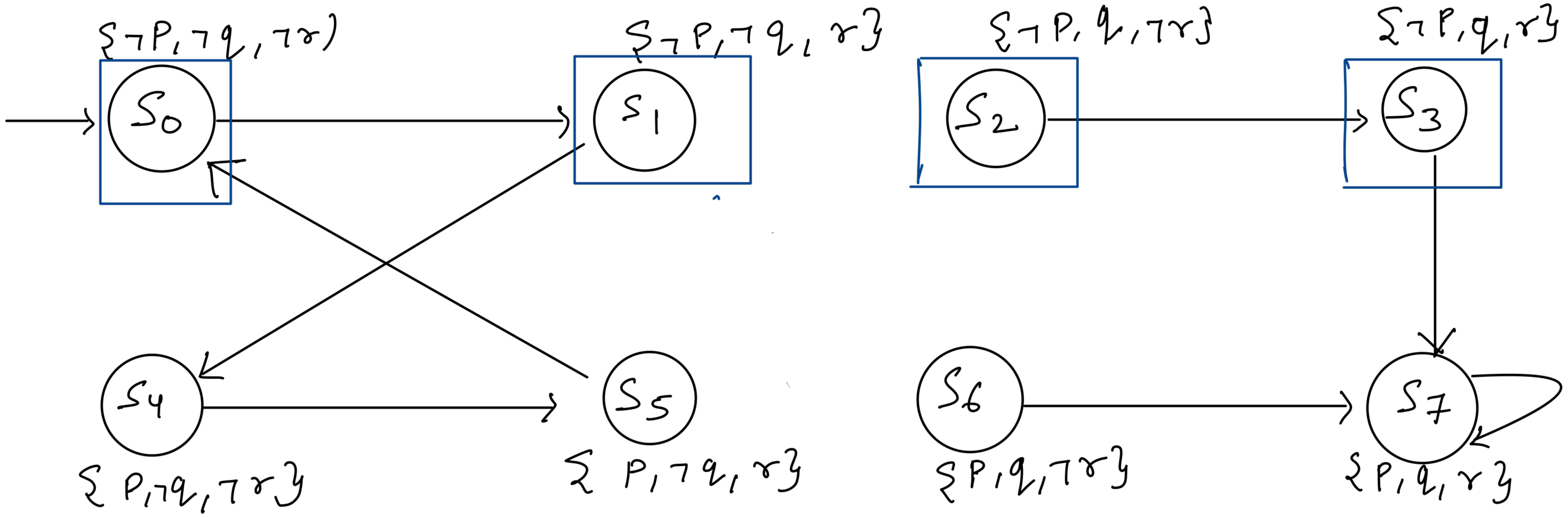
Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg(p \wedge q \wedge r)$.

Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$Q = \{s_o, s_1, s_2, s_3\} \quad \bigvee_{\forall s \in Q} \underbrace{\{Q(s_o) \wedge T(s_o, s_1)\}}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B}$$



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \square \neg (p \wedge q \wedge r)$. Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$Q = \{s_o, s_1, s_2, s_3\}$

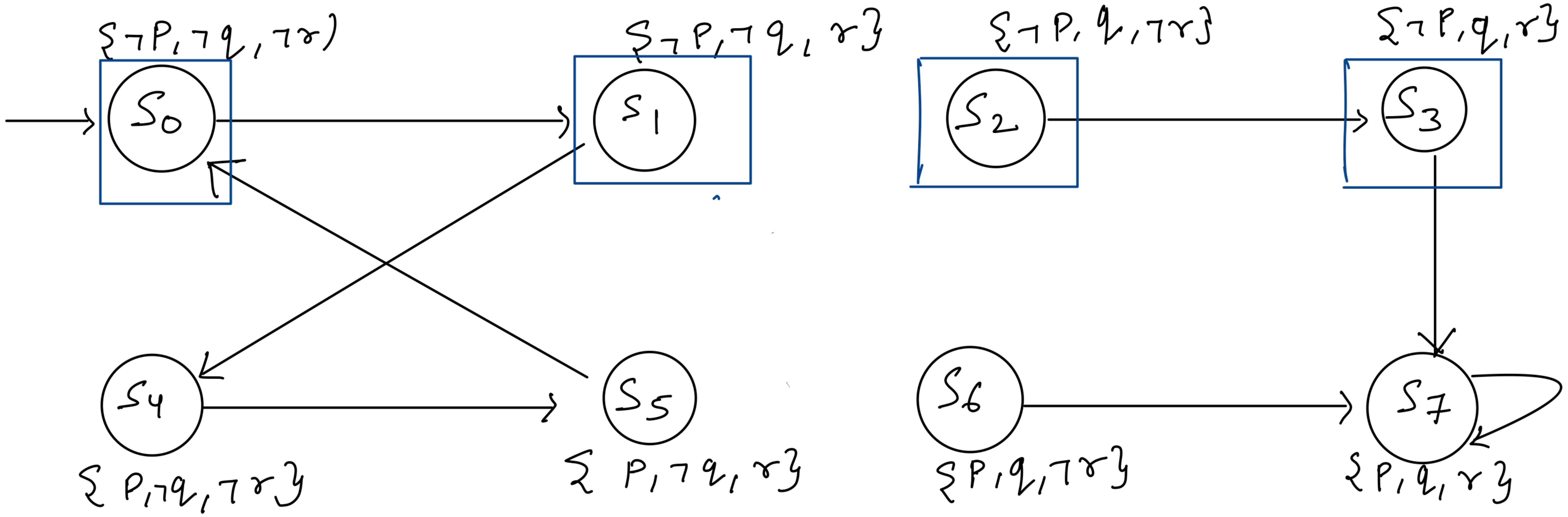
$$\bigvee_{\forall s \in O} \underbrace{\{Q(s_o) \wedge T(s_o, s_1)\}}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B}$$

K = 1

$A = [(\neg p_o \wedge \neg q_o \wedge \neg r_o) \wedge (\neg p_1 \wedge \neg q_1 \wedge r_1)] \vee [(\neg p_o \wedge \neg q_o \wedge r_o) \wedge (p_1 \wedge \neg q_1 \wedge \neg r_1)] \vee [(\neg p_o \wedge q_o \wedge \neg r_o) \wedge (\neg p_1 \wedge q_1 \wedge r_1)] \vee [(\neg p_o \wedge q_o \wedge r_o) \wedge (p_1 \wedge q_1 \wedge r_1)]$

$B = (p_1 \wedge q_1 \wedge r_1)$

$A \wedge B$ is SAT.



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg(p \wedge q \wedge r)$. Only Bad state is S_7

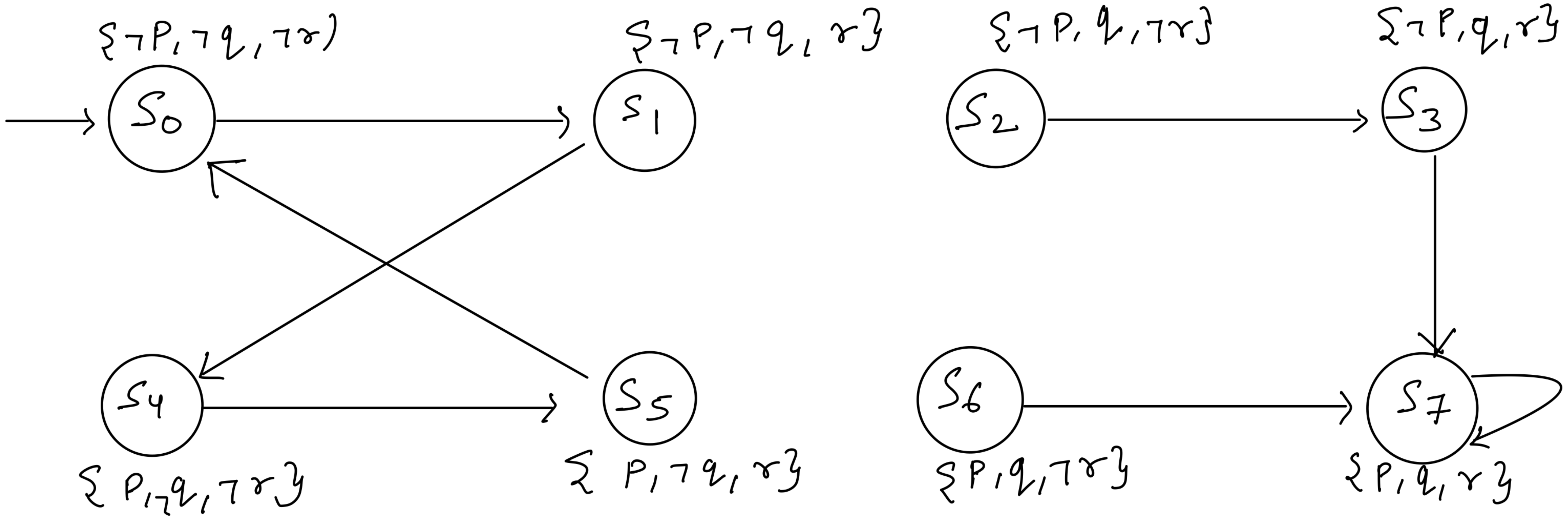
Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$Q = \{s_o, s_1, s_2, s_3\}$

$$\bigvee_{\forall s \in O} \underbrace{\{Q(s_o) \wedge T(s_o, s_1)\}}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B}$$

K = 1

If $A \wedge B$ is SAT, check if $Q = I$ Q = I, then Return counter-example.
Else, increase k to build trust!



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \square \neg (p \wedge q \wedge r)$.

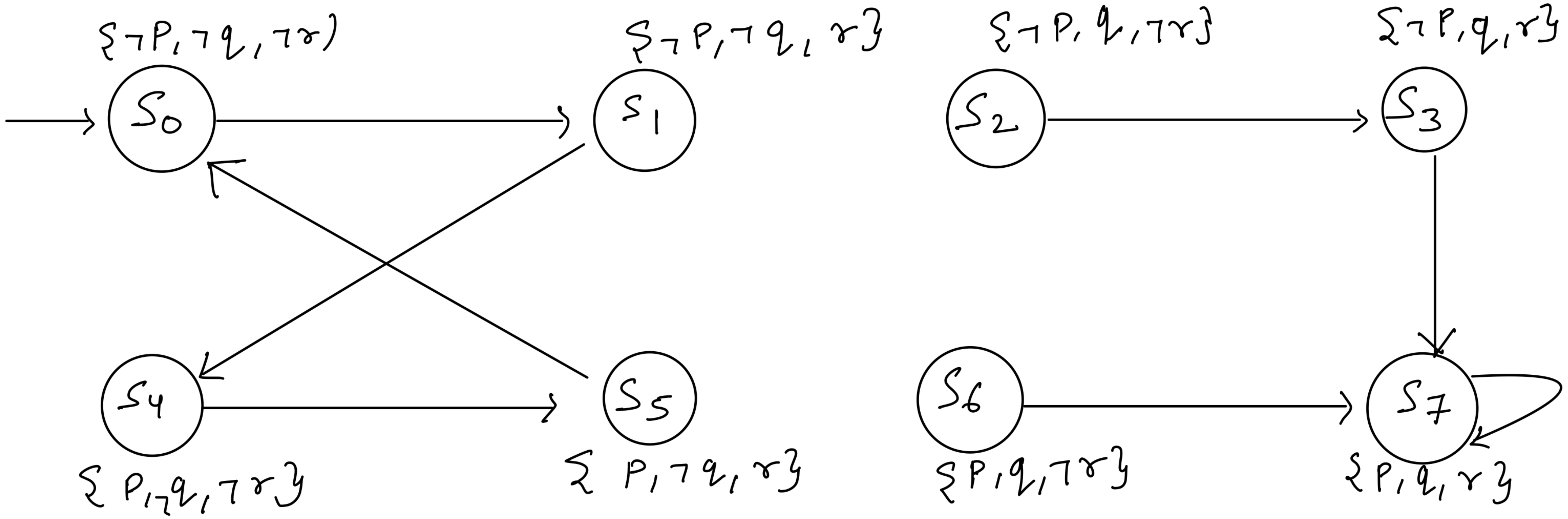
Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$\underbrace{Q(s_o) \wedge T(s_o, s_1)}_{\text{A}} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{\text{B}} \qquad Q = \{s_o\} \quad \text{K} = 2$$

$$\underbrace{(\neg p_o \wedge \neg q_o \wedge \neg r_o) \wedge (\neg p_1 \wedge \neg q_1 \wedge r_1)}_{\text{A}} \quad \underbrace{\wedge (\neg p_1 \wedge \neg q_1 \wedge r_1 \wedge p_2 \wedge \neg q_2 \wedge \neg r_2) \wedge [(p_1 \wedge q_1 \wedge r_1) \vee (p_2 \wedge q_2 \wedge r_2)]}_{\text{B}}$$

UNSAT



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \Box \neg (p \wedge q \wedge r).$

Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$\underbrace{Q(s_o) \wedge T(s_o, s_1)}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B}$$

$Q = \{s_o\}$ K = 2

UNSAT

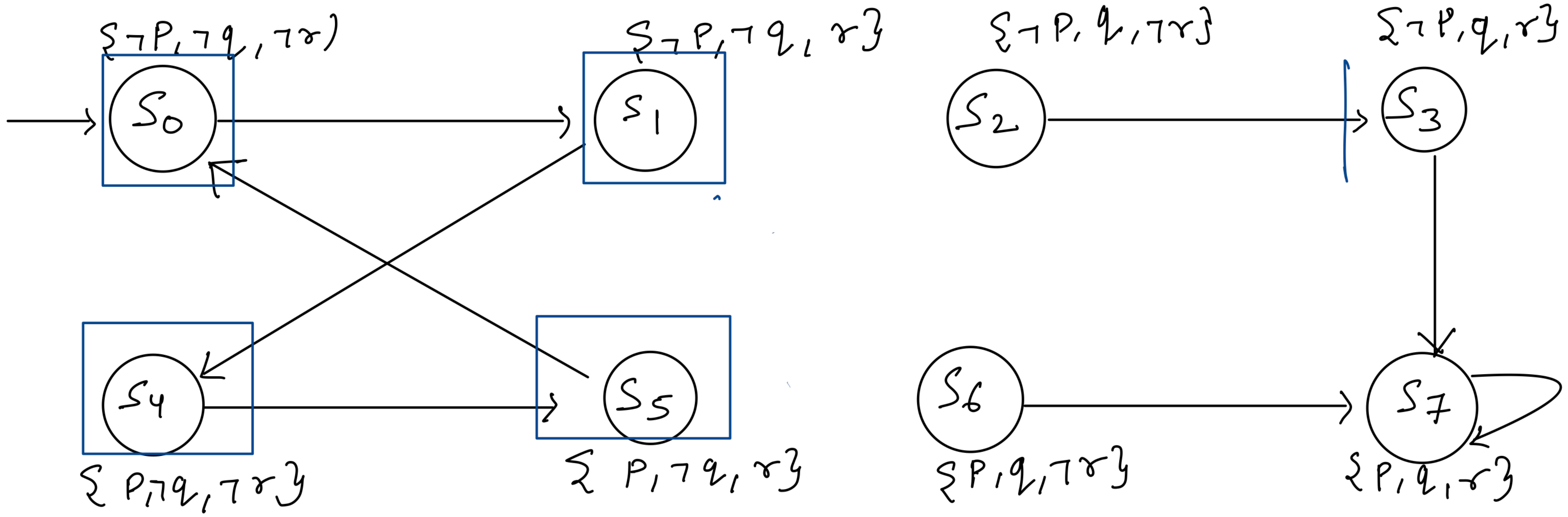
Interpolant := $\neg q_1$

$I_s : \{s \mid I \in L(s)\}$

$Q = Q \cup I_s$

Check the reachability with Over-approximate set

$I_S = \{s_o, s_1, s_4, s_5\}$



Let us consider the above example: Look carefully at the labelling function.

$F = \forall \square \neg (p \wedge q \wedge r)$.

Only Bad state is S_7

Reachability analysis — can we reach to state where $p \wedge q \wedge r$ holds initial states?

$$\underbrace{Q(s_o) \wedge T(s_o, s_1)}_{A} \wedge \underbrace{\bigwedge_{i=1}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} p(s_i)}_{B}$$

$Q = \{s_o\}$ K = 2

UNSAT

Interpolant := $\neg q_1$

$I_S = \{s_o, s_1, s_4, s_5\}$

$I_s : \{s \mid I \in L(s)\}$

$Q = Q \cup I_s$

Q is inductive invariant!!!

$M \vDash F$

Model Checking using Interpolants

General idea:

1. Perform BMC

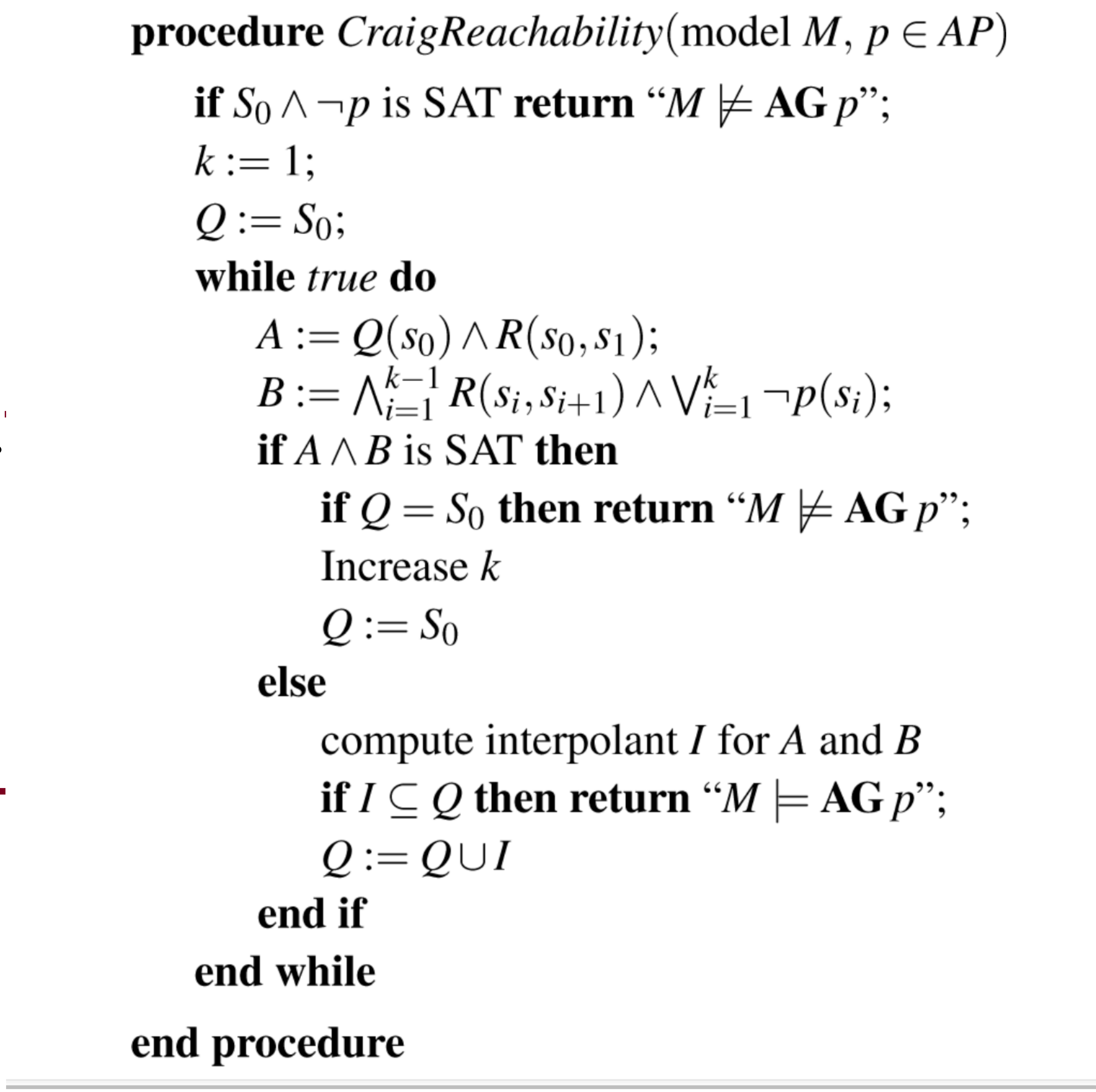
2. If BMC is UNSAT:

    Iteratively compute and refine an over-approximation of states reachable in K steps.

    Compute Interpolant as over-approximation.
    If interpolant is inductive
        Return True.
    else
        use interpolant to over-approximate.

3. If BMC is SAT:

    Check if over-approximation is same as initial states
    otherwise increase K.



```
procedure $CraigReachability$(model $M$, $p \in AP$)
    if $S_0 \wedge \neg p$ is SAT return "$M \not\models \mathbf{AG}\, p$";
    $k := 1$;
    $Q := S_0$;
    while $true$ do
        $A := Q(s_0) \wedge R(s_0, s_1)$;
        $B := \bigwedge_{i=1}^{k-1} R(s_i, s_{i+1}) \wedge \bigvee_{i=1}^{k} \neg p(s_i)$;
        if $A \wedge B$ is SAT then
            if $Q = S_0$ then return "$M \not\models \mathbf{AG}\, p$";
            Increase $k$
            $Q := S_0$
        else
            compute interpolant $I$ for $A$ and $B$
            if $I \subseteq Q$ then return "$M \models \mathbf{AG}\, p$";
            $Q := Q \cup I$
        end if
    end while
end procedure
```