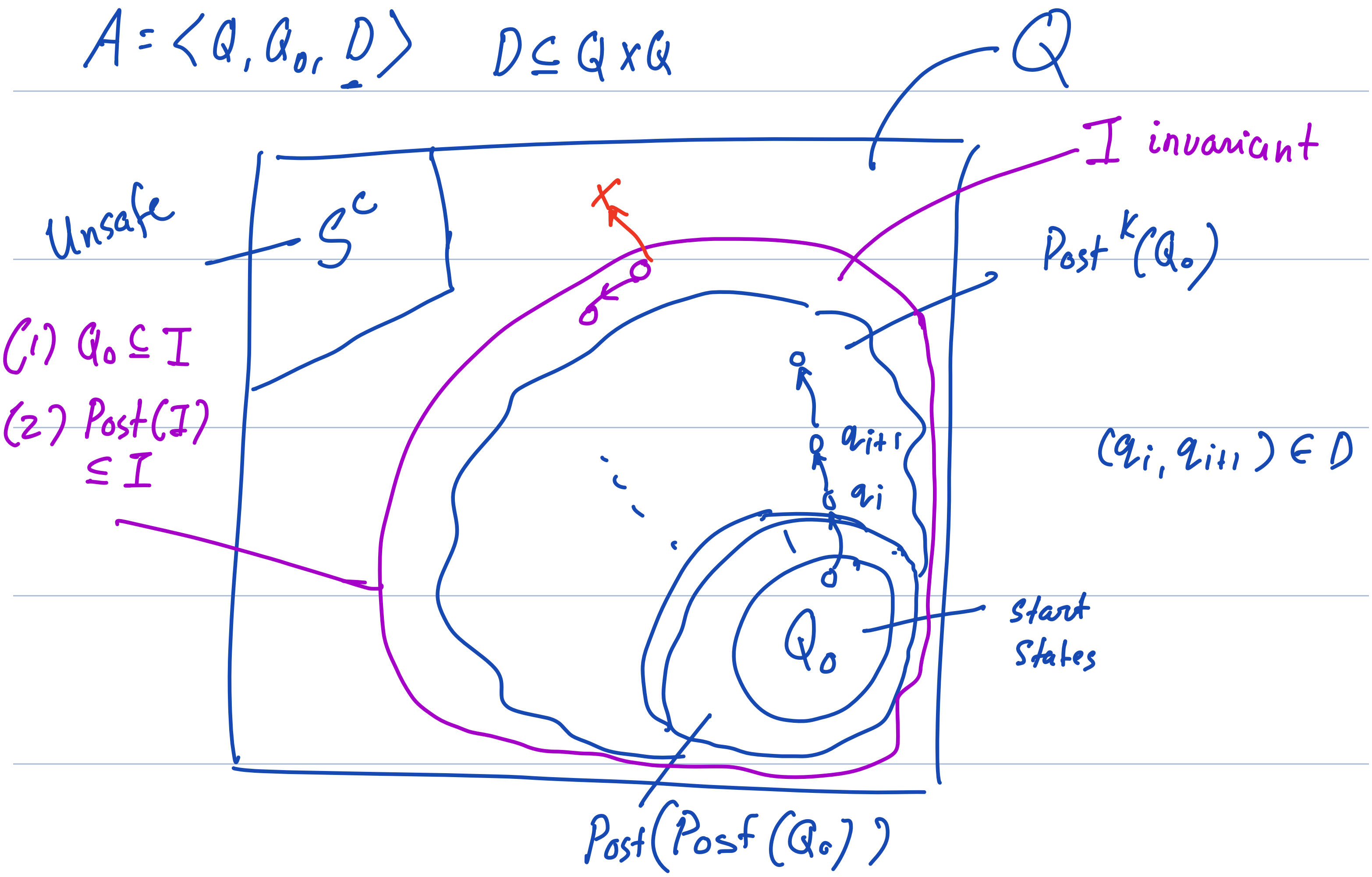
# Lecture 3 : System-level Safety

$A = \langle Q, Q_0, D \rangle$ $D \subseteq Q \times Q$

(1) $Q_0 \subseteq I$

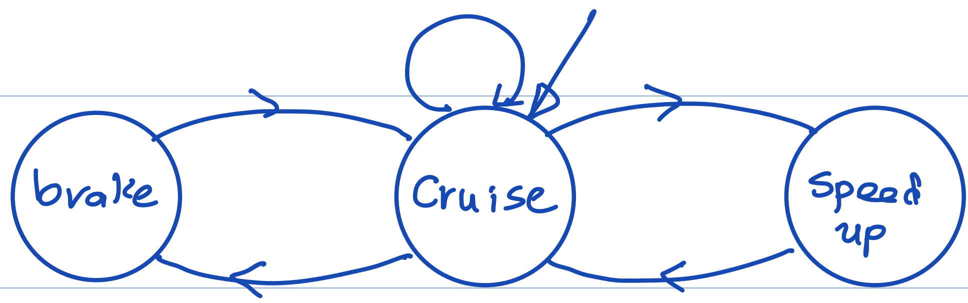
(2) $Post(I) \subseteq I$



**Def.** A <u>state machine</u> or <u>automaton</u> $A$ is defined by

(1) a set of <u>states</u> $Q$
(2) a set of <u>start states</u> $Q_0 \subseteq Q$
(3) a set of <u>transitions</u> $D \subseteq Q \times Q$
<u>transition relation</u>

<u>Example</u>.




$Q = \{C, B, S\}$ $\quad Q_0 = \{C\}$
$D = \{\langle B,C\rangle, \langle C,B\rangle, \langle C,C\rangle, \langle C,S\rangle, \langle S,C\rangle\}$

<u>Nondeterministic</u>.

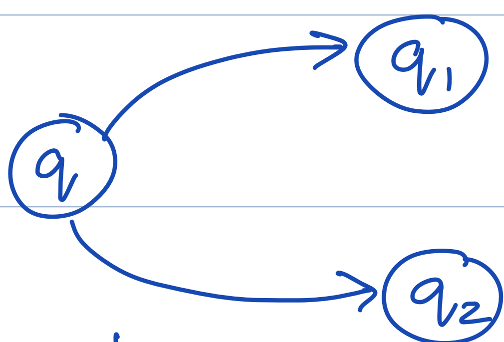
- From the same state $A$ can go to different states
- Useful for modeling uncertainty e.g. action of human driver or environment.

Aside. If we add probabilities to transitions then we get a Markov Chain (MC).

$D : Q \to \mathcal{P}(Q)$

We can have both nondeterminism & probabilistic uncertainty
$\longrightarrow$ Markov Decision Processes

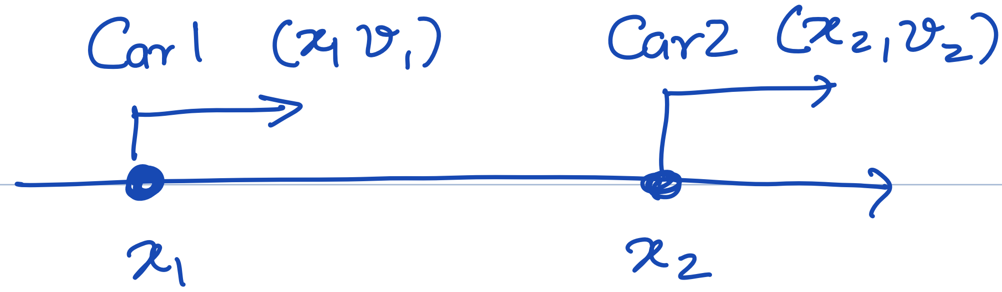
Deterministic automaton $|Q_0| = 1$ and
$\forall q \in Q,\ q_1, q_2 \in Q$ if $\langle q, q_1 \rangle \in D$
and $\langle q, q_2 \rangle \in D$ then $q_1 = q_2$




X not allowed

For deterministic automata
$D : Q \to Q$ is a transition function.

# Example 2




$Q = \mathbb{R}^4$

$Q_0 = \{ x_{10}, v_{10}, x_{20}, v_{20} \}$ $\quad$ $x_{20} > x_{10} > 0$

$v_{10}, v_{20} \geq 0$

$D \subseteq \mathbb{R}^4 \times \mathbb{R}^4$

Often $D$ will be described by a program or a physics model (differential equations)

If $x_2 - x_1 < d_s$

$\quad v_1 := \max(0, v_1 - a_b)$

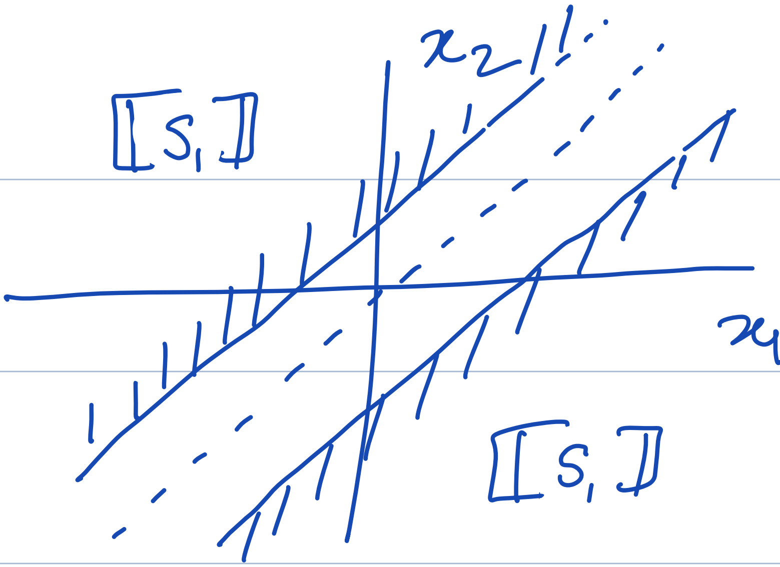
else $\quad v_1 := v_1$

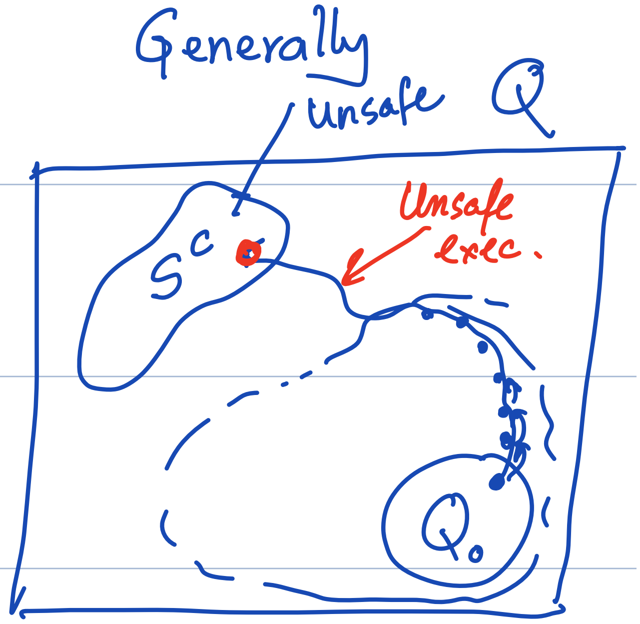
$x_1 := x_1 + v_1$

$x_2 := x_2 + v_2$

Do you see how this defines $D$?

Is it deterministic ?



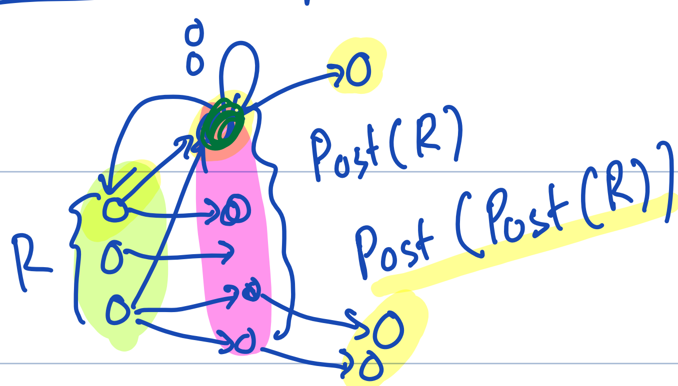

## Safety Verification Problem

Does there exist any execution $\alpha = q_0 \cdots q_k$ of $A$ such that $q_k \notin S^c$?

Such an execution is called a counter-example

**Def.**

If for every finite execution $\alpha = q_0 \cdots q_k$ of $\mathcal{A}$ and for every $q_i$ in $\alpha$, $q_i \in S$ then we say <u>$\mathcal{A}$ is safe</u> w.r.t. $S$.



# Reasoning about all executions

**Def.** For any set of states $R \subseteq Q$

$Post(R) := \{ q' \in Q \mid \exists q \in R \text{ and } \langle q, q' \rangle \in D \}$

**Exercise** The $Post()$ operator is monotonic

if $R_1 \subseteq R_2$ then $Post(R_1) \subseteq Post(R_2)$

**Proof.** Choose any $R_1 \subseteq R_2 \subseteq Q$

Choose any $x \in Post(R_1)$

[we have to show $x \in Post(R_2)$ ]

By def of Post $\exists x_0 \in R_1 \quad \langle x_0, x \rangle \in D$

Since $R_1 \subseteq R_2 \Rightarrow x_0 \in R_2$

$\Rightarrow x \in Post(R_2)$ ∎

We can apply Post recursively.

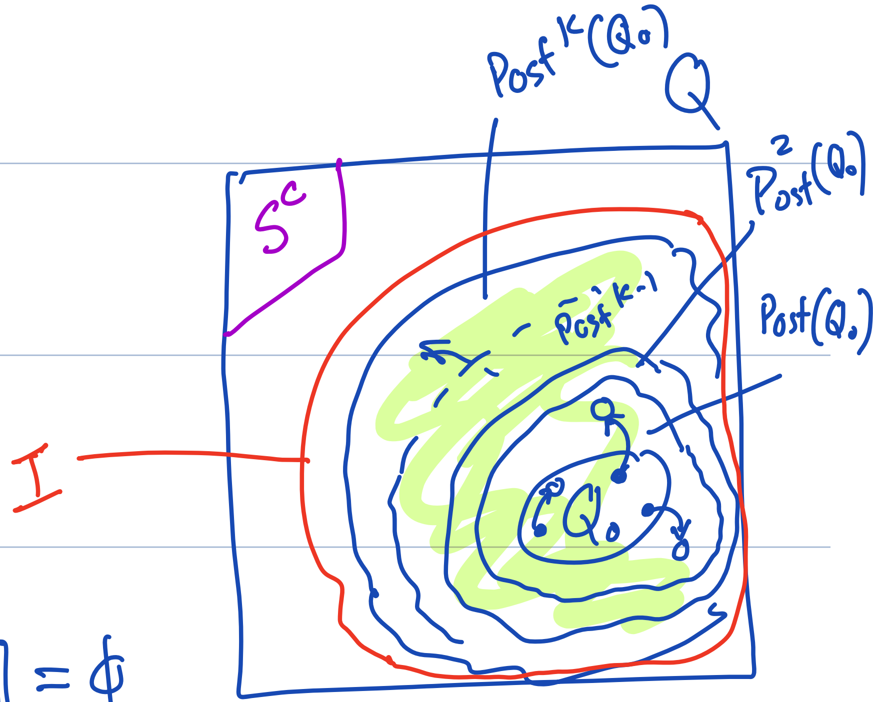
**Def** $Post^k : 2^Q \to 2^Q$

$Post^0(R) = R \qquad k = 0$

$Post^k(R) = Post(Post^{k-1}(R)) \quad k > 0$

**Exercise** $Post^k(Q_0)$
is exactly the set of states that the automaton can reach after executions of length $k$.

**Proof.**




$$\left[\bigcup_{k=0}^{T} Post^k(Q_0)\right] \cap [\![S^c]\!] = \phi$$

Reachability analysis tools can Compute or over approximate $post^k()$
E.g. Verse, SpaceEx, Flow*

In general computing $Post^k(R)$ can be hard (1) $Q$ high dimensional
(2) $D$ complex, (3) $k$ large

# Alternative Solution to Safety verification Problem

Find an <u>inductive invariant</u> for proving safety of $S$.

inductive invariant

**Thm** if there exists $I \subseteq Q$ such that

(1) $Q_0 \subseteq I$ (2) $Post(I) \subseteq I$

Then all executions of $A$ stay in $I$.

Further if $I \subseteq S$ then

Then $A$ is safe w.r.t $S$.

Sufficient condition for proving safety

Requires us to find $I$

existential not constructive

not unique $I$ necessarily

$A = \langle Q, Q_0, D \rangle$

$Q = \langle x_1, x_2, v_1, v_2 \rangle$ $\quad Q_0 :$ $\quad x_{20} > x_{10} > 0$

$v_{10}, v_{20} > 0$

$q$ Prestate $\quad q.x_1 < q\ x_2$

If $x_2 - x_1 < d_s$ $\quad q.x_2 - q.x_1 < d_s$

$\quad v_1 := \max(0, v_1 - a_b)$ $\quad q'.v_1 := \max\ldots$

else $\quad v_1 := v_1$

$x_1 := x_1 + v_1$ $\quad q'.x_1 = q.x_1 + q'.v_1$

$x_2 := x_2 + v_2$ $\quad q'.x_2 = q.x_2 + q'.v_2$

$q'$ Post state $\quad q'.x_1 < q'.x_2$

__Proof__. Consider any execution of $\mathcal{A}$ $\alpha = q_0 q_1 \cdots q_k$. We will prove by induction on $k$ that $\forall i \; q_i \in I$.

__Base Case__. $k = 0$ $\quad \alpha = q_0 \in Q_0 \subseteq I$ by (1)

__Inductive step__. $\alpha = q_0 \cdots q_{k-1} q_k$ and $q_{k-1} \in I$. We will show $a_k \in I$.

By (2) $Post(I) \subseteq I$

as $q_{k-1} \in I \Rightarrow q_k \in I$

Therefore $\forall i \quad q_i \in I$

Further if $I \subseteq S$ then $\forall i \; q_i \in S$

$\blacksquare$

Candidate

Simple, invariant and Safety

$S_1 := v_1 \geq 0$

How to prove that Carl never moves back?

Choose $I_1 = [\![ S_1 ]\!]$ This may not always work

Use inductive invariance theorem

Does $I_1$ meet the conditions (1) & (2)?

(1) $Q_0 \subseteq I_1 \triangleq \{q \mid q.v_1 \geq 0\}$

$\forall q_0 \in Q_0$ show $q_0 \in I$

$q_0.v_{10} \geq 0 \implies q_0 \in I_1$ ✓

$Q_0$

$q_0.x_2 > q_0.x_1 > 0$

$q_0.v_1 > 0$

$q_0.v_2 > 0$

$Post(I) \subseteq I$

(2) $Post(I) := \{q' \mid q \in I \text{ and } (q,q') \in D\}$

For any state $q \in I$ if $q.v_1 \geq 0$

and $(q,q') \in D$ then we have to

show that $q'.v_1$ is also $\geq 0$

How are $q$ and $q'$ related by $D$?

if $\quad q.x_2 - q.x_1 < ds$

(A) $\quad q'.v_1 = \max(0, q.v_1 - a_b)$

else

(B) $\quad q'.v_1 = q.v_1$

(A) $\quad q'.v_1 \geqslant 0$

(B) $\quad q'.v_1 = q.v_1 \geqslant 0 \quad$ [inductive hypothesis]

Another Safety requirement

$S_2 : \quad x_1 < x_2$

Is $S_2$ an inductive invariant?

(1) $Q_0 \subseteq S_2$ ✓ $\quad 0 < x_{10} < x_{20}$

(2) $Post(S_2) \subseteq S_2$ ?

Not necessarily true

if $q.v_1 \gg q.x_2 - q.x_1$

then $q'.x_1$ may exceed $q'.x_2$

We cannot prove $S_2$

We need to add or "discover" assumptions about $d_s$, $a_b$ ....
to prove $S_2$.

Add more information in the model

$$
\begin{aligned}
& timer := 0 \\
& \text{if } \; x_2 - x_1 < d_s \\
& \quad \text{if } \; v_1 > a_b \\
& \qquad \left.\begin{aligned} & v_1 := v_1 - a_b \\ & timer := timer + 1 \end{aligned}\right\} \; A \\
& \quad \text{else } \; v_1 := 0 \quad - \; B \\
& \text{else } \; v_1 := v_1 \quad - \; C \\
& x_1 := x_1 + v_1 \\
& x_2 := x_2 + v_2
\end{aligned}
$$

$I_3.\quad \text{timer} \leq \dfrac{v_{10} - v_1}{a_b}$

(1) $q_0.\text{timer} = 0 \leq \dfrac{v_{10} - \overset{q_0.v_1}{\overset{\parallel}{v_{10}}}}{a_b} \leq 0$

(2) $q \in I_3 \implies q' \in I_3$

Three Cases to consider

(A) if $q.x_2 - q.x_1 < d_s$ and $q.v_1 > a_b$

then $q'.\text{timer} = q.\text{timer} + 1$

$\leq \dfrac{v_{10} - q.v_1}{a_b} + 1$ [by inductive hypothesis

$v_1 := v_1 - a_b$

$q'.v_1 = q.v_1 - a_b$

$= \dfrac{v_{10} - (q'.v_1 + a_b)}{a_b} + 1$

$q'.\text{timer} \leq \dfrac{v_{10} - q'.v_1}{a_b}$

(B) if $q.x_2 - q.x_1 < d_s$ and $q.v_1 \leq a_b$

$q'.\text{timer} = q.\text{timer}$

$\leq \dfrac{v_{10} - q.v_1}{a_b}$ [By inductive hypothesis

Using $q.v_1 \geq 0$

$$\leq \frac{v_{10} + 0}{a_b}$$

(C) if. $q.x_2 - q.x_1 \geq d_s$

$$q'.timer = q.timer \leq \frac{v_{10} - q.v_1}{a_b}$$

$$\leq \frac{v_{10} - q'.v_1}{a_b}$$

Again, using inductive hypothesis at $q$

$I_3$ : $timer \leq \frac{v_{10} - v_1}{a_b}$ and $v_1 \geq 0$

$$\Rightarrow timer \leq \frac{v_{10}}{a_b} \quad \text{— (4)}$$

$I_3$ Still not enough to prove $x_2 - x_1 > 0$

Max distance traversed by Car1 after detection $\leq v_{10} \times timer \leq \frac{v_{10}^2}{a_b}$ using (4)

So, if $d_s > v_{10}^2 / a_b$ and $v_2 \geq 0$

then $I_3 \Rightarrow S_0 : x_2 > x_1$

That is, if $d_s > v_{10}^2/a_b$ then in any execution $\alpha$ of $\mathcal{A}$ and all states $q_1 \cdots q_k$ in $\alpha$, $q_i.x_2 > q_i.x_1$.

Summary

1. Safety requirements stated as sets of states or formula over state variables
2. $Post^k(Q_0) \cap [\![S^c]\!] = \phi$
   Reachability analysis for proving safety
3. $Q_0 \subseteq I$ and $Post(I) \subseteq I$ and $I \subseteq S$
   Inductive invariant for proving safety
4. Finding $I$ may require guess & check.