Proposition 2 Consider any automaton $\mathcal{A} = \langle Q, Q_0, \delta \rangle$ and a set $I \subseteq Q$ such that (i) $Q_0 \subseteq I$ (ii) $Post(I) \subseteq I$.
Then $Post^k(Q_0) \subseteq I$.

Such an I is called an inductive invariant.

Recall $Post(S) = \{ x' \mid \exists x \in S \ (x, x') \in \delta \}$

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

$Post(\cdot)$ is monotonic.

Proof. Induction on k.

Base $k=0$ $\quad Post^k(Q_0) = Post^0(Q_0) = Q_0$ [def Post]
$Q_0 \subseteq I$ [by (i)]

Inductive step Assume $Post^k(Q_0) \subseteq I$ for some k. (i)
We have to show that $Post^{k+1}(Q_0) \subseteq I$.
We apply $post(\cdot)$ to both sides of (i)
By monotonicity of $Post(\cdot)$ $\quad Post(Post^k(Q_0)) \subseteq Post(I)$
$\Rightarrow Post^{k+1}(Q_0) \subseteq Post(I)$ [def $Post^k$]
$\Rightarrow Post^{k+1}(Q_0) \subseteq I$ ▨ [by (ii)]

Remark (i) If we can find an $I \subseteq Q$ satisfying (i) and (ii) and $I \cap Unsafe = \phi$ then we have proven that all executions of $\mathcal{A}$ – are safe [never enter unsafe].

Remark (2) Prop 2 is IF ___ Then ___
not iff it is a <u>sufficient condition</u>
for proving — $Post^R(Q_0) \subseteq I$.

Can you propose an obvious invariant I ?

Example from last lecture

if $x_2 - x_4 < d_s$

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

else $v_1 := v_1$

$x_2 := x_2 + v_2$

$x_4 := x_4 + v_1$

Unsafe : " $x_1 \geq x_2$ "

$Unsafe \triangleq \{ x \in \mathbb{R}^4 \mid x.x_4 \geq x.x_2 \}$

$Safe = Unsafe^c = \{ x \mid x.x_4 < x.x_2 \}$

Is safe an inductive invariant?

(i) $\Theta_0 \subseteq Safe$ ✓

(ii) $Post(Safe) \subseteq Safe$ ✗

For an arbitrary state x with $x.x_4 < x.x_2$ we cannot show that if $(x, x') \in D$ the x' is also safe.

x does not have enough velocity information

What if $x.v_1 \gg x.x_2 - x.x_4$?

Thus we need to add more information in $X.x_1 < X.x_2 \wedge X.v_1 > \ldots$

We will also have to add assumptions about d_s : Sensing dist

a_b : braking force etc

Notice how trying to get an absolute proof is forcing us to "discover" assumptions that make the system work

New idea for I_0 bound max time of braking

Back to our example with small mods

initially

$x_1 = x_{10}$ $\quad x_2 = x_{20}$ $\quad v_1 = v_{10}$ $\quad v_2 = 0$ $\qquad Q_0$

timer = 0

if $x_2 - x_1 \leq d_s$
  if $v_1 \geq a_b$
    ① $v_1 := v_1 - a_b$
       timer := timer + 1
  ② else $v_1 := 0$
else $v_1 := v_1$ ③
$x_1 := x_1 - v_1$ (1,2,3)

Candidate invariant: $\quad timer + \frac{v_1}{a_b} \leq \frac{v_{10}}{a_b} \quad - I_2$

Claim: I_2 is an inductive invariant

Proof I_2 satisfies conditions (i) & (ii) of prop2.

(i) $\forall x \in Q_0 \quad x \in I_2 \quad x.timer + \frac{x.v_1}{a_b} \leq \frac{v_{10}}{a_b}$

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

(ii)

$\forall\ x, x' \in Q,\ x \in I_2, (x, x') \in D \quad x' \in I_2$

$\Downarrow$

$x.timer + \frac{x.v_1}{a_b} \leq \frac{v_{10}}{a_b}$

3 Cases

① $x'.timer + \frac{x'.v_1}{a_b}$

$= x.timer + 1 + \frac{x.v_1}{a_b} - \frac{a_b}{a_b} = x.timer + \frac{x.v_1}{a_b}$

$\leq \frac{v_{10}}{a_b} \qquad [x \in I_2]$

② $x'.timer + \frac{x'.v_1}{a_b} = x.timer + 0 \leq \frac{v_{10}}{a_b} \qquad [x \in I_2]$

③ $x'.timer + \frac{x'.v_1}{a_b} = x.timer + \frac{x.v_1}{a_b} \leq \frac{v_{10}}{a_b} \quad [x \in I_2]$

$\Rightarrow$ I_2 is an invariant in any execution at any step

$$\alpha[k].timer + \frac{\alpha[k].v_1}{a_b} \leq \frac{v_{10}}{a_b}$$

$$\Rightarrow \alpha[k].timer \leq \frac{v_{10}}{a_b}$$

Is this enough to infer safety?

No, what if d_s is too small for this tio time & v_{10}?

Maximum distance traveled after detection

$$v_{10} \cdot timer \leq v_{10} \cdot \frac{v_{10}}{a_b}$$

So, if $d_s > v_{10}^2 / a_b$ then $I_2 \Rightarrow$ Safe

Final statement. If the sensing range $d_s > v_{10}^2 / a_b$ then in any reachable state $x_2 > x_1$, i.e. there is no collision.