<u>Proposition 2</u> Consider any automaton $\mathcal{A} = \langle Q, Q_0, \mathcal{D} \rangle$ and a set $I \subseteq Q$ such that (i) (ii)

Then

Recall $Post(S) =$

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

$Post(\cdot)$ is monotonic.

<u>Proof</u>.

<u>Base</u>

<u>Remark</u> (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 – $Post^k(Q_0) \subseteq I$.

Can you propose an obvious invariant I ?

Example from last lecture

if $x_2 - x_1 < d_s$

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

else $v_1 := v_1$

$x_2 := x_2 + v_2$

$x_1 := x_1 + v_1$

Unsafe : " $x_1 \geq x_2$ "

$Unsafe \triangleq \{ x \in \mathbb{R}^4 \mid x.x_1 \geq x.x_2 \}$

$Safe = Unsafe^c = \{ x \mid x.x_1 < x.x_2 \}$

Is safe an inductive invariant?

For an arbitrary state x with $x.x_1 < x.x_2$

we cannot show that if $(x, x') \in D$ the

x' is also safe.

X does not have enough velocity information

What if $x.v_1 \gg x.x_2 - x.x_1$?

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

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

$x_1 = x_{10}$ $\quad x_2 = x_{20}$ $\quad v_1 = v_{10}$ $\quad v_2 = 0$ $\qquad S_0$

timer $= 0$

if $x_2 - x_1 \leq d_s$

Candidate invariant: $\quad timer + \frac{v_1}{a_b} \leq \frac{v_0}{a_b} \quad — I_2$

<u>Claim</u>: I_2 is an inductive invariant

<u>Proof</u>

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

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

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

Is this enough to infer safety?

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

Maximum distance traveled after detection

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

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.