Printout

Tuesday, August 30, 2022   10:38 AM

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

$\boxed{Post(S) := \{x' \mid \exists x \in S, (x, x') \in D\}}$

Recall $Post(S) =$

$\boxed{Post^k(S)} = S \quad k = 0$

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

$\boxed{Post(\cdot) \text{ is monotonic}}$

$\boxed{S_1 \subseteq S_2}$

$\boxed{\Rightarrow post(S_1) \subseteq post(S_2)}$

Consider $\boxed{x \in post(S_1)}$

$\{x' \in S_1 \mid (x', x) \in D\}$

$\boxed{x' \in S_2}$ $\quad [S_1 \subseteq S_2]$

$(x', x) \in D$

$x \in \boxed{post(S_2)}$

Proof: By induction on k

Base $k = 0$: $post^0(Q_0) = Q_0$

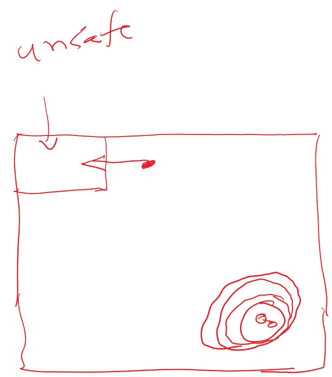
$(S_1) \subseteq (S_2)$: $Q_0 \subseteq I$ by [i]

Assume $\boxed{post^k(Q_0) \subseteq I}$

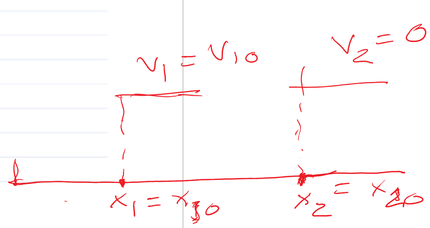
$post(post^k(Q_0)) \subseteq post(I) \subseteq I$

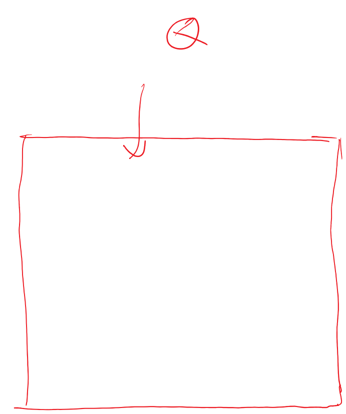
$\boxed{post^{k+1}(Q_0) \subseteq I}$

Remark (1) If we can find an $I \subseteq Q$ satisfying (i) and (ii) and $I \cap Unsafe = \emptyset$ 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 sufficient condition for proving $Post^k(Q_0) \subseteq I$.





$\boxed{I = Q}$

Can you propose an obvious invariant I?

Example from last lecture

if $(x_2 - x_1) < d_s$

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

else $v_1 := v_1$

$I = Q$

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?

(i) $Q_0 \subseteq$ safe $\quad \boxed{x_{10} < x_{20}}$

(ii) post (safe) $\not\subseteq$ safe

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 $x.v_1 >> x.x_2 - x.x_1$?

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 fore etc

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

New idea for I. bound max time of braking

Back to our example with small mods

initially

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

timer = 0

if $x_2 - x_1 \leq d_s$

if $v_1 \geq a_b$

$\Rightarrow v_1 := v_1 - a_b$ (1)

timer := timer + 1

else $v_1 := 0$ (2)

else

$v_1 := v_1$ (3)

$x_1 := x_1 + v_1$

Transition Rule.

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

Claim: I_2 is an inductive invariant

Proof (0) $x \in \Theta_0$; $x.\text{timer} + \frac{x.v_1}{a_b}$

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

Inductive Case:

Consider, $x \in I_2$; $x' \in Q$; $(x, x') \in D$ show $x' \in I_2$

we know

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

(1)

$$x'.\text{timer} + \frac{x'.v_1}{a_b} \Rightarrow x.\text{timer} + 1 + \frac{v_1 - a_b}{a_b}$$

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

(2)

$$x'.\text{timer} + \frac{x'.v_1}{a_b}$$

$$\boxed{x.\text{timer}} + 0 \leq \frac{v_{10}}{a_b}$$

(3)

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

$$\boxed{x' \in I_2}$$

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

$\alpha = \alpha_1 \alpha_2 \cdots \alpha_k$

$\alpha_k = \alpha[k]$

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

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

Is this enough to infer safety?

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

Maximum distance traveled after detection

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

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

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.