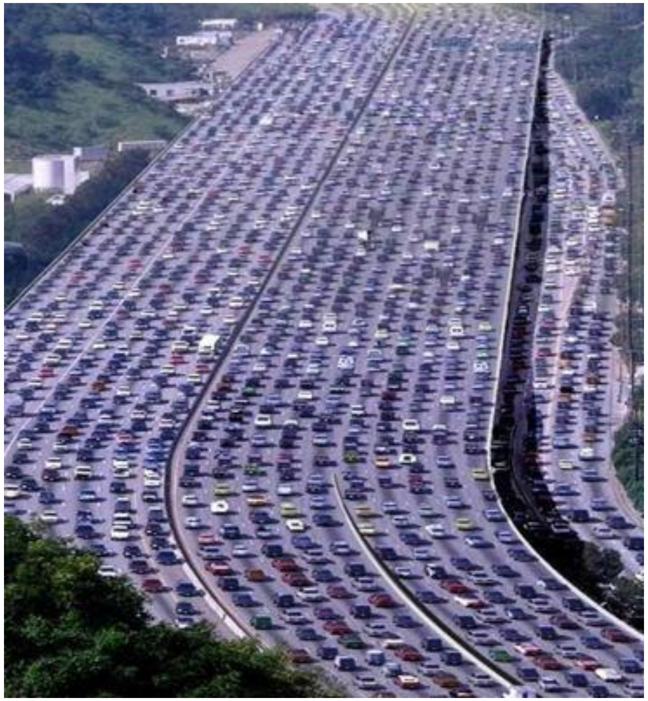
Adaptive Cruise Control:
Hybrid, Distributed, and Now Formally Verified

Sarah Loos, André Platzer, and Ligia Nistor
Computer Science Department
Carnegie Mellon University

June 22, 2011

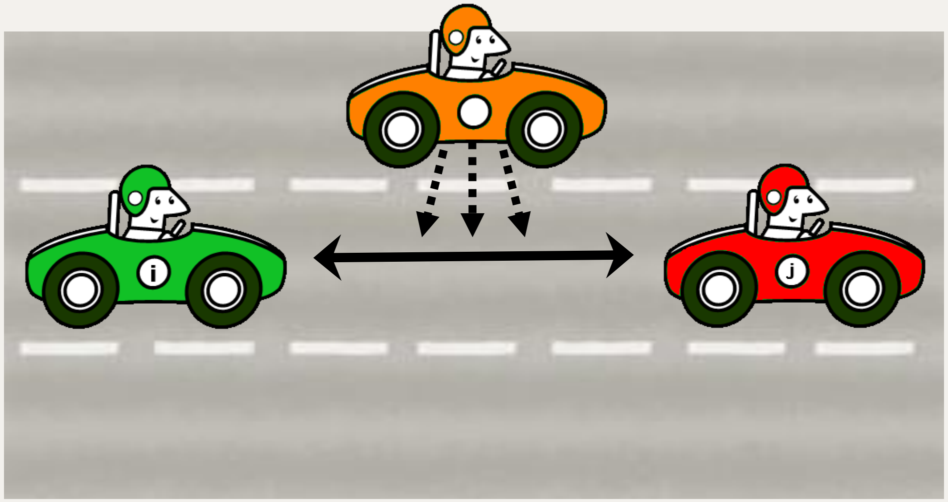
How Can We Prove Complex Highways?



Simplifying Assumptions

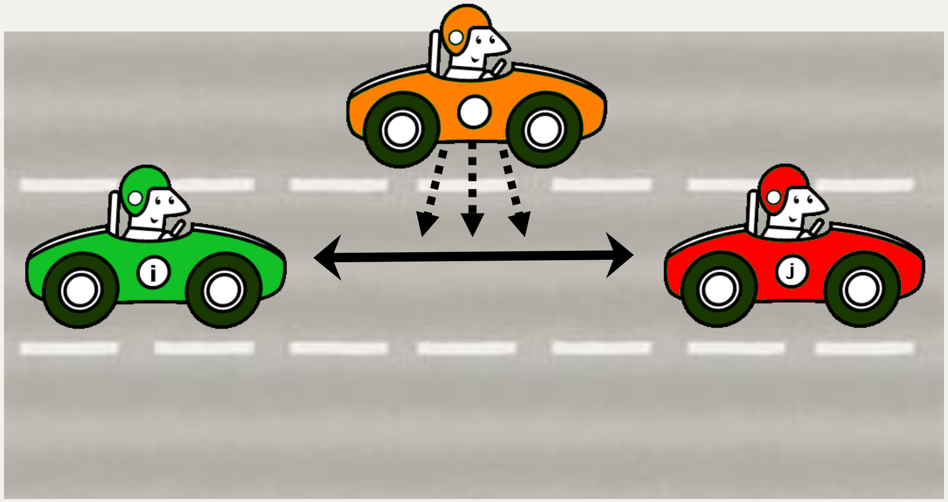
- Vehicles have positive velocity
- Accurate sensing
- Instantaneous braking and acceleration
- Time synchronization
- Delays for sensor updates is bounded
- Straight lane dynamics

How Can We Prove Complex Highways?



Sensor limits on actual cars are always local.

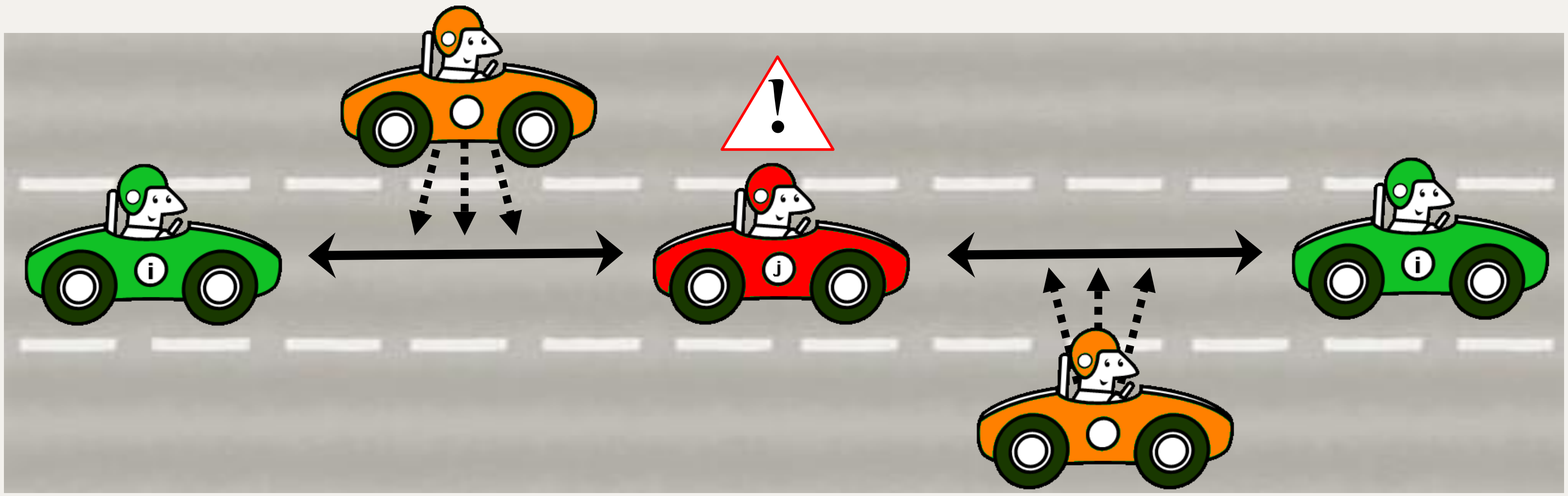
How Can We Prove Complex Highways?



Sensor limits on actual cars are always local.

Sometimes a maneuver may look safe locally...

How Can We Prove Complex Highways?



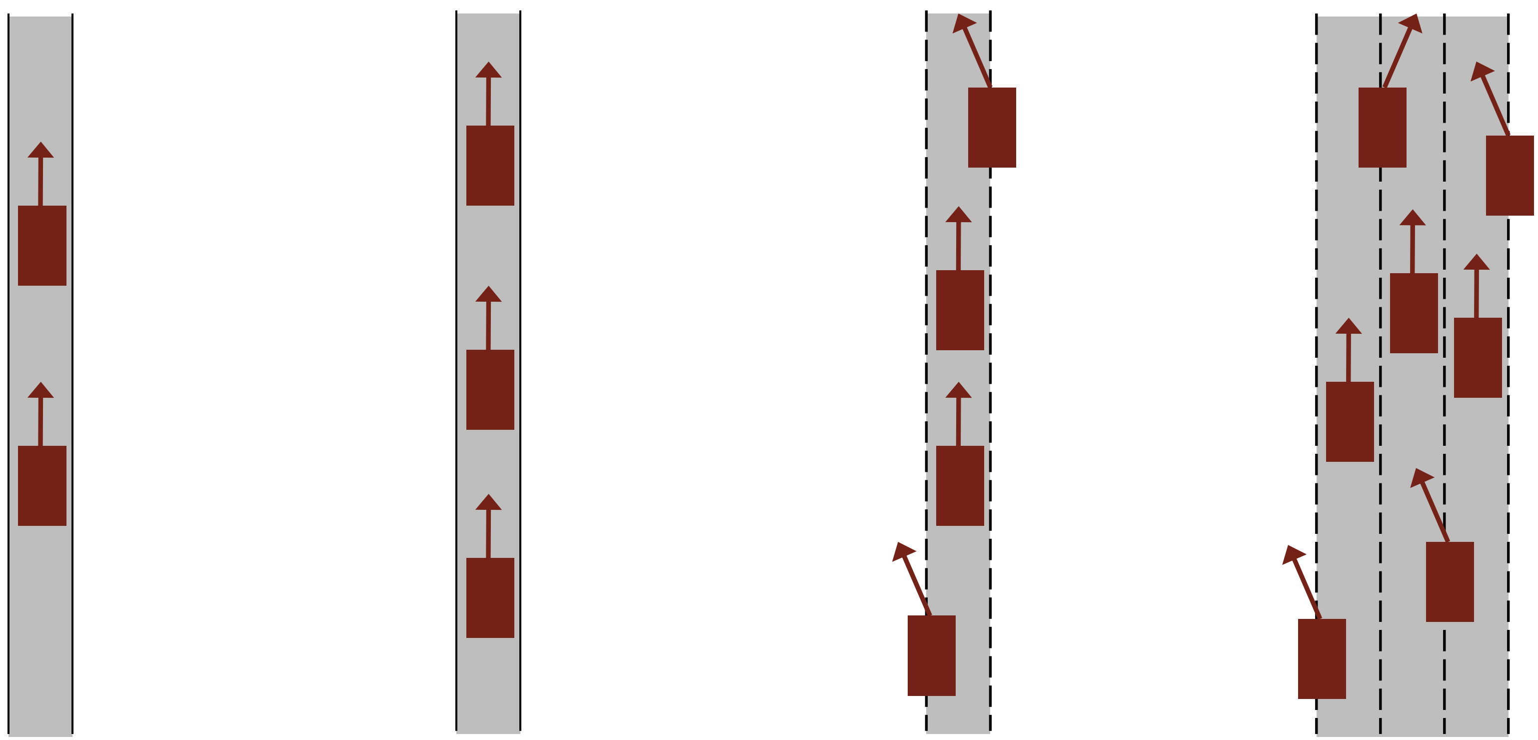
Sensor limits on actual cars are always local.

Sometimes a maneuver may look safe locally…

But is a terrible idea when implemented globally.

Car Control: Proof Sketch

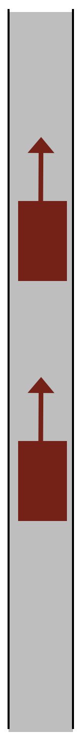
Local Lane Control	Global Lane Control	Local Highway Control	Global Highway Control



2 vehicles 1 lane no lane change	n vehicles 1 lane no lane change	n vehicles 1 lane lane changes	n vehicles m lanes lane changes

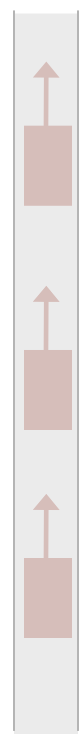
Car Control: Local Lane Control

Local Lane Control



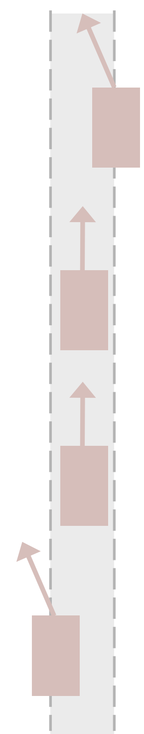
2 vehicles
1 lane
no lane change

Global Lane Control



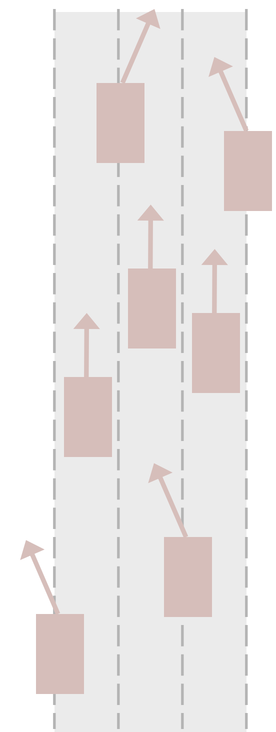
n vehicles
1 lane
no lane change

Local Highway Control



n vehicles
1 lane
lane changes

Global Highway Control



n vehicles
m lanes
lane changes

Differential Dynamic Logic*

*The short version.

Initial Conditions → [Model] Requirements

Differential Dynamic Logic

Initial Conditions $\rightarrow$ [Model] Requirements

Differential Dynamic Logic

$$\underbrace{\text{Initial Conditions}}_{\text{logical formula}} \rightarrow [\text{Model}]\ \underbrace{\text{Requirements}}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \leq x_\ell)}_{\text{logical formula}} \rightarrow [\text{Model}] \underbrace{(x_f \leq x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \le x_\ell)}_{\text{logical formula}} \rightarrow [\color{red}{\text{Model}}] \underbrace{(x_f \le x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \leq x_\ell)}_{\text{logical formula}} \rightarrow [\underbrace{\color{red}{\text{Model}}}_{\text{hybrid program}}] \underbrace{(x_f \leq x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \le x_\ell)}_{\text{logical formula}} \rightarrow [\overbrace{\underbrace{\color{red}{\text{Model}}}_{\text{hybrid program}}}^{\text{discrete control} \quad \text{continuous dynamics}}] \underbrace{(x_f \le x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

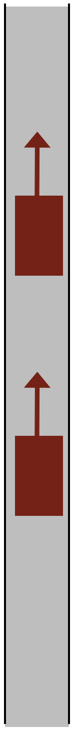
$$\underbrace{(x_f \le x_\ell)}_{\text{logical formula}} \rightarrow \underbrace{[(\overbrace{\text{ctrl}}^{\text{discrete control}};\overbrace{\text{dyn}}^{\text{continuous dynamics}})^*]}_{\text{hybrid program}} \; \underbrace{(x_f \le x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \le x_\ell)}_{\text{logical formula}} \rightarrow \underbrace{[(\overbrace{\mathrm{ctrl}}^{\text{discrete control}};\ \overbrace{\mathrm{x}' = \mathrm{v};\ \mathrm{v}' = \mathrm{a}}^{\text{continuous dynamics}})^*]}_{\text{hybrid program}}\underbrace{(x_f \le x_\ell)}_{\text{logical formula}}$$

Car Control: Definition of Safety

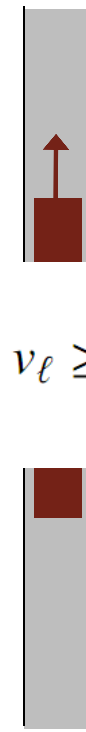
Car f is safely following car ℓ if $(f \ll \ell)$



Car Control: Definition of Safety

Car f is safely following car ℓ if $(f \ll \ell)$

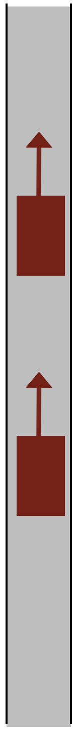
$$(f \ll \ell) \equiv (x_f \le x_\ell) \wedge (f \ne \ell) \rightarrow \left(x_f < x_\ell \wedge x_f + \frac{v_f^2}{2b} < x_\ell + \frac{v_\ell^2}{2B} \wedge v_f \ge 0 \wedge v_\ell \ge 0 \right)$$



Car Control: Definition of Safety

Car f is safely following car ℓ if $(f \ll \ell)$

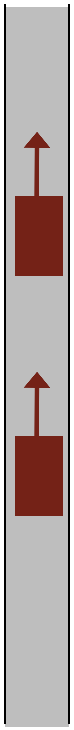
$$(f \ll \ell) \;\equiv\; x_f + \frac{v_f^2}{2b} < x_\ell + \frac{v_\ell^2}{2B}$$



Car Control: Local Lane Control

To Prove: $(f \ll \ell) \rightarrow [\mathtt{llc}](f \ll \ell)$

$$
\begin{aligned}
\mathtt{llc} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \,\|\, f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *;\ \ ?(-B \le a_\ell \le A)) \\
f_{ctrl} &\equiv (a_f := *;\ \ ?(-B \le a_f \le -b)) \\
&\qquad \cup\ \ (?\mathbf{Safe}_\varepsilon;\ \ a_f := *;\ \ ?(-B \le a_f \le A)) \\
&\qquad \cup\ \ (?(v_f = 0);\ a_f := 0) \\
\mathbf{Safe}_\varepsilon &\equiv x_f + \frac{v_f^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_f\right) < x_\ell + \frac{v_\ell^2}{2B} \\
dyn &\equiv (t := 0;\ x_f' = v_f,\ v_f' = a_f,\ x_\ell' = v_\ell,\ v_\ell' = a_\ell, t' = 1 \\
&\qquad v_f \ge 0 \ \wedge\ v_\ell \ge 0 \ \wedge\ t \le \varepsilon)
\end{aligned}
$$



Initial Conditions $\longrightarrow$ [Model] Requirements

Car Control: Local Lane Control

To Prove: $(f \ll \ell) \rightarrow [\mathtt{llc}](f \ll \ell)$

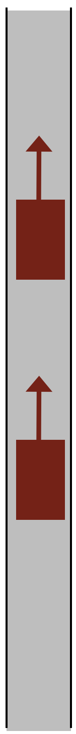
✔ **Verified in KeYmaera**

$$
\begin{aligned}
\mathtt{llc} &\equiv (ctrl; dyn) \\
ctrl &\equiv \ell_{ctrl} \parallel f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *;\ \ ?(-B \le a_\ell \le A)) \\
f_{ctrl} &\equiv (a_f := *;\ \ ?(-B \le a_f \le -b)) \\
&\quad \cup\ (?\mathbf{Safe}_\varepsilon;\ \ a_f := *;\ \ ?(-B \le a_f \le A)) \\
&\quad \cup\ (?(v_f = 0);\ a_f := 0) \\
\mathbf{Safe}_\varepsilon &\equiv x_f + \frac{v_f^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_f\right) < x_\ell + \frac{v_\ell^2}{2B} \\
dyn &\equiv (t := 0;\ x_f' = v_f,\ v_f' = a_f,\ x_\ell' = v_\ell,\ v_\ell' = a_\ell, t' = 1 \\
&\qquad v_f \ge 0\ \wedge\ v_\ell \ge 0\ \wedge\ t \le \varepsilon)
\end{aligned}
$$

Initial Conditions $\longrightarrow$ [Model] Requirements

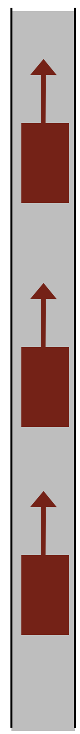
Car Control: Global Lane Control

Local Lane Control



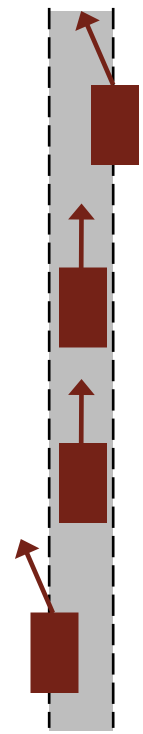
2 vehicles
1 lane
no lane change

Global Lane Control



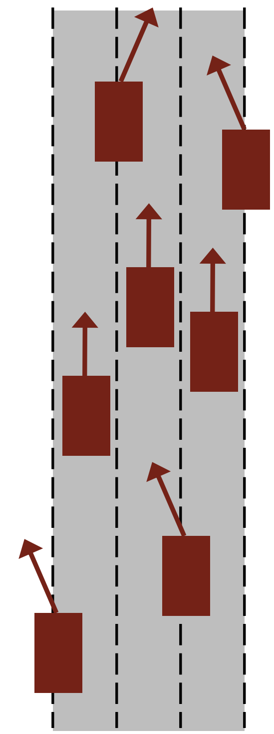
n vehicles
1 lane
no lane change

Local Highway Control



n vehicles
1 lane
lane changes

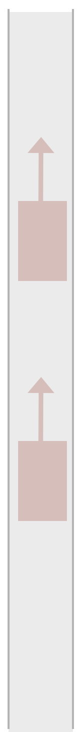
Global Highway Control



n vehicles
m lanes
lane changes

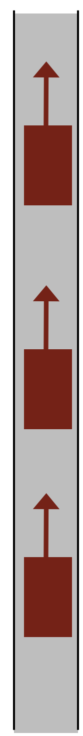
Car Control: Global Lane Control

Local Lane Control



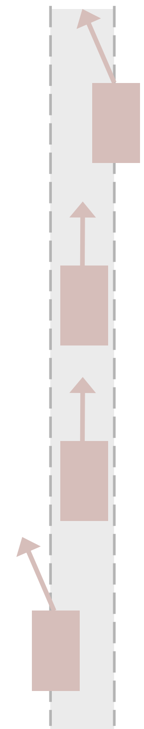
2 vehicles
1 lane
no lane change

Global Lane Control



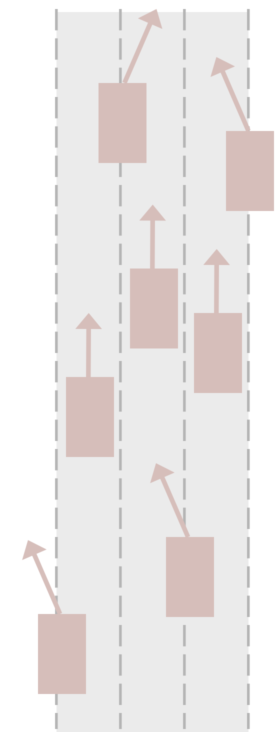
n vehicles
1 lane
no lane change

Local Highway Control



n vehicles
1 lane
lane changes

Global Highway Control



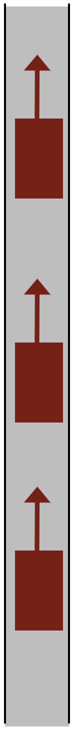
n vehicles
m lanes
lane changes

Car Control: Global Lane Control

To Prove:

$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\texttt{glc}](\forall i : C(i \ll L^*(i)))$$

$$\begin{aligned}
\texttt{glc} &\equiv (ctrl^n; dyn^n)^* \\
ctrl^n &\equiv \forall i : C\ (ctrl(i)) \\
ctrl(i) &\equiv (a(i) := *; ?(-B \le a(i) \le -b)) \\
&\quad \cup\ (?\mathbf{Safe}_\varepsilon(i);\ a(i) := *;\ ?(-B \le a(i) \le A)) \\
&\quad \cup\ (?(v(i) = 0);\ a(i) := 0) \\
\mathbf{Safe}_\varepsilon(i) &\equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B} \\
dyn^n &\equiv (t := 0;\ \forall i : C\ (dyn(i)), t' = 1, t \le \varepsilon) \\
dyn(i) &\equiv x'(i) = v(i), v'(i) = a(i), v(i) \ge 0
\end{aligned}$$



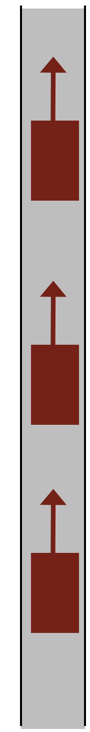
Initial Conditions $\rightarrow$ [Model] Requirements

Car Control: Global Lane Control

To Prove:

$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\mathtt{glc}](\forall i : C(i \ll L^*(i)))$$

$$\begin{aligned}
\mathtt{glc} &\equiv (ctrl^n; dyn^n)^* \\
ctrl^n &\equiv \forall i : C\ (ctrl(i)) \\
ctrl(i) &\equiv (a(i) := *; ?(-B \leq a(i) \leq -b)) \\
&\quad \cup \ (?\mathbf{Safe}_\varepsilon(i);\ a(i) := *;\ ?(-B \leq a(i) \leq A)) \\
&\quad \cup \ (?(v(i) = 0);\ a(i) := 0) \\
\mathbf{Safe}_\varepsilon(i) &\equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B} \\
dyn^n &\equiv (t := 0;\ \forall i : C\ (dyn(i)), t' = 1, t \leq \varepsilon) \\
dyn(i) &\equiv x'(i) = v(i), v'(i) = a(i), v(i) \geq 0
\end{aligned}$$



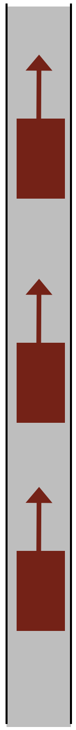
Initial Conditions $\longrightarrow$ [Model] Requirements

Car Control: Global Lane Control

To Prove:

$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\mathtt{glc}](\forall i : C(i \ll L^*(i)))$$

$$\begin{aligned}
\mathtt{glc} &\equiv (ctrl^n; dyn^n)^* \\
ctrl^n &\equiv \forall i : C\,(ctrl(i)) \\
ctrl(i) &\equiv (a(i) := *; ?(-B \le a(i) \le -b)) \\
&\qquad \cup \;\; (?\mathbf{Safe}_\varepsilon(i);\; a(i) := *;\; ?(-B \le a(i) \le A)) \\
&\qquad \cup \;\; (?(v(i) = 0);\; a(i) := 0) \\
\mathbf{Safe}_\varepsilon(i) &\equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B} \\
dyn^n &\equiv (t := 0;\; \forall i : C\;(dyn(i)), t' = 1, t \le \varepsilon) \\
dyn(i) &\equiv x'(i) = v(i), v'(i) = a(i), v(i) \ge 0
\end{aligned}$$



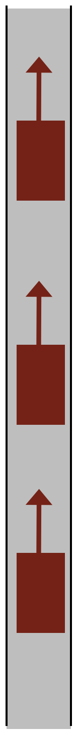
Initial Conditions $\longrightarrow$ [Model] Requirements

Car Control: Global Lane Control

To Prove:

$$\forall i : C(i \ll L(i)) \rightarrow [\texttt{glc}](\forall i : C(i \ll L^*(i)))$$

$$\begin{aligned}
\texttt{glc} &\equiv (ctrl^n; dyn^n)^* \\
ctrl^n &\equiv \forall i : C\ (ctrl(i)) \\
ctrl(i) &\equiv (a(i) := *; ?(-B \le a(i) \le -b)) \\
&\quad \cup\ (?\mathbf{Safe}_\varepsilon(i);\ a(i) := *;\ ?(-B \le a(i) \le A)) \\
&\quad \cup\ (?(v(i) = 0);\ a(i) := 0) \\
\mathbf{Safe}_\varepsilon(i) &\equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B} \\
dyn^n &\equiv (t := 0;\ \forall i : C\ (dyn(i)), t' = 1, t \le \varepsilon) \\
dyn(i) &\equiv x'(i) = v(i), v'(i) = a(i), v(i) \ge 0
\end{aligned}$$



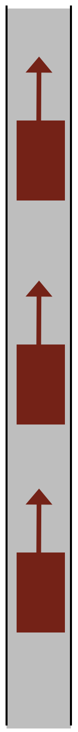
Initial Conditions $\longrightarrow$ [Model] Requirements

Car Control: Global Lane Control

To Prove:

$$\forall i : C(i \ll L(i)) \ \rightarrow\ [\mathtt{glc}](\forall i : C(i \ll L^*(i)))$$

$$\begin{aligned}
\mathtt{glc} &\equiv (ctrl^n; dyn^n)^* \\
ctrl^n &\equiv \forall i : C\ (ctrl(i)) \\
ctrl(i) &\equiv (a(i) := *; ?(-B \le a(i) \le -b)) \\
&\qquad \cup\ (?\mathbf{Safe}_\varepsilon(i);\ a(i) := *;\ ?(-B \le a(i) \le A)) \\
&\qquad \cup\ (?(v(i) = 0);\ a(i) := 0) \\
\mathbf{Safe}_\varepsilon(i) &\equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B} \\
dyn^n &\equiv (t := 0;\ \forall i : C\ (dyn(i)), t' = 1, t \le \varepsilon) \\
dyn(i) &\equiv x'(i) = v(i), v'(i) = a(i), v(i) \ge 0
\end{aligned}$$

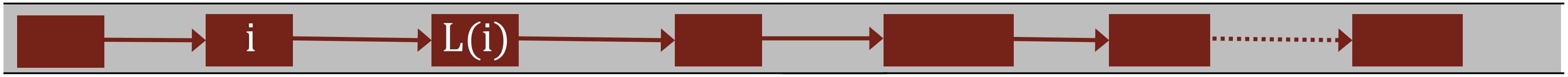


Initial Conditions $\longrightarrow$ [Model] Requirements

Transitive Leader

To Prove:

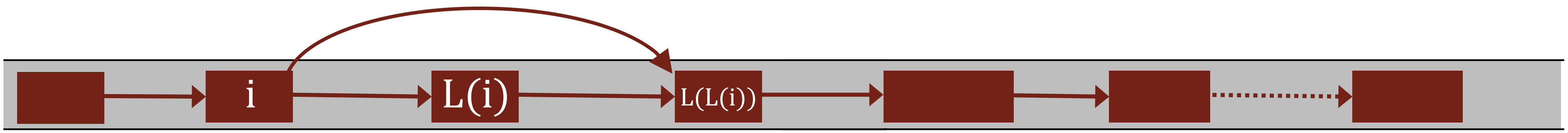
$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\mathtt{glc}](\forall i : C(i \ll L^{*}(i)))$$



Transitive Leader

To Prove:

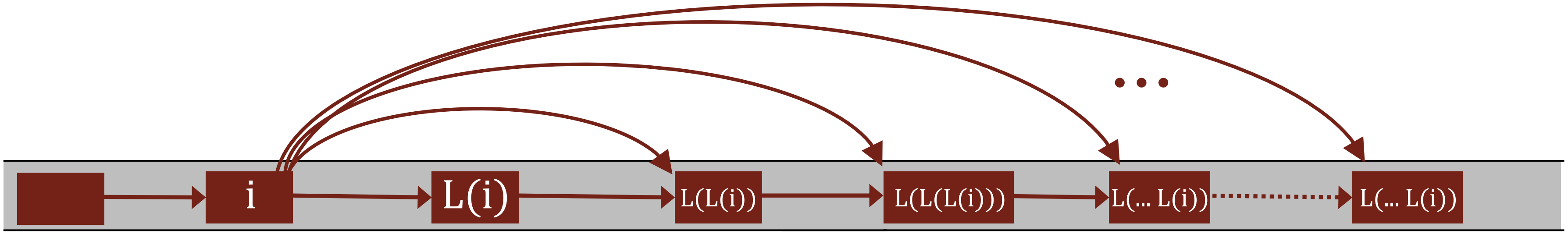
$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\mathtt{glc}](\forall i : C(i \ll L^{*}(i)))$$



Transitive Leader

To Prove:

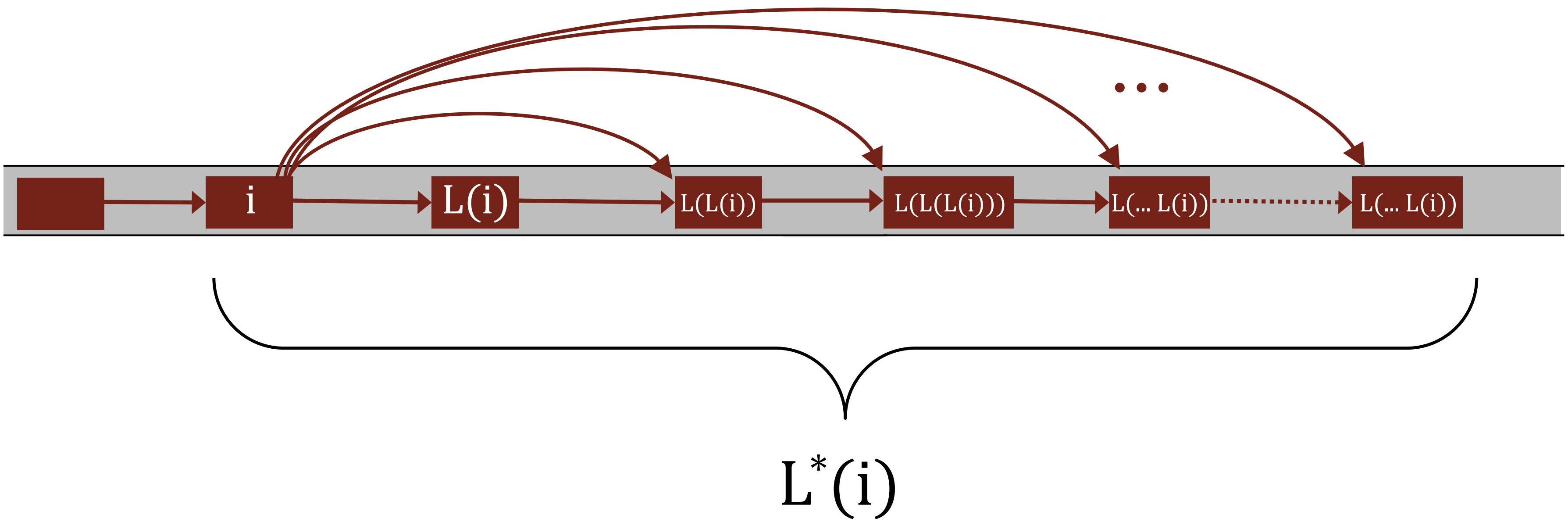
$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\texttt{glc}](\forall i : C(i \ll L^*(i)))$$



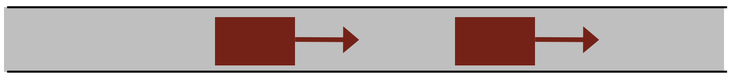
Transitive Leader

To Prove:

$$\forall i : C(i \ll L(i)) \rightarrow [\texttt{glc}](\forall i : C(i \ll L^*(i)))$$



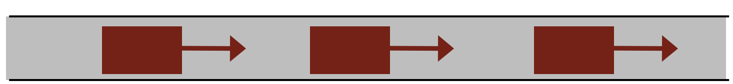
Proof: Global Lane Control



$$\dfrac{}{\forall i\, x(i) \ll x\big(L(i)\big) \rightarrow [glc]\, \forall i\, x(i) \ll x(L(i))}$$

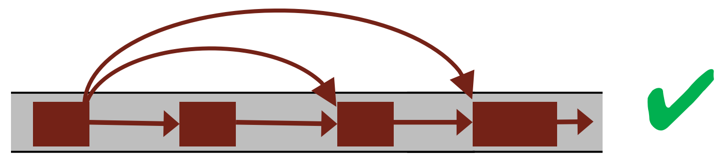
$$\dfrac{\dfrac{\text{Safety is Transitive}}{\forall i\, x(i) \ll x\big(L(i)\big) \rightarrow\ \forall i\, x(i) \ll x(L^{*}(i))}}{[glc]\, \forall i\, x(i) \ll x\big(L(i)\big) \rightarrow\ [glc]\, \forall i\, x(i) \ll x(L^{*}(i))}\ \textbf{([] gen)}$$

$$\dfrac{}{\forall i\, x(i) \ll x\big(L(i)\big) \rightarrow\ [glc]\, \forall i\, x(i) \ll x(L^{*}(i))}\ \textbf{(cut)}$$



Proof: Global Lane Control

$$\forall i\; x(i) \ll x\big(L(i)\big) \to [glc]\,\forall i\; x(i) \ll x(L(i))$$



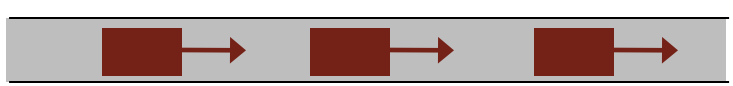
$$\forall i\; x(i) \ll x\big(L(i)\big) \to \forall i\; x(i) \ll x(L^*(i))$$

([] gen)

$$[glc]\,\forall i\; x(i) \ll x\big(L(i)\big) \to [glc]\,\forall i\; x(i) \ll x(L^*(i))$$

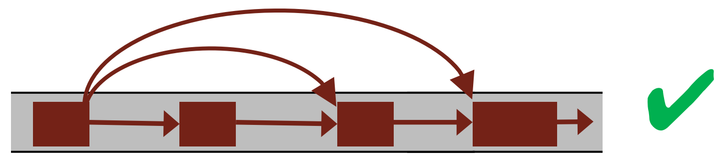
(cut)

$$\forall i\; x(i) \ll x\big(L(i)\big) \to [glc]\,\forall i\; x(i) \ll x(L^*(i))$$



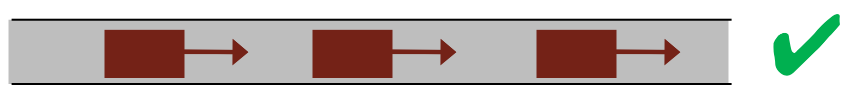
Proof: Global Lane Control

$$\dfrac{}{\forall i\ x(i) \ll x\big(L(i)\big) \rightarrow [glc]\ \forall i\ x(i) \ll x(L(i))}$$



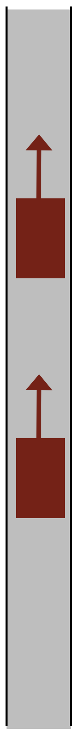
$$\dfrac{\dfrac{}{\forall i\ x(i) \ll x\big(L(i)\big) \rightarrow\ \forall i\ x(i) \ll x(L^*(i))}}{[glc]\ \forall i\ x(i) \ll x\big(L(i)\big) \rightarrow\ [glc]\ \forall i\ x(i) \ll x(L^*(i))}\ \textbf{([] gen)}$$

$$\dfrac{}{\forall i\ x(i) \ll x\big(L(i)\big) \rightarrow\ [glc]\ \forall i\ x(i) \ll x(L^*(i))}\ \textbf{(cut)}$$



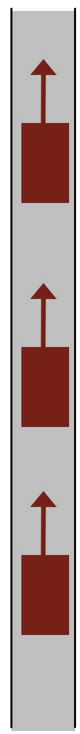
Car Control: Local Highway Control

Local Lane Control



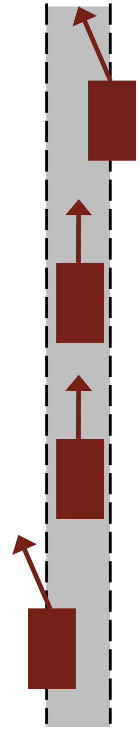
2 vehicles
1 lane
no lane change

Global Lane Control



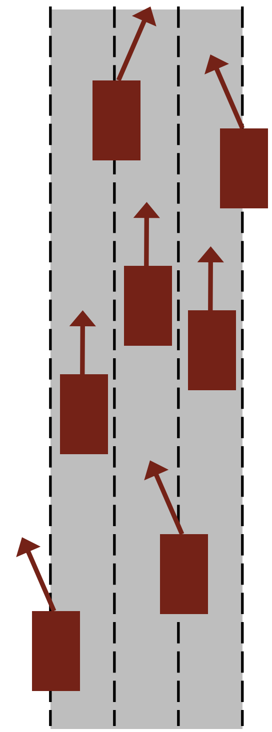
n vehicles
1 lane
no lane change

Local Highway Control



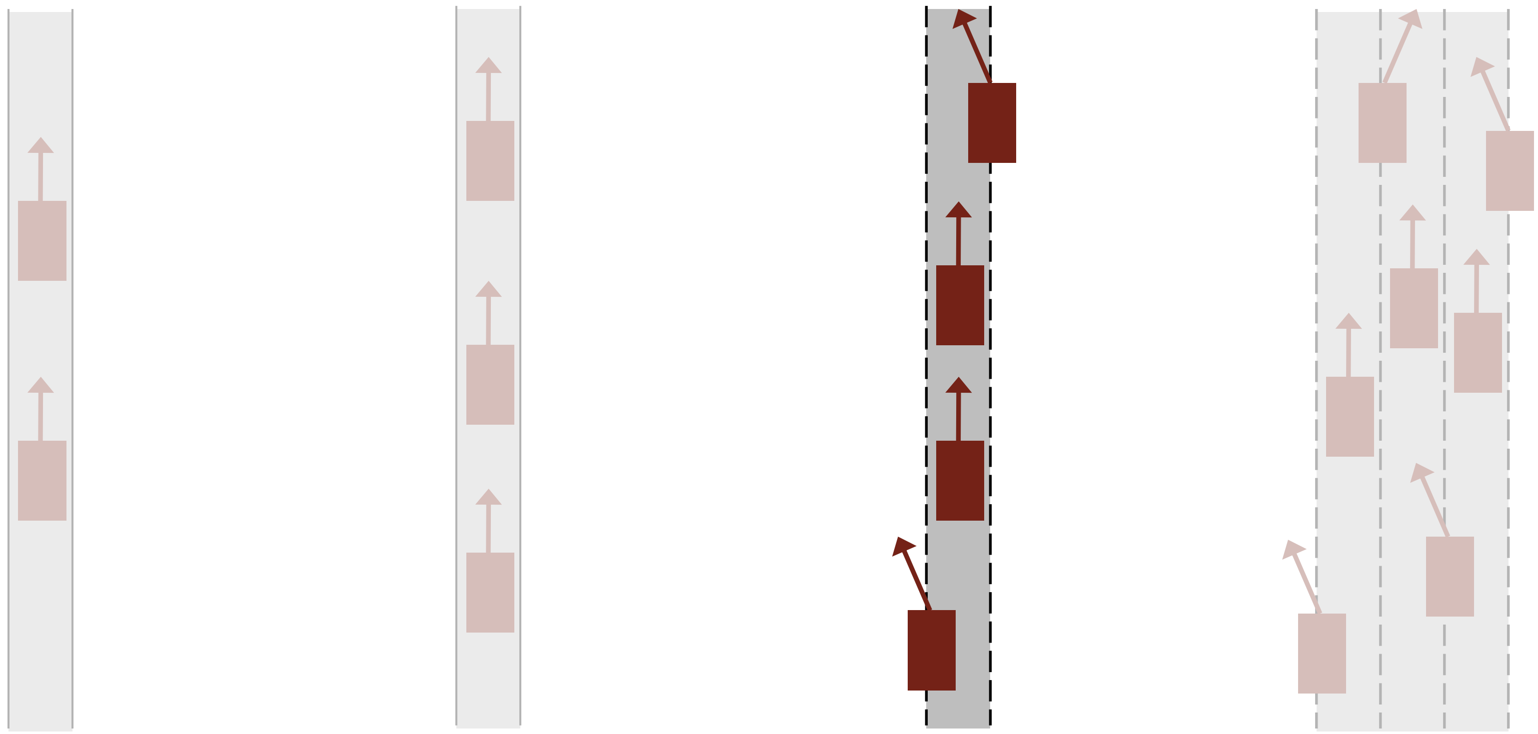
n vehicles
1 lane
lane changes

Global Highway Control



n vehicles
m lanes
lane changes

Car Control: Local Highway Control



Local Lane Control

2 vehicles
1 lane
no lane change

Global Lane Control

n vehicles
1 lane
no lane change

Local Highway Control

n vehicles
1 lane
lane changes

Global Highway Control

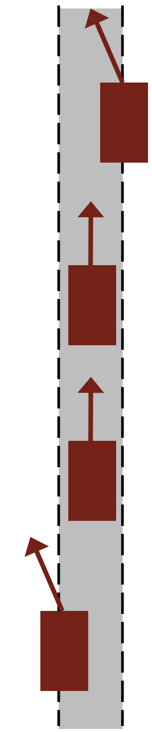
n vehicles
m lanes
lane changes

Car Control: Local Highway Control

To Prove:

$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\mathtt{lhc}]\forall i : C(i \ll L^*(i))$$

$$\begin{aligned}
\mathtt{lhc} &\equiv (delete^*; create^*; ctrl^n; dyn^n)^* \\
create &\equiv n := new;\; ?((F(n) \ll n) \land (n \ll L(n))) \\
(n := new) &\equiv n := *;\; ?(\mathrm{E}(n) = 0);\; \mathrm{E}(n) := 1 \\
(F(n) \ll n) &\equiv \forall j : C\,(L(j) = n \rightarrow (j \ll n)) \\
delete &\equiv n := *;\; ?(\mathrm{E}(n) = 1);\; \mathrm{E}(n) := 0
\end{aligned}$$



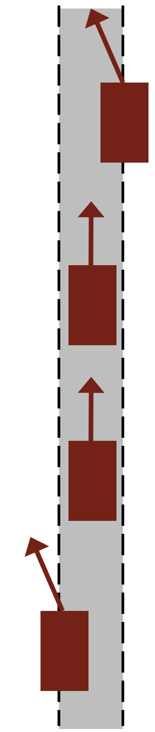
Initial Conditions $\longrightarrow$ [Model] Requirements

Car Control: Local Highway Control

To Prove:

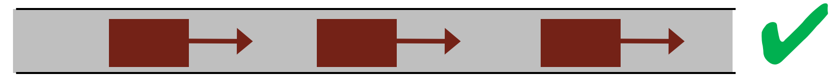
$$\forall i : C(i \ll L(i)) \;\rightarrow\; [\texttt{lhc}]\forall i : C(i \ll L^*(i))$$

$$\begin{aligned}
\texttt{lhc} &\equiv (delete^*; create^*; ctrl^n; dyn^n)^* \\
create &\equiv n := new;\ ?((F(n) \ll n) \land (n \ll L(n))) \\
(n := new) &\equiv n := *;\ ?(\mathrm{E}(n) = 0);\ \mathrm{E}(n) := 1 \\
(F(n) \ll n) &\equiv \forall j : C\,(L(j) = n \rightarrow (j \ll n)) \\
delete &\equiv n := *;\ ?(\mathrm{E}(n) = 1);\ \mathrm{E}(n) := 0
\end{aligned}$$



Initial Conditions → [Model] Requirements

Proof: Local Highway Control



$$\forall i\, x(i) \ll L\big(x(i)\big) \rightarrow [glc]\forall i\, x(i) \ll L^*(x(i))$$

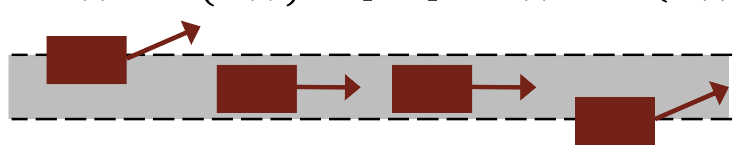
Transitivity

$$\forall i\, x(i) \ll L\big(x(i)\big) \rightarrow [create^*]\forall i\, x(i) \ll L^*(x(i))$$

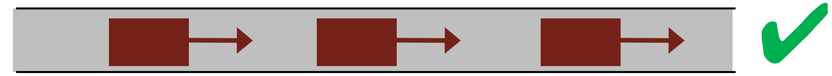
Transitivity

$$\forall i\, x(i) \ll L\big(x(i)\big) \rightarrow [delete^*]\forall i\, x(i) \ll L^*(x(i))$$

$$\dfrac{\dfrac{}{\forall i\, x(i) \ll L\big(x(i)\big) \rightarrow [delete^*][create^*][glc]\forall i\, x(i) \ll L^*(x(i))}\;\textbf{([] split)}}{\forall i\, x(i) \ll L\big(x(i)\big) \rightarrow [lhc]\forall i\, x(i) \ll L^*(x(i))}\;\textbf{([;])}$$



Proof: Local Highway Control



$$\forall i\ x(i) \ll L\big(x(i)\big) \to [glc]\forall i\ x(i) \ll L^*(x(i))$$

Transitivity

$$\forall i\ x(i) \ll L\big(x(i)\big) \to [create^*]\forall i\ x(i) \ll L^*(x(i))$$

Transitivity

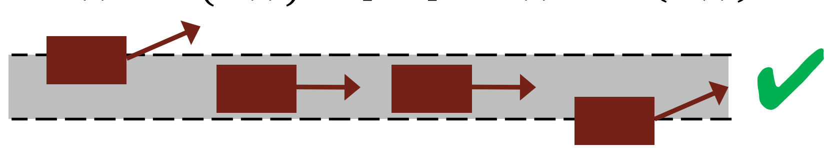
$$\forall i\ x(i) \ll L\big(x(i)\big) \to [delete^*]\forall i\ x(i) \ll L^*(x(i))$$

([] split)

$$\forall i\ x(i) \ll L\big(x(i)\big) \to [delete^*][create^*][glc]\forall i\ x(i) \ll L^*(x(i))$$

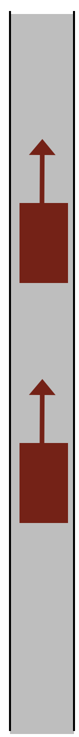
([;])

$$\forall i\ x(i) \ll L\big(x(i)\big) \to [lhc]\forall i\ x(i) \ll L^*(x(i))$$



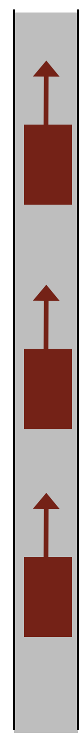
Car Control: Global Highway Control

Local Lane Control



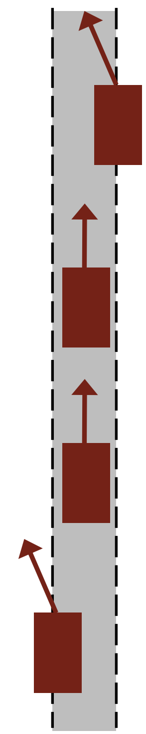
2 vehicles
1 lane
no lane change

Global Lane Control



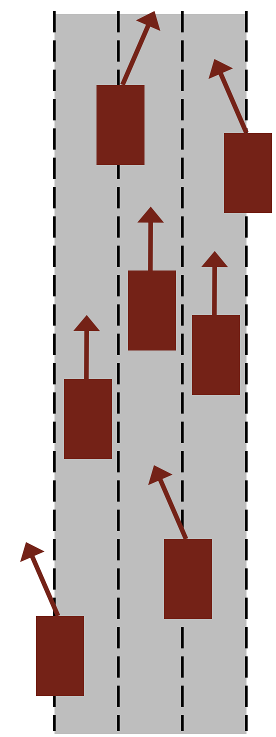
n vehicles
1 lane
no lane change

Local Highway Control



n vehicles
1 lane
lane changes

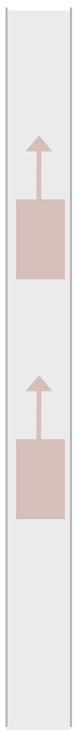
Global Highway Control



n vehicles
m lanes
lane changes

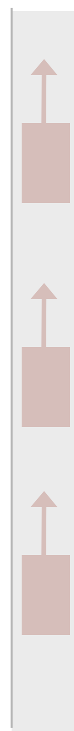
Car Control: Global Highway Control

Local Lane Control



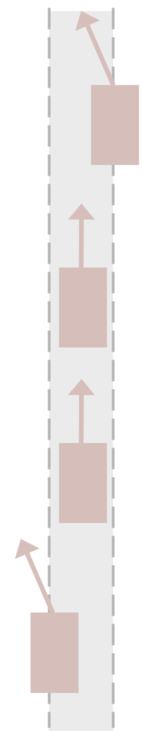
2 vehicles
1 lane
no lane change

Global Lane Control



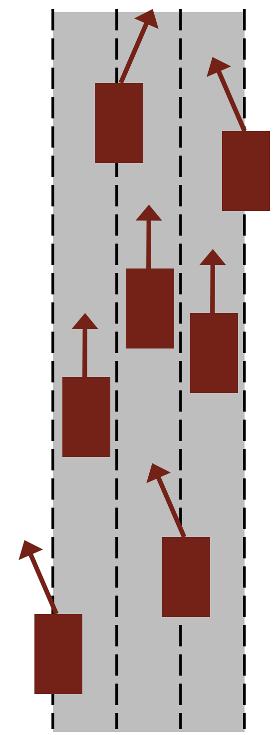
n vehicles
1 lane
no lane change

Local Highway Control



n vehicles
1 lane
lane changes

Global Highway Control



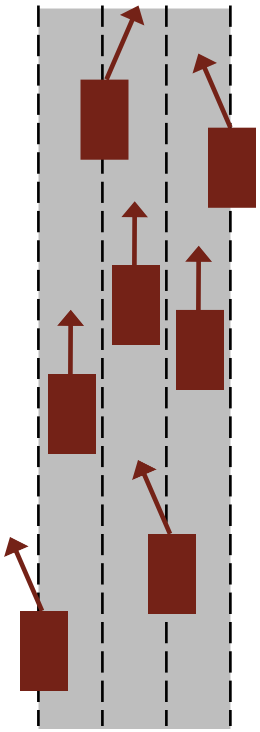
n vehicles
m lanes
lane changes

Car Control: Global Highway Control

To Prove:

$$\forall l : L \forall i : C_l (i \ll L_l(i)) \rightarrow [\text{ghc}] \, \forall l : L \forall i : C_l (i \ll L_l^*(i))$$

$$\text{ghc} \; ::= \; (\forall l : L \; delete_l^*; \; \forall l : L \; new_l^*; \; \forall l : L \; ctrl_l^n; \; \forall l : L \; dyn_l^n)^*$$



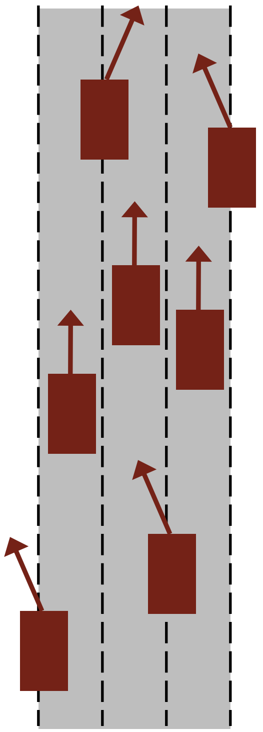
Initial Conditions $\longrightarrow$ [Model] Requirements

Car Control: Global Highway Control

To Prove:

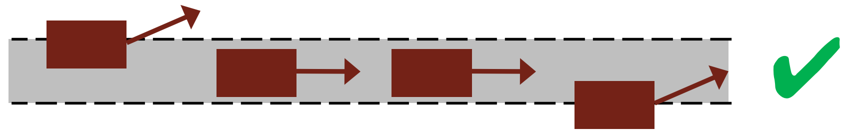
$$\forall l : L \forall i : C_l(i \ll L_l(i)) \rightarrow [\text{ghc}]\ \forall l : L \forall i : C_l(i \ll L_l^*(i))$$

$$\text{ghc} ::= (\forall l : L\, delete_l^*;\ \forall l : L\, new_l^*;\ \forall l : L\, ctrl_l^n;\ \forall l : L\, dyn_l^n)^*$$



Initial Conditions $\longrightarrow$ [Model] Requirements

Proof: Global Highway Control



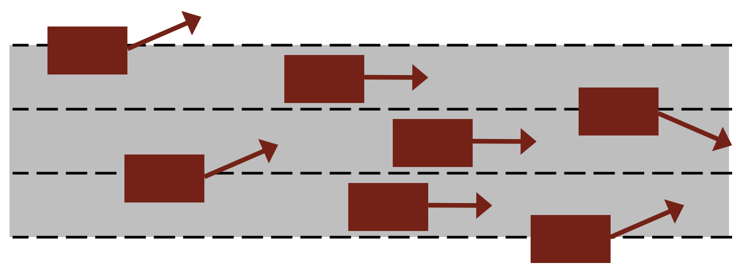
$$\forall i\ x(i) \ll L_l\big(x(i)\big) \to [lhc]\ \forall i\ x(i) \ll L_l^*\big(x(i)\big)$$

$$\forall l\ \Big(\forall i\ x(i) \ll L_l\big(x(i)\big) \to [lhc]\forall i\ x(i) \ll L_l^*\big(x(i)\big)\Big)$$

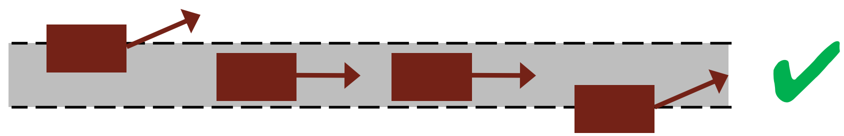
$$\forall l\ \forall i\ x(i) \ll L_l\big(x(i)\big) \to \forall l\ [lhc]\forall i\ x(i) \ll L_l^*\big(x(i)\big)$$

$$\forall l\ \forall i\ x(i) \ll L_l\big(x(i)\big) \to \big[\forall l\ (lhc)\ \ \big]\forall l\ \forall i\ x(i) \ll L_l^*(x(i))$$

$$\forall l\ \forall i\ x(i) \ll L_l\big(x(i)\big) \to [ghc]\forall l\ \forall i\ x(i) \ll L_l^*(x(i))$$



Proof: Global Highway Control



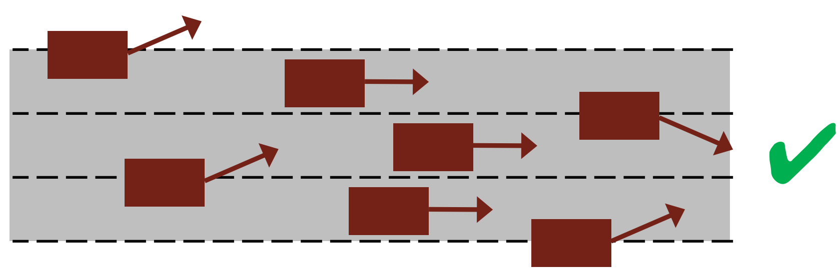
$$\forall i\ x(i) \ll L_l\big(x(i)\big) \rightarrow [lhc]\ \forall i\ x(i) \ll L_l^*\big(x(i)\big)$$

$$\forall l\ \Big(\forall i\ x(i) \ll L_l\big(x(i)\big) \rightarrow [lhc] \forall i\ x(i) \ll L_l^*\big(x(i)\big)\Big)$$

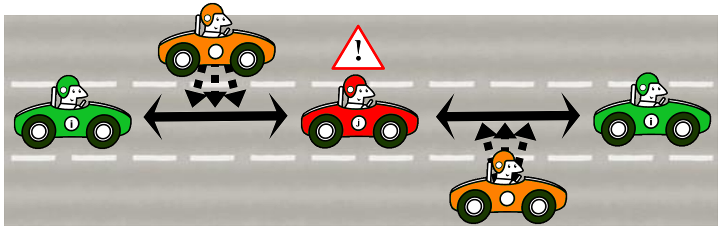
$$\forall l\ \forall i\ x(i) \ll L_l\big(x(i)\big) \rightarrow \forall l\ [lhc] \forall i\ x(i) \ll L_l^*\big(x(i)\big)$$

$$\forall l\ \forall i\ x(i) \ll L_l\big(x(i)\big) \rightarrow \big[\forall l\ (lhc)\ \ \big] \forall l\ \forall i\ x(i) \ll L_l^*(x(i))$$

$$\forall l\ \forall i\ x(i) \ll L_l\big(x(i)\big) \rightarrow [ghc] \forall l\ \forall i\ x(i) \ll L_l^*(x(i))$$



Conclusions



Challenges

- Infinite, continuous, and evolving state space, $\mathbb{R}^\infty$
- Continuous dynamics
- Discrete control decisions
- Distributed dynamics
- Arbitrary number of cars, changing over time
- Emergent behaviors

Solutions

- Quantifiers for distributed dynamics and changing number of cars
- Compositionality – using small problems to solve the big ones
- Hierarchical and modular proofs
- Variations in system design
- Future work: curved road dynamics

Thank You!

FM2011

IEEE COMPUTER SOCIETY

Reference

The full length paper for this research can be found here:

Sarah M. Loos, André Platzer, and Ligia Nistor.
Adaptive cruise control: Hybrid, distributed, and now formally verified.
In Michael Butler and Wolfram Schulte, editors, *17th International Symposium on Formal Methods, FM, Limerick, Ireland, Proceedings, LNCS.* Springer, 2011.