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
Sensor limits on actual cars are always local.
Sensor limits on actual cars are always local.
Sometimes a maneuver may look safe locally...
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

- 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 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 $\rightarrow$ [Model] Requirements
Initial Conditions $\rightarrow$ [Model] Requirements
Differential Dynamic Logic

Initial Conditions $\rightarrow$ [Model] Requirements

logical formula

logical formula
Differential Dynamic Logic

\[(x_f \leq x_\ell) \implies [\text{Model}] \quad (x_f \leq x_\ell)\]
Differential Dynamic Logic

\[(x_f \leq x_\ell) \rightarrow \text{[Model]} \quad (x_f \leq x_\ell)\]

logical formula

logical formula
Differential Dynamic Logic

\[(x_f \leq x_\ell) \rightarrow \text{[Model]} \quad (x_f \leq x_\ell)\]

- logical formula
- hybrid program
- logical formula
Differential Dynamic Logic

\[ (x_f \leq x_\ell) \rightarrow [\text{Model}] \]

- discrete control
- continuous dynamics

- logical formula
- hybrid program
- logical formula
Differential Dynamic Logic

\[
(x_f \leq x_\ell) \rightarrow [(ctrl;dyn)^*] (x_f \leq x_\ell)
\]

- discrete control
- continuous dynamics
- logical formula
- hybrid program
- logical formula
Differential Dynamic Logic

\[(x_f \leq x_\ell) \rightarrow [(\text{ctrl}; \ x' = v; \ v' = a)^* (x_f \leq x_\ell)] \]

- logical formula
- hybrid program
- logical formula
Car $f$ is safely following car $\ell$ if $(f \ll \ell)$
Car Control: Definition of Safety

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

$$(f \ll \ell) \equiv (x_f \leq x_\ell) \land (f \neq \ell) \rightarrow \left( x_f < x_\ell \land x_f + \frac{v_f^2}{2b} < x_\ell + \frac{v_\ell^2}{2B} \land v_f \geq 0 \land v_\ell \geq 0 \right)$$
Car $f$ is safely following car $\ell$ 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: $(f \ll \ell) \rightarrow [11c](f \ll \ell)$

\[
11c \equiv (ctrl; \text{dyn})^*
\]

\[
ctrl \equiv \ell_{ctrl} \parallel f_{ctrl};
\]

\[
\ell_{ctrl} \equiv (a_\ell := *; \ (-B \leq a_\ell \leq A))
\]

\[
f_{ctrl} \equiv (a_f := *; \ (-B \leq a_f \leq -b))
\]

\[
\cup (\text{Safe}_\varepsilon; \ a_f := *; \ (-B \leq a_f \leq A))
\]

\[
\cup (\text{Safe}_\varepsilon; \ a_f := 0)
\]

\[
\text{Safe}_\varepsilon \equiv x_f + \frac{v_f^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2} \varepsilon^2 + \varepsilon v_f\right) < x_\ell + \frac{v_\ell^2}{2B}
\]

\[
dyn \equiv (t := 0; \ x'_f = v_f, \ v'_f = a_f, \ x'_\ell = v_\ell, \ v'_\ell = a_\ell, t' = 1)
\]

\[
v_f \geq 0 \land v_\ell \geq 0 \land t \leq \varepsilon)
\]

Initial Conditions $\rightarrow$ [Model] Requirements
To Prove: \((f \ll \ell) \rightarrow [\llc](f \ll \ell)\)

\[
\llc = (\ctrl; \dyn)
\]

\[
\ctrl \equiv \ell_{ctrl} \parallel f_{ctrl};
\]

\[
\ell_{ctrl} \equiv (a_{\ell} := \ast; \ ?(-B \leq a_{\ell} \leq A))
\]

\[
f_{ctrl} \equiv (a_{f} := \ast; \ ?(-B \leq a_{f} \leq -b))
\]

\[
\cup (\text{Safe}_e; \ a_{f} := \ast; \ ?(-B \leq a_{f} \leq A))
\]

\[
\cup (\text{v}_f = 0; \ a_{f} := 0)
\]

\[
\text{Safe}_e \equiv x_f + \frac{v^2_f}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}e^2 + e v_f\right) < x_\ell + \frac{v^2_\ell}{2B}
\]

\[
dyn \equiv (t := 0; \ x'_f = v_f, \ v'_f = a_f, \ x'_\ell = v_\ell, \ v'_\ell = a_\ell, \ t' = 1)
\]

\[
v_f \geq 0 \land v_\ell \geq 0 \land t \leq \varepsilon)
\]
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:

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

\[ \text{glc} \equiv (\text{ctrl}^n; \text{dyn}^n)^* \]

\[ \text{ctrl}^n \equiv \forall i : C (\text{ctrl}(i)) \]

\[ \text{ctrl}(i) \equiv (a(i) \triangleright \ast; ?(-B \leq a(i) \leq -b)) \]

\[ \cup (\text{Safe}_\varepsilon(i); a(i) \triangleright \ast; ?(-B \leq a(i) \leq A)) \]

\[ \cup (\triangleright (v(i) = 0); a(i) \triangleright 0) \]

\[ \text{Safe}_\varepsilon(i) \equiv x(i) + \frac{v(i)^2}{2b} + \left( \frac{A}{b} + 1 \right) \left( \frac{A}{2} \varepsilon^2 + \varepsilon v(i) \right) < x(L(i)) + \frac{v(L(i))^2}{2B} \]

\[ \text{dyn}^n \equiv (t \triangleleft 0; \forall i : C (\text{dyn}(i)), t' = 1, t \leq \varepsilon) \]

\[ \text{dyn}(i) \equiv x'(i) = v(i), v'(i) = a(i), v(i) \geq 0 \]

Initial Conditions → [Model] Requirements
Car Control: Global Lane Control

To Prove:
\[ \forall i : C(i \ll L(i)) \rightarrow [\text{glc}](\forall i : C(i \ll L^*(i))) \]

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

Initial Conditions → [Model] Requirements
To Prove:
\[
\forall i : C(i \ll L(i)) \rightarrow [\text{glc}](\forall i : C(i \ll L^*(i)))
\]

\[
\text{glc} \equiv (\text{ctrl}^n; \text{dyn}^n)^*
\]

\[
\text{ctrl}^n \equiv \forall i : C(\text{ctrl}(i))
\]

\[
\text{ctrl}(i) \equiv (a(i) := \ast; \ ?(-B \leq a(i) \leq -b))
\]

\[
\bigcup \ (\text{Safe}_{\varepsilon}(i); \ a(i) := \ast; \ ?(-B \leq a(i) \leq A))
\]

\[
\bigcup \ (?(v(i) = 0); \ a(i) := 0)
\]

\[
\text{Safe}_{\varepsilon}(i) \equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B}
\]

\[
\text{dyn}^n \equiv (t := 0; \ \forall i : C(\text{dyn}(i)), t' = 1, t \leq \varepsilon)
\]

\[
\text{dyn}(i) \equiv x'(i) = v(i), v'(i) = a(i), v(i) \geq 0
\]
Car Control: Global Lane Control

To Prove:

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

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

Initial Conditions → [Model] Requirements
Car Control: Global Lane Control

To Prove:
\[ \forall i : C(i \ll L(i)) \rightarrow [\text{glc}](\forall i : C(i \ll L^*(i))) \]

\[ \text{glc} \equiv (\text{ctrl}^n; \text{dyn}^n)^* \]
\[ \text{ctrl}^n \equiv \forall i : C(\text{ctrl}(i)) \]
\[ \text{ctrl}(i) \equiv (a(i) := *; ?(-B \leq a(i) \leq -b)) \]
\[ \cup \ (\text{Safe}^\varepsilon(i); a(i) := *; ?(-B \leq a(i) \leq A)) \]
\[ \cup \ (?(v(i) = 0); a(i) := 0) \]
\[ \text{Safe}^\varepsilon(i) \equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(L(i)) + \frac{v(L(i))^2}{2B} \]
\[ \text{dyn}^n \equiv (t := 0; \forall i : C(\text{dyn}(i)), t' = 1, t \leq \varepsilon) \]
\[ \text{dyn}(i) \equiv x'(i) = v(i), v'(i) = a(i), v(i) \geq 0 \]

Initial Conditions \rightarrow [Model] Requirements
To Prove:

\[ \forall i : C(i \ll L(i)) \rightarrow [\text{glc}](\forall i : C(i \ll L^*(i))) \]
Transitive Leader

To Prove:

\[ \forall i : C(i \ll L(i)) \rightarrow [\text{glc}] (\forall i : C(i \ll L^*(i))) \]
To Prove:

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

To Prove:
\[ \forall i : C(i \ll L(i)) \rightarrow [\text{glc}] (\forall i : C(i \ll L^*(i))) \]
Proof: Global Lane Control

∀i x(i) ≪ x(L(i)) → [glc] ∀i x(i) ≪ x(L(i))

Safety is Transitive

∀i x(i) ≪ x(L(i)) → ∀i x(i) ≪ x(L^*(i))

[glc] ∀i x(i) ≪ x(L(i)) → [glc] ∀i x(i) ≪ x(L^*(i))

∀i x(i) ≪ x(L(i)) → [glc] ∀i x(i) ≪ x(L^*(i))
Proof: Global Lane Control

∀i x(i) \ll x(L(i)) \rightarrow [glc] ∀i x(i) \ll x(L(i))

∀i x(i) \ll x(L(i)) \rightarrow ∀i x(i) \ll x(L^*(i))

[glc] ∀i x(i) \ll x(L(i)) \rightarrow [glc] ∀i x(i) \ll x(L^*(i))

∀i x(i) \ll x(L(i)) \rightarrow [glc] ∀i x(i) \ll x(L^*(i))

=cut

(l| gen)
Proof: Global Lane Control

∀i x(i) ≪ x(L(i)) → [glc] ∀i x(i) ≪ x(L(i))

∀i x(i) ≪ x(L(i)) → ∀i x(i) ≪ x(L*(i))

[glc] ∀i x(i) ≪ x(L(i)) → [glc] ∀i x(i) ≪ x(L*(i))

∀i x(i) ≪ x(L(i)) → [glc] ∀i x(i) ≪ x(L*(i))
Car Control: Local Highway Control

Local Lane Control

<table>
<thead>
<tr>
<th>2 vehicles</th>
<th>n vehicles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 lane</td>
<td>1 lane</td>
</tr>
<tr>
<td>no lane change</td>
<td>no lane change</td>
</tr>
</tbody>
</table>

Global Lane Control

Local Highway Control

<table>
<thead>
<tr>
<th>n vehicles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 lane</td>
</tr>
<tr>
<td>lane changes</td>
</tr>
</tbody>
</table>

Global Highway Control

<table>
<thead>
<tr>
<th>n vehicles</th>
</tr>
</thead>
<tbody>
<tr>
<td>m lanes</td>
</tr>
<tr>
<td>lane changes</td>
</tr>
</tbody>
</table>
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
To Prove:

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

\[ \text{lhc} \equiv (\text{delete}^*; \text{create}^*; \text{ctrl}^n; \text{dyn}^n)^* \]

\[ \text{create} \equiv n := \text{new}; \ ?((F(n) \ll n) \land (n \ll L(n))) \]

\[ (n := \text{new}) \equiv n := \_; \ ?(E(n) = 0); \ E(n) := 1 \]

\[ (F(n) \ll n) \equiv \forall j : C \ (L(j) = n \rightarrow (j \ll n)) \]

\[ \text{delete} \equiv n := \_; \ ?(E(n) = 1); \ E(n) := 0 \]

Initial Conditions → [Model] Requirements
To Prove:
\[ \forall i : C(i \ll L(i)) \rightarrow [\text{lhc}] \forall i : C(i \ll L^*(i)) \]

\[ \text{lhc} \equiv (\text{delete}^*; \text{create}^*; \text{ctrl}^n; \text{dyn}^n)^* \]

\[ \text{create} \equiv n := \text{new}; ?((F(n) \ll n) \land (n \ll L(n))) \]

\[ (n := \text{new}) \equiv n := *; ?(E(n) = 0); E(n) := 1 \]

\[ (F(n) \ll n) \equiv \forall j : C (L(j) = n \rightarrow (j \ll n)) \]

\[ \text{delete} \equiv n := *; ?(E(n) = 1); E(n) := 0 \]

Initial Conditions → [Model] Requirements
Proof: Local Highway Control

∀i \ x(i) \ll L(x(i)) \rightarrow [create^*]∀i \ x(i) \ll L^*(x(i))

Transitivity

∀i \ x(i) \ll L(x(i)) \rightarrow [delete^*]∀i \ x(i) \ll L^*(x(i))

Transitivity

∀i \ x(i) \ll L(x(i)) \rightarrow [delete^*][create^*][glc]∀i \ x(i) \ll L^*(x(i))

∀i \ x(i) \ll L(x(i)) \rightarrow [lhc]∀i \ x(i) \ll L^*(x(i))

([i] split) (|[;])
Proof: Local Highway Control

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

Transitivity

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

Transitivity

\[ \forall i \ x(i) \ll L(x(i)) \rightarrow [delete^*][create^*][glc] \forall i \ x(i) \ll L^*(x(i)) \]

([] split) ([;])

\[ \forall i \ x(i) \ll L(x(i)) \rightarrow [lhc] \forall i \ x(i) \ll L^*(x(i)) \]
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
To Prove:

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

\[ \text{ghc} \triangleq (\forall l : L \text{ delete}_i^*; \ \forall l : L \text{ new}_i^*; \ \forall l : L \text{ ctrl}_i^n; \ \forall l : L \text{ dyn}_i^n)^* \]
Car Control: Global Highway Control

To Prove:

\[ (\forall l : L \not\exists i : C_l(i \ll L_l(i)) \rightarrow [\text{ghc}] \ \forall l : L \forall i : C_l(i \ll L^*_l(i)) \]

\[
\text{ghc} := (\forall l : L \text{delete}^*_l; \ \forall l : L \text{new}^*_l; \ \forall l : L \text{ctrl}^n_l; \ \forall l : L \text{dyn}^n_l)^*
\]

Initial Conditions → [Model] Requirements
Proof: Global Highway Control

\[ \forall i \ x(i) \ll L_i(x(i)) \rightarrow [lhc] \forall i \ x(i) \ll L_i^*(x(i)) \]

\[ \forall \ l \ \left( \forall i \ x(i) \ll L_i(x(i)) \rightarrow [lhc] \forall i \ x(i) \ll L_i^*(x(i)) \right) \]

\[ \forall \ l \ \forall i \ x(i) \ll L_i(x(i)) \rightarrow \forall \ [lhc] \forall i \ x(i) \ll L_i^*(x(i)) \]

\[ \forall \ l \ \forall i \ x(i) \ll L_i(x(i)) \rightarrow [\forall \ (lhc)] \forall i \ x(i) \ll L_i^*(x(i)) \]

\[ \forall \ l \ \forall i \ x(i) \ll L_i(x(i)) \rightarrow [ghc] \forall i \ x(i) \ll L_i^*(x(i)) \]
Proof: Global Highway Control

∀i x(i) ≪ L_l(x(i)) → [lhc] ∀i x(i) ≪ L^*_l(x(i))

∀l (∀i x(i) ≪ L_l(x(i)) → [lhc] ∀i x(i) ≪ L^*_l(x(i)))

∀l ∀i x(i) ≪ L_l(x(i)) → ∀l [lhc] ∀i x(i) ≪ L^*_l(x(i))

∀l ∀i x(i) ≪ L_l(x(i)) → [∀ (lhc)] ∀l ∀i x(i) ≪ L^*_l(x(i))

∀l ∀i x(i) ≪ L_l(x(i)) → [ghc] ∀l ∀i x(i) ≪ 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!
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.