Proving Safety of Traffic Manoeuvres on Country Roads

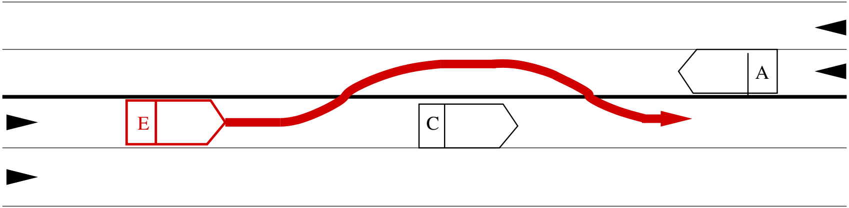
Martin Hilscher, Sven Linker, Ernst-Rüdiger Olderog

Department of Computing Science, University of Oldenburg

September 2013

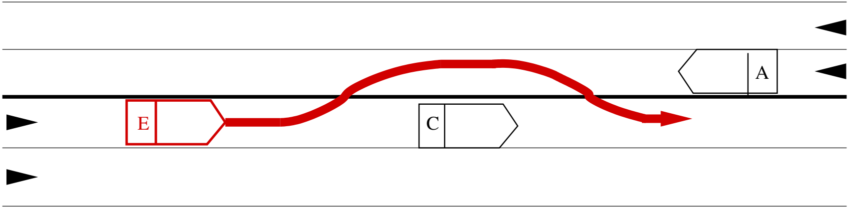
The Challenge

Prove safety (collision freedom) of
traffic on country roads including overtaking:



The Challenge

Prove safety (collision freedom) of
traffic on country roads including overtaking:



Hybrid system verification problem:

car dynamics + car controller(s) + assumptions $\models$ safety

Our Approach

Abstract model of multi-lane road traffic
based on spatial properties hiding car dynamics.

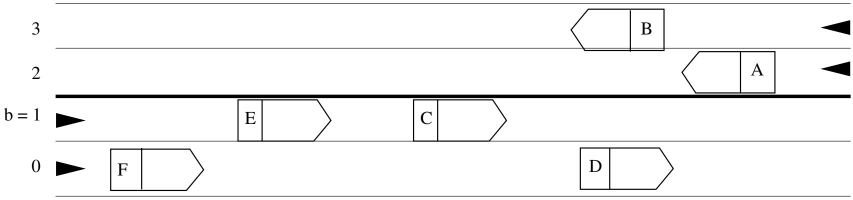
Our Approach

Abstract model of multi-lane road traffic
based on spatial properties hiding car dynamics.

Properties expressed in a Multi-Lane Spatial Logic inspired by:

- Moszkowski's interval temporal logic [Mos85]
- Zhou, Hoare and Ravn's Duration Calculus [ZHR91]
- Schäfer's Shape Calculus [Sch07]

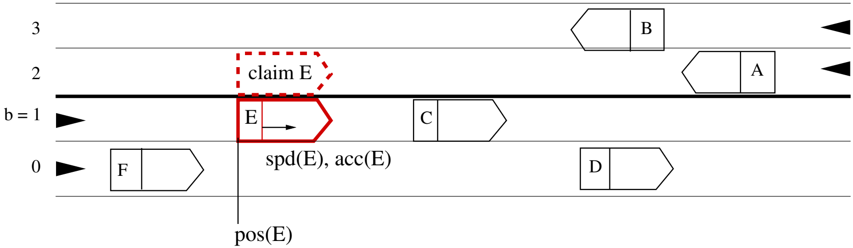
Model



Preliminaries:

- Car identifiers globally unique: $A, B, \ldots$
  Set of all car identifiers: $\mathbb{I}$
- Infinite road ($\mathbb{R}$)
- Lanes: $\mathbb{L} = \{0, \ldots, N\}$
  Border: $b \in \mathbb{L}$

Model



A traffic snapshot is a structure $\mathcal{TS} = (res, clm, pos, spd, acc)$, where

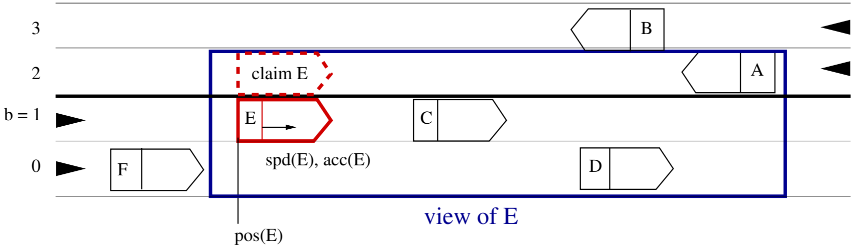
- $res : \mathbb{I} \to \mathcal{P}(\mathbb{L})$ reserved lanes,
- $clm : \mathbb{I} \to \mathcal{P}(\mathbb{L})$ claimed lanes,
- $pos : \mathbb{I} \to \mathbb{R}$ car positions,
- $spd : \mathbb{I} \to \mathbb{R}$ current speeds,
- $acc : \mathbb{I} \to \mathbb{R}$ current accelerations.

Transitions

$\mathcal{TS} \xrightarrow{\alpha} \mathcal{TS}'$ for an action α of the following type:

$\mathcal{TS} \xrightarrow{t} \mathcal{TS}'$	time passes
$\mathcal{TS} \xrightarrow{\mathsf{acc}(C,a)} \mathcal{TS}'$	accelerate
$\mathcal{TS} \xrightarrow{\mathsf{c}(C,n)} \mathcal{TS}'$	claim
$\mathcal{TS} \xrightarrow{\mathsf{wd\ c}(C)} \mathcal{TS}'$	withdraw claim
$\mathcal{TS} \xrightarrow{\mathsf{r}(C)} \mathcal{TS}'$	reserve
$\mathcal{TS} \xrightarrow{\mathsf{wd\ r}(C,n)} \mathcal{TS}'$	withdraw reservation

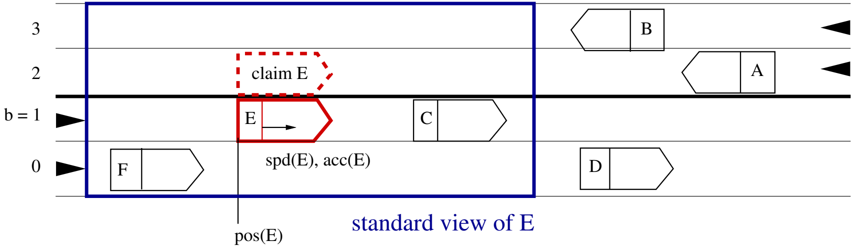
Local View



View $V = (L, X, E)$, where

- $L = [m, n]$ subinterval of $\mathbb{L}$,
- $X = [r, t]$ subinterval of $\mathbb{R}$,
- $E \in \mathbb{I}$ identifier of car under consideration.

Local View

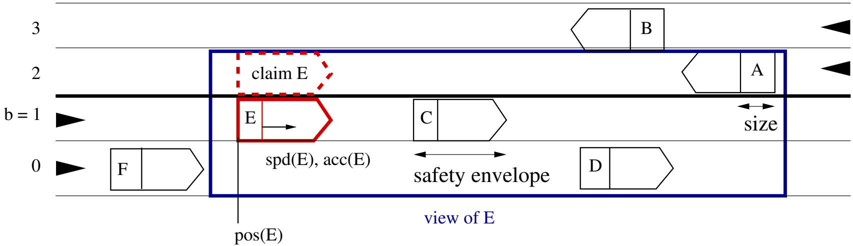


Standard view $V_s = (L, X, E)$, where

- $L = \mathbb{L}$,
- $X = [pos(E) - h, pos(E) + h]$,
- $E \in \mathbb{I}$,

and h is the horizon.

Sensor Function



Sensor function covering directions:

$$\Omega_E : \mathbb{I} \times \mathbb{TS} \to \mathbb{R}$$

e.g., perfect knowledge

$$\Omega_E(I, \mathcal{TS}) \equiv se(I, \mathcal{TS}).$$

Syntax: MLSL + ℓ

Multi-Lane Spatial Logic with length measurements:

- Car variables: c, d, special variable ego
- Real variables: x, y

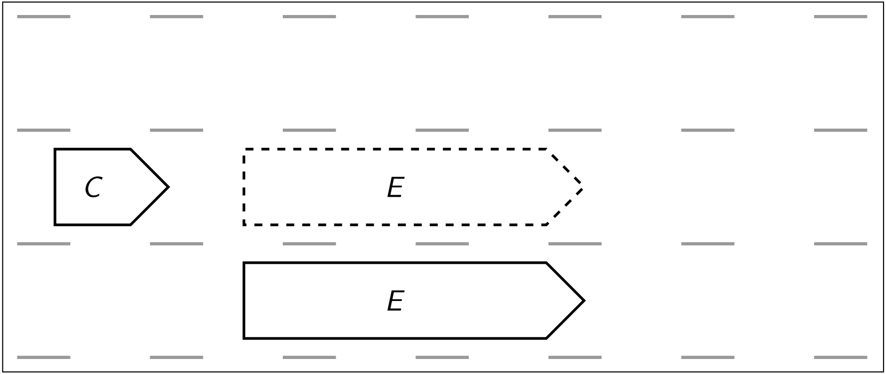
Real-valued terms θ

$$\theta ::= r \mid x \mid f(c_1, \ldots, c_n) \mid g(\theta_1, \ldots, \theta_n),$$

Formulae ϕ

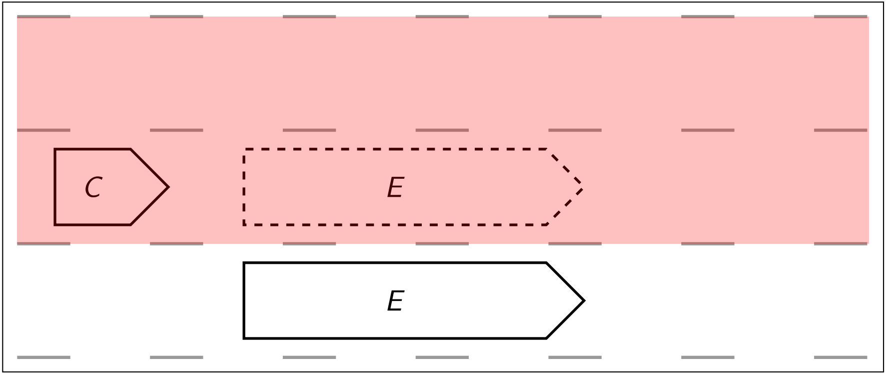
$$\begin{aligned} \phi ::= \; & \mathit{true} \mid c = d \mid \ell = \theta \mid \mathit{free} \mid \mathit{re}(c) \mid \mathit{cl}(c) && (\mathit{Atoms}) \\ & \mid \phi_1 \land \phi_2 \mid \neg \phi_1 \mid \exists c \colon \phi_1 && (\mathit{FOL}) \\ & \mid \phi_1 \frown \phi_2 \mid \begin{matrix} \phi_2 \\ \phi_1 \end{matrix} && (\mathit{Spatial}) \end{aligned}$$

Semantics



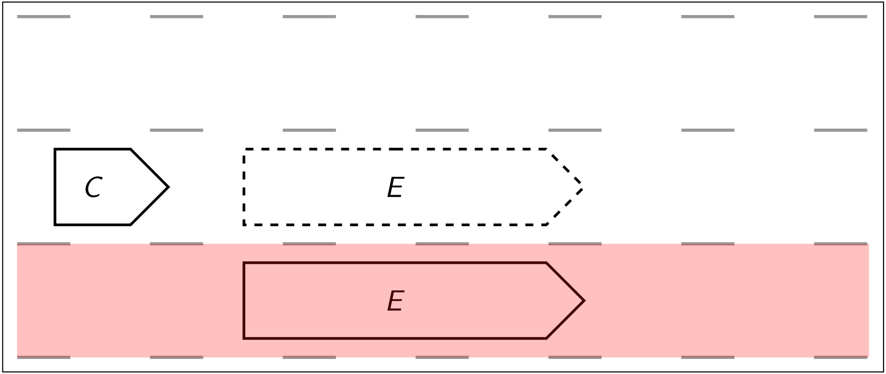
$$\phi \equiv \begin{pmatrix} \mathit{true} \\ \mathit{free} \frown \mathit{re}(\mathrm{ego}) \frown \mathit{free} \end{pmatrix}$$

Semantics



$$\phi \equiv \begin{pmatrix} \color{red}{\mathit{true}} \\ \mathit{free} \frown \mathit{re}(\mathrm{ego}) \frown \mathit{free} \end{pmatrix}$$

Semantics



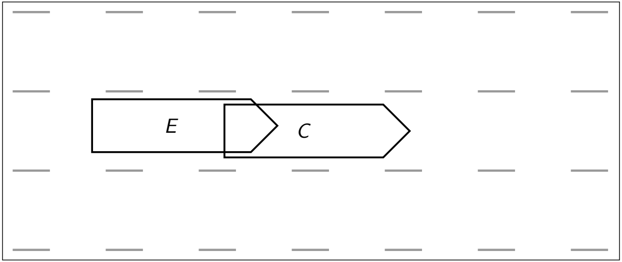
$$\phi \equiv \begin{pmatrix} \mathit{true} \\ \mathit{free} \frown \mathit{re}(\mathrm{ego}) \frown \mathit{free} \end{pmatrix}$$

Example: Collision Check

Somewhere: $\langle \phi \rangle \equiv true \frown \begin{pmatrix} true \\ \phi \\ true \end{pmatrix} \frown true$

Example: Collision Check

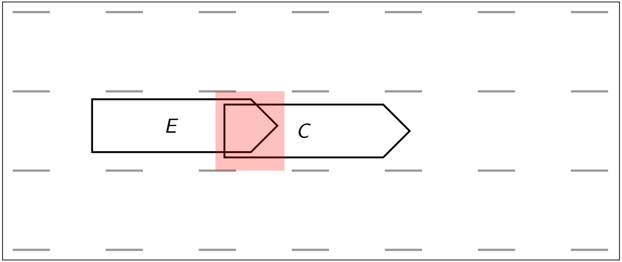
Somewhere: $$\langle \phi \rangle \equiv \mathit{true} \frown \begin{pmatrix} \mathit{true} \\ \phi \\ \mathit{true} \end{pmatrix} \frown \mathit{true}$$



$$\langle re(\mathrm{ego}) \land re(c) \rangle$$

Example: Collision Check

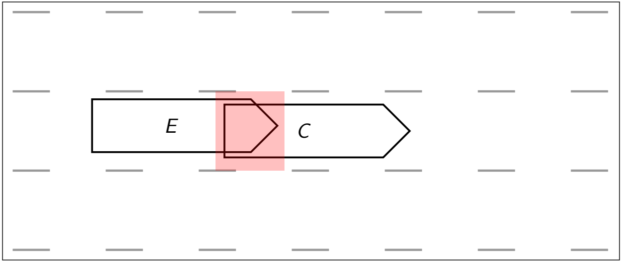
Somewhere: $\langle \phi \rangle \equiv \mathit{true} \frown \begin{pmatrix} \mathit{true} \\ \phi \\ \mathit{true} \end{pmatrix} \frown \mathit{true}$



$$\langle re(\mathrm{ego}) \wedge re(c) \rangle$$

Example: Collision Check

Somewhere: $\langle \phi \rangle \equiv \mathit{true} \frown \begin{pmatrix} \mathit{true} \\ \phi \\ \mathit{true} \end{pmatrix} \frown \mathit{true}$

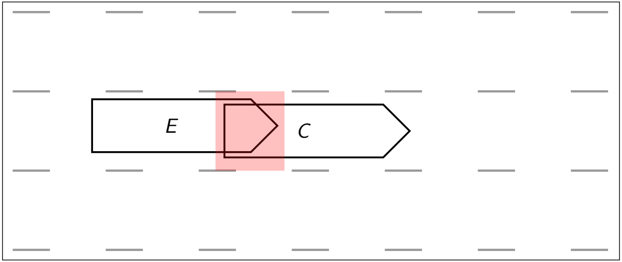


$$\langle re(\mathrm{ego}) \land re(c) \rangle$$

$$cc \equiv \exists c \colon c \neq \mathrm{ego} \land \langle re(\mathrm{ego}) \land re(c) \rangle$$

Example: Collision Check

Somewhere: $$\langle \phi \rangle \equiv \mathit{true} \frown \begin{pmatrix} \mathit{true} \\ \phi \\ \mathit{true} \end{pmatrix} \frown \mathit{true}$$



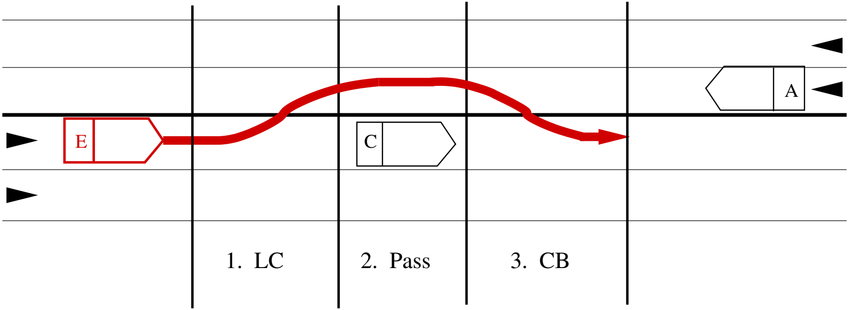
$$cc \equiv \exists c \colon c \neq \mathrm{ego} \land \langle re(\mathrm{ego}) \land re(c) \rangle$$

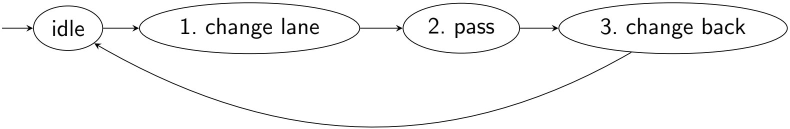
Safety from ego's perspective: $\neg cc$

Controller: General Idea

- Perfect knowledge, i.e.,
  sensors return full safety envelopes of all cars
- Instantaneous broadcast communication
- Timed automaton with data variables:
  - variable n: original lane,
  - variable ℓ: target lane,
  - clock x,
  - guards and invariants:
    MLSL formulae and clock/data constraints,
  - actions:
    transitions of cars, clock/data updates.

Protocol for Overtaking





Aim: Safety of Overtaking

A traffic snapshot safe if it satisfies

$$Safe \equiv \forall c, d : c \neq d \Rightarrow \neg \langle re(c) \wedge re(d) \rangle .$$

Aim: Safety of Overtaking

A traffic snapshot safe if it satisfies

$$Safe \equiv \forall c, d : c \neq d \Rightarrow \neg \langle re(c) \wedge re(d) \rangle .$$

Assumptions:

A1. There is an initial safe traffic snapshot.

A2. Every car C is equipped with a distance controller.

A3. Every car is equipped with a contoller implementing the protocol for overtaking.

A4. The horizon in the standard view is sufficiently large.

Aim: Safety of Overtaking

A traffic snapshot safe if it satisfies

$$Safe \equiv \forall c, d : c \neq d \Rightarrow \neg \langle re(c) \wedge re(d) \rangle \,.$$

Assumptions:

A1. There is an initial safe traffic snapshot.

A2. Every car C is equipped with a distance controller.

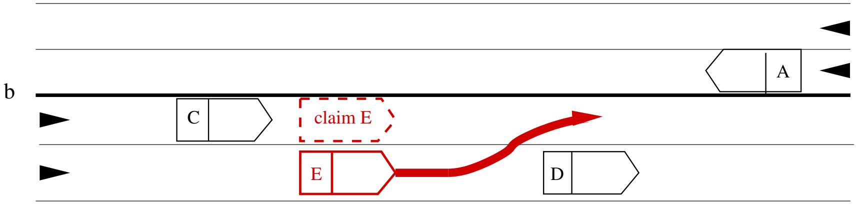
A3. Every car is equipped with a contoller implementing the protocol for overtaking.

A4. The horizon in the standard view is sufficiently large.

Safety of Overtaking

Under the assumptions A1 to A4,
the protocol specifying the overtaking procedure is safe.

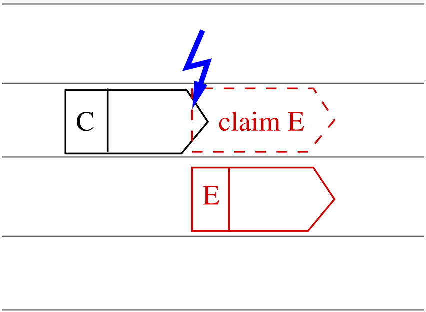
Lane Change on Non-Borders



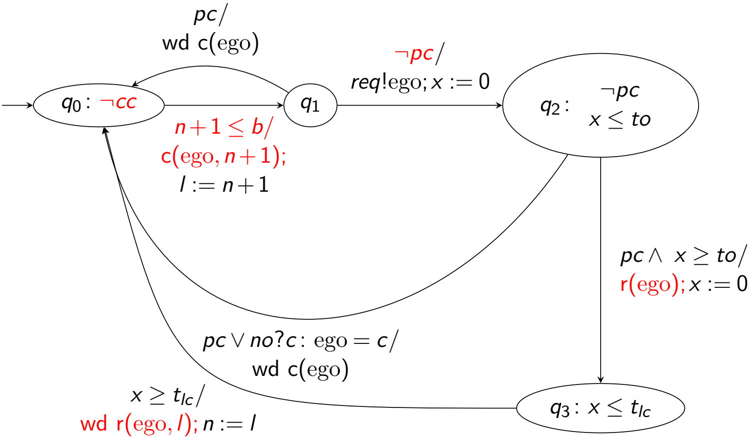
Relevant traffic in one direction as on motorways: [HLOR11]

Lane Change on Non-Borders

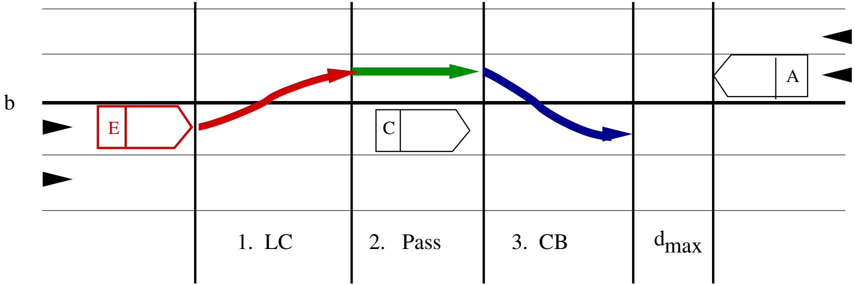
- Potential collision: $pc \equiv \exists c : c \neq \mathrm{ego} \land \langle re(c) \land cl(\mathrm{ego}) \rangle$



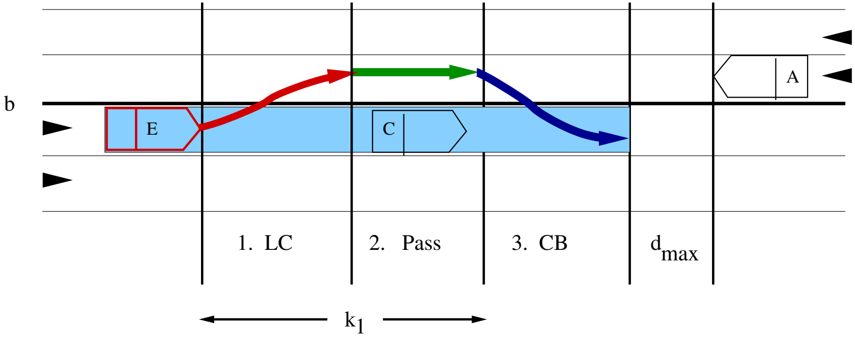
Lane Change on Non-Borders



Lane Change into Opposing Traffic



Lane Change into Opposing Traffic

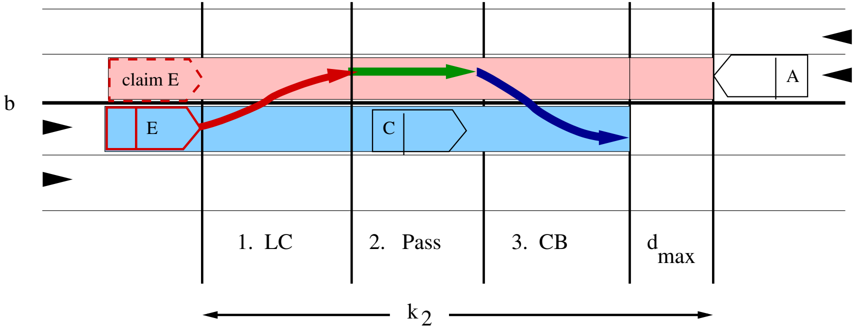


- Enough space on original lane:

$$esol(c) \;\equiv\; \langle re(\mathrm{ego}) \frown (free \frown re(c) \frown free)^{k_1} \frown free^{d_{lcb}} \rangle$$

where $\phi^{\theta} \;\equiv\; \phi \wedge \ell = \theta$.

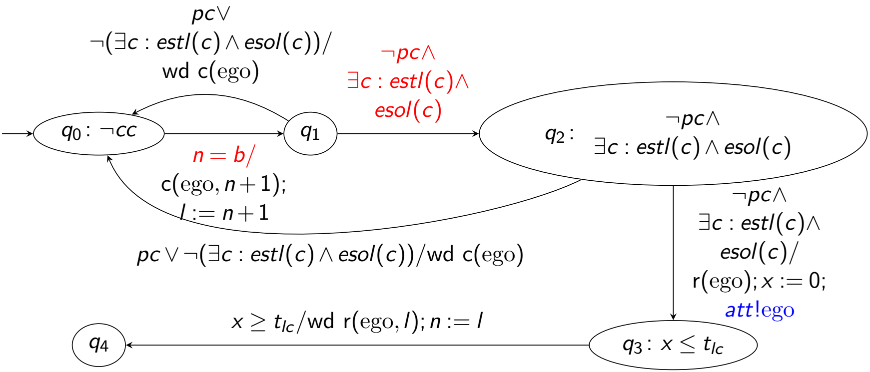
Lane Change into Opposing Traffic



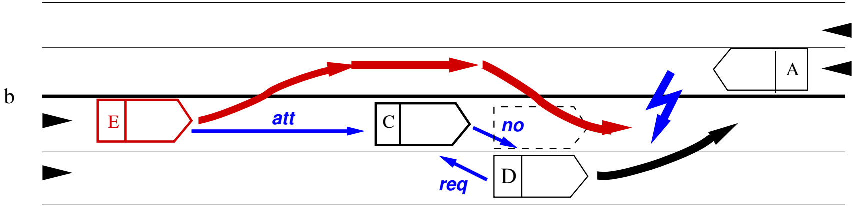
- Enough space on target lane:

$$estl(c) \equiv \langle cl(\mathrm{ego}) \frown free^{k_2} \rangle$$

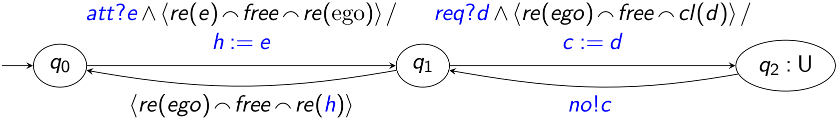
Lane Change into Opposing Traffic



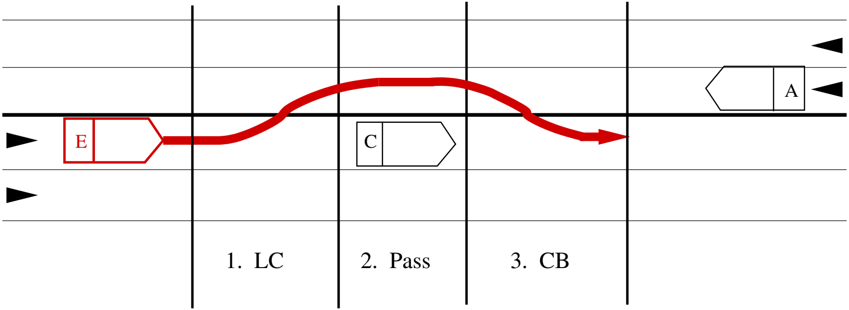
Additional Helper Controller



Inside car C in the role of ego:



Pass and Change Back



Simple controllers for phases 2 and 3

Safety of Overtaking

A traffic snapshot $\mathcal{TS}$ safe if it satisfies

$$Safe \equiv \forall c, d : c \neq d \Rightarrow \neg \langle re(c) \wedge re(d) \rangle .$$

Assumptions:

A1. There is an initial safe traffic snapshot $\mathcal{TS}_0$.

A2. Every car C is equipped with a distance controller that keeps *Safe* invariant under time and accelaration transitions.

A3. Every car is equipped with a contoller implementing the protocol for overtaking.

A4. The horizon in the standard view is $h = se_{max} + 2 \cdot d_{max}$.

Theorem (Safety of Overtaking)

Under the assumptions A1 to A4,
the protocol specifying the overtaking procedure is safe.

Theorem (Safety of Overtaking)

Under the assumptions A1 to A4, the protocol specifying the overtaking procedure is safe.

Proof idea.

We show that every traffic snapshot $\mathcal{TS}$ that is reachable from $\mathcal{TS}_0$ by time and acceleration transitions and transitions allowed by the controller implementing the overtaking protocol is safe.

Future and Further Work

- Here: perfect knowledge

  Next: limited sensor functions, where
  each car E sees own safety envelope and the size of other cars:

  $$\Omega_E(I, \mathcal{TS}) \equiv \text{if } I = E \text{ then } se(I, \mathcal{TS}) \text{ else } size(I) \text{ fi}.$$

  Done for motorways in [HLOR11].

- Link to car dynamics

- Proof theory of MLSL: see [LH13] at ICTAC 2013, towards automatic verification

- Visual specification: S. Linker

Related Work

California PATH project: car platoons including lane change

- Lygeros et al. [LGS98]: sketch of safety proof taking car dynamics into accout, admitting *safe collisions*.

Lane Change Manoeuvres

- Platzer et al. [LPN11]: Quantified differential dynamic Logic QdL expresses car dynamics and creation of new cars.

Controller design for hybrid systems

- Raisch et al. [MRD03]: abstraction and refinement for hierarchical design of hybrid control systems.
- Van Schuppen et al. [HCvS06]: synthesis of control laws for piecewise-affine hybrid systems based on simplices.

References

L. C. G. J. M. Habets, P.J. Collins, and J.H. van Schuppen.
Reachability and control synthesis for piecewise-affine hybrid systems on simplices.
IEEE Trans. on Automatic Control, 51(6):938–948, June 2006.

Jifeng He, C. A. R. Hoare, M. Fränzle, M. Müller-Olm, E.-R. Olderog, M. Schenke, M. R. Hansen, A. P. Ravn, and H. Rischel.
Provably correct systems.
In H. Langmaack, W. P. de Roever, and J. Vytopil, editors, *FTRTFT*, volume 863 of *LNCS*, pages 288–335. Springer, 1994.

M. Hilscher, S. Linker, E.-R. Olderog, and A.P. Ravn.
An abstract model for proving safety of multi-lane traffic manoeuvres.
In Shengchao Qin and Zongyan Qiu, editors, *Int'l Conf. on Formal Engineering Methods (ICFEM)*, volume 6991 of *LNCS*, pages 404–409. Springer, 2011.

J. Lygeros, D. N. Godbole, and S. S. Sastry.
Verified hybrid controllers for automated vehicles.
IEEE Transactions on Automatic Control, 43(4):522–539, 1998.

S. Linker and M. Hilscher.
Proof theory of a multi-lane spatial logic.
In Zhiming Liu, Jim Woodcock, and Huibiao Zhu, editors, *Int'l Conf. on Theoret. Aspects of Comput. (ICTAC)*, volume 8049 of *LNCS*, pages 231–248. Springer, 2013.

S. M. Loos, A. Platzer, and L. Nistor.
Adaptive cruise control: Hybrid, distributed, and now formally verified.
In M. Butler and W. Schulte, editors, *FM 2011: Formal Methods*, volume 6664 of *LNCS*, pages 42–56. Springer, 2011.

B. Moszkowski.
A temporal logic for multilevel reasoning about hardware.
Computer, 18(2):10–19, 1985.

T. Moor, J. Raisch, and J.M Davoren.
Admissiblity criteria for a hierarchical design of hybrid systems.
In *Proc. IFAD Conf. on Analysis and Design of Hybrid Systems*, pages 389–394, St. Malo, France, 2003.

A. Schäfer.
Axiomatisation and decidability of multi-dimensional duration calculus.
Information and Computation, 205:25–64, 2007.

C. Zhou, C.A.R. Hoare, and A.P. Ravn.
A calculus of durations.
Information Processing Letters, 40(5):269–276, 1991.