Space for Traffic Manoeuvres

Ernst-Rüdiger Olderog

Department of Computing Science, University of Oldenburg

IFIP WG 2.2 Meeting in Bordeaux, September 2017

CARL VON OSSIETZKY universität OLDENBURG

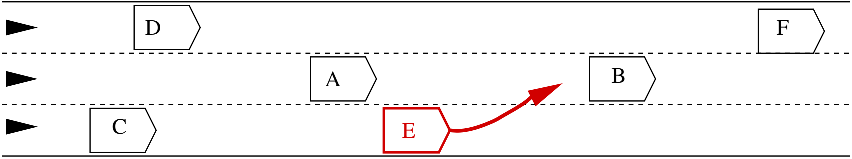
The Challenge

Prove safety (collision freedom) of
traffic manoeuvres on different types of roads.

The Challenge

Prove safety (collision freedom) of
traffic manoeuvres on different types of roads.

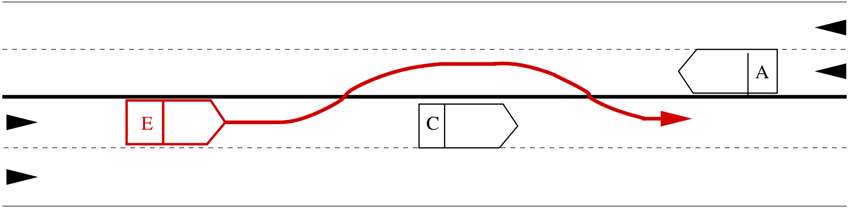
motorways [HLOR11]:



The Challenge

Prove safety (collision freedom) of
traffic manoeuvres on different types of roads.

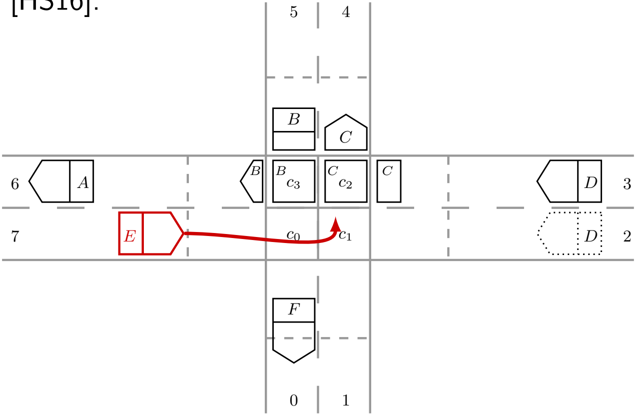
country roads [HLO13]:



The Challenge

Prove safety (collision freedom) of
traffic manoeuvres on different types of roads.

crossings [HS16]:



Our Approach [HLOR11]

Safety is hybrid system verification problem:

$$\text{car dynamics} + \text{car controllers} + \text{assumptions} \models \text{safety}$$

Our Approach [HLOR11]

Safety is hybrid system verification problem:

car dynamics + car controllers + assumptions $\models$ safety

Collision freedom is a spatial property.

Our approach is based on

spatial logic + abstract controllers

hiding car dynamics.

Our Approach [HLOR11]

Safety is hybrid system verification problem:

$$\text{car dynamics} + \text{car controllers} + \text{assumptions} \models \text{safety}$$

Collision freedom is a spatial property.

Our approach is based on

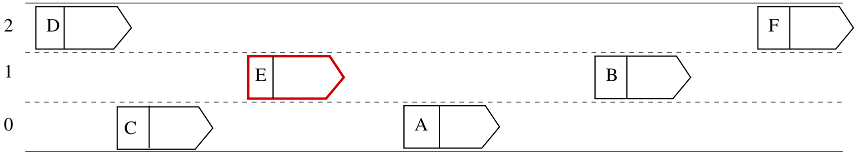
$$\text{spatial logic} + \text{abstract controllers}$$

hiding car dynamics.

Dedicated Multi-Lane Spatial Logic inspired by work in ProCoS:

- Moszkowski's interval temporal logic
- Zhou, Hoare and Ravn's Duration Calculus

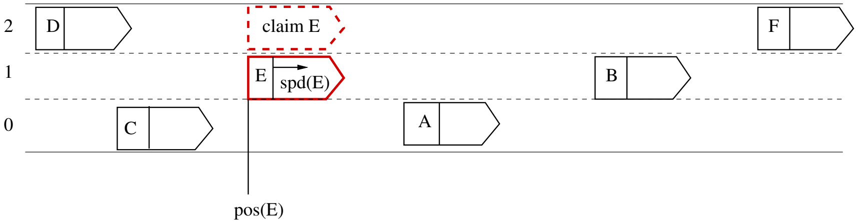
Model



Preliminaries:

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

Model



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

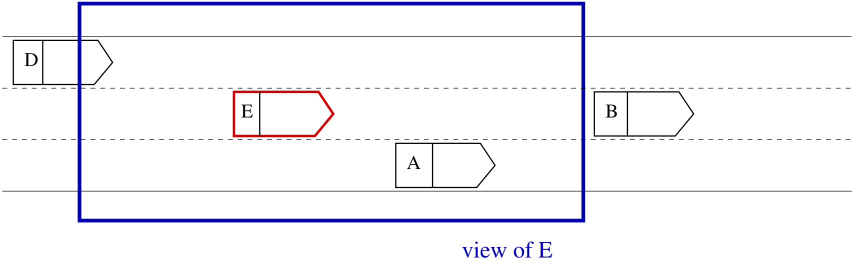
- $pos : \mathbb{I} \to \mathbb{R}$ car positions,
- $spd : \mathbb{I} \to \mathbb{R}$ current speeds,
- $res : \mathbb{I} \to \mathcal{P}(\mathbb{L})$ reserved lanes,
- $clm : \mathbb{I} \to \mathcal{P}(\mathbb{L})$ claimed lanes.

Transitions

$\mathcal{T} \xrightarrow{\alpha} \mathcal{T}'$ for an action α of the following type:

$\mathcal{T} \xrightarrow{t} \mathcal{T}'$	time passes
$\mathcal{T} \xrightarrow{\mathsf{c}(C,n)} \mathcal{T}'$	claim
$\mathcal{T} \xrightarrow{\mathsf{wd\_c}(C)} \mathcal{T}'$	withdraw claim
$\mathcal{T} \xrightarrow{\mathsf{r}(C)} \mathcal{T}'$	reserve
$\mathcal{T} \xrightarrow{\mathsf{wd\_r}(C,n)} \mathcal{T}'$	withdraw reservation

Local View



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

- L subinterval of $\mathbb{L}$,
- X subinterval of $\mathbb{R}$,
- $E \in \mathbb{I}$ identifier of car under consideration.

MLSL: Syntax

Multi-Lane Spatial Logic (basic form)

Car variables: c, d, special variable ego

Formulae ϕ

$$\phi ::= \mathit{true} \mid c = d \mid \mathit{free} \mid \mathit{re}(c) \mid \mathit{cl}(c) \qquad (\mathit{Atoms})$$

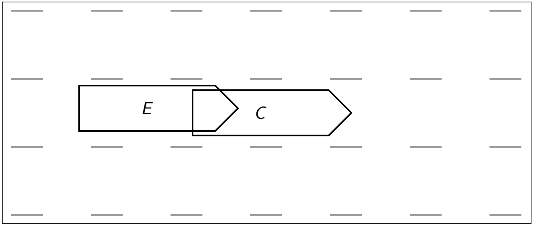
$$\mid \phi_1 \wedge \phi_2 \mid \neg \phi_1 \mid \exists c \colon \phi_1 \qquad (\mathit{FOL})$$

$$\mid \phi_1 \frown \phi_2 \mid \begin{matrix} \phi_2 \\ \phi_1 \end{matrix} \qquad (\mathit{Spatial})$$

MLSL: Semantics

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

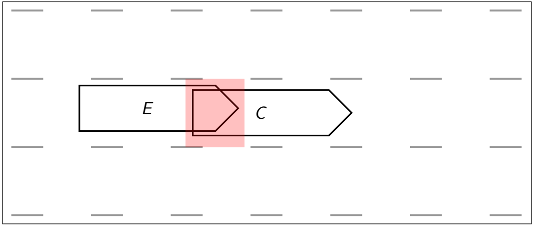
Example: Collision check



MLSL: Semantics

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

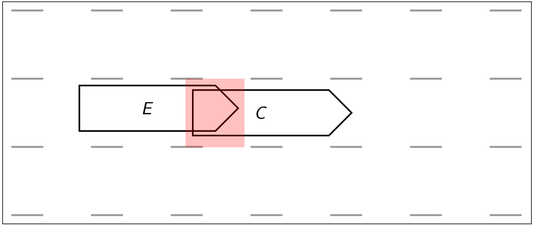
Example: Collision check



MLSL: Semantics

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

Example: Collision check

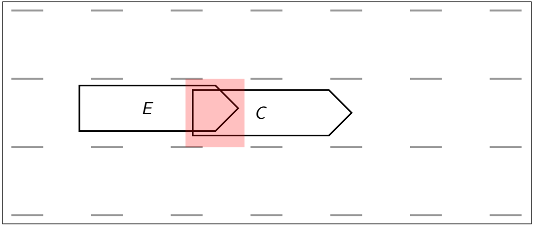


$$\langle re(\text{ego}) \land re(c) \rangle$$

MLSL: Semantics

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

Example: Collision check



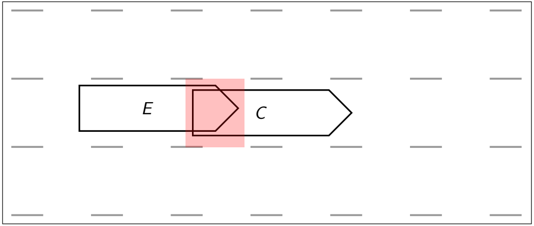
$$\langle re(\text{ego}) \land re(c) \rangle$$

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

MLSL: Semantics

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

Example: Collision check



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

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

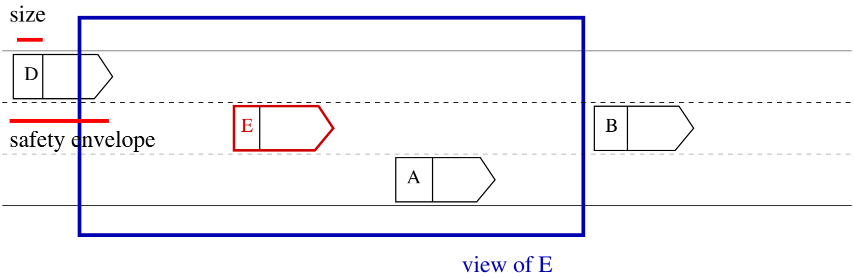
Controller

- Automotive Controlling Timed Automata (ACTA) with data variables:
  - guards and invariants:

    MLSL formulae and clock/data constraints,
  - actions:

    transitions of cars, clock/data updates.

Controller: Sensor Function

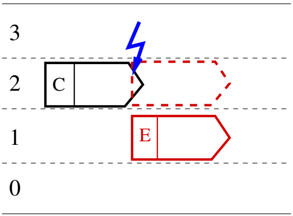


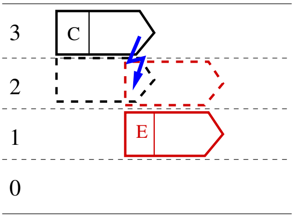
Sensor function describes what a car E can see of other cars.

We assume perfect knowledge: E sees the full safety envelope.

Controller LCP: Lane Change Perfect Knowledge

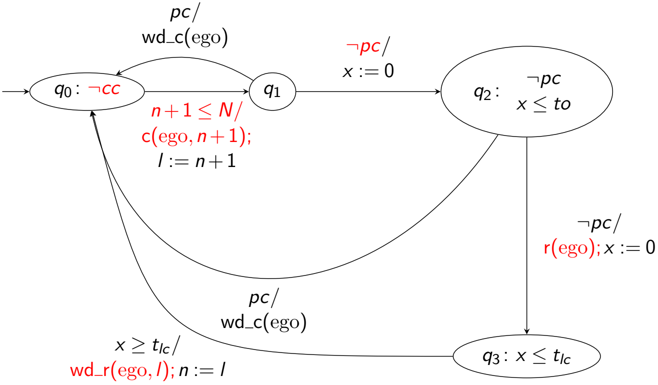
Potential collision: $pc \equiv \exists c : c \neq \mathrm{ego} \land \langle cl(\mathrm{ego}) \land (re(c) \lor cl(c))\rangle$





Controller LCP: Lane Change Perfect Knowledge

- q_0: driving: no collision
- q_1: claiming new lane
- q_2: checking for potential collisions
- q_3: reserving new lane and changing lanes
- q_0: withdrawing reservation of old lane



Safety of LCP

A traffic snapshot safe if it satisfies

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

Safety of LCP

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 E has a distance controller DC keeping

$$\neg cc \equiv \neg \exists c : c \neq \mathrm{ego} \wedge \langle re(\mathrm{ego}) \wedge re(c) \rangle$$

invariant under time transitions

A3. Every car E is equipped with the controller LCP.

Safety of LCP

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 E has a distance controller DC keeping

$$\neg cc \equiv \neg \exists c : c \neq \mathrm{ego} \wedge \langle re(\mathrm{ego}) \wedge re(c) \rangle$$

invariant under time transitions

A3. Every car E is equipped with the controller LCP.

Theorem

Under the assumptions A1 to A3,
every reachable traffic snapshot is safe.

Linking Spatial and Dynamic Model [ORW17]

- Spatial model using MLSL formulae built up from atoms like

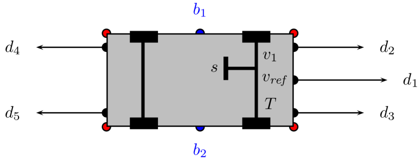
$$free, re(c), cl(c)$$

- Dynamic model built up from

  differential equations for car dynamics

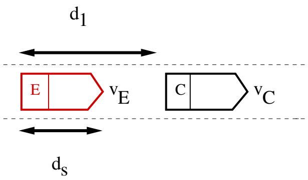
  and

  sensors and actuators of the cars:



Concrete Dynamic Model

Car E follows car C:



Differential equations of the motion of car E:

$$\dot{d}_1(t) = v_C(t) - v_E(t)$$
$$\dot{v}_E(t) = -a(d_1(t), v_C(t))\, v_E(t)^2 + u(t),$$

where $u(t) \in [\underline{u}, \overline{u}]$ and a is an auxiliary function.

Safety distance d_s of car E with initial velocity v_E^0 can be calculated from these equations.

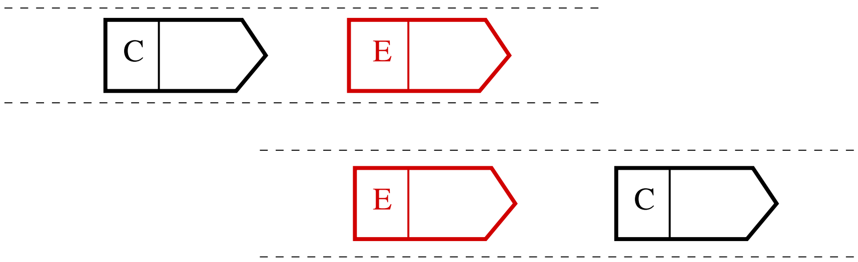
Linking: Distance Controller DC

DC keeps “no collision”

$$\neg cc \;\equiv\; \neg\exists c : c \neq \mathrm{ego} \wedge \langle re(\mathrm{ego}) \wedge re(c)\rangle$$

invariant under time transitions.

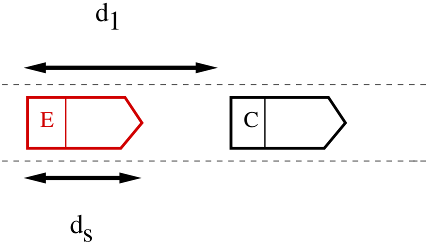
“No collision” is symmetric:



Linking: Distance Controller DC

"No collision forward":

$$\neg ccf \equiv \neg\exists c : c \neq \mathrm{ego} \land \langle re(\mathrm{ego}) \land re(c)\rangle \land \langle c \ ahead \ \mathrm{ego}\rangle$$



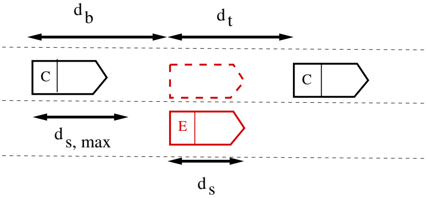
Linking predicate:

$$\neg ccf \Leftarrow d_s < d_1.$$

Linking: Lane-Change Controller LPC

"No potential collision": $\neg\exists c : c \neq \text{ego} \wedge \langle cl(\text{ego}) \wedge (re(c) \vee cl(c))\rangle$

Case 1 : $\phi_{re} \equiv \neg\exists c : c \neq \text{ego} \wedge \langle cl(\text{ego}) \wedge re(c)\rangle$



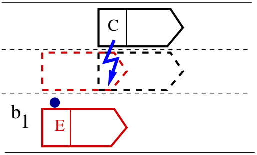
Linking predicate:

$$\phi_{re} \Leftarrow d_s < d_t \wedge d_{s,max} < d_b.$$

Linking: Lane-Change Controller LPC

"No potential collision": $\neg\exists c : c \neq \mathrm{ego} \wedge \langle cl(\mathrm{ego}) \wedge (re(c) \vee cl(c))\rangle$

Case 2 : $\phi_{cl} \equiv \neg\exists c : c \neq \mathrm{ego} \wedge \langle cl(\mathrm{ego}) \wedge cl(c)\rangle$



Linking predicate:

$\phi_{cl} \Leftarrow \neg b_t$ holds.

Search for Tool Support

- Satisfiability Problem:

  Given: MLSL formula ϕ

  Question: $\exists M = (\mathcal{T}, V, \nu): \; M \models \phi$?

- Undecidability Result 1 [LH15, Lin15]:

  Halting Problem of two-counter machines

  $\leq$ Satisfiability Problem for MLSL + length ℓ

  Inspired by undecidability proof for the satisfiability problem of the Duration Calculus by Zhou, Hansen and Sestoft.

Search for Tool Support

- Satisfiability Problem:

  Given: MLSL formula ϕ

  Question: $\exists\, M = (\mathcal{T}, V, \nu) :\; M \models \phi$?

- Undecidability Result 1 [LH15, Lin15]:

   Halting Problem of two-counter machines
  $\leq$ Satisfiability Problem for MLSL + length ℓ

  Inspired by undecidability proof for the satisfiability problem of the Duration Calculus by Zhou, Hansen and Sestoft.

- Undecidability Result 2 [Ody15]:

   Empty Intersection Problem for context-free languages
  $\leq$ Satisfiability Problem for MLSL without length

Search for Tool Support

- EMLSL and Isabelle/HOL : [Lin15, Lin17]
  abstract view of controllers and checked safety proof

Search for Tool Support

- EMLSL and Isabelle/HOL : [Lin15, Lin17]
  abstract view of controllers and checked safety proof

- Checking MLSL formulas on specific traffic snapshots:
  - translation into QdL [BSc: Bis16]
    (Quantified differential Dynamic Logic) of A. Platzer
  - translation into QLIRA [FHO15]
    (Quantified Linear Integer-Real Aritmetic)

Search for Tool Support

- EMLSL and Isabelle/HOL : [Lin15, Lin17]
  abstract view of controllers and checked safety proof

- Checking MLSL formulas on specific traffic snapshots:
  - translation into QdL [BSc: Bis16]
    (Quantified differential Dynamic Logic) of A. Platzer
  - translation into QLIRA [FHO15]
    (Quantified Linear Integer-Real Aritmetic)

- Controller verification:
  translation into and use of UPPAAL [OS17]

EMLSL with Modalities

- Sven Linker,
  Proofs for Traffic Safety: Combining Diagrams and Logics.
  PhD thesis, 2015.

- MLSL extended with modalities:

$\Box_{\mathsf{c}(d)}$	
$\Box_{\mathsf{r}(d)}$	after all reservations of d
$\Box_{\mathsf{wd\_c}(d)}$	
$\Box_{\mathsf{wd\_r}(d)}$	
$\Box_{\tau}$	after all time transitions
$\mathbf{G}$	globally, i.e. after all sequences of transitions

Formal Safety Specification

- Safe of a car e :

$$safe(e) \equiv \forall c : c \neq e \wedge \neg \langle re(c) \wedge re(e) \rangle$$

- Global Safety:

$$Safe \equiv \forall e : \mathbf{G}\ safe(e)$$

Formal Safety Specification

- Safe of a car e :

$$safe(e) \equiv \forall c : c \neq e \land \neg \langle re(c) \land re(e) \rangle$$

- Global Safety:

$$Safe \equiv \forall e : \mathbf{G}\ safe(e)$$

- Distance Controller:

$$\mathrm{DC} \equiv \mathbf{G}\ \forall c, d : c \neq d \rightarrow (\neg \langle re(c) \land re(d) \rangle \rightarrow \Box_\tau \neg \langle re(c) \land re(d) \rangle)$$

Formal Safety Specification

- Safe of a car e :

$$safe(e) \equiv \forall c : c \neq e \wedge \neg \langle re(c) \wedge re(e) \rangle$$

- Global Safety:

$$Safe \equiv \forall e : \mathbf{G}\ safe(e)$$

- Distance Controller:

$$\mathrm{DC} \equiv \mathbf{G}\ \forall c, d : c \neq d \rightarrow (\neg \langle re(c) \wedge re(d) \rangle \rightarrow \Box_{\tau} \neg \langle re(c) \wedge re(d) \rangle)$$

- Potential collision check:

$$pc(c,d) \equiv c \neq d \wedge \langle cl(d) \wedge (re(c) \vee cl(c)) \rangle$$

Formal Safety Specification

- Safe of a car e :

$$safe(e) \equiv \forall c : c \neq e \wedge \neg \langle re(c) \wedge re(e) \rangle$$

- Global Safety:

$$Safe \equiv \forall e : \mathbf{G}\ safe(e)$$

- Distance Controller:

$$\mathrm{DC} \equiv \mathbf{G}\ \forall c, d : c \neq d \rightarrow (\neg \langle re(c) \wedge re(d) \rangle \rightarrow \Box_{\tau} \neg \langle re(c) \wedge re(d) \rangle)$$

- Potential collision check:

$$pc(c, d) \equiv c \neq d \wedge \langle cl(d) \wedge (re(c) \vee cl(c)) \rangle$$

- Lane Change property:

$$\mathrm{LC} \equiv \mathbf{G}\ \forall d : (\exists c : pc(c, d) \rightarrow \Box_{r(d)} \bot)$$

Formal Safety Proofs

- [Lin15]: using a system of labelled natural deduction for EMLSL:

$$\{ts, v : \mathrm{DC},\ ts, v : \mathrm{LC},\ ts, v : \forall e : safe(e)\}$$
$$\vdash \quad ts, v : \forall e : \mathbf{G}\ safe(e)$$

- [Lin17]: using a formalisation of the semantics of EMLSL

  in Isabelle/HOL

Future Work

- Imperfect knowledge: communication [HLOR11] [BSc: Lam17]
- more on automatisation and tool support

Acknowledgements

Anders P. Ravn
Rafael Wisniewsky
Gregor v. Bochmann

Sven Linker
Martin Hilscher
Heinrich Ody
Maike Schwammberger

Christopher Bischopink
Lasse Hammer
Christian Harken
Sven Lampe

AVACS Project H3 (Cooperating Traffic Agents):

Werner Damm
Jan-David Quesel

References

M. Fränzle, M. R. Hansen, and H. Ody.
No need knowing numerous neighbours – towards a realizable interpretation of MLSL.
In R. Meyer, A. Platzer, and H. Wehrheim, editors, *Correct System Design*, volume 9360 of *LNCS*, pages 152–171. Springer, 2015.

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.

M. Hilscher, S. Linker, and E.-R. Olderog.
Proving safety of traffic manoeuvres on country roads.
In Zhiming Liu, Jim Woodcock, and Huibiao Zhu, editors, *Theories of Programming and Formal Methods*, volume 8051 of *LNCS*, pages 196–212. Springer, 2013.

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, *Intern. Conf. on Formal Engineering Methods (ICFEM)*, volume 6991 of *LNCS*, pages 404–409. Springer, 2011.

M. Hilscher and M. Schwammberger.
An abstract model for proving safety of autonomous urban traffic.
In A. Sampaio and F. Wang, editors, *Intern. Conf. on Theoret. Aspects of Comput. (ICTAC)*, volume 9965 of *LNCS*, pages 274–292. Springer, 2016.

Sven Linker and Martin Hilscher.
Proof theory of a multi-lane spatial logic.
Logical Methods in Computer Science, 11(3), 2015.

S. Linker.
Proofs for Traffic Safety: Combining Diagrams and Logics.
PhD thesis, Department of Computing, University of Oldenburg, 2015.

S. Linker.
Spatial reasoning about motorway traffic safety with Isabelle/HOL.
In N. Polikarpova and S. Schneider, editors, *Integrated Formal Methods (IFM)*, volume 10510 of *LNCS*, pages 34–49. Springer, 2017.

K. G. Larsen, M. Mikucionis, and J. H. Taankvist.
Safe and optimal adaptive cruise control.
In R. Meyer, A. Platzer, and H. Wehrheim, editors, *Correct System Design*, volume 9360 of *LNCS*, pages 260–277, 2015.

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.

T. Moor, J. Raisch, and S. O'Young.
Discrete supervisory control of hybrid systems based on l-complete approximations.
Discrete Event Dynamic Systems, 12:83–107, 2002.

Simin Nadjm-Tehrani and Jan-Erik Strömberg.
From physical modelling to compositional models of hybrid systems.
In *Formal Techniques in Real-Time and Fault-Tolerant Systems, Third International Symp. Organized Jointly with the Working Group Provably Correct Systems – ProCoS*, pages 583–604, 1994.

H. Ody.
Undecidability results for multi-lane spatial logic.
In M. Leucker, C. Rueda, and F. D. Valencia, editors, *Intern. Conf. on Theoret. Aspects of Comput. (ICTAC)*, volume 9399 of *LNCS*, pages 404–421. Springer, 2015.
.

E.-R. Olderog, A.P. Ravn, and R. Wisniewski.
Linking discrete and continuous models, applied to traffic manoeuvres.
In M.G. Hinchey, J.P. Bowen, and E.-R. Olderog, editors, *Provably Correct Systems*, NASA Monographs in Systems and Softw. Engin., pages 95–120. Springer, 2017.
.

E.-R. Olderog and M. Schwammberger.
Formalising a hazard warning communication protocol with timed automata.
In L. Aceto, G. Bacci, G. Bacci, A. Ingólfsdóttir, A. Legay, and R. Mardare, editors, *Models, Algorithms, Logics and Tools*, volume 10460 of *LNCS*, pages 640–660. Springer, 2017.

A. Platzer.
Quantified differential dynamic logic for distributed hybrid systems.
In A. Dawar and H. Veith, editors, *Computer Science Logic (CSL)*, volume 6247 of *LNCS*, pages 469–483. Springer, 2010.

G. v. Bochmann, M. Hilscher, S. Linker, and E.-R. Olderog.
Synthesizing and verifying controllers for multi-lane traffic maneuvers.
Formal Aspects of Computing, 29(4):583–600, 2017.

Bingqing Xu and Qin Li.
A spatial logic for modeling and verification of collision-free control of vehicles.
In Hai Wang and Mounir Mokhtari, editors, *21st Intern. Conf. on Engineering of Complex Computer Systems (ICECCS)*, pages 33–42. IEEE Computer Society, 2016.