André Platzer

Carnegie Mellon University, Pittsburgh, PA
1 Motivation

2 Quantified Differential Dynamic Logic QdL
   - Design
   - Syntax
   - Semantics

3 Proof Calculus for Distributed Hybrid Systems
   - Compositional Verification Calculus
   - Deduction Modulo with Free Variables & Skolemization
   - Actual Existence and Creation
   - Soundness and Completeness
   - Quantified Differential Invariants

4 Applications

5 Conclusions
Q: I want to verify my car

Challenge
Q: I want to verify my car  
A: Hybrid systems

Challenge (Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Complex Physical Systems: Hybrid Systems

Q: I want to verify my car
A: Hybrid systems
Q: But there’s a lot of cars!

Challenge (Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Q: I want to verify a lot of cars

Challenge

Distributed Systems

Local computation (finite state automaton)
Remote communication (network graph)
Q: I want to verify a lot of cars  
A: Distributed systems

**Challenge (Distributed Systems)**

- Local computation (finite state automaton)
- Remote communication (network graph)
Q: I want to verify a lot of cars
A: Distributed systems
Q: But they move!

Challenge (Distributed Systems)

- Local computation
  (finite state automaton)
- Remote communication
  (network graph)
Q: I want to verify lots of moving cars

Challenge

Discrete dynamics (control decisions)
Continuous dynamics (differential equations)
Structural dynamics (remote communication)
Dimensional dynamics (appearance)
Q: I want to verify lots of moving cars  
A: Distributed hybrid systems

Challenge (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (remote communication)
Q: I want to verify lots of moving cars  
A: Distributed hybrid systems

Challenge (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (remote communication)
- Dimensional dynamics (appearance)
Q: I want to verify lots of moving cars
A: Distributed hybrid systems
Q: How?

Challenge (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (remote communication)
- Dimensional dynamics (appearance)
State of the Art: Modeling and Simulation

No formal verification of distributed hybrid systems


Hybrid CSP [6] Semantics in Extended Duration Calculus

Φ-calculus [9] Semantics in rich set theory


ACP_{srt} [10] Modeling language proposal

χ process algebra [8] Simulation, translation of fragments to PHAVER, UPPAAL

Contributions

1. System model and semantics for distributed hybrid systems: QHP
2. Specification and verification logic: QdL
3. Proof calculus for QdL
4. First verification approach for distributed hybrid systems
5. Sound and complete axiomatization relative to differential equations
6. Prove collision freedom in a (simple) distributed car control system, where new cars may appear dynamically on the road
7. Logical foundation for analysis of distributed hybrid systems
8. Fundamental extension: first-order $x(i)$ versus primitive $x$
1 Motivation

2 Quantified Differential Dynamic Logic QdL
   - Design
   - Syntax
   - Semantics

3 Proof Calculus for Distributed Hybrid Systems
   - Compositional Verification Calculus
   - Deduction Modulo with Free Variables & Skolemization
   - Actual Existence and Creation
   - Soundness and Completeness
   - Quantified Differential Invariants

4 Applications

5 Conclusions
Outline (Conceptual Approach)

1. Motivation

2. Quantified Differential Dynamic Logic QdL
   - Design
   - Syntax
   - Semantics

3. Proof Calculus for Distributed Hybrid Systems
   - Compositional Verification Calculus
   - Deduction Modulo with Free Variables & Skolemization
   - Actual Existence and Creation
   - Soundness and Completeness
   - Quantified Differential Invariants

4. Applications

5. Conclusions
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ x'' = a \]
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ x'' = a \]
- Discrete dynamics (control decisions)
  \[ a := \text{if } \ldots \text{then } A \text{ else } -b \]
- Structural dynamics (communication/coupling)
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ x'' = a \]

- Discrete dynamics (control decisions)
  \[ a := \text{if .. then } A \text{ else } -b \]

- Structural dynamics (communication/coupling)
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ x'' = a \]
- Discrete dynamics (control decisions)
  \[ a := \text{if .. then } A \text{ else } -b \]
- Structural dynamics (communication/coupling)
Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ x(i)'' = a(i) \]

- Discrete dynamics (control decisions)
  \[ a(i) := \text{if} \cdots \text{then} A \text{else} -b \]

- Structural dynamics (communication/coupling)
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ \forall i \ x(i)'' = a(i) \]
- Discrete dynamics (control decisions)
  \[ \forall i \ a(i) := \text{if } \ldots \text{then } A \text{ else } -b \]
- Structural dynamics (communication/coupling)
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ \forall i \ x(i)'' = a(i) \]
- Discrete dynamics (control decisions)
  \[ \forall i \ a(i) := \text{if} \ldots \text{then} A \text{else} -b \]
- Structural dynamics (communication/coupling)
  \[ \ell(i) := \text{carInFrontOf}(i) \]
Q: How to model distributed hybrid systems
A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ \forall i \, x(i)'' = a(i) \]
- Discrete dynamics (control decisions)
  \[ \forall i \, a(i) := \text{if .. then } A \text{ else } -b \]
- Structural dynamics (communication/coupling)
  \[ \ell(i) := \text{carInFrontOf}(i) \]
- Dimensional dynamics (appearance)
Q: How to model distributed hybrid systems  
A: Quantified Hybrid Programs

Continuous dynamics (differential equations)
\[ \forall i \quad x(i)'' = a(i) \]

Discrete dynamics (control decisions)
\[ \forall i \quad a(i) := \text{if} \ldots \text{then} A \text{else} -b \]

Structural dynamics (communication/coupling)
\[ \ell(i) := \text{carInFrontOf}(i) \]

Dimensional dynamics (appearance)
\[ n := \text{new Car} \]
## Definition (Quantified hybrid program $\alpha$)

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall i : C ; x(i)' = \theta$</td>
<td>(quantified ODE)</td>
</tr>
<tr>
<td>$\forall i : C ; x(i) := \theta$</td>
<td>(quantified assignment)</td>
</tr>
<tr>
<td>$?Q$</td>
<td>(conditional execution)</td>
</tr>
<tr>
<td>$\alpha; \beta$</td>
<td>(seq. composition)</td>
</tr>
<tr>
<td>$\alpha \cup \beta$</td>
<td>(nondet. choice)</td>
</tr>
<tr>
<td>$\alpha^*$</td>
<td>(nondet. repetition)</td>
</tr>
</tbody>
</table>

- jump & test
- Kleene algebra
Definition (Quantified hybrid program $\alpha$)

\[
\begin{align*}
\forall i : C &\ \ x(s)' = \theta \quad \text{(quantified ODE)} \\
\forall i : C &\ \ x(s) := \theta \quad \text{(quantified assignment)} \\
?Q &\quad \text{(conditional execution)} \\
\alpha ; \beta &\quad \text{(seq. composition)} \\
\alpha \cup \beta &\quad \text{(nondet. choice)} \\
\alpha^* &\quad \text{(nondet. repetition)}
\end{align*}
\]
Definition (Quantified hybrid program $\alpha$)

\[
\forall i : C \ x(s)' = \theta \\
\forall i : C \ x(s) := \theta \\
?Q \\
\alpha; \beta \\
\alpha \cup \beta \\
\alpha^*
\]

(quantified ODE)  
(quantified assignment)  
(conditional execution)  
(seq. composition)  
(nondet. choice)  
(nondet. repetition)  

\[
DCCS \equiv (ctrl; \ drive)^*
\]

\[
ctrl \equiv \forall i : C \ a(i) := \text{if } \forall j : C \ \text{far}(i, j) \text{ then } A \text{ else } -b
\]

\[
drive \equiv \forall i : C \ x(i)'' = a(i)
\]
Definition (Quantified hybrid program $\alpha$)

\[
\begin{align*}
\forall i : C \quad x(s)' &= \theta \quad \text{(quantified ODE)} \\
\forall i : C \quad x(s) &= \theta \quad \text{(quantified assignment)} \\
?q \quad \text{(conditional execution)} \\
\alpha; \beta \quad \text{(seq. composition)} \\
\alpha \cup \beta \quad \text{(nondet. choice)} \\
\alpha^* \quad \text{(nondet. repetition)}
\end{align*}
\]

\[
DCCS \equiv (\text{appear}; \text{ctrl}; \text{drive})^*
\]

appear $\equiv n := \text{new } C; \quad ?(\forall j : C \quad \text{far}(j, n))$

ctrl $\equiv \forall i : C \quad a(i) := \text{if } \forall j : C \quad \text{far}(i, j) \text{ then } A \text{ else } -b$

drive $\equiv \forall i : C \quad x(i)'' = a(i)$
Quantified Differential Dynamic Logic QdL: Syntax

Definition (Quantified hybrid program $\alpha$)

\[
\begin{align*}
\forall i: C \ x(s)' &= \theta \
\forall i: C \ x(s) &:= \theta \\
?q &\text{ (quantified ODE)} \\
?Q &\text{ (quantified assignment)} \\
\alpha; \beta &\text{ (conditional execution)} \\
\alpha \cup \beta &\text{ (seq. composition)} \\
\alpha^{*} &\text{ (nondet. choice)} \\
\alpha^{*} &\text{ (nondet. repetition)}
\end{align*}
\]

\{ jump & test \}

\{ Kleene algebra \}

\[DCCS \equiv (\text{appear}; \ ctrl; \ drive)^{*}\]

appear \equiv \ n := \text{new} \ C; \ ?(\forall j: C \ \text{far}(j, n))

ctrl \equiv \ \forall i: C \ a(i) := \text{if } \forall j: C \ \text{far}(i, j) \ \text{then } A \ \text{else } b

drive \equiv \ \forall i: C \ x(i)'' = a(i)

new C is definable!
Quantified Differential Dynamic Logic $Qd\mathcal{L}$: Syntax

Definition ($Qd\mathcal{L}$ Formula $\phi$)

$\neg, \land, \lor, \rightarrow, \forall x, \exists x, =, \geq, +, \cdot$  ($\mathbb{R}$-first-order part)

$[\alpha]\phi, \langle \alpha \rangle \phi$  (dynamic part)

$[(appear; ctrl; drive)^*] \forall i \neq j : C \ x(i) \neq x(j)$
Definition (QdŁ Formula \( \phi \))

\[\neg, \land, \lor, \rightarrow, \forall x, \exists x, =, \geq, +, \cdot\] (\(\mathbb{R}\)-first-order part)

\[[\alpha]\phi, \langle \alpha \rangle \phi\] (dynamic part)

\[\forall i, j : C \ far(i, j) \rightarrow [(appear; ctrl; drive)^*] \ \forall i \neq j : C \ x(i) \neq x(j)\]
Quantified Differential Dynamic Logic QdŁ: Syntax

Definition (QdŁ Formula $\phi$)

$\neg, \land, \lor, \rightarrow, \forall x, \exists x, =, \geq, +, \cdot \quad (\mathbb{R}\text{-first-order part})$

$[\alpha]\phi, \langle \alpha \rangle \phi \quad (\text{dynamic part})$

$\forall i, j : C \ far(i, j) \rightarrow [(\text{appear}; \text{ctrl}; \text{drive})^*] \ \forall i \neq j : C \ x(i) \neq x(j)$

$far(i, j) \equiv i \neq j \rightarrow x(i) < x(j) \land v(i) \leq v(j) \land a(i) \leq a(j)$

$\lor x(i) > x(j) \land v(i) \geq v(j) \land a(i) \geq a(j) \ldots$
Definition (Quantified hybrid program $\alpha$: transition semantics)

$$\forall i : C \ x(s) := \theta$$

if $w(x)(v^e_i[s]) = v^e_i[\theta]$ (for all $e$) and otherwise unchanged
Definition (Quantified hybrid program $\alpha$: transition semantics)

\[
\forall i : C \ x(s)' = \theta
\]

\[
\forall i \ x(s)' = \theta
\]

\[
\frac{d}{dt} \varphi(t)_i^e [x(s)](\zeta) = \varphi(\zeta)_i^e [\theta] \quad \text{(for all e)}
\]
Definition (Quantified hybrid program $\alpha$: transition semantics)
Definition (Quantified hybrid program $\alpha$: transition semantics)

$\alpha; \beta$

$\alpha$

$\beta$

$X$

$t$

$v$

$s$

$w$
Definition (Quantified hybrid program $\alpha$: transition semantics)
Definition (Quantified hybrid program $\alpha$: transition semantics)

$V \xrightarrow{\alpha} S_1 \xrightarrow{\alpha} S_2 \xrightarrow{\alpha} S_n \xrightarrow{\alpha} W$

$\alpha^*$
Definition (Quantified hybrid program $\alpha$: transition semantics)
Definition (Quantified hybrid program $\alpha$: transition semantics)

$$v \xrightarrow{\alpha} w_1$$
$$v \xrightarrow{\alpha \cup \beta} w_2$$
Definition (Quantified hybrid program $\alpha$: transition semantics)

- $\alpha$ from $v$ to $w_1$
- $\beta$ from $v$ to $w_2$
- $\alpha \cup \beta$ connects $w_1$ and $w_2$
Definition (Quantified hybrid program $\alpha$: transition semantics)

If $v \models Q$,

- $\nu$ is unchanged.

Otherwise, no transition.
Definition (Quantified hybrid program $\alpha$: transition semantics)

$$\text{if } v \not\models Q$$

no change if $v \models Q$
otherwise no transition
Definition (Qd\(\mathcal{L}\) Formula \(\phi\))
Definition (QdŁ Formula $\phi$)
Definition (QdŁ Formula $\phi$)

$[\alpha] \phi$

$\alpha$-span
Definition (QdL Formula $\phi$)

$$[\alpha] \phi$$

$$\langle \beta \rangle \phi$$

$\alpha$-span

$\beta$-span

compositional semantics $\Rightarrow$ compositional calculus
Definition (QdL Formula $\phi$)

- $\langle \beta \rangle \phi$ (β-span)
- $[\alpha] \phi$ (α-span)
- Compositional semantics $\Rightarrow$ Compositional calculus
Definition (QdL Formula $\phi$)

compositional semantics $\Rightarrow$ compositional calculus!
Outline (Verification Approach)

1. Motivation

2. Quantified Differential Dynamic Logic QdŁ
   - Design
   - Syntax
   - Semantics

3. Proof Calculus for Distributed Hybrid Systems
   - Compositional Verification Calculus
   - Deduction Modulo with Free Variables & Skolemization
   - Actual Existence and Creation
   - Soundness and Completeness
   - Quantified Differential Invariants

4. Applications

5. Conclusions
Proof Calculus for Quantified Differential Dynamic Logic

\[
\phi(\left[\forall i \ x(i) := \theta\right] x(u))
\]
∀i (i = u → φ(θ))

\[\phi([\forall i x(i) := \theta] x(u))\]
\[
\forall i \left( i = [\forall i x(i) := \theta] u \rightarrow \phi(\theta) \right) \\
\phi([\forall i x(i) := \theta] x(u))
\]
\( \forall i \ (i = [\forall i x(i) := \theta]u \to \phi(\theta)) \)

\[ \phi([\forall i x(i) := \theta]x(u)) \]

\( \phi([\forall i x(s) := \theta]x(u)) \)
\[
\forall i \ (i = [\forall i x(i) := \theta] u \to \phi(\theta)) \\
\phi([\forall i x(i) := \theta] x(u))
\]

if \( \exists i \ s = u \) then \( \forall i \ (s = u \to \phi(\theta)) \) else \( \phi(x(u)) \)

\[
\phi([\forall i x(s) := \theta] x(u))
\]
∀i (i = [∀i x(i) := θ] u → φ(θ))

\[∀i \frac{∀i x(i) := θ [x(u)]}{\phi} \] [x(u)]

if ∃i s = u then ∀i (s = u → φ(θ)) else φ(x(u))

\[∀i \frac{∀i x(s) := θ [x(u)]}{\phi} \] [x(u)]
∀i (i = [∀i x(i) := θ]u → φ(θ))

\[ \phi([∀i x(i) := θ]x(u)) \]

if \( \exists i s = u \) then \( \forall i (s = u → φ(θ)) \) else \( φ(x(u)) \)

\[ \phi([∀i x(s) := θ]x(u)) \]
\[
\forall i \ (i = [\forall i x(i) := \theta] u \rightarrow \phi(\theta))
\]

\[
\phi([\forall i x(i) := \theta] x(u))
\]

\[
\text{if } \exists i \ s = u \text{ then } \forall i \ (s = u \rightarrow \phi(\theta)) \text{ else } \phi(x(u))
\]

\[
\phi([\forall i x(s) := \theta] x(u))
\]
∀i (i = [∀i x(i) := θ] u → φ(θ))

φ([∀i x(i) := θ] x(u))

if ∃i s = [A] u then ∀i (s = [A] u → φ(θ)) else φ(x([A] u))

φ([∀i x(s) := θ] x(u))

∀i x(s) := θ

φ

∀i x(s) := θ

∀i x(i) := θ → φ(θ)

∀i x(i) := θ

x(u)

ϕ

∀i x(i) := θ

∀i x(i) := θ

∀i x(i) := θ

∀i x(i) := θ

∀i x(i) := θ

∀i x(i) := θ

∀i x(i) := θ

∀i x(i) := θ
\[ \forall i (i = [\forall x(i) := \theta]u \rightarrow \phi(\theta)) \]

\[ \phi([\forall x(i) := \theta]x(u)) \]

If \( \exists s = [A]u \) then \( \forall i (s = [A]u \rightarrow \phi(\theta)) \) else \( \phi(x([A]u)) \)

\[ \phi([\forall x(s) := \theta]x(u)) \]

If \( \exists t \geq 0 [\forall x(i) := x_i(t)] \phi \) then \( [\forall x(i)' = \theta] \phi \)
∀i (i = [∀i x(i) := θ]u → φ(θ))

φ([∀i x(i) := θ]x(u))

if ∃i s = [A]u then ∀i (s = [A]u → φ(θ)) else φ(x([A]u))

φ([∀i x(s) := θ]x(u))

∀t ≥ 0 [∀i x(i) := x_i(t)]φ

[∀i x(i)' = θ]φ

∀i x(i) := x_i(t)
compositional semantics \Rightarrow \text{compositional rules!}
\[
\frac{[\alpha] \phi \land [\beta] \phi}{[\alpha \cup \beta] \phi}
\]
\[
\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}
\]

\[
\frac{[\alpha][\beta]\phi}{[\alpha; \beta]\phi}
\]
\[
\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}
\]

\[
\frac{[\alpha][\beta]\phi}{[\alpha; \beta]\phi}
\]

\[
\frac{\phi \ (\phi \rightarrow [\alpha]\phi)}{[\alpha^*]\phi}
\]
$$\forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)^{''} = -b] \ \forall j \neq k \ x(j) \neq x(k)$$
∀i ≠ j x(i) ≠ x(j) → [∀i x(i)' = v(i), v(i)' = −b] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → [∀i x(i)" = −b] ∀j ≠ k x(j) ≠ x(k)
\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow \forall t \geq 0 [\forall i \ x(i) := -\frac{b}{2} t^2 + v(i) t + x(i)] \forall j \neq k \ x(j) \neq x(k) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)' = v(i), v(i)' = -b] \forall j \neq k \ x(j) \neq x(k) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)'' = -b] \forall j \neq k \ x(j) \neq x(k) \]
\( \forall i \neq j \ x(i) \neq x(j) \rightarrow s \geq 0 \rightarrow [\forall i \ x(i) := -\frac{b}{2}s^2 + v(i)s + x(i)] \forall j \neq k \ x(j) \neq x(k) \)

\( \forall i \neq j \ x(i) \neq x(j) \rightarrow \forall t \geq 0 [\forall i \ x(i) := -\frac{b}{2}t^2 + v(i)t + x(i)] \forall j \neq k \ x(j) \neq x(k) \)

\( \forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)' = v(i), \ v(i)' = -b] \forall j \neq k \ x(j) \neq x(k) \)

\( \forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)'' = -b] \forall j \neq k \ x(j) \neq x(k) \)
\[
\forall i \neq j \; x(i) \neq x(j), s \geq 0 \rightarrow [\forall i \; x(i) := -\frac{b}{2} s^2 + v(i) s + x(i)] \forall j \neq k \; x(j) \neq x(k)
\]

\[
\forall i \neq j \; x(i) \neq x(j) \rightarrow s \geq 0 \rightarrow [\forall i \; x(i) := -\frac{b}{2} s^2 + v(i) s + x(i)] \forall j \neq k \; x(j) \neq x(k)
\]

\[
\forall i \neq j \; x(i) \neq x(j) \rightarrow \forall t \geq 0 \; [\forall i \; x(i) := -\frac{b}{2} t^2 + v(i) t + x(i)] \forall j \neq k \; x(j) \neq x(k)
\]

\[
\forall i \neq j \; x(i) \neq x(j) \rightarrow [\forall i \; x(i)' = v(i), v(i)' = -b] \; \forall j \neq k \; x(j) \neq x(k)
\]

\[
\forall i \neq j \; x(i) \neq x(j) \rightarrow [\forall i \; x(i)'' = -b] \forall j \neq k \; x(j) \neq x(k)
\]
\[
\forall i \neq j \ x(i) \neq x(j), s \geq 0 \rightarrow \forall j \neq k \ (\frac{-b}{2} s^2 + v(j) s + x(j) \neq \frac{-b}{2} s^2 + v(k) s + x(k))
\]

\[
\forall i \neq j \ x(i) \neq x(j), s \geq 0 \rightarrow [\forall i \ x(i) := -\frac{b}{2} s^2 + v(i) s + x(i)] \forall j \neq k \ x(j) \neq x(k)
\]

\[
\forall i \neq j \ x(i) \neq x(j) \rightarrow s \geq 0 \rightarrow [\forall i \ x(i) := -\frac{b}{2} s^2 + v(i) s + x(i)] \forall j \neq k \ x(j) \neq x(k)
\]

\[
\forall i \neq j \ x(i) \neq x(j) \rightarrow \forall t \geq 0 [\forall i \ x(i) := -\frac{b}{2} t^2 + v(i) t + x(i)] \forall j \neq k \ x(j) \neq x(k)
\]

\[
\forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i) := v(i), v(i) := -b] \forall j \neq k \ x(j) \neq x(k)
\]

\[
\forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i) := v(i), v(i) := -b] \forall j \neq k \ x(j) \neq x(k)
\]
$\forall i \neq j \; x(i) \neq x(j) \rightarrow \forall j \neq k$  \quad $\forall s \geq 0 \left( -\frac{b}{2}s^2 + v(j)s + x(j) \neq -\frac{b}{2}s^2 + v(k)s + x(k) \right)$

$\forall i \neq j \; x(i) \neq x(j), s \geq 0 \rightarrow \forall j \neq k \left( -\frac{b}{2}s^2 + v(j)s + x(j) \neq -\frac{b}{2}s^2 + v(k)s + x(k) \right)$

$\forall i \neq j \; x(i) \neq x(j), s \geq 0 \rightarrow [\forall i \; x(i) := -\frac{b}{2}s^2 + v(i)s + x(i)] \forall j \neq k \; x(j) \neq x(k)$

$\forall i \neq j \; x(i) \neq x(j) \rightarrow s \geq 0 \rightarrow [\forall i \; x(i) := -\frac{b}{2}s^2 + v(i)s + x(i)] \forall j \neq k \; x(j) \neq x(k)$

$\forall i \neq j \; x(i) \neq x(j) \rightarrow t \geq 0 \rightarrow [\forall i \; x(i) := -\frac{b}{2}t^2 + v(i)t + x(i)] \forall j \neq k \; x(j) \neq x(k)$

$\forall i \neq j \; x(i) \neq x(j) \rightarrow \forall t \geq 0 \left( -\frac{b}{2}t^2 + v(i)t + x(i) \right) \forall j \neq k \; x(j) \neq x(k)$

$\forall i \neq j \; x(i) \neq x(j) \rightarrow [\forall i \; x(i)' = v(i), v(i)' = -b] \forall j \neq k \; x(j) \neq x(k)$

$\forall i \neq j \; x(i) \neq x(j) \rightarrow \forall t \geq 0 \left( -\frac{b}{2}t^2 + v(i)t + x(i) \right) \forall j \neq k \; x(j) \neq x(k)$

$\forall i \neq j \; x(i) \neq x(j) \rightarrow [\forall i \; x(i)' = v(i), v(i)' = -b] \forall j \neq k \; x(j) \neq x(k)$
∀i\neq j x(i)\neq x(j) \rightarrow \forall j \neq k \text{ QE } \forall s \geq 0 (-\frac{b}{2}s^2 + v(j)s + x(j) \neq -\frac{b}{2}s^2 + v(k)s + x(k))

∀i\neq j x(i)\neq x(j), s \geq 0 \rightarrow \forall j \neq k (-\frac{b}{2}s^2 + v(j)s + x(j) \neq -\frac{b}{2}s^2 + v(k)s + x(k))

∀i\neq j x(i)\neq x(j), s \geq 0 \rightarrow [\forall i x(i) := -\frac{b}{2}s^2 + v(i)s + x(i)] \forall j \neq k x(j) \neq x(k)

∀i\neq j x(i)\neq x(j) \rightarrow s \geq 0 \rightarrow [\forall i x(i) := -\frac{b}{2}s^2 + v(i)s + x(i)] \forall j \neq k x(j) \neq x(k)

∀i\neq j x(i)\neq x(j) \rightarrow \forall t \geq 0 [\forall i x(i) := -\frac{b}{2}t^2 + v(i)t + x(i)] \forall j \neq k x(j) \neq x(k)

∀i\neq j x(i)\neq x(j) \rightarrow [\forall i x(i)' = v(i), v(i)' = -b] \forall j \neq k x(j) \neq x(k)

∀i\neq j x(i)\neq x(j) \rightarrow [\forall i x(i)'' = -b] \forall j \neq k x(j) \neq x(k)
\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow \forall j \neq k \ (x(j) \leq x(k) \land v(j) \leq v(k) \lor x(j) \geq x(k) \land v(j) \geq v(k)) \]

\[ \forall i \neq j \ x(i) \neq x(j), s \geq 0 \rightarrow \forall j \neq k \ (-\frac{b}{2} s^2 + v(j)s + x(j) \neq -\frac{b}{2} s^2 + v(k)s + x(k)) \]

\[ \forall i \neq j \ x(i) \neq x(j), s \geq 0 \rightarrow \left[ \forall i \ x(i) := -\frac{b}{2} s^2 + v(i)s + x(i) \right] \forall j \neq k \ x(j) \neq x(k) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow s \geq 0 \rightarrow \left[ \forall i \ x(i) := -\frac{b}{2} s^2 + v(i)s + x(i) \right] \forall j \neq k \ x(j) \neq x(k) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow \forall t \geq 0 \left[ \forall i \ x(i) := -\frac{b}{2} t^2 + v(i)t + x(i) \right] \forall j \neq k \ x(j) \neq x(k) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow \left[ \forall i \ x(i)' = v(i), v(i)' = -b \right] \forall j \neq k \ x(j) \neq x(k) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow \left[ \forall i \ x(i)'' = -b \right] \forall j \neq k \ x(j) \neq x(k) \]
∀X, Y, V, W (X ≠ Y → X ≤ Y ∧ V ≤ W ∨ X ≥ Y ∧ V ≥ W)

∀i ≠ j x(i) ≠ x(j) → ∀j ≠ k (x(j) ≤ x(k) ∧ v(j) ≤ v(k) ∨ x(j) ≥ x(k) ∧ v(j) ≥ v(k))

∀i ≠ j x(i) ≠ x(j), s ≥ 0 → ∀j ≠ k (−b 2 s 2 + v(j)s + x(j) ≠ −b 2 s 2 + v(k)s + x(k))

∀i ≠ j x(i) ≠ x(j), s ≥ 0 → [∀i x(i) := −b 2 s 2 + v(i)s + x(i)] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → s ≥ 0 → [∀i x(i) := −b 2 s 2 + v(i)s + x(i)] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → ∀t ≥ 0 [∀i x(i) := −b 2 t 2 + v(i)t + x(i)] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → [∀i x(i)′ = v(i), v(i)′ = −b] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → [∀i x(i)'' = −b] ∀j ≠ k x(j) ≠ x(k)
∀X, Y, V, W (X ≠ Y → X ≤ Y ∧ V ≤ W ∨ X ≥ Y ∧ V ≥ W)

∀i ≠ j x(i) ≠ x(j) → ∀j ≠ k (x(j) ≤ x(k) ∧ v(j) ≤ v(k) ∨ x(j) ≥ x(k) ∧ v(j) ≥ v(k))

∀i ≠ j x(i) ≠ x(j), s ≥ 0 → ∀j ≠ k (−b/2 s^2 + v(j) s + x(j) ≠ −b/2 s^2 + v(k) s + x(k))

∀i ≠ j x(i) ≠ x(j), s ≥ 0 → [∀i x(i) := −b/2 s^2 + v(i) s + x(i)] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → s ≥ 0 → [∀i x(i) := −b/2 s^2 + v(i) s + x(i)] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → ∀t ≥ 0 [∀i x(i) := −b/2 t^2 + v(i) t + x(i)] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → [∀i x(i)' = v(i), v(i)' = −b] ∀j ≠ k x(j) ≠ x(k)

∀i ≠ j x(i) ≠ x(j) → [∀i x(i)'' = −b] ∀j ≠ k x(j) ≠ x(k)
Actual Existence and Creation

Actual Existence Function $E(\cdot)$

$$E(i) = \begin{cases} 
0 & \text{if } i \text{ denotes a possible object} \\
1 & \text{if } i \text{ denotes an actively existing objects}
\end{cases}$$

André Platzer (CMU)

FCPS / 25: Distributed Systems & Hybrid Systems
Actual Existence and Creation

Actual Existence Function $E(\cdot)$

$$E(i) = \begin{cases} 
0 & \text{if } i \text{ denotes a possible object} \\
1 & \text{if } i \text{ denotes an actively existing objects}
\end{cases}$$

$$[n := \text{new } C] \phi$$
Actual Existence Function $E(\cdot)$

$$E(i) = \begin{cases} 
0 & \text{if } i \text{ denotes a possible object} \\
1 & \text{if } i \text{ denotes an actively existing objects}
\end{cases}$$

$$\frac{[(\forall j : C \ n := j);] \phi}{[n := \text{new } C] \phi}$$
Actual Existence and Creation

Actual Existence Function $\mathbb{E}(\cdot)$

$$
\mathbb{E}(i) = \begin{cases} 
0 & \text{if } i \text{ denotes a possible object} \\
1 & \text{if } i \text{ denotes an actively existing object} 
\end{cases}
$$

$$
[(\forall j : C \ n := j); \ ?(\mathbb{E}(n) = 0); \ \phi] \\
\quad [n := \text{new } C] \phi
$$
Actual Existence Function $\mathcal{E}(\cdot)$

$$\mathcal{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

$$[(\forall j : C \ n := j); \ ?(\mathcal{E}(n) = 0); \ E(n) := 1] \phi$$

$$[n := \text{new } C] \phi$$
Actual Existence Function $E(\cdot)$

$E(i) = \begin{cases} 
0 & \text{if } i \text{ denotes a possible object} \\
1 & \text{if } i \text{ denotes an actively existing object}
\end{cases}$

\[
[(\forall j : C \ n := j) ; ?(E(n) = 0) ; E(n) := 1] \phi
\]

\[n := \text{new } C] \phi
\]

$\forall i : C! \phi \equiv$

$\forall i : C! f(s) := \theta \equiv$

$\forall i : C! f(s)' = \theta \equiv$
Actual Existence and Creation

**Actual Existence Function** $E(\cdot)$

$$E(i) = \begin{cases} 
0 & \text{if } i \text{ denotes a possible object} \\
1 & \text{if } i \text{ denotes an actively existing objects}
\end{cases}$$

$$[(\forall j : C \; n := j); \; ?(E(n) = 0); \; E(n) := 1]\phi$$

$$[n := \text{new } C]\phi$$

$$\forall i : C! \; \phi \equiv \forall i : C \; (E(i) = 1 \rightarrow \phi)$$

$$\forall i : C! \; f(s) := \theta \equiv \forall i : C \; f(s) := (\text{if } E(i) = 1 \text{ then } \theta \text{ else } f(s))$$

$$\forall i : C! \; f(s)' = \theta \equiv \forall i : C \; f(s)' = E(i)\theta$$
Theorem (Relative Completeness)

QdŁ calculus is a sound & complete axiomatisation of distributed hybrid systems relative to quantified differential equations.

Proof 16p.
Soundness and Completeness

Theorem (Relative Completeness)

QdL calculus is a sound & complete axiomatisation of distributed hybrid systems relative to quantified differential equations.

Proof 16p.

Corollary (Proof-theoretical Alignment)

proving distributed hybrid systems = proving dynamical systems!
Theorem (Quantified Differential Invariant) (HSCC’11)

\[
\text{(QdI)} \quad \begin{align*}
Q \rightarrow [\forall i : C \ f(i)' & := \theta] F' \\
F \rightarrow [\forall i : C \ f(i)' & = \theta \& Q] F
\end{align*}
\]

is sound
∀i : C 2x(i)^3 ≥ 1 → [∀i : C x(i)' = x(i)^2 + x(i)^4 + 2] ∀i : C 2x(i)^3 ≥ 1
∀i: C x(i)′ := x(i)^2 + x(i)^4 + 2](∀i: C 2x(i)^3 ≥ 0)'

∀i: C 2x(i)^3 ≥ 1 → [∀i: C x(i)′ = x(i)^2 + x(i)^4 + 2]∀i: C 2x(i)^3 ≥ 1
A Simple Proof with Quantified Differential Invariants

\[ \forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2 \forall i : C \ (2x(i)^3)' \geq 0 \]

\[ \forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2 \forall i : C \ 2x(i)^3 \geq 0 \]

\[ \forall i : C \ 2x(i)^3 \geq 1 \rightarrow \left[ \forall i : C \ x(i)' = x(i)^2 + x(i)^4 + 2 \forall i : C \ 2x(i)^3 \geq 1 \right] \]
∀i : C x(i)′ := x(i)^2 + x(i)^4 + 2]∀i : C 6x(i)^2x(i)′ ≥ 0

∀i : C x(i)′ := x(i)^2 + x(i)^4 + 2]∀i : C (2x(i)^3)′ ≥ 0

∀i : C x(i)′ := x(i)^2 + x(i)^4 + 2](∀i : C 2x(i)^3 ≥ 0)′

∀i : C 2x(i)^3 ≥ 1 → [∀i : C x(i)′ = x(i)^2 + x(i)^4 + 2]∀i : C 2x(i)^3 ≥ 1
\[ \forall i : C \ 6x(i)^2(x(i)^2 + x(i)^4 + 2) \geq 0 \]

\[ [\forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2] \forall i : C \ 6x(i)^2x(i)' \geq 0 \]

\[ [\forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2] \forall i : C \ (2x(i)^3)' \geq 0 \]

\[ [\forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2](\forall i : C \ 2x(i)^3 \geq 0)' \]

\[ \forall i : C \ 2x(i)^3 \geq 1 \rightarrow [\forall i : C \ x(i)' = x(i)^2 + x(i)^4 + 2] \forall i : C \ 2x(i)^3 \geq 1 \]
true

\[ \forall i: C \ 6x(i)^2(x(i)^2 + x(i)^4 + 2) \geq 0 \]

\[ [\forall i: C \ x(i)' := x(i)^2 + x(i)^4 + 2] \forall i: C \ 6x(i)^2x(i)' \geq 0 \]

\[ [\forall i: C \ x(i)' := x(i)^2 + x(i)^4 + 2] \forall i: C \ (2x(i)^3)' \geq 0 \]

\[ [\forall i: C \ x(i)' := x(i)^2 + x(i)^4 + 2] (\forall i: C \ 2x(i)^3 \geq 0)' \]

\[ \forall i: C \ 2x(i)^3 \geq 1 \rightarrow [\forall i: C \ x(i)' = x(i)^2 + x(i)^4 + 2] \forall i: C \ 2x(i)^3 \geq 1 \]
Outline

1 Motivation

2 Quantified Differential Dynamic Logic \( \text{QdL} \)
   - Design
   - Syntax
   - Semantics

3 Proof Calculus for Distributed Hybrid Systems
   - Compositional Verification Calculus
   - Deduction Modulo with Free Variables & Skolemization
   - Actual Existence and Creation
   - Soundness and Completeness
   - Quantified Differential Invariants

4 Applications

5 Conclusions
Driver’s License Test for Robotic Cars?

André Platzer (CMU)
Driver’s License Test for Robotic Cars?
Driver’s License Test for Robotic Cars? Proof!

André Platzer (CMU)

FCPS / 25: Distributed Systems & Hybrid Systems
Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:
Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:

  \[ f \ll \ell \rightarrow [(a_i := ctrl; \ x_i'' = a_i)^*] f \ll \ell \]
Car Control: Local Lane Control Challenge

Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:

  \[ f \ll \ell \rightarrow [(a_i := ctrl; x_i'' = a_i)^*] f \ll \ell \]

  \[
  f \ll \ell \equiv (x_f \leq x_{\ell}) \land (f \neq \ell) \rightarrow \\
  (x_{\ell} > x_f + \frac{v_f^2}{2b} - \frac{v_{\ell}^2}{2B} \\
  \land x_{\ell} > x_f \land v_f \geq 0 \land v_{\ell} \geq 0)
  \]
Challenge: Global lane dynamics

- All controllers for arbitrarily many differential equations respect separation globally on lane.
Challenge: Global lane dynamics

- All controllers for arbitrarily many differential equations respect separation globally on lane.
- Each car safe behind all others
Challenge: Global lane dynamics

- All controllers for arbitrarily many differential equations respect separation globally on lane.
- Each car safe behind all others

\[
(\forall i \ a(i) := ctrl; \ \forall i \ x(i)'' = a(i))^* \ \forall i, j \ i \ll j
\]
Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.
Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.
- For each lane: all controllers for the differential equations respect separation even if cars appear or disappear.
Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.
- For each lane: all controllers for the differential equations respect separation even if cars appear or disappear.
- Each car safe behind all others, even if new cars appear or disappear.
Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.
- For each lane: all controllers for the differential equations respect separation even if cars appear or disappear.
- Each car safe behind all others, even if new cars appear or disappear.

\[ (n := \text{new } C; \ \forall i \ a(i) := \text{ctrl}; \ \forall i \ x(i)'' = a(i))^*] \forall i, j \ i \ll j \]
Car Control: Global Highway Control Challenge

Challenge: Global highway dynamics

- All controllers for arbitrarily many differential equations respect separation globally on highway.

\[ \forall l (n := \text{new} C; \forall i a (i) := \text{ctrl}; \forall i x (i)'' = a (i)) \]
**Challenge: Global highway dynamics**

- All controllers for arbitrarily many differential equations respect separation globally on highway.
- All controllers for the differential equations respect separation even if cars switch lanes.
Challenge: Global highway dynamics

- All controllers for arbitrarily many differential equations respect separation globally on highway.
- All controllers for the differential equations respect separation even if cars switch lanes.
- On all lanes, all car safe behind all others on their lanes, even if cars switch lanes.
Challenge: Global highway dynamics

- All controllers for arbitrarily many differential equations respect separation globally on highway.
- All controllers for the differential equations respect separation even if cars switch lanes.
- On all lanes, all car safe behind all others on their lanes, even if cars switch lanes.

\[
\forall l \left( n := \text{new} \ C; \ \forall i \ a(i) := \text{ctrl}; \ \forall i \ x(i)'' = a(i))^* \right) \forall l \ \forall i, j \ i \ll j
\]
Outline

1. Motivation

2. Quantified Differential Dynamic Logic QdL
   - Design
   - Syntax
   - Semantics

3. Proof Calculus for Distributed Hybrid Systems
   - Compositional Verification Calculus
   - Deduction Modulo with Free Variables & Skolemization
   - Actual Existence and Creation
   - Soundness and Completeness
   - Quantified Differential Invariants

4. Applications

5. Conclusions
Conclusions

- Distributed hybrid systems everywhere
- System model and semantics
- Logic for distributed hybrid systems
- Compositional proof calculus
- First verification approach
- Sound & complete / diff. eqn.
- Quantified differential invariants
- Distributed car control verified
- Distributed aircraft control verified

quantified differential dynamic logic

\[ \text{QdL} = \text{FOL} + \text{DL} + \text{QHP} \]
Conclusions

quantified differential dynamic logic

\[ \mathcal{QdL} = \text{FOL} + \text{DL} + \text{QHP} \]

- Distributed hybrid systems everywhere
- System model and semantics
- Logic for distributed hybrid systems
- Compositional proof calculus
- First verification approach
- Sound & complete / diff. eqn.
- Quantified differential invariants
- Distributed car control verified
- Distributed aircraft control verified
André Platzer.
A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems.
Special issue for selected papers from CSL’10.

André Platzer.
Quantified differential dynamic logic for distributed hybrid systems.

André Platzer.
Quantified differential invariants.

Akash Deshpande, Aleks Göllü, and Pravin Varaiya.
SHIFT: A formalism and a programming language for dynamic networks of hybrid automata.


D. A. van Beek, Ka L. Man, Michel A. Reniers, J. E. Rooda, and Ramon R. H. Schifflers. Syntax and consistent equation semantics of hybrid Chi.
William C. Rounds.
A spatial logic for the hybrid $\pi$-calculus.

Jan A. Bergstra and C. A. Middelburg.
Process algebra for hybrid systems.

José Meseguer and Raman Sharykin.
Specification and analysis of distributed object-based stochastic hybrid systems.
In Hespanha and Tiwari [12], pages 460–475.

João P. Hespanha and Ashish Tiwari, editors.