Logic of Distributed Hybrid Systems

André Platzer

Carnegie Mellon University
Outline

1 Motivation

2 Quantified Differential Dynamic Logic \( Qd\mathcal{L} \)
   - 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
   - Distributed Car Control
   - Surgical Robot

5 Conclusions
Complex Physical Systems:

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)
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

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

[Diagram of multiple cars connected by dashed lines, indicating some form of communication or coordination.]
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)
No formal verification of distributed hybrid systems

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid CSP [6]</td>
<td>Semantics in Extended Duration Calculus</td>
</tr>
<tr>
<td>Φ-calculus [9]</td>
<td>Semantics in rich set theory</td>
</tr>
<tr>
<td>ACP_{hs}^{srt} [10]</td>
<td>Modeling language proposal</td>
</tr>
<tr>
<td>χ process algebra [8]</td>
<td>Simulation, translation of fragments to PHAVER, UPPAAL</td>
</tr>
</tbody>
</table>
Contributions

1. System model and semantics for distributed hybrid systems: QHP
2. Specification and verification logic: Qd\(\mathcal{L}\)
3. Proof calculus for Qd\(\mathcal{L}\)
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 \(x\)
Outline

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
   - Distributed Car Control
   - Surgical Robot

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
   - Distributed Car Control
   - Surgical Robot

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)
  \[ a := \text{if } .. \text{ then } A \text{ else } -b \]

- 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)
  \[ a := \text{if } \ldots \text{ then } A \text{ else } -b \]

- 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)
  \[ a := \text{if } .. \text{then } A \text{ else } -b \]

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

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ x(i)'' = a(i) \]
- Discrete dynamics (control decisions)
  \[ a(i) := \text{if } \ldots \text{then } A \text{ else } \neg b \]
- 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)
  \[ \forall i \, a(i) := \text{if .. then } A \text{ else } -b \]

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

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  \[ \forall i \quad x(i)'' = a(i) \]
- Discrete dynamics (control decisions)
  \[ \forall i \quad a(i) := \text{if } \ldots \text{ then } A \text{ else } -b \]
- Structural dynamics (communication/coupling)
  \[ \ell(i) := \text{carInFrontOf}(i) \]
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)
  \[ \ell(i) := carInFrontOf(i) \]
- Dimensional dynamics (appearance)

André Platzer (CMU) Logic of Distributed Hybrid Systems
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)
  \[ \forall i \ a(i) := \text{if } .. \text{ then } A \text{ else } -b \]
- Structural dynamics (communication/coupling)
  \[ \ell(i) := \text{carInFrontOf}(i) \]
- Dimensional dynamics (appearance)
  \[ n := \text{new Car} \]
### Definition (Quantified hybrid program $\alpha$)

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

\{ \text{jump & test} \}

\{ \text{Kleene algebra} \}
### Definition (Quantified hybrid program $\alpha$)

- $\forall i : C \ x(s)' = \theta$ (quantified ODE)
- $\forall i : C \ x(s) := \theta$ (quantified assignment)
- $? Q$ (conditional execution)
- $\alpha; \beta$ (seq. composition)
- $\alpha \cup \beta$ (nondet. choice)
- $\alpha^*$ (nondet. repetition)

### Operations
- $\alpha \cup \beta$ (nondet. choice)
- $\alpha^*$ (nondet. repetition)

### Kleene Algebra
- $\alpha \cup \beta$ (nondet. choice)
- $\alpha^*$ (nondet. repetition)

### Jump & Test
- $\forall i : C \ x(s)' = \theta$
- $\forall i : C \ x(s) := \theta$

---

- Quantified Differential Dynamic Logic QdL: Syntax
Definition (Quantified hybrid program $\alpha$)

- $\forall i : C \ x(s)' = \theta$ (quantified ODE)
- $\forall i : C \ x(s) := \theta$ (quantified assignment)
- $?Q$ (conditional execution)
- $\alpha; \beta$ (seq. composition)
- $\alpha \cup \beta$ (nondet. choice)
- $\alpha^*$ (nondet. repetition)

$\text{jump & test}$

$\{ \text{Kleene algebra} \}$

$\text{DCCS} \equiv (\text{ctrl} ; \text{drive})^*$

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

\[
\text{drive} \equiv \forall i : C \ x(i)'' = a(i)
\]
Quantified Differential Dynamic Logic $\text{QdL}$: Syntax

Definition (Quantified hybrid program $\alpha$)

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

\[
\begin{aligned}
\text{DCCS} & \equiv (\text{appear}; \text{ctrl}; \text{drive})^* \\
\text{appear} & \equiv n := \text{new } C; \ ?(\forall j : C \ \text{far}(j, n)) \\
\text{ctrl} & \equiv \forall i : C \ a(i) := \text{if } \forall j : C \ \text{far}(i, j) \ \text{then } A \ \text{else } -b \\
\text{drive} & \equiv \forall i : C \ x(i)'' = a(i)
\end{aligned}
\]
#### Definition (Quantified hybrid program $\alpha$)

- $\forall i : C \ x(s)' = \theta$ (quantified ODE)
- $\forall i : C \ x(s) := \theta$ (quantified assignment)
- $?Q$ (conditional execution)
- $\alpha;\beta$ (seq. composition)
- $\alpha \cup \beta$ (nondet. choice)
- $\alpha^*$ (nondet. repetition)

#### Kleene algebra

- $DCCS \equiv (appear; \ ctrl; \ drive)^*$
- $appear \equiv n := \text{new } C; \ ?(\forall j : C \ far(j, n))$
- $ctrl \equiv \forall i : C \ a(i) := \text{if } \forall j : C \ far(i, j) \ \text{then } A \ \text{else } -b$
- $drive \equiv \forall i : C \ x(i)'' = a(i)$

$\text{new } C$ is definable!
Quantified Differential Dynamic Logic QdŁ: Syntax

Definition (QdŁ Formula φ)

¬, ∧, ∨, →, ∀x, ∃x, =, ≥, +, · (ℝ-first-order part)  
[α]φ,  ⟨α⟩φ (dynamic part)

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

$\neg, \wedge, \vee, \rightarrow, \forall x, \exists x, =, \geq, +, \cdot$ \hspace{1cm} ($\mathbb{R}$-first-order part)

$[\alpha]\phi, \langle \alpha \rangle \phi$ \hspace{1cm} (dynamic part)

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

Definition (QdŁ Formula $\phi$)

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

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

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

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

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

$\alpha; \beta$

$V \xrightarrow{\alpha} S \xrightarrow{\beta} W$

$x$

$V \xrightarrow{\alpha} S \xrightarrow{\beta} W$

André Platzer (CMU)

Logic of Distributed Hybrid Systems
Definition (Quantified hybrid program \( \alpha \): transition semantics)

\[
\alpha; \beta
\]

\[
\begin{array}{ccc}
V & \xrightarrow{\alpha} & S \\
 & \xrightarrow{\beta} & W
\end{array}
\]
Definition (Quantified hybrid program $\alpha$: transition semantics)
Definition (Quantified hybrid program $\alpha$: transition semantics)

$$\alpha^*$$

$V \xrightarrow{\alpha} S_1 \xrightarrow{\alpha} S_2 \xrightarrow{\ldots} S_n \xrightarrow{\alpha} W$
Definition (Quantified hybrid program $\alpha$: transition semantics)
Definition (Quantified hybrid program $\alpha$: transition semantics)
Definition (Quantified hybrid program $\alpha$: transition semantics)

\[ ?Q \quad \text{if } v \models Q \]

\[ t \quad \text{no change if } v \models Q \quad \text{otherwise no transition} \]

Andre Platzer (CMU) Logic of Distributed Hybrid Systems
Definition (Quantified hybrid program $\alpha$: transition semantics)

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

no change if $v \models Q$

otherwise no transition
Definition (QdŁ Formula $\phi$)
Definition (QdŁ Formula $\phi$)

$v \langle \alpha \rangle \phi \rightarrow \phi \beta\text{-span}$

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

$[\alpha] \phi$

$\alpha$-span

[Diagram showing a compositional semantics arrow from $\nu$ to $\alpha$-span, with $[\alpha] \phi$ as a node.]

André Platzer (CMU) Logic of Distributed Hybrid Systems 10 / 24
Definition (QdL Formula $\phi$)

$[\alpha]\phi$

$\langle \beta \rangle \phi$

$\beta$-span

$\alpha$-span

compositional semantics $\Rightarrow$ compositional calculus!
Definition (QdŁ Formula $\phi$)

$\langle \beta \rangle \phi$

$[\alpha] \phi$

$\beta$-span

$\alpha$-span

compositional semantics $\Rightarrow$ compositional calculus
Definition (QdŁ 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
   - Distributed Car Control
   - Surgical Robot

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

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

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

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

\phi([∀i x(i) := θ]x(u))

\textbf{if } \exists i s = u \textbf{ then } \forall i (s = u \rightarrow \phi(θ)) \textbf{ else } \phi(x(u))

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

\[ \phi([∀ix(i) := θ]x(u)) \]

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

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

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

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

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

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

\[ \exists \bar{Q} \quad \bar{Q} \equiv \forall 0 \leq s \leq t \langle x := y \rangle \phi \]

\[ \langle x' = \theta \rangle \phi \]

\[ x' = \theta \]

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

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

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

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

\[ \forall t \geq 0 \ [\forall i \ x(i) := x_i(t)] \phi \]

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

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

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

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

\[ \forall t \geq 0 [\forall i x(i) := x_i(t)] \phi \]

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

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

\[
\frac{[\alpha][\beta] \phi}{[\alpha; \beta] \phi}
\]
\[
\frac{[\alpha] \phi \land [\beta] \phi}{[\alpha \cup \beta] \phi}
\]
\[
\frac{[\alpha][\beta] \phi}{[\alpha; \beta] \phi}
\]
\[
\frac{\phi \quad (\phi \rightarrow [\alpha] \phi)}{[\alpha^*] \phi}
\]
∀i ≠ j x(i) ≠ x(j) → [∀i x(i)'' = −b] ∀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)
\[
\forall i \neq j \ x(i) \neq x(j) \rightarrow \forall t \geq 0 \left[ \forall i \ x(i) := -\frac{b}{2} t^2 + v(i) t + x(i) \right] \forall j \neq k \ x(j) \neq x(k)
\]

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

\[
\forall i \neq j \ x(i) \neq x(j) \rightarrow \left[ \forall i \ x(i)'' = -b \right] \forall j \neq k \ x(j) \neq x(k)
\]
∀i ≠ j x(i) ≠ x(j) → s ≥ 0 → [∀ i x(i) := −\( \frac{b}{2} \) s^2 + v(i) s + x(i)] ∀ j ≠ k x(j) ≠ x(k)

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

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

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

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

∀\(i \neq j \land x(i) \neq x(j)\) → [\(\forall i \ x(i)^{''} = -b\)] \(\forall j \neq k \ x(j) \neq x(k)\)
∀i ≠ j \ x(i) ≠ x(j), s ≥ 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)

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

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

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

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

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

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

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

\( \forall i \neq j x(i) \neq x(j) \rightarrow [\forall i x(i)'' = -b] \forall j \neq k x(j) \neq x(k) \)
∀i ≠ j x(i) ≠ x(j) → ∀j ≠ k QE ∀ s ≥ 0 (−\(\frac{b}{2}\) s^2 + v(j)s + x(j) ≠ −\(\frac{b}{2}\) s^2 + v(k)s + x(k))

∀i ≠ j x(i) ≠ x(j), s ≥ 0 → ∀ j ≠ k (−\(\frac{b}{2}\) s^2 + v(j)s + x(j) ≠ −\(\frac{b}{2}\) s^2 + v(k)s + x(k))

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

∀i ≠ j x(i) ≠ x(j) → ∀ t ≥ 0 [∀ i x(i) := −\(\frac{b}{2}\) 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)
\( \forall i \neq j \mathbf{x}(i) \neq \mathbf{x}(j) \rightarrow \forall j \neq k \ (\mathbf{x}(j) \leq \mathbf{x}(k) \land \mathbf{v}(j) \leq \mathbf{v}(k) \lor \mathbf{x}(j) \geq \mathbf{x}(k) \land \mathbf{v}(j) \geq \mathbf{v}(k)) \)

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

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

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

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

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

\( \forall i \neq j \mathbf{x}(i) \neq \mathbf{x}(j) \rightarrow [\forall i \mathbf{x}(i)'' = -b] \forall j \neq k \mathbf{x}(j) \neq \mathbf{x}(k) \)
\[ \forall X, Y, V, W \ (X \neq Y \rightarrow X \leq Y \land V \leq W \lor X \geq Y \land V \geq W) \]

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow \forall j \neq k \ (x(j) \leq x(k) \land v(j) \leq v(k) \lor x(j) \geq x(k) \land v(j) \geq v(k)) \]

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

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

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

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

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

\[ \forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)'' = -b] \forall j \neq k \ x(j) \neq x(k) \]
\[\forall X, Y, V, W \ (X \neq Y \rightarrow X \leq Y \land V \leq W \lor X \geq Y \land V \geq W)\]

\[\forall i \neq j \ x(i) \neq x(j) \rightarrow \forall j \neq k \ (x(j) \leq x(k) \land v(j) \leq v(k) \lor x(j) \geq x(k) \land v(j) \geq v(k))\]

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

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

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

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

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

\[\forall i \neq j \ x(i) \neq x(j) \rightarrow [\forall i \ x(i)'' = -b] \forall j \neq k \ x(j) \neq x(k)\]
Actual Existence Function $E(\cdot)$

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

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

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

\[\forall i : C \models \phi \equiv \forall i : C \left( \exists(i) = 1 \rightarrow \phi \right)\]

\[\forall i : C : f(s) := \theta \equiv \forall i : C : f(s) := \begin{cases} 
\theta & \text{if } \exists(i) = 1 \\
f(s) & \text{if } \exists(i) = 0
\end{cases}\]

\[\forall i : C : f(s) = \theta \equiv \exists(i) \theta\]
Actual Existence and Creation

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

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

$$
[(\forall j : C \ n := j); \ ?(\mathbb{E}(n) = 0); \ \mathbb{E}(n) := 1] \phi \\
[n := \text{new } C] \phi
$$
Actual Existence Function $E(\cdot)$

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

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

$$[n := \text{new } C] \phi$$
Actual Existence and Creation

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

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

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

$$[n := \text{new } C] \phi$$
Actual Existence and Creation

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

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

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

\Rightarrow

[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 Function $E(\cdot)$

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

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

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

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

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

$$\forall i : C! \ f(s)' = \theta \equiv \forall i : C \ f(s)' = E(i)\theta$$
QdL calculus is a sound & complete axiomatisation of distributed hybrid systems relative to quantified differential equations.
Soundness and Completeness

<table>
<thead>
<tr>
<th>Theorem (Relative Completeness) (LMCS’12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>QdŁ calculus is a sound &amp; complete axiomatisation of distributed hybrid systems relative to quantified differential equations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Corollary (Proof-theoretical Alignment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>proving distributed hybrid systems = proving dynamical systems!</td>
</tr>
</tbody>
</table>
Theorem (Quantified Differential Invariant) (HSCC’11)

\[ (QdI) \quad \frac{Q \rightarrow [\forall i : C \ f(i)' := \theta] F'}{F \rightarrow [\forall i : C \ f(i)' = \theta \& Q] F} \quad \text{is sound} \]
∀i : C 2x(i)^3 ≥ 1 \to [∀i : C x(i)' = x(i)^2 + x(i)^4 + 2] ∀i : C 2x(i)^3 ≥ 1
A Simple Proof with Quantified Differential Invariants

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

\[ \forall i : C \ 2x(i)^3 \geq 1 \rightarrow [ \forall i : C \ x(i)' = x(i)^2 + x(i)^4 + 2 ] \forall i : C \ 2x(i)^3 \geq 1 \]
\[
\begin{align*}
[\forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2] &\forall i : C \ (2x(i)^3)' \geq 0 \\
[\forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2] &\forall i : C \ 2x(i)^3 \geq 0)
\end{align*}
\]
\[\forall i : C \ 2x(i)^3 \geq 1 \rightarrow [\forall i : C \ x(i)' = x(i)^2 + x(i)^4 + 2] \forall i : C \ 2x(i)^3 \geq 1\]
∀ i : C  x(i)′ := x(i)^2 + x(i)^4 + 2 \forall i : C \ 6x(i)^2x(i)′ ≥ 0

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

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

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

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

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

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

\[ \forall i : C \ 2x(i)^3 \geq 1 \rightarrow [\forall i : C \ x(i)' = x(i)^2 + x(i)^4 + 2] \forall i : C \ 2x(i)^3 \geq 1 \]
\begin{align*}
& \text{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)'^2 \geq 0 \\
& [\forall i : C \ x(i)' := x(i)^2 + x(i)^4 + 2] \forall i : C \ (2x(i)^3)'^2 \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
\end{align*}
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
   - Distributed Car Control
   - Surgical Robot

5 Conclusions
Driver’s License Test for Robotic Cars?
Driver’s License Test for Robotic Cars?
Driver’s License Test for Robotic Cars? **Proof!**
Car Control: Local Lane Control Challenge

Challenge: Local lane dynamics

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

\[
\begin{align*}
  \text{follower} & \ll \text{leader} \\
  f & \ll \ell \\
  f & \ll \ell \\
  x_f & \leq x_l \\
  f & \neq \ell \\
  x_l & > x_f + v_f^2f^2b - v_l^2\ell^2B \\
  x_l & > x_f \\
  v_f & \geq 0 \\
  v_l & \geq 0
\end{align*}
\]
Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:
  \[ f \ll \ell \rightarrow [(a_i := \text{ctrl}; x''_i = a_i)^*] f \ll \ell \]
Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:
  \[ f \ll \ell \rightarrow [(a_i := \text{ctrl}; \; x_i'' = a_i)^*] \; f \ll \ell \]

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

\[
\left( \forall i \ a(i) := ctrl; \ \forall i \ x(i)'' = a(i) \right)^* \ \forall i, j \ i \ll j
\]
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.
Car Control: Local Highway Control Challenge

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.

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

- All controllers for arbitrarily many differential equations respect separation globally on highway.
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.
Car Control: Global Highway Control Challenge

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.

\[
\forall \forall (n := \text{new } C; \ \forall i a(i) := \text{ctrl}; \ \forall i x(i)'' = a(i))^* \forall \forall i, j i \ll j
\]
Virtual fixture boundary

Time
Continuous Control
Robot responds infinitely fast
Time
Robot responds within ε

Negligible lag?

Redesign to predictive control

HSCC’13

André Platzer (CMU) Logic of Distributed Hybrid Systems
Conclusions

Quantified differential dynamic logic

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

- 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
- Robot verified for many obstacles
Conclusions

quantified differential dynamic logic

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

- 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
- Robot verified for many obstacles
I Part: Elementary Cyber-Physical Systems
2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays

II Part: Differential Equations Analysis
10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory

III Part: Adversarial Cyber-Physical Systems
14-17. Hybrid Systems & Hybrid Games

IV Part: Comprehensive CPS Correctness
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.

**Fabian Kratz, Oleg Sokolsky, George J. Pappas, and Insup Lee.**
R-Charon, a modeling language for reconfigurable hybrid systems. In Hespanha and Tiwari [17], pages 392–406.

**Zhou Chaochen, Wang Ji, and Anders P. Ravn.**

**Pieter J. L. Cuijpers and Michel A. Reniers.**

**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 π-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 [17], pages 460–475.

Yanni Kouskoulas, David W. Renshaw, André Platzer, and Peter Kazanzides.
Certifying the safe design of a virtual fixture control algorithm for a surgical robot.
In Belta and Ivancic [18], pages 263–272.
Sarah M. Loos, André Platzer, and Ligia Nistor.
Adaptive cruise control: Hybrid, distributed, and now formally verified.


Sarah M. Loos, David W. Renshaw, and André Platzer.
Formal verification of distributed aircraft controllers.
In Belta and Ivancic [18], pages 125–130.

Stefan Mitsch, Khalil Ghorbal, David Vogelbacher, and André Platzer.
Formal verification of obstacle avoidance and navigation of ground robots.

André Platzer.
*Logical Foundations of Cyber-Physical Systems.*

João P. Hespanha and Ashish Tiwari, editors.
Calin Belta and Franjo Ivancic, editors.