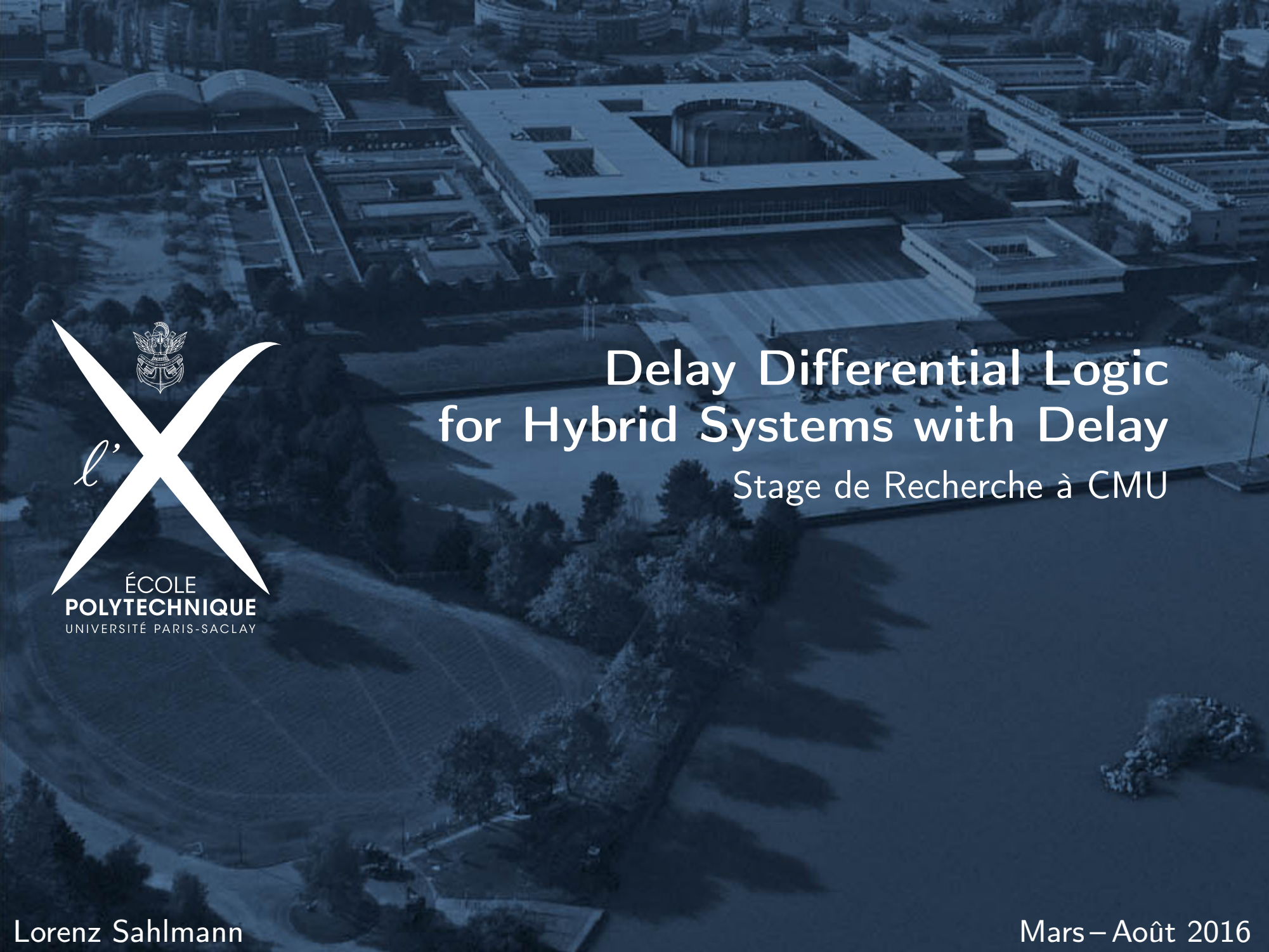


Delay Differential Logic for Hybrid Systems with Delay

Stage de Recherche à CMU

ÉCOLE POLYTECHNIQUE
UNIVERSITÉ PARIS-SACLAY

Lorenz Sahlmann

Mars – Août 2016

Time-delay Systems

- $\mathsf{d}\mathcal{L}$ for hybrid (dynamical) systems with ODEs
- CPS: connection between physical world and cyber part may be delayed
- introduce **delay differential dynamic logic** ($\mathsf{dd}\mathcal{L}$)
- a first-order modal logic for time-delay systems

Time-delay Systems

- $\mathsf{d}\mathcal{L}$ for hybrid (dynamical) systems with ODEs
- CPS: connection between physical world and cyber part may be delayed
- introduce **delay differential dynamic logic** ($\mathsf{dd}\mathcal{L}$)
- a first-order modal logic for time-delay systems

Time-delay Systems

- $\mathsf{d}\mathcal{L}$ for hybrid (dynamical) systems with ODEs
- CPS: connection between physical world and cyber part may be delayed
- introduce **delay differential dynamic logic** ($\mathsf{dd}\mathcal{L}$)
- a first-order modal logic for time-delay systems

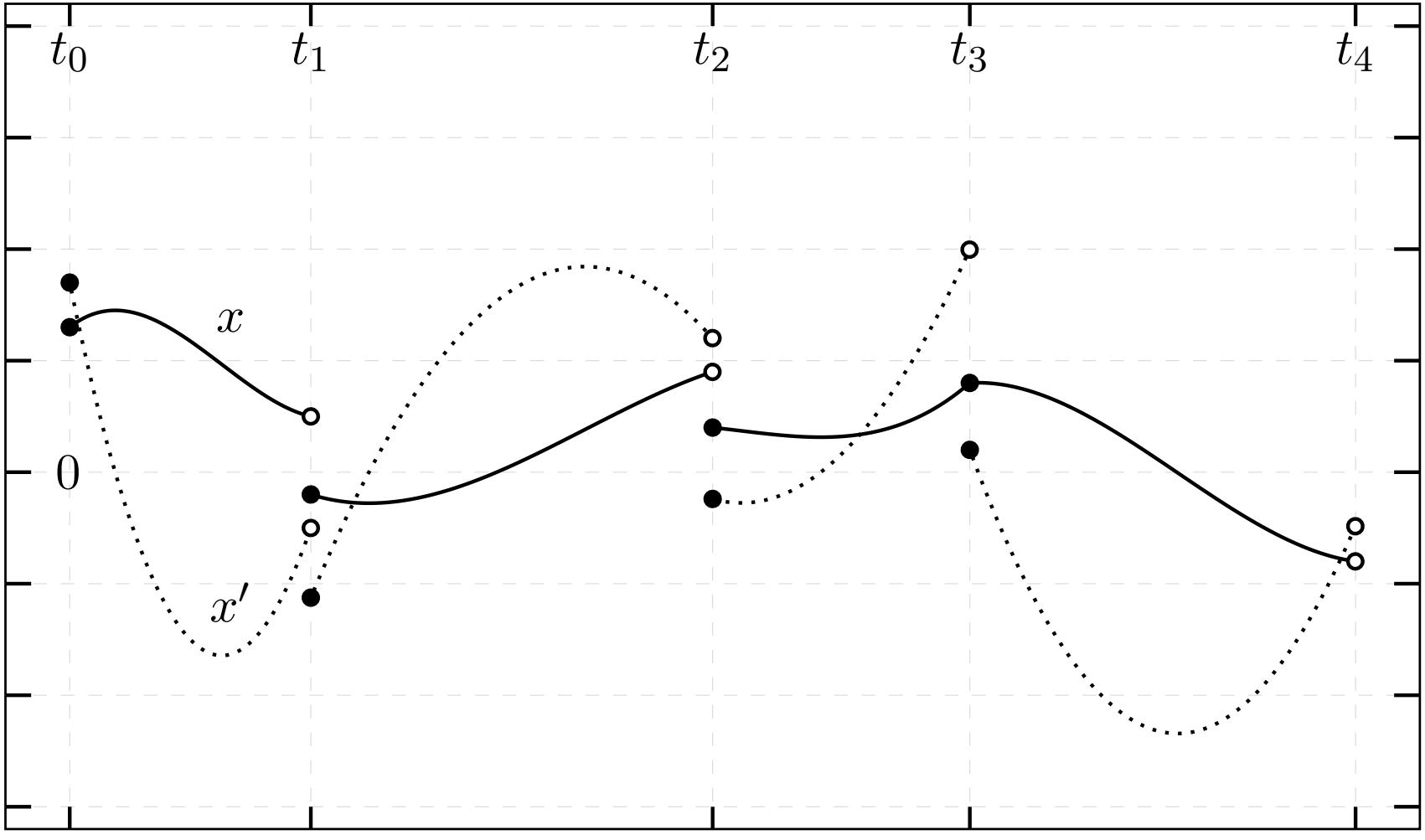
Time-delay Systems

- $\mathsf{d}\mathcal{L}$ for hybrid (dynamical) systems with ODEs
- CPS: connection between physical world and cyber part may be delayed
- introduce **delay differential dynamic logic** ($\mathsf{dd}\mathcal{L}$)
- a first-order modal logic for time-delay systems

Example

TODO

Piecewise



Piecewise

Definition (Piecewise Continuously Differentiable)

Given a finite partition $\{a = t_0 < t_1 < \ldots < t_p = b\}$ of $[a, b]$,

$$x \colon [a, b] \to \mathbb{R}^n$$

is m-times **piecewise continuously differentiable** iff

1. x is m-times continuously differentiable on each (t_i, t_{i+1})
2. $\lim\limits_{\substack{t \nearrow t_{i+1} \\ t \in (t_i, t_{i+1})}} x^{(k)}(t)$ exist
3. $\lim\limits_{\substack{t \searrow t_i \\ t \in (t_i, t_{i+1})}} x^{(k)}(t) = x^{(k)}(t_i)$

for all $k = 0, \ldots, m$.

Delay Differential Equations

Definition (DDE)

For $\{\tau_j \in \mathbb{R} \mid 0 < \tau_1 < \ldots < \tau_k\}$ and $f \colon \mathbb{R} \times \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}^n$

$$x'(t) = f(t, x(t), x(t-\tau_1), \ldots, x(t-\tau_k))$$

is a **delay differential equation** with multiple constant delays. Let $\tau_{\max} \stackrel{\text{def}}{=} \tau_k$ **maximal** and $\tau_{\min} \stackrel{\text{def}}{=} \tau_1$ **minimal delay**.

Definition (IVP)

For an **initial condition** $x_\sigma \colon [\sigma - \tau_{\max}, \sigma] \to \mathbb{R}^n$, solving

$$\begin{cases} x'(t) = f(t, x(t), x(t-\tau_1), \ldots, x(t-\tau_k)) & \text{for } t \geq \sigma \\ x(t) = x_\sigma(t) & \text{for } t \in [\sigma - \tau_{\max}, \sigma] \end{cases}$$

is the **initial value problem**.

Delay Differential Equations

Definition (DDE)

For $\{\tau_j \in \mathbb{R} \mid 0 < \tau_1 < \ldots < \tau_k\}$ and $f \colon \mathbb{R} \times \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}^n$

$$x'(t) = f(t, x(t), x(t-\tau_1), \ldots, x(t-\tau_k))$$

is a **delay differential equation** with multiple constant delays. Let $\tau_{\max} \stackrel{\text{def}}{=} \tau_k$ **maximal** and $\tau_{\min} \stackrel{\text{def}}{=} \tau_1$ **minimal delay**.

Definition (IVP)

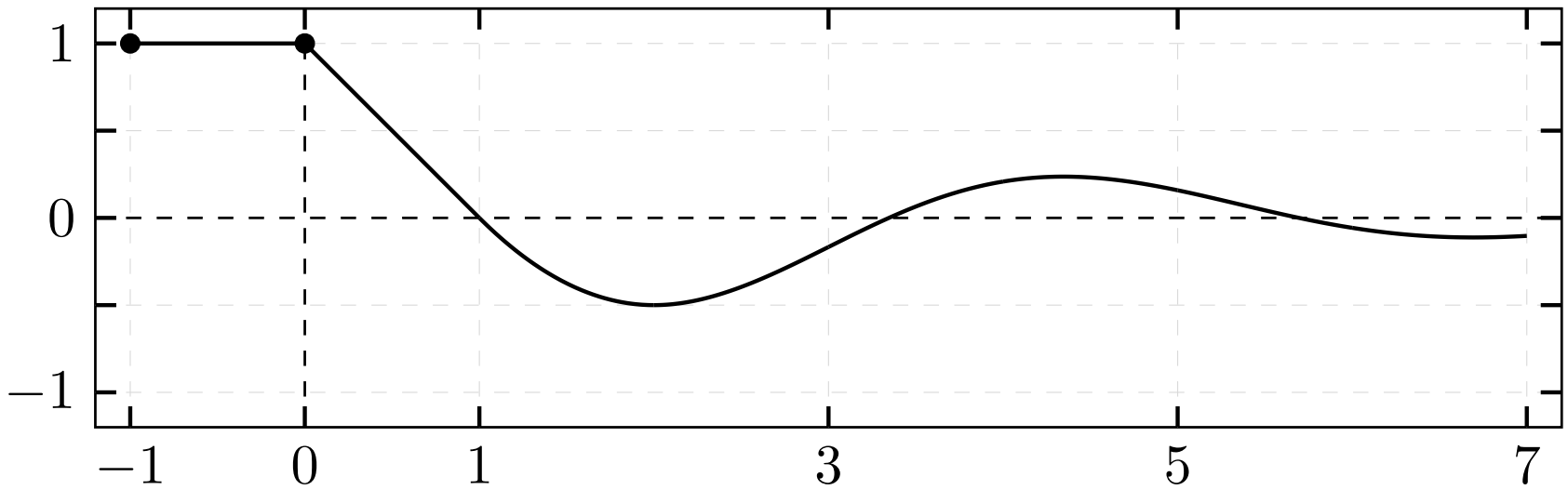
For an **initial condition** $x_\sigma \colon [\sigma - \tau_{\max}, \sigma] \to \mathbb{R}^n$, solving

$$\begin{cases} x'(t) = f(t, x(t), x(t-\tau_1), \ldots, x(t-\tau_k)) & \text{for } t \geq \sigma \\ x(t) = x_\sigma(t) & \text{for } t \in [\sigma - \tau_{\max}, \sigma] \end{cases}$$

is the **initial value problem**.

Example DDE

$$\begin{cases} x'(t) = -x(t-1) & t \geq 0 \\ x(t) = 1 & t \in [-1, 0] \end{cases}$$



Solutions

Theorem (Existence of a unique solution)

Let $f : \mathbb{R} \times \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}^n$ *continuous and Lipschitz in its first argument and* x_σ ***piecewise continuous***,
then there ***exists*** *a* ***unique local solution*** *of the IVP on a time interval* $[\sigma - \tau_{\max}, \sigma + T]$.

ddℒ Syntax

Notation for **hybrid programs** with DDEs:

Definition (dHPs)

Delay hybrid programs are defined by

$$\alpha, \beta ::= x := \theta \mid x' := \theta \mid ?\phi \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \mid x' = \theta \,\&\, \chi$$

with ddℒ term θ, ddℒ formula ϕ, $\mathrm{FOL}_{\mathbb{R}}$ formula χ.

dd$\mathcal{L}$ Syntax

Definition (s-Terms)

S-terms are defined by

$$
\begin{aligned}
\theta(s), \eta(s) ::= {} & a && \text{constants} \\
| {} & x[s] \mid x'[s] && \text{delay range symbols} \\
| {} & x[c] \mid x'[c] && \text{const. delay symbols} \\
| {} & f(\theta_1(s), \ldots, \theta_k(s)) && \text{functions} \\
| {} & \theta(s) + \eta(s) && \text{addition} \\
| {} & \theta(s) \cdot \eta(s) && \text{multiplication} \\
| {} & (\theta(s))' && \text{differentials}
\end{aligned}
$$

with $a \in \mathbb{Q}$, $c \in \mathbb{Q}_0^-$ constant parameter, s past parameter, variable $x \in \mathcal{V}$, differential symbol $x' \in \mathcal{V}'$.

dd$\mathcal{L}$ Syntax

Definition (s-Terms)

S-terms are defined by

$$
\begin{aligned}
\theta(s), \eta(s) ::= {} & a && \text{constants} \\
| {} & x[s] \mid x'[s] && \text{delay range symbols} \\
| {} & x[c] \mid x'[c] && \text{const. delay symbols} \\
| {} & f(\theta_1(s), \ldots, \theta_k(s)) && \text{functions} \\
| {} & \theta(s) + \eta(s) && \text{addition} \\
| {} & \theta(s) \cdot \eta(s) && \text{multiplication} \\
| {} & (\theta(s))' && \text{differentials}
\end{aligned}
$$

with $a \in \mathbb{Q}$, $c \in \mathbb{Q}_0^-$ constant parameter, s past parameter, variable $x \in \mathcal{V}$, differential symbol $x' \in \mathcal{V}'$.

If $x[s] \notin \theta(s)$ and $x'[s] \notin \theta(s)$, write θ and x for $x[0]$.

dd$\mathcal{L}$ Syntax

Definition (s-Formulas)

S-formulas are defined by

$$
\begin{array}{rll}
\phi(s), \psi(s) ::= & \forall[-T)\, \phi(s) & \text{state domain} \\
& \mid \theta(s) = \eta(s) \mid \theta(s) \geq \eta(s) & \text{comparisons} \\
& \mid p(\theta_1(s), \ldots, \theta_k(s)) & \text{predicates} \\
& \mid \neg\phi(s) \mid \phi(s) \wedge \psi(s) & \text{propositional logic} \\
& \mid \forall x\, \phi(s) \mid \exists x\, \phi(s) & \text{quantifiers} \\
& \mid [\alpha]\phi(s) \mid \langle\alpha\rangle\phi(s) & \text{modalities}
\end{array}
$$

with s-terms $\theta(s), \eta(s)$. $T \geq 0$ is defined by static semantics.

dd$\mathcal{L}$ Syntax

Definition (s-Formulas)

S-formulas are defined by

$$
\begin{aligned}
\phi(s), \psi(s) ::= {} & \forall[-T)\, \phi(s) && \text{state domain} \\
& \mid \theta(s) = \eta(s) \mid \theta(s) \geq \eta(s) && \text{comparisons} \\
& \mid p(\theta_1(s), \ldots, \theta_k(s)) && \text{predicates} \\
& \mid \neg\phi(s) \mid \phi(s) \wedge \psi(s) && \text{propositional logic} \\
& \mid \forall x\, \phi(s) \mid \exists x\, \phi(s) && \text{quantifiers} \\
& \mid [\alpha]\phi(s) \mid \langle\alpha\rangle\phi(s) && \text{modalities}
\end{aligned}
$$

with s-terms $\theta(s), \eta(s)$. $T \geq 0$ is defined by static semantics.

The only way to **bind** s is by $\forall[-T)$. Write ϕ if s is **not free**.

dd$\mathcal{L}$ Syntax

Definition (s-Formulas)

S-formulas are defined by

$$
\begin{aligned}
\phi(s), \psi(s) ::= {} & \forall[-T)\, \phi(s) && \text{state domain} \\
& \mid \theta(s) = \eta(s) \mid \theta(s) \geq \eta(s) && \text{comparisons} \\
& \mid p(\theta_1(s), \ldots, \theta_k(s)) && \text{predicates} \\
& \mid \neg\phi(s) \mid \phi(s) \wedge \psi(s) && \text{propositional logic} \\
& \mid \forall x\, \phi(s) \mid \exists x\, \phi(s) && \text{quantifiers} \\
& \mid [\alpha]\phi(s) \mid \langle\alpha\rangle\phi(s) && \text{modalities}
\end{aligned}
$$

with s-terms $\theta(s), \eta(s)$. $T \geq 0$ is defined by static semantics.

The only way to **bind** s is by $\forall[-T)$. Write ϕ if s is **not free**. $\phi(r)$ substitutes s by $r \in \mathbb{R}_0^-$, even if in scope of $\forall[-T)$.

Semantics

- state space $C^1_{\text{pw}}([-T, 0], \mathbb{R}^n)$
- valuation depends on assignment $r \in [-T, 0]$ to s
- Example

$$[\![\forall[-T)\, \phi(s)]\!]^I_r = \left\{ \nu \in \mathcal{S} \;\middle|\; \forall \tilde{r} \in [-T, 0) \,:\, \nu \in [\![\phi(s)]\!]^I_{\tilde{r}} \right\}$$

with set of states $\mathcal{S}$.

Semantics

- state space $C^1_{\text{pw}}([-T, 0], \mathbb{R}^n)$
- valuation depends on assignment $r \in [-T, 0]$ to s
- Example

$$[\![\forall[-T)\, \phi(s)]\!]^I_r = \left\{ \nu \in \mathcal{S} \;\middle|\; \forall \tilde{r} \in [-T, 0) \,:\, \nu \in [\![\phi(s)]\!]^I_{\tilde{r}} \right\}$$

with set of states $\mathcal{S}$.

Semantics

- state space $C^1_{\text{pw}}([-T, 0], \mathbb{R}^n)$
- valuation depends on assignment $r \in [-T, 0]$ to s
- Example

$$[\![\forall[-T)\, \phi(s)]\!]^I_r = \left\{ \nu \in \mathcal{S} \;\middle|\; \forall \tilde{r} \in [-T, 0) : \; \nu \in [\![\phi(s)]\!]^I_{\tilde{r}} \right\}$$

with set of states $\mathcal{S}$.

Proof Calculus

Hilbert style calculus with proof rules:

$$\text{(G)} \quad \frac{\phi(s)}{[\alpha]\phi(s)}$$

$$\text{(MP)} \quad \frac{\phi(s) \to \psi(s) \quad \phi(s)}{\psi(s)}$$

$$(\forall) \quad \frac{\phi(s)}{\forall x\, \phi(s)}$$

Axiomatization

$\langle\cdot\rangle \quad \langle\alpha\rangle\phi(s) \leftrightarrow \neg[\alpha]\neg\phi(s)$

$[\cup] \quad [\alpha \cup \beta]\phi(s) \leftrightarrow [\alpha]\phi(s) \wedge [\beta]\phi(s)$

$[;] \quad [\alpha;\beta]\phi(s) \leftrightarrow [\alpha][\beta]\phi(s)$

$[*] \quad [\alpha^*]\phi(s) \leftrightarrow \phi(s) \wedge [\alpha][\alpha^*]\phi(s)$

$\mathrm{K} \quad [\alpha]\big(\phi(s) \to \psi(s)\big) \to \big([\alpha]\phi(s) \to [\alpha]\psi(s)\big)$

$\mathrm{I} \quad [\alpha^*]\big(\phi(s) \to [\alpha]\phi(s)\big) \to \big(\phi(s) \to [\alpha^*]\phi(s)\big)$

$\mathrm{B} \quad \forall x\,[\alpha]\phi(s) \to [\alpha]\forall x\,\phi(s) \qquad (x \notin \alpha)$

$\mathrm{V} \quad \phi(s) \to [\alpha]\phi(s) \qquad (\mathrm{FV}(\phi) \cap \mathrm{BV}(\alpha) = \emptyset)$

Axiomatization

Assignment only changes present value, not past!

$$[:=] \quad [x := \theta]\phi(s, x[0]) \leftrightarrow \phi(s, \theta)$$

Test condition over entire state possible

$$[?] \quad [?\psi]\phi(s) \leftrightarrow \big(\psi \rightarrow \phi(s)\big)$$

Axiomatization

$$c' \quad (a)' = 0$$

$$x[\cdot]' \quad x'[c] = (x[c])', \quad x'[s] = (x[s])'$$

$$+' \quad (\theta(s) + \eta(s))' = (\theta(s))' + (\eta(s))'$$

$$\cdot' \quad (\theta(s) \cdot \eta(s))' = (\theta(s))' \cdot \eta(s) + \theta(s) \cdot (\eta(s))'$$

$$\text{DW} \quad [x' = \theta \,\&\, \chi]\chi$$

$$\text{DC} \quad \big([x' = \theta \,\&\, \chi]\phi(s) \leftrightarrow [x' = \theta \,\&\, \chi \wedge \varphi]\phi(s)\big) \leftarrow [x' = \theta \,\&\, \chi]\varphi$$

$$\text{DE} \quad [x' = \theta \,\&\, \chi]\phi(s, x, x') \leftrightarrow [x' = \theta \,\&\, \chi][x' := \theta]\phi(s, x, x')$$

$$\text{DI} \quad [x' = \theta \,\&\, \chi]\varphi \leftarrow \big(\chi \rightarrow \varphi \wedge [x' = \theta \,\&\, \chi](\varphi)'\big)$$

Delay Differential Weakening

- Extend notation

$$\forall[-T)\,\phi(s) \land \phi(0) \leftrightarrow \forall[-T]\,\phi(s)$$

  to include $s = 0$ into quantification over state domain.
- **delay differential weakening** axiom

$$\text{DDW}\quad \big(\psi \to [x' = \theta \,\&\, \chi]\forall[-T]\,\phi(s)\big) \leftarrow \big((\psi \to \forall[-T)\,\phi(s)) \land \forall x\,(\chi \to \phi(0))\big)$$

  where $x[c] \notin \phi(s)$ (only $x[s]$ and $x'[s]$).
- values in the state after a DDE were either specified in the initial condition or result from evolution

Delay Differential Weakening

- Extend notation

$$\forall[-T)\,\phi(s) \land \phi(0) \leftrightarrow \forall[-T]\,\phi(s)$$

  to include $s = 0$ into quantification over state domain.
- **delay differential weakening** axiom

$$\text{DDW}\quad \big(\psi \to [x' = \theta \,\&\, \chi]\forall[-T]\,\phi(s)\big) \leftarrow \big((\psi \to \forall[-T)\,\phi(s)) \land \forall x\,(\chi \to \phi(0))\big)$$

  where $x[c] \notin \phi(s)$ (only $x[s]$ and $x'[s]$).
- values in the state after a DDE were either specified in the initial condition or result from evolution

Delay Differential Weakening

- Extend notation

$$\forall[-T)\,\phi(s) \wedge \phi(0) \leftrightarrow \forall[-T]\,\phi(s)$$

  to include $s = 0$ into quantification over state domain.
- **delay differential weakening** axiom

$$\text{DDW}\quad \big(\psi \rightarrow [x' = \theta \,\&\, \chi]\forall[-T]\,\phi(s)\big) \leftarrow \big((\psi \rightarrow \forall[-T)\,\phi(s)) \wedge \forall x\,(\chi \rightarrow \phi(0))\big)$$

  where $x[c] \notin \phi(s)$ (only $x[s]$ and $x'[s]$).
- values in the state after a DDE were either specified in the initial condition or result from evolution

Delay Differential Induction

derived **delay differential induction** axiom

$$\text{DDI}\ \frac{\psi \to \forall[-T)\,\phi(s) \quad \forall x\,\big(\chi \wedge \varphi \to \phi(0)\big) \quad \psi \wedge \chi \to \varphi \quad \psi \to [x' = \theta \,\&\, \chi](\varphi)'}{\psi \to [x' = \theta \,\&\, \chi]\forall[-T]\,\phi(s)}$$

with $x[c] \notin \phi(s)$ (as for DDW) and $\text{FOL}_{\mathbb{R}}$ formula φ.

Axiom of Steps

- **method of steps** for DDEs
- reduce DDE to ODE by plugging in initial condition

$$[\rightarrowtail] \quad [x' = \theta \,\&\, \chi]\phi(s) \leftrightarrow [?\chi; x' := \theta; (t := 0; t' = 1, x' = \theta \,\&\, \chi \wedge 0 \leq t \leq \tau_{\min})^*]\phi(s)$$

Example

Prove $x(t) \geq 0$ for all $t \geq 0$:

$$\begin{cases} x'(t) = x(t-\tau) & t \geq 0 \\ x(t) \geq 0 & t \in [-\tau, 0] \end{cases}$$

for any $\tau > 0$, using the invariant $\varphi \equiv (x^3 \geq 0)$

Example (Proof)

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(\forall[-T]\,x[s]\geq 0 \to x^3\geq 0 \wedge 3x^2x[-\tau]\geq 0 \wedge \forall[-T)\,x[s]\geq 0) \wedge \forall x\,(x^3\geq 0 \to x\geq 0)}\,\mathbb{R}}{(\forall[-T]\,x[s]\geq 0 \to x^3\geq 0 \wedge [x':=x[-\tau]](3x^2x'\geq 0) \wedge \forall[-T)\,x[s]\geq 0) \wedge \forall x\,(x^3\geq 0 \to x\geq 0)}\,[:=]}{(\forall[-T]\,x[s]\geq 0 \to x^3\geq 0 \wedge [x'=x[-\tau]](3x^2x'\geq 0) \wedge \forall[-T)\,x[s]\geq 0) \wedge \forall x\,(x^3\geq 0 \to x\geq 0)}\,\text{DE,G}}{\forall[-T]\,x[s]\geq 0 \to x^3\geq 0 \wedge [x'=x[-\tau]\,\&\,x^3\geq 0](\forall[-T]\,x[s]\geq 0) \wedge [x'=x[-\tau]](3x^2x'\geq 0)}\,\text{DDW}}{\forall[-T]\,x[s]\geq 0 \to [x'=x[-\tau]\,\&\,x^3\geq 0](\forall[-T]\,x[s]\geq 0) \wedge [x'=x[-\tau]](x^3\geq 0)}\,\text{DI}}{\forall[-T]\,x[s]\geq 0 \to [x'=x[-\tau]](\forall[-T]\,x[s]\geq 0)}\,\text{DC}
$$

The first three axioms correspond to the derived axiom DDI.

Outlook

- Examples!
- How to find differntial invariants?
- implementation in KeYmaera X
- complete reduction to d$\mathcal{L}$ via [$\rightarrow\!\!|$]-axiom
- More general DDEs...

Outlook

- Examples!
- How to find differntial invariants?
- implementation in KeYmaera X
- complete reduction to $\mathrm{d}\mathcal{L}$ via $[\rightarrow\!\!|]$-axiom
- More general DDEs...

Outlook

- Examples!
- How to find differntial invariants?
- implementation in KeYmaera X
- complete reduction to d$\mathcal{L}$ via [→]-axiom
- More general DDEs...

Outlook

- Examples!
- How to find differntial invariants?
- implementation in KeYmaera X
- complete reduction to $\mathsf{d}\mathcal{L}$ via $[\rightarrow\!\!|]$-axiom
- More general DDEs...

Outlook

- Examples!
- How to find differntial invariants?
- implementation in KeYmaera X
- complete reduction to $\mathsf{d}\mathcal{L}$ via $[\rightarrow\!\!|]$-axiom
- More general DDEs...