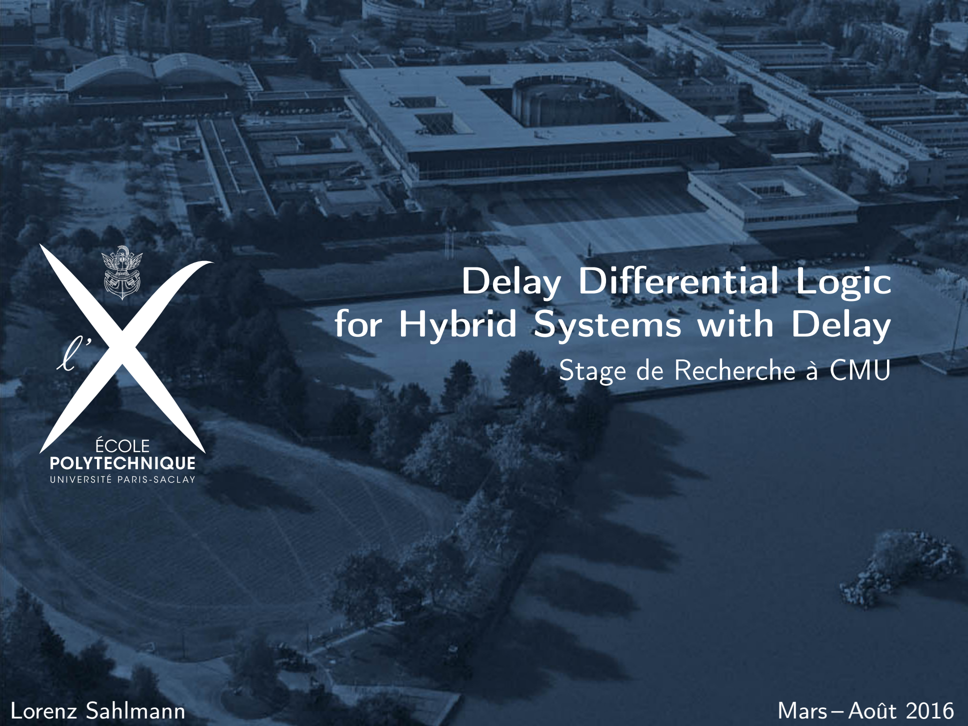


Delay Differential Logic for Hybrid Systems with Delay

Stage de Recherche à CMU

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

Example: stop sign controller

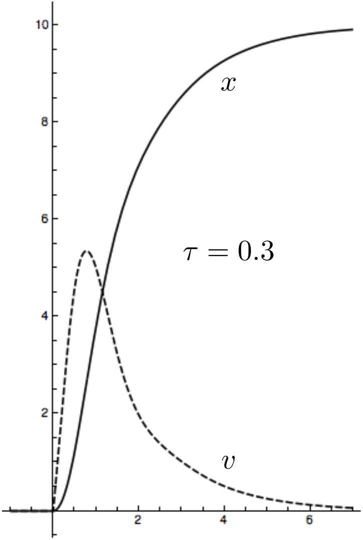
- discrete controller for reference position p_r
- PD-controller for acceleration

$$\begin{cases} x' = v \\ v' = -K_p(x - p_r) - K_d\, v \end{cases}$$

- delay in sensing

$$\begin{cases} x' = v \\ v' = -K_p\big(x(t-\tau) - p_r\big) - K_d\, v(t-\tau) \end{cases}$$

- oscillations



Example: stop sign controller

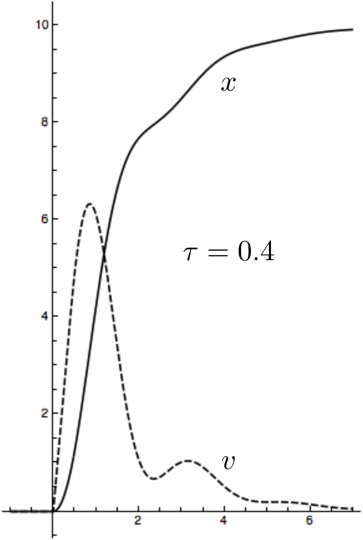
- discrete controller for reference position p_r
- PD-controller for acceleration

$$\begin{cases} x' = v \\ v' = -K_p(x - p_r) - K_d\, v \end{cases}$$

- delay in sensing

$$\begin{cases} x' = v \\ v' = -K_p\big(x(t-\tau) - p_r\big) - K_d\, v(t-\tau) \end{cases}$$

- oszillations



Example: stop sign controller

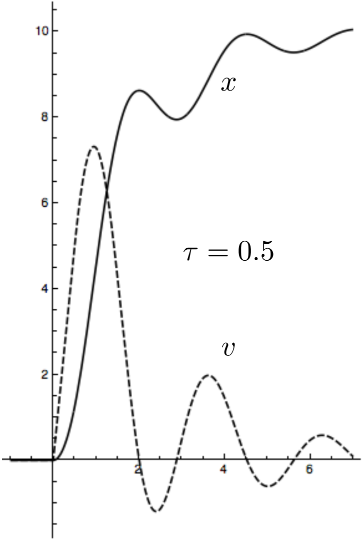
- discrete controller for reference position p_r
- PD-controller for acceleration

$$\begin{cases} x' = v \\ v' = -K_p(x - p_r) - K_d\, v \end{cases}$$

- delay in sensing

$$\begin{cases} x' = v \\ v' = -K_p\big(x(t-\tau) - p_r\big) - K_d\, v(t-\tau) \end{cases}$$

- oszillations



Delay Differential Equations

Definition (DDE)

For delay $\tau > 0$ and $f\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$,

$$x'(t) = f(x(t), x(t-\tau))$$

is a **delay differential equation** with constant delay.
Can be extended to multiple delays.

Definition (IVP)

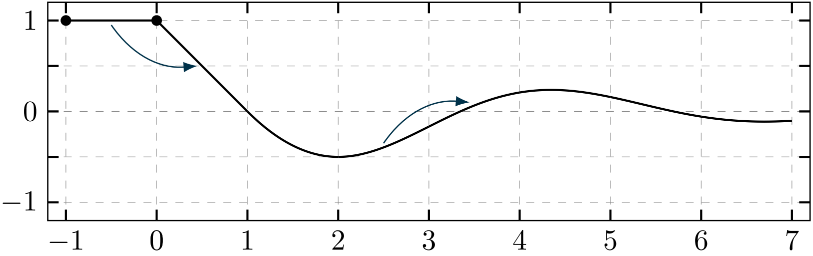
For an **initial condition** $x_\sigma\colon [\sigma - \tau, \sigma] \to \mathbb{R}^n$, solving

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

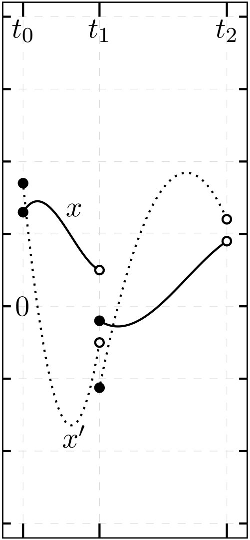
is the **initial value problem**.

Example DDE

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



Piecewise



Definition (Piecewise Cont. Differentiable)

For a partition $\{a = t_0 < t_1 < \ldots < t_p = b\}$,

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

is m-times **piecewise continuously differentiable** iff for all $k = 0, \ldots, m$:

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. $\lim\limits_{\substack{t \searrow t_i \\ t \in (t_i, t_{i+1})}} x^{(k)}(t) = x^{(k)}(t_i)$

Solutions

Theorem (Existence of a unique solution)

*Let $f: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ 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 $[\sigma - \tau, \sigma + T]$.*

Towards Logics

Example DDE: show $x(t) \le 1$ for all $t \ge 0$

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

Notation in $\mathsf{dd}\mathcal{L}$

$$\forall [-1]\, x[s] = 1 \to [x' = x[-1]](x \le 1)$$

dd$\mathcal{L}$ 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 dd$\mathcal{L}$ term θ, dd$\mathcal{L}$ formula ϕ, $\mathrm{FOL}_{\mathbb{R}}$ formula χ.

dd$\mathcal{L}$ Syntax

Definition (s-Terms)

S-terms are defined by

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

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

d$\mathcal{L}$ Syntax

Definition (s-Formulas)

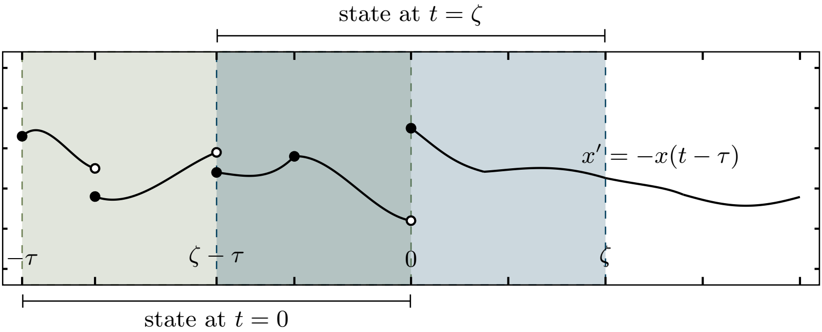
S-formulas are defined by

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

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**.

Semantics



- state space $C^1_{\mathrm{pw}}([-T, 0], \mathbb{R}^n)$

Semantics

- valuation of s-terms and s-formulas
- depends on assignment $r \in [-T, 0]$ to s
- Example

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

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

Proof Calculus

Hilbert style calculus with proof rules:

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

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

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

Proof Calculus

$$
\begin{array}{rll}
\langle\cdot\rangle & \langle\alpha\rangle\phi(s) \leftrightarrow \neg[\alpha]\neg\phi(s) & \\
[\cup] & [\alpha\cup\beta]\phi(s) \leftrightarrow [\alpha]\phi(s) \wedge [\beta]\phi(s) & \\
[;] & [\alpha;\beta]\phi(s) \leftrightarrow [\alpha][\beta]\phi(s) & \\
[*] & [\alpha^*]\phi(s) \leftrightarrow \phi(s) \wedge [\alpha][\alpha^*]\phi(s) & \\
\mathrm{K} & [\alpha]\big(\phi(s) \rightarrow \psi(s)\big) \rightarrow \big([\alpha]\phi(s) \rightarrow [\alpha]\psi(s)\big) & \\
\mathrm{I} & [\alpha^*]\big(\phi(s) \rightarrow [\alpha]\phi(s)\big) \rightarrow \big(\phi(s) \rightarrow [\alpha^*]\phi(s)\big) & \\
\mathrm{B} & \forall x\,[\alpha]\phi(s) \rightarrow [\alpha]\forall x\,\phi(s) & (x \notin \alpha) \\
\mathrm{V} & \phi(s) \rightarrow [\alpha]\phi(s) & (\mathrm{FV}(\phi) \cap \mathrm{BV}(\alpha) = \emptyset)
\end{array}
$$

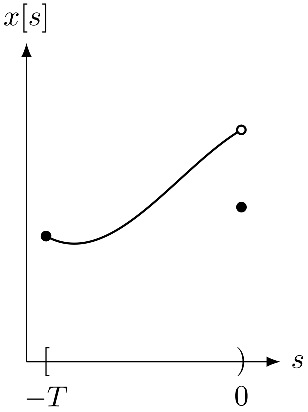
Proof Calculus

- Assignment only changes present value, not past!

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

- Test condition over entire state possible: $\psi \equiv \forall[-T)\,\tilde{\psi}(s)$

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



Proof Calculus

$$
\begin{array}{rl}
c' & (a)' = 0 \\[2ex]
x[\cdot]' & x'[c] = (x[c])', \quad x'[s] = (x[s])' \\[2ex]
+' & (\theta(s) + \eta(s))' = (\theta(s))' + (\eta(s))' \\[2ex]
\cdot' & (\theta(s) \cdot \eta(s))' = (\theta(s))' \cdot \eta(s) + \theta(s) \cdot (\eta(s))' \\[2ex]
\mathrm{DW} & [x' = \theta \,\&\, \chi]\chi \\[2ex]
\mathrm{DC} & \big([x' = \theta \,\&\, \chi]\phi(s) \leftrightarrow [x' = \theta \,\&\, \chi \wedge \varphi]\phi(s)\big) \leftarrow [x' = \theta \,\&\, \chi]\varphi \\[2ex]
\mathrm{DE} & [x' = \theta \,\&\, \chi]\phi(s, x, x') \leftrightarrow [x' = \theta \,\&\, \chi][x' := \theta]\phi(s, x, x') \\[2ex]
\mathrm{DI} & [x' = \theta \,\&\, \chi]\varphi \leftarrow \big(\chi \to \varphi \wedge [x' = \theta \,\&\, \chi](\varphi)'\big)
\end{array}
$$

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

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

  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 Induction

- derived **delay differential induction** axiom
- for s-quantified safety condition

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

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

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

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)

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

The first three axioms correspond to the derived axiom DDI.

Outlook

- Example proofs!
- How to find differential invariants?
- implementation in KeYmaera X
- complete reduction to d$\mathcal{L}$ via [$\rightarrowtail$]-axiom
- more general DDEs...