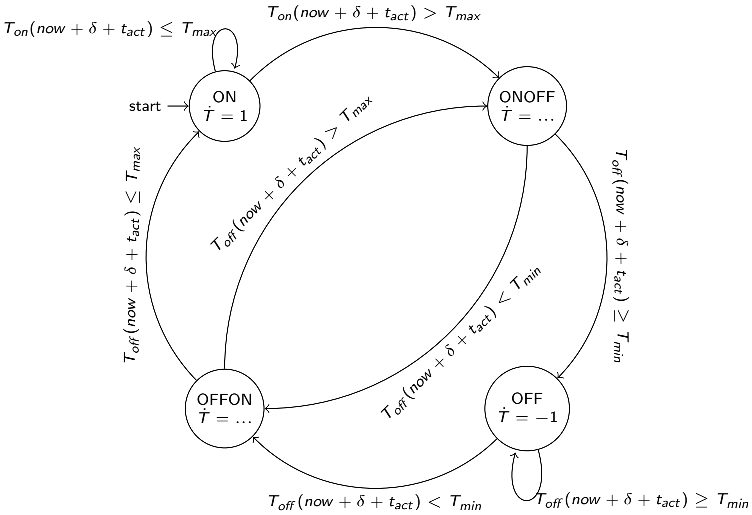
Dependable Hybrid Systems Design: Coping With Errors

Dominique Méry   Zheng Cheng

LORIA

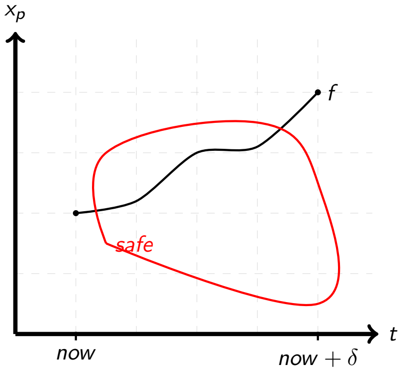
Nov, 2020

Simulation


$T_{on}(now + \delta + t_{act}) \leq T_{max}$
$T_{on}(now + \delta + t_{act}) > T_{max}$
start
ON
$\dot{T} = 1$
ONOFF
$\dot{T} = \dots$
$T_{off}(now + \delta + t_{act}) > T_{max}$
$T_{off}(now + \delta + t_{act}) \leq T_{max}$
$T_{off}(now + \delta + t_{act}) \geq T_{min}$
$T_{off}(now + \delta + t_{act}) < T_{min}$
OFFON
$\dot{T} = \dots$
OFF
$\dot{T} = -1$
$T_{off}(now + \delta + t_{act}) < T_{min}$
$T_{off}(now + \delta + t_{act}) \geq T_{min}$

Assumptions

- Control logic/Simulation based on unique analytic solutions



Determine Uniqueness

Given initial value problem:

$$\begin{cases} \dot{x} = f(t,x) \\ x(t_0) = x_0 \end{cases}$$

Lipschitz-continuous

f is Lipschitz-continuous on set D if there is constant K such that:

$$|f(t,u) - f(t,v)| \leq K|u - v| \text{ for all } (t,u)\ (t,v) \in D \quad (1)$$

Cauchy-Lipschitz theorem

if f is Lipschitz-continuous on D, then initial value problem of f with $(t_0, x_0) \in D$ has a unique solution

Determine Uniqueness: Example

Ex: Let D=R^2, and let $f(t,x) = t^2 + 2x$, for each (t,u) and (t,v) in D, consider:

$$\begin{aligned} |f(t,u) - f(t,v)| &= |(t^2 + 2u) - (t^2 + 2v)| \\ &= 2|u - v| \end{aligned}$$

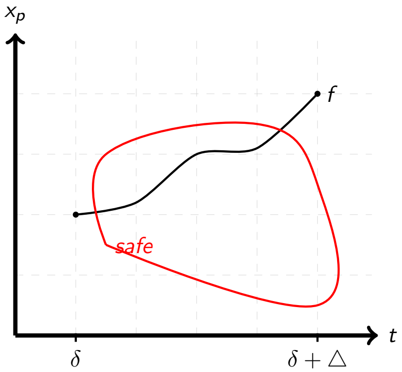
So, f is Lipschitz-continuous on D=R^2 with K=2.

Determine Analytic Solution

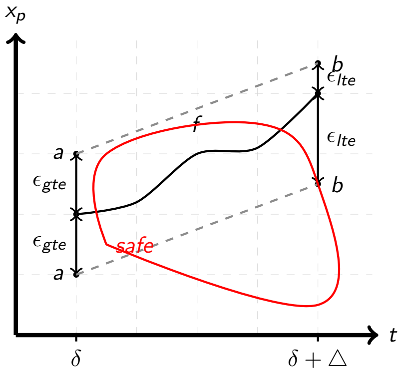
TRY HARD

Assumptions

- Control logic/Simulation based on unique analytic solutions
- Abort if:
  - non-unique
  - non-analytic?

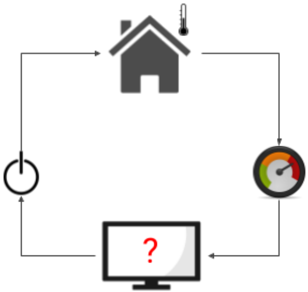


Control Logic Design based on Forward-Euler Method and Truncation Errors



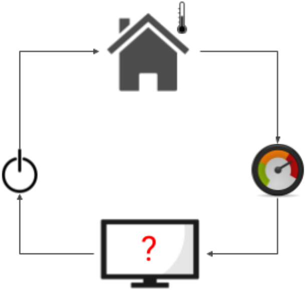
New Heating System

- 2 modes: ON/OFF
- ~~Simple dynamics: $\dot{T}$=1/-1~~
- monotonic T_{on} and T_{off} (no analytic solutions)
- Sample at δ s
- Switch mode costs t_{act} s ($t_{act} < \delta$)
- Safety: $T_{min} \leq$ T $\leq T_{max}$

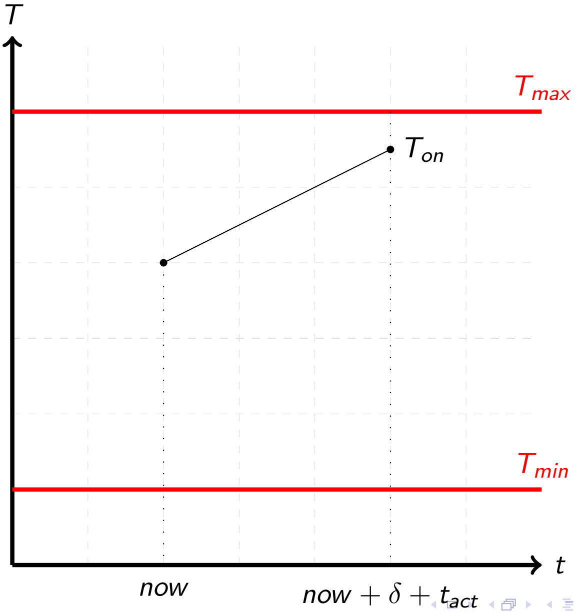


New Heating System

- $|T_{on}(\delta)$ - $Te_{on}(\delta)| \leq \epsilon_{gteon}$
- $|T_{off}(\delta)$ - $Te_{off}(\delta)| \leq \epsilon_{gteoff}$
- $|T_{on}(\delta + \triangle)$ - $Te_{on}(\delta + \triangle)| \leq \epsilon_{lteon}$
- $|T_{off}(\delta + \triangle)$ - $Te_{off}(\delta + \triangle)| \leq \epsilon_{lteoff}$
- $Min \leq \dot{T}_{on}(\delta,\ T_{on}(\delta)) \leq Max$
- $Min \leq \dot{T}_{off}(\delta,\ T_{off}(\delta)) \leq Max$



Case 1: ON mode safe



Case 1: ON mode safe

$$
\begin{aligned}
T_{on}(now + \triangle) &\leq Te_{on}(now + \triangle) + \epsilon_{lte} && (\text{prop}_{lte}) \\
&= T_{on}(now) + \dot{T}_{on}(now, T_{on}(now)) \cdot \triangle + \epsilon_{lte} && (Euler) \\
&\leq T_{on}(now) + Max \cdot \triangle + \epsilon_{lte} && (prop_{\dot{fc}}) \\
&\leq Te_{on}(now) + \epsilon_{gteon} + Max \cdot \triangle + \epsilon_{lte} && (prop_{gte}) \\
&\leq T_{max} && (\text{predict})
\end{aligned}
$$

Case 2: ON mode unsafe

$$\begin{aligned} T_{on}(now + \triangle) &= ... \\ &> T_{max} && \text{(predict)} \end{aligned}$$