

Robust Sampling for MJTL Specifications



Georgios E. Fainekos and George J. Pappas

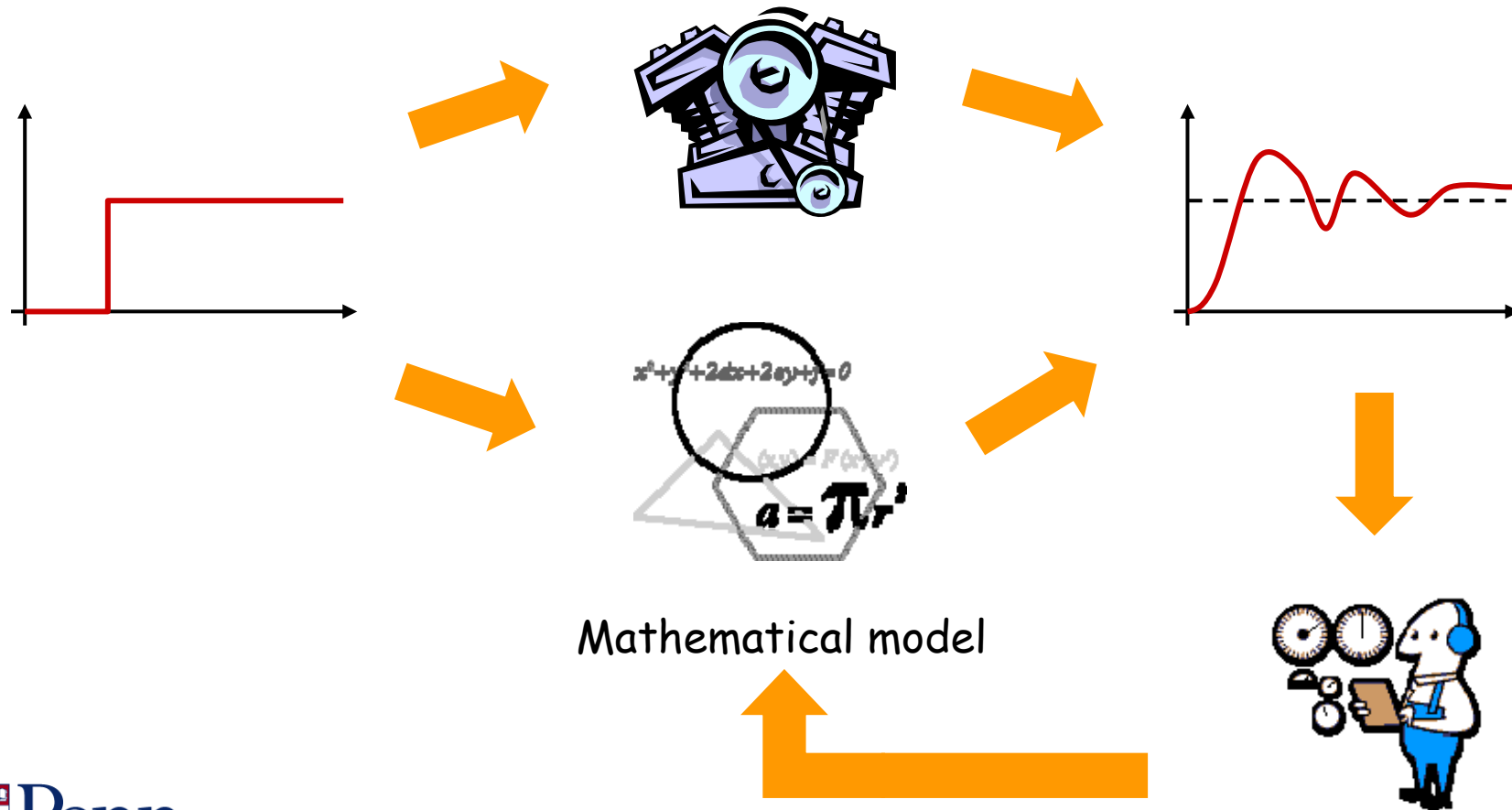
Department of Computer and Information Science
University of Pennsylvania

✉ fainekos @ seas.upenn.edu

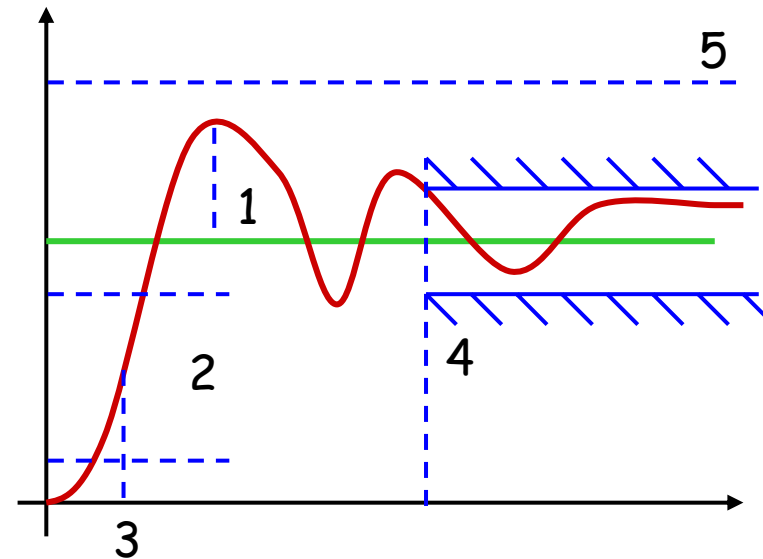
🌐 <http://www.seas.upenn.edu/~fainekos/>

Motivation - a study of transient dynamics

Black-box controller tuning



Motivation - a study of transient dynamics

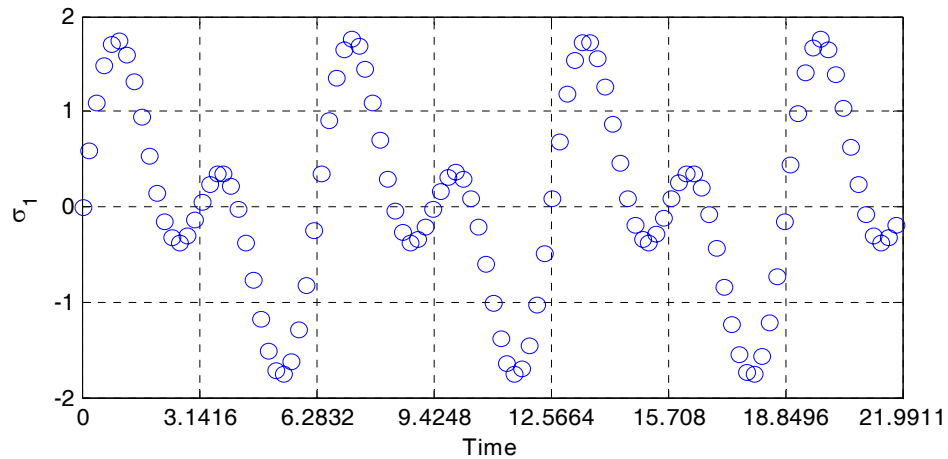
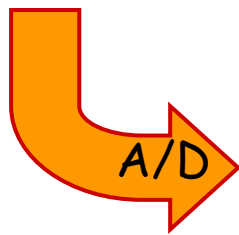
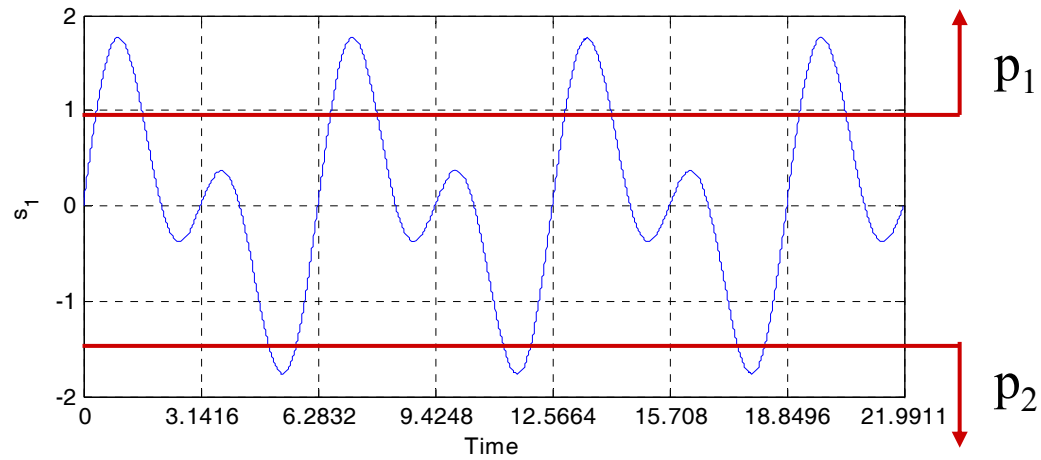


Desired Performance Characteristics

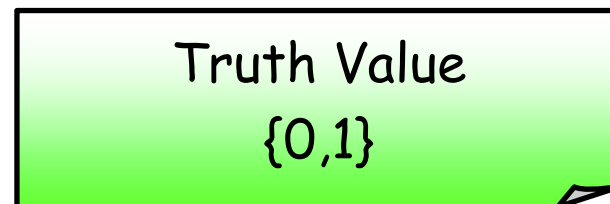
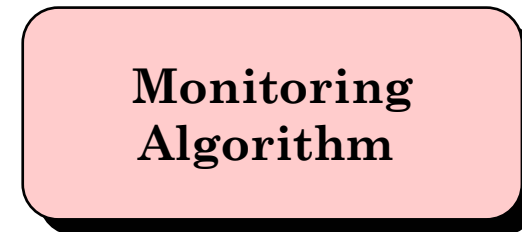
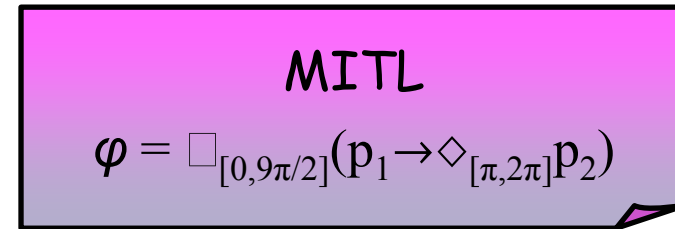
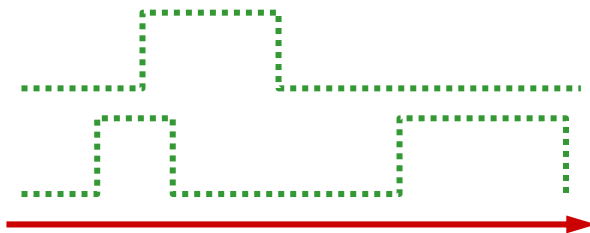
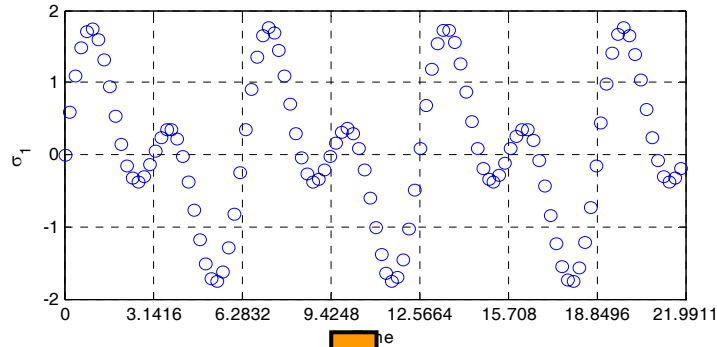
1. Overshoot
2. Rise time
3. Delay time
4. Settling time
5. Constraints on input/states
6. Response sensitivity

Can be captured with
Metric Interval
Temporal Logic

Example

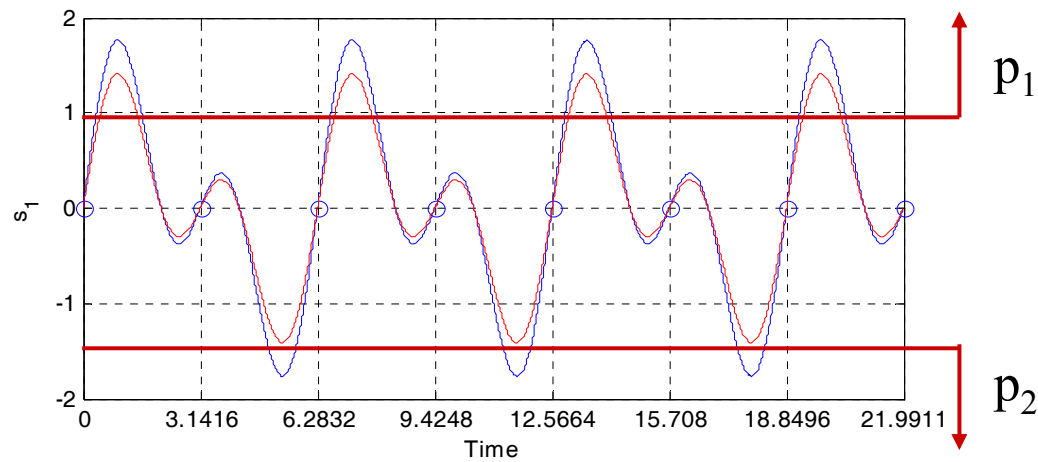


Boolean Monitoring / Testing



[Maler and Nickovic '04]
[Thati and Rosu '04]
[Rosu and Havelund '05]
[Geilen '01]
others ...

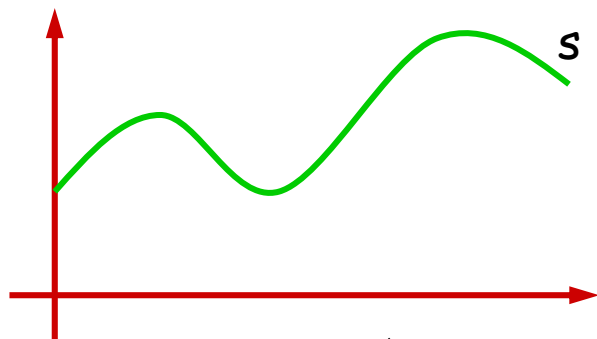
Example - Bad sampling



MITL

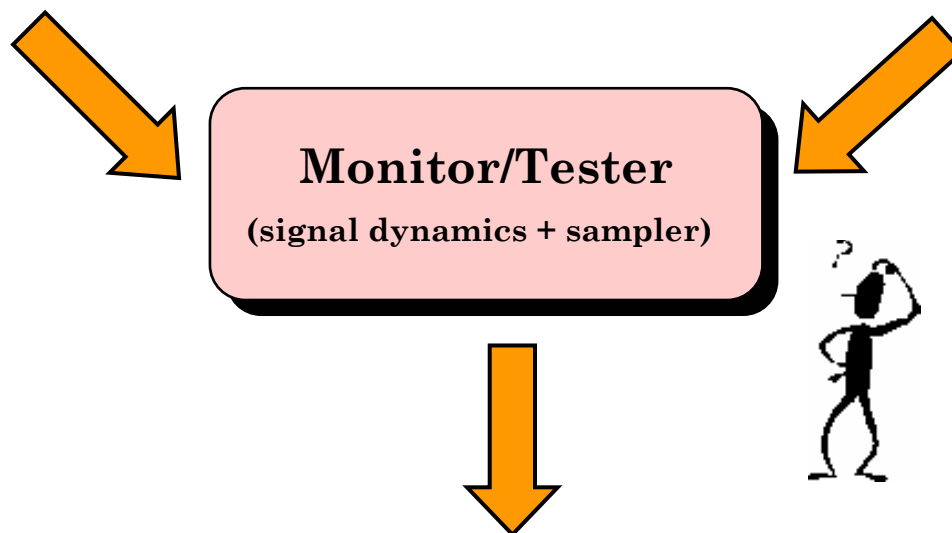
$$\varphi = \square_{[0, 9\pi/2]}(p_1 \rightarrow \diamond_{[\pi, 2\pi]} p_2)$$

Problem formulation



MITL

$$\varphi = \square_{[0,9\pi/2]}(p_1 \rightarrow \diamond_{[\pi,2\pi]} p_2)$$



$$s \models_C \varphi \text{ iff } (s \circ \tau, \tau) \models_D \varphi$$

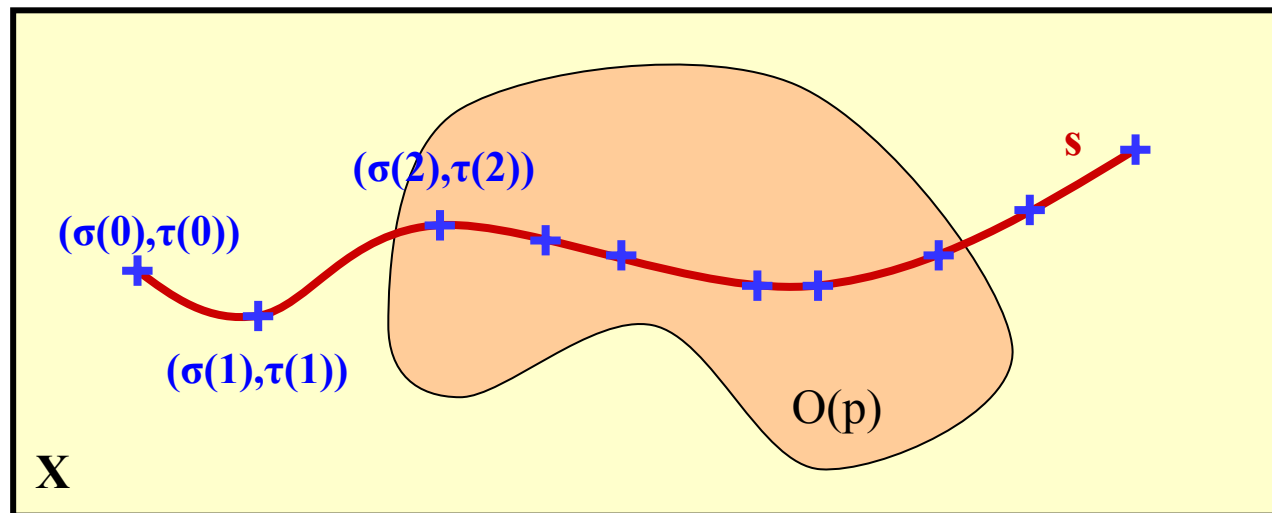
Signals & Timed State Sequences (TSS)

A signal is a function $s : \mathbb{R} \rightarrow X, \mathbb{R} \subseteq \mathbb{R}^+$

A sampling function is a function $\tau : \mathbb{N} \rightarrow \mathbb{R}^+, \mathbb{N} \subseteq \mathbb{N}$

A discrete time signal is a function $\sigma : \mathbb{N} \rightarrow X$ with $\sigma = s \circ \tau$

A timed state sequence μ is the pair (σ, τ)



Metric Interval Temporal Logic (MITL)

Syntax:

$$\Phi_{\mathbb{B}}^+ ::= p \mid \neg p \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2 \mid \varphi_1 \mathcal{R}_I \varphi_2$$

I can be of any bounded or unbounded interval of \mathbb{R}^+ , but $I \neq \emptyset$
i.e. $I = [0, +\infty)$, $I = [2.5, 9.8]$

Boolean Continuous-time MITL Semantics

$$\langle\langle \cdot, \cdot \rangle\rangle_C : \Phi_{\mathbb{B}} \times \mathcal{F}(AP, \mathcal{P}(X)) \rightarrow (\mathcal{F}(R, X) \times R \rightarrow \mathbb{B})$$

$$\langle\langle \phi, \mathcal{O} \rangle\rangle_C(s, t) = \top \iff (\mathcal{O}^{-1} \circ s, t) \models_C \phi$$

$$\langle\langle p \rangle\rangle_C(s, t) := K_{\epsilon}(s(t), \mathcal{O}(p)) = \begin{cases} \top & \text{if } s(t) \in \mathcal{O}(p) \\ \perp & \text{otherwise} \end{cases}$$

$$\langle\langle \neg \phi_1 \rangle\rangle_C(s, t) := \neg \langle\langle \phi_1 \rangle\rangle_C(s, t)$$

$$\langle\langle \phi_1 \vee \phi_2 \rangle\rangle_C(s, t) := \langle\langle \phi_1 \rangle\rangle_C(s, t) \sqcup \langle\langle \phi_2 \rangle\rangle_C(s, t)$$

$$\langle\langle \phi_1 \mathcal{U}_I \phi_2 \rangle\rangle_C(s, t) := \bigsqcup_{t' \in (t +_R \mathcal{I})} \left(\langle\langle \phi_2 \rangle\rangle_C(s, t') \sqcap \prod_{t < t'' < t'} \langle\langle \phi_1 \rangle\rangle_C(s, t'') \right)$$

$$t + \mathcal{I} := \{t + t' \mid t' \in \mathcal{I}\} \quad \text{and} \quad t +_R \mathcal{I} := (t + \mathcal{I}) \cap R$$

$$x \sqcup y := \max(\{x, y\}) \quad x \sqcap y := \min(\{x, y\})$$

MITL Discrete-time Semantics

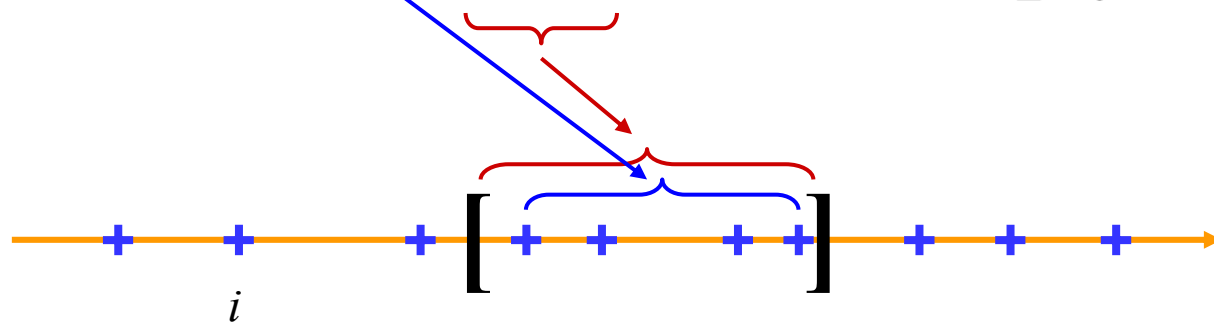
Timed state sequence $\mu = (\sigma, \tau)$, where $\sigma = s \circ \tau$

$$\langle\langle p \rangle\rangle_D(\mu, i) := K_\epsilon(\sigma(i), \mathcal{O}(p))$$

$$\langle\langle \neg \phi_1 \rangle\rangle_D(\mu, i) := \neg \langle\langle \phi_1 \rangle\rangle_D(\mu, i)$$

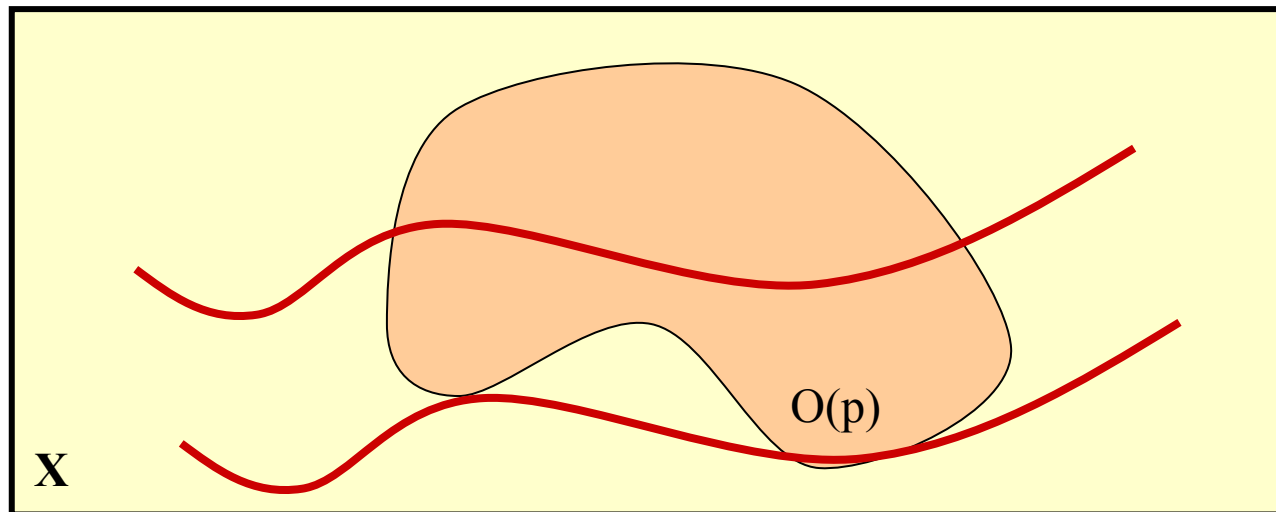
$$\langle\langle \phi_1 \vee \phi_2 \rangle\rangle_D(\mu, i) := \langle\langle \phi_1 \rangle\rangle_D(\mu, i) \sqcup \langle\langle \phi_2 \rangle\rangle_D(\mu, i)$$

$$\langle\langle \phi_1 \mathcal{U}_I \phi_2 \rangle\rangle_D(\mu, i) := \bigsqcup_{j \in \tau^{-1}(\tau(i) + RI)} \left(\langle\langle \phi_2 \rangle\rangle_D(\mu, j) \sqcap \prod_{i \leq k < j} \langle\langle \phi_1 \rangle\rangle_D(\mu, k) \right)$$



Observation

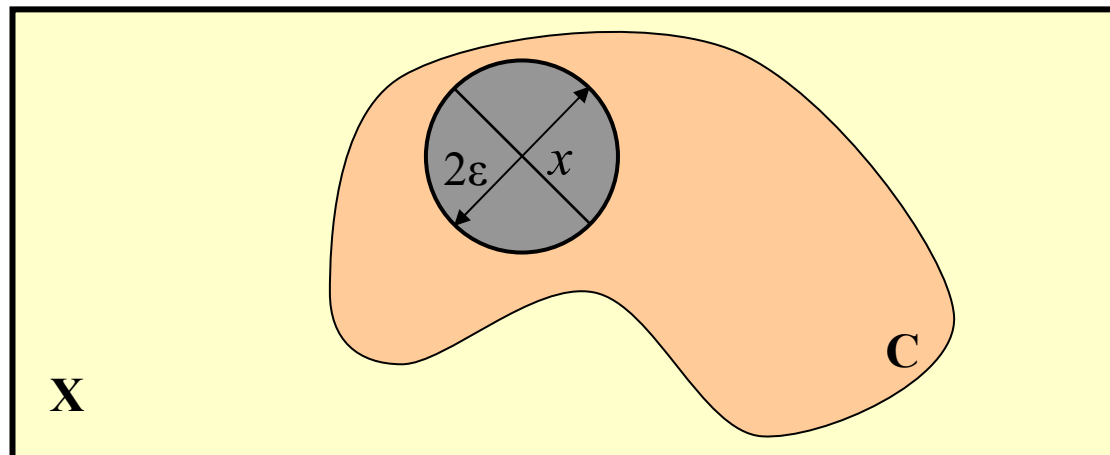
Specification : $\diamond p = T \mathcal{U} p$



Metric Spaces

- A *metric space* (X, d) is a set X with a metric d
- A *metric* on a set X is a positive function $d: X \times X \rightarrow \mathbb{R}^+$, such that the three following properties hold
 - for all $x_1, x_2, x_3 \in X$ it is $d(x_1, x_3) \leq d(x_1, x_2) + d(x_2, x_3)$
 - for all $x_1, x_2 \in X$ it is $d(x_1, x_2) = 0$ iff $x_1 = x_2$
 - for all $x_1, x_2 \in X$ it is $d(x_1, x_2) = d(x_2, x_1)$
- Given a metric d , a radius $\varepsilon \in \mathbb{R}^+$ and a point $x \in X$, then the *open ε -ball* centered at x is defined as

$$B_d(x, \varepsilon) = \{ y \in X \mid d(x, y) < \varepsilon \}$$



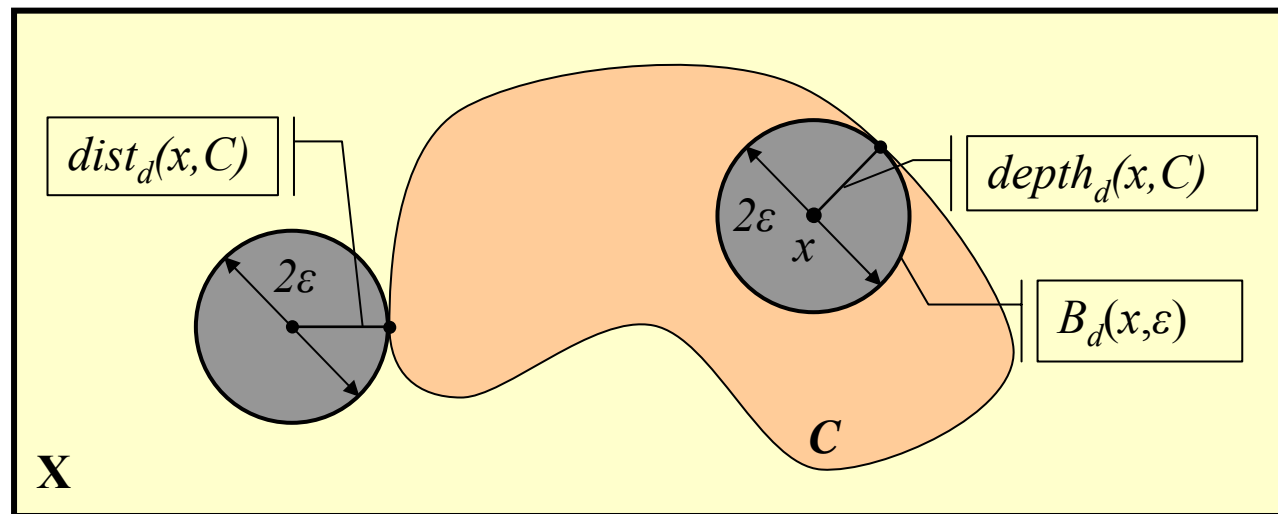
(Signed) Distance

Let $x \in X$ be a point, $C \subseteq X$ be a set and d be a metric. Then we define

$$\text{dist}_d(x, C) := \inf\{d(x, y) \mid y \in \text{cl}(C)\}$$

$$\text{depth}_d(x, C) := \text{dist}_d(x, X \setminus C)$$

$$\text{Dist}_d(x, C) := \begin{cases} -\text{dist}_d(x, C) & \text{if } x \notin C \\ \text{depth}_d(x, C) & \text{if } x \in C \end{cases}$$



Discrete-time Robust Semantics for MITL

$$\llbracket \cdot, \cdot \rrbracket_D : (\Phi_{\text{RUB}} \times \mathcal{F}(AP, \mathcal{P}(X))) \rightarrow (\mathcal{F}(N, X) \times \mathcal{F}_{si}(N, \mathbb{R}_{\geq 0}) \times N \rightarrow \overline{\mathbb{R}})$$

$$\sqcup : \overline{\mathbb{R}} \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}} \quad \sqcap : \overline{\mathbb{R}} \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$$

$$x \sqcup y := \max(\{x, y\}) \quad x \sqcap y := \min(\{x, y\})$$

$$\llbracket c \rrbracket_D(\mu, i) := c$$

$$\llbracket p \rrbracket_D(\mu, i) := \mathbf{Dist}_d(\sigma(i), \mathcal{O}(p))$$

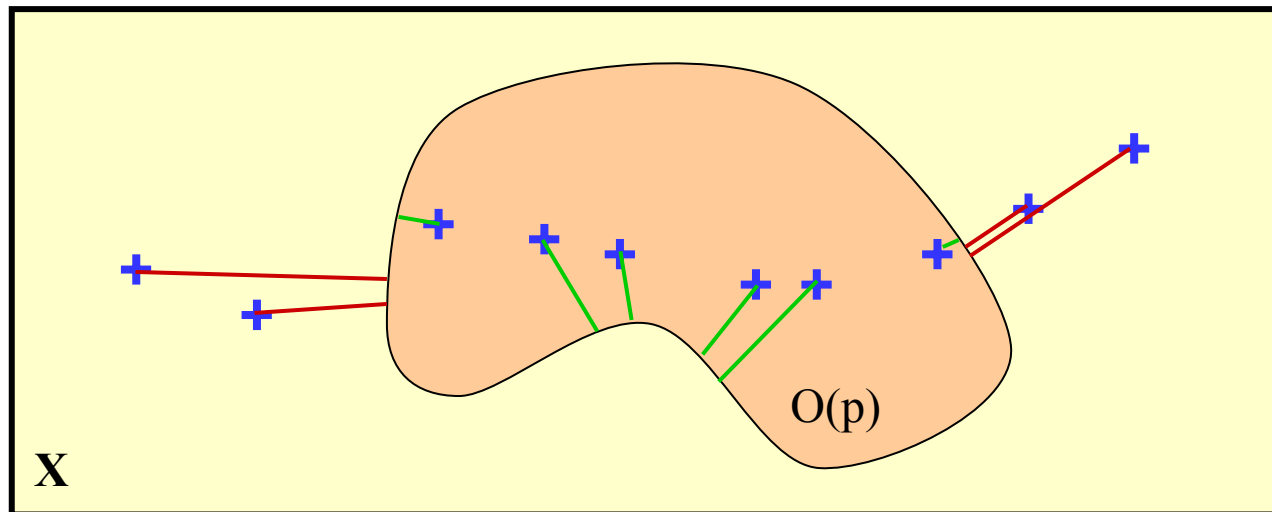
$$\llbracket \neg \phi_1 \rrbracket_D(\mu, i) := -\llbracket \phi_1 \rrbracket_D(\mu, i)$$

$$\llbracket \phi_1 \vee \phi_2 \rrbracket_D(\mu, i) := \llbracket \phi_1 \rrbracket_D(\mu, i) \sqcup \llbracket \phi_2 \rrbracket_D(\mu, i)$$

$$\llbracket \phi_1 \mathcal{U}_I \phi_2 \rrbracket_D(\mu, i) := \bigsqcup_{j \in \tau^{-1}(\tau(i) + RI)} \left(\llbracket \phi_2 \rrbracket_D(\mu, j) \sqcap \prod_{i \leq k < j} \llbracket \phi_1 \rrbracket_D(\mu, k) \right)$$

Intuition - Example

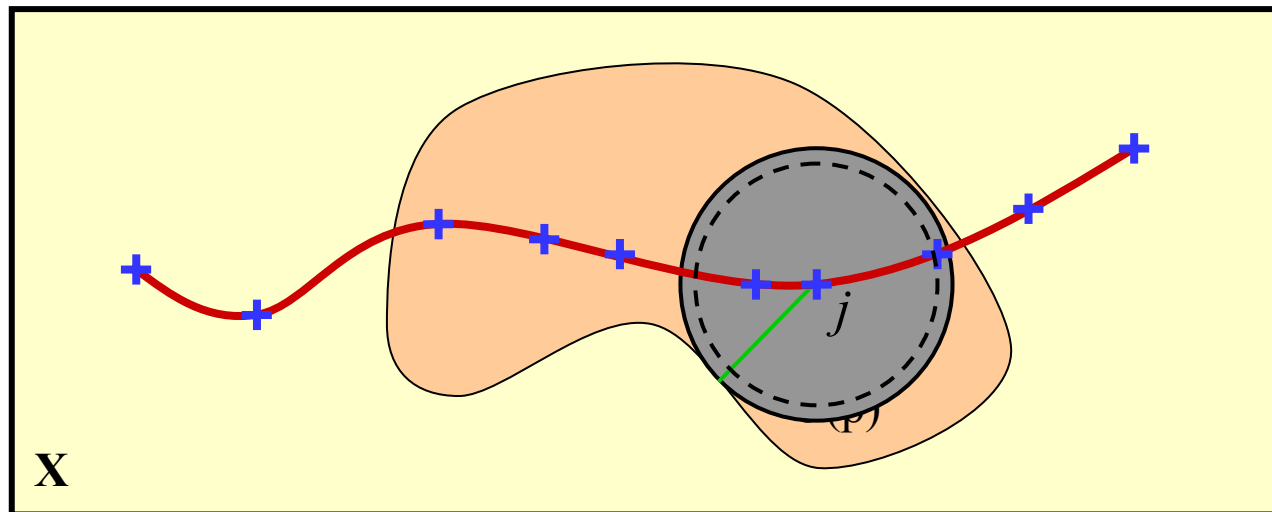
Specification : $\diamond p = T \mathcal{U} p$



$$[[\phi_1 \mathcal{U}_I \phi_2]]_D(\mu, i) := \bigsqcup_{j \in \tau^{-1}(\tau(i) + R\mathcal{I})} \left([[\phi_2]]_D(\mu, j) \sqcap \prod_{i \leq k < j} [[\phi_1]]_D(\mu, k) \right)$$

Observation

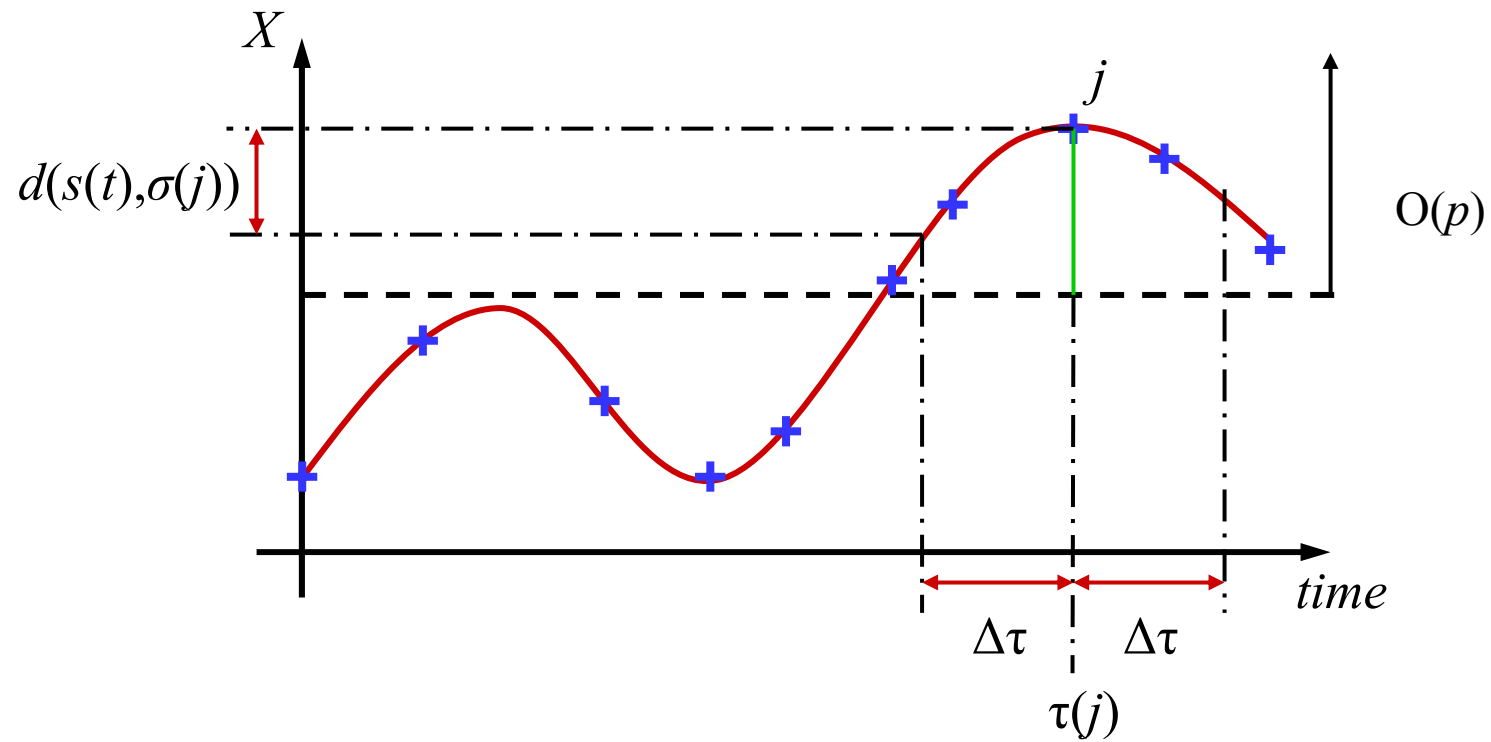
Specification : $\diamond p = T \mathcal{U} p$



If $\forall t \in [\tau(j)-\Delta\tau, \tau(j)+\Delta\tau]$, where $\Delta\tau = \sup_i \tau(i+1)-\tau(i)$, the distance $d(s(t), \sigma(j))$ is bounded and smaller than $\text{depth}_d(\sigma(j), O(p))$, then both $s(t)$ and $\sigma(j)$ satisfy p .

Observation - 1D

Specification : $\diamond p = T \mathcal{U} p$



Assumption on signal dynamics

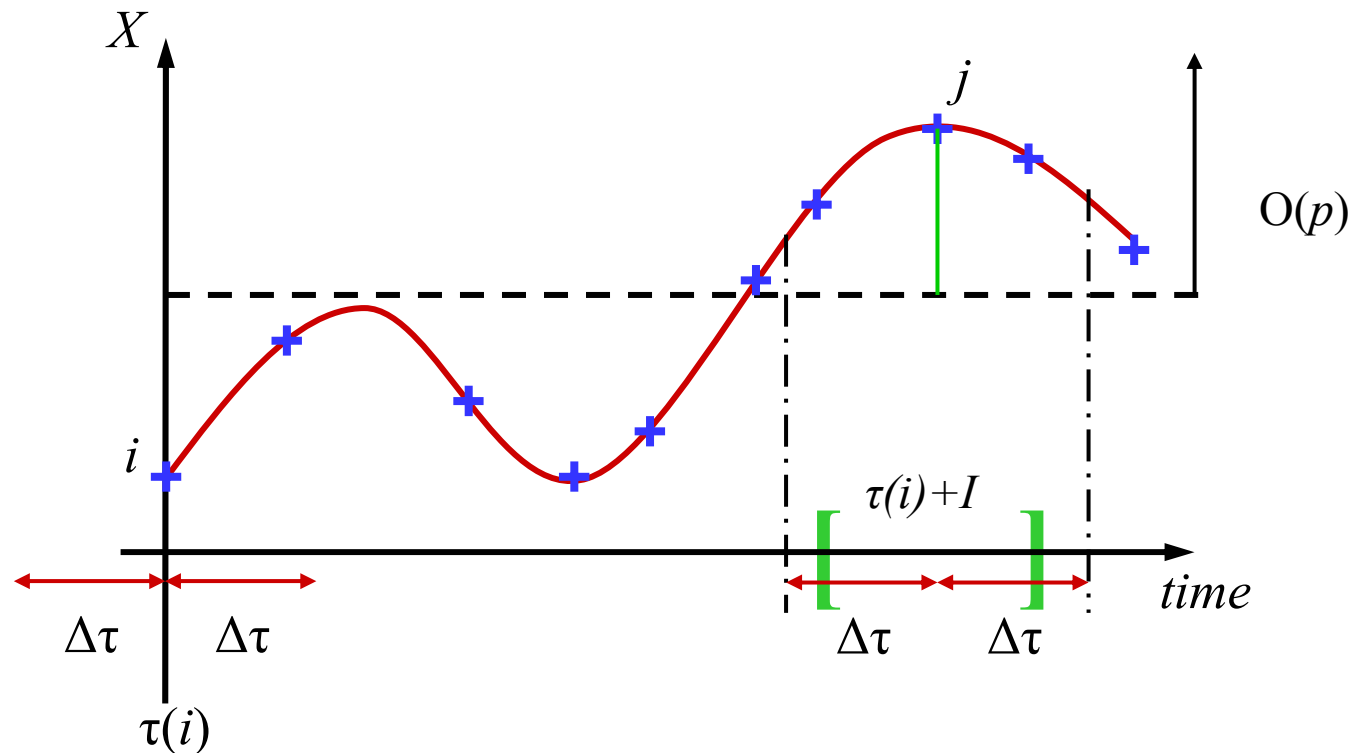
Assumption 1 *The signals in the set $\mathcal{F}(R, X)$ satisfy the condition*

$$\forall t, t' \in R . d(s(t), s(t')) \leq \mathcal{E}(|t - t'|),$$

where $\mathcal{E} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is a positive nondecreasing function.

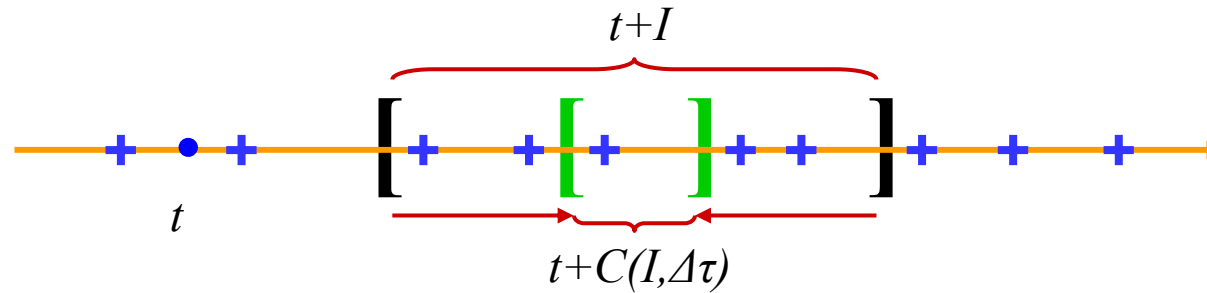
In order to use induction ...

Specification : $\diamond_I p = T \mathcal{U}_I p$



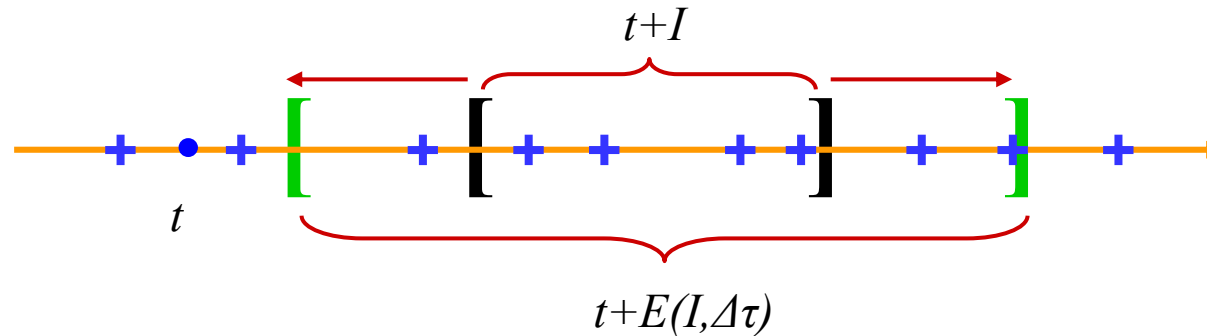
$$[\phi_1 \mathcal{U}_I \phi_2]_D(\mu, i) := \bigsqcup_{j \in \tau^{-1}(\tau(i) + RI)} \left([\phi_2]_D(\mu, j) \sqcap \prod_{i \leq k < j} [\phi_1]_D(\mu, k) \right)$$

Strengthening MITL formulas



$$\mathbf{str}_{\Delta\tau}(\phi_1 \mathcal{U}_I \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \mathcal{U}_{C(I, \Delta\tau)} \mathbf{str}_{\Delta\tau}(\phi_2)$$

$$\mathbf{str}_{\Delta\tau}(\phi_1 \mathcal{R}_I \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \mathcal{R}_{E(I, \Delta\tau)} \mathbf{str}_{\Delta\tau}(\phi_2)$$



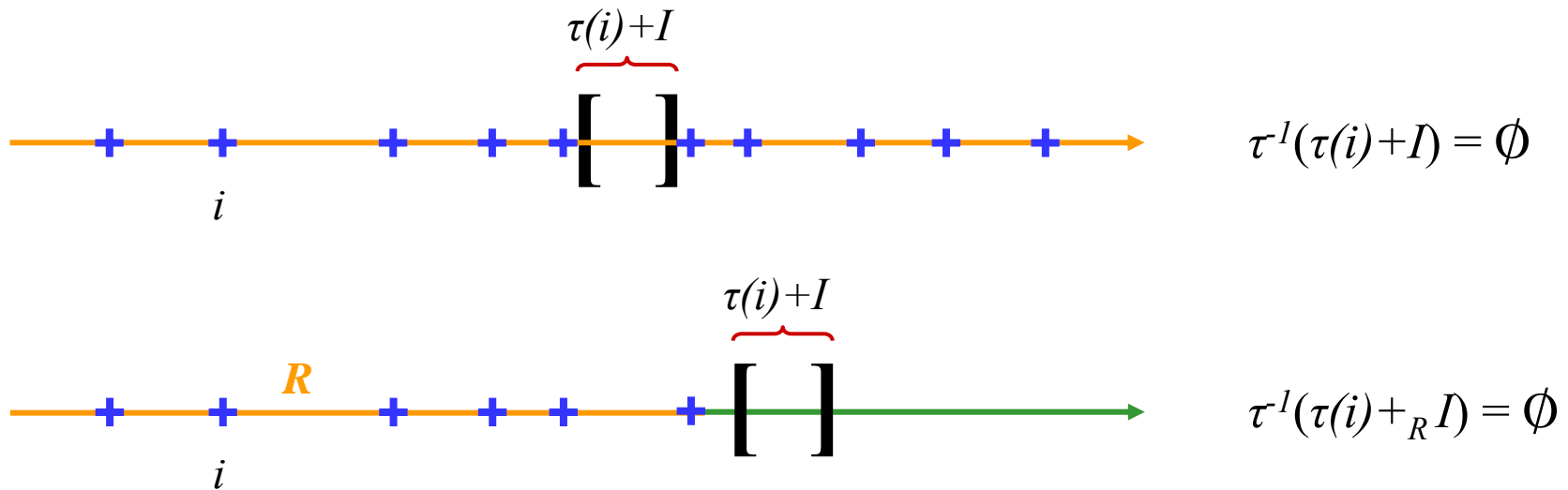
$$\mathbf{str}_{\Delta\tau}(p) = p, \quad \mathbf{str}_{\Delta\tau}(\neg p) = \neg p$$

$$\mathbf{str}_{\Delta\tau}(\phi_1 \vee \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \vee \mathbf{str}_{\Delta\tau}(\phi_2)$$

$$\mathbf{str}_{\Delta\tau}(\phi_1 \wedge \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \wedge \mathbf{str}_{\Delta\tau}(\phi_2)$$

The importance of the sampling function

Specification: $\square_I p = \perp R_I p$



$$\langle\langle \phi_1 \mathcal{R}_I \phi_2 \rangle\rangle_D(\mu, i) := \prod_{j \in \tau^{-1}(\tau(i)+_R I)} (\langle\langle \phi_2 \rangle\rangle_D(\mu, j) \sqcup \bigsqcup_{i \leq k < j} \langle\langle \phi_1 \rangle\rangle_D(\mu, k))$$

Sampling Assumptions

Assumption 2 Given a formula $\phi \in \Phi_{\mathbb{B}}^+$, the sampling functions in the set $\mathcal{F}_{si}(N, R)$ satisfy the constraint:

$$\Delta\tau < \min_{\mathcal{I} \in (\mathfrak{I}_{\text{str}_{\Delta\tau}(\phi)} \cup \mathfrak{I}_{\phi})} \{\sup \mathcal{I} - \inf \mathcal{I}\}.$$

When R is bounded, the sampling functions in the set $\mathcal{F}_{si}(N, R)$ must also satisfy the constraint : $\sup R - \tau(\max N) < \Delta\tau$.

Assumption 3 If the time domain R of the set of signals $\mathcal{F}(R, X)$ is bounded, i.e., $\sup R < +\infty$, then for the MITL formula ϕ under consideration it must be $\sup \mathcal{I} < +\infty$ for all $\mathcal{I} \in \mathfrak{I}_{\phi}$ and, also, $\sup R > \text{dur}(\text{str}_{\Delta\tau}(\phi))$.

Assumptions 2&3 imply that $\tau^{-1}(\tau(i) + I) \neq \emptyset$

Main Result

Theorem: Let ϕ be an MITL formula, $s \in F(\mathbb{R}, X)$ be a continuous time signal, $\tau \in F_{si}(\mathbb{N}, \mathbb{R})$ be a sampling function and let Assumptions 1-3 hold. Let $\mu = (s, \tau)$, then

$$\llbracket \text{str}_{\Delta\tau}(\phi) \rrbracket_D(\mu, i) > \mathcal{E}(\Delta\tau)$$

implies

$$\forall t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap \mathbb{R}. \llbracket \phi \rrbracket_C(s, t) = \top$$

Relationship of discrete and continuous time semantics

Proposition: Let ϕ be an MITL formula and μ be a TSS, then
 $\llbracket \text{str}_{\Delta\tau}(\phi) \rrbracket_D(\mu, i) = \top$ implies $\llbracket \phi \rrbracket_D(\mu, i) = \top$

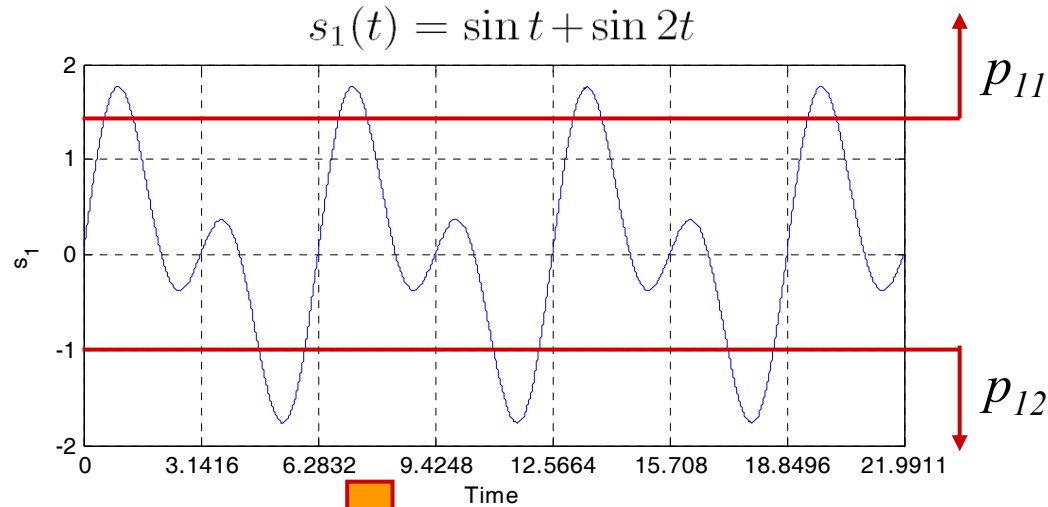
Proposition: Let ϕ be an MITL formula and μ be a TSS, then

- (1) $\llbracket \phi \rrbracket_D(\mu, i) > 0 \Rightarrow \llbracket \phi \rrbracket_D(\mu, i) = \top$ and $\llbracket \phi \rrbracket_D(\mu, i) < 0 \Rightarrow \llbracket \phi \rrbracket_D(\mu, i) = \perp$
- (2) $\llbracket \phi \rrbracket_D(\mu, i) = \top \Rightarrow \llbracket \phi \rrbracket_D(\mu, i) \geq 0$ and $\llbracket \phi \rrbracket_D(\mu, i) = \perp \Rightarrow \llbracket \phi \rrbracket_D(\mu, i) \leq 0$

Corollary: Let ϕ be an MITL formula, $s \in F(\mathbb{R}, X)$ be a continuous time signal, $\tau \in F_{s_i}(\mathbb{N}, \mathbb{R})$ be a sampling function and let Assumptions 1-3 hold. Let $\mu = (s \circ \tau, \tau)$, then $\llbracket \text{str}_{\Delta\tau}(\phi) \rrbracket_D(\mu, i) > \mathcal{E}(\Delta\tau)$ implies

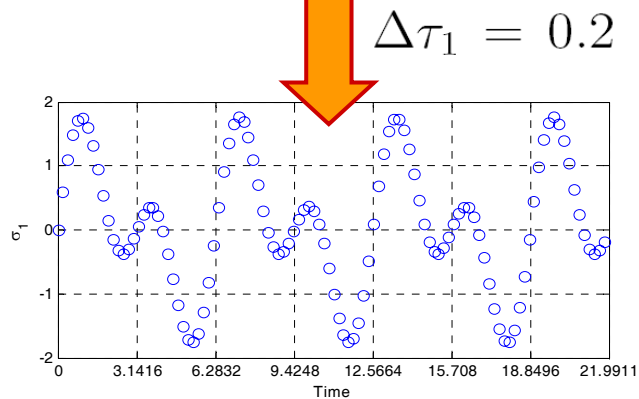
$$\llbracket \phi \rrbracket_C(s) = \llbracket \phi \rrbracket_D(\mu) = \top$$

Example 1



MITL

$$\Phi_1 = \square_{[0,9\pi/2]}(p_{11} \rightarrow \diamond_{[\pi,2\pi]} p_{12})$$



Also,
 $|\dot{s}_1(t)| \leq |\cos t| + 2|\cos 2t| \leq 1 + 2 = 3$
 thus $\mathcal{E}_1(t) = 3t$ and $\mathcal{E}_1(\Delta\tau_1) = 0.6$

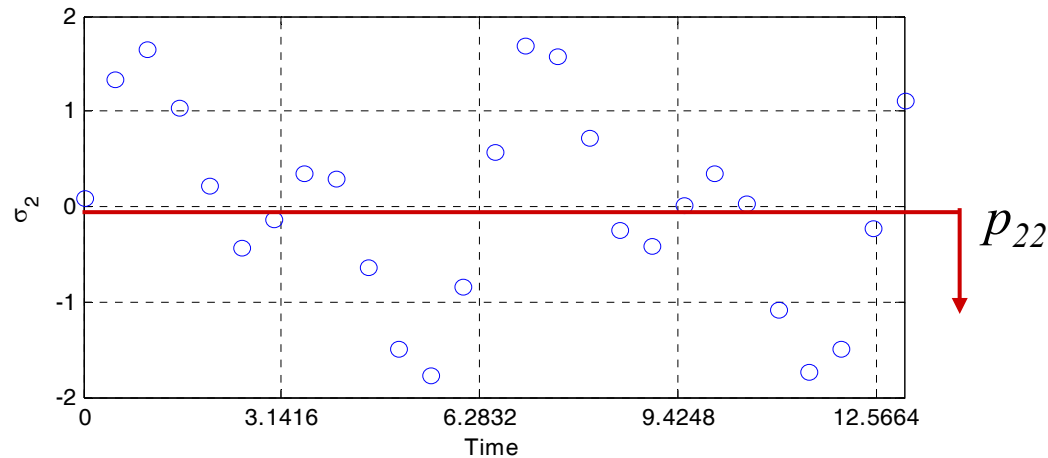
We compute*

$$\llbracket \text{str}_{\Delta\tau}(\phi_1) \rrbracket_D(\mu_1) = 0.7428$$

thus $\llbracket \phi_1 \rrbracket_C(s_1) = \top$

Example 2

$s_2(t) = \sin(t) + \sin(2t) + w(t)$, where $|w(t)| \leq 0.1$



$$\Delta\tau_2 = 0.5$$

MITL

$$\phi_2 = \square_{[0,4\pi]} p_{21} \wedge \diamond_{[3\pi,4\pi]} p_{22}$$

$$\mathcal{O}(p_{21}) = [-4, 4]$$

In this case, $|s_2(t_1) - s_2(t_2)| \leq L_{s_1}|t_1 - t_2| + |w(t_1)| + |w(t_2)|$
 thus $\mathcal{E}_2(\Delta\tau_2) = 1.7$

We compute* $\llbracket \text{str}_{\Delta\tau}(\phi_2) \rrbracket_D(\mu_2) = 1.7372$ thus $\langle\langle \phi_2 \rangle\rangle_C(s_2) = \top$

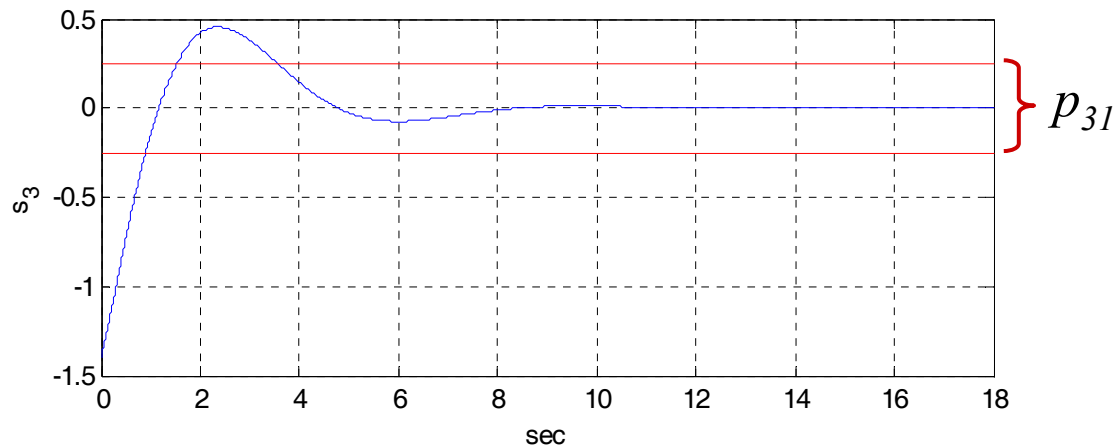
Example 3

linear system with nonlinear feedback

$$\dot{x}(t) = Ax(t) - b \text{sat}(cx(t)), \quad s_3(t) = cx(t)$$

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad c = \begin{bmatrix} 2 & 1 \end{bmatrix}$$

$$\text{sat}(y) = \begin{cases} -1 & \text{for } y < -1 \\ y & \text{for } |y| \leq 1 \\ 1 & \text{for } y > 1 \end{cases}$$



MITL

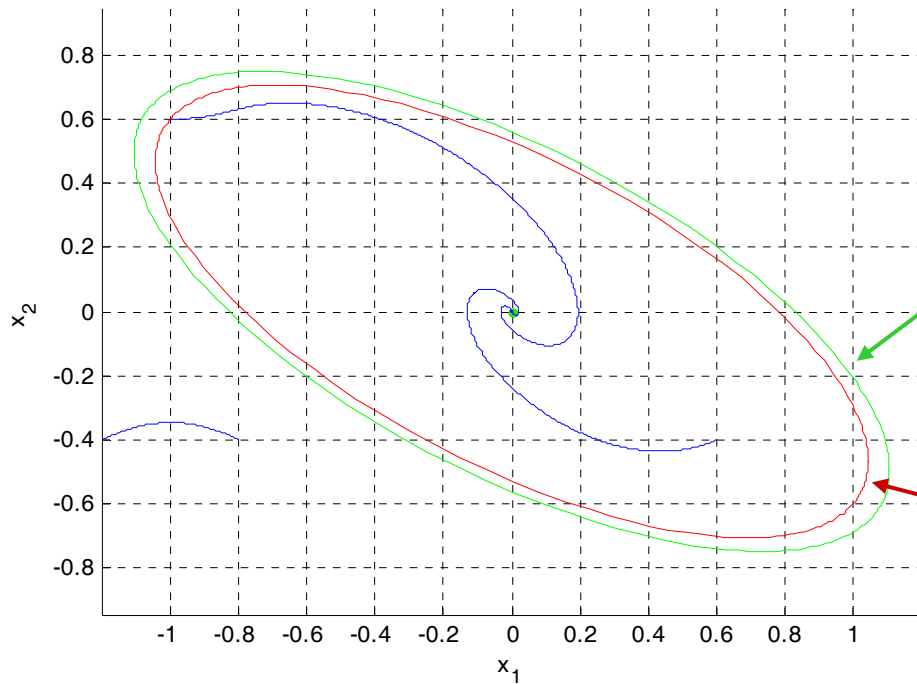
$$\Phi_3 = \diamond_{[6,8]} \square_{[0,10]} p_{31}$$

$$\Delta\tau_3 = 0.045 \quad \text{and} \quad \mathcal{E}_3(\Delta\tau_3) = 0.2182$$

$$\llbracket \text{str}_{\Delta\tau}(\phi_3) \rrbracket_D(\mu_3) = 0.2372$$

$$\langle\langle \phi_3 \rangle\rangle_C(s_3) = \top$$

Example 3 - Determination of \mathcal{E}_3



$$\Omega = \{x \in \mathbb{R}^2 \mid V(x) \leq 0.34\}$$

$$V(x) = x^T P x$$

$$P = \begin{bmatrix} 0.4946 & 0.4834 \\ 0.4834 & 1.0774 \end{bmatrix}$$

$$x(t) \in \{x \in \mathbb{R}^2 \mid V(x) \leq V(x(0))\}$$

$$P_e = V(x(0))P^{-1}$$

$$\|x(t)\| \leq \sqrt{\lambda_{\max}(P_e)}$$

$$\dot{x}(t) = Ax(t) - b \text{sat}(cx(t)), \quad s_3(t) = cx(t)$$

$$\|\dot{x}(t)\| \leq \|A\|\|x(t)\| + \|b\| \leq \|A\|\sqrt{\lambda_{\max}(P_e)} + \|b\| = L_x$$

Thus, for any $t, t' \in \mathbb{R}$, we have

$$|s_3(t) - s_3(t')| \leq \|c\|\|x(t) - x(t')\| \leq \|c\|L_x|t - t'|$$

That is, $\mathcal{E}_3(t) = \|c\|L_x t$

Related Research

1. [de Alfaro & Manna] Verification in Continuous Time by Discrete Reasoning
2. [Furia & Rossi] Integrating Discrete and Continuous Time Metric Temporal Logics Through Sampling
3. [Henzinger; Manna & Pnueli] What Good Are Digital Clocks?

Conclusions / Future Work

- ✓ Continuous time satisfiability using discrete time reasoning
 - ✓ Derive conditions on the dynamics of the signal
 - ✓ Derive conditions on the sampling function
- ✓ Derive bounds on the continuous time robustness from the discrete time robustness of the signal

➤ Future work

- Use methods from optimization theory to determine ε
- Design on-line monitoring algorithm
 - improve bounds
 - apply to hybrid systems
 - use approximate metrics to compute bounds





Thank You!
Questions?