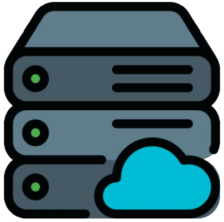
Time Robustness for Point-Based Semantics of Metric Interval Temporal Logic

Simone Silvetti[1], Ivan Compagnucci[2], Francesca Cairoli[1]
Catia Trubiani[2] and Laura Nenzi[1]

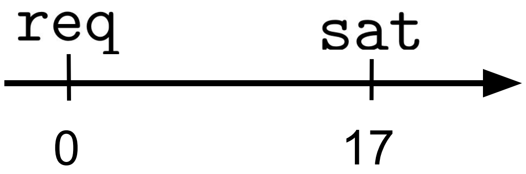
[1] University of Trieste – [2] Gran Sasso Science Institute

GRAN SASSO SCIENCE INSTITUTE

System



Traces



Requirements

Every request must be acknowledged between 10 and 20 time units

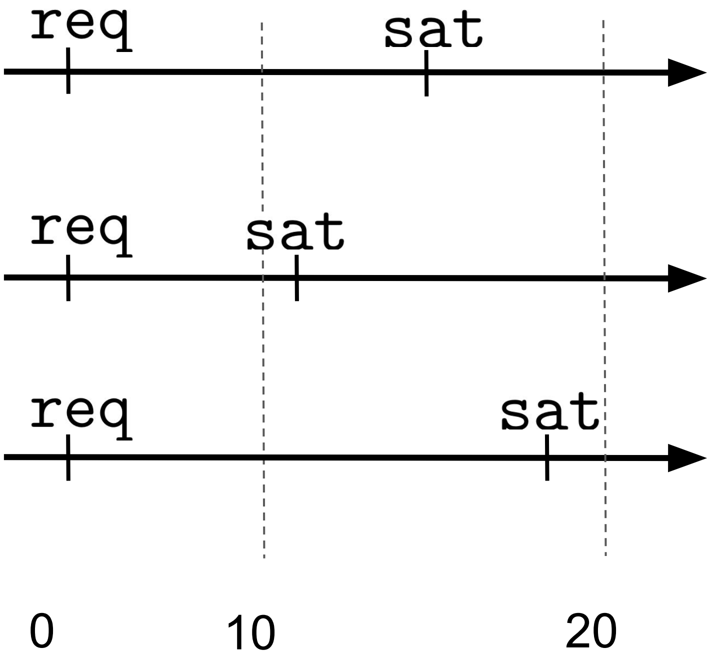
MITL

$$\sigma \qquad \varphi = \mathbf{G}(\mathtt{req} \rightarrow \mathbf{F}_{[10,20]}\mathtt{sat})$$

$$\sigma \models \varphi$$ Boolean Semantics

Beyond Boolean Semantics

$$\varphi = \mathbf{G}(\mathtt{req} \rightarrow \mathbf{F}_{[10,20]}\mathtt{sat})$$



Reliably under perturbation	The earlier the better	?
		
		
		

Beyond Boolean Semantics

$$\varphi = \mathbf{G}(\mathtt{req} \rightarrow \mathbf{F}_{[10,20]}\mathtt{sat})$$

Boolean Semantics

Enrich the Boolean interpretation by assigning a numerical value relevant in some domain

Quantitative Semantics

Soundness property

Correctness property

Distinguish behaviours with same Boolean value

Enable comparison and ranking

Enable optimization and synthesis

Contribution

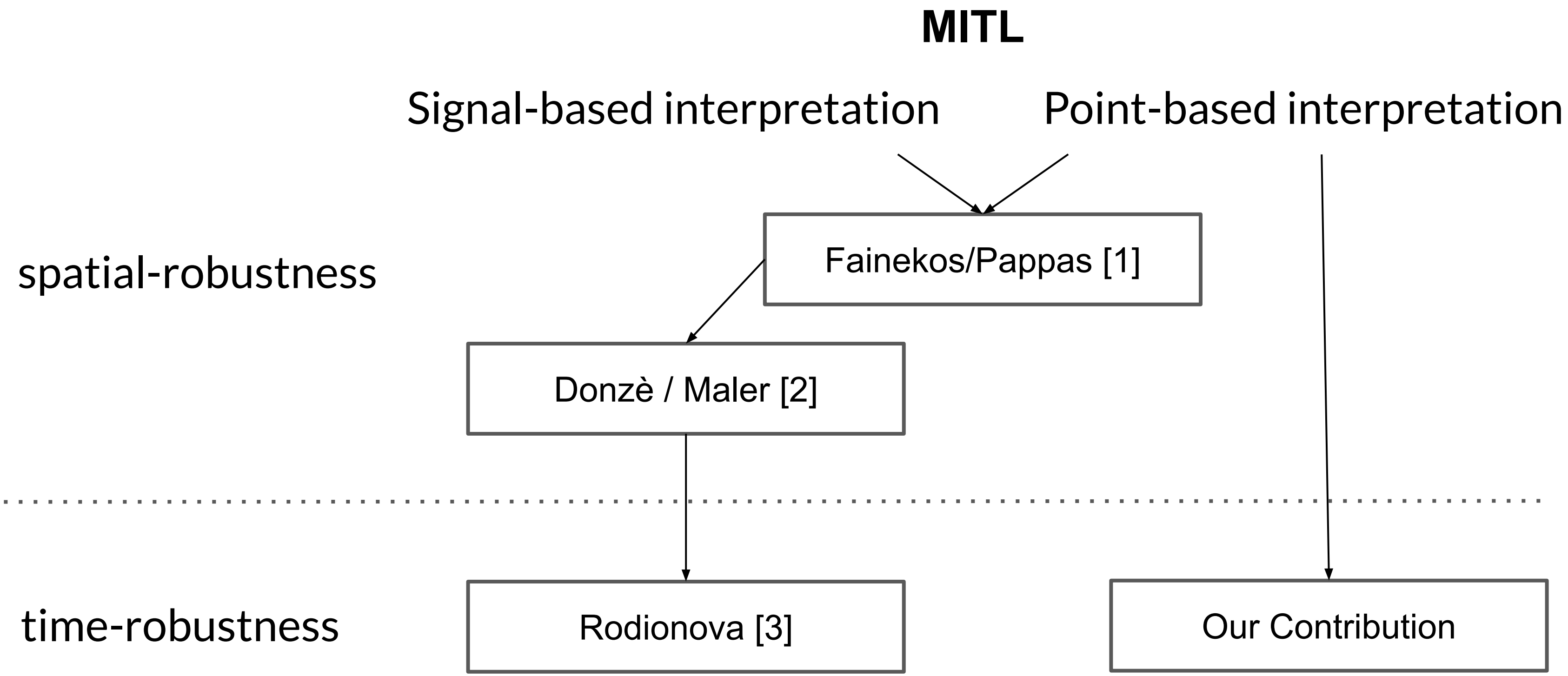
Definition of a new time-robustness semantics for the point-based interpretation of Metric Interval Temporal Logic (MITL)

Proof of soundness and stability guarantees wrt the Boolean Semantics of MITL

Evidence of relation between time robustness and tolerance under temporal uncertainty

2 use cases

A bit of history



[1] Fainekos, Pappas (2009). Robustness of temporal logic specifications for continuous-time signals. Theor. Comput. Sci. 410(42))

[2] Donzé, Maler (2010). Robust Satisfaction of Temporal Logic over Real-Valued Signals. FORMATS 2010

[3] Rodionova et al. (2022). Temporal robustness of temporal logic specifications: Analysis and control design. ACM Transactions on Embedded Computing Systems 22(1):1–44

A bit of history

rpretation

Trace alignment ~ Time robustness

[4] Giuseppe De Giacomo, Aniello Murano, Fabio Patrizi, Giuseppe Perelli: Timed Trace Alignment with Metric Temporal Logic over Finite Traces. KR 2021: 227-236

time-robustness

Rodionova [3]

Our Contribution

[1] Fainekos, Pappas (2009). Robustness of temporal logic specifications for continuous-time signals. Theor. Comput. Sci. 410(42))

[2] Donzé, Maler (2010). Robust Satisfaction of Temporal Logic over Real-Valued Signals. FORMATS 2010

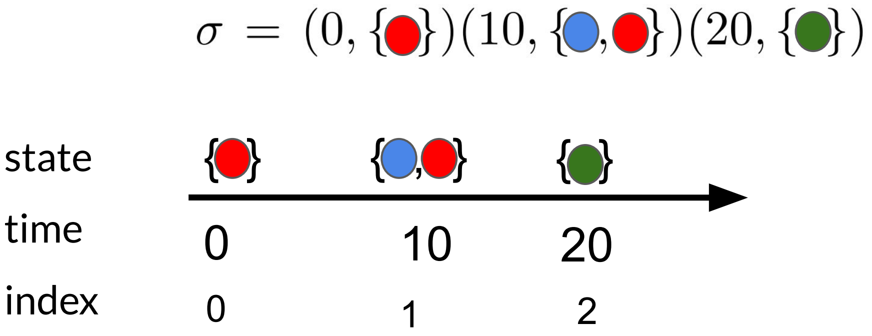
[3] Rodionova et al. (2022). Temporal robustness of temporal logic specifications: Analysis and control design. ACM Transactions on Embedded Computing Systems 22(1):1–44

Definition

Finite event trace $\sigma = (t_0, s_0)(t_1, s_1) \ldots (t_{n-1}, s_{n-1})$

Event $\in \mathbb{R}_{\geq 0} \times 2^{\mathsf{AP}}$

$\{\mathrm{p}_0, \mathrm{p}_1, \ldots, \mathrm{p}_{m-1}\}$



MITL Syntax

$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

Atomic predicate   Until   Next

MITL Syntax

$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

Atomic predicate

Until

Next

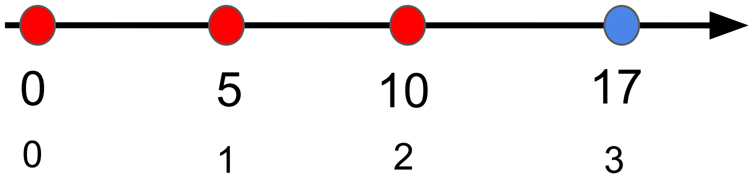
$$\mathbf{F}_I \varphi := \top \mathbf{U}_I \varphi$$

$$\mathbf{G}_I \varphi := \neg \mathbf{F}_I \neg \varphi$$

MITL Semantics

$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

$$(\sigma, i) \models \varphi_1 \mathbf{U}_I \varphi_2 \;\; \textit{if} \; \exists j \geq i, (\sigma, j) \models \varphi_2, \, t_j - t_i \in I,$$
$$\forall k \in [i, j), \, (\sigma, k) \models \varphi_1$$

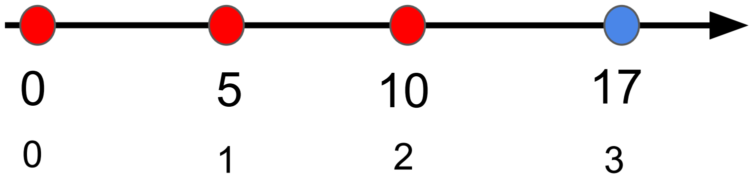


$$(\sigma, 0) \models \mathbf{U}_{[15,20]}$$

MITL Semantics

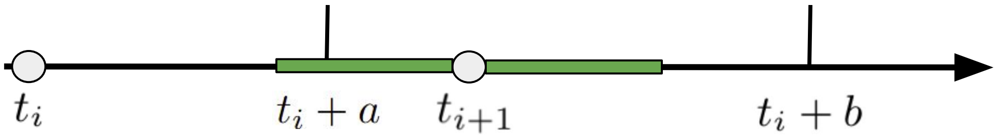
$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

$$(\sigma, i) \models \mathbf{X}_I \varphi \ \ if \ \ i < n-1 \ \ and \ \ (\sigma, i+1) \models \varphi, \ \ and \\ t_{i+1} - t_i \in I$$



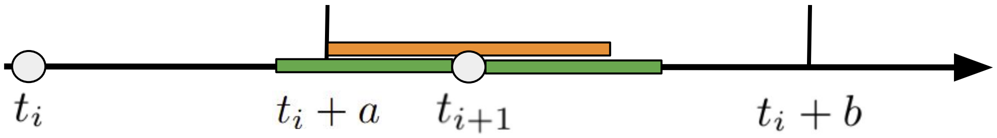
$$(\sigma, 2) \models \mathbf{X}_{[5,10]}$$

From Boolean to Time Robustness



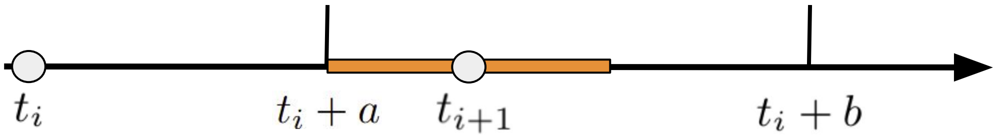
$$(\sigma, i) \models \mathbf{X}_I\varphi \;\; \textit{if} \;\; i < n - 1 \;\; \textit{and} \;\; \underline{(\sigma, i + 1) \models \varphi}, \;\; \textit{and}$$
$$t_{i+1} - t_i \in I$$

From Boolean to Time Robustness



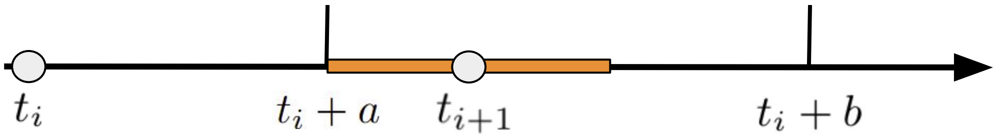
$$(\sigma, i) \models \mathbf{X}_I \varphi \ \textit{if} \ i < n-1 \ \textit{and} \ \underline{(\sigma, i+1) \models \varphi}, \ \textit{and}$$
$$\underline{t_{i+1} - t_i \in I}$$

From Boolean to Time Robustness



$$(\sigma, i) \models \mathbf{X}_I \varphi \ \ \textit{if} \ \ i < n - 1 \ \ \textit{and} \ \ (\sigma, i+1) \models \varphi, \ \ \textit{and} \ \ t_{i+1} - t_i \in I$$

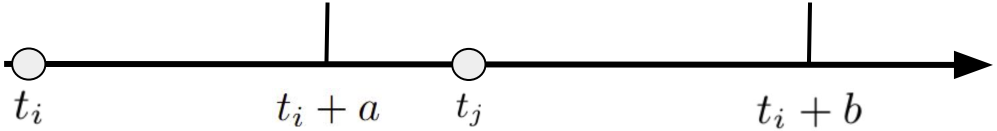
From Boolean to Time Robustness



$$(\sigma, i) \models \mathbf{X}_I \varphi \;\; \mathit{if} \;\; i < n-1 \;\; \mathit{and} \;\; (\sigma, i+1) \models \varphi, \;\; \mathit{and} \;\; t_{i+1} - t_i \in I$$

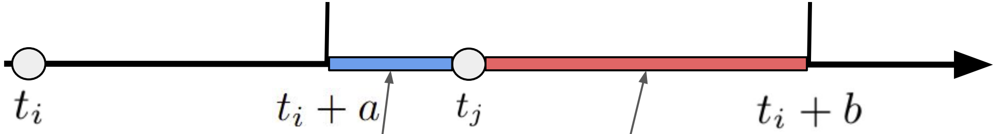
$$\rho(\mathbf{X}_I \varphi, \sigma, i) = \begin{cases} \min(\rho(\varphi, \sigma, i+1), d(t_i, t_{i+1}, I)) \;\; \mathit{if}\; i < n-1, \\ -\infty \qquad\qquad \mathit{otherwise.} \end{cases}$$

From Boolean to Time Robustness



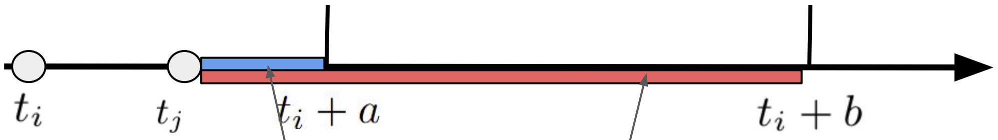
$$d(t_i, t_j, [a, b]) = \begin{cases} t_i + b - t_j & \textit{if } a = 0, \\ \min(t_j - t_i - a, t_i + b - t_j) & \textit{otherwise}. \end{cases}$$

From Boolean to Time Robustness



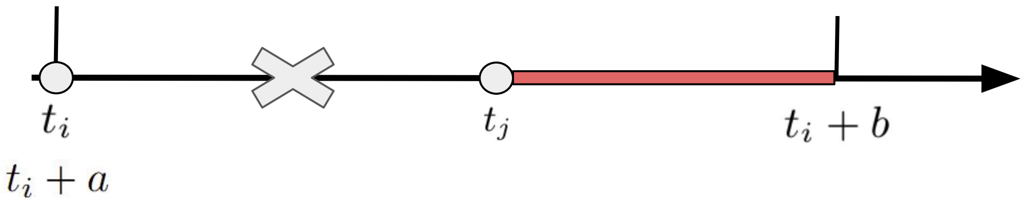
$$d(t_i, t_j, [a, b]) = \begin{cases} t_i + b - t_j & \textit{if } a = 0, \\ \min(t_j - t_i - a, t_i + b - t_j) & \textit{otherwise.} \end{cases}$$

From Boolean to Time Robustness



$$d(t_i, t_j, [a,b]) = \begin{cases} t_i + b - t_j & \textit{if } a = 0, \\ \min(t_j - t_i - a, t_i + b - t_j) & \textit{otherwise.} \end{cases}$$

From Boolean to Time Robustness



$$d(t_i, t_j, [a,b]) = \begin{cases} t_i + b - t_j & \textit{if } a = 0, \\ \min(t_j - t_i - a, t_i + b - t_j) & \textit{otherwise.} \end{cases}$$

We do not allow changing the order of events

Time Robustness

$$\rho(\top, \sigma, i) = +\infty$$

$$\rho(p, \sigma, i) = \begin{cases} +\infty & \textit{if } (\sigma, i) \models p, \\ -\infty & \textit{otherwise.} \end{cases}$$

$$\rho(\neg\varphi, \sigma, i) = -\rho(\varphi, \sigma, i)$$

$$\rho(\varphi_1 \wedge \varphi_2, \sigma, i) = \min(\rho(\varphi_1, \sigma, i), \rho(\varphi_2, \sigma, i))$$

$$\rho(\varphi_1 \mathbf{U}_I \varphi_2, \sigma, i) = \max_{j \geq i}\Big(\min\Big(\rho(\varphi_2, \sigma, j),\ d(t_i, t_j, I),$$

$$\min_{i \leq k < j} \rho(\varphi_1, \sigma, k)\Big)\Big)$$

$$\rho(\mathbf{X}_I \varphi, \sigma, i) = \begin{cases} \min(\rho(\varphi, \sigma, i+1), d(t_i, t_{i+1}, I)) \textit{ if } i < n-1, \\ -\infty \qquad \textit{otherwise.} \end{cases}$$

Soundness

Theorem 1 (Soundness of time robustness). *The time robustness is sound with respect to Boolean semantics of MITL, meaning that for each formula φ, event trace σ and $i < |\sigma|$ we have:*

$$\rho(\varphi, \sigma, i) > 0 \Rightarrow (\sigma, i) \models \varphi \tag{1}$$

$$\rho(\varphi, \sigma, i) < 0 \Rightarrow (\sigma, i) \not\models \varphi \tag{2}$$

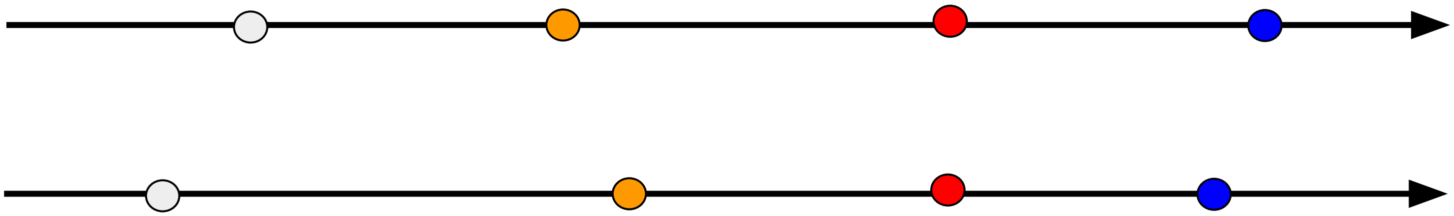
$$(\sigma, i) \models \varphi \Rightarrow \rho(\varphi, \sigma, i) \geq 0 \tag{3}$$

$$(\sigma, i) \not\models \varphi \Rightarrow \rho(\varphi, \sigma, i) \leq 0. \tag{4}$$

Stability

Theorem 2 (Stability property of time robustness). *Let us consider $\varphi \in \mathcal{L}_{MITL}$ and two trajectories σ and σ' such that $\boxed{\vec{s}(\sigma) = \vec{s}(\sigma')}$, then*

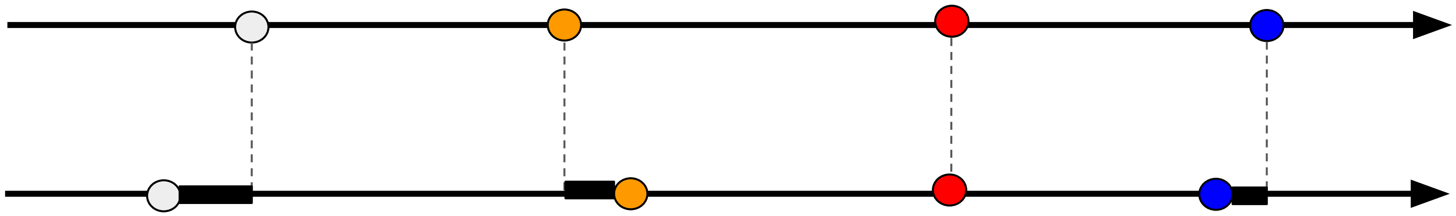
$$\forall i \leq |\sigma|, \quad |\rho(\varphi, \sigma', i) - \rho(\varphi, \sigma, i)| \leq \|\vec{t}(\sigma') - \vec{t}(\sigma)\|_1. \quad (5)$$



Stability

Theorem 2 (Stability property of time robustness). *Let us consider $\varphi \in \mathcal{L}_{MITL}$ and two trajectories σ and σ' such that $\vec{s}(\sigma) = \vec{s}(\sigma')$, then*

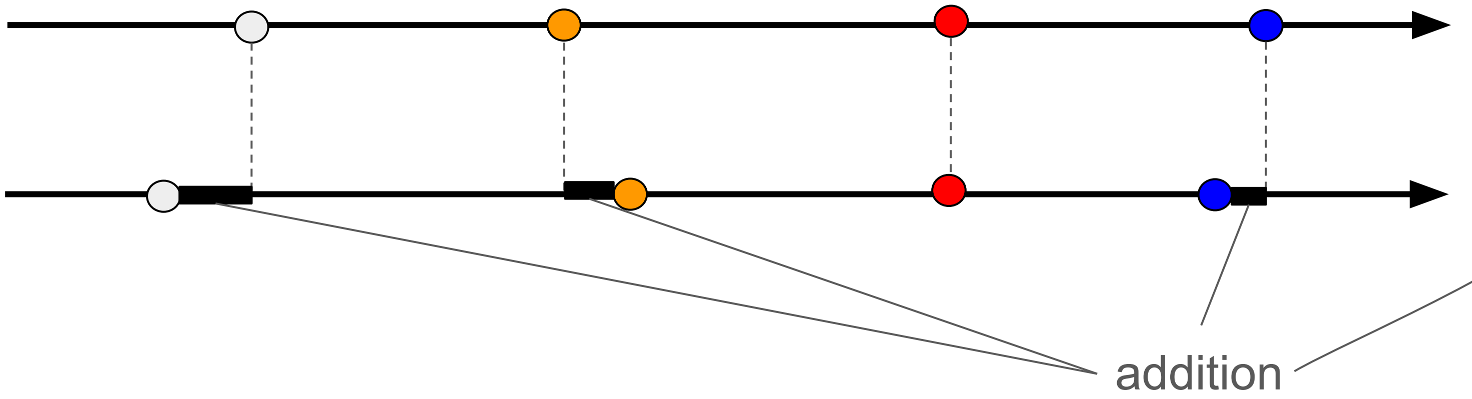
$$\forall i \leq |\sigma|, \quad |\rho(\varphi, \sigma', i) - \rho(\varphi, \sigma, i)| \leq \|\vec{t}(\sigma') - \vec{t}(\sigma)\|_1. \quad (5)$$



Stability

Theorem 2 (Stability property of time robustness). *Let us consider* $\varphi \in \mathcal{L}_{MITL}$ *and two trajectories* σ *and* σ' *such that* $\vec{s}(\sigma) = \vec{s}(\sigma')$, *then*

$$\forall i \leq |\sigma|, \quad |\rho(\varphi, \sigma', i) - \rho(\varphi, \sigma, i)| \leq \|\vec{t}(\sigma') - \vec{t}(\sigma)\|_1. \quad (5)$$

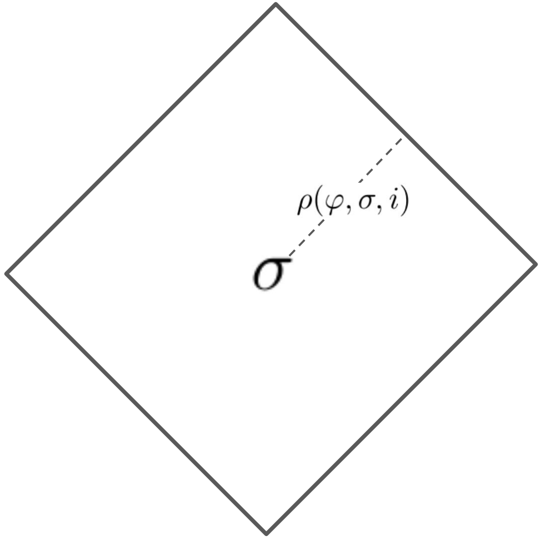


Stability

Theorem 2 (Stability property of time robustness). *Let us consider $\varphi \in \mathcal{L}_{MITL}$ and two trajectories σ and σ' such that $\vec{s}(\sigma) = \vec{s}(\sigma')$, then*

$$\forall i \le |\sigma|, \quad |\rho(\varphi, \sigma', i) - \rho(\varphi, \sigma, i)| \le \boxed{\|\vec{t}(\sigma') - \vec{t}(\sigma)\|_1} \qquad (5)$$

$$< \rho(\varphi, \sigma, i)$$



Stability

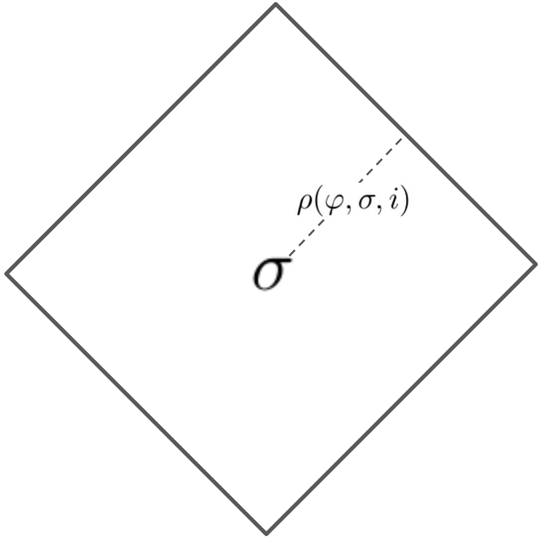
Theorem 2 (Stability property of time robustness). *Let us consider $\varphi \in \mathcal{L}_{MITL}$ and two trajectories σ and σ' such that $\vec{s}(\sigma) = \vec{s}(\sigma')$, then*

$$\forall i \leq |\sigma|, \quad |\rho(\varphi, \sigma', i) - \rho(\varphi, \sigma, i)| \leq \boxed{\|\vec{t}(\sigma') - \vec{t}(\sigma)\|_1}. \quad (5)$$

$$< \rho(\varphi, \sigma, i)$$

$$\Downarrow$$

$$\rho(\varphi, \sigma', i) > 0$$

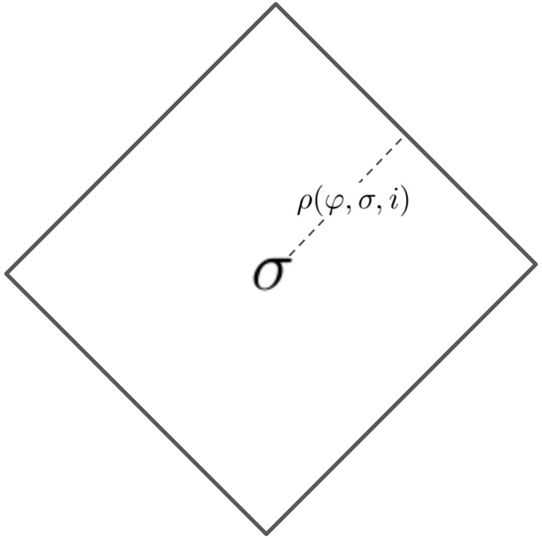


Stability

Theorem 2 (Stability property of time robustness). *Let us consider $\varphi \in \mathcal{L}_{MITL}$ and two trajectories σ and σ' such that $\vec{s}(\sigma) = \vec{s}(\sigma')$, then*

$$\forall i \leq |\sigma|, \quad |\rho(\varphi, \sigma', i) - \rho(\varphi, \sigma, i)| \leq \boxed{\|\vec{t}(\sigma') - \vec{t}(\sigma)\|_1}. \quad (5)$$

$$< \rho(\varphi, \sigma, i)$$



$$\Downarrow$$

$$\rho(\varphi, \sigma', i) > 0$$

$$\Downarrow \text{ soundness}$$

$$(\sigma', i) \models \varphi$$

Monitoring Algorithm

$$\rho(\varphi_1 \mathbf{U}_I \varphi_2, \sigma, i) = \max_{j \geq i} \Big(\min \Big(\rho(\varphi_2, \sigma, j),\ d(t_i, t_j, I), \min_{i \leq k < j} \rho(\varphi_1, \sigma, k) \Big) \Big)$$

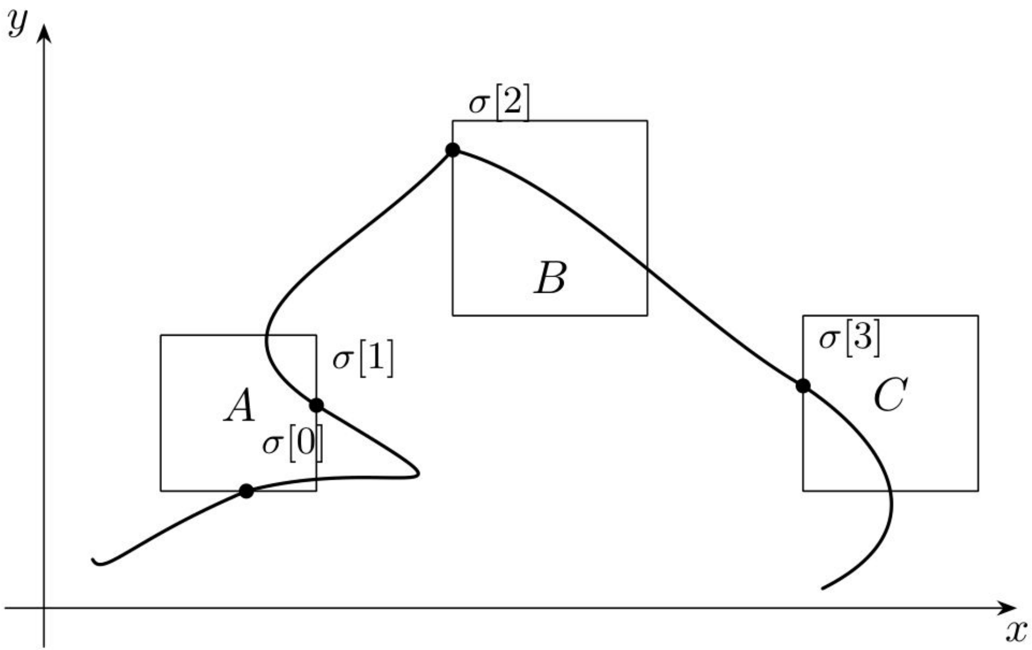
+

Tree structure of the formula

Complexity $\mathcal{O}(n^2|\varphi|)$

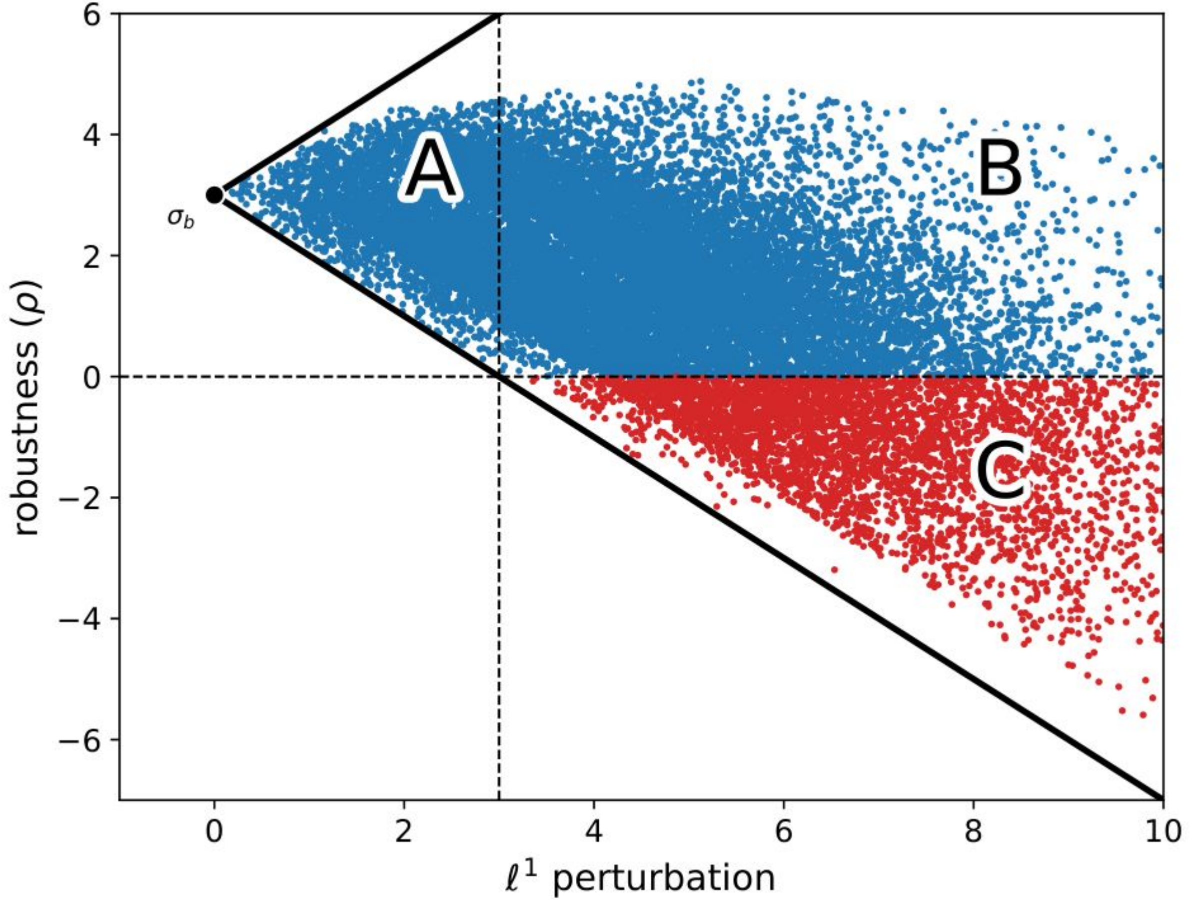
TIRO tool

Drone surveillance system

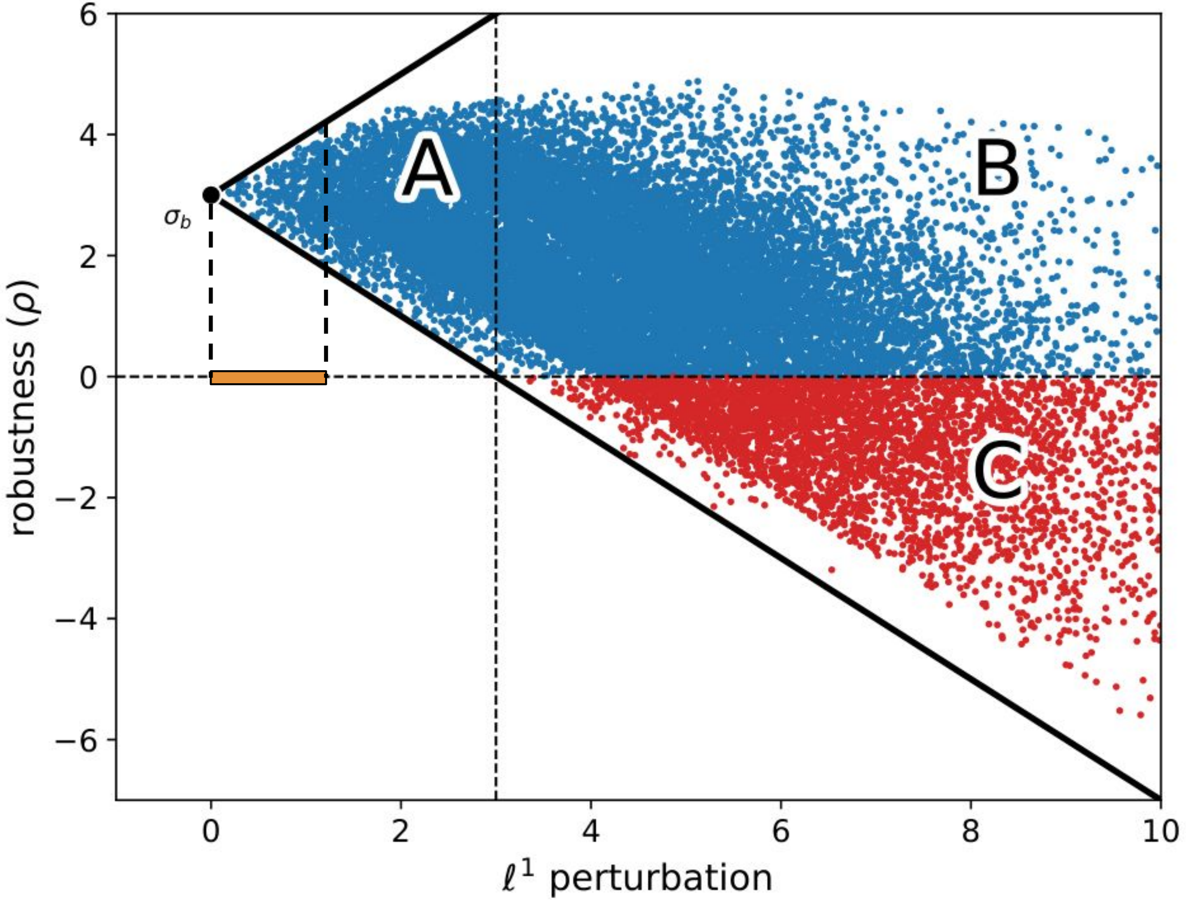


$$\psi_d = \mathbf{F}_{[10,20]}(\texttt{enterA} \wedge \mathbf{F}_{[40,50]}(\texttt{enterB} \wedge \mathbf{F}_{[20,30]}\ \texttt{enterC}))$$

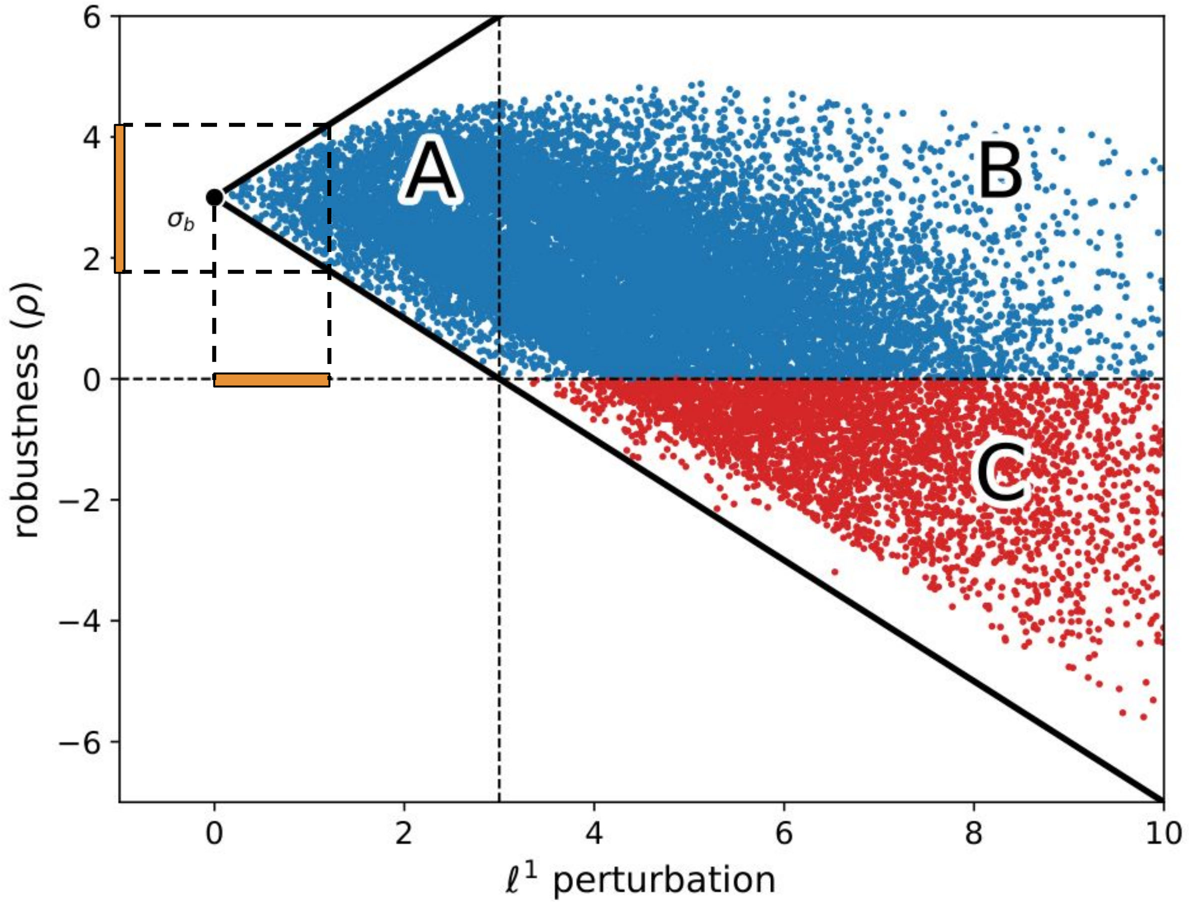
Drone surveillance system



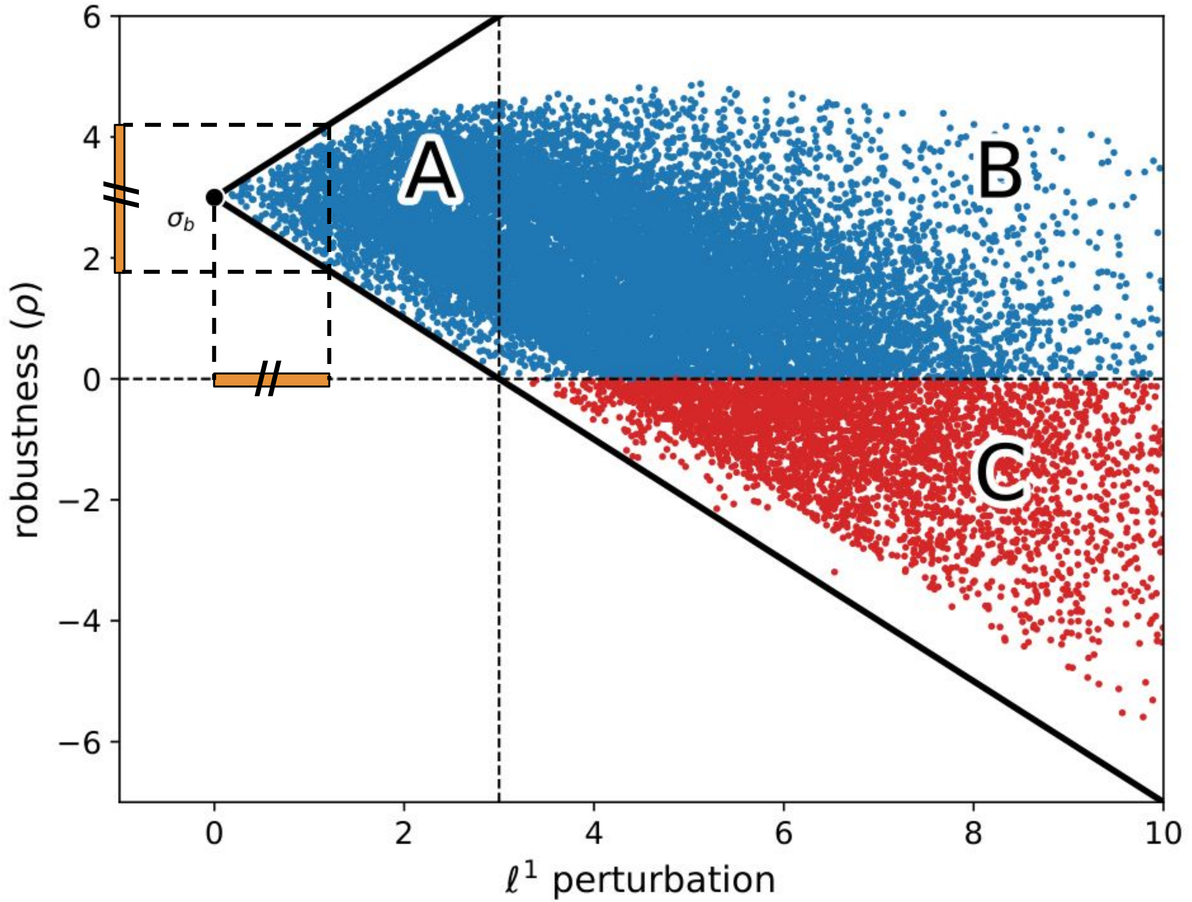
Drone surveillance system



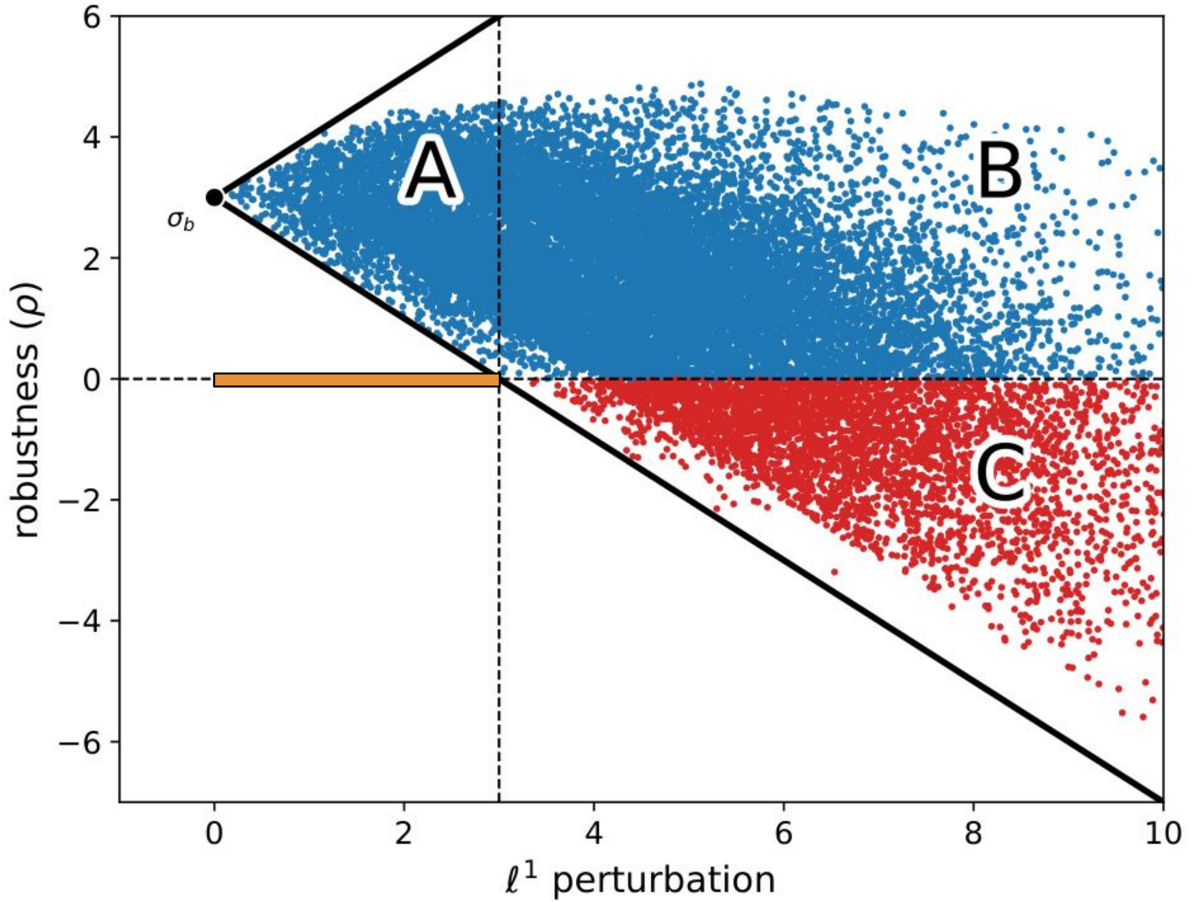
Drone surveillance system



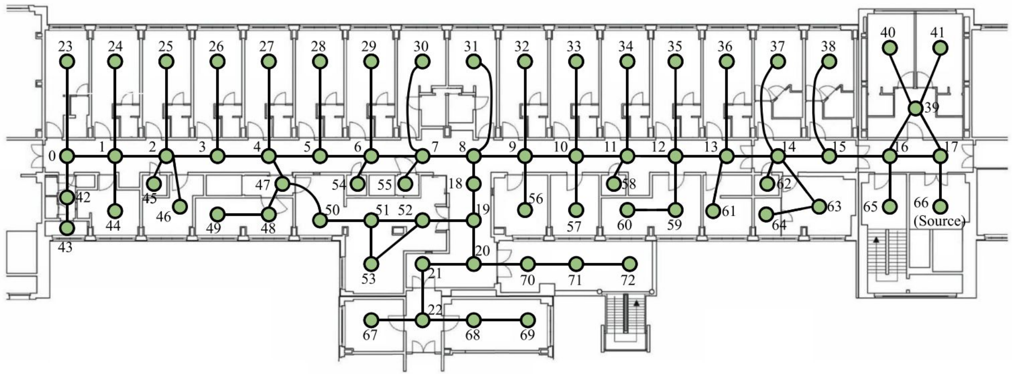
Drone surveillance system



Drone surveillance system



Smart Hospital



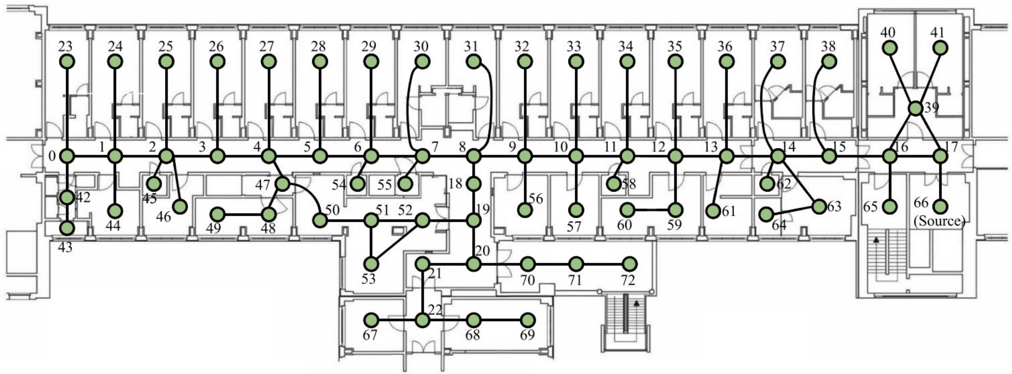
Robots delivering medical items from pharmacy to target rooms

might fail and ask for another robot to recover them

malicious: request fake recovering

Pinciroli, R., and Trubiani, C. 2023. Performance Analysis of Fault-Tolerant Multiagent Coordination Mechanisms. IEEE Trans. Ind. Informatics 19(9):9821–9832.

Smart Hospital



$$\varphi_a = \mathbf{G}(\texttt{create} \rightarrow \mathbf{F}_{[0,20]}\ \texttt{load})$$

$$\varphi_b = \mathbf{G}(\texttt{load} \rightarrow \mathbf{F}_{[L,U]}\ \texttt{deliver})$$

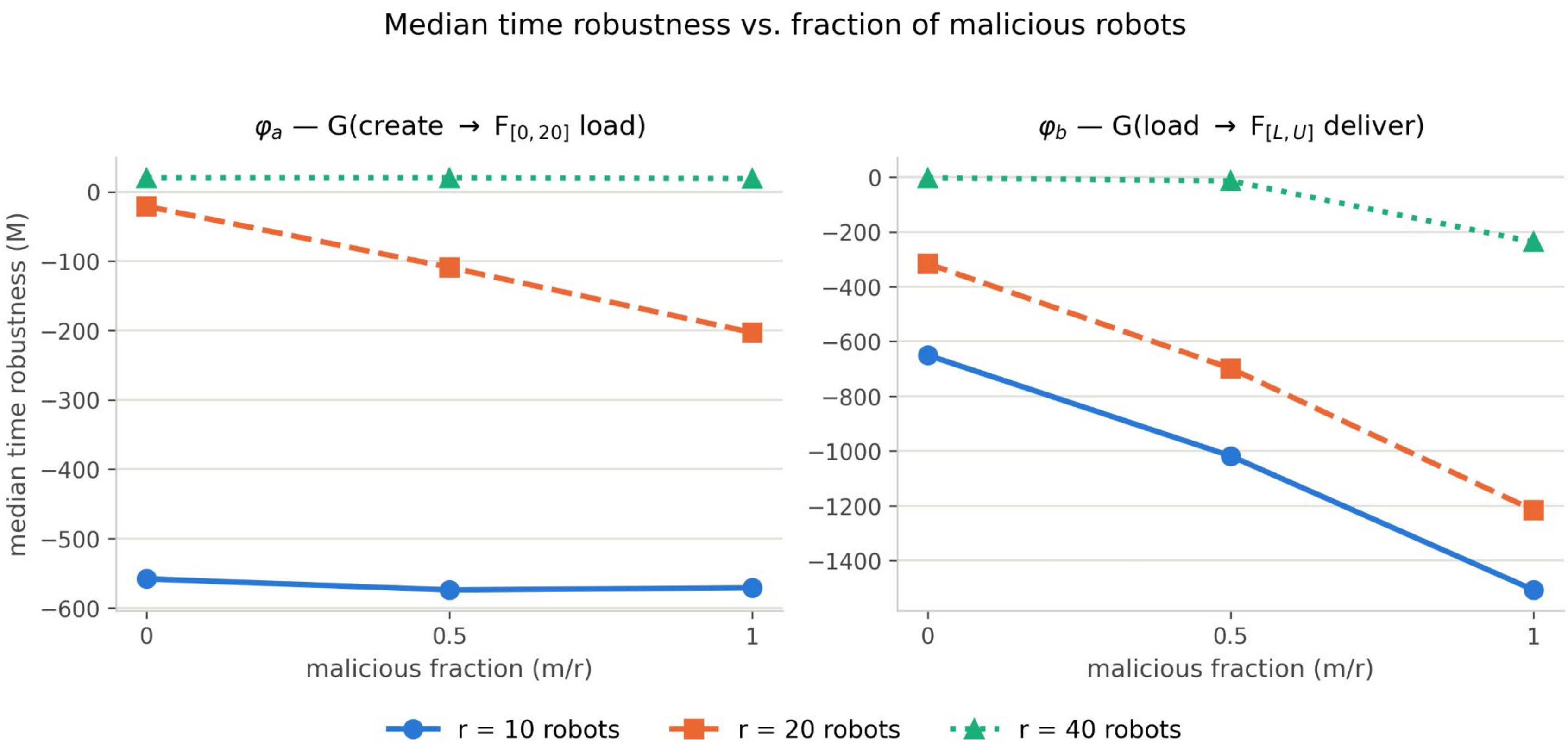
$$\varphi_c = \mathbf{G}(\texttt{fail} \rightarrow X_{[0,2500]}\ \texttt{recover})$$

Robots delivering medical items from pharmacy to target rooms

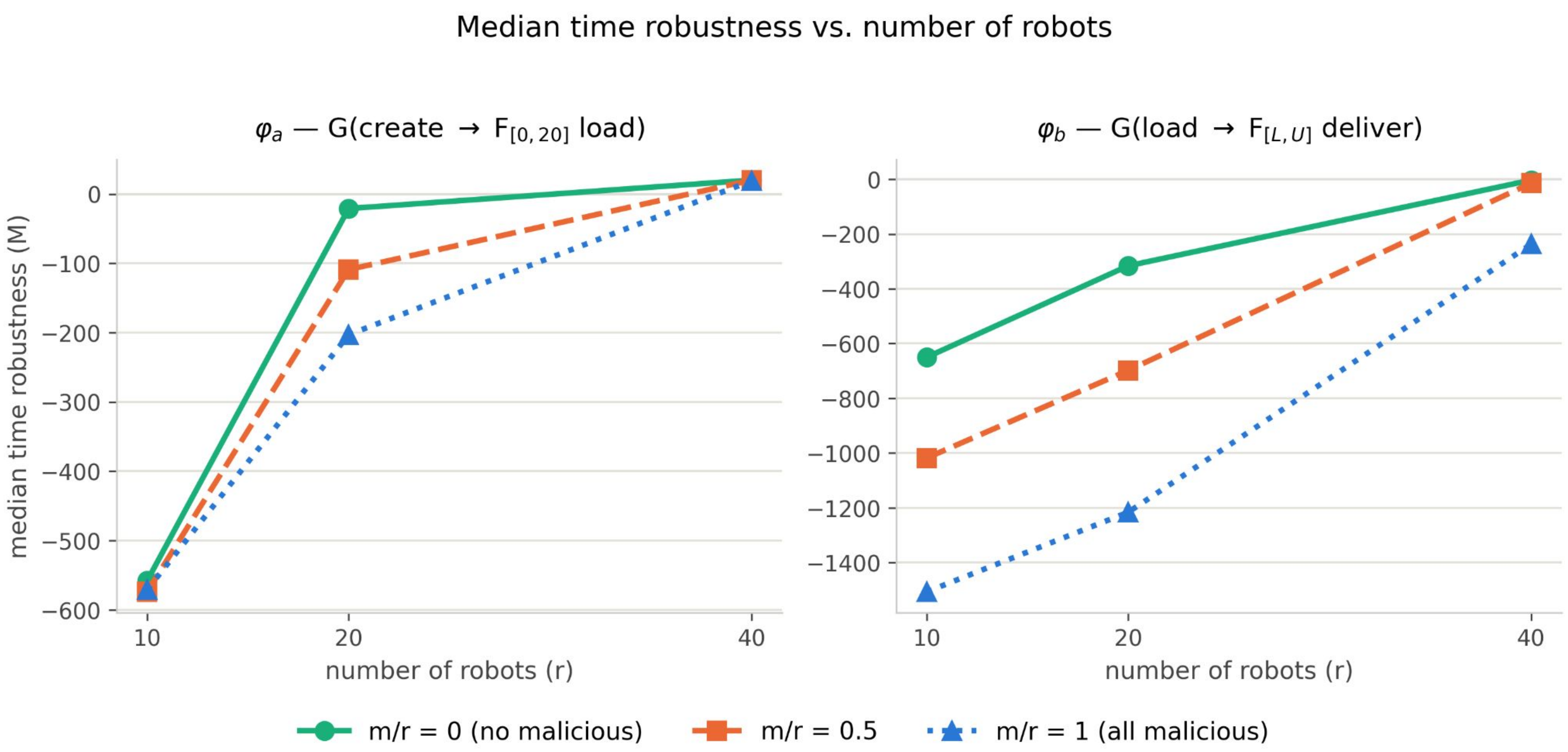
might fail and ask for another robot to recover them

malicious: request fake recovering

Smart Hospital



Smart Hospital



Future work

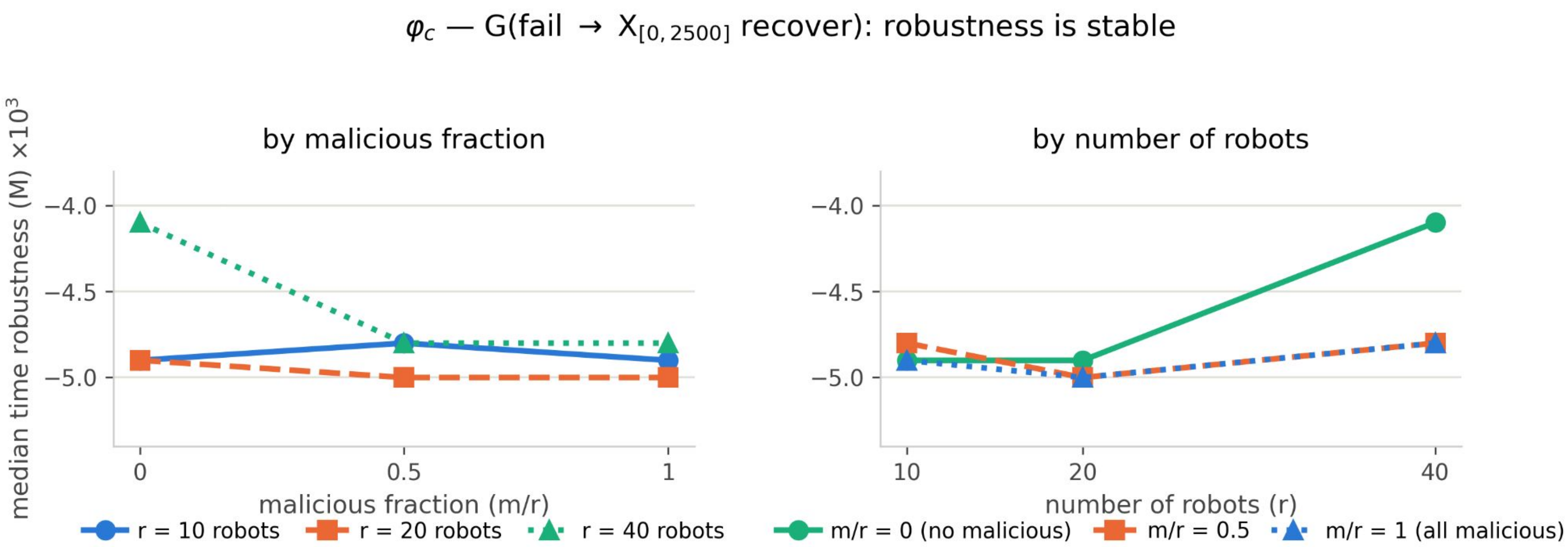
Use time robustness for synthesis problem

Define an optimized algorithm for time robustness

Remove the constraint of fixed ordering

Thanks

Smart Hospital



Conclusions

Introduced a quantitative semantics for MITL under point-based interpretation extending the concept of time robustness to event-based systems

Proved soundness and stability property

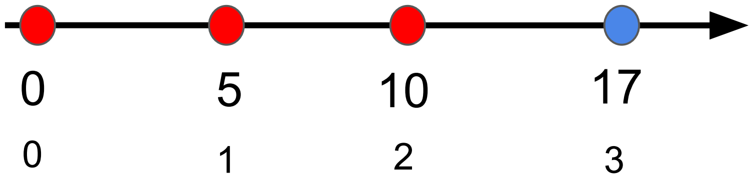
Defined a simple monitoring algorithm

Link time robustness to the resilience of a system to timing deviation with two experiments

MITL Semantics

$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

$$(\sigma, i) \models \top$$

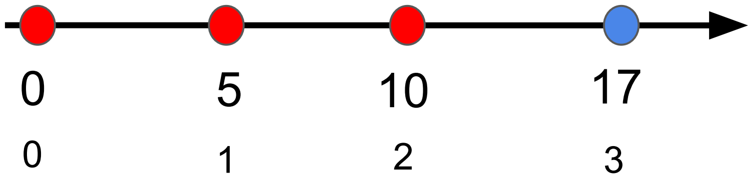


$$(\sigma, 0) \models \top \qquad (\sigma, 1) \models \top \qquad \ldots$$

MITL Semantics

$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

$$(\sigma, i) \models \mathrm{p} \;\; \textit{if} \;\; \mathrm{p} \in s_i$$

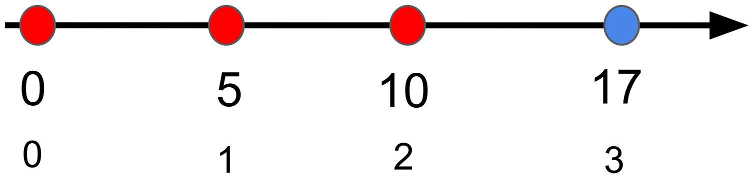


$(\sigma, 0) \models$ $\qquad$ $(\sigma, 3) \models$

MITL Semantics

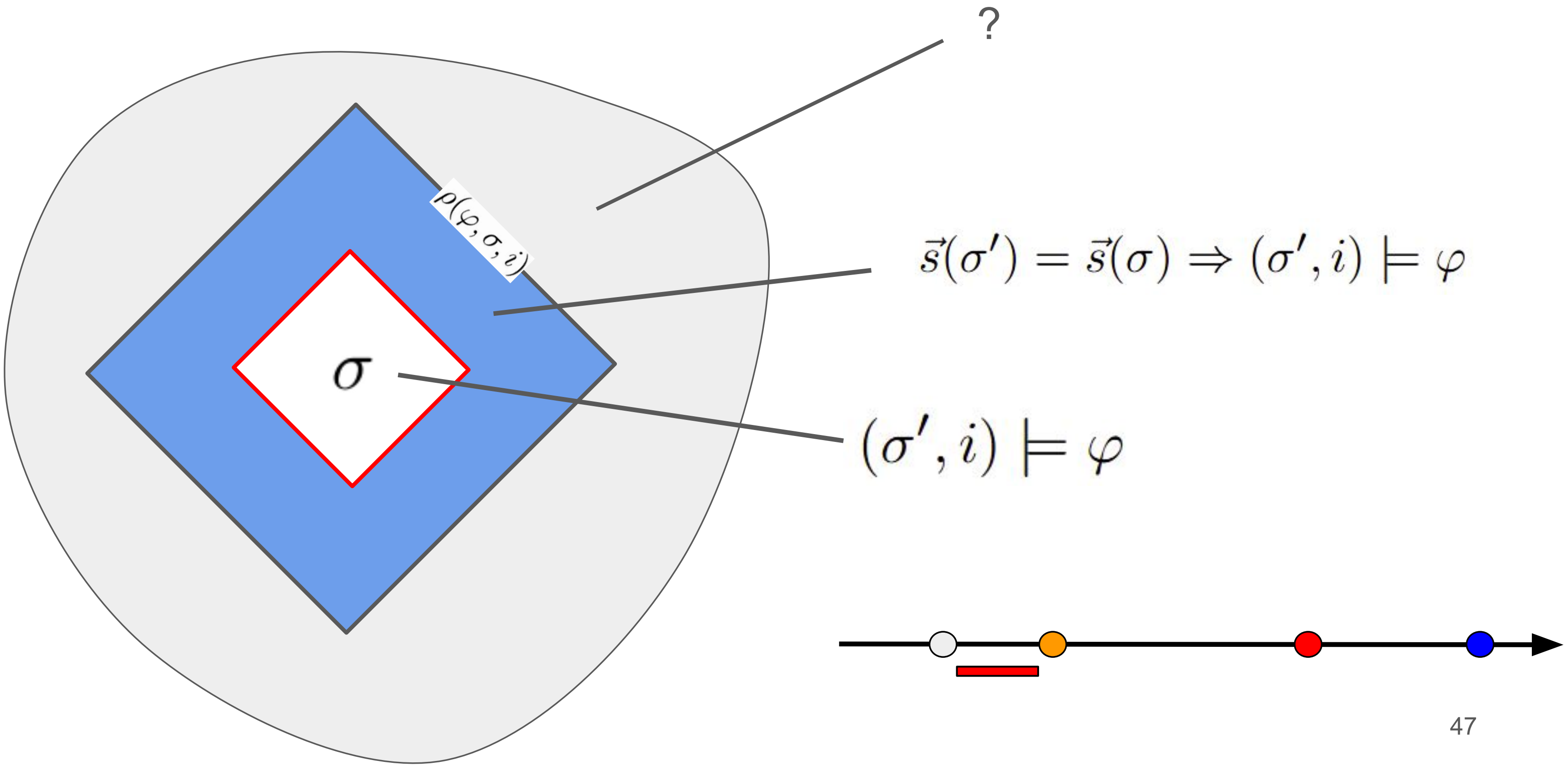
$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathbf{U}_I \varphi \mid \mathbf{X}_I \varphi$$

$$(\sigma, i) \models \neg\varphi \ \ \mathit{if} \ \ (\sigma, i) \not\models \varphi$$
$$(\sigma, i) \models \varphi_1 \wedge \varphi_2 \ \ \mathit{if} \ \ (\sigma, i) \models \varphi_1 \ \ \mathit{and} \ \ (\sigma, i) \models \varphi_2$$

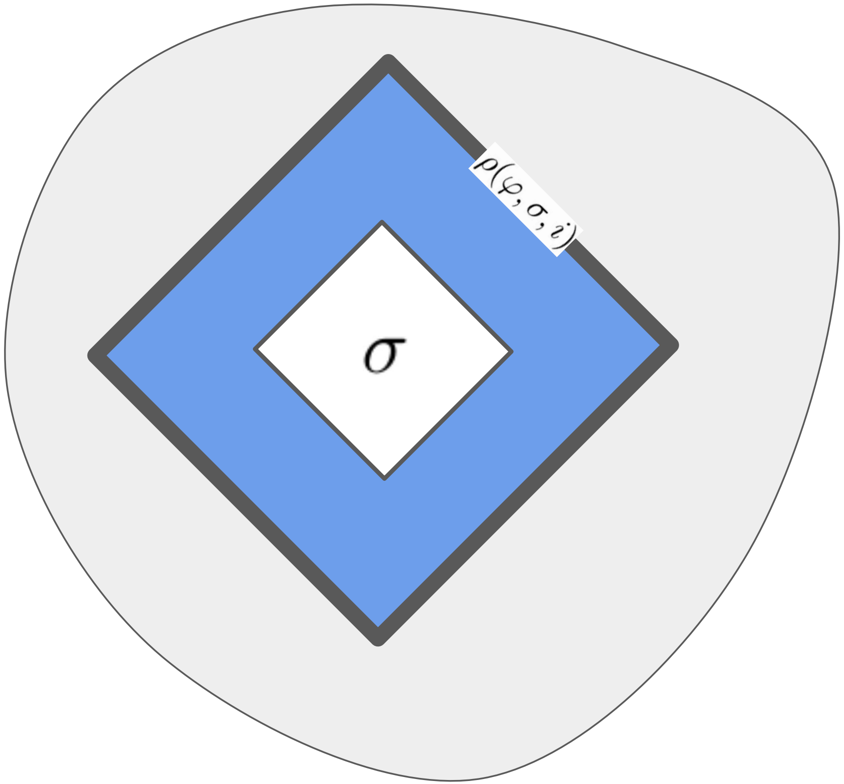


$(\sigma, 0) \models \neg$ $\qquad$ $(\sigma, 0) \models \neg \wedge$

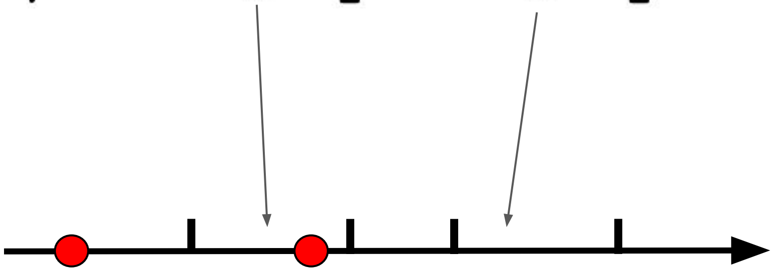
Topology of satisfaction



Under Approximation



$$\varphi = \mathbf{F}_I \neg \mathrm{p} \vee \mathbf{F}_J \neg \mathrm{p}$$



Smart Hospital

#malicious

median

#robots

			φ_a			φ_b			φ_c $(\times 10^3)$		
r	**m**	**m/r**	M	Q_1	Q_3	M	Q_1	Q_3	M	Q_1	Q_3
10	0	0	-558	-55929	-178	-650	-5661	9	-4.9	-6.5	-3.8
10	5	0.5	-574	-3533	-189	-1018	-7247	8	-4.8	-6.1	-3.8
10	10	1	-571	-2033	-201	-1507	-9772	6	-4.9	-6.4	-3.9
20	0	0	-21	-204	20	-316	-4059	10	-4.9	-6.6	-3.8
20	10	0.5	-109	-424	-2	-698	-8275	5	-5.0	-6.4	-3.8
20	20	1	-203	-1093	-42	-1216	-18478	-12	-5.0	-6.6	-3.9
40	0	0	20	20	20	-3	-512	15	-4.1	-5.5	-2.9
40	20	0.5	20	20	20	-14	-606	13	-4.8	-6.2	-3.7
40	40	1	19	-23	20	-237	-1758	4	-4.8	-6.4	-3.8

Smart Hospital

#malicious
median
#robots

r	m	m/r	φ_a M	φ_a Q_1	φ_a Q_3	φ_b M	φ_b Q_1	φ_b Q_3	φ_c $(\times 10^3)$ M	φ_c $(\times 10^3)$ Q_1	φ_c $(\times 10^3)$ Q_3
10	0	0	-558	-55929	-178	-650	-5661	9	-4.9	-6.5	-3.8
10	5	0.5	-574	-3533	-189	-1018	-7247	8	-4.8	-6.1	-3.8
10	10	1	-571	-2033	-201	-1507	-9772	6	-4.9	-6.4	-3.9
20	0	0	-21	-204	20	-316	-4059	10	-4.9	-6.6	-3.8
20	10	0.5	-109	-424	-2	-698	-8275	5	-5.0	-6.4	-3.8
20	20	1	-203	-1093	-42	-1216	-18478	-12	-5.0	-6.6	-3.9
40	0	0	20	20	20	-3	-512	15	-4.1	-5.5	-2.9
40	20	0.5	20	20	20	-14	-606	13	-4.8	-6.2	-3.7
40	40	1	19	-23	20	-237	-1758	4	-4.8	-6.4	-3.8

Smart Hospital

#malicious
median
#robots

			φ_a			φ_b			$\varphi_c\ (\times 10^3)$		
r	**m**	**m/r**	M	Q_1	Q_3	M	Q_1	Q_3	M	Q_1	Q_3
10	0	0	-558	-55929	-178	-650	-5661	9	-4.9	-6.5	-3.8
10	5	0.5	-574	-3533	-189	-1018	-7247	8	-4.8	-6.1	-3.8
10	10	1	-571	-2033	-201	-1507	-9772	6	-4.9	-6.4	-3.9
20	0	0	-21	-204	20	-316	-4059	10	-4.9	-6.6	-3.8
20	10	0.5	-109	-424	-2	-698	-8275	5	-5.0	-6.4	-3.8
20	20	1	-203	-1093	-42	-1216	-18478	-12	-5.0	-6.6	-3.9
40	0	0	20	20	20	-3	-512	15	-4.1	-5.5	-2.9
40	20	0.5	20	20	20	-14	-606	13	-4.8	-6.2	-3.7
40	40	1	19	-23	20	-237	-1758	4	-4.8	-6.4	-3.8

Smart Hospital

#malicious

median

#robots

			φ_a			φ_b			φ_c $(\times 10^3)$		
r	**m**	**m/r**	M	Q_1	Q_3	M	Q_1	Q_3	M	Q_1	Q_3
10	0	0	-558	-55929	-178	-650	-5661	9	-4.9	-6.5	-3.8
10	5	0.5	-574	-3533	-189	-1018	-7247	8	-4.8	-6.1	-3.8
10	10	1	-571	-2033	-201	-1507	-9772	6	-4.9	-6.4	-3.9
20	0	0	-21	-204	20	-316	-4059	10	-4.9	-6.6	-3.8
20	10	0.5	-109	-424	-2	-698	-8275	5	-5.0	-6.4	-3.8
20	20	1	-203	-1093	-42	-1216	-18478	-12	-5.0	-6.6	-3.9
40	0	0	20	20	20	-3	-512	15	-4.1	-5.5	-2.9
40	20	0.5	20	20	20	-14	-606	13	-4.8	-6.2	-3.7
40	40	1	19	-23	20	-237	-1758	4	-4.8	-6.4	-3.8

Time robustness captures the resilience of a system to timing deviations