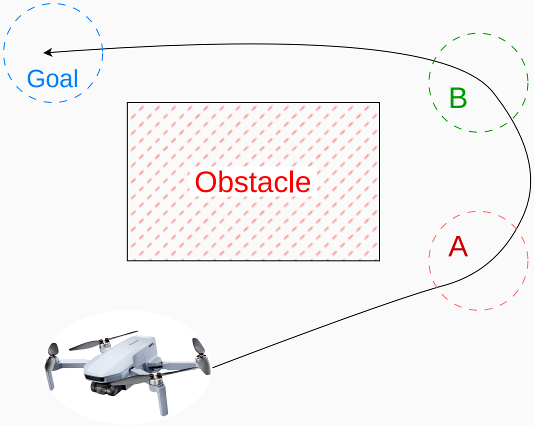
Confidence-Based Signal Temporal Logic and Application to Uncertain Cyber-Physical Systems

ECC26: Set-Based Methods for Verified Parameter Identification, State Estimation, and Control

Antoine Besset   Joris Tillet   Julien Alexandre dit Sandretto

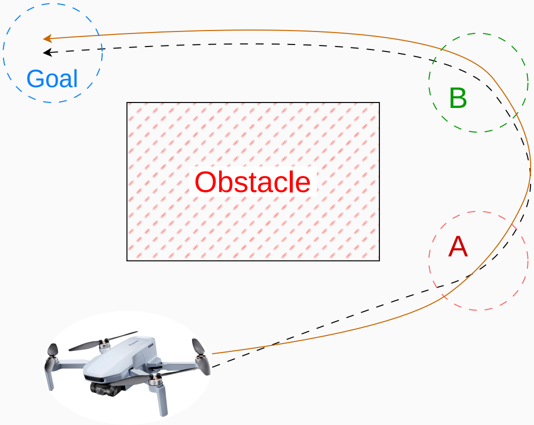
ENSTA Paris, IP Paris, France

Problem statement

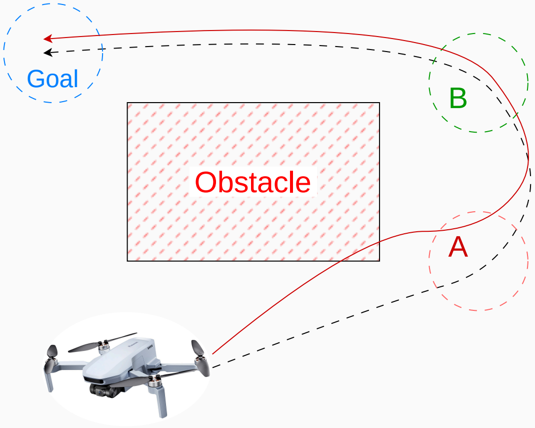


- *“If the drone reaches A, it must reach B within 3–5 seconds, avoid the obstacle and reach ultimately a goal.”*

Problem statement

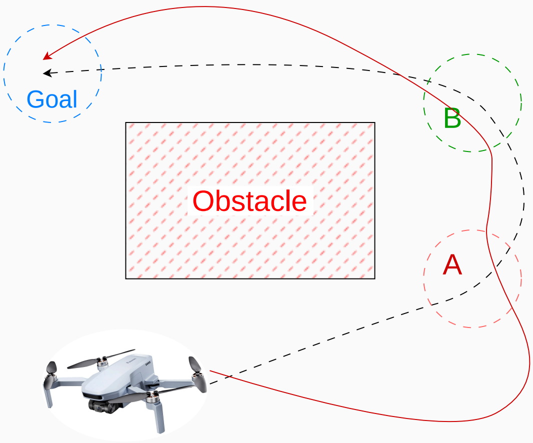


- In practice, the system is subject to model uncertainties and environmental perturbations.



- In practice, the system is subject to model uncertainties and environmental perturbations.

Problem statement



- **Key Question:** Can it be guaranteed that the system will always perform as designed?

Motivation and Contributions

- **Goal:** verify that a nonlinear continuous-time system with uncertainty satisfies a Signal Temporal Logic (STL) specification.
- We combine reachability analysis and STL monitoring to reason about *all trajectories* at once.

Motivation and Contributions

- **Goal:** verify that a nonlinear continuous-time system with uncertainty satisfies a Signal Temporal Logic (STL) specification.
- We combine reachability analysis and STL monitoring to reason about *all trajectories* at once.
- **Main issues:**
  - Over-approximated reachable sets $\Rightarrow$ undecidable satisfaction, pessimism.
  - Long STL horizons $\Rightarrow$ expensive tubes over large time intervals.
  - Mismatch between integration step and temporal bounds in the formula.

Motivation and Contributions

- **Goal:** verify that a nonlinear continuous-time system with uncertainty satisfies a Signal Temporal Logic (STL) specification.
- We combine reachability analysis and STL monitoring to reason about *all trajectories* at once.
- **Main issues:**
  - Over-approximated reachable sets $\Rightarrow$ undecidable satisfaction, pessimism.
  - Long STL horizons $\Rightarrow$ expensive tubes over large time intervals.
  - Mismatch between integration step and temporal bounds in the formula.
- **Our contributions:**
  - STL semantics over reachable sets via Boolean interval arithmetic.
  - Tri-valued satisfaction signals with *uncertainty markers*.
  - Incremental refinement: only reachable sets causing uncertainty are recomputed.
  - Probabilistic approach based on confidence level.

Content

Problem and Challenges

Setup. $\dot{y}(t) = f(y(t), u)$, $y(t) \in \mathbb{R}^n$, $u \in \mathcal{W} \subset \mathbb{R}^w$, $f()$ a nonlinear function. This ODE admits a unique trajectory $y(\cdot, y_0, u)$ for fixed y_0, u, under some assumption.

Definitions. (reachable set)

$$\mathrm{Reach}_t(\mathcal{Y}_0, \mathcal{W}) = \{\, y(t, y_0, u) \mid y_0 \in \mathcal{Y}_0,\ u \in \mathcal{W} \,\},$$

Time stepping with enclosures. For each step $[t_j, t_{j+1}]$ (with $t_{j+1} = t_j + h_j$), VNI delivers a set $[\,\tilde{y}_j\,]$ such that

$$\mathrm{Reach}_{[t_j, t_{j+1}]} \;\subset\; [\,\tilde{y}_j\,], \qquad \bigcup_{j=0}^{N-1} [t_j, t_{j+1}] = [t_0, T].$$

The piecewise tube $[\,\tilde{y}\,](t)$ preserves continuous-time behavior (no missed events due to sparse sampling).

J. Alexandre dit Sandretto, "Validated explicit and implicit runge-kutta methods," 2016

Pros:

- Sound over-approximation $\Rightarrow$ if formula (property) holds, it holds for all trajectories.

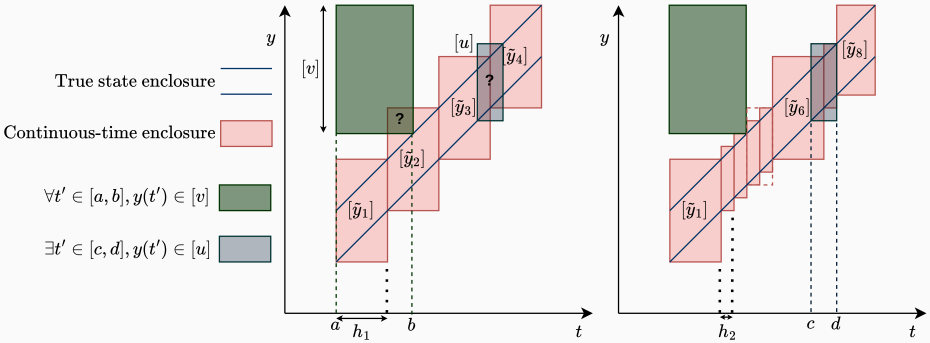
Pros:

- Sound over-approximation $\Rightarrow$ if formula (property) holds, it holds for all trajectories.

Cons / sub-problems:

- **Mismatch integration step / STL timing:**
  - Temporal operators use precise time intervals, while validated numerical integration (VNI) uses adaptive steps h_j, relying on the dynamic of the system.
  - On large step size: the state enclosure may be over-approximated.
  - Small h_j increase precision but increase the computational cost.

Illustration



- Multiple step size configuration can satisfy the precision requirements of the verification problem.
- Temporal logic formulas can be arbitrarly nested !

Background: STL

Syntax:

$$\varphi \ ::= \ \mu \ | \ \top \ | \ \neg\varphi \ | \ \varphi_1 \vee \varphi_2 \ | \ \varphi_1 \, \mathrm{U}_{[a,b]} \, \varphi_2$$

where:

- μ are atomic predicates on signals (e.g. $g(y(t)) \geq 0$).
- $\mathrm{U}_{[a,b]}$ is a bounded until operator.

Derived operators:

$$\mathrm{F}_{[a,b]}\varphi = \top \, \mathrm{U}_{[a,b]}\varphi, \qquad \mathrm{G}_{[a,b]}\varphi = \neg\mathrm{F}_{[a,b]}(\neg\varphi).$$

Signal Temporal Logic (STL) – Reminder

Syntax:

$$\varphi \ ::= \ \mu \ | \ \top \ | \ \neg\varphi \ | \ \varphi_1 \vee \varphi_2 \ | \ \varphi_1 \, \mathrm{U}_{[a,b]} \, \varphi_2$$

where:

- μ are atomic predicates on signals (e.g. $g(y(t)) \geq 0$).
- $\mathrm{U}_{[a,b]}$ is a bounded until operator.

Derived operators:

$$\mathrm{F}_{[a,b]}\varphi = \top \, \mathrm{U}_{[a,b]}\varphi, \qquad \mathrm{G}_{[a,b]}\varphi = \neg\mathrm{F}_{[a,b]}(\neg\varphi).$$

Example specification:

- "Always avoid unsafe set P": $\mathrm{G}_{[0,T]}\neg p$.
- "If we enter region V, we must reach region W within τ": $\mathrm{G}_{[0,T]}(v \Rightarrow \mathrm{F}_{[0,\tau]} w)$.

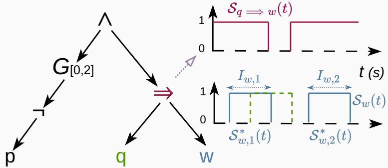
For a trajectory $s(\cdot)$, the **satisfaction signal** of φ is

$$S_\varphi : \mathbb{R}_+ \to \{0,1\}, \qquad S_\varphi(t) = 1 \text{ iff } (s,t) \vDash \varphi.$$

Unitary decomposition

The Boolean signal S_φ can be written as a disjunction of *unitary signals* $S^*_{\varphi,j}$, each one being true on a single connected time interval $I_{\varphi,j}$:

$$S_\varphi(t) = \bigvee_{j=0}^{N} S^*_{\varphi,j}(t).$$



This structure is convenient to handle temporal operators such as $\mathrm{U}_{[a,b]}$ using *back-shifting* and interval operations. *(Maler O. Monitoring 2004)*

Formula Horizon and Incremental Verification

The **necessary length** associated with a formula φ is denoted $\|\varphi\|$ and defined recursively:

$$\|\mu\| = 0, \qquad \|\neg\varphi\| = \|\varphi\|,$$
$$\left\|\varphi_1 \vee \varphi_2\right\| = \max\left(\|\varphi_1\|, \|\varphi_2\|\right),$$
$$\left\|\varphi_1 \, U_{[a,b]} \, \varphi_2\right\| = \max\left(\|\varphi_1\|, \|\varphi_2\|\right) + b.$$

The **necessary length** associated with a formula φ is denoted $\|\varphi\|$ and defined recursively:

$$\|\mu\| = 0, \qquad \|\neg\varphi\| = \|\varphi\|,$$
$$\left\|\varphi_1 \vee \varphi_2\right\| = \max\left(\|\varphi_1\|, \|\varphi_2\|\right),$$
$$\left\|\varphi_1 \, U_{[a,b]} \, \varphi_2\right\| = \max\left(\|\varphi_1\|, \|\varphi_2\|\right) + b.$$

sub-problems:

- Tube must cover at least the horizon of the formula $\|\varphi\|$ *(e.g. Reachset Temporal Logic)*.
- However, only a partial tube can enable a guaranteed satisfaction. e.g $\varphi = F_{[0,100]}p, \|\varphi\| = 100$ but if $(s,2) \vDash p \implies (s,0) \vDash \varphi$.

The **necessary length** associated with a formula φ is denoted $\|\varphi\|$ and defined recursively:

$$\|\mu\| = 0, \qquad \|\neg\varphi\| = \|\varphi\|,$$
$$\left\|\varphi_1 \vee \varphi_2\right\| = \max\left(\|\varphi_1\|, \|\varphi_2\|\right),$$
$$\left\|\varphi_1 \, U_{[a,b]} \, \varphi_2\right\| = \max\left(\|\varphi_1\|, \|\varphi_2\|\right) + b.$$

sub-problems:

- Tube must cover at least the horizon of the formula $\|\varphi\|$ *(e.g. Reachset Temporal Logic)*.
- However, only a partial tube can enable a guaranteed satisfaction. e.g $\varphi = F_{[0,100]} p$, $\|\varphi\| = 100$ but if $(s,2) \vDash p \implies (s,0) \vDash \varphi$.

Existing four-valued approaches:

- Introduce additional truth values to distinguish *insufficient horizon* (completion) vs. *inherent ambiguity*. *(e.g. Lercher & Althoff, CAV 2024)*
- They may require recomputing the tube with smaller steps before uncertainty is resolved.

Tri-Valued STL over Reachable Sets

STL over Reachable Sets: Boolean Intervals

We evaluate predicates μ on reachable sets $[\tilde{y}](t)$ instead of a single trajectory:

$$([\tilde{y}], t) \models \mu := \begin{cases} 1 & \text{if } [\tilde{y}](t) \subset \mathcal{X}^{\mu}, \\ 0 & \text{if } [\tilde{y}](t) \cap \mathcal{X}^{\mu} = \emptyset, \\ [0, 1] & \text{otherwise.} \end{cases}$$

STL over Reachable Sets: Boolean Intervals

We evaluate predicates μ on reachable sets $[\tilde{y}](t)$ instead of a single trajectory:

$$([\tilde{y}], t) \models \mu := \begin{cases} 1 & \text{if } [\tilde{y}](t) \subset \mathcal{X}^{\mu}, \\ 0 & \text{if } [\tilde{y}](t) \cap \mathcal{X}^{\mu} = \emptyset, \\ [0,1] & \text{otherwise.} \end{cases}$$

Boolean intervals:

$$\mathbb{I}_B = \{[0,0],\ [1,1],\ [0,1]\},$$

with extended Boolean operations $\wedge, \vee, \neg$.

$$0 \wedge [0,1] = 0, \qquad 0 \vee [0,1] = [0,1], \quad \text{etc.}$$

Interpretation:

- $[1,1]$: certainly true,
- $[0,0]$: certainly false,
- $[0,1]$: uncertain.

Interval Satisfaction Signals with Uncertainty

We extend the satisfaction signal to Boolean intervals:

$$[\mathcal{S}_\varphi] : \mathbb{R}^+ \to \mathbb{I}_B.$$

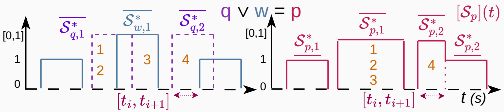
Decomposition into *certain* and *uncertain* unitary parts:

$$[\mathcal{S}_\varphi](t) = \bigvee_{j=0}^{N} \overline{\mathcal{S}^*_{\varphi,j}}(t) \vee \bigvee_{i=0}^{K} \underline{\mathcal{S}^*_{\varphi,i}}(t),$$

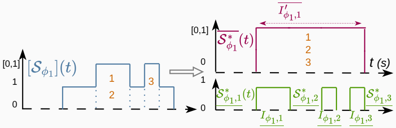
where:

- $\underline{\mathcal{S}^*_{\varphi,i}}$ is a unitary signal equal to 1 on an interval $\underline{I}_{\varphi,i}$,
- $\overline{\mathcal{S}^*_{\varphi,j}}$ is a unitary signal equal to $[0,1]$ on an interval $\overline{I}_{\varphi,j}$.

Example: OR operator



Computation of new uncertain intervals



Propagation in temporal operator

$\psi = \phi_1 \mathcal{U}_{[a,b]} \phi_2$

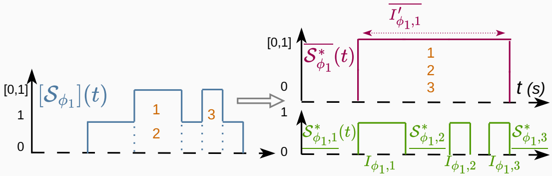
Defining the signal $\overline{\mathcal{S}_\psi}(\cdot)$ with case disjunction:

$$\overline{\mathcal{S}_\psi}(t) = \overline{\mathcal{S}_\psi}_{\underline{\varphi_2}}(t) \vee \overline{\mathcal{S}_\psi}_{\overline{\varphi_2}}(t), \text{ with}$$

$$\begin{cases} \overline{\mathcal{S}_\psi}_{\underline{\varphi_2}}(t) = \bigvee_{i=1}^{m} \bigvee_{j=1}^{n} \overline{\mathcal{S}^*_\psi}_{\underline{\varphi_2},i,j}(t), \\ \text{with, } \overline{I_\psi}_{\underline{\varphi_2},i,j} = \left(\left(\overline{I'_{\varphi_1,i}} \cap \underline{I_{\varphi_2,j}}\right) \ominus [a,b]\right) \cap \overline{I'_{\varphi_1,i}}. \end{cases} \quad (1)$$

with the $[a,b]$-back shifting defined as

$I \ominus [a,b] = [m-b, n-a) \cap \mathbb{T}$ *(Maler O. Monitoring 2004)*



Marker Propagation and Incremental Refinement

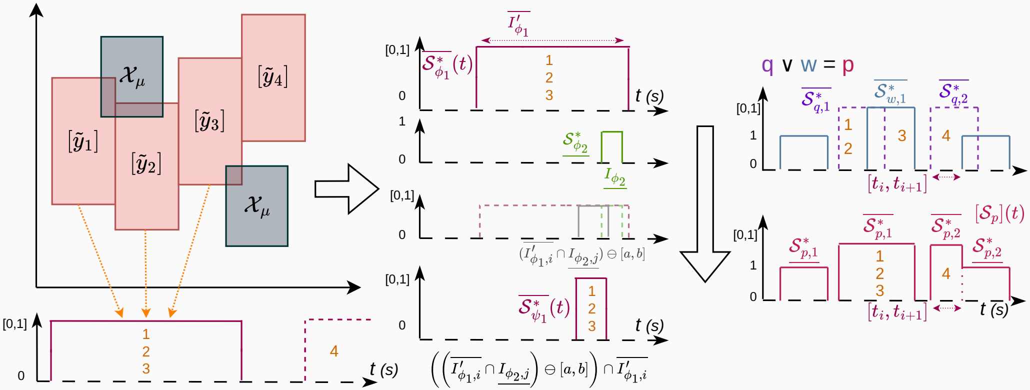
Markers on Uncertain Intervals

Uncertainty in $[\mathcal{S}_\varphi]$ arises from:

- Inherent ambiguity;
- Over-aproximation of the reachable tube;
- Large step size computing the reachable sets $[\tilde{y}_j]$;
- Incomplete tube (insufficient time horizon for the formula).

Idea: attach markers to each uncertain unitary interval to indicate its *origin*:

- index of the time step / box $[\tilde{y}_j]$ that caused uncertainty,
- type of uncertainty (spatial over-approximation vs. missing horizon).

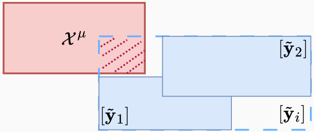


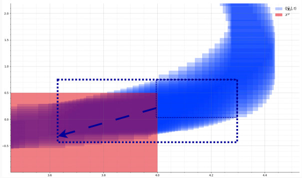
Markers are defined at predicate level and propagated through the STL syntax tree.

Incremental Refinement Algorithm

High-level procedure:

1. Compute an initial reachable tube $[\tilde{y}](t)$ with VNI and evaluate $[\mathcal{S}_\varphi]$ with markers.
2. While there exists a satisfaction value $[0, 1]$ or above minimum step size:
   - If markers indicate predicate set crossing:
     - bisect in time the corresponding boxes (refine in state space),
     - recompute the local reachable sets with higher order method and update the tube.
   - If markers indicate missing horizon:
     - extend the final time by ΔT and complete the tube.
3. Re-evaluate $[\mathcal{S}_\varphi]$.



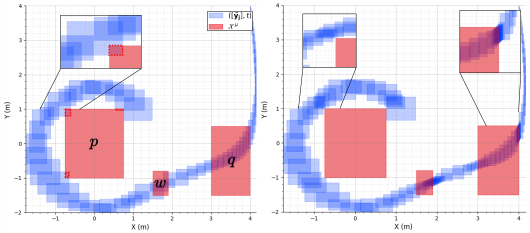


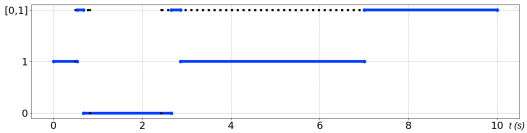
Incremental Tube and Satisfaction

The studied formula is as follow: $\varphi = G_{[0,1]}(G_{[0,2]}(\neg p) \wedge (q \implies F_{[1,2]}w))$.

Tube computed from markers

Satisfaction signal of a formula





Initially, large time segments are labelled as $[0,1]$. After a few refinement iterations guided by markers, uncertainty is confined or removed, and most of the original tube is never recomputed.

At $t = 2.63$s, high precision is required: tighter step size tolerance and higher-order integration increase simulation time. Using the same reachability software, uncertainty tracking is **7x** faster than using a blind incremental approach.

Confidence level

Let $\mathcal{P} \subseteq \mathbb{R}^m$ be the parameter space and $\mathcal{S}_c$ a subset of this space.

Definition
Upper enclosure of a Cloud

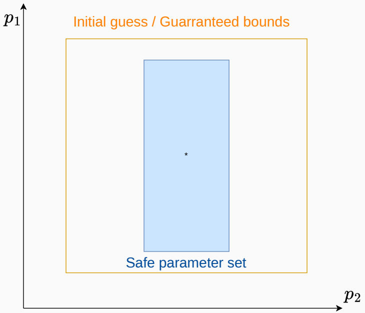
$$\overline{\text{Cloud}}_{\mathcal{Y}} = \left\{ [\tilde{y}]_{\mathcal{S}_c^i}(\cdot) \mid i \in \{1, \ldots, f\}\right\}. \tag{2}$$

We have P a $\mathcal{P}$-valued stationary random variable on a probability space $(\Omega, \mathcal{A}, \mathbb{P})$.

$$\boxed{\Pr(P \in \mathcal{S}_c) \leq \ \Pr\left(\hat{y}(t) \in [\tilde{y}]_{\mathcal{S}_c}(t)\right), \ t \in [t_0, T].} \tag{3}$$

In the context of ODEs, a cloud yields a collection of reachable tube for varying subset sets $\mathcal{S}_c^i$, forming a *potential cloud* a probabilistic semantic of state-space uncertainty.

Main Idea



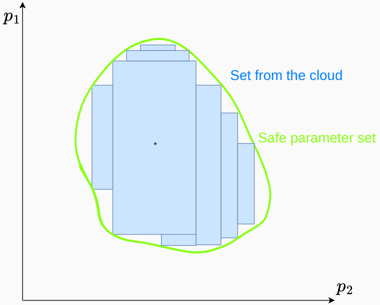
Safe set $\mathcal{S}_c$ in parameter space with probability mass c.

Theorem (Guaranteed probabilistic bound)
Let $\mathcal{S}_c \subseteq \Omega$ be a measurable bounded set of stationary independent parameters with

$$\Pr(\hat{p} \in \mathcal{S}_c) = c.$$

And under three valued semantic, we have the double enclosure:

$$\boxed{\begin{aligned} ([\tilde{y}]_{\mathcal{S}_c}, t) \models \varphi &\implies \Pr\big((\hat{y}, t) \models \varphi\big) \geq c, \\ ([\tilde{y}]_{\mathcal{S}_c}, t) \not\models \varphi &\implies \Pr\big((\hat{y}, t) \not\models \varphi\big) \geq c. \end{aligned}}$$



Pavement from a Cloud in blue, true validation set $\mathcal{P}_\phi$ in green

Corollary (Safe set construction and tight bound)
To obtain the tightest possible lower bound on the probability of satisfaction, we construct a cloud of reachable tubes

$$\overline{\mathrm{Cloud}}_{\mathcal{Y}}^{\phi} = \{[\tilde{y}]_{\mathcal{S}^i}(\cdot) \mid i \in \{1,\dots,f\}\} \tag{4}$$

such that $\forall i \in \{1,\dots,f\}$, $([\tilde{y}]_{\mathcal{S}^i}, t) \models \phi$, *define the safe set* $\mathcal{S}_v = \bigcup_{i=1}^{f} \mathcal{S}^i$. *Then* $\mathcal{S}_v$ *is the largest guaranteed validation set satisfying* $\mathcal{S}_v \subseteq \mathcal{P}_\phi$, *and*

$$v = \Pr\left((\hat{y}, t) \models \phi\right), \text{ whenever } \mathcal{S}_v = \mathcal{P}_\phi.$$

Finding a Safe Set

Global certainty clause ψ

$$\psi \iff (([\tilde{y}]_{\mathcal{S}_c}, t) \models \varphi \neq [0,1])$$

ψ is true iff the formula evaluation is **certain** (not indeterminate).

Clause Q_j: is reachable set j resolved*?

$$Q_j \iff \underbrace{([\tilde{y}_j]_{\mathcal{S}_c} \subset \mathcal{X}^\mu)}_{\text{fully inside}} \vee \underbrace{([\tilde{y}_j]_{\mathcal{S}_c} \cap \mathcal{X}^\mu = \emptyset)}_{\text{fully outside}}$$

DNF of ψ

$$\psi \equiv \bigvee_{k \in \mathcal{K}} \left(\bigwedge_{j \in C_k} Q_j \right)$$

* *The choice of inclusion depends on the center of the parameter-set.*

Finding a Safe Set

Global certainty clause ψ

$$\psi \iff (([\tilde{y}]_{\mathcal{S}_c}, t) \models \varphi \neq [0,1])$$

ψ is true iff the formula evaluation is **certain** (not indeterminate).

Clause Q_j: is reachable set j resolved*?

$$Q_j \iff \underbrace{([\tilde{y}_j]_{\mathcal{S}_c} \subset \mathcal{X}^\mu)}_{\text{fully inside}} \vee \underbrace{([\tilde{y}_j]_{\mathcal{S}_c} \cap \mathcal{X}^\mu = \emptyset)}_{\text{fully outside}}$$

* *The choice of inclusion depends on the center of the parameter-set.*

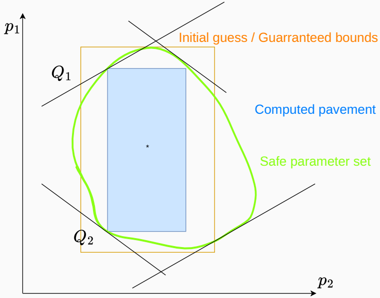
DNF of ψ

$$\psi \equiv \bigvee_{k \in \mathcal{K}} \left(\bigwedge_{j \in C_k} Q_j \right)$$

Why DNF?

Each disjunct C_k is an independent **sufficient condition** for **certainty**. We search for the one with the highest probability mass.

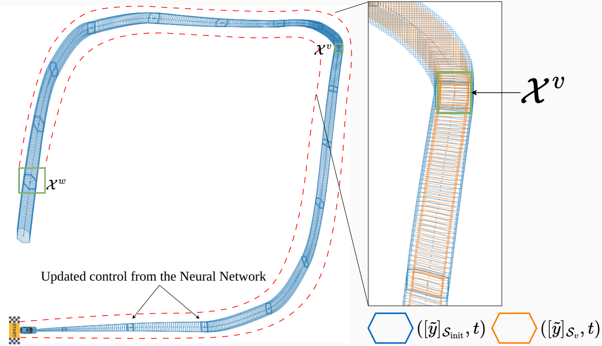
Uncertainty tracking drastically reduces the number of clause to test and the combinatorial problem becomes tractable in practice.



Safe set $\mathcal{S}_c$

For example $Q_1 \wedge Q_2$ are two clauses derived from uncertain reachable sets.
Linear constraint are derived symbolically from the zonotope of each reachable sets.

As an example, consider a car driven by a neural network under the temporal constraint: $\varphi = G_{[0,6.7]}(v \Rightarrow F_{[3.5,4.5]} w) \wedge F_{[5.2,5.7]} v$.



With Gaussian uncertainties in the steering and throttle response.

Here a Monte Carlo gives $\Pr((\hat{y}, t) \models \varphi) \approx 0.98$, evaluating only one mean centered parameter set gives:

$$\Pr((\hat{y}, t) \models \varphi) \geq 0.853$$

- A guaranteed satisfaction of the specification is computed
- A method is proposed to compute parsimoniously the tube
- All tools are available in Dynibex

Future works:

- Limiting temporal overaproximation of the markers

Code on GitHub:

Thank you!