Guaranteed Satisfaction of a Temporal Logic Formula with a Confidence Parameter

Joris Tillet, Elena Vanneaux, Julien Alexandre Dit Sandretto

Guaranteed Satisfaction of a Temporal Logic Formula with a Confidence Parameter

Joris Tillet, Julien Alexandre dit Sandretto and Elena Vanneaux

ENSTA Paris, Institut Polytechnique de Paris
828, boulevard des maréchaux, 91762 Palaiseau Cedex, France
{joris.tillet,julien.alexandre-dit-sandretto,elena.vanneaux}
@ensta-paris.fr

Keywords: STL, Interval Methods, Confidence on Uncertainties

Signal Temporal Logic (STL) [3] is a classical formalism used for verification of hybrid systems. In this work, the satisfaction of a temporal logic formula for a given uncertain signal is computed. We consider an approach using interval analysis to ensure computation guarantees and take into account uncertainties in a robust manner. In addition, a confidence level parameter allows considering more or less uncertainties, making calculable the risk to violate specifications.

STL is defined recursively by:

$$\phi := \mu \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \,\mathcal{U}_{[a,b]}\, \phi_2 \mid \top \tag{1}$$

with ϕ an STL formula, and $\mathcal{U}$ the *until* operator. The interval $[a, b]$ is defined with $a, b \in \mathbb{R}^+$. We have

$$(x,t) \vDash \phi_1 \,\mathcal{U}_{[a,b]} \phi_2 \iff \exists t' \in [a,b]\ (x, t+t') \vDash \phi_2 \text{ and } \forall t'' \in [t,t']\ (x,t'') \vDash \phi_1, \tag{2}$$

and μ is an atomic predicate: $\mu_x \equiv f(x_1(t), \ldots, x_n(t)) > 0$. Several operators can be derived from STL, such as the well known *finally* operator $\mathcal{F}_{[a,b]}\phi \equiv \top \,\mathcal{U}_{[a,b]}\phi$.

The satisfaction of ϕ by a signal $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is written $(\mathbf{x}, t) \vDash \mu$ and is true if and only if we have $f(x_1(t), \ldots, x_n(t)) > 0$.

Formalism

Instead of defining the satisfaction of an STL formula just by a classical boolean value, we use boolean intervals to take into account undetermined cases due to uncertainties and set-abstraction [2]. Thus, we use intervals from the set $\{\emptyset, 0, 1, [0,1]\}$, where $\emptyset$ stands for impossible, 0 for false ($\bot$), 1 for true ($\top$) and $[0,1]$ for undetermined. We define this new STL with:

$$\phi := \mu \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \,\mathcal{U}_{[a,b]}\, \phi_2 \mid 1 \mid [0,1]. \tag{3}$$

And we have:

$$\begin{array}{lll}
\neg[0,1] \equiv [0,1] & [0,1] \vee 1 \equiv 1 & [0,1] \,\mathcal{U}_{[a,b]}\, 0 \equiv 0 \\
[0,1] \wedge 1 \equiv [0,1] & [0,1] \vee 0 \equiv [0,1] & 1 \,\mathcal{U}_{[a,b]}\, [0,1] \equiv [0,1] \\
[0,1] \wedge 0 \equiv 0 & [0,1] \,\mathcal{U}_{[a,b]}\, 1 \equiv [0,1] & 0 \,\mathcal{U}_{[a,b]}\, [0,1] \equiv 0.
\end{array}$$

As we use intervals (sets) to represent uncertainties, when testing the satisfaction of an atomic predicate, it is equivalent to use set operators such that inclusion and emptiness intersection.

We can define the level set representing a predicate $\mu \equiv x > 0$ by $\mathcal{X}^\mu = \{x \in \mathbb{R} \mid x > 0\}$. Then we have:

$$(\mathbf{x}, t) \vDash \mu \equiv \begin{cases} 1 & \text{if } \mathbf{x}(t) \subset \mathcal{X}^\mu; \\ 0 & \text{if } \mathbf{x}(t) \cap \mathcal{X}^\mu = \emptyset; \\ [0,1] & \text{otherwise.} \end{cases} \tag{4}$$

Confidence-based Tubes

We define a *confidence* parameter noted $cc \in [0, 1]$. It denotes the confidence we have in a set to contain the actual trajectory. It is inspired from [1]. When $cc = 1$, then we are sure to not miss the solution, at the risk of having huge sets. Taking a smaller cc parameter implies a greater accuracy, at the cost of a less reliable result.

Figure 1 gives an example of three tubes representing the same trajectory but with different confidences. Darker strokes are used for higher confidences.

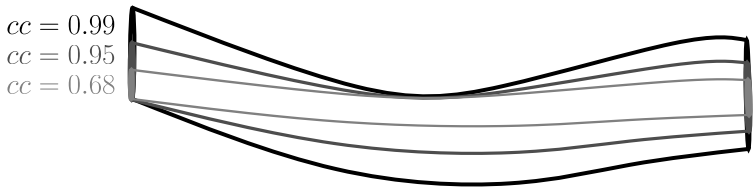

Figure 1: Example of three different values of cc for a tube.

We have:

$$(cc_1, cc_2) \in [0, 1]^2,\ cc_1 \leq cc_2 \implies \mathcal{X}^{cc_1} \subseteq \mathcal{X}^{cc_2}. \tag{5}$$

Now we can add this parameter in our formalism to define a satisfaction of an STL formula with respect to a given confidence. In other words, we allow concluding the satisfaction of a specification if only the $(1 - cc)$ part of the tube violates the formula.

For instance, depending on the confidence on the initial set of a system, we can deduce if it will satisfy some constraints. On the other hand, we can also approximate the maximum value for cc such that we ensure the specifications are satisfied, helping to measure the risk to launch a critical system.

Acknowledgement

The authors acknowledge support from the CIEDS[1] with the STARTS project.

References

[1] Julien Alexandre Dit Sandretto. Confidence-based contractor, propagation and potential clouds for differential equations. pages 49–68.

[2] Luc Jaulin, Michel Kieffer, Olivier Didrit, and Éric Walter. Applied interval analysis. In *Applied Interval Analysis: With Examples in Parameter and State Estimation, Robust Control and Robotics*, pages 11–43. Springer.

[3] Oded Maler and Dejan Nickovic. Monitoring temporal properties of continuous signals. In *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, Lecture Notes in Computer Science, pages 152–166. Springer.

[1] CIEDS: French Interdisciplinary Center for Defense and Security.