



HAL
open science

Interval Methods applied to Signal Temporal Logic - Overview and Extension on Tubes

Joris Tillet, Elena Vanneaux, Julien Alexandre Dit Sandretto

► **To cite this version:**

Joris Tillet, Elena Vanneaux, Julien Alexandre Dit Sandretto. Interval Methods applied to Signal Temporal Logic - Overview and Extension on Tubes. Summer Workshop on Interval Methods (SWIM) 2024, Jun 2024, Maastricht, Netherlands. hal-04716742

HAL Id: hal-04716742

<https://hal.science/hal-04716742v1>

Submitted on 1 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Interval Methods applied to Signal Temporal Logic – Overview and Extension on Tubes

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

Introduction

Designers and users of cyber-physical systems often require guarantees on the system's behavior, hence the need of a runtime verification process. This formal verification can be done using temporal logic, a formalism able to specify the system's requirements with temporal constraints. In 1977, Linear Temporal Logic (LTL) [9] is introduced, allowing to describe discrete time properties on a discrete signal. This is mainly used for formal verification of software or digital hardware, but reaches its limits when considering real-time constraints. When considering CPS, which are hybrid systems, man needs an extension of LTL able to handle real-time properties on real-value signal. This is the purpose of Signal Temporal Logic (STL) [8]. We consider an approach using interval analysis to ensure computation guarantees and take into account uncertainties in a robust manner.

STL is defined recursively by:

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

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

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

μ is an atomic predicate: $\mu_x \equiv f(x_1(t), \dots, x_n(t)) > 0$.

Several operators can be derived from STL, such as the well known finally operator $\mathcal{F}_{[a,b]} \phi \equiv \top \mathcal{U}_{[a,b]} \phi$, noted \diamond , which is sometimes called *eventually*. The satisfaction of ϕ by a signal $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ is written $(\mathbf{x}, t) \models \mu$ and is true if and only if we have $f(x_1(t), \dots, x_n(t)) > 0$.

Monitoring using intervals

Related works

The qualitative satisfaction of an STL formula is a boolean value. This binary result can not contain an information of robustness of satisfaction. Quantitative satisfaction [5] introduces this notion of robustness to provide a measure of how much a trace satisfy or violate a given property. This approach can be used to handle some uncertainties, as in [4] where spatial and temporal uncertainties are considered, sometimes by the help of intervals. For instance, in [11], an offline monitoring algorithm with intervals for finite time STL formulas is proposed. In [3], an online monitoring is proposed using an interval of all the possible quantitative satisfaction of a partial signal with unbounded future.

In the literature, most of the researchers proposing STL monitors deal with single traces. However, in our approach, we want to go further by providing a robustness to numerical and model approximations. We then consider set of traces that can be represented by tubes (interval of trajectories).

Tubes

Interval STL is introduced in [1] to take uncertainties in predicates. Signals of intervals are considered, and quantitative satisfaction is returned as an interval. Then, depending on the inclusion or not of the zero value in this interval, the resulting satisfaction is a three-valued logical value: true, false, or undef. In [10], the authors cut the tubes in the time dimension and interpret STL formulas as successive discrete states in a new formalism called Reachset Temporal Logic. When there exists a trace in the set of trace that does not satisfy the constraint, then the proposed monitor returns false. The approach proposed in [6] is closer to [8]: it searches times when properties become true or false, and then propagates the information in a bottom up manner to deduce the result for the whole STL formula. In the latter, there is no completeness: the algorithm can return “unknown” when there is an ambiguity on the satisfaction or the violation of every trace.

Boolean interval extension

In our work, we propose to extend these previous results to boolean interval, such that the ambiguous “unknown” result is represented by the interval $[0, 1]$, and the ambiguity may be eliminated later if enough information are provided. Indeed, in the following example, both approaches from [10] and [6] lead to an unknown or false result, despite the signal does satisfy the formula.

Consider the tube $[x](t)$ represented in the Figure 1. We have a set point $\rho \in \mathbb{R}$ we want our system to reach in the time interval $[a, b] \subset \mathbb{R}^+$ (and not before). The corresponding STL formula Φ is:

$$\Phi \equiv \neg\phi \mathcal{U}_{[a,b]}\phi$$

with $\phi \equiv [x] \geq \rho$.

In this example, during the period $[a, b]$, the satisfaction of the predicate ϕ is ambiguous. However, the STL formula Φ is well satisfied by any trace taken in the tube $[x](t)$. In order to conclude the satisfaction rather than an unknown or false result, we propose to use

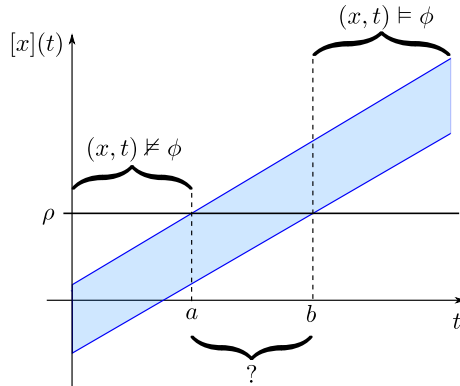


Figure 1: The tube is represented in blue. Before a and after b , there is no doubt on satisfaction or violation of the predicate $\phi \equiv x \geq \rho$. However, during the period $[a, b]$, some traces may satisfy ϕ while other not.

reachability analysis to obtain the result. The difficulty lies in the fact that the time t' from equation (2) may be different for every possible trace included in the tube, so there is an infinite number of trace and time to check.

The proposed solution is to use a branching algorithm on the time interval $[a, b]$, such that we can conclude the satisfaction of the formula when the set $[\mathbf{x}](0)$ is completely covered by the union of the inner backward reachsets starting from the set X_ϕ of states satisfying ϕ and from times $[t'] \subset [a, b]$ (see e.g. [7]).

Acknowledgement

The authors acknowledge support from the CIEDS¹ with the STARTS project.

References

- [1] Luke Baird, Akash Harapanahalli, and Samuel Coogan. Interval signal temporal logic from natural inclusion functions. Conference Name: IEEE Control

¹CIEDS: French Interdisciplinary Center for Defense and Security.

Systems Letters.

- [2] Ezio Bartocci, et al. Maler, Dejan Ničković, and Sriram Sankaranarayanan. Specification-based monitoring of cyber-physical systems: A survey on theory, tools and applications. *Lectures on Runtime Verification*, volume 10457, pages 135–175. Springer.
- [3] Jyotirmoy V. Deshmukh, et al. Robust online monitoring of signal temporal logic.
- [4] Alexandre Donzé and Oded Maler. Robust satisfaction of temporal logic over real-valued signals. *Formal Modeling and Analysis of Timed Systems*, volume 6246, pages 92–106. Springer.
- [5] Georgios E. Fainekos and George J. Pappas. Robustness of temporal logic specifications for continuous-time signals.
- [6] Daisuke Ishii, Naoki Yonezaki, and Alexandre Goldsztejn. Monitoring temporal properties using interval analysis.
- [7] Alexander B. Kurzhanski and Pravin Varaiya. *Dynamics and Control of Trajectory Tubes: Theory and Computation*, volume 85 of *Systems & Control: Foundations & Applications*. Springer International Publishing.
- [8] Oded Maler and Dejan Nickovic. Monitoring temporal properties of continuous signals. *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, pages 152–166. Springer.
- [9] Amir Pnueli. The temporal logic of programs. In *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*, pages 46–57.
- [10] Hendrik Roehm, et al. STL model checking of continuous and hybrid systems. *Automated Technology for Verification and Analysis*, Lecture Notes in Computer Science, pages 412–427. Springer.
- [11] Bingzhuo Zhong, Claudius Jordan, and Julien Provost. Extending signal temporal logic with quantitative semantics by intervals for robust monitoring of cyber-physical systems.