Work-in-Progress: Towards a Theory of Robust Quantitative Semantics for Signal Temporal Logic

Jean-Baptiste Jeannin
University of Michigan

Jiawei Chen
University of Michigan

José Luiz Vargas de Mendonça
University of Michigan

Konstantinos Mamouras
Rice University

***Abstract*—Several quantitative semantics of temporal logics have been investigated recently. We propose a general form to model those quantitative semantics, establish requirements for soundness, and evaluate the framework on a few examples.**

I. Introduction

The seminal works of Fainekos and Pappas [1] and Donzé and Maler [2] have defined and popularized the modern concept of quantitative semantics for a Signal Temporal Logic (STL) formula. Those semantics play an important role in both the falsification and control synthesis for dynamical systems. Recently, several different quantitative semantics have been proposed, offering better performance in many cases. Yet a general, systematic understanding of the structure and properties of quantitative semantics is missing. In this paper, we develop a general framework to model quantitative semantics. We focus on soundness, which ensures that the quantitative semantics of a statement is positive when the statement is true, and negative when the statement is false. We derive simple, sufficient conditions in our framework for soundness. We compare the performance of different quantitative semantics of our framework on several benchmarks. Our general framework has already helped us generalize and mix some existing semantics, and we believe that it will lead to the discovery of new, interesting quantitative semantics in the future.

II. Quantitative Semantics

A. Syntax and Qualitative Semantics

We consider properties of a real-valued signal over a discrete or continuous domain $\mathbb{T}$. In the continuous-time case, $\mathbb{T} = \mathbb{R}_+$; in the discrete-time case $\mathbb{T} = \mathbb{N}$. We denote by I a *bounded* interval over $\mathbb{T}$, and by $\mathbb{I}$ the set of all such bounded intervals. In the continuous case, we assume that the signal is integrable on any bounded interval $I \in \mathbb{I}$. A signal σ over n variables $x_1, ..., x_n$ is a function from $\mathbb{T}^n$ to $\mathbb{R}$, and we write $l(\sigma)$ a function using any of those n variables. We also write $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ and $\overline{\mathbb{R}_+} = \mathbb{R}_+ \cup \{+\infty\}$.

a) Syntax.: An STL formula φ is given by:

$$\varphi, \psi ::= \top \mid l(\sigma) \geq 0 \mid l(\sigma) > 0 \mid \neg\varphi \mid \varphi \wedge \psi \mid \psi \mathbf{U}_I \varphi$$

Operators $\bot$, $\vee$, $\mathbf{F}_I$ and $\mathbf{G}_I$ are defined in the standard way. The qualitative semantics of STL, $\sigma^t \vDash \varphi$, defines the truth value of σ at time t with respect to φ, and is standard [1], [2].

B. Standard Quantitative Semantics

The standard quantitative semantics $\rho_0(\varphi, \sigma, t) \in \overline{\mathbb{R}}$ is defined for a specification φ, a trace σ over $\mathbb{T}$, and a time $t \in \mathbb{T}$ [1], [2]. It is defined as $\rho_0(\varphi, \sigma, t) = \rho_0^+(\varphi, \sigma, t) + \rho_0^-(\varphi, \sigma, t)$, where ρ_0^+ and ρ_0^- are:

- $\rho_0^+(\top, \sigma, t) = +\infty$ and $\rho_0^-(\top, \sigma, t) = 0$
- $\rho_0^+(l(\sigma) \geq 0, \sigma, t) = \rho_0^+(l(\sigma) > 0, \sigma, t) = \max(0, l(\sigma[t]))$
- $\rho_0^-(l(\sigma) \geq 0, \sigma, t) = \rho_0^-(l(\sigma) > 0, \sigma, t) = \min(0, l(\sigma[t]))$
- $\rho_0^+(\neg\varphi, \sigma, t) = -\rho_0^-(\varphi, \sigma, t)$
- $\rho_0^-(\neg\varphi, \sigma, t) = -\rho_0^+(\varphi, \sigma, t)$
- $\rho_0^+(\varphi \wedge \psi, \sigma, t) = \min(\rho_0^+(\varphi, \sigma, t), \rho_0^+(\psi, \sigma, t))$
- $\rho_0^-(\varphi \wedge \psi, \sigma, t) = \min(\rho_0^-(\varphi, \sigma, t), \rho_0^-(\psi, \sigma, t))$
- $\rho_0^+(\psi \mathbf{U}_I \varphi, \sigma, t) = \max\limits_{t' \in I} \left(\min(\rho_0^+(\varphi, \sigma, t+t'), \min\limits_{t'' \in [t, t+t']} \rho_0^+(\psi, \sigma, t'')) \right)$
- $\rho_0^-(\psi \mathbf{U}_I \varphi, \sigma, t) = \max\limits_{t' \in I} \left(\min(\rho_0^-(\varphi, \sigma, t+t'), \min\limits_{t'' \in [t, t+t']} \rho_0^-(\psi, \sigma, t'')) \right)$

An essential property of quantitative semantics is soundness, proved by structural induction on the STL formula [1], [2]:

Theorem 1: if $\rho_0(\varphi, \sigma, t) > 0$ then $\sigma^t \vDash \varphi$, and if $\rho_0(\varphi, \sigma, t) < 0$ then $\sigma^t \nvDash \varphi$.

III. A family of quantitative semantics

A. A general form

The goal of this work is to establish a generalized form for quantitative semantics, parameterized by unary functions $\nu : \mathbb{R} \to \overline{\mathbb{R}}_+$ and $\mu : \mathbb{R} \to \overline{\mathbb{R}}_-$, binary integrators α, β, ζ, $\eta : \overline{\mathbb{R}}_+ \times \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+$, as well as time integrators Γ, Δ, Θ, $\Xi : \mathbb{I} \times (\mathbb{I} \to \overline{\mathbb{R}}_+) \to \overline{\mathbb{R}}_+$. Using those operators, we can define a generic $\rho(\varphi, \sigma, t) = \rho^+(\varphi, \sigma, t) + \rho^-(\varphi, \sigma, t)$ with:

- $\rho^+(\top, \sigma, t) = +\infty$ and $\rho^-(\top, \sigma, t) = 0$
- $\rho^+(l(\sigma) \geq 0, \sigma, t) = \rho^+(l(\sigma) > 0, \sigma, t) = \nu(l(\sigma[t]))$
- $\rho^-(l(\sigma) \geq 0, \sigma, t) = \rho^-(l(\sigma) > 0, \sigma, t) = \mu(l(\sigma[t]))$
- $\rho^+(\neg\varphi, \sigma, t) = -\rho^-(\varphi, \sigma, t)$
- $\rho^-(\neg\varphi, \sigma, t) = -\rho^+(\varphi, \sigma, t)$
- $\rho^+(\varphi \wedge \psi, \sigma, t) = \alpha(\rho^+(\varphi, \sigma, t), \rho^+(\psi, \sigma, t))$
- $\rho^-(\varphi \wedge \psi, \sigma, t) = -\beta(-\rho^-(\varphi, \sigma, t), -\rho^-(\psi, \sigma, t))$
- $\rho^+(\psi \mathbf{U}_I \varphi, \sigma, t) = \Gamma\limits_{t' \in I} \zeta(\rho^+(\varphi, \sigma, t+t'), \Delta\limits_{t'' \in [t, t+t']} \rho^+(\psi, \sigma, t''))$
- $\rho^-(\psi \mathbf{U}_I \varphi, \sigma, t) = -\Theta\limits_{t' \in I} \eta(-\rho^-(\varphi, \sigma, t+t'), \Xi\limits_{t'' \in [t, t+t']} (-\rho^-(\psi, \sigma, t'')))$

This general form can instantiate several previous works, e.g.:

- Donzé and Maler [2] use $\nu = \max(\cdot, 0)$, $\mu = \min(\cdot, 0)$, $\alpha = \zeta = \min$, $\beta = \eta = \max$, $\Gamma = \Xi = \max$, $\Delta = \Theta = \min$.
- Haghighi et al. [3] use $\nu = \max(\cdot, 0)$, $\mu = \min(\cdot, 0)$, $\alpha = \zeta = \min$, $\beta = \eta = \max$, $\Gamma = \Theta = \Sigma$ (sum operator), $\Delta = \min$, $\Xi = \max$.

B. General requirements for soundness

We now introduce novel, sufficient soundness conditions on the aforementioned functions:

1) If $\nu(x) > 0$ then $x > 0$. Example of possible ν: $\max(\cdot, 0)$.
2) If $\mu(x) < 0$ then $x < 0$. Examples of possible μ: $\min(\cdot, 0)$.

	Max	Add	MARV	Const	TeLEx
AFC	4	4	4	4	4
autotrans_01	2	2	2	2	2
Proj	26	26	49	127	350
Path	55	63	56	178	358

TABLE I: Number of iterations until falsification

3) If $x \geq 0$, $y \geq 0$ and $\alpha(x, y) > 0$, then $x > 0$ **and** $y > 0$. Examples of possible α: min, product $\prod$.
4) If $x \geq 0$, $y \geq 0$ and $\beta(x, y) > 0$, then $x > 0$ **or** $y > 0$. Examples of possible β: max, sum $\sum$.
5) If all $x_k \geq 0$ and $\left(\Gamma_k x_k\right) > 0$, then $\exists k, x_k > 0$. Example Γ: max, $\sum$ (discrete sum), $\int$ (integral).
6) If all $x_k \geq 0$ and $\left(\Delta_k x_k\right) > 0$, then $\forall k, x_k > 0$. Examples of possible Δ: min, $\prod$ (product, discrete case).
7) ζ follows the requirements of α, and η the ones of β.
8) Θ follows the requirements of Δ, and Ξ the ones of Γ.

We now prove a novel generic soundness theorem:

Theorem 2: Under conditions (1)-(8), if $\rho(\varphi, \sigma, t) > 0$ then $\sigma^t \models \varphi$, and if $\rho(\varphi, \sigma, t) < 0$ then $\sigma^t \not\models \varphi$.

IV. Experimental Results

We tested quantitative semantics in the MATLAB toolkit Breach [4], including built-in Max (max/min), Add (addition-based semantics [5]), MARV (Mean Alternative Robustness Value [6]), and Const (Constant), where $\nu(\cdot) = \max(100(\mathrm{sgn}(\cdot)),\ 0)$. We extended Breach with a MATLAB implementation of the TeLEx semantics [7]. We benchmarked the various semantics on iterations until falsification (Table 1). We tested the semantics on four Simulink based benchmarks. *AFC* (Abstract Fuel Control) and *autotrans_01* simulate various automotive control systems [4], [8]. *Proj* (Projectile) simulates the motion of a projectile, and *Path* simulates a robot on a Dubins path. *AFC* and *autotrans_01* finished in very few iterations. We hypothesize that this is because their specifications are falsified by extreme values, which are tested early in the search. *Proj* and *Path* are falsified for a narrow range of intermediate parameters, which resulted in higher iteration counts and more variation between semantics. TeLEx sees higher iteration counts, which may be a result of its semantics favoring tightness over robustness. Further testing may reveal the effects of semantics complexity on runtime.

V. Related Work

Fainekos and Pappas [1] define the spatial robustness semantics for temporal properties, which quantifies the degree of satisfaction using the extended real numbers. Donzé and Maler [2] consider an extension of spatial robustness that also takes temporal displacement into account. Akazaki and Hasuo [9] proposed an extension of MITL with averaged temporal operators. Another average-based robustness was explored in [10], [11]. The original robustness semantics [1] uses $\max$ (resp., $\min$) for interpreting disjunction (resp., conjunction), which are not smooth functions. Since smoothness is a valuable property in the context of falsification and synthesis, many authors have considered smooth variants of the robustness semantics [12], [3], [13]. The quantitative semantics of temporal properties is viewed as linear time-invariant filtering in [14]. A robustness measure based on weighted edit distance has been proposed in [15]. Algebraic generalizations of the robustness semantics using semirings and lattices as quantitative truth domains have also been considered in [16], [17] (semirings) and in [18] (lattices).

VI. Future Work

A next step is to explore smoothness of semantics. The standard spatial robustness semantics [1] has limitations for applications that use the semantics to solve optimization problems, because the functions min and max are non-smooth and non-differentiable. To use powerful gradient-based optimization algorithms, smooth robustness semantics are desirable [7].

References

[1] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theoretical Computer Science*, 2009.

[2] A. Donzé and O. Maler, "Robust satisfaction of temporal logic over real-valued signals," in *Formal Modeling and Analysis of Timed Systems*, 2010.

[3] I. Haghighi, N. Mehdipour, E. Bartocci, and C. Belta, "Control from signal temporal logic specifications with smooth cumulative quantitative semantics," in *Conference on Decision and Control (CDC)*. IEEE, 2019.

[4] A. Donzé, "Breach, A Toolbox for Verification and Parameter Synthesis of Hybrid Systems," in *Computer Aided Verification*, 2010, vol. 6174.

[5] K. Claessen, N. Smallbone, J. Eddeland, Z. Ramezani, and K. Åkesson, "Using Valued Booleans to Find Simpler Counterexamples in Random Testing of Cyber-Physical Systems," *IFAC-PapersOnLine*, vol. 51, 2018.

[6] J. Eddeland, S. Miremadi, M. Fabian, and K. Akesson, "Objective functions for falsification of signal temporal logic properties in cyber-physical systems," in *Conference on Automation Science and Engineering (CASE)*, Aug. 2017.

[7] S. Jha, A. Tiwari, S. A. Seshia, T. Sahai, and N. Shankar, "TeLEx: learning signal temporal logic from positive examples using tightness metric," *Formal Methods in System Design*, vol. 54, no. 3, Nov. 2019.

[8] B. Hoxha, H. Abbas, and G. Fainekos, "Benchmarks for Temporal Logic Requirements for Automotive Systems," 2015, pp. 25–18.

[9] T. Akazaki and I. Hasuo, "Time robustness in mtl and expressivity in hybrid system falsification," in *Computer Aided Verification*, 2015.

[10] N. Mehdipour, C.-I. Vasile, and C. Belta, "Arithmetic-geometric mean robustness for control from signal temporal logic specifications," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 1690–1695.

[11] L. Lindemann and D. V. Dimarogonas, "Robust control for signal temporal logic specifications using discrete average space robustness," *Automatica*, vol. 101, pp. 377–387, 2019.

[12] Y. V. Pant, H. Abbas, and R. Mangharam, "Smooth operator: Control using the smooth robustness of temporal logic," in *Control Technology and Applications (CCTA)*. IEEE, 2017, pp. 1235–1240.

[13] Y. Gilpin, V. Kurtz, and H. Lin, "A smooth robustness measure of signal temporal logic for symbolic control," *IEEE Control Systems Letters*, 2020.

[14] A. Rodionova, E. Bartocci, D. Nickovic, and R. Grosu, "Temporal logic as filtering," in *Hybrid Systems: Computation and Control*, 2016.

[15] S. Jakšić, E. Bartocci, R. Grosu, T. Nguyen, and D. Ničković, "Quantitative monitoring of stl with edit distance," *Formal methods in system design*, vol. 53, no. 1, pp. 83–112, 2018.

[16] S. Jakšić, E. Bartocci, R. Grosu, and D. Ničković, "An algebraic framework for runtime verification," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 11, 2018.

[17] K. Mamouras, A. Chattopadhyay, and Z. Wang, "Algebraic quantitative semantics for efficient online temporal monitoring," in *Tools and Algorithms for the Construction and Analysis of Systems*, 2021, pp. 330–348.

[18] ——, "A compositional framework for quantitative online monitoring over continuous-time signals," in *Runtime Verification*, 2021.