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 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, general systematic requirements for soundness, parameterized by unary functions $\rho$. An STL formula $\phi$ is given by:

\[ \phi, \sigma, t \]

where $\phi$ is defined as

\[ \rho^+ (\phi, \sigma, t) = +\infty \quad \rho^- (\phi, \sigma, t) = 0 \]

\[ \rho^+ (I(\sigma) \geq 0, \sigma, t) = \rho^- (I(\sigma) > 0, \sigma, t) = \max(0, I(\sigma[t])) \]

\[ \rho^+ (I(\sigma) \geq 0, \sigma, t) = \rho^- (I(\sigma) > 0, \sigma, t) = \min(0, I(\sigma[t])) \]

\[ \rho^+ (\neg \phi, \sigma, t) = -\rho^- (\phi, \sigma, t) \]

\[ \rho^+ (\phi \land \psi, \sigma, t) = \min(\rho^+ (\phi, \sigma, t), \rho^+ (\psi, \sigma, t)) \]

\[ \rho^- (\phi \land \psi, \sigma, t) = \min(\rho^- (\phi, \sigma, t), \rho^- (\psi, \sigma, t)) \]

\[ \rho^+ (\psi U \phi, \sigma, t) = \max \left\{ \min\left(\rho^+ (\phi, \sigma, t) + t', \min_{t' \leq t} \rho^+ (\psi, \sigma, t') \right) \right\} \]

\[ \rho^- (\psi U \phi, \sigma, t) = \max \left\{ \min\left(\rho^- (\phi, \sigma, t) + t', \min_{t' \leq t} \rho^- (\psi, \sigma, t') \right) \right\} \]

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

Theorem 1: If $\rho_0 (\phi, \sigma, t) > 0$ then $\sigma^t \models \phi$, and if $\rho_0 (\phi, \sigma, t) < 0$ then $\sigma^t \not\models \phi$.

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 $\nu : \mathbb{R} \to \mathbb{R}_+$ and $\mu : \mathbb{R} \to \mathbb{R}_-$, binary integrators $\alpha, \beta, \zeta, \eta : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$, as well as time integrators $\Gamma, \Delta, \Theta, \Xi : \mathbb{I} \times (I \to \mathbb{R}_+) \to \mathbb{R}_+$. Using those operators, we can define a generic $\rho (\phi, \sigma, t) = \rho^+ (\phi, \sigma, t) + \rho^- (\phi, \sigma, t)$ with:

\[ \rho^+ (\Gamma, \sigma, t) = +\infty \quad \rho^- (\Gamma, \sigma, t) = 0 \]

\[ \rho^+ (I(\sigma) \geq 0, \sigma, t) = \rho^- (I(\sigma) > 0, \sigma, t) = \nu(I(\sigma[t])) \]

\[ \rho^+ (I(\sigma) \geq 0, \sigma, t) = \rho^- (I(\sigma) > 0, \sigma, t) = \mu(I(\sigma[t])) \]

\[ \rho^+ (\neg \phi, \sigma, t) = -\rho^- (\phi, \sigma, t) \]

\[ \rho^+ (\phi \land \psi, \sigma, t) = \alpha(\rho^+ (\phi, \sigma, t), \rho^+ (\psi, \sigma, t)) \]

\[ \rho^- (\phi \land \psi, \sigma, t) = -\beta(\rho^- (\phi, \sigma, t), -\rho^- (\psi, \sigma, t)) \]

\[ \rho^+ (\psi U \phi, \sigma, t) = \Gamma \sum_{t' \leq t} (\rho^+ (\phi, \sigma, t') + \rho^- (\psi, \sigma, t')) \]

\[ \rho^- (\psi U \phi, \sigma, t) = -\Theta \sum_{t' \leq t} (\rho^- (\phi, \sigma, t') + \rho^- (\psi, \sigma, t')) \]

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

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

- Haghhighi 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 $\nu$: $\max(\cdot, 0)$.
2) If $\mu(x) < 0$ then $x < 0$. Examples of possible $\mu$: $\min(\cdot, 0)$.
TABLE I: Number of iterations until falsification

<table>
<thead>
<tr>
<th></th>
<th>Max</th>
<th>Add</th>
<th>MARV</th>
<th>Const</th>
<th>TeLEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFC</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>autotrans_01</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Proj</td>
<td>26</td>
<td>26</td>
<td>49</td>
<td>127</td>
<td>350</td>
</tr>
<tr>
<td>Path</td>
<td>55</td>
<td>63</td>
<td>56</td>
<td>178</td>
<td>358</td>
</tr>
</tbody>
</table>

3) If \( x \geq 0 \) and \( y \geq 0 \) and \( \alpha(x, y) > 0 \), then \( x > 0 \) and \( y > 0 \).
4) If \( x \geq 0 \) and \( y \geq 0 \) and \( \beta(x, y) > 0 \), then \( x > 0 \) or \( y > 0 \).
5) If all \( \alpha_k \geq 0 \) and \( \sum \alpha_k \) > 0, then \( \exists k, \alpha_k > 0 \).
6) If all \( \alpha_k \geq 0 \) and \( \Delta_k \alpha_k > 0 \), then \( \forall k, \alpha_k > 0 \).
7) \( \alpha \) follows the requirements of \( \alpha \), and \( \eta \) the ones of \( \beta \).
8) \( \Theta \) follows the requirements of \( \Delta \), and \( \Pi \) the ones of \( \Gamma \).

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 \( \nu(\cdot) = \max(100(\sgn(\cdot)), 0) \). 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