October 2007

Robust Sampling for MITL Specifications

Georgios E. Fainekos
University of Pennsylvania

George J. Pappas
University of Pennsylvania, pappasg@seas.upenn.edu

Postprint version. Published in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Volume 4763, Formal Modeling and Analysis of Timed Systems - 5th International Conference, FORMATS 2007, Proceedings, October 2007, pages 147-162.

Robust Sampling for MITL Specifications

Abstract

Real-time temporal logic reasoning about trajectories of physical systems necessitates models of time which are continuous. However, discrete time temporal logic reasoning is computationally more efficient than continuous time. Moreover, in a number of engineering applications only discrete time models are available for analysis. In this paper, we introduce a framework for testing MITL specifications on continuous time signals using only discrete time analysis. The motivating idea behind our approach is that if the dynamics of the signal fulfills certain conditions and the discrete time signal robustly satisfies the MITL specification, then the corresponding continuous time signal should also satisfy the same MITL specification.

Comments

Postprint version. Published in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Volume 4763, Formal Modeling and Analysis of Timed Systems - 5th International Conference, FORMATS 2007, Proceedings, October 2007, pages 147-162.

Robust Sampling for MITL Specifications

Georgios E. Fainekos and George J. Pappas

School of Engineering and Applied Science, University of Pennsylvania
{fainekos,pappasg}@seas.upenn.edu

Abstract. Real-time temporal logic reasoning about trajectories of physical systems necessitates models of time which are continuous. However, discrete time temporal logic reasoning is computationally more efficient than continuous time. Moreover, in a number of engineering applications only discrete time models are available for analysis. In this paper, we introduce a framework for testing MITL specifications on continuous time signals using only discrete time analysis. The motivating idea behind our approach is that if the dynamics of the signal fulfills certain conditions and the discrete time signal robustly satisfies the MITL specification, then the corresponding continuous time signal should also satisfy the same MITL specification.

1 Introduction

Assume that we would like to test the transient response of an electronic circuit to a predetermined input signal. Since analytical solutions exist only for a few simple cases, the design, verification and validation of such systems still relies heavily on testing the actual circuit or, more commonly, on simulations [1]. In either case, we end up with a discrete time (or sampled) representation of the continuous time signal that we have to analyze. On the other hand, the properties of the system that we would like to verify are – in most of the cases – with respect to the continuous time behavior of the system.

In particular, properties like overshoot, rise time, delay time, settling time and other constraints on the output signal [2] can be very naturally captured using Metric Temporal Logic (MTL) with continuous time semantics [3]. A restricted version of MTL, namely the Metric Interval Temporal Logic (MITL) [4], has been shown to be decidable over continuous time models even without the finite variability assumption [5]. Recent advances on the monitoring [6] and on the synthesis of timed automata from MITL formulas [7] make possible the verification of real-time properties over continuous time models, however as mentioned earlier, such a representation is hard to be obtained for systems with complex dynamics [8].

Therefore, we must resort to approaches that test MTL specifications on timed words, i.e., sequences of states paired with their respective time stamps. Such testing methodologies are mainly based on formula rewriting methods [9] or monitors generated from automata [10, 11]. But then, one major issue is immediately apparent. The continuous time signals and their corresponding sampled versions do not necessarily satisfy the same MTL formula ϕ.

In this paper, we derive conditions on the dynamics of the signal and on the sampling function such that MITL reasoning over timed words can be applied to continuous time signals. The main machinery that we employ for this purpose is the computation of the robustness estimate [12] of a sampled signal with respect to an MITL specification ϕ. In this framework, the atomic propositions in a formula label regions in the value space of the signal. Intuitively, the robustness estimate is the minimum distance of a point of the sampled signal to such a region, which if it was to be entered by the sampled signal, the truth value of ϕ would change. Hence, all we need to do is to guarantee that the dynamics of the signal are such that between any two sampled points the actual continuous time signal does not violate the aforementioned distance. The constraints on the sampling function play another role. They guarantee that there exist enough sampling points such that the validity of MITL formulas is maintained between the two different semantics [13].

Our theoretical results are demonstrated through some examples that indicate the range of systems that the method can be applied to. Even though our analysis holds for signals of infinite duration, we focus our attention to signals of finite duration. This is so, because the analysis of the asymptotic properties of physical systems is a mature research area [8], while the analysis of the transient properties has not received much attention.

2 Temporal Logics and Continuous Time Signals

In this section, we define signals over metric spaces and provide a brief overview of the temporal logics that are interpreted over linear time structures. Let $\mathbb{R}$ be the set of real numbers and $\mathbb{N}$ the set of natural numbers. We denote the extended real number line by $\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$. In addition, we use pseudo-arithmetic expressions to represent certain subsets of the aforementioned sets. For example, $\mathbb{R}_{\geq 0}$ denotes the subset of the reals whose elements are greater or equal to zero. We let $\mathbb{B} = \{\bot, \top\}$, where $\top$ and $\bot$ are the symbols for the boolean constants *true* and *false* respectively. Given two sets A, B, let B^A define the set of all functions from A to B. That is, for any $f \in B^A$ we have $f : A \to B$. Finally, given a set A, $\mathcal{P}(A)$ denotes its powerset.

2.1 Continuous Time Signals in Metric Spaces

In this paper, we use continuous time signals in order to capture the behavior of real-time or physical systems. For example, the temperature in a room is a signal whose domain is $\mathbb{R}_{\geq 0}$ and its range is $\mathbb{R}$ (which hopefully stays in the $[20, 25]$ Celsius degree range). Considering real-valued signals instead of just Boolean values allows us to reason about how far are two points in that space. For example, a temperature of 25°C is closer to the temperature of 30°C than to 40°C.

Formally, a continuous time *signal* s is a map $s : R \to X$ such that R is the time domain and X is a metric space. When we consider bounded time signals,

as for example in testing algorithms, then $R = [0, r] \subseteq \mathbb{R}_{\geq 0}$ with $r > 0$, otherwise we let $R = \mathbb{R}_{\geq 0}$. In the following, $\mathfrak{S}$ denotes the set of all possible signals, i.e., $\mathfrak{S} = X^R$. We fix R to refer to a time domain as described above. A metric space is a pair (X, d) such that the topology of the set X is induced by a metric d. In this paper, we only use the notions of metric and neighborhood which we define below.

Definition 1 (Metric) *A metric on a set X is a positive function $d : X \times X \to \mathbb{R}_{\geq 0}$, such that the three following properties hold*

1. $\forall x_1, x_2 \in X.\ d(x_1, x_2) = 0 \Leftrightarrow x_1 = x_2$
2. $\forall x_1, x_2 \in X.\ d(x_1, x_2) = d(x_2, x_1)$
3. $\forall x_1, x_2, x_3 \in X.\ d(x_1, x_3) \leq d(x_1, x_2) + d(x_2, x_3)$

Using a metric d, we can define the distance of a point $x \in X$ from a set $S \subseteq X$. Intuitively, this distance is the shortest distance from x to all the points in S. In a similar way, the depth of a point x in a set S is defined to be the shortest distance of x from the boundary of S.

Definition 2 (Distance, Depth [14] §8) *Let $x \in X$ be a point, $S \subseteq X$ be a set and d be a metric on X. Then, we define the*

- *Distance from x to S to be* $\mathbf{dist}_d(x, S) := \inf\{d(x, y) \mid y \in S\}$
- *Depth of x in S to be* $\mathbf{depth}_d(x, S) := \mathbf{dist}_d(x, X \backslash S)$

We should point out that we use the extended definition of supremum and infimum. In other words, the supremum of the empty set is defined to be bottom element of the domain, while the infimum of the empty set is defined to be the top element of the domain. For example, when we reason over $\overline{\mathbb{R}}$, then $\sup \emptyset := -\infty$ and $\inf \emptyset := +\infty$. Also of importance is the notion of an open ball of radius ε centered at a point $x \in X$.

Definition 3 (ε-Ball) *Given a metric d, a radius $\varepsilon > 0$ and a point $x \in X$, the open ε-ball centered at x is defined as $B_d(x, \varepsilon) = \{y \in X \mid d(x, y) < \varepsilon\}$.*

It is easy to verify that if the distance ($\mathbf{dist}_d$) of a point x from a set S is $\varepsilon > 0$, then $B_d(x, \varepsilon) \cap S = \emptyset$. And similarly, if $\mathbf{depth}_d(x, S) = \varepsilon > 0$, then $B_d(x, \varepsilon) \subseteq S$.

2.2 Metric Interval Temporal Logic over Signals

The Metric Temporal Logic (MTL) was introduced in [3] in order to reason about the quantitative timing properties of boolean signals. A decidable, but restricted version of MTL, namely the Metric Interval Temporal Logic (MITL), was presented in [4]. In this section, we review the basics of the propositional MITL over signals.

Definition 4 (Syntax of MITL in Negation Normal Form) *Let $\mathbb{C}$ be the set of truth degree constants, AP be the set of atomic propositions and $\mathcal{I}$ be a non-empty non-singular interval of R. The set $\Phi_{\mathbb{C}}$ of all well-formed formulas (wff) is inductively defined using the following rules:*

- *Terms: All constants $c \in \mathbb{C}$ and propositions p, $\neg p$ for $p \in AP$ are terms.*
- *Formulas: if ϕ_1 and ϕ_2 are terms or formulas, then $\phi_1 \vee \phi_2$, $\phi_1 \wedge \phi_2$, $\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$ and $\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$ are formulas.*

The atomic propositions in our case label subsets of the set X. In other words, we define an observation map $\mathcal{O} : AP \to \mathcal{P}(X)$ such that for each $p \in AP$ the corresponding set is $\mathcal{O}(p) \subseteq X$. In the above definition, $\mathcal{U}_{\mathcal{I}}$ is the timed *until* operator and $\mathcal{R}_{\mathcal{I}}$ the timed *release* operator. The subscript $\mathcal{I}$ imposes timing constraints on the temporal operators. The interval $\mathcal{I}$ can be open, half-open or closed, bounded or unbounded, but it must be non-empty ($\mathcal{I} \neq \emptyset$) and non-singular ($\mathcal{I} \neq \{t\}$) in order to be in spirit with the definitions in [4]. Moreover, we define the following operations on the timing constraints $\mathcal{I}$ of the temporal operators:

$$t + \mathcal{I} := \{t + t' \mid t' \in \mathcal{I}\} \quad \text{and} \quad t +_R \mathcal{I} := (t + \mathcal{I}) \cap R$$

for any t in R. Sometimes for clarity in the presentation, we replace $\mathcal{I}$ with pseudometric expressions, e.g. $\mathcal{U}_{[0,1]}$ is written as $\mathcal{U}_{\leq 1}$. In the case where $\mathcal{I} = [0, +\infty)$, we remove the subscript $\mathcal{I}$ from the temporal operators, i.e., we just write $\mathcal{U}$, and $\mathcal{R}$.

Metric Interval Temporal Logic (MITL) formulas are interpreted over signals s. In this paper, we define the boolean semantics of MITL formulas using a valuation function $\langle\!\langle \cdot, \cdot \rangle\!\rangle : \Phi_{\mathbb{B}} \times \mathcal{P}(X)^{AP} \to (\mathfrak{S} \times R \to \mathbb{B})$ and we write $\langle\!\langle \phi, \mathcal{O} \rangle\!\rangle(s, t) = \top$ instead of the usual notation $(\mathcal{O}^{-1} \circ s, t) \models \phi$. In this case, we say that the signal s under observation map $\mathcal{O}$ satisfies the formula ϕ at time t. Here, $\circ$ denotes function composition : $(f \circ g)(t) = f(g(t))$ and $\mathcal{O}^{-1} : X \to \mathcal{P}(AP)$ is defined as $\mathcal{O}^{-1}(x) := \{p \in AP \mid x \in \mathcal{O}(p)\}$ for $x \in X$. For brevity, we drop $\mathcal{O}$ from the notation since without loss of generality we can consider it constant throughout this paper. From an application perspective, we are interested in checking whether $\langle\!\langle \phi \rangle\!\rangle(s, 0) = \top$. In this case, we refer to s as a *model* of ϕ and we just write $\langle\!\langle \phi \rangle\!\rangle(s) = \top$ for brevity.

Before proceeding to the actual definition of the semantics, we introduce some auxiliary notation. If $(\mathbb{V}, <)$ is a totally ordered set, then we define the binary operators $\sqcup : \mathbb{V} \times \mathbb{V} \to \mathbb{V}$ and $\sqcap : \mathbb{V} \times \mathbb{V} \to \mathbb{V}$ using the supremum and infimum functions as $x \sqcup y := \sup\{x, y\}$ and $x \sqcap y := \inf\{x, y\}$. Also, for any $V \subseteq \mathbb{V}$ we extend the above definitions as follows $\bigsqcup V := \sup V$ and $\bigsqcap V := \inf V$. Again, we use the extended definition of the supremum and infimum, i.e., $\sup \emptyset := \bot$ and $\inf \emptyset := \top$. Recall that if $(\mathbb{V}, \leq)$ is a totally ordered set, then it is *distributive*, i.e., for all $a, b, c \in \mathbb{S}$ it is $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$ and $a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$. Note that the structure $(\mathbb{B}, <)$ is a totally ordered set with $\bot < \top$ and that $(\mathbb{B}, \sqcap, \sqcup, \neg)$ is a boolean algebra with the complementation defined as $\neg\top = \bot$ and $\neg\bot = \top$.

Definition 5 (CT Semantics of MITL) *Let $s \in \mathfrak{S}$, $\mathcal{O} \in \mathcal{P}(X)^{AP}$ and $t, t', t'' \in R$, then the continuous time semantics of any formula $\phi \in \Phi_{\mathbb{B}}$ is defined by*

$$\langle\!\langle \top \rangle\!\rangle(s,t) := \top \qquad \langle\!\langle \bot \rangle\!\rangle(s,t) := \bot$$
$$\langle\!\langle p \rangle\!\rangle(s,t) := K_{\in}(s(t), \mathcal{O}(p)) \qquad \langle\!\langle \neg p \rangle\!\rangle(s,t) := K_{\in}(s(t), X \backslash \mathcal{O}(p))$$
$$\langle\!\langle \phi_1 \vee \phi_2 \rangle\!\rangle(s,t) := \langle\!\langle \phi_1 \rangle\!\rangle(s,t) \sqcup \langle\!\langle \phi_2 \rangle\!\rangle(s,t)$$
$$\langle\!\langle \phi_1 \wedge \phi_2 \rangle\!\rangle(s,t) := \langle\!\langle \phi_1 \rangle\!\rangle(s,t) \sqcap \langle\!\langle \phi_2 \rangle\!\rangle(s,t)$$
$$\langle\!\langle \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2 \rangle\!\rangle(s,t) := \bigsqcup_{t' \in (t +_R \mathcal{I})} \left(\langle\!\langle \phi_2 \rangle\!\rangle(s,t') \sqcap \bigsqcap_{t \leq t'' < t'} \langle\!\langle \phi_1 \rangle\!\rangle(s,t'') \right)$$
$$\langle\!\langle \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2 \rangle\!\rangle(s,t) := \bigsqcap_{t' \in (t +_R \mathcal{I})} \left(\langle\!\langle \phi_2 \rangle\!\rangle(s,t') \sqcup \bigsqcup_{t \leq t'' < t'} \langle\!\langle \phi_1 \rangle\!\rangle(s,t'') \right)$$

In the above definition, $K_{\in}$ is the characteristic function of the $\in$ relation, i.e., $K_{\in}(a, A) = \top$ if $a \in A$ and $\bot$ otherwise. Informally, the formula $\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$ expresses the property that over the signal s there exists some time in the interval $\mathcal{I}$ that makes ϕ_2 true and, furthermore, for all previous times s satisfies ϕ_1. Intuitively, the release operator $\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$ states that ϕ_2 should always hold during the time interval $\mathcal{I}$, a requirement which is released when ϕ_1 becomes true. We can also define the temporal operators *eventually* $\Diamond_{\mathcal{I}} \phi = \top \mathcal{U}_{\mathcal{I}} \phi$ and *always* $\Box_{\mathcal{I}} \phi = \bot \mathcal{R}_{\mathcal{I}} \phi$.

3 Temporal Logics and Discrete Time Signals

Even though MITL is decidable over continuous time Boolean signals [5], there do not exist efficient decision procedures as it is the case for the discrete untimed systems [15]. Matters become even worse when we consider hybrid systems with real time requirements and states that evolve in metric spaces. For such systems, a discrete time representation of their continuous time behavior can provide a valuable tool for analysis.

3.1 Sampled Signals

A sampled (or discrete time) signal can represent computer simulated trajectories of physical models or the sampling process that takes place when we digitally monitor physical systems. In the following, we assume that a continuous time signal s is a mathematical object that represents the behavior of a physical system and we define a *sampling function* $\tau \in R^N$ which returns the point in time at which the i-th sample was taken. The set of all sampling functions is denoted by $\mathfrak{T}$, i.e., $\mathfrak{T} = R^N$. We fix $N \subseteq \mathbb{N}$ to be the set indexes for the sampled points. In other words, the discrete time signal $\hat{s} = s \circ \tau$ corresponds to the observable (discretized) behavior of the physical system (see Fig. 1). Two necessary assumptions on any sampling function are : (i) τ must be a monotonic function, i.e., $\tau(i) < \tau(j)$ for $i < j$ and (ii) if R is unbounded then $N = \mathbb{N}$. Notice that the pair $(\mathcal{O}^{-1} \circ \hat{s}, \tau)$ is actually a *timed state sequence*, which is a widely accepted model for reasoning about real time systems [16].

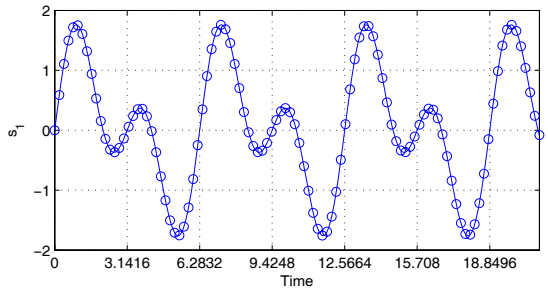

Fig. 1. A continuous time signal $s_1(t) = \sin t + \sin 2t$ (*solid line*) and the corresponding sampled signal $\hat{s}_1$ (*circles*) generated using a constant sampling step of 0.2.

3.2 Metric Interval Temporal Logic over Sampled Signals

We proceed on to define MITL semantics over discrete time signals. Here, we slightly deviate from the usual definition of the semantics over timed state sequences. We consider as a model of ϕ the actual continuous time signal s under the sampling function τ. This will enable us to reason about all the continuous time signals which have the same sampled representation in a transparent way. Again, the MITL semantics is defined using a valuation function which now also depends on the sampling function $\tau \in \mathfrak{T}$. We write $\langle\!\langle \phi \rangle\!\rangle_\tau(s,i) = \top$ when the signal s under sampling function τ satisfies the formula ϕ at sample i (as before, the observation map $\mathcal{O}$ is implied). Similarly to the continuous time case, when $i = 0$ and the formula evaluates to $\top$, then we refer to s as a *model* of ϕ under the sampling function τ and we write $\langle\!\langle \phi \rangle\!\rangle_\tau(s) = \top$. In the definition below, we also use the following notation : for $Q \subseteq R$, the *preimage* of Q under τ is defined as : $\tau^{-1}(Q) := \{i \in N \mid \tau(i) \in Q\}$. Notice that $N = \tau^{-1}(R)$.

Definition 6 (DT Semantics of MITL) *Let $s \in \mathfrak{S}$, $\tau \in \mathfrak{T}$, $\mathcal{O} \in \mathcal{P}(X)^{AP}$ and $i, j, k \in N$, then the discrete time semantics of any formula $\phi \in \Phi_{\mathbb{B}}$ is defined by*

$$
\begin{aligned}
\langle\!\langle \top \rangle\!\rangle_\tau(s,i) &:= \top & \langle\!\langle \bot \rangle\!\rangle_\tau(s,i) &:= \bot \\
\langle\!\langle p \rangle\!\rangle_\tau(s,i) &:= K_\in(\hat{s}(i), \mathcal{O}(p)) & \langle\!\langle \neg p \rangle\!\rangle_\tau(s,i) &:= K_\in(\hat{s}(i), X \backslash \mathcal{O}(p)) \\
\langle\!\langle \phi_1 \vee \phi_2 \rangle\!\rangle_\tau(s,i) &:= \langle\!\langle \phi_1 \rangle\!\rangle_\tau(s,i) \sqcup \langle\!\langle \phi_2 \rangle\!\rangle_\tau(s,i) \\
\langle\!\langle \phi_1 \wedge \phi_2 \rangle\!\rangle_\tau(s,i) &:= \langle\!\langle \phi_1 \rangle\!\rangle_\tau(s,i) \sqcap \langle\!\langle \phi_2 \rangle\!\rangle_\tau(s,i) \\
\langle\!\langle \phi_1 \mathcal{U}_\mathcal{I} \phi_2 \rangle\!\rangle_\tau(s,i) &:= \bigsqcup_{j \in \tau^{-1}(\tau(i) +_R \mathcal{I})} \Big(\langle\!\langle \phi_2 \rangle\!\rangle_\tau(s,j) \sqcap \bigsqcap_{i \le k < j} \langle\!\langle \phi_1 \rangle\!\rangle_\tau(s,k) \Big) \\
\langle\!\langle \phi_1 \mathcal{R}_\mathcal{I} \phi_2 \rangle\!\rangle_\tau(s,i) &:= \bigsqcap_{j \in \tau^{-1}(\tau(i) +_R \mathcal{I})} \Big(\langle\!\langle \phi_2 \rangle\!\rangle_\tau(s,j) \sqcup \bigsqcup_{i \le k < j} \langle\!\langle \phi_1 \rangle\!\rangle_\tau(s,k) \Big)
\end{aligned}
$$

4 Robustness Estimate

The main goal of this paper is to derive conditions that guarantee that a signal is a model of an MITL formula with continuous time semantics using only discrete time reasoning. The main tool that we employ in order to achieve this goal is the *robustness estimate* [12]. In [12], the robustness estimate was used in order to determine neighborhoods of finite timed state sequences that satisfy the same MTL specification. In this paper, the robustness estimate will help us determine a critical distance-threshold that guarantees that a signal satisfies an MITL formula with continuous time semantics.

The robustness estimate can be computed by introducing multi-valued semantics for MITL formulas. In this paper, we differentiate from previous works – see for example [17] – by providing the definition of multi-valued semantics for MITL based on robustness considerations. Let $\mathfrak{R} = (\overline{\mathbb{R}}, \leq)$ be the real line with the usual ordering relation. We propose multi-valued semantics for the Metric Interval Temporal Logic where the valuation function on the predicates takes values over the totally ordered set $\mathfrak{R}$ according to the metric d operating on the state space X of the signal s. For this purpose, we let the valuation function be the depth (or the distance) of the current point of the signal $s \circ \tau(i)$ in a set $\mathcal{O}(p)$ labeled by the atomic proposition p. Intuitively, this distance represents how robustly is the point $s \circ \tau(i)$ within a set $\mathcal{O}(p)$. If this metric is zero, then even the smallest perturbation of the point can drive it inside or outside the set $\mathcal{O}(p)$, dramatically affecting membership.

For the purposes of the following discussion, we use the notation $[\![\phi]\!]$ to denote the robustness estimate with which the signal s satisfies the specification ϕ under the sampling function τ (formally, $[\![\phi]\!]_\tau : \mathfrak{S} \times N \to \overline{\mathbb{R}}$ and, again, the observation map $\mathcal{O}$ is implied).

Definition 7 (Robustness Estimate) *Let $s \in \mathfrak{S}$, $\tau \in \mathfrak{T}$, $c \in \overline{\mathbb{R}}$, $\mathcal{O} \in \mathcal{P}(X)^{AP}$ and $i, j, k \in N$, then the robustness estimate of any formula $\phi \in \Phi_{\mathbb{R}\cup\mathbb{B}}$ with respect to s under the sampling function τ is recursively defined as follows*

$$
\begin{aligned}
[\![\top]\!]_\tau(s,i) &:= +\infty & [\![\bot]\!]_\tau(s,i) &:= -\infty \\
[\![p]\!]_\tau(s,i) &:= \mathbf{depth}_d(\hat{s}(i), \mathcal{O}(p)) & [\![\neg p]\!]_\tau(s,i) &:= \mathbf{dist}_d(\hat{s}(i), \mathcal{O}(p)) \\
[\![c]\!]_\tau(s,i) &:= c \\
[\![\phi_1 \vee \phi_2]\!]_\tau(s,i) &:= [\![\phi_1]\!]_\tau(s,i) \sqcup [\![\phi_2]\!]_\tau(s,i) \\
[\![\phi_1 \wedge \phi_2]\!]_\tau(s,i) &:= [\![\phi_1]\!]_\tau(s,i) \sqcap [\![\phi_2]\!]_\tau(s,i) \\
[\![\phi_1 \mathcal{U}_\mathcal{I} \phi_2]\!]_\tau(s,i) &:= \bigsqcup_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_\tau(s,j) \sqcap \bigsqcap_{i \leq k < j} [\![\phi_1]\!]_\tau(s,k) \Big) \\
[\![\phi_1 \mathcal{R}_\mathcal{I} \phi_2]\!]_\tau(s,i) &:= \bigsqcap_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_\tau(s,j) \sqcup \bigsqcup_{i \leq k < j} [\![\phi_1]\!]_\tau(s,k) \Big)
\end{aligned}
$$

It is easy to verify that the semantics of the negation operator give us all the usual nice properties such as the *De Morgan laws*: $a \sqcup b = -(-a \sqcap -b)$ and

$a \sqcap b = -(-a \sqcup -b)$, *involution*: $-(-a) = a$ and *antisymmetry*: $a \leq b$ iff $-a \geq -b$ for $a, b \in \overline{\mathbb{R}}$.

5 Continuous Time Satisfiability by Discrete Reasoning

To this point one question remains unanswered. What is the relationship between $\langle\langle\phi\rangle\rangle(s)$ and $\langle\langle\phi\rangle\rangle_\tau(s)$ for a given MITL formula ϕ, signal s and sampling function τ? This is an important question since a sampling function τ may not just change the satisfiability of a formula ϕ with respect to a signal s, but also the validity of the formula [13]. In this section, we develop conditions for the signals in the set $\mathfrak{S}$ and the sampling function τ which can guarantee the equality $\langle\langle\phi\rangle\rangle_\tau(s) = \langle\langle\phi\rangle\rangle(s)$. In the following, we introduce a sequence of assumptions.

First, we need to derive conservative bounds on the divergence of the value of signal s between two consecutive samples i and $i+1$. We do that by requiring that the state distance between any two points in time is bounded by a positive nondecreasing function $\mathcal{E}$ which depends only on the time difference between these two points.

Assumption 1 *The signals in the set $\mathfrak{S}$ satisfy the following condition:*

$$\forall t, t' \in R \,.\, d(s(t), s(t')) \leq \mathcal{E}(|t - t'|), \tag{1}$$

where $\mathcal{E}$ is a positive nondecreasing function.

Such bounds can be easily derived when a signal is Lipschitz continuous.

Definition 8 (Lipschitz Continuity) *Let (X, d) and (X', d') be two metric spaces. A function $f : X' \to X$ is called Lipschitz continuous if there exists a constant $L_f \geq 0$ such that:*

$$\forall x'_1, x'_2 \in X'.d(f(x'_1), f(x'_2)) \leq L_f d'(x'_1, x'_2). \tag{2}$$

The smallest constant L_f is called Lipschitz constant of the function f.

What we are actually interested in is Lipschitz continuity of a signal s with respect to time:

$$\forall t, t' \in R \,.\, d(s(t), s(t')) \leq L_s|t - t'|. \tag{3}$$

Any signal with bounded time derivative satisfies the above condition. Whenever only a number of values of the signal are available to us, instead of an analytical description, we can use methods from optimization theory in order to estimate a Lipschitz constant for the signal [18]. Moreover, if the signal s is the solution of an ordinary differential equation $\dot{s}(t) = f(s(t))$, where f is Lipschitz continuous with constant L_f, then it is possible to estimate a constant L_s for eq. (3).

Example 1 *Consider an autonomous linear system $\dot{s}(t) = As(t)$, where A is Hurwitz. Then, $\|\dot{s}(t)\| = \|As(t)\| \leq \|A\|\|s(t)\|$, where $\|\cdot\|$ is the Euclidean norm. Consider the customary Lyapunov function for stable linear systems $V(x) =$*

$x^T Px$, where P is a symmetric and positive definite matrix [8]. It is easy to see that the Lyapunov level sets $\{x \in X \mid V(x) \leq c\}$ are ellipsoids. Recall that any signal which crosses the surface of such a set always remains in the set. Therefore, the distance of $s(t)$ from the origin is always bounded by the radius of the minimum ball that contains the ellipsoid $\{x \in X \mid x^T Px \leq s(0)^T Ps(0)\}$. The matrix P determines the shape of the ellipsoids and it can be computed by solving the Lyapunov equation : $PA + A^T P + I = 0$. The lengths of the axis of the ellipsoid are given by the square roots of the eigenvalues of the matrix $P_e = V(s(0))P^{-1}$ [14]. Let $\lambda_{\max}(P_e)$ be the maximum eigenvalue of P_e, then $\|s(t)\| \leq \sqrt{\lambda_{\max}(P_e)}$ for all $t \in R$. Hence, $\|\dot{s}(t)\| \leq \|A\|\sqrt{\lambda_{\max}(P_e)}$ and the Lipschitz constant is $L_s = \|A\|\sqrt{\lambda_{\max}(P_e)}$. In this case, the Lipschitz constant depends on the initial condition $s(0)$. □

Notice that the bound on the distance between two values of the signal depends on the sampling function τ. In particular, one parameter of the sampling function that we might wish to control is the *maximum sampling step*:

$$\Delta\tau = \sup_{i \in N_{>0}} \{\tau(i) - \tau(i-1)\}. \tag{4}$$

The sampling function τ, i.e., the maximum sampling step $\Delta\tau$, must be such that the relationship between valid formulas in continuous and sampled semantics is maintained [13]. For example, it is easy to see that the formula $\Box_{[1,2]}p$ is true for any signal s if there is no sample in the interval $[1, 2]$. In order to avoid such situations, we must impose certain constraints to $\Delta\tau$. But first, a slight modification of the timing constraints of the temporal operators is required.

Similarly to [19], we strengthen MITL formulas by changing the timing requirements of a given formula ϕ. In detail, we introduce a function $\mathcal{H} : \Phi_{\mathbb{B}} \to \Phi_{\mathbb{B}}$ that recursively operates on a formula ϕ and strengthens the timing constraints as follows:

$$\begin{array}{ll} \mathcal{H}(p) = p & \mathcal{H}(\neg p) = \neg p \\ \mathcal{H}(\phi_1 \vee \phi_2) = \mathcal{H}(\phi_1) \vee \mathcal{H}(\phi_2) & \mathcal{H}(\phi_1 \wedge \phi_2) = \mathcal{H}(\phi_1) \wedge \mathcal{H}(\phi_2) \\ \mathcal{H}(\phi_1 \,\mathcal{U}_{\mathcal{I}} \phi_2) = \mathcal{H}(\phi_1)\,\mathcal{U}_{C(\mathcal{I},\Delta\tau)}\mathcal{H}(\phi_2) & \mathcal{H}(\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2) = \mathcal{H}(\phi_1)\mathcal{R}_{E(\mathcal{I},\Delta\tau)}\mathcal{H}(\phi_2) \end{array}$$

where $C(\mathcal{I}, \delta) = \{r \in R \mid cl(B_d(r, \delta)) \subseteq \mathcal{I}\}$ is the δ-contraction and $E(\mathcal{I}, \delta) = \{r \in R \mid cl(B_d(r, \delta)) \cap \mathcal{I} \neq \emptyset\}$ is the δ-expansion of the interval $\mathcal{I}$. Here, cl denotes the closure of a set. The intuition behind the function $\mathcal{H}$ is that a robust specification with respect to the atomic propositions must also be robust with respect to the timing constraints. The necessity of the robustification of the timing requirements will become apparent in the proof of Theorem 1. For example, in order to determine the Boolean truth value of ϕ_2 in $\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$ for the whole interval $\mathcal{I}$ in continuous time, we must also consider the first samples after and before the interval $\tau(i) +_R \mathcal{I}$.

Remark 1 *The authors in [19] have proven that for any $\phi \in \Phi_{\mathbb{B}}$, $s \in \mathfrak{S}$, $\tau \in \mathfrak{T}$ and $\mathcal{O} \in P(X)^{AP}$, $\langle\!\langle \mathcal{H}(\phi) \rangle\!\rangle_\tau(s, i) = \top$ implies $\langle\!\langle \phi \rangle\!\rangle_\tau(s, i) = \top$.*

Assumption 2 *The sampling functions in the set $\mathfrak{T}$ satisfy the constraint:*

$$\Delta\tau < \min_{\mathcal{I}\in(\mathfrak{I}_{\mathcal{H}(\phi)}\cup\mathfrak{I}_{\phi})} \{\sup\mathcal{I} - \inf\mathcal{I}\}. \tag{5}$$

When R is bounded, the sampling functions in the set $\mathfrak{T}$ must also satisfy the constraint : $\sup R - \tau(\max N) < \Delta\tau$.

In the assumption above, $\mathfrak{I}_{\phi}$ denotes the set of all the timing constraints $\mathcal{I}$ that appear in the temporal operators of an MITL formula ϕ. Notice that if there exists a singleton interval in the set $\mathfrak{I}_{\phi}$, then the above assumption cannot be satisfied. This observation justifies the choice of MITL as a specification language instead of MTL. It is easy to see that with respect to the initial formula ϕ, Assumption 2 can be satisfied by the following constraint:

$$\Delta\tau < 1/3 \min_{\mathcal{I}\in\mathfrak{I}_{\phi}} \{\sup\mathcal{I} - \inf\mathcal{I}\}. \tag{6}$$

Whenever R is a bounded time interval, we have to impose additional constraints on the signal and the MITL formulas. First, we require that all the intervals in $\mathfrak{I}_{\phi}$ are bounded as it was initially suggested in [6]. This enables us to compute a minimum time $\mathcal{D}(\phi)$ that guarantees in combination with Assumption 2 that there are no subformulas whose truth value was determined by the lack of sampling points. The computation of the minimum time $\mathcal{D}(\phi)$ is performed recursively:

$$\begin{array}{ll}
\mathcal{D}(p) := 0 & \mathcal{D}(\neg p) := 0 \\
\mathcal{D}(\phi_1 \vee \phi_2) := \mathcal{D}(\phi_1) \sqcup \mathcal{D}(\phi_2) & \mathcal{D}(\phi_1 \wedge \phi_2) := \mathcal{D}(\phi_1) \sqcup \mathcal{D}(\phi_2) \\
\mathcal{D}(\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2) := \sup\mathcal{I} + \mathcal{D}(\phi_1) \sqcup \mathcal{D}(\phi_2) & \mathcal{D}(\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2) := \sup\mathcal{I} + \mathcal{D}(\phi_1) \sqcup \mathcal{D}(\phi_2)
\end{array}$$

In particular, we would like to avoid the case where R is a bounded domain and $t + \mathcal{I} \not\subseteq R$. For the shake of example, consider the formula $\Box_{[3,4]}p$ and let the domain of the signal s be $R = [0, 2]$. Then, the formula $\Box_{[3,4]}p$ evaluates to $\top$ simply because $0 +_{[0,2]} [3, 4] = \emptyset$. In order to avert such situations, we must impose one additional constraint (when R is bounded). Namely, for a given formula ϕ and signal s we let $\mathcal{D}(\phi) < \sup R < +\infty$. In other words, both the domain of the signal and all the timing constraints in the formula are bounded from above and below. Now, assume that a temporal subformula $\psi = \psi_1 \mathcal{W}_{\mathcal{I}_k} \psi_2$ of ϕ is at a nesting depth k, where $\mathcal{W} \in \{\mathcal{U}, \mathcal{R}\}$, and let $\{\mathcal{I}_j\}_{j<k}$ be the timing constraints of the temporal operators at lower nesting depths. Informally, the nesting depth of a formula ϕ is defined to be the maximum number of nested temporal operators and it is computed in a similar way to $\mathcal{D}$ where $\sup\mathcal{I}$ is replaced by 1. Then, for all $t \in [0, \sum_{j<k} \sup\mathcal{I}_j]$ we have $t + \mathcal{I}_k \subseteq R$ since $\sum_{j\leq k} \sup\mathcal{I}_j \leq \mathcal{D}(\phi) < \sup R$. Therefore, $t + \mathcal{I}_k = t +_R \mathcal{I}_k$.

Assumption 3 *If the time domain R of the set of signals $\mathfrak{S}$ is bounded, i.e.,* $\sup R < +\infty$*, then for the MITL formula ϕ under consideration it must be* $\sup\mathcal{I} < +\infty$ *for all $\mathcal{I} \in \mathfrak{I}_{\phi}$ and, also,* $\sup R > \mathcal{D}(\mathcal{H}(\phi))$.

Lemma 1 *Consider a formula $\phi \in \Phi_{\mathbb{B}}$ and a sampling function $\tau \in \mathfrak{T}$ and let the Assumptions 2 and 3 hold. Let $\psi = \psi_1 \mathcal{W}_{\mathcal{I}_k} \psi_2$, where $\mathcal{W} \in \{\mathcal{U}, \mathcal{R}\}$, be a subformula of ϕ at nesting depth k and let $\{\mathcal{I}_j\}_{j<k}$ be the timing constraints of the temporal operators at lower nesting depths. If $I = \tau^{-1}(T) \neq \emptyset$, where $T = [0, \sum_{j<k} \sup \mathcal{I}_j]$, then for all $i \in I$ we have $\tau^{-1}(\tau(i) +_R \mathcal{I}_k) \neq \emptyset$.*

Proof. First note that, as mentioned above, by Assumption 3 the set $\tau(i) +_R \mathcal{I}_k$ is equal to $\tau(i) + \mathcal{I}_k$ and, hence, $\tau(i) +_R \mathcal{I}_k \neq \emptyset$. Now, assume that $I = \tau^{-1}(T) \neq \emptyset$. If both R and $\mathcal{I}_k$ are unbounded, then we immediately get $\tau^{-1}(\tau(i) + \mathcal{I}_k) \neq \emptyset$ for any $i \in I$ since otherwise $N = \tau^{-1}(R)$ would be finite. Assume now that $\mathcal{I}_k$ is bounded and that for some $i \in I$ we get that $\tau^{-1}(\tau(i) + \mathcal{I}_k) = \emptyset$. In other words, we assume that there does not exist $i' \geq i$ such that $\tau(i') \in \tau(i) + \mathcal{I}_k$. Then, the following may hold since $\tau(i) + \mathcal{I}_k$ is an interval of R:

1. for all $i' \in N_{\geq i}$ we have $\tau(i') \prec \inf(\tau(i) + \mathcal{I}_k)$, where $\prec \in \{<, \leq\}$ depending on the constraints of $\mathcal{I}_k$. Note that this can only be the case when R is bounded. Hence, we get that $\sup R - \tau(\max N) \succ \sup R - \inf(\tau(i) + \mathcal{I}_k) \geq \sup(\tau(i) + \mathcal{I}_k) - \inf(\tau(i) + \mathcal{I}_k) \geq \sup \mathcal{I}_k - \inf \mathcal{I}_k > \Delta\tau$, which a contradiction by Assumption 2.
2. there exists $i' \in N_{\geq i}$ such that $\tau(i') \prec \inf(\tau(i) + \mathcal{I}_k)$ and $\sup(\tau(i) + \mathcal{I}_k) \prec \tau(i' + 1)$, where $\prec \in \{<, \leq\}$ depending on the constraints of $\mathcal{I}_k$. That is, $\tau(i' + 1) - \tau(i') \succ \sup(\tau(i) + \mathcal{I}_k) - \inf(\tau(i) + \mathcal{I}_k) = \sup \mathcal{I}_k - \inf \mathcal{I}_k > \Delta\tau$, which is a contradiction by Assumption 2.

Since $\tau^{-1}(\tau(i) +_R \mathcal{I}_k) \neq \emptyset$, we also get that $\tau^{-1}([0, \sum_{j \leq k} \sup \mathcal{I}_j]) \neq \emptyset$. □

The above assumptions enable us to prove the following theorem which is the main result of this paper.

Theorem 1 *Consider $\phi \in \Phi_{\mathbb{B}}$, $\mathcal{O} \in \mathcal{P}(X)^{AP}$, $s \in \mathfrak{S}$, $\tau \in \mathfrak{T}$ and let Assumptions 1 to 3 hold. Then, $[\![\mathcal{H}(\phi)]\!]_\tau(s, i) > \mathcal{E}(\Delta\tau)$ implies*

$$\forall t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R \,.\, \langle\!\langle \phi \rangle\!\rangle(s, t) = \top \tag{7}$$

for any $i \in N$ which satisfies the conditions of Lemma 1.

Proof. The proof of the theorem is by induction on the structure of formula ϕ.

Case $\phi = p \in AP$: $[\![\mathcal{H}(p)]\!]_\tau(s, i) > \mathcal{E}(\Delta\tau)$, i.e., $\mathbf{depth}_d(\hat{s}(i), \mathcal{O}(p)) > \mathcal{E}(\Delta\tau)$. Therefore, $d(\hat{s}(i), x) > \mathcal{E}(\Delta\tau)$ for any $x \in X \backslash \mathcal{O}(p)$. Moreover by Assumption 1, we get that $d(\hat{s}(i), s(t)) \leq \mathcal{E}(\Delta\tau)$ for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$ and $d(\hat{s}(i), s(t)) \leq \mathcal{E}(\Delta\tau) < d(\hat{s}(i), x)$. Also, since d is a metric : $d(\hat{s}(i), x) \leq d(\hat{s}(i), s(t)) + d(s(t), x)$. Hence, $d(s(t), x) > 0$. Since this holds for any $x \in X \backslash \mathcal{O}(p)$, we conclude that $\mathbf{depth}_d(s(t), \mathcal{O}(p)) > 0$ or $s(t) \in \mathcal{O}(p)$ and, thus, $\langle\!\langle p \rangle\!\rangle(s, t) = \top$ for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$.

Case $\phi = \neg p \in AP$: $[\![\mathcal{H}(\neg p)]\!]_\tau(s, i) > \mathcal{E}(\Delta\tau)$, i.e., $\mathbf{dist}_d(\hat{s}(i), \mathcal{O}(p)) > \mathcal{E}(\Delta\tau)$. The proof is similar to the previous case.

Cases $\phi = \phi_1 \vee \phi_2$ and $\phi = \phi_1 \wedge \phi_2$: straightforward.

Case $\phi = \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$: We know that $[\![\mathcal{H}(\phi_1)\mathcal{U}_{C(\mathcal{I},\Delta\tau)}\mathcal{H}(\phi_2)]\!]_\tau(s,i) > \mathcal{E}(\Delta\tau)$. By Lemma 1 and the definition of until : there exists a $j \in \tau^{-1}(\tau(i) +_R C(\mathcal{I},\Delta\tau))$ such that $[\![\mathcal{H}(\phi_2)]\!]_\tau(s,j) > \mathcal{E}(\Delta\tau)$ and for all k such that $i \leq k < j$ we have $[\![\mathcal{H}(\phi_1)]\!]_\tau(s,k) > \mathcal{E}(\Delta\tau)$. By the induction hypothesis, we get that $\langle\!\langle\phi_2\rangle\!\rangle(s,t) = \top$ for all $t \in [\tau(j) - \Delta\tau, \tau(j) + \Delta\tau] \cap R$ and $\langle\!\langle\phi_1\rangle\!\rangle(s,t) = \top$ for all $t \in [\tau(k) - \Delta\tau, \tau(k) + \Delta\tau] \cap R$ and for all $k \in [i,j)$. We set $t' = \tau(j)$. Note that for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$ we have $t' \in t +_R \mathcal{I}$ since $\tau(j) \in \tau(i) +_R C(\mathcal{I},\Delta\tau)$. Also, since $\tau(j) \leq \tau(j-1) + \Delta\tau$ we get that for all $t'' \in [t,t')$ we have $\langle\!\langle\phi_1\rangle\!\rangle(s,t'') = \top$. Hence, we conclude that $\langle\!\langle\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2\rangle\!\rangle(s,t) = \top$ for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$.

Case $\phi = \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$: We know that $[\![\mathcal{H}(\phi_1)\mathcal{R}_{E(\mathcal{I},\Delta\tau)}\mathcal{H}(\phi_2)]\!]_\tau(s,i) > \mathcal{E}(\Delta\tau)$. By Lemma 1 and the definition of release : for all $j \in \tau^{-1}(\tau(i) +_R E(\mathcal{I},\Delta\tau))$ we have $[\![\mathcal{H}(\phi_2)]\!]_\tau(s,j) > \mathcal{E}(\Delta\tau)$ or there exists k such that $i \leq k < j$ and $[\![\mathcal{H}(\phi_1)]\!]_\tau(s,k) > \mathcal{E}(\Delta\tau)$. By the induction hypothesis, we get that for all $j \in \tau^{-1}(\tau(i) +_R E(\mathcal{I},\Delta\tau))$ we have $\langle\!\langle\phi_2\rangle\!\rangle(s,t) = \top$ for all $t \in [\tau(j) - \Delta\tau, \tau(j) + \Delta\tau] \cap R$ and $\langle\!\langle\phi_1\rangle\!\rangle(s,t) = \top$ for all $t \in [\tau(k) - \Delta\tau, \tau(k) + \Delta\tau] \cap R$. Let $j_m = \min \tau^{-1}(\tau(i) +_R E(\mathcal{I},\Delta\tau))$ and $j_M = \max \tau^{-1}(\tau(i) +_R E(\mathcal{I},\Delta\tau))$. For all $t' \in [\tau(j_m) - \Delta\tau, \tau(j_M) + \Delta\tau]$ we have $\langle\!\langle\phi_2\rangle\!\rangle(s,t') = \top$. But, for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$ we have $t +_R \mathcal{I} \subseteq \tau(i) +_R E(\mathcal{I},\Delta\tau)$. Hence, for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$, for all $t' \in t +_R \mathcal{I}$, we have $\langle\!\langle\phi_2\rangle\!\rangle(s,t') = \top$ or there exists some $t'' \in [t,t')$ such that $\langle\!\langle\phi_1\rangle\!\rangle(s,t'') = \top$. Hence, $\langle\!\langle\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2\rangle\!\rangle(s,t) = \top$ for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$. □

We should remark that the conclusion (7) of Theorem 1 does not imply that the continuous time Boolean signal $\mathcal{O}^{-1} \circ s$ satisfies the finite variability property as it is defined in [5]. It only states that there exists some time interval in R of length at least $2\Delta\tau$ such that the Boolean truth value of some atomic propositions remains constant.

Corollary 1 *Consider $\phi \in \Phi_{\mathbb{B}}$, $\mathcal{O} \in \mathcal{P}(X)^{AP}$, $s \in \mathfrak{S}$, $\tau \in \mathfrak{T}$ and let Assumptions 1–3 hold. Then, $[\![\mathcal{H}(\phi)]\!]_\tau(s) > \mathcal{E}(\Delta\tau)$ implies $\langle\!\langle\phi\rangle\!\rangle(s) = \top$.*

If the condition $[\![\mathcal{H}(\phi)]\!]_\tau(s) > \mathcal{E}(\Delta\tau)$ fails, then in general we cannot infer anything about the relationship of the two semantics. Two strategies in order to guarantee the above condition would be (i) to reduce the size of the sampling step $\Delta\tau$ or (ii) to devise an on-line monitoring procedure that can adjust real-time the sampling step according to the robustness estimate of a signal with respect to an MITL formula ϕ.

6 Examples

In this section, we demonstrate the proposed methodology with some examples. The discrete time signals under consideration could be the result of sampling a physical signal or a simulated one. The latter is meaningful in cases where we would like to use fewer sampled points for temporal logic testing, while simulating the actual trajectory with finer integration step. The robustness estimate is computed using the algorithm that was presented in [12].

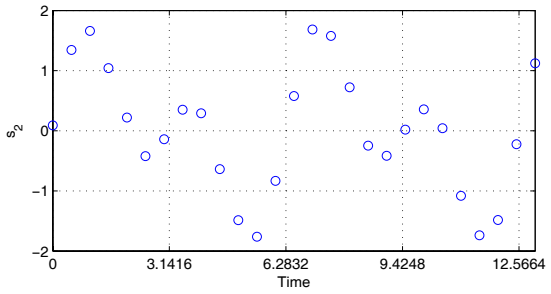

Fig. 2. The sampled signal $\hat{s}_2$ generated by sampling the continuous time signal $s_2(t) = \sin(t) + \sin(2t) + w(t)$, where $|w(t)| \leq 0.1$, with constant sampling period 0.5. In this case, it is $|s_2(t_1) - s_2(t_2)| \leq L_{s_1}|t_1 - t_2| + |w(t_1)| + |w(t_2)|$. Thus, $\mathcal{E}_2(t) = L_{s_1}t + 0.2$.

Example 2 *Assume that we are given a discrete representation of a signal* $\hat{s}_1$ *(Fig. 1) which has constant sampling step of magnitude* 0.2*, i.e.,* $\Delta\tau_1 = 0.2$*. We are also provided with the constraint* $\mathcal{E}_1(t) = 3t$ *(notice that* $|\dot{s}_1(t)| \leq |\cos t| + 2|\cos 2t| \leq 1 + 2 = 3$ *for all* $t \in R$*, therefore* s_1 *is Lipschitz continuous with* $L_{s_1} = 3$*). We would like to test whether the underlying continuous time signal* s_1 *satisfies the specification* $\phi_1 = \Box_{[0,9\pi/2]}(p_{11} \rightarrow \Diamond_{[\pi,2\pi]}p_{12})$*, with* $\mathcal{O}(p_{11}) = \mathbb{R}_{\geq 1.5}$ *and* $\mathcal{O}(p_{12}) = \mathbb{R}_{\leq -1}$*. Notice that the sampling function* τ_1 *satisfies the constraints of the Assumptions 2 and 3. Using the computational procedure proposed in [12], we compute a robustness estimate of* $[\![\mathcal{H}(\phi_1)]\!]_{\tau_1}(s_1) = 0.7428$*, while* $\mathcal{E}_1(\Delta\tau_1) = 0.6$*. Therefore, by Corollary 1 we conclude that* $\langle\!\langle\phi_1\rangle\!\rangle(s_1) = \top$*.* □

The next example manifests a very intuitive attribute of the framework, namely, that the more robust a signal is with respect to the MITL specification the larger the sampling period can be.

Example 3 *Consider the discrete time signal* $\hat{s}_2$ *in Fig. 2. The MITL specification is* $\phi_2 = \Box_{[0,4\pi]}p_{21} \wedge \Diamond_{[3\pi,4\pi]}p_{22}$ *with* $\mathcal{O}(p_{21}) = [-4, 4]$ *and* $\mathcal{O}(p_{22}) = \mathbb{R}_{\leq 0}$*. In this case, we compute a robustness estimate of* $[\![\mathcal{H}(\phi_2)]\!]_{\tau_2}(s_2) = 1.7372$*, while* $\mathcal{E}_2(\Delta\tau_2) = 1.7$ *where* $\Delta\tau_2 = 0.5$*. Therefore, we conclude that* $\langle\!\langle\phi_2\rangle\!\rangle(s_2) = \top$*.* □

In the following example, we utilize our framework in order to test trajectories of nonlinear systems. More specifically, we consider linear feedback systems with saturation. Such systems have nonlinearities that model sensor/actuator constraints (for example see [8, §10]).

Example 4 (Example 10.5 in [8]) *Consider the following linear dynamical system with nonlinear feedback*

$$\dot{x}(t) = Ax(t) - b\,\mathrm{sat}(cx(t)), \quad s_3(t) = cx(t) \tag{8}$$

where the saturation function sat *is defined as*

$$\mathrm{sat}(y) = \begin{cases} -1 & \text{for } y < -1 \\ y & \text{for } |y| \leq 1 \\ 1 & \text{for } y > 1 \end{cases}$$

and A, b, c are the matrices

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad c = \begin{bmatrix} 2 & 1 \end{bmatrix}.$$

First note that the origin $x = [0\ 0]^T$ is an equilibrium point of the system and that the system is absolutely stable with a finite domain (also note that A is not Hurwitz). An estimate of the region of attraction of the origin is the set $\Omega = \{x \in \mathbb{R}^2 \mid V(x) \leq 0.34\}$, where $V(x) = x^T P x$ and

$$P = \begin{bmatrix} 0.4946 & 0.4834 \\ 0.4834 & 1.0774 \end{bmatrix}$$

(see Example 10.5 in [8] for details). For any initial condition $x(0) \in \Omega$, we know that $x(t) \in \{x \in \mathbb{R}^2 \mid V(x) \leq V(x(0))\}$ for all $t \in R$. Thus, $\|x(t)\| \leq \sqrt{\lambda_{\max}(V(x(0))P^{-1})} = \sqrt{\lambda_{\max}(P_e)}$ for all $t \in R$. Moreover,

$$\|\dot{x}(t)\| \leq \|A\|\|x(t)\| + \|b\| \leq \|A\|\sqrt{\lambda_{\max}(P_e)} + \|b\| = L_x$$

and, thus, we have $|s_3(t) - s_3(t')| \leq \|c\|\|x(t) - x(t')\| \leq \|c\|L_x|t - t'|$ for any $t, t' \in R$, i.e., $\mathcal{E}_3(t) = \|c\|L_x t$. Assume, now, that we would like to verify that the signal enters an acceptable stability region within 6 *to* 8 sec*, that is, the MITL formula is $\phi_3 = \Diamond_{[6,8]}\Box_{[0,10]}p_{31}$ with $\mathcal{O}(p_{31}) = [-0.25, 0.25]$. The initial condition is $x(0) = [-1\ 0.6]^T \in \Omega$. The system (8) is integrated with a maximum step-size of* 0.001 *using the MATLAB ode45 solver. The observable discrete time signal $\hat{s}_3$ has maximum step-size $\Delta\tau_3 = 0.045$. The robustness estimate is $[\![\mathcal{H}(\phi_3)]\!]_{\tau_3}(s_3) = 0.2372$, while $\mathcal{E}_3(\Delta\tau_3) = 0.2182$. Therefore, we conclude that $\langle\!\langle \phi_3 \rangle\!\rangle(s_3) = \top$. Note that in this example, we assume that the simulation is accurate and, hence, we ignore the possible simulation error. The incorporation of the simulation error into $\mathcal{E}_3$ will be part of future research.* □

7 Conclusions and Discussion

We have developed a framework that enables continuous time reasoning using discrete time methods. The target application is on continuous time signals generated by physical systems with real-time constraints. Our solution utilizes the notion of robustness of MTL specifications [12] and provides conditions on the signal dynamics and the sampling function.

We should point out that the idea of continuous time verification by discrete reasoning is not new. In [20], the authors show that if a formula has the finite

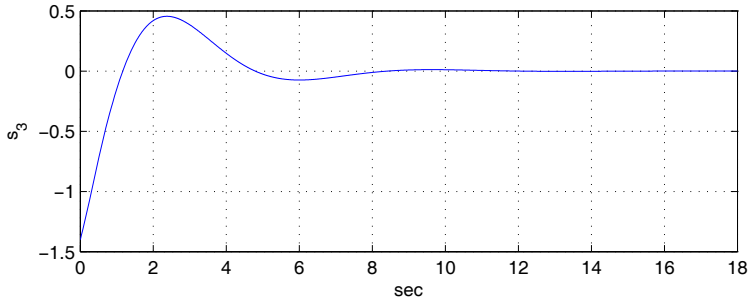

Fig. 3. The output signal s_3 of Example 4.

variability property, then its validity in discrete time implies validity in continuous time. This result enables the application of verification rules for discrete time semantics to continuous time problems. The work that is the most related to ours appears in [21]. There, the authors give conditions that enable the uniform treatment of both discrete and continuous time semantics within the temporal logic TRIO (they also note that their results should be easily transferable to MTL). Despite the apparent differences (for example, we do not assume finite variability and we use analog clocks in our discrete time logic) between [21] and our work, the two papers are in fact complementary. We actually provide concrete and practical conditions on the signals such that what is defined as "closure under inverse sampling" in [21] holds.

In the current framework, we require a global bound $\mathcal{E}(\Delta\tau)$ on the deviation of the signal between two samples. This might be too conservative for applications with variable sampling step. One important modification to this theory will be to use local bounds $\mathcal{E}(\tau(i) - \tau(i-1))$ in coordination with an on-line monitoring algorithm. Related to the previous modification is the extension of the present methodology to hybrid systems [22]. Currently, hybrid systems can be handled by taking as bound $\mathcal{E}$ the most conservative bound $\mathcal{E}_c$ of all control locations c of the hybrid automaton. Finally, as it is well known, the Lipschitz constant might be a very conservative estimate on the deviation of the signal between two points in time. In future work, we plan to use approximate metrics [23] in order to obtain better bounds.

Acknowledgments The authors would like to thank A. Agung Julius for the useful discussions. This work has been partially supported by NSF EHS 0311123, NSF ITR 0324977 and ARO MURI DAAD 19-02-01-0383.

References

1. Pillage, L., Rohrer, R., Visweswariah, C.: Electronic Circuit and System Simulation Methods. McGraw-Hill (1995)
2. Ogata, K.: Modern Control Engineering. 4 edn. Prentice Hall (2001)

3. Koymans, R.: Specifying real-time properties with metric temporal logic. Real-Time Systems **2** (1990) 255–299
4. Alur, R., Feder, T., Henzinger, T.A.: The benefits of relaxing punctuality. Journal of the ACM **43** (1996) 116–146
5. Hirshfeld, Y., Rabinovich, A.: Logics for real time: Decidability and complexity. Fundam. Inf. **62** (2004) 1–28
6. Maler, O., Nickovic, D.: Monitoring temporal properties of continuous signals. In: Proceedings of FORMATS-FTRTFT. Volume 3253 of LNCS. (2004) 152–166
7. Maler, O., Nickovic, D., Pnueli, A.: From MITL to Timed Automata. In: Proceedings of FORMATS. Volume 4202 of LNCS., Springer (2006) 274–289
8. Khalil, H.K.: Nonlinear Systems. Second edn. Prentice-Hall (1996)
9. Thati, P., Rosu, G.: Monitoring algorithms for metric temporal logic specifications. In: Runtime Verification. Volume 113 of ENTCS., Elsevier (2005) 145–162
10. Bensalem, S., Bozga, M., Krichen, M., Tripakis, S.: Testing conformance of real-time applications with automatic generation of observers. In: Proceedings of Runtime Verification Workshop, Barcelona, Spain (2004)
11. Tan, L., Kim, J., Sokolsky, O., Lee, I.: Model-based testing and monitoring for hybrid embedded systems. In: Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration. (2004) 487–492
12. Fainekos, G.E., Pappas, G.J.: Robustness of temporal logic specifications. In: Proceedings of FATES/RV. Volume 4262 of LNCS., Springer (2006) 178–192
13. Pnueli, A.: Development of hybrid systems. In: FTRTFT. Volume 863 of LNCS., Springer (1994) 77–85
14. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press (2004)
15. Emerson, E.A.: Temporal and modal logic. In van Leeuwen, J., ed.: Handbook of Theoretical Computer Science: Formal Models and Semantics. Volume B. North-Holland Pub. Co./MIT Press (1990) 995–1072
16. Alur, R., Henzinger, T.A.: Real-Time Logics: Complexity and Expressiveness. In: Fifth Annual IEEE Symposium on Logic in Computer Science, Washington, D.C., IEEE Computer Society Press (1990) 390–401
17. de Alfaro, L., Faella, M., Stoelinga, M.: Linear and branching metrics for quantitative transition systems. In: Proceedings of the 31st ICALP. Volume 3142 of LNCS., Springer (2004) 97–109
18. Wood, G.R., Zhang, B.P.: Estimation of the Lipschitz constant of a function. Journal of Global Optimization **8** (1996) 91–103
19. Huang, J., Voeten, J., Geilen, M.: Real-time property preservation in approximations of timed systems. In: Proceedings of the 1st ACM & IEEE International Conference on Formal Methods and Models for Co-Design. (2003) 163–171
20. de Alfaro, L., Manna, Z.: Verification in continuous time by discrete reasoning. In: Proceedings of the 4th AMAST. Volume 936 of LNCS., Springer (1995) 292–306
21. Furia, C.A., Rossi, M.: Integrating discrete and continuous time metric temporal logics through sampling. In: FORMATS. Volume 4202 of LNCS., Springer (2006) 215–229
22. Julius, A.A., Fainekos, G.E., Anand, M., Lee, I., Pappas, G.J.: Robust test generation and coverage for hybrid systems. In: Hybrid Systems: Computation and Control. Number 4416 in LNCS, Springer (2007) 329–342
23. Girard, A., Pappas, G.J.: Approximation metrics for discrete and continuous systems. IEEE Trans. Auto. Cont. **52** (2007) 782–798