Robustness of Temporal Logic Specifications for Continuous-Time Signals ⋆

Georgios E. Fainekos [a], George J. Pappas [a,b]

[a] *Department of Computer and Information Science, University of Pennsylvania, 3330 Walnut Street, Philadelphia, PA 19104-6389, USA*

[b] *Department of Electrical and Systems Engineering, University of Pennsylvania, 200 South 33rd Street, Philadelphia, PA 19104, USA*

Abstract

In this paper, we consider the robust interpretation of Metric Temporal Logic (MTL) formulas over signals that take values in metric spaces. For such signals, which are generated by systems whose states are equipped with nontrivial metrics, for example continuous or hybrid, robustness is not only natural, but also a critical measure of system performance. Thus, we propose multi-valued semantics for MTL formulas, which capture not only the usual Boolean satisfiability of the formula, but also topological information regarding the distance, ε, from unsatisfiability. We prove that any other signal that remains ε-close to the initial one also satisfies the same MTL specification under the usual Boolean semantics. Finally, our framework is applied to the problem of testing formulas of two fragments of MTL, namely Metric Interval Temporal Logic (MITL) and closed Metric Temporal Logic (clMTL), over continuous-time signals using only discrete-time analysis. The motivating idea behind our approach is that if the continuous-time signal fulfills certain conditions and the discrete time signal robustly satisfies the temporal logic specification, then the corresponding continuous-time signal should also satisfy the same temporal logic specification.

Key words: Linear & Metric Temporal Logic, Robustness, Metric Spaces, Testing.

⋆ This research has been partially supported by NSF EHS 0311123, NSF ITR 0324977 and ARO MURI DAAD 19-02-01-0383. Preliminary results of this work have appeared in [17] and [19].

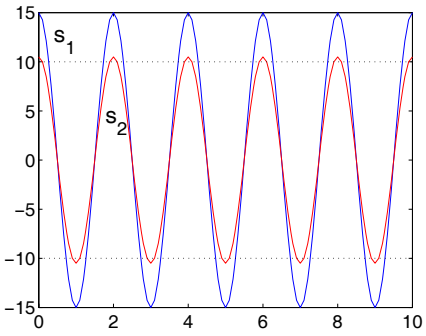

Fig. 1. Two signals s_1 and s_2 which satisfy the specification: $\Box(p_1 \rightarrow \Diamond_{\leq 2} p_2)$. Here, $\mathcal{O}(p_1) = \mathbb{R}_{\leq -10}$ and $\mathcal{O}(p_2) = \mathbb{R}_{\geq 10}$.

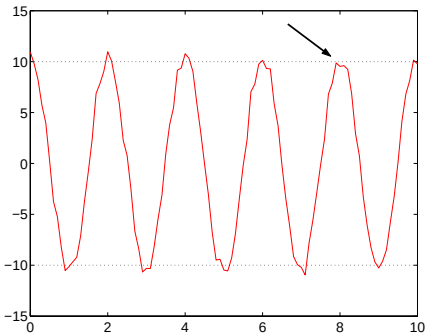

Fig. 2. The signal s_2 modified by random noise. The arrow points to the point in time where the property fails.

1 Introduction

Model checking [11] has been proven to be a very useful tool for the verification of software and hardware systems. The tools and methodologies developed for such systems do not naturally extend to systems whose state space is some general infinite space, for example continuous and hybrid systems. In this case, the model checking problem becomes harder and in most of the cases is undecidable [1]. In practice, the validation of such systems still relies heavily on methods that involve systematic testing [34,33]. More recently, temporal logic testing [53,40] has been proposed as a framework that can provide us with additional information about the properties of continuous or discrete-time signals. However, the classical approaches to temporal logic testing involve a Boolean abstraction of the value of the signal with respect to the atomic propositions in the formula. This loss of information can be quite critical when we consider systems that model or control physical processes. For example, consider the signals s_1 and s_2 in Fig. 1. Both of them satisfy the same specification "if the value of the signal drops below -10, then it should also raise above 10 within 2 time units". Nevertheless, a visual inspection of Fig. 1 indicates that there exists a qualitative difference between s_1 and s_2. The latter "barely" satisfies the specification. Indeed as we can see in Fig. 2, adding a bounded noise on s_2 renders the property unsatisfiable on s_2.

In order to differentiate between such trajectories of a system, in [17] we introduced the concept of *robustness degree* for finite timed state sequences. Here, we extend the results of [17] to continuous-time signals with potentially unbounded time domain. Informally, the robustness degree is the bound on the perturbation that the signal can tolerate without changing the truth value of a specification expressed in Metric Temporal Logic (MTL) [36]. In detail, we consider signals which take values in some set X equipped with a metric d. If the time domain of these signals is R, then we can consider each signal as

a point in X^R, which is the space of all possible signals with time domain R. In order to quantify how close are two different signals in X^R, we define the notion of distance using a metric ρ on the space X^R. Given an MTL formula ϕ, we can partition the space X^R into two sets: the set $\mathcal{L}(\phi)$ of signals that satisfy ϕ and the set $\mathcal{L}(\neg\phi)$ of signals that do not satisfy ϕ. Then, the formal definition of the robustness degree comes naturally, it is just the distance of a signal $s \in \mathcal{L}(\phi)$ from the set $\mathcal{L}(\neg\phi)$. Using the degree of robustness and the metric ρ, we can define an open ball (tube) around s and, therefore, we can be sure that any signal s' that remains within the open ball also stays in $\mathcal{L}(\phi)$. In this paper, we refer to such tubes as robust neighborhoods.

The robustness degree is not the only way to define robust neighborhoods. One can define multi-valued (or *robust* as it will be referred to in this paper) semantics for MTL formulas. An atomic proposition in the robust version of MTL evaluates to the distance between the current value of the signal and the subset of X that the atomic proposition represents. As established in the framework of multi-valued logics [9,13], the conjunction and disjunction in the Boolean logic are replaced by the inf and sup operations. In this paper, the logical negation is replaced by the usual negation over the reals. We prove that when an MTL formula is evaluated with robust semantics over a signal s, then its value is an under-approximation ε (*robustness estimate*) of the robustness degree and, therefore, any other signal s' that remains ε-close to s also satisfies the same specification.

Application-wise the importance of the robustness degree / estimate is immediate : if a system has the property that for near-by initial conditions (or under bounded disturbances etc) its signals remain δ-close to the nominal one and, also, its robustness degree / estimate with respect to an MTL formula ϕ is $\varepsilon > \delta$, then we know that all the system's signals also satisfy the same specification. This basic idea has been applied to the bounded time temporal logic verification of linear systems in [15]. Along the same lines, the framework that we present in this paper can be readily used in several other applications such as Qualitative Simulation [52], mobile robot path planning [16] and in behavioral robotics [38].

In this paper, we present one additional application of the robustness estimate. 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 rely heavily on testing the actual circuit or, more commonly, on simulations [46]. 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 con-

straints on the output signal [44] can be very naturally captured using MTL with continuous-time semantics [36]. The question that arises then is : Can we verify continuous-time properties of a system using only discrete-time reasoning? In [19], we answered this question in the positive for the satisfiability problem of Metric Interval Temporal Logic (MITL) [3] specifications. Here, we revisit the problem and derive conditions for approximating the continuous-time robustness estimate of a signal with respect to a specification in clMTL, a restricted version of MTL which allows only closed intervals as timing constraints [40]. In addition, this new result makes possible the approximation of the robustness estimate of any Linear Temporal Logic (LTL) [47] formula with respect to a continuous-time signal.

Our proposed solution derives conditions on the dynamics of the signal, on the sampling function and on the timing constraints of MTL such that temporal logic reasoning over discrete-time signals can be applied to continuous-time signals. The main machinery that we employ for this purpose is the computation of the robustness estimate. 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 exceed the distance that is computed using the robust semantics. The constraints on the sampling function play another role. They guarantee that there exist enough sampling points such that the validity of temporal logic formulas is maintained between the two different semantics [48].

The structure of the paper is as follows. Section 2 introduces the continuous-time semantics of MTL and the notions of robustness degree (Section 2.3) and robustness estimate (Section 2.4) for continuous-time signals. In Section 3, we restate some of the results of Section 2 for discrete-time signals. Section 3 concludes by presenting a monitoring algorithm (similar to [54,26]) that is based on the discrete-time robust semantics of MTL. The conditions on the signal and the sampling function and the logic such that continuous-time reasoning using discrete-time methods is possible are presented in Section 4. Our theoretical results are demonstrated in Section 4.4 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 [35,44], while the analysis of the transient properties has not received much attention.

2 Temporal Logic Robustness for 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. Then,

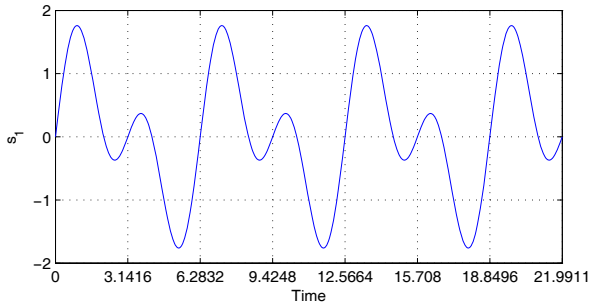

Fig. 3. A continuous-time signal s_1 with time domain $R = [0, 7\pi]$.

we proceed to define our notion of robustness for temporal logic formulas. Let $\mathbb{R}$ be the set of the real numbers, $\mathbb{Q}$ be the set of rationals and $\mathbb{N}$ the set of the 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 than 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, the set $\mathcal{F}(A, B)$ denotes the set of all functions from A to B. That is, $\mathcal{F}(A, B) = B^A$ and for any $f \in \mathcal{F}(A, B)$, we have $f : A \to B$. The domain of a function $f \in \mathcal{F}(A, B)$ is denoted by $\mathbf{dom}(f)$. Given a set A, $\mathcal{P}(A)$ denotes its powerset and $|A|$ denotes its cardinality. Finally, if A is a subset of a topological space, then $cl(A)$ denotes its closure, that is, the intersection of all closed sets containing A.

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. Typical models of real time systems are the formalisms of timed automata [2], hybrid automata [27] and dynamical systems [10,35]. 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, then $R = [0, r] \subseteq \mathbb{R}_{\geq 0}$ with $r > 0$, otherwise we let $R = \mathbb{R}_{\geq 0}$. In the following, we fix R to refer to a time domain as described above. As an example of a continuous-time signal, consider the function $s_1(t) = \sin t + \sin 2t$ in Fig. 3 such that $R = [0, 7\pi]$.

A metric space (X, d) is a set X with a metric d. For a short introduction to metric spaces see [43]. 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 $d : X \times X \to \overline{\mathbb{R}}_{\geq 0}$, such that the 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, Signed Distance [8] §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* $\mathbf{dist}_d(x, S) := \inf\{d(x, y) \mid y \in cl(S)\}$
- *Depth of x in S to be* $\mathbf{depth}_d(x, S) := \mathbf{dist}_d(x, X \backslash S)$
- *Signed Distance from x to S to be*

$$\mathbf{Dist}_d(x, S) := \begin{cases} -\mathbf{dist}_d(x, S) & \text{if } x \notin S \\ \mathbf{depth}_d(x, S) & \text{if } x \in S \end{cases}$$

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 $\overline{\mathbb{R}}$ as above, 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 $B_d(x, \varepsilon) = \{y \in X \mid d(x, y) < \varepsilon\}$.*

The following properties of the ε-ball are immediate. Given $0 < \varepsilon < \varepsilon'$ and a point $x \in X$, we have $B_d(x, \varepsilon) \subseteq B_d(x, \varepsilon')$. Also, if $\mathbf{dist}_d(x, S) = \varepsilon > 0$, then $B_d(x, \varepsilon) \cap S = \emptyset$. Note that $\mathbf{dist}_d$ actually returns the radius of the largest ball $B_d(x, \varepsilon)$ that fits in the set $X \backslash S$. Similarly, it is easy to see that if $\mathbf{depth}_d(x, S) = \varepsilon > 0$, then $B_d(x, \varepsilon) \subseteq S$.

2.2 Metric Temporal Logic over Continuous-Time Signals

Metric Temporal Logic (MTL) was introduced in [36] in order to reason about the quantitative timing properties of boolean signals. In this section, we review the basics of propositional MTL over continuous-time signals. Also, we present the syntax and semantics of Metric Interval Temporal Logic (MITL) [3] and closed Metric Temporal Logic (clMTL) as fragments of MTL.

Definition 4 (MTL Syntax) *Let $\mathbb{C}$ be the set of truth degree constants and*

AP be the set of atomic propositions. The set $MTL_{\mathbb{C}}$ of all well-formed formulas (wff) is inductively defined using the following grammar:

$$\phi \ ::= \ c \mid p \mid \neg\phi \mid \phi \vee \phi \mid \phi \mathcal{U}_{\mathcal{I}} \phi$$

where $p \in AP$ and $\mathcal{I}$ ranges over intervals of $\mathbb{R}_{\geq 0}$. The cases in the grammar above correspond respectively to constants, atomic propositions, negation, disjunction and until. If the rule $\neg\phi$ is replaced by $\neg p$ and we add the rules $\phi \wedge \phi$ (conjunction) and $\phi \mathcal{R}_{\mathcal{I}} \phi$ (release) to the grammar, then we say that the formula is in Negation Normal Form (NNF). In this case, the set of wff is denoted by $MTL^{+}_{\mathbb{C}}$. The set $MTL_{\mathbb{C}}(op_1, op_2, \ldots)$ denotes the subset of MTL formulas that contain only the operators $op_1, op_2, \ldots$. If, also, we require that $\mathcal{I}$ is not a singleton set, i.e., $\mathcal{I} \neq \{a\}$ for some $a \in \mathbb{R}_{\geq 0}$, then we get the set $MITL_{\mathbb{C}}$ of all wff MITL formulas. Finally, if $\mathcal{I}$ ranges over intervals of $\mathbb{Q}_{\geq 0}$, i.e., $\mathcal{I} \subseteq \mathbb{Q}_{\geq 0}$, such that $cl(\mathcal{I}) = \mathcal{I}$, then we get the set $clMTL_{\mathbb{C}}$ of all wff clMTL formulas.

In Boolean logic, the set of truth degree constants simply consists of the *true* ($\top$) and *false* ($\bot$) values. When we consider multi-valued logics, this set contains more then two elements and, in certain cases, it can also be an infinite set. 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. In MTL, the subscript $\mathcal{I}$ is essentially any interval of $\mathbb{R}_{\geq 0}$ and it imposes timing constraints on the temporal operators. Note that the interval $\mathcal{I}$ can be open, half-open or closed, bounded or unbounded, and it might even be the empty set $\emptyset$. 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 $\mathcal{U}_{\leq 1}$.

Metric Temporal Logic (MTL) formulas are interpreted over continuous-time signals. In this paper, we define the continuous-time Boolean semantics of MTL formulas using a valuation function $\langle\!\langle \cdot, \cdot \rangle\!\rangle_C : MTL_{\mathbb{B}} \times \mathcal{F}(AP, \mathcal{P}(X)) \to (\mathcal{F}(R, X) \times R \to \mathbb{B})$ and we write $\langle\!\langle \phi, \mathcal{O} \rangle\!\rangle_C(s, t) = \top$ instead of the usual notation $(\mathcal{O}^{-1} \circ s, t) \models \phi$. 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 $x \in X$. In this case, we say that the signal s under observation map $\mathcal{O}$ satisfies the formula ϕ at time t. For brevity, we drop $\mathcal{O}$ from the notation since without loss of generality we can consider it constant throughout this paper. We are therefore interested in checking whether $\langle\!\langle \phi \rangle\!\rangle_C(s, 0) = \top$. In

this case, we refer to s as a *model* of ϕ and we just write $\langle\!\langle \phi \rangle\!\rangle_C(s) = \top$ 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 some $V \subseteq \mathbb{V}$ 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 $\inf \emptyset := \top$. Since $(\mathbb{V}, <)$ is a totally ordered set, it is also a *distributive lattice* (see Example 4.6 (2) in [12]), i.e., for all $a, b, c \in \mathbb{V}$, we have $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$ 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 MTL) *Let $\phi \in MTL_{\mathbb{B}}$ be a formula, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ be an observation map and $s \in \mathcal{F}(R, X)$ be a continuous-time signal, then the continuous-time semantics of ϕ is defined by*

$$
\begin{aligned}
\langle\!\langle \top \rangle\!\rangle_C(s,t) &:= \top \\
\langle\!\langle p \rangle\!\rangle_C(s,t) &:= K_{\in}(s(t), \mathcal{O}(p)) = \begin{cases} \top \text{ if } s(t) \in \mathcal{O}(p) \\ \bot \text{ otherwise} \end{cases} \\
\langle\!\langle \neg\phi_1 \rangle\!\rangle_C(s,t) &:= \neg\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) \\
\langle\!\langle \phi_1 \vee \phi_2 \rangle\!\rangle_C(s,t) &:= \langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) \sqcup \langle\!\langle \phi_2 \rangle\!\rangle_C(s,t) \\
\langle\!\langle \phi_1 \,\mathcal{U}_{\mathcal{I}}\, \phi_2 \rangle\!\rangle_C(s,t) &:= \bigsqcup_{t' \in (t +_R \mathcal{I})} \Big(\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') \sqcap \bigsqcap_{t < t'' < t'} \langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') \Big)
\end{aligned}
$$

where $t, t', t'' \in R$ and $K_{\in}$ is the characteristic function of the $\in$ relation.

Informally, the formula $\phi_1 \,\mathcal{U}_{\mathcal{I}}\, \phi_2$ expresses the property that over the signal s and in the time interval $t +_R \mathcal{I}$, there exists some time t' such that s makes ϕ_2 true and, furthermore, for all previous time (besides the current time t), s satisfies ϕ_1. Notice that in the definition of until the time t' is quantified over the set $t +_R \mathcal{I}$ instead of simply $t + \mathcal{I}$. This is necessary since the signal s might be of bounded duration and, thus, it is not defined for any time value that does not belong to the set R. Intuitively, the release operator $\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$ states that ϕ_2 should always hold during the interval $t +_R \mathcal{I}$, a requirement which is released when ϕ_1 becomes true. More formally, the semantics of $\mathcal{R}_{\mathcal{I}}$ can be defined using the semantics of $\mathcal{U}_{\mathcal{I}}$ and the following syntactic equivalence, $\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2 \equiv \neg(\neg\phi_1 \,\mathcal{U}_{\mathcal{I}}\, \neg\phi_2)$. We can also define the temporal operators *eventually* $\Diamond_{\mathcal{I}} \phi \equiv \top \,\mathcal{U}_{\mathcal{I}}\, \phi$ and *always* $\Box_{\mathcal{I}} \phi \equiv \bot \mathcal{R}_{\mathcal{I}} \phi$.

The until operator as defined above is also referred to as *strict non-matching* until [23]. In addition, we define two more versions of the until temporal operator. Namely, (i) the *non-strict non-matching* version of until $\phi_1 \,\overleftarrow{\mathcal{U}}_{\mathcal{I}}\, \phi_2$ with

definition if $0 \notin \mathcal{I}$, then $\phi_1 \wedge (\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2)$, else $\phi_2 \vee (\phi_1 \wedge (\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2))$ and (ii) the *non-strict matching* version of until $\phi_1 \overleftrightarrow{\mathcal{U}}_{\mathcal{I}} \phi_2 = \phi_1 \overleftarrow{\mathcal{U}}_{\mathcal{I}} (\phi_1 \wedge \phi_2)$. The respective versions of release are defined using the duality property. Intuitively, the formula $\phi_1 \overleftrightarrow{\mathcal{U}}_{\mathcal{I}} \phi_2$ requires that there exists some time t' in $t +_R \mathcal{I}$ such that both ϕ_2 and ϕ_1 are true and that for all previous time ϕ_1 holds. We will denote the versions of MTL which have as basic temporal operators the $\overleftrightarrow{\mathcal{U}}$ and $\overleftarrow{\mathcal{U}}$ instead of $\mathcal{U}$ by $\overleftrightarrow{\text{MTL}}$ and $\overleftarrow{\text{MTL}}$ respectively. A comparison between the expressive power of the different versions of MTL, i.e., MTL, $\overleftrightarrow{\text{MTL}}$ and $\overleftarrow{\text{MTL}}$, can be found in [23].

In this paper, we also present some results on Linear Temporal Logic (LTL) [47]. Comparing the two logics, MTL is used to reason about the quantitative timing properties, whereas LTL only about qualitative timing properties. Here, we will only consider the standard version of LTL which can be regarded as a fragment of $\overleftarrow{MTL}$ where all the intervals $\mathcal{I}$ of the temporal operators are of the form $[0, +\infty)$. Similar to MTL, we denote the set of all LTL formulas that have truth constants from the set $\mathbb{C}$ by $LTL_{\mathbb{C}}$. When $\mathcal{I} = [0, +\infty)$, we can drop the subscript $\mathcal{I}$ from the temporal operators, i.e., we just write $\overleftarrow{\mathcal{U}}$.

We denote by $\mathcal{L}_t(\phi) = \{s \in \mathcal{F}(R, X) \mid \langle\!\langle \phi \rangle\!\rangle_C(s, t) = \top\}$ the set of all signals that satisfy ϕ at time t. Then $\mathcal{L}(\phi) = \mathcal{L}_0(\phi)$ is the set of all models of ϕ. We say that the formula ϕ is *valid* when $\mathcal{L}(\phi) = \mathcal{F}(R, X)$ and *invalid* when $\mathcal{L}(\phi) = \emptyset$. Note that $\mathcal{L}_t(\neg\phi) = \{s \in \mathcal{F}(R, X) \mid \langle\!\langle \phi \rangle\!\rangle_C(s, t) = \bot\}$ since $\langle\!\langle \neg\phi \rangle\!\rangle_C(s, t) = \neg\langle\!\langle \phi \rangle\!\rangle_C(s, t) = \top$. Thus, the sets $\mathcal{L}_t(\phi)$ and $\mathcal{L}_t(\neg\phi)$ are complements of each other with respect to $\mathcal{F}(R, X)$. Thus, $\mathcal{F}(R, X) \backslash \mathcal{L}_t(\phi) = \mathcal{L}_t(\neg\phi)$ and vice versa.

Remark 6 *We conclude this section with a word of caution. Even though we allow in our definitions signals of unbounded duration, our logical framework cannot capture asymptotic properties with respect to time. For example, consider the signal* $s(t) = \exp(-t)$ *which converges to* 0 *as* t *goes to* $+\infty$*. This signal does not satisfy the specification* $\Diamond p$*, where* $\mathcal{O}(p) = (-\infty, 0]$ *since there does not exist some time* t *such that* $s(t) = 0$*, i.e.,* $s(t) \in \mathcal{O}(p)$*. Therefore, it is natural to consider bounded time domains since we cannot express asymptotic properties with MTL.*

2.3 Robust Satisfaction of MTL Specifications in Continuous-Time

In this section, we define what it means for a signal $s \in \mathcal{F}(R, X)$ to satisfy a Metric Temporal Logic specification *robustly*. For the signals that we consider in this paper, we can naturally quantify how close two signals are by using the

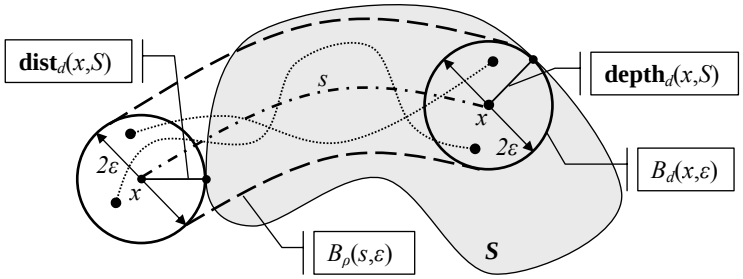

Fig. 4. The definition of distance and depth and the associated neighborhoods. Also, a tube (*dashed lines*) around a nominal signal s (*dash-dotted line*). The tube encloses a set of signals (*dotted lines*).

metric d. Let s and s' be signals in $\mathcal{F}(R, X)$, then

$$\rho(s, s') = \sup_{t \in R} \{d(s(t), s'(t))\} \tag{1}$$

is a metric [1] on the set $\mathcal{F}(R, X) = X^R$. Since the space of signals is equipped with a metric, we can define a tube around a signal s (see Fig. 4). Given an $\varepsilon > 0$, $B_\rho(s, \varepsilon) \subseteq \mathcal{F}(R, X)$ is the set of all signals that remain ε-close to s.

Informally, we define the robustness degree to be the bound on the perturbation that a signal can tolerate without changing its Boolean truth value with respect to a specification expressed in Metric Temporal Logic (MTL) [36]. Abstractly speaking, the degree of robustness that a signal s satisfies an MTL formula ϕ is a number $\varepsilon \in \overline{\mathbb{R}}$. Intuitively, a positive ε means that the formula ϕ is satisfiable in the Boolean sense and, moreover, that all the other signals that remain ε-close to the nominal one also satisfy ϕ. Accordingly, if ε is negative, then s does not satisfy ϕ and all the other signals that remain within the open tube of radius $|\varepsilon|$ also do not satisfy ϕ.

Definition 7 (Robustness Degree) *Let $\phi \in MTL_{\mathbb{B}}$ be an MTL formula, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ be an observation map and $s \in \mathcal{F}(R, X)$ be a continuous-time signal, then $\mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi))$ is the robustness degree of s with respect to ϕ at time t and $\mathbf{Dist}_\rho(s, \mathcal{L}(\phi))$ is the robustness degree of s with respect to ϕ.*

The following proposition is a direct consequence of the definitions. It states that all the signals s', which have distance from s less than the absolute value of the robustness degree of s with respect to ϕ at time t, satisfy the same specification ϕ as s at time t. Note that the property ϕ could be satisfied or falsified on s.

Proposition 8 *Let $\phi \in MTL_{\mathbb{B}}$ be an MTL formula, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ be*

[1] This is the standard metric - namely the *sup metric* - used in spaces of bounded functions [43, §43]. Since in our definitions we allow a metric to take the value $+\infty$, ρ is also a metric over the set $\mathcal{F}(R, X)$.

an observation map and $s \in \mathcal{F}(R, X)$ *be a continuous-time signal. If* $\varepsilon = \mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi)) \neq 0$ *for some* $t \in R$*, then for all* $s' \in B_\rho(s, |\varepsilon|)$*, we have* $\langle\!\langle \phi \rangle\!\rangle_C(s', t) = \langle\!\langle \phi \rangle\!\rangle_C(s, t)$*.*

In the following, given an $\varepsilon > 0$, we will call as *robust neighborhood* any ball (or tube) $B_\rho(s, \varepsilon)$ such that for all $s' \in B_\rho(s, \varepsilon)$, we have $\langle\!\langle \phi \rangle\!\rangle_C(s', t) = \langle\!\langle \phi \rangle\!\rangle_C(s, t)$. Note that the robustness degree of s with respect to ϕ is actually the radius of the largest robustness neighborhood around s.

Remark 9 *If* $\varepsilon = 0$*, then the truth value of* ϕ *with respect to* s *is not robust, i.e., there exists some time* t *such that a small perturbation of the signal's value* $s(t)$ *can change the Boolean truth value of the formula with respect to* s*.*

Nevertheless, the set $\mathcal{L}(\phi)$ cannot be computed or represented analytically. In the next sections, we develop a series of approximations that will enable us to compute an under-approximation of the robustness degree by directly operating on a given signal.

2.4 Robustness Estimate for Continuous-Time Signals

As explained in the previous section, the robustness degree is the maximum radius of the neighborhood that we can fit around a given signal s without changing the truth value of the formula. But are there other ways to determine and compute robust neighborhoods? In this section, we answer this question in a positive manner by introducing *robust semantics* for MTL formulas.

The robust semantics for MTL formulas are multi-valued semantics over the linearly ordered set $\overline{\mathbb{R}}$. We define the valuation function on the atomic propositions to be the depth (or the negative distance) of the current value of the signal $s(t)$ in (from) the set $\mathcal{O}(p)$ labeled by the atomic proposition p. Intuitively, if this distance is positive, then it represents how robustly is the point $s(t)$ within the set $\mathcal{O}(p)$. If, on the other hand, this distance is negative, then it represents how robustly is the point $s(t)$ outside the set $\mathcal{O}(p)$. If this metric is zero, then the point $s(t)$ lies on the boundary of the set $\mathcal{O}(p)$. Therefore, even the smallest perturbation of the point can drive it inside or outside the set $\mathcal{O}(p)$, which dramatically affects the set membership of the point.

For the purposes of the following discussion, we use the notation $[\![\phi, \mathcal{O}]\!]_C(s, t)$ to denote the robust valuation of the formula ϕ over the signal s at time t. Formally, $[\![\cdot, \cdot]\!]_C : (MTL_{\overline{\mathbb{R}} \cup \mathbb{B}} \times \mathcal{F}(AP, \mathcal{P}(X))) \rightarrow (\mathcal{F}(R, X) \times R \rightarrow \overline{\mathbb{R}})$ and, again, the observation map $\mathcal{O}$ is omitted.

Definition 10 (CT Robust Semantics) *Let* $s \in \mathcal{F}(R, X)$*,* $c \in \overline{\mathbb{R}}$ *and* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$*, then the continuous-time robust semantics of any formula* $\phi \in$

$MTL_{\overline{\mathbb{R}}\cup\mathbb{B}}$ with respect to s is recursively defined as follows

$$\begin{aligned}
[\![\top]\!]_C(s,t) &:= +\infty \\
[\![c]\!]_C(s,t) &:= c \\
[\![p]\!]_C(s,t) &:= \mathbf{Dist}_d(s(t), \mathcal{O}(p)) \\
[\![\neg\phi_1]\!]_C(s,t) &:= -[\![\phi_1]\!]_C(s,t) \\
[\![\phi_1 \vee \phi_2]\!]_C(s,t) &:= [\![\phi_1]\!]_C(s,t) \sqcup [\![\phi_2]\!]_C(s,t) \\
[\![\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2]\!]_C(s,t) &:= \bigsqcup_{t' \in (t +_R \mathcal{I})} \Big([\![\phi_2]\!]_C(s,t') \sqcap \prod_{t < t'' < t'} [\![\phi_1]\!]_C(s,t'') \Big)
\end{aligned}$$

where $t, t', t'' \in R$.

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 $a, b \in \overline{\mathbb{R}}$. Therefore using the standard rewriting rules, we can convert any MTL formula into an equivalent formula in NNF under both Boolean and robust semantics. NNF will be necessary in order to derive results on the continuous-time satisfiability of a formula using discrete-time reasoning (Section 4). The following result is immediate.

Definition 11 *Given $\phi \in MTL_{\overline{\mathbb{R}}\cup\mathbb{B}}$, the translation of ϕ to its equivalent formula in Negation Normal Form is achieved using the following rules*

$$\begin{aligned}
&\neg\neg\phi = \phi \\
&\neg(\phi_1 \vee \phi_2) = \neg\phi_1 \wedge \neg\phi_2 \qquad\qquad \neg(\phi_1 \wedge \phi_2) = \neg\phi_1 \vee \neg\phi_2 \\
&\neg(\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2) = \neg\phi_1 \mathcal{R}_{\mathcal{I}} \neg\phi_2 \qquad\qquad \neg(\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2) = \neg\phi_1 \mathcal{U}_{\mathcal{I}} \neg\phi_2
\end{aligned}$$

We denote the function that applies the above rules to ϕ in a recursive way by **nnf***, that is,* $\mathbf{nnf} : MTL_{\overline{\mathbb{R}}\cup\mathbb{B}} \to MTL^{+}_{\overline{\mathbb{R}}\cup\mathbb{B}}$.

Lemma 12 *Consider any signal $s \in \mathcal{F}(R, X)$ and time $t \in R$, then we have $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \langle\!\langle \mathbf{nnf}(\phi) \rangle\!\rangle_C(s,t)$ and $[\![\phi]\!]_C(s,t) = [\![\mathbf{nnf}(\phi)]\!]_C(s,t)$.*

The next theorem comprises the basic step for establishing that the robust interpretation of an MTL formula ϕ over a signal s evaluates to the radius of a robust neighborhood.

Theorem 13 *Given an MTL formula $\phi \in MTL_{\mathbb{B}}$, an observation map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ and a continuous-time signal $s \in \mathcal{F}(R, X)$, then for any $t \in R$, we have $-\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi)) \leq [\![\phi]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi))$.*

Essentially, Theorem 13 states that the evaluation of the robust semantics of a formula can be bounded by its robustness degree. In detail, we have : (i) if $s \in \mathcal{L}_t(\phi)$, then $0 \leq [\![\phi]\!]_C(s,t) \leq \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi))$, and if $s \in \mathcal{L}_t(\neg\phi)$, then

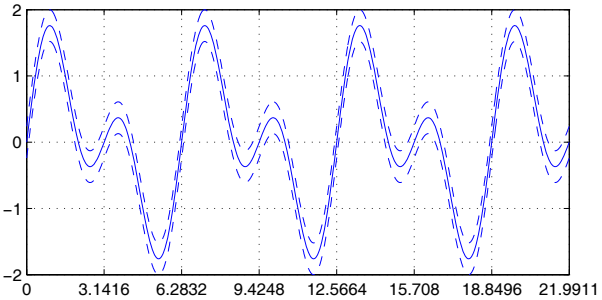

Fig. 5. The signal s_1 and its robustness neighborhood with radius 0.2398.

$-\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi)) \leq [\![\phi]\!]_C(s,t) \leq 0$. Hence, the inequality

$$|[\![\phi]\!]_C(s,t)| \leq |\mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi))| \tag{2}$$

holds. Therefore from Theorem 13 and Proposition 8, we establish as corollary that the robust interpretation of a formula indeed evaluates to the radius of a robust neighborhood.

Corollary 14 *Given an MTL formula $\phi \in MTL_{\mathbb{B}}$, an observation map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ and a continuous-time signal $s \in \mathcal{F}(R, X)$, if for some $t \in R$, we have $\varepsilon = [\![\phi]\!]_C(s,t) \neq 0$, then for all $s' \in B_\rho(s, |\varepsilon|)$, we have $\langle\!\langle\phi\rangle\!\rangle_C(s',t) = \langle\!\langle\phi\rangle\!\rangle_C(s,t)$.*

Example 15 *Consider again the continuous-time signal s_1 in Fig. 3 and assume that we are given the MTL specification $\phi_0 = \Box p_1 \wedge \Diamond_{[7\pi,+\infty)} p_2$, where $\mathcal{O}(p_1) = [-2,2]$ and $\mathcal{O}(p_2) = (-\infty, 0]$. Then, $[\![\phi_0]\!]_C(s_1) \approx 0.2398$. Note that any other signal that remains within the tube around s_1 in Fig. 5 also satisfies the specification ϕ_0.*

The following proposition states the relationship between the Boolean and the robust semantics of MTL.

Proposition 16 *For an MTL formula $\phi \in MTL_{\mathbb{B}}$, an observation map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, a continuous-time signal $s \in \mathcal{F}(R, X)$ and some time $t \in R$, the following two results hold*

(1) $[\![\phi]\!]_C(s,t) > 0 \Rightarrow \langle\!\langle\phi\rangle\!\rangle_C(s,t) = \top$ *and* $[\![\phi]\!]_C(s,t) < 0 \Rightarrow \langle\!\langle\phi\rangle\!\rangle_C(s,t) = \bot$
(2) $\langle\!\langle\phi\rangle\!\rangle_C(s,t) = \top \Rightarrow [\![\phi]\!]_C(s,t) \geq 0$ *and* $\langle\!\langle\phi\rangle\!\rangle_C(s,t) = \bot \Rightarrow [\![\phi]\!]_C(s,t) \leq 0$

Note that the equivalence $[\![\phi]\!]_C(s,t) \geq 0$ *iff* $\langle\!\langle\phi\rangle\!\rangle_C(s,t) = \top$ does not hold, because if a point is on the boundary of the set, its distance to the set or its depth in the set is by definition zero. Therefore, we cannot determine whether the point belongs to that set or not since any information whether the set is open or closed is lost.

At this point, we have not yet answered what is the exact relationship be-

tween $[\![\phi]\!]_C(s,t)$ and $\mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi))$. For example, could we have replaced the inequality in equation (2) with an equality? As the following example indicates, the inequality in equation (2) is usually strict. Therefore, in the following we refer to the evaluation of the robust semantics $[\![\phi]\!]_C(s,t)$ as the *robustness estimate*.

Example 17 *Consider the constant signal $s(t) = 0$ for $t \geq 0$ and the formula $\psi = \Box(p_1 \vee p_2)$ with $\mathcal{O}(p_1) = (-1, 2)$ and $\mathcal{O}(p_2) = (-2, 1)$. It is easy to see that $\mathcal{L}(\psi) = (-2, 2)^{\mathbb{R}_{\geq 0}}$ and, thus, $\mathbf{Dist}_\rho(s, \mathcal{L}(\psi)) = 2$. However, $[\![\psi]\!]_C(s) = \bigsqcap_{t\geq 0} ([\![p_1]\!]_C(s,t) \sqcup [\![p_2]\!]_C(s,t)) = \bigsqcap_{t\geq 0} (1 \sqcup 1) = 1$. In other words, the robust MTL semantics evaluate to an under-approximation of the robustness degree.*

Unfortunately, the robust semantics cannot always capture the fact that a signal is robust with respect to a specification. The next example demonstrates how the robustness estimate might evaluate to zero even when the formula is valid.

Example 18 *Consider the constant signal $s(t) = 0$ for $t \geq 0$ and the formula $\psi = \Box(p_1 \vee p_2)$ with $\mathcal{O}(p_1) = [0, +\infty)$ and $\mathcal{O}(p_2) = (-\infty, 0]$. Clearly, $\mathcal{L}(\psi) = \mathbb{R}^{\mathbb{R}_{\geq 0}}$, i.e., the formula is valid, and, thus, $\mathbf{Dist}_\rho(s, \mathcal{L}(\psi)) = +\infty$. However, $[\![\psi]\!]_C(s) = \bigsqcap_{t\geq 0} ([\![p_1]\!]_C(s,t) \sqcup [\![p_2]\!]_C(s,t)) = \bigsqcap_{t\geq 0} (0 \sqcup 0) = 0$.*

These undesirable effects can be minimized or even avoided if we understand how equality breaks. Generally speaking, the strict inequality between the robustness estimate and robustness degree manifests itself in four distinct ways: (i) at the level of the atomic propositions, e.g., $p_1 \vee p_2$, (ii) due to the existence of tautologies in the formula, e.g., $p \vee \neg p$, (iii) when we consider disjuncts of MTL subformulas, e.g., $\phi_1 \vee \phi_2$, and more importantly, (iv) due to the supremum operator in the semantics of the until temporal operator. The mathematical principle that is behind the above four cases is the fact that the distance of a point from the intersection of two sets is not equal to the maximum of the distance of the point from each set [42]. The details of how this is manifested in the relationship between the robustness degree and the robustness estimate can be found in the proof of Theorem 13 in Appendix A.

However, some applications (see for example [15]) might benefit from specifications ϕ in MTL for which the equality holds, that is,

$$[\![\phi]\!]_C(s) = \mathbf{Dist}_\rho(s, \mathcal{L}(\phi)). \tag{3}$$

The following result indicates a fragment of MTL for which equality (3) holds. This fragment includes only formulas in NNF which are built using only the conjunction and always operators. Note that we have not imposed any conditions on the metric d, the set $\mathcal{F}(R, X)$ or the topology of the sets $\mathcal{O}(p)$.

Proposition 19 *Consider a formula $\phi \in MTL^+_{\mathbb{B}}(\wedge, \Box_{\mathcal{I}})$, an observation map*

$\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ *and a signal* $s \in \mathcal{F}(R, X)$*, then for any* $t \in R$*,* $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$ *implies* $[\![\phi]\!]_C(s,t) = \mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi)) = \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi))$*.*

Since duality holds in our definition of the robust semantics, the next result is immediate.

Corollary 20 *Consider a formula* $\phi \in MTL^+_{\mathbb{B}}(\vee, \Diamond_{\mathcal{I}})$*, an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ *and a signal* $s \in \mathcal{F}(R, X)$*, then for any* $t \in R$*,* $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \bot$ *implies* $[\![\phi]\!]_C(s,t) = \mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi)) = -\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi))$*.*

Remark 21 *The results in Section 2 hold for any linearly ordered time domain and not just the real line. As it can be seen in the proofs in Appendix A, the only requirement is that the timing constraints* $\mathcal{I}$ *in a formula* ϕ *must refer to the same time domain as the domain of the signal* s*. For example, consider a discrete-time signal* $\sigma \in \mathcal{F}(N, X)$*, where* $N \subseteq \mathbb{N}$*, and the formula* $\Diamond_{[1,3]} p_1$*. In this case, the timing constraints* $[1, 3]$ *refer to the discrete-time domain of* σ *where the time now counts clock ticks or samples instead of real time.*

3 Revisiting Robustness for Discrete-Time Signals

Physical world processes evolve in real time and, hence, the requirements for such systems must be specified in continuous-time formalisms as well. However, in virtually all the practical cases, the representation of the behavior of such systems that is available to us for analysis is in discrete-time. For example when we monitor the temperature in a room, we cannot know the value of the continuous-time signal at all points in time, but only at those points in time that are attainable through an analog-to-digital converter. This is also true when we test, simulate or verify a continuous-time signal using a digital computer. Some form of discretization of time is always necessary.

As briefly mentioned in the previous section, the robustness degree and the robustness estimate can be defined for signals whose domain is any linearly ordered time flow. Therefore, it is possible to define a signal over the natural numbers and perform discrete-time temporal logic analysis over that. However, the timing constraints in this case refer to the number of samples taken from the continuous-time signal and not to the actual real-time constraints. When the sampling step is constant, then there exists a simple conversion between the number of samples and the time that they were taken. But it is not always the case that the sampling step is constant and, moreover, the user often needs to provide real-time requirements on the signal which refer to the actual evolution of time and not the number of samples.

Hence, in this section we introduce and use *timed state sequences* (TSSs) as

models for the discrete-time representation of signals that also maintain the required timing information. TSSs are a widely accepted model for reasoning about real time systems [4]. The goal of this section is to briefly revisit the results of the previous section and reintroduce them using TSSs.

3.1 Timed State Sequences in Metric Spaces

A *discrete-time signal* σ can represent computer simulated trajectories of physical models or the sampling process that takes place when we digitally monitor physical systems. Informally, a discrete-time signal σ is a sequence of snapshots of the continuous-time behaviour of a system. Each such snapshot represents the state of the system at a particular point in time (see Fig. 6). However, as explained earlier a discrete-time signal does not provide us with any timing information. In order to reason about the timing properties of a discrete-time signal, we introduce the *timing function* τ. The role of the timing function is to pair each snapshot with a time stamp.

More formally, we define a discrete-time signal σ to be a function from the set $\mathcal{F}(N, X)$. Such a signal can be of bounded or unbounded duration. In the former case we set $N = \mathbb{N}_{\leq n}$ for some $n \in \mathbb{N}$, while in the latter $N = \mathbb{N}$. In the following, we fix $N \subseteq \mathbb{N}$ to be the domain of the discrete-time signal. Analogously, a timing function τ is a member of the set $\mathcal{F}(N, \mathbb{R}_{\geq 0})$. Two important restrictions on a timing function τ are

(1) τ must be a strictly increasing function, i.e., $\tau(i) < \tau(j)$ for $i < j$.
(2) if $\mathbf{dom}(\tau)$ is an infinite set, then τ must diverge, i.e., $\lim_{i \to +\infty} \tau(i) = +\infty$.

We denote the set of strictly increasing functions from $\mathbb{N}$ to $\mathbb{R}_{\geq 0}$ which diverge by $\mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$. Of particular interest to us are the timing functions for which the time difference between any two consecutive timestamps is constant. That is, for each timing function τ in this class there exists some constant $\alpha \in \mathbb{R}_{>0}$ such that $\tau(i) = \alpha i$ for $i \in N$. We will denote the set of such functions from N to $\mathbb{R}_{\geq 0}$ by $\mathcal{F}_c^{\uparrow}(N, \mathbb{R}_{\geq 0}) \subseteq \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, where c stands for constant.

By pairing a discrete-time signal σ with a timing function τ, we define what is usually referred to as a *timed state sequence* $\mu = (\sigma, \tau)$, i.e., $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$. In the following, we let $\mu^{(1)}$ be the first member of the pair, i.e., $\mu^{(1)} = \sigma$, and $\mu^{(2)}$ be the second member of the pair, i.e., $\mu^{(2)} = \tau$. Notice that the pair $(\mathcal{O}^{-1} \circ \sigma, \tau)$ is actually a Boolean-valued timed state sequence, which is a widely accepted model for reasoning about real time systems [4,45].

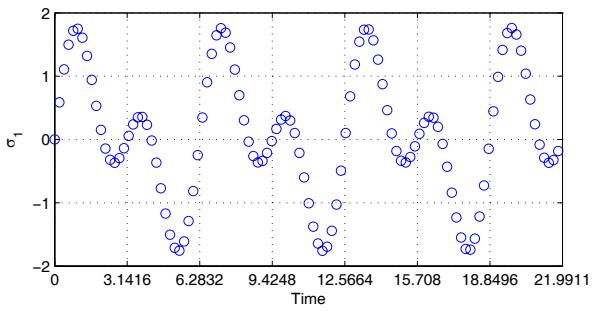

Fig. 6. A discrete-time signal $\sigma_1(i) = \sin \tau_1(i) + \sin 2\tau_1(i)$ where the timing function is $\tau_1(i) = 0.2i$.

3.2 Metric Temporal Logic over Timed State Sequences

We proceed on to define MTL semantics over timed state sequences. Again, the semantics is defined using a valuation function. Given a TSS μ, we write $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \top$ when μ satisfies the formula ϕ at moment 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 μ as a *model* of ϕ and we write $\langle\!\langle \phi \rangle\!\rangle_D(\mu) = \top$. In the definition below, we also use the following notation : for $P \subseteq \mathbb{R}_{\geq 0}$, the *preimage* of P under τ is defined as : $\tau^{-1}(P) := \{i \in N \mid \tau(i) \in P\}$.

Definition 22 (DT Semantics of MTL) *Let $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$ and $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, then the discrete-time semantics of any formula $\phi \in MTL_{\mathbb{B}}$ is defined recursively as follows*

$$
\begin{aligned}
\langle\!\langle \top \rangle\!\rangle_D(\mu, i) &:= \top \\
\langle\!\langle p \rangle\!\rangle_D(\mu, i) &:= K_{\in}(\sigma(i), \mathcal{O}(p)) \\
\langle\!\langle \neg\phi_1 \rangle\!\rangle_D(\mu, i) &:= \neg\langle\!\langle \phi_1 \rangle\!\rangle_D(\mu, i) \\
\langle\!\langle \phi_1 \vee \phi_2 \rangle\!\rangle_D(\mu, i) &:= \langle\!\langle \phi_1 \rangle\!\rangle_D(\mu, i) \sqcup \langle\!\langle \phi_2 \rangle\!\rangle_D(\mu, i) \\
\langle\!\langle \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2 \rangle\!\rangle_D(\mu, i) &:= \bigsqcup_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big(\langle\!\langle \phi_2 \rangle\!\rangle_D(\mu, j) \sqcap \bigsqcap_{i<k<j} \langle\!\langle \phi_1 \rangle\!\rangle_D(\mu, k) \Big)
\end{aligned}
$$

where $i, j, k \in N$, $\sigma = \mu^{(1)}$, $\tau = \mu^{(2)}$ and $K_{\in}$ is the characteristic function of the $\in$ relation.

We denote by $TSS_i(\phi) = \{\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0}) \mid \langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \top\}$ the set of all timed state sequences that satisfy ϕ at time i. Then, $TSS(\phi) = TSS_0(\phi)$ is the set of all timed state sequences that are models of ϕ. In this work, we are not interested in all the discrete-time models of ϕ, but only in those that have the same timing function τ with the input timed state sequence μ. This is because we are not interested in studying the robustness of the input timed state sequence with respect to its timing constraints as it is done in [6,32], but with respect to the constraints imposed on the value of

the signal by the atomic propositions.

Since we only consider models with the same timing function, we can ignore the timing function altogether and use the corresponding discrete-time signal when we define the robustness degree of a timed state sequence μ. Therefore, we define the set $\mathcal{L}_i^\tau(\phi) = \{\sigma \in \mathcal{F}(N, X) \mid (\sigma, \tau) \in TSS_i(\phi)\}$. Since $\mu \notin TSS_i(\phi)$ if and only if $\mu \in TSS_i(\neg\phi)$, we also get that $\sigma \notin \mathcal{L}_i^\tau(\phi)$ if and only if $\sigma \in \mathcal{L}_i^\tau(\neg\phi)$ for $\sigma = \mu^{(1)}$. Hence, $\mathcal{L}_i^\tau(\neg\phi) = \mathcal{F}(N, X) \backslash \mathcal{L}_i^\tau(\phi)$.

3.3 Robustness Degree for Discrete-Time Signals

Similar to the continuous-time case, we define a metric for the discrete-time signals. Let σ and σ' be discrete-time signals in $\mathcal{F}(N, X)$, then

$$\hat{\rho}(\sigma, \sigma') = \sup_{i \in N} \{d(\sigma(i), \sigma'(i))\} \tag{4}$$

is a metric on the set $\mathcal{F}(N, X) = X^N$. The formulation of the robustness degree for the discrete-time case is straightforward.

Definition 23 (DT Robustness Degree) *Let $\phi \in MTL_{\mathbb{B}}$ be a formula, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ be an observation map and $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^\uparrow(N, \mathbb{R}_{\geq 0})$ be a timed state sequence, then $\mathbf{Dist}_{\hat{\rho}}(\sigma, \mathcal{L}_i^\tau(\phi))$, where $\sigma = \mu^{(1)}$ and $\tau = \mu^{(2)}$, is the discrete-time robustness degree of μ with respect to ϕ at time $i \in N$ and $\mathbf{Dist}_{\hat{\rho}}(\sigma, \mathcal{L}^\tau(\phi))$ is the discrete-time robustness degree of μ with respect to ϕ.*

As before, the following proposition is derived directly from the definitions.

Proposition 24 *Let $\phi \in MTL_{\mathbb{B}}$ be an MTL formula, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ be an observation map and $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^\uparrow(N, \mathbb{R}_{\geq 0})$ be a timed state sequence. Also, let $\sigma = \mu^{(1)}$ and $\tau = \mu^{(2)}$. If $\varepsilon = \mathbf{Dist}_{\hat{\rho}}(\sigma, \mathcal{L}_i^\tau(\phi)) \neq 0$ for some $i \in N$, then for all $\mu' = (\sigma', \tau)$ such that $\sigma' \in B_{\hat{\rho}}(\sigma, |\varepsilon|)$, we have $\langle\!\langle \phi \rangle\!\rangle_D(\mu', i) = \langle\!\langle \phi \rangle\!\rangle_D(\mu, i)$.*

A major advantage of the discrete-time robustness, when compared to the continuous-time case, is that now the set $\mathcal{L}^\tau(\phi)$ can be computed when $N = \mathbf{dom}(\tau)$ is a finite set. In [45], it was proven that one can construct an acceptor $\mathcal{A}_\phi$ (in the form of a timed alternating automaton with one clock) for the finite models of any formula ϕ in the logic MTL with point-based semantics. Assume now that we are given an MTL formula $\phi \in MTL_{\mathbb{B}}$ and a timing function $\tau \in \mathcal{F}^\uparrow(N, \mathbb{R}_{\geq 0})$. For that particular τ, we can find the set $TSS^\tau(\mathcal{A}_\phi)$ of all timed state sequences (or timed words) (w, τ) with $w \in \mathcal{F}(N, \mathcal{P}(AP))$ that are accepted by $\mathcal{A}_\phi$. One way to do so is to construct the set W of all possible untimed words w of length $|N|$, that is $W = \mathcal{F}(N, \mathcal{P}(AP))$, and, then, for each $w \in W$ verify whether (w, τ) is accepted by $\mathcal{A}_\phi$, i.e., whether

$(w,\tau) \in TSS^{\tau}(\mathcal{A}_{\phi})$. From the set $TSS^{\tau}(\mathcal{A}_{\phi})$, we can easily derive the set

$$\mathcal{L}^{\tau}(\phi) = \bigcup_{(w,\tau)\in TSS^{\tau}(\mathcal{A}_{\phi})} \prod_{i\in N} \left(\bigcap_{p\in w(i)} \mathcal{O}(p) \cap \bigcap_{p\in AP\setminus w(i)} X\setminus\mathcal{O}(p) \right).$$

The following example illustrates the concept of robustness for temporal logic formulas interpreted over finite (timed) state sequences.

Example 25 *Assume that we are given the LTL specification $\phi = p_1 \mathcal{U} p_2$ such that $\mathcal{O}(p_1) = [1,2] \subseteq \mathbb{R}$ and $\mathcal{O}(p_2) = [0,1) \subseteq \mathbb{R}$. Note that the sets $\mathcal{O}(p_1)$ and $\mathcal{O}(p_2)$ are disjoint. Consider now two timed state sequences $\mu_1 = (\sigma_1, \tau)$ and $\mu_2 = (\sigma_2, \tau)$ with time domain $N = \{0,1\}$ taking values in $\mathbb{R}$ such that $\sigma_1(0) = 1$, $\sigma_1(1) = 0.5$ and $\sigma_2(0) = 1.7$, $\sigma_2(1) = 1.3$. In this simple case, we can compute the set $\mathcal{L}^{\tau}(\phi)$ with the procedure described above. The four untimed words that generate non-empty sets and satisfy the specification ϕ are $w_1 = (\{p_2\},\{p_1\})$, $w_2 = (\{p_2\},\{p_2\})$, $w_3 = (\{p_2\},\emptyset)$ and $w_4 = (\{p_1\},\{p_2\})$. Hence, we get $\mathcal{L}^{\tau}(\phi) = \mathcal{O}(p_2)\times\mathcal{O}(p_1) \cup \mathcal{O}(p_2)\times\mathcal{O}(p_2) \cup \mathcal{O}(p_2)\times X\setminus(\mathcal{O}(p_1)\cup\mathcal{O}(p_2)) \cup \mathcal{O}(p_1)\times\mathcal{O}(p_2) = [0,1)\times\mathbb{R} \cup [1,2]\times[0,1)$. Therefore, $\varepsilon_1 = \mathbf{Dist}_{\hat{\rho}}(\sigma_1, \mathcal{L}^{\tau}(\phi)) = 0.5$ and $\varepsilon_2 = \mathbf{Dist}_{\hat{\rho}}(\sigma_2, \mathcal{L}^{\tau}(\phi)) = -0.3$.*

3.4 Robustness Estimate for Timed State Sequences

The aforementioned theoretical construction of the set $\mathcal{L}^{\tau}(\phi)$ cannot be of significant practical interest. Moreover, the definition of robustness degree involves a number of set operations (union, intersection and complementation) in the possibly high dimensional spaces X and $\mathcal{F}(N,X)$, which can be computationally expensive in practice. Fortunately, the discrete-time robust semantics of MTL can provide us with a feasible method for under-approximating the robustness degree of (finite) timed state sequences.

Definition 26 (DT Robust Semantics) *Let $\mu \in \mathcal{F}(N,X) \times \mathcal{F}^{\uparrow}(N,\mathbb{R}_{\geq 0})$, $c \in \overline{\mathbb{R}}$ and $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, then the discrete-time robust semantics of any formula $\phi \in MTL_{\overline{\mathbb{R}}\cup\mathbb{B}}$ with respect to μ is recursively defined as follows*

$$\begin{aligned}
[\![\top]\!]_D(\mu,i) &:= +\infty \\
[\![c]\!]_D(\mu,i) &:= c \\
[\![p]\!]_D(\mu,i) &:= \mathbf{Dist}_d(\sigma(i), \mathcal{O}(p)) \\
[\![\neg\phi_1]\!]_D(\mu,i) &:= -[\![\phi_1]\!]_D(\mu,i) \\
[\![\phi_1 \vee \phi_2]\!]_D(\mu,i) &:= [\![\phi_1]\!]_D(\mu,i) \sqcup [\![\phi_2]\!]_D(\mu,i) \\
[\![\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2]\!]_D(\mu,i) &:= \bigsqcup_{j\in\tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_D(\mu,j) \sqcap \bigsqcap_{i<k<j} [\![\phi_1]\!]_D(\mu,k) \Big)
\end{aligned}$$

where $i, j, k \in N$, $\sigma = \mu^{(1)}$ *and* $\tau = \mu^{(2)}$.

Similar to the continuous-time robust semantics, the following results hold.

Lemma 27 *Given an MTL formula* $\phi \in MTL_{\mathbb{B}}$, *an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, *a timed state sequence* $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$ *and some time instant* $i \in N$, *we have* $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \langle\!\langle \mathbf{nnf}(\phi) \rangle\!\rangle_D(\mu, i)$ *and* $[\![\phi]\!]_D(\mu, i) = [\![\mathbf{nnf}(\phi)]\!]_D(\mu, i)$.

Again, the robust semantics evaluate to the radius of a robust neighborhood.

Theorem 28 *Given an MTL formula* $\phi \in MTL_{\mathbb{B}}$, *an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ *and a timed state sequence* $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, *then for any* $i \in N$, *we have* $-\mathbf{dist}_{\hat{\rho}}(\mu^{(1)}, \mathcal{L}_i^{\tau}(\phi)) \leq [\![\phi]\!]_D(\mu, i) \leq \mathbf{depth}_{\hat{\rho}}(\mu^{(1)}, \mathcal{L}_i^{\tau}(\phi))$.

Corollary 29 *Given an MTL formula* $\phi \in MTL_{\mathbb{B}}$, *an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ *and a timed state sequence* $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, *let* $\sigma = \mu^{(1)}$ *and* $\tau = \mu^{(2)}$. *If for some* $i \in N$, *we have* $\varepsilon = [\![\phi]\!]_D(\mu, i) \neq 0$, *then for all* $\mu' = (\sigma', \tau)$ *such that* $\sigma' \in B_{\hat{\rho}}(\sigma, |\varepsilon|)$ *we have* $\langle\!\langle \phi \rangle\!\rangle_D(\mu', i) = \langle\!\langle \phi \rangle\!\rangle_D(\mu, i)$.

Moreover, the relationship between robust and Boolean semantics in discrete-time is maintained.

Proposition 30 *For an MTL formula* $\phi \in MTL_{\mathbb{B}}$, *an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, *a timed state sequence* $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$ *and some time instant* $i \in N$, *the following two results hold*

(1) $[\![\phi]\!]_D(\mu, i) > 0 \Rightarrow \langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \top$ *and* $[\![\phi]\!]_D(\mu, i) < 0 \Rightarrow \langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \bot$
(2) $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \top \Rightarrow [\![\phi]\!]_D(\mu, i) \geq 0$ *and* $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \bot \Rightarrow [\![\phi]\!]_D(\mu, i) \leq 0$

Finally, we close this section by restating Proposition 19 and Corollary 20 for discrete-time semantics.

Proposition 31 *Consider a formula* $\phi \in MTL^{+}_{\mathbb{B}}(\wedge, \Box_{\mathcal{I}})$, *an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ *and a timed state sequence* $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, *then for any* $i \in N$, $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \top$ *implies* $[\![\phi]\!]_D(\mu, i) = \mathbf{Dist}_{\hat{\rho}}(\sigma, \mathcal{L}_i^{\tau}(\phi)) = \mathbf{depth}_{\hat{\rho}}(\sigma, \mathcal{L}_i^{\tau}(\phi))$, *where* $\sigma = \mu^{(1)}$ *and* $\tau = \mu^{(2)}$.

Corollary 32 *Consider a formula* $\phi \in MTL^{+}_{\mathbb{B}}(\vee, \Diamond_{\mathcal{I}})$, *an observation map* $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ *and a timed state sequence* $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, *then for any* $i \in N$, $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \bot$ *implies* $[\![\phi]\!]_D(\mu, i) = \mathbf{Dist}_{\hat{\rho}}(\sigma, \mathcal{L}_i^{\tau}(\phi)) = -\mathbf{dist}_{\hat{\rho}}(\sigma, \mathcal{L}_i^{\tau}(\phi))$, *where* $\sigma = \mu^{(1)}$ *and* $\tau = \mu^{(2)}$.

In this section, we present a procedure that computes the robustness estimate of a finite timed state sequence μ with respect to a specification ϕ stated in the Metric Temporal Logic. For this purpose, we design a monitoring algorithm based on the robust semantics of MTL. This algorithm has been implemented and it is distributed on-line as the software toolbox TaLiRo [20].

Similar to the monitoring algorithm in [54], we start from the definition of the robust semantics of the strict non-matching until operator and using the distributive law, we can derive an equivalent formulation (see Appendix B.1). In the following, consider a timed state sequence μ and let $\tau = \mu^{(2)}$, $\delta\tau(i) = \tau(i+1)-\tau(i)$ and $K_{\in}^{\infty}(a, A) = +\infty$ if $a \in A$ and $-\infty$ otherwise. If $i < \mathbf{dom}(\tau)$, then

$$[\![\phi_1 \,\mathcal{U}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) = (K_{\in}^{\infty}(0, \mathcal{I}) \sqcap [\![\phi_2]\!]_D(\mu, i)) \sqcup [\![\phi_1 \overleftarrow{\mathcal{U}}_{(-\delta\tau(i))+_R\mathcal{I}} \phi_2]\!]_D(\mu, i+1)$$

otherwise $[\![\phi_1 \,\mathcal{U}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) = K_{\in}^{\infty}(0, \mathcal{I}) \sqcap [\![\phi_2]\!]_D(\mu, i)$. Similarly, we can derive the recursive formulation of the non-strict non-matching until temporal operator. If $i < \mathbf{dom}(\tau)$, then $[\![\phi_1 \overleftarrow{\mathcal{U}}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) =$

$$(K_{\in}^{\infty}(0, \mathcal{I}) \sqcap [\![\phi_2]\!]_D(\mu, i)) \sqcup ([\![\phi_1]\!]_D(\mu, i) \sqcap [\![\phi_1 \overleftarrow{\mathcal{U}}_{(-\delta\tau(i))+_R\mathcal{I}} \phi_2]\!]_D(\mu, i+1))$$

otherwise $[\![\phi_1 \overleftarrow{\mathcal{U}}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) = K_{\in}^{\infty}(0, \mathcal{I}) \sqcap [\![\phi_2]\!]_D(\mu, i)$.

Using the above recursive definitions, it is easy to derive Algorithm 1 that returns the robustness estimate of a given finite timed state sequence μ with respect to an MTL formula ϕ. Algorithm 2 is the core of the monitoring procedure. It takes as input the temporal logic formula ϕ, the current state $\sigma(i)$ and the time period before the next state occurs, it evaluates the part of the formula that must hold on the current state and returns the formula that has to hold at the next state of the timed state sequence.

In order to avoid the introduction of additional connectives in our logic that would unnecessarily increase the length of this paper, we have presented Algorithm 2 as merely a rewriting procedure on the input formula ϕ. This implies that the procedure Monitor would return a Boolean combination ψ of numbers from $\overline{\mathbb{R}}$. Then, the robustness estimate would simply be $[\![\psi, \mathcal{O}]\!]_D(\mu)$. For example, if $\psi = \wedge_{a\in A} \vee_{b\in B_a} c_{ab}$ with $c_{ab} \in \overline{\mathbb{R}}$, then $[\![\psi, \mathcal{O}]\!]_D(\mu) = \sqcap_{a\in A} \sqcup_{b\in B_a} c_{ab}$. In an implementation of the algorithm, the following simplifications must be performed at each call of Algorithm 2 : $\varepsilon_1 \vee \varepsilon_2$ is replaced by $\varepsilon = \varepsilon_1 \sqcup \varepsilon_2$, $\neg\varepsilon$ is replaced by $-\varepsilon$ and, also, $\phi \wedge +\infty \equiv \phi$, $\phi \vee -\infty \equiv \phi$, $\phi \vee +\infty \equiv +\infty$ and $\phi \wedge -\infty \equiv -\infty$.

The following lemma is immediate since the formulation of until in Algorithm

Algorithm 1 Monitoring the Robustness of Timed State Sequences

Input: An MTL formula ϕ, a finite timed state sequence $\mu = (\sigma, \tau)$ and an observation map $\mathcal{O}$

Output: The formula's robustness estimate

procedure MONITOR($\phi, \mu, \mathcal{O}$)
  $i \leftarrow 0$
  while $\phi \neq \varepsilon \in \overline{\mathbb{R}}$ **do** ▷ ϕ has not been reduced to a value
    if $i < \max \mathbf{dom}(\tau)$ **then** $\phi \leftarrow$ DERIVE($\phi, \sigma(i), \tau(i+1) - \tau(i), \bot, \mathcal{O}$)
    else $\phi \leftarrow$ DERIVE($\phi, \sigma(i), 0, \top, \mathcal{O}$)
    end if
    $i \leftarrow i + 1$
  end while
end procedure

Algorithm 2 Deriving the Future

Input: The MTL formula ϕ, the current value of the signal x, the time period δt before the next value in the signal, a variable *last* indicating whether the next state is the last and the observation map $\mathcal{O}$

Output: The MTL formula ϕ that has to hold at the next moment in time

procedure DERIVE($\phi, x, \delta t, last, \mathcal{O}$)
  if $\phi = \top$ **then return** $+\infty$
  else if $\phi = \varepsilon \in \overline{\mathbb{R}}$ **then return** ε
  else if $\phi = p \in AP$ **then return** $\mathbf{Dist}_d(x, \mathcal{O}(p))$
  else if $\phi = \neg\phi_1$ **then return** $\neg$DERIVE($\phi_1, x, \delta t, last, \mathcal{O}$)
  else if $\phi = \phi_1 \vee \phi_2$ **then**
    return DERIVE($\phi_1, x, \delta t, last, \mathcal{O}$)$\vee$DERIVE($\phi_2, x, \delta t, last, \mathcal{O}$)
  else if $\phi = \phi_1 \, \mathcal{U}_{\mathcal{I}} \phi_2$ **then**
    $\alpha \leftarrow K_{\in}^{\infty}(0, \mathcal{I}) \wedge$DERIVE($\phi_2, x, \delta t, last, \mathcal{O}$)
    if $last = \top$ **then return** α
    else return $\alpha \vee (\phi_1 \overleftarrow{\mathcal{U}}_{(-\delta t) +_R \mathcal{I}} \phi_2)$
    end if
  else if $\phi = \phi_1 \overleftarrow{\mathcal{U}}_{\mathcal{I}} \phi_2$ **then**
    $\alpha \leftarrow K_{\in}^{\infty}(0, \mathcal{I}) \wedge$DERIVE($\phi_2, x, \delta t, last, \mathcal{O}$)
    if $last = \top$ **then return** α
    else return $\alpha \vee ($DERIVE$(\phi_1, x, \delta t, last, \mathcal{O}) \wedge \phi_1 \overleftarrow{\mathcal{U}}_{(-\delta t) +_R \mathcal{I}} \phi_2)$
    end if
  end if
end procedure

2 is equivalent with the robust interpretation of until in Definition 26.

Lemma 33 *Given an MTL formula $\phi \in MTL_{\mathbb{B}}$, a map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ and a finite timed state sequence $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, then for any $i < \max N$ we have $[\![\phi]\!]_D(\mu, i) = [\![$DERIVE$(\phi, \sigma(i), \delta\tau(i), \bot, \mathcal{O})]\!]_D(\mu, i+1)$, where $\sigma = \mu^{(1)}$, $\tau = \mu^{(2)}$ and $N = \mathbf{dom}(\tau)$.*

Using Lemma 33 and the fact that the temporal operators are eliminated from ϕ when $last = \top$, we derive the following theorem as corollary.

Theorem 34 *Given an MTL formula $\phi \in MTL_{\mathbb{B}}$, a map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ and a finite timed state sequence $\mu \in \mathcal{F}(N, X) \times \mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$, then $[\![\phi]\!]_D(\mu) = [\![\textsc{Monitor}(\phi, \mu, \mathcal{O})]\!]_D(\mu)$.*

The theoretical complexity of the Boolean-valued monitoring algorithms has been studied in the past for both the Linear [41] and the Metric Temporal Logic [54]. Practical algorithms for monitoring of Boolean-valued finite timed state sequences using rewriting have been developed by several authors [26,37].

Essentially, the new part in Algorithm 2 - when compared with Boolean monitoring - is the evaluation of the atomic propositions. How easy is to compute the signed distance? When the set X is just $\mathbb{R}$, the set S is an interval and the metric d is the function $d(x, y) = |x - y|$, then the problem reduces to finding the minimum of two values. For example, if $S = [a, b] \subseteq \mathbb{R}$ and $x \in S$, then $\mathbf{Dist}_d(x, S) = \min\{|x - a|, |x - b|\}$. When the set X is $\mathbb{R}^n$, $S \subseteq \mathbb{R}^n$ is a convex set and the metric d is the Euclidean distance, i.e., $d(x, y) = \|x - y\| = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$, then we can calculate the distance ($\mathbf{dist}_d$) by solving very efficient convex optimization problems. If, in addition, the set S is just a halfspace $S = \{x \mid a^T x \leq b\}$, then there exists an analytical solution : $\mathbf{dist}_d(x, S) = |b - a^T x|/\|a\|$ if $a^T x > b$ and 0 if $a^T x \leq b$. Moreover, if the set S a is concave set defined by a finite union of halfspaces S_i, i.e., $S = \cup_{i \in I} S_i$, then the distance of a point x from S is simply $\mathbf{dist}_d(x, S) = \min_{i \in I} \mathbf{dist}_d(x, S_i)$. Similar results hold for ellipsoidal sets. For further details on such distance computation problems see [8, §8].

The theoretical complexity of Algorithm 1 is an open problem which we plan to address in the future. Note however that the theoretical running times of convex optimization algorithms are only approximate (see Part III in [8]) and, thus, they do not capture the efficient running times of actual practical implementations. Nevertheless, it is immediate that the theoretical complexity of Algorithm 1 cannot be easier than the complexity of the Boolean monitoring algorithms in [41,54].

4 Continuous-Time Satisfiability by Discrete-Time Reasoning

The discrete-time robust semantics for MTL formulas have at least one important application. Given a continuous-time signal s and a timed state sequence $\mu = (\sigma, \tau)$ such that $\sigma = s \circ \tau$, we can determine the relationship between $\langle\!\langle \phi \rangle\!\rangle_C(s)$ and $\langle\!\langle \phi \rangle\!\rangle_D(\mu)$. This is an important problem since the timing (or

better the *sampling*) function[2] τ may not just change the satisfiability of a formula ϕ with respect to a signal s, but also the validity of the formula [48]. In Section 4.2, we develop conditions for the sampling function τ which can guarantee the equality $\langle\langle\phi\rangle\rangle_D(\mu) = \langle\langle\phi\rangle\rangle_C(s)$ for MITL formulas. Another important question that arises especially in testing and verification (see for example [15]) is whether we can use the discrete-time robustness estimate in order to infer the value of the continuous-time robustness estimate of the underlying continuous-time signal. This problem is addressed in Section 4.3 for clMTL formulas. But first, we present a condition on the dynamics of the signals in the set $\mathcal{F}(R, X)$ which is required for the solution of both problems.

4.1 Bounds on the Signal Values

In order to reason about the behavior of continuous-time signals using discrete-time methods, we need to derive conservative bounds on the divergence of the value of a signal s between two consecutive samples (for example 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 35 *The signals in the set $\mathcal{F}(R, X)$ satisfy the condition*

$$\forall t, t' \in R \,.\, d(s(t), s(t')) \leq \mathcal{E}(|t - t'|), \tag{5}$$

where $\mathcal{E} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a positive nondecreasing function.

Notice that in (5) 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*:

$$\Delta\tau = \sup_{i \in N_{>0}} \{\tau(i) - \tau(i-1)\}. \tag{6}$$

If, moreover, the sampling function τ has a constant sampling rate α, then $\Delta\tau = \alpha$. Thus, in this case the control parameter becomes the sampling rate α. In the next two sections, we develop conditions for $\Delta\tau$ for two different fragments of MTL.

[2] Now, the timing function represents something more concrete. It returns the points in time at which we have sampled the continuous-time signal. Hence, in this section, we refer to the timing function as *sampling function* and we assume that it is a member of the set $\mathcal{F}^{\uparrow}(N, R)$ instead of $\mathcal{F}^{\uparrow}(N, \mathbb{R}_{\geq 0})$.

One of the main issues that arise when one tries to employ discrete-time methods in order to determine the satisfiability of a temporal logic formula over a continuous-time signal is that the relationship between valid formulas in continuous and sampled semantics is not always maintained [48]. 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 $[1, 2]$. This issue can be addressed through the sampling function τ, which essentially implies that we must impose conditions on the the maximum sampling step $\Delta\tau$. But first, a slight modification of the timing constraints of the temporal operators is required.

In order to modify the timing constraints of the temporal operators in a consistent way, we must convert the input formula $\phi \in MTL_{\mathbb{B}}$ into Negation Normal Form (NNF). In the following we assume that the input formula is given directly in NNF. Similar to [32], we strengthen MTL formulas by changing the timing requirements of a given formula ϕ. In addition, we convert the strict temporal operators to their corresponding non-strict versions. In detail, we introduce a function $\mathbf{str}_{\Delta\tau} : MTL^{+}_{\mathbb{B}} \rightarrow MTL^{+}_{\mathbb{B}}$ that recursively operates on a formula ϕ and modifies the temporal operators as follows

$$\mathbf{str}_{\Delta\tau}(\phi_1 \,\mathcal{U}_{\mathcal{I}} \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \,\overleftarrow{\mathcal{U}}_{C(\mathcal{I},\Delta\tau)}\, \mathbf{str}_{\Delta\tau}(\phi_2)$$
$$\mathbf{str}_{\Delta\tau}(\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \,\overleftarrow{\mathcal{R}}_{E(\mathcal{I},\Delta\tau)}\, \mathbf{str}_{\Delta\tau}(\phi_2)$$

while keeping the atomic propositions and constants the same, i.e., $\mathbf{str}_{\Delta\tau}(\top) = \top$, $\mathbf{str}_{\Delta\tau}(\bot) = \bot$, $\mathbf{str}_{\Delta\tau}(p) = p$, $\mathbf{str}_{\Delta\tau}(\neg p) = \neg p$, and simply recursing in the case of Boolean connectives, i.e., $\mathbf{str}_{\Delta\tau}(\phi_1 \vee \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \vee \mathbf{str}_{\Delta\tau}(\phi_2)$ and $\mathbf{str}_{\Delta\tau}(\phi_1 \wedge \phi_2) = \mathbf{str}_{\Delta\tau}(\phi_1) \wedge \mathbf{str}_{\Delta\tau}(\phi_2)$. In the above formulas, we use the operators $C(\mathcal{I}, \delta) = \{r \in R \mid cl(B_d(r, \delta)) \subseteq \mathcal{I}\}$ and $E(\mathcal{I}, \delta) = \{r \in R \mid cl(B_d(r, \delta)) \cap \mathcal{I} \neq \emptyset\}$. Informally, the operator $C(\mathcal{I}, \delta)$ contracts the interval $\mathcal{I}$ by δ, while the operator $E(\mathcal{I}, \delta)$ expands it by δ. The intuition behind the function $\mathbf{str}_{\Delta\tau}$ is that a robust specification with respect to the atomic propositions must also be robust with respect to the timing constraints. 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 $\tau(i) + \mathcal{I}$.

Proposition 36 *For any $\phi \in MTL^{+}_{\mathbb{B}}$, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ and $s \in \mathcal{F}(R, X)$, $\tau \in \mathcal{F}^{\uparrow}(N, R)$ such that $\mu = (s \circ \tau, \tau)$, we have that $\langle\!\langle \mathbf{str}_{\Delta\tau}(\phi) \rangle\!\rangle_D(\mu, i) = \top$ implies $\langle\!\langle \phi \rangle\!\rangle_D(\mu, i) = \top$.*

The next two assumptions guarantee the existence of at least one sampling point within each timing interval of the temporal operators.

Assumption 37 *Given a formula $\phi \in MTL^{+}_{\mathbb{B}}$, the sampling functions in the set $\mathcal{F}^{\uparrow}(N,R)$ satisfy the constraint:*

$$\Delta\tau < \min_{\mathcal{I}\in(\mathfrak{I}(\mathbf{str}_{\Delta\tau}(\phi))\cup\mathfrak{I}(\phi))}\{\sup\mathcal{I}-\inf\mathcal{I}\}. \tag{7}$$

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

In the assumption above, $\mathfrak{I}(\phi)$ denotes the set of all timing constraints $\mathcal{I}$ that appear in the temporal operators of an MTL 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 mandates the choice of the Metric Interval Temporal Logic (MITL) [3] as a specification language instead of MTL. MITL is a decidable fragment of MTL where the timing constraints $\mathcal{I}$ of the temporal operators are not allowed to be singleton sets, i.e., $\inf\mathcal{I} < \sup\mathcal{I}$. It is easy to see that with respect to the initial formula ϕ, Assumption 37 can be satisfied by the following constraint:

$$\Delta\tau < 1/3 \min_{\mathcal{I}\in\mathfrak{I}(\phi)}\{\sup\mathcal{I}-\inf\mathcal{I}\}. \tag{8}$$

Lemma 38 *Consider a formula $\phi \in MITL^{+}_{\mathbb{B}}$ and a sampling function $\tau \in \mathcal{F}^{\uparrow}(N,R)$ and let Assumption 37 hold. Let $\mathcal{I} \in \mathfrak{I}(\phi)$. If for some $i \in N$, $\tau(i)+\mathcal{I} \subseteq R$, then $\tau^{-1}(\tau(i)+\mathcal{I}) \neq \emptyset$.*

Whenever R is a bounded time interval, we have to impose additional constraints on the signal and the MITL formulas. That is, we require that all the intervals in $\mathfrak{I}(\phi)$ are bounded as it was initially suggested in [40]. This enables us to compute a minimum time $\mathbf{dur}(\phi)$ that guarantees in combination with Assumption 37 that there are no subformulas whose truth value was determined by the lack of sampling points. The computation of the minimum time $\mathbf{dur}(\phi)$ is performed recursively:

$$\begin{aligned}
\mathbf{dur}(\alpha) &:= 0 && \text{for } \alpha \in \{p, \neg p, \top, \bot\}\\
\mathbf{dur}(\phi_1 \sim \phi_2) &:= \mathbf{dur}(\phi_1) \sqcup \mathbf{dur}(\phi_2) && \text{for } \sim \in \{\wedge, \vee\}\\
\mathbf{dur}(\phi_1 \mathcal{W}_{\mathcal{I}} \phi_2) &:= \sup\mathcal{I} + \mathbf{dur}(\phi_1) \sqcup \mathbf{dur}(\phi_2) && \text{for } \mathcal{W} \in \{\mathcal{U}, \mathcal{R}\}
\end{aligned}$$

In particular, we would like to avoid the case where R is a bounded domain and $(t+\mathcal{I}) \cap R \neq \emptyset$, but $t+\mathcal{I} \not\subseteq R$ and there is no sample in $t +_R \mathcal{I}$.

Example 39 *Consider the sampling function $\tau(i) = 0.5i$, i.e., $\Delta\tau = 0.5$, and the formula $\phi = \Box_{[2.2,4.2]}p$. Let the domain of the signal s be $R = [0, 2.4]$, then $N = \{0,1,2,3,4\}$ and $\tau(N) = \{0, 0.5, 1, 1.5, 2\}$. Note that the constraints of Assumption 37 are satisfied, that is, $\Delta\tau < 1/3(4.2-2.2)$ and $\sup R - \tau(\max N) = 2.4 - 2 = 0.4 < \Delta\tau$. The formula $\Box_{[2.2,4.2]}p$ evaluates to $\top$ simply*

because $\tau^{-1}(0+[2.2,4.2]) = \tau^{-1}([2.2,4.2]) = \emptyset$. *However, over the time interval* $[2.2,2.4]$ *it might not be true that* s *satisfies* ϕ.

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 $\mathbf{dur}(\phi) < \sup R < +\infty$. 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 the temporal nesting depth of a formula ϕ is m and that a temporal subformula $\psi = \psi_1 \mathcal{W}_{\mathcal{I}_k} \psi_2$ of ϕ is at nesting depth k, where $\mathcal{W} \in \{\mathcal{U}, \mathcal{R}\}$. Let $\{\mathcal{I}_j\}_{m \geq j > k}$ be any sequence of timing constraints of nested temporal operators at higher nesting depths j than k. Informally, the temporal 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 **dur** where $\sup \mathcal{I}$ is replaced by 1. Then, for all $t \in [0, \sum_{j=k+1}^{m} \sup \mathcal{I}_j]$, we have $t + \mathcal{I}_k \subseteq R$ since $\sum_{j=k}^{m} \sup \mathcal{I}_j \leq \mathbf{dur}(\phi) < \sup R$. Therefore, $t + \mathcal{I}_k = t +_R \mathcal{I}_k$.

Example 40 *Let* $\phi = (p_1 \mathcal{U}_{[1,2]} p_2 \vee p_3 \mathcal{U}_{[3,4]} p_4) \mathcal{U}_{[4,6]} (p_5 \mathcal{U}_{[0,1]} p_6)$. *Then,* $\mathbf{dur}(\phi) = 10$ *and the temporal nesting depth of* ϕ *is* 2. *All the possible sequences of timing constraints of nested temporal operators are :* $\{[4,6],[1,2]\}$, $\{[4,6],[3,4]\}$ *and* $\{[4,6],[0,1]\}$. *Let* $\sup R > 10$ *and consider the sequence* $\{\mathcal{I}_2, \mathcal{I}_1\}$ *where* $\mathcal{I}_2 = [4,6]$ *and* $\mathcal{I}_1 = [1,2]$, *then at nesting depth* $k = 1$, *for all* $t \in [0, \sum_{j=2}^{2} \sup \mathcal{I}_j] = [0,6]$, *we have* $t + \mathcal{I}_1 = [t+1, t+2] \subseteq R$.

Assumption 41 *If the domain* R *of the set of signals* $\mathcal{F}(R,X)$ *is bounded, i.e.,* $\sup R < +\infty$, *then for the formula* $\phi \in MITL^{+}_{\mathbb{B}}$ *under consideration the following conditions must hold : for all* $\mathcal{I} \in \mathfrak{I}(\phi)$, *we have* $\sup \mathcal{I} < +\infty$ *and, also,* $\sup R > \mathbf{dur}(\mathbf{str}_{\Delta\tau}(\phi))$.

Lemma 42 *Consider a formula* $\phi \in MITL^{+}_{\mathbb{B}}$ *and a sampling function* $\tau \in \mathcal{F}^{\uparrow}(N,R)$ *and let Assumptions 37 and 41 hold. Let* $\psi = \psi_1 \mathcal{W}_{\mathcal{I}_k} \psi_2$, *where* $\mathcal{W} \in \{\mathcal{U}, \mathcal{R}\}$, *be a subformula of* $\mathbf{str}_{\Delta\tau}(\phi)$ *at nesting depth* k *and let* $\{\mathcal{I}_j\}_{k>j}$ *be any sequence of timing constraints of nested temporal operators at higher nesting depths* $j > k$. *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* $(\tau(i) +_R \mathcal{I}_k) = (\tau(i) + \mathcal{I}_k)$ *and* $\tau^{-1}(\tau(i) + \mathcal{I}_k) \neq \emptyset$.

The above assumptions enable us to prove the following theorem.

Theorem 43 *Consider* $\phi \in MITL^{+}_{\mathbb{B}}$, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, $s \in \mathcal{F}(R,X)$, $\tau \in \mathcal{F}^{\uparrow}(N,R)$ *and let Assumptions 35 to 41 hold. Then,* $[\![\mathbf{str}_{\Delta\tau}(\phi)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$ *with* $\mu = (s \circ \tau, \tau)$ *implies*

$$\forall t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R \,.\, \langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top \tag{9}$$

for any $i \in N$ *which satisfies the conditions of Lemma 42.*

We should remark that the conclusion (9) of Theorem 43 does not imply that

the continuous-time Boolean signal $\mathcal{O}^{-1} \circ s$ satisfies the finite variability property as it is defined in [31]. It only states that there exists some interval in R of length at least $2\Delta\tau$ such that the Boolean truth value of some atomic propositions remains constant. The following corollary is immediate from Theorem 43 and Propositions 30 and 36.

Corollary 44 *Consider $\phi \in MITL^{+}_{\mathbb{B}}$, $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, $s \in \mathcal{F}(R, X)$, $\tau \in \mathcal{F}^{\uparrow}(N, R)$ and let Assumptions 35–41 hold. Then, $[\![\mathbf{str}_{\Delta\tau}(\phi)]\!]_D(\mu) > \mathcal{E}(\Delta\tau)$ with $\mu = (s \circ \tau, \tau)$ implies $\langle\!\langle \phi \rangle\!\rangle_C(s) = \langle\!\langle \phi \rangle\!\rangle_D(\mu) = \top$.*

If the condition $[\![\mathbf{str}_{\Delta\tau}(\phi)]\!]_D(\mu) > \mathcal{E}(\Delta\tau)$ 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.

4.3 Sampling for clMTL Robustness

Corollary 44 provides sufficient conditions for MITL formulas for semantic equality between the two different time domains, i.e., $\langle\!\langle \phi \rangle\!\rangle_C(s) = \langle\!\langle \phi \rangle\!\rangle_D(\mu)$. Another interesting question is whether we can relate the continuous and discrete-time robustness estimates. This is possible, but more stringent conditions on the MTL formula and the sampling function are required. In detail, we have to impose a constant sampling rate on the sampling function and, moreover, the timing constraints on the temporal operators must be closed intervals and must have sampling instants as bounds. In other words, the logic that we consider in this section is clMTL. Since the timing constraints $\mathcal{I}$ of any clMTL formula have rational numbers as bounds, we can always find a common divisor α (or the greatest common divisor) and use it as a sampling constant. This sampling constant guarantees that the corresponding sampling function τ will always sample time instants that are at least on the boundaries of the required timing intervals. Examples of such signals and MTL specifications can be found in [20]. Note that in this case, we can allow punctual timing requirements, that is, $\mathcal{I}$ can be a singleton set.

Assumption 45 *Given a formula $\phi \in clMTL_{\mathbb{B}}$, we construct a sampling function $\tau \in \mathcal{F}^{\uparrow}_{c}(N, R)$ with constant sampling rate α, where α is a common divisor of all the finite bounds of the temporal operators in $\mathfrak{I}(\phi)$.*

The following result is immediate if we rewrite the bounds of the time intervals in $\mathfrak{I}(\phi)$ as multiples of the constant α (for example, $\mathcal{I} = [\alpha i_1, \alpha i_2]$ for some $i_1 \leq i_2 \in \mathbb{N}$) and define the sampling function τ to be $\tau(i) = \alpha i$ for $i \in N$.

Lemma 46 *Consider a formula $\phi \in clMTL_{\mathbb{B}}$ and a sampling function $\tau \in \mathcal{F}_c^{\uparrow}(N, R)$ which satisfies Assumption 45. If for some $i \in N$, we have $(\tau(i) + \mathcal{I}) \cap R \neq \emptyset$, then $\tau^{-1}(\tau(i) + \mathcal{I}) \neq \emptyset$.*

An implication of Lemma 46 is that if the signal s is of unbounded duration, i.e., $\sup R = +\infty$, then no other assumptions are required since we will always have enough sampling points in order to infer a robustness estimate for the formula. On the other hand, if the time domain of s is bounded, then we must impose additional constraints on the clMTL formula ϕ or the time domain R as in Section 4.2.

Assumption 47 *Let $\tau \in \mathcal{F}_c^{\uparrow}(N, R)$. If the time domain R of the set of signals $\mathcal{F}(R, X)$ is bounded, i.e., $\sup R < +\infty$, then for the formula $\phi \in clMTL_{\mathbb{B}}$ under consideration at least one of the following two conditions must hold:*

(1) For all $\mathcal{I} \in \mathfrak{I}(\phi)$, we have $\sup \mathcal{I} < +\infty$ and, also, $\sup R > \mathbf{dur}(\phi) + \Delta\tau$.
(2) For all $\mathcal{I} \in \mathfrak{I}(\phi)$, we have $\min \mathcal{I} = 0$.

Note that in the above assumption the second condition does not impose any requirements on the minimum duration of the continuous-time signal. Intuitively, the condition $0 \in \mathcal{I}$ guarantees that the set $\tau^{-1}(\tau(i)+\mathcal{I})$ for $i \in N$ always contains at least one sampling point, namely, i. Similar to Section 4.2, we can prove the following result.

Lemma 48 *Consider a formula $\phi \in clMTL_{\mathbb{B}}$ and a sampling function $\tau \in \mathcal{F}_c^{\uparrow}(N, R)$ which satisfy Assumptions 45 and 47. 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 $\{\mathcal{I}_j\}_{k>j}$ be any sequence of timing constraints of nested temporal operators at higher nesting depths $j > k$. 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 $\tau^{-1}(\tau(i) + \mathcal{I}_k) \neq \emptyset$ and, moreover, $\forall t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$ we have $t +_R \mathcal{I}_k \neq \emptyset$.*

Before we proceed to state the main result of this section, we need to define one more translation function that operates on MTL formulas. In detail, we define a new translation function $\mathbf{mtc} : MTL_{\mathbb{B}} \to MTL_{\mathbb{B}}$ that recursively operates on a formula ϕ and modifies the temporal operators as follows

$$\mathbf{mtc}(\phi_1 \, \mathcal{U}_{\mathcal{I}} \phi_2) = \mathbf{mtc}(\phi_1) \, \overleftrightarrow{\mathcal{U}}_{\mathcal{I}} \, \mathbf{mtc}(\phi_2)$$

Similar to the function $\mathbf{str}_{\Delta\tau}$, the Boolean connectives just recursively call **mtc** and the atomic propositions and the constants remain the same, e.g., $\mathbf{mtc}(\top) = \top$, $\mathbf{mtc}(p) = p$, $\mathbf{mtc}(\neg\phi) = \neg\mathbf{mtc}(\phi)$ and $\mathbf{mtc}(\phi_1 \vee \phi_2) = \mathbf{mtc}(\phi_1) \vee \mathbf{mtc}(\phi_2)$. Here, **mtc** stands for matching as it is defined for the until operator in [23]. The necessity for non-strict matching versions of the temporal operators will become apparent in the proof of Theorem 49. Now, we are in position to prove the following theorem.

Theorem 49 *Consider a formula $\phi \in clMTL_{\mathbb{B}}$, a map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, a continuous-time signal $s \in \mathcal{F}(R, X)$ and a sampling function $\tau \in \mathcal{F}_c^{\uparrow}(N, R)$. Let Assumptions 35, 45 and 47 hold and set $\mu = (s \circ \tau, \tau)$. Then,*

$$\forall t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R\,.$$
$$[\![\mathbf{mtc}(\phi)]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![\phi]\!]_C(s, t) \leq [\![\mathbf{mtc}(\phi)]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)$$

for any $i \in N$ which satisfies the conditions of Lemma 48.

Theorem 49 allows us to bound the robustness estimate of a continuous-time signal with respect to an clMTL formula ϕ. Note that the shorter the sampling constant $\Delta\tau = \alpha$ of the timed state sequence is, the tighter are the bounds on the robustness estimate. However, since we cannot always assume that $\lim_{\Delta\tau \to 0} \mathcal{E}(\Delta\tau) = 0$ (see Example 53), we cannot make any further claims. Moreover, we can not only guarantee that the continuous-time signal s satisfies the specification ϕ when $[\![\phi]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$, but also that the signal does not satisfy ϕ when $[\![\phi]\!]_D(\mu, i) < -\mathcal{E}(\Delta\tau)$.

Note that LTL is a fragment of clMTL which satisfies the second condition of Assumption 47. Hence, the following corollary of Theorem 49 is particularly useful in the case of LTL formulas.

Corollary 50 *Consider a formula $\phi \in LTL_{\mathbb{B}}$, a map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$, a continuous-time signal $s \in \mathcal{F}(R, X)$ and a sampling function $\tau \in \mathcal{F}_c^{\uparrow}(N, R)$. Let Assumption 35 hold and set $\sigma = s \circ \tau$. Then,*

$$\forall t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R\,.$$
$$[\![\mathbf{mtc}(\phi)]\!]_D(\sigma, i) - \mathcal{E}(\Delta\tau) \leq [\![\phi]\!]_C(s, t) \leq [\![\mathbf{mtc}(\phi)]\!]_D(\sigma, i) + \mathcal{E}(\Delta\tau).$$

LTL formulas, as opposed to MTL formulas, do not provide us with any information on how to sample the continuous-time signal. In this case, the shorter the sampling rate is, the better the approximation.

4.4 Examples

In this section, we demonstrate the proposed methodology with some examples. As mentioned in the introduction, we want to study the transient behavior of dynamical systems, thus all our examples study signals of bounded duration. 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. Since

we analyze discrete-time signals of bounded duration, we can compute their robustness estimate with respect to an MTL formula ϕ using Algorithm 1.

First, we demonstrate that for certain classes of signals it is straightforward to construct a bounding function $\mathcal{E}$ that satisfies the conditions of Assumption 35. For example, the function $\mathcal{E}$ can be easily derived when a signal is Lipschitz continuous.

Definition 51 (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:*

$$\forall x'_1, x'_2 \in X'.d(f(x'_1), f(x'_2)) \leq L_f d'(x'_1, x'_2). \tag{10}$$

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:

$$\forall t, t' \in R \; . \; d(s(t), s(t')) \leq L_s|t - t'|. \tag{11}$$

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 [55]. 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 always possible to estimate a constant L_s for eq. (11) when the time domain R of s is compact [39]. This estimate is very conservative and it cannot be employed in practical applications. However, it can be used as a local estimate for the Lipschitz constant at a sampling point i, i.e., for the time period $\tau(i + 1) - \tau(i)$, in connection with an on-line monitoring algorithm.

In all the examples that follow, we set $X = \mathbb{R}$ and $d(x_1, x_2) = |x_1 - x_2|$. The first example exploits the fact that the derivative of the signal can be bounded.

Example 52 *Assume that we are given a discrete-time representation σ_1 (Fig. 6) of the continuous-time signal s_1 (Fig. 3) 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 $\phi_1 = \Box_{[0,9\pi/2]}(p_{11} \to \Diamond_{[\pi,2\pi]} p_{12})$, 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 37 and 41. Using Algorithm 1, we compute a robustness estimate of $[\![\mathbf{str}_{\Delta\tau}(\phi_1)]\!]_D(\mu_1) \approx 0.7428$ where $\mu_1 = (\sigma_1, \tau_1)$, while $\mathcal{E}_1(\Delta\tau_1) = 0.6$. Therefore, by Corollary 44 we conclude that $\langle\!\langle \phi_1 \rangle\!\rangle_C(s_1) = \langle\!\langle \phi_1 \rangle\!\rangle_D(\mu_1) = \top$.*

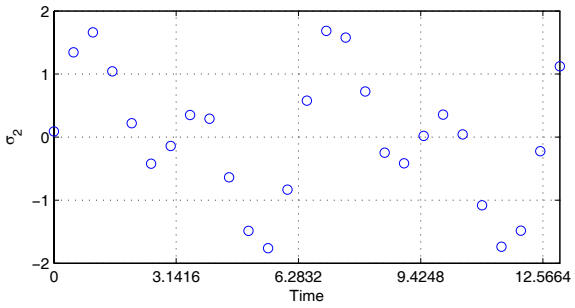

Fig. 7. The sampled signal σ_2 generated by sampling the continuous-time signal $s_2(t) = \sin(t) + \sin(2t) + w(t)$, where $|w(t)| \leq 0.1$, with constant sampling period 0.5. In this case, it is $|s_2(t_1) - s_2(t_2)| \leq L_{s_1}|t_1 - t_2| + |w(t_1)| + |w(t_2)|$. Thus, $\mathcal{E}_2(t) = L_{s_1}t + 0.2$.

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

Example 53 *Consider the discrete-time signal σ_2 in Fig. 7. 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 $[\![\mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu_2) \approx 1.7372$ where $\mu_2 = (\sigma_2, \tau_2)$, while $\mathcal{E}_2(\Delta\tau_2) = 1.7$ where $\Delta\tau_2 = 0.5$. Therefore by Corollary 44, we conclude that $\langle\!\langle \phi_2 \rangle\!\rangle_C(s_2) = \top$.*

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 [35, §10]).

Example 54 (Example 10.5 in [35]) *Consider the following linear system with nonlinear feedback*

$$\dot{x}(t) = Ax(t) - b\,\mathrm{sat}(cx(t)), \quad s_3(t) = cx(t) \tag{12}$$

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 [35] 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* $t \in R$*. In addition, the distance of* $x(t)$ *from the origin* $[0\ 0]^T$ *is always bounded by the radius of the minimum ball that contains the ellipsoid* $\{x \in \mathbb{R}^2 \mid V(x) \leq V(x(0))\}$*. The lengths of the axis of the ellipsoid are given by the square roots of the eigenvalues of the matrix* $P_e = V(x(0))P^{-1}$ *(see §2.2.2 in [8]). Let* $\lambda_{\max}(P_e)$ *be the maximum eigenvalue of* P_e*, then* $\|x(t)\| \leq \sqrt{\lambda_{\max}(P_e)}$ *for all* $t \in R$ *and*

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

Thus, for any $t, t' \in R$*, we have*

$$|s_3(t) - s_3(t')| \leq \|c\|\|x(t) - x(t')\| \leq \|c\|L_x|t - t'|.$$

That is, $\mathcal{E}_3(t) = \|c\|L_x t$*. 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 (12) is integrated with a maximum step-size of* 0.001 *using the MATLAB ode45 solver. The observable discrete-time signal* σ_3 *has maximum step-size* $\Delta\tau_3 = 0.045$*. The robustness estimate is* $[\![\mathbf{str}_{\Delta\tau}(\phi_3)]\!]_D(\mu_3) \approx 0.2372$ *where* $\mu_3 = (\sigma_3, \tau_3)$*, while* $\mathcal{E}_3(\Delta\tau_3) \approx 0.2182$*. Hence by Corollary 44, we conclude that* $\langle\!\langle \phi_3 \rangle\!\rangle_C(s_3) = \top$*. In addition, assume that we would like to estimate the continuous-time robustness estimate of* s_3 *with respect to the specification* ϕ_3*. In this case, the system (12) is integrated with a constant step-size of* 0.001 *using the MATLAB ode3 solver. We let the observable discrete-time signal* σ'_3 *have a constant step-size with* $\Delta\tau'_3 = 0.01$*. The discrete-time robustness estimate is approximately* $[\![\mathbf{mtc}(\phi_3)]\!]_D(\mu'_3) \approx 0.2379$ *where* $\mu'_3 = (\sigma'_3, \tau'_3)$ *and the function* $\mathcal{E}_3$ *takes the value* $\mathcal{E}_3(\Delta\tau'_3) \approx 0.0485$*. Thus, for all* $t \in [0, 0.01]$*, we have* $0.1894 \leq [\![\phi_3]\!]_C(s_3, t) \leq 0.2864$*. Note that in this example, we can assume that the simulation is accurate and, hence, we can ignore the possible simulation error.*

5 Related Research and Discussion

Since our research on robustness for temporal logic specifications spans many different research areas, the related literature is equally diverse. Here, we will just provide a few such references without attempting to be exhaustive.

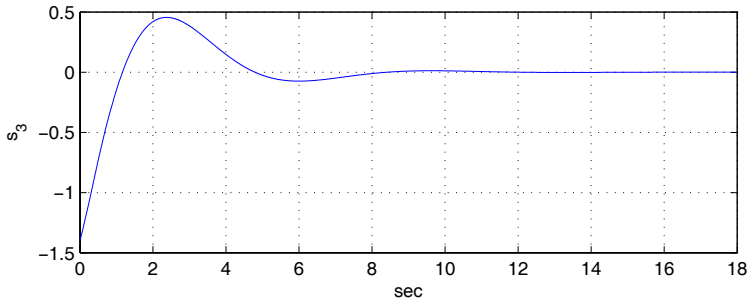

Fig. 8. The output signal s_3 of Example 54.

Robustness in timed automata has been studied by several authors, for example [25,30,49,5,6,56]. Out of the aforementioned literature, the work in [6] addresses the problem of robust temporal logic model checking of timed automata. The authors in [32] also consider robustness issues in MITL, but there the robustness is with respect to time. In hybrid systems, robustness issues have been analyzed in [21] and [30] among other works. We should point out that the authors in [25] and [30] define a notion of tube acceptance for timed and linear hybrid systems very similar to ours.

The authors in [40,54,37,26] develop temporal logic monitoring algorithms for (Boolean valued) signals. In particular, in [40] the problem of MITL testing over continuous-time signals is addressed. The authors in [54] and [37] present algorithms for monitoring timed temporal logics over timed state sequences. Lastly, in [26] the authors develop efficient algorithms for LTL monitoring.

Our work on robustness has the same underlying motivation with quantitative temporal logics [13,28] as well as multi-valued temporal logics [9]. Namely, we need to determine the degree that a system (or signal) satisfies a specification. The difference in our approach is that our quantitative semantics are used to capture systems that are (or are not) robustly correct with respect to continuous signal perturbations. Very recently in [51], motivated by applications to biology, a related notion of robustness was introduced.

One open problem which is very interesting is whether we can get rid of the requirement in Section 3 that all the timed state sequences have the same timing function (or time-stamps). It might be possible to address this issue by introducing robustness also with respect to time. Another important extension to our framework is to allow Boolean signals along with signals that take values in non-trivial metric spaces. This will enable the possibility to express more complicated properties without sacrificing the very intuitive notion of robustness that we have introduced in Section 2.3.

We should point out that the idea of continuous-time temporal logic verification by discrete-time methods is not new. In [29], the relationship between analog and digital clocks for timed state sequences is studied. In this paper,

the authors demonstrate that discrete-time verification techniques can be applied to the verification of bounded time invariance and bounded time response properties of continuous-time systems that can be modeled by timed transition systems. A more generalized version of the same problem is studied in [50]. In [14], the authors show that if a formula has the finite 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 [22]. 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 [22] and our work, the two approaches 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 [22] holds.

6 Conclusions and Future Work

The fundamental contribution of this work is the definition of a notion of robust satisfaction of Metric Temporal Logic (MTL) formulas which are interpreted over continuous or discrete-time signals. The robustness, which we consider, is with respect to the value of the signal and not with respect to the timing constraints imposed by the formula. As mentioned in the introduction, several application areas [52,16,38] may benefit from the notion of robustness that we have introduced. In addition, we have presented an algorithmic procedure that can monitor a finite timed state sequence and compute its robustness. This algorithm comprises the basis for our recent results on the bounded time temporal logic verification of continuous and discrete-time dynamical systems [15].

Another contribution of this paper is a framework that enables continuous-time reasoning using discrete-time methods. In particular, we have achieved two additional goals. First, we can infer the continuous-time satisfiability of an MITL formula. Our solution utilizes the notion of discrete-time robustness of MTL specifications and provides conditions on the signal dynamics and the sampling function. Second, we can compute bounds on the continuous-time robustness of a clMTL formula. In this case, it is required that the sampling function has a constant sampling rate. The latter contribution is quite interesting since it might be the only way to under-approximate the continuous-time robustness of a temporal logic formula with respect to a signal.

We are currently exploring several new directions such as the incorporation of robustness also with respect to time as advocated in [25,5,6,56,7]. In the front of continuous-time verification by discrete-time reasoning, there exist several directions for future research. 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 [33]. 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 [24] in order to obtain better bounds.

Acknowledgments The authors would like to thank Rajeev Alur, Antoine Girard, Nader Motee and Oleg Sokolsky for the fruitful discussions. The authors would also like to express their appreciation to the reviewers whose careful reading and subsequent comments helped to improve this paper.

References

[1] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, The algorithmic analysis of hybrid systems, Theoretical Computer Science 138 (1) (1995) 3–34.

[2] R. Alur, D. L. Dill, Theory of timed automata, Theoretical Computer Science 126 (2) (1994) 183–235.

[3] R. Alur, T. Feder, T. A. Henzinger, The benefits of relaxing punctuality, Journal of the ACM 43 (1996) 116–146.

[4] R. Alur, T. A. Henzinger, Real-Time Logics: Complexity and Expressiveness, in: Fifth Annual IEEE Symposium on Logic in Computer Science, IEEE Computer Society Press, Washington, D.C., 1990.

[5] R. Alur, S. L. Torre, P. Madhusudan, Perturbed timed automata., in: Hybrid Systems: Computation and Control, vol. 3414 of LNCS, 2005.

[6] P. Bouyer, N. Markey, P.-A. Reynier, Robust model-checking of linear-time properties in timed automata, in: J. R. Correa, A. Hevia, M. Kiwi (eds.), Proceedings of the 7th Latin American Symposium on Theoretical Informatics (LATIN'06), vol. 3887 of LNCS, Springer, Valdivia, Chile, 2006.

[7] P. Bouyer, N. Markey, P.-A. Reynier, Robust analysis of timed automata viachannel machines., in: R. M. Amadio (ed.), Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures, vol. 4962 of LNCS, Springer, 2008.

[8] S. Boyd, L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.

[9] M. Chechik, B. Devereux, A. Gurfinkel, Model-checking infinite state-space systems with fine-grained abstractions using SPIN, in: 8th International SPIN Workshop, vol. 2057 of LNCS, Springer, 2001.

[10] C.-T. Chen, Linear System Theory and Design, 3rd ed., Oxford University Press, 1998.

[11] E. M. Clarke, O. Grumberg, D. A. Peled, Model Checking, MIT Press, Cambridge, Massachusetts, 1999.

[12] B. A. Davey, H. A. Priestley, Introduction to Lattices and Order, 2nd ed., Cambridge University Press, Cambridge, United Kingdom, 2002.

[13] L. de Alfaro, M. Faella, M. Stoelinga, Linear and branching metrics for quantitative transition systems, in: Proceedings of the 31st ICALP, vol. 3142 of LNCS, Springer, 2004.

[14] L. de Alfaro, Z. Manna, Verification in continuous time by discrete reasoning, in: Proceedings of the 4th AMAST, vol. 936 of LNCS, Springer, 1995.

[15] G. E. Fainekos, A. Girard, G. J. Pappas, Temporal logic verification using simulation, in: E. Asarin, P. Bouyer (eds.), Proceedings of the 4th International Conference on Formal Modelling and Analysis of Timed Systems, vol. 4202 of LNCS, Springer, 2006.

[16] G. E. Fainekos, A. Girard, G. J. Pappas, Hierarchical synthesis of hybrid controllers from temporal logic specifications, in: Hybrid Systems: Computation and Control, No. 4416 in LNCS, Springer, 2007.

[17] G. E. Fainekos, G. J. Pappas, Robustness of temporal logic specifications, in: Formal Approaches to Testing and Runtime Verification, vol. 4262 of LNCS, Springer, 2006.

[18] G. E. Fainekos, G. J. Pappas, Robustness of temporal logic specifications for finite state sequences in metric spaces, Tech. Rep. MS-CIS-06-05, Dept. of CIS, Univ. of Pennsylvania (May 2006).

[19] G. E. Fainekos, G. J. Pappas, Robust sampling for MITL specifications, in: J.-F. Raskin, P. S. Thiagarajan (eds.), Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems, vol. 4763 of LNCS, Springer, 2007.

[20] G. E. Fainekos, G. J. Pappas, A user guide for TaLiRo, Tech. rep., Dept. of CIS, Univ. of Pennsylvania (2008).

[21] M. Fränzle, Analysis of hybrid systems: An ounce of realism can save an infinity of states, in: Proceedings of the 13th International Workshop and 8th Annual Conference of the EACSL on Computer Science Logic (CSL), Springer-Verlag, London, UK, 1999.

[22] C. A. Furia, M. Rossi, Integrating discrete and continuous time metric temporal logics through sampling, in: E. Asarin, P. Bouyer (eds.), Proceedings of the 4th International Conference on Formal Modelling and Analysis of Timed Systems, vol. 4202 of LNCS, Springer, 2006.

[23] C. A. Furia, M. Rossi, On the expressiveness of mtl variants over dense time, in: J.-F. Raskin, P. S. Thiagarajan (eds.), Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems, vol. 4763 of Lecture Notes in Computer Science, Springer, 2007.

[24] A. Girard, G. J. Pappas, Approximation metrics for discrete and continuous systems, IEEE Trans. Auto. Cont. 52 (5) (2007) 782–798.

[25] V. Gupta, T. A. Henzinger, R. Jagadeesan, Robust timed automata, in: HART '97: Proceedings of the International Workshop on Hybrid and Real-Time Systems, Springer-Verlag, London, UK, 1997.

[26] K. Havelund, G. Rosu, Monitoring programs using rewriting, in: Proceedings of the 16th IEEE international conference on Automated software engineering, 2001.

[27] T. A. Henzinger, The theory of hybrid automata, in: Proceedings of the 11th Annual Symposium on Logic in Computer Science, IEEE Computer Society Press, 1996.

[28] T. A. Henzinger, R. Majumdar, V. S. Prabhu, Quantifying similarities between timed systems., in: FORMATS, vol. 3829 of LNCS, Springer, 2005.

[29] T. A. Henzinger, Z. Manna, A. Pnueli, What good are digital clocks?, in: Proceedings of the 19th ICALP, vol. 623 of LNCS, Springer, 1992.

[30] T. A. Henzinger, J.-F. Raskin, Robust undecidability of timed and hybrid systems, in: N. A. Lynch, B. H. Krogh (eds.), Hybrid Systems: Computation and Control, vol. 1790 of LNCS, Springer, 2000.

[31] Y. Hirshfeld, A. Rabinovich, Logics for real time: Decidability and complexity, Fundam. Inf. 62 (1) (2004) 1–28.

[32] J. Huang, J. Voeten, M. Geilen, 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.

[33] A. A. Julius, G. E. Fainekos, M. Anand, I. Lee, G. J. Pappas, Robust test generation and coverage for hybrid systems, in: Hybrid Systems: Computation and Control, No. 4416 in LNCS, Springer, 2007.

[34] J. Kapinski, B. H. Krogh, O. Maler, O. Stursberg, On systematic simulation of open continuous systems., in: Hybrid Systems: Computation and Control, vol. 2623 of LNCS, Springer, 2003.

[35] H. K. Khalil, Nonlinear Systems, 2nd ed., Prentice-Hall, 1996.

[36] R. Koymans, Specifying real-time properties with metric temporal logic., Real-Time Systems 2 (4) (1990) 255–299.

[37] K. J. Kristoffersen, C. Pedersen, H. R. Andersen, Runtime verification of timed LTL using disjunctive normalized equation systems, in: Proceedings of the 3rd Workshop on Run-time Verification, vol. 89 of ENTCS, 2003.

[38] K. B. Lamine, F. Kabanza, Reasoning about robot actions: A model checking approach, in: Advances in Plan-Based Control of Robotic Agents, vol. 2466 of LNCS, Springer, 2002.

[39] I. Luigi, K. H. Johansson, U. Jonsson, V. Francesco, Averaging of nonsmooth systems using dither, Automatica 42 (4) (2006) 669–676.

[40] O. Maler, D. Nickovic, Monitoring temporal properties of continuous signals, in: Proceedings of FORMATS-FTRTFT, vol. 3253 of LNCS, 2004.

[41] N. Markey, Ph. Schnoebelen, Model checking a path (preliminary report), in: Proceedings of the 14th International Conference on Concurrency Theory, vol. 2761 of LNCS, 2003.

[42] A. Martinon, Distance to the intersection of two sets, Bull. Austral. Math. Soc. 70 (2004) 329341.

[43] J. Munkres, Topology, 2nd ed., Prentice Hall, 1999.

[44] K. Ogata, Modern Control Engineering, 4th ed., Prentice Hall, 2001.

[45] J. Ouaknine, J. Worrell, On the decidability of metric temporal logic, in: 20th IEEE Symposium on Logic in Computer Science (LICS), 2005.

[46] L. Pillage, R. Rohrer, C. Visweswariah, Electronic Circuit and System Simulation Methods, McGraw-Hill, 1995.

[47] A. Pnueli, The temporal logic of programs, in: Proceedings of the 18th IEEE Symposium Foundations of Computer Science, 1977.

[48] A. Pnueli, Development of hybrid systems, in: Formal Techniques in Real-Time and Fault-Tolerant Systems, vol. 863 of LNCS, Springer, 1994.

[49] A. Puri, Dynamical properties of timed automata, Discrete Event Dynamic Systems 10 (1-2) (2000) 87–113.

[50] J.-F. Raskin, P.-Y. Schobbens, Real-time logics: Fictitious clock as an abstraction of dense time, in: E. Brinksma (ed.), Proceedings of the 3rd International Workshop on Tools and Algorithms for Construction and Analysis of Systems (TACAS), vol. 1217 of LNCS, Springer, 1997.

[51] A. Rizk, G. Batt, F. Fages, S. Soliman, On a continuous degree of satisfaction of temporal logic formulae with applications to systems biology, in: M. Heiner, A. Uhrmacher (eds.), 6th International Conference on Computational Methods in Systems Biology, No. 5307 in LNCS, Springer, 2008.

[52] B. Shults, B. Kuipers, Qualitative simulation and temporal logic: proving properties of continuous systems, Tech. Rep. TR AI96-244, Dept. of Computer Sciences, University of Texas at Austin (January 1996).

[53] L. Tan, J. Kim, O. Sokolsky, I. Lee, Model-based testing and monitoring for hybrid embedded systems, in: Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, 2004.

[54] P. Thati, G. Rosu, Monitoring algorithms for metric temporal logic specifications, in: Runtime Verification, vol. 113 of ENTCS, Elsevier, 2005.

[55] G. R. Wood, B. P. Zhang, Estimation of the Lipschitz constant of a function, Journal of Global Optimization 8 (1) (1996) 91–103.

[56] M. D. Wulf, L. Doyen, J.-F. Raskin, Almost asap semantics: from timed models to timed implementations, Form. Asp. Comput. 17 (3) (2005) 319–341.

A Proofs of Section 2

A.1 Proof of Theorem 13

In this proof, we will use the following lemmas.

Lemma 55 *Let (X, d) be a metric space and $\{S_a\}_{a\in A}$ be an arbitrary collection of subsets of X. For any $x \in X$, $\mathbf{dist}_d(x, \cup_{a\in A} S_a) = \inf_{a\in A} \mathbf{dist}_d(x, S_a)$.*

PROOF. For any $x \in X$, we have

$$\begin{aligned}\mathbf{dist}_d(x, \cup_{a\in A} S_a) &= \inf_{y\in cl(\cup_{a\in A} S_a)} d(x, y) = \inf_{y\in \cup_{a\in A} S_a} d(x, y)\\ &= \inf_{a\in A} \inf_{y\in S_a} d(x, y) = \inf_{a\in A} \inf_{y\in cl(S_a)} d(x, y)\\ &= \inf_{a\in A} \mathbf{dist}_d(x, S_a) \qquad \square\end{aligned}$$

Lemma 56 *Let (X, d) be a metric space and $\{S_a\}_{a\in A}$ be an arbitrary collection of subsets of X. For any $x \in X$, $\mathbf{dist}_d(x, \cap_{a\in A} S_a) \geq \sup_{a\in A} \mathbf{dist}_d(x, S_a)$.*

PROOF. We have that $\cap_{a\in A} S_a \subseteq S_a$ for any $a \in A$. Thus, $\mathbf{dist}_d(x, \cap_{a\in A} S_a) \geq \mathbf{dist}_d(x, S_a)$. Since this holds for any $a \in A$ we get that $\mathbf{dist}_d(x, \cap_{a\in A} S_a) \geq \sup_{a\in A} \mathbf{dist}_d(x, S_a)$. $\square$

Lemma 57 *Consider an atomic proposition $p \in AP$, an observation map $\mathcal{O} \in \mathcal{F}(AP, \mathcal{P}(X))$ and a continuous-time signal $s \in \mathcal{F}(R, X)$, then for any time $t \in R$, we have* $\mathbf{Dist}_\rho(s, \mathcal{L}_t(p)) = [\![p]\!]_C(s,t)$.

PROOF. We only show the proof for the case that $s \in \mathcal{L}_t(p)$, because the proof for the case $s \notin \mathcal{L}_t(p)$ is similar. We have

$$\begin{aligned}\mathbf{Dist}_\rho(s, \mathcal{L}_t(p)) &= \mathbf{depth}_\rho(s, \mathcal{L}_t(p)) = \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg p)) \\ &= \inf_{s' \in cl(\mathcal{L}_t(\neg p))} \rho(s, s') = \inf_{s' \in cl(\mathcal{L}_t(\neg p))} \sup_{t' \in R} d(s(t'), s'(t')) \\ &= \inf_{s' \in cl(\mathcal{L}_t(\neg p))} \max\{d(s(t), s'(t)), \sup_{t' \in R_{\neq t}} d(s(t'), s'(t'))\}\end{aligned}$$

For each $s' \in cl(\mathcal{L}_t(\neg p))$ with $d(s(t), s'(t)) < \sup_{t' \in R_{\neq t}} d(s(t'), s'(t'))$, there exists some $s'' \in cl(\mathcal{L}_t(\neg p))$ with $s''(t) = s'(t)$ and $s''(t') = s(t')$ for all $t' \in R_{\neq t}$. That is, $0 = \sup_{t' \in R_{\neq t}} d(s(t'), s''(t')) \leq d(s(t), s''(t)) = d(s(t), s'(t)) < \sup_{t' \in R_{\neq t}} d(s(t'), s'(t'))$ or in other words $\rho(s, s'') < \rho(s, s')$. Thus,

$$\begin{aligned}\mathbf{Dist}_\rho(s, \mathcal{L}_t(p)) &= \inf_{s' \in cl(\mathcal{L}_t(\neg p))} d(s(t), s'(t)) = \inf_{x \in cl(X \backslash \mathcal{O}(p))} d(s(t), x) \\ &= \mathbf{dist}_d(s(t), X \backslash \mathcal{O}(p)) = [\![p]\!]_C(s,t) \qquad \square\end{aligned}$$

The proof of Theorem 13 is by induction on the structure of formula ϕ.

Constant $\phi = \top$: We have $\mathcal{L}_t(\top) = \mathcal{F}(R, X)$, thus

$$0 = -\mathbf{dist}_\rho(s, \mathcal{L}_t(\top)) \leq [\![\top]\!]_C(s,t) = +\infty = \mathbf{dist}_\rho(s, \emptyset) = \mathbf{depth}_\rho(s, \mathcal{L}_t(\top))$$

Atomic Propositions $\phi = p$: Immediate from Lemma 57.

Negation $\phi = \neg\phi_1$: By the induction hypothesis, we have

$$\begin{gathered}-\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_1)) \leq [\![\phi_1]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi_1)) \implies \\ -\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_1)) \leq -[\![\neg\phi_1]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi_1)) \implies \\ \mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_1)) \geq [\![\neg\phi_1]\!]_C(s,t) \geq -\mathbf{depth}_\rho(s, \mathcal{L}_t(\phi_1)) \implies \\ \mathbf{depth}_\rho(s, \mathcal{L}_t(\neg\phi_1)) \geq [\![\neg\phi_1]\!]_C(s,t) \geq -\mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi_1)) \implies \\ -\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi)) \leq [\![\phi]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi))\end{gathered}$$

Disjunction $\phi = \phi_1 \vee \phi_2$: By the induction hypothesis we get that for $i = 1, 2$

$$-\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_i)) \leq [\![\phi_i]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi_i))$$

for $i = 1, 2$. Thus, by the monotonicity property of the supremum, we get

$$\sqcup_{i=1,2} - \mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_i)) \leq \sqcup_{i=1,2} [\![\phi_i]\!]_C(s,t) \leq \sqcup_{i=1,2} \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi_i))$$

Note that by the definition of the language we get

$$\mathcal{L}_t(\phi) = \mathcal{L}_t(\phi_1 \vee \phi_2) = \mathcal{L}_t(\phi_1) \cup \mathcal{L}_t(\phi_2) \tag{A.1}$$

Moreover, by eq. (A.1) and Lemma 55, we have

$$\begin{gathered}\sqcup_{i=1,2} - \mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_i)) = - \sqcap_{i=1,2} \mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_i)) = \\ = -\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi_1) \cup \mathcal{L}_t(\phi_2)) = -\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi))\end{gathered}$$

Also, by eq. (A.1) and Lemma 56, we have

$$\begin{gathered}\sqcup_{i=1,2}\mathbf{depth}_\rho(s, \mathcal{L}_t(\phi_i)) = \sqcup_{i=1,2}\mathbf{dist}_\rho(s, \mathcal{F}(R,X)\backslash\mathcal{L}_t(\phi_i)) \leq \\ \leq \mathbf{dist}_\rho(s, \cap_{i=1,2}\mathcal{F}(R,X)\backslash\mathcal{L}_t(\phi_i)) = \mathbf{dist}_\rho(s, \mathcal{F}(R,X)\backslash \cup_{i=1,2} \mathcal{L}_t(\phi_i)) = \\ = \mathbf{depth}_\rho(s, \cup_{i=1,2}\mathcal{L}_t(\phi_i)) = \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi))\end{gathered}$$

Thus, by definition we have

$$-\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi)) \leq [\![\phi]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi))$$

Until $\phi = \phi_1 \,\mathcal{U}_\mathcal{I} \phi_2$: By definition, we have

$$[\![\phi_1 \,\mathcal{U}_\mathcal{I} \phi_2]\!]_C(s,t) = \bigsqcup_{t' \in (t +_R \mathcal{I})} \Big([\![\phi_2]\!]_C(s,t') \sqcap \prod_{t < t'' < t'} [\![\phi_1]\!]_C(s,t'') \Big)$$

By the induction hypothesis, we get

$$-\mathbf{dist}_\rho(s, \mathcal{L}_{t'}(\phi_2)) \leq [\![\phi_2]\!]_C(s,t') \leq \mathbf{depth}_\rho(s, \mathcal{L}_{t'}(\phi_2))$$

for any $t' \in (t +_R \mathcal{I})$ and

$$-\mathbf{dist}_\rho(s, \mathcal{L}_{t''}(\phi_1)) \leq [\![\phi_1]\!]_C(s,t'') \leq \mathbf{depth}_\rho(s, \mathcal{L}_{t''}(\phi_1))$$

for any $t'' \in (t, t')$. By the monotonicity property of infimum we have

$$\prod_{t'' \in (t,t')} -\mathbf{dist}_\rho(s, \mathcal{L}_{t''}(\phi_1)) \leq \prod_{t'' \in (t,t')} [\![\phi_1]\!]_C(s,t'') \leq \prod_{t'' \in (t,t')} \mathbf{depth}_\rho(s, \mathcal{L}_{t''}(\phi_1)).$$

Also, by Lemma 56 we have that

$$\begin{gathered}\mathbf{dist}_\rho(s, \cap_{t'' \in (t,t')}\mathcal{L}_{t''}(\phi_1)) \geq \sqcup_{t'' \in (t,t')}\mathbf{dist}_\rho(s, \mathcal{L}_{t''}(\phi_1)) \implies \\ -\mathbf{dist}_\rho(s, \cap_{t'' \in (t,t')}\mathcal{L}_{t''}(\phi_1)) \leq \sqcap_{t'' \in (t,t')} - \mathbf{dist}_\rho(s, \mathcal{L}_{t''}(\phi_1))\end{gathered}$$

and by Lemma 55 we have that

$$\begin{gathered}\sqcap_{t'' \in (t,t')}\mathbf{depth}_\rho(s, \mathcal{L}_{t''}(\phi_1)) = \sqcap_{t'' \in (t,t')}\mathbf{dist}_\rho(s, \mathcal{F}(R,X)\backslash\mathcal{L}_{t''}(\phi_1)) = \\ = \mathbf{dist}_\rho(s, \cup_{t'' \in (t,t')}\mathcal{F}(R,X)\backslash\mathcal{L}_{t''}(\phi_1)) =\end{gathered}$$

$$= \mathbf{dist}_\rho(s, \mathcal{F}(R,X) \setminus \cap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)) = \mathbf{depth}_\rho(s, \cap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)).$$

Therefore, we have that $-\mathbf{dist}_\rho(s, \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)) \leq \bigsqcap_{t'' \in (t,t')} [\![\phi_1]\!]_C(s,t'') \leq \mathbf{depth}_\rho(s, \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1))$. Similarly, we get that for any $t' \in (t +_R \mathcal{I})$

$$-\mathbf{dist}_\rho\left(s, \mathcal{L}_{t'}(\phi_2) \cap \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)\right) \leq [\![\phi_2]\!]_C(s,t') \sqcap \bigsqcap_{t'' \in (t,t')} [\![\phi_1]\!]_C(s,t'') \leq$$
$$\leq \mathbf{depth}_\rho\left(s, \mathcal{L}_{t'}(\phi_2) \cap \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)\right).$$

Finally, similar to the disjunction case, we get that

$$-\mathbf{dist}_\rho\left(s, \bigcup_{t' \in (t +_R \mathcal{I})} \left(\mathcal{L}_{t'}(\phi_2) \cap \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)\right)\right) \leq$$
$$\bigsqcup_{t' \in (t +_R \mathcal{I})} \left([\![\phi_2]\!]_C(s,t') \sqcap \bigsqcap_{t'' \in (t,t')} [\![\phi_1]\!]_C(s,t'')\right) \leq$$
$$\leq \mathbf{depth}_\rho\left(s, \bigcup_{t' \in (t +_R \mathcal{I})} \left(\mathcal{L}_{t'}(\phi_2) \cap \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)\right)\right).$$

Since

$$\mathcal{L}_t(\phi) = \{s \in \mathcal{F}(R,X) \mid \langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top\} =$$
$$= \left\{s \in \mathcal{F}(R,X) \mid \bigsqcup_{t' \in (t +_R \mathcal{I})} \left(\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') \sqcap \bigsqcap_{t < t'' < t'} \langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'')\right) = \top\right\} =$$
$$= \left\{s \in \mathcal{F}(R,X) \mid \bigvee_{t' \in (t +_R \mathcal{I})} \left(\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') = \top \wedge \bigwedge_{t < t'' < t'} \langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') = \top\right)\right\} =$$
$$= \bigcup_{t' \in (t +_R \mathcal{I})} \left(\mathcal{L}_{t'}(\phi_2) \cap \bigcap_{t'' \in (t,t')} \mathcal{L}_{t''}(\phi_1)\right),$$

we conclude that $-\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi)) \leq [\![\phi]\!]_C(s,t) \leq \mathbf{depth}_\rho(s, \mathcal{L}_t(\phi))$.

A.2 Proof of Proposition 16

Note that the first statement – i.e., if $[\![\phi]\!]_C(s,t) > 0$, then $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$, and if $[\![\phi]\!]_C(s,t) < 0$, then $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \bot$ – is immediate from Corollary 14. Therefore, we will only prove by induction on the structure of the formula $\phi \in MTL_{\mathbb{B}}$ the second statement, that is, if $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$, then $[\![\phi]\!]_C(s,t) \geq 0$, and if $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \bot$, then $[\![\phi]\!]_C(s,t) \leq 0$.

Case $\phi = \top$ **or** $\phi = \bot$**:** Immediate from the semantics.

Case $\phi = p \in AP$**:** If $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$, then by definition $s(t) \in \mathcal{O}(p)$, which implies that $\mathbf{Dist}_d(s(t), \mathcal{O}(p)) \geq 0$, and, thus, that $[\![\phi]\!]_C(s,t) \geq 0$. If on the other hand $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \bot$, then by definition $s(t) \notin \mathcal{O}(p)$, which implies that $\mathbf{Dist}_d(s(t), \mathcal{O}(p)) \leq 0$ and, thus, that $[\![\phi]\!]_C(s,t) \leq 0$.

Case $\phi = \neg\phi_1$**: (i)** If $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$, then by definition $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \bot$. By the induction hypothesis, we get that $[\![\phi_1]\!]_C(s,t) \leq 0$, which implies $[\![\neg\phi_1]\!]_C(s,t) \geq 0$. **(ii)** If $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \bot$, then by definition $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \top$. By the induction hypothesis, we get that $[\![\phi_1]\!]_C(s,t) \geq 0$, which implies $[\![\neg\phi_1]\!]_C(s,t) \leq 0$.

Case $\phi = \phi_1 \vee \phi_2$**: (i)** If $\langle\!\langle \phi_1 \vee \phi_2 \rangle\!\rangle_C(s,t) = \top$, then by definition we get that $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \top$ or $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t) = \top$. By the induction hypothesis, we have $[\![\phi_1]\!]_C(s,t) \geq 0$ or $[\![\phi_2]\!]_C(s,t) \geq 0$. Thus, $[\![\phi_1]\!]_C(s,t) \sqcup [\![\phi_2]\!]_C(s,t) \geq 0$, which implies $[\![\phi]\!]_C(s,t) \geq 0$. **(ii)** If $\langle\!\langle \phi_1 \vee \phi_2 \rangle\!\rangle_C(s,t) = \bot$, then by definition $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \bot$ and $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t) = \bot$. By the induction hypothesis, we get that $[\![\phi_1]\!]_C(s,t) \leq 0$ and $[\![\phi_2]\!]_C(s,t) \leq 0$. Thus, $[\![\phi_1]\!]_C(s,t) \sqcup [\![\phi_2]\!]_C(s,t) \leq 0$, which implies $[\![\phi]\!]_C(s,t) \leq 0$.

Case $\phi = \phi_1 \mathcal{U}_\mathcal{I} \phi_2$**: (i)** If $\langle\!\langle \phi_1 \mathcal{U}_\mathcal{I} \phi_2 \rangle\!\rangle_C(s,t) = \top$, then by the definition of until, there exists some time $t' \in (t +_R \mathcal{I})$ such that $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') = \top$ and for all $t'' \in (t,t')$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') = \top$. Using the induction hypothesis we get that $[\![\phi_2]\!]_C(s,t') \geq 0$ and for all $t'' \in (t,t')$, we have $[\![\phi_1]\!]_C(s,t'') \geq 0$. Therefore, $[\![\phi]\!]_C(s,t) = \bigsqcup_{t' \in (t+_R\mathcal{I})} \Big([\![\phi_2]\!]_C(s,t') \sqcap \bigsqcap_{t<t''<t'} [\![\phi_1]\!]_C(s,t'') \Big) \geq 0$. **(ii)** If $\langle\!\langle \phi_1 \mathcal{U}_\mathcal{I} \phi_2 \rangle\!\rangle_C(s,t) = \bot$, then $(t +_R \mathcal{I}) = \emptyset$ or for all time $t' \in (t +_R \mathcal{I})$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') \sqcap \bigsqcap_{t<t''<t'} \langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') = \bot$. In the former case, we immediately get by the definition that $[\![\phi]\!]_C(s,t) = -\infty$. In the latter case, for all time $t' \in (t +_R \mathcal{I})$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') = \bot$ or there exists some time $t'' \in (t,t')$ such that $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') = \bot$. Using the induction hypothesis we get that for all $t' \in (t +_R \mathcal{I})$, $[\![\phi_2]\!]_C(s,t') \leq 0$ or there exists $t'' \in (t,t')$ such that $[\![\phi_1]\!]_C(s,t'') \leq 0$. Therefore, $[\![\phi]\!]_C(s,t) \leq 0$ by definition.

A.3 Proof of Proposition 19

The proof of Proposition 19 is by induction on the structure of ϕ.

Constant $\phi = \top$: We have

$$\mathbf{Dist}_\rho(s, \mathcal{L}_t(\top)) = \mathbf{depth}_\rho(s, \mathcal{L}_t(\top)) = \mathbf{dist}_\rho(s, \emptyset) = +\infty = [\![\top]\!]_C(s,t)$$

Atomic Propositions $\phi = p$ **or** $\phi = \neg p$ **with** $p \in AP$: Immediate from Lemma 57.

Conjunction $\phi = \phi_1 \wedge \phi_2$: Since $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \top$ and $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t) = \top$. By the induction hypothesis we get that $[\![\phi_1]\!]_C(s,t) = \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi_1))$ and $[\![\phi_2]\!]_C(s,t) = \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi_2))$. Moreover,

$$\mathcal{L}_t(\neg\phi) = \mathcal{L}_t(\neg\phi_1 \vee \neg\phi_2) = \mathcal{L}_t(\neg\phi_1) \cup \mathcal{L}_t(\neg\phi_2).$$

Hence, using Lemma 55, and the induction hypothesis we have

$$\begin{aligned}\mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi)) &= \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi)) = \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi_1) \cup \mathcal{L}_t(\neg\phi_2)) \\ &= \min\{\mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi_1)), \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi_2))\} \\ &= [\![\phi_1]\!]_C(s,t) \sqcap [\![\phi_2]\!]_C(s,t) = [\![\phi]\!]_C(s,t)\end{aligned}$$

Always $\phi = \Box_{\mathcal{I}}\phi_1$: Since $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \top$, we get that $(t +_R \mathcal{I}) = \emptyset$ or that for all $t' \in (t +_R \mathcal{I})$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t') = \top$. In the former case, we immediately get that $\mathcal{L}_t(\phi) = \mathcal{F}(R, X)$ and

$$\mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi)) = \mathbf{dist}_\rho(s, \emptyset) = +\infty = \sqcap_{t' \in \emptyset}[\![\phi_1]\!]_C(s,t') = [\![\phi]\!]_C(s,t)$$

In the latter case, by the induction hypothesis we get that for all $t' \in (t +_R \mathcal{I})$, we have $[\![\phi_1]\!]_C(s,t') = \mathbf{dist}_\rho(s, \mathcal{L}_{t'}(\neg\phi_1))$. Also, $\mathcal{L}_t(\neg\phi) = \cup_{t' \in (t +_R \mathcal{I})}\mathcal{L}_{t'}(\neg\phi_1)$. Hence, using Lemma 55, and the induction hypothesis we have

$$\begin{aligned}\mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi)) &= \mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\phi)) = \mathbf{dist}_\rho(s, \cup_{t' \in (t +_R \mathcal{I})}\mathcal{L}_{t'}(\neg\phi_1)) \\ &= \inf_{t' \in (t +_R \mathcal{I})} \mathbf{dist}_\rho(s, \mathcal{L}_{t'}(\neg\phi_1)) = \sqcap_{t' \in (t +_R \mathcal{I})}[\![\phi_1]\!]_C(s,t') \\ &= [\![\phi]\!]_C(s,t)\end{aligned}$$

A.4 Proof of Corollary 20

Note that if $\phi \in MTL_{\mathbb{B}}(\vee, \Diamond)$, then $\psi = \mathbf{nnf}(\neg\phi) \in MTL_{\mathbb{B}}(\wedge, \Box)$. Also, since $\langle\!\langle \phi \rangle\!\rangle_C(s,t) = \bot$, we have $\langle\!\langle \psi \rangle\!\rangle_C(s,t) = \top$. Then, by Proposition 19, we have

$$\begin{aligned}[\![\phi]\!]_C(s,t) &= -[\![\neg\phi]\!]_C(s,t) = -[\![\psi]\!]_C(s,t) \\ &= -\mathbf{dist}_\rho(s, \mathcal{L}_t(\neg\psi)) = -\mathbf{dist}_\rho(s, \mathcal{L}_t(\phi)) = \mathbf{Dist}_\rho(s, \mathcal{L}_t(\phi))\end{aligned}$$

B Proofs of Section 3

For easy reference, we state here the discrete-time semantics of the (strict non-matching) release

$$\langle\!\langle \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2 \rangle\!\rangle_D(\mu, i) := \bigsqcap_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big(\langle\!\langle \phi_2 \rangle\!\rangle_D(\mu, j) \sqcup \bigsqcup_{i<k<j} \langle\!\langle \phi_1 \rangle\!\rangle_D(\mu, k) \Big) \tag{B.1}$$

$$[\![\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) := \bigsqcap_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_D(\mu, j) \sqcup \bigsqcup_{i<k<j} [\![\phi_1]\!]_D(\mu, k) \Big), \tag{B.2}$$

the discrete-time robust semantics of the temporal operators $\overleftarrow{\mathcal{U}}$ and $\overleftarrow{\mathcal{R}}$

$$[\![\phi_1 \overleftarrow{\mathcal{U}}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) := \bigsqcup_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{i \le k < j} [\![\phi_1]\!]_D(\mu, k) \Big) \tag{B.3}$$

$$[\![\phi_1 \overleftarrow{\mathcal{R}}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) := \bigsqcap_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_D(\mu, j) \sqcup \bigsqcup_{i \le k < j} [\![\phi_1]\!]_D(\mu, k) \Big), \tag{B.4}$$

as well as the discrete-time robust semantics of the temporal operator $\overleftrightarrow{\mathcal{U}}$

$$[\![\phi_1 \overleftrightarrow{\mathcal{U}}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) := \bigsqcup_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{i \le k \le j} [\![\phi_1]\!]_D(\mu, k) \Big). \tag{B.5}$$

Most of the proofs in Section 3 are essentially identical to the proofs of Section 2 and, hence, we omit these proofs. An explicit presentation of the proofs for finite timed state sequences appears in [18].

B.1 Recursive Formulation of Strict Non-Matching Until in Section 3.5

Starting from the definition of until, we have

$$\begin{aligned}
&[\![\phi_1 \mathcal{U}_{\mathcal{I}} \phi_2]\!]_D(\mu, i) = \bigsqcup_{j \in \tau^{-1}(\tau(i)+\mathcal{I})} \Big([\![\phi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{i<k<j} [\![\phi_1]\!]_D(\mu, k) \Big) \\
&= \bigsqcup_{j \ge i} \Big(K^{\infty}_{\in}(j, \tau^{-1}(\tau(i)+\mathcal{I})) \sqcap [\![\phi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{i<k<j} [\![\phi_1]\!]_D(\mu, k) \Big) \\
&= \Big(K^{\infty}_{\in}(i, \tau^{-1}(\tau(i)+\mathcal{I})) \sqcap [\![\phi_2]\!]_D(\mu, i) \Big) \sqcup \\
&\quad \sqcup \bigsqcup_{j \ge i+1} \Big(K^{\infty}_{\in}(j, \tau^{-1}(\tau(i)+\mathcal{I})) \sqcap [\![\phi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{i<k<j} [\![\phi_1]\!]_D(\mu, k) \Big) \\
&= \Big(K^{\infty}_{\in}(i, \tau^{-1}(\tau(i)+\mathcal{I})) \sqcap [\![\phi_2]\!]_D(\mu, i) \Big) \sqcup \\
&\quad \sqcup \bigsqcup_{j \ge i+1} \Big(K^{\infty}_{\in}(j, \tau^{-1}((\tau(i+1) - \delta\tau(i)) + \mathcal{I})) \sqcap [\![\phi_2]\!]_D(\mu, j) \sqcap \\
&\quad \sqcap \bigsqcap_{i+1 \le k < j} [\![\phi_1]\!]_D(\mu, k) \Big)
\end{aligned}$$

$$\overset{(B.3)}{=} \Big(K^{\infty}_{\in}(i, \tau^{-1}(\tau(i) + \mathcal{I})) \sqcap [\![\phi_2]\!]_D(\mu, i)\Big) \sqcup [\![\phi_1 \overleftarrow{\mathcal{U}}_{(-\delta\tau(i))+_R\mathcal{I}} \phi_2]\!]_D(\mu, i+1)$$

Since $\tau(i) \in R$, we have $\tau(i) \in (\tau(i) +_R \mathcal{I})$ iff $\tau(i) \in (\tau(i) + \mathcal{I})$ iff $0 \in \mathcal{I}$. Also, when $\mathbf{dom}(\tau)$ is finite and $i = \max \mathbf{dom}(\tau)$, for all $j \geq i+1$, we have $K^{\infty}_{\in}(j, \tau^{-1}(\tau(i) + \mathcal{I})) = -\infty$. Thus, we derive the recursive formulation of strict non-matching until in Section 3.5.

B.2 Proof of Lemma 33

The proof uses induction on the structure of ϕ. Since $i < \max N$, we have $last = \bot$. We only present the base case and the case for until since the rest of the cases are similar.

Base case $\phi = p \in AP$: then

$$\begin{aligned}[\![p]\!]_D(\mu, i) &= \mathbf{Dist}_d(\sigma(i), \mathcal{O}(p)) = \textsc{Derive}(\phi, \sigma(i), \delta\tau(i), \bot, \mathcal{O}) \\ &= [\![\textsc{Derive}(\phi, \sigma(i), \delta\tau(i), \bot, \mathcal{O})]\!]_D(\mu, i+1)\end{aligned}$$

since $\mathbf{Dist}_d(\sigma(i), \mathcal{O}(p)) \in \overline{\mathbb{R}}$. The proof is similar when $\phi = \top$ or $\phi = c \in \overline{\mathbb{R}}$.

Until $\phi = \phi_1 \overleftarrow{\mathcal{U}}_{\mathcal{I}} \phi_2$: Now using the equivalence from Section 3.5, we derive

$$\begin{aligned}[\![\phi]\!]_D(\mu, i) &= \Big(K^{\infty}_{\in}(0, \mathcal{I}) \sqcap [\![\phi_2]\!]_D(\mu, i)\Big) \sqcup \\ &\quad \sqcup \Big([\![\phi_1]\!]_D(\mu, i) \sqcap [\![\phi_1 \overleftarrow{\mathcal{U}}_{(-\delta\tau(i))+_R\mathcal{I}} \phi_2]\!]_D(\mu, i+1)\Big) \\ &= \Big(K^{\infty}_{\in}(0, \mathcal{I}) \sqcap \sqcap [\![\textsc{Derive}(\phi_2, \sigma(i), \delta\tau(i), \bot, \mathcal{O})]\!]_D(\mu, i+1)\Big) \sqcup \\ &\quad \sqcup \Big([\![\textsc{Derive}(\phi_1, \sigma(i), \delta\tau(i), \bot, \mathcal{O})]\!]_D(\mu, i+1) \sqcap \qquad \textit{by I.H.} \\ &\quad \sqcap [\![\phi_1 \overleftarrow{\mathcal{U}}_{(-\delta\tau(i))+_R\mathcal{I}} \phi_2]\!]_D(\mu, i+1)\Big) \\ &= [\![\textsc{Derive}(\phi, \sigma(i), \delta\tau(i), \bot, \mathcal{O})]\!]_D(\mu, i+1)\end{aligned}$$

C Proofs of Section 4

C.1 Proof of Proposition 36

The proof is by induction on the structure of formula ϕ. The cases for $\top$, p and $\neg p$ are immediate from the definitions. Similarly, the cases $\phi_1 \wedge \phi_2$ and $\phi_1 \vee \phi_2$ are immediate from the induction hypothesis.

Case $\phi = \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$**:** We have $\langle\!\langle \mathbf{str}_{\Delta\tau}(\phi_1) \overleftarrow{\mathcal{U}}_{C(\mathcal{I}, \Delta\tau)} \mathbf{str}_{\Delta\tau}(\phi_2) \rangle\!\rangle_D(\mu, i) = \top$. Thus, by the definition of non-strict non-matching until (B.3) and the induc-

tion hypothesis, there exists some $j \in \tau^{-1}(\tau(i) + C(\mathcal{I}, \Delta\tau)) \subseteq \tau^{-1}(\tau(i) + \mathcal{I})$ such that $\langle\!\langle \phi_2 \rangle\!\rangle_D(\mu, j) = \top$ and for all k such that $i \leq k < j$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_D(\mu, k) = \top$. We conclude that $\langle\!\langle \phi_1 \, \mathcal{U}_{\mathcal{I}} \phi_2 \rangle\!\rangle_D(\mu, i) = \top$ by the definition of until. Note that if $C(\mathcal{I}, \Delta\tau) = \emptyset$, then $\mathbf{str}_{\Delta\tau}(\phi)$ would evaluate to $\bot$ which is a contradiction.

Case $\phi = \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$**:** We have $\langle\!\langle \mathbf{str}_{\Delta\tau}(\phi_1) \; \overleftarrow{\mathcal{R}}_{E(\mathcal{I},\Delta\tau)} \; \mathbf{str}_{\Delta\tau}(\phi_2) \rangle\!\rangle_D(\mu, i) = \top$. Thus, by the definition of the non-strict non-matching release (B.4) and the induction hypothesis, for all $j \in \tau^{-1}(\tau(i) + E(\mathcal{I}, \Delta\tau))$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_D(\mu, j) = \top$ or there exists $k \in [i, j)$ such that $\langle\!\langle \phi_1 \rangle\!\rangle_D(\mu, k) = \top$. Since $\tau^{-1}(\tau(i) + E(\mathcal{I}, \Delta\tau)) \supseteq \tau^{-1}(\tau(i) + \mathcal{I})$, by the definition of release, we conclude that $\langle\!\langle \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2 \rangle\!\rangle_D(\mu, i) = \top$.

C.2 Proof of Lemma 38

If both R and $\mathcal{I}$ are unbounded, then we immediately get $\tau^{-1}(\tau(i) + \mathcal{I}) \neq \emptyset$ since τ is strictly increasing and diverging. Assume now that $\mathcal{I}$ is bounded and that for some $i \in I$ we get that $\tau^{-1}(\tau(i) + \mathcal{I}) = \emptyset$. In other words, we assume that for all $j \geq i$ (since τ is strictly increasing), we have $\tau(j) \notin (\tau(i) + \mathcal{I})$. One of the following two options must hold since $\tau(i) + \mathcal{I}$ is an interval of R:

(1) All the samples $j \geq i$ map to points in time that occur sooner than the minimum required time by $\tau(i) + \mathcal{I}$. Formally, for all $j \in N_{\geq i}$ we have $\tau(j) \prec \inf(\tau(i) + \mathcal{I})$, where $\prec \in \{<, \leq\}$ depending on the bounds of $\mathcal{I}$. Note that this can only be the case when R is bounded, i.e., N is bounded and, thus, $\tau(\max N) \prec \inf(\tau(i) + \mathcal{I})$. Hence, we get that $\sup R - \tau(\max N) \succ \sup R - \inf(\tau(i) + \mathcal{I}) \geq \sup(\tau(i) + \mathcal{I}) - \inf(\tau(i) + \mathcal{I}) \geq \sup \mathcal{I} - \inf \mathcal{I} > \Delta\tau$, which is a contradiction by Assumption 37.
(2) There exists some sample $j \geq i$ such that the time interval $\tau(i) + \mathcal{I}$ fits between the samples j and $j + 1$. Formally, there exists $j \in N_{\geq i}$ such that $\tau(j) \prec \inf(\tau(i) + \mathcal{I})$ and $\sup(\tau(i) + \mathcal{I}) \prec \tau(j + 1)$, where $\prec \in \{<, \leq\}$ depending on the constraints of $\mathcal{I}$. That is, $\tau(j + 1) - \tau(j) \succ \sup(\tau(i) + \mathcal{I}) - \inf(\tau(i) + \mathcal{I}) = \sup \mathcal{I} - \inf \mathcal{I} > \Delta\tau$, which is a contradiction by definition (equation (6)).

Note that the case where all the samples $j \geq i$ map to points in time that happen later than the maximum required time by $\tau(i) + \mathcal{I}$ cannot be considered since the time $\tau(i)$ cannot occur after the time interval $\tau(i) + \mathcal{I}$. Thus, $\tau^{-1}(\tau(i) + \mathcal{I}) \neq \emptyset$.

C.3 Proof of Lemma 42

If R is unbounded, then the result is immediate from Lemma 38. If now R is bounded, we have by definition that $\sum_{j\geq k} \sup \mathcal{I}_j \leq \mathbf{dur}(\mathbf{str}_{\Delta\tau}(\phi)) < \sup R$. Thus, for any $i \in I$, we have $\tau(i)+\sup \mathcal{I}_k < \sup R$ and, therefore, $(\tau(i)+\mathcal{I}_k) \subseteq R$. Thus, $(\tau(i) + \mathcal{I}_k) = (\tau(i) +_R \mathcal{I}_k)$. The result follows by Lemma 38. Since $\tau^{-1}(\tau(i) + \mathcal{I}_k) \neq \emptyset$, we also get that $\tau^{-1}([0, \sum_{j\geq k} \sup \mathcal{I}_j]) \neq \emptyset$ (note that by assumption $\tau^{-1}(T) \neq \emptyset$).

C.4 Proof of Theorem 43

The proof of the theorem is by induction on the structure of formula ϕ. In the following, we set $\sigma = s \circ \tau$, $\mu = (\sigma, \tau)$ and $T_i = [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$ for $i \in N$.

Case $\phi = \top$: $[\![\mathbf{str}_{\Delta\tau}(\top)]\!]_D(\mu, i) = +\infty > \mathcal{E}(\Delta\tau)$. Therefore, for all $t \in T_i$, we have $\langle\!\langle \top \rangle\!\rangle_C(s, t) = \top$.

Case $\phi = p \in AP$: $[\![\mathbf{str}_{\Delta\tau}(p)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$, i.e., $\mathbf{depth}_d(\sigma(i), \mathcal{O}(p)) > \mathcal{E}(\Delta\tau)$. Therefore, $d(\sigma(i), x) > \mathcal{E}(\Delta\tau)$ for any $x \in cl(X\backslash\mathcal{O}(p))$. Moreover by Assumption 35, we get that $d(\sigma(i), s(t)) \leq \mathcal{E}(\Delta\tau)$ for all $t \in T_i$ and $d(\sigma(i), s(t)) \leq \mathcal{E}(\Delta\tau) < d(\sigma(i), x)$. Also, since d is a metric : $d(\sigma(i), x) \leq d(\sigma(i), s(t)) + d(s(t), x)$. Hence, $d(s(t), x) > 0$. Since this holds for any $x \in cl(X\backslash\mathcal{O}(p))$, we conclude that $s(t) \in \mathcal{O}(p)$ and, thus, $\langle\!\langle p \rangle\!\rangle_C(s, t) = \top$ for all $t \in T_i$.

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

Case $\phi = \phi_1 \wedge \phi_2$: We have that $[\![\mathbf{str}_{\Delta\tau}(\phi_1) \wedge \mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$. Thus, both $[\![\mathbf{str}_{\Delta\tau}(\phi_1)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$ and $[\![\mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$. By the induction hypothesis, we get that for all $t \in T_i$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_C(s, t) = \top$ and for all $t \in T_i$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_C(s, t) = \top$. That is, for all $t \in T_i$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_C(s, t) = \top$ and $\langle\!\langle \phi_2 \rangle\!\rangle_C(s, t) = \top$. Hence, for all $t \in T_i$, we have $\langle\!\langle \phi \rangle\!\rangle_C(s, t) = \top$.

Case $\phi = \phi_1 \vee \phi_2$: The proof is similar to the previous case.

Case $\phi = \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$: We know that $[\![\mathbf{str}_{\Delta\tau}(\phi_1) \overleftarrow{\mathcal{U}}_{C(\mathcal{I},\Delta\tau)} \mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$. By Lemma 42, we have $J = \tau^{-1}(\tau(i) + C(\mathcal{I}, \Delta\tau)) \neq \emptyset$. By equation (B.3), there exists some $j \in J$ such that $[\![\phi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{i\leq k<j} [\![\phi_1]\!]_D(\mu, k) > \mathcal{E}(\Delta\tau)$. Hence, $[\![\mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu, j) > \mathcal{E}(\Delta\tau)$ and for all k such that $i \leq k < j$, we have $[\![\mathbf{str}_{\Delta\tau}(\phi_1)]\!]_D(\mu, k) > \mathcal{E}(\Delta\tau)$. By the induction hypothesis, we get

that $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t) = \top$ for all $t \in T_j$ and $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \top$ for all $t \in T_k$ and for all $k \in [i,j)$. We set $t' = \tau(j)$. Note that for all $t \in T_i$, we have $\tau(j) \in \tau(i) + C(\mathcal{I}, \Delta\tau) \subseteq (t + \mathcal{I})$. But $\tau(j) \in \tau(i) +_R C(\mathcal{I}, \Delta\tau)$, thus we have $t' = \tau(j) \in (t +_R \mathcal{I}) \neq \emptyset$. Also, since $\tau(j) \leq \tau(j-1) + \Delta\tau$, we get that for all $t'' \in (t, t')$, we have $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') = \top$. Hence, we conclude that $\langle\!\langle \phi_1 \, \mathcal{U}_{\mathcal{I}} \phi_2 \rangle\!\rangle_C(s,t) = \top$ for all $t \in T_i$ by the definition of $\mathcal{U}$.

Case $\phi = \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2$: We have $[\![\mathbf{str}_{\Delta\tau}(\phi_1) \overleftarrow{\mathcal{R}}_{E(\mathcal{I},\Delta\tau)} \mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu, i) > \mathcal{E}(\Delta\tau)$. By Lemma 42, we have $J = \tau^{-1}(\tau(i) + E(\mathcal{I}, \Delta\tau)) \neq \emptyset$. By the definition of release, for all $j \in J$, we have $[\![\mathbf{str}_{\Delta\tau}(\phi_2)]\!]_D(\mu, j) > \mathcal{E}(\Delta\tau)$ or there exists k such that $i \leq k < j$ and $[\![\mathbf{str}_{\Delta\tau}(\phi_1)]\!]_D(\mu, k) > \mathcal{E}(\Delta\tau)$. By the induction hypothesis, we get that for all $j \in J$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t) = \top$ for all $t \in T_j$ and $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t) = \top$ for all $t \in T_k$. Let $j_m = \min J$ and $j_M = \max J$. For all $t' \in [\tau(j_m) - \Delta\tau, \tau(j_M) + \Delta\tau] \cap R$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') = \top$. Moreover, for all $t \in T_i$, we have $(t + \mathcal{I}) \subseteq \tau(i) + E(\mathcal{I}, \Delta\tau)$. But by Lemma 42, we get $\tau(i) +_R E(\mathcal{I}, \Delta\tau) = \tau(i) + E(\mathcal{I}, \Delta\tau)$. We conclude that $(t +_R \mathcal{I}) \neq \emptyset$ since $(t +_R \mathcal{I}) \subseteq \tau(i) +_R E(\mathcal{I}, \Delta\tau)$. Hence, for all $t \in T_i$, for all $t' \in (t +_R \mathcal{I})$, we have $\langle\!\langle \phi_2 \rangle\!\rangle_C(s,t') = \top$ or there exists some $t'' \in (t, t')$ such that $\langle\!\langle \phi_1 \rangle\!\rangle_C(s,t'') = \top$. Hence, $\langle\!\langle \phi_1 \mathcal{R}_{\mathcal{I}} \phi_2 \rangle\!\rangle_C(s,t) = \top$ for all $t \in T_i$.

C.5 Proof of Lemma 48

If R is unbounded, then the result is immediate from Lemma 46. If R is bounded, we need to consider two cases.

- Case 1 of Assumption 47: Consider any $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$. We have that $t + \sup \mathcal{I}_k \leq \tau(i) + \Delta\tau + \sup \mathcal{I}_k \leq \mathbf{dur}(\phi) + \Delta\tau < \sup R$. Thus, $t +_R \mathcal{I}_k \neq \emptyset$ and $\tau^{-1}(\tau(i) + \mathcal{I}_k) \neq \emptyset$.
- Case 2 of Assumption 47: Since $0 \in \mathcal{I}$, we immediately get that $i \in \tau^{-1}(\tau(i) + \mathcal{I}_k) \neq \emptyset$ and that for all $t \in [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$, $t \in (t +_R \mathcal{I}_k) \neq \emptyset$.

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

C.6 Proof of Theorem 49

The proof is by induction on the structure of formula ϕ. In the following, we always set $\sigma = s \circ \tau$, $\mu = (\sigma, \tau)$ and $\psi = \mathbf{mtc}(\phi)$. For the sake of brevity, we also define $T_i = [\tau(i) - \Delta\tau, \tau(i) + \Delta\tau] \cap R$ for $i \in N$. By Assumption 45, there exists some $\alpha \in \mathbb{Q}_{>0}$ such that $\tau(i) = ai$ for $i \in N$. Thus, $\Delta\tau = \alpha$ and $T_i = [a(i-1), a(i+1)] \cap R$.

Case $\phi = \top$: We have $\psi = \top$. By definition, for all $t \in T_i$, we have $[\![\top]\!]_C(s,t) = +\infty$ and, also, $[\![\top]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) = [\![\top]\!]_D(\mu,i) + \mathcal{E}(\Delta\tau) = +\infty$.

Case $\phi = p \in AP$: We have $\psi = p$. In the following, we let $t \in T_i$. By Assumption 35, we have

$$d(\sigma(i), s(t)) \leq \mathcal{E}(\Delta\tau) \tag{C.1}$$

We must consider 4 cases according to the values of $\langle\!\langle p \rangle\!\rangle_D(\mu,i)$ and $\langle\!\langle p \rangle\!\rangle_C(s,t)$.

(1) Assume that $s(t), \sigma(i) \in \mathcal{O}(p)$, that is, $[\![p]\!]_D(\mu,i) = \mathbf{dist}_d(\sigma(i), X\backslash\mathcal{O}(p))$ and $[\![p]\!]_C(s,t) = \mathbf{dist}_d(s(t), X\backslash\mathcal{O}(p))$. Since we have $\mathbf{dist}_d(\sigma(i), X\backslash\mathcal{O}(p)) \leq d(\sigma(i), x)$ for any $x \in cl(X\backslash\mathcal{O}(p))$, from the triangle inequality, we get

$$\mathbf{dist}_d(\sigma(i), X\backslash\mathcal{O}(p)) \leq d(\sigma(i), x) \leq d(\sigma(i), s(t)) + d(s(t), x) \overset{(C.1)}{\Longrightarrow}$$
$$[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) \leq d(s(t), x)$$

That is, $[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau)$ is a lower bound on $d(s(t),x)$ over the set $cl(X\backslash\mathcal{O}(p))$ and, thus, $[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau)$ is less than or equal to the greatest lower bound (glb) on $d(s(t),x)$ over the set $cl(X\backslash\mathcal{O}(p))$ or

$$[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) \leq \inf\{d(s(t),x) \mid x \in cl(X\backslash\mathcal{O}(p))\} = [\![p]\!]_C(s,t)$$

By symmetry, we get

$$[\![p]\!]_C(s,t) - \mathcal{E}(\Delta\tau) \leq [\![p]\!]_D(\mu,i) \implies [\![p]\!]_C(s,t) \leq [\![p]\!]_D(\mu,i) + \mathcal{E}(\Delta\tau)$$

(2) Assume that $s(t), \sigma(i) \in X\backslash\mathcal{O}(p)$, i.e., $[\![p]\!]_D(\mu,i) = -\mathbf{dist}_d(\sigma(i), \mathcal{O}(p))$ and $[\![p]\!]_C(s,t) = -\mathbf{dist}_d(s(t), \mathcal{O}(p))$. Since $\mathbf{dist}_d(\sigma(i), \mathcal{O}(p)) \leq d(\sigma(i), x)$ for any $x \in cl(\mathcal{O}(p))$, using the triangle inequality and the glb argument from the previous case, we have

$$\mathbf{dist}_d(\sigma(i), \mathcal{O}(p)) \leq d(\sigma(i), x) \leq d(\sigma(i), s(t)) + d(s(t), x) \overset{(C.1)}{\Longrightarrow}$$
$$-[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) \leq d(s(t), x) \overset{(glb)}{\Longrightarrow}$$
$$-[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) \leq \mathbf{dist}_d(s(t), \mathcal{O}(p)) = -[\![p]\!]_C(s,t) \implies$$
$$[\![p]\!]_C(s,t) \leq [\![p]\!]_D(\mu,i) + \mathcal{E}(\Delta\tau)$$

By symmetry, we get

$$[\![p]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) \leq [\![p]\!]_C(s,t)$$

(3) Now, we prove the case where $\sigma(i) \in \mathcal{O}(p)$ and $s(t) \in X\backslash\mathcal{O}(p)$. Let $\varepsilon_D = [\![p]\!]_D(\mu,i)$ and $\varepsilon_C = -[\![p]\!]_C(s,t)$.

- Case $\varepsilon_D > 0$ and $\varepsilon_C > 0$: let $B_D = B_d(\sigma(i), \varepsilon_D)$ and $B_C = B_d(s(t), \varepsilon_C)$. Since $\sigma(i) \in \mathcal{O}(p)$ and $s(t) \in X\backslash\mathcal{O}(p)$, we have $B_D \subseteq \mathcal{O}(p)$ and $B_C \subseteq X\backslash\mathcal{O}(p)$. Hence, $B_D \cap B_C = \emptyset$, which implies that $\varepsilon_D + \varepsilon_C \leq d(\sigma(i), s(t))$.

- Case $\varepsilon_D = 0$ and $\varepsilon_C > 0$: $\sigma(i)$ is on the boundary of the set $\mathcal{O}(p)$ and, thus, on the boundary of the set $X \backslash \mathcal{O}(p)$. Since ε_C is the shortest distance from $s(t)$ to the boundary of the set $X \backslash \mathcal{O}(p)$, we get that $d(\sigma(i), s(t)) \geq \varepsilon_C = \varepsilon_D + \varepsilon_C$.
- Case $\varepsilon_D > 0$ and $\varepsilon_C = 0$: similarly to the previous case, we have $d(\sigma(i), s(t)) \geq \varepsilon_D = \varepsilon_D + \varepsilon_C$.
- Case $\varepsilon_D = 0$ and $\varepsilon_C = 0$: this case is included in the cases (1) or (2) above since both points belong to the same sets.

Therefore in every case, by using the inequality (C.1), we get

$$\varepsilon_D + \varepsilon_C \leq \mathcal{E}(\Delta\tau) \implies [\![p]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![p]\!]_C(s, t)$$

Moreover, since $[\![p]\!]_D(\mu, i) \geq 0$ and $[\![p]\!]_C(s, t) \leq 0$, we immediately get

$$[\![p]\!]_C(s, t) \leq [\![p]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)$$

(4) Similar to the previous case, when $s(t) \in \mathcal{O}(p)$ and $\sigma(i) \in X \backslash \mathcal{O}(p)$, then $\varepsilon_D = -[\![p]\!]_D(\mu, i)$ and $\varepsilon_C = [\![p]\!]_C(s, t)$

$$\varepsilon_D + \varepsilon_C \leq \mathcal{E}(\Delta\tau) \implies [\![p]\!]_C(s, t) \leq [\![p]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)$$

Moreover, since $[\![p]\!]_D(\mu, i) \leq 0$ and $[\![p]\!]_C(s, t) \geq 0$, we immediately get

$$[\![p]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![p]\!]_C(s, t)$$

Therefore, we conclude that for all $t \in T_i$ we have

$$[\![p]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![p]\!]_C(s, t) \leq [\![p]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)$$

Case $\phi = \neg\phi_1$: Let $\psi_1 = \mathbf{mtc}(\phi_1)$. By the induction hypothesis, for all $t \in T_i$, we have

$$\begin{gathered}
[\![\psi_1]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![\phi_1]\!]_C(s, t) \leq [\![\psi_1]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau) \implies \\
-[\![\neg\psi_1]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq -[\![\neg\phi_1]\!]_C(s, t) \leq -[\![\neg\psi_1]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau) \implies \\
[\![\neg\psi_1]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau) \geq [\![\neg\phi_1]\!]_C(s, t) \geq [\![\neg\psi_1]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \implies \\
[\![\psi]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![\phi]\!]_C(s, t) \leq [\![\psi]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)
\end{gathered}$$

Case $\phi = \phi_1 \vee \phi_2$: Let $\psi_1 = \mathbf{mtc}(\phi_1)$ and $\psi_2 = \mathbf{mtc}(\phi_2)$. By the induction hypothesis, we get that for $j = 1, 2$, for all $t \in T_i$, we have

$$[\![\psi_j]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![\phi_j]\!]_C(s, t) \leq [\![\psi_j]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)$$

Since $\sqcup$ is monotonic with respect to the relation $\leq$, for all $t \in T_i$, we have

$$\begin{gathered}
([\![\psi_1]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau)) \sqcup ([\![\psi_2]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau)) \leq [\![\phi_1]\!]_C(s, t) \sqcup [\![\phi_2]\!]_C(s, t) \leq \\
\leq ([\![\psi_1]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)) \sqcup ([\![\psi_2]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau)) \implies
\end{gathered}$$

$$
\begin{gathered}
([\![\psi_1]\!]_D(\mu,i) \sqcup [\![\psi_2]\!]_D(\mu,i)) - \mathcal{E}(\Delta\tau) \leq [\![\phi_1]\!]_C(s,t) \sqcup [\![\phi_2]\!]_C(s,t) \leq \\
\leq ([\![\psi_1]\!]_D(\mu,i) \sqcup [\![\psi_2]\!]_D(\mu,i)) + \mathcal{E}(\Delta\tau) \implies \\
[\![\psi_1 \vee \psi_2]\!]_D(\mu,i) - \mathcal{E}(\Delta\tau) \leq [\![\phi_1 \vee \phi_2]\!]_C(s,t) \leq [\![\psi_1 \vee \psi_2]\!]_D(\mu,i) + \mathcal{E}(\Delta\tau)
\end{gathered}
$$

Case $\phi = \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$: We have $\psi = \psi_1 \overset{\leftrightarrow}{\mathcal{U}}_{\mathcal{I}} \psi_2$, where $\psi_1 = \mathbf{mtc}(\phi_1)$ and $\psi_2 = \mathbf{mtc}(\phi_2)$. Let $J = \tau^{-1}(\tau(i) + \mathcal{I})$. By Lemma 42, we know that the set J is nonempty. Now let $t \in T_i$ and consider any $t' \in (t +_R \mathcal{I})$, which is a non-empty set by Lemma 42. Since $t +_R \mathcal{I} \subseteq \cup_{j \in J} T_j$, there exists some $j \in J$ such that $t' \in T_j$. Note that for all $l = i, i+1, \ldots, \max J$ (if J is a finite set), we have $T_l \neq \emptyset$. By the induction hypothesis, for all $\tilde{t} \in T_j$, we get that

$$
[\![\psi_2]\!]_D(\mu,j) - \mathcal{E}(\Delta\tau) \leq [\![\phi_2]\!]_C(s,\tilde{t}) \leq [\![\psi_2]\!]_D(\mu,j) + \mathcal{E}(\Delta\tau) \tag{C.2}
$$

and for all $k \in [i,j]$, for all $\bar{t} \in T_k$, we have

$$
[\![\psi_1]\!]_D(\mu,k) - \mathcal{E}(\Delta\tau) \leq [\![\phi_1]\!]_C(s,\bar{t}) \leq [\![\psi_1]\!]_D(\mu,k) + \mathcal{E}(\Delta\tau) \tag{C.3}
$$

Let $Q_k^{t,t'} = T_k \cap (t,t')$. Note that for any $k \in [i,j]$, we have $Q_k^{t,t'} \neq \emptyset$. From (C.3), for any $k \in [i,j]$, for all $\bar{t} \in Q_k^{t,t'}$, we have

$$
\bigsqcap_{t'' \in Q_k^{t,t'}} [\![\phi_1]\!]_C(s,t'') \leq [\![\phi_1]\!]_C(s,\bar{t}) \leq [\![\psi_1]\!]_D(\mu,k) + \mathcal{E}(\Delta\tau) \tag{C.4}
$$

Also, since $[\![\psi_1]\!]_D(\mu,k) - \mathcal{E}(\Delta\tau)$ is a lower bound on $[\![\phi_1]\!]_C(s,\cdot)$ over the set $Q_k^{t,t'}$ and $\bigsqcap_{t'' \in Q_k^{t,t'}} [\![\phi_1]\!]_C(s,t'')$ is the greatest lower bound, we have

$$
[\![\psi_1]\!]_D(\mu,k) - \mathcal{E}(\Delta\tau) \leq \bigsqcap_{t'' \in Q_k^{t,t'}} [\![\phi_1]\!]_C(s,t'') \tag{C.5}
$$

Then, using the last two inequalities and the monotonicity of $\sqcap$ with respect to the ordering relation $\leq$, we get

$$
\begin{gathered}
\bigsqcap_{k \in [i,j]} ([\![\psi_1]\!]_D(\mu,k) - \mathcal{E}(\Delta\tau)) \leq \bigsqcap_{k \in [i,j]} \bigsqcap_{t'' \in Q_k^{t,t'}} [\![\phi_1]\!]_C(s,t'') \leq \\
\leq \bigsqcap_{k \in [i,j]} ([\![\psi_1]\!]_D(\mu,k) + \mathcal{E}(\Delta\tau))
\end{gathered}
$$

Note that $\cup_{k=i}^{j} Q_k^{t,t'} = (t,t')$. We should point out that this is true only because we are using the matching until operator. If instead we were using the non-matching operator, then there would exist some $t \in T_i$ and some $t' \in (t +_R \mathcal{I})$

such that $\cup_{k=i}^{j-1} Q_k^{t,t'} \subset (t,t')$. Thus, we have

$$\begin{aligned} \bigsqcap_{k\in[i,j]} [\![\psi_1]\!]_D(\mu,k) - \mathcal{E}(\Delta\tau) \leq \bigsqcap_{t''\in(t,t')} [\![\phi_1]\!]_C(s,t'') \leq \\ \leq \bigsqcap_{k\in[i,j]} [\![\psi_1]\!]_D(\mu,k) + \mathcal{E}(\Delta\tau) \end{aligned} \tag{C.6}$$

Again, by using the monotonicity of $\sqcap$ and by pulling out the constant $\mathcal{E}(\Delta\tau)$ from the min operator, from (C.2) and (C.6), for any $t' \in T_j$, we have

$$\begin{aligned} \left([\![\psi_2]\!]_D(\mu,j) \sqcap \bigsqcap_{k\in[i,j]} [\![\psi_1]\!]_D(\mu,k) \right) - \mathcal{E}(\Delta\tau) \leq \\ \leq [\![\phi_2]\!]_C(s,t') \sqcap \bigsqcap_{t''\in(t,t')} [\![\phi_1]\!]_C(s,t'') \leq \\ \leq \left([\![\psi_2]\!]_D(\mu,j) \sqcap \bigsqcap_{k\in[i,j]} [\![\psi_1]\!]_D(\mu,k) \right) + \mathcal{E}(\Delta\tau) \end{aligned}$$

Let $P_j^t = T_j \cap (t +_R \mathcal{I})$. Note that if Assumption 45 does not hold, then it is not true that $P_j^t \neq \emptyset$. Next, we prove by contradiction that $P_j^t \neq \emptyset$ since Assumptions 45 and 47 hold.

Claim 58 *For any $j \in J$, the set $P_j^t = T_j \cap (t +_R \mathcal{I})$ is not empty.*

PROOF. First note that since $t \in T_i$, we have

$$\max\{0, \alpha(i-1)\} \leq t \leq \min\{\alpha(i+1), \sup R\} \tag{C.7}$$

Moreover, we have $T_j \neq \emptyset$ and $(t +_R \mathcal{I}) \neq \emptyset$. Assume now that $P_j^t = \emptyset$. We consider two cases which depend on $\mathcal{I}$:

(1) $\mathcal{I} = [\alpha i_1, +\infty)$ for some $i_1 \in \mathbb{N}$: This is possible only if R is unbounded or $i_1 = 0$, i.e., $\mathcal{I} = [0, +\infty)$. Since $j \in J$, we have

$$\begin{aligned} \tau(j) \in (\tau(i) +_R \mathcal{I}) \implies \alpha j \in (\alpha i +_R [\alpha i_1, +\infty)) \implies \\ \alpha j \in [\alpha i + \alpha i_1, +\infty) \cap R \implies \alpha j \geq \alpha(i+i_1) \implies i + i_1 \leq j \end{aligned} \tag{C.8}$$

Also, $P_j^t = \emptyset$ implies that

- either $\sup T_j < \inf(t +_R \mathcal{I})$, that is,

$$\begin{aligned} 0 \leq \min\{\alpha(j+1), \sup R\} < \inf([t+\alpha i_1, +\infty) \cap R) = \min\{0, t+\alpha i_1\} \implies \\ \min\{\alpha(j+1), \sup R\} < t + a i_1 \end{aligned}$$

$\sup R < t + \alpha i_1$ is a contradiction, because in this case $t +_R \mathcal{I} = \emptyset$. Thus,

$$\alpha(j+1) < t + \alpha i_1 \overset{(C.8)}{\implies} \alpha(i + i_1 + 1) < t + \alpha i_1 \implies \alpha(i+1) < t$$

which is a contradiction by eq. (C.7).

- or $\sup(t +_R \mathcal{I}) < \inf T_j$. If $\sup R = +\infty$, then this is immediately a contradiction. If R is bounded, then $\sup(t +_R [0, +\infty)) = \sup R < \inf T_j$, which is a contradiction since $T_j \neq \emptyset$.

(2) $\mathcal{I} = [\alpha i_1, \alpha i_2]$ for some $i_1, i_2 \in \mathbb{N}$ such that $i_1 < i_2$: R can be bounded or unbounded. In either case, we have $t +_R \mathcal{I} \subseteq R$ by assumption and, thus, $t +_R \mathcal{I} = t + \mathcal{I}$. Since $j \in J$, we have

$$\begin{gathered} \tau(j) \in (\tau(i) + \mathcal{I}) \implies \alpha j \in (\alpha i + [\alpha i_1, \alpha i_2]) \implies \\ \alpha j \in [\alpha i + \alpha i_1, \alpha i + \alpha i_2] \implies \\ \alpha(i + i_1) \leq \alpha j \leq \alpha(i + i_2) \implies i + i_1 \leq j \leq i + i_2 \end{gathered} \tag{C.9}$$

Also, $P_j^t = \emptyset$ implies that $\sup T_j < \inf(t + \mathcal{I})$ or $\sup(t + \mathcal{I}) < \inf T_j$. The case $\sup T_j < \inf(t + \mathcal{I})$ is the same as above. For the case $\sup(t + \mathcal{I}) < \inf T_j$, we have

$$\begin{gathered} \sup[t + \alpha i_1, t + \alpha i_2] < \alpha(j-1) \implies t + \alpha i_2 < \alpha(j-1) \overset{(C.9)}{\implies} \\ t + \alpha i_2 < \alpha(i + i_2 - 1) \implies t < \alpha(i-1) \end{gathered}$$

which is a contradiction by eq. (C.7). $\square$

Since $\cup_{j \in J} P_j^t = (t +_R \mathcal{I})$, similarly to the derivation of (C.6), for any $t \in T_i$, we get

$$\begin{gathered} \left(\bigsqcup_{j \in J} [\![\psi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{k \in [i,j]} [\![\psi_1]\!]_D(\mu, k) \right) - \mathcal{E}(\Delta\tau) \leq \\ \leq \bigsqcup_{t' \in (t +_R \mathcal{I})} [\![\phi_2]\!]_C(s, t') \sqcap \bigsqcap_{t'' \in (t, t')} [\![\phi_1]\!]_C(s, t'') \leq \\ \leq \left(\bigsqcup_{j \in J} [\![\psi_2]\!]_D(\mu, j) \sqcap \bigsqcap_{k \in [i,j]} [\![\psi_1]\!]_D(\mu, k) \right) + \mathcal{E}(\Delta\tau) \implies \\ [\![\psi]\!]_D(\mu, i) - \mathcal{E}(\Delta\tau) \leq [\![\phi]\!]_C(s, t) \leq [\![\psi]\!]_D(\mu, i) + \mathcal{E}(\Delta\tau) \end{gathered}$$