

# Robustness of Temporal Logic Specifications for Finite State Sequences in Metric Spaces

Technical Report MS-CIS-06-05

May, 2006

Georgios E. Fainekos<sup>1</sup> and George J. Pappas<sup>2</sup>

<sup>1</sup> Department of Computer and Information Science, Univ. of Pennsylvania  
fainekos @ cis.upenn.edu

<sup>2</sup> Department of Electrical and Systems Engineering, Univ. of Pennsylvania  
pappasg @ ee.upenn.edu

**Abstract.** In this paper, we consider the robust interpretation of metric temporal logic (MTL) formulas over timed sequences of states. For systems whose states are equipped with nontrivial metrics, such as continuous, hybrid, or general metric transition systems, robustness is not only natural, but also a critical measure of system performance. In this paper, we define robust, multi-valued semantics for MTL formulas, which capture not only the usual Boolean satisfiability of the formula, but also topological information regarding the distance,  $\varepsilon$ , from unsatisfiability. We prove that any other timed trace which remains  $\varepsilon$ -close to the initial one also satisfies the same MTL specification with the usual Boolean semantics. We derive a computational procedure for determining the robustness degree  $\varepsilon$  of the specification with respect to a given finite timed trace. Our approach can be used for robust system simulation and testing, as well as form the basis for simulation-based verification.

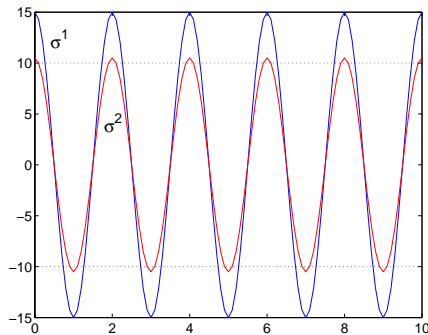
## 1 Introduction

Model checking [1] has been proven to be a very useful tool for the verification of the properties of software and hardware systems. Such systems can be represented by Boolean models, which are usually finite, and the properties to be verified are stated in modal or temporal logics with the Boolean valued semantics. The tools and methodologies developed for such systems do not naturally extend to systems whose state space is some general metric space, for example linear, nonlinear and hybrid systems. In this case, the model checking problem becomes harder and in most of the cases is undecidable [2]. Therefore, the verification of such systems still relies heavily on methods that involve monitoring and testing [3–6].

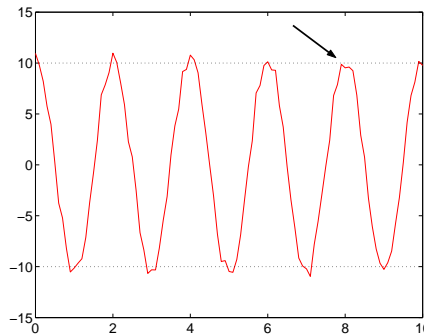
Furthermore, general metric transition systems either model physical processes or the interaction between some software and/or hardware system and the continuous physical world. Up to now no formal model exists that can capture accurately the behaviour of such a system – especially if it also exhibits

a chaotic behaviour. Moreover, these types of systems have a certain degree of sensitivity with respect to initial conditions or to system parameters [7, 8]. This has one major implication. Deciding the Boolean truth value of a temporal logic specification with respect to a system’s trajectory - in some of the cases - does not allow us to draw any conclusions about the real system. A small perturbation of the trajectory or the parameters of the system can lead to a different truth value for the formula.

For example, consider the trajectories  $\sigma^1$  and  $\sigma^2$  in Figure 1. Both of them satisfy the same specification “if the value of the state drops below -10, then it should also raise above 10 within 2 time units”. Nevertheless, a visual inspection of Figure 1 indicates that there exists a qualitative difference between  $\sigma^1$  and  $\sigma^2$ . The later “barely” satisfies the specification. Indeed as we can see in Figure 1, adding a bounded noise on  $\sigma^2$  renders the property unsatisfiable on  $\sigma^2$ .



**Fig. 1.** Two trajectories  $\sigma^1$  and  $\sigma^2$  which satisfy the specification:  $\Box(\pi_1 \rightarrow \Diamond_{\leq 2}\pi_2)$ . Here,  $\mathcal{O}(\pi_1) = \mathbb{R}_{\leq -10}$  and  $\mathcal{O}(\pi_2) = \mathbb{R}_{\geq 10}$ .



**Fig. 2.** The trajectory  $\sigma^2$  modified by random noise. The arrow points to the point in time where the property fails.

In order to differentiate between such trajectories of the system, we introduce the concept of robustness degree. Informally, we define the robustness degree to be the bound on the perturbation that the trajectory<sup>3</sup> can tolerate without changing the truth value of a specification expressed in the Linear [9] or Metric Temporal Logic [10]. To formally define the robustness degree, we take a topological perspective. We consider finite timed state sequences which take values in some space  $X$  equipped with a metric  $d$ . If these trajectories are of length  $n$ , then each sequence of states is isomorphic to a point in  $X^n$ , which is the space of all possible trajectories of length  $n$ . In order to quantify how close are

<sup>3</sup> We should bring to notice that we are not interested in the properties of the (possibly) continuous trajectory, but in the properties of its finite representation. Here, we model the finite representation of a continuous trajectory using timed state sequences. Under certain assumptions about the structure of the system, the results in this paper could be mapped back to the continuous case.

two different points  $\sigma^1$  and  $\sigma^2$  in  $X^n$ , we define the notion of distance using a metric  $\rho$  on the space  $X^n$  with definition  $\rho(\tau, \sigma) = \sup_{i \leq n} \{d(\sigma_i^1, \sigma_i^2)\}$ . Given an MTL formula  $\phi$ , we can partition the space  $X^n$  into two sets: the set  $P^\phi$  of state sequences that satisfy  $\phi$  and the set  $N^\phi$  of state sequences that do not satisfy  $\phi$ . Then the formal definition of robustness comes naturally, it is just the distance of a state sequence  $\sigma^1$  from the set  $P^\phi$  or its complement  $N^\phi$ . Using the degree of robustness and the metric  $\rho$ , we can define an open ball (tube) around  $\sigma^1$  and, therefore, we can be sure that any state sequence  $\sigma^2$  that remains within the open ball also stays either in  $P^\phi$  or in  $N^\phi$ .

However, the computation of the set  $P^\phi$  and, hence, the computation of the robustness degree are hard problems. To address them, we develop an algorithm that computes an under-approximation of the robustness degree. For that purpose, we use the formalism of multi-valued logics [11–14] in order to define robust semantics for MTL. Our definition is very similar to QLTL, but now the truth values of the MTL formulas range over the closure of the reals instead of the closed interval  $[0, 1]$ . The atomic propositions in the robust version of MTL evaluate to the distance from the current state in the timed state sequence to the subset of  $X$  that the atomic proposition represents. As established in the aforementioned works, the conjunction and disjunction in the Boolean logic are replaced by the min and max operations. Here, the logical negation is replaced by the usual negation of the reals. We prove that when an MTL formula is evaluated with robust semantics over a timed state sequence  $\mathcal{T}_1$ , then it returns an under-approximation  $\varepsilon$  of the robustness degree and, therefore, any other timed state sequence  $\mathcal{T}_2$  that remains  $\varepsilon$ -close to  $\mathcal{T}_1$  satisfies the same specification. We conclude the paper by presenting a monitoring algorithm (similar to [15, 16]) that is based on the robust semantics of MTL and computes the under-approximation of the robustness degree.

Application-wise the importance of the main contribution of this paper is straightforward: if a system has the property that under bounded disturbances its trajectories remain  $\delta$  close to the nominal one and, also, its robustness degree with respect to an MTL formula  $\phi$  is  $\varepsilon > \delta$  then we know that all the system’s trajectories also satisfy the same specification. The timing bounds on the temporal operators, that is the use of MTL instead of LTL, can be justified if one considers that the applications of such a framework are within the systems area. For example, signal processing and simulations of physical systems most of the times do require such constraints. The methodology that we present in this paper can be readily used in several applications such as Qualitative Simulation [17], verification using simulation [18] and in behavioral robotics [19].

Finally, we would like to point out that in the past several authors have also studied the robustness of real time specifications with respect to timed or dense time traces of real time systems [20–22], but the robustness is considered with respect to the timing constraints. The work which is the closest related to this paper appears in [13] where the authors give quantitative semantics to the branching-time logic CTL (called Discounted CTL) in order to achieve robust-

ness with respect to model perturbations. Model checking algorithms for the discounted CTL are also analyzed in that paper.

## 2 Metric Temporal Logic over Timed State Sequences

### 2.1 Metric Spaces

Let  $\mathbb{R}$  be the set of the real numbers,  $\mathbb{Q}$  the set of the rational numbers and  $\mathbb{N}$  the set of the natural numbers. We denote the extended real number line by  $\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$ . If  $(X, \leq)$  is a totally ordered set with an ordering relation  $\leq$ , then an interval of  $X$  is denoted by  $[a, b]_X = \{x \in X \mid a \leq x \leq b\}$ . When  $X = \mathbb{R}$ , we drop the subscript  $\mathbb{R}$ . In addition, we use pseudo-arithmetic expressions to represent certain subsets of the aforementioned sets. For example,  $\mathbb{R}_{\geq 0}$  denotes the subset of the reals whose elements are greater or equal to zero. If  $C$  is a set, then  $int(C)$ ,  $bd(C)$  and  $cl(C)$  denote<sup>4</sup> the *interior*, *boundary* and the *closure* of the set  $C$ . Let  $(X, d)$  be a metric space, i.e. a set  $X$  whose topology is induced by the metric  $d$ .

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

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

Using a metric  $d$ , we can define the distance of a point  $x \in X$  from a subset of  $C \subseteq X$ . Intuitively, this distance is the shortest distance from  $x$  to all the points in  $C$ . In a similar way, the depth of a point  $x$  in a set  $C$  is defined to be shortest distance of  $x$  from the boundary of  $C$ . Both the notions of distance and depth (Fig. 3) will play a fundamental role in the definition of the robustness degree (see Section 3).

**Definition 2 (Distance, Depth, Signed Distance [23] §8).** *Let  $x \in X$  be a point,  $C \subseteq X$  be a set and  $d$  be a metric. Then we define the*

- Distance from  $x$  to  $C$  to be  $\mathbf{dist}_d(x, C) := \inf\{d(x, y) \mid y \in cl(C)\}$
- Depth of  $x$  in  $C$  to be  $\mathbf{depth}_d(x, C) := \mathbf{dist}_d(x, X \setminus C)$
- Signed Distance from  $x$  to  $C$  to be

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

Note that if  $x \in bd(C)$ , then  $\mathbf{Dist}_d(x, C) = 0$ . We should point out that we use the extended definition of supremum and infimum, where  $\sup \emptyset = -\infty$  and  $\inf \emptyset = +\infty$ . Also of importance is the notion of an open ball of radius  $\varepsilon$  centered at a point  $x \in X$ .

<sup>4</sup> Formally, if  $C$  is a subset of a topological space  $X$ , then the interior of  $C$  is the union of all the open sets contained in  $C$ , while the closure of  $C$  is the intersection of all the closed sets which contain  $C$ . The boundary is  $bd(C) = cl(C) \setminus int(C)$ .

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

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

## 2.2 Timed State Sequences in Metric Spaces

In this paper, we use *timed state sequences* (TSS) to describe the behavior of a real-time system. Typical models of real time systems are the formalisms of hybrid automata, timed automata, linear and non-linear systems. A *state* of such a system is a point  $x$  in a metric space  $\mathcal{X} = (X, d)$ . With each state of the system  $x$  we associate a *time period*  $\Delta t$ , which represents the duration between the occurrence of the current and the previous system states.

Let  $AP$  be a finite set of atomic propositions, then the *predicate mapping*  $\mathcal{O} : AP \rightarrow 2^X$  is a set valued function that assigns to each atomic proposition  $\pi \in AP$  a set of states  $\mathcal{O}(\pi) \subseteq X$ . Furthermore, if the collection of sets  $\{\mathcal{O}(\pi)\}_{\pi \in AP}$  is not a cover of  $X$ , i.e.  $\cup_{\pi \in AP} \mathcal{O}(\pi) \neq X$ , then we add to  $AP$  a special proposition  $\pi_c$  that maps to the set  $\mathcal{O}(\pi_c) = X \setminus \cup_{\pi \in AP} \mathcal{O}(\pi)$ . Therefore, we can now define the “inverse” map of  $\mathcal{O}$  as  $\mathcal{O}^{-1}(x) = \{\pi \in AP \mid x \in \mathcal{O}(\pi)\}$  for  $x \in X$ . Finally, we overload the notation to extend the definition of  $\mathcal{O}$  over boolean combinations of atomic propositions in the natural way:  $\mathcal{O}(\pi_1 \vee \pi_2) = \mathcal{O}(\pi_1) \cup \mathcal{O}(\pi_2)$  and  $\mathcal{O}(\neg\pi) = X \setminus \mathcal{O}(\pi)$ . If  $x \in \mathcal{O}(\pi)$ , then we say that  $x$  is a  $\pi$  state. Notice that using the notion of distance, we can quantify how close is a state  $x$  to becoming a  $\pi$  state.

The execution of a system can result in an infinite or finite sequence of states. In this paper, we focus on finite sequences of states.

**Definition 4 (TSS).** A *timed state sequence*  $\mathcal{T}$  is a tuple  $(\sigma, \tau, \mathcal{O})$  where:  $\sigma = x_0, x_1, \dots, x_n$  is a sequence of states,  $\tau = \Delta t_0, \Delta t_1, \dots, \Delta t_n$  is a sequence of time periods and  $\mathcal{O}$  is a predicate mapping such that  $n \in \mathbb{N}$ ,  $x_i \in X$  and  $\Delta t_i \in \mathbb{R}_{\geq 0}$  for all  $i \in \{0, 1, \dots, n\}$  and  $t_0, t_1, \dots, t_n$ , where  $t_i = \sum_{j=0}^i \Delta t_j$ , is a strictly monotonically increasing sequence.

We let  $\sigma_i$  and  $\tau_i$  denote  $x_i$  and  $\Delta t_i$  respectively. By convention, we set  $\Delta t_0 = 0$ . We define  $\sigma \downarrow_i$  to be the prefix of the state sequence  $\sigma$ , i.e.  $\sigma \downarrow_i = x_0, x_1, \dots, x_i$ , while  $\sigma \uparrow_i$  is the suffix, i.e.  $\sigma \uparrow_i = x_i, x_{i+1}, \dots, x_n$ . The length of  $\sigma = x_0, x_1, \dots, x_n$  is defined to be  $|\sigma| = n + 1$ . For convenience, we let  $|\mathcal{T}| = |\tau| = |\sigma|$  and  $\mathcal{T} \uparrow_i = (\sigma \uparrow_i, \tau \uparrow_i, \mathcal{O})$  (similarly for  $\downarrow$ ).

In the following, we use the convention that  $\mathcal{T}$  and  $\mathcal{S}$  denote the timed state sequences  $\mathcal{T} = (\sigma, \tau, \mathcal{O})$  and  $\mathcal{S} = (\sigma', \tau, \mathcal{O})$  (and similarly for their primed or superscripted versions). We define  $\Sigma_X$  to be the set of all possible timed state sequences in the space  $\mathcal{X} = (X, d)$  and  $\Sigma(\mathcal{T})$  to be the set of all possible timed state sequences with the same predicate mapping  $\mathcal{O}$  and the same sequence of time stamps as  $\mathcal{T}$ . That is  $\Sigma(\mathcal{T}) = \{(\sigma', \tau, \mathcal{O}) \mid \sigma' \in X^{|\mathcal{T}|}\}$ . Notice that the sequence  $\sigma$  is isomorphic to a point in the product space  $X^{|\sigma|}$ .

### 2.3 Metric Temporal Logic over Finite Timed State Sequences

The Metric Temporal Logic (MTL) [10] is an extension of the Linear Temporal Logic (LTL) [9]. In MTL, the syntax of the logic is extended to include timing constraints on the usual temporal operators of LTL. Using LTL specifications we can check qualitative timing properties, while with MTL specifications quantitative timing properties. Recently, it was shown by Ouaknine and Worrell [24] that MTL is decidable over finite timed state sequences. In this section, we review the basics of MTL with point-based semantics (as opposed to interval based semantics [25]) over finite timed state sequences.

**Definition 5 (Syntax of MTL).** *An MTL formula  $\phi$  is inductively defined according to the grammar*

$$\phi ::= \top \mid \pi \mid \neg\phi_1 \mid \phi_1 \vee \phi_2 \mid \bigcirc_{\mathcal{I}} \phi_1 \mid \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$$

where  $\pi \in AP$ ,  $\top$  is the symbol for the boolean constant true and  $\mathcal{I}$  is an interval of  $\mathbb{R}_{\geq 0}$  with rational endpoints.

Even though we can derive the constant true ( $\top$ ) from the law of excluded middle ( $\top = \pi \vee \neg\pi$ ), we chose to add it in the syntax of MTL for reasons that will be clear in Section 3. The constant *false* is denoted by  $\perp = \neg\top$ . We can also derive additional temporal operators such as *release*  $\phi_1 \mathcal{R}_{\mathcal{I}} \phi_2 = \neg((\neg\phi_1) \mathcal{U}_{\mathcal{I}} \neg\phi_2)$  (which is the dual of the until operator), *unless*  $\phi_1 \mathcal{W}_{\mathcal{I}} \phi_2 = \square_{\mathcal{I}} \phi_1 \vee \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$ , *weak next*  $\bigodot_{\mathcal{I}} \phi = \neg \bigcirc_{\mathcal{I}} \neg\phi$  (which is the dual of the next operator), *eventually*  $\diamond_{\mathcal{I}} \phi = \top \mathcal{U}_{\mathcal{I}} \phi$  and *always*  $\square_{\mathcal{I}} \phi = \perp \mathcal{R}_{\mathcal{I}} \phi$ . In the case where  $\mathcal{I} = [0, +\infty)$ , we remove the subscript  $\mathcal{I}$  from the temporal operators, i.e. we just write  $\mathcal{U}$ ,  $\mathcal{R}$ ,  $\bigcirc$ ,  $\diamond$  and  $\square$ . When all the subscripts of the temporal operators are of the form  $[0, +\infty)$ , then the MTL formula  $\phi$  reduces to an LTL formula and we can ignore the time stamps.

The subscript  $\mathcal{I}$  imposes timing constraints on the temporal operators. The interval  $\mathcal{I}$  can be open, half-open or closed, bounded or unbounded. The function *lb* returns the lower (or left) bound of the interval  $\mathcal{I}$  whereas the function *ub* returns the upper (or right) bound. Note that  $lb(\mathcal{I}), ub(\mathcal{I}) \in \mathbb{Q}_{\geq 0}$  and that it could be the case that  $ub(\mathcal{I}) = lb(\mathcal{I})$ , i.e.  $\mathcal{I}$  is a singleton. For any  $t \in \mathbb{Q}$ , we define  $\mathcal{I} + t = \{t' + t \mid t' \in \mathcal{I}\}$ . Also, we do not consider relative [15] and absolute congruences [26] and we have not included the *since* and *last* temporal operators (the past fragment) in the syntax of MTL.

Metric Temporal Logic (MTL) formulas are interpreted over timed state sequences  $\mathcal{T}$  with  $|\mathcal{T}| > 0$ . The constraint  $|\mathcal{T}| > 0$  implies that the sequence has at least one state, that is we ignore the pathological cases of empty state sequences. In this paper, we denote formula satisfiability using a membership function  $\langle\langle\phi\rangle\rangle : \Sigma_{\mathcal{X}} \rightarrow \{\perp, \top\}$  instead of the usual notation  $\mathcal{T} \models \phi$ . The functional approach enables us to maintain a uniform presentation throughout this paper. We say that a timed state sequence  $\mathcal{T}$  satisfies the formula  $\phi$  when  $\langle\langle\phi\rangle\rangle(\mathcal{T}) = \top$ . In this case,  $\mathcal{T}$  is a *model* of  $\phi$ . The set of all models of  $\phi$  is denoted by  $\mathcal{L}(\phi)$ , i.e.  $\mathcal{L}(\phi) = \{\mathcal{T} \in \Sigma_{\mathcal{X}} \mid \langle\langle\phi\rangle\rangle(\mathcal{T}) = \top\}$ .

**Definition 6 (Semantics of MTL).** Let  $\mathcal{T} = (\sigma, \tau, \mathcal{O})$ ,  $\pi \in AP$ ,  $i, j \in \mathbb{N}$  and  $K_{\mathcal{I}}^{\mathcal{T}} = \{i \in [0, |\mathcal{T}| - 1]_{\mathbb{N}} \mid t_i \in \mathcal{I}\}$ , then the semantics of  $\phi$  are

$$\begin{aligned}
\langle\langle \top \rangle\rangle(\mathcal{T}) &:= \top \\
\langle\langle \pi \rangle\rangle(\mathcal{T}) &:= \sigma_0 \in \mathcal{O}(\pi) \\
\langle\langle \neg\psi \rangle\rangle(\mathcal{T}) &:= \neg\langle\langle \psi \rangle\rangle(\mathcal{T}) \\
\langle\langle \phi_1 \vee \phi_2 \rangle\rangle(\mathcal{T}) &:= \langle\langle \phi_1 \rangle\rangle(\mathcal{T}) \vee \langle\langle \phi_2 \rangle\rangle(\mathcal{T}) \\
\langle\langle \bigcirc_{\mathcal{I}}\psi \rangle\rangle(\mathcal{T}) &:= \begin{cases} (\tau_1 \in \mathcal{I}) \wedge \langle\langle \psi \rangle\rangle(\mathcal{T}\uparrow_1) & \text{if } |\mathcal{T}| > 1 \\ \perp & \text{otherwise} \end{cases} \\
\langle\langle \phi_1 \mathcal{U}_{\mathcal{I}}\phi_2 \rangle\rangle(\mathcal{T}) &:= \bigvee_{i=0}^{|\mathcal{T}|-1} ((i \in K_{\mathcal{I}}^{\mathcal{T}}) \wedge \langle\langle \phi_2 \rangle\rangle(\mathcal{T}\uparrow_i) \wedge \bigwedge_{j=0}^{i-1} \langle\langle \phi_1 \rangle\rangle(\mathcal{T}\uparrow_j))
\end{aligned}$$

Informally, the path formula  $\phi_1 \mathcal{U}_{[a,b]}\phi_2$  expresses the property that over the timed state sequence  $\mathcal{T}$  and in the time interval  $[a, b]$ ,  $\phi_2$  becomes true and for all previous time  $\phi_1$  holds. The usual (unbounded) semantics of until are captured by the specification  $\phi_1 \mathcal{U}_{[0,+\infty)}\phi_2$ . The formula  $\diamond_{[a,b]}\phi$  indicates that the subformula  $\phi$  becomes true sometime in  $[a, b]$ , whereas the formula  $\square_{[a,b]}\phi$  indicates that  $\phi$  is always true over  $\sigma$  during the time interval  $[a, b]$ . Note that the bounds on the temporal operators express timing conditions with respect to the occurrence of a previous event. For example, the formula  $\pi_1 \mathcal{U}_{[a,b]}(\pi_2 \mathcal{U}_{[c,d]}\pi_3)$  specifies that the event  $\pi_2$  should occur before time  $b$  and the event  $\pi_3$  should happen before time  $b + d$ .

### 3 Robust Satisfaction of MTL Specifications

#### 3.1 Toward a Notion of Robust Satisfaction

In this section, we define what it means for a timed state sequence (taking values in some metric space) to satisfy a Metric Temporal Logic specification *robustly*. In the case of the timed state sequences that we consider in this paper, we can quantify how close are two different state sequences by using the metric  $d$ . Let  $\mathcal{T} = (\sigma, \tau, \mathcal{O})$  be a timed state sequence and  $(\sigma', \tau, \mathcal{O}) \in \Sigma(\mathcal{T})$ , then

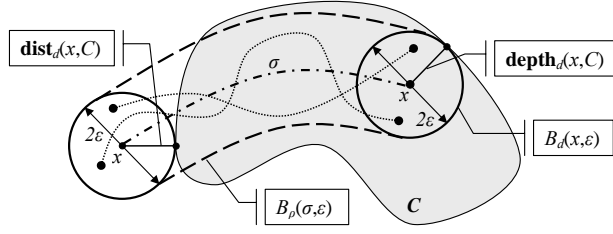
$$\rho(\sigma, \sigma') = \max\{d(\sigma_i, \sigma'_i) \mid i \in [0, |\sigma| - 1]_{\mathbb{N}}\} \quad (1)$$

is a metric on the set  $X^{|\mathcal{T}|}$ , which is well defined since  $|\mathcal{T}|$  is finite. Now that the space of state sequences is equipped with a metric, we can define a tube around a timed state sequence  $\mathcal{T}$ . Given an  $\varepsilon > 0$ , we let

$$\Sigma_{\varepsilon}(\mathcal{T}) = \{(\sigma', \tau, \mathcal{O}) \in \Sigma(\mathcal{T}) \mid \sigma' \in B_{\rho}(\sigma, \varepsilon)\}$$

to be the set of all timed state sequences that remain  $\varepsilon$ -close to  $\mathcal{T}$ .

Informally, we define the degree of robustness that a timed state sequence  $\mathcal{T}$  satisfies an MTL formula  $\phi$  to be a number  $\varepsilon \in \overline{\mathbb{R}}$ . Intuitively, a positive  $\varepsilon$  means that the formula  $\phi$  is satisfiable and, moreover, that all the other timed state



**Fig. 3.** A tube (dashed lines) around a nominal state sequence  $\sigma$  (dash-dotted line). The tube encloses a set of state sequences (dotted lines). Also, the definition of distance and depth and the associated neighborhoods.

sequences that remain  $\varepsilon$ -close to the nominal one also satisfy  $\phi$ . Accordingly, if  $\varepsilon$  is negative, then  $\mathcal{T}$  does not satisfy  $\phi$  and all the other timed state sequences that remain within the open tube of radius  $|\varepsilon|$  also do not satisfy  $\phi$ .

**Definition 7 (Robustness Degree).** Let  $\phi$  be an MTL formula,  $\mathcal{T} \in \Sigma_X$  and  $\rho$  be the metric (1). Define  $P_{\mathcal{T}}^{\phi} := \{\sigma' \mid (\sigma', \tau, \mathcal{O}) \in \Sigma(\mathcal{T}) \cap \mathcal{L}(\phi)\}$ , then the robustness degree  $\varepsilon \in \overline{\mathbb{R}}$  of  $\mathcal{T}$  is defined as  $\varepsilon := \mathbf{Dist}_{\rho}(\sigma, P_{\mathcal{T}}^{\phi})$ .

*Remark 1.*  $P_{\mathcal{T}}^{\phi}$  is the set of all models with time stamp sequence  $\tau$  that satisfy  $\phi$ . If we define  $N_{\mathcal{T}}^{\phi} := \{\sigma' \mid (\sigma', \tau, \mathcal{O}) \in \Sigma(\mathcal{T}) \cap \Sigma_X \setminus \mathcal{L}(\phi)\}$ , then the set  $\{P_{\mathcal{T}}^{\phi}, N_{\mathcal{T}}^{\phi}\}$  forms a partition of the set  $X^{|\mathcal{T}|}$ . Therefore, we have duality  $P_{\mathcal{T}}^{\phi} = X^{|\mathcal{T}|} \setminus N_{\mathcal{T}}^{\phi}$  and  $N_{\mathcal{T}}^{\phi} = X^{|\mathcal{T}|} \setminus P_{\mathcal{T}}^{\phi}$ .

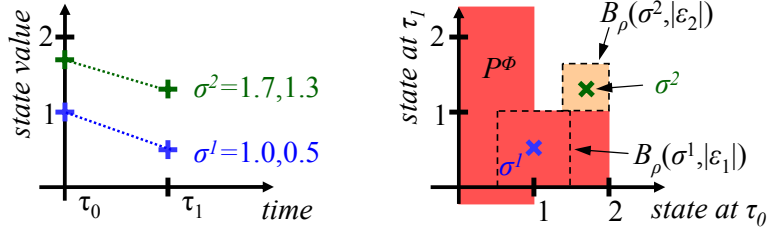
The following proposition is derived directly from the definitions. It states that all the timed state sequences  $\mathcal{S}$ , which have distance from  $\mathcal{T}$  less than the robustness degree of  $\mathcal{T}$  with respect to  $\phi$ , satisfy the same specification  $\phi$  as  $\mathcal{T}$ .

**Proposition 1.** Let  $\phi$  be an MTL formula,  $\mathcal{T} \in \Sigma_X$  and  $\varepsilon = \mathbf{Dist}_{\rho}(\sigma, P_{\mathcal{T}}^{\phi})$ . If  $|\varepsilon| > 0$ , then  $\langle\langle \phi \rangle\rangle(\mathcal{S}) = \langle\langle \phi \rangle\rangle(\mathcal{T})$  for all  $\mathcal{S} \in \Sigma_{|\varepsilon|}(\mathcal{T})$ .

*Remark 2.* If  $\varepsilon = 0$ , then the truth value of  $\phi$  with respect to  $\mathcal{T}$  is not robust, i.e. any small perturbation of a critical state in the timed state sequence can change the satisfiability of the formula with respect to  $\mathcal{T}$ .

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

*Example 1.* Assume that we are given the specification  $\phi = \pi_1 \mathcal{U} \pi_2$  such that  $\mathcal{O}(\pi_1) = [1, 2]$  and  $\mathcal{O}(\pi_2) = [0, 1]$ . Consider now two timed state sequences  $\mathcal{T}_1 = (\sigma^1, \tau, \mathcal{O})$  and  $\mathcal{T}_2 = (\sigma^2, \tau, \mathcal{O})$  such that  $\sigma^1 = 1, 0.5$  and  $\sigma^2 = 1.7, 1.3$ . In this simple case, we have  $P^{\phi} = P_{\mathcal{T}_1}^{\phi} = P_{\mathcal{T}_2}^{\phi} = [0, 1] \times \mathbb{R} \cup [1, 2] \times [0, 1]$  (see Figure 4). Therefore,  $\varepsilon_1 = \mathit{Dist}(\sigma^1, P^{\phi}) = 0.5$  and  $\varepsilon_2 = \mathit{Dist}(\sigma^2, P^{\phi}) = -0.3$ .



**Fig. 4.** On the left is the space of state sequences of length 2, while on the right is the time-domain representation of the timed state sequences  $\mathcal{T}_1$  and  $\mathcal{T}_2$  of Example 1.

Theoretically, the set  $P_{\mathcal{T}}^{\phi}$  (or  $N_{\mathcal{T}}^{\phi}$ ) can be computed. A naive, but straightforward, way to construct the set  $P_{\mathcal{T}}^{\phi}$  is as follows. Instead of timed state sequences in a metric space  $X$ , let us consider finite timed state sequences where each state is a set of atomic propositions. We will refer to the later as timed words for clarity. In more detail, consider the timed word  $\mathcal{T}_w = (\xi, \tau)$  where for all  $i = 0, 1, \dots, |\mathcal{T}_w| - 1$  it is  $\xi_i \in \overline{AP} = 2^{AP} \setminus \emptyset$ . In [24], it was proven the one can construct an acceptor  $\mathcal{A}_{\phi}$  (in the form of a timed alternating automaton with one clock) for the finite models  $\mathcal{T}_w$  of any formula  $\phi$  in the logic MTL with the standard semantics (that is  $\langle\langle \pi \rangle\rangle(\mathcal{T}_w) := \pi \in \xi_0$ ). Assume now that we are given an MTL formula  $\phi$ , a sequence of time stamps  $\tau$  and a predicate mapping  $\mathcal{O}$ . For that particular  $\tau$ , we can find the set  $TW_{\tau}$  of timed words  $(\xi, \tau)$  that are accepted by  $\mathcal{A}_{\phi}$ . One way to do so is to construct the set  $UW_{\tau}$  of all possible untimed words  $\xi$  of length  $|\tau|$ , that is  $UW_{\tau} = \overline{AP}^{|\tau|}$ , and, then, for each  $\xi \in UW_{\tau}$  verify whether  $(\xi, \tau)$  is accepted by  $\mathcal{A}_{\phi}$ , i.e. whether  $(\xi, \tau) \in \mathcal{L}(\mathcal{A}_{\phi})$ . In other words,  $\mathcal{L}'_{\tau}(\phi) = TW_{\tau} \cap \mathcal{L}(\mathcal{A}_{\phi})$ . This can be done in time  $O(|\tau| |\overline{AP}|^{|\tau|})$  since given the automaton  $\mathcal{A}_{\phi}$  it takes linear time in the length of the timed word to decide whether the word is in the language or not. From the set  $\mathcal{L}'_{\tau}(\phi)$ , we can easily derive the set  $P_{\mathcal{T}}^{\phi} = \bigcup_{\xi \in \mathcal{L}'_{\tau}(\phi)} ((\cap_{\pi \in \xi_0} \mathcal{O}(\pi)) \times \dots \times (\cap_{\pi \in \xi_{|\tau|-1}} \mathcal{O}(\pi)))$ .

*Remark 3.* In the case where the logic is LTL the construction of the set  $P_{\mathcal{T}}^{\phi}$  can be slightly improved. Giannakopoulou and Havelund [27] have developed an efficient algorithm for the translation of LTL formulas over finite traces to finite automata. In turn, we can use methodologies as in [28] to randomly generate words of fixed length in the language of the finite automaton and thus under-approximate the set  $P_{\mathcal{T}}^{\phi}$ .

### 3.2 Computing an Under-Approximation of the Robustness Degree

The aforementioned theoretical construction of the set  $P_{\mathcal{T}}^{\phi}$  cannot be of any practical interest. Moreover, the definition of robustness degree involves a number of set operations (union, intersection and complementation) in the possibly high dimensional space  $X$ , which can be computationally expensive in practice. Therefore in this section, we develop an algorithm that computes the robustness

degree  $\varepsilon$  by directly operating on the timed state sequence while avoiding set operations.

In order to define robust semantics for MTL, we must extend the classical notion of formula satisfiability to the multi-valued case. In this framework, each formula takes truth values over a finite or infinite set of values that have an associated partial or total order relation (for a survey see [29]). In this paper, we differentiate from previous works [11–13] by providing the definition of multi-valued semantics for MTL based on robustness considerations.

Let  $\mathfrak{R} = (\overline{\mathbb{R}}, \leq)$  be the closure of the reals with the usual ordering relation. We define the binary operators  $\sqcup : \overline{\mathbb{R}} \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$  and  $\sqcap : \overline{\mathbb{R}} \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$  using the maximum and minimum functions as  $x \sqcup y := \max\{x, y\}$  and  $x \sqcap y := \min\{x, y\}$ . Also, for some  $R \subseteq \overline{\mathbb{R}}$  we extend the above definitions as follows  $\bigsqcup R := \sup R$  and  $\bigsqcap R := \inf R$ . Recall that  $\bigsqcup \overline{\mathbb{R}} = +\infty$  and  $\bigsqcap \overline{\mathbb{R}} = -\infty$  and that any subset of  $\overline{\mathbb{R}}$  has a supremum and infimum. Finally, because  $\mathfrak{R}$  is a totally ordered set, it is distributive, i.e. for all  $a, b, c \in \overline{\mathbb{R}}$  it is  $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$  (and its order dual).

We propose multi-valued semantics for the Metric Temporal Logic where the valuation function on the atomic propositions takes values over the totally ordered set  $\mathfrak{R}$  according to the metric  $d$  operating on the state space  $X$  of the timed state sequence  $\mathcal{T}$ . For this purpose, we let the valuation function to be the signed distance from the current point in the trace  $x$  to a set  $C$  labeled by the atomic proposition. Intuitively, this distance represents how robustly is a point  $x$  within a set  $C$ . If this metric is zero, then even the smallest perturbation of the point can drive it inside or outside the set  $C$ , dramatically affecting membership.

For the purposes of the following discussion, we use the notation  $\llbracket \phi \rrbracket(\mathcal{T})$  to denote the robustness estimate with which the structure  $\mathcal{T}$  satisfies the specification  $\phi$  (formally  $\llbracket \phi \rrbracket : \Sigma_X \rightarrow \overline{\mathbb{R}}$ ).

**Definition 8 (Robust Semantics of MTL).** *For an MTL formula  $\phi$  and  $\mathcal{T} \in \Sigma_X$ , the robust semantics of  $\phi$  with respect to  $\mathcal{T}$  are defined as (let  $\pi \in AP$  and  $K_{\mathcal{T}}^{\mathcal{T}} = \{i \in [0, |\mathcal{T}| - 1]_{\mathbb{N}} \mid \sum_{j=0}^i \Delta t_j \in \mathcal{I}\}$ )*

$$\begin{aligned}
\llbracket \top \rrbracket(\mathcal{T}) &:= +\infty \\
\llbracket \pi \rrbracket(\mathcal{T}) &:= \mathbf{Dist}_a(\sigma_0, \mathcal{O}(\pi)) \\
\llbracket \neg \psi \rrbracket(\mathcal{T}) &:= -\llbracket \psi \rrbracket(\mathcal{T}) \\
\llbracket \phi_1 \vee \phi_2 \rrbracket(\mathcal{T}) &:= \llbracket \phi_1 \rrbracket(\mathcal{T}) \sqcup \llbracket \phi_2 \rrbracket(\mathcal{T}) \\
\llbracket \bigcirc_{\mathcal{I}} \psi \rrbracket(\mathcal{T}) &:= \begin{cases} \llbracket \tau_1 \in \mathcal{I} \rrbracket(\mathcal{T}) \sqcap \llbracket \psi \rrbracket(\mathcal{T} \uparrow_1) & \text{if } |\mathcal{T}| > 1 \\ -\infty & \text{otherwise} \end{cases} \\
\llbracket \phi_1 \mathcal{U}_{\mathcal{T}} \phi_2 \rrbracket(\mathcal{T}) &:= \bigsqcap_{i=0}^{|\mathcal{T}|-1} (\llbracket i \in K_{\mathcal{T}}^{\mathcal{T}} \rrbracket(\mathcal{T}) \sqcap \llbracket \phi_2 \rrbracket(\mathcal{T} \uparrow_i) \sqcap \bigsqcap_{j=0}^{i-1} \llbracket \phi_1 \rrbracket(\mathcal{T} \uparrow_j))
\end{aligned}$$

where the unary operator  $(-)$  is defined to be the negation over the reals.

*Remark 4.* 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  $a, b \in \overline{\mathbb{R}}$ .

The following proposition states the relationship between the usual and the robust semantics of MTL (the proof uses induction on the structure of  $\phi$ ; see Appendix B).

**Proposition 2.** *Let  $\phi$  be an MTL formula and  $\mathcal{T} \in \Sigma_X$ , then*

- |   |  |
|---|--|
| (1) $\llbracket \phi \rrbracket(\mathcal{T}) > 0 \Rightarrow \langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$  | (2) $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top \Rightarrow \llbracket \phi \rrbracket(\mathcal{T}) \geq 0$  |
| (3) $\llbracket \phi \rrbracket(\mathcal{T}) < 0 \Rightarrow \langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ | (4) $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp \Rightarrow \llbracket \phi \rrbracket(\mathcal{T}) \leq 0$ |

Note that the equivalence fails 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, the point is classified to belong to that set even if the set is open in the topology.

**Theorem 1.** *Given an MTL formula  $\phi$  and  $\mathcal{T} \in \Sigma_X$ , then*

$$\llbracket \phi \rrbracket(\mathcal{T}) \leq |\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi)| \quad (2)$$

*In more detail,  $-\mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\phi) \leq \llbracket \phi \rrbracket(\mathcal{T}) \leq \mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi)$ .*

In the above theorem, the equality in  $\llbracket \phi \rrbracket(\mathcal{T}) \leq |\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi)|$  fails for two reasons. First, due to the Boolean combinations of atomic propositions (see Remark 5 in Appendix C). This can be easily remedied by introducing a new symbol for each Boolean combination of atomic propositions. Second, and more importantly, due to the fact that the state sequences in  $B_\rho(\sigma, |\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi)|)$  can satisfy or falsify the specification  $\phi$  at different time instants than  $\mathcal{T}$ . The robust MTL semantics as defined above cannot capture this. In a sense,  $\llbracket \phi \rrbracket(\mathcal{T})$  returns the “diameter” of the tube of the timed state sequences that satisfy  $\phi$  at least at the same time instant as  $\mathcal{T}$ . Going back to Example 1, it is easy to verify that  $\llbracket \phi \rrbracket(\mathcal{T}_1) = 0$ .

The above discussion gives pointers on how we can get equality in (2). Consider the MTL fragment where the only allowed operators are the conjunction and always. Let us denote this fragment of MTL by  $\Phi_{\text{MTL}}(\wedge, \square)$ . In this fragment, the negation ( $\neg$ ) can appear only in front of atomic propositions. Note though that  $\Phi_{\text{MTL}}(\wedge, \square)$  is still an interesting fragment of the logic since it can capture invariance specifications. Now, using the syntactic equivalences  $\square\square\phi \equiv \square\phi$  and  $\square(\phi_1 \wedge \phi_2) = \square\phi_1 \wedge \square\phi_2$ , any formula  $\phi \in \Phi_{\text{MTL}}(\wedge, \square)$  can be rewritten as  $\phi = (\bigwedge_{\pi \in AP_1} \pi) \wedge \square(\bigwedge_{\pi \in AP_2} \pi)$ , where  $AP_1$  and  $AP_2$  are sets of (possibly negated) atomic propositions. Following the proof of Theorem 1, it can be shown that if  $\phi \in \Phi_{\text{MTL}}(\wedge, \square)$  and  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$ , that is, if the formula  $\phi$  holds over the TSS  $\mathcal{T}$ , then  $\llbracket \phi \rrbracket(\mathcal{T}) = \mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi)$ . Moreover, due to the duality of  $\wedge$  and  $\vee$ , the equality in (2) holds also when  $\phi \in \Phi_{\text{MTL}}(\vee, \diamond)$  and  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ .

From Proposition 1 and Theorem 1 we derive the next theorem as a corollary.

**Theorem 2.** *Given an MTL formula  $\phi$  and  $\mathcal{T} \in \Sigma_X$ , if  $\llbracket \phi \rrbracket(\mathcal{T}) = \varepsilon$  and  $|\varepsilon| > 0$ , then  $\langle\langle \phi \rangle\rangle(\mathcal{S}) = \langle\langle \phi \rangle\rangle(\mathcal{T})$  for all  $\mathcal{S} \in \Sigma_{|\varepsilon|}(\mathcal{T})$ .*

Theorem 2 has several implications. First of all, in the simplest case where we just simulate the response of a system, we can derive bounds for the magnitude of the disturbances that the system can tolerate while still satisfying the same MTL specification. Along the same lines, systems of difference equations [8] sometimes have continuous dependence on initial conditions and/or parameters, which implies that if a parameter of the system is bounded then all the possible trajectories remain close to the initial trajectory. Second, we can use approximation metrics [30] in order to verify a system using simulations [31].

## 4 Monitoring the Robustness of Temporal Properties

In this section, we present a procedure that computes how robustly a timed state sequence  $\mathcal{T}$  satisfies a specification  $\phi$  stated in the Metric Temporal Logic. For this purpose, we design an monitoring algorithm based on the classical and robust semantics of MTL.

Starting from the definition of the semantics of the until operator, we can derive an equivalent recursive formulation (see also [15]):

$$\llbracket \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2 \rrbracket (\mathcal{T}) = \begin{cases} ((0 \in \mathcal{I}) \wedge \llbracket \phi_2 \rrbracket (\mathcal{T})) \vee \\ \vee (\llbracket \phi_1 \rrbracket (\mathcal{T}) \wedge \llbracket \phi_1 \mathcal{U}_{\mathcal{I}-\Delta t_1} \phi_2 \rrbracket (\mathcal{T}\uparrow_1)) & \text{if } |\mathcal{T}| > 1 \\ (0 \in \mathcal{I}) \wedge \llbracket \phi_2 \rrbracket (\mathcal{T}) & \text{otherwise} \end{cases}$$

A similar recursive formulation holds for the robust MTL semantics.

$$\llbracket \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2 \rrbracket (\mathcal{T}) = \begin{cases} (\llbracket 0 \in \mathcal{I} \rrbracket (\mathcal{T}) \sqcap \llbracket \phi_2 \rrbracket (\mathcal{T})) \sqcup \\ \sqcup (\llbracket \phi_1 \rrbracket (\mathcal{T}) \sqcap \llbracket \phi_1 \mathcal{U}_{\mathcal{I}-\Delta t_1} \phi_2 \rrbracket (\mathcal{T}\uparrow_1)) & \text{if } |\mathcal{T}| > 1 \\ \llbracket 0 \in \mathcal{I} \rrbracket (\mathcal{T}) \sqcap \llbracket \phi_2 \rrbracket (\mathcal{T}) & \text{otherwise} \end{cases}$$

Using the above recursive definitions, it is easy to derive an algorithm that returns the Boolean truth value<sup>5</sup> of the formula and its robustness degree. The main observation is that each value node in the parse tree of the MTL formula should also contain its robustness degree. Therefore, the only operations that we need to modify are the negation and disjunction which must perform, respectively, a negation and a maximum operation on the robustness values of their operands. Then, the new semantics for the conjunction operator can be easily derived from these two.

**Definition 9 (Hybrid Semantics for Negation and Disjunction).** *Let  $(v_1, \varepsilon_1), (v_2, \varepsilon_2) \in \{\top, \perp\} \times \overline{\mathbb{R}}$ , then we define*

- *Negation:*  $\neg(v, \varepsilon) := (\neg v, -\varepsilon)$
- *Disjunction:*  $(v_1, \varepsilon_1) \vee (v_2, \varepsilon_2) := (v_1 \vee v_2, \max\{\varepsilon_1, \varepsilon_2\})$

<sup>5</sup> Note that the Boolean truth valued is required in the cases where the robustness degree is zero (see Proposition 2).

---

**Algorithm 1** Monitoring Timed State Sequences

---

**Input:** The MTL formula  $\phi$  and the timed state sequence  $\mathcal{T} = (\sigma, \tau, \mathcal{O})$

**Output:** The formula's Boolean truth value and the robustness parameter

```
1: procedure MONITOR( $\phi, \mathcal{T}$ )
2:   if  $|\mathcal{T}| > 1$  then return  $\phi \leftarrow \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O})$ 
3:   else return  $\phi \leftarrow \text{PROGRESS}(\phi, \sigma_0, 0, \top, \mathcal{O})$ 
4:   end if
5:   if  $\phi = (v, \varepsilon)$  then return  $(v, \varepsilon)$   $\triangleright v \in \{\top, \perp\}$  and  $\varepsilon \in \overline{\mathbb{R}}$ 
6:   else return MONITOR( $\phi, \mathcal{T}\uparrow_1$ )
7:   end if
8: end procedure
```

---

---

**Algorithm 2** Formula Progression Algorithm

---

**Input:** The MTL formula  $\phi$ , the current state  $s$ , the time period  $\Delta t$  for the next state and a variable  $last$  indicating whether the next state is the last and the mapping  $\mathcal{O}$

**Output:** The MTL formula  $\phi$  that has to hold at the next state

```
1: procedure PROGRESS( $\phi, s, \Delta t, last, \mathcal{O}$ )
2:   if  $\phi = (v, \varepsilon) \in \{\perp, \top\} \times \overline{\mathbb{R}}$  then return  $(v, \varepsilon)$ 
3:   else if  $\phi = \pi$  then return  $(s \in \mathcal{O}(\pi), \text{Dist}_d(s, \mathcal{O}(\pi)))$ 
4:   else if  $\phi = \neg\psi$  then return  $\neg\text{PROGRESS}(\psi, s, \Delta t, last, \mathcal{O})$ 
5:   else if  $\phi = \phi_1 \vee \phi_2$  then
6:     return  $\text{PROGRESS}(\phi_1, s, \Delta t, last, \mathcal{O}) \vee \text{PROGRESS}(\phi_2, s, \Delta t, last, \mathcal{O})$ 
7:   else if  $\phi = \bigcirc_{\mathcal{I}}\psi$  then return  $\text{HYBRID}(\neg last \wedge (\Delta t \in \mathcal{I})) \wedge \psi$ 
8:   else if  $\phi = \phi_1 \mathcal{U}_{\mathcal{I}}\phi_2$  then
9:      $\alpha \leftarrow \text{HYBRID}(0 \in \mathcal{I}) \wedge \text{PROGRESS}(\phi_2, s, \Delta t, last, \mathcal{O})$ 
10:     $\beta \leftarrow \text{HYBRID}(\neg last \wedge (0 \in \overleftarrow{\mathcal{I}})) \wedge \text{PROGRESS}(\phi_1, s, \Delta t, last, \mathcal{O}) \wedge \phi_1 \mathcal{U}_{\mathcal{I}-\Delta t}\phi_2$ 
11:    return  $\alpha \vee \beta$ 
12:   end if
13: end procedure

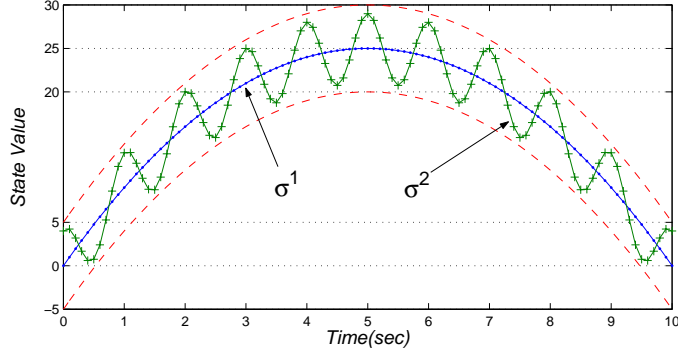
1: function HYBRID( $Bool$ )
2:   if  $Bool = \top$  return  $(\top, +\infty)$  else return  $(\perp, -\infty)$  end if
3: end function
```

---

Given a timed state sequence  $\mathcal{T}$  and an MTL formula  $\phi$ , we can construct a monitoring algorithm (Algorithm 1) that can decide both the satisfaction of the formula and the robustness parameter  $\varepsilon$  on-the-fly. Algorithm 2 is the core of the monitoring procedure. It takes as input the temporal logic formula  $\phi$ , the current state  $s$  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 it has to hold at the next state of the timed trace. In Algorithm 2,  $\overleftarrow{\mathcal{I}}$  is defined as follows

$$\overleftarrow{\mathcal{I}} = \begin{cases} [0, lb(\mathcal{I})] \cup \mathcal{I} & \text{if } 0 < lb(\mathcal{I}) \\ \mathcal{I} & \text{otherwise} \end{cases}$$

The constraint  $0 \in \overleftarrow{\mathcal{I}}$  is added in order to terminate the propagation of the subformula  $\phi_1 \mathcal{U}_{\mathcal{I}-\Delta t_1}\phi_2$ , when the timing constraints for the occurrence of



**Fig. 5.** Two timed state sequences  $\mathcal{T}_1 = (\sigma^1, \tau, \mathcal{O})$  and  $\mathcal{T}_2 = (\sigma^2, \tau, \mathcal{O})$ . The function  $\mathcal{O}$  is defined to be:  $\mathcal{O}(\alpha) = \{x \in \mathbb{R} \mid 20 \leq x \leq 30\}$  and  $\mathcal{O}(\beta) = \{x \in \mathbb{R} \mid -5 \leq x \leq 25\}$ .

$\phi_2$  have already been violated. Note that this timing constraint is meaningful only if we also perform the following simplifications at each recursive call of the algorithm PROGRESS.

$$\begin{aligned} \phi \wedge (\top, +\infty) &\equiv \phi & \phi \vee (\perp, -\infty) &\equiv \phi \\ \phi \vee (\top, +\infty) &\equiv (\top, +\infty) & \phi \wedge (\perp, -\infty) &\equiv (\perp, -\infty) \end{aligned}$$

When we check how robustly a trace satisfies a specification, we cannot stop the monitoring process as soon as we can determine the truth value of the MTL formula. This is because a future state in the timed trace may satisfy the specification more robustly. Therefore, we must execute the procedure MONITOR for the whole length of the timed state sequence  $\mathcal{T}$ .

*Example 2.* Consider the timed state sequence  $\mathcal{T}_1$  of Figure 5 and the formula  $\phi = \diamond_{[0,10]}\alpha$ . If we stop the evaluation as soon as the formula  $\phi$  becomes true, then  $\llbracket \phi \rrbracket(\mathcal{T}_1) = 0$ . On the other hand, if we continue the evaluation of the formula for the whole interval  $[0, 10]$ , then the robustness degree becomes  $\llbracket \phi \rrbracket(\mathcal{T}_1) = 5$  which corresponds to the time  $t = 5$  sec.

The proof of the following theorem is standard and uses induction on the structure of  $\phi$  based on the classical and robust semantics of MTL.

**Theorem 3.** *Given an MTL formula  $\phi$  and a timed state sequence  $\mathcal{T} \in \Sigma_X$ , the procedure MONITOR( $\phi, \mathcal{T}$ ) returns (i)  $(\top, \varepsilon)$  if and only if  $\llbracket \phi \rrbracket(\mathcal{T}) = \top$  and  $\llbracket \phi \rrbracket(\mathcal{T}) = \varepsilon$  and (ii)  $(\perp, \varepsilon)$  if and only if  $\llbracket \phi \rrbracket(\mathcal{T}) = \perp$  and  $\llbracket \phi \rrbracket(\mathcal{T}) = \varepsilon$ .*

The theoretical complexity of the monitoring algorithms has been studied in the past for both the Linear [32] and the Metric Temporal Logic [15]. Practical algorithms for monitoring using rewriting have been developed by several authors [16, 33]. The new part in Algorithm 2 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  $C$  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  $C = [a, b] \subseteq \mathbb{R}$  and  $x \in C$ , then  $\mathbf{Dist}_d(x, C) = \min\{|x - a|, |x - b|\}$ . When the set  $X$  is  $\mathbb{R}^n$ ,  $C \subseteq \mathbb{R}^n$  is a closed and convex set and the metric  $d$  is the Euclidean distance, i.e.  $d(x, y) = \|x - y\|_2$ , then we can calculate the distance ( $\mathbf{dist}_d$ ) by solving a convex optimization problem. If in addition the set  $C$  is a hyperplane  $C = \{x \mid a^T x = b\}$  or a halfspace  $C = \{x \mid a^T x \leq b\}$ , then there exist analytical solutions. For further details see [23].

*Example 3.* In Example 2, the robustness of the signal  $\mathcal{T}_1$  was calculated to be  $\llbracket \phi \rrbracket(\mathcal{T}_1) = 5$ . In Figure 5, the signal  $\mathcal{T}_2$  satisfies the condition  $\rho(\sigma^1, \sigma^2) < 5$ , thus we can conclude that  $\llbracket \phi \rrbracket(\mathcal{T}_2) = \top$  without using the procedure MONITOR.

## 5 Conclusions and Future Work

The main contribution of this work is the definition of a notion of robust satisfaction of a Metric Temporal Logic (MTL) formula  $\phi$  which is interpreted over timed state sequences that reside in some metric space. We have also presented an algorithmic procedure that can monitor such a timed state sequence and determine an under-approximation of its robustness degree. As mentioned in the introduction, the applications of this framework can extend to several areas. We are currently building a Simulink toolbox for the verification of signals and simulations using MTL specifications.

We should point out that the definitions presented in this paper can be extended to handle continuous signals with topological dense time semantics in the same way as the work by Maler and Nickovic [4]. The problem is that in this case we cannot abstract the continuous signal to a Boolean one since we need to maintain all the relevant information in order to determine its robustness. Therefore, we again need a finite (discretized) representation of the continuous signal or, if it is possible, an analytical representation of the signal.

We are currently exploring several new directions such as the extension of the definitions of the robustness degree and the robust MTL semantics so we can handle infinite timed state sequences. Also of interest to us is the addition of a metric on the time bounds as it is advocated in [20] and [21]. Finally, the methodology that we have presented in this paper comprises the basis for the extension of recent results on the safety verification of discrete time systems [18] to a more general verification framework using the metric temporal logic as a specification language. Such an approach is critically based on the notion of approximate bisimilarity [30].

*Acknowledgments* The authors would like to thank Oleg Sokolsky, Rajeev Alur and Antoine Girard for the fruitful discussions.

## References

1. Clarke, E.M., Grumberg, O., Peled, D.A.: Model Checking. MIT Press, Cambridge, Massachusetts (1999)
2. Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T.A., Ho, P.H., Nicollin, X., Olivero, A., Sifakis, J., Yovine, S.: The algorithmic analysis of hybrid systems. *Theoretical Computer Science* **138** (1995) 3–34
3. Tan, L., Kim, J., Sokolsky, O., Lee, I.: Model-based testing and monitoring for hybrid embedded systems. In: Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration. (2004) 487–492
4. Maler, O., Nickovic, D.: Monitoring temporal properties of continuous signals. In: Proceedings of FORMATS-FTRTFT. Volume 3253 of LNCS. (2004) 152–166
5. Kapinski, J., Krogh, B.H., Maler, O., Stursberg, O.: On systematic simulation of open continuous systems. In: Hybrid Systems: Computation and Control. Volume 2623 of LNCS., Springer (2003) 283–297
6. Esposito, J.M., Kim, J., Kumar, V.: Adaptive RRTs for validating hybrid robotic control systems. In: Proceedings of the International Workshop on the Algorithmic Foundations of Robotics. (2004)
7. Khalil, H.K.: Nonlinear Systems. Second edn. Prentice-Hall (1996)
8. Agarwal, R.P.: Difference equations and inequalities: theory, methods, and applications. 2nd edn. CRC (2000)
9. Emerson, E.A.: Temporal and modal logic. In van Leeuwen, J., ed.: Handbook of Theoretical Computer Science: Formal Models and Semantics. Volume B. North-Holland Pub. Co./MIT Press (1990) 995–1072
10. Koymans, R.: Specifying real-time properties with metric temporal logic. *Real-Time Systems* **2** (1990) 255–299
11. Bruns, G., Godefroid, P.: Model checking with multi-valued logics. In: Proceedings of the 31st International Colloquium on Automata, Languages and Programming (ICALP). Volume 3142 of LNCS. (2004) 281–293
12. Chechik, M., Devereux, B., Easterbrook, S., Gurfinkel, A.: Multi-valued symbolic model-checking. *ACM Transactions on Software Engineering and Methodology* **12** (2004) 1–38
13. de Alfaro, L., Faella, M., Henzinger, T.A., Majumdar, R., Stoelinga, M.: Model checking discounted temporal properties. In: Tools and Algorithms for the Construction and Analysis of Systems. Volume 2988 of LNCS., Springer (2004) 77–92
14. de Alfaro, L., Faella, M., Stoelinga, M.: Linear and branching metrics for quantitative transition systems. In: Proceedings of the 31st ICALP. Volume 3142 of LNCS., Springer (2004) 97–109
15. Thati, P., Rosu, G.: Monitoring algorithms for metric temporal logic specifications. In: Runtime Verification. Volume 113 of ENTCS., Elsevier (2005) 145–162
16. Havelund, K., Rosu, G.: Monitoring programs using rewriting. In: Proceedings of the 16th IEEE international conference on Automated software engineering. (2001)
17. Shults, B., Kuipers, B.: Qualitative simulation and temporal logic: proving properties of continuous systems. Technical Report TR AI96-244, Dept. of Computer Sciences, University of Texas at Austin (1996)
18. Girard, A., Pappas, G.J.: Verification using simulation. In: Hybrid Systems: Computation and Control (HSCC). Volume 3927 of LNCS., Springer (2006) 272 – 286
19. Lamine, K.B., Kabanza, F.: Reasoning about robot actions: A model checking approach. In: Advances in Plan-Based Control of Robotic Agents. Volume 2466 of LNCS., Springer (2002) 123–139

20. Huang, J., Voeten, J., Geilen, M.: Real-time property preservation in approximations of timed systems. In: Proceedings of the 1st ACM & IEEE International Conference on Formal Methods and Models for Co-Design. (2003) 163–171
21. Henzinger, T.A., Majumdar, R., Prabhu, V.S.: Quantifying similarities between timed systems. In: FORMATS. Volume 3829 of LNCS., Springer (2005) 226–241
22. Alur, R., Torre, S.L., Madhusudan, P.: Perturbed timed automata. In: Hybrid Systems: Computation and Control. Volume 3414 of LNCS. (2005) 70–85
23. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press (2004)
24. Ouaknine, J., Worrell, J.: On the decidability of metric temporal logic. In: 20th IEEE Symposium on Logic in Computer Science (LICS). (2005) 188–197
25. Alur, R., Feder, T., Henzinger, T.A.: The benefits of relaxing punctuality. In: Symposium on Principles of Distributed Computing. (1991) 139–152
26. Alur, R., Henzinger, T.A.: Real-Time Logics: Complexity and Expressiveness. In: Fifth Annual IEEE Symposium on Logic in Computer Science, Washington, D.C., IEEE Computer Society Press (1990) 390–401
27. Giannakopoulou, D., Havelund, K.: Automata-based verification of temporal properties on running programs. In: Proceedings of the 16th IEEE international conference on Automated software engineering. (2001)
28. Kannan, S., Sweedyk, Z., Mahaney, S.: Counting and random generation of strings in regular languages. In: Proceedings of the sixth annual ACM-SIAM symposium on Discrete algorithms. (1995) 551–557
29. Fainekos, G.E.: An introduction to multi-valued model checking. Technical Report MS-CIS-05-16, Dept. of CIS, Univ. of Pennsylvania (2005)
30. Girard, A., Pappas, G.J.: Approximation metrics for discrete and continuous systems. Technical Report MS-CIS-05-10, Dept. of CIS, Univ. of Pennsylvania (2005)
31. Fainekos, G.E., Girard, A., Pappas, G.J.: Temporal logic verification using simulation. In: Proceedings of FORMATS. Volume 4202 of LNCS., Springer (2006) 171–186
32. Markey, N., Schnoebelen, Ph.: Model checking a path (preliminary report). In: Proceedings of the 14th International Conference on Concurrency Theory. Volume 2761 of LNCS. (2003) 251–265
33. Kristoffersen, K.J., Pedersen, C., Andersen, H.R.: Runtime verification of timed LTL using disjunctive normalized equation systems. In: Proceedings of the 3rd Workshop on Run-time Verification. Volume 89 of ENTCS. (2003) 1–16

## A Properties

Recall the following properties:

1. Let  $(X, d)$  be a metric space and  $A \subseteq B \subseteq X$ , then for all  $x \in X$  it is

$$\mathbf{dist}_d(x, B) \leq \mathbf{dist}_d(x, A)$$

2. Let  $(X, d)$  be a metric space,  $A_1, A_2 \subseteq X$  and  $A = A_1 \cup A_2$ , then for all  $x \in X \setminus A$  it is

$$\mathbf{dist}_d(x, A) = \min\{\mathbf{dist}_d(x, A_1), \mathbf{dist}_d(x, A_2)\}$$

3. For  $a, b \in \overline{\mathbb{R}}$ , the following hold

$$\begin{aligned} a \sqcup b \geq 0 &\text{ iff } a \geq 0 \text{ or } b \geq 0 \\ a \sqcup b < 0 &\text{ iff } a < 0 \text{ and } b < 0 \end{aligned}$$

4. (Monotonicity of min and max) For  $a, b, c, d \in \overline{\mathbb{R}}$ , the following hold

$$\begin{aligned} a \leq b &\text{ implies } a \sqcup c \leq b \sqcup c \text{ and } a \sqcap c \leq b \sqcap c \\ a \leq b \text{ and } c \leq d &\text{ imply } a \sqcup c \leq b \sqcup d \text{ and } a \sqcap c \leq b \sqcap d \end{aligned}$$

5. For an MTL formula  $\phi$  and  $\mathcal{T} \in \Sigma_X$ , it is

$$\begin{aligned} \mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi) &= \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^\phi) \\ \mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi) &= -\mathbf{Dist}_\rho(\sigma, N_{\mathcal{T}}^\phi) \end{aligned}$$

## B Proof of Proposition 2

The proof is a straightforward induction on the structure of the MTL formula  $\phi$ , nevertheless we present the proof here for completeness of the presentation. First, we must prove by induction that (1) if  $\llbracket \phi \rrbracket(\mathcal{T}) > 0$ , then  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$  and (3) if  $\llbracket \phi \rrbracket(\mathcal{T}) < 0$ , then  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ .

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

**Case  $\phi = \pi \in AP$ :** If  $\llbracket \phi \rrbracket(\mathcal{T}) > 0$ , then by definition  $\mathbf{Dist}_d(\sigma_0, \mathcal{O}(\pi)) > 0$ , which implies that  $\sigma_0 \in \mathcal{O}(\pi)$  and, thus, that  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$ . If  $\llbracket \phi \rrbracket(\mathcal{T}) < 0$ , then by definition  $\mathbf{Dist}_d(\sigma_0, \mathcal{O}(\pi)) < 0$ , which implies that  $\sigma_0 \notin \mathcal{O}(\pi)$  and, thus, that  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ .

**Case  $\phi = \neg\phi_1$ :** (i) If  $\llbracket \neg\phi_1 \rrbracket(\mathcal{T}) > 0$ , then by definition  $\llbracket \phi_1 \rrbracket(\mathcal{T}) < 0$ . By the induction hypothesis, we get that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}) = \perp$ , which implies  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$ . (ii) If  $\llbracket \neg\phi_1 \rrbracket(\mathcal{T}) < 0$ , then by definition  $\llbracket \phi_1 \rrbracket(\mathcal{T}) > 0$ . By the induction hypothesis, we get that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}) = \top$ , which implies  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ .

**Case  $\phi = \phi_1 \vee \phi_2$ :** (i) If  $\llbracket \phi_1 \vee \phi_2 \rrbracket(\mathcal{T}) > 0$ , then by definition  $\llbracket \phi_1 \rrbracket(\mathcal{T}) \sqcup \llbracket \phi_2 \rrbracket(\mathcal{T}) > 0$ , i.e.,  $\llbracket \phi_1 \rrbracket(\mathcal{T}) > 0$  or  $\llbracket \phi_2 \rrbracket(\mathcal{T}) > 0$ . By the induction hypothesis, we get that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}) = \top$  or  $\langle\langle \phi_2 \rangle\rangle(\mathcal{T}) = \top$ , which implies  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$ . (ii) If  $\llbracket \phi_1 \vee \phi_2 \rrbracket(\mathcal{T}) < 0$ , then by definition  $\llbracket \phi_1 \rrbracket(\mathcal{T}) \sqcup \llbracket \phi_2 \rrbracket(\mathcal{T}) < 0$ , i.e.,  $\llbracket \phi_1 \rrbracket(\mathcal{T}) < 0$  and  $\llbracket \phi_2 \rrbracket(\mathcal{T}) < 0$ . By the induction hypothesis, we get that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}) = \perp$  and  $\langle\langle \phi_2 \rangle\rangle(\mathcal{T}) = \perp$ , which implies  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \langle\langle \phi_1 \rangle\rangle(\mathcal{T}) \vee \langle\langle \phi_2 \rangle\rangle(\mathcal{T}) = \perp$ .

**Case  $\phi = \bigcirc_{\mathcal{I}} \phi_1$ :** (i) If  $\llbracket \phi \rrbracket(\mathcal{T}) > 0$ , then by definition  $|\mathcal{T}| > 1$ ,  $\tau_1 \in \mathcal{I}$  and  $\llbracket \phi_1 \rrbracket(\mathcal{T}\uparrow_1) > 0$ . By the induction hypothesis, we get that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}\uparrow_1) = \top$ , which implies  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$ . (ii) If  $\llbracket \phi \rrbracket(\mathcal{T}) < 0$ , then by definition  $|\mathcal{T}| \leq 1$  or  $\tau_1 \notin \mathcal{I}$  or  $\llbracket \phi_1 \rrbracket(\mathcal{T}\uparrow_1) < 0$ . In the last case, by the induction hypothesis we get that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}\uparrow_1) = \perp$ . Thus in any case, by the induction hypothesis we get that  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ .

**Case  $\phi = \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2$ :** (i) If  $\llbracket \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2 \rrbracket(\mathcal{T}) > 0$ , then by the definition of until:  $\bigsqcup_{i=0}^{|\mathcal{T}|-1} (\llbracket i \in K_{\mathcal{I}}^{\mathcal{T}} \rrbracket(\mathcal{T}) \cap \llbracket \phi_2 \rrbracket(\mathcal{T}\uparrow_i) \cap \prod_{j=0}^{i-1} \llbracket \phi_1 \rrbracket(\mathcal{T}\uparrow_j)) > 0$ . This implies that there exists some time  $i \in K_{\mathcal{I}}^{\mathcal{T}}$  such that  $\llbracket \phi_2 \rrbracket(\mathcal{T}\uparrow_i) > 0$  and for all  $j \in [0, i-1]$ , we have  $\llbracket \phi_1 \rrbracket(\mathcal{T}\uparrow_j) > 0$ . Using the induction hypothesis we get that  $\langle\langle \phi_2 \rangle\rangle(\mathcal{T}\uparrow_i) = \top$  and for all  $j \in [0, i-1]$ , we have  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}\uparrow_j) = \top$ . Therefore,  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$  by definition. (ii) If  $\llbracket \phi_1 \mathcal{U}_{\mathcal{I}} \phi_2 \rrbracket(\mathcal{T}) < 0$ , then  $K_{\mathcal{I}}^{\mathcal{T}} = \emptyset$  or for all time  $i \in K_{\mathcal{I}}^{\mathcal{T}}$ , we have  $\llbracket \phi_2 \rrbracket(\mathcal{T}\uparrow_i) \cap \prod_{0 \leq j < i} \llbracket \phi_1 \rrbracket(\mathcal{T}\uparrow_j) < 0$ . In the former case, we immediately get by the definition that  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ . In the latter case, for all time  $i \in K_{\mathcal{I}}^{\mathcal{T}}$ , we have  $\llbracket \phi_2 \rrbracket(\mathcal{T}\uparrow_i) < 0$  or there exists some time  $j \in [0, i-1]$  such that  $\llbracket \phi_1 \rrbracket(\mathcal{T}\uparrow_j) < 0$ . Using the induction hypothesis we get that for all  $i \in K_{\mathcal{I}}^{\mathcal{T}}$ ,  $\langle\langle \phi_2 \rangle\rangle(\mathcal{T}\uparrow_i) = \perp$  or there exists  $j \in [0, i-1]$  such that  $\langle\langle \phi_1 \rangle\rangle(\mathcal{T}\uparrow_j) = \perp$ . Therefore,  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$  by definition.

The proof for the second statement of the proposition, i.e., (2) if  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \top$ , then  $\llbracket \phi \rrbracket(\mathcal{T}) \geq 0$  and (4) if  $\langle\langle \phi \rangle\rangle(\mathcal{T}) = \perp$ , then  $\llbracket \phi \rrbracket(\mathcal{T}) \leq 0$ , is similar to the previous one.

## C Proof of Theorem 1

**Proposition 3.** *Let  $\phi = \phi_1 \vee \phi_2$  be an MTL formula and  $\mathcal{T} \in \Sigma_X$ . Assume that for  $i = 1, 2$  it is*

$$-\mathbf{dist}_{\rho}(\sigma, P_{\mathcal{T}}^{\phi_i}) \leq \llbracket \phi_i \rrbracket(\mathcal{T}) \leq \mathbf{dist}_{\rho}(\sigma, N_{\mathcal{T}}^{\phi_i}) \quad (3)$$

then  $-\mathbf{dist}_{\rho}(\sigma, P_{\mathcal{T}}^{\phi}) \leq \llbracket \phi \rrbracket(\mathcal{T}) \leq \mathbf{dist}_{\rho}(\sigma, N_{\mathcal{T}}^{\phi})$ .

*Proof.* First note that

$$P_{\mathcal{T}}^{\phi} = \{\sigma' \mid \mathcal{S} \in \Sigma(\mathcal{T}) \text{ and } (\langle\langle \phi_1 \rangle\rangle(\mathcal{S}) = \top \text{ or } \langle\langle \phi_2 \rangle\rangle(\mathcal{S}) = \top)\} = P_{\mathcal{T}}^{\phi_1} \cup P_{\mathcal{T}}^{\phi_2}$$

$$N_{\mathcal{T}}^{\phi} = \{\sigma' \mid \mathcal{S} \in \Sigma(\mathcal{T}) \text{ and } (\langle\langle \phi_1 \rangle\rangle(\mathcal{S}) = \perp \text{ and } \langle\langle \phi_2 \rangle\rangle(\mathcal{S}) = \perp)\} = N_{\mathcal{T}}^{\phi_1} \cap N_{\mathcal{T}}^{\phi_2}$$

Therefore we have the set inclusions

$$P_{\mathcal{T}}^{\phi} \supseteq P_{\mathcal{T}}^{\phi_1} \text{ and } P_{\mathcal{T}}^{\phi} \supseteq P_{\mathcal{T}}^{\phi_2} \quad (4)$$

$$N_T^\phi \subseteq N_T^{\phi_1} \text{ and } N_T^\phi \subseteq N_T^{\phi_2} \quad (5)$$

The proof proceeds by a case-by-case analysis.

1. **Case**  $\langle\langle\phi_1\rangle\rangle(\mathcal{T}) = \langle\langle\phi_2\rangle\rangle(\mathcal{T}) = \top$ : By definition, we get that

$$\sigma \in P_T^{\phi_1} \text{ and } \sigma \in P_T^{\phi_2} \xrightarrow{(4)} \sigma \in P_T^\phi \implies \mathbf{dist}_\rho(\sigma, P_T^\phi) = 0 \quad (6)$$

By Proposition 2, we get that  $\llbracket\phi_1\rrbracket(\mathcal{T}) \geq 0$  and  $\llbracket\phi_2\rrbracket(\mathcal{T}) \geq 0$ . Therefore  $\llbracket\phi\rrbracket(\mathcal{T}) \geq 0$  and by (6)

$$-\mathbf{dist}_\rho(\sigma, P_T^\phi) \leq \llbracket\phi\rrbracket(\mathcal{T})$$

Moreover by definition

$$\begin{aligned} \sigma \notin N_T^{\phi_1} \text{ and } \sigma \notin N_T^{\phi_2} &\implies \sigma \notin N_T^\phi \implies \text{(By (5) and Property 1)} \\ \mathbf{dist}_\rho(\sigma, N_T^{\phi_1}) \leq \mathbf{dist}_\rho(\sigma, N_T^\phi) \text{ and } \mathbf{dist}_\rho(\sigma, N_T^{\phi_2}) \leq \mathbf{dist}_\rho(\sigma, N_T^\phi) &\implies \\ \max\{\mathbf{dist}_\rho(\sigma, N_T^{\phi_1}), \mathbf{dist}_\rho(\sigma, N_T^{\phi_2})\} \leq \mathbf{dist}_\rho(\sigma, N_T^\phi) &\quad (7) \end{aligned}$$

From (3) we get that

$$\begin{aligned} \llbracket\phi_1\rrbracket(\mathcal{T}) \sqcup \llbracket\phi_2\rrbracket(\mathcal{T}) \leq \max\{\mathbf{dist}_\rho(\sigma, N_T^{\phi_1}), \mathbf{dist}_\rho(\sigma, N_T^{\phi_2})\} &\xrightarrow{(7)} \\ \llbracket\phi\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_T^\phi) & \end{aligned}$$

2. **Case**  $\langle\langle\phi_1\rangle\rangle(\mathcal{T}) = \top$  and  $\langle\langle\phi_2\rangle\rangle(\mathcal{T}) = \perp$ : By definition, we get that

$$\sigma \in P_T^{\phi_1} \text{ and } \sigma \notin P_T^{\phi_2} \xrightarrow{(4)} \sigma \in P_T^\phi \implies \mathbf{dist}_\rho(\sigma, P_T^\phi) = 0 \quad (8)$$

By Proposition 2, we get that  $\llbracket\phi_1\rrbracket(\mathcal{T}) \geq 0$  and  $\llbracket\phi_2\rrbracket(\mathcal{T}) \leq 0$ . Therefore  $\llbracket\phi\rrbracket(\mathcal{T}) \geq 0$  and by (8)

$$-\mathbf{dist}_\rho(\sigma, P_T^\phi) \leq \llbracket\phi\rrbracket(\mathcal{T})$$

Moreover by definition

$$\begin{aligned} \sigma \notin N_T^{\phi_1} \text{ and } \sigma \in N_T^{\phi_2} &\implies \text{(By (5) and Property 1)} \\ \mathbf{dist}_\rho(\sigma, N_T^{\phi_1}) \leq \mathbf{dist}_\rho(\sigma, N_T^\phi) \text{ and } \mathbf{dist}_\rho(\sigma, N_T^{\phi_2}) = 0 &\quad (9) \end{aligned}$$

From (3) and (9) we get that

$$\llbracket\phi\rrbracket(\mathcal{T}) = \llbracket\phi_1\rrbracket(\mathcal{T}) \sqcup \llbracket\phi_2\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_T^{\phi_1}) \leq \mathbf{dist}_\rho(\sigma, N_T^\phi)$$

3. **Case**  $\langle\langle\phi_1\rangle\rangle(\mathcal{T}) = \perp$  and  $\langle\langle\phi_2\rangle\rangle(\mathcal{T}) = \perp$ : From (3) we get that

$$\max\{-\mathbf{dist}_\rho(\sigma, P_T^{\phi_1}), -\mathbf{dist}_\rho(\sigma, P_T^{\phi_2})\} \leq \llbracket\phi_1\rrbracket(\mathcal{T}) \sqcup \llbracket\phi_2\rrbracket(\mathcal{T}) \implies$$

$$\begin{aligned}
-\min\{\mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^{\phi_1}), \mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^{\phi_2})\} &\leq \llbracket\phi_1\rrbracket(\mathcal{T}) \sqcup \llbracket\phi_2\rrbracket(\mathcal{T}) \stackrel{\text{Property 2}}{\implies} \\
-\mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^\phi) &\leq \llbracket\phi\rrbracket(\mathcal{T})
\end{aligned}$$

and by definition

$$\sigma \in N_{\mathcal{T}}^{\phi_1} \text{ and } \sigma \in N_{\mathcal{T}}^{\phi_2} \stackrel{(5)}{\implies} \sigma \in N_{\mathcal{T}}^\phi \implies \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^\phi) = 0 \quad (10)$$

By Proposition 2, we get that  $\llbracket\phi_1\rrbracket(\mathcal{T}) \leq 0$  and  $\llbracket\phi_2\rrbracket(\mathcal{T}) \leq 0$ . Therefore  $\llbracket\phi\rrbracket(\mathcal{T}) \leq 0$  and by (10) we get that  $\llbracket\phi\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^\phi)$   $\square$

The next proposition follows naturally from the previous one.

**Proposition 4.** *Let  $\phi = \bigvee_{i=1}^n \phi_i$  for some  $n \in \mathbb{N}_{>0}$  be an MTL formula and  $\mathcal{T} \in \Sigma_X$ . Assume that for all  $i \leq n$  it is  $-\mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^{\phi_i}) \leq \llbracket\phi_i\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^{\phi_i})$ , then  $-\mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^\phi) \leq \llbracket\phi\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^\phi)$ .*

Using the De Morgan laws, the properties of the negation and Property 5, we derive the following result.

**Proposition 5.** *Let  $\phi = \bigwedge_{i=1}^n \phi_i$  for some  $n \in \mathbb{N}_{>0}$  be an MTL formula and  $\mathcal{T} \in \Sigma_X$ . Assume that for all  $i \leq n$  it is  $-\mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^{\phi_i}) \leq \llbracket\phi_i\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^{\phi_i})$ , then  $-\mathbf{dist}_\rho(\sigma, P_{\mathcal{T}}^\phi) \leq \llbracket\phi\rrbracket(\mathcal{T}) \leq \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^\phi)$ .*

The next proposition states the very intuitive property that given a timed state sequence (of finite length) and a formula  $\phi = \pi$ , then the length of the sequence of states  $\sigma$  does not affect the distance of  $\sigma$  from the set of state sequences that do not satisfy  $\phi$ .

**Proposition 6.** *Let  $\phi = \pi$  and  $\mathcal{T} \in \Sigma_X$ , then  $\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\pi) = \mathbf{Dist}_d(\sigma_0, \mathcal{O}(\pi))$ .*

*Proof.* We prove the statement by induction on the length of  $\sigma$ . First assume that  $\sigma \in P_{\mathcal{T}}^\pi$ . Consider the sequence of trace structures  $\mathcal{S}^j \in \Sigma(\mathcal{T} \downarrow_j)$  for  $j \in \{0, 1, \dots, |\mathcal{T}| - 1\}$  such that  $\tilde{\sigma}_i^j = \sigma_i$  for  $i = 0, 1, \dots, j$ . The base case for  $j = 0$  is straightforward

$$\mathbf{depth}_\rho(\tilde{\sigma}^0, P_{\mathcal{S}^0}^\pi) = \inf\{d(\tilde{\sigma}_0^0, \sigma'_0) \mid \sigma'_0 \in N_{\mathcal{S}^0}^\pi\} = \mathbf{depth}_d(\tilde{\sigma}_0^0, \mathcal{O}(\pi))$$

For the induction step assume that  $\mathbf{depth}_\rho(\tilde{\sigma}^k, P_{\mathcal{S}^k}^\pi) = \mathbf{depth}_\rho(\tilde{\sigma}^0, P_{\mathcal{S}^0}^\pi)$ . We have to show that  $\mathbf{depth}_\rho(\tilde{\sigma}^{k+1}, P_{\mathcal{S}^{k+1}}^\pi) = \mathbf{depth}_\rho(\tilde{\sigma}^0, P_{\mathcal{S}^0}^\pi)$ . By Property 5, we get that

$$\mathbf{dist}_\rho(\tilde{\sigma}^{k+1}, N_{\mathcal{S}^{k+1}}^\pi) = \inf\left\{\max_{i \in \{0, \dots, k+1\}} \{d(\tilde{\sigma}_i^{k+1}, \sigma'_i)\} \mid \sigma' \in N_{\mathcal{S}^{k+1}}^\pi\right\}$$

$$= \inf \left\{ \max \left\{ d(\tilde{\sigma}_{k+1}^{k+1}, \sigma'_{k+1}), \max_{i \in \{0, \dots, k\}} \{d(\tilde{\sigma}_i^{k+1}, \sigma'_i)\} \right\} \mid \sigma' \in N_{\mathcal{S}^{k+1}}^\pi \right\}$$

Now consider some particular  $\sigma'$  in  $N_{\mathcal{S}^{k+1}}^\pi$ , there exist only two possibilities

- if  $d(\tilde{\sigma}_{k+1}^{k+1}, \sigma'_{k+1}) \leq \max_{i \in \{0, \dots, k\}} \{d(\tilde{\sigma}_i^{k+1}, \sigma'_i)\}$ , then  $\rho(\tilde{\sigma}^{k+1}, \sigma') = \rho(\tilde{\sigma}^k, \sigma' \downarrow_k)$
- if  $d(\tilde{\sigma}_{k+1}^{k+1}, \sigma'_{k+1}) > \max_{i \in \{0, \dots, k\}} \{d(\tilde{\sigma}_i^{k+1}, \sigma'_i)\}$ , then  $\rho(\tilde{\sigma}^{k+1}, \sigma') > \rho(\tilde{\sigma}^k, \sigma' \downarrow_k)$

Therefore the extension of a state sequence by one more state cannot decrease the distance. We just have to look for a state that does not increase it either. This is easy as for all  $\sigma' \in N_{\mathcal{S}^{k+1}}^\pi$ , it is  $\sigma'_{k+1} \in X$ . Therefore, there exists some value of  $\sigma'_{k+1}$ , i.e.  $\sigma'_{k+1} = \tilde{\sigma}_{k+1}^{k+1}$ , such that  $d(\tilde{\sigma}_{k+1}^{k+1}, \sigma'_{k+1}) \leq \max_{i \in \{0, \dots, k\}} \{d(\tilde{\sigma}_i^{k+1}, \sigma'_i)\}$ . We conclude that the infimum over all traces in  $N_{\mathcal{S}^{k+1}}^\pi$  remains the same with the infimum over all traces in  $N_{\mathcal{S}^k}^\pi$ . Hence,  $\mathbf{depth}_\rho(\tilde{\sigma}^{k+1}, P_{\mathcal{S}^{k+1}}^\pi) = \mathbf{depth}_\rho(\tilde{\sigma}^k, P_{\mathcal{S}^k}^\pi)$  and using the induction hypothesis we get the desired result.

The proof for the case  $\sigma \in N_{\mathcal{T}}^\pi$  is similar.  $\square$

In the following,  $\bigcirc$  denotes the next temporal operator, i.e.  $\bigcirc_{[0, +\infty)}$ .

**Proposition 7.** *Let  $\phi = \bigcirc\psi$  be an MTL formula and  $\mathcal{T} \in \Sigma_X$  such that  $|\sigma| > 0$ . Then  $\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi) = \mathbf{Dist}_\rho(\sigma \uparrow_1, P_{\mathcal{T} \uparrow_1}^\psi)$ .*

*Proof.* Assume that  $\sigma \in P_{\mathcal{T}}^\phi$ . By Property 5, we get that

$$\begin{aligned} \mathbf{dist}_\rho(\sigma, N_{\mathcal{T}}^\phi) &= \inf \left\{ \max_{i \in \{0, \dots, |\sigma|\}} \{d(\sigma_i, \sigma'_i)\} \mid \sigma' \in N_{\mathcal{T}}^\phi \right\} \\ &= \inf \left\{ \max \left\{ d(\sigma_0, \sigma'_0), \max_{i \in \{1, \dots, |\sigma|\}} \{d(\sigma_i, \sigma'_i)\} \right\} \mid \sigma' \in N_{\mathcal{T}}^\phi \right\} \end{aligned}$$

Now consider some particular  $\sigma'$  in  $N_{\mathcal{T}}^\phi$ , there exist only two possibilities

- if  $d(\sigma_0, \sigma'_0) \leq \max_{i \in \{1, \dots, |\sigma|\}} \{d(\sigma_i, \sigma'_i)\}$ , then  $\rho(\sigma, \sigma') = \rho(\sigma \uparrow_1, \sigma' \uparrow_1)$
- if  $d(\sigma_0, \sigma'_0) > \max_{i \in \{1, \dots, |\sigma|\}} \{d(\sigma_i, \sigma'_i)\}$ , then  $\rho(\sigma, \sigma') > \rho(\sigma \uparrow_1, \sigma' \uparrow_1)$

But it is  $N_{\mathcal{T}}^\phi = \{\sigma' \mid \mathcal{S} \in \Sigma(\mathcal{T}) \text{ and } \langle\langle \phi \rangle\rangle(\mathcal{S}) = \perp\} = \{\sigma' \mid \mathcal{S} \in \Sigma(\mathcal{T}) \text{ and } \langle\langle \phi \rangle\rangle(\mathcal{S} \uparrow_1) = \perp\}$  so for all  $\sigma' \in N_{\mathcal{T}}^\phi$  it is  $\sigma'_0 \in X$ . Therefore, there exists some value of  $\sigma'_0$ , i.e.  $\sigma'_0 = \sigma_0$ , such that  $d(\sigma_0, \sigma'_0) \leq \sup \{d(\sigma_i, \sigma'_i) \mid i \in \{1, 2, \dots, |\sigma|\}\}$ . We conclude that the infimum over all traces in  $N_{\mathcal{T}}^\phi$  remains the same with the infimum over all traces in  $N_{\mathcal{T} \uparrow_1}^\psi$ . Hence,  $\mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi) = \mathbf{depth}_\rho(\sigma \uparrow_1, P_{\mathcal{T} \uparrow_1}^\psi)$ .

The proof for the case  $\sigma \in N_{\mathcal{T}}^\phi$  is similar.  $\square$

The next proposition derives immediately from the previous one. Here,  $\bigcirc^i$  denotes the composition of  $i$  unbounded next time temporal operators. By convention  $\bigcirc^0\psi = \psi$ .

**Proposition 8.** *Let  $\phi = \bigcirc^i\psi$  for  $i \geq 0$  be an MTL formula and  $\mathcal{T} \in \Sigma_X$  such that  $|\sigma| \geq i$ . Then  $\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi) = \mathbf{Dist}_\rho(\sigma \uparrow_i, P_{\mathcal{T} \uparrow_i}^\psi)$ .*

**Theorem 1.** Given an MTL formula  $\phi$  and  $\mathcal{T} \in \Sigma_X$ , then  $|\llbracket \phi \rrbracket(\mathcal{T})| \leq |\mathbf{Dist}_\rho(\sigma, P_{\mathcal{T}}^\phi)|$ .  
In more detail,  $-\mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\phi) \leq \llbracket \phi \rrbracket(\mathcal{T}) \leq \mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi)$ .

*Proof.* The proof is by induction on the structure of the formula  $\phi$ .

– **Case  $\phi = \top$ :** It is

$$P_{\mathcal{T}}^\top = \{\sigma' \mid \mathcal{S} = (\sigma', \tau, \mathcal{O}) \in \Sigma(\mathcal{T}) \text{ and } \llbracket \top \rrbracket(\mathcal{S}) = \top\} = X^{|\mathcal{T}|} \text{ and } N_{\mathcal{T}}^\top = \emptyset$$

Therefore,  $\mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\top) = +\infty = \llbracket \top \rrbracket(\mathcal{T})$  and  $\mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\top) = 0$ .

– **Case  $\phi = \pi$  for  $\pi \in AP$ :** Immediate from Proposition 6 and the definition  $\llbracket \pi \rrbracket(\mathcal{T}) = \mathbf{Dist}_d(\sigma_0, \mathcal{O}(\pi))$ .  
– **Case  $\phi = \neg\psi$ :** Note that  $P_{\mathcal{T}}^\phi = P_{\mathcal{T}}^{\neg\psi} = N_{\mathcal{T}}^\psi$  and similarly for  $N_{\mathcal{T}}^\phi$ . By the induction hypothesis we get that

$$\begin{aligned} -\mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\psi) \leq \llbracket \psi \rrbracket(\mathcal{T}) \leq \mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\psi) &\implies \\ -\mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi) \leq -\llbracket \neg\psi \rrbracket(\mathcal{T}) \leq \mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\psi) &\implies \\ -\mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\phi) \leq \llbracket \phi \rrbracket(\mathcal{T}) \leq \mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi) & \end{aligned}$$

– **Case  $\phi = \phi_1 \vee \phi_2$ :** Immediate from Proposition 3.

– **Case  $\phi = \bigcirc_{\mathcal{I}}\psi$ :** If  $\tau_1 \in \mathcal{I}$ , then we get that  $\llbracket \bigcirc_{\mathcal{I}}\psi \rrbracket(\mathcal{T}) = \llbracket \psi \rrbracket(\mathcal{T}\uparrow_1)$ . By the induction hypothesis we get that

$$\begin{aligned} -\mathbf{depth}_\rho(\sigma\uparrow_1, N_{\mathcal{T}\uparrow_1}^\psi) \leq \llbracket \psi \rrbracket(\mathcal{T}\uparrow_1) \leq \mathbf{depth}_\rho(\sigma\uparrow_1, P_{\mathcal{T}\uparrow_1}^\psi) &\stackrel{\text{Proposition 7}}{\implies} \\ -\mathbf{depth}_\rho(\sigma, N_{\mathcal{T}}^\phi) \leq \llbracket \phi \rrbracket(\mathcal{T}) \leq \mathbf{depth}_\rho(\sigma, P_{\mathcal{T}}^\phi) & \end{aligned}$$

Now consider the case where  $\tau_1 \notin \mathcal{I}$ . By definition  $\phi$  evaluates to  $\perp$  and, thus,  $N_{\mathcal{T}}^\phi = X^{|\mathcal{T}|}$ . This is similar to the first case of this theorem.

– **Case  $\phi = \phi_1 \mathcal{U}_{\mathcal{I}}\phi_2$ :** The result follows immediately by applying Propositions 4, 5 and 8, Property 4 and noting that  $\llbracket \phi \rrbracket(\mathcal{T})$  can be rewritten as

$$\llbracket \phi \rrbracket(\mathcal{T}) = \bigsqcup_{i=0}^{|\mathcal{T}|-1} (\llbracket i \in K_{\mathcal{T}}^{\mathcal{I}} \rrbracket(\mathcal{T}) \sqcap \llbracket \bigcirc^i \phi_2 \rrbracket(\mathcal{T}) \sqcap \prod_{j=0}^{i-1} \llbracket \bigcirc^j \phi_1 \rrbracket(\mathcal{T}))$$

*Remark 5.* Case 1 in Proposition 3 describes under what conditions the equality in Theorem 1 between the robust semantics of MTL (Definition 8) and the robustness degree (as given in Definition 7) does not hold.

## D Proof of Theorem 3

First, let us denote the valuation function for the hybrid semantics as they were introduced in Section 4 by  $\llbracket \cdot \rrbracket_H$ . First, we must prove the following lemma.

**Lemma 1.** Given an MTL formula  $\phi$  and a finite timed state sequence  $\mathcal{T} \in \Sigma_X$ , then for any  $|\mathcal{T}| > 1$  we have  $\llbracket \phi \rrbracket_H(\mathcal{T}) = \llbracket \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1)$ .

*Proof.* The proof uses a straightforward induction on the structure of  $\phi$ . We present the proof for completeness of the presentation. Since  $|\mathcal{T}| > 1$ , we have  $last = \perp$ .

**Atomic Proposition**  $\phi = \pi \in AP$ : then

$$\begin{aligned} \llbracket \pi \rrbracket_H(\mathcal{T}) &= (\sigma_0 \in \mathcal{O}(\pi), \mathbf{Dist}_d(\sigma_0, \mathcal{O}(\pi))) = \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \\ &= \llbracket \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \end{aligned}$$

by definition. The proof is similar when  $\phi = (v, \varepsilon) \in \{\perp, \top\} \times \overline{\mathbb{R}}$ .

**Negation**  $\phi = \neg\phi_1$ : then

$$\begin{aligned} \llbracket \phi \rrbracket_H(\mathcal{T}) &= \neg \llbracket \phi_1 \rrbracket_H(\mathcal{T}) && \text{by I.H.} \\ &= \neg \llbracket \text{PROGRESS}(\phi_1, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \\ &= \llbracket \neg \text{PROGRESS}(\phi_1, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \\ &= \llbracket \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \end{aligned}$$

**Disjunction**  $\phi = \phi_1 \vee \phi_2$ : then

$$\begin{aligned} \llbracket \phi \rrbracket_H(\mathcal{T}) &= \llbracket \phi_1 \rrbracket_H(\mathcal{T}) \vee \llbracket \phi_2 \rrbracket_H(\mathcal{T}) && \text{by I.H.} \\ &= \llbracket \text{PROGRESS}(\phi_1, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \vee \\ &\quad \vee \llbracket \text{PROGRESS}(\phi_2, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \\ &= \llbracket \text{PROGRESS}(\phi_1, \sigma_0, \tau_1, \perp, \mathcal{O}) \vee \\ &\quad \vee \text{PROGRESS}(\phi_2, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \\ &= \llbracket \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \end{aligned}$$

**Next**  $\phi = \bigcirc_{\mathcal{I}}\phi_1$ : then

$$\begin{aligned} \llbracket \phi \rrbracket_H(\mathcal{T}) &= \llbracket \tau_1 \in \mathcal{I} \rrbracket_H(\mathcal{T}) \wedge \llbracket \phi_1 \rrbracket_H(\mathcal{T}\uparrow_1) && \text{by Def. and I.H.} \\ &= \text{HYBRID}(\tau_1 \in \mathcal{I}) \wedge \llbracket \phi_1 \rrbracket_H(\mathcal{T}\uparrow_1) \\ &= \llbracket \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \end{aligned}$$

**Until**  $\phi = \phi_1 \mathcal{U}_{\mathcal{I}}\phi_2$ : Now using the recursive formulation of until, we derive

$$\begin{aligned} \llbracket \phi \rrbracket_H(\mathcal{T}) &= (\llbracket 0 \in \mathcal{I} \rrbracket_H(\mathcal{T}) \wedge \llbracket \phi_2 \rrbracket_H(\mathcal{T})) \vee \\ &\quad \vee (\llbracket \phi_1 \rrbracket_H(\mathcal{T}) \wedge \llbracket \phi_1 \mathcal{U}_{\mathcal{I}-\tau_1} \phi_2 \rrbracket_H(\mathcal{T}\uparrow_1)) && \text{by Def. and I.H.} \\ &= (\text{HYBRID}(0 \in \mathcal{I}) \wedge \\ &\quad \wedge \llbracket \text{PROGRESS}(\phi_2, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1)) \vee \\ &\quad \vee (\llbracket \text{PROGRESS}(\phi_1, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \wedge \\ &\quad \wedge \llbracket \phi_1 \mathcal{U}_{\mathcal{I}-\tau_1} \phi_2 \rrbracket_H(\mathcal{T}\uparrow_1)) \\ &= \llbracket \text{PROGRESS}(\phi, \sigma_0, \tau_1, \perp, \mathcal{O}) \rrbracket_H(\mathcal{T}\uparrow_1) \end{aligned}$$

□

Using the above lemma and the fact that the temporal operators are eliminated from  $\phi$  when  $last = \top$ , we derive Theorem 3 as corollary.