Logical Characterisation of Hybrid Conformance

Maciej Gazda   Mohammad Reza Mousavi

July 5, 2019

Abstract

Logical characterisation of a behavioural equivalence relation precisely specifies the set of formulae that are preserved and reflected by the relation. Such characterisations have been studied extensively for exact semantics on discrete models such as bisimulation equivalences for labelled transition systems and Kripke structures, but to a much lesser extent for approximate relations, in particular in the context of hybrid systems. We present what is, to our knowledge, the first characterisation result for an approximate notion of hybrid conformance involving tolerance thresholds in both time and value. Since the notion of conformance in this setting is approximate, any characterisation will unavoidably involve a notion of relaxation, denoting how the specification formulae should be relaxed in order to hold for the implementation. To this end, we show that the existing relaxation scheme on Metric Temporal Logic used for preservation results in this setting is not tight enough for providing a characterisation and propose a tighter relaxation that we subsequently prove to be adequate for the purpose. The characterisation result, while interesting in its own right, paves the way to more applied research, as our notion of hybrid conformance underlies a formal model-based technique for the verification of cyber-physical systems.

1 Introduction

Cyber-physical systems integrate discrete aspects of computation, with continuous aspects of physical phenomena, and asynchronous aspects of communication protocols. To test cyber-physical systems against their discrete abstractions (also called discrete-event systems), several notions of conformance have been proposed [13, 28, 31]; we refer to the tutorial volume edited by Broy et al. [8] for an overview. Logical characterisations of conformance [20, 3] are of particular importance in this context, because they precisely specify the set of logical formulae that are preserved and reflected under conformance (we refer to [4] for an accessible introduction). Such logical characterisations provide a rigorous basis for design trajectories that involves subsequent conformance test among different layers of abstraction. Moreover, logical characterisations are stepping stones towards devising the notion of characterising formulae, which have been used and algorithms and tools for checking conformance [4, 10].

In the context of hybrid systems, i.e., abstractions of CPSs integrating both discrete and continuous aspects, some notions of conformance have been proposed in the recent literature [2, 1, 11, 15] (see [21] for an overview). However, not much is known about the logical characterisation of such notions; to our knowledge, the closest known results to a logical characterisation of hybrid conformance are the logical preservation results [15, 1] and the characterisation of metric bisimulation [12] and stochastic bisimulation for systems with rewards [16] (see the related work section for an in-depth discussion). This paper aims at bridging this gap and comes up with, to the best of our knowledge, the first logical characterisation of approximate conformance for hybrid systems [2, 1] in terms of Metric Temporal Logic [22, 5].

To this end, we start with the notion of (τ, ϵ)-conformance, due to Abbas, Mittelmann and Fainekos [2, 1] and their recent results pertaining to preservation of Metric Temporal Logic (MTL) under this notion of conformance. We show that the relaxation proposed in the aforementioned preservation result is insufficiently precise to lead to a logical characterisation. Subsequently, we propose a tighter notion of relaxation and prove that our notion indeed leads to a characterisation of approximate conformance. We formulate our results in a general semantic domain, called generalised timed traces, which encompasses both discretised hybrid systems (as studied by Abbas, Mittelmann, and Fainekos [1]) and their continuous variants. Moreover, we study a generalisation of these results for both bounded and unbounded nondeterministic systems.

The contributions of this paper have both theoretical and practical motivation and relevance. The theoretical motivation for logical characterisation is that it not only provides an idea about the logic that is preserved under conformance (subject to relaxation) such as – in our case – MTL, but also it specifies precise bounds on the relaxation required for such formulae to hold. The practical motivation is that firstly, it provides designers with a precisely specified set of properties that carry over from specification to implementation (while preservation results only provide a rough approximation of such properties) and moreover, logical characterisation sets the scene for developing algorithms for finding distinguishing formulae, and hence, provide an alternative means for checking hybrid conformance. Logical characterisations have also proven to be a versatile auxiliary tool in e.g. developing congruence formats for operational semantics [7], as well as providing approximations of hybrid systems [26].

The rest of this paper is organised as follows. In Section 2, we review the related work and position our contributions with respect to the state of the art. In Section 3, we define some preliminary notions, including our semantic domain, the notion of hybrid conformance [1] and Metric Temporal Logic [6]. Subsequently in Section 4, we show that the existing relaxation schemes for Metric Temporal Logic are too lax to serve for a logical characterisation of hybrid conformance; namely, we prove there is a class of non-conforming implementations that do satisfy all relaxed MTL formulae satisfied by the specification. This sets the scene for the definition of a tighter notion of relaxation in Section 5, which is proven to provide a logical characterisation. In Section 6, we conclude the paper, and present the directions of our ongoing research in this domain.

2 Related work

Logical characterisations for conformance relations allow for identifying conforming systems by means of the logical formulae satisfied by them. They also facilitate the converse operation, important from a practical perspective, namely, distinguishing non-conforming systems with a formula that forms a succinct counterexample.

Characterisations using modal logic have been studied extensively in the setting of exact behavioural semantics on discrete models such as labelled transition systems [20, 30]. In this context, characterisations use direct comparison of sets of formulae satisfied by systems in question; distinguishing formulae are those belonging to a set difference of such sets. Our work differs from this line of work in that it deals with approximate behavioural semantics and hence, cannot literally compare the sets of satisfied formulae.

To our knowledge, the first notion of characterisation for approximate behavioural semantics has been offered by de Alfaro, Faela, and Stoelinga [12] in the context of Metric Transition Systems. In this work, linear and branching distances, strongly related to approximate relations and metrics by Girard and Pappas [19, 18], are proved to be characterised using certain quantitative modal and temporal logics (such as the quantitative modal μ-calculus). Due to the quantitative nature of the semantics of the logics, the characterisations are based on bounds on the satisfaction values of formulae over different systems. Hence a distinguishing formula is simply one for which the difference of satisfaction values falls outside a certain bound. We differ from this line of work in two aspects. On a general level, our semantic model and conformance relation are different from those in [12, 19] in that they involve separate time and value dimensions, both of which can be subject to perturbations. Our choices for the semantic model and the notion of conformance are motivated by the practical applications of hybrid conformance [2, 1] in testing cyber-physical systems, e.g., in the automotive- [29] and healthcare domain [27]. Moreover, from a technical perspective, we base our characterisation on a logic with a qualitative (binary) satisfaction relation, but with quantities embedded in its syntax, namely, the Metric Temporal Logic (MTL). However, our approach can be easily translated to a quantitative setting of [12], by defining an evaluation of a formulae as the least degree of relaxation after applying which the formula is satisfied by a system. Also in this case, the choice of Metric Temporal Logic [22, 5] (and its concrete instantiation with signal values for propositions: Signal Temporal Logic [23]) is motivated by its wide-spread use in the literature and in practice [1, 17, 14].

Prabhakar, Vladimerou, Viswanathan, and Dullerud [26] provide a characterisation theorem for approximate simulation [18]; the characterisation serves as an auxiliary tool for developing approximations of hybrid systems with polynomial flows. In terms of semantic domain and relation under consideration, their characterisation result is strongly related to [12]. One technical feature which makes that paper somewhat closer in style to ours than [12] is the use of a relaxation operator (called a shrink of a formula in [26]).

Gburek and Baier [16] have recently investigated characterisation of bismulation for stochastic systems with actions and rewards with two probabilistic logics: a very expressive APCTL*, and simpler APCTL$_\circ$, that can provide succinct distinguishing formula. Unlike their approach [16], our work is set in the context of standard hybrid systems.

The results that appear closest to ours in terms of underlying models, and conformance relations that allow for disturbances in both time and space values, are logical preservation results for hybrid conformance [1] and Skorokhod conformance [15]. Both papers define syntactical transformations on temporal logics yielding more relaxed formulae; they differ on the conformance relations and temporal logics investigated. We improve upon them by providing different relaxation schemes that are proven to be tight, i.e., are precisely sufficient for a characterisation. Moreover, we generalise their results to semantic models that can encompass both discrete and continuous behaviour and non-determinism. Our framework of generalised timed traces subsumes both discrete TSSs and continuous trajectories, e.g., allowing for a comparison of behaviours of different types (such as sampled discretised behaviour against continuous trajectories).

Abbas, Mittelmann, and Fainekos [1] introduced a notion of relaxation for MTL in the context of timed state sequences (TSSs) and (τ, ϵ)-conformance. The authors have shown the following preservation property: whenever a state in a TSS satisfies an MTL formula, then all states in a (τ, ϵ)-conforming TSS that are sufficiently close to the given state (i.e., within the distance of at most τ in time and ϵ in value) satisfy the relaxed formula. In this paper, we show that for the purpose of providing a logical characterisation of hybrid systems, this particular relaxation scheme is insufficiently precise. More specifically, we show that there is a general class of non-(τ, ϵ)-conforming systems that do preserve the relaxed formulas. Our relaxation scheme alleviates these issues.

Another notion of relaxation has been presented by Deshmukh, Majumdar, and Prabhu [15]. It is defined on the Freeze Linear Temporal Logic (Freeze LTL or LTL with freeze variables) in the context of continuous traces/trajectories, and the Skorokhod metric. Skorokhod metric is a stronger notion than (τ, ϵ)-conformance, that like (τ, ϵ)-conformance also allows for discrepancies in time and space. This relaxation scheme yields in general stronger formulae than the relaxation scheme of [1]; in particular, the relaxed formulae maintain the timeline order, and hence cannot be preserved under the relaxation by (τ, ϵ)-conformance due to its local disorder phenomenon. On the other hand, the relaxed formulae are preserved by traces that are sufficiently close according to the stronger Skorokhod metric, as shown in [15]. It remains to be investigated whether the relaxation proposed by Deshmukh et al. can be seen as a basis for a logical characterisation of Skorokhod conformance.

3 Preliminaries

In this section, we define some preliminaries regarding our semantic domain, Metric Temporal Logic and the notion of hybrid conformance.

3.1 Generalised timed traces and hybrid systems

In order for our theory to remain as general as possible, we define generalised timed traces, a notion that generalises both discrete semantic models, such as timed state sequences (TSSs) [1], and continuous-time trajectories [15]. A generalised timed trace is essentially a mapping from a discrete or continuous time domain to a set of values within some metric space.

Definition 1. *Let $(\mathcal{Y}, d_{\mathcal{Y}})$ be a metric space. A $\mathcal{Y}$-valued generalised timed trace is a function $\mu : \mathcal{T} \to \mathcal{Y}$ such that $\mathcal{T} \subseteq \mathbb{R}_{\geq 0}$ is the time domain, and in addition $0 \in \mathcal{T}$ is the least element in $\mathcal{T}$. The set of all $\mathcal{Y}$-valued generalised timed traces is denoted by $GTT(\mathcal{Y})$.*

Observe that a timed state sequence (TSS) is simply a generalised timed trace with $\mathcal{T}$ being a finite subset of $\mathbb{R}_{\geq}$; moreover, in case $\mathcal{T}$ is an interval within $\mathbb{R}_{\geq 0}$, we obtain a standard continuous-time trajectory. We could generalise the domain of μ to any totally-ordered metric space, but we dispense with this generalisation here for the sake of simplicity. Likewise, the assumption that 0 is the minimal element of the time domain could be also dispensed with.

A hybrid system, defined below, is a mapping from initial conditions and inputs to sets of generalised (output) traces. We use the notation $\mathcal{P}(S)$ and $\mathcal{P}_{_{FIN}}(S)$ denote, respectively, a powerset of S, and the powerset of S restricted to the finite subsets.

Definition 2. *Given sets $\mathcal{C}$ and $\mathcal{I}$ of initial conditions and input space, the set of $\mathcal{Y}$-valued hybrid systems, denoted by $\mathcal{H}(\mathcal{C}, \mathcal{I}, \mathcal{Y})$ is the set of all functions of the type $\mathcal{C} \times \mathcal{I} \to \mathcal{P}(GTT(\mathcal{Y}))$. In addition, we distinguish the following classes of hybrid systems:*

- finitely branching hybrid systems $\mathcal{H}_{FIN}(\mathcal{C}, \mathcal{I}, \mathcal{Y}) = \{H : \mathcal{C}\times\mathcal{I} \to \mathcal{P}_{FIN}(GTT(\mathcal{Y}))\}$
- deterministic hybrid systems $\mathcal{H}_{DET}(\mathcal{C}, \mathcal{I}, \mathcal{Y}) = \{H : \mathcal{C}\times\mathcal{I} \to \mathcal{P}(GTT(\mathcal{Y})) \,|\, \forall_{c\in\mathcal{C}, i\in\mathcal{I}} |H(c, i)| = 1\}$

Note that we intentionally left the nature of the initial conditions and input space implicit, as they play no role in the development of this paper. In reality, input conditions are typically constraints on input signals and the input space is typically a generalised timed trace with the same domain as the generalised timed trace for output. Also note that we focus mainly on finitely branching hybrid systems. When the parameters $\mathcal{I}, \mathcal{C}, \mathcal{Y}$ are not relevant or are clear from the context, we leave them out and refer to the set of hybrid systems with fixed parameters as $\mathcal{H}$.

3.2 Metric Temporal Logic

Metric Temporal Logic (MTL) [22, 5] is an extension of Linear Temporal Logic [25] with intervals; the introduction of intervals allows for reasoning about the real-time behaviour of dynamic systems and once the propositions of the logic are interpreted over real-valued signals [23] (this interpretation of MTL is also called Signal Temporal Logic, or STL in the literature). MTL serves as an intuitive formalism for reasoning about hybrid systems [23, 1, 17, 14].

We work with the following language MTL^{+} of MTL formulas in the negation-normal form

$$\phi ::= \mathsf{T} \mid \mathsf{F} \mid p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \, \mathcal{U}_I \, \phi \mid \phi \, \mathcal{R}_I \, \phi$$

where p ranges over a collection of atomic propositions AP, and I ranges over intervals, $\mathcal{U}_I$ denotes the until operator and $\mathcal{R}_I$ denotes the release operator (both annotated with interval I).

For the purpose of relaxation, we shall also use the slightly extended language MTL^{+}_{ext} that in addition includes $p^{+}(\epsilon)$ and $p^{-}(\epsilon)$ constructs. Intuitively, they denote, respectively, the expansion- and contraction of the domain of validity of proposition p by ϵ.

$$\phi ::= \quad \mathsf{T} \mid \mathsf{F} \mid p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \, \mathcal{U}_I \, \phi \mid \phi \, \mathcal{R}_I \, \phi \mid p^{+}(\epsilon) \mid p^{-}(\epsilon)$$

In order to provide the semantics for MTL^{+}, we need two auxiliary definitions. Below, we assume the context of some metric space $(\mathcal{Y}, d_{\mathcal{Y}})$, and S ranges over subsets of $\mathcal{Y}$.

- $E(S, \delta) := \{y \in \mathcal{Y} \mid \inf_{s \in S} d_{\mathcal{Y}}(y, s) \leq \delta\}$ (δ-expansion)
- $C(S, \delta) := \mathcal{Y} \setminus E(\mathcal{Y} \setminus S, \delta)$ (δ-contraction)

We also remark that the semantics of MTL^{+}_{ext} is provided in the context of an interpretation function $\mathcal{O} : AP \to \mathcal{P}(\mathcal{Y})$. This is a standard approach, similar to e.g. [1], but also to Signal Temporal Logic [23]. Note that the nature of the interpretation function restricts the expressive power of the logic, as the propositions are interpreted over the domain of values only (excluding time domain), which precludes expressing more powerful properties such as signal tracking (which is possible in Freeze LTL [15]).

The semantics of MTL^{+}_{ext} for generalised timed traces is given below:

Definition 3. *Let $\mu : \mathcal{T} \to \mathcal{Y}$ be a generalised timed trace, $t \in \mathbb{R}$, and $\mathcal{O} : AP \to \mathcal{P}(\mathcal{Y})$ be an interpretation mapping for atomic propositions. The semantics of MTL^{+}_{ext} formula is defined as follows:*
$(\mu, t) \models \mathsf{T} \quad (\mu, t) \not\models \mathsf{F}$
$(\mu, t) \models p$ *iff* $t \in \mathcal{T}$ *and* $\mu(t) \in \mathcal{O}(p)$
$(\mu, t) \models \neg p$ *iff* $t \in \mathcal{T}$ *and* $\mu(t) \notin \mathcal{O}(p)$
$(\mu, t) \models p^{+}(\epsilon)$ *iff* $t \in \mathcal{T}$ *and* $\mu(t) \in E(\mathcal{O}(p), \epsilon)$
$(\mu, t) \models p^{-}(\epsilon)$ *iff* $t \in \mathcal{T}$ *and* $\mu(t) \in C(\mathcal{O}(p), \epsilon)$
$(\mu, t) \models \phi \wedge \psi$ *iff* $(\mu, t) \models \phi$ *and* $(\mu, t) \models \psi$
$(\mu, t) \models \phi \vee \psi$ *iff* $(\mu, t) \models \phi$ *or* $(\mu, t) \models \psi$
$(\mu, t) \models \phi \, \mathcal{U}_I \, \psi$ *iff* $\exists t' \in \mathcal{T}.\ t' - t \in I.\, (\mu, t') \models \psi$
$\wedge \forall t'' \in \mathcal{T}.\, t'' \in [t, t') \implies ((\mu, t'') \models \phi \vee (t'' - t \in I \wedge (\mu, t'') \models \psi))$
$(\mu, t) \models \phi \, \mathcal{R}_I \, \psi$ *iff* $\forall t' \in \mathcal{T}.\, (t' - t \in I \wedge (y, t') \not\models \psi) \implies (\exists t_1 \in \mathcal{T}.\, t_1 < t' \wedge t_1 - t \in I \wedge (\mu, t_1) \models \phi)$

We say that a generalised timed trace $\mu : \mathcal{T} \to \mathcal{Y}$ satisfies an MTL^+ formula ϕ, notation $\mu \models \phi$ iff $(\mu, 0) \models \phi$. Moreover, the satisfaction relation is lifted to hybrid systems in the following manner:

$$H(c,i) \models \phi \iff \forall \mu \in H(c,i).\, \mu \models \phi$$

In the remainder of this paper, we also use the following shorthand notation:

$$\Diamond_I \phi := \mathsf{T}\, \mathcal{U}_I\, \phi \qquad \Box_I \phi := \mathsf{F}\, \mathcal{R}_I\, \phi$$

Note that the semantics allows for certain "ambiguous" cases where neither a formula nor its negation (which can be syntactically obtained by an appropriate transformation) is satisfied by a given state. This happens in case of (negated) propositions, and tuples of the form (μ, t), where t does not belong to the time domain $\mathcal{T}$. For instance, in case of a generalised timed trace $\mu : \{0, 1, 2, 3\} \to \mathbb{R}$ corresponding to a small sampling of a real-valued signal, and proposition pos such that $\mathcal{O}(\mathsf{pos}) = \mathbb{R}_{>0}$ we have $(\mu, \sqrt{2}) \not\models \mathsf{pos}$, and $(\mu, \sqrt{2}) \not\models \neg\, \mathsf{pos}$, regardless of the actual values of μ for the sampling points in the time domain.

However, if all occurrences of propositions in a formula are guarded by an until of release operator, the satisfaction status of a formula is never ambiguous – this is because semantics of those operators refer only to time points within the time domain. Therefore, the ambiguity is never an issue in the context of our theory, as our relaxation operator always produces unambiguous formulae guarded with until or release operators.

We also remark that the semantics of until operator makes it possible for the "ultimate" formula ψ to hold *before* the current state (time point); this is because we allow formulae to be annotated with arbitrary intervals, in particular those with negative endpoints.

For the purpose of logical characterisation, we introduce the following relation.

Definition 4. *We say that a system* potentially exhibits property ϕ, *notation* $H(c,i) \models_\exists \phi$, *whenever* there exists $\mu \in H(c,i)$ *such that* $\mu \models \phi$.

The relation $\models_\exists$ can be seen as a variant of satisfaction relation for nondeterministic systems that has existential, rather than universal interpretation, the latter being the traditional interpretation in LTL literature. This alternative view on satisfaction is similar to one that is used in the context of Hennessy-Milner logic and its variations for behavioural models [20, 30], where a logical formula represents a (potentially) observable behaviour of a system. This approach is more suitable for the purpose of logical chracterisation.

3.3 Hybrid Conformance

Next, we provide the definition of hybrid conformance, due to Abbas and Fainekos [2, 1], in the context of our generalised semantic domain. Intuitively, hybrid conformance allows for conforming signal to differ up to τ in time and up to ϵ in the value.

We start with a one-directional conformance relation on individual traces.

Definition 5. *Let $\mu_1 : \mathcal{T}_1 \to \mathcal{Y}$ and $\mu_2 : \mathcal{T}_2 \to \mathcal{Y}$ be $\mathcal{Y}$-valued generalised timed traces. A trace μ_1 is (τ, ϵ)-close to μ_2, notation $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$, iff:*

$$\forall t_1 \in dom(\mu_1).\ \exists t_2 \in dom(t_2).\ |t_2 - t_1| \leq \tau \wedge d_{\mathcal{Y}}(\mu_2(t_2), \mu_1(t_1)) \leq \epsilon$$

In the above definition, μ_2 can match any value in μ_1 within a sufficiently small time interval, but can potentially contain some other signal values that cannot be matched by μ_1. We know at least that the "behaviour"of μ_1 in terms of signal values does not go beyond those of μ_2 (up to (τ, ϵ)-window).

By requiring two traces to be mutually conforming, we obtain the standard notion of hybrid conformance for individual traces:

Definition 6. *Let $\mu_1 : \mathcal{T}_1 \to \mathcal{Y}$ and $\mu_2 : \mathcal{T}_2 \to \mathcal{Y}$ be $\mathcal{Y}$-valued generalised timed traces. μ_1 and μ_2 are (τ, ϵ)-close, denoted by $\mu_1 \sim_{\tau,\epsilon} \mu_2$, whenever $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$ and $\mu_2 \sqsubseteq_{\tau,\epsilon} \mu_1$.*

When the precise value of τ and ϵ is not relevant, we refer to (τ, ϵ)-closeness as hybrid conformance. Below, we lift the notion of conformance from generalised timed traces to hybrid systems.

Definition 7. *Two hybrid systems $H_1, H_2 \in \mathcal{H}(\mathcal{C}, \mathcal{I}, \mathcal{Y})$ are (τ, ϵ)-close, denoted by $H_1 \sim_{\tau,\epsilon} H_2$, if and only if for all $c \in \mathcal{C}$ and $i \in \mathcal{I}$, it holds that*

$$\forall \mu_1 \in H_1(c, i)\ \exists \mu_2 \in H_2(c, i) :\ \mu_1 \sim_{\tau,\epsilon} \mu_2$$

$$\forall \mu_2 \in H_2(c, i)\ \exists \mu_1 \in H_1(c, i) :\ \mu_1 \sim_{\tau,\epsilon} \mu_2$$

We remark that there is another way of lifting the closeness relation of individual traces to systems, which is directly based on the one-directional (τ, ϵ)-closeness.

Definition 8. *A system H_1 is (τ, ϵ)-close to H_2, notation $H_1 \sqsubseteq_{\tau,\epsilon} H_2$, if for all c, i:*

$$\forall \mu_1 \in H_1(c, i).\ \exists \mu_2 \in H_2(c, i).\ \mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$$

Furthermore, one can define the symmetric variant of one-directional closeness relation on systems – this notion will become important in the context of logical characterisation.

Definition 9. *Two systems H_1 and H_2 are mutually (τ, ϵ)-close, notation $H_1 \equiv_{\tau,\epsilon} H_2$, iff $H_1 \sqsubseteq_{\tau,\epsilon} H_2$ and $H_2 \sqsubseteq_{\tau,\epsilon} H_1$.*

One can easily observe that on individual traces, as well as deterministic systems, the relation $\equiv_{\tau,\epsilon}$ coincides with the original (τ, ϵ)-closeness, i.e. the relation $\sim_{\tau,\epsilon}$. However, in case of nondeterministic systems, the relation $\equiv_{\tau,\epsilon}$ is strictly coarser.

Proposition 1. *The relation $\equiv_{\tau,\epsilon}$ is strictly coarser than $\sim_{\tau,\epsilon}$.*

Proof. That $\sim_{\tau,\epsilon}$ is at least as fine as $\equiv_{\tau,\epsilon}$ follows immediately from the definitions. To show strictness, we define two systems H_1 and H_2 such that $H_1 \equiv_{\tau,\epsilon} H_2$, while $H_1 \not\sim_{\tau,\epsilon} H_2$.

Given a trace μ, we use the notation $\mu[t_1 \mapsto y_1, \ldots, t_n \mapsto y_n]$ for a trace μ' with the same domain as μ whose values coincide with those of μ at every time point except $t_1, \ldots, t_n$, where $\mu'(t_i) = y_i$.

Let us define $\mu^0 : [0, 2] \to \mathbb{R}$ as $\mu^0(t) = 0$ for all $t \in [0, 2]$.

Furthermore, we define the following traces:

$$\begin{array}{rclrcl} \mu^1 & = & \mu^0[0 \mapsto 1] & \mu^2 & = & \mu^0[0 \mapsto \frac{1}{2}, 1 \mapsto 1] \\ \mu^3 & = & \mu^0[1 \mapsto \frac{1}{2}, 2 \mapsto 1] & \mu^4 & = & \mu^0[0 \mapsto 1, 2 \mapsto \frac{1}{2}] \end{array}$$

One can easily observe that by taking any $\tau \in (0, 1)$ and $\epsilon \in [\frac{1}{2}, 1)$, for instance $\tau = \frac{1}{10}, \epsilon = \frac{3}{4}$, we have the following relationships:

$\mu^1 \sqsubseteq_{\tau,\epsilon} \mu^2 \sqsubseteq_{\tau,\epsilon} \mu^3 \sqsubseteq_{\tau,\epsilon} \mu^4 \sim_{\tau,\epsilon} \mu_1$

Moreover, the first three one-directional closeness relations are strict. This is due to the general phenomenon that a locally continuous trace obtained by another one by adding singularity points on which the difference with the original trace exceeds ϵ, can match the original trace within any (τ, ϵ)-window for a nonzero τ. On the other hand, values in singularities cannot be matched by the original trace.

By taking H_1 whose behaviour, for all relevant c and i, consists of traces μ^1 and μ^3, and on the other hand H_2 whose behaviour are precisely μ_2 and μ_4, we obtain $H_1 \equiv_{\tau,\epsilon} H_2$ while $H_1 \not\sim_{\tau,\epsilon} H_2$. To see that the latter holds, observe that for instance the trace μ^2 from H_2 cannot be matched in the sense of $\sim_{\tau,\epsilon}$ by any trace in H_1. $\square$

3.4 Logical Characterisation via Relaxation

Logical characterisation of a relation provides means to uniquely identify classes of related systems by sets of formulae in a certain logic. In case of non-exact relations involving some tolerance thresholds for disturbances, such as hybrid conformance, one cannot directly compare sets of formulae satisfied by systems in question.

Our approach to characterisation involves the notion of relaxation of logical formulae, that has been used in the context of hybrid systems [1, 15, 26]. It involves a syntactical transformation of a formula to a weaker one, which is supposed to be also satisfied by at least one trace of a conforming system.

Assume a logic (a collection of formulae) $\mathcal{L}$ and a notion of relaxation $\mathsf{rlx} : \mathcal{L} \to \mathcal{L}$. We shall use the following notation for preservation of logical formulae under relaxation by systems (note the use of $\models_\exists$ relation):

- $H \preceq^{\mathsf{rlx}}_{\mathcal{L}} H'$ iff $\forall_{c \in \mathcal{C}, i \in \mathcal{I}} H(c, i) \models_\exists \phi \implies H'(c, i) \models_\exists \mathsf{rlx}(\phi)$
- $H \approx^{\mathsf{rlx}}_{\mathcal{L}} H'$ iff $H \preceq^{\mathsf{rlx}}_{\mathcal{L}} H' \wedge H' \preceq^{\mathsf{rlx}}_{\mathcal{L}} H$

Our notion of characterisation can now be defined as follows

Definition 10. *A logic $\mathcal{L}$ and a notion of relaxation $\mathsf{rlx}: \mathcal{L} \to \mathcal{L}$ characterise a [symmetric] relation $R \subseteq \mathcal{H} \times \mathcal{H}$ if and only if, for any two systems H and H' such that $H\,R\,H'$, we have $H \preceq_{\mathcal{L}}^{\mathsf{rlx}} H'$ [$H \approx_{\mathcal{L}}^{\mathsf{rlx}} H'$]*

The implication from left to right is called preservation and there already exist some preservation results in the literature [1, 15]; the implication from right to left (called reflection) has not been studied for hybrid conformance and MTL to the best of our knowledge.

3.5 AMF-Relaxation

Abbas, Mittelmann, and Fainekos [1] showed that the satisfaction of MTL formulae is preserved by hybrid conformance. However, to formulate a logical preservation result for an approximate notion of conformance such as hybrid conformance, they had to cater for the possible perturbation of intervals in the MTL formulae, using a notion of relaxation, which we call AMF-relaxation (for Abbas, Mittelmann, and Fainekos). Originally the definition was given on the super-dense time domain (i.e., a time domain that allows for specifying the ordering of simultaneous events). Since the "super-denseness" of the time domain does not have any influence on our study, we simplify the time domain to a dense time domain (such as non-negative real numbers). We also adapt the presentation to the generalised timed traces framework.

Definition 11. *Given $\tau, \epsilon \geq 0$, the relaxation operator $[]^{\text{AMF}}_{\tau,\epsilon} : \mathit{MTL}^+ \to \mathit{MTL}^+_{ext}$ is defined as follows:*

$$\begin{array}{lcl}
[\mathsf{T}]^{\text{AMF}}_{\tau,\epsilon} = \mathsf{T} & , & [\mathsf{F}]^{\text{AMF}}_{\tau,\epsilon} = \mathsf{F} \\
[p]^{\text{AMF}}_{\tau,\epsilon} = p^+(\epsilon) & , & [\neg p]^{\text{AMF}}_{\tau,\epsilon} = p^-(\epsilon) \\
[\phi_1 \wedge \phi_2]^{\text{AMF}}_{\tau,\epsilon} & = & [\phi_1]^{\text{AMF}}_{\tau,\epsilon} \wedge [\phi_2]^{\text{AMF}}_{\tau,\epsilon} \\
[\phi_1 \vee \phi_2]^{\text{AMF}}_{\tau,\epsilon} & = & [\phi_1]^{\text{AMF}}_{\tau,\epsilon} \vee [\phi_2]^{\text{AMF}}_{\tau,\epsilon} \\
[\phi\,\mathcal{U}_I\,\psi]^{\text{AMF}}_{\tau,\epsilon} & = & (\Diamond_{(-2\tau,0]}[\phi]^{\text{AMF}}_{\tau,\epsilon})\,\mathcal{U}_{I_{<-2\tau,2\tau>}}\,(\Diamond_{[0,2\tau)}[\psi]^{\text{AMF}}_{\tau,\epsilon}) \\
[\phi\,\mathcal{R}_I\,\psi]^{\text{AMF}}_{\tau,\epsilon} & = & (\Diamond_{(-2\tau,0]}[\phi]^{\text{AMF}}_{\tau,\epsilon})\,\mathcal{R}_{I_{<2\tau,-2\tau>}}\,(\Diamond_{[0,2\tau)}[\psi]^{\text{AMF}}_{\tau,\epsilon}),
\end{array}$$

where $I_{<a,b>}$ is the relaxation of the bounds of interval I with constants a and b, formally defined as follows. For $a, b \in \mathbb{R}$, let $\mathcal{T}(a,b) := \{[a,b], (a,b], [a,b), (a,b)\}$; then for any interval $I \in \mathcal{T}(a,b)$, $I_{<c,d>} := (a+c, b+d)$.

It follows from Definition 11 that the relaxation operator $[]^{\text{AMF}}_{\tau,\epsilon}$ applied to until or release formulae annotated with any interval from $\mathcal{T}(a,b)$ produces the same formulae:

Observation 1. *For any $I \in \mathcal{T}(a,b)$, we have:*

$$\begin{array}{lcl}
[\phi\,\mathcal{U}_I\,\psi]^{\text{AMF}}_{\tau,\epsilon} & = & (\Diamond_{(-2\tau,0]}[\phi]^{\text{AMF}}_{\tau,\epsilon})\,\mathcal{U}_{(a-2\tau,b+2\tau)}\,(\Diamond_{[0,2\tau)}[\psi]^{\text{AMF}}_{\tau,\epsilon}) \\
[\phi\,\mathcal{R}_I\,\psi]^{\text{AMF}}_{\tau,\epsilon} & = & (\Diamond_{(-2\tau,0]}[\phi]^{\text{AMF}}_{\tau,\epsilon})\,\mathcal{R}_{(a+2\tau,b-2\tau)}\,(\Diamond_{[0,2\tau)}[\psi]^{\text{AMF}}_{\tau,\epsilon})
\end{array}$$

The following preservation result can be found in [1].

Theorem 1. *Let $\phi \in \mathsf{MTL}^+$. Let $\mu_1 : \mathcal{T}_1 \to \mathcal{Y}$ and $\mu_2 : \mathcal{T}_2 \to \mathcal{Y}$ be two discrete GTTs, i.e. $\mathcal{T}_1, \mathcal{T}_2 \subseteq \mathcal{P}_{FIN}(\mathbb{R}_{\geq 0})$. If $\mu_1 \sim_{\tau,\epsilon} \mu_2$, then for any $t_1 \in \mathcal{T}_1$ if $(\mu_1, t_1) \models \phi$, then for all $t_2 \in \mathcal{T}_2$ such that $|t_2 - t_1| \leq \tau$ and $|\mu_2(t_2) - \mu_1(t_1)| \leq \epsilon$, we have*

$$(\mu_2, t_2) \models [\phi]^{\text{AMF}}_{\tau,\epsilon}$$

Observe that the above preservation property is very strong: it holds for *any* sampling point in the conforming trace that matches the given point within the (τ, ϵ)-"window". This kind of result comes at a price of having to employ a relaxation operator which yields considerably weaker formulae, which explains the significant relaxation of intervals in $[]^{\text{AMF}}_{\tau,\epsilon}$.

4 Laxness in AMF-Relaxation

In this section, we prove that the notion of AMF-relaxation is too lax for the purpose of logical characterisation of hybrid conformance, i.e., there is a class of non-conforming implementations which preserve AMF-relaxations of all MTL properties satisfied by their specifications.

Throughout this section, we assume a simple setting where values range over Booleans, i.e. $\mathcal{Y} = \mathbb{B} = \{\mathbf{true}, \mathbf{false}\}$. The associated metric on $\mathcal{P}(\mathbb{B})$ is defined as $d(b_1, b_2) = 0$ if $b_1 = b_2$, and ∞ otherwise.

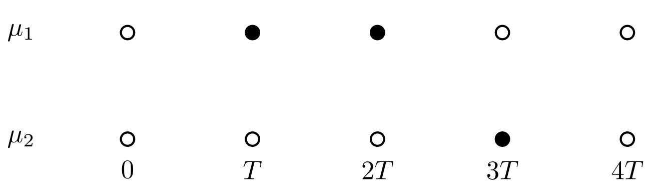
As explained in the previous section, generalised timed traces with a finite time domain shall be called timed state sequences, or TSSs.

We first explain the gist of our proof by showing one instance of the above-mentioned family of non-conforming counter-examples.

Example 1. *Fix $\tau > 0$ and let $T = \tau - \delta$, where $\delta \ll \tau$. Consider the following two timed state sequences μ_1 and μ_2:*

$$\begin{array}{ll} \mu_1(0) = \mathbf{true} & \mu_2(0) = \mathbf{true} \\ \mu_1(T) = \mathbf{false} & \mu_2(T) = \mathbf{true} \\ \mu_1(2T) = \mathbf{false} & \mu_2(2T) = \mathbf{true} \\ \mu_1(3T) = \mathbf{true} & \mu_2(3T) = \mathbf{false} \\ \mu_1(4T) = \mathbf{true} & \mu_2(4T) = \mathbf{true} \end{array}$$

The two TSSs can be depicted as follows (white/black dots represent states that have value, respectively, **true** */* **false***):*



μ_1 and μ_2 are not $(\tau, 0)$-equivalent, not even $(t, 0)$-equivalent for any $t < 2T$. To observe this note that for instance $\mu_1(T)$ cannot be matched by μ_2 within $(-T, 3T)$ since no state in μ_2 has value **false** *in this interval. On the other hand,*

as we show next, TSSs μ_2 satisfies the AMF-relaxation of all MTL formulae satisfied by μ_1 (relaxed by parameters $(\tau, 0)$ and vice versa. Intuitively, this is because the intervals in the until and release formulae are respectively expanded and compressed by 2τ, allowing for shifts by 2τ in the states of TSS without affecting the satisfaction of formulae.

In the remainder of this section, we generalise this example and prove this fact for a broader, infinite class of pairs of TSSs which are not $(t, 0)$-equivalent for any $t < 2\tau$.

Definition 12. *For a pair of TSSs $\mu_A : \mathcal{T}_A \to \mathbb{B}$ and $\mu_B : \mathcal{T}_B \to \mathbb{B}$, we say that μ_B is* stretched to the right of μ_A by less than t, *if there is some $K \in \mathbb{N}$ and functions $\textsc{chunk}_A : \mathcal{T}_A \to \{1, \ldots, K\}$ and $\textsc{chunk}_B : \mathcal{T}_B \to \{1, \ldots, K\}$ such that the following hold:*

- *$\textsc{chunk}_A$ and $\textsc{chunk}_B$ are surjective and non-decreasing*
- *all states that map to the same chunk number have the same value, i.e. for all $k \in \{1, \ldots, K\}$ and for all $t_A \in \mathcal{T}_A$, $t_B \in \mathcal{T}_A$ such that $\textsc{chunk}_A(t_A) = \textsc{chunk}_B(t_B) = k$, we have $\mu_A(t_A) = \mu_B(t_B)$*
- *for any $t_A \in \mathcal{T}_A$, there is some $t_B \in \mathcal{T}_B$ such that*

$$(*) \quad 0 \leq t_B - t_A < t \quad \wedge \quad \textsc{chunk}_A(t_A) = \textsc{chunk}_B(t_B)$$

  *and conversely, for any $t_B \in \mathcal{T}_B$ there is some $t_A \in \mathcal{T}_A$ such that (*) holds. We shall call a pair $(\mu_A, t_A), (\mu_B, t_B)$ satisfying (*) a pair of **t-corresponding states**.*

Note that in the last condition, the inequality in (*) involves the actual difference between t_B and t_A, not its absolute value – we allow μ_B to be shifted only to the right as compared to μ_A. The following example illustrates this definition.

Example 2. *Consider the TSSs in Example 1; the TSS μ_2 is stretched to the right of μ_1 by less than 2τ, as witnessed by the following functions $\textsc{chunk}_1$ and $\textsc{chunk}_2$:*

$\textsc{chunk}_1(0) = 1$	$\textsc{chunk}_2(t) = 1$
$\textsc{chunk}_1(t) = 2$ *for* $t \in \{T, 2T\}$	*for* $t \in \{0, T, 2T\}$
$\textsc{chunk}_1(t) = 3$ *for* $t \in \{3T, 4T\}$	$\textsc{chunk}_2(3T) = 2$
	$\textsc{chunk}_2(4T) = 3$

The key proposition below states that for 2τ-corresponding states, the satisfaction of all formulae in MTL^+ is preserved modulo relaxation $[]^{\text{AMF}}_{\tau,0}$.

Example 3. *Considering Example 1 and propositions $p_\mathbf{t}$ and $p_\mathbf{f}$ such that $\mathcal{O}(p_\mathbf{t}) = \{\mathbf{true}\}$ and $\mathcal{O}(p_\mathbf{f}) = \{\mathbf{false}\}$; we have $(\mu_2, 0) \models p_\mathbf{t}\, \mathcal{U}_{[3T,3T]}\, p_\mathbf{f}$, and the 2τ-corresponding state $(\mu_1, 0)$ satisfies the relaxed formula $[p_\mathbf{t}\, \mathcal{U}_{[3T,3T]}\, p_\mathbf{f}]^{\text{AMF}}_{\tau,0}$. The latter statement can be easily deduced from the fact that $(\mu_1, 0)$ satisfies $p_\mathbf{t}\, \mathcal{U}_{(3T-2\tau,3T+2\tau)}\, p_\mathbf{f}$, a simpler formula that logically entails $[p_\mathbf{t}\, \mathcal{U}_{[3T,3T]}\, p_\mathbf{f}]^{\text{AMF}}_{\tau,0}$.*

Proposition 2. *Suppose μ_B is stretched to the right of μ_A by less than 2τ. Then for any $t_A \in \mathcal{T}_A$, and any $t_B \in \mathcal{T}_B$ satisfying*

$$(*) \quad 0 \leq t_B - t_A < 2\tau \quad \wedge \quad \textsc{chunk}_A(t_A) = \textsc{chunk}_B(t_B)$$

we have, for all formulae $\phi \in \mathsf{MTL}^+$:

- $(\mu_A, t_A) \models \phi \implies (\mu_B, t_B) \models [\phi]^{\text{AMF}}_{\tau,0}$
- $(\mu_B, t_B) \models \phi \implies (\mu_A, t_A) \models [\phi]^{\text{AMF}}_{\tau,0}$

5 Logical Characterisation of Hybrid Conformance

As proven in the previous section, the existing notions of relaxation in the literature are not sufficiently tight for the purpose of a logical characterisation of (τ, ϵ)-conformance. In this section, we define a novel (and in our view, very natural) relaxation operator on MTL which, as we subsequently show, precisely serves for this purpose.

5.1 The relaxation operator

We shall now introduce the new relaxation operator on MTL. Syntactically, it has a simpler structure than the one in [1], as here the actual relaxation is performed on the level of propositions only.

Definition 13. *Let $\tau, \epsilon \geq 0$. The relaxation operator $\mathit{rlx}_{\tau,\epsilon} : \mathsf{MTL}^+ \to \mathsf{MTL}^+_{ext}$ is defined as follows:*

$$\begin{array}{lcl}
\mathit{rlx}_{\tau,\epsilon}(\mathsf{T}) = \mathsf{T} & , & \mathit{rlx}_{\tau,\epsilon}(\mathsf{F}) = \mathsf{F} \\
\mathit{rlx}_{\tau,\epsilon}(p) = \Diamond_{[-\tau,\tau]}\, p^+(\epsilon) & , & \mathit{rlx}_{\tau,\epsilon}(\neg p) = \Diamond_{[-\tau,\tau]}\, p^-(\epsilon) \\
\mathit{rlx}_{\tau,\epsilon}(\phi_1 \wedge \phi_2) & = & \mathit{rlx}_{\tau,\epsilon}(\phi_1) \wedge \mathit{rlx}_{\tau,\epsilon}(\phi_2) \\
\mathit{rlx}_{\tau,\epsilon}(\phi_1 \vee \phi_2) & = & \mathit{rlx}_{\tau,\epsilon}(\phi_1) \vee \mathit{rlx}_{\tau,\epsilon}(\phi_2) \\
\mathit{rlx}_{\tau,\epsilon}(\phi\, \mathcal{U}_I\, \psi) & = & \mathit{rlx}_{\tau,\epsilon}(\phi)\, \mathcal{U}_I\, \mathit{rlx}_{\tau,\epsilon}(\psi) \\
\mathit{rlx}_{\tau,\epsilon}(\phi\, \mathcal{R}_I\, \psi) & = & \mathit{rlx}_{\tau,\epsilon}(\phi)\, \mathcal{R}_I\, \mathit{rlx}_{\tau,\epsilon}(\psi)
\end{array}$$

Note that each relaxation of a formula different than T and F is guarded by either release or until formulae, and hence its satisfaction status is always unambiguous.

5.2 Characterisation of traces and deterministic systems

We proceed to show that the introduced relaxation operator can be used to characterise the (τ, ϵ)-closeness, starting with the individual timed traces. Note that since the results below concern arbitrary generalised timed traces, they apply also to the setting with two traces of different kind, e.g., a discrete TSS against a continuous trajectory.

5.2.1 Preservation modulo relaxation

We start by proving that the satisfaction of MTL^+ formulae is preserved by (τ, ϵ)-close timed traces modulo $\mathsf{rlx}_{\tau,\epsilon}$ relaxation.

Proposition 3. *Let $\mu_1 : \mathcal{T}_1 \to \mathcal{Y}$, $\mu_2 : \mathcal{T}_2 \to \mathcal{Y}$ be two $\mathcal{Y}$-valued generalised timed traces, and ϕ be an MTL formula. If $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$, then, for any $t \in \mathbb{R}$:*

$$(\mu_1, t) \models \phi \implies (\mu_2, t) \models \mathsf{rlx}_{\tau,\epsilon}(\phi)$$

Proof. The proof proceeds by structural induction on the formula ϕ.

- $\phi = p$: since $(\mu_1, t) \models p$, we have $t \in \mathcal{T}_1$ and $\mu_1(t) \in \mathcal{O}(p)$. Furthermore, since $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$, we know that there is some t' such that $|t' - t| \leq \tau$ and $d(y_1(t), y_2(t')) \leq \epsilon$. We have thus $y_2(t') \in \mathcal{O}(p^+(\epsilon))$, and hence $(\mu_2, t') \models p^+(\epsilon)$. Moreover, since $|t' - t| \leq \tau$, we obtain $(y_2, t) \models \Diamond_{[-\tau,\tau]}\, p^+(\epsilon) = \mathsf{rlx}_{\tau,\epsilon}(p)$.
- $\phi = \phi\,\mathcal{U}_I\,\psi$: since $(\mu_1, t) \models \phi\,\mathcal{U}_I\,\psi$, there is some $t_1 \in \mathcal{T}_1$ such that $t_1 - t \in I$ and $(\mu_1, t_1) \models \psi$, and moreover for any $t_0 \in [t, t_1)$ we have $(\mu_1, t_0) \models \phi \vee (\mu_1, t_0) \models \psi$. By applying the inductive hypothesis, we obtain that $(\mu_2, t_1) \models \mathsf{rlx}_{\tau,\epsilon}(\psi)$, and for any $t_0 \in [t, t_1)$ we have $(\mu_2, t_0) \models \mathsf{rlx}_{\tau,\epsilon}(\phi)$ or $(\mu_2, t_0) \models \mathsf{rlx}_{\tau,\epsilon}(\psi)$. We thus have $(\mu_2, t) \models \mathsf{rlx}_{\tau,\epsilon}(\phi)\,\mathcal{U}_I\, \mathsf{rlx}_{\tau,\epsilon}(\psi)$, and from the definition of relaxation we immediately obtain $(y_2, t) \models \mathsf{rlx}_{\tau,\epsilon}(\phi\,\mathcal{U}_I\,\psi)$.
- $\phi = \phi\,\mathcal{R}_I\,\psi$: take any $t' \in \mathcal{T}_2$ such that $t' - t \in I$ and $(\mu_2, t') \not\models \psi$. From the inductive hypothesis, we have $(\mu_1, t') \not\models \psi$, and since $(\mu_1, t) \models \phi\,\mathcal{R}_I\,\psi$, we know that there is some $t_1 \in \mathcal{T}_1$ such that $t_1 < t'$, $t_1 - t$, and $(\mu_1, t_1) \models \phi$. By applying the inductive hypothesis again, we obtain $(\mu_2, t_1) \models \phi$. From the statements obtained above we can now infer that $(\mu_2, t) \models \phi\,\mathcal{R}_I\,\psi$.

□

5.2.2 Existence of distinguishing formula for non-conforming traces

We shall now prove that the converse of the preceding theorem holds as well: whenever a timed traces is not (τ, ϵ)-close to another, we can always find an MTL formula that witnesses this, that is, for which preservation modulo $\mathsf{rlx}_{\tau,\epsilon}$ relaxation operator does not hold.

Proposition 4. *Let $\mu_1 : \mathcal{T}_1 \to \mathcal{Y}$ and $\mu_2 : \mathcal{T}_2 \to \mathcal{Y}$ be two $\mathcal{Y}$-valued timed traces. If $\mu_1 \not\sqsubseteq_{\tau,\epsilon} \mu_2$, then there is a formula $\phi \in \mathsf{MTL}^+$ such that ϕ distinguishes μ_1 from μ_2 modulo relaxation $\mathsf{rlx}_{\tau,\epsilon}$, that is:*

$$\mu_1 \models \phi \ \wedge \ \mu_2 \not\models \mathsf{rlx}_{\tau,\epsilon}(\phi)$$

Proof. Suppose that there is some $t_1 \in \mathcal{T}_1$ for which there is no $t_2 \in \mathcal{T}_2$ such that $|t_2 - t_1| \leq \tau$ and $|\mu_2(t_2) - \mu_1(t_1)| \leq \epsilon$. Consider an MTL formula $\phi = \Diamond_{[t_1,t_1]}p$, where $\mathcal{O}(p) = \{\mu_1(t_1)\}$. Obviously, we have $\mu_1 \models \phi$, however, the relaxed version of the formula $\mathsf{rlx}_{\tau,\epsilon}(\phi) = \Diamond_{[t_1,t_1]}\Diamond_{[-\tau,\tau]}p^+(\epsilon)$ cannot be satisfied by μ_2. □

To illustrate the above proposition, recall the timed state sequences μ_1 and μ_2 from Example 1. The value of μ_1 at time point T cannot be matched by μ_2 within the interval $[T-\tau, T+\tau]$. The construction from Proposition 4 yields the formula $\phi_d = \Diamond_{[-\tau,\tau]} p_{\mathbf{f}}$, where $\mathcal{O}(p_{\mathbf{f}}) = \{\mathbf{false}\}$; this formula is obviously satisfied by μ_1. On the other hand, the relaxed formula $\mathsf{rlx}_{\tau,\epsilon}(\phi_d) = \Diamond_{[T,T]}\Diamond_{[-\tau,\tau]} p_{\mathbf{f}}$ is not satisfied by μ_2, as this would require $\Diamond_{[-\tau,\tau]} p_{\mathbf{f}}$ to hold in (μ_2, T). This in turn is impossible, because in all three states in μ_2 with time points belonging to $[T-\tau, T+\tau]$, the proposition $p_{\mathbf{f}}$ does not hold.

5.2.3 Characterisation theorem for deterministic systems

Propositions 3 and 4 provide the characterisation of relations $\sqsubseteq_{\tau,\epsilon}$ and $\sim_{\tau,\epsilon}$ by MTL^+ and the relaxation $\mathsf{rlx}_{\tau,\epsilon}$ on individual traces. As an immediate corollary, we also obtain the characterisation theorem for deterministic systems.

Theorem 2. *For any two deterministic systems H and H', the following characterisation results hold:*

- $H \sqsubseteq_{\tau,\epsilon} H' \iff H \preceq^{\mathsf{rlx}_{\tau,\epsilon}}_{\mathsf{MTL}^+} H'$
- $H \sim_{\tau,\epsilon} H' \iff H \equiv_{\tau,\epsilon} H' \iff H \approx^{\mathsf{rlx}_{\tau,\epsilon}}_{\mathsf{MTL}^+} H'$

Note that the equivalence $H \sim_{\tau,\epsilon} H' \iff H \equiv_{\tau,\epsilon} H'$ holds specifically because were are in the setting of deterministic systems.

5.3 Nondeterministic systems

Unfortunately, if one ventures beyond deterministic systems, the standard hybrid conformance relation $\sim_{\tau,\epsilon}$ proves difficult to characterise in the traditional sense, that is, by pinpointing a formula that is satisfied, or potentially exhibited, by one system and not the other. This is because, given a trace μ_1 from one system that is not conforming (in the $\sim_{\tau,\epsilon}$ sense) to any relevant trace μ_2^j in the other system, the reason why it is not conforming may be that for some of the traces μ_2^j only $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2^j$ fails, whereas for other traces only $\mu_2^j \sqsubseteq_{\tau,\epsilon} \mu_1$ fails. In such situation, the distinguishing formulae witnessing lack of one-directional conformance are sometimes satisfied only by a trace in one system, and sometimes only by a trace in the other system, making it impossible to construct a single formula satisifed/exhibited by one system. In fact, any logic preserved under relaxation by $\sqsubseteq_{\tau,\epsilon}$ (i.e. such that proposition 3 holds) cannot distinguish systems H_1 and H_2 from the proof of proposition 1.

While we believe that in order to provide a "proper" characterisation of $\sim_{\tau,\epsilon}$ on nondeterministic systems one would likely need a notion of characterisation vastly different in style from those that have appeared in the literature, in the remainder of this section we show that the relations $\sqsubseteq_{\tau,\epsilon}$ and $\equiv_{\tau,\epsilon}$ admit such characterisation.

5.3.1 Finitely branching systems

For hybrid systems that are finitely branching (i.e. have bounded non-determinism, see definition 2), the characterisation result can be obtained for $\sqsubseteq_{\tau,\epsilon}$ and $\equiv_{\tau,\epsilon}$ in a straightforward manner.

Theorem 3. *The logic MTL^+, together with the relaxation operator $\mathsf{rlx}_{\tau,\epsilon}$, characterise the conformance relations $\sqsubseteq_{\tau,\epsilon}$ and $\equiv_{\tau,\epsilon}$ on finitely branching hybrid systems. That is, for arbitrary finitely branching hybrid systems H and H', the following statements hold:*

- $H \sqsubseteq_{\tau,\epsilon} H' \iff H \preceq^{\mathsf{rlx}_{\tau,\epsilon}}_{\mathsf{MTL}^+} H'$
- $H \equiv_{\tau,\epsilon} H' \iff H \approx^{\mathsf{rlx}_{\tau,\epsilon}}_{\mathsf{MTL}^+} H'$

Proof. We provide proof for $\sqsubseteq_{\tau,\epsilon}$, the characterisation of $\equiv_{\tau,\epsilon}$ follows as immediate corollary.

- (preservation): Take any two hybrid systems H_1, H_2 such that $H_1 \sqsubseteq_{\tau,\epsilon} H_2$. Take any $c \in \mathcal{C}, i \in \mathcal{I}$. Suppose w.l.o.g. that $H_1(c,i) \models_\exists \phi$; we need to show that $H_2(c,i) \models_\exists \mathsf{rlx}_{\tau,\epsilon}(\phi)$. Take any $\mu_1 \in H_1(c,i)$ such that $\mu_1 \models \phi$. Since $H_1 \sqsubseteq_{\tau,\epsilon} H_2$, there is some $\mu_2 \in H_2(c,i)$ such that $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$. Since $\mu_1 \models \phi$, from proposition 3 we obtain $\mu_2 \models \mathsf{rlx}_{\tau,\epsilon}(\phi)$. It follows that $H_2(c,i) \models_\exists \mathsf{rlx}_{\tau,\epsilon}(\phi)$.
- (reflection/distinguishing formula): Suppose that $H_1 \not\sqsubseteq_{\tau,\epsilon} H_2$, and moreover w.l.o.g. suppose that for certain $c \in \mathcal{C}, i \in \mathcal{I}$ there is some $\mu_1 \in H_1(c,i)$ such that for all $\mu_2^j \in H_2(c,i)$ we have $\mu_1 \not\sqsubseteq_{\tau,\epsilon} \mu_2^j$. From proposition 4 we know that for each such $\mu_2^j \in H_2(c,i)$ there is a distinguishing formula ϕ_j such that $\mu_1 \models \phi_j$ and $\mu_2^j \not\models \mathsf{rlx}_{\tau,\epsilon}(\phi_j)$. Consider a formula $\Phi = \bigwedge_{j:\mu_2^j \in H_2(c,i)} \phi_j$. Since $H_2(c,i)$ is a finite set, Φ is a well-formed MTL^+formula. We now have $H_1(c,i) \models_\exists \Phi$, but since obviously for any j, $\mu_2^j \not\models \mathsf{rlx}_{\tau,\epsilon}(\Phi)$, we also have $H_2(c,i) \not\models_\exists \mathsf{rlx}_{\tau,\epsilon}(\Phi)$. Hence Φ distinguishes $H_1(c,i)$ from $H_2(c,i)$.

$\square$

5.3.2 Systems with unbounded non-determinism

In order to provide characterisation for $\sqsubseteq_{\tau,\epsilon}$ and $\equiv_{\tau,\epsilon}$ on systems with infinite branching, one needs to endow the logic MTL^+ with infinite conjunctions and disjunctions; the syntax of such logic, denoted with MTL^+_∞, is given below (Ind ranges over arbitrary sets of indices).

$$\phi ::= \mathsf{T} \mid \mathsf{F} \mid p \mid \neg p \mid \bigwedge_{i \in Ind} \phi_i \mid \bigvee_{i \in Ind} \phi_i \mid \phi\, \mathcal{U}_I\, \phi \mid \phi\, \mathcal{R}_I\, \phi$$

Theorem 4. *The logic MTL^+_∞, together with the relaxation operator $\mathsf{rlx}_{\tau,\epsilon}$, characterise the conformance relations $\sqsubseteq_{\tau,\epsilon}$ and $\equiv_{\tau,\epsilon}$ on arbitrary hybrid systems.*

Proof. The proof is nearly the same as the one of Theorem 3, except that while proving the reflection property, the set of distinguishing formulae for individual traces may be infinite. However, a disjunction over such a set is now a well-formed $\mathsf{MTL}^{+}_{\infty}$ formula, hence the construction is valid. □

6 Conclusions and Future Work

In this paper, we have presented a characterisation of hybrid conformance in Metric Temporal Logic. Since the notion of hybrid conformance allows for some deviations (in time and value), the characterisation is expressed in terms of a relaxation of the set of formulae satisfied by a system. We showed that the existing relaxation scheme proposed by Abbas, Fainekos, and Mittelmann is too lax to serve for a characterisation, i.e., there is a class of non-conforming systems that do satisfy all relaxations of the specification properties. Hence, we proposed a tighter notion of relaxation and showed that it is the appropriate notion to provide a characterisation of hybrid conformance.

Regarding future research, an open question remains whether and how one could characterise the original notion of hybrid conformance on nondeterministic systems. As explained in section 5.3, this may require a different approach to characterisation than what we have encountered so far in the literature – a potential solution could involve considering hyperproperties [9, 24] on a composition of two systems, with some well-defined family of formulae consituting witnesses for non-conformance of systems.

We would also like to investigate the possibility of characterising of Skorokhod conformance with Freeze Temporal Logic and the notion of relaxation provided by Deshmukh, Majumdar, and Prabhu [15]. Coming up with the notion of characteristic formulae is another avenue for our future research, which leads to a new technique for checking hybrid conformance.

References

[1] Houssam Abbas, Hans D. Mittelmann, and Georgios E. Fainekos. Formal property verification in a conformance testing framework. *Proceedings of MEMOCODE 2014*, pages 155–164, 2014. URL: https://doi.org/10.1109/MEMCOD.2014.6961854, doi:10.1109/MEMCOD.2014.6961854.

[2] Houssam Y. Abbas. *Test-Based Falsification and Conformance Testing for Cyber-Physical Systems*. PhD thesis, Arizona State University, 2015. URL: http://hdl.handle.net/2286/R.A.150686.

[3] Samson Abramsky. Observation equivalence as a testing equivalence. *Theor. Comput. Sci.*, 53:225–241, 1987.

[4] Luca Aceto, Anna Ingolfsdottir, Kim Guldstrand Larsen, and Jiri Srba. *Reactive Systems: Modelling, Specification and Verification*. Cambridge University Press, 2007. doi:10.1017/CBO9780511814105.

[5] Rajeev Alur, Tomás Feder, and Thomas A. Henzinger. The benefits of relaxing punctuality. *J. ACM*, 43(1):116–146, 1996. URL: http://doi.acm.org/10.1145/227595.227602, doi:10.1145/227595.227602.

[6] Rajeev Alur and Thomas A. Henzinger. Real-time logics: Complexity and expressiveness. *Information and Computation*, 104(1):35 – 77, 1993. URL: http://www.sciencedirect.com/science/article/pii/S0890540183710254, doi:https://doi.org/10.1006/inco.1993.1025.

[7] Bard Bloom, Wan Fokkink, and Rob J. van Glabbeek. Precongruence formats for decorated trace preorders. In *15th Annual IEEE Symposium on Logic in Computer Science, Santa Barbara, California, USA, June 26-29, 2000*, pages 107–118. IEEE Computer Society, 2000. URL: https://doi.org/10.1109/LICS.2000.855760, doi:10.1109/LICS.2000.855760.

[8] Manfred Broy, Bengt Jonsson, Joost-Pieter Katoen, Martin Leucker, and Alexander Pretschner. *Model-Based Testing of Reactive Systems*, volume 3472 of *Lecture Notes in Computer Science*. Springer, 2005.

[9] Michael R. Clarkson, Bernd Finkbeiner, Masoud Koleini, Kristopher K. Micinski, Markus N. Rabe, and César Sánchez. Temporal logics for hyperproperties. In Martín Abadi and Steve Kremer, editors, *POST 2014*, volume 8414 of *LNCS*, pages 265–284. Springer, 2014. URL: http://dx.doi.org/10.1007/978-3-642-54792-8_15, doi:10.1007/978-3-642-54792-8_15.

[10] Rance Cleaveland and Steve Sims. The NCSU concurrency workbench. In *Proceedings of the 8th International Conference on Computer Aided Verification (CAV '96)*, volume 1102 of *Lecture Notes in Computer Science*, pages 394–397. Springer, 1996. doi:10.1007/3-540-61474-5_87.

[11] Thao Dang. Model-based testing of hybrid systems. *Monograph in Model-Based Testing for Embedded Systems, CRC Press*, 2010.

[12] Luca de Alfaro, Marco Faella, and Mariëlle Stoelinga. Linear and branching system metrics. *IEEE Trans. Software Eng.*, 35(2):258–273, 2009.

[13] Rocco De Nicola and Matthew Hennessy. Testing equivalences for processes. *Theor. Comput. Sci.*, 34:83–133, 1984. URL: https://doi.org/10.1016/0304-3975(84)90113-0, doi:10.1016/0304-3975(84)90113-0.

[14] Jyotirmoy V. Deshmukh, Alexandre Donzé, Shromona Ghosh, Xiaoqing Jin, Garvit Juniwal, and Sanjit A. Seshia. Robust online monitoring of signal temporal logic. *Formal Methods in System Design*, 51(1):5–30, 2017. doi:10.1007/s10703-017-0286-7.

[15] Jyotirmoy V. Deshmukh, Rupak Majumdar, and Vinayak S. Prabhu. Quantifying conformance using the Skorokhod metric. *Formal Methods in System Design*, 50(2-3):168–206, 2017. URL: https://doi.org/10.1007/s10703-016-0261-8, doi:10.1007/s10703-016-0261-8.

[16] Daniel Gburek and Christel Baier. Bisimulations, logics, and trace distributions for stochastic systems with rewards. In *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (HSCC 2018)*, pages 31–40. ACM, 2018.

[17] Shromona Ghosh, Dorsa Sadigh, Pierluigi Nuzzo, Vasumathi Raman, Alexandre Donzé, Alberto L. Sangiovanni-Vincentelli, S. Shankar Sastry, and Sanjit A. Seshia. Diagnosis and repair for synthesis from signal temporal logic specifications. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, HSCC 2016, Vienna, Austria, April 12-14, 2016*, pages 31–40. ACM, 2016. `doi:10.1145/2883817.2883847`.

[18] Antoine Girard, A. Agung Julius, and George J. Pappas. Approximate simulation relations for hybrid systems. *Discrete Event Dynamic Systems*, 18(2):163–179, 2008. URL: `https://doi.org/10.1007/s10626-007-0029-9`, `doi:10.1007/s10626-007-0029-9`.

[19] Antoine Girard and George J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Trans. Automat. Contr.*, 52(5):782–798, 2007. URL: `https://doi.org/10.1109/TAC.2007.895849`, `doi:10.1109/TAC.2007.895849`.

[20] Mathew Hennessy and Robin Milner. Algebraic laws for nondeterminism and concurrency. *J. ACM*, 32(1):137–161, 1985. URL: `http://doi.acm.org/10.1145/2455.2460`, `doi:10.1145/2455.2460`.

[21] Narges Khakpour and Mohammad Reza Mousavi. Notions of conformance testing for cyber-physical systems: Overview and roadmap (invited paper). In *Proc. of the 26th International Conference on Concurrency Theory, CONCUR 2015*, volume 42 of *LIPIcs*, pages 18–40. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

[22] Ron Koymans. Specifying real-time properties with metric temporal logic. *Real-Time Systems*, 2(4):255–299, 1990. URL: `https://doi.org/10.1007/BF01995674`, `doi:10.1007/BF01995674`.

[23] Oded Maler and Dejan Nickovic. Monitoring temporal properties of continuous signals. In *Proceedings of the Joint International Conferences on Formal Modelling and Analysis of Timed Systems and Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant (FORMATS and FTRTFT) 2004*, volume 3253 of *Lecture Notes in Computer Science*, pages 152–166. Springer, 2004. URL: `https://doi.org/10.1007/978-3-540-30206-3_12`, `doi:10.1007/978-3-540-30206-3\_12`.

[24] Luan Viet Nguyen, James Kapinski, Xiaoqing Jin, Jyotirmoy V. Deshmukh, and Taylor T. Johnson. Hyperproperties of real-valued signals. In

Jean-Pierre Talpin, Patricia Derler, and Klaus Schneider, editors, *Proceedings of the 15th ACM-IEEE International Conference on Formal Methods and Models for System Design, MEMOCODE 2017, Vienna, Austria, September 29 - October 02, 2017*, pages 104–113. ACM, 2017. URL: https://doi.org/10.1145/3127041.3127058, doi:10.1145/3127041.3127058.

[25] Amir Pnueli. The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science (FOCS 1977)*, pages 46–57. IEEE Computer Society, 1977. URL: https://doi.org/10.1109/SFCS.1977.32, doi:10.1109/SFCS.1977.32.

[26] Pavithra Prabhakar, Vladimeros Vladimerou, Mahesh Viswanathan, and Geir E. Dullerud. Verifying tolerant systems using polynomial approximations. In Theodore P. Baker, editor, *Proceedings of the 30th IEEE Real-Time Systems Symposium, RTSS 2009, Washington, DC, USA, 1-4 December 2009*, pages 181–190. IEEE Computer Society, 2009. URL: https://doi.org/10.1109/RTSS.2009.28, doi:10.1109/RTSS.2009.28.

[27] Sriram Sankaranarayanan, Suhas Akshar Kumar, Faye Cameron, B. Wayne Bequette, Georgios E. Fainekos, and David M. Maahs. Model-based falsification of an artificial pancreas control system. *SIGBED Review*, 14(2):24–33, 2017. doi:10.1145/3076125.3076128.

[28] Jan Tretmans. Model based testing with labelled transition systems. In *Formal Methods and Testing, An Outcome of the FORTEST Network, Revised Selected Papers*, volume 4949 of *Lecture Notes in Computer Science*, pages 1–38. Springer, 2008.

[29] Cumhur Erkan Tuncali, Bardh Hoxha, Guohui Ding, Georgios E. Fainekos, and Sriram Sankaranarayanan. Experience report: Application of falsification methods on the UxAS system. In *Proceedings of the 10th International NASA Formal Methods Symposium (NFM 2018)*, volume 10811 of *Lecture Notes in Computer Science*, pages 452–459. Springer, 2018. doi:10.1007/978-3-319-77935-5_30.

[30] Rob J. van Glabbeek. The linear time-branching time spectrum (extended abstract). In Jos C. M. Baeten and Jan Willem Klop, editors, *CONCUR '90, Theories of Concurrency: Unification and Extension, Amsterdam, The Netherlands, August 27-30, 1990, Proceedings*, volume 458 of *Lecture Notes in Computer Science*, pages 278–297. Springer, 1990. URL: https://doi.org/10.1007/BFb0039066, doi:10.1007/BFb0039066.

[31] Mihalis Yannakakis and David Lee. Testing of finite state systems. In *Proceedings of Computer Science Logic (CSL 1999)*, volume 1584 of *Lecture Notes in Computer Science*, pages 29–44. Springer Berlin Heidelberg, 1999.

Appendix: Proof of Proposition 2

Proof. We proceed by structural induction on ϕ.

The ground cases F and T are straightforward. For the atomic propositions, note that in our setting, where we consider TSSs over metric spaces of booleans, the formulae $p^+(\epsilon)$ and $p^-(\epsilon)$ occurring in the relaxation are logically equivalent to p. The statement holds then immediately from the way μ_A and μ_B are defined.

We now proceed with the until and release operators. In order to avoid dealing with multiple interval types in the formulae of the form $\chi\,\mathcal{X}_I\,\psi$, where $\mathcal{X} \in \{\mathcal{U}, \mathcal{R}\}$, annotated with different types of intervals, we can simplify the proof using Observation 1. That is, for any $a, b \in \mathbb{R}$, we prove the statement only for the weakest formula of the type $\chi\,\mathcal{X}_I\,\psi$, where I ranges over $\mathcal{T}(a, b)$, namely $\chi\,\mathcal{X}_{[a,b]}\,\psi$. Since the other formulae annotated with intervals from $\mathcal{T}(a, b)$ logically entail $\chi\,\mathcal{X}_{[a,b]}\,\psi$, and their relaxations are the same, we will then have proven the statement for all four interval types.

To reduce the notational overhead, whenever we are supposed to prove that the relevant relaxed formula $[\chi\,\mathcal{X}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$ holds in a particular state, we shall do so by proving that a stronger and syntactically simpler formula holds, namely:

- in case of until, $[\chi]^{\text{AMF}}_{\tau,0}\,\mathcal{U}_{(a-2\tau,b+2\tau)}\,[\psi]^{\text{AMF}}_{\tau,0}$ (stronger than $[\chi\,\mathcal{U}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$)
- in case of release, $[\chi]^{\text{AMF}}_{\tau,0}\,\mathcal{R}_{(a+2\tau,b-2\tau)}\,[\psi]^{\text{AMF}}_{\tau,0}$ (stronger than $[\chi\,\mathcal{R}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$)

Take an arbitrary $t_A \in \mathcal{T}_A$ and $t_B \in \mathcal{T}_B$ such that

$$(*)\quad 0 \le t_B - t_A < 2\tau \quad\wedge\quad \text{CHUNK}_A(t_A) = \text{CHUNK}_B(t_B)$$

We will show the relevant preservation results in the case analysis below.

- We first consider the case where $\phi = \chi\,\mathcal{U}_{[a,b]}\,\psi$.

  I. Proof that $(\mu_A, t_A) \models \chi\,\mathcal{U}_{[a,b]}\,\psi \implies (\mu_B, t_B) \models [\chi\,\mathcal{U}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$.

  Suppose that $(\mu_A, t_A) \models \chi\,\mathcal{U}_{[a,b]}\,\psi$; we need to show that $(\mu_B, t_B) \models [\chi\,\mathcal{U}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$. As explained above, we shall prove this by showing that (μ_B, t_B) satisfies a stronger formula, namely $[\chi]^{\text{AMF}}_{\tau,0}\,\mathcal{U}_{(a-2\tau,b+2\tau)}\,[\psi]^{\text{AMF}}_{\tau,0}$. From the semantics of until operator, this amounts to showing that:

  1. there is some $t_B^\psi \in \mathcal{T}_B$ such that
     – $(\mu_B, t_B^\psi) \models [\psi]^{\text{AMF}}_{\tau,0}$
     – $t_B^\psi - t_B \in (a - 2\tau, b + 2\tau)$
  2. for all $t'_B : t_B \le t'_B < t_B^\psi$, we have $(\mu_B, t'_B) \models [\chi]^{\text{AMF}}_{\tau,0}$

  1. Since $(\mu_A, t_A) \models \chi\,\mathcal{U}_{[a,b]}\,\psi$, there must be some t_A^ψ such that $(\mu_A, t_A^\psi) \models \psi$ and $t_A^\psi - t_A \in [a, b]$. Moreover, since μ_B is stretched to the right of μ_A by at most 2τ, there must be some t_B^ψ such that $0 \le t_B^\psi - t_A^\psi < 2\tau$

and $\textsc{chunk}_A(t_A^\psi) = \textsc{chunk}_B(t_B^\psi)$. Let t_B^ψ be the *smallest* time point from $\mathcal{T}_B$ with this property.
From this, the fact that $(\mu_A, t_A^\psi) \models \psi$, and IH, we obtain $(\mu_B, t_B^\psi) \models [\psi]^{\text{AMF}}_{\tau,0}$. We now proceed to show that

$$a - 2\tau < t_B^\psi - t_B < b + 2\tau$$

We have the following inequalities:

$$(1) \;\; 0 \leq t_B - t_A < 2\tau$$

$$(2) \;\; a \leq t_A^\psi - t_A \leq b$$

$$(3) \;\; 0 \leq t_B^\psi - t_A^\psi < 2\tau$$

By multiplying all sides of (1) by -1 we obtain:

$$(4) \quad -2\tau < t_A - t_B \leq 0$$

Adding respective sides of (2) and (4) yields:

$$(5) \;\; a - 2\tau < t_A^\psi - t_B \leq b$$

By adding (3) to (5), we finally obtain:

$$a - 2\tau < t_B^\psi - t_B \leq b + 2\tau$$

2. Take any $t'_B : t_B \leq t'_B < t_B^\psi$ (if there is no such t'_B, the statement holds trivially). We need to show that

$$(\mu_B, t'_B) \models [\chi]^{\text{AMF}}_{\tau,0}$$

Note that, since $(\mu_A, t_A) \models \chi\,\mathcal{U}_{[a,b]}\,\psi$, we have:

$$(**) \;\; \forall t'_A : t_A \leq t'_A < t_A^\psi.\; (\mu_A, t'_A) \models \chi$$

We now need to show that there is some $t_A^0 : t_A \leq t_A^0 < t_A^\psi$ such that

$$(***) \;\; 0 \leq t'_B - t_A^0 < 2\tau \;\wedge\; \textsc{chunk}_A(t_A^0) = \textsc{chunk}_B(t'_B)$$

Since μ_B is stretched to the right of μ_A by at most 2τ, we know that there is at least one t_A^0 satisfying (***), what remains to be shown is that there is t_A^0 satisfying (***) such that $t_A \leq t_A^0 < t_A^\psi$
Suppose, towards contradiction, that it is not the case. There are two possible cases:

- there is some $t_A^0 < t_A$ that makes (***) true. Since $\textsc{chunk}$ functions are non-decreasing, we have $\textsc{chunk}_B(t'_B) \geq \textsc{chunk}_B(t_B) = \textsc{chunk}_A(t_A) \geq \textsc{chunk}_A(t_A^0)$, and since $\textsc{chunk}_B(t'_B) = \textsc{chunk}_A(t_A^0)$, we obtain $\textsc{chunk}_A(t_A) = \textsc{chunk}_A(t_A^0)$.
  We proceed to prove the following:

  $$0 \overset{(1)}{\leq} t'_B - t_A \overset{(2)}{<} 2\tau$$

  Proof of (1): From the initial assumptions about t_A and t_B, we have:

  $$0 \leq t_B - t_A$$

  On the other hand, since points in TSS are non-decreasing w.r.t. time, we have $t'_B \geq t_B$, which combined with the above inequality yields:

  $$0 \leq t'_B - t_A$$

  which proves (1).
  Proof of (2): From (***) we have:

  $$t'_B - t_A^0 < 2\tau$$

  On the other hand, since points in TSS are non-decreasing w.r.t. time, we have $t_A \geq t_A^0$, which combined with the above inequality yields:

  $$t'_B - t_A < 2\tau$$

  which proves (2).
  We have thus proved that if we substitute t_A for t_A^0 in (***), it makes (***) true, a contradiction.
- there is some $t_A^0 \geq t_A^\psi$ that makes (***) true.
  We shall prove that, contrary to the assumption about t_B^ψ, t'_B and t_A^ψ are 2τ-corresponding states.
  Since $\textsc{chunk}$ functions are non-decreasing, we have $\textsc{chunk}_A(t_A^0) \geq \textsc{chunk}_A(t_A^\psi) = \textsc{chunk}_B(t_B^\psi) \geq \textsc{chunk}_B(t'_B)$, and since $\textsc{chunk}_A(t_A^0) = \textsc{chunk}_B(t'_B)$, we obtain $\textsc{chunk}_A(t_A^\psi) = \textsc{chunk}_B(t'_B)$. What remains to be shown is:

  $$0 \overset{(1)}{\leq} t'_B - t_A^\psi) \overset{(2)}{<} 2\tau$$

  Proof of (1): From (***) we have:

  $$0 \leq t'_B - t_A^0$$

  Combined with our assumption that $t_A^0 \geq t_A^\psi$, this yields

  $$0 \leq t'_B - t_A^\psi$$

Proof of (2): From the definition of t_B^ψ, we have

$$t_B^\psi - t_A^\psi < 2\tau$$

In addition, since $t'_B < t_B^\psi$, we have $t'_B \leq t_B^\psi$. Hence

$$t'_B - t_A^\psi < 2\tau$$

We have thus shown that t'_B and t_A^ψ are 2τ-corresponding states, which contradicts our assumption about t_B^ψ being the smallest index that is 2τ-corresponding to t_A^ψ.

II. Proof that $(\mu_B, t_B) \models \chi\,\mathcal{U}_{[a,b]}\,\psi \implies (\mu_A, t_A) \models [\chi\,\mathcal{U}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$.

Note that this proof virtually mirrors the previous one in its structure; however, since this direction does not automatically follow from the previous one, we present it here for the sake of completeness.

Suppose that $(\mu_B, t_B) \models \chi\,\mathcal{U}_{[a,b]}\,\psi$; we will show that (μ_A, t_A) satisfies $[\chi]^{\text{AMF}}_{\tau,0}\,\mathcal{U}_{(a-2\tau,b+2\tau)}\,[\psi]^{\text{AMF}}_{\tau,0}$. From the semantics of until operator, this amounts to showing that:

1. there is some $t_A^\psi \in \mathcal{T}_A$ such that
   - $(\mu_A, t_A^\psi) \models [\psi]^{\text{AMF}}_{\tau,0}$
   - $t_A^\psi - t_A \in (a - 2\tau, b + 2\tau)$
2. for all $t'_A : t_A \leq t'_A < t_A^\psi$, we have $(\mu_A, t'_A) \models [\chi]^{\text{AMF}}_{\tau,0}$

1. Since $(\mu_B, t_B) \models \chi\,\mathcal{U}_{[a,b]}\,\psi$, there must be some t_B^ψ such that $(\mu_B, t_B^\psi) \models \psi$ and $t_B^\psi - t_B \in [a, b]$. Moreover, since μ_B is stretched to the right of μ_A by at most 2τ, there must be some t_A^ψ such that $0 \leq t_B^\psi - t_A^\psi < 2\tau$ and $\textsc{chunk}_A(t_A^\psi) = \textsc{chunk}_B(t_B^\psi)$. Let t_A^ψ be the smallest index from $\mathcal{T}_A$ with this property.
   From this, the fact that $(\mu_B, t_B^\psi) \models \psi$, and IH, we obtain $(\mu_A, t_A^\psi) \models [\psi]^{\text{AMF}}_{\tau,0}$. We now need to show that

   $$a - 2\tau < t_A^\psi - t_A < b + 2\tau$$

   We have the following inequalities:

   $$(1)\quad 0 \leq t_B - t_A < 2\tau$$

   $$(2)\quad a \leq t_B^\psi - t_B \leq b$$

   $$(3)\quad 0 \leq t_B^\psi - t_A^\psi < 2\tau$$

   By multiplying all sides of (3) by -1 we obtain:

   $$(4)\quad -2\tau < t_A^\psi - t_B^\psi \leq 0$$

   Adding respective sides of (1), (2) and (4) finally yields:

   $$a - 2\tau < t_A^\psi - t_A \leq b + 2\tau$$

2. Take any $t'_A : t_A \leq t'_A < t^{\psi}_A$ (if there is no such t'_A, the statement holds trivially). We need to show that

$$(\mu_A, t'_A) \models [\chi]^{\text{AMF}}_{\tau,0}$$

Note that, since $(\mu_B, t_B) \models \chi\, \mathcal{U}_{[a,b]}\, \psi$, we have:

$$(**) \quad \forall t'_B : t_B \leq t'_B < t^{\psi}_B.\ (\mu_B, t'_B) \models \chi$$

We now need to show that there is some $t^0_B : t_B \leq t^0_B < t^{\psi}_B$ such that

$$(***) \quad 0 \leq t^0_B - t'_A < 2\tau \ \wedge\ \text{CHUNK}_A(t'_A) = \text{CHUNK}_B(t^0_B)$$

Since μ_B is stretched to the right of μ_A by at most 2τ, we know that there is at least one t^0_B satisfying (***), what remains to be shown is that there is t^0_B satisfying (***) such that $t_B \leq t^0_B < t^{\psi}_B$

Suppose, towards contradiction, that it is not the case. There are two possible cases:

- there is some $t^0_B < t_B$ that makes (***) true. Since CHUNK functions are non-decreasing, we have $\text{CHUNK}_A(t'_A) \geq \text{CHUNK}_A(t_A) = \text{CHUNK}_B(t_B) \geq \text{CHUNK}_B(t^0_B)$, and since $\text{CHUNK}_A(t'_A) = \text{CHUNK}_B(t^0_B)$, we obtain $\text{CHUNK}_B(t_B) = \text{CHUNK}_A(t'_A)$.
  We proceed to prove the following:

  $$0 \overset{(1)}{\leq} t_B - t'_A \overset{(2)}{<} 2\tau$$

  Proof of (1): From the initial assumptions about t_B, we have:

  $$0 \leq t_B - t_A$$

  On the other hand, since points in TSS are non-decreasing w.r.t. time, we have $t'_A \geq t_A$, which combined with the above inequality yields:

  $$0 \leq t_B - t'_A$$

  which proves (1).
  Proof of (2): From (***) we have:

  $$t^0_B - t'_A < 2\tau$$

  Since points in TSS are non-decreasing w.r.t. time, we have $t_B \geq t^0_B$, which combined with the above inequality yields:

  $$t_B - t'_A < 2\tau$$

  which proves (2).
  We have thus proved that if we substitute t_B for t^0_B in (***), it makes (***) true, a contradiction.

– there is some $t_B^0 \geq t_B^\psi$ that makes (***) true.
We shall prove that, contrary to the assumption about t_A^ψ, t'_A and t_B^ψ are 2τ-corresponding states.
Since CHUNK functions are non-decreasing, we have $\text{CHUNK}_B(t_B^0) \leq \text{CHUNK}_B(t_B^\psi) = \text{CHUNK}_A(t_A^\psi) \leq \text{CHUNK}_A(t'_A)$, and since $\text{CHUNK}_B(t_B^0) = \text{CHUNK}_A(t'_A)$, we obtain $\text{CHUNK}_B(t_B^\psi) = \text{CHUNK}_A(t'_A)$. What remains to be shown is:

$$0 \overset{(1)}{\leq} t_B^\psi - t'_A \overset{(2)}{<} 2\tau$$

Proof of (1): Since t_A^ψ, t_B^ψ are 2τ-corresponding, we have

$$0 \leq t_B^\psi - t_A^\psi$$

Combined with $t'_A \geq t_A^\psi$, this yields

$$0 \leq t_B^\psi - t'_A$$

Proof of (2): From (***) we have

$$t_B^0 - t'_A < 2\tau$$

In addition, since $t_B^0 \geq t_B^\psi$, we have $t_B^0 \geq t_B^\psi$. Hence

$$t_B^\psi - t'_A < 2\tau$$

We have thus shown that t'_A and t_B^ψ are 2τ-corresponding states, which contradicts our assumption about t_A^ψ.

- We proceed to show that the statement holds for $\phi = \chi\,\mathcal{R}_{[a,b]}\,\psi$.

I. Proof that

$$(\mu_A, t_A) \models \chi\,\mathcal{R}_{[a,b]}\,\psi \implies (\mu_B, t_B) \models [\chi\,\mathcal{R}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$$

Suppose $(\mu_A, t_A) \models \chi\,\mathcal{R}_{[a,b]}\,\psi$. We will show that (μ_B, t_B) satisfies a stronger formula than $[\chi\,\mathcal{R}_{[a,b]}\,\psi]^{\text{AMF}}_{\tau,0}$, namely $[\chi]^{\text{AMF}}_{\tau,0}\,\mathcal{R}_{(a+2\tau,b-2\tau)}\,[\psi]^{\text{AMF}}_{\tau,0}$. This in turn can be done by showing that for any t'_B such that $t'_B - t_B \in (a+2\tau, b-2\tau)$ and $(\mu_B, t'_B) \not\models [\psi]^{\text{AMF}}_{\tau,0}$, there must be some t_B^χ such that $t_B \leq t_B^\chi < t'_B$ and $(\mu_B, t_B^\chi) \models [\chi]^{\text{AMF}}_{\tau,0}$.

Take any t'_B such that $t'_B - t_B \in (a+2\tau, b-2\tau)$, and $(\mu_B, t'_B) \not\models [\psi]^{\text{AMF}}_{\tau,0}$. Let t'_A be a time point 2τ-corresponding to t'_B. It must be the case that $(\mu_A, t'_A) \not\models \psi$, otherwise from IH we would obtain $(\mu_B, t'_B) \models [\psi]^{\text{AMF}}_{\tau,0}$, contrary to our assumption. We now need to show that

$$t'_A - t_A \in [a, b]$$

From the constraints on 2τ-corresponding states, we have $t'_B - t'_A \in [0, 2\tau)$ and $t_B - t_A \in [0, 2\tau)$. Thus, the following three inequalities hold:

$$(1) \;\; a + 2\tau < t'_B - t_B < b - 2\tau$$

$$(2) \;\; 0 \le t_B - t_A < 2\tau$$

$$(3) \;\; 0 \le t'_B - t'_A < 2\tau$$

Multiplying (3) by (-1) we obtain:

$$(4) \quad -2\tau < t'_A - t'_B \le 0$$

By adding all sides of $(1), (2)$ and (4), we now obtain:

$$a < t'_A - t_A < b$$

We have thus shown that:

$$t'_A - t_A \in (a, b) \subseteq [a, b]$$

From the above, the fact that $(\mu_A, t_A) \models \chi \,\mathcal{R}_{[a,b]}\, \psi$, and $(\mu_A, t'_A) \not\models \psi$, we can deduce that there is some t^χ_A such that $t_A \le t^\chi_A < t'_A$ and $\mu_A(t^\chi_A) \models \chi$. Let us pick t^χ_A such that in addition $\mu_A(t^\chi_A) \models \psi$ (existence of such state can be deduced from the semantics of the release operator).

Let t^χ_B be the latest 2τ-corresponding state to t^χ_A. From IH we have $(\mu_B, t^\chi_B) \models [\chi]^{\text{AMF}}_{\tau,0}$. We still need to show that $t_B \le t^\chi_B < t'_B$.

It is not difficult to see that for any $t^1_A, t^2_A \in \mathcal{T}_A$ such that $t^1_A \le t^2_A$, if t^2_B is the largest 2τ-corresponding time point to t^2_A, then for any t^1_B that is a 2τ-corresponding time point to t^1_A, we have $t^1_B \le t^2_B$, and moreover, if in addition we assume that $\textsc{chunk}_A(t^1_A) \ne \textsc{chunk}_A(t^2_A)$, then $t^1_B < t^2_B$. From this property, we immediately obtain $t_B \le t^\chi_B$. Since $\mu_A(t^\chi_A) \models \psi$ and $(\mu_B, t'_B) \not\models [\psi]^{\text{AMF}}_{\tau,0}$, from IH we obtain that $\textsc{chunk}_A(t^\chi_A) \ne \textsc{chunk}_B(t'_B)$, which combined with $\textsc{chunk}_B(t'_B) = \textsc{chunk}_A(t'_A)$ yields $\textsc{chunk}_A(t^\chi_A) \ne \textsc{chunk}_A(t'_A)$. Hence $t^\chi_B < t'_B$.

II. Proof that

$$(\mu_B, t_B) \models \chi \,\mathcal{R}_{[a,b]}\, \psi \implies (\mu_A, t_A) \models [\chi \,\mathcal{R}_{[a,b]}\, \psi]^{\text{AMF}}_{\tau,0}$$

Similarly as in the case of until formuale, the proof has nearly the same structure as the other direction.

Suppose $(\mu_B, t_B) \models \chi \,\mathcal{R}_{[a,b]}\, \psi$. We will show that (μ_A, t_A) satisfies the formula $[\chi]^{\text{AMF}}_{\tau,0} \,\mathcal{R}_{(a+2\tau, b-2\tau)}\, [\psi]^{\text{AMF}}_{\tau,0}$. This in turn can be done by showing that for any t'_A such that $t'_A - t_A \in (a + 2\tau, b - 2\tau)$ and $(\mu_A, t'_A) \not\models [\psi]^{\text{AMF}}_{\tau,0}$, there must be some t^χ_A such that $i \le t^\chi_A < t'_A$ and $(\mu_A, t^\chi_A) \models [\chi]^{\text{AMF}}_{\tau,0}$.

Take any t'_A such that $t'_A - t_A \in (a + 2\tau, b - 2\tau)$, and $(\mu_A, t'_A) \not\models [\psi]^{\text{AMF}}_{\tau,0}$. Let t'_B be a time point 2τ-corresponding to t'_A. It must be the case that

$(\mu_B, t'_B) \not\models \psi$, otherwise from IH we would obtain $(\mu_A, t'_A) \models [\psi]^{\text{AMF}}_{\tau,0}$, contrary to our assumption.

We now need to show that

$$t'_B - t_B \in [a, b]$$

From the constraints on 2τ-corresponding states, we have $t'_B - t'_A \in [0, 2\tau)$ and $t_B - t_A \in [0, 2\tau)$.

Let $t_A = t_A$, $t'_A = t'_A$, $t_B = t_B$, $t'_B = t'_B$. The following inequalities hold:

$$(1) \quad a + 2\tau < t'_A - t_A < b - 2\tau$$

$$(2) \quad 0 \leq t_B - t_A < 2\tau$$

$$(3) \quad 0 \leq t'_B - t'_A < 2\tau$$

Multiplying (2) by (-1) we obtain:

$$(4) \quad -2\tau < t_A - t_B \leq 0$$

By adding all sides of $(1), (3)$ and (4), we now obtain:

$$a < t'_B - t_B < b$$

We have thus shown that:

$$t'_B - t_B \in (a, b) \subseteq [a, b]$$

From the above, the fact that $(\mu_B, t_B) \models \chi\, \mathcal{R}_{[a,b]}\, \psi$, and $(\mu_B, t'_B) \not\models \psi$, we can deduce that there is some t^χ_B such that $t_B \leq t^\chi_B < t'_B$ and $\mu_B(t^\chi_B) \models \chi$. Let us pick t^χ_B such that in addition $\mu_A(t^\chi_B) \models \psi$ (existence of such state can be deduced from the semantics of the release operator).

Let t^χ_A be the latest 2τ-corresponding state to t^χ_B. From IH we have $(\mu_A, t^\chi_A) \models [\chi]^{\text{AMF}}_{\tau,0}$. We still need to show that $t_A \leq t^\chi_A < t'_A$.

It is not difficult to see that for any $t^1_B, t^2_B \in \mathcal{T}_B$ such that $t^1_B \leq t^2_B$, if t^2_A is the largest 2τ-corresponding state to t^2_A, then for any t^1_A that is a 2τ-corresponding state to t^1_B, we have $t^1_A \leq t^2_A$, and moreover, if in addition we assume that $\text{CHUNK}_B(t^1_B) \neq \text{CHUNK}_B(t^2_B)$, then $t^1_A < t^2_A$. From this property, we immediately obtain $t_A \leq t^\chi_A$. Since $\mu_B(t^\chi_B) \models \psi$ and $(\mu_A, t'_A) \not\models [\psi]^{\text{AMF}}_{\tau,0}$, from IH we obtain that $\text{CHUNK}_B(t^\chi_B) \neq \text{CHUNK}_A(t'_A)$, which combined with $\text{CHUNK}_A(t'_A) = \text{CHUNK}_B(t'_B)$ yields $\text{CHUNK}_B(t^\chi_B) \neq \text{CHUNK}_B(t'_B)$. Hence $t^\chi_A < t'_A$.

$\square$