Logical Characterisation of Hybrid Conformance

Maciej Gazda
Department of Computer Science, University of Sheffield, UK
m.gazda@sheffield.ac.uk

Mohammad Reza Mousavi
School of Informatics, University of Leicester, UK
mm789@le.ac.uk

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 bisimulations 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 approximate notions of hybrid refinement and 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. We also show that an existing relaxation scheme on Metric Temporal Logic used for preservation results in this setting is not tight enough for providing a characterisation of neither hybrid conformance nor refinement. 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.

2012 ACM Subject Classification Theory of computation → Logic and verification; Software and its engineering → Formal software verification

Keywords and phrases Logical Characterisation, Metric Temporal Logic, Conformance, Behavioural Equivalence, Hybrid Systems, Relaxation

Digital Object Identifier 10.4230/LIPIcs.ICALP.2020.130

Category Track B: Automata, Logic, Semantics, and Theory of Programming

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 [21, 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 at different layers of abstraction. Moreover, logical characterisations are stepping stones towards devising the notion of characterising formulae, which have been used in tools and algorithms 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, 16] (see [22] for an overview). However, not much is known about logical characterisation of such notions; to our knowledge, the closest known results to a logical characterisation of hybrid conformance are the logical preservation results [16, 1] and the characterisation of metric bisimulation [12] and stochastic bisimulation for systems with rewards [17] (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 [23, 5].

To this end, we study the hybrid conformance notion due to Abbas, Mittelmann and Fainekos [2, 1], as well as its its associated preorder which we call hybrid refinement (for both notions, we also study their extensions to non-deterministic hybrid-systems). We provide logical characterisations for each of theses notions in terms of Metric Temporal Logic (MTL) and suitable notions of relaxation. We also show that the notions of relaxation proposed in the preservation result by Abbas, Mittelmann and Fainekos [1] is insufficiently precise to lead to a logical characterisation. 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 that have not been given a logical characterisation so far, to the best of our knowledge. 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 preservations 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 notions of hybrid refinement and conformance [1] and Metric Temporal Logic [6]. Subsequently in Section 4, we define appropriate notions of relaxations to characterise these notions using Metric Temporal Logic. We compare our results to the past preservation results in Section 5, where we show that the existing relaxation scheme for Metric Temporal Logic are too lax to serve for a logical characterisation of hybrid refinement and conformance. Namely, we prove there is a class of non-conforming implementations that do satisfy all relaxed MTL formulae satisfied by the specification. In Section 6, we conclude the paper, and present the directions of our ongoing research in this domain.

2 Related work

Logical characterisations of 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 [21, 30]. In this context, characterisations use direct comparison i.e. inclusion 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 use standard inclusion check between sets of satisfied formulae.

To our knowledge, the first notion of characterisation for approximate behavioural semantics has been offered in the context of Metric Transition Systems [12] for linear and branching distances based on Metric Bisimulation [20, 19].

On a general level, our semantic model and conformance relation are different from those in [12, 20] 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 [23, 5] (and its concrete instantiation with signal values for propositions: Signal Temporal Logic [24]) is motivated by its wide-spread use in the hybrid systems literature and in practice [1, 18, 15].

Prabhakar, Vladimerou, Viswanathan, and Dullerud [26] provide a characterisation theorem for approximate simulation [19]; 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]).

Desharnais, Gupta, Jagadeesan and Panangaden [14] provide an approximate characterisation of probabilistic bisimulation for labelled Markov processes. They do so using a quantitative extension of Hennessy-Milner logic. This work has led to several follow-up applications, e.g., to a logical characterisation of differential privacy by Castiglioni, Chatzikokolakis, and Palamidessi [9]. Gburek and Baier [17] have recently investigated characterisation of bisimulation for stochastic systems with actions and rewards with two probabilistic logics: a very expressive APCTL^*, and simpler $\mathrm{APCTL}_\circ$, that can provide succinct distinguishing formulae. Unlike their approach [17], 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 [16]. 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 timed state sequences (TSSs) and continuous trajectories, e.g., allowing for a comparison of behaviours of different types (such as sampled discretised behaviour against continuous trajectories).

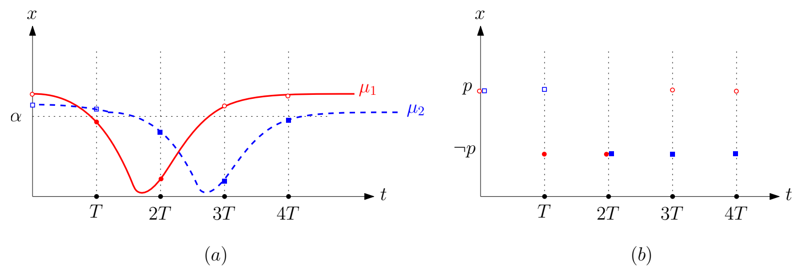


Figure 1 Examples of (a) continuous and (b) discretised GTTs

3 Preliminaries

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

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 [16]. 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 $\mathbb{R}_{\geq 0}$; 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 least element of the time domain could be also dispensed with.

▶ **Example 2.** Consider trajectories μ_1 and μ_2 depicted in Figure 1.(a), where μ_1 represents the specification of a system and μ_2 its implementation. The mappings from the subset of reals in the domain of each trajectory to the value of x at the corresponding point form real-valued GTTs.

Consider the discretisation of these two trajectories where we sample the trajectories with a period T and we record whether the value of x at the sampling point is higher than α (denoted by $p \doteq x > \alpha$) or at most α (denoted by $\neg p \doteq x \leq \alpha$). The corresponding mappings from $\{0, T, 2T, 3T, 4T\}$ to $P = \{p, \neg p\}$ are discretised GTTs depicted in Figure 1.(b) are P-valued GTTs.

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 3.** *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 two classes of hybrid systems: the class of* finitely branching hybrid systems *is defined as $\mathcal{H}_{FIN}(\mathcal{C}, \mathcal{I}, \mathcal{Y}) := \{H : \mathcal{C} \times$*

$\mathcal{I} \to \mathcal{P}_{FIN}(GTT(\mathcal{Y}))\}$; *similarly, the class of* deterministic hybrid systems *is defined as* $\mathcal{H}_{DET}(\mathcal{C},\mathcal{I},\mathcal{Y}) := \{H : \mathcal{C} \times \mathcal{I} \to \mathcal{P}(GTT(\mathcal{Y})) \,|\, \forall_{c\in\mathcal{C},i\in\mathcal{I}} |H(c,i)| = 1\}$.

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 $\mathcal{H}$.

3.1 Metric Temporal Logic

Metric Temporal Logic (MTL) [23, 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 once the propositions of the logic are interpreted over real-valued signals [24] (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 [24, 1, 18, 15].

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.

$$\phi ::= \quad \mathsf{T} \mid \mathsf{F} \mid p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi\, \mathcal{U}_I\, \phi \mid \phi\, \mathcal{R}_I\, \phi \mid p^+(\epsilon) \mid p^-(\epsilon) \qquad (\epsilon \in \mathbb{R}_{\geq 0})$$

▶ **Example 4.** To illustrate the intuitive meaning of $p^+(\epsilon)$ and $p^-(\epsilon)$ consider the predicate $p := x > \alpha$ in Example 2. $p^+(\epsilon)$ relaxes p into $x > \alpha - \epsilon$; in other words $p^+(\epsilon)$ allows for an error margin of ϵ when checking p, while $p^-(\epsilon)$ shrinks p into $x > \alpha + \epsilon$. The latter is helpful for defining the relaxation of negated propositions.

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

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

Note that our definitions slightly differ from [1]. In particular, for any $y_0 \in \mathcal{Y}$, and the set $\overline{B_\epsilon}(y_0) = \{y \in \mathcal{Y} \,|, d_{\mathcal{Y}}(y,y_0) > \epsilon\}$ (complement of an ϵ-ball of point y_0), we have $E(\overline{B_\epsilon}(y_0), \epsilon) = \{y_0\}$ (rather than $\emptyset$ which the expansion of [1] would yield).

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 [24]. 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 [16]).

▶ **Definition 5.** *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} formulas 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* $\mu(t) \notin C(\mathcal{O}(p), \epsilon)$

$(\mu, t) \models \phi \wedge \psi$ *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* $\exists t' \in \mathcal{T}.\ t' - t \in I.\, (\mu, t') \models \psi$
$\wedge \forall t'' \in \mathcal{T}.\, t'' \in [t, t') \implies ((\mu, t'') \models \phi \vee (t'' - t \in I \wedge (\mu, t'') \models \psi))$

$(\mu, t) \models \psi\, \mathcal{R}_I\, \phi$ *iff* $\forall t' \in \mathcal{T}.\, (t' - t \in I\ \wedge\ (\mu, t') \not\models \phi) \implies (\exists t_1 \in \mathcal{T}.\, t_1 \in [t, t')\ \wedge\ (\mu, t_1) \models \psi)$

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

In the remainder of this paper, we use the common shorthand notation for eventually and always, defined as: $\Diamond_I \phi := \mathsf{T}\, \mathcal{U}_I\, \phi \quad \Box_I \phi := \mathsf{F}\, \mathcal{R}_I\, \phi$.

We remark that the semantics of the until operator slightly differs from the standard one used e.g. for MTL over discrete-time models. There, one simply requires the safety formula ϕ to hold in every time point before the "ultimate" formula ψ holds. In order to cater for dense-time domains where there may be no "earliest" time point satisfying ψ, we require that in all the preceding time points either ϕ, *or* ψ holds. A similar kind of semantics can be found in [16].

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.

Furthermore, 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 or 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. Throughout the rest of the paper, we work with propositions that are guarded with until or release and hence, in our context, the ambiguity is never an issue in the context of our theory.

3.2 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. In addition to the "standard" hybrid conformance, which is a symmetric relation on traces, we also define its one-directional variant which we call hybrid refinement.

▶ **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. A trace μ_1 is a (τ, ϵ)-refinement of μ_2, notation $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$, iff:*

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

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 the (τ, ϵ)-window).

By requiring two traces to be mutually conforming, we obtain the standard notion of hybrid conformance [2, 1] for individual traces:

▶ **Definition 7.** *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)-refinement, and (τ, ϵ)-closeness, as respectively, hybrid refinement, and hybrid conformance. The two notions can be lifted to hybrid systems in the following manner:

▶ **Definition 8.**
1. *A system H_1 is a (τ, ϵ)-refinement of H_2, notation $H_1 \sqsubseteq_{\tau,\epsilon} H_2$, if for all $c \in \mathcal{C}$ and $i \in \mathcal{I}$, it holds that:*
$$\forall \mu_1 \in H_1(c, i).\ \exists \mu_2 \in H_2(c, i).\ \mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$$
2. *Two hybrid systems H_1, H_2 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*
$$\forall \mu_1 \in H_1(c, i).\ \exists \mu_2 \in H_2(c, i).\ \mu_1 \sim_{\tau,\epsilon} \mu_2$$
$$\forall \mu_2 \in H_2(c, i).\ \exists \mu_1 \in H_1(c, i).\ \mu_1 \sim_{\tau,\epsilon} \mu_2$$

4 Logical Characterisation of Hybrid Refinement and Hybrid Conformance

4.1 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 or refinement, 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, 16, 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.

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

▶ **Definition 9.** *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 [21, 30], where a logical formula represents a (potentially) observable behaviour of a system. This approach is more suitable for the purpose of logical chracterisation.

Assume a logic (a collection of formulae) $\mathcal{L}$ and a notion of relaxation $\mathsf{rlx} : \mathcal{L} \to \mathcal{L}$. 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 relation $R \subseteq \mathcal{H} \times \mathcal{H}$ if and only if, for any two systems H and H' we have:*

$$H\, R\, H' \iff \forall \phi \in \mathcal{L}.\ H \models_{\exists} \phi \implies H' \models_{\exists} \mathsf{rlx}(\phi)$$

The implication from left to right is called preservation; in our context, there already exist some preservation results in the literature [1, 16]; the implication from right to left (called reflection) has not been studied for hybrid conformance and MTL to the best of our knowledge.

We remark that for certain classes of "well-behaved" relations, the implication under the existential interpretation in definition 10, namely $H \models_{\exists} \phi \implies H' \models_{\exists} \mathsf{rlx}(\phi)$, is equivalent to a dual one under the more common universal interpretation, i.e. $H' \models \phi \implies H \models \mathsf{rlx}(\phi)$. Regarding the two relations considered in our work, only hybrid conformance has this property on all systems, while hybrid refinement does not. This is because the underlying relation on individual traces is not symmetric, and moreover allows the presence of considerably different values on the side of the "larger" trace (as long as it also matches all the required values on other timepoints within the relevant time interval).

In this section, we define two novel (and in our view, very natural) relaxation operators on MTL which, as we subsequently show, precisely serve this purpose.

4.2 Characterisation of hybrid refinement

Relaxation operator $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$. We shall now introduce the first relaxation operator on MTL, which (as we subsequently prove) gives rise to the characterisation of hybrid refinement. Syntactically, it has a very simple structure: the actual relaxation is performed on the level of propositions only.

▶ **Definition 11.** *Let $\tau, \epsilon \geq 0$. The relaxation operator $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon} : MTL^{+} \to MTL^{+}_{ext}$ is defined as follows:*

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

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.

4.2.1 Characterisation of traces.

We proceed to show that the introduced relaxation operator can be used to characterise the (τ, ϵ)-refinement, 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.

4.2.1.1 Preservation modulo relaxation

We start by proving that the satisfaction of MTL^{+} formulae is preserved by the refinement relation $\sqsubseteq_{\tau,\epsilon}$ on timed traces modulo $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$ relaxation.

▶ **Proposition 12.** *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 $t \in \mathbb{R}$:*

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

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

◀

4.2.1.2 Existence of distinguishing formula

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

▶ **Proposition 13.** *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 $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$, that is $\mu_1 \models \phi \wedge \mu_2 \not\models \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi)$*

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 $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi) = \Diamond_{[t_1,t_1]} \Diamond_{[-\tau,\tau]} p^+(\epsilon)$ cannot be satisfied by μ_2. ◀

4.2.2 Characterisation of hybrid systems.

4.2.2.1 Finitely branching systems

Propositions 12 and 13 provide the characterisation of relation $\sqsubseteq_{\tau,\epsilon}$ by MTL^+ through the relaxation $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$ on individual traces. Based on those results, for hybrid systems that are finitely branching (i.e. have bounded non-determinism, see definition 3), the characterisation result for hybrid refinement can be obtained in a straightforward manner.

▶ **Theorem 14.** *The logic MTL^+, together with the relaxation operator $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$, characterise the conformance relation $\sqsubseteq_{\tau,\epsilon}$ on finitely branching hybrid systems. That is, for arbitrary finitely branching hybrid systems H and H', the following statements hold:*

$$H \sqsubseteq_{\tau,\epsilon} H' \iff (\forall \phi \in \mathsf{MTL}^+.\ H \models_\exists \phi \implies H' \models_\exists \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi)$$

Proof.

- (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 $H_2(c,i) \models_\exists \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi)$. From $H_1(c,i) \models_\exists \phi$ we know that there is a $\mu_1 \in H_1(c,i)$ such that $\mu_1 \models \phi$. Moreover, since $H_1 \sqsubseteq_{\tau,\epsilon} H_2$, there is some $\mu_2 \in H_2(c,i)$ such that $\mu_1 \sqsubseteq_{\tau,\epsilon} \mu_2$. From Proposition 12 we thus obtain $\mu_2 \models \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi)$, and hence $H_2(c,i) \models_\exists \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi)$.
- (reflection/distinguishing formula): Suppose that $H_1 \not\sqsubseteq_{\tau,\epsilon} H_2$. Then 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 13 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 $\mu_2^j \not\models \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi_j)$. 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, $\mu_2^j \not\models \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\Phi)$, we also have $H_2(c,i) \not\models_\exists \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\Phi)$. Hence Φ distinguishes $H_1(c,i)$ from $H_2(c,i)$.

◀

4.2.2.2 Systems with unbounded non-determinism

In order to provide characterisation for hybrid refinement on systems with infinite branching, one needs to endow the logic MTL^+ with infinite conjunctions and disjunction; 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 15.** *The logic MTL^+_∞, together with the relaxation operator $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$, characterise the conformance relation $\sqsubseteq_{\tau,\epsilon}$ on arbitrary hybrid systems.*

Proof. The proof is nearly the same as the one of Theorem 14, 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 MTL^+_∞ formula, hence the construction is valid. ◀

4.3 Characterisation of hybrid conformance

4.3.1 Relaxation operator $\mathsf{rlx}^{\sim}_{\tau,\epsilon}$

While the relaxation operator $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$ introduced in the previous section allows one to preserve – up to the relevant (τ,ϵ)-window – properties of (signal values at) individual timepoints, it falls short of preserving properties of entire intervals. Therefore, in order to characterise the standard, symmetric notion of (τ,ϵ)-closeness, or hybrid conformance, one needs a finer notion of relaxation.

In what follows, we shall use the following notation: for an interval I, by $I_{<a,b>}$ we denote the modified interval: $I_{<a,b>} := \{x \in \mathbb{R} \mid \exists x_a, x_b \in I : x_a + a \leq x \wedge x \leq x_b + b\}$.

Below, we define a relaxation operator $\mathsf{rlx}^{\sim}_{\tau,\epsilon}$ where:

- for propositions not in the scope of a temporal operator, the relaxation is done similarly as in the $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$ operator
- for temporal operators, the interval endpoints are modified (i.e. “shrinked” to relax the temporal obligations accordingly)
- for propositions guarded by a temporal operator, only ϵ-relaxation of a signal value is perfomed (the relaxation of timeline has already been handled through interval relaxation)

▶ **Definition 16.** *Let $\tau, \epsilon \geq 0$. The relaxation operator $\mathit{rlx}^{\sim}_{\tau,\epsilon} : \mathit{MTL}^+ \to \mathit{MTL}^+_{ext}$ is defined as follows:*

$$
\begin{array}{lcl}
\mathit{rlx}^{\sim}_{\tau,\epsilon}(\mathsf{T}) = \mathsf{T} & , & \mathit{rlx}^{\sim}_{\tau,\epsilon}(\mathsf{F}) = \mathsf{F} \\
\mathit{rlx}^{\sim}_{\tau,\epsilon}(p) = \Diamond_{[-\tau,\tau]} p^+(\epsilon) & , & \mathit{rlx}^{\sim}_{\tau,\epsilon}(\neg p) = \Diamond_{[-\tau,\tau]} p^-(\epsilon) \\
\mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi_1 \wedge \phi_2) & = & \mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi_1) \wedge \mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi_2) \\
\mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi_1 \vee \phi_2) & = & \mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi_1) \vee \mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi_2) \\
\mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi\, \mathcal{U}_I\, \psi) & = & \begin{cases} \Diamond_{[\tau,\tau]} \left(\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi)\, \mathcal{U}_{I_{<0,-2\tau>}}\, (\Diamond_{[0,2\tau]} \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi))\right) & \mathit{if}\ \ I_{<0,-2\tau>} \neq \emptyset \\ \Diamond_{I_{<-\tau,\tau>}} \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi) & \mathit{if}\ \ I_{<0,-2\tau>} = \emptyset \end{cases} \\
\mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi\, \mathcal{R}_I\, \psi) & = & (\Diamond_{[-\tau,\tau]} \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi))\, \mathcal{R}_{I_{<\tau,-\tau>}}\, \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi)
\end{array}
$$

where the auxilliary relaxation $\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}$ for subformulae guarded by a temporal operator is defined as follows:

$$
\begin{array}{lcl}
\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\mathsf{T}) = \mathsf{T} & , & \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\mathsf{F}) = \mathsf{F} \\
\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(p) = p^+(\epsilon) & , & \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\neg p) = p^-(\epsilon) \\
\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi_1 \wedge \phi_2) & = & \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi_1) \wedge \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi_2) \\
\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi_1 \vee \phi_2) & = & \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi_1) \vee \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi_2) \\
\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi\, \mathcal{U}_I\, \psi) & = & \begin{cases} \Diamond_{[\tau,\tau]} \left(\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi)\, \mathcal{U}_{I_{<0,-2\tau>}}\, (\Diamond_{[0,2\tau]} \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi))\right) & \mathit{if}\ I_{<0,-2\tau>} \neq \emptyset \\ \Diamond_{I_{<-\tau,\tau>}} \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi) & \mathit{if}\ I_{<0,-2\tau>} = \emptyset \end{cases} \\
\mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi\, \mathcal{R}_I\, \psi) & = & (\Diamond_{[-\tau,\tau]} \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi))\, \mathcal{R}_{I_{<\tau,-\tau>}}\, \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi)
\end{array}
$$

4.3.2 Characterisation of traces

4.3.2.1 Preservation

Before stating the main preservation property, we prove the key lemma which lists certain properties of the auxilliary relaxation operator $\mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}$.

▶ **Lemma 17.** *Suppose $\mu_1 \sim_{\tau,\epsilon} \mu_2$. For any $\phi \in \mathit{MTL}^+$ we have:*

1. $\mu_1, t \models \phi \implies \exists t' \in [t-\tau, t+\tau].\ \mu_2, t' \models \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi)$
2. $(\forall t \in I.\, \mu_1, t \models \phi) \implies (\forall t \in I_{<\tau,-\tau>}.\ \mu_2, t \models \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi))$
3. *if in addition ϕ is of the form $\chi\, \mathcal{U}_I\, \psi$ or $\psi\, \mathcal{R}_I\, \chi$, then $\mu_1, t \models \phi \implies \mu_2, t \models \mathit{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\phi)$*

Proof. We proceed by structural induction on ϕ; for technical reasons, it is convenient to prove all the properties simultaneously. We focus on three key cases: atomic propositions, as well as the until and release operators.

- $\phi = p$:
  1. Suppose $\mu_1, t \models p$; from the semantics of MTL^+ this means that $\mu_1(t) \in \mathcal{O}(p)$. Since $\mu_1 \sim_{\tau,\epsilon} \mu_2$, there is some $t' \in [t-\tau, t+\tau]$ such that $d_{\mathcal{Y}}(\mu_1(t), \mu_2(t)') \leq \epsilon$. From this and $\mu_1(t) \in \mathcal{O}(p)$ we obtain $\mu_2(t') \in E(\mathcal{O}(p), \epsilon)$, and hence $\mu_2, t' \models p^+(\epsilon) = \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(p)$.

2. Suppose that for all $t \in I$ we have $\mu_1, t \models p$, that is, for all $t \in I$ $\mu_1(t) \in \mathcal{O}(p)$. Take any $t_2 \in I_{<\tau,-\tau>}$. Observe that the "matching" timepoint for μ_2 and t_2 in μ_1 must be in the interval I, i.e. there is some $t_1 \in I$ such that $d_{\mathcal{Y}}(\mu_1(t_1), \mu_2(t_2)) \leq \epsilon$. Since $t_1 \in I$, we have $\mu_1(t_1) \in \mathcal{O}(p)$, and hence $\mu_2(t_2) \in E(\mathcal{O}(p, \epsilon))$, from which $\mu_2, t_2 \models p^+(\epsilon) = \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(p)$ follows.

- $\phi = \chi \mathcal{U}_I \psi$: we only need to prove the third statement, as it is stronger than the first two. Moreover, we consider only the more involved case when $I_{<0,-2\tau>} \neq \emptyset$.
  Suppose $\mu_1, t \models \chi \mathcal{U}_I \psi$. Then there is some $t_\psi \in t + I$ such that $\mu_1, t_\psi \models \psi$ (note that since $I_{<0,-2\tau>} \neq \emptyset$, we have $t_\psi - t \geq 2\tau$). From $\mu_1 \sim_{\tau,\epsilon} \mu_2$ and applying the inductive hypothesis on statement 1 of Lemma 17 there is some $t'_\psi \in [t_\psi - \tau, t_\psi + \tau]$ such that $\mu_2, t'_\psi \models \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi)$. This in particular implies that
  (*) $\mu_2, t_\psi - \tau \models \Diamond_{[0,2\tau]} \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi)$.
  From $\mu_1, t \models \chi \mathcal{U}_I \psi$ it further follows that for all $t' \in [t, t_\psi)$ we have $\mu_1, t' \models \chi$. From applying the inductive hypothesis on statement 2 of Lemma 17 we therefore have
  (**) for all $t' \in [t + \tau, t_\psi - \tau)$ we have $\mu_2, t' \models \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi)$.
  That $\mu_2, t \models \Diamond_{[\tau,\tau]} \big(\mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi) \mathcal{U}_{I_{<0,-2\tau>}} (\Diamond_{[0,2\tau]} \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi))\big) = \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi \mathcal{U}_I \psi)$ now follows immediately from (*) and (**).
- $\phi = \psi \mathcal{R}_I \chi$: similarly as above, we only prove the third statement. Note that whenever the interval I is strictly shorter than 2τ, we have $I_{<0,-2\tau>} = \emptyset$, and the relaxation yields a formula equivalent to T.
  Take any $t'_{\neg\chi} \in t + I_{<\tau,-\tau>}$ such that $\mu_2, t'_{\neg\chi} \not\models \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi)$. Consider the interval $I \cap [t, t'_{\neg\chi} + \tau]$. There must be some $t_{\neg\chi} \in [t'_{\neg\chi} - \tau, t'_{\neg\chi} + \tau] \subseteq t + I$ such that $\mu_1, t_{\neg\chi} \not\models \chi$. Indeed, were it not the case, then from the inductive hypothesis (statement 2), we would have that for all $t' \in [t'_{\neg\chi}, t'_{\neg\chi}]$, $t' \models \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi)$, contradicting $\mu_2, t'_{\neg\chi} \not\models \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi)$.
  From $\mu_1, t \models \psi \mathcal{R}_I \chi$ and $\mu_1, t_{\neg\chi} \not\models \chi$, one obtains existence of some $t_\psi \in [t, t_{\neg\chi})$ such that $\mu_1, t_\psi \models \psi$. From the inductive hypothesis (1) we know that $\mu_2, t_\psi \models \Diamond_{[-\tau,\tau]} \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi)$.
  We have thus shown that $\mu_2, t \models (\Diamond_{[-\tau,\tau]} \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi)) \mathcal{R}_{I_{<\tau,-\tau>}} \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\chi) = \mathsf{t\text{-}rlx}^{\sim}_{\tau,\epsilon}(\psi \mathcal{R}_I \chi)$
  ◀

The preservation property is given in the proposition below.

▶ **Proposition 18.** $\mu_1 \sim_{\tau,\epsilon} \mu_2 \implies \forall \phi, t.\ \mu_1, t \models \phi \implies \mu_2, t \models \mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi)$

Proof. Formally, the proof proceeds by structural induction. However, the key cases of temporal operators are now immediate corollaries of Lemma 17 (point 3); while for the remaining cases including base the proof is very straightforward. ◀

4.3.2.2 Reflection

We proceed to show that for non-conforming traces, one can always find a distinguishing formula, regardless of the "direction" in which the conformance fails. Since $\sim_{\tau,\epsilon}$ is symmetric, this is equivalent to the statement that if $\mu_1 \not\sim_{\tau,\epsilon} \mu_2$, then one can find both a formula distinguishing μ_1 from μ_2, and also one that distinguishes μ_2 from μ_1.

▶ **Proposition 19.** $\mu_1 \not\sim_{\tau,\epsilon} \mu_2 \implies \exists \phi.\ \mu_1 \models \phi \wedge \mu_2 \not\models \mathit{rlx}^{\sim}_{\tau,\epsilon}(\phi)$

Proof. Suppose $\mu_1 \not\sim_{\tau,\epsilon} \mu_2$; we show that there is always a formula that distinguishes μ_1 from μ_2. We distinguish two cases:

- there is some $t_1 \in \mathcal{T}_1$ such that the value $\mu_1(t_1)$ cannot be matched within the (τ, ϵ)-window by μ_2, that is:

  $$(*)\quad \forall t' \in \mathcal{T}_2.\ |t' - t_1| \leq \tau \implies d_{\mathcal{Y}}(\mu_2(t'), \mu_1(t_1)) > \epsilon$$

We use a similar construction as for the relaxation $\mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}$, by defining

$$\Phi_{DIST} := \Diamond_{[t_1,t_1]} p$$

where $\mathcal{O}(p) = \{\mu_1(t_1)\}$. Then $\mathsf{rlx}^{\sim}_{\tau,\epsilon}(\Phi_{DIST}) = \Diamond_{[t_1-\tau,t_1+\tau]}\, p^+(\epsilon)$. We have $\mu_1 \models \Phi_{DIST}$, but from (*) we clearly have $\mu_2 \not\models \mathsf{rlx}^{\sim}_{\tau,\epsilon}(\Phi_{DIST})$.

- there is some $t_2 \in \mathcal{T}_2$ that cannot be matched by μ_1, that is: that is:

$$\forall t' \in \mathcal{T}_1.\ |t' - t_2| \leq \tau \implies d_{\mathcal{Y}}(\mu_1(t'), \mu_2(t_2)) > \epsilon$$

we define

$$\Phi_{DIST} := \Box_{[t_2-\tau,t_2+\tau]} p$$

where $\mathcal{O}(p) = \{y \in \mathcal{Y} \mid d_{\mathcal{Y}}(y, \mu_2(t_2)) > \epsilon\}$. Note that $p^+(\epsilon) = \mathcal{Y} \setminus \{\mu_2(t_2)\}$ (at this point using our definition of expansion operator rather than the one from [1] proves essential). We have $\mu_1 \models \Phi_{DIST}$, but on the other hand: $\mathsf{rlx}^{\sim}_{\tau,\epsilon}(\Phi_{DIST}) = (\Diamond_{[-\tau,\tau]}\mathsf{F})\, \mathcal{R}_{[t_2,t_2]}\, p^+(\epsilon) \equiv \Box_{[t_2,t_2]} p^+(\epsilon)$, and since $\mu_2(t_2) \notin \mathcal{Y} \setminus \{\mu_2(t_2)\} = p^+(\epsilon)$, we have $\mu_2 \not\models \mathsf{rlx}^{\sim}_{\tau,\epsilon}(\Phi_{DIST})$

◀

4.3.3 Characterisation of hybrid systems

Characterisation results for hybrid conformance and their proofs share many similarities with those for hybrid refinement. One fine point worth noting is the proof of reflection property: when, similarly as in the proof of Theorem 14, we arrive at the case when $\mu_1 \not\sim_{\tau,\epsilon} \mu_2^j$, we know from Proposition 19 that for all j there is a formula that distinguishes μ_1 *from* μ_2^j, regardless of the direction in which the (τ, ϵ)-matching fails . We therefore have a family of formulae distinguishing μ_1 from μ_2^j for each j, and hence can construct a distinguishing formula by taking their conjunction.

In addition, since hybrid conformance is based on a symmetric relation on individual traces, the characterisation result holds for the standard (universal) interpretation of satisfaction relation as well.

▶ **Theorem 20.** *The logic MTL^+ [resp. MTL^+_∞], together with the relaxation operator $\mathsf{rlx}^{\sim}_{\tau,\epsilon}$, characterise the conformance relation $\sqsubseteq_{\tau,\epsilon}$ on finitely branching [resp. arbitrary] hybrid systems. That is, for finitely branching [resp. arbitrary] hybrid systems H and H', the following statements hold:*

$$H \sim_{\tau,\epsilon} H' \iff (\forall \phi \in \mathsf{MTL}^+\, [\mathsf{MTL}^+_\infty].\ H \models_\exists \phi \implies H' \models_\exists \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi))$$

Moreover, the characterisation result holds for the universal interpretation of satisfaction relation as well, that is:

$$H \sim_{\tau,\epsilon} H' \iff (\forall \phi \in \mathsf{MTL}^+\, [\mathsf{MTL}^+_\infty].\ H' \models \phi \implies H \models \mathsf{rlx}^{\sqsubseteq}_{\tau,\epsilon}(\phi))$$

5 Comparison with an existing relaxation

In this section, we discuss the existing relaxation operator for MTL from the literature due to Abbas, Mittelmann, and Fainekos [1], which is known to preserve MTL formulae for discrete samplings (timed-state sequences). We show that their relaxation cannot distinguish between traces not related by hybrid conformance, and hence is too lax for the purpose of logical characterisation for either hybrid conformance, or refinement.

5.1 AMF-Relaxation

We recall the relaxation operator from [1], 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 21.** *Given $\tau, \epsilon \geq 0$, the relaxation operator $[]^{\text{AMF}}_{\tau,\epsilon} : \mathsf{MTL}^+ \to \mathsf{MTL}^+_{ext}$ is defined as follows:*

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

where $I_{\ll a,b \gg}$ 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 $I \in \mathcal{T}(a,b)$, $I_{\ll c,d \gg} := (a+c, b+d)$.

Note that the interval relaxation $I_{\ll a,b \gg}$ differs from $I_{<a,b>}$ in that the former always yields an open interval, while the latter yields an interval of the same kind as I. For instance $[4,7]_{\ll -1,1 \gg} = (3,8)$, whereas $[4,7]_{<-1,1>} = [3,8]$.

It follows from Definition 21 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 22.** *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 $\mu_1, t_1 \models \phi \implies \mu_2, t_2 \models [\phi]^{\text{AMF}}_{\tau,\epsilon}$.*

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 $[]^{\text{AMF}}_{\tau,\epsilon}$.

5.2 Laxness of AMF-Relaxation

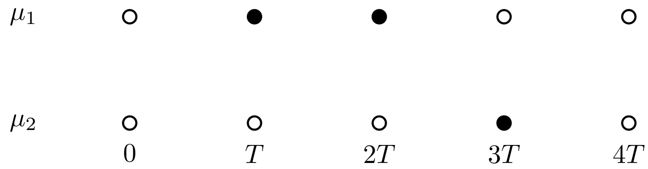
In this section, we prove that the notion of AMF-relaxation is too lax for the purpose of logical characterisation of hybrid conformance, i.e. there is a class of non-conforming implementations which preserve AMF-relaxations of all MTL properties satisfied by their specifications.

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.

Recall that we refer to generalised timed traces with a finite time domain as 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 23.** Fix $\tau > 0$ and let T be a value very slightly smaller than τ, i.e. $T = \tau - \delta$, where $\delta \ll \tau$. Consider the discretised GTTs presented in Example 2, which we recall here for the sake of convenience; μ_1 holds value **true** only at T and $2T$ and μ_2 holds value **true** at $3T$ and **false**, otherwise. 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 $(\tau, 0)$-close, not even $(t, 0)$-close 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 24.** *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 25.** Consider the TSSs in Example 23; 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 $\textsc{chunk}_2$:

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

▶ **Example 26.** Considering Example 23 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 $[p_{\mathbf{t}}\, \mathcal{U}_{[3T,3T]}\, p_{\mathbf{f}}]^{\mathrm{AMF}}_{\tau,0}$. The latter statement can be deduced from 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 $[p_{\mathbf{t}}\, \mathcal{U}_{[3T,3T]}\, p_{\mathbf{f}}]^{\mathrm{AMF}}_{\tau,0}$.

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

▶ **Proposition 27.** *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*

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

we have, for all formulae $\phi \in \mathsf{MTL}^+$: $(\mu_A, t_A) \models \phi \implies (\mu_B, t_B) \models [\phi]^{\mathrm{AMF}}_{\tau,0}$, and $(\mu_B, t_B) \models \phi \implies (\mu_A, t_A) \models [\phi]^{\mathrm{AMF}}_{\tau,0}$.

Proof. The proof by structural induction on ϕ is rather tedious and technical, and omitted in this version of the paper. ◀

6 Conclusions and Future Work

In this paper, we have studied the notion of hybrid conformance from the literature, as well its associated preorder, called hybrid refinement. We have presented a logical characterisation of both relations in Metric Temporal Logic. Since the notions of refinement and conformance allow 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. The relaxation operators corresponding to the two relations differ considerably – while for hybrid refinement it suffices to perform relaxation on the level of propositions only, characterising hybrid conformance requires relaxing bounds of intervals in temporal operators. We note that with hybrid conformance we obtain stronger characterisation result; it holds in particular under both existential and universal interpretation of the satisfaction relation.

We have also 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.

Our preservation and characterisation results for hybrid refinement are formulated using the existential interpretation of the satisfaction relation, while our results for hybrid conformance hold both for the existential- and universal interpretation of the satisfaction relation. This is inherent to our notion of hybrid refinement and cannot be remedied in any straightforward manner, as far as we could investigate. We envisage that there could be other definitions of hybrid refinement that are well-behaved in this respect and we would like to study and propose such notions in the future.

As another line of future research, we would also like to investigate the possibility of characterising Skorokhod conformance with Freeze Temporal Logic and the notion of relaxation provided by Deshmukh, Majumdar, and Prabhu [16]. 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.

Acknowledgements We thank Rayna Dimitrova for her helpful comments on an earlier version of this article. We also thank anonymous ICALP reviewers for their thorough feedback which helped us improve the paper.

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. 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. 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 Valentina Castiglioni, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. A logical characterization of differential privacy. *Sci. Comput. Program.*, 188:102388, 2020. doi:10.1016/j.scico.2019.102388.

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. doi:10.1016/0304-3975(84)90113-0.

14 Josee Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labelled markov processes. *Theor. Comput. Sci.*, 318(3):323–354, 2004. doi:10.1016/j.tcs.2003.09.013.

15 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.

16 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. doi:10.1007/s10703-016-0261-8.

17 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.

18 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.

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

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

21 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.

22 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.

23 Ron Koymans. Specifying real-time properties with metric temporal logic. *Real-Time Systems*, 2(4):255–299, 1990. doi:10.1007/BF01995674.

24 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. doi:10.1007/978-3-540-30206-3_12.

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. 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. 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. 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.