

A Metric Temporal Logic for Dealing with Zero-time Transitions

Luca Ferrucci, Dino Mandrioli, Angelo Morzenti, Matteo Rossi

Dipartimento di Elettronica e Informazione - Politecnico di Milano, 20133 Milano, Italy

Email: {ferrucci,mandrioli,morzenti,rossi}@elet.polimi.it

Abstract—Many industrial systems include components interacting with each other that evolve with possibly very different speeds. To deal with this situation many formalisms adopt the abstraction of “zero-time transitions”, which do not consume time. These, however, have several drawbacks in terms of naturalness and logic consistency, as a system is modeled to be in different states at the same time. We introduce a metric temporal logic, called X-TRIO, that uses non-standard analysis to elegantly deal with zero-time transitions in an abstract, descriptive way. We study the decidability of the logic, and we introduce a decision procedure for a subset thereof. X-TRIO has been applied in companion works to the design and verification of industrial systems.

I. INTRODUCTION

In a traditional view of time-dependent systems the state is a function of time, i.e., the system is in exactly one state at each time instant. Some (though not all) temporal logics also adopt this view: formulae refer to an (implicit) time instant, the (sub)formulae are evaluated with respect to the unique system state associated with it, and the logic’s modal operators refer to other time instants and related states.

If the modeled system evolves by *discrete* computation steps then a correspondingly discrete underlying time structure is naturally adopted, and the next-time operator (and possibly, in addition, a previous-time operator) are provided, such as the X (respectively, Y) operators of Linear Temporal Logic. The time domain, then consists of the set of the naturals \mathbb{N} or the integers \mathbb{Z} ; the time taken by each computation step is uniform, and it corresponds to the adopted time unit, say, seconds or microseconds.

If a genuinely quantitative notion of time is adopted for modeling strict real-time features, or a need arises to characterize asynchronous behaviors, the underlying time domain may be dense or continuous, like the set of real numbers, and modal operators are provided such as $\text{Dist}(\bullet, d)$ of TRIO [1], or similar operators in MTL [2], to refer to the time point at a generic distance d from the current time. Then, the next operator X, which adopts a fixed time displacement, becomes just an abbreviation for $\text{Dist}(\bullet, 1)$. This assumption, however, becomes too simplistic if the various computational steps that move the system from one state to the next one take a variable amount of time to complete. In some cases, the duration of some steps is orders of magnitude smaller than others so that, at some level of abstraction, it can be neglected entirely. This situation

occurs in many practical cases, like in hardware devices where several gate-switches occur during a single clock period, or in heterogeneous control systems, where different components evolve at sharply different time granularities, say microseconds vs. seconds or minutes or even longer ones.

In such cases, the literature often proposes a sharp distinction between micro- and macro-steps. Normally, only macro-steps are assumed to “consume time” — often just one unit — whereas micro-steps are considered as zero-time transitions. Various operational formalisms, like Timed Petri nets or variants of the Statecharts notations adopt this assumption [3]. For such systems, however, the use of fixed-duration next-time operator is inadequate.

In temporal logics that adopt a view of system state as a function of time such a notion of zero-time transition is however counterintuitive (when a zero-time micro-step is performed more than one state is associated with a single time instant), and may lead to logical contradiction.

Some temporal logics adopt instead a time structure where more than one system state may be associated with a single time instant [4] and therefore must provide distinct notations to refer to time and state change. In these notations, the progress of time and state evolution are fully decoupled, which is rather unnatural in most practical cases.

In previous work [5], we proposed the adoption of Non-Standard Analysis (NSA) to formalize micro-steps. Intuitively, in NSA the domain of any variable is extended by introducing non-standard numbers, which, roughly speaking, include infinitesimal quantities: an infinitesimal number is strictly less than any positive standard one. We exploited this idea by formalizing micro-steps in terms of transitions that take a non-null, infinitesimal time in the context of our metric temporal logic language TRIO.

In this paper, we develop the approach by defining a framework consisting of: a time domain T enriched with non-standard numbers; the TRIO temporal logic, providing a metric on time through the $\text{Dist}(\bullet, d)$ operator; a sequence σ of instants in $-T$, the augmented version of $-T$, in which the modeled system changes state; a new next operator X to refer to the next system state, which occurs in a non-standard time instant in case of a micro-step, or in a standard one in case of an ordinary (macro-) step.

The overall framework is called X-TRIO: we provide its syntax and semantics, and prove that the logic is in

general undecidable; we then define a decidable fragment that is expressive enough to model computing devices that are typically embedded in many industrial systems, such as Flexible Manufacturing Systems (FMS). The decidability of this subset of X-TRIO is obtained through its encoding into the Propositional Linear Temporal Logic with Both future and past operators (PLTLB); from this encoding, we built a prototype verification tool using decision procedures based on bounded model-checking implemented in the Zot tool [6].

Two companion papers apply the X-TRIO language to formalize the semantics of the Stateflow notation used in many application fields, and to automatically analyze properties of critical system: [7] focuses on the modeling and analysis of single Stateflow components whereas [8] deals with the integration of several cooperating modules.

Notions of zero-time transitions appear very naturally when reasoning about computations of embedded systems. For instance, in [9], while developing and analyzing a formal model of an aerospace satellite system, the authors repeatedly emphasize the need for "algorithmic detection of Zeno behavior". An early approach in the field of temporal logics introduced a time structure suitable to support the notion of micro- and macro-steps [2]. Our approach, based on NSA, allows us to frame the problem in a general and elegant way, and provides means to equip the resulting logic with suitable verification mechanisms. In the literature, other works have used NSA to provide a formal and rigorous semantics to timing features of various kinds of notations for system modeling: in [10] NSA is used to describe a hybrid system modeled in Simulink in presence of cascaded mode changes, while in [11] a complete system theory is defined, adopting a theoretical approach to investigate computability issues.

This paper is structured as follows. Section II defines the syntax and semantics of X-TRIO. Section III studies decidability issues, identifies a decidable fragment of the logic, and provides its encoding into PLTLB. Section IV draws conclusions and hints at possible extensions of this work.

II. THE X-TRIO LOGIC

In this section, we first introduce some necessary background, then we define the syntax and semantics of X-TRIO.

A. Syntax

The original TRIO language [1] is a general-purpose specification language suitable for modeling real-time systems. It is a temporal logic supporting a metric on time. TRIO formulae are built out of the usual first-order connectives, operators, and quantifiers, and the single basic modal operator *Dist*: for any formula ϕ and term t indicating a time distance, formula $\text{Dist}(\phi, t)$ specifies that ϕ holds at a time instant whose distance is exactly t time units from

the current instant. TRIO formulae can be interpreted both in discrete and dense time domains.

X-TRIO extends TRIO along two main lines. First, the temporal domain T is augmented with infinitesimal numbers from the theory of non-standard analysis founded by A. Robinson [12], which has already been exploited in TRIO [5] to deal with time-critical systems. Intuitively, for any numerical domain D , ϵ is infinitesimal in D if $\epsilon \geq 0$ and ϵ is smaller than any number in $D_{>0}$. The original values of D are classified as *standard* and are characterized by predicate *st*, that is, x is standard iff $st(x)$ holds. D is augmented with infinitesimal numbers and all numbers resulting from adding and subtracting infinitesimal non-zero numbers to and from standard ones, respectively. Predicate *ns*(x) denotes that x is *non-standard*. For each x , $st(x)$ holds if and only if $ns(x)$ does not hold. Notice that 0 is the only infinitesimal standard number and that non-standard numbers are of the form $v \pm \epsilon$, where $st(v)$ holds, and ϵ is infinitesimal greater than 0. NSA provides an axiomatization that allows one to apply all arithmetic operations and properties of traditional analysis in an intuitive way: for instance, the sum of two standard numbers is standard, the sum of two infinitesimal numbers is an infinitesimal and the sum of an infinitesimal with a standard number is a non-standard number. The theory of NSA introduces, in addition to the notion of infinitesimal numbers and operations on them, the notion of infinite numbers (which are, intuitively, greater than any value in D), plus a rich set of results that make NSA an appealing framework for reasoning on both familiar and new objects. In this paper we exploit some of the terminology and concepts of NSA to provide an elegant characterization of zero-time steps, but we do not make use of the full power of the theory; for example, we do not deal with infinite numbers (i.e., we have that $ns(x)$ iff $x = v \pm \epsilon$, with $st(v)$ and ϵ infinitesimal), as they are of no use when modeling zero-time steps.

We assume as the original time domain D either \mathbb{N} or $\mathbb{R}_{\geq 0}$ and denote its extension with infinitesimal numbers as \bar{T} . \bar{T} is a totally ordered set of numbers.

The second major novelty of X-TRIO is the introduction of the *next* operator X which is typical to describe the evolution of dynamical systems as a sequence of discrete steps. Unlike the traditional use of the operator in a metric setting, however, the time distance between two consecutive states is not implicitly assumed as a time unit; on the contrary, it can be any standard or non-standard positive number. Precisely, we introduce two different types of X operator, namely, X_{st} and X_{ns} . Intuitively, the formula $X_{st}(\phi)$ is true in the current instant iff ϕ is true in the next state entered by the system and this occurs at a time instant that is a standard number; conversely, formula $X_{ns}(\phi)$ is true iff, in the next state, ϕ is true and the occurrence time is a non-standard number. We will use these two operators to distinguish between two typical ways of

OPERATOR	DEFINITION
$\text{AlwF}(\phi)$	$\forall t(t \geq 0 \rightarrow \text{Dist}(\phi, t))$
$\text{SomF}(\phi)$	$\exists t(t \geq 0 \wedge \text{Dist}(\phi, t))$
$\text{Until}(\phi, \psi)$	$\exists t \geq 0(\text{Dist}(\psi, t) \wedge \forall v(0 \leq v < t \rightarrow \text{Dist}(\phi, v)))$
$\text{Since}(\phi, \psi)$	$\exists t \geq 0(\text{Dist}(\psi, -t) \wedge \forall v(-t < v \leq 0 \rightarrow \text{Dist}(\phi, v)))$

Table I
X-TRIO DERIVED TEMPORAL OPERATORS.

modeling system evolution: X_{st} will formalize *macro-steps* i.e., transitions that "consume real, tangible time", whereas X_{ns} will describe *micro-steps*, which are often formalized as zero-time transitions. *Yesterday* operators Y_{st} and Y_{ns} are introduced in a similar manner.

The syntax of X-TRIO is defined as follows:

$$\begin{aligned}\phi &:= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \text{Dist}(\phi, k) \mid \\ &\quad X_{\text{st}}(\phi) \mid X_{\text{ns}}(\phi) \mid Y_{\text{st}}(\phi) \mid Y_{\text{ns}}(\phi) \mid \forall t.\tau \\ \tau &:= \phi \mid \text{Dist}(\phi, t) \mid t = k \mid t < k \mid \tau_1 \wedge \tau_2 \mid \neg\tau\end{aligned}$$

In this paper, we restrict the set of atomic propositions AP to propositional variables p , and the set V of temporal terms to variables t and constants k . Temporal terms t take values in the time domain \bar{T} and can appear only in closed formulae. We leave first-order extensions of the logic to future work. Symbols \top , \perp , \vee , \rightarrow , \exists , etc. are derived as usual. We introduce the derived operators of X-TRIO as in TRIO; Table I shows those used in this paper.

B. Semantics

A model-theoretic semantics for X-TRIO is defined by following a fairly standard path on the basis of a temporal structure $S = \langle \bar{T}, \beta, \nu, \sigma \rangle$, where:

- (i) \bar{T} is the time domain such that $\forall t \in \bar{T}$ it is $t \geq 0$.
- (ii) $\beta : \bar{T} \mapsto 2^{AP}$ is an interpretation function that associates each instant of time t with the set of atomic propositions $\beta(t)$ that are true in t .
- (iii) $\nu : V \mapsto \bar{T}$ is an evaluation function that associates with each temporal term of the set V a value in \bar{T} .
- (iv) $\sigma = \{\sigma_i \mid i \in \mathbb{N} : \sigma_i \in \bar{T} \wedge \sigma_0 = 0 \wedge \forall j \in \mathbb{N}(j < i \Rightarrow \sigma_j < \sigma_i) \wedge \forall t \in \bar{T}(\sigma_i < t < \sigma_{i+1} \Rightarrow \beta(\sigma_i) = \beta(t))\}$ is the distinguishing element of the X-TRIO temporal structure. It is a (possibly infinite) sequence of time instants starting from the initial instant 0, called *History*. Intuitively, it represents the discrete sequence of instants when the system changes state. Thus, the X operator represents a step moving from σ_i to σ_{i+1} . Then, the satisfaction relation \models of an X-TRIO formula ϕ by structure $S = \langle \bar{T}, \beta, \nu, \sigma \rangle$ at a time instant $t \in \bar{T}$ is defined as in Table II. A formula ϕ is *satisfiable* in a structure $S = \langle \bar{T}, \beta, \nu, \sigma \rangle$ when $S, 0 \models \phi$.

In the rest of this paper, we study some relevant properties of the X-TRIO logic, with focus on the case $T = \mathbb{N}$.

$$\begin{aligned}S, t &\models p \text{ iff } p \in \beta(t) \\ S, t &\models \neg\phi \text{ iff } S, t \not\models \phi \\ S, t &\models \phi_1 \wedge \phi_2 \text{ iff } S, t \models \phi_1 \text{ and } S, t \models \phi_2 \\ S, t &\models \text{Dist}(\phi, k) \text{ iff } t + \nu(k) \in \bar{T} \text{ and } S, t + \nu(k) \models \phi \\ S, t &\models \text{Dist}(\phi, d) \text{ iff } t + \nu(d) \in \bar{T} \text{ and } S, t + \nu(d) \models \phi \\ S, t &\models X_{\text{st}}(\phi) \text{ iff there is } i \in \mathbb{N} \text{ s.t. } \sigma_i \leq t < \sigma_{i+1}, st(\sigma_{i+1}) \\ &\quad \text{and } S, \sigma_{i+1} \models \phi \\ S, t &\models X_{\text{ns}}(\phi) \text{ iff there is } i \in \mathbb{N} \text{ s.t. } \sigma_i \leq t < \sigma_{i+1}, ns(\sigma_{i+1}) \\ &\quad \text{and } S, \sigma_{i+1} \models \phi \\ S, t &\models Y_{\text{st}}(\phi) \text{ iff there is } i \in \mathbb{N} \text{ s.t. } \sigma_{i-1} < t \leq \sigma_i, i > 0, \\ &\quad st(\sigma_{i-1}) \text{ and } S, \sigma_{i-1} \models \phi \\ S, t &\models Y_{\text{ns}}(\phi) \text{ iff there is } i \in \mathbb{N} \text{ s.t. } \sigma_{i-1} < t \leq \sigma_i, i > 0, \\ &\quad ns(\sigma_{i-1}) \text{ and } S, \sigma_{i-1} \models \phi \\ S, t &\models \forall d.\phi \text{ iff for all } \nu' \text{ that differ from } \nu \text{ at most for } d, \\ &\quad \langle \bar{T}, \beta, \nu', \sigma \rangle, t \models \phi\end{aligned}$$

Table II
SEMANTICS OF X-TRIO.

III. DECIDABILITY OF X-TRIO

Let us consider the following syntactic fragment of X-TRIO, which we name X-TRIO_N:

$$\begin{aligned}\phi &:= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \text{Dist}(\phi, 1) \mid \text{Dist}(\phi, \epsilon) \mid \\ &\quad \text{Dist}(\phi, -1) \mid \text{Dist}(\phi, -\epsilon) \mid \text{Until}(\phi_1, \phi_2) \mid \\ &\quad \text{Since}(\phi_1, \phi_2) \mid X_{\text{st}}(\phi) \mid X_{\text{ns}}(\phi) \mid Y_{\text{st}}(\phi) \mid Y_{\text{ns}}(\phi)\end{aligned}$$

As the name suggests, we interpret X-TRIO_N formulae over the non-standard temporal domain $\bar{\mathbb{N}}$. In X-TRIO_N, $\text{Dist}(\phi, 1 + \epsilon)$ is an abbreviation for $\text{Dist}(\text{Dist}(\phi, \epsilon), 1)$; similarly for $\text{Dist}(\phi, 1 - \epsilon)$. The *Until* and *Since* operators are now primitive, and we have the following abbreviations: $\text{SomF}(\phi) = \text{Until}(\top, \phi)$ and $\text{AlwF}(\phi) = \neg\text{SomF}(\neg\phi)$. Notice that, as the syntax of X-TRIO_N does not allow variables, its temporal structures become triples of the form $S = \langle \bar{T}, \beta, \sigma \rangle$. We also restrict the interpretation domain to the numbers of $\bar{\mathbb{N}}$ of the form $v + k\epsilon$, where $v, k \in \mathbb{N}$ and ϵ is an infinitesimal number. Thus, standard numbers are identified by the coefficient $k = 0$. We indicate this domain by $\bar{\mathbb{N}}_+$. In addition, since by definition for all $k \in \mathbb{N}$, $v + k\epsilon < v + 1 - k\epsilon$, due to the restriction above we have $v - k\epsilon \notin \bar{\mathbb{N}}_+$ for all k . Hence, for all ϕ , $\text{Dist}(\phi, -\epsilon)$ is false in all standard instants t (i.e., such that $st(t)$).

Despite the restrictions introduced in X-TRIO_N, however, the logic is undecidable, and the following holds.

Theorem 1. *The satisfiability problem of the X-TRIO_N logic is undecidable.*

Proof sketch. In classic fashion (see, e.g., [13]), we reduce the halting problem of a 2-counter machine to the satisfiability problem of X-TRIO_N formulae, by defining a set of X-TRIO_N formulae that formalize the increment and decrement of the 2 counters.

We associate one counter with the sequence of even standard numbers, and one with the sequence of odd standard

numbers, as detailed below. We associate two propositional letters, E and O , with each standard instant of σ so that when the current standard instant is even (resp., odd) then only E (resp., O) holds. They do not hold in non-standard instants. These constraints are represented by the following X-TRIO_N formulae (we show the case of even instants):

$$\begin{aligned} E &\Rightarrow X_{st}(O) \vee \\ &\quad X_{ns}(\text{Until}(\neg O \wedge \neg E, X_{st}(O) \wedge \neg O \wedge \neg E)) \\ E &\Leftrightarrow \text{Dist}(O, 1) \end{aligned}$$

Given two consecutive standard instants σ_j and σ_i in σ (i.e., such that $\sigma_i = \sigma_j + 1$), there is a finite (possibly empty) sequence $\sigma_{[j,i]}$ of length $i - (j + 1)$ of non-standard instants in σ between them since σ is discrete. We introduce X-TRIO_N formulae (not shown here for brevity) to partition $\sigma_{[j,i]}$ into two subsequences such that, at each instant, either propositional letter A or propositional letter B holds. We use letters A and B to “mark” each instant in $\sigma_{[j,i]}$ as shown in Figure 1. The sequence of B ’s ends in the last non-standard instant of $\sigma_{[j,i]}$.

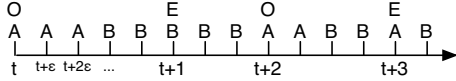


Figure 1. Part of trace representing counters.

We use the sequence of A and B to represent the two counters: the numbers of A ’s starting from standard numbers marked with E (resp. O) represent the first (resp. second) counter. We encode the operations *increase/decrease/check if 0*, by manipulating the length of the sequence of A ’s. For example, the counter associated with E increases its current value if the sequence of A ’s that starts at the next even standard instant is such that the last A of that sequence dists $2 + \epsilon$ from the last A of the current sequence of A ’s. This is encoded through the following X-TRIO_N formula, reminding that all the naturals numbers belong to the temporal domain:

$$E \rightarrow (A \rightarrow \text{Until}(A, B \wedge \text{Dist}(A \wedge X_{ns}(B), 2))) \wedge (B \rightarrow \text{Dist}(A \wedge X_{ns}(B), 2))$$

The other cases are omitted for brevity.

The counter is zero when the sequence of A ’s is empty. In the case of the counter associated with even standard numbers we can encode this check with the formula $E \wedge B$.

Finally, at the initial instant of the sequence σ , which is an even number, E holds and the corresponding counter value is 0 (i.e., $E \wedge B$ holds at 0).

The halting of the formalized machine is expressed simply as reachability of a final state. Hence, we conclude that the satisfiability problem of X-TRIO_N is undecidable. ■

The counting mechanism can be simulated by X-TRIO_N thanks to the $\text{Dist}(\bullet, 1 + \epsilon)$ operator, which allows us to move from a non-standard instant $v + k\epsilon$ to the non-standard

$(v + 1) + (k + 1)\epsilon$, whose infinitesimal distance from $v + 1$ increases of ϵ w.r.t to the distance of $v + k\epsilon$ from v . This generality, however, is unnecessary for interesting classes of applications such as those tackled in [7], [8], for which we do not need the full expressive power of X-TRIO_N. In the next section, we investigate a sufficient condition that allows us to build a decision procedure for a subset of the logic that can be used in many relevant practical applications. The study of other sufficient conditions is left for future work.

A. A decision procedure for X-TRIO

In this section, we show the decidability of a fragment of X-TRIO_N by reducing its satisfiability problem to that of PLTLB. The transformation is effective and has been implemented in the Zot satisfiability checker.

PLTLB extends classic LTL [14] with past operators; its syntax (as used in the rest of this paper) is the following:

$$\phi := p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid X_L(\phi) \mid Y_L(\phi) \mid \phi_1 U_L \phi_2 \mid \phi_1 S_L \phi_2$$

We have also the usual abbreviations $F_L(\phi) = \top U_L \phi$ and $G_L(\phi) = \neg F_L(\neg\phi)$. The semantics of PLTLB is defined over discrete *traces*. A trace is an infinite word $\pi = \pi(0)\pi(1)\dots$ over the finite alphabet $\Sigma = 2^{AP}$, where each $\pi(i)$ represents the set of atomic propositions that are true in i . \models_L denotes the satisfiability relation of PLTLB. The definition of \models_L is straightforward if one considers that, for any ϕ , $Y_L(\phi)$ is false at 0 [14].

As a first step to encode X-TRIO_N into PLTLB, we restrict histories σ according to the following constraints:

- 1) Either all standard natural numbers or a bounded interval thereof including 0 belong to σ .
- 2) If σ_{i+1} is non-standard ($ns(\sigma_{i+1})$), then $\sigma_{i+1} - \sigma_i = \epsilon$.

These constraints are not strictly necessary to obtain decidability, but they are not overly restrictive and they simplify the encoding for our purposes. Notice also that, if σ_{i+1} is standard ($st(\sigma_{i+1})$), then between σ_i and σ_{i+1} there is an infinite sequence of nonstandard numbers $\sigma_i + \epsilon, \sigma_i + 2\epsilon, \dots$ such that, for all $k \in \mathbb{N}$, $\beta(\sigma_i + k\epsilon) = \beta(\sigma_i)$.

In order to reduce the satisfiability problem of X-TRIO_N (which is in general undecidable) to that of PLTLB (which is decidable), we need to apply further restrictions to the former. As mentioned above, the key to encoding a counting mechanism in X-TRIO_N is to evaluate operator $\text{Dist}(\bullet, v + k\epsilon)$ (with $v \geq 1$) in non-standard instants. This suggests, to obtain decidability, to make the evaluation of this operator meaningful only in standard instants. For this, we introduce an X-TRIO_N predicate, NowST, that evaluates to true only in standard instants. Such a predicate corresponds to the following X-TRIO_N formula:

$$\text{NowST} \equiv \neg \text{Dist}(\top, -\epsilon) \quad (1)$$

In fact, $\text{Dist}(\top, -\epsilon)$ holds in $t \in \overline{\mathbb{N}}_+$ iff $t - \epsilon \notin \overline{\mathbb{N}}_+$, which is true iff $st(t)$. Then, every occurrence of

$\text{Dist}(\phi, v + k\epsilon)$, with $v \geq 1$, will be intended as an abbreviation for $\text{Dist}(\phi, v + k\epsilon) \wedge \text{NowST}$. Hence, by convention $\text{Dist}(\phi, v + k\epsilon)$ is false in all non-standard instants if $v \geq 1$.

In addition, we introduce a further restriction that allows us to obtain a quite simple decision procedure for the logic, with a rather limited cost in expressiveness, as discussed below. The restriction consists of imposing that the value of formulae is meaningful only in instants that are “covered” by the history σ . In fact, by definition of σ in Section II-B, there can be instants $t \in \bar{T}$ such that, for all i , $\sigma_i < t$. In this case, σ shows a classic “Zeno behavior” [3], where it accumulates at a finite instant, signaling a model that changes state infinitely often in a finite interval. Then, by convention, we state that formulae that are evaluated after one such accumulation point are false. This can be achieved by considering every subformula ψ of an X-TRIO_N formula ϕ as an abbreviation for $\psi \wedge \text{SomF}(\text{X}_{\text{st}}(\top) \vee \text{X}_{\text{ns}}(\top))$. We have the following result.

Lemma 2. *Given an X-TRIO_N formula ϕ in which all subformulae have the form $\psi \wedge \text{SomF}(\text{X}_{\text{st}}(\top) \vee \text{X}_{\text{ns}}(\top))$, and given two structures $S_1 = \langle \bar{\mathbb{N}}_+, \beta_1, \sigma \rangle$, $S_2 = \langle \bar{\mathbb{N}}_+, \beta_2, \sigma \rangle$ (i.e., which have the same history σ) such that, for all $t \in \bar{\mathbb{N}}_+$ for which there is $i \in \mathbb{N}$ such that $t < \sigma_i$, it is $\beta_1(t) = \beta_2(t)$, then $S_1, 0 \models \phi$ iff $S_2, 0 \models \phi$.*

Proof sketch. We show a stronger result, from which Lemma 2 descends as corollary. More precisely, we show that, given any $t \in \bar{\mathbb{N}}_+$, $S_1, t \models \phi$ iff $S_2, t \models \phi$. First of all, we remark that, if for each $t \in \bar{\mathbb{N}}_+$ there is a σ_i such that $t < \sigma_i$, then for all $t \in \bar{\mathbb{N}}_+$ it is $\beta_1(t) = \beta_2(t)$, hence the desired result. In addition, notice that, in this case, condition $\text{SomF}(\text{X}_{\text{st}}(\top) \vee \text{X}_{\text{ns}}(\top))$ is true for all $t \in \bar{\mathbb{N}}_+$, so the value of ϕ does not depend on it.

In the rest of the proof, we consider the case in which there are instants t such that, for all i , $\sigma_i < t$. The set of such instants can be shown to have a minimum, which we indicate with \bar{t} , such that $st(\bar{t})$. Then, history σ accumulates at \bar{t} , and we separate two cases: $t < \bar{t}$ and $t \geq \bar{t}$. In the case $t \geq \bar{t}$, $\text{SomF}(\text{X}_{\text{st}}(\top) \vee \text{X}_{\text{ns}}(\top))$ is false, hence for all ϕ both $S_1, t \not\models \phi$ and $S_2, t \not\models \phi$. Then, we only need to consider the case $t < \bar{t}$. The rest of the proof is by induction on the structure of ϕ : consider a subformula ψ of ϕ .

If $\psi = p$, by hypothesis $\beta_1(t) = \beta_2(t)$; hence the result. If $\psi = \text{Dist}(\zeta, 1)$, then $S_1, t \models \psi$ iff $S_1, t + 1 \models \zeta$, hence, by inductive hypothesis, iff $S_2, t + 1 \models \zeta$, and iff $S_2, t \models \psi$. All other cases are similar and are omitted for brevity. ■

As a consequence of Lemma 2, and also of the next lemma 3, given the restrictions introduced above, in order to determine whether an X-TRIO_N formula is satisfiable we only need to focus on the sequence σ , and we can disregard the instants following an accumulation point, if any.

In order to introduce our PLTLB-based decision procedure for X-TRIO_N, we need a further intermediate result. We show that, in each interval (σ_i, σ_{i+1}) such that $st(\sigma_{i+1})$,

there is an instant \bar{t} such that the subformulae of ϕ have the same value in all $t \in [\bar{t}, \sigma_{i+1})$. In addition, \bar{t} is a number of non-standard instants that is equal to the maximum nesting depth δ of $\text{Dist}(\bullet, -\epsilon)$ operators far from σ_i . More precisely, given a formula ϕ , the nesting $\delta(\phi)$ of $\text{Dist}(\bullet, -\epsilon)$ operators is defined as follows: $\delta(p) = 0$; $\delta(\psi_1 \wedge \psi_2) = \max(\delta(\psi_1), \delta(\psi_2))$, and similarly for the Until and Since operators; $\delta(\neg\psi) = \delta(\psi)$ (similarly for $\text{Dist}(\psi, \pm 1)$ and for $\text{Dist}(\psi, \epsilon)$); finally, $\delta(\text{Dist}(\psi, -\epsilon)) = 1 + \delta(\psi)$. Then, we have the following result.

Lemma 3. *Given an X-TRIO_N formula ϕ and a structure $S = \langle \bar{\mathbb{N}}_+, \beta, \sigma \rangle$, if $st(\sigma_{i+1})$, then for any two instants $j, k \in \bar{\mathbb{N}}_+$ such that $\sigma_i + \delta(\phi)\epsilon < j < k < \sigma_{i+1}$, $S, j \models \phi$ iff $S, k \models \phi$.*

Proof. First of all, we notice that it must be $ns(j)$ and $ns(k)$, as, by constraint 1, $\sigma_i \geq \sigma_{i+1} - 1$. Then, the proof proceeds by induction on the structure of ϕ .

If $\phi = p \in AP$, then $p \in \beta(j)$ iff $p \in \beta(k)$, as $\beta(j) = \beta(k)$ by definition of σ , hence the result.

If $\phi = \neg\psi$, $S, j \models \phi$ iff $S, j \not\models \psi$, which holds iff $S, k \not\models \psi$ by inductive hypothesis, as $\delta(\phi) = \delta(\psi)$, i.e., iff $S, k \models \phi$. The case for $\text{Dist}(\psi, \epsilon)$ is similar.

If $\phi = \psi_1 \wedge \psi_2$, $S, j \models \phi$ iff both $S, j \models \psi_1$ and $S, j \models \psi_2$, which, by inductive hypothesis, holds iff both $S, k \models \psi_1$ and $S, k \models \psi_2$, as $\delta(\phi) \geq \delta(\psi_1)$ and $\delta(\phi) \geq \delta(\psi_2)$.

If $\phi = \text{Dist}(\psi, 1)$, then both $S, j \not\models \phi$ and $S, k \not\models \phi$, as $\text{Dist}(\psi, 1)$ is by convention false in non-standard instants. Similarly when $\phi = \text{Dist}(\psi, -1)$.

If $\phi = \text{Until}(\psi_1, \psi_2)$, we have that $S, k \models \phi$ iff there is a $t \geq k$ s.t. $S, t \models \psi_2$, and for all $k \leq t' < t$ it is $S, t' \models \psi_1$. By inductive hypothesis, since $\delta(\phi) \geq \delta(\psi_1)$, for all t', t'' s.t. $j \leq t'' < k \leq t' < \sigma_{i+1}$, we have that $S, t' \models \psi_1$ iff $S, t'' \models \psi_1$. Hence, $S, t' \models \psi_1$ holds for all $k \leq t' < t$ iff also for all $j \leq t'' < t$ it is $S, t'' \models \psi_1$. Then, $S, k \models \phi$ iff $S, j \models \phi$. The case $\phi = \text{Since}(\psi_1, \psi_2)$ is similar.

If $\phi = \text{X}_{\text{st}}(\psi)$, $S, j \models \phi$ iff $S, \sigma_{i+1} \models \psi$, as $st(\sigma_{i+1})$. We have also $S, k \models \phi$ iff $S, \sigma_{i+1} \models \psi$, hence the result.

If $\phi = \text{X}_{\text{ns}}(\psi)$, both $S, j \not\models \phi$ and $S, k \not\models \phi$, as $st(\sigma_{i+1})$.

If $\phi = \text{Y}_{\text{st}}(\psi)$, both $S, j \models \phi$ and $S, k \models \phi$ hold iff $st(\sigma_i)$ and $S, \sigma_i \models \psi$. Similarly for the case $\phi = \text{Y}_{\text{ns}}(\psi)$.

If $\phi = \text{Dist}(\psi, -\epsilon)$, $S, j \models \phi$ iff $S, j - \epsilon \models \psi$; since $j - \epsilon > \sigma_i + (\delta(\phi) - 1)\epsilon$ and $\delta(\phi) = \delta(\psi) + 1$, then $k - \epsilon > j - \epsilon > \sigma_i + \delta(\psi)\epsilon$ hence, by inductive hypothesis, we have $S, k - \epsilon \models \psi$, i.e., $S, k \models \phi$. ■

Notice that Lemma 3 does not hold if $j = \sigma_i + \delta(\phi)\epsilon$. For example, if $j = \sigma_0 = 0$, $\sigma_1 = 1$, and $p \in \beta(\sigma_0)$, with $\delta(\phi) = 0$, then $\text{Y}_{\text{st}}(p)$ holds in $k = \sigma_0 + \epsilon$, but not in j .

The basic idea of the encoding is, given an X-TRIO_N formula ϕ , to build a corresponding PLTLB formula $\tau(\phi)$ such that each model $S = \langle \bar{\mathbb{N}}_+, \beta, \sigma \rangle$ of ϕ corresponds to a trace π that is a model of $\tau(\phi)$, where each $t \in \bar{\mathbb{N}}_+$ such that there is $\sigma_i > t$ is mapped onto an element $\pi(\rho_S(t))$,

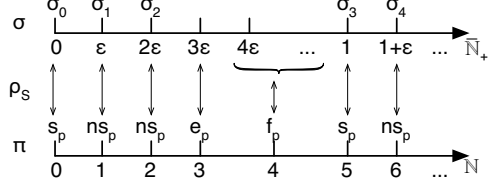


Figure 2. An example of ρ_S (with $\delta(\phi) = 1$).

and $\beta(t) = \pi(\rho_S(t))$, where $\rho_S : \overline{\mathbb{N}}_+ \mapsto \mathbb{N}$ is monotonic. Then, we represent the transition $\sigma_i \mapsto \sigma_{i+1}$ through the PLTLB operator X_L . Constraints 1 and 2 guarantee that the difference between σ_{i+1} and $\sigma_i = v + k\epsilon$ is either $1 - k\epsilon$ or ϵ , depending on whether σ_{i+1} is standard or not.

The encoding “flattens” the history σ over π : it represents each σ_i through an element of π . Then, to separate the elements of π that represent standard instants from those that represent non-standard ones, we introduce a PLTLB propositional letter s_p such that $s_p \in \pi(i)$ iff i in π corresponds to a standard number. In addition, we need to introduce “filling” elements in π to represent the (infinite) non-standard instants between σ_i and σ_{i+1} when $st(\sigma_{i+1})$. Lemma 3 suggests that the required number of these elements is finite, equal to $\delta(\phi) + 1$; in fact, all non-standard instants such that $\sigma_i + \delta(\phi) < t < \sigma_{i+1}$ are equivalent from the point of view of the truth of subformulae, hence they can be “condensed” in one single element. We mark the first $\delta(\phi)$ elements of π following the one corresponding to σ_i with proposition e_p , and the element corresponding to all instants $\sigma_i + \delta(\phi) < t < \sigma_{i+1}$ with f_p . Figure 2 depicts an example of history σ , and its corresponding trace π .

Then, trace π must obey the following PLTLB constraint, where ns_p is an abbreviation for $\neg s_p \wedge \neg f_p \wedge \neg e_p$:

$$\begin{aligned}
 & s_p \wedge \\
 & G_L((e_p \rightarrow \neg f_p \wedge \neg s_p) \wedge (f_p \rightarrow \neg s_p) \wedge \\
 & \quad (s_p \rightarrow \\
 & \quad X_L \left(ns_p U_L \left(\bigwedge_{k=1}^{\delta(\phi)} X_L^k(e_p) \wedge \right. \right. \\
 & \quad \quad \left. \left. X_L^{\delta(\phi)+1}(f_p \wedge X_L(s_p)) \right) \right)) \\
 & \quad \vee \\
 & \quad X_L(G_L(ns_p))) \wedge \\
 & (e_p \vee f_p \rightarrow \bigwedge_{p \in AP} p \leftrightarrow Y_L(p))
 \end{aligned} \quad (2)$$

PLTLB formula (2) imposes, respectively, that (i) s_p holds in $\pi(0)$, (ii) e_p , f_p and s_p are mutually exclusive, (iii) each element marked s_p is followed either by an infinity of ns_p elements or by a finite number of ns_p elements, until there is a sequence of exactly $\delta(\phi)$ e_p elements followed, in turn, by a f_p element, which is in turn followed by a s_p element, (iv) if e_p or $f_p \in \pi(i+1)$, then all propositions that hold in $\pi(i+1)$ also hold in $\pi(i)$. In other words, traces π have one of the following two forms: $s_p(ns_p^* e_p^{\delta(\phi)} f_p s_p)^\omega$ or $s_p(ns_p^* e_p^{\delta(\phi)} f_p s_p)^*(ns_p)^\omega$.

Transformation τ of Table III takes an X-TRIO $_{\mathbb{N}}$ formula ϕ and produces an equisatisfiable PLTLB formula ϕ_L .

$$\begin{aligned}
 \tau(p) &= p \\
 \tau(\neg\phi) &= \neg\tau(\phi) \\
 \tau(\phi_1 \wedge \phi_2) &= \tau(\phi_1) \wedge \tau(\phi_2) \\
 \tau(X_{ns}(\phi)) &= X_L(ns_p \wedge \tau(\phi)) \\
 \tau(X_{st}(\phi)) &= X_L((e_p \vee f_p) U_L(s_p \wedge \tau(\phi))) \\
 \tau(Y_{ns}(\phi)) &= Y_L((e_p \vee f_p) S_L(ns_p \wedge \tau(\phi))) \\
 \tau(Y_{st}(\phi)) &= Y_L((e_p \vee f_p) S_L(s_p \wedge \tau(\phi))) \\
 \tau(\text{Dist}(\phi, 0)) &= \tau(\phi) \\
 \tau(\text{Dist}(\phi, \epsilon)) &= (\neg f_p \wedge X_L(\tau(\phi))) \vee (f_p \wedge \tau(\phi)) \\
 \tau(\text{Dist}(\phi, -\epsilon)) &= \neg s_p \wedge \\
 & \quad ((\neg f_p \wedge Y_L(\tau(\phi))) \vee (f_p \wedge \tau(\phi))) \\
 \tau(\text{Dist}(\phi, 1)) &= s_p \wedge X_L(\neg s_p U_L(s_p \wedge \tau(\phi))) \\
 \tau(\text{Dist}(\phi, -1)) &= s_p \wedge Y_L(\neg s_p S_L(s_p \wedge \tau(\phi))) \\
 \tau(\text{Until}(\phi, \psi)) &= \tau(\phi) U_L \tau(\psi) \\
 \tau(\text{Since}(\phi, \psi)) &= \tau(\phi) S_L(f_p \wedge \tau(\phi) \wedge \tau(\psi)) \vee \\
 & \quad \tau(\phi) S_L(\neg f_p \wedge \tau(\psi))
 \end{aligned}$$

Table III
TRANSLATION SCHEMA τ .

Given a structure $S = \langle \overline{\mathbb{N}}_+, \beta, \sigma \rangle$, for all $t \in \overline{\mathbb{N}}_+$ such that there is $\sigma_i > t$, we define function $\rho_S : \overline{\mathbb{N}}_+ \mapsto \mathbb{N}$ as follows (see Figure 2 for a graphical representation): (i) $\rho_S(0) = 0$ ($\sigma_0 = 0$); (ii) if $ns(t)$, and $\exists i$ s.t. $t = \sigma_i$ (hence $t = \sigma_{i-1} + \epsilon$), then $\rho_S(t) = \rho_S(\sigma_{i-1}) + 1$; (iii) if $ns(t)$, and $\exists i$ s.t. $\sigma_i + \delta(\phi)\epsilon < t < \sigma_{i+1}$ (hence $st(\sigma_{i+1})$), then $\rho_S(t) = \rho_S(\sigma_i) + \delta(\phi) + 1$; (iv) if $t > 0$ and $st(t)$ (hence there is $i > 0$ s.t. $t = \sigma_i$), then $\rho_S(t) = \rho_S(\sigma_{i-1}) + \delta(\phi) + 2$; (v) if $ns(t)$, and $\exists i$ s.t. $\sigma_i < t \leq \sigma_i + \delta(\phi)\epsilon < \sigma_{i+1}$, then there is k s.t. $t = \sigma_i + k\epsilon$, and $\rho_S(t) = \rho_S(\sigma_i) + k$; Notice that rule (iii) is applied to all nonstandard instants in between $\sigma_i + \delta(\phi)\epsilon$ and σ_{i+1} , and it maps each of them onto a “filling” element in π . As a consequence, rule (iv) maps a standard instant onto $\rho_S(\sigma_{i-1}) + \delta(\phi) + 2$, i.e., to the element in π that follows a “filling” one. Then, if $t < t'$, we have $\rho_S(t) \leq \rho_S(t')$. The following result holds.

Theorem 4. *Given an X-TRIO $_{\mathbb{N}}$ formula ϕ , there is a structure $S = \langle \overline{\mathbb{N}}_+, \beta, \sigma \rangle$ such that $S, 0 \models \phi$ iff there exists a trace π such that $\pi \models_{\text{L}} \tau(\phi) \wedge (2)$.*

Proof: Suppose we have a structure $S = \langle \overline{\mathbb{N}}_+, \beta, \sigma \rangle$. The corresponding infinite word π is built from S as follows (where AP are the atomic propositions in ϕ): for each $p \in AP$ and $t \in \overline{\mathbb{N}}_+$ such that there is $\sigma_i > t$ (hence $\rho_S(t)$ is defined), $p \in \beta(t)$ iff $p \in \pi(\rho_S(t))$. In addition, $s_p \in \pi(\rho_S(t))$ iff $st(t)$, $f_p \in \pi(\rho_S(t))$ iff there i s.t. $\sigma_i + \delta(\phi) < t < \sigma_{i+1}$ and $st(\sigma_{i+1})$, and $e_p \in \pi(\rho_S(t))$ iff $\sigma_i < t \leq \sigma_i + \delta(\phi) < \sigma_{i+1}$. It can be shown that trace π built in this way satisfies formula (2).

Dually, if π is such that $\pi \models_{\text{L}} \tau_e(\phi) \wedge (2)$, structure $S = \langle \overline{\mathbb{N}}_+, \beta, \sigma \rangle$ is obtained in the following way. Given an $l \in \mathbb{N}$, if $e_p, f_p \notin \pi(l)$ (i.e., l is not a “filling” element), $\langle l_0 \dots l_v \rangle$

(where $\forall j \in [0, v)$, we have $l_j < l_{j+1}$) are all the elements of the infinite word π such that $l_v \leq l$ and $\forall j \in [0, v] : s_p \in \pi(l_j)$ (i.e., they are all the elements that correspond to standard instants in π preceding element l), and $k = l - l_v$ (i.e., k is the number of elements between $\pi(l)$ and $\pi(l_v)$), then $\sigma_l = v + k\epsilon$. This entails that, since σ_l is a standard number iff it is of the form $v + 0\epsilon$, we have that $st(\sigma_l)$ iff $s_p \in \pi(l)$. In addition, by (2), $s_p \in \pi(0)$, hence $\sigma_0 = 0$ as expected. This defines the points of the history σ of S , which in turn defines ρ_S . β is defined as follows: for each t such that there is $\sigma_i > t$, for each $p \in AP$, $p \in \beta(t)$ iff $p \in \pi(\rho_S(t))$. If, instead, there is no $\sigma_i > t$, we can chose the value of $\beta(t)$ arbitrarily, as, by Lemma 2, it does not affect the truth of ϕ in S ; then, in this case we have $p \notin \beta(t)$ for all $p \in AP$.

We prove Theorem 4 by induction on the structure of formula ϕ . First of all, by Lemma 2, if there is an accumulation point \bar{t} , instants $t \geq \bar{t}$ do not affect the satisfiability of ϕ , hence we need only analyze instants $t < \bar{t}$. Then, we show that, for all $t < \bar{t}$ (where $\bar{t} = +\infty$ if there is no accumulation point), it is $S, t \models \psi$ (where ψ is a subformula of ϕ) iff $\pi, \rho_S(t) \models_L \tau(\psi)$.

If $\psi = p$, then $S, t \models p$ iff $p \in \beta(t)$, which holds, by construction, iff $p \in \pi(\rho_S(t))$, i.e. iff $\pi, \rho_S(t) \models_L p$, and $\tau(p) = p$, hence the result. The cases $\psi = \neg \zeta$ and $\psi = \psi_1 \wedge \psi_2$ are immediate.

If $\psi = X_{ns}(\zeta)$, $S, t \models \psi$ iff $\sigma_i \leq t < \sigma_{i+1}$, $ns(\sigma_{i+1})$ and $S, \sigma_{i+1} \models \zeta$; by inductive hypothesis this holds iff $\pi, \rho_S(\sigma_{i+1}) \models_L \tau(\zeta)$, and by construction $s_p, f_p, e_p \notin \pi(\rho_S(\sigma_{i+1}))$, hence $\pi, \rho_S(\sigma_{i+1}) - 1 \models_L X_L(\tau(\zeta) \wedge ns_p)$, and by construction $\rho_S(t) + 1 = \rho_S(\sigma_{i+1})$, since it must be $t = \sigma_i$, because $\sigma_{i+1} = \sigma_i + \epsilon$.

If $\psi = X_{st}(\zeta)$, $S, t \models \psi$ iff $\sigma_i \leq t < \sigma_{i+1}$, $st(\sigma_{i+1})$ and $S, \sigma_{i+1} \models \zeta$; by inductive hypothesis this holds iff $\pi, \rho_S(\sigma_{i+1}) \models_L \tau(\zeta)$, and by construction $s_p \in \pi(\rho_S(\sigma_{i+1}))$, hence $\pi, \rho_S(\sigma_{i+1}) \models_L \tau(\zeta) \wedge s_p$. It is either $\sigma_i < t$, or $\sigma_i = t$. If $\sigma_i < t$, $f_p \in \pi(\rho_S(t))$ or $e_p \in \pi(\rho_S(t))$ and $\rho_S(\sigma_{i+1}) \geq \rho_S(t) + 1$. If $\sigma_i = t$, $f_p, e_p \notin \pi(\rho_S(t))$, and $\rho_S(\sigma_{i+1}) = \rho_S(t) + \delta(\phi) + 2$. In both cases for all $\rho_S(t) < l < \rho_S(\sigma_{i+1})$ it is $f_p \in \pi(\rho_S(t))$ or $e_p \in \pi(\rho_S(t))$, hence $\pi, \rho_S(t) \models_L X_L((f_p \vee e_p) \cup_L (s_p \wedge \tau(\zeta)))$, i.e., $\pi, \rho_S(t) \models_L \tau(\psi)$. The cases for the Y_{ns} and Y_{st} operators are similar.

$\text{Dist}(\psi, 0)$ is equivalent to ψ , hence this case is trivial.

If $\psi = \text{Dist}(\zeta, \epsilon)$, $S, t \models \psi$ iff $S, t + \epsilon \models \zeta$, which, by inductive hypothesis, holds iff $\pi, \rho_S(t + \epsilon) \models_L \tau(\zeta)$. We have two cases: $\sigma_i \leq t \leq \delta(\phi) < \sigma_{i+1}$ and $\sigma_i + \delta(\phi) < t < \sigma_{i+1}$ (hence $st(\sigma_{i+1})$). In the first case, $f_p \notin \pi(\rho_S(t))$, $\rho_S(t + \epsilon) = \rho_S(t) + 1$, hence $\pi, \rho_S(t) \models_L \neg f_p \wedge X_L(\tau(\zeta))$. In the second case, $f_p \in \pi(\rho_S(t))$, and by Lemma 3 $S, t + \epsilon \models \zeta$ iff $S, t \models \zeta$, which in turn holds iff $\pi, \rho_S(t) \models_L \tau(\zeta)$, hence $\pi, \rho_S(t) \models_L f_p \wedge \tau(\zeta)$. All in all, $\pi, \rho_S(t) \models_L \neg f_p \wedge X_L(\neg s_p \wedge \tau(\zeta)) \vee f_p \wedge \tau(\zeta)$, i.e., $\pi, \rho_S(t) \models_L \tau(\psi)$.

The case $\psi = \text{Dist}(\zeta, -\epsilon)$ is similar to the previous

one, with the addition that $S, t \models \psi$ only if $t - \epsilon \in \overline{N}_+$ (i.e., $ns(t)$) which, by inductive hypothesis, holds iff $s_p \notin \pi(\rho_S(t))$, i.e., $\pi, \rho_S(t) \models_L \neg s_p$.

If $\psi = \text{Dist}(\zeta, 1)$, $S, t \models \psi$ iff $st(t)$, $t + 1 < \bar{t}$, and $S, t + 1 \models \zeta$. It is $st(t)$ iff $s_p \in \pi(\rho_S(t))$. Also, $t + 1 < \bar{t}$ holds iff there is $\sigma_i > t + 1$, i.e., iff $\rho_S(t + 1)$ is defined, and $s_p \in \pi(\rho_S(t + 1))$. In addition, when $\rho_S(t + 1)$ is defined, $S, t + 1 \models \zeta$ iff $\pi, \rho_S(t + 1) \models_L \tau(\zeta)$, by inductive hypothesis. As $\rho_S(t + 1) > \rho_S(t)$, and there are no standard instants in between, then $\pi, \rho_S(t) \models_L s_p \wedge X_L(\neg s_p \cup_L (s_p \wedge \tau(\zeta)))$, i.e., $\pi, \rho_S(t) \models_L \tau(\psi)$. The case $\psi = \text{Dist}(\zeta, -1)$ is similar.

If $\psi = \text{Since}(\psi_1, \psi_2)$, then $S, t \models \psi$ iff there is $0 \leq t' \leq t$ s.t. $S, t' \models \psi_2$ and for all $t' < t'' \leq t$ it is $S, t'' \models \psi_1$. By inductive hypothesis we have $\pi, \rho_S(t') \models_L \tau(\psi_2)$. We have two cases: $\sigma_i \leq t' \leq \sigma_i + \delta(\phi) < \sigma_{i+1}$ for some i , or $\sigma_i + \delta(\phi) < t' < \sigma_{i+1}$. In the former case, then for all $t' < t'' \leq t$ it is also $\rho_S(t') < \rho_S(t'') \leq \rho_S(t)$, hence, by inductive hypothesis, for all $\rho_S(t') < \rho_S(t'') \leq \rho_S(t)$ it is $\pi, \rho_S(t'') \models_L \tau(\psi_1)$, hence $\pi, \rho_S(t) \models_L \tau(\psi_1) S_L \tau(\psi_2)$. In the latter case, instead, there are some $t' < t'' < \sigma_{i+1}$ hence, by Lemma 3, $S, t' \models \psi_1$, and also $\rho_S(t') = \rho_S(t'')$ and $f_p \in \pi(\rho_S(t'))$. Then, by inductive hypothesis, we have $\pi, \rho_S(t') \models_L \tau(\psi_2)$ and for all $\rho_S(t') \leq \rho_S(t'') \leq \rho_S(t)$ it is $\pi, \rho_S(t'') \models_L \tau(\psi_1)$. Then, $\pi, \rho_S(t) \models_L \tau(\psi_1) S_L (f_p \wedge \tau(\psi_1) \wedge \tau(\psi_2))$. Overall, $\pi, \rho_S(t) \models_L \tau(\psi_1) S_L \tau(\psi_2) \vee \tau(\psi_1) S_L (f_p \wedge \tau(\psi_1) \wedge \tau(\psi_2))$, i.e., $\pi, \rho_S(t) \models_L \tau(\psi)$. The case for the Until operator is similar. ■

Remark 5. As mentioned above, Lemma 3 does not hold if we relax the condition on j and allow it to be $j = \sigma_i + \delta(\phi)$. However, if we allow $\sigma_i + \delta(\phi) \leq j < k < \sigma_{i+1}$, the only cases where the proof fails are those for Y_{ns} , Y_{st} , and $\text{Dist}(\bullet, 1)$ (when $st(\sigma_i)$ and $\delta(\phi) = 0$). This suggests that, if ϕ does not include instances of operator $\text{Dist}(\bullet, -\epsilon)$ (in which case $\delta(\phi) = 0$, and, by constraint (2), no elements marked with e_p appear in π), nor instances of the Y_{ns} and Y_{st} operators, the encoding can be simplified. In fact, in this case we can use the following modified encoding τ_f (we only show the cases that differ from τ):

$$\begin{aligned} \tau_f(X_{ns}(\phi)) &= X_L(\tau_f(\phi) \wedge \neg s_p) \\ \tau_f(X_{st}(\phi)) &= X_L(s_p \wedge \tau_f(\phi)) \vee (f_p \wedge X_L(\tau_f(\phi))) \\ \tau_f(\text{Dist}(\phi, \epsilon)) &= X_L(\neg s_p \wedge \tau_f(\phi)) \vee (X_L(s_p) \wedge \tau_f(\phi)) \\ \tau_f(\text{Since}(\phi, \psi)) &= \tau_f(\phi) S_L (X_L(\neg s_p) \wedge \tau_f(\psi)) \vee \\ &\quad \tau_f(\phi) S_L (X_L(s_p) \wedge \tau_f(\phi) \wedge \tau_f(\psi)) \end{aligned}$$

Also, constraint (2) is replaced by the following formula:

$$s_p \wedge G_L \left((s_p \rightarrow X_L(f_p \vee \neg s_p)) \wedge (f_p \rightarrow (Y_L(s_p) \wedge \neg s_p \wedge X_L(s_p))) \wedge (f_p \rightarrow \bigwedge_{p \in AP} p \leftrightarrow Y_L(p)) \right)$$

As it happens with other logic formalisms, past operators allow users to obtain more succinct and intuitive formulae, paying a little price in terms of computational complexity.

Finally, from translation schema τ and Theorem 4 we can prove the following.

Theorem 6. *The satisfiability problem of the fragment of X-TRIO_N defined above is PSPACE-complete.*

Proof: First of all, we remark that the satisfiability problem of PLTLB is PSPACE-complete [14]. Then, to show the PSPACE-hardness of the satisfiability problem for X-TRIO_N we reduce the satisfiability problem of PLTLB to that of X-TRIO_N. To achieve this, given a PLTLB formula ϕ_L , we can build a corresponding X-TRIO_N formula simply by applying the following transformation: $U_L \mapsto \text{Until}$, $S_L \mapsto \text{Since}$, $X_L \mapsto \text{Dist}(\bullet, 1)$, $Y_L \mapsto \text{Dist}(\bullet, -1)$, and by including the constraint $\text{AlwF}(\neg X_{\text{ns}}(\top))$.

To show the PSPACE-completeness, it is enough to note that, given an X-TRIO_N formula ϕ , transformation τ produces an equisatisfiable PLTLB formula ϕ_L , whose size is polynomial in the size of ϕ . ■

IV. CONCLUSIONS AND FUTURE WORK

We presented a novel approach to model and analyze systems evolving through discrete steps in a generic time domain, which can be either discrete or continuous; these steps may have quite different durations, up to the point that some are negligible w.r.t. others. The language supporting our approach, X-TRIO, extends the TRIO metric temporal logic with non-standard numbers and the next-state operator X . It can be used to model many types of heterogeneous real-time systems, and to give formal semantics to many informal or semiformal notations widely adopted in the practice of industrial applications, as done for Stateflow and FMS [7], [8]. The approach could also be applied to other logic languages for real-time systems such as MTL [2].

In its full generality X-TRIO is undecidable. In this context, however, we are motivated by the need to offer users fully automated “push-button” analysis tools. We obtained such a goal by suitable restrictions in the syntax of the language and by encoding the resulting subset into the “kernel PLTLB” supported by the Zot tool (zot.googlecode.com). Theorem 1 provides a basic hint on where the obstacles to achieve decidability abide, and it also suggests a few guidelines to find new sufficient conditions that lead to other, possibly more general, decidable versions of the basic language X-TRIO.

This is the direction of our ongoing research. For instance, we are interested in macro- and micro-steps with time durations not fixed *a priori*. In particular, the assumption that every micro-step takes exactly a constant infinitesimal value ϵ is adequate for applications such as those examined so far where the effects of many micro-steps become visible only at the beginning and end of macro-steps, but a finer view could become necessary when, e.g., synchronizing several components whose micro-steps have incommensurable durations but still have to guarantee some critical properties,

say, module A must reach a stable state after a sequence of micro-steps always before module B does.

Acknowledgments. Work supported by the European Commission, Programme IDEAS-ERC, Project 227977-SMScom. We thank the anonymous reviewers for their comments.

REFERENCES

- [1] C. Ciapessoni, P. Mirandola, A. Coen-Porisini, D. Mandrioli, and A. Morzenti, “From formal models to formally-based methods: an industrial experience,” *ACM TOSEM*, vol. 8, no. 1, pp. 79–113, 1999.
- [2] R. Koymans, “Specifying real-time properties with metric temporal logic,” *Real-Time Systems*, vol. 2, no. 4, pp. 255–299, 1990.
- [3] C. A. Furia, D. Mandrioli, A. Morzenti, and M. Rossi, “Modeling time in computing: a taxonomy and a comparative survey,” *ACM CSUR*, vol. 42, no. 2, pp. 6:1–59, 2010.
- [4] J. S. Ostroff, *Temporal Logic for Real Time Systems*, ser. Adv. Soft. Dev. Series. John Wiley & Sons, 1989.
- [5] A. Gargantini, D. Mandrioli, and A. Morzenti, “Dealing with zero-time transitions in axiom systems,” *Information and Computation*, vol. 150, no. 2, pp. 119–131, 1999.
- [6] M. Pradella, A. Morzenti, and P. San Pietro, “Refining real-time system specifications through bounded model- and satisfiability-checking,” in *Proc. of ASE*, 2008, pp. 119–127.
- [7] L. Ferrucci, D. Mandrioli, A. Morzenti, and M. Rossi, “Non-null infinitesimal micro-steps: a metric temporal logic approach,” Online at <http://arxiv.org/abs/1206.0911>, 2012.
- [8] —, “Modular automated verification of flexible manufacturing systems with metric temporal logic and non-standard analysis,” in *Proc. of FMICS*, 2012, to appear.
- [9] M.-A. Esteve, J.-P. Katoen, V. Y. Nguyen, B. Postma, and Y. Yuste, “Formal correctness, safety, dependability, and performance analysis of a satellite,” in *Proc. of ICSE*, 2012, pp. 1022–1031.
- [10] A. Benveniste, T. Bourke, B. Caillaud, and M. Pouzet, “Non-standard semantics of hybrid systems modelers,” *J. of Comp. and Sys. Sci.*, vol. 78, no. 3, pp. 877 – 910, 2012.
- [11] S. Bliudze and D. Krob, “Modelling of complex systems: Systems as dataflow machines,” *F. Inf.*, vol. 91, pp. 251–274, 2009.
- [12] A. Robinson, *Non-standard analysis*. Princeton University Press, 1996.
- [13] R. Alur and T. A. Henzinger, “A really temporal logic,” *Journal of the ACM*, vol. 41, pp. 181 – 203, 1994.
- [14] P. Schnoebelen, “The complexity of temporal logic model checking,” in *Adv. in Modal Logic*, 2002, pp. 393–436.