Axioms for Real-Time Logics [1]

P.-Y. Schobbens [a] J.-F. Raskin [b,c] T.A. Henzinger [b] L. Ferier [a]

[a] *Computer Science Institute, University of Namur, Belgium*

[b] *Electrical Engineering and Computer Sciences, University of California, Berkeley, USA*

[c] *Computer Science Department, Free University of Brussels, Belgium*

Abstract

This paper presents a complete axiomatization of two decidable propositional real-time linear temporal logics: Event Clock Logic (EventClockTL) and Metric Interval Temporal Logic with past (MetricIntervalTL). The completeness proof consists of an effective proof building procedure for EventClockTL. From this result we obtain a complete axiomatization of MetricIntervalTL by providing axioms translating MITL formulae into EventClockTL formulae, the two logics being equally expressive. Our proof is structured to yield axiomatizations also for interesting fragments of these logics, such as the linear temporal logic of the real numbers (LTR).

Key words: Temporal logic, real-time, axiomatization, completeness.

1 Introduction

Many real-time systems are safety-critical, and therefore deserve to be specified with mathematical precision. To this end, real-time linear temporal logics [5] have been proposed and served as the basis of specification languages. They use real numbers for time, which has advantages for specification and compositionality. Several syntaxes are possible to deal with real time: freeze

* This work is supported in part by the ONR YIP award N00014-95-1-0520, the NSF CAREER award CCR-9501708, the NSF grant CCR-9504469, the DARPA/NASA grant NAG2-1214, the ARO MURI grant DAAH-04-96-1-0341, the Belgian National Fund for Scientific Research (FNRS), the European Commission under WGs Aspire and Fireworks, the Portuguese FCT under Praxis XXI, the Walloon region, and Belgacom.

quantification [4,12], explicit clocks in a first-order temporal logic [11,21], integration over intervals [10], and time-bounded operators [17]. We study logics with time-bounded operators, because those logics are the only ones which have, under certain restrictions, a decidable satisfiability problem [5].

The logic $\mathsf{MetricTL}_{\mathbb{R}+}$ extends the operators of temporal logic to allow the specification of time bounds on the scope of temporal operators. For example, the $\mathsf{MetricTL}_{\mathbb{R}+}$ formula $\Box(p \rightarrow \Diamond_{=1} q)$ expresses that "every p event is followed by some q event after exactly 1 time unit." It has been shown that the logic $\mathsf{MetricTL}_{\mathbb{R}+}$ is undecidable and even not recursively axiomatizable [4]. One reason for this undecidability result is the ability of $\mathsf{MetricTL}_{\mathbb{R}+}$ to specify exact distances between events; these exact distance properties are called punctuality properties. The logic $\mathsf{MetricIntervalTL}$ is obtained from $\mathsf{MetricTL}_{\mathbb{R}+}$ by removing the ability to specify punctuality properties: all bounds appearing in temporal operators must be non-singular intervals. For example, the formula $\Box(p \rightarrow \Diamond_{[1,2]} q)$, which expresses that "every p event is followed by some q event after at least 1 time unit and at most 2 time units," is a $\mathsf{MetricIntervalTL}$ formula, because the interval $[1, 2]$ is non-singular. The logic $\mathsf{MetricIntervalTL}$ is decidable [3]. This decidability result allows program verification using automatic techniques. However, when the specification is large or when it contains first-order parts, a mixture of automatic and manual proof generation is more suitable. Unfortunately, the current automatic reasoning techniques (based on timed automata) do not provide explicit proofs. Secondly, an axiomatization provides deep insights into a logic. Third, a complete axiomatization serves as a yardstick for a definition of *relative completeness* for more expressive logics (such as first-order extensions) that are not completely axiomatizable, in the style of [16,20]. This is why the axiomatization of time-bounded operator logics is cited as an important open question in [5,17].

We provide a complete axiom system for decidable real-time logics, and a proof-building procedure. We build the axiom system by considering increasingly complex logics: LTR [6], $\mathsf{EventClockTL}$ with past clocks only, $\mathsf{EventClockTL}$ with past and future clocks (also called SCL [22]), $\mathsf{MetricIntervalTL}$ [3] with past and future operators.

The method that we use to show the completeness of our axiomatization is standard: we show that it is possible to construct a model for each consistent formula. More specifically, our proof of completeness is an adaptation and an extension of the proof of completeness of the axiomatization of TL [19]. The handling of the real-time operators requires care and represents the core technical contribution of this paper. Some previous works presented axioms for real-time logics, but no true (versus relative) completeness result for dense real-time. In [12], completeness results are given for real-time logics with explicit clocks and time-bounded operators, but for time modeled by a discrete time domain, the natural numbers. In [9,7], a completeness result is presented for the qualitative (non real-time) part of the logics considered in this paper. There, the time domain considered is dense but the hypothesis of *finite variability* that we consider [1] is dropped and, as a consequence, different techniques have to be applied. In [17], axioms for real-time logics are proposed. These axioms are given for first-order extensions of our logics, but no relative completeness results are studied (note that no completeness result can be given for first-order temporal logics.) Finally, a relative completeness result is given for the duration calculus in [10]. The completeness is relative to the hypothesis that valid interval logic formulae are provable.

2 Models and logics for real-time

2.1 Models

As time domain $\mathbb{T}$, we choose the nonnegative real numbers $\mathbb{R}^{\geq 0} = \{x \in \mathbb{R} | x \geq 0\}$. This dense domain is natural and gives many advantages detailed elsewhere: compositionality [6], full abstractness [6], stuttering independence [1], easy refinement. These advantages, and the results of this paper, mainly depend on density: they can easily be adapted for the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$. To avoid Zeno's paradox, we add to our models the condition of *finite variability* [6] (condition (3) below): only finitely many state changes can occur in a finite amount of time.

An *interval* $I \subseteq \mathbb{T}$ is a convex subset of time. Given $t \in \mathbb{T}$, we freely use notations such as $t + I$ for the interval $\{t' \mid \exists t'' \in I \text{ with } t' = t + t''\}$, $t > I$ for the constraint "$t > t'$ for all $t' \in I$", $\downarrow I$ for the interval $\{t > 0 | \exists t' \in I : t \leq t'\}$. A bounded non-empty interval has an infimum (also called greatest lower bound, or left endpoint, or begin) and a supremum (also called least upper bound, or right endpoint, or end). Such an interval is thus usually written as e.g. $(l, r]$, where l is the left endpoint, the rounded parenthesis in "$(l$" indicates that l is excluded from the interval, r is the right endpoint, and the square parenthesis in "$r]$" indicates that r is included in the interval. The interval is called left-open and right-closed. If we extend the notation, as usual, by allowing r to be ∞, then any interval can be written in this form. Two intervals I and J are *adjacent* if the right endpoint of I, noted $r(I)$, is equal to the left endpoint of J, noted $l(J)$, and either I is right-open and J is left-closed or I is right-closed and J is left-open. We say that a non-empty interval I is *singular* if $l(I) = r(I)$. In this case, we often use the notation $= t$ rather than $[t, t]$. Similarly, $< l$ abbreviates $(0, l)$, etc. An *interval sequence*

[1] In every finite interval of time, the interpretation of propositions can change only finitely many times.

$\bar{I} = I_0, I_1, I_2, \ldots$ is an infinite sequence of non-empty bounded intervals so that (1) the first interval I_0 is left-closed with left endpoint 0, (2) for all $i \geq 0$, the intervals I_i and I_{i+1} are adjacent, and (3) for all $t \in \mathbb{T}$, there exists an $i \geq 0$ such that $t \in I_i$. Consequently, an interval sequence partitions time so that every bounded subset of $\mathbb{T}$ is covered by finitely many elements of the partition. Let P be a set of propositional symbols. A *state* $s \subseteq P$ is a set of propositions. A *timed state sequence* $\tau = (\bar{s}, \bar{I})$ is a pair that consists of an infinite sequence $\bar{s}$ of states and an interval sequence $\bar{I}$. Intuitively, it states the period I_i during which the state was s_i. Thus, a timed state sequence τ can be viewed as a function from $\mathbb{T}$ to 2^P, indicating for each time $t \in \mathbb{T}$ a state $\tau(t) = s_i$ where $t \in I_i$.

*2.2 The Linear Temporal Logic of Real Numbers (*LTR*)*

The formulae of LTR [6] are built from propositional symbols, boolean connectives, the temporal "until" and "since" and are generated by the following grammar:

$$\phi \ ::= \ p \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid \phi_1 \mathsf{U} \phi_2 \mid \phi_1 \mathsf{S} \phi_2$$

where p is a proposition.

The LTR formula ϕ holds at time $t \in \mathbb{T}$ of the timed state sequence τ, written $(\tau, t) \models \phi$ according to the following definition, where we omit τ:

$t \models p$ iff $p \in \tau(t)$
$t \models \phi_1 \vee \phi_2$ iff $t \models \phi_1$ or $t \models \phi_2$
$t \models \neg\phi$ iff $t \not\models \phi$
$t \models \phi_1 \mathsf{U} \phi_2$ iff $\exists t' > t \wedge t' \models \phi_2$ and $\forall t'' \in (t, t')$, $t'' \models \phi_1 \vee \phi_2$
$t \models \phi_1 \mathsf{S} \phi_2$ iff $\exists t' < t \wedge t' \models \phi_2$ and $\forall t'' \in (t', t)$, $t'' \models \phi_1 \vee \phi_2$

An LTR formula ϕ is satisfiable if there exists τ and a time t such that $(\tau, t) \models \phi$, an LTR formula ϕ is valid if for every τ and every time t we have $(\tau, t) \models \phi$.

This logic was shown to be expressively equivalent to the monadic first-order logic of the order over the reals [15].

Our operators U, S are slightly non-classical, but more intuitive: they do not require ϕ_2 to start in a left-closed interval.

On the other hand, each of them is slightly weaker than its classical variant, but together they have the same expressive power, as we show by providing mutual translations below in sections 2.2.1 and 2.4.1. It is thus a simple matter of taste. We will note the classical until as $\hat{\mathsf{U}}$.

2.2.1 Abbreviations

In the sequel we use the following abbreviations:

- $\phi_1 \hat{\mathsf{U}} \phi_2 \equiv \phi_1 \mathsf{U} (\phi_2 \wedge \ominus \phi_1)$ ($\ominus$ is defined below).
- $\phi_1 \mathsf{U}^+ \phi_2 \equiv \phi_1 \wedge \phi_1 \mathsf{U} \phi_2$, the "Until" reflexive for its first argument;
- $\phi_1 \mathsf{U}^{\geq} \phi_2 \equiv \phi_2 \vee \phi_1 \mathsf{U}^+ \phi_2$, the "Until" reflexive for its two arguments;
- $\bigcirc \phi \equiv \bot \mathsf{U} \phi$, meaning "just after in the future" or "for a short time in the future". The dual of $\bigcirc$ is noted K^+ in [9], and it means thus "arbitrarily close in the future". We don't introduce it, since we will see that due to finite variability, $\bigcirc$ is his own dual.
- $\Diamond \phi \equiv \top \mathsf{U} \phi$, meaning "eventually in the future";
- $\Box \phi \equiv \neg \Diamond \neg \phi$, meaning "always in the future";
- their reflexive counterparts: $\Diamond^{\geq}, \Box^{\geq}$;
- $\phi_1 \mathsf{W} \phi_2 \equiv \phi_1 \mathsf{U} \phi_2 \vee \Box \phi_1$, meaning "unless in the future";
- its reflexive counterparts: W^+, $\mathsf{W}^{\geq}$.

and the past counterpart of all those abbreviations:

- $\phi_1 \hat{\mathsf{S}} \phi_2 \equiv \phi_1 \mathsf{S} (\phi_2 \wedge \bigcirc \phi_1)$;
- $\phi_1 \mathsf{S}^+ \phi_2 \equiv \phi_1 \wedge \phi_1 \mathsf{S} \phi_2$, the "Since" reflexive for its first argument;
- $\phi_1 \mathsf{S}^{\leq} \phi_2 \equiv \phi_2 \vee \phi_1 \mathsf{S}^+ \phi_2$, the "Since" reflexive for its two arguments;
- $\ominus \phi \equiv \bot \mathsf{S} \phi$, meaning "just before in the past" or "arbitrarily close in the past";
- $\diamondminus \phi \equiv \top \mathsf{S} \phi$, meaning "eventually in the past";
- $\boxminus \phi \equiv \neg \diamondminus \neg \phi$, meaning "always in the past";
- their reflexive counterparts: $\diamondminus^{\leq}, \boxminus^{\leq}$;
- $\phi_1 \mathsf{Z} \phi_2 \equiv \phi_1 \mathsf{S} \phi_2 \vee \boxminus \phi_1$, meaning "unless in the past";
- its reflexive counterparts: Z^+, $\mathsf{Z}^{\leq}$.

2.3 Event-Clock Temporal Logic

The formulae of $\mathsf{EventClockTL}$ [22] are built from propositional symbols, boolean connectives, the temporal "until" and "since" operators, and two real-time operators: at any time t, the history operator $\triangleleft_I \phi$ asserts that ϕ was true last in the interval $t - I$, and the prediction operator $\triangleright_I \phi$ asserts that ϕ will be true next in the interval $t + I$. The formulae of $\mathsf{EventClockTL}$ are generated by the following grammar:

$$\phi \ ::= \ p \mid \phi_1 \vee \phi_2 \mid \neg \phi \mid \phi_1 \mathsf{U} \phi_2 \mid \phi_1 \mathsf{S} \phi_2 \mid \triangleleft_I \phi \mid \triangleright_I \phi$$

where p is a proposition and I is an interval which can be empty, singular and whose bounds are natural numbers (or infinite). The $\mathsf{EventClockTL}$ formula ϕ holds at time $t \in \mathbb{T}$ of the timed state sequence τ, written $(\tau, t) \models \phi$ according

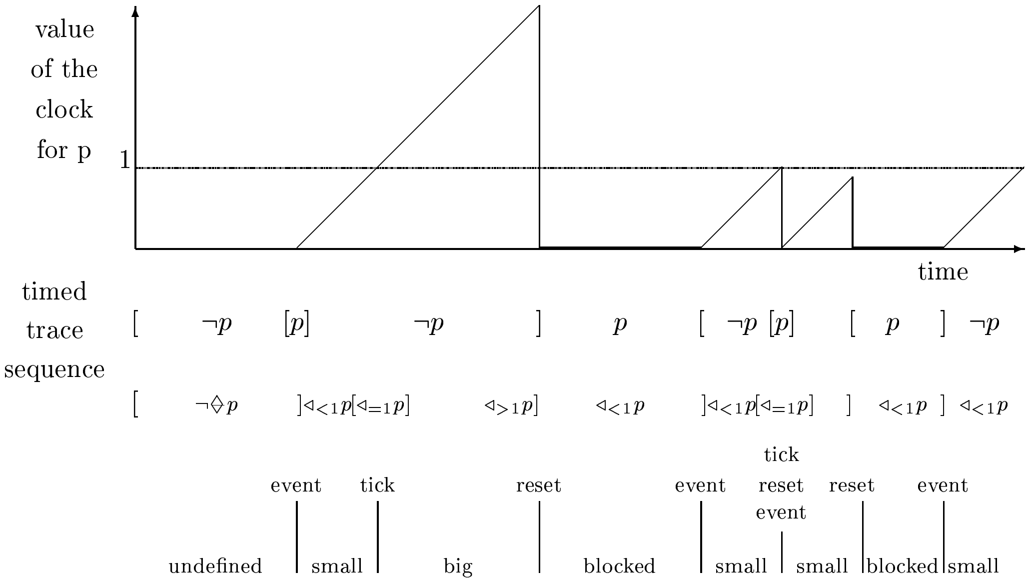

Fig. 1. A History clock evolving over time

to the rules for LTR and the following additional clauses:

$t \models \lhd_I \phi$ iff $\exists t' < t \wedge t' \in t - I \wedge t' \models \phi$ and $\forall t'' : t - I < t'' < t, t'' \not\models \phi$
$t \models \rhd_I \phi$ iff $\exists t' > t \wedge t' \in t + I \wedge t' \models \phi$ and $\forall t'' : t < t'' < t + I, t'' \not\models \phi$

A $\rhd_I \phi$ formula can intuitively be seen as expressing a constraint on the value of a clock that measures the distance from now to the next time where the formula ϕ will be true. In the sequel, we use this analogy and call this clock a *prediction clock* for ϕ. Similarly, a $\lhd_I \phi$ formula can be seen as a constraint on the value of a clock that records the distance from now to the last time such that the formula ϕ was true. We call such a clock a *history clock* for ϕ. For a history (resp. prediction) clock about ϕ,

- the next $\lhd_{=1}\phi$ (resp. previous $\rhd_{=1}\phi$) is called its *tick*;
- the point where ϕ held last (resp. will hold next) is called its *event*;
- the point (if any) at which ϕ will hold again (resp. held last) is called its *reset*;
- if ϕ is true at time t and was true just before t (resp. and will still be true just after t) then we say that the clock is *blocked* at time t;
- if ϕ was never true before t (resp. will never be true after t) then the clock is *undefined* at time t.

The main part of our axiomatization consists in describing the behavior and the relation of such clocks over time. For a more formal account on the relation between EventClockTL formulae and clocks, we refer the interested reader to [22]. We simply recall:

Theorem 1 [22] *The satisfiability problem for* EventClockTL *is complete for*

PSPACE.

which is the best result that can be expected, since any temporal logic has this complexity.

Example 1 $\Box(p \rightarrow \triangleright_{=5} p)$ asserts that after every p state, the first subsequent p state is exactly 5 units later (so in between, p is false); the formula $\Box(\triangleleft_{=5} p \rightarrow q)$ asserts that whenever the last p state is exactly 5 units ago, then q is true now (time-out).

2.4 Metric-Interval Temporal Logic

MetricIntervalTL restricts the power of MetricTLin an apparently different way from EventClockTL: here the real-time constraints are attached directly to the until, but cannot be punctual. The formulae of MetricIntervalTL [3] are built from propositional symbols, boolean connectives, and the time-bounded "until" and "since" operators:

$$\phi \ ::= \ p \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \phi_1 \hat{\mathsf{U}}_I\, \phi_2 \mid \phi_1 \hat{\mathsf{S}}_I\, \phi_2$$

where p is a proposition and I is a *nonsingular* interval whose bounds are natural numbers or infinite. The MetricIntervalTL formula ϕ holds at time $t \in \mathbb{T}$ of the timed state sequence τ, written $(\tau, t) \models \phi$ according to the following definition (the propositional and boolean clauses are as for LTR):

$$t \models \phi_1 \hat{\mathsf{U}}_I\, \phi_2 \text{ iff } \exists t' \in t + I \wedge t' \models \phi_2 \text{ and } \forall t'' : t < t'' < t', t'' \models \phi_1$$
$$t \models \phi_1 \hat{\mathsf{S}}_I\, \phi_2 \text{ iff } \exists t' \in t - I \wedge t' \models \phi_2 \text{ and } \forall t'' : t' < t'' < t, t'' \models \phi_1$$

Here, we have used the classical until to respect the original definition, but this doesn't matter as explained in subsection 2.2.1.

Theorem 2 [3] *The satisfiability problem for* MetricIntervalTL *is complete for* EXPSPACE.

So although the logics are equally expressive, their translation must be difficult enough to absorb the difference in complexity. Our translation, presented in section 5, indeed gives an exponential blowup of formulae.

2.4.1 Abbreviations

In the sequel we use the following abbreviations:

- $\phi_1 \hat{\mathsf{U}} \phi_2 \equiv \phi_1 \hat{\mathsf{U}}_{(0,\infty)} \phi_2$, the untimed "Until" of MetricIntervalTL.
- $\mathsf{C}\phi \equiv \neg\phi \hat{\mathsf{U}} \phi$ expresses that the next ϕ-interval is left-closed.

- $\phi_1 \mathsf{U}_I \phi_2 \equiv (\phi_1 \vee \phi_2) \hat{\mathsf{U}}_I \phi_2$.
- $\Diamond_I \phi \equiv \top \hat{\mathsf{U}}_I \phi$, meaning "within I";
- $\Box_I \phi \equiv \neg \Diamond_I \neg \phi$, meaning "always within I";

and the past counterpart of all those abbreviations. The fact that we use the same notations as in the other logics is intentional and harmless, since the definitions are semantically equivalent.

Furthermore, now that we have re-defined the basic operators of EventClockTL, we also use its abbreviations.

Example 2 $\Box(q \to r \hat{\mathsf{S}}_{\leq 5}\, p)$ asserts that every q state is preceded by a p state of time difference at most 5, which is right-closed, and all intermediate states are r states; the formula $\Box(p \to \Diamond_{[5,6)} p)$ asserts that every p state is followed by a p state at a time difference of at least 5 and less than 6 time units. This is weaker than the EventClockTL example, since p might also hold in between, and of course because 5 units are not exactly required.

3 Axiomatization of EventClockTL

In section 4, we will present a proof-building procedure for EventClockTL. In this section, we simply collect the axioms used in the procedure, and present their intuitive meaning. Our logics are symmetric for past and future (a duality that we call the "mirror principle"), except that time begins but does not end: therefore the axioms will be only written for the future, but with the understanding that their mirror images, obtained by replacing U by S, $\triangleright$ by $\triangleleft$, etc. are also axioms. This does not mean that we have an axiomatization of the future fragment of these logics: our axioms make past and future interact, and our proof technique makes this interaction is unavoidable, mainly in axiom (11).

3.1 Qualitative axioms (complete for LTR*)*

We use the rule of inference of replacement of equivalent formulae:

$$\frac{\phi \leftrightarrow \phi' \qquad \psi(\phi)}{\psi(\phi')} \tag{1}$$

$$\text{All propositional tautologies} \tag{2}$$

For the non-metric part, we use the following axioms and their mirror images:

$$\neg(\psi \mathsf{U} \bot) \tag{3}$$
$$\phi \mathsf{U}(\psi \wedge \psi') \rightarrow \phi \mathsf{U} \psi \tag{4}$$
$$\bigcirc(\psi \wedge \phi) \leftrightarrow \bigcirc\psi \wedge \bigcirc\phi \tag{5}$$
$$\ominus\top \rightarrow (\ominus\neg\phi \leftrightarrow \neg\ominus\phi) \tag{6}$$
$$\bigcirc(\psi \mathsf{U} \phi) \leftrightarrow \psi \mathsf{U} \phi \tag{7}$$
$$\bigcirc(\psi \mathsf{S} \phi) \leftrightarrow \bigcirc\phi \vee (\bigcirc\psi \wedge (\psi \mathsf{S}^{\leq} \phi)) \tag{8}$$
$$\psi \mathsf{U} \phi \leftrightarrow \bigcirc(\psi \mathsf{U}^{\geq} \phi) \tag{9}$$
$$\phi \mathsf{U} \psi \rightarrow \Diamond\psi \tag{10}$$
$$\Box((\psi \wedge \bigcirc\top \rightarrow \bigcirc\psi) \wedge (\ominus\psi \rightarrow \psi)) \rightarrow (\bigcirc\psi \rightarrow \Box\psi) \tag{11}$$

They mainly make use of the $\bigcirc$ operator, because as we shall see, it corresponds to the transition relation of our structure. Axiom (3) is the usual necessitation or modal generalization rule, expressed as an axiom. Similarly, (4) is the usual weakening principle, expressed in a slightly non-classical form. (5), (6) allow to distribute $\bigcirc$ with boolean operators. Note that the validity of (6) requires finite variability. (7), (8) describe how the U and S operators are transmitted over interval boundaries. (9) gives local consistency conditions over this transmission. (10) ensures eventuality when combined with (11). It can also be seen as weakening the left side of the U to $\top$. The induction axiom (11) is essential to express finite variability: If a property is transmitted over interval boundaries, then it will be true at any point; said otherwise, any point is reached by crossing finitely many interval boundaries.

The axioms below express that time begins (12) but has no end (13):

$$\diamondminus^{\leq}\neg\ominus\top \tag{12}$$
$$\bigcirc\top \tag{13}$$

We have written the other axioms so that they are independent of the begin or end axioms, in order to deal easily with other time domains (see subsection 4.4). This is why some apparently spurious $\bigcirc\top$ occur above, e.g. in (11): they are useful when the future is bounded.

Remark 3 *Theorem 21 shows that the axioms above form a complete axiomatization of the logic of the real numbers with finite variability, defined as* LTR *in [6]. The system proposed in [6] is unfortunately unsound, redundant and incomplete. Indeed, axiom F5 of [6] is unsound; axiom F7 can be deduced from axiom F8; and the system cannot derive the induction axiom* (11). *To see this last point, take the structure formed by* $\mathbb{R}^{\geq 0}$ *followed by* $\mathbb{R}$, *with finite variability: it satisfies the system of [6] (corrected according to [7]) but not the induction axiom. Thus this valid formula cannot be derived in their system.*

3.2 Quantitative axioms

For the real-time part, we first describe the static behavior; intersection, union of intervals can be translated into conjunction, disjunction due to the fact that there is a single next event:

$$\rhd_{I \cup J}\phi \leftrightarrow \rhd_I \phi \vee \rhd_J \phi \tag{14}$$
$$\rhd_{I \cap J}\phi \leftrightarrow \rhd_I \phi \wedge \rhd_J \phi \tag{15}$$

Since $\rhd$ is a strict future operator, the value 0 is never used:

$$\neg \rhd_{=0} \phi \tag{16}$$

If we do not constrain the time of next occurrence, we simply require a future occurrence:

$$\rhd_{>0}\psi \leftrightarrow \Diamond\psi \tag{17}$$

Finally the addition corresponds to nesting:

$$\rhd_{\leq m+n}\phi \leftrightarrow \rhd_{\leq m} \rhd_{\leq n} \phi \tag{18}$$
$$\rhd_{<m+n}\phi \leftrightarrow \rhd_{<m} \rhd_{\leq n} \phi \tag{19}$$

The next step of the proof is to describe how a single real-time $\rhd_I\phi$ evolves over time, using $\bigcirc$ and $\ominus$. We use (20) to reduce left-open events to the easier case of left-closed ones.

$$\neg(\mathsf{C}\phi) \rightarrow (\rhd_{[l,m)} \bigcirc \phi \leftrightarrow \rhd_{(l,m)}\phi) \tag{20}$$
$$\neg \bigcirc \rhd_{=m}\psi \tag{21}$$
$$\mathsf{C}\psi \rightarrow (\bigcirc \rhd_{<m} \psi \leftrightarrow \rhd_{\leq m}\psi) \tag{22}$$
$$\ominus \rhd_{<m} \psi \leftrightarrow ((\rhd_{<m}\psi \vee \psi \vee \ominus\psi) \wedge \ominus\top) \tag{23}$$
$$\bigcirc\psi \rightarrow \rhd_{<m}\psi \tag{24}$$

These axioms are complete for formulae where the only real-time operators are prediction operators $\rhd_I\phi$ and they all track the same (qualitative) formula ϕ. For a single history tracked formula, we use the mirror of the axioms plus an axiom expressing that the future time is infinite, so that any bound will be exceeded:

$$\psi \rightarrow (\Diamond\psi \vee \Diamond \lhd_{>m} \psi) \tag{25}$$

The description provided by these axioms are mostly expressed by the automaton of figure 2, showing the possible evolution of history predicates. This figure will receive a formal status in lemma 22. Most consequences of

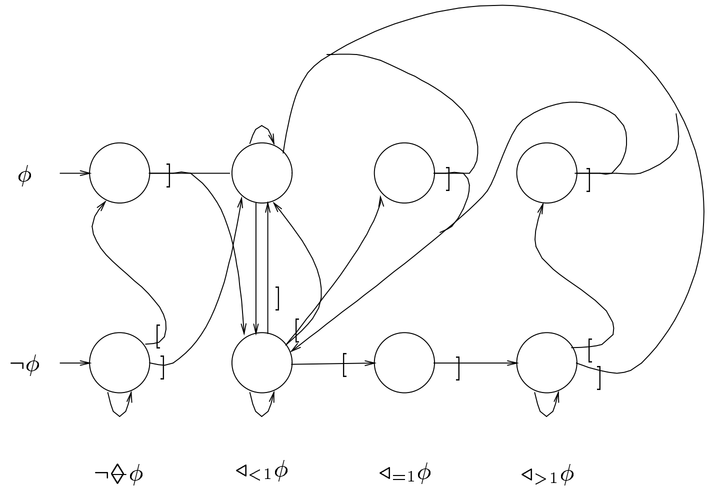

Fig. 2. The possible evolutions of a history clock

these axioms can simply be read from this automaton: For instance, $\lhd_{>1}\phi \rightarrow (\lhd_{>1}\phi \wedge \neg\phi)\mathsf{U}^{\geq} \bigcirc \lhd_{<1}\phi$ is checked by looking at paths starting from $\lhd_{>1}\phi$.

As soon as several such formulae are present, we cannot just combine their individual behavior, because the $\rhd, \lhd$ have to evolve synchronously (with the common implicit real time). We use a family of axioms (and their mirrors) to express this common speed. They express the properties of order and addition, but expressed with different clocks. Said otherwise, the ordering of the ticks should correspond to the ordering of their events. We use U (or W) to express the ordering: $\neg p\mathsf{U}q$ means that q will occur before (or at the same time as) any p. E.g. in (26), the antecedent $\lhd_{=1}\phi$ states that ϕ ticks now, thus after of together with ψ. Then their events shall be in the same order: $\neg\phi\mathsf{S}\psi$. Similarly, (30) says that if last ϕ was less than 1 ago, and ψ was even closer, than last ψ was less than 1 ago as well.

$$\lhd_{=1}\phi \rightarrow (\lhd_{\leq 1}\psi \leftrightarrow \neg\phi\mathsf{S}\psi \tag{26}$$
$$(\rhd_{<1}\psi \vee \psi) \wedge \neg\psi\mathsf{U}^{\geq}\phi \rightarrow \neg \rhd_{=1} \phi\mathsf{Z}(\rhd_{\geq 1}\psi \vee \psi) \tag{27}$$
$$(\rhd_{<1}\psi \vee \psi) \wedge \neg\psi\mathsf{U}^{\geq} \lhd_{=1} \phi \rightarrow \neg\phi\mathsf{Z} \rhd_{=1} \psi \vee \neg\phi\mathsf{Z}\psi \tag{28}$$
$$\lhd_{\leq 1}\psi \wedge \phi \rightarrow \neg \rhd_{=1} \phi\mathsf{S}\psi \tag{29}$$
$$\lhd_{<1}\phi \wedge \neg\phi\mathsf{S}\psi \rightarrow \lhd_{<1}\psi \tag{30}$$
$$\lhd_{<1}\psi \wedge \neg\psi\mathsf{S} \rhd_{=1} \phi \rightarrow \rhd_{<1}\phi \wedge \neg\phi \tag{31}$$

3.3 Theorems

We will use in the proof some derived rules of LTR (and thus $\mathsf{EventClockTL}$):

Lemma 4 *The rules of* modus ponens *and* modal generalization *are derivable.*

$$\frac{\phi \quad \phi \rightarrow \psi}{\psi} \tag{32}$$

$$\frac{\phi}{\Box\phi} \tag{33}$$

Proof.

- the rule of *modus ponens* (32) is derived from replacement (1) as follows: from ϕ we deduce propositionally $\phi \leftrightarrow \top$; by (1) we replace ϕ by $\top$ in $\phi \rightarrow \psi$ giving $\top \rightarrow \psi$ which yields propositionally ψ.
- the rule of *modal generalization* (33) (also called necessitation) is derived similarly from (1) and (3): From ϕ, we deduce $\neg\phi \leftrightarrow \bot$. Replacing in (3), we obtain $\neg(\psi \mathsf{U} \neg\phi)$. By taking $\psi := \top$, we get $\Box\phi$.

■

We'll also need some $\mathsf{EventClockTL}$ theorems:

$$\neg \bigcirc \psi \leftrightarrow \bigcirc\neg\psi \tag{34}$$

$$\bigcirc(\phi_1 \vee \phi_2) \leftrightarrow \bigcirc\phi_1 \vee \bigcirc\phi_2 \tag{35}$$

$$\ominus\psi \rightarrow \ominus\top \tag{36}$$

$$\neg \ominus \top \rightarrow (\ominus\phi \leftrightarrow \bot) \tag{37}$$

$$\bigcirc \ominus \phi \leftrightarrow \bigcirc\phi \tag{38}$$

$$\bigcirc \bigcirc \phi \leftrightarrow \bigcirc\phi \tag{39}$$

$$\Diamond\top \tag{40}$$

$$\neg \lhd_{\emptyset} \psi \tag{41}$$

$$\lhd_I\psi \rightarrow \ominus\top \tag{42}$$

$$\neg \rhd_I \phi \leftrightarrow \neg\Diamond\phi \vee \rhd_{\overline{I}}\phi \tag{43}$$

$$\rhd_I\phi \leftrightarrow \neg \rhd_{<I} \phi \wedge \rhd_{\downarrow I}\phi \tag{44}$$

$$\rhd_I\phi \rightarrow \rhd_J\phi \text{ with } (I \subseteq J) \tag{45}$$

$$\Box(\phi_1 \wedge \phi_2) \rightarrow \Box\phi_1 \tag{46}$$

Proof.

(34) By (13), we can remove the condition $\bigcirc\top$ in the mirror of (6).
(35) We use (5) and duality through (34).
(36) Expanding the definition of $\ominus$, we have to prove $\bot \mathsf{S} \phi \rightarrow \bot \mathsf{S} \top$. This results from the mirror of (4) with $\phi := \bot, \psi := \top, \psi' := \phi$.
(37) From (36). So all $\ominus$ formulae are false at the beginning of time.
(38) By (8).
(39) By (7).

(40) By (13), (10).
(41) Take (14) with $I := \emptyset$, $J := [0, 0]$. By (16) we obtain $\triangleleft_{\emptyset}\psi \leftrightarrow \bot$.
(42) We'll prove its mirror. By (14), $\triangleleft_I\psi \to \triangleleft_{>}0\psi$. By (17), $\Diamond\psi$. By (10), $\bigcirc\psi$.
(43) By (15), (14), (17).
(44) By (15), (14), (17).
(45) By (15). (or by (14)).
(46) By (4).

■

4 Completeness of the axiomatic system for EventClockTL

As usual, the soundness of the system of axioms can be proved by a simple inductive reasoning on the structure of the axioms. We concentrate here on the more difficult part: the completeness of the proposed axiomatic system. As usual with temporal logic, we only have *weak completeness*: for every valid formula of EventClockTL, there exists a finite formal derivation in our axiomatic system for that formula. So if $\models \phi$ then $\vdash \phi$. As often, it is more convenient to prove the contrapositive: every consistent EventClockTL formula is satisfiable. Due to the mirror principle, most explanations will be given for the future only.

Our proof is divided in steps, that prove the completeness for increasing fragments of EventClockTL.

(1) We first deal with the qualitative part, without real-time. This part of the proof follows roughly the completeness proof of [19] for discrete-time logic.
    (a) We work with worlds that are built syntactically, by maximal consistent sets of formulae.
    (b) We identify the transition relation, and its syntactic counterpart: it was the "next" operator for discrete-time logic [19], here it is the $\bigcirc$, expressing the transition from a closed to an open interval, and $\ominus$, expressing the transition from an open to a closed interval.
    (c) We impose axioms describing the possible transitions for each operator.
    (d) We give an induction principle (11) that extends the properties of local transitions to global properties.
(2) For the real-time part:
    (a) We give the statics of a clock;
    (b) We describe the transitions of a clock;
    (c) By further axioms, we force the clocks to evolve simultaneously. The completeness of these axioms is proved by showing that only realistic

clock evolutions are allowed by the axioms.

4.1 Qualitative part

Let us assume that the formula α is consistent and let us prove that it is satisfiable. To simplify the presentation of the proof, we use the following lemma:

Lemma 5 *Every* $\mathsf{EventClockTL}$ *formula can be rewritten into an equivalent formula of* $\mathsf{EventClockTL}_1$ *(using only the constant* 1*).*

Proof. First by the use of the theorem $\rhd_I \phi \leftrightarrow \neg \rhd_{<I} \phi \wedge \rhd_{\downarrow I} \phi$ (44), every formula $\rhd_I \phi$ with $l(I) \neq 0$ can be rewritten as a conjunction of formulae with 0-bounded intervals. Using the axioms $\rhd_{\leq m+n}\phi \leftrightarrow \rhd_{\leq m} \rhd_{\leq n} \phi$ (18) and $\rhd_{<m+n}\phi \leftrightarrow \rhd_{<m} \rhd_{\leq n} \phi$ (19) every interval can be decomposed into a nesting of operators associated with intervals of length 1. ■

In the sequel, we assume that the formula α for which we want to construct a model is in $\mathsf{EventClockTL}_1$, as allowed by lemma 5.

We now define the set $C(\alpha)$ of formulae associated with α:

- Sub: the sub-formulae of α.
- The formulae of Sub subject to a future real-time constraint: $R = \{\phi | \rhd_I \phi \in Sub\}$. We will say that a prediction clock is associated to these formulae.
- For these formulae, we will also track $\bigcirc\phi$ when the next occurrence of ϕ is left-open: this will simplify the notation. The information about ϕ will be reconstructed by axiom (20). $J = \{\bigcirc\phi | \phi \in R\}$.
- To select whether to track ϕ or $\bigcirc\phi$, we need the formulae giving the openness of next interval: $L = \{\mathsf{C}\phi | \phi \in R \cup J\}$.
- The formulae giving the current integer value of the clocks: $I = \{\rhd_{<1}\phi, \rhd_{=1}\phi, \rhd_{>1}\phi | \phi \in R \cup J\}$. Thanks to our initial transformation, we only have to consider whether the integer value is below or above 1.
- Among these, the "tick" formulae will be used in F to determine the fractional parts of the clocks: $T = \{\rhd_{=1}\phi \in I\}$.
- We also define the mirror sets. For instance, $R^- = \{\phi | \lhd_I \phi \in Sub\}$.
- The formulae giving the ordering of the fractional parts of the clocks, coded by the ordering of the ticks: $F = \{\neg\phi \mathsf{U} \psi, \neg\phi \mathsf{S} \psi | \phi, \psi \in T \cup R \cup J \cup T^- \cup R^- \cup J^-\}$.
- The eventualities: $E = \{\Diamond\phi | \psi \mathsf{U} \phi \text{ or } \psi \hat{\mathsf{U}} \phi \in Sub \cup L \cup L^-\}$
- The constant true $\top$, because $\ominus\top$ will be used in lemma 14.

We close the union of all sets above under $\neg, \bigcirc, \ominus$ to obtain the closure of α, noted $C(\alpha)$. This step preserves finiteness since we stop after adding just one of each of these operators. Theorems (39), (38) show that further addition would be semantically useless. For the past, we only have (6), (37). They also give the same result, since we only have two possible cases: if $\ominus\top$ is true, we can move all negations outside and cancel them, except perhaps one. Otherwise, we know that all $\ominus\psi$ are false by (4). In each case, at most one $\ominus$ or $\bigcirc$ and one $\neg$ are needed. We use the notational convention to identify formulas with their simplified form. For example, we write $\phi \in C(\alpha) \leftrightarrow \bigcirc\phi \in C(\alpha)$ to mean $\downarrow \phi \in C(\alpha) \leftrightarrow\downarrow (\bigcirc\phi) \in C(\alpha)$, where $\downarrow$ is the simplification operator.

Note that although we are in the qualitative part, we need already include the real-time formulae that will be used later. In this subsection they behave as simple propositions.

A propositionally consistent structure

A set of formulae $F \subset C(\alpha)$ is *complete* w.r.t. $C(\alpha)$ if for all formulae $\phi \in C(\alpha)$, either $\phi \in F$ or $\neg\phi \in F$; it is *propositionally consistent* if (i) for all formulae $\phi_1 \vee \phi_2 \in C(\alpha)$, $\phi_1 \in F$ or $\phi_2 \in F$ iff $\phi_1 \vee \phi_2 \in F$; (ii) for all formulae $\phi \in C(\alpha)$, $\phi \in F$ iff $\neg\phi \notin F$. We call such a set a *propositional atom* of $C(\alpha)$.

We define our first *structure*, which is a finite graph, $\Pi = (\Lambda, \Delta)$ where Λ is the set of all propositional atoms of $C(\alpha)$ and $\Delta \subseteq \Lambda \times \Lambda$ is the transition relation of the structure. Δ is defined by considering two sub-relations:

- $\Delta_]$ represents the transition from a right-closed to a left-open interval;
- $\Delta_[$ represents the transition from a right-open to a left-closed interval.

Let A, B be propositional atoms. We define

- $A\Delta_]B \Leftrightarrow \forall \bigcirc \phi \in C(\alpha), \bigcirc\phi \in A \leftrightarrow \phi \in B$;
- $A\Delta_[B \Leftrightarrow \forall \ominus \phi \in C(\alpha), \phi \in A \leftrightarrow \ominus\phi \in B$.

The *transition relation* Δ is the union of $\Delta_]$ and $\Delta_[$, i.e. $A\Delta B$ iff either $A\Delta_]B$ or $A\Delta_[B$.

Now we can define that the atom A is *singular* iff it contains a formula of the form $\phi \wedge \neg \bigcirc \phi$ or symmetrically $\phi \wedge \neg \ominus \phi$.

Lemma 6 *In the following, A and B are atoms:*

(1) A is singular iff it is irreflexive (i.e. $\neg A\Delta_]A$, equivalently $\neg A\Delta_[A$, also $\neg A\Delta_[A$).
(2) If $A\Delta_[B$, then A is not singular and (B is singular or $B = A$).
(3) If $B\Delta_]A$, then A is not singular and (B is singular or $B = A$).

(4) If B is singular, then there is at most one atom A such that $A\Delta_{[}B$ and a unique C such that $B\Delta_{]}C$.

A is *initial* iff it contains $\neg \ominus \top$. It is then singular, since it contains $\top \wedge \neg \ominus \top$. A is *monitored* iff it contains α, the formula of which we check floating satisfiability.

Any atom A is exactly represented by the conjunction of the formulae that it contains, written $\hat{A}$. By propositional completeness, we have:

Lemma 7 $\vdash \bigvee_{A \in \Lambda} \hat{A}$.

For any relation Δ, we define the formula $\Delta(A)$ to be $\bigvee_{B|A\Delta B} \hat{B}$. The formula $\bigvee_{B|A\Delta_{]}B} \hat{B}$ can be simplified to $\bigwedge_{\bigcirc\phi \in A} \phi \wedge \bigwedge_{\neg\bigcirc\phi \in A} \neg\phi$, because in the propositional structure, all other members of a B are allowed to vary freely and thus cancel each other by the distribution rule.

Lemma 8 $\vdash \hat{A} \wedge \bigcirc\top \to \bigcirc\Delta_{]}(A)$.

Proof. $\bigcirc\Delta_{]}(A) = \bigcirc \bigvee_{B|A\Delta_{]}B} \hat{B} = \bigcirc(\bigwedge_{\bigcirc\phi\in A} \phi \wedge \bigwedge_{\neg\bigcirc\phi\in A} \neg\phi) = \bigwedge_{\bigcirc\phi\in A} \bigcirc\phi \wedge \bigwedge_{\neg\bigcirc\phi\in A} \neg \bigcirc \phi$ by (5), (34). ■

Dually, $\bigvee_{B|A\Delta_{[}B} \hat{B}$ can be simplified to $\bigwedge_{\phi\in A} \ominus\phi$. Therefore:

Lemma 9 $\vdash \ominus\hat{A} \to \Delta_{[}(A)$.

Now let Δ^+ be the transitive closure of Δ. Since $\Delta_{[} \subseteq \Delta^+$, we have:

Lemma 10 $\vdash \ominus\hat{A} \to \Delta^+(A)$.

Similarly,

Lemma 11 $\vdash \hat{A} \wedge \bigcirc\top \to \bigcirc\Delta^+(A)$.

Using the disjunction rule for each reachable $\hat{A}$, we obtain: $\vdash \Delta^+(A) \wedge \bigcirc\top \to \bigcirc\Delta^+(A)$ and $\vdash \ominus\Delta^+(A) \to \Delta^+(A)$. Now we can use the induction axiom (11) provided by finite variability, i.e. $\Box((\psi \wedge \bigcirc\top \to \bigcirc\psi) \wedge (\ominus\psi \to \psi)) \to (\bigcirc\psi \to \Box\psi)$. Using necessitation (33) and modus ponens (32), we obtain:

Lemma 12 $\vdash \hat{A} \to \Box\Delta^+(A)$.

An EventClockTL*-consistent structure*

We say that an atom A is EventClockTL-*consistent* if it is propositionally consistent and consistent with the axioms and rules given in section 3. Now, we consider the structure $\hat{\Pi} = (\hat{\Lambda}, \hat{\Delta})$, where $\hat{\Lambda}$ is the subset of propositional atoms that are EventClockTL-consistent and $\hat{\Delta} = \{(A, B) | A\Delta B \text{ and } A, B \in \hat{\Lambda}\}$. Note that the lemmas above are still valid in the structure $\hat{\Pi}$ as only inconsistent atoms are suppressed. We now investigate more deeply the properties of the structure $\hat{\Pi}$ and show how we can prove from that structure that the consistent formula α is satisfiable.

We first have to define some notions.

- A *maximal strongly connected substructure* (MSCS) Ω is a non-empty set of atoms $\Omega \subseteq \hat{\Lambda}$ of the structure $\hat{\Pi}$ such that:
  (1) for all $D_1, D_2 \in \Omega$, $D_1 \hat{\Delta}^+ D_2$, i.e. every atom can reach all atoms of Ω, i.e., Ω is strongly connected;
  (2) for all $D_1, D_2 \in \hat{\Lambda}$ such that $D_1 \hat{\Delta}^+ D_2$ and $D_2 \in \hat{\Delta}^+ D_1$ and $D_1 \in \Omega$ then $D_2 \in \Omega$, i.e., Ω is maximal.
- A MSCS Ω is called *initial* if for all $D_1 \hat{\Delta} D_2$ and $D_2 \in \Omega$ then $D_1 \in \Omega$, i.e. Ω has no incoming edges.
- A MSCS Ω is called *final* if for all $D_1 \hat{\Delta} D_2$ and $D_1 \in \Omega$ then $D_2 \in \Omega$, i.e. Ω has no outgoing edges.
- A MSCS Ω is called *self-fulfilling* if for every formula of the form $\phi_1 \mathsf{U} \phi_2 \in A$ with $A \in \Omega$, there exists $B \in \Omega$ such that $\phi_2 \in B$.

We now establish two properties of MSCS of our structure $\hat{\Pi}$.

Lemma 13 *Every final MSCS Ω of the structure $\hat{\Pi}$ is self-fulfilling.*

Proof. Let us make the hypothesis that there exists $\phi_1 \mathsf{U} \phi_2 \in A$ with $A \in \Omega$ and for all $B \in D$, $\phi_2 \notin B$. By lemma 12 and as by hypothesis $\phi_2 \notin B$, for all $B \in \hat{\Delta}^+(A)$, by theorem (46) and a propositional reasoning, we conclude $\vdash \hat{A} \rightarrow \Box\neg\phi_2$. Using the axiom (10) and the hypothesis that $\phi_1 \mathsf{U} \phi_2 \in A$, we obtain $\vdash \hat{A} \rightarrow \Diamond\phi_2$ and by definition of $\Diamond$, we obtain $\vdash \hat{A} \rightarrow \neg\Box\neg\phi_2$ in contradiction with $\vdash \hat{A} \rightarrow \Box\neg\phi_2$ which is impossible since A is, by hypothesis, consistent. ■

Lemma 14 *Every non-empty initial MSCS Ω of the structure $\hat{\Pi}$ contains an initial atom, i.e. there exists $A \in \Omega$ such that $\ominus\top \notin A$.*

Proof. By definition of initial MSCS, we know that for all $D_1 \hat{\Delta} D_2$ and $D_2 \in \Omega$, then $D_1 \in \Omega$. Let us make the hypothesis that for all $A \in \Omega$, $\ominus\top \in A$. By the mirror of lemma 12 we conclude, by a propositional reasoning and the hypothesis that $\ominus\top \in D$ for all D such that $D\hat{\Delta}^+ A$, that $\vdash \hat{A} \rightarrow \boxminus \ominus \top$. This contradicts axiom (12), so $A \notin \hat{\Pi}$, thus Ω is empty. ■ Actually such initial MSCS are made of a single initial atom.

In the sequel, we concentrate on particular paths, called runs, of the structure $\hat{\Pi}$. A *run* of the structure $\hat{\Pi} = (\hat{\Lambda}, \hat{\Delta})$ is a pair $\rho = (\bar{A}, \bar{I})$ where $\bar{A} = A_0 A_1 \ldots (A_n \ldots A_{n+m})^\omega$ is an infinite sequence of atoms and $\bar{I} = I_0 I_1 \ldots I_n \ldots$ is an infinite sequence of intervals such that:

(1) Initiality: A_0 is an initial atom;
(2) Consecution: for every $i \geq 0$, $A_i \hat{\Delta} A_{i+1}$;
(3) Singularity: for every $i \geq 0$, if A_i is a singular atom then I_i is singular;
(4) Alternation: $I_0 I_1 \ldots I_n \ldots$ alternates between singular and open intervals, i.e. for all $i > 0$, I_{2i} is singular and I_{2i+1} is open.
(5) Eventuality: the set $\{A_n, ..., A_{n+m}\}$ is a final MSCS.

Note that, for the moment, the timing information provided in $\bar{I}$ is purely qualitative (singular or open); therefore any alternating sequence is adequate at this qualitative stage. Later, we will construct a specific sequence satisfying also the real-time constraints. In the sequel, given $\rho = (\bar{A}, \bar{I})$, $\rho(t)$ denotes the atom A_i such that $t \in I_i$.

Lemma 15 *The transition relation $\hat{\Delta}$ of the structure $\hat{\Pi}$ is total, i.e. for all atoms $A \in \hat{\Lambda}$, there exists an atom $B \in \hat{\Lambda}$ such that $A \hat{\Delta} B$.*

Proof. We prove $\hat{\Delta}_]$ total, i.e. for all $A \in \hat{\Lambda}, \Phi = \{\phi | \bigcirc\phi \in A\} \cup \{\neg\phi | \neg\bigcirc\phi \in A\}$ is consistent and can thus be completed to form an atom B. Assume it is not: by definition $\vdash \neg\hat{\Phi}$, i.e. $\vdash \neg\hat{\Phi} \leftrightarrow \top$. We can replace $\top$ in (13), giving $\vdash \bigcirc\neg\hat{\Phi}$. By (34), $\vdash \neg \bigcirc \hat{\Phi}$. By (5), the set $\{\bigcirc\phi | \bigcirc \phi \in A\} \cup \{\bigcirc\neg\phi | \neg \bigcirc \phi \in A\}$ is inconsistent. Using (34) again, the set $\{\bigcirc\phi | \bigcirc\phi \in A\} \cup \{\neg\bigcirc\phi | \neg\bigcirc\phi \in A\} \subseteq A$ is inconsistent, and thus A is inconsistent, contradicting $A \in \hat{\Lambda}$. ■

Lemma 16 *For every atom A of the structure $\hat{\Pi}$, there is a run ρ that passes through A.*

Proof.

(1) *Initiality*, i.e. every atom of $\hat{\Pi}$ is either initial or can be reached by an initial atom. Let us consider an atom A, if A is initial then we are done, otherwise, let us make the hypothesis that it can not be reached by an initial atom, it means: for all $B \hat{\Delta}^+ A$ then $\neg \ominus \top \notin B$, so by propositional completeness $\ominus\top \in B$. By lemma 12 and a propositional reasoning, we obtain $\vdash \hat{A} \rightarrow \boxminus \ominus \top$. Using axiom (12) we obtain a contradiction in A. We use this path for the first part of the run.
(2) *Consecution*, by construction.
(3) *Singularity*: i.e., every odd atom is not singular. For the first and second part of the run, we can obtain this by taking a simple path (thus without

self-loops). Since the first atom A_0 is initial, it is singular; from there on, non-singular and singular states will alternate by lemma 6. For the final repetition, this technique might not work when the MSCS is a single atom. Then we know that this single atom is non-singular, and thus Singularity is also verified.

(4) *Alternation*: we can choose any alternating interval sequence, since the timing information is irrelevant at this point.

(5) *Eventuality*, i.e. every atom of $\hat{\Pi}$ can reach one of the final MSCS of $\hat{\Pi}$. It is a direct consequence of the fact that $\hat{\Delta}$ is total and the fact that $\hat{\Pi}$ is finite. We use this reaching path for the second part of the run, then an infinite repetition of this final MSCS.

■

A run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$ *has the qualitative Hintikka property* if it respects the semantics of the qualitative temporal operators which is expressed by the following conditions (real-time operators will be treated in the following section):

H1 if A_i is singular then I_i is singular;

H2 $\phi_1 \mathsf{U} \phi_2 \in A_i$ iff
- · **either** I_i is singular and there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i < k < j$, $\phi_1 \in A_k$;
- · **or** I_i is not singular and
  (1) **either** $\phi_2 \in A_i, i = j$
  (2) **or** there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i \leq k < j$, $\phi_1 \in A_k$;

H3 if $\phi_1 \mathsf{S} \phi_2 \in A_i$ iff
- · **either** I_i is singular and there exists $j < i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $j < k < i$, $\phi_1 \in A_k$;
- · **or** I_i is not singular and
  (1) **either** $\phi_2 \in A_i, i = j$
  (2) **or** there exists $j < i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $j < k \leq i$, $\phi_1 \in A_k$;

We call such a run a *qualitative Hintikka run*. Next, we show properties of some additional properties of runs related to the Hintikka properties above:

Lemma 17 *For every run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$, with $\bar{A} = A_0 A_1 \ldots$, for every $i \geq 0$ such that $\Diamond \phi \in A_i$:*

- **either** *I_i is singular and there exists $j > i$ such that $\phi \in A_j$;*
- **or** *I_i is non-singular and there exists $j \geq i$ such that $\phi \in A_j$.*

Proof. First let us prove the following properties of the transition relation $\hat{\Delta}$:

- let $A \hat{\Delta}_] B$ and $\Diamond \phi \in A$ then either $\phi \in B$ or $\Diamond \phi \in B$. Recall that $\Diamond \phi \equiv \top \mathsf{U} \phi$, and by definition of $\hat{\Delta}_]$, axiom (9) and a propositional reasoning, we obtain that $\Diamond\phi \in A$ iff $\phi \in B$ or $\Diamond\phi \in B$;

- let $A\hat{\Delta}_{[}B$ and $\Diamond\phi \in A$ then either $\phi \in A$, $\phi \in B$ or $\top\mathsf{U}\phi \in B$. By definition of $\hat{\Delta}_{[}$, the mirror of axiom (8) and a propositional reasoning, we obtain $\phi \in A$ or $\phi \in B$ or $\Diamond\phi \in B$.

By the two properties above, we have that if $\Diamond\phi \in A_i$ then either ϕ appears in A_j with $j > i$ if I_i is singular (and thus right closed), $j \geq i$ if I_i is not singular (and thus an open interval) or ϕ is never true and $\Diamond\phi$ propagates for the rest of the run. But this last possibility is excluded by our definition of run: by clause (5), every run eventually loops into a final (thus self-fulfilling by lemma 13) MSCS Ω. Then either ϕ is realized before this looping or $\Diamond\phi \in \Omega$ and by lemma 13 $\phi \in \Omega$ and is thus eventually realized. ■

Lemma 18 *For every run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$, for every position i in the run if $\phi_1\mathsf{U}\phi_2 \in A_i$ then the right implication of property H2 is verified, i.e:*

- **either** *A_i is singular and there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i < k < j$, $\phi_1 \in A_k$;*
- *or A_i is not singular and*

(1) **either** *$\phi_2 \in A_j, j = i$*

(2) **or** *there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i \leq k < j$, $\phi_1 \in A_k$.*

Proof. By hypothesis we know that $\phi_1\mathsf{U}\phi_2 \in A_i$ and we first treat the case where A_i is singular.

- By the axiom (10) and lemma 17, we know that there exists $j > i$ such that $\phi_2 \in A_j$. Let us make the hypothesis that A_j is the first ϕ_2-atom after A_i.
- It remains us to show that: for all k s.t. $i < k < j$, $\phi_1 \in A_k$. We reason by induction on the value of k.
  - Base case: $k = i+1$. By hypothesis we have $\phi_1\mathsf{U}\phi_2 \in A_i$ and also $A_i\hat{\Delta}_{]}A_{i+1}$ (as A_i is right closed) and thus for all $\bigcirc\phi \in A_i, \phi \in A_{i+1}$ by definition of $\hat{\Delta}_{]}$. By axiom (7), we conclude that $\phi_1\mathsf{U}\phi_2 \in A_{i+1}$ and by axiom (9), theorem (35) and axiom (5), and the fact that by hypothesis $\phi_2 \notin A_{i+1}$, (Prop) allows us to conclude that $\phi_1 \in A_{i+1}$.
  - Induction case: $k = i + l$ with $1 < l < j - i$. By induction hypothesis, we know that $\phi_1 \in A_{k-1}$ and $\phi_1\mathsf{U}\phi_2 \in A_{k-1}$, also $\neg\phi_2 \in A_k$ and $\neg\phi_2 \in A_{k-1}$ as $k < j$ (by hypothesis j is the first position after i where ϕ_2 is verified). To establish the result, we reason by cases :
    1. I_k is open and thus I_{k-1} is singular and right closed. We have $A_{k-1}\hat{\Delta}_{]}A_k$, and thus for all $\bigcirc\phi \in C(\alpha), \bigcirc\phi \in A_i \leftrightarrow \phi \in A_{i+1}$ by definition of $\hat{\Delta}_{]}$. As $\phi_1\mathsf{U}\phi_2 \in A_{k-1}$ by induction hypothesis and the axiom (7) we conclude that $\phi_1\mathsf{U}\phi_2 \in A_k$. Using the axiom (9), theorem (35), axiom (5) and the fact that $\phi_2 \notin A_k$, and (Prop), we conclude that $\phi_1 \in A_k$.
    2. I_k is closed which implies that I_{k-1} is right open and $A_{k-1}\hat{\Delta}_{[}A_k$. By

definition of $\hat{\Delta}_{[}$ we have that for all $\ominus\phi \in C(\alpha), \ominus\phi \in A_k \leftrightarrow \phi \in A_{k-1}$. So we have $\ominus(\phi_1 \mathsf{U} \phi_2), \ominus\neg\phi_2 \in A_k$, by hypothesis $k < j$ thus we have $\neg\phi_2 \in A_k$. Using those properties and the mirror of axiom (8) we conclude that $\phi_1 \wedge \phi_1 \mathsf{U} \phi_2 \in A_k$.

We now have to treat the case where A_i is not singular. By the axiom (10) and lemma 17 we know that there exists a later atom A_j, i.e. $j \geq i$, such that $\phi_2 \in A_j$. If $j = i$ then $\phi_2 \in A_i$ and we are done. Otherwise $j > i$, and we must prove that for all k s.t. $i \leq k < j$, $\phi_1 \in A_k$, this can be done by the reasoning above. ■

We now prove the reverse, i.e. every time that $\phi_1 \mathsf{U} \phi_2$ is verified in an atom along the run then $\phi_1 \mathsf{U} \phi_2$ appears in that atom. This lemma is not necessary for qualitative completeness but we use this property in the lemmas over real-time operators.

Lemma 19 *For every run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$, for every position $i \geq 0$, for every $\phi_1 \mathsf{U} \phi_2 \in C(\alpha)$,* **if** *:*

- **either** *A_i is singular and there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i < k < j$, $\phi_1 \in A_k$;*
- **or** *A_i is not singular and*

(1) **either** *$\phi_2 \in A_j, j = i$*
(2) **or** *there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i \leq k < j$, $\phi_1 \in A_k$.*

then *$\phi_1 \mathsf{U} \phi_2 \in A_i$.*

Proof. We reason by considering the three following mutually exclusive cases:

(1) A_i is singular and there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i < k < j$, $\phi_1 \in A_k$. We reason by induction to show that $\phi_1 \mathsf{U} \phi_2 \in A_{j-l}$ for all l s.t. $1 \leq l \leq j - i$.
  - Base case: $l = 1$. By hypothesis, we know that $\phi_2 \in A_j$. We now reason by cases:
    (a) if A_{j-1} is right closed then we have $A_{j-1} \hat{\Delta}_{]} A_j$ and by definition of $\hat{\Delta}_{]}$, $\bigcirc\phi_2 \in A_{j-1}$. Using the axiom (9) we deduce by (Prop) that $\phi_1 \mathsf{U} \phi_2 \in A_{j-1}$.
    (b) if A_{j-1} is right open then we know that $j - 1 > i$ (as I_i is singular by hypothesis) and thus $\phi_1 \in A_{j-1}$. Also as $A_{j-1} \hat{\Delta}_{[} A_j$, $\ominus\phi_1 \in A_j$. Using the mirror of axiom (8) and a propositional reasoning, we obtain $\ominus(\phi_1 \mathsf{U} \phi_2) \in A_j$ and by definition of $\hat{\Delta}_{[}$, $\phi_1 \mathsf{U} \phi_2 \in A_{j-1}$.
  - Induction case: $1 \leq l < i - j - 1$ and we have established the result for $l - 1$, i.e. $\phi_1 \mathsf{U} \phi_2 \in A_{j-(l-1)}$. Let us show that we have the result for A_{j-l}. First note that by hypothesis, $\phi_1 \in A_{j-(l-1)}$. We again reason by cases:

(a) I_{j-l} is right closed. Then we have $A_{j-l}\hat{\Delta}_{]}A_{j-(l-1)}$ and by definition of $\hat{\Delta}_{]}$, for all $\bigcirc\phi \in C(\alpha)$, $\bigcirc\phi \in A_{j-l}$ iff $\phi \in A_{j-(l-1)}$,thus $\bigcirc(\phi_1 \mathsf{U} \phi_2) \in A_{j-l}$ and by axiom (7) we have that $\phi_1 \mathsf{U} \phi_2 \in A_{j-l}$.

(b) A_{j-l} is right open. Then we have $A_{j-l}\hat{\Delta}_{[}A_{j-(l-1)}$ and by definition of $\hat{\Delta}_{[}$, for all $\ominus\phi \in C(\alpha)$, $\ominus\phi \in A_{j-(l-1)}$ iff $\phi \in A_{j-l}$. We know that by hypothesis, $\phi_1 \in A_{j-l}$ as $j-l \neq i$ (I_i is singular and I_{j-l} not), thus $\ominus\phi_1 \in A_{j-(l-1)}$, also $\phi_1 \mathsf{U} \phi_2 \in A_{j-(l-1)}$ (by induction hypothesis). Using the mirror of axiom (8) and a propositional reasoning, we obtain $\ominus(\phi_1 \mathsf{U} \phi_2) \in A_{j-(l-1)}$ and by definition of $\hat{\Delta}_{[}$ that $\phi_1 \mathsf{U} \phi_2 \in A_{j-l}$.

(2) A_i is not singular and $\phi_2 \in A_j$. As A_i is not singular, we have $A_i\hat{\Delta}_{]}A_i$, by definition of $\hat{\Delta}_{]}$, we have $\bigcirc\phi_2 \in A_i$. By the axiom (9) and a proposition reasoning, we obtain the desired result: $\phi_1 \mathsf{U} \phi_2 \in A_i$.

(3) A_i is not singular, $\phi_2 \notin A_j$, and there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i \leq k < j$, $\phi_1 \in A_k$. This case is treated by an inductive reasoning similar to the first one above.

■

We have also the two corresponding mirror lemmas for the S-operator.

From the previous proved lemmas, it can be shown that the qualitative axioms of section 3 are complete for the qualitative fragment of $\mathsf{EventClockTL}$, i.e. the logic LTR.

Lemma 20 *A run ρ has the Hintikka property for* LTR *formulae: for every* LTR *formula $\phi \in C(\alpha), \phi \in \rho(t) \leftrightarrow (\rho, t) \models \phi$.*

Proof. The Hintikka property was proved in the lemmas above, but expressed without reference to time t. It remains to prove that this implies the usual definition, by induction on formulae.

(1) Let $t \in I_i$. We must prove $\exists t' > t \wedge t' \models \phi_2$ and $\forall t'' \in (t, t')$, $t'' \models \phi_1 \vee \phi_2$ from H2. Of course, we take t' somewhere in I_j, so that $t' \models \phi_2$.
   (t, t') can be divided in 3 parts: the part in I_i, which is empty when I_i is singular, the part in some I_k ($i < k < j$), the part in I_j. Each of them satisfies $\phi_1 \vee \phi_2$.

(2) Conversely, the usual definition implies H2: First note that given t, if $A_i = \rho(t)$ is not singular but I_i is singular, it means that $A_{i+1} = A_i$ by lemma 6. Thus we can merge I_i, I_{i+1} to ensure that I_i is singular iff A_i is singular without loss of generality. Let j be the first index where ϕ_2, $j > i$ if I_i is singular, or else $j \geq i$. We can take $t' > t$ in I_j without loss of generality. Since we need $t'' \models \phi_1 \vee \phi_2$, all intermediate intervals must satisfy ϕ_1.

(H3) is symmetric. ■

Finally, we have the following theorem that expresses the completeness of the qualitative axioms for the logic LTR:

Theorem 21 *Every* LTR *formula that is consistent with the qualitative axioms is satisfiable.*

Proof. Let α be a consistent LTR formula. We construct $\hat{\Pi}^\alpha = (\hat{\Lambda}, \hat{\Delta})$. Let $B \in \hat{\Lambda}$ be an atom of the structure such that $\alpha \in \hat{\Lambda}$. Such an atom B exists as α is consistent. By lemma 16, there exists a run $\rho = (\bar{A}, \bar{I})$ such that $B = A_i$ for some $i \geq 0$. By lemma 20, we have $(\rho, t) \models \alpha$ for all $t \in I_i$ and thus α is satisfiable. ■

We now turn to the completeness of real-time axioms.

4.2 Quantitative part

A run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$ has the *timed Hintikka property* if it respects the Hintikka properties defined previously and the two following additional properties:

H4 $\triangleright_I \phi \in \rho(t)$ iff there exists $t' \in t{+}I$ such that $\phi \in \rho(t')$ and $\forall t'' : t < t'' < t{+}I$, $\neg\phi \in \rho(t'')$
H5 $\triangleleft_I \phi \in \rho(t)$ iff there exists $t' \in t{-}I$ such that $\phi \in \rho(t')$ and $\forall t'' : t > t'' > t{-}I$, $\neg\phi \in \rho(t'')$

A run that respects those additional properties is called a *well-timed run*. In the sequel, we will show that for each run of the structure $\hat{\Pi}$, we can modify its sequence of intervals, using a procedure, in such a way that the modified run is well-timed.

Recall that given a tracked formula $\phi \in R$,

- $\triangleright_{=1}\phi$ is called its *tick*;
- $(\phi \wedge \bigcirc\neg\phi) \vee (\neg\phi \wedge \ominus\phi)$ is called its *event* (note that the second case need not be considered thanks to the axioms (20), (22));
- $(\phi \wedge \ominus\neg\phi) \vee (\neg\phi \wedge \bigcirc\phi)$ is called its *reset*.

The evolution of the real-time predicates is described by figure 2. We can now see the status of this drawing:

Lemma 22 *For any tracked formula $\phi \in R$, the projection of $\hat{\Pi}$ (restricted to atoms containing the formulae $\mathsf{C}\phi$) on $\phi, \triangleleft_{<1}\phi, \triangleleft_{=1}\phi, \triangleleft_{>1}\phi, \diamondsuit\phi$ is contained in figure 2.*

Proof. It suffices to show that no further consistent atoms nor transitions can be added to the figure.

- Atoms: from the axioms (15), (17), (14), (16).
- Transitions: We simply take all missing arrows of the figure, and show that they cannot exist. As the proof is fairly long, we only show some excerpts.

(1) Assume that an atom A containing $\phi, \lhd_{=1}\phi$ is linked to an atom B containing $\neg\phi, \lhd_{>1}\phi$ in this way: $A\hat{\Delta}_{]}B$. Since $\lhd_{>1}\phi \in B$, by axioms (14), (15), (16), we have $\neg \lhd_{<1} \phi \in B$. Now by definition of $\hat{\Delta}_{]}$, $\bigcirc\neg \lhd_{<1} \phi \in A$, and by (34), $\neg \bigcirc \lhd_{<1}\phi \in A$. Now the main step: we use the mirror of (23), negated on both sides. $\neg \bigcirc \top$ is impossible by (13), and thus we can conclude $\neg\phi \in A$ contradicting $\phi \in A$.

(2) Now we show the only two transitions which are eliminated by the restriction to $\mathsf{C}\phi$. The first one is $A\hat{\Delta}_{]}B$ where A contains $\lhd_{<1}\phi, \neg\phi, \mathsf{C}\phi$ and B contains $\lhd_{<1}\phi, \phi$. We prove $\mathsf{C}\phi \to \neg \bigcirc \phi$ using (9). In more detail, $\mathsf{C}\phi$ abbreviates $\neg\phi\mathsf{U}(\phi \wedge \ominus\neg\phi)$. Applying (9) and unfolding $\mathsf{U}^{\geq}$, we obtain using (35): $\bigcirc(\phi \wedge \ominus\neg\phi) \vee \bigcirc(\neg\phi \wedge \dots)$. The first disjunct is impossible, by (5), (34), (38).

On the other hand, by definition of $\hat{\Delta}_{]}$, $\bigcirc\phi \in A$, whence the contradiction.

(3) The second transition eliminated is $A\hat{\Delta}_{]}B$ where A contains $\lhd_{>1}\phi, \neg\phi, \mathsf{C}\phi$ and B contains $\lhd_{<1}\phi, \neg\phi$. By definition of $\hat{\Delta}_{]}$, $\bigcirc \lhd_{<1} \phi \in A$. By axiom (22), $\lhd_{\leq 1}\phi \in A$, contradicting $\lhd_{>1}\phi \in A$.

■

A *constraint* is a real-time formula of an atom A_i. The *begin* of a constraint is the index e at which its previous event, tick or reset occurred. The *end* of a constraint is the index j at which its next event, tick or reset occurs. This vocabulary refers to the order of time only: the begin is always before the corresponding end, whether for history or prediction operators. Begins, ends, ticks, resets, events are always singular. We say that (the history clock of) ϕ is *active* between an event ϕ and the next reset of ϕ. It is *small* between its event and the next tick or reset. After this, it is *big*. When it is big, it doesn't give actual constraints, since it can stay big for any time, on one hand, and on the other hand because it has passed first through a tick, which is forced to be 1 time unit apart from the event. Thus the monotonicity of time will ensure that big constraints are indeed semantically true. We define the *scope* of a constraint as the interval between the event and the next tick or reset, or equivalently between its begin and its end. The same vocabulary applies symmetrically for prediction operators. Actual constraints are either equalities (the time spend in their scope must be 1), linking an event to a tick, or inequalities (the time spend in their scope must be less than 1). An inequality is always linked to a small clock. Constraints can be partially ordered by scope: it is enough to solve constraints of maximal scope, as we shall see. A constraint of maximal scope always owns indexes: they are found at the end of its scope. The scope of an inequality extends from an event to a reset. Whether an atom A_i is in the scope of a constraint, and which, can be deduced from its contents. The table below shows the contents of an atom A_i that is the end of an equality. We distinguish the prediction and history cases. The table is simplified by the fact that we can assume that events are closed. The begin atom is the closest one in the past to contain the indicated formulae.

Table 1
Equality constraints – ticking clocks

begin	end in A_i
ϕ (event)	$\lhd_{=1}\phi$ (tick)
$\rhd_{=1}\phi$ (tick)	$\phi, \neg\phi \mathsf{S} \rhd_{=1} \phi$ (event)

The table below shows the contents of an atom A_i indicating that the clock is small. It is thus in the scope of a constraint, whose begin is before and whose end is after. The begin (resp. end) is the closest atoms with the indicated contents.

Table 2
Small clocks

begin	in A_i	end
$\rhd_{=1}\phi$ (tick)	$\rhd_{<1}\phi, \neg\phi\mathsf{S}^{+} \rhd_{=1} \phi$	ϕ (event)
ϕ (event)	$\lhd_{<1}\phi, \neg\phi\hat{\mathsf{S}}\phi$	$\lhd_{=1}\phi \vee \phi \vee \bigcirc\phi$ (tick or reset)
$\phi \vee \ominus\phi$ (reset)	$\neg \rhd_{=1} \phi\mathsf{S}\phi, \neg(\neg\phi\mathsf{S} \rhd_{=1} \phi), (\rhd_{<1}\phi \vee (\phi \wedge \ominus\neg\phi)$	ϕ (event)

Note that the existence of the begin and ends is guaranteed by fig. 2: a clock cannot stay small forever. In this section, we furthermore enforce that it will not stay small more than 1 unit of time.

The proof shows that these constraints can be solved iff they are compatible in the sense that the scope of an equality cannot be included in the scope of an inequality, nor strictly in the scope of another equality. The axioms for several clocks ensure this compatibility.

The previous section has built a run $\rho = (\bar{A}, \bar{I})$, where $\bar{I}$ is irrelevant, that is qualitatively correct. From any such run $\rho = (\bar{A}, \bar{I})$, we now build a well-timed run $Attr(\rho) = (\bar{A}, \bar{J})$ by attributing a well-chosen sequence of intervals $\bar{J} = J_0 J_1 \dots J_n \dots$ to the atoms of the run, so as to satisfy the real-time constraints.

Before, we introduce two lemmas on which the algorithm relies, that can also be read from fig. 2:

Lemma 23 *For every run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$, we have that if $\lhd_{=1}\psi \in A_i$ then there exists $0 \leq j < i$ such that $\psi \in A_j$.*

Proof. This lemma is a direct consequence of the mirrors of axioms (14) and (17). ■

Lemma 24 *For every run $\rho = (\bar{A}, \bar{I})$ of the structure $\hat{\Pi}$, we have that if $\ominus\neg\psi, \psi, \neg\psi \mathsf{S} \rhd_{=1} \psi \in A_i$ then there exists $0 \leq j < i$ such that $\rhd_{=1}\psi \in A_j$.*

Proof. This lemma is a direct consequence of the mirror of axiom (10). ■

The algorithm proceeds by induction along the run, attributing time points $[t_i, t_i]$ when i is even. As a consequence, an open interval (t_{i-1}, t_{i+1}) is attributed when i is odd: we don't mention it, and just define t_i for even i.

(1) Base: $t_0 = 0$, i.e. we attribute the interval $[0, 0]$ to the initial atom A_0.
(2) Induction: we identify and solve the tightest constraint containing i. We define b as the begin of this tightest constraint, by cases:
  (a) equality constraints:
    (i) If there is an $\lhd_{=1}\psi \in A_i$ there has been a last (singular) atom A_b containing ψ before at time t_b.
    (ii) Else, if $\ominus\neg\psi, \psi, \neg\psi \mathsf{S} \rhd_{=1} \psi \in A_i$ there has been a last atom A_b containing $\rhd_{=1}\psi$ before A_i, at time t_b.
  We set $t_i = t_e + 1$, i.e., we attribute $[t_b + 1, t_b + 1]$ to A_i.
  (b) If there are no equality constraints, we consider inequality constraints:
    (i) We compute the earliest begin b of the small clocks using table 2. t_i has to be between t_{i-2} and $t_b + 1$. We choose $t_i = (t_{i-2} + t_b + 1)/2$.
    (ii) Otherwise, we attribute (say) $t_{i-2} + 1/2$ to A_i.

The algorithm selects arbitrarily an equality constraint, but is still deterministic:

Lemma 25 *If two equality constraints have the same end i, their begins b_1, b_2 are identical.*

Proof. Four combinations of equality constraints are possible:

(1) The first constraint is $\lhd_{=1}\phi$
  (a) The second constraint is $\lhd_{=1}\psi$: A_i contains thus $\lhd_{\leq 1}\psi$ by (14). We apply (26) to obtain $\neg\phi \mathsf{S} \psi$.
  We repeat this with ψ, ϕ inverted to obtain $\neg\psi \mathsf{S} \phi$. These formulae imply by the mirror of Lemma 19 that ψ cannot occur before ϕ, and conversely, thus they occur in the same atom.
  (b) The second constraint is the event $\psi, \neg \ominus \psi$ with $\neg\psi \mathsf{S} \rhd_{=1} \psi$: then A_i contains $\lhd_{\leq 1}\phi$ by (14). We apply (29) to obtain $\neg \rhd_{=1} \psi \mathsf{S} \phi$.

Since A_i contains $\neg\psi \mathsf{U}^{\geq} \triangleleft_{=1} \phi$ since its eventuality $\triangleleft_{=1}\phi$ is true now. We apply (28) to obtain $\neg\phi \mathsf{Z}(\triangleright_{\geq 1}\psi \vee \psi)$. Since $\neg\psi \mathsf{S} \triangleright_{=1} \psi \in A_i$, we know that the tick occurs first (perhaps ex-aequo) among the possibilities that end the Z.

These formulae imply by Lemma 19 that $\triangleright_{=1}\psi$ cannot occur before ϕ, and conversely, thus they occur in the same atom.

(2) The first constraint is the event ϕ with $\neg\phi \mathsf{S} \triangleright_{=1} \phi \in A_i$:
   (a) The second constraint is $\triangleleft_{=1}\psi \in A_i$: This case is simply the previous one, with ϕ, ψ inverted.
   (b) The second constraint is the event ψ with $\neg\psi \mathsf{S} \triangleright_{=1} \psi$: A_i contains $\neg\psi \mathsf{U}^{\geq}\phi$ since its eventuality ϕ is true now. We apply (27) to obtain $\neg \triangleright_{=1} \phi \mathsf{Z}(\triangleright_{\leq 1}\psi \vee \psi)$. By $\neg\psi \mathsf{S} \triangleright_{=1} \psi$, the tick $\triangleright_{=1}\psi$ occurred first.

   We repeat this with ψ, ϕ inverted. These formulae imply by Lemma 19 that $\triangleright_{=1}\psi$ cannot occur before $\triangleright_{=1}\phi$, and conversely, thus they occur in the same atom.

■

Solving an equation at its end also solves current partial inequations:

Lemma 26 *If A_i is in the scope of an inequation, and the end of an equation, then the begin A_j of the inequation is after the begin A_b of the equation ($b < j$).*

Proof. There are 3 possible forms of inequations in A_i (see table 4.2):

(1) $\triangleright_{<1}\psi, \neg\psi \mathsf{S}^+ \triangleright_{=1} \psi \in A_i$ and $\triangleright_{=1}\psi \in A_j$:
   let $j \leq i$ be its begin, i.e. $\triangleright_{=1}\psi \in A_j$. We must show that $b < j$. The equation can be:
   (a) $\triangleleft_{=1}\phi \in A_i$ and $\phi \in A_b$:
   thus $\neg\psi \mathsf{U}^{\geq} \triangleleft_{=1} \phi \in A_i$; by (28) $\neg\phi \mathsf{Z}(\triangleright_{\geq 1}\psi \vee \psi) \in A_i$. The first case is true as by hypothesis $\neg\psi \mathsf{S}^+ \triangleright_{=1} \psi \in A_i$ ($\triangleright_{=1}\psi$ must occur before ψ in the past), and gives $b \leq j$.
   (b) $\phi, \neg\phi \mathsf{S} \triangleright_{=1} \phi \in A_i$ and $\triangleright_{=1}\phi \in A_b$:
   using (27), we obtain $\neg \triangleright_{=1} \phi \mathsf{Z}(\triangleright_{\leq 1}\psi \vee \psi) \in A_i$. The first case is true, by hypothesis, and gives $b \leq j$.

   We cannot assume $b = j$, because the mirror of lemma 25 then gives $\psi \in A_i$, contradicting $\neg\psi \mathsf{S}^+ \triangleright_{=1} \psi \in A_i$. We conclude $b < j$.

(2) $\triangleleft_{<1}\psi, \neg\psi \hat{\mathsf{S}}\psi \in A_i$:
   let $j \leq i$ be its begin (its event), i.e. $\psi \in A_j$. We must show that $b < j$. The equation can be:
   (a) $\triangleleft_{=1}\phi \in A_i$ and $\phi \in A_e$:
   We apply (26) to obtain $\neg\phi \mathsf{S}\psi$, meaning by the mirror of lemma 19 that $b \leq j$. $\neg\psi \mathsf{S}\phi \notin A_i$, for otherwise we apply (30) yielding $\triangleleft_{<1}\phi \in A_i$ contradicting $\triangleleft_{=1}\phi \in A_i$ by (15), so we conclude $b < j$.
   (b) $\phi, \neg\phi \mathsf{S} \triangleright_{=1} \phi \in A_i$ and $\triangleright_{=1}\phi \in A_b$:

by (29) $\neg \rhd_{=1} \phi \mathsf{S} \psi \in A_j$, so $b \leq j$. We cannot have the reverse $\neg\psi \mathsf{S} \rhd_{=1} \phi$, for otherwise we apply the mirror of (31) and deduce $\neg\phi \in A_i$, so we conclude $b < j$.

(3) $\neg \rhd_{=1} \psi \mathsf{S} \psi, \neg(\neg\psi \mathsf{S} \rhd_{=1} \psi), (\rhd_{<1}\psi \vee \psi) \in A_i$:
let $j \leq i$ be its begin (a reset). Either $\rhd_{<1}\psi \in A_i$ already, or if the event is in A_i, we use axiom (23) to show $\rhd_{<1}\psi \in A_{i-1}$. Since there is no intervening ψ between j and i, the fig.2 implies $\rhd_{<1}\psi \in A_{j+1}$ and thus $\rhd_{\leq 1}\psi \in A_j$ by (22). Because $\neg(\neg\psi \mathsf{S} \rhd_{=1} \psi) \in A_i$, we deduce $\rhd_{<1}\psi \in A_j$. Now, we must show that $b < j$. The equation can be:
   (a) $\lhd_{=1}\phi \in A_i$ and its event $\phi \in A_b$:
   As $\rhd_{<1}\psi \vee \psi \in A_i$, we apply (28) to obtain $\neg\phi \mathsf{Z}(\rhd_{\leq 1}\psi \vee \psi)$, which means $b \leq j$. Again because there are no intervening ψ between j and i, using lemma 19 we have $\neg\psi \mathsf{U} \lhd_{=1} \phi \in A_j$. Using the mirror of (31), $\lhd_{<1}\phi, \neg\phi \in A_j$, thus $j = b$ is impossible, since $\neg\phi \in A_j$ and $\phi \in A_b$. We conclude $b < j$.
   (b) $\phi, \neg\phi \mathsf{S} \rhd_{=1} \phi \in A_i$ and $\rhd_{=1}\phi \in A_b$:
   so $\neg\psi \mathsf{U}^{\geq}\phi \in A_i$, and we use (27) to obtain $\neg \rhd_{=1} \phi \mathsf{Z}(\rhd_{\leq 1}\psi \vee \psi) \in A_i$. The reset ψ occurs strictly before the tick, so the first case is excluded, giving $\neg \rhd_{=1} \psi \in A_j$; using $\rhd_{\leq 1}\psi \in A_j$, $\rhd_{<1}\psi \in A_j$. Again because there are no intervening ψ between positions j and i, we have $\neg\psi \mathsf{U} \lhd_{=1} \phi \in A_j$. Using the mirror of (30), $\rhd_{<1}\phi \in A_j$. The second case is thus true, and means $b \leq j$. $b = j$ is impossible, since $\rhd_{<1}\phi \in A_j, \rhd_{=1}\phi \in A_b$. We conclude $b < j$.

■

We now show that the algorithm *Attr* assigns time bounds of intervals that are increasing.

Lemma 27 *The sequence t_i built by Attr is increasing.*

Proof. In the notation of the definition, this amounts to prove $t_{i-2} < t_b + 1$ when b is defined, since t_i is either $t_b + 1$ (in the case of an equality) or the middle point of $(t_{i-2}, t_b + 1)$ (in the case of an inequality). If b is not defined (no constraints) then it is trivially verified as we attribute $t_{i-2} + 1/2$ to t_i. We prove the non trivial cases by induction on i:

(1) base case: $i = 2$. Either:
   (a) no constraint is active, b is undefined;
   (b) $b = 0, t_b = 0, t_{i-2} = 0$. We just have to prove $0 < 1$.

(2) induction: We divide in cases according to the constraint selected at $i-2$, whose begin is called b_{i-2}:
   (a) an equality: by lemmas 25, 26, its begin was before, i.e., $b_{i-2} < b$. By inductive hypothesis, t_i is increasing: $t_{b_{i-2}} < t_b$. Thus $t_{i-2} = t_{b_{i-2}} + 1 < t_b + 1$.

(b) an inequality: Thus the begin $b_{i-2} \leq b_i$, since it was obtained by sorting. By inductive hypothesis, t_i is increasing: so $t_{b_{i-2}} \leq t_b$. By inductive hypothesis, $t_{i-4} < t_{b_{i-2}}+1$. Thus $t_{i-2} = (t_{i-4}+t_{b_{i-2}}+1)/2 < (t_{b_{i-2}} + 1 + t_{b_{i-2}} + 1)/2 = t_{b_{i-2}} + 1 \leq t_b + 1$.

■

Furthermore, the algorithm *Attr* ensures that time increases beyond any bounds:

Lemma 28 *The sequence of intervals $\bar{J}$ of $Attr(\rho) = (\bar{A}, \bar{J})$ built by our algorithm has finite variability: for all $t \in \mathbb{R}^+$, there exists an $i \geq 0$ such that $t \in I_i$.*

Proof. Although there is no lower bound on the duration of an interval, we show that the time spend in each passage through the final cycle of $\bar{A} = A_0 A_1 \ldots (A_n A_{n+1} \ldots A_{n+m})^\omega$ is at least $1/2$. Thus any real number t will be reached before index $2tc$, where c is the number of atoms in the final cycle. We divide in cases:

(1) If the cycle $A_n A_{n+1} \ldots A_{n+m}$ contains an atom which is not in the scope of any constraint, the time spent there will be $1/2$.
(2) Else, the cycle contains constraints, and thus constraints of maximal scope. This scope, however, cannot be greater than one cycle. Let e the end of such a constraint. Thus e is in the scope of no other constraint with an earlier begin.
    The time spent in the scope of the constraint until i is at least $1/2$: Let again b be the begin of the scope of the constraint. $t_{e-2} \geq t_b$ (since the begin and end are singular and distinct), thus our algorithm gives $t_e \geq (t_{e-2} + t_b + 1)/2 \geq t_b + 1/2$. Since the scope cannot be greater than one cycle, the time spent in a cycle is at least $1/2$.

■

This procedure correctly solves all constraints:

Lemma 29 *The interval attribution Attr transforms any run ρ in a well-timed run $Attr(\rho)$.*

Proof. We show the two supplementary properties of a well-timed run:

(1) Let $\lhd_I \psi \in \rho(t) = A_i$. We must show that the next ψ occurs in $t - I$. $\lhd_I \psi$ can be:
    (a) $\lhd_{>1} \psi$: These constraints are automatically satisfied because:
        (i) the mirror of the eventuality rule (17) guarantees ψ has occurred. $\exists j < i \quad \psi \in A_j$; Let us take the first such j, which is the corresponding event.

(ii) According to fig.2, ψ will stay false, and eventually we will reach $\lhd_{=1}\psi$: $\exists k \quad j < k < i, \lhd_{=1}\psi \in A_k$;

(iii) the axiom (25) guarantees that satisfying the equality will entail satisfying the greater-than constraint, since they refer to the same tracked event, and since the equality is later. In formulae, for any $t_i \in I_i$, $t_k < t_i$ by lemma 27, $t_k = t_j + 1$, so that $t_i > t_j + 1$.

(b) $\lhd_{=1}\psi$: Since this is an equality constraint, the algorithm *Attr* must have chosen an equality constraint with begin b. Thus $t_i = t_b + 1$. By lemma 25, the begin event ϕ is also in A_b.

(c) $\lhd_{<1}\psi$: If i isn't even (singular), we know that the constraint will still be active in the next atom $i + 1$, because the end of a constraint is always singular. By (22):

- It might become an equality (the clock may tick), in which case it is treated as in the previous case (with $i+1$ instead of i). Then the monotonicity of time will ensure that $I_i < t_{i+1} = t_b + 1$.
- If it is still the same inequality, it is treated below (with $i + 1$ instead of i). Then the monotonicity of time will ensure that $I_i < t_{i+1} < t_b + 1$.

Thus at this point we can assume that i is even. Let $j < i$ be the begin of the constraint, $\phi \in A_j$. The constraint selected by *Attr* at i can be:

(i) an equality: by lemma 26, its begin $b < j$, so that $t_i = t_b + 1 < t_j + 1$.

(ii) or the constraint chosen in A_i is an inequality. The pair $\lhd_{<1}\psi \in A_i, \psi \in A_j$ is also an inequality in A_i: let f be its begin. The algorithm has selected the constraint with the earliest begin b. Thus $b \leq f \leq j < i$, and $t_i < t_b + 1$. Thus $t_i < t_j + 1$.

(2) Let $\rhd_I\psi \in \rho(t) = A_i$. Very similarly, we must show that the next ψ occurs in $t + I$. $\rhd_I\psi$ can be:

(a) $\rhd_{>1}\psi$: These constraints are automatically satisfied because:

(i) the eventuality rule (17) guarantees ψ will occur: $\exists j > i \quad \psi \in A_j$. We take the first such j, which is the corresponding event. We can assume it is singular.

(ii) Figure 2 guarantees that there is first a tick: $\exists k \quad i < k < j, \rhd_{=1}\psi \in A_k$;

(iii) the reset rule (25) guarantees that satisfying the equality will entail satisfying the greater-than constraint, since they refer to the same end event, and since the equality is later. In formulae, for any $t_i \in I_i$, $t_k > t_i$ by lemma 27, $t_k = t_j - 1$, so that $t_i < t_j - 1$.

(b) $\rhd_{=1}\psi$: let A_j contain the next event of ψ. Since this is an equality constraint, the algorithm *Attr* must have chosen an equality constraint at A_j. By lemma 25, its begin is i. Thus $t_j = t_i + 1$.

(c) $\rhd_{<1}\psi$: Let A_j contain the next event of ψ. The constraint selected by *Attr* at j can be:

(i) an equality: by lemma 26 its begin $b < i$, so that $t_j = t_b + 1 <$

$t_i + 1$ for any $t_i \in I_i$.

(ii) or the constraint chosen in A_j is an inequality. The pair $\triangleright_{<1}\psi \in A_i, \psi \in A_j$ is also an inequality in A_j: let f be its begin. The algorithm has selected the constraint with the earliest begin b. Thus $b \leq f \leq i \leq j$, and $t_j < t_b + 1$. Thus $t_j < t_i + 1$, for any $t_i \in I_i$.

The reader now expects a proof for the converse implication. This is not needed thanks to (43). ■

As a consequence of the last lemmas, we have:

Lemma 30 *A timed run built by Attr has the Hintikka property for* EventClockTL*:* $\forall \phi \in C, \phi \in \rho(t) \leftrightarrow (\rho, t) \models \phi$.

Finally, we obtain the desired theorem:

Theorem 31 *Every* EventClockTL*-consistent formula is satisfiable.*

Proof. If α is a EventClockTL-consistent formula then there exists an α-monitored atom A_α in $\hat{\Pi}$. By lemma 16, there exists a set of runs Σ that pass through A_α and by the properties of the procedure *Attr*, lemma 18, lemma 28 and lemma 29, at least one run $(\bar{A}, \bar{I}) \in \Sigma$ has the Hintikka property for EventClockTL. It is direct to see that $(\bar{A} \cap \mathsf{P}, \bar{I})$ is a model for α at time $t \in I_\alpha$ (the interval of time associated to A_α in $(\bar{A}, \bar{I})$) and thus α is satisfiable. ■

Corollary 32 *The rule (1) and axioms (2)-(31) form a complete axiomatization of* EventClockTL.

4.3 Comparison with automata construction

In spirit, the procedure given above can be considered as building an automaton corresponding to a formula. The known procedures [3] for deciding MetricIntervalTL use a similar construction, first building a *timed automaton* and then its *region automaton*. We could not use this construction directly here, because it involves features of automata that have no counterpart in the logic, and thus could not be expressed by axioms. However, the main ideas are similar. The region automaton will record the integer value of each clock: we code this by formulae of the form $\triangleright_{<1} \triangleright_{=1} ... \triangleright_{=1} \phi$. It will also record the ordering of the fractional parts of the clocks: this is coded here by formulae of the form $\neg \triangleright_{=1} ... \triangleright_{=1} \phi \mathsf{U} \triangleright_{=1} ... \triangleright_{=1} \psi$. There are some small differences, however. For simplicity we maintain more information than needed. For instance we record the ordering of any two ticks, even if these ticks are not linked to the current value of the clock. This relationship is only inverted for a very special case:

when a clock has no previous and no following tick, we need not and cannot maintain its fractional information. It is easy to build a more careful and more efficient tableau procedure, that only records the needed information.

The structure of atoms constructed here treats the eventualities in a different spirit than automata: here, there may be invalid paths in the graph of atoms. It is immediate to add acceptance conditions to eliminate them and obtain a more classical automaton. But it is less obvious to design a class of automata that is as expressive as the logic: this is done in [14].

4.4 Other time domains

As we have already indicated incidentally, our proofs are written to adapt to other time domains $\mathbb{T}$ with minimal change. We only consider totally ordered dense time, however. For instance, we could use as time domain:

(1) The real numbers, $\mathbb{T} = \mathbb{R}$: We replace (12) by the mirror of (13).
(2) The rational numbers, $\mathbb{T} = \mathbb{Q}$: If we force the bounds of an interval to be rational as well, nothing has to be changed. Otherwise, a transition from an open interval to an open interval is now possible, if the common bound is irrational. This defeats the induction axiom (11). We postpone the study of this case to a further paper, but the basic ideas of the proof still apply.
(3) A bounded real interval:
    (a) closed $\mathbb{T} = [l, r]$: For the qualitative part, we replace (13) by the mirror of (12). For the quantitative part, we first remove the axiom (25). If the duration of the interval $d = l - r$ is integer, we add:

$$\neg \ominus \top \rightarrow \triangleright_{=d} \neg \bigcirc \top \tag{47}$$

    stating that the beginning is at distance d from the end. Otherwise, we add the best approximation of this:

$$\neg \ominus \top \rightarrow \triangleright_{(\lfloor d \rfloor, \lceil d \rceil)} \neg \bigcirc \top \tag{48}$$

    (b) open $\mathbb{T} = [l, r)$: For the qualitative part, we replace (13) by the mirror of (12): from a qualitative point of view, an open interval is indistinguishable from an infinite one.

5 Translating MetricIntervalTL into EventClockTL

The logics have been designed from a different philosophical standpoint: MetricIntervalTL restricts the undecidable logic MetricTL by "relaxing punctuality", i.e., forbidding to look at exact time values; EventClockTL, in contrast, forbids to look past the next event in the future. However, we have shown in [14] that, surprisingly, they have the same expressive power. The power given by nesting connectives allows to each logic to do some of its forbidden work. Here, we need more than a mere proof of expressiveness, we need a finite number of axioms expressing the translation between formulae of the two logics. We give below both the axioms and a procedure that use them to provide a proof of the equivalence.

First, we suppress intervals containing 0:

$$\phi \hat{\mathsf{U}}_I \psi \leftrightarrow \psi \vee (\phi \hat{\mathsf{U}}_J \psi) \quad \text{with } J = I \setminus \{0\} \text{ and } 0 \in I \tag{49}$$

Then we replace bounded untils $\hat{\mathsf{U}}_I$ with $0 \notin I$ by simpler $\Diamond_I$, provided $0 \notin I$:

$$\phi \hat{\mathsf{U}}_I \psi \leftrightarrow \Box_{\leq I}(\psi \vee \phi \hat{\mathsf{U}} \psi) \wedge \Box_{<I}(\phi \wedge \phi \hat{\mathsf{U}} \psi) \wedge \phi \hat{\mathsf{U}} \psi \wedge \Diamond_I \psi \tag{50}$$

where l is the left endpoint of I, the intervals $J = \{t | 0 < t < I\}$, $J_0 = \{t | O \leq t < I\}$.

We suppress classical until using:

$$\phi \hat{\mathsf{U}} \psi \leftrightarrow \phi \mathsf{U}(\psi \wedge \ominus \phi) \tag{51}$$

For infinite intervals, we reduce the lower bound $l > 0$ to 0 using

$$\Diamond_{(l,\infty)} \phi \leftrightarrow \Box_{(0,l]} \Diamond \phi \tag{52}$$

$$\Diamond_{[l,\infty)} \phi \leftrightarrow \Box_{(0,l]} (\phi \vee \Diamond \phi) \tag{53}$$

For finite intervals with left bound equal to 0, we exclude it if needed with (49), and we use the $\triangleright$ operator:

$$\Diamond_{(0,u)} \phi \leftrightarrow \triangleright_{<u} \phi \tag{54}$$

$$\Diamond_{(0,u]} \phi \leftrightarrow \triangleright_{\leq u} \phi \tag{55}$$

Note that the formulae $\triangleright_{<u} \phi$ and $\triangleright_{\leq u} \phi$ can be reduced to formulae that only use constant 1 using the axioms (18) and (19).

When the left bound of the interval is different from 0 and the right bound different from ∞, we reduce the length of the interval to 1 using:

$$\Diamond_{I\cup J}\phi \leftrightarrow \Diamond_I\phi \vee \Diamond_J\phi \tag{56}$$

Then we use the following rules recursively until the lower bound is reduced to 0:

$$\Diamond_{(l,l+1)}\phi \leftrightarrow \Diamond_{[l-1,l)} \rhd_{=1} \bigcirc\phi \vee \Diamond_{(l-1,l)} \rhd_{=1} \phi \vee \Box_{(l-1,l]} \rhd_{<1} \phi \tag{57}$$
$$\Diamond_{(l,l+1]}\phi \leftrightarrow \Diamond_{[l-1,l)} \rhd_{=1} \bigcirc\phi \vee \Diamond_{(l-1,l]} \rhd_{=1} \phi \vee \Box_{(l-1,l]} \rhd_{<1} \phi \tag{58}$$
$$\Diamond_{[l,l+1)}\phi \leftrightarrow \Diamond_{[l-1,l)} \rhd_{=1} \bigcirc\phi \vee \Diamond_{[l-1,l)} \rhd_{=1} \phi \vee \Box_{(l-1,l]}\Diamond_{[0,1)}\phi \tag{59}$$
$$\Diamond_{[l,l+1]}\phi \leftrightarrow \Diamond_{[l-1,l)} \rhd_{=1} \bigcirc\phi \vee \Diamond_{[l-1,l]} \rhd_{=1} \phi \vee \Box_{(l-1,l]}\Diamond_{[0,1)}\phi \tag{60}$$

In this way, any MetricIntervalTL formula can be translated into a EventClockTL formula where bounds are always 0 or 1. Actually, we used a very small part of EventClockTL; we can further eliminate $\rhd_{<1}\phi$:

$$\rhd_{<1}\phi \leftrightarrow (\mathsf{C}\phi \wedge \neg \rhd_{=1} \phi\mathsf{U}^+\phi) \vee (\neg(\mathsf{C}\phi) \wedge \neg \rhd_{=1} \bigcirc\phi\mathsf{U}^+ \bigcirc \phi) \tag{61}$$

showing that the very basic operators $\rhd_{=1}, \lhd_{=1}$ have the same expressive power as full MetricIntervalTL.

The converse translation is much simpler:

$$\rhd_I\phi \leftrightarrow \neg\Diamond_{<I}\phi \wedge \Diamond_{I\setminus\{0\}}\phi \tag{62}$$
$$\phi\mathsf{U}\psi \leftrightarrow (\phi \vee \psi)\hat{\mathsf{U}}\psi \tag{63}$$

5.1 Axiomatization of MetricIntervalTL

To obtain an axiom system for MetricIntervalTL, we simply translate the axioms of EventClockTL and add axioms expressing the translation.

Indeed, we have translations in each direction:
T : EventClockTL $\rightarrow$ MetricIntervalTL
S : MetricIntervalTL $\rightarrow$ EventClockTL.
Therefore, to prove a MetricIntervalTL formula μ, we translate it into EventClockTL and prove it there using the procedure of section 4. The proof π can be translated back to MetricIntervalTL in $T(\pi)$ proving $T(S(\mu))$. Indeed, each step is a replacement, and replacements are invariant under syntax-directed translation preserving equivalence:

$$T(\psi \leftrightarrow \phi) = T(\psi) \leftrightarrow T(\phi)$$

$$T(\phi[p := \psi]) = T(\phi)[p := T(\psi)]$$

To finish the proof we only have to add $\frac{T(S(\mu))}{\mu}$. Actually the translation axioms above are stronger, stating $T(S(\mu)) \leftrightarrow \mu$. In our case, T (defined by (62), (63)) is so simple that it can be considered as a mere shorthand. Thus the axioms (1)–(29) and (49)–(60) form a complete axiomatization of $\mathsf{MetricIntervalTL}$, with $\triangleright_I, \mathsf{U}$ now understood as shorthands.

Theorem 33 *The rule (1), axioms (2)-(29), and axioms (49)-(60) form a complete axiomatization of* $\mathsf{MetricIntervalTL}$.

6 Conclusion

The specification of real-time systems using dense time is natural, and has many semantical advantages, but discrete-time techniques (here proof techniques [8,18]) have to be generalized. The model-checking and decision techniques have been generalized in [2,3]. Unfortunately, the technique of [3] uses a translation to automata which are more powerful and complex than temporal logic, and thus is not suitable for building a completeness proof.

This paper provides complete axiom systems and proof-building procedures for linear real time, extending the technique of [19]. This procedure can be used to automate the proof construction of propositional fragments of a larger first-order proof.

Some possible extensions of this work are:

- The proof rules are admittedly cumbersome, since they exactly reflect the layered structure of the proof: for instance, real-time axioms are clearly separated from the qualitative axioms. More intuitive rules can be devised if we relax this constraint. This paper provides an easy way to show their completeness: it is enough to prove the axioms of this paper. This also explains why we have not generalized the axioms, even when obvious generalizations are possible: we prefer to stick to the axioms needed in the proof, to facilitate a later completeness proof using this technique.
- The logics used in this paper assume that concrete values are given for real-time constraints. As demonstrated in the HyTech checker [13], it is often useful to mention parameters instead (symbolic constants), and derive the needed constraints on the parameters, instead of a simple yes/no answer.
- The extension of the results of this paper to first-order variants of $\mathsf{MetricIntervalTL}$ should be explored. However, completeness is often lost in first-order variants [23].
- The development of programs from specifications should be supported: the automaton produced by the proposed technique might be helpful as a program skeleton in the style of [24].

References

[1] M. Abadi and L. Lamport. The existence of refinement mappings. *Theoretical Computer Science*, 82(2):253–284, 1991.

[2] R. Alur, C. Courcoubetis, and D.L. Dill. Model checking in dense real time. *Information and Computation*, 104(1):2–34, 1993.

[3] R. Alur, T. Feder, and T.A. Henzinger. The benefits of relaxing punctuality. *Journal of the ACM*, 43(1):116–146, 1996.

[4] R. Alur and T.A. Henzinger. A really temporal logic. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, pages 164–169. IEEE Computer Society Press, 1989.

[5] R. Alur and T.A. Henzinger. Logics and models of real time: a survey. In J.W. de Bakker, K. Huizing, W.-P. de Roever, and G. Rozenberg, editors, *Real Time: Theory in Practice*, Lecture Notes in Computer Science 600, pages 74–106. Springer-Verlag, 1992.

[6] H. Barringer, R. Kuiper, and A. Pnueli. A really abstract concurrent model and its temporal logic. In *Proceedings of the 13th Annual Symposium on Principles of Programming Languages*, pages 173–183. ACM Press, 1986.

[7] J.P. Burgess. Basic tense logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, volume II, pages 89–133. D. Reidel Publishing Company, 1984.

[8] E.M. Clarke, E.A. Emerson, and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal-logic specifications. *ACM Transactions on Programming Languages and Systems*, 8(2):244–263, 1986.

[9] D. M. Gabbay and I. M. Hodkinson. An axiomatization of the temporal logic with Until and Since over the real numbers. *Journal of Logic and Computation*, 1(2):229–259, December 1990.

[10] M. R. Hansen and Zhou Chaochen. Semantics and completeness of duration calculus. In J. W. de Bakker, C. Huizing, W. P. de Roever, and G. Rozenberg, editors, *Proceedings of Real-Time: Theory in Practice*, volume 600 of *LNCS*, pages 209–225, Berlin, Germany, June 1992. Springer.

[11] E. Harel, O. Lichtenstein, and A. Pnueli. Explicit-clock temporal logic. In *Proceedings of the Fifth Annual Symposium on Logic in Computer Science*, pages 402–413. IEEE Computer Society Press, 1990.

[12] T.A. Henzinger. Half-order modal logic: how to prove real-time properties. In *Proceedings of the Ninth Annual Symposium on Principles of Distributed Computing*, pages 281–296. ACM Press, 1990.

[13] T.A. Henzinger, P.-H. Ho, and H. Wong-Toi. HyTech: the next generation. In *Proceedings of the 16th Annual Real-time Systems Symposium*, pages 56–65. IEEE Computer Society Press, 1995.

[14] Thomas A. Henzinger, Jean-Francois Raskin, and Pierre-Yves Schobbens. The regular real-time languages. In K. Larsen, editor, *Proceedings of ICALP'98: International Colloquium on Automata, Languages and Programming*, volume 1343 of *Lecture Notes in Computer Science*, pages 580–591, Aalborg, Denmark, July 1998. Springer-Verlag.

[15] J.A.W. Kamp. *Tense Logic and the Theory of Order*. PhD thesis, UCLA, 1968.

[16] Yonit Kesten and Amir Pnueli. A complete proof systems for QPTL. In *Proceedings, Tenth Annual IEEE Symposium on Logic in Computer Science*, pages 2–12, San Diego, California, 26–29 June 1995. IEEE Computer Society Press.

[17] Ron Koymans. *Specifying message passing and time-critical systems with temporal logic*. LNCS 651, Springer-Verlag, 1992.

[18] O. Lichtenstein and A. Pnueli. Checking that finite-state concurrent programs satisfy their linear specification. In *Proceedings of the 12th Annual Symposium on Principles of Programming Languages*, pages 97–107. ACM Press, 1985.

[19] O. Lichtenstein, A. Pnueli, and L.D. Zuck. The glory of the past. In R. Parikh, editor, *Logics of Programs*, Lecture Notes in Computer Science 193, pages 196–218. Springer-Verlag, 1985.

[20] Z. Manna and A. Pnueli. The anchored version of the temporal framework. In J.W. de Bakker, W.-P. de Roever, and G. Rozenberg, editors, *Linear Time, Branching Time, and Partial Order in Logics and Models for Concurrency*, Lecture Notes in Computer Science 354, pages 201–284. Springer-Verlag, 1989.

[21] J.S. Ostroff. *Temporal Logic of Real-time Systems*. Research Studies Press, 1990.

[22] J.-F. Raskin and P.-Y. Schobbens. State clock logic: a decidable real-time logic. In O. Maler, editor, *HART 97: Hybrid and Real-time Systems*, Lecture Notes in Computer Science 1201, pages 33–47. Springer-Verlag, 1997.

[23] A. Szalas and L. Holenderski. Incompleteness of first-order temporal logic with until. *Theoretical Computer Science*, 57(2-3):317–325, May 1988.

[24] P. Wolper. *Synthesis of Communicating Processes from Temporal-Logic Specifications*. PhD thesis, Stanford University, 1982.