I N F O R M A T I K

Axioms for Real-Time Logics

Thomas Henzinger
Jean-François Raskin
Pierre-Yves Schobbens

MPI–I–99–3–005 August 1999

FORSCHUNGSBERICHT RESEARCH REPORT

M A X - P L A N C K - I N S T I T U T
F Ü R
I N F O R M A T I K

Im Stadtwald 66123 Saarbrücken Germany

Authors' Addresses

Thomas Henzinger
Max-Planck-Institut für Informatik
Im Stadtwald
66123 Saarbrücken
`tah@mpi-sb.mpg.de`

Jean-François Raskin
Max-Planck-Institut für Informatik
Im Stadtwald
66123 Saarbrücken
`jfr@mpi-sb.mpg.de`

Pierre-Yves Schobbens
Computer Science Department
University of Namur
Namur
Begium `pys@info.fundp.ac.be`

Publication Notes

A revised version of this report has been accepted for publication in the journal of *Theoretical Computer Science.*

Acknowledgements

This work was supported by the Belgian National Fund for Scientific Research (FNRS).

Keywords

Temporal Logic, Real-Time Logic, Completness, Decidability, Complexity.

1 Introduction

Many real-time systems are critical, and therefore deserve to be specified with mathematical precision. To this end, real-time temporal logics [6] have been proposed 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 quantification [4, 11], explicit clocks in a first-order temporal logic [18, 9] and time-bounded operators [14]. We study logics with time bounded operators because those logics are the only ones that have a decidable satisfiability problem. Note however that the propositional fragment of the time-bounded operator logics, called $\mathsf{MetricTL}_{\mathbb{R}+}$, is undecidable and furthermore not recursively axiomatizable. It becomes decidable with certain restrictions ($\mathsf{MetricIntervalTL}$ [3]), allowing programs verification using automata-based 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 these logics. Third, the complete axiomatization serves as a yardstick for a definition of *relative completeness* for more expressive logics that are not completely axiomatizable, in the style of [17, 13]. This is why the axiomatization of these logics is cited as an important open question in [6, 14].

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 [7], $\mathsf{EventClockTL}$ with past clocks only, $\mathsf{EventClockTL}$ with past and future clocks (also called SCL [19]), $\mathsf{MetricIntervalTL}$ [3] with past and future operators, also called $\mathsf{MetricIntervalTL}_P$ [5].

Previous works on axiomatization of real-time logics have concentrated on models where time is modeled by the natural numbers. For that case, [11] gives a complete axiomatization. When time is modeled by the real-time numbers, only "intuitive" axioms were proposed, e.g. in [14], without taking into account completeness issues.

2 Models and logics for real-time

2.1 Models

As time domain, we choose the nonnegative reals $\mathbb{R}^+$. This dense domain is natural and gives many advantages detailed elsewhere: compositionality [7], full abstractness [7], stuttering independence [1], easy refinement. To avoid Zeno's paradox, we add to our models the condition of *finite variability* [7] (condition (3) below): only finitely many state changes can occur in a finite amount of time.

An *interval* $I \subseteq \mathbb{R}^+$ is a convex non-empty subset of the nonnegative reals. Given $t \in \mathbb{R}^+$, 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 $\{t > 0 | \exists t' \in I : t \leq t'\}$ and $\rfloor I$ for the interval $\{t > 0 | \exists t' \in I : t < t'\}$. 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 an interval I is *singular* if $l(I) = r(I)$. An *interval sequence* $\bar{I} = I_0, I_1, I_2, \ldots$ is an infinite sequence of (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 $t \in \mathbb{R}^+$, there exists an $i \geq 0$ such that $t \in I_i$. Consequently, an interval sequence partitions the nonnegative real line so that every bounded subset of $\mathbb{R}^+$ 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 $\mathbb{R}^+$ to 2^P, indicating for each time $t \in \mathbb{R}^+$ 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 [13] are built from propositional symbols, boolean connectives, the temporal "until" and "since" and are generated by the following grammar:

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

where p is a proposition.

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

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

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 $(\tau, t) \models \phi$. Our operators U, S are slightly non-classical, but more intuitive: they do not require ϕ_2 to start in a left-closed interval.

2.3 Event-Clock Temporal Logic

The formulae of EventClockTL [19] 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 $\lhd_I \phi$ asserts that ϕ was true last in the interval $t - I$, and the prophecy operator $\rhd_I \phi$ asserts that ϕ will be true next in the interval $t + I$. The formulae of EventClockTL are generated by the following grammar:

$$\phi \ ::= \ p \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \phi_1 \mathsf{U} \phi_2 \mid \phi_1 \mathsf{S} \phi_2 \mid \lhd_I \phi \mid \rhd_I \phi$$

where p is a proposition and I is an interval which can be singular and whose bounds are natural numbers. The EventClockTL formula ϕ holds at time $t \in \mathbb{R}^+$ of the timed state sequence τ, written $(\tau, t) \models \phi$ according to the rules for LTR and the following additional clauses:
$(\tau, t) \models \lhd_I \phi$ iff $\exists t' < t \wedge t' \in t - I \wedge (\tau, t') \models \phi$ and $\forall t'' : t - I < t'' < t, (\tau, t'') \not\models \phi$
$(\tau, t) \models \rhd_I \phi$ iff $\exists t' > t \wedge t' \in t + I \wedge (\tau, t') \models \phi$ and $\forall t'' : t < t'' < t + I, (\tau, t'') \not\models \phi$

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 *prophecy 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 an history (resp. prophecy) 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 [19].

Example 1 $\Box(p \rightarrow \rhd_{=5} p)$ asserts that after every p state, the first subsequent p state is exactly 5 units later (so in the interval t+(0,5), p is false); the formula $\Box(\lhd_{=5} p \rightarrow q)$ asserts that whenever the last p state is exactly 5 units ago, then q is true now (time-out).

Theorem 1 [19] *The satisfiability problem for* EventClockTL *is complete for* PSPACE.

2.4 Metric-Interval Temporal Logic

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. The MetricIntervalTL formula ϕ holds at time $t \in \mathbb{R}^+$ 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):

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

Example 2 $\Box(q \rightarrow r\hat{\mathsf{S}}_{\leq 5}\, p)$ asserts that every q state is preceded by a p state of time difference at most 5, and all intermediate states are r states; the formula $\Box(p \rightarrow \hat{\Diamond}_{[5,6)} p)$ 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.

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

2.5 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. Let us note that $\phi_1 \hat{\mathsf{U}} \phi_2 \equiv \phi_1 \mathsf{U}(\phi_2 \wedge \ominus\phi_1)$ ($\ominus$ is defined below); [1]
- $\phi_1 \mathsf{U}^+ \phi_2 \equiv \phi_1 \wedge \phi_1 \mathsf{U} \phi_2$, 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 "arbitrarily closed in the future";
- $\Diamond\phi \equiv \top \mathsf{U} \phi$, meaning "eventually in the future";
- $\Box\phi \equiv \neg\Diamond\neg\phi$, meaning "always in the future";
- their reflexive counterparts: $\Diamond^{\geq}, \Box^{\leq}$;

[1] Let us note that the "Until" of EventClockTL and the "Until" of MetricIntervalTL are interdefinable, in fact, we also have: $\phi_1 \mathsf{U} \phi_2 \equiv (\phi_1 \vee \phi_2) \hat{\mathsf{U}} \phi_2$.

- $\phi_1 \mathsf{W} \phi_2 \equiv \phi_1 \mathsf{U} \phi_2 \vee \Box \phi_1$, meaning "unless";
- its reflexive counterparts: W^+, $\mathsf{W}^{\geq}$.

and the past counterpart of all those abbreviations:

- $\phi_1 \hat{\mathsf{S}} \phi_2 \equiv \phi_1 \hat{\mathsf{S}}_{(0,\infty)} \phi_2$, the untimed "Since" of MetricIntervalTL. Let us note that $\phi_1 \hat{\mathsf{S}} \phi_2 \equiv \phi_1 \mathsf{S}(\phi_2 \wedge \ominus \phi_1)$;
- $\phi_1 \mathsf{S}^+ \phi_2 \equiv \phi_1 \wedge \phi_1 \mathsf{S} \phi_2$, 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 closed 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: $\diamondminus^{\leq}, \boxminus^{\geq}$;
- $\phi_1 \mathsf{Z} \phi_2 \equiv \phi_1 \mathsf{S} \phi_2 \vee \boxminus \phi_1$, meaning "unless in the past";
- its reflexive counterparts: Z^+, $\mathsf{Z}^{\leq}$.

3 Axiomatization of EventClockTL

In Subsection 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 we believe that this interaction is unavoidable.

3.1 Qualitative axioms (complete for LTR)

We use the rule of inference:

$$\frac{\phi \leftrightarrow \psi \qquad \chi(\psi)}{\chi(\phi)} \tag{RE}$$

All propositional tautologies

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

$$\neg(\psi \mathsf{U} \bot) \tag{N}$$

$$\phi \mathsf{U}(\psi \wedge \psi') \rightarrow \phi \mathsf{U} \psi \tag{K}$$

$$\ocircle(\psi \wedge \phi) \leftrightarrow \ocircle\psi \wedge \ocircle\phi \tag{JA}$$

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

$$\ocircle(\psi \mathsf{U} \phi) \leftrightarrow \psi \mathsf{U} \phi \tag{JU}$$

$$\ocircle(\psi \mathsf{S} \phi) \leftrightarrow \ocircle\phi \vee (\ocircle\psi \wedge (\psi \mathsf{S}^{\leq} \phi)) \tag{JS}$$

$$\psi \mathsf{U} \phi \leftrightarrow \ocircle(\psi \mathsf{U}^{\geq} \phi) \tag{UJ}$$

$$\phi \mathsf{U} \psi \rightarrow \Diamond\psi \tag{SF}$$

$$\Box((\psi \wedge \ocircle\top \rightarrow \ocircle\psi) \wedge (\ominus\psi \rightarrow \psi)) \rightarrow (\ocircle\psi \rightarrow \Box\psi) \tag{JI}$$

They mainly make use of the $\ocircle$ operator, because as we shall see, it corresponds to the transition relation of our structure. Axiom (N) is the usual necessitation or modal generalization rule, expressed as an axiom. Similarly, (K) is the usual weakening principle, expressed in a slightly non-classical form. (JA), (BN) allow to distribute $\ocircle$ with boolean operators. Note that the validity of (BN) requires finite variability. (JU), (JS) describe how the U and S operators are transmitted over interval boundaries. (UJ) gives local consistency conditions over this transmission. (SF) ensures eventuality when combined with (JI). It can also be seen as weakening the left side of the U to $\top$. The induction axiom (JI) 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 (B) but has no end (JT):

$$\overleftarrow{\Diamond}^{\leq}\neg\ominus\top \tag{BE}$$

$$\ocircle\top \tag{JT}$$

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. For instance, to deal with the (positive and negative) reals numbers, we just use the mirror of (JT) instead of (BE).

Remark 1 *It is easy to check that the proof of completeness of section 4 only uses the axioms above for a formula without real-time; therefore they form a complete axiomatization of the logic of the reals with finite variability, defined as* LTR *in [7]. The system proposed in [7] is unfortunately unsound, redundant and incomplete. Indeed, axiom F5 of [7] is unsound (this is a simple typo); axiom F7 can be deduced from axiom F8; and the system cannot derive the induction axiom (JI). To see this last point, take the structure* *formed by $\mathbb{R}^+$ followed by $\mathbb{R}$, with finite variability: it satisfies the system of [7] but not the induction axiom. Thus this valid formula cannot be proved 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:

$$\rhd_{I \cup J}\phi \leftrightarrow \rhd_I \phi \vee \rhd_J \phi \tag{OR}$$
$$\rhd_{I \cap J}\phi \leftrightarrow \rhd_I \phi \wedge \rhd_J \phi \tag{AND}$$
$$\neg \rhd_{=0} \phi \tag{F}$$
$$\rhd_{>0}\psi \leftrightarrow \Diamond\psi \tag{P-S}$$
$$\rhd_{\leq m+n}\phi \leftrightarrow \rhd_{\leq m} \rhd_{\leq n} \phi \tag{NLE}$$
$$\rhd_{<m+n}\phi \leftrightarrow \rhd_{<m} \rhd_{\leq n} \phi \tag{NLT}$$

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 (LO) to reduce left-open events to the easier case of left-closed ones. The formula $\neg\phi \hat{\mathsf{U}} \phi$ expresses that the next ϕ-interval is left-closed and its negation that the next ϕ-interval, if it exists, is left-open.

$$\neg(\neg\phi\hat{\mathsf{U}}\phi) \rightarrow (\rhd_{[l,m)} \bigcirc \phi \leftrightarrow \rhd_{(l,m)}\phi) \tag{LO}$$
$$\neg \bigcirc \rhd_{=m}\psi \tag{J=}$$
$$\neg\psi\hat{\mathsf{U}}\psi \rightarrow (\bigcirc \rhd_{<m}\psi \leftrightarrow \rhd_{\leq m}\psi) \tag{JP}$$
$$\ominus \rhd_{<m} \psi \leftrightarrow ((\rhd_{<m}\psi \vee \psi \vee \ominus\psi) \wedge \ominus\top) \tag{JH}$$
$$\bigcirc\psi \rightarrow \rhd_{<m}\psi \tag{J-P}$$

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:

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

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 "shift" and "order" axioms and their mirrors to express this common speed. These axioms use U to express the ordering of events: $\neg p \mathsf{U} q$ means that q will occur before (or at the same time than) any p. The "shift" axioms say that the ordering the ticks should be preserved: the main antecedent $\neg \lhd_{=1} \psi \mathsf{U}^{\geq} \lhd_{=1} \phi$ in (SHH) states that ϕ will tick before ψ; in this case the events shall be in the same order: $\neg\phi\mathsf{S}\psi$. The side conditions ensure that the clocks were active in the meantime, so that the ticks indeed refer to events ϕ, ψ of the conclusion. The "order" axioms states a similar but simpler property: (OHH) says that if last ϕ was less than 1 ago, and ψ was before, than last ψ was less than 1 ago.

$$\lhd_{\leq 1}\psi \wedge \neg\psi\mathsf{U}^{\geq} \lhd_{=1} \phi \wedge \neg \lhd_{=1} \psi\mathsf{U}^{\geq} \lhd_{=1} \phi \to \neg\phi\mathsf{S}\psi \tag{SHH}$$

$$(\rhd_{<1}\psi \vee \psi) \wedge \neg\psi\mathsf{U}^{\geq}\phi \to \neg \rhd_{=1} \phi\mathsf{Z} \rhd_{=1} \psi \vee \neg \rhd_{=1} \phi\mathsf{Z}\psi \tag{SPP}$$

$$(\rhd_{<1}\psi \vee \psi) \wedge \neg\psi\mathsf{U}^{\geq} \lhd_{=1} \phi \to \neg\phi\mathsf{Z} \rhd_{=1} \psi \vee \neg\phi\mathsf{Z}\psi \tag{SPH}$$

$$\lhd_{\leq 1}\psi \wedge \neg\psi\mathsf{U}^{\geq}\phi \wedge \neg \lhd_{=1} \psi\mathsf{U}^{\geq}\phi \to \neg \rhd_{=1} \phi\mathsf{S}\psi \tag{SHP}$$

$$\lhd_{<1}\phi \wedge \neg\phi\mathsf{S}\psi \to \lhd_{<1}\psi \tag{OHH}$$

$$\lhd_{<1}\psi \wedge \neg\psi\mathsf{S} \rhd_{=1} \phi \to \rhd_{<1}\phi \wedge \neg\phi \tag{OHP}$$

3.3 Theorems

We also use in the proof some derived rules and theorems:

- the rule of *Modus Ponens* is derivable from replacement as follows: from A we deduce propositionally $A \leftrightarrow \top$; by replacement we replace A by $\top$ in $A \to B$ giving $\top \to B$ which yields propositionally B;
- the rule of *modal generalization* (also called necessitation) is derived from (RE) and (N).

$$\neg\neg\phi \leftrightarrow \phi \tag{NN}$$

$$\neg \ominus \top \to (\ominus\phi \leftrightarrow \bot) \tag{BB}$$

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

$$\ominus\psi \to \ominus\top \tag{BT}$$

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

$$\Diamond\top \tag{ST}$$

$$\lhd_I\psi \to \ominus\top \tag{HB}$$

$$\neg(\neg\psi\hat{\mathsf{U}}\psi) \to \neg \rhd_{=m} \phi \tag{N=}$$

$$\neg(\neg\psi\hat{\mathsf{U}}\psi) \to (\Diamond\bigcirc\phi \leftrightarrow \Diamond\phi) \tag{SO}$$

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

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

$$\rhd_I\phi \to \rhd_J\phi \text{ with } (I \subseteq J) \tag{MON}$$

$$\Box\phi_1 \wedge \phi_2 \to \Box\phi_1 \tag{KA}$$

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 of the adequation of the proposed axiomatic system: its completeness. 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. Our logics are symmetric for past and future (a duality that we call "mirror principle"), except that time begin but does not end: therefore most explanations will be given for the future, but the careful reader will check their applicability to the past as well.

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 [16] 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 [16], 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 (JI) that extend 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 constrain the clocks to evolve simultaneously. The completeness of these axioms is shown by solving the constraints on real-time generated the clock evolutions.

4.1 Qualitative part

Let us make the hypothesis 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 1 *Every* EventClockTL *formula* ψ *can be rewritten into an equivalent* ψ^T *formula of* $\mathsf{EventClockTL}_1$ *(using only the constant* 1*).*

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

In the sequel, we make the hypothesis that the formula α for which we want to construct a model is in $\mathsf{EventClockTL}_1$, this does not harm completeness as by lemma 1, every EventClockTL formula can first be transformed in an equivalent $\mathsf{EventClockTL}_1$ formula.

We now defined 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: $R = \{\phi \in S | \triangleright_I \phi \in Sub\}$. 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 (LO). $J = \{\bigcirc \phi | \phi \in R\}$.
- To select whether to track ϕ or $\bigcirc \phi$, we need the formulae giving the openness of next interval: $L = \{\neg \phi \hat{\mathsf{U}} \phi | \phi \in R \cup J\}$.
- The formulae giving the current integer value of the clocks: $I = \{\triangleright_{<1} \phi, \triangleright_{=1} \phi, \triangleright_{>1} \phi | \phi \in R \cup J\}$. 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: $T = \{\triangleright_{=1} \phi \in I\}$.
- We also define the mirror sets. For instance, $R^- = \{\phi \in Sub | \triangleleft_I \phi \in Sub\}$.
- 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: $E = \{\Diamond \phi | \psi \mathsf{U} \phi \text{ or } \psi \hat{\mathsf{U}} \phi \in Sub \cup L \cup L^-\}$

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:

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

$$\neg\neg\phi \leftrightarrow \phi \tag{NN}$$

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

For the negation, we only have

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

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

We only have two possible cases: if $\ominus\top$ is true, we can move all negations outside and cancel them, except one. else, we know that all $\ominus\psi$ are false. In each case, at most one $\ominus, \bigcirc$ and one $\neg$ are needed.

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 a first *structure*, which is a finite graph, $\mathfrak{S} = (\mathfrak{A}, \mathfrak{R})$ where $\mathfrak{A}$ is the set of all propositional atoms of $C(\alpha)$ and $\mathfrak{R} \subseteq \mathfrak{A} \times \mathfrak{A}$ is the transition relation of the structure. $\mathfrak{R}$ is defined by considering two subtransition relations:

- $\mathfrak{R}_]$ represents the transition from a right-closed to a left-open interval;
- $\mathfrak{R}_[$ represents the transition from a right-open to a left-closed interval.

Let A, B be propositional atoms. We define

- $A\mathfrak{R}_]B \Leftrightarrow \forall \bigcirc\phi \in C(\alpha), \bigcirc\phi \in A \leftrightarrow \phi \in B$;
- $A\mathfrak{R}_[B \Leftrightarrow \forall \ominus \phi \in C(\alpha), \phi \in A \leftrightarrow \ominus\phi \in B$.

The *transition relation* $\mathfrak{R}$ is the union of $\mathfrak{R}_]$ and $\mathfrak{R}_[$, i.e. $\mathfrak{R}(A, B)$ iff either $\mathfrak{R}_](A, B)$ or $\mathfrak{R}_[(A, B)$.

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. Thus any atom containing a tick $(\rhd_{=1}\phi)$ is singular. As a consequence, A is singular iff $\neg A\mathfrak{R}_]A$ iff $\neg A\mathfrak{R}_[A$ (this is expected since the logic is stuttering-insensitive), and that a singular state is only connected to non-singular states. A is *initial* iff it contains $\neg \ominus \top$. Thus it contains no formula of the form: $\phi_1 \mathsf{S} \phi_2$ or $\lhd_I \phi$. It is 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 is exactly represented by the conjunction of the formulae that it contains. For an atom A, we write $\hat{A}$ for that formula, that formula is finite by definition of A. By propositional completeness, we have:

Lemma 2 *$\vdash \bigvee_{A \in \mathfrak{A}} \hat{A}$.*

We define the formula $\mathfrak{R}(A)$ to be $\bigvee_{B | A \mathfrak{R} B} \hat{B}$. $\bigvee_{B | A \mathfrak{R}_] B} \hat{B}$ can be simplified to $\bigwedge_{\bigcirc \phi \in A} \phi$, 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 3 *$\vdash \hat{A} \to \bigcirc \mathfrak{R}_](A)$.*

Proof. $\bigcirc \mathfrak{R}_](\hat{A}) = \bigcirc \bigvee_{B | A \mathfrak{R}_] B} \hat{B} = \bigwedge_{\bigcirc \phi \in A} \bigcirc \phi$. Using (JA) we obtain the thesis. ■

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

Lemma 4 *$\vdash \ominus \hat{A} \to \mathfrak{R}_[(\hat{A})$.*

Now let $\mathfrak{R}^+$ be transitive closure of $\mathfrak{R}$. Since $\mathfrak{R}_] \subseteq \mathfrak{R}^+$, we have:

Lemma 5 *$\vdash \ominus \hat{A} \to \mathfrak{R}^+(\hat{A})$.*

Similarly,

Lemma 6 *$\vdash \hat{A} \to \bigcirc \mathfrak{R}^+(\hat{A})$.*

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

Lemma 7 *$\vdash \hat{A} \to \Box \mathfrak{R}^+(\hat{A})$.*

A 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 $\hat{\mathfrak{S}} = (\hat{\mathfrak{A}}, \hat{\mathfrak{R}})$, where $\hat{\mathfrak{A}}$ is the subset of propositional atoms that are EventClockTL-consistent and $\hat{\mathfrak{R}} = \{(A, B) | \mathfrak{R}(A, B) \text{ and } A, B \in \hat{\mathfrak{A}}\}$. Note that the lemmas above are still valid in the structure $\hat{\mathfrak{S}}$ as only inconsistent atoms are suppressed. We now investigate more deeply the properties of the structure $\hat{\mathfrak{S}}$ and show how we can prove from that structure that the consistent formula α is satisfiable.

A *maximally strongly connected substructure* (MSCS) D is a set of atoms $D \subseteq \hat{\mathfrak{A}}$ of the structure $\hat{\mathfrak{S}}$ such that (i) for all $D_1, D_2 \in D$, $\hat{\mathfrak{R}}^+(D_1, D_2)$ and $\hat{\mathfrak{R}}^+(D_2, D_1)$, i.e. every atom can reach the other atoms of the set D and conversely, and (ii) for all $D_1, D_2 \in \hat{\mathfrak{A}}$ such that $(D_1, D_2) \in \hat{\mathfrak{R}}^+$ and $(D_2, D_1) \in \hat{\mathfrak{R}}^+$ and $D_1 \in D$ then $D_2 \in D$, i.e. D is maximal. A MSCS D is called *initial* if for all $(D_1, D_2) \in \hat{\mathfrak{R}}$ and $D_2 \in D$ then $D_1 \in D$, i.e. D has no incoming edges. Conversely, a MSCS D is called *final* if for all $(D_1, D_2) \in \hat{\mathfrak{R}}$ and $D_1 \in D$ then $D_2 \in D$, i.e. D has no outgoing edges.

Lemma 8 *Every final MSCS D of the structure $\hat{\mathfrak{S}}$ is self-fulfilling, i.e. for every formula of the form $\phi_1 \mathsf{U} \phi_2 \in A$ with $A \in D$, there exists $B \in D$ such that $\phi_2 \in B$.*

Proof. Let us make the hypothesis that there exists $\phi_1 \mathsf{U} \phi_2 \in A$ with $A \in D$ and for all $B \in D$, $\phi_2 \notin B$. By lemma 7, $\vdash \hat{A} \rightarrow \Box \hat{\mathfrak{R}}^+(A)$ and as by hypothesis $\phi_2 \notin B$, for all $B \in \hat{\mathfrak{R}}^+(A)$, by theorem (KA) and a propositional reasoning, we conclude $\vdash \hat{A} \rightarrow \Box \neg \phi_2$. Using the axiom (SF) 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 9 *Every initial MSCS D of the structure $\hat{\mathfrak{S}}$ contains an initial atom, i.e. there exists $A \in D$ such that $\ominus \top \notin A$.*

Proof. By definition of initial MSCS, we know that for all $(D_1, D_2) \in \hat{\mathfrak{R}}^+$ and $D_2 \in D$, then $D_1 \in D$. Let us make the hypothesis that for all $D \in D$, $\ominus \top \in D$. By the mirror of lemma 7 $\vdash \hat{A} \rightarrow \boxminus \bigvee_{B | \hat{\mathfrak{R}}^+(B,A)} \hat{B}$ we conclude, by a propositional reasoning and the hupothesis that $\ominus \top \in D$ for all D such that $\hat{\mathfrak{R}}^+(D, A)$, that $\vdash \hat{A} \rightarrow \boxminus \ominus \top$, but as A is a consistent atom by axiom (BE), we know that $\diamondminus \neg \ominus \top \in A$, thus we obtain a contradiction since $\boxminus \phi \equiv \neg \diamondminus \neg \phi$. ■

In the sequel, we concentrate on particular paths, called runs, of the structure $\hat{\mathfrak{S}}$. A *run* of the structure $\hat{\mathfrak{S}} = (\hat{\mathfrak{A}}, \hat{\mathfrak{R}})$ is an infinite sequence $\sigma = A_0 A_1 \ldots (A_n \ldots A_{n+m})^\omega \ldots$, paired with an infinite sequence of intervals $\bar{I} = I_0 I_1 \ldots I_n \ldots$ such that:

1. Initiality: A_0 is an initial atom;
2. Consecution: for every $i \geq 0$, $(A_i, A_{i+1}) \in \hat{\mathfrak{R}}$;
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. I_0 is singular, and for all $i > 0$, I_i is singular iff I_{i-1} is open, I_i is open iff I_{i-1} is singular;

5. Eventuality: the set $\{A_n, ..., A_{n+m}\}$ is a final MSCS of the structure S.

Note that 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.

Lemma 10 *The transition relation $\hat{\mathfrak{R}}$ of the structure $\hat{\mathfrak{S}}$ is total, i.e. for all atom $A \in \hat{\mathfrak{A}}$, there exists an atom $B \in \hat{\mathfrak{A}}$ such that $\hat{\mathfrak{R}}(A, B)$.*

Proof. We prove $\hat{\mathfrak{R}}_]$ total, i.e. for all $A \in \hat{\mathfrak{A}}, \{\phi | \bigcirc\phi \in A\}$ is consistent. Then it will be included in an atom. Assume it is not. We have then $\bigcirc\phi, \bigcirc\neg\phi \in A$. Using (JA), (N) this yields a contradiction in A. (Note: the (JT) axiom is implicitly used in the definition of $\hat{\mathfrak{R}}$, instead of appearing here). ■

Lemma 11 *For every atom A of the structure $\hat{\mathfrak{S}}$, for every alternating interval sequence $\bar{I}$, there is a run $(\sigma, \bar{I})$ that passes through A.*

Proof. First the alternation and singularity constraints can always be verified by taking stuttering steps when needed and by noting that in $\hat{\mathfrak{S}}$ two singular atoms are never linked by $\hat{\mathfrak{R}}$. It remains us to show that :

1. *Initiality*, i.e. every atom of $\hat{\mathfrak{S}}$ 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 such that $\hat{\mathfrak{R}}^+(B, A)$ then $\neg\ominus\top \notin B$, so by propositional completeness $\ominus\top \in B$. By lemma 7 and a propositional reasoning, we obtain $\vdash \hat{A} \to \boxminus\ominus\top$. Using axiom (BE) and our hypothesis $\ominus\top$, through $\diamondminus\neg\ominus\top$, we obtain a contradiction.

2. *Finality*, i.e. every atom of $\hat{\mathfrak{S}}$ either is part of a final MSCS or can reach one of the final MSCS of $\hat{\mathfrak{S}}$. It is a direct consequence of the fact that $\hat{\mathfrak{R}}$ is total and the fact that $\hat{\mathfrak{S}}$ is finite.

■

A run $\rho = (\sigma, \bar{I})$ of the structure $\hat{\mathfrak{S}}$ is *semantically sound* 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):

1. if σ_i is singular then I_i is singular;

2. if $\phi_1 \mathsf{U} \phi_2 \in \sigma_i$ then:

   - **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
  (a) **either** $\phi_2 \in A_i$
  (b) **or** there exists $j > i$ s.t. $\phi_2 \in A_j$ and for all k s.t. $i \leq k < j$, $\phi_1 \in A_k$;

3. if $\phi_1 \mathsf{S} \phi_2 \in \sigma_i$ then:

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

A semantically sound run is called an *Hintikka sequence*. Next, we show properties of runs:

Lemma 12 *For every run $\rho = (\sigma, \bar{I})$ of the structure $\hat{\mathfrak{S}}$, with $\sigma = A_0 A_1 \dots$, for every A_i such that $\Diamond\phi \in A_i$:*

- *A_i is singular and there exists $j > i$ such that $\phi \in A_j$;*
- *A_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 $\hat{\mathfrak{R}}$:

- let $\hat{\mathfrak{R}}_](A, B)$ and $\Diamond\phi \in A$ then either $\phi \in B$ or $\Diamond\phi \in B$. In fact, recall that $\Diamond\phi \equiv \top \mathsf{U} \phi$, and by definition of $\hat{\mathfrak{R}}_]$, axiom $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc(\phi_2 \vee (\phi_1 \wedge \phi_1 \mathsf{U} \phi_2))$ (UJ) and a propositional reasoning, we obtain that $\top \mathsf{U} \phi \in A$ iff $\phi \in B$ or $\top \mathsf{U} \phi \in B$;

- let $\hat{\mathfrak{R}}_[(A, B)$ and $\Diamond\phi \in A$ then either $\phi \in A$, $\phi \in B$ or $\top \mathsf{U} \phi \in B$. By definition of $\hat{\mathfrak{R}}_[$, axiom $\ominus(\phi_1 \mathsf{U} \phi_2) \leftrightarrow \ominus\phi_2 \vee (\ominus\phi_1 \wedge \phi_2 \vee (\phi_1 \wedge \phi_1 \mathsf{U} \phi_2))$ mirror of (JS) and a propositional reasoning, we obtain $\phi \in A$ or $\phi \in B$ or $\top \mathsf{U} \phi \in B$.

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 A_i is singular (and thus right closed), $j \geq i$ if A_i is not singular (and thus associated with an open interval) or ϕ is never true and $\Diamond\phi$ propagates for the rest of the run. But let us show that this last possibility is excluded by our definition of run. In fact, every run eventually loops into a final self-fulfilling MSCS D. Then either the fatality ϕ associated with $\Diamond\phi$ is realized before this looping or $\Diamond\phi \in D$ and by lemma 8 the fatality $\phi \in D$ and is thus eventually realized. ■

Lemma 13 *For every run $\rho = (\sigma, \bar{I})$ of the structure $\hat{\mathfrak{S}}$, for every position i in the run if $\phi_1 \mathsf{U} \phi_2 \in A_i$ then the property 2 of timed Hintikka sequences 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** $\phi_2 \in A_j$
    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 $\phi_1 \mathsf{U} \phi_2 \to \Diamond \phi_2$ and lemma 12, 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 $A_i R_{]} A_{i+1}$ (as A_i is right closed) and thus for all $\bigcirc \phi \in A_i, \phi \in A_{i+1}$ by definition of $R_{]}$. By axiom $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc(\phi_1 \mathsf{U} \phi_2)$, we conclude that $\phi_1 \mathsf{U} \phi_2 \in A_{i+1}$ and by axiom $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc(\phi_2 \vee (\phi_1 \wedge \bigcirc(\phi_1 \mathsf{U} \phi_2)))$, $\bigcirc(\phi_1 \vee \phi_2) \leftrightarrow \bigcirc \phi_1 \vee \bigcirc \phi_2$, $\bigcirc(\phi_1 \wedge \phi_2) \leftrightarrow \bigcirc \phi_1 \wedge \bigcirc \phi_2$, and the fact that by hypothesis $\phi_2 \notin A_{i+1}$, a propositional reasoning 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 case : (i) I_k is open and thus I_{k-1} is singular and right closed. We have $A_{k-1} R_{]} A_k$, and thus for all $\bigcirc \phi \in C(\psi), \bigcirc \phi \in A_i \leftrightarrow \phi \in A_{i+1}$ by definition of $R_{]}$. As $\phi_1 \mathsf{U} \phi_2 \in A_{k-1}$ by induction hypothesis and the axiom $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc(\phi_1 \mathsf{U} \phi_2)$, we conclude that $\phi_1 \mathsf{U} \phi_2 \in A_k$. Using the axioms $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc(\phi_2 \vee (\phi_1 \wedge \bigcirc(\phi_1 \mathsf{U} \phi_2)))$, $\bigcirc(\phi_1 \vee \phi_2) \leftrightarrow \bigcirc \phi_1 \vee \bigcirc \phi_2$, $\bigcirc(\phi_1 \wedge \phi_2) \leftrightarrow \bigcirc \phi_1 \wedge \bigcirc \phi_2$, and the fact that $\phi_2 \notin A_k$, and a proposition reasoning, we conclude that $\phi_1 \in A_k$. (ii) I_k is closed which implies that I_{k-1} is right open and $A_{k-1} R_{[} A_k$. By definition of $R_{[}$ we have that for all $\ominus \phi \in C(\psi), \ominus \phi \in A_k \leftrightarrow \phi \in A_{k-1}$. 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, the axiom $\ominus(\phi_1 \mathsf{U} \phi_2) \leftrightarrow \ominus \phi_2 \vee (\ominus \phi_1 \wedge (\phi_2 \vee (\phi_1 \wedge \phi_1 \mathsf{U} \phi_2)))$, 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 $\phi_1 \mathsf{U} \phi_2 \rightarrow \Diamond \phi_2$ and lemma 12 we know that there exists a later atom A_j $j \geq i$ 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 completeness but we use this property in the lemmas over real-time operators.

Lemma 14 *For every run $\rho = (\sigma, I)$ of the structure $\hat{\mathfrak{S}}$, for every position i in the run, 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** *$\phi_2 \in A_j$*
  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 $\phi_1 \mathsf{U} \phi_2 \in A_j$ 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: (i) if A_{j-1} is right closed then we have $A_{j-1} R_{]} A_j$ and by definition of $R_{]}$, $\bigcirc \phi_2 \in A_{j-1}$. Using the axiom $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc \phi_2 \vee (\phi_1 \wedge \phi_1 \mathsf{U} \phi_2)$, we deduce by a propositional reasoning that $\phi_1 \mathsf{U} \phi_2 \in A_{j-1}$. (ii) if A_{j-1} is right open then we know that $j - 1 > i$ (as A_i is singular by hypothesis) and thus $\phi_1 \in A_{j-1}$. Also as $A_{j-1} R_{[} A_j$, $\ominus \phi_1 \in A_j$. Using the axiom $\ominus(\phi_1 \mathsf{U} \phi_2) \leftrightarrow \ominus \phi_2 \vee (\ominus \phi_1 \wedge (\phi_2 \vee (\phi_1 \wedge \phi_1 \mathsf{U} \phi_2)))$ and a propositional reasoning, we obtain $\ominus(\phi_1 \mathsf{U} \phi_2) \in A_j$ and by definition of $R_{[}$, $\phi_1 \mathsf{U} \phi_2 \in A_{j-1}$.
   - 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: (i) I_{j-l} is right closed. Then we have $A_{j-l} R_{]} A_{j-(l-1)}$ and by definition of $R_{]}$, for all $\bigcirc \phi \in C(\psi)$, $\bigcirc \phi \in A_{j-l}$ iff $\phi \in A_{j-(l-1)}$,thus $\bigcirc(\phi_1 \mathsf{U} \phi_2) \in A_{j-l}$ and by axiom

$\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc(\phi_1 \mathsf{U} \phi_2)$, we have that $\phi_1 \mathsf{U} \phi_2 \in A_{j-l}$. *(ii)* A_{j-l} is right open. Then we have $A_{j-l} R_{[} A_{j-(l-1)}$ and by definition of $R_{[}$, for all $\ominus\phi \in C(\psi)$, $\ominus\phi \in A_{j-(l-1)}$ iff $\phi \in A_{j-l}$. We know that by hypothesis, $\phi_1 \in A_{j-l}$ as $j - l \neq i$ (A_i is singular and A_{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 axiom $\ominus(\phi_1 \mathsf{U} \phi_2) \leftrightarrow \ominus\phi_2 \vee (\ominus\phi_1 \wedge (\phi_1 \wedge \phi_1 \mathsf{U} \phi_2))$ and a propositional reasoning, we obtain $\ominus(\phi_1 \mathsf{U} \phi_2) \in A_{j-(l-1)}$ and by definition of $R_{[}$ 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 $A_i R_{]} A_i$, by definition of $R_{]}$, we have $\bigcirc\phi_2 \in A_i$. By the axiom $\phi_1 \mathsf{U} \phi_2 \leftrightarrow \bigcirc\phi_2 \vee (\phi_1 \wedge \bigcirc(\phi_1 \mathsf{U} \phi_2))$ 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 EventClockTL, i.e. the logic LTR.

Lemma 15 *A run ρ has the Hintikka property for* LTR *formula: for every* LTR *formula $\phi \in C, \phi \in \rho(t) \leftrightarrow (\rho, t) \models \phi$.*

As a consequence, we have the following theorem:

Theorem 3 *Every* LTR *formula that is consistent with the qualitative axioms is satisfiable.*

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

4.2 Quantitative part

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

1. if $\triangleright_I \phi \in \rho(t)$ then at a later time $t' \in t + I, \phi \in \rho(t')$ and $\forall t'' : t < t'' < t + I$, $\neg\phi \in \rho(t'')$

2. if $\triangleleft_I \phi \in \rho(t)$ then at an earlier time t' with $t' \in t - I, \phi \in \rho(t')$ 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 $\hat{\mathfrak{S}}$, 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 $\phi \in R$,

- $\rhd_{=1}\phi$ 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 (LO), (JP));
- $(\phi \wedge \ominus\neg\phi) \vee (\neg\phi \wedge \bigcirc\phi)$ is called its *reset*.

A *constraint* is a real-time formula of an atom A_i. The *reference* of a constraint is the index e at which its previous event, tick or reset occurred. The reference is always singular. The *anchor* of a constraint is the index j at which its next event, tick or reset occurred. 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. It is sufficient to solve small constraints, as we shall see. Thus we define the *scope* of a history constraint as the interval between the event and the next tick or reset. 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). The scope of an inequality extends from an event to a reset. Constraints can be partially ordered by scope: it is enough to solve constraints of maximal scope, as we shall see. An index is *owned* by a constraint, if it is in the scope of no other constraint with an earlier reference. A constraint of maximal scope always owns indexes: they are found at the end of its scope. We will also use partial inequalities, representing the constraints known up to an index of a path. Whether an atom is in the scope of a constraint, and whether it is an equality, can be deduced from its contents. The table below shows the contents of an atom A_i that is the anchor of an equality:

Table 1: Equality constraints

reference	anchor 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 that defines an inequality:

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.

Table 2: Inequality constraints

reference	in A_i	anchor
$\triangleright_{=1}\phi$ (tick)	$\triangleright_{<1}\phi \wedge \neg\phi \mathsf{S}^+ \triangleright_{=1} \phi$	ϕ (event)
$\phi \wedge \bigcirc\neg\phi$ (event)	$\triangleleft_{<1}\phi \wedge \neg\phi\hat{\mathsf{S}}\phi$	$\triangleleft_{=1}\phi \vee \phi$ (tick or reset)
$(\phi \wedge \bigcirc\neg\phi) \vee (\ominus\phi \wedge \neg\phi)$ (reset)	$\neg \triangleright_{=1} \phi\mathsf{S}\phi \wedge \neg(\neg\phi\mathsf{S} \triangleright_{=1} \phi) \wedge (\triangleright_{<1}\phi \vee \phi)$	ϕ (event)

From any run $\rho = (\sigma, \bar{I})$, we now build a timed run $Attr(\rho) = (\sigma, \bar{J})$ by attributing well-chosen intervals to the atoms of the run. Recall that the interval information $\bar{I}$ in the run ρ has only a qualitative value: the intervals associated to the atoms are either open or singular. We now show that we can attribute a new sequence of intervals $\bar{J}$, given the timed run $Attr(\rho)$ that will satisfy the real-time constraints. We proceed by induction along the run, attributing time points $[t_i, t_i]$ to the singular atoms A_i with i even. Therefore, an open interval (t_{i-1}, t_{i+1}) is attributed to non-singular atoms A_i with i odd.

1. Base: We attribute the interval $[0, 0]$ to the initial atom A_0.
2. Induction: we identify 20 and solve the tightest constraint, that owns the current index i. We define e as the reference of this tightest constraint, by cases:
   (a) equality constraints:
      i. If there is an $\triangleleft_{=1}\psi \in A_i$ there has been a last (singular) atom A_e containing ψ before at time t_e.
      ii. Else, if $\ominus\neg\psi \wedge \psi \wedge \neg\psi\mathsf{S} \triangleright_{=1} \psi \in A_i$ there has been a last atom A_e containing $\triangleright_{=1}\psi$ before A_i, at time t_e.

      We attribute $[t_e + 1, t_e + 1]$ to A_i.
   (b) inequality constraints:
      i. Else, we compute the earliest reference e of the small clocks using table 2. t_i has to be between t_{i-2} and $t_e + 1$. We choose $t_i = (t_{i-2} + t_e + 1)/2$.
      ii. Finally, when all clocks are undefined or blocked, we attribute (say) $t_{i-2} + 1/2$ to A_i.

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

Lemma 16 *If two equality constraints have the same anchor i, their references e_1, e_2 are identical.*

Proof. Four combinations of equality constraints are possible:

- The first constraint is $\lhd_{=1}\phi$
  - The second constraint is $\lhd_{=1}\psi$: A_i contains $\neg\psi\mathsf{U}^{\geq}\lhd_{=1}\phi, \neg\lhd_{=1}\psi\mathsf{U}^{\geq}\lhd_{=1}\phi$ since its eventuality $\lhd_{=1}\phi$ is true now. It contains $\lhd_{=1}\psi$, and thus $\lhd_{\leq 1}\psi$ by (OR). We apply (SHH) 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 14 that ψ cannot occur before ϕ, and conversely, thus they occur in the same atom.
  - The second constraint is the event $\psi \wedge \neg\circleddash\psi$ with $\neg\psi\mathsf{S}\rhd_{=1}\psi$: then A_i contains $\neg\phi\mathsf{U}^{\geq}\psi, \neg\lhd_{=1}\phi\mathsf{U}^{\geq}\psi$ since its eventuality ψ is true now. It contains $\lhd_{=1}\psi$, and thus $\lhd_{\leq 1}\psi$ by (OR). We apply (SHP) to obtain $\neg\rhd_{=1}\psi\mathsf{S}\phi$.

    Since A_i contains $\neg\psi\mathsf{U}^{\geq}\lhd_{=1}\phi$ since its eventuality $\lhd_{=1}\phi$ is true now. We apply (SPH) to obtain $\neg\phi\mathsf{Z}\rhd_{=1}\psi \vee \neg\phi\mathsf{Z}\psi$. Since $\neg\psi\mathsf{S}\rhd_{=1}\psi$, we know that the first branch is true.

    These formulae imply by Lemma 14 that ψ cannot occur before ϕ, and conversely, thus they occur in the same atom.
- The first constraint is the event ϕ with $\neg\phi\mathsf{S}\rhd_{=1}\phi$:
  - The second constraint is $\lhd_{=1}\psi$: This case is simply the previous one, with ϕ, ψ inverted.
  - The second constraint is the event ψ with $\neg\psi\mathsf{S}\rhd_{=1}\psi$: A_i contains $\neg\psi\mathsf{U}^{\geq}\phi$ since its eventuality ϕ is true now. We apply (SPP) to obtain $\neg\rhd_{=1}\phi\mathsf{Z}(\rhd_{=1}\psi \vee \psi)$. By $\neg\psi\mathsf{S}\rhd_{=1}\psi$, the tick $\rhd_{=1}\psi$ occurred. We repeat this with ψ, ϕ inverted. These formulae imply by Lemma 14 that $\rhd_{=1}\psi$ cannot occur before $\rhd_{=1}\phi$, and conversely, thus they occur in the same atom.

■

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

Lemma 17 *If A_i is in the scope of an inequation, and the anchor of an equation, then the reference A_j of the inequation is after the reference A_e of the equation.*

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

1. $\lhd_{<1}\psi, \neg\psi\hat{\mathsf{S}}\psi \in A_i$:
   let $j \leq i$ be its reference (its event), i.e. $\psi \in A_j$. We must show that $e < j$. The equation can be:
   - $\lhd_{=1}\phi \in A_i$ and $\phi \in A_e$:
     A_i contains $\neg\psi\mathsf{U}^{\geq}\lhd_{=1}\phi, \neg\lhd_{=1}\psi\mathsf{U}^{\geq}\lhd_{=1}\phi$ since its eventuality

$\triangleleft_{=1}\phi$ is true now. We apply (SHH) to obtain $\neg\phi \mathsf{S} \psi$, meaning by the mirror of lemma 14 that $e \leq j$. $\neg\psi\mathsf{S}\phi \notin A_i$, for otherwise we apply (OHH) yielding$\triangleleft_{<1}\phi \in A_i$ contradicting $\triangleleft_{=1}\phi \in A_i$ by (AND), so we conclude $e < j$.

- $\phi, \neg\phi\mathsf{S} \triangleright_{=1} \phi \in A_i$ and $\triangleright_{=1}\phi \in A_e$:
  by (SHP) $\neg \triangleright_{=1} \phi\mathsf{S}\psi \in A_j$, so $e \leq j$. We cannot have the reverse $\neg\psi\mathsf{S}\triangleright_{=1}\phi$, for otherwise we apply the mirror of (OHP) and deduce $\neg\phi \in A_i$, so we conclude $e < j$.

2. $\neg \triangleright_{=1} \psi\mathsf{S}\psi \wedge \neg(\neg\psi\mathsf{S} \triangleright_{=1} \psi) \wedge (\triangleright_{<1}\psi \vee \psi) \in A_i$:
   let $j \leq i$ be its reference (a reset), i.e. $\phi \wedge \bigcirc\neg\phi \in A_j$. Since $\triangleright_{<1}\psi \in A_{i-1}$ and there is no intervening ψ between j and i, the transition rules imply $\triangleright_{<1}\psi \in A_{j+1}$ and thus $\triangleright_{\leq 1}\psi \in A_j$ by (JH). We must show that $e < j$. The equation can be:

   - $\triangleleft_{=1}\phi \in A_i$ and $\phi \in A_e$:
     if $\triangleright_{<1}\psi \vee \psi \in A_i$, we apply (SPH) to obtain $\neg\phi\mathsf{Z} \triangleright_{=1} \psi \vee \neg\phi\mathsf{Z}\psi$, which means $e \leq j$. The first branch is false by hypothesis as $\neg(\neg\psi\mathsf{S} \triangleright_{=1} \psi) \in A_i$, since we deal with an inequality. Thus $\neg \triangleright_{=1} \psi \in A_j$; using $\triangleright_{\leq 1}\psi \in A_j$, $\triangleright_{<1}\psi \in A_j$. Again because there are no intervening ψ between j and i, using lemma 14 we have $\neg\psi\mathsf{U} \triangleleft_{=1} \phi \in A_j$. Using the mirror of (OPH), $\triangleleft_{<1}\phi \wedge \neg\phi \in A_j$, thus $j = e$ is impossible, since $\neg\phi \in A_j$ and $\phi \in A_e$. We conclude $e < j$.
   - $\phi, \neg\phi\mathsf{S} \triangleright_{=1} \phi \in A_i$ and $\triangleright_{=1}\phi \in A_e$:
     so $\neg\psi\mathsf{U}^{\geq}\phi \in A_i$, and we use (SPP) to obtain $\neg \triangleright_{=1} \phi\mathsf{Z} \triangleright_{=1} \psi \vee \neg \triangleright_{=1} \phi\mathsf{Z}\psi \in A_i$. ψ must occur first ($\neg \triangleright_{=1} \psi\mathsf{S}\psi \in A_i$), so the first case is excluded, giving $\neg \triangleright_{=1} \psi \in A_j$; using $\triangleright_{\leq 1}\psi \in A_j$, $\triangleright_{<1}\psi \in A_j$. Again because there are no intervening ψ between positions j and i, we have $\neg\psi\mathsf{U} \triangleleft_{=1} \phi \in A_j$. Using the mirror of (OHH), $\triangleright_{<1}\phi \in A_j$. The second case is thus true, and means $e \leq j$. $e = j$ is impossible, since $\triangleright_{<1}\phi \in A_j \wedge \triangleright_{=1}\phi \in A_e$. We conclude $e < j$.

3. $\triangleright_{<1}\psi \wedge \neg\psi\mathsf{S}^{+} \triangleright_{=1} \psi \in A_i$ and $\triangleright_{=1}\psi \in A_j$:
   let $j \leq i$ be its reference, i.e. $\triangleright_{=1}\psi \in A_j$. We must show that $e < j$. The equation can be:

   - $\triangleleft_{=1}\phi \in A_i$ and $\phi \in A_e$:
     thus $\neg\psi\mathsf{U}^{\geq} \triangleleft_{=1} \phi \in A_i$; by (SPH) $\neg\phi\mathsf{Z} \triangleright_{=1} \psi \vee \neg\phi\mathsf{Z}\psi \in A_i$. 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 $e \leq j$.
   - $\phi, \neg\phi\mathsf{S} \triangleright_{=1} \phi \in A_i$ and $\triangleright_{=1}\phi \in A_e$:
     using (SPP), we obtain $\neg \triangleright_{=1} \phi\mathsf{Z} \triangleright_{=1} \psi \vee \neg \triangleright_{=1} \phi\mathsf{Z}\psi \in A_i$. The

first case is true, by hypothesis, and gives $e \leq j$. We cannot assume $e = j$, because the mirror of lemma 16 then gives $\psi \in A_i$, contradicting $\neg\psi \mathsf{S}^+ \triangleright_{=1} \psi \in A_i$. We conclude $e < j$.

■

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

Lemma 18 *The sequence t_i built by Attr is increasing.*

Proof. In the notation of the definition, this amounts to prove $t_{i-2} < t_e + 1$ when e is defined, since t_i is either $t_e + 1$ (in the case of an equality) or the middle point of $(t_{i-2}, t_e + 1)$ (in the case of an inequality). If e 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:
   - no constraint is active, e is undefined;
   - $e = 0, t_e = 0, t_{i-2} = 0$. We just have to prove $0 < 1$.
2. induction: We divide in cases according to the constraint selected at $i - 2$, whose reference is called e_{i-2}:
   (a) an equality: by lemmas 16, 17, its reference was before, i.e., $e_{i-2} < e$. By inductive hypothesis, t_i is increasing: $t_{e_{i-2}} < t_e$. Thus $t_{i-2} = t_{e_{i-2}} + 1 < t_e + 1$.
   (b) an inequality: Thus the reference $e_{i-2} \leq e_i$, since it was obtained by sorting. By inductive hypothesis, t_i is increasing: so $t_{e_{i-2}} \leq t_e$. By inductive hypothesis, $t_{i-4} < t_{e_{i-2}} + 1$. Thus $t_{i-2} = (t_{i-4} + t_{e_{i-2}} + 1)/2 < (t_{e_{i-2}} + 1 + t_{e_{i-2}} + 1)/2 = t_{e_{i-2}} + 1 \leq t_e + 1$.

■

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

Lemma 19 *The sequence of intervals $\bar{I}$ of $Attr(\rho) = (\sigma, \bar{I})$ built above 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 $\bar{\sigma} = A_0 A_1 \ldots (A_n A_{n+1} \ldots A_{n+m})^\omega$ 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. Let i be owned by such a constraint. The time spent in the scope of the constraint until i is at least $1/2$: Since e is the beginning of the scope of the constraint, and, $t_{i-2} \geq t_e$, and $t_i \geq (t_{i-2}+t_e+1)/2 \geq t_e+1/2$. Furthermore, note that the scope cannot be greater than one cycle: thus the time spent is a cycle is at least $1/2$.

■

This procedure correctly solves all constraints:

Lemma 20 *The interval attribution Attr transforms any run ρ in a well-timed run Attr(ρ).*

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

1. Let $\triangleleft_I \psi \in \rho(t) = A_i$. We must show that the next ψ occurs in $t - I$. $\triangleleft_I \psi$ can be:

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

   - the mirror of the eventuality rule (P-S) guarantees ψ has occurred: $\exists j < i \quad \psi \in A_j$;
   - the transition rules (J axioms) guarantee that there is first a time where equality is satisfied: $\exists k \quad i < k < j \wedge \triangleleft_{=1}\psi \in A_k$;
   - the reset rule (CR) 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.

   (b) $\triangleleft_{=1}\psi$: Since this is an equality constraint, the algorithm *Attr* must have chosen an equality constraint with reference e. Thus $t_i = t_e + 1$. By lemma 16, the reference event ϕ is also in A_e.

   (c) $\triangleleft_{<1}\psi$: Let $j \leq i$ be its reference, $\phi \in A_j$. The constraint selected by *Attr* at i can be:

   - an equality, by lemma 17, its reference $e < j$, so that $t_i = t_e + 1 < t_j + 1$.
   - or the constraint chosen in A_i is an inequality. The pair $\triangleleft_{<1}\psi \in A_i, \psi \in A_j$ is also an inequality in A_i: let f be its reference. The algorithm has selected the constraint with the earliest reference e. Thus $e \leq f \leq j \leq i$, and $t_i < t_e + 1$. Thus $t_i < t_j + 1$.

2. Let $\triangleright_I \psi \in \rho(t) = A_i$. We must show that the next ψ occurs in $t + I$. $\triangleright_I \psi$ can be:

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

- the eventuality rule (P-S) guarantees ψ will occur: $\exists j < i \quad \psi \in A_j$;
- the transition rules (J axioms) guarantee that there is first a tick: $\exists k \quad i < k < j \wedge \triangleright_{=1}\psi \in A_k$;
- the reset rule (CR) guarantees that satisfying the equality will entail satisfying the greater-than constraint, since they refer to the same anchor event, and since the equality is later.

(b) $\triangleright_{=1}\psi$: 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 16, its reference is i. Thus $t_j = t_i + 1$.

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

- an equality by lemma 17 its reference $e < i$, so that $t_j = t_e + 1 < t_i + 1$.
- 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 reference. The algorithm has selected the constraint with the earliest reference e. Thus $e \leq f \leq i \leq j$, and $t_j < t_e + 1$. Thus $t_j < t_i + 1$.

■

Theorem 4 *A timed run has the Hintikka property for* EventClockTL*:* $\forall \phi \in C, \phi \in \rho(t) \leftrightarrow (\rho, t) \models \phi$.

Proof. In lemma 14, we proved this for the (qualitative) runs. In theorem 20, we proved the implication for the real-time operators. It remains only to prove the converse, which also results from timed: if $\triangleright_I \phi \notin \rho(t)$, by maximality $\neg \triangleright_I \phi \in \rho(t)$ and thus either $\neg \Diamond \phi \in \rho(t)$ and the result follows by lemma 14, or $\triangleright_I \phi \in \rho(t)$ and the result follows by lemma 20. ■

Finally, we obtain the desired theorem:

Theorem 5 *Every* EventClockTL*-consistent formula* α *is satisfiable.*

Proof. If α is a EventClockTL-consistent formula then there exists an α-monitored atom A_α in $\hat{\mathfrak{S}}$. By lemma 11, there exists a set of runs Σ that pass through A_α and by the properties of the procedure *Attr*, lemma 13, lemma 19 and lemma 20, at least one run $(\sigma, \bar{I}) \in \Sigma$ has the Hintikka property for EventClockTL. It is direct to see that $(\sigma \cap \mathsf{P}, \bar{I})$ is a model for α at time $t \in I_\alpha$ (the interval of time associated to A_α in $(\sigma, \bar{I})$) and thus α is satisfiable. ■

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 $\rhd_{<1} \rhd_{=1} \ldots \rhd_{=1} \phi$. It will also record the ordering of the fractional parts of the clocks: this is coded here by formulae of the form $\neg \rhd_{=1} \ldots \rhd_{=1} \phi \mathsf{U} \rhd_{=1} \ldots \rhd_{=1} \psi$. 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 [10].

5 Translating EventClockTLand MetricIntervalTL

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 [10] 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:

$$\phi \hat{\mathsf{U}}_I \psi \leftrightarrow \psi \vee (\phi \hat{\mathsf{U}}_J \psi) \quad \text{with } J = I \setminus \{0\} \text{ and } 0 \in I \tag{R0}$$

Then we replace bounded untils $\hat{\mathsf{U}}_I$ by simpler $\Diamond_I$:

$$\phi \hat{\mathsf{U}}_I \psi \leftrightarrow \Box_{\leq I}(\psi \vee \phi \hat{\mathsf{U}} \psi) \wedge \Box_{<_0 I}(\phi \hat{\mathsf{U}} \psi) \wedge \Box_{<I} \phi \wedge \Diamond_I \psi \tag{RU}$$

where the intervals $\leq I = \{t > 0 | \forall t_i \in I, t \leq t_i\}$, $< I = \{t > 0 | \forall t_i \in I, t < t_i\}$, $<_0 I = \{t \geq 0 | \forall t_i \in I, t < t_i\}$.

We suppress classical until using:

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

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

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

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

For finite intervals with left bound equal to 0, we use the $\triangleright$ operator: we reduce the length of the interval to 1 using:

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

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

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 (NLE) and (NLT).

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:

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

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

$$\Diamond_{(l,l+1)} \phi \leftrightarrow \Diamond_{[l-1,l)} \triangleright_{=1} \bigcirc \phi \vee \Diamond_{(l-1,l)} \triangleright_{=1} \phi \vee \Box_{(l-1,l]} \triangleright_{<1} \phi \tag{FOO}$$

$$\Diamond_{(l,l+1]} \phi \leftrightarrow \Diamond_{[l-1,l)} \triangleright_{=1} \bigcirc \phi \vee \Diamond_{(l-1,l]} \triangleright_{=1} \phi \vee \Box_{(l-1,l]} \triangleright_{<1} \phi \tag{FOC}$$

$$\Diamond_{[l,l+1)} \phi \leftrightarrow \Diamond_{[l-1,l)} \triangleright_{=1} \bigcirc \phi \vee \Diamond_{[l-1,l)} \triangleright_{=1} \phi \vee \Box_{(l-1,l]} \Diamond_{[0,1)} \phi \tag{FCO}$$

$$\Diamond_{[l,l+1]} \phi \leftrightarrow \Diamond_{[l-1,l)} \triangleright_{=1} \bigcirc \phi \vee \Diamond_{[l-1,l]} \triangleright_{=1} \phi \vee \Box_{(l-1,l]} \Diamond_{[0,1)} \phi \tag{FCC}$$

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

$$\triangleright_{<1} \phi \leftrightarrow (\neg \phi \hat{\mathsf{U}} \phi \wedge \neg \triangleright_{=1} \phi \mathsf{U}^{+} \phi) \vee (\neg (\neg \phi \hat{\mathsf{U}} \phi) \wedge \neg \triangleright_{=1} \bigcirc \phi \mathsf{U}^{+} \bigcirc \phi) \tag{LT=}$$

showing that the very basic operators $\triangleright_{=1}$ and its mirror image have the same expressive power as full $\mathsf{MetricIntervalTL}$.

The converse translation is much simpler:

$$\triangleright_I \phi \leftrightarrow \neg \Diamond_{<I} \phi \wedge \Diamond_{I \setminus \{0\}} \phi \tag{P}$$

$$\phi \mathsf{U} \psi \leftrightarrow (\phi \vee \psi) \hat{\mathsf{U}} \psi \tag{U}$$

5.1 Axiomatization of MetricIntervalTL

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

Indeed, we have translations T : EventClockTL $\rightarrow$ MetricIntervalTL, S : MetricIntervalTL $\rightarrow$ EventClockTL. Therefore when we want 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:

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

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

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 (P), (U)) is so simple that it can be considered as a mere shorthand. Thus the axioms (RE)–(SHP) and (0)–(FCC) form a complete axiomatization of MetricIntervalTL, with $\triangleright_I, \mathsf{U}$ now understood as shorthands.

6 Conclusion

The specification of real-time systems using dense time is more natural, and has many semantical advantages, but requires our discrete-time techniques [8, 15] to be generalized. The model-checking and decision techniques have been generalized in [2, 3].

This paper provides complete axiom systems and proof-building procedures for linear real time, extending the technique of [16]. This procedure can be used to automate the proof construction of propositional fragments of a larger proof.

Our work also presents the following shortcomings, that we hope to address in the future:

- 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 explain why we have not generalized the axioms, even if 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 proofs constructed by our procedure are often tedious case analyses. A proof beautification procedure will be useful when the proof has to be understood by a user, e.g. when the user is attempting to generalize a machine-generated propositional proof to a first-order one. This procedure would use the nicer axioms mentioned in the previous point.

- The logics used in this paper assume that concrete values are given for real-time constraints. As demonstrated in the HyTech checker [12], 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. We hope to obtain a similar procedure for the validity of MetricIntervalTL formulae.

- The extension of the results of this paper to first-order variants of MetricIntervalTL should be explored. Fragments with a complete proof-building procedure are our main interest.

- 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 [20].

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. Back to the future: towards a theory of timed regular languages. In *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*, pages 177–186. IEEE Computer Society Press, 1992.

[6] 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.

[7] 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.

[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] 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.

[10] T. Henzinger, J.-F. Raskin, and P.-Y. Schobbens. The regular real-time languages. In Kim G. Larsen, editor, *ICALP 98: Automata, Languages, and Programming*, Lecture Notes in Computer Science. Springer-Verlag, 1998.

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] Z. Manna and A. Pnueli. Completing the temporal picture. In G. Ausiello, M. Dezani-Ciancaglini, and S. Ronchi Della Rocca, editors, *ICALP 89: Automata, Languages, and Programming*, Lecture Notes in Computer Science 372, pages 534–558. Springer-Verlag, 1989.

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

[19] 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.

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

I N F O R M A T I K

Below you find a list of the most recent technical reports of the research group *Logic of Programming* at the Max-Planck-Institut für Informatik. They are available by anonymous ftp from our ftp server `ftp.mpi-sb.mpg.de` under the directory `pub/papers/reports`. Most of the reports are also accessible via WWW using the URL `http://www.mpi-sb.mpg.de`. If you have any questions concerning ftp or WWW access, please contact `reports@mpi-sb.mpg.de`. Paper copies (which are not necessarily free of charge) can be ordered either by regular mail or by e-mail at the address below.

Max-Planck-Institut für Informatik
Library
attn. Birgit Hofmann
Im Stadtwald
D-66123 Saarbrücken
GERMANY
e-mail: `library@mpi-sb.mpg.de`

MPI-I-98-2-011	A. Degtyarev, A. Voronkov	Equality Reasoning in Sequent-Based Calculi
MPI-I-98-2-010	S. Ramangalahy	Strategies for Conformance Testing
MPI-I-98-2-009	S. Vorobyov	The Undecidability of the First-Order Theories of One Step Rewriting in Linear Canonical Systems
MPI-I-98-2-008	S. Vorobyov	AE-Equational theory of context unification is Co-RE-Hard
MPI-I-98-2-007	S. Vorobyov	The Most Nonelementary Theory (A Direct Lower Bound Proof)
MPI-I-98-2-006	P. Blackburn, M. Tzakova	Hybrid Languages and Temporal Logic
MPI-I-98-2-005	M. Veanes	The Relation Between Second-Order Unification and Simultaneous Rigid E-Unification
MPI-I-98-2-004	S. Vorobyov	Satisfiability of Functional+Record Subtype Constraints is NP-Hard
MPI-I-98-2-003	R.A. Schmidt	E-Unification for Subsystems of S4
MPI-I-97-2-012	L. Bachmair, H. Ganzinger, A. Voronkov	Elimination of Equality via Transformation with Ordering Constraints
MPI-I-97-2-011	L. Bachmair, H. Ganzinger	Strict Basic Superposition and Chaining
MPI-I-97-2-010	S. Vorobyov, A. Voronkov	Complexity of Nonrecursive Logic Programs with Complex Values
MPI-I-97-2-009	A. Bockmayr, F. Eisenbrand	On the Chvátal Rank of Polytopes in the 0/1 Cube
MPI-I-97-2-008	A. Bockmayr, T. Kasper	A Unifying Framework for Integer and Finite Domain Constraint Programming
MPI-I-97-2-007	P. Blackburn, M. Tzakova	Two Hybrid Logics
MPI-I-97-2-006	S. Vorobyov	Third-order matching in $\lambda \rightarrow$-Curry is undecidable
MPI-I-97-2-005	L. Bachmair, H. Ganzinger	A Theory of Resolution
MPI-I-97-2-004	W. Charatonik, A. Podelski	Solving set constraints for greatest models
MPI-I-97-2-003	U. Hustadt, R.A. Schmidt	On evaluating decision procedures for modal logic
MPI-I-97-2-002	R.A. Schmidt	Resolution is a decision procedure for many propositional modal logics