Metric Temporal Logic with Durations

Yassine Lakhneche
Institut für Informatik und Praktische Mathematik
Christian-Albrechts-Universität zu Kiel
Preußerstr. 1-9, D-24105 Kiel, Germany
e-mail: yl@informatik.uni-kiel.d400.de

Jozef Hooman
Dept. of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
e-mail: wsinjh@win.tue.nl

Abstract. *We present a formal framework based on metric temporal logic (MTL) for specifying and verifying real-time systems with a continuous environment. Metric temporal logic is extended to allow specification of properties about duration of system's states. We prove that every formula of the duration calculus (DC) can be translated into an equivalent MTL-$\int$ formula. Expressiveness of DC and MTL-$\int$ are compared. We formulate axioms for MTL-$\int$ and a sound rule for proving duration properties of timed transition systems.*

1 Introduction

In this paper, we extend metric temporal logic [16, 17, 3] (MTL for short) with a duration concept similar to the one in the duration calculus. We present a specification language MTL-$\int$ that extends MTL to allow the expression of properties about durations of system's states. Axioms for proving valid theorems about those properties are presented and proved sound. Furthermore, we extend the proof methodology presented in [12] by a proof rule for proving *limited-duration properties* of timed transition systems. A limited-duration property imposes a bound on the duration of a system's state. A typical limited-duration property is the requirement that the duration of a critical state is in any interval of length α less than β. Furthermore, we show that each formula of duration calculus can be translated into MTL-$\int$ and that MTL-$\int$ is more expressive than the duration calculus.

Hybrid systems are reactive systems involving components with continuous changes. Computer controlled manufacturing and transport systems are typical hybrid systems with discrete components, as the control program, that act in a continuous environment. In the last few years a number of formal methods for dealing with hybrid systems have been suggested in the literature. Some of the researchers argue that continuously changing observables can be modelled by the same techniques that are used to model time [25, 1, 21], others have suggested techniques for extending existing models to hybrid systems [10, 22, 26, 27].

While many systems can be analysed in a model where continuous changes are represented by discrete events, this may lead in some cases to a discrepancy between the real physical system and its representation in the model resulting in an unreliable analysis and inconsistent conclusions. Hybrid systems are by far the most complex and critical reactive systems; therefore, formal methods for their analysis, synthesis, and verification are needed.

An important class of properties of hybrid systems are those about durations of system's states. It is often the case that the states of a hybrid system can be classified in critical and non-critical states. The analysis of such systems requires the ability to specify and prove relations between these states and their durations. If one uses the set of nonnegative reals as time domain and functions $f_B : \mathbf{R}_{\geq 0} \rightarrow \{0, 1\}$, for each state B, to represent whether the system is at time t in state B ($f_B(t) = 1$) or not ($f_B(t) = 0$), one can calculate the duration of a state B in an interval $[a, b]$ as the integral $\int_a^b f_B(x)dx$.

The duration calculus [9, 11] (DC for short) provides a requirement specification language that allows to express properties about such durations and a calculus to reason about them. Many examples have been analysed using DC [34, 33] such as the classical gas burner system. While DC only allows the expression of safety properties and there is hardly any program verification theory based on it, there exist a number of formal frameworks based on temporal logic that allow the specification of both safety and liveness properties and provide a powerful theory for proving real-time properties of programs (e.g. [30, 12, 1]). It is self-evident that any formal framework for hybrid systems must be able to deal with real-time.

In this paper we present a formal framework that includes a duration concept similar to the one of DC and that benefits from the extensive study of temporal frameworks by many researchers. As metric temporal logic [16, 17, 3] provides a concise notation for specifying real-time requirements and as it is equipped with a proof theory for verifying programs, we take it as basis for our work. The work of Manna, Henzinger, and Pnueli [12] provides a proof methodology based on MTL, and the work of the second author of this paper [14] presents a compositional proof system for proving real-time properties specified in MTL of distributed systems. Since compositionality is a possible technique for managing complexity and since it makes verification during the design process possible, we start from a version of metric temporal logic that supports compositional program verification [14]. We enrich metric temporal logic with a state duration concept. This is achieved by including duration functions $\int^r \phi$, for a term r and a formula ϕ. Such a function measures the duration of ϕ during the next r time units. As time domain we choose the set of nonnegative real numbers. This allows us to define the semantics of durations by means of Riemann integrals. Syntax and semantics of the extended specification language MTL-$\int$ are presented in section 2. In section 3, we show that every property that can be expressed in the duration calculus can also be expressed in MTL-$\int$. We define a function that translates every formula of the duration calculus into MTL-$\int$ and prove a correspondence between every formula and its translation. We also prove that MTL-$\int$ is more expressive than the duration calculus. In section 4, we present axioms that allow the derivation of valid duration formulae, prove their soundness, and compare them with the axioms present in the duration calculus. This section also includes an example that shows how to specify and prove duration formulae in MTL-$\int$. A rule for proving limited-duration properties and its soundness proof are presented in section 5, where we apply this rule to verify a control strategy for the gas burner system. Section 6 includes some concluding remarks. Proofs of lemmas appearing in these sections are presented in appendix A.

2 Specification Language MTL-$\int$

Temporal logic (or tense logic) provides a natural and abstract approach for the analysis of safety and liveness properties of reactive systems. The use of temporal logic as a framework for specifying such properties was first proposed by Pnueli [31]. Traditional temporal operators do not allow the expression of speed-dependent, quantitative real-time constraints. Two main possibilities for extending the expressive power of temporal logic to deal with real-time constraints have been suggested in the literature.

The first approach suggests the use of an ordinary variable to model time. In this approach, real-time constraints can be expressed by referring explicitly to time through the use of this variable (e.g. [30]). An alternative approach uses so-called bounded-operators. For each temporal operator, such as the (strong) until operator U, one or more timed versions are introduced, such as $\mathrm{U}_{<\tau}$. While the formula $\phi \, \mathrm{U} \, \psi$ states that ϕ holds until ψ becomes true and that ψ will become true eventually, the formula $\phi \, \mathrm{U}_{<\tau} \, \psi$ puts the additional constraint that ψ becomes true within τ time units. This approach, to which we refer as *metric temporal approach*, has been advocated in [19], [18], and [16]. In contrast to the first approach, time is implicit in the metric temporal one.

In this section we extend MTL to allow the expression of constraints on the durations of formulae. In section 2.1 we formulate the syntax of this language. The semantics of the extended logic can be found in section 2.2.

2.1 Syntax of the Specification Language

We give the syntax of a specification language, called MTL-$\int$, which is an extension of MTL with durations. Formulae of this logic are constructed from atomic formulae by applying future real-time operators $\mathrm{U}_{<\tau}$ (strong until before τ) and $\mathrm{U}_{=\tau}$ (strong until in τ), past real-time operators $\mathrm{S}_{<\tau}$ (strong since before τ) and $\mathrm{S}_{=\tau}$ (strong since in τ), and logical connectives $\neg$ (negation) and $\vee$ (disjunction). Although in this paper we do not consider the compositional verification of real-time systems, the aim is to design a specification language that can be used at all levels involved in the process of specification and design of a real-time system. Since compositionality is a prerequisite for hierarchical and top-down development of programs, we include the operator $\mathcal{C}$ that allows the formulation of a compositional proof rule for sequential composition (cf. [5], [14]). Moreover, this operator is used in section 3 where we prove that each formula of DC can be translated into our specification language MTL-$\int$.

Furthermore, MTL-$\int$ includes existential quantification over variables ranging over real numbers and the logical constant *true*. To be able to express duration properties, we introduce terms of the form $\int^r \phi$, for a term r and a formula ϕ. Such a term measures the accumulated time during the next r time units in which ϕ holds. For instance, the requirement that the duration of a critical state, characterised by ϕ, is less than β during the next α time units can be specified by $\int^\alpha \phi \leq \beta$.

Let $\mathcal{PL}$ be a set of propositional letters and Var a set of logical variables. We use P, Q, ... as typical elements of $\mathcal{PL}$ and x, y, ... as typical elements of Var. Logical variables in Var range over the set of real numbers, which is denoted by $\mathbb{R}$. The set of nonnegative real numbers is denoted by $\mathbb{R}_{\geq 0}$. Furthermore, we use a special element ∞ with the usual properties (e.g. $\alpha < \infty$, for every $\alpha \in \mathbb{R}$).

The syntax of our specification language MTL-$\int$ is given in table 1, with $\tau \in \mathbb{R}_{\geq 0} \cup \{\infty\}$, $\tau' \in \mathbb{R}_{\geq 0}$, $\alpha \in \mathbb{R}$, $n \geq 1$, $x \in$ Var, f a function symbol of arity n, R a relation symbol of arity n, and $P \in \mathcal{PL}$.

Henceforth, we use $\mathcal{TE}$ to denote the set of terms.

The informal meaning of *true*, P, $R(r_1, \ldots, r_n)$, $\phi_1 \vee \phi_2$, $\neg\phi$, and $\exists x \phi$ is as usual.

- The formula $\phi_1 \mathrm{U}_{<\tau} \phi_2$ states that ϕ_1 is continuously true until ϕ_2 becomes true and that ϕ_2

Table 1: Syntax of MTL-$\int$

Term	$r ::=$	$\alpha \mid x \mid \int^r \phi \mid f(r_1,\ldots,r_n)$
Formula	$\phi ::=$	$true \mid P \mid R(r_1,\ldots,r_n) \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid \exists x\phi \mid$
		$\phi_1 \mathrm{U}_{<\tau} \phi_2 \mid \phi_1 \mathrm{U}_{=\tau'} \phi_2 \mid \phi_1 \mathrm{S}_{<\tau} \phi_2 \mid \phi_1 \mathrm{S}_{=\tau'} \phi_2 \mid \phi_1 \mathcal{C} \phi_2$

will be true within τ time units. Note that we allow $\tau = \infty$ and that $\mathrm{U}_{<\infty}$ is the ordinary qualitative strong until operator.

- The formula $\phi_1 \mathrm{U}_{=\tau} \phi_2$ states that ϕ_1 is continuously true during the next τ time units and that ϕ_2 will be true in exactly τ time units.
- The formula $\phi_1 \mathrm{S}_{<\tau} \phi_2$ states that ϕ_2 has been true within the past τ units and that since that time ϕ_1 has been continuously true. Again, $\mathrm{S}_{<\infty}$ is the ordinary qualitative strong since operator.
- The formula $\phi_1 \mathrm{S}_{=\tau} \phi_2$ states that ϕ_2 has been true exactly τ time units ago and that ϕ_1 has been continuously true during the last τ time units.
- Formula $\phi_1 \mathcal{C} \phi_2$ holds if the future can be partitioned into two periods; a first period that together with the past satisfies ϕ_1 and a second period that satisfies ϕ_2.

2.2 Semantics of the Specification Language

In this section, we present the formal semantics of our specification language MTL-$\int$. To be able to assign meanings to MTL-$\int$ formulae we need to interpret atomic formulae and assign values to the terms in $\mathcal{TE}$. Therefore, we assume a total function $\underline{f} : \mathbb{R}^n \to \mathbb{R}$ to be associated with each n-ary function symbol f and a relation $\underline{R} \subseteq \mathbb{R}^n$ to be associated with each n-ary relation symbol R.

2.2.1 Semantic Model

As hybrid systems have continuously changing observables, we use the set of nonnegative reals, $\mathbb{R}_{\geq 0}$, as time domain. MTL-$\int$-formulae are interpreted over models which are pairs consisting of an *observation* and a *logical environment*.

An *observation* σ of length δ ($\delta \in \mathbb{R}_{\geq 0} \cup \{\infty\}$) over $\mathcal{PL}$ is a function from $\mathcal{PL}$ into the set of functions from interval $[0,\delta)$ into $\{tt, f\!f\}$, i.e. $\sigma{:}\mathcal{PL}{\to}([0,\delta){\to}\{tt, f\!f\})$. Intuitively, for an observation σ, a propositional letter P, and a real number t in $[0,\delta)$, $\sigma(P)(t) = tt$ denotes that σ represents an observation where P holds at time t. Clearly, $\sigma(P)(t) = \mathit{ff}$ denotes that according to observation σ, P does not hold at t. The length of an observation σ is denoted by $\#\sigma$.

An observation σ is required to satisfy the following *finite variability* condition:

- For every propositional letter P, the function $\sigma(P)$ has only finitely many discontinuity points on each bounded subinterval of $[0, \#\sigma)$.

The finite variability condition guarantees that each bounded subinterval of $[0, \#\sigma)$ can be partitioned in a finite number of subintervals in which $\sigma(P)$ is constant (cf. [6]). The set of all observations over $\mathcal{PL}$ is denoted by $\mathcal{O}$.

The concatenation of two observations σ_1 and σ_2, denoted by $\sigma_1\sigma_2$, is defined to be the observation of length $\#\sigma_1 + \#\sigma_2$ satisfying for all $P \in \mathcal{PL}$:

$$(\sigma_1\sigma_2)(P)(t) = \begin{cases} \sigma_1(P)(t) & ; \text{for all } t \text{ with } 0 \leq t < \#\sigma_1 \\ \sigma_2(P)(t - \#\sigma_1) & ; \text{for all } t \text{ with } \#\sigma_1 \leq t < \#\sigma_1 + \#\sigma_2 \end{cases}$$

Let $t \in \mathbb{R}_{\geq 0}$. The t-prefix of observation σ, denoted by $\sigma{\downarrow}t$, is defined to be the observation of length $\min(t, \#\sigma)$ satisfying $(\sigma{\downarrow}t)(P)(t') = \sigma(P)(t')$, for any $P \in \mathcal{PL}$ and $t' \in [0, \min(t, \#\sigma))$. The t-suffix of σ, denoted by $\sigma{\uparrow}t$, is defined to be the observation of length $\max(0, \#\sigma - t)$ satisfying $(\sigma{\uparrow}t)(P)(t') = \sigma(P)(t' + t)$, for any $P \in \mathcal{PL}$ and $t' \in [0, \max(0, \#\sigma - t))$. It is easy to prove that the concatenation of a t-prefix and a t-suffix of an observation σ equals σ, i.e. $(\sigma{\downarrow}t)(\sigma{\uparrow}t)=\sigma$, for all $t \in \mathbb{R}_{\geq 0}$.

A *logical environment* is a mapping that assigns a real number to each logical variable. The set of all logical environments is denoted by Θ. We will use ϑ as a typical element of Θ. For any logical variable x, any real number τ, and any logical environment ϑ, we define the variant of ϑ w.r.t. τ and x, denoted by ϑ_x^τ, as the logical environment that maps every variable y different from x to $\vartheta(y)$ and x to τ.

2.2.2 Meaning of Formulae

We define when a formula ϕ holds in an observation σ, a logical environment ϑ, and a time t, denoted by $(\sigma, \vartheta, t) \models \phi$. First a value is assigned to each term in $\mathcal{TE}$. To deal with the integration over formulae, we define for each formula ϕ and model (σ, ϑ) the function $1_{\phi(\sigma,\vartheta)} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ as follows:

$$1_{\phi(\sigma,\vartheta)}(t) \stackrel{\text{def}}{=} \begin{cases} 1 & ; \quad \text{if } (\sigma, \vartheta, t) \models \phi \\ 0 & ; \quad \text{otherwise} \end{cases}$$

The meaning of a duration $\int^r \phi$ in a model (σ, ϑ) is defined by means of a Riemann integral of the function $1_{\phi(\sigma,\vartheta)}$. However, $1_{\phi(\sigma,\vartheta)}$ is not necessarily Riemann integrable, as shown in example 2.3, below. To deal with this, we require $1_{\phi(\sigma,\vartheta)}$ to satisfy the *Dirichlet condition* [7], when defining the meaning of a duration $\int^r \phi$.

Definition 2.1 *A function is said to satisfy the* Dirichlet condition *iff for any bounded interval I, it is bounded in I and has a finite number of discontinuity points in I.* $\Box$

The Dirichlet condition implies Riemann integrability, which is needed to have the semantics of our terms well-defined. For any formula ϕ and model (σ, ϑ), $1_{\phi(\sigma,\vartheta)}$ is trivially bounded in any finite interval I but it does not necessarily satisfy the second clause of the Dirichlet condition.

Since observations satisfy the finite variability condition, it can be proved that for every formula ϕ which is obtained by applying boolean operators to propositional letters, the function $1_{\phi(\sigma,\vartheta)}$ satisfies the Dirichlet condition for every model (σ, ϑ).

We are now able to define the semantics of terms. The value $\mathcal{T}[\![r]\!](\sigma, \vartheta)t$ of a term r in a model (σ, ϑ) and a nonnegative real number t is as follows.

- $\mathcal{T}[\![\alpha]\!](\sigma, \vartheta)t \stackrel{\mathrm{def}}{=} \alpha$,
- $\mathcal{T}[\![x]\!](\sigma, \vartheta)t \stackrel{\mathrm{def}}{=} \vartheta(x)$,
- $\mathcal{T}[\![\int^r \phi]\!](\sigma, \vartheta)t \stackrel{\mathrm{def}}{=} \begin{cases} \int_t^{t+\mathcal{T}[\![r]\!](\sigma,\vartheta)t} 1_{\phi(\sigma,\vartheta)}(t_1)\, dt_1 & ; \text{ if } 1_{\phi(\sigma,\vartheta)} \text{ satisfies the Dirichlet condition} \\ & \text{ and } \mathcal{T}[\![r]\!](\sigma,\vartheta)t \geq 0 \\ 0 & ; \text{ otherwise,} \end{cases}$

  and
- $\mathcal{T}[\![f(r_1, \ldots, r_n)]\!](\sigma, \vartheta)t \stackrel{\mathrm{def}}{=} \underline{f}(\mathcal{T}[\![r_1]\!](\sigma, \vartheta)t, \ldots, \mathcal{T}[\![r_n]\!](\sigma, \vartheta)t)$.

Satisfiability of a formula ϕ in a model (σ, ϑ) and a nonnegative real number t is denoted by $(\sigma, \vartheta, t) \models \phi$. It is recursively defined by:

- $(\sigma, \vartheta, t) \models \mathit{true}$.
- $(\sigma, \vartheta, t) \models P$ iff $\sigma(P)(t) = \mathit{tt}$ and $t < \#\sigma$.
- $(\sigma, \vartheta, t) \models R(r_1, \ldots, r_n)$ iff $(\mathcal{T}[\![r_1]\!](\sigma, \vartheta)t, \ldots, \mathcal{T}[\![r_n]\!](\sigma, \vartheta)t) \in \underline{R}$.
- $(\sigma, \vartheta, t) \models \phi_1 \vee \phi_2$ iff $(\sigma, \vartheta, t) \models \phi_1$ or $(\sigma, \vartheta, t) \models \phi_2$.
- $(\sigma, \vartheta, t) \models \neg\phi$ iff $(\sigma, \vartheta, t) \not\models \phi$.
- $(\sigma, \vartheta, t) \models \phi_1 \,\mathrm{U}_{<\tau}\, \phi_2$ iff there exist $t' \in \mathbb{R}_{\geq 0}$ such that $t \leq t' < t + \tau$, $(\sigma, \vartheta, t') \models \phi_2$ and for all $t'' \in \mathbb{R}_{\geq 0}$, $t \leq t'' < t'$, $(\sigma, \vartheta, t'') \models \phi_1$.
- $(\sigma, \vartheta, t) \models \phi_1 \,\mathrm{U}_{=\tau'}\, \phi_2$ iff $(\sigma, \vartheta, t + \tau') \models \phi_2$ and for all $t' \in \mathbb{R}_{\geq 0}$, $t \leq t' < t + \tau'$, $(\sigma, \vartheta, t') \models \phi_1$.

- $(\sigma, \vartheta, t) \models \phi_1 \, \mathrm{S}_{<\tau} \, \phi_2$ iff there exist $t' \in \mathbb{R}_{\geq 0}$ such that $t - \tau < t' \leq t$, $(\sigma, \vartheta, t') \models \phi_2$, and for all $t'' \in \mathbb{R}_{\geq 0}$, $t' < t'' \leq t$, $(\sigma, \vartheta, t'') \models \phi_1$.

- $(\sigma, \vartheta, t) \models \phi_1 \, \mathrm{S}_{=\tau'} \, \phi_2$ iff $t \geq \tau$, $(\sigma, \vartheta, t - \tau') \models \phi_2$, and for all $t' \in \mathbb{R}_{\geq 0}$, $t - \tau' < t' \leq t$, $(\sigma, \vartheta, t') \models \phi_1$.

- $(\sigma, \vartheta, t) \models \phi_1 \mathcal{C} \phi_2$ iff there exist observations σ_1 and σ_2 such that $\sigma = \sigma_1 \sigma_2$, $\#\sigma_1 \geq t$, $(\sigma_1, \vartheta, t) \models \phi_1$ and $(\sigma_2, \vartheta, 0) \models \phi_2$.

- $(\sigma, \vartheta, t) \models \exists x \, \phi$ iff there exists a value $\tau \in \mathbb{R}$ such that $(\sigma, \vartheta_x^\tau, t) \models \phi$.

Satisfiability of a formula ϕ in a model (σ, ϑ) is defined by $(\sigma, \vartheta, 0) \models \phi$ and it is denoted by $(\sigma, \vartheta) \models \phi$. A formula ϕ is called valid, denoted by $\models \phi$, if $(\sigma, \vartheta) \models \phi$ holds for each model (σ, ϑ).

Useful is the following lemma that relates variants and substitutions.

Lemma 2.2 *For any formula ϕ, any model (σ, ϑ), any logical variable x, and any real numbers $d \in \mathbb{R}$ and $t \in \mathbb{R}_{\geq 0}$,*

$$(\sigma, \vartheta_x^d, t) \models \phi \textit{ iff } (\sigma, \vartheta, t) \models \phi[d/x]$$

□

In this paper, we consider a specification language that includes the function symbol "+" and the relation symbols "$\leq$", "<", and "=". The interpretations of these function and relation symbols are such that they coincide with their standard interpretations on $\mathbb{R}$.

Furthermore, we assume that we have a propositional letter T such that for every observation σ and every $t \in \mathbb{R}_{\geq 0}$, $\sigma(T)(t) = tt$ iff $t \in [0, \#\sigma)$.

The following example shows that the function $1_{\phi(\sigma,\vartheta)}$, induced by a formula ϕ and a model (σ, ϑ), is not necessarily Riemann integrable.

Example 2.3 *In this example we assume the following relation and function symbols to be in our formal language:*

1. *A unary relation symbol rat with the set Q of rational numbers as interpretation, i.e.* $\underline{rat}$=Q, *and*

2. *a unary function symbol f with the following function $\underline{f}$ as interpretation: $\underline{f}\colon \mathbb{R} \to \mathbb{R}$, with $\underline{f}(a) \stackrel{\mathrm{def}}{=} 1 - a$, for all $a \in \mathbb{R}$.*

Now, consider the formula $\phi \stackrel{\mathrm{def}}{=} \exists x(rat(x) \wedge f(x) = \int^1 T)$ and consider a model (σ, ϑ) with $\#\sigma = 1$.

Since for each $t \in [0, 1)$, $\mathcal{T}[\![\int^1 T]\!](\sigma, \vartheta)(t) = 1 - t$, one can prove that, for each $t \in [0, 1)$, $(\sigma, \vartheta, t) \models \phi$ iff $t = q$, for a rational number q. Hence, for each $t \in [0, 1)$, $1_{\phi(\sigma,\vartheta)}(t) = tt$ iff

$t = q$, for some rational number q. This implies that $1_{\phi(\sigma,\vartheta)}$ has infinitely many discontinuity points on $[0,1)$, namely all points equal to q, for some rational number q. Moreover, $1_{\phi(\sigma,\vartheta)}$ is not Riemann integrable, since $\inf\{\int_0^1 g(x)\,dx \mid g$ is a step function on $[0,1]$ and $g \geq 1_{\phi(\sigma,\vartheta)}\} = 1$ and $\sup\{\int_0^1 g(x)\,dx \mid g$ is a step function on $[0,1]$ and $g \leq 1_{\phi(\sigma,\vartheta)}\} = 0$. $\square$

In table 2 we define a number of abbreviations, where ϕ, ϕ_1, and ϕ_2 are formulae, x is a logical variable, τ is a constant in $\mathbb{R}_{\geq 0} \cup \{\infty\}$, and τ' is a constant in $\mathbb{R}_{\geq 0}$.

We give the informal meaning of the most interesting abbreviations:

Table 2: Syntactic Abbreviations

false	$\stackrel{\text{def}}{=}$	*true*	$\Diamond_{\leq\tau'}\phi$	$\stackrel{\text{def}}{=}$	$\Diamond_{<\tau'}\phi \vee \Diamond_{=\tau'}\phi$
$\phi_1 \wedge \phi_2$	$\stackrel{\text{def}}{=}$	$\neg(\neg\phi_1 \vee \neg\phi_2)$	$\Diamond\phi$	$\stackrel{\text{def}}{=}$	$\Diamond_{<\infty}\phi$
$\phi_1 \rightarrow \phi_2$	$\stackrel{\text{def}}{=}$	$\neg\phi_1 \vee \phi_2$	$\Box_{<\tau}\phi$	$\stackrel{\text{def}}{=}$	$\neg\Diamond_{<\tau}\neg\phi$
$\phi_1 \leftrightarrow \phi_2$	$\stackrel{\text{def}}{=}$	$(\phi_1 \rightarrow \phi_2) \wedge (\phi_2 \rightarrow \phi_1)$	$\Box\phi$	$\stackrel{\text{def}}{=}$	$\Box_{<\infty}\phi$
$\forall x\phi$	$\stackrel{\text{def}}{=}$	$\neg\exists x\neg\phi$	$\phi_1 \Rightarrow \phi_2$	$\stackrel{\text{def}}{=}$	$\Box(\phi_1 \rightarrow \phi_2)$
$\Diamond_{=\tau'}\phi$	$\stackrel{\text{def}}{=}$	*true* $\mathrm{U}_{=\tau'}\ \phi$	$\phi_1 \Leftrightarrow \phi_2$	$\stackrel{\text{def}}{=}$	$\Box(\phi_1 \leftrightarrow \phi_2)$
$\Diamond_{<\tau}\phi$	$\stackrel{\text{def}}{=}$	*true* $\mathrm{U}_{<\tau}\ \phi$			

- $\Diamond_{=\tau'}\phi$: ϕ will be true in exactly τ' time units.
- $\Diamond_{<\tau}\phi$: ϕ will be eventually true before τ time units.
- $\Diamond_{\leq\tau'}\phi$: ϕ will be eventually true before or in exactly τ' time units.
- $\Diamond\phi$: ϕ will be eventually true.
- $\Box_{<\tau}\phi$: ϕ is continuously true during the next τ time units.
- $\Box\phi$: henceforth ϕ will be true.

Example 2.4 *The first requirement of the Gas Burner example in [34] states that gas must never leak for more than 4 time units in any period of at most 30 time units. If we use the proposition* Leak *to represent whether gas is leaking or not, we can express this requirement in MTL-$\int$ by*

$$Req_0 \qquad \Box\forall x(x \leq 30 \rightarrow \textstyle\int^x \mathrm{Leak} \leq 4)$$

An equivalent requirement is that gas never leaks for more than 4 time units in any period of 30 time units. This requirement can be specified in MTL-$\int$ by

$$Req \qquad \Box\textstyle\int^{30} \mathrm{Leak} \leq 4$$

Whereas the first formulation constraints all periods of length less or equal 30, the second formulation only mentions periods of length equal 30. The equivalence of these requirements follows from the monotonicity of the duration operator $\int^x$. This will be formalised in axiom (D4) of section 4.

$\square$

3 Comparison of the Duration Calculus with MTL-$\int$

In this section we investigate the relationship between MTL-$\int$ and the duration calculus. We show that any formula of the duration calculus can be translated into an MTL-$\int$-formula and that MTL-$\int$ is more expressive than the duration calculus.

To do so we briefly introduce the duration calculus. (For a more detailed presentation of the duration calculus we refer to [9, 11].) It has been introduced in [9] as a notation to specify real-time requirements, and a calculus to verify theorems about such requirements, and can be considered as an extension of interval temporal logic [28]. The duration calculus has also been used to give semantics to communicating processes executed on a shared processor configuration [8] and has been extended to handle hybrid systems [10].

Formulae of the duration calculus are interpreted in models and in bounded intervals $[b, d] \subseteq \mathbf{R}_{\geq 0}$. An important operator of the duration calculus is the "$\frown$" operator. Intuitively, $D_1 \frown D_2$ holds in model (σ, ϑ) and interval $[b, d] \subseteq \mathbf{R}_{\geq 0}$ iff the interval $[b, d]$ can be partitioned into two intervals $[b, m]$ and $[m, d]$ such that D_1 holds in model (σ, ϑ) and interval $[b, m]$, and D_2 holds in model (σ, ϑ) and interval $[m, d]$.

A central notion in the duration calculus is the *duration of a boolean assertion*, denoted by $\int B$, where boolean assertions are defined by:

$$B ::= \mathit{true} \mid P \mid B_1 \vee B_2 \mid \neg B, \text{ with } P \in \mathcal{PL}.$$

Note that boolean assertions are a subset of the formulae of the previous section. We use $(\sigma, \vartheta, t) \models B$ and $1_{B(\sigma,\vartheta)}$ as defined there. Remember that because of the finite variability condition imposed on observations, for each boolean assertion B and model (σ, ϑ), the function $1_{B(\sigma,\vartheta)}$ is Riemann integrable.

Terms of the duration calculus are defined as follows:

$$r^D ::= \tau \mid \int B \mid x \mid f(r_1^D, \ldots, r_n^D),$$

where τ is a real number, B is a boolean assertion, and x is a variable. In this definition we have omitted the term ℓ since it can be introduced as an abbreviation of $\int \mathit{true}$.

Terms of the duration calculus are interpreted in an interval, as opposed to the previous section where only points are used. Thus for a term r^D and an interval $[b,d] \subseteq \mathbf{R}_{\geq 0}$, we define $\nu[\![r^D]\!](\sigma,\vartheta)[b,d]$ as follows.

$\nu[\![\tau]\!](\sigma,\vartheta)[b,d] \overset{\text{def}}{=} \tau$

$\nu[\![\int B]\!](\sigma,\vartheta)[b,d] \overset{\text{def}}{=} \int_b^d 1_{B(\sigma,\vartheta)}(t)\, dt.$

$\nu[\![x]\!](\sigma,\vartheta)[b,d] \overset{\text{def}}{=} \vartheta(x)$

$\nu[\![f(r_1^D,\ldots,r_n^D)]\!](\sigma,\vartheta)[b,d] \overset{\text{def}}{=} \underline{f}(\nu[\![r_1^D]\!](\sigma,\vartheta)[b,d],\ldots,\nu[\![r_n^D]\!](\sigma,\vartheta)[b,d]).$

Thus, the term $\int B$ when evaluated in an interval $[b,d]$ has as value the duration of B in this interval. Note that both end-points of the interval are implicit, that is, there are not mentioned in the syntax.

Let $r^D[\int^x / \int]$ denote the term obtained from r^D by substituting all occurrences of $\int$ by $\int^x$. Then we have the following lemma, relating the value of a term in the duration calculus to one in $\mathcal{TE}$.

Lemma 3.1 *For any term r^D of the duration calculus, interval $[b,d] \subseteq \mathbf{R}_{\geq 0}$, and model (σ,ϑ),*

$$\nu[\![r^D]\!](\sigma,\vartheta)[b,d] = \mathcal{T}[\![r^D[\textstyle\int^x / \int]]\!](\sigma,\vartheta_x^{d-b})b, \text{ where } x \text{ does not occur in } r^D.$$

□

Proof. *By induction on the structure of r^D. Note that $r^D[\int^x / \int]$ is an element of $\mathcal{TE}$. The main observation is that for any variable x and any boolean assertion B,*
$\nu[\![\int B]\!](\sigma,\vartheta)[b,d] = \int_b^d 1_{B(\sigma,\vartheta)}(t)\, dt = \int_b^{b+(d-b)} 1_{B(\sigma,\vartheta)}(t)\, dt = \mathcal{T}[\![\int^x B]\!](\sigma,\vartheta_x^{d-b})b.$ □

The set $\mathcal{D}$ of formulae of the duration calculus is defined by:

$$D ::= \mathit{true} \mid R(r_1^D,\ldots,r_n^D) \mid \neg D \mid D_1 \vee D_2 \mid D_1 {}^\frown D_2 \mid \exists x D,$$

where D_1 and D_2 are formulae in $\mathcal{D}$, x is a variable, and r_i^D, for $i = 1,\ldots,n$, are terms.

Next we define when a formula D of the duration calculus holds in a model (σ,ϑ) and an interval $[b,d] \subseteq \mathbf{R}_{\geq 0}$, denoted by $(\sigma,\vartheta,[b,d]) \models_D D$:

- $(\sigma,\vartheta,[b,d]) \models_D \mathit{true}$,
- $(\sigma,\vartheta,[b,d]) \models_D R(r_1^D,\ldots,r_n^D)$ iff $(\nu[\![r_1^D]\!](\sigma,\vartheta)[b,d],\ldots,\nu[\![r_n^D]\!](\sigma,\vartheta)[b,d]) \in \underline{R}$,
- $(\sigma,\vartheta,[b,d]) \models_D \neg D$ iff $(\sigma,\vartheta,[b,d]) \not\models_D D$,

- $(\sigma, \vartheta, [b,d]) \models_D D_1 \vee D_2$ iff $(\sigma, \vartheta, [b,d]) \models_D D_1$ or $(\sigma, \vartheta, [b,d]) \models_D D_2$,
- $(\sigma, \vartheta, [b,d]) \models_D D_1 {}^\frown D_2$ iff there exists m with $b \leq m \leq d$, $(\sigma, \vartheta, [b,m]) \models_D D_1$, and $(\sigma, \vartheta, [m,d]) \models_D D_2$, and
- $(\sigma, \vartheta, [b,d]) \models_D \exists x D$ iff $(\sigma, \vartheta^a_x, [b,d]) \models_D D$, for some real number a.

The following lemma expresses that truth of $(\sigma, \vartheta, [b,d]) \models_D D$ does only depend on a finite interval of observation σ.

Lemma 3.2 *For any interval $[b,d] \subseteq \mathbb{R}_{\geq 0}$, any model (σ, ϑ), and any formula $D \in \mathcal{D}$, the following are equivalent:*

(a) $(\sigma, \vartheta, [b,d]) \models_D D$,

(b) $((\sigma{\downarrow}d){\uparrow}b, \vartheta, [0, d-b]) \models_D D$,

(c) $(\sigma{\uparrow}b, \vartheta, [0, d-b]) \models_D D$, *and*

(d) $(\sigma{\downarrow}d, \vartheta, [b,d]) \models_D D$.

□

Proof. *See appendix A.* □

Next, we show how formulae of the duration calculus can be translated into MTL-$\int$. We define for each logical variable x a function $\mathcal{E}_x$ that translates any formula $D \in \mathcal{D}$ into an MTL-$\int$ formula $\mathcal{E}_x(D)$, provided x does not occur in D.

Before defining function $\mathcal{E}_x$, we introduce $dist(r)$, for a term $r \in \mathcal{TE}$, as an abbreviation of the formula $\forall y(r \leq y \rightarrow \int^y T = r)$. Intuitively, $dist(r)$ holds in a model (σ, ϑ) and $t \in \mathbb{R}_{\geq 0}$ iff the distance from t to the end of the observation σ is r. Thus, if we consider a model (σ, ϑ) with $\#\sigma = 2$, then $(\sigma, \vartheta, 0) \models dist(2)$ and $(\sigma, \vartheta, 1) \not\models dist(2)$. Formally, for each model (σ, ϑ), $x \in \mathrm{Var}$, and $t \leq \#\sigma$, $(\sigma, \vartheta, t) \models dist(r)$ iff $\#\sigma - t = \mathcal{T}[\![r]\!](\sigma, \vartheta)t$, as can be shown as follows.
For each $\tau \in \mathbb{R}_{\geq 0}$, $\int_t^{t+\tau} 1_{T(\sigma,\vartheta)}(t_1)dt_1 = \min(\tau, \#\sigma - t)$; therefore, we have that $\int_t^{t+\tau} 1_{T(\sigma,\vartheta)}(t_1)dt_1$ $= \mathcal{T}[\![r]\!](\sigma, \vartheta)t \in \mathbb{R}_{\geq 0}$, for all $\tau \in \mathbb{R}_{\geq 0}$ with $\tau \geq \mathcal{T}[\![r]\!](\sigma, \vartheta)t \in \mathbb{R}_{\geq 0}$, iff $\#\sigma - t = \mathcal{T}[\![r]\!](\sigma, \vartheta)t$.

Let D, D_1, and D_2 be duration formulae in which x does not occur. Then, we define

$\mathcal{E}_x(true) \stackrel{\text{def}}{=} true$,

$\mathcal{E}_x(R(r_1^D, \ldots, r_n^D)) \stackrel{\text{def}}{=} R(r_1^D[\int^x / \int], \ldots, r_n^D[\int^x / \int])$,

$\mathcal{E}_x(\neg D) \stackrel{\text{def}}{=} \neg \mathcal{E}_x(D)$,

$\mathcal{E}_x(D_1 {}^\frown D_2) \stackrel{\text{def}}{=} \exists x_0(0 \leq x_0 \leq x \wedge ((\mathcal{E}_{x_0}(D_1) \wedge dist(x_0))\, \mathcal{C}(\mathcal{E}_x(D_2)[x - x_0/x])))$, where x_0 is different from x and it does not occur in D_1 and D_2, and

$\mathcal{E}_x(\exists y D) \stackrel{\text{def}}{=} \exists y \mathcal{E}_x(D)$.

Then we have the following theorem relating formula $D \in \mathcal{D}$ and $\mathcal{E}_x(D)$.

Theorem 3.3 *For any formula D of the duration calculus, any interval $[b,d] \subseteq \mathbb{R}_{\geq 0}$, any logical variable x which does not occur in D, and any model (σ, ϑ) with $\#\sigma \geq d$,*

$$(\sigma, \vartheta, [b,d]) \models_D D \textit{ iff } (\sigma, \vartheta_x^{d-b}, b) \models \mathcal{E}_x(D).$$

$\square$

Proof. *By induction on the structure of D. We only present the case of $D_1 \frown D_2$.*

Using lemma 3.2 we have that $(\sigma, \vartheta, [b,d]) \models_D D_1 \frown D_2$ holds iff there exists m with $b \leq m \leq d$, $(\sigma{\downarrow}m, [b,m]) \models_D D_1$, and $(\sigma{\uparrow}m, \vartheta, [0, d-m]) \models_D D_2$.

Therefore, by the induction hypothesis, for any distinct variables x and x_0 such that x and x_0 do not occur in D_1 and D_2, $(\sigma, \vartheta, [b,d]) \models_D D_1 \frown D_2$ holds iff there exists m with $b \leq m \leq d$, $(\sigma{\downarrow}m, \vartheta_{x_0}^{m-b}, b) \models \mathcal{E}_{x_0}(D_1)$, and $(\sigma{\uparrow}m, \vartheta_x^{d-m}, 0) \models \mathcal{E}_x(D_2)$.

Since $\#\sigma \geq d$ implies for every m with $m \leq d$, $\#(\sigma{\downarrow}m) = m$, and since $\sigma = (\sigma{\downarrow}m)(\sigma{\uparrow}m)$, this leads to

$(\sigma, \vartheta, [b,d]) \models_D D_1 \frown D_2$ iff

there exist m with $b \leq m \leq d$, and observations σ_1 and σ_2 with $\sigma = \sigma_1\sigma_2$, $(\sigma_1, \vartheta_{x_0}^{m-b}, b) \models \mathcal{E}_{x_0}(D_1)$, $\#\sigma_1 = m$, and $(\sigma_2, \vartheta_x^{d-m}, 0) \models \mathcal{E}_x(D_2)$ iff

there exist m with $b \leq m \leq d$ and observations σ_1 and σ_2 with $\sigma = \sigma_1\sigma_2$, $\#\sigma_1 \geq b$,$(\sigma_1, \vartheta_{x,x_0}^{d-b,m-b}, b)$ $\models \mathcal{E}_{x_0}(D_1)$, $(\sigma_1, \vartheta_{x,x_0}^{d-b,m-b}, b) \models dist(x_0)$, and $(\sigma_2, \vartheta_{x,x_0}^{d-b,m-b}, 0) \models \mathcal{E}_x(D_2)[x - x_0/x]$ iff

there exist m with $b \leq m \leq d$ and observations σ_1 and σ_2 with $\sigma = \sigma_1\sigma_2$, $\#\sigma_1 \geq b$, $(\sigma_1, \vartheta_{x,x_0}^{d-b,m-b}, b)$ $\models \mathcal{E}_{x_0}(D_1) \wedge dist(x_0)$ and $(\sigma_2, \vartheta_{x,x_0}^{d-b,m-b}, 0) \models \mathcal{E}_x(D_2)[x - x_0/x]$ iff

$(\sigma, \vartheta_x^{d-b}, b) \models \exists x_0 (0 \leq x_0 \leq x \wedge ((\mathcal{E}_{x_0}(D_1) \wedge dist(x_0))\,\mathcal{C}(\mathcal{E}_x(D_2)[x - x_0/x])))$ iff

$(\sigma, \vartheta_x^{d-b}, b) \models \mathcal{E}_x(D_1 \frown D_2)$. $\square$

Thus we have shown that any D of DC can be translated to a formula in MTL-$\int$ by applying function $\mathcal{E}_x$ and we have proved a correspondence between D and $\mathcal{E}_x(D)$.

What does this correspondence imply for the validity of a formula D of DC and its corresponding MTL-$\int$ formula $\mathcal{E}_x(D)$? Do we have $\models_D D$ iff $\models \mathcal{E}_x(D)$, where $\models_D D$ denotes validity of D?

Before answering these questions, we have to define when a formula of the duration calculus holds in a model and when it is valid. We adopt the definition given in [8], i.e. we have

$$(\sigma, \vartheta) \models_D D \text{ iff } \forall t \geq 0 \cdot (\sigma, \vartheta, [0,t]) \models_D D,$$

that is, D holds in (σ, ϑ) iff it holds in (σ, ϑ) and any prefix interval $[0,t]$ of $[0, \infty)$. (We decided to use the same notation , i.e. $\models_D$, since there is no danger of ambiguity.)

We then define validity of D, $\models_D D$, as follows:

$$\models_D D \text{ iff for every model } (\sigma, \vartheta),\ (\sigma, \vartheta) \models_D D.$$

It is worth to note that a formula D of DC is valid if and only if D holds in every model and every interval. Formally, we have:

Lemma 3.4 *For any formula D of DC,*

$$\models_D D \textit{ iff } (\sigma, \vartheta, [b,d]) \models_D D, \textit{ for any model } (\sigma, \vartheta) \textit{ and interval } [b,d]$$

□

Proof. *The "**if**" implication is obvious. To prove the "**only if**" implication, take an arbitrary formula D of DC with $\models_D D$, an arbitrary model (σ, ϑ), and an arbitrary interval $[b,d]$. We have to prove $(\sigma, \vartheta, [b,d]) \models_D D$.*
Since $\models_D D$ holds, we have $(\sigma \upharpoonright b, \vartheta, [0, b-d]) \models_D D$. Hence by lemma 3.2, $(\sigma, \vartheta, [b,d]) \models_D D$. □

We now return to the questions above and provide the following answers. In general, we don't have $\models_D D$ iff $\models \mathcal{E}_x(D)$, as shown by the following example. Let D_0 denote the following formula of DC:

$$true^\frown(\int true = 0).$$

D_0 is a valid formula, since for every model (σ, ϑ) and $t \geq 0$, $(\sigma, \vartheta, [0,t]) \models_D true$ and $(\sigma, \vartheta, [t,t]) \models_D \int true = 0$. The corresponding MTL-$\int$ formula $\mathcal{E}_x(D_0)$ is, however, not valid, since $\mathcal{E}_x(D_0) \equiv \exists x_0 (0 \leq x_0 \leq x \wedge ((true \wedge dist(x_0))\, \mathcal{C}(\int^{x-x_0} true = 0)))$ and for any model (σ, ϑ) with $\vartheta(x) < 0$ and any $a \in \mathbb{R}$, $(\sigma, \vartheta^a_{x_0}, 0) \models 0 \leq x_0 \leq x$ does not hold. To understand the problem let us look closely at theorem 3.3. This theorem tells us that under some restrictions, we have :

$$(\sigma, \vartheta, [b,d]) \models_D D \text{ iff } (\sigma, \vartheta^{d-b}_x, b) \models \mathcal{E}_x(D).$$

However, since we assume $b \leq d$, this theorem does not say any thing about models (σ, ϑ) with $\vartheta(x) < 0$. A possible solution to this problem is to restrict validity of $\mathcal{E}_x(D)$ to models with $\vartheta(x) \geq 0$, i.e. to consider the formula $x \geq 0 \rightarrow \mathcal{E}_x(D)$ rather than $\mathcal{E}_x(x)$. Thus, the question is now whether we have $\models_D D$ iff $\models x \geq 0 \rightarrow \mathcal{E}_x(D)$.

The answer is again **no**, as shown now. Consider a model (σ, ϑ) with $\#\sigma = 1$ and $\vartheta(x) = 3$; thus, $\vartheta(x) \geq 0$. We show that $(\sigma, \vartheta, 0) \models \mathcal{E}_x(D_0)$ does not hold, which implies that $(\sigma, \vartheta, 0) \models x \geq 0 \rightarrow \mathcal{E}_x(D_0)$ does not hold, too.
Assume $(\sigma, \vartheta, 0) \models \mathcal{E}_x(D_0)$. Thus, there exists $m \in \mathbb{R}$ with $0 \leq m \leq 3$ and there exist σ_1 and σ_2 with $\sigma_1 \sigma_2 = \sigma$, $(\sigma_1, \vartheta^m_{x_0}, 0) \models dist(x_0)$, and $(\sigma, \vartheta^m_{x_0}, 0) \models \int^{x-x_0} true = 0$. Since $\#\sigma_1 \geq 0$, we

have from $(\sigma_1, \vartheta^m_{x_0}, 0) \models \mathit{dist}(x_0)$ that $\#\sigma_1 = m$ holds. From $(\sigma, \vartheta^m_{x_0}, 0) \models \int^{x-x_0} \mathit{true} = 0$, we have $\vartheta^m_{x_0}(x) = \vartheta^m_{x_0}(x_0)$. Therefore, $m = 3$. Since $\sigma = \sigma_1\sigma_2$ implies $\#\sigma_1 \leq \#\sigma$, this contradicts $\sigma_1\sigma_2 = \sigma$, $\#\sigma = 1$, and $\#\sigma_1 = m$.

The problem is that for each possible value $\vartheta(x) \geq 0$ for x, we have to find models σ_1 and σ_2 with $\sigma_1\sigma_2 = \sigma$ and $\#\sigma_1 = \vartheta(x)$. This is, however, not possible if σ is finite, since $\sigma_1\sigma_2 = \sigma$ implies $\#\sigma_1 \leq \sigma$, and therefore, for $\vartheta(x) > \#\sigma$, one cannot find σ_1 and σ_2 as above.

This discussion leads to the following result:

Lemma 3.5 *Let $\models_{D,\infty} D$ denote validity of D in all models (σ, ϑ) with $\#\sigma = \infty$, i.e. $\models_{D,\infty} D$ iff for every (σ, ϑ) with $\#\sigma = \infty$, $(\sigma, \vartheta) \models_D D$.*
Then, for any formula $D \in \mathcal{D}$ in which x does not occur,

$$\models_{D,\infty} D \text{ iff } \models (\forall x \exists y \int^y T > x) \wedge x \geq 0 \rightarrow \mathcal{E}_x(D).$$

□

Proof. *By definition of $\models_{D,\infty}$, we have $\models_{D,\infty} D$ iff for every model (σ, ϑ) and $t \geq 0$, if $\#\sigma = \infty$ then $(\sigma, \vartheta, 0) \models_D D$. Using theorem 3.3, we obtain, $\models_{D,\infty} D$ iff for every model (σ, ϑ) and $t \geq 0$, if $\#\sigma = \infty$ then $(\sigma, \vartheta^t_x, 0) \models \mathcal{E}_x(D)$. Hence, $\models_{D,\infty} D$ iff for every model (σ, ϑ), if $\#\sigma = \infty$ and $\vartheta(x) \geq 0$ then $(\sigma, \vartheta, 0) \models \mathcal{E}_x(D)$. Now, since for every model (σ, ϑ), $(\sigma, \vartheta, 0) \models \forall x \exists y \int^y T > x$ iff $\#\sigma = \infty$, we have $\models_{D,\infty} D$ iff for every model (σ, ϑ) $(\sigma, \vartheta, 0) \models (\forall x \exists y \int^y T > x) \wedge x \geq 0 \rightarrow \mathcal{E}_x(D)$. Consequently, $\models_{D,\infty} D$ iff $\models (\forall x \exists y \int^y T > x) \wedge x \geq 0 \rightarrow \mathcal{E}_x(D)$.* □

3.1 Comparison of Expressiveness of MTL-$\int$ and of the Duration Calculus

In this section, we show that MTL-$\int$ is more expressive than the duration calculus. We prove that the duration calculus allows expression of safety properties, only. As shown in the previous section, any formula of the duration calculus can be translated into an MTL-$\int$ formula. Since MTL-$\int$ allows the expression of liveness properties, as for instance $\Diamond P$, for some $P \in \mathcal{PL}$, this shows that MTL-$\int$ is more expressive than the duration calculus.

To prove that the duration calculus only allows expression of safety properties, we use the topological characterisation of safety properties proposed by Alpern and Schneider [2]. This characterisation identifies safety properties with *topologically closed sets of models*, i.e. sets that contain all their limit points.

Let χ_D denote the set of all models in which D holds, i.e. $\chi_D = \{(\sigma, \vartheta) \mid (\sigma, \vartheta) \models_D D\}$. We show that for any formula $D \in \mathcal{D}$ this set is topologically closed w.r.t. the topology induced by the following notion of convergence.

Definition 3.6 *A sequence of models* $\langle(\sigma_i, \vartheta)\rangle_{i\geq 0}$ *is said to be* convergent to the model (σ, ϑ), *denoted by* $\lim_{i\to\infty}(\sigma_i, \vartheta) = (\sigma, \vartheta)$, *iff for all* $t \in \mathbb{R}_{\geq 0}$ *there exists a natural number* n *such that* $\sigma_k{\downarrow}t = \sigma{\downarrow}t$, *for all* $k \geq n$. □

Definition 3.7 *A set of models* Σ *is said to be* topologically closed *iff for any sequence* $\langle(\sigma_i, \vartheta)\rangle_{i\geq 0}$ *in* Σ *and model* (σ, ϑ), *if* $\lim_{i\to\infty}(\sigma_i, \vartheta) = (\sigma, \vartheta)$ *then* $(\sigma, \vartheta) \in \Sigma$. □

It can be argued that with the above definition of convergence the identification of safety properties with topologically closed sets of models capture our intuition behind safety properties, namely that a safety property stipulates that an undesired behaviour does not happen during observation [2]. We can now prove the following result:

Lemma 3.8 *For any formula* $D \in \mathcal{D}$, χ_D *is topologically closed, i.e. for any sequence* $\langle(\sigma_i, \vartheta)\rangle_{i\geq 0}$ *in* χ_D *and model* (σ, ϑ), *if* $\lim_{i\to\infty}(\sigma_i, \vartheta) = (\sigma, \vartheta)$ *then* $(\sigma, \vartheta) \in \chi_D$. □

Proof. *Let* D *be a formula in* $\mathcal{D}$, *and let* $\langle(\sigma_i, \vartheta)\rangle_{i\geq 0}$ *be a sequence in* χ_D, *i.e.* $(\sigma_i, \vartheta) \models_D D$, *for all* $i \geq 0$. *Let* (σ, ϑ) *be a model with* $\lim_{i\to\infty}(\sigma_i, \vartheta) = (\sigma, \vartheta)$.
We have to prove $(\sigma, \vartheta) \in \chi_D$, *i.e.* $(\sigma, \vartheta) \models_D D$.
By definition we have to show that for every $t \geq 0$, $(\sigma, \vartheta, [0, t]) \models_D D$.
Assume $t \geq 0$. *By the definition of convergence, there exists* $n \geq 0$ *such that for all* $k \geq n$, $\sigma_k{\downarrow}t = \sigma{\downarrow}t$ *holds. Since* $(\sigma_i, \vartheta) \models_D D$ *holds for all* $i \geq 0$, *we have* $(\sigma_n, \vartheta, [0, t]) \models_D D$.
Using lemma 3.2, this leads to $(\sigma_n{\downarrow}t, \vartheta, [0, t]) \models_D D$. *Consequently,* $(\sigma{\downarrow}t, \vartheta, [0, t]) \models_D D$, *and again using lemma 3.2, we obtain* $(\sigma, \vartheta, [0, t]) \models_D D$. □

As shown in the previous section, any formula of the duration calculus can be translated into an MTL-$\int$ formula. Since MTL-$\int$ allows the expression of liveness properties, as for instance $\Diamond P$, for some $P \in \mathcal{PL}$, this shows that MTL-$\int$ is more expressive than the duration calculus.

4 Axioms for Durations

Having extended the specification language of metric temporal logic to allow the expression of duration properties, we present axiom schemas to derive valid duration formulae. (From now on, we refer to axiom schemas as axioms.) We concentrate on the part of the logic that concerns duration formulae and adopt all valid metric temporal logic formulae as axioms and use tautologies of real arithmetic. A deductive system for metric temporal logic is presented in [17, 32]. In the remainder of this section ϕ and ψ stand for boolean assertions, i.e. formulae obtained from propositional letters by applying boolean connectives. Since application of boolean connectives preserves finite variability, if ϕ is a boolean assertion, $1_{\phi(\sigma,\vartheta)}$ is Riemann integrable for each model (σ, ϑ).

As the meaning of a duration term $\int^r \phi$ is defined as an integral, we have axioms that capture properties of integrals.

(D0)	$r \geq 0 \Rightarrow \int^r \mathit{true} = r.$
(D1)	$\Box \int^r \mathit{false} = 0.$
(D2)	$\Box \int^0 \phi = 0.$
(D3)	$\Box \int^r \phi \vee \psi = \int^r \phi + \int^r \psi - \int^r \phi \wedge \psi.$
(D4)	$r \leq r' \Rightarrow \int^r \phi \leq \int^{r'} \phi.$
(D5)	$r \leq \alpha \wedge \Box_{<\alpha}(\phi \rightarrow \psi) \Rightarrow \int^r \phi \leq \int^r \psi$, for any $\alpha \in \mathbb{R}_{\geq 0} \cup \{\infty\}$.

Soundness of axioms (D0)-(D5) follows immediately from the semantics. Note, however, that axioms (D3) and (D5) are unsound without the assumption that ϕ and ψ are Boolean assertions.

In addition to (D0)-(D5) we present three more axioms that relate duration formulae to the metric temporal operators $\mathcal{C}$, $\Diamond_{\leq\alpha}$, and $\Box_{<\alpha}$. Before we give these axioms, we need to define rigid-terms. A *rigid-term* is a term that does not contain the symbol $\int$. The following lemma expresses that the value of a rigid term only depends on the logical environment.

Lemma 4.1 *For every term r, observations σ and σ', and $t, t' \in \mathbb{R}_{\geq 0}$, if r is a rigid-term then $\mathcal{T}[\![r]\!](\sigma, \vartheta)t = \mathcal{T}[\![r]\!](\sigma', \vartheta)t'$.* $\Box$

Proof. *Straightforward induction on the structure of r.* $\Box$

(D6)	$x' \geq 0 \wedge y' \geq 0 \wedge T \wedge \int^r \phi = x' + y' \Rightarrow \exists x_0((\int^{x_0} \phi = x')\, \mathcal{C}(\int^{r-x_0} \phi = y'))$, provided r is a rigid-term.

Informally, axiom (D6) states that a nonempty interval I in which the duration of ϕ is $x' + y'$, for positive x' and y' can be partitioned in two intervals I_1 and I_2 such that the duration of ϕ in I_1 is x' and in I_2 is y'.

Lemma 4.2 *Axiom (D6) is sound.* $\Box$

Proof. *Consider an arbitrary model (σ, ϑ) and $t \in \mathbb{R}_{\geq 0}$ with $(\sigma, \vartheta, t) \models x' \geq 0 \wedge y' \geq 0 \wedge T \wedge \int^r \phi = x' + y'$. We have to prove that there exists a real number a and observations σ_1 and σ_2 with $\#\sigma_1 \geq t$, $\sigma = \sigma_1\sigma_2$, $(\sigma_1, \vartheta^a_{x_0}, t) \models \int^{x_0} \phi = x'$, and $(\sigma_2, \vartheta^a_{x_0}, 0) \models \int^{r-x_0} \phi = y'$.*
Let $\alpha = \mathcal{T}[\![r]\!](\sigma, \vartheta)t$. Since r is a rigid-term, we have by lemma 4.1 $\alpha = \mathcal{T}[\![r]\!](\sigma', \vartheta)t'$, for each σ' and t'. We can distinguish two cases: (1) $\alpha < 0$ and (2) $\alpha \geq 0$.

Consider the first case, i.e. $\alpha < 0$.

By the definition of the semantics of terms, we have $\mathcal{T}[\![\int^r \phi]\!](\sigma,\vartheta)t = 0$. *Hence,* $\vartheta(x') = 0$ *and* $\vartheta(y') = 0$. *Choose 0 for a,* $\sigma{\downarrow}t$ *for* σ_1, *and* $\sigma{\uparrow}t$ *for* σ_2. *Since* $\#\sigma > t$, *we have* $\#\sigma_1 = t \geq t$. *It is now not difficult to see that* $(\sigma_1, \vartheta^0_{x_0}, t) \models \int^{x_0} \phi = x'$, *and* $(\sigma_2, \vartheta^0_{x_0}, 0) \models \int^{r-x_0} \phi = y'$.

Next consider case (2), i.e. $\alpha \geq 0$.

Let f be the real function that maps each $b \in [0,\alpha]$ *to* $\int_t^{t+b} 1_{\phi(\sigma,\vartheta)}(z)dz$. *Observe that f is monotonic,* $f(0) = 0$, *and* $f(\alpha) = \vartheta(x') + \vartheta(y')$. *Together with* $\vartheta(x') \geq 0$ *and* $\vartheta(y') \geq 0$ *this leads to* $\vartheta(x') \in [f(0), f(\alpha)]$. *Because f is continuous the intermediate value theorem implies that there exists* $a \in [0,\alpha]$ *with* $f(a) = \vartheta(x')$. *Let* $\sigma_1 = \sigma{\downarrow}(t+a)$ *and* $\sigma_2 = \sigma{\uparrow}(t+a)$. *We consider two cases,* $t + a \leq \#\sigma$ *and* $t + a > \#\sigma$.

1. **Case:** $t + a \leq \#\sigma$.

   In this case, $\#\sigma_1 = t + a$ *and* $\#\sigma_2 = \#\sigma - (t+a)$. *Hence,*

   - $1_{\phi(\sigma,\vartheta)}(t') = 1_{\phi(\sigma_1,\vartheta)}(t')$, *for each* $t' \in [t, t+a)$ *and*
   - $1_{\phi(\sigma,\vartheta)}(t' + (t+a)) = 1_{\phi(\sigma_2,\vartheta)}(t')$, *for each* $t' \geq 0$

   This implies $\int_t^{t+a} 1_{\phi(\sigma_1,\vartheta)}(z)dz = \vartheta(x')$ *and* $\int_0^{\alpha-a} 1_{\phi(\sigma_2,\vartheta)}(z)dz = \vartheta(y')$.
   Consequently, $(\sigma_1, \vartheta^a_{x_0}, t) \models \int^{x_0} \phi = x'$, *and* $(\sigma_2, \vartheta^a_{x_0}, 0) \models \int^{r-x_0} \phi = y'$.

2. **Case:** $t + a > \#\sigma$. *In this case,* $\#\sigma_1 = \#\sigma > t$ *and* $\#\sigma_2 = 0$. *Therefore,* $1_{\phi(\sigma,\vartheta)}(t') = 1_{\phi(\sigma_1,\vartheta)}(t')$, *for each* $t' \in [t, t+a)$, *and since* ϕ *is a Boolean assertion* $1_{\phi(\sigma,\vartheta)}(t' + (t+a)) = 1_{\phi(\sigma_2,\vartheta)}(t')$, *for each* $t' \geq 0$. *The rest of the proof is similar to the first case.*

$\square$

(D7) $\quad \Diamond_{\leq\alpha} \int^r \phi \leq r' \Rightarrow \int^{\alpha+r} \phi \leq \alpha + r'$, provided r and r' are rigid-terms and $\alpha \in \mathbb{R}_{\geq 0}$.

Axiom (D7) states that if $\int^r \phi \leq r'$ is satisfied before the next α time units then $\int^{\alpha+r} \phi \leq \alpha + r'$ is satisfied now. Thus, if a system has to satisfy the requirement that the duration of the critical state ϕ is less than ω in any period of γ time units, i.e. $\Box \int^\gamma \phi \leq \omega$, then the system can postpone a reaction to the occurrence of a state in which ϕ holds during α time units, but then it must ensure that the duration of ϕ during the next $\gamma - \alpha$ time units is less than $\omega - \alpha$, i.e. $\int^{\gamma-\alpha} \phi \leq \omega - \alpha$.

Lemma 4.3 *Axiom (D7) is sound.* $\square$

Proof. *Consider a model* (σ,ϑ) *and* $t \in \mathbb{R}_{\geq 0}$ *with* $(\sigma,\vartheta,t) \models \Diamond_{\leq\alpha} \int^r \phi \leq r'$. *Thus, there exists* $t' \in [t, t+\alpha]$ *with* $(\sigma,\vartheta,t') \models \int^r \phi \leq r'$. *Let* $\beta = \mathcal{T}[\![r]\!](\sigma,\vartheta)t'$ *and* $\omega = \mathcal{T}[\![r']\!](\sigma,\vartheta)t'$. *Since r and r'* *are rigid-terms,* $\beta = \mathcal{T}[\![r]\!](\sigma,\vartheta)t$ *and* $\omega = \mathcal{T}[\![r']\!](\sigma,\vartheta)t$.

If $\beta < 0$, *then* $0 = \int_{t'}^{t'+\beta} 1_{\phi(\sigma,\vartheta)}(x)dx \leq \omega$. *Hence,* $\omega \geq 0$ *and* $\alpha + \beta < \alpha$, *and therefore,* $\mathcal{T}[\![\int^{\alpha+r}\phi]\!](\sigma,\vartheta)(t) = \int_t^{t+\alpha+\beta} 1_{\phi(\sigma,\vartheta)}(x)dx \leq \alpha \leq \alpha+\omega = \mathcal{T}[\![\alpha+r']\!](\sigma,\vartheta)(t)$.
If $\beta \geq 0$, *then* $\int_{t'}^{t'+\beta} 1_{\phi(\sigma,\vartheta)}(x)dx \leq \omega$. *Consequently,*

$$\begin{aligned}
\mathcal{T}[\![\textstyle\int^{\alpha+r}\phi]\!](\sigma,\vartheta)(t) = \int_t^{t+\alpha+\beta} 1_{\phi(\sigma,\vartheta)}(x)dx &= \int_t^{t'} 1_{\phi(\sigma,\vartheta)}(x)dx + \int_{t'}^{t'+\beta} 1_{\phi(\sigma,\vartheta)}(x)dx + \\
&\quad \int_{t'+\beta}^{t+\alpha+\beta} 1_{\phi(\sigma,\vartheta)}(x)dx \\
&\leq t'-t+\omega+t-t'+\alpha \\
&= \alpha+\omega = \mathcal{T}[\![\alpha+r']\!](\sigma,\vartheta)(t)
\end{aligned}$$

□

The next axiom claims that in order to satisfy $\int^\alpha \phi \leq \beta$, it suffices to ensure that $\int^\alpha \phi \leq \beta$ is satisfied in every point in which ϕ holds during the next α time units.

(D8)	$\Box_{<\alpha}(\phi \to \int^\alpha \phi \leq \beta) \Rightarrow \int^\alpha \phi \leq \beta$, provided $\alpha \in \mathbb{R}_{\geq 0}$.

To prove soundness of Axiom (D8), first consider the following lemma.

Lemma 4.4 *Let* $f : \mathbb{R}_{\geq 0} \to \{0,1\}$ *be a function that satisfies the finite variability condition, that is,* f *has in each bounded subinterval of* $\mathbb{R}_{\geq 0}$ *finitely many discontinuity points. For all* $\alpha, t, \beta \in \mathbb{R}_{\geq 0}$, *if* $\int_t^{t+\alpha} f(x)dx > \beta$ *then there exists* $t_0 \in [t, t+\alpha)$ *with* $\int_{t_0}^{t_0+\alpha} f(x)dx > \beta$ *and* $f(t_0) = 1$. □

Proof. *Consider a function* f, t, α, *and* β *as above. Since* f *satisfies the finite variability condition, interval* $[t, t+\alpha)$ *can be partitioned into finitely many intervals* $I_1, \ldots, I_n$, *such that* $\bigcup_{i=1}^n I_i = [t, t+\alpha)$, f *is constant on* I_n, *and for each* $i < n$:

1. $t < t'$, *for each* $t \in I_i$ *and* $t' \in I_{i+1}$ *and*
2. f *is constant on* I_i,
3. *there exist* $t' \in I_i$, $t'' \in I_{i+1}$ *with* $f(t') \neq f(t'')$,

Since $\int_t^{t+\alpha} f(x)dx > \beta \geq 0$ *and* $\bigcup_{i=1}^n I_i = [t, t+\alpha)$, *the set* $\{i \mid \exists t \in I_i\, f(t) = 1\}$ *is nonempty, and therefore, there exists a least index* k *such that there exists* $t' \in I_k$ *with* $f(t') = 1$. *Let* $l(I_k)$ *denote the left end-point of* I_k *and* l *its length. By condition 1.,* $\bigcup_{i=1}^n I_i = [t, t+\alpha)$, *and definition of* I_k, *for each* $t \leq t' < l(I_k)$, $f(t') = 0$. *Thus,* $\int_t^{l(I_k)} f(x)dx = 0$.

Let $t_0 = l(I_k) + \min(\frac{l}{2}, \frac{\int_t^{t+\alpha} f(x)\,dx - \beta}{2})$. *By definition of* I_k, $l > 0$ *and since* $\int_t^{t+\alpha} f(x)dx - \beta > 0$, *we have* $t \leq t_0 < l(I_k) + l \leq t + \alpha$. *Thus,* $t_0 \in [t, t+\alpha)$ *and by condition 2.,* $f(t_0) = 1$. *Furthermore, we have*
$\int_{t_0}^{t_0+\alpha} f(x)\,dx \geq \int_{t_0}^{t+\alpha} f(x)\,dx = \int_{l(I_k)}^{t+\alpha} f(x)\,dx - \int_{l(I_k)}^{t_0} f(x)\,dx$

$$\geq \int_{l(I_k)}^{t+\alpha} f(x)\,dx - \min(\tfrac{l}{2}, \tfrac{\int_t^{t+\alpha} f(x)\,dx - \beta}{2})$$
$$\geq \int_t^{t+\alpha} f(x)\,dx - \tfrac{\int_t^{t+\alpha} f(x)\,dx - \beta}{2} = \tfrac{\int_t^{t+\alpha} f(x)\,dx + \beta}{2} > \beta. \qquad \square$$

Corollary 4.5 *Axiom (D8) is sound.* $\square$

Proof. *Consider a model* (σ, ϑ) *and* $t \in \mathbf{R}_{\geq 0}$. *By lemma 4.4,* $(\sigma, \vartheta, t) \models \int^{\alpha} \phi > \beta$ *implies* $(\sigma, \vartheta, t) \models \Diamond_{<\alpha}(\phi \wedge \int^{\alpha} \phi > \beta)$. *The corollary follows by contraposition.* $\square$

4.1 Example

To illustrate the use of these axioms, consider again the Gas Burner requirement of example 2.4, which has been specified in MTL-$\int$ by

$$\mathit{Req} \qquad \Box \int^{30} \mathit{Leak} \leq 4$$

A possible control strategy for the Gas Burner system is to ensure that whenever gas leaks the system enters within 4 time units a purge period of 26 time units, during which gas cannot leak. This strategy can be specified in MTL-$\int$ by the following formula:

$$\mathit{Des} \qquad \mathit{Leak} \Rightarrow \Diamond_{\leq 4} \Box_{<26} \neg \mathit{Leak}$$

To prove that this strategy meets the requirement Req, we have to prove that $\mathit{Des} \Rightarrow \mathit{Req}$ is a valid formula. We show that this formula is derivable by our axioms, adopting all valid MTL formulae as axioms. Derivation steps that are justified by metric temporal reasoning are marked by MTR. Steps using propositional reasoning are indicated by PROP. The notation $\vdash \phi$ means that ϕ is derivable.

(0)	$\vdash \Box_{<26} \neg \mathit{Leak} \Rightarrow \Box_{<26}(\mathit{Leak} \rightarrow \mathit{false})$	PROP
(1)	$\vdash 26 \leq 26 \wedge \Box_{<26}(\mathit{Leak} \rightarrow \mathit{false}) \Rightarrow \int^{26} \mathit{Leak} \leq \int^{26} \mathit{false}$	$(D5)$
(2)	$\vdash \Box_{<26} \neg \mathit{Leak} \Rightarrow \int^{26} \mathit{Leak} \leq \int^{26} \mathit{false}$	$(0), (1)$, PROP
(3)	$\vdash \Box \int^{26} \mathit{false} = 0$	$(D1)$
(4)	$\vdash \Box_{<26} \neg \mathit{Leak} \Rightarrow \int^{26} \mathit{Leak} \leq 0$	PROP, $(2), (3)$
(5)	$\vdash \Diamond_{\leq 4} \Box_{<26} \neg \mathit{Leak} \Rightarrow \Diamond_{\leq 4} \int^{26} \mathit{Leak} \leq 0$	MTR, (4)
(6)	$\vdash \Diamond_{\leq 4} \int^{26} \mathit{Leak} \leq 0 \Rightarrow \int^{30} \mathit{Leak} \leq 4$	$(D7)$
(7)	$\vdash \Diamond_{\leq 4} \Box_{<26} \neg \mathit{Leak} \Rightarrow \int^{30} \mathit{Leak} \leq 4$	PROP, $(5), (6)$
(8)	$\vdash \mathit{Des} \Rightarrow (\mathit{Leak} \Rightarrow \int^{30} \mathit{Leak} \leq 4)$	PROP, Def. of Des, (7)
(9)	$\vdash (\mathit{Leak} \Rightarrow \int^{30} \mathit{Leak} \leq 4) \Rightarrow \Box \Box_{<30}(\mathit{Leak} \rightarrow \int^{30} \mathit{Leak} \leq 4)$	MTR
(10)	$\vdash \Box_{<30}(\mathit{Leak} \rightarrow \int^{30} \mathit{Leak} \leq 4) \Rightarrow \int^{30} \mathit{Leak} \leq 4$	$(D8)$
(11)	$\vdash (\mathit{Leak} \Rightarrow \int^{30} \mathit{Leak} \leq 4) \Rightarrow \Box \int^{30} \mathit{Leak} \leq 4$	PROP, $(9), (10)$
(12)	$\vdash \mathit{Des} \Rightarrow \Box \int^{30} \mathit{Leak} \leq 4$	PROP, $(8), (11)$

4.2 Concluding Remarks

There are two main differences between the proof system of DC in [11] (PSDC for short) and ours (apart from axioms (D6), (D7), and (D8) that relate duration formulae to metric temporal operators and therefore do not correspond to any axiom in PSDC). The first one is that axioms (D2) and (D4) of our proof system do not have their counterparts in PSDC. The reason for this is that terms in DC do not refer to the end-points of the interval in which they are evaluated, whereas a duration term $\int^r \phi$ in MTL-$\int$ explicitly mentions the right end-point of the interval in which the duration of ϕ is measured. Thus, in DC one cannot write $\int^{30} \phi = 4$ as in MTL-$\int$; one would write $\int true = 30 \rightarrow \int \phi = 4$. Axioms (D2) and (D4) describe how a duration term of MTL-$\int$ $\int^r \phi$ depends on the explicit argument r. Axiom (D2) states that if this argument is zero then the whole term has zero as semantics, this is because the duration of any formula in a singular interval is zero, and axiom (D4) states that duration terms are monotonic in this argument.

The second main difference is the absence of any induction rule in our proof system, while PSDC includes two (symmetric) induction rules. For DC, it is possible to formulate a sound induction rule because terms and formulae are interpreted in *finite* intervals. As shown in section 3.1, this, however, has the consequence that *only safety* properties can be specified in DC. As soon as one introduces infinite intervals, the induction rules become unsound, since using them one can prove that each non-point interval I, i.e. each interval of positive length l, either does not contain any subinterval in which $\neg P$ is almost everywhere true, or the duration of P in I is strictly less than l, that is, one can derive:

$$Prop \qquad \int true = 0 \vee ((true ^\frown (\int \neg P = \int true > 0)^\frown true) \rightarrow \int P < \int true).$$

It is not difficult to see that whereas $Prop$ is valid for finite intervals, it is not valid for infinite ones, since for an infinite interval I if P is everywhere true except for a finite subinterval, the duration of P is infinite, and hence, equal to the length of I.

Skakkebæk [35] has recently extended DC to allow expression of liveness properties by including two extra chopping operators, $\lhd$ and $\rhd$. Informally, $A \lhd B$ holds in an interval $[b, c]$ if there exists an interval $[a, c]$ such that A holds in $[a, b]$ and B holds in $[a, c]$; and $A \rhd B$ holds in an interval $[a, b]$ if there exists an interval $[b, c]$ such that A holds in $[a, c]$ and B holds in $[b, c]$. The resulting calculus DCL is based on Venema's modal interval logic CDT [36] in the same way as DC is based on Moszkowski's interval temporal logic [28].

5 Proof Methodologies

Proof methodologies for verifying bounded-invariance and bounded-response properties of timed transition systems are presented in [12]. Bounded-invariance properties are formulae of the form $\phi \to \Box_{<T}\psi$, bounded-response properties of the form $\phi \to \Diamond_{\leq T}\psi$, where ϕ and ψ are state formulae. In this section, we extend the proof methodology given in [12] by a proof rule for verifying *limited-duration* properties. A *limited-duration property* is a formula of the form $\Box \int^{\alpha} B \leq \beta$, where $\alpha, \beta \in \mathbb{R}_{\geq 0}$ and B is a boolean assertion. Informally, a limited-duration property asserts that the duration of state B is less than β in any period of α time units.

5.1 Computational Model

The abstract computational model we use is that of *timed transition systems* as presented in [4]. Closely related models are presented in [12, 13, 1]. A timed transition system generates a set of *timed state sequences.* A timed state sequence is a sequence of pairs of states and intervals in $\mathbf{R}_{\geq 0}$. Each of these pairs describes the state of the system in all points in the interval. The semantics of concrete systems can be defined by associating a timed transition system to each concrete one.

Definition 5.1 *A* timed transition system $\mathrm{TTS} = (\mathsf{P}, \mathcal{I}, \mathcal{T}, l, u)$ *consists of the following components:*

1. *A finite set* P *of propositional letters.*
2. *A set* $\mathcal{I} \subseteq 2^{\mathsf{P}}$ *of possible initial states.*
3. *A finite set* $\mathcal{T}$ *of transitions. Each transition consists of a name* τ *and a relation* ρ_τ *on* 2^{P}*. We assume that all transitions in* $\mathcal{T}$ *have different names and identify a transition with its name. A transition* τ *is called* enabled on state s *if there exists* $s' \in 2^{\mathsf{P}}$ *with* $(s, s') \in \rho_\tau$*.* τ *is called* disabled on s *if it is not enabled on* s*.*
4. *A minimal delay* $l_\tau \in \mathbf{R}_{\geq 0}$*, for each transition* $\tau \in \mathcal{T}$*.*
5. *A maximal delay* $u_\tau \geq l_\tau$ *with* $u_\tau \in \mathbb{R}_{\geq 0} \cup \{\infty\}$*, for each* $\tau \in \mathcal{T}$*.*

□

Time is incorporated in this model by specifying constraints on the times at which transitions may happen, assuming that transitions happen instantaneously. A minimal delay l_τ asserts that transition τ can only be taken if it has been continuously enabled for l_τ time units, a maximal delay u_τ asserts that τ cannot be continuously enabled more than u_τ time units without being taken. An infinite maximal delay, $u_\tau = \infty$, introduces a weak fairness assumption for transition τ.

We assume that the set P of each timed transition system TTS includes for every transition τ the proposition $En(\tau)$ and that, for each state s, $En(\tau) \in s$ iff τ is enabled on s. To simplify the formalism, we also assume that every timed transition system TTS contains the idle transition τ_I with $\rho_{\tau_I} = \{(s,s) \mid s \in 2^{\mathsf{P}}\}$, $l_{\tau_I} = 0$, and $u_{\tau_I} = \infty$. This assumption ensures that timed transition systems generate only infinite sequences.

Let from now on $l(I)$ denote the left end-point of interval I and $r(I)$ denote the right end-point of I, if it exists. For a bounded interval in $\mathbb{R}_{\geq 0}$ both left- and right-end points exist. Two intervals I and I' are called adjacent iff (1) $r(I) = l(I')$ and (2) either I is right-open and I' is left-closed, or I is right-closed and I' is left-open.

A *timed state sequence* consists of an infinite sequence $(s_0, I_0) \xrightarrow{\tau_0} (s_1, I_1) \cdots$, satisfying for each $i \geq 0$, that $s_i \in 2^{\mathsf{P}}$, I_i is nonempty and right-closed, I_i and I_{i+1} are adjacent intervals in $\mathbb{R}_{\geq 0}$, and $\bigcup_{i \geq 0} I_i = \mathbb{R}_{\geq 0}$.

Consider a time t and let i be the (unique) index such that $t \in I_i$. A transition τ is said to be enabled, respectively disabled, at t in a timed state sequence, if τ is enabled, respectively disabled, on s_i. A transition τ is said to be taken at a point in time t if there exists an i with $r(I_i) = t$ and $\tau_i = \tau$.

For each transition τ we define a function δ_τ that maps each timed state sequence ts and $t \in \mathbb{R}_{\geq 0}$ to $\delta_\tau(ts, t)$, the time that has elapsed since transition τ became enabled in ts after t. For a timed state sequence $ts = (s_0, I_0) \xrightarrow{\tau_0} (s_1, I_1) \cdots$ and $t \in I_i$, we have that if τ is enabled at t and not taken at $l(I_i)$, then $\delta_\tau(ts, t) = \delta_\tau(ts, l(I_i)) + t - l(I_i)$; if τ is enabled at t and taken at $l(I_i)$, then $\delta_\tau(ts, t) = t - l(I_i)$; if τ is not enabled at t then $\delta_\tau(ts, t) = 0$.

Example 5.2 *Let us consider a concrete timed state sequence and see what values function δ_τ yields at different time points. Let ts be the following sequence*

$$(\{En(\tau), En(\tau_I)\}, [0,1]) \xrightarrow{\tau} (\{En(\tau), En(\tau_I)\}, (1,2]) \xrightarrow{\tau} (\{En(\tau_I)\}, (2,5]) \xrightarrow{\tau_I} \cdots$$

Then, $\delta_\tau(ts, 1) = 1$, since τ is enabled at 1 and not taken at 0; $\delta_\tau(ts, 1.5) = 0.5$, since τ is enabled at 1.5 and taken at 1; and finally $\delta_\tau(ts, 4) = 0$, since τ is disabled at 4. □

A *computation* cp of a timed transition system $TTS = (\mathsf{P}, \mathcal{I}, \mathcal{T}, l, u)$ is a timed state sequence $(s_0, I_0) \xrightarrow{\tau_0} (s_1, I_1) \cdots$ satisfying:

1. Initiality: $s_0 \in \mathcal{I}$.

2. Consecution: For each $i \geq 0$, there is a transition $\tau \in \mathcal{T}$ with $(s_i, s_{i+1}) \in \rho_\tau$.

3. Lower bound: For each transition $\tau \in \mathcal{T}$, and $t \in \mathbb{R}_{\geq 0}$, if τ is taken at t in cp then $\delta_\tau(cp, t) \geq l_\tau$.

4. Upper bound: For each transition $\tau \in \mathcal{T}$, and $t \in \mathbb{R}_{\geq 0}$, $\delta_\tau(cp, t) \leq u_\tau$. Further, if $u_\tau = \infty$ then there exists $t' \geq t$ with $\delta_\tau(cp, t') = 0$ or τ is taken at t' in cp.

Thus, the lower bound condition rules out timed state sequences in which a transition τ is taken without being enabled for l_τ units. The upper bound condition rules out timed state sequences in which a transition τ is continuously enabled for more than u_τ without being taken. If $u_\tau = \infty$, the upper bound condition forbids timed state sequences that are weakly unfair w.r.t. τ.

It is not difficult to see that, for each timed state sequence and for each $t \in \mathbb{R}_{\geq 0}$, there exists a unique i with $t \in I_i$. This implies that timed transition systems only generate NonZeno timed state sequences [1], i.e. only sequences in which there are finitely many changes within each finite interval. Observe also that each timed state sequence ts can be transformed into an observation $R(ts)$ in $\mathcal{O}$, where R is defined as follows: for every $P \in \mathcal{P}$ and every $t \in \mathbb{R}_{\geq 0}$, $R(ts)(P)(t) = tt$ iff there exists an i with $t \in I_i$ and $P \in s_i$. Finite variability of observation $R(ts)$ follows from the NonZenoness of sequence ts.

We can now define when a timed transition system TTS satisfies an MTL-$\int$ formula ϕ, denoted by $TTS \models \phi$:

Definition 5.3 *A timed transition system* TTS *satisfies* ϕ *iff for every computation* cp *of* TTS *and every* $\vartheta \in \Theta$, $(R(cp), \vartheta) \models \phi$. □

5.2 Verification of Limited-duration Properties

In this section we show how to prove that a given timed transition system TTS satisfies a limited-duration property. We present proof rules for verifying such properties. These rules use minimal and maximal delays of transitions. Before we present the proof rules, we need a few preparations.

Let $\mathcal{I}(B)$ denote the interpretation of boolean assertion B as a set of states in 2^{P}, i.e. $\mathcal{I}(true) = 2^{\mathsf{P}}$, $\mathcal{I}(P) = \{s \in 2^{\mathsf{P}} \mid P \in s\}$, for $P \in \mathcal{PL}$, $\mathcal{I}(B_1 \wedge B_2) = \mathcal{I}(B_1) \cap \mathcal{I}(B_2)$, and $\mathcal{I}(\neg B) = 2^{\mathsf{P}} - \mathcal{I}(B)$. We call a state s a B-state if $s \in \mathcal{I}(B)$.

For given observation σ and $t \in \mathbb{R}_{\geq 0}$, we call a set $s \in 2^{\mathsf{P}}$ *σ-observed at t*, if s is the set of all propositional letters $P \in \mathsf{P}$ with $\sigma(P)(t) = tt$, i.e. $s = \{P \in \mathsf{P} \mid \sigma(P)t = tt\}$.

One can prove the following result.

Lemma 5.4 *For every model* (σ, ϑ), *state* $s \in 2^{\mathsf{P}}$ *and* $t \in \mathbb{R}_{\geq 0}$, *if* s *is* σ*-observed at* t *then* $(\sigma, \vartheta, t) \models B$ *iff* $s \in \mathcal{I}(B)$. □

Proof. *Straightforward induction on the structure of* B. □

Corollary 5.5 *For every boolean assertion* B, $\mathcal{I}(B) = 2^{\mathsf{P}}$ *iff* $\models \Box B$. □

Our proof rule has verification conditions $\{B\}\tau\{B'\}$, where τ is a transition and B and B' are boolean assertions, as premises. A verification condition $\{B\}\tau\{B'\}$ is satisfied if for every states s and s' such that s is a B-state and $(s, s') \in \rho_\tau$, s' is a B'-state. We use $\{B\}\mathcal{T}\{B'\}$ as abbreviation of $\bigwedge_{\tau \in \mathcal{T}} \{B\}\tau\{B'\}$.

Using lemma 5.4 one can prove the following result.

Lemma 5.6 *For every transition τ, every boolean assertions B and B' with $\{B\}\tau\{B'\}$, and every model (σ, ϑ) with s and s' as σ-observed states at t, respectively t', if $(\sigma, \vartheta, t) \models B$ and $(s, s') \in \rho_\tau$ then $(\sigma, \vartheta, t') \models B'$.* □

Proof. *Follows from lemma 5.4 and the definition of $\{B\}\tau\{B'\}$.* □

We are now ready to formulate our proof rule for verifying limited-durations. It shows how to prove that a timed transition system $TTS = (\mathsf{P}, \mathcal{I}, \mathcal{T}, l, u)$ satisfies a limited-duration property $\Box \int^\alpha B \leq \beta$.

In the rule three subsets of $\mathcal{T}$ are used, namely H, $\tilde{H}$, and L, and two assertions ϕ and ψ. The formula ϕ, called the invariant of the rule, usually (but not necessarily) characterises the reachable states of TTS or is a weaker invariant of the timed transition system. The transitions in $\tilde{H}$ are harmless transitions, since they never lead to a B-state when executed in a reachable $\neg B$-state. Intuitively, the transitions in L are dangerous in the sense that they may lead to a B-state and have a small lower bound. Formula ψ characterises the states in which transitions in L are disabled during the next γ time units, implying by the lower bound condition that a $\tau \in L$ cannot be taken during the next $\gamma + l_\tau$ time units. The set H contains helpful transitions that lead to a $\neg B$-state in which ψ holds.

LD

(0) $TTS \vdash B \Rightarrow \phi \wedge \bigvee_{\tau \in H} En(\tau)$

(1) $TTS \vdash \psi \Rightarrow \Box_{<\gamma} \bigwedge_{\tau \in L} \neg En(\tau)$

(2) $\bigwedge_{\tau \in H} \{\phi \wedge En(\tau)\}\ \mathcal{T} - H\ \{\phi \wedge En(\tau)\}$

(3) $\{\phi \wedge \neg B\}\ \tilde{H}\ \{\phi \wedge \neg B\}$

(4) $\bigwedge_{\tau \in \mathcal{T} - \tilde{H}} \{\phi \wedge En(\tau)\}\ H\ \{\neg En(\tau)\}$

(5) $\{\phi\}\ H\ \{\neg B \wedge \psi \wedge \phi\}$

$$\overline{\qquad TTS \vdash \Box \int^{M+m} B \leq M \qquad}$$

Here ϕ and ψ are Boolean assertions, $M = \max\{u_\tau \mid \tau \in H\}$,
$m = \min(\{\gamma + l_\tau \mid \tau \in L\} \cup \{l_\tau \mid \tau \in \mathcal{T} - (\tilde{H} \cup L)\})$ and provided $M + m \in \mathbb{R}_{\geq 0}$.

To establish premises (0) and (1), one has to derive that timed transition system TTS satisfies the invariance property $B \Rightarrow \phi \wedge \bigvee_{\tau \in H} En(\tau)$ and the bounded-invariance property $\psi \Rightarrow \Box_{<\gamma} \bigwedge_{\tau \in L} \neg En(\tau)$. Complete rules for deriving such formulae are given in [12].

Premise (0) ensures that on each B-state at least one helpful transition is enabled and premise (2) ensures that this transition remains enabled unless a helpful transition is taken. Premises (1) and (5) state that after execution of a helpful transition, all transitions in L are disabled during γ time units. Premise (3) states that transitions in $\tilde{H}$ never lead to a B-state when executed in a $\neg B$-state. Premise (4) ensures that each helpful transition τ disables any transition that is enabled when τ is taken and that is not harmless. Premise (5) ensures that any helpful transition that is taken in a ϕ-state leads to a $\neg B$-state. Since by premise (0) every reachable B-state is a ϕ-state, this implies that any helpful transition that is taken in a B-state leads to a $\neg B$-state.

Theorem 5.7 *Proof rule LD is sound.* $\Box$

Proof. *Consider a timed transition system* TTS*. Assume that all premises of rule LD are satisfied. Thus, we have sets H, $\tilde{H}$, and L of transitions in $\mathcal{T}$ such that*

(0) $\text{TTS} \models B \Rightarrow \phi \wedge \bigvee_{\tau \in H} En(\tau)$,

(1) $\text{TTS} \models \psi \Rightarrow \Box_{<\gamma} \bigwedge_{\tau \in L} \neg En(\tau)$,

(2) $\{\phi \wedge En(\tau)\}\tau'\{\phi \wedge En(\tau)\}$ *is satisfied, for each* $\tau \in H$ *and each* $\tau' \in \mathcal{T} - H$,

(3) $\{\phi \wedge \neg B\}\tau\{\phi \wedge \neg B\}$ *is satisfied for each* $\tau \in \tilde{H}$,

(4) $\{\phi \wedge En(\tau)\}\tau'\{\neg En(\tau)\}$ *is satisfied, for each* $\tau \in \mathcal{T} - \tilde{H}$ *and each* $\tau' \in H$, *and*

(5) $\{\phi\}\tau\{\neg B \wedge \psi \wedge \phi\}$ *is satisfied, for each* $\tau \in H$.

Take an arbitrary computation $cp : (s_0, I_0) \xrightarrow{\tau_0} (s_1, I_1) \cdots$ *of* TTS *and take an arbitrary environment* $\vartheta \in \Theta$. *We have to prove* $(R(cp), \vartheta, 0) \models \Box \int^{M+m} B \leq M$.
The proof is by contradiction. Consider $t \in \mathbb{R}_{\geq 0}$ *with* $(R(cp), \vartheta, t) \not\models \int^{M+m} B \leq M$.
Thus, $\int_t^{M+m} 1_{B(R(cp),\vartheta)}(x)\, dx > M$, *and hence,* $M \in \mathbb{R}_{\geq 0}$. *By lemma 4.4, there exists* $t_0 \in \mathbb{R}_{\geq 0}$ *with* $1_{B(r(cp),\vartheta)}(t_0) = 1$ *and* $\int_{t_0}^{M+m} 1_{B(R(cp),\vartheta)}(x)\, dx > M$, *i.e.*
$(R(cp), \vartheta, t_0) \models B \wedge \int^{M+m} B > M$. (†).
We show that (0)-(5) imply $(R(cp), \vartheta, t_0) \models \int^{M+n} B \leq m$, *which contradicts* (†).
From (†) *and (0), we have* $(R(cp), \vartheta, t_0) \models \phi \wedge \bigvee_{\tau \in H} En(\tau)$.
Hence, by the definition of R, there exists $\tau \in H$ *such that* τ *is enabled at* t_0 *in cp.* (‡).

Next, we prove that there exists $t_1 \in \mathbb{R}_{\geq 0}$ *and a transition* $\tau' \in H$ *such that* $t_0 \leq t_1 \leq t_0 + M$, $(R(cp), \vartheta, t_1) \models \phi$, *and* τ' *is taken at* t_1 *in cp.*

Assume that for every $t_1 \in \mathbb{R}_{\geq 0}$ *with* $t_0 \leq t_1 \leq t_0 + M$ *and every transition* $\tau' \in H$ *with* $\tau' \neq \tau$, τ' *is not taken at* t_1 *in cp. Then, by (2) and (‡), if* τ *is not taken at any* t_1 *with* $t_0 \leq t_1 \leq t_0 + M$ *in cp then* τ *is enabled at each* t_1, *with* $t_0 \leq t_1 \leq t_0 + M$ *in cp. Since the latter contradicts the upper bound condition, there exists* $t_1 \in \mathbb{R}_{\geq 0}$ *with* $t_0 \leq t_1 \leq t_0 + M$ *such that* τ *is taken at* t_1 *in cp. On the other hand, since cp is NonZeno,* t_1 *can be chosen such that no transition in* H *is taken at any* $t'' \in [t_0, t_1)$ *in cp. Thus, by (2),* t_1 *can be chosen such that* $(R(cp), \vartheta, t_1) \models \phi$.

We proceed to show that the existence of such a t_1 *leads to a contradiction to (†). This is done in two steps. First, we prove that if such a* t_1 *exists then each transition that is taken in* $(t_1, t_1 + m)$ *is in* $\tilde{H}$ *and then use (3) and (5) to derive a contradiction.*
Consider $t_1 \in \mathbb{R}_{\geq 0}$ *and* $\tau' \in H$ *such that* τ' *is taken at* t_1 *in cp,* $t_0 \leq t_1 \leq t_0 + M$, *and* $(R(cp), \vartheta, t_1) \models \phi$.
Let J *be the set of all transitions in* $\mathcal{T} - (\tilde{H} \cup L)$ *that are disabled at* t_1 *in cp. By the lower bound condition, for all* $t' \in (t_1, t_1 + \min\{l_\tau \mid \tau \in J\})$, *each transition* $\tau \in J$ *is not taken at* t'. *Hence, for all* $t' \in (t_1, t_1 + m)$, *each transition* $\tau \in J$ *is not taken at* t'. **(¶)**

Let $i \geq 0$ *such that* $t_1 = r(I_i)$. *The existence of* i *follows from the definition of computation and because* τ' *is taken at* t_1. *By the definition of* J, *each transition in* $\mathcal{T} - (\tilde{H} \cup J \cup L)$ *is enabled at* t_1, *therefore, since* $(R(cp), \vartheta, t_1) \models \phi$, *by (4), the definition of* R, *and lemma 5.6, for all* $t' \in I_{i+1}$, *each transition* $\tau \in \mathcal{T} - (\tilde{H} \cup J \cup L)$ *is disabled at* t' *in cp. Therefore, by the lower bound condition, for all* $t' \in (t_1, r(I_{i+1}) + \min(\{l_\tau \mid \tau \in \mathcal{T} - (\tilde{H} \cup J \cup L)\}))$, *each transition* $\tau \in \mathcal{T} - (\tilde{H} \cup J \cup L)$ *is not taken at* t' *in cp. This and* **(¶)** *imply that, for all* $t' \in (t_1, t_1 + m)$, *each transition* $\tau \in \mathcal{T} - (\tilde{H} \cup L)$ *is not taken at* t' *in cp.*

Until now, we have proved that no transition in $\mathcal{T} - (\tilde{H} \cup L)$ *can be taken at any* $t' \in (t_1, t_1 + m)$. *Next, we prove that also no transition in* L *can be taken at any* $t' \in (t_1, t_1 + m)$.

We distinguish two cases, either $\gamma = 0$ *or* $\gamma > 0$. *If* $\gamma = 0$ *then each transition in* L *is either disabled at* t_1 *and therefore not taken at any* $t' \in (t_1, t_1 + \min\{l_\tau \mid \tau \in L\})$ *or it is enabled at* t_1 *and hence, by (4), disabled at* t', *for each* $t' \in I_{i+1}$, *implying by the lower bound condition that it cannot be taken at any* $t' \in (t_1, t_1 + \min\{l_\tau \mid \tau \in L\})$. *Since if* $\gamma = 0$, $m \leq \min\{l_\tau \mid \tau \in L\}$, *we have that each transition in* L *cannot be taken at any* $t' \in (t_1, t_1 + m)$.
We now consider the case of $\gamma > 0$. *We have by (5)* $(R(cp), \vartheta, r(I_{i+1})) \models \neg B \wedge \psi \wedge \phi$, *hence by (1) and the minimal delay condition, for all* $t' \in (t_1, r(I_{i+1}) + \min(\{\gamma + l_\tau \mid \tau \in L\}))$, *each transition in* L *is not taken at* t' *in cp. Hence, for all* $t' \in (t_1, t_1 + m)$, *each transition in* L *is not taken at* t' *in cp.*

Consequently, for all $t' \in (t_1, t_1+m)$, each transition in $\mathcal{T} - \tilde{H}$ is not taken at t' in cp, which implies that any transition that is taken in some t' in (t_1, t_1+m) is in $\tilde{H}$. Since by (3) all transitions $\tau \in \tilde{H}$ satisfy $\{\phi \wedge \neg B\}\tau\{\phi \wedge \neg B\}$ and since by (5), for each $t'' \in I_{i+1}$, $(R(cp), \vartheta, t'') \models \neg B \wedge \phi$, we have that, for all $t' \in (t_1, t_1+m)$, $(R(cp), \vartheta, t') \models \neg B$. Therefore, $\int_{t_1}^{t_1+m} 1_{B(R(cp),\vartheta)}(x)\,dx = 0$.

Since $t_0 \leq t_1 \leq t_0 + M$, we have

$$
\begin{aligned}
&\int_{t_0}^{t_o+M+m} 1_{B(R(cp),\vartheta)}(x)\,dx \\
&\quad = \int_{t_0}^{t_1} 1_{B(R(cp),\vartheta)}(x)\,dx + \int_{t_1}^{t_1+m} 1_{B(R(cp),\vartheta)}(x)\,dx + \int_{t_1+m}^{t_o+M+m} 1_{B(R(cp),\vartheta)}(x)\,dx \\
&\quad \leq t_1 - t_0 + t_0 + M + m - t_1 - m = M.
\end{aligned}
$$

This is the contradiction we wanted to prove. □

Rule LD requires that at least one helpful transition is enabled whenever computation reaches a B-state. One can, however, imagine the situation where computation reaches a B-state on which no helpful transition is enabled, but such a transition becomes enabled within α time units. The following rule is a generalization of rule LD and deals with the situation described above:

LD$\Diamond$	(0)	$TTS \vdash B \Rightarrow \Diamond_{\leq\alpha}(\phi \wedge \bigvee_{\tau\in H} En(\tau))$
	(1)	$TTS \vdash \psi \Rightarrow \Box_{<\gamma} \bigwedge_{\tau\in L} \neg En(\tau)$
	(2)	$\bigwedge_{\tau\in H} \{\phi \wedge En(\tau)\}\mathcal{T} - H\{\phi \wedge En(\tau)\}$
	(3)	$\{\phi \wedge \neg B\}\tilde{H}\{\phi \wedge \neg B\}$
	(4)	$\bigwedge_{\tau\in\mathcal{T}-\tilde{H}} \{\phi \wedge En(\tau)\}H\{\neg En(\tau)\}$
	(5)	$\{\phi\}H\{\neg B \wedge \psi \wedge \phi\}$
		$TTS \vdash \Box \int^{M+m+\alpha} B \leq M + \alpha$
Here ϕ and ψ are Boolean assertions, $M = \max\{u_\tau \mid \tau \in H\}$,		
$m = \min(\{\gamma + l_\tau \mid \tau \in L\} \cup \{l_\tau \mid \tau \in \mathcal{T} - (\tilde{H} \cup L)\})$ and provided $M + m \in \mathbb{R}_{\geq 0}$.		

Premiss (0) has been relaxed in rule LD$\Diamond$ where it is not required that each B-state satisfies $\phi \wedge \bigvee_{\tau\in H} En(\tau)$ but merely that this formula becomes true within α time units. It is easy to see that rule LD is a special case of rule LD$\Diamond$.

5.3 Example

To show an application of rule LD, we consider a timed transition system *CS*, as depicted in figure 1, that specifies the control strategy for the gas burner of section 4. The aim is to prove by means of rule LD that timed transition system *CS* satisfies the limited-duration property $\Box \int^{30} Leak \leq 4$.

Transition system *CS* has $\mathsf{P} = \{Leak, atl_i, En(\tau_i) \mid i = 0, 1, 2\} \cup \{En(\tau_I)\}$ as set of propositional letters and $\mathcal{I} = \{s_0\}$ with $s_0 = \{atl_0, En(\tau_0), En(\tau_I)\}$ as set of possible initial states. *CS* has three transitions (apart from the idling transition) τ_0, τ_1, and τ_2, i.e. $\mathcal{T} = \{\tau_0, \tau_1, \tau_2, \tau_I\}$, with

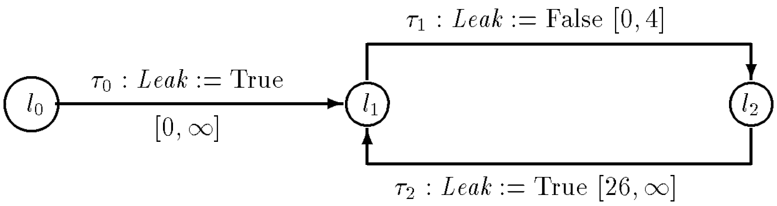

Figure 1: Transition System *CS*

- $(s, s') \in \tau_0$ iff $s = s_0$ and $s' = \{atl_1, Leak, En(\tau_1), En(\tau_I)\}$, $l_{\tau_0} = 0$, and $u_{\tau_0} = \infty$.
- $(s, s') \in \tau_1$ iff $atl_1 \in s$, and $s' = (s - \{atl_1, En(\tau_1), Leak\}) \cup \{atl_2, En(\tau_2)\}$, $l_{\tau_1} = 0$, and $u_{\tau_1} = 4$.
- $(s, s') \in \tau_2$ iff $atl_2 \in s$, and $s' = (s - \{atl_2, En(\tau_2)\}) \cup \{atl_1, Leak, En(\tau_1)\}$, $l_{\tau_2} = 26$, and $u_{\tau_2} = \infty$.

To apply rule LD, we have to define sets H, L, and $\tilde{H}$ of transitions and Boolean assertions ϕ and ψ and to prove that premises (0)-(5) are established. We define H, $\tilde{H}$, and L as follows, $H = \{\tau_1\}$, $\tilde{H} = \{\tau_1, \tau_I\}$, and $L = \{\tau_0\}$. Hence, $\mathcal{T} - (\tilde{H} \cup L) = \{\tau_2\}$. Furthermore, let ϕ abbreviate $\Box((Leak \leftrightarrow atl_1) \wedge \bigoplus_{i=0}^{2} atl_i \wedge \bigwedge_{i=0}^{2} (atl_i \leftrightarrow En(\tau_i))$, where $\bigoplus$ denotes the exclusive-or operator. It is clear that the exclusive-or operator can be defined in MTL-$\int$. Let ψ abbreviate atl_2. We want to prove that $CS \vdash Leak \Rightarrow \phi \wedge En(\tau_1)$ and $CS \vdash \psi \Rightarrow \Box\neg En(\tau_0)$ hold, which correspond to premises (0) and (1) (with $\gamma = \infty$) of the LD rule. In this case, we show that ϕ is an invariant of *CS*, i.e. $CS \vdash \Box\phi$, by ordinary timeless reasoning [23]. (Remark that timeless reasoning is sound for timed transition systems [13].) It is not difficult to see that initial state s_0 satisfies ϕ and that $\{\phi\}\tau_i\{\phi\}$ is valid for $i = 0, 1, 2$. Since $\{\phi\}\tau_I\{\phi\}$, we have $CS \vdash \Box\phi$, and by definition of ϕ, $CS \vdash Leak \Rightarrow \phi \wedge En(\tau_1)$. To establish $CS \vdash \psi \Rightarrow \Box\neg En(\tau_0)$, it suffices to prove $\vdash \phi \wedge \psi \rightarrow \neg En(\tau_0)$, and $\{\neg En(\tau_0)\}\mathcal{T}\{\neg En(\tau_0)\}$. It is easy to check that both conditions are satisfied. The main observation for establishing premises (2) and (4) is that $\{\phi \wedge En(\tau_1)\}\tau_I\{\phi \wedge En(\tau_1)\}$ holds by the definition of τ_I and $\phi \wedge En(\tau_0) \wedge En(\tau_1)$ and $\phi \wedge En(\tau_2) \wedge En(\tau_1)$ cannot be satisfied by any state, which implies that $\{\phi \wedge En(\tau_1)\}\{\tau_0, \tau_2\}\{\phi \wedge En(\tau_1)\}$, $\{\phi \wedge En(\tau_0)\}\tau_1\{\neg En(\tau_0)\}$, and $\{\phi \wedge En(\tau_2)\}\tau_1\{\neg En(\tau_2)\}$ are vacuously true. Premises (3) and (5) follow immediately from the definition of ρ_{τ_1} and ρ_{τ_I}. By the definitions of H, $\tilde{H}$, and L, we have $M = 4$ and $m = 26$. Therefore, by the LD rule $CS \vdash \Box \int^{30} Leak \leq 4$.

6 Concluding remarks

We have extended metric temporal logic with a concept of duration. The resulting logic allows the expression of properties about the duration of system's states, and the possibility to specify liveness properties makes it more expressive than the duration calculus. We have formulated a number of axioms that deal with durations and their relation to MTL operators. A further development of the axiomatisation of MTL-$\int$ is subject of future research.

We believe that many other logics can be extended with a duration concept (e.g. [15]). Our choice for metric temporal logic is based on two reasons. The first one is that many real-time properties, as bounded-response and bounded invariance, can be expressed in a natural way in metric temporal logic. The second reason is that there is a proof theory based on metric temporal logic for verifying real-time properties of programs.

An interesting direction of future work is an extension of the framework of section 5, based on [12], to enable the verification of duration properties for timed transition systems. Further the expressibility of the logic, and the power of the verification method, can be enhanced by allowing flexible variables that may change in time. Using these variables we can consider more elaborated computational models in which states are characterised by first-order formulae rather than propositions [13]. Furthermore, one can characterise each timed transition system TTS by a formula ϕ, that is, one can express a formula ϕ with $\{\sigma \mid \sigma \models \phi\} = \{R(cp) \mid cp \in \mathcal{C}(TTS)\}$, where $\mathcal{C}(TTS)$ is the set of computations generated by TTS. Based on this, one can reduce the refinement problem for timed transition systems, i.e. the question whether $\mathcal{C}(TTS) \subseteq \mathcal{C}(TTS')$, to proving a formula in MTL-$\int$ valid. This can be seen as follows. Suppose ϕ characterises TTS', ψ characterises TTS, and TTS operates on the same variables as TTS' and additionally on the variables $u_1, \ldots, u_n$. Then $\mathcal{C}(TTS) \subseteq \mathcal{C}(TTS')$ iff $\models \exists u_1, \ldots, \exists u_n \psi \rightarrow \phi$. This idea is used for proving refinement for transition systems (e.g. [20, 29]).

As an alternative to the non-compositional method of section 5 we intend to investigate the use of a compositional proof system for the top-down design of hybrid systems. The general idea is that first the top-level specification of a hybrid system is expressed in MTL-$\int$. Next the control program is specified in MTL and, using specifications of the (continuous) components of its environment, it is shown that this leads to the top-level specification. Hence the problem is reduced to the implementation of a system according to an MTL specification. The design of such a system can then be done in the compositional proof system of [14] which is based on MTL. Finally, it would be interesting to compare both approaches on a simple but typical example of a hybrid system, such as the gas burner [34].

Acknowledgements

We would like to thank Zhou Chaochen for detailed comments and useful suggestions.

References

[1] M. Abadi and L. Lamport, An old-fashioned recipe for real-time, in: J.W. de Bakker, C. Huizing, W.P. de Roever, and G. Rozenberg, ed., *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, Lecture Notes in Compute Science, Vol. 600 (Springer-Verlag 1992) 1-27.

[2] B. Alpern and F.B. Schneider, Defining liveness, *Inf. Proc. Letters* **21** (1985) 181-185.

[3] R. Alur and T.A. Henzinger, Real-time logics: Complexity and expressiveness, in: *Proc. of the 5th IEEE Symp. Logic in Comp. Sci.* (IEEE Computer Society Press, 1990) 390-401.

[4] R. Alur and T.A. Henzinger, Logics and models of real-time: A survey, in: J.W. de Bakker, C. Huizing, W.P. de Roever, and G. Rozenberg, ed., *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, Lecture Notes in Compute Science, Vol. 600 (Springer-Verlag 1992) 74-106.

[5] H. Barringer, R. Kuiper, and A. Pnueli, Now you may compose temporal logic specifications, in: *Proc. of the 16th Annual ACM Symp. on Theory of Comp.* (1984) 51-63.

[6] H. Barringer, R. Kuiper, and A. Pnueli, A really abstract concurrent model and its temporal logic, in: *Proc. of the 13th ACM Symp. on Princ. of Progr. Lang.* (1986) 173-183.

[7] H.S. Carslaw, *An introduction to the Theory of Fourier's Series and Integrals* (Dover Publications, Inc., New York, 1950.)

[8] Zhou Chaochen, M.R. Hansen, A.P. Ravn, and H. Rischel, Duration specifications for shared processors, in: J. Vytopil, ed., *Second International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems, Nijmegen, The Netherlands*, Lecture Notes in Compute Science, Vol. 571 (Springer-Verlag 1992) 21-32.

[9] Zhou Chaochen, C.A.R. Hoare, and A.P. Ravn, A calculus of durations, *Inf. Proc. Letters* **40(5)** (1991) 269-276.

[10] Zhou Chaochen, A.P. Ravn, and M.R. Hansen, An extended duration calculus for hybrid real-time systems, in: R.L. Grossman, A. Nerode, A.P. Ravn, and H. Rischel, ed., *Workshop on hybrid systems*, Lecture Notes in Compute Science, Vol. 736 (Springer-Verlag 1993) 36-59.

[11] 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, ed., *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, Lecture Notes in Compute Science, Vol. 600 (Springer-Verlag 1992) 209-225.

[12] T.A. Henzinger, Z. Manna, and A. Pnueli, Temporal proof methodologies for real-time, in: *Proc. of the 18th ACM Symp. on Princ. of Progr. Lang.* (1991) 353-366.

[13] T.A. Henzinger, Z. Manna, and A. Pnueli, Timed transition systems, in: J.W. de Bakker, C. Huizing, W.P. de Roever, and G. Rozenberg, ed., *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, Lecture Notes in Compute Science, Vol. 600 (Springer-Verlag 1992) 226-251.

[14] J. Hooman, Specification and Compositional Verification of Real-Time Systems, Lecture Notes in Compute Science, Vol. 558 (Springer-Verlag 1991).

[15] Y. Kesten and A. Pnueli, Age before beauty, Technical report, dept. of Applied Mathematics, Weizmann Institute of Science, 1992.

[16] R. Koymans, Specifying real-time properties with metric temporal logic, in: *Real-Time Systems,* **2(4)** (1990) 255-299.

[17] R. Koymans, Specifying message passing and time-critical systems with temporal logic, Lecture Notes in Compute Science, Vol. 651 (Springer-Verlag 1992).

[18] R. Koymans and W.P. de Roever, Examples of a real-time temporal logic specification, in: *The Analysis of Concurrent Systems,* Lecture Notes in Compute Science, Vol. 207 (Springer-Verlag 1985) 231-252.

[19] R. Koymans, J. Vytopil, and W.P. de Roever, Real-Time programming and asynchronous message passing, in: *Proc. of the 2nd ACM Symp. on Princ. of Dist. Comp.* (1983) 187-197.

[20] L. Lamport, The Temporal Logic of Actions, Technical report, Digital Equipment Corporation, Systems Research Center, 1991.

[21] L. Lamport, Hybrid systems in TLA$^+$, in: R.L. Grossman, A. Nerode, A.P. Ravn, and H. Rischel, ed., *Workshop on hybrid systems*, Lecture Notes in Compute Science, Vol. 736 (Springer-Verlag 1993) 77-102.

[22] O. Maler, Z. Manna, and A Pnueli, From timed to hybrid systems, in: J.W. de Bakker, C. Huizing, W.P. de Roever, and G. Rozenberg, ed., *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, Lecture Notes in Compute Science, Vol. 600 (Springer-Verlag 1992) 447-484.

[23] Z. Manna and A. Pnueli, Completing the temporal picture, in: *16th EATCS ICALP* (1989).

[24] Z. Manna and A. Pnueli, Verifying hybrid systems, in: R.L. Grossman, A. Nerode, A.P. Ravn, and H. Rischel, ed., *Workshop on hybrid systems*, Lecture Notes in Computer Science, Vol. 736 (Springer-Verlag 1993) 4-35.

[25] K. Marzullo, F.B. Schneider, and N. Budhiraja, Derivation of sequential, real-time process-control programs, in: A.M. van Tilborg and G.M. Koob, ed., *Foundations of Real-Time Computing: Formal Specifications and Methods*, (Kluver Academic Publishers 1991) chapter2, 39-54.

[26] X. Nicollin, J Sifakis, and S. Yovine, From ATP to timed graphs and hybrid systems, in: J.W. de Bakker, C. Huizing, W.P. de Roever, and G. Rozenberg, ed., *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, Lecture Notes in Compute Science, Vol. 600 (Springer-Verlag 1992) 549-572.

[27] X. Nicollin, J Sifakis, and S. Yovine, An approach to the description and analysis of hybrid systems, in: R.L. Grossman, A. Nerode, A.P. Ravn, and H. Rischel, ed., *Workshop on hybrid systems*, Lecture Notes in Compute Science, Vol. 736 (Springer-Verlag 1993) 149-178.

[28] B. Moszkowski, A temporal logic for multilevel reasoning about hardware, in: *IEEE Computer* **18(2)** (1985) 10-19.

[29] A. Pnueli, System Specification and Refinement in Temporal Logic, in: *Foundations of Software Technology and Theoretical Computer Science*, Lecture Notes in Compute Science, Vol. 652 (Springer-Verlag 1993) 1-38.

[30] J.S. Ostroff, *Temporal logic for real-time systems*, (Research Studies Press, 1989).

[31] A. Pnueli, The temporal logic of programs, in: *Proc. 18th IEEE Symp. on Found. of Comp. Sci.,* (1977) 46-57.

[32] P. Prior, *Past, Present, and Future* (Oxford University Press 1967).

[33] A.P. Ravn and H. Rischel, Requirements capture for embedded real-time systems, in: *Proc. IMACS-MCTS'91 Symp. Modelling and Control of technological Systems,* Vol. 2, 147-152 (Villeneuve d'Asq, France, 1991).

[34] A.P. Ravn, H. Rischel, and K.M. Hansen, Specifying and verifying requirements of real-time systems, in: *IEEE Transaction on Software Engeneering* (January 1993).

[35] J. U. Skakkebæk, Liveness and fairness in a Duration Calculus, Proc. CONCUR '94, Lecture Notes in Compute Science, (Springer-Verlag 1994).

[36] Y. Venema, A modal logic for chopping intervals, in: *Journal of Logic Computation,* **1(4)** (1991) 453-476.

A Proof of lemma 3.2

The following lemmas are useful for proving lemma 3.2.

Lemma A.1 *Consider an arbitrary observation σ, a Boolean assertion B, and nonnegative real numbers b and d with $b \leq d$. Let σ' denote $(\sigma{\downarrow}d){\uparrow}b$. Then, for all $t \in [0, d-b)$, $1_{B(\sigma',\vartheta)}(t) = 1_{B(\sigma,\vartheta)}(t+b)$.* □

Proof. *By induction on the structure of B. The induction step is easy and the induction basis for true is trivial. Therefore we only prove the claim for propositional letters. To do so, we first prove:*

1. $t \in [0, d-b) \cap [0, \#\sigma')$ *iff* $t + b \in [b, d) \cap [0, \#\sigma)$, *and*

2. $\sigma'(P)(t) = \sigma(P)(t+b)$, *for any* $t \in [0, d-b) \cap [0, \#\sigma')$ *and any proposition* P.

At 1. It suffices to prove $[b, d) \cap [b, \#\sigma' + b) = [b, d) \cap [0, \#\sigma)$. From the definitions of prefix and suffix of observations, one can prove $\#\sigma' = \max(0, \#(\sigma{\downarrow}d) - b) = \max(0, \min(\#\sigma, d) - b)$. Let $I \stackrel{\text{def}}{=} [b, \#\sigma' + b)$. We distinguish three cases:

- $b \geq \#\sigma$. *Then* $\#\sigma' = 0$ *and thus* $I = \emptyset = [b, d] \cap [0, \#\sigma)$.

- $b < \#\sigma < d$. *Then* $\#\sigma' = \#\sigma - b$ *and* $I = [b, \#\sigma)$. *Hence,* $I \cap [b, d) = [b, d) \cap [0, \#\sigma)$.

- *$d \leq \#\sigma$. Then $\#\sigma' = d - b$, thus $I = [b, d)$ and $[b, d) \cap [0, \#\sigma) = [b, d)$. Hence, $I \cap [b, d) = [b, d) \cap [0, \#\sigma)$.*

At 2. Consider an arbitrary $t \in [0, d - b) \cap [0, \#\sigma')$. From the definitions of prefix and suffix of observations, we have $\sigma'(P)(t) = (\sigma{\downarrow}d)(P)(t + b) = \sigma(P)(t + b)$.

It is now easy to see that 1. and 2. imply for each $t \in [0, d - b)$, that $t + b \leq \#\sigma$ iff $t \leq \#\sigma'$, and $\sigma(P)(t + b) = \sigma'(P)(t)$. Hence, for all $t \in [0, d - b)$, $1_{B(\sigma',\vartheta)}(t) = 1_{B(\sigma,\vartheta)}(t + b)$. □

Lemma A.2 *For any duration term r^D, any interval $[b, d] \subseteq \mathbb{R}_{\geq 0}$, and any model (σ, ϑ),*

$$\nu[\![r^D]\!](\sigma, \vartheta)[b, d] = \nu[\![r^D]\!]((\sigma{\downarrow}d){\uparrow}b, \vartheta)[0, d - b].$$

□

Proof. *By induction on the structure of r^D. The cases of r^D a constant or r^D a variable are trivial, since in these cases the interpretation of r^D does not depend on σ. Hence, we only consider the case $r^D \equiv \int B$, for some Boolean assertion B. Take an interval $[b, d] \subseteq \mathbb{R}_{\geq 0}$ and a model (σ, ϑ). Let σ' denote the observation $(\sigma{\downarrow}d){\uparrow}b$. We then have to prove $\int_b^d 1_{B(\sigma,\vartheta)}(t)\ dt = \int_0^{d-b} 1_{B(\sigma',\vartheta)}(t)\ dt$. By lemma A.1, we have $1_{B(\sigma',\vartheta)}(t) = 1_{B(\sigma,\vartheta)}(t + b)$, for all $t \in [0, d - b)$. Let g denote the function from real numbers to real numbers that maps x to $x + b$. Then, $\int_0^{d-b} 1_{B(\sigma',\vartheta)}(t)\ dt = \int_0^{d-b} 1_{B(\sigma,\vartheta)}(g(t))\ dt$. Since the differential of g equals 1, the substitution rule for integrals leads to $\int_0^{d-b} 1_{B(\sigma,\vartheta)}(g(t))\ dt = \int_b^d 1_{B(\sigma,\vartheta)}(t)\ dt$. Hence, $\int_b^d 1_{B(\sigma,\vartheta)}(t)\ dt = \int_0^{d-b} 1_{B(\sigma',\vartheta)}(t)\ dt$.* □

Lemma A.3 *For any interval $[b, d] \subseteq \mathbb{R}_{\geq 0}$, any model (σ, ϑ), and any formula $D \in \mathcal{D}$,*

$$(\sigma, \vartheta, [b, d]) \models_D D \text{ iff } ((\sigma{\downarrow}d){\uparrow}b, \vartheta, [0, d - b]) \models_D D$$

□

Proof. *By induction on the structure of D using lemma A.2.* □

We are now ready to prove lemma 3.2.

Proof of lemma 3.2:

Since by lemma A.3, (a) and (b) of lemma 3.2 are equivalent, it suffices to prove (b) equivalent to (c) and to (d), that is,

1. *$((\sigma{\downarrow}d){\uparrow}b, \vartheta, [0, d - b]) \models_D D$ iff $(\sigma{\uparrow}b, \vartheta, [0, d - b]) \models_D D$ and*

2. *$((\sigma{\downarrow}d){\uparrow}b, \vartheta, [0, d - b]) \models_D D$ iff $(\sigma{\downarrow}d, \vartheta, [b, d]) \models_D D$.*

- *At 1: By lemma A.3 and $((\sigma{\uparrow}b){\downarrow}(d - b)){\uparrow}0 = (\sigma{\downarrow}d){\uparrow}b$.*

- *At 2: By lemma A.3 and $((\sigma{\downarrow}d){\downarrow}d){\uparrow}b = (\sigma{\downarrow}d){\uparrow}b$.*

□