A Robust Interpretation of Duration Calculus

Martin Fränzle[1] and Michael R. Hansen[2]

[1] Carl von Ossietzky Universität Oldenburg,
FK II, Dpt. Informatik, D-26111 Oldenburg, Germany
Phone: +49-441-9722 566
fraenzle@informatik.uni-oldenburg.de
[2] Informatics and Mathematical Modelling, Technical University of Denmark,
Richard Petersens Plads, Bldg. 322, DK-2800 Kgs. Lyngby, Denmark
Phone: +45-4525 3727
mrh@imm.dtu.dk

Abstract. We transfer the concept of robust interpretation from arithmetic first-order theories to metric-time temporal logics. The idea is that the interpretation of a formula is robust iff its truth value does not change under small variation of the constants in the formula. Exemplifying this on Duration Calculus (DC), our findings are that the robust interpretation of DC is equivalent to a multi-valued interpretation that uses the real numbers as semantic domain and assigns Lipschitz-continuous interpretations to all operators of DC. Furthermore, this continuity permits approximation between discrete and dense time, thus allowing exploitation of discrete-time (semi-)decision procedures on dense-time properties.

Keywords: Metric-time temporal logic; Robust interpretation; Discrete time vs. dense time.

1 Introduction

As embedded systems become more and more complex, early availability of unambiguous specification of their intended behaviour has become an important factor for quality and timely delivery. Consequently, the quest for automatic analysis methods for specifications arises. This quest becomes even more pronounced if specifications are to be formal, because formal specifications are often found to be particularly hard to write and maintain. Therefore, decision procedures for entailment between specifications, satisfiability of specifications, etc., may be extremely helpful in their design process. The price to be paid for such procedures is, however, a firmly constrained expressiveness of the specification formalisms: one has to sacrifice all elements that could give rise to undecidability.

However, the logically motivated notions of entailment between specifications, satisfiability of specifications, etc., have often been criticized from an engineering standpoint, as their validity or invalidity may well depend on the *exact* values of certain constants (e.g., the exact length of a steering rod relative to the exact distance of two joints), while any technical realization of these constants can only be approximate. In system design, the role of any decision problem

D.V. Hung and M. Wirsing (Eds.): ICTAC 2005, LNCS 3722, pp. 257–271, 2005.

prone to changing its truth value under arbitrarily small variations of constants may be considered questionable. Based on this insight, research has in recent years addressed more "robust" notions of property satisfaction, where a property is considered to be *robustly (in-)valid* iff it does not change its validity under small variation of constants and/or values of variables [6,8,3,1,4,9,10]. The ultimate hope is that, besides being more relevant to engineering problems, such robust notions enhance decidability as, e.g., existence of non-computable reals cannot influence their validity.

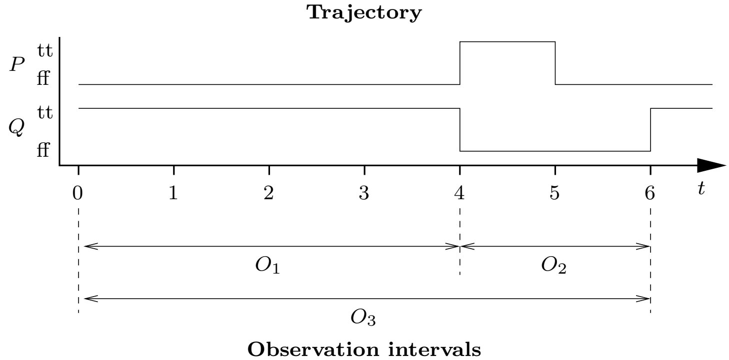
With respect to design of embedded systems, such robust properties have by now mainly been investigated in the automata-based modeling context. Starting with Gupta's, Henzinger's, and Jagadeesan's [6] as well as Puri's [8] investigation of timed automata, the idea has been to exploit topological properties of systems in order to obtain robust answers. Asarin and Bouajjani [1] have applied this approach to reach set computation of, a.o., hybrid automata and Turing machines. Fränzle introduced a variant thereof in [3] by applying the concept to decision problems about hybrid automata instead of reach-set computation, e.g. invariance of a first-order property over hybrid states [3] or progress [4], thereby obtaining automatic analysis procedures that succeed in all robust cases, even such which are undecidable wrt. non-robust notions of property satisfaction.

Independently, constraint solving technology for numerical constraints over the real numbers was developed that has perfectly corresponding properties: one can solve otherwise undecidable constraints (containing functions over the real numbers other than polynomials [14]), provided they are robust, in the sense that their solvability does not change under small perturbations of the constants the constraints contain [9,10,11]. Even in cases where constraints are decidable, robust constraints can be solved much more efficiently.

In this paper, we unite above two lines of research by addressing logical models of embedded systems. In Section 3, we provide a robust interpretation of a very expressive metric-time temporal logic, Duration Calculus [17,15], and show its equivalence to a multi-valued interpretation that uses the real numbers as semantic domain and assigns Lipschitz-continuous interpretations to all operators of DC in Section 4. Sections 5 and 6 deal with approximation of the multi-valued truth value, in particular discrete-time approximation of the dense-time interpretation, and with decidability issues.

2 Duration Calculus

Duration Calculus (abbreviated DC in the remainder) is a real-time logic that is specially tailored towards reasoning about durational constraints on time-dependent Boolean-valued states. Since its introduction in [17], many variants of Duration Calculus have been defined [15]. Aiming at a mechanizable design calculus, we present a slight syntactic subset of the Duration Calculus as defined in [17]. Our subset allows full treatment of the gas burner case study [13], the primary case study of the ProCoS project. This indicates that our subset offers an interesting vocabulary for specifying embedded real-time controllers.



The formula $\int Q > 3$ holds on observation interval $O_1 = [0, 4]$, as the accumulated duration of Q being true over this interval exceeds 3. Analogously, $\int(P \wedge \neg Q) \geq 1$ holds on observation interval $O_2 = [4, 6]$. Consequently, the formula $(\int Q > 3) \frown (\int(P \wedge \neg Q) \geq 1)$ holds on the catenation $O_3 = [0, 6]$ of the other two observation intervals.

Fig. 1. The meaning of $\int S \sim k$ and of the chop modality

Syntax. The syntax of DC used in this paper is as follows.

$$
\begin{aligned}
\phi &::= \int S \geq c \mid \int S > c \mid \neg\phi \mid (\phi \wedge \phi) \mid (\phi \frown \phi) \\
S &::= P \mid \neg S \mid (S \wedge S) \\
P &::\in \mathit{Varname} \\
c &::\in \mathbb{R} \ ,
\end{aligned}
$$

where *Varname* is a countable set of state-variable names. Note that, in contrast to other expositions of DC, we allow negative constants as this makes the theory more homogeneous.

Formulae are interpreted over trajectories providing Boolean-valued valuation of state variables that vary finitely, in the sense of featuring only finitely many changes over any finite interval of time. For a given bounded and closed time interval, also called an "observation interval", a formula is either true or false. While the meaning of the Boolean connectives used in DC formulae should be obvious, the temporal connective $\frown$ (pronounced "chop") may need some explanation. A formula $\phi \frown \psi$ is true of an observation interval iff the observation interval can be split into a left and a right subinterval s.t. ϕ holds of the left part and ψ of the right part. A duration formula $\int S \geq k$ is true of an observation interval iff the state assertion S, interpreted over the trajectory, is true for an accumulated duration of at least k time units within the observation interval. Fig. 1 provides an illustration of the meaning of these formulae.

Despite its simple syntax, DC is very expressive, as can be seen from the following abbreviations frequently used in formulae:

– $\int S < k \stackrel{\text{def}}{=} \neg \int S \geq k$ means that S holds for strictly less than k time units in the current observation interval;

- $\int S \leq k \stackrel{\text{def}}{=} \neg \int S > k$ means that S holds for at most k time units in the current observation interval,
- $\ell \geq k \stackrel{\text{def}}{=} \int \texttt{true} \geq k$, where $\texttt{true}$ is an arbitrary tautologous state assertion, denotes the fact that the observation interval has length k or more; likewise, $\ell \leq k \stackrel{\text{def}}{=} \int \texttt{true} \leq k$, $\ell < k \stackrel{\text{def}}{=} \int \texttt{true} < k$, etc.;[1]
- the temporal operators $\Diamond$ and $\Box$, meaning 'in some subinterval of the observation interval' and 'in each subinterval of the observation interval', can be defined as $\Diamond\phi \stackrel{\text{def}}{=} (\texttt{true} \frown \phi \frown \texttt{true})$ and $\Box\phi \stackrel{\text{def}}{=} \neg\Diamond\neg\phi$.

Semantics. Duration Calculus is interpreted over trajectories Traj_T, where T is the time domain. We will deal here with the discrete-time interpretation (i.e. $T = \mathbb{N}$), the rational-time interpretation (i.e. $T = \mathbb{Q}_{\geq 0}$), and the real-time interpretation (i.e. $T = \mathbb{R}_{\geq 0}$) of DC. The definition of trajectories is as follows:

$$\mathit{Traj}_T \stackrel{\text{def}}{=} \mathbb{R}_{\geq 0} \to \mathit{Varname} \to \mathbb{B} \ ,$$

where for every $tr \in \mathit{Traj}_T$, we require for each function $\underline{P}(t) = tr(t)(P)$, where $P \in \mathit{Varname}$, that the discontinuity points of $\underline{P}$ belongs to T, and the function $\underline{P}$ is finitely varied, in the sense that it has at most a finite number of discontinuity points in every bounded and closed interval.

Satisfaction of a formula ϕ by a trajectory tr is defined as a limit property over a chain of finite chunks from tr called *observations*, where an observation is a pair $(tr, [a,b]) \in \mathit{Obs}_T \stackrel{\text{def}}{=} \mathit{Traj}_T \times \mathit{TimeInterval}_T$ with $\mathit{TimeInterval}_T$ being the set of bounded and closed time intervals $\{\, [a,b] \subseteq \mathbb{R}_{\geq 0} \mid a, b \in T \,\}$.

First, we will define when an *observation* $(tr, [a,b])$ *satisfies a formula* ϕ when interpreted over time domain T, denoted $tr, [a,b] \models_T \phi$. For atomic duration formulae $\int S \geq k$ or $\int S > k$, this is defined by

$$\begin{aligned} tr, [a,b] \models_T \textstyle\int S \geq k \ \ &\text{iff} \ \ \int_{t=a}^{b} \chi \circ [\![S]\!] \circ tr(t)\,\mathrm{d}t \geq k \ , \\ tr, [a,b] \models_T \textstyle\int S > k \ \ &\text{iff} \ \ \int_{t=a}^{b} \chi \circ [\![S]\!] \circ tr(t)\,\mathrm{d}t > k \ , \end{aligned}$$

where $[\![S]\!](\sigma)$ canonically lifts a Boolean-valued interpretation $\sigma : \mathit{Varname} \to \mathbb{B}$ of state variables to an interpretation of the state assertion S, e.g. $[\![P \wedge \neg Q]\!](\sigma) = \sigma(P) \wedge \neg\sigma(Q)$, and χ maps truth values to $\{0, 1\}$ according to the convention $\chi(\texttt{false}) = 0$ and $\chi(\texttt{true}) = 1$. I.e., $\int S \geq k$ holds on $(tr, [a,b])$ iff S holds for an accumulated duration of at least k time units within $[a,b]$.
The interpretation of Boolean connectives is classical:

$$\begin{aligned} tr, [a,b] &\models_T \neg\phi && \text{iff} \ \ tr, [a,b] \not\models_T \phi \ , \\ tr, [a,b] &\models_T \phi \wedge \psi && \text{iff} \ \ tr, [a,b] \models_T \phi \ \ \text{and} \ \ tr, [a,b] \models_T \psi \ . \end{aligned}$$

[1] Note that ℓ in $\ell \sim k$ is not a state variable, but a piece of concrete syntax that denotes the length of the current observation interval.

Satisfaction of a chop formula $\phi \frown \psi$, finally, requires that the observation interval can be split into two subintervals $[a, m]$ and $[m, b]$ s.t. ϕ resp. ψ hold on the two subintervals:

$$tr, [a, b] \models_T \phi \frown \psi \text{ iff } \exists\, m \in T \cap [a, b] \,.\, \big(tr, [a, m] \models_T \phi \text{ and } tr, [m, b] \models_T \psi\big) \ .$$

A trajectory *tr satisfies a formula* ϕ, which is denoted by $tr \models_T \phi$, iff any prefix-observation of *tr* satisfies ϕ — formally, $tr \models_T \phi$ iff $tr, [0, t] \models_T \phi$ for each $t \in T$. For notational convenience, we denote the set of models of ϕ over time domain T (where $T \in \{\mathbb{N}, \mathbb{Q}_{\geq 0}, \mathbb{R}_{\geq 0}\}$), i.e. the set of trajectories satisfying ϕ wrt. to that interpretation, by $\mathcal{M}_T[\![\phi]\!]$. As usual, we say that ϕ *is valid over* T, denoted $\models_T \phi$, iff $\mathcal{M}_T[\![\phi]\!] = \mathit{Traj}_T$.

3 Robust Interpretation of DC

From an engineering perspective, arguments that become invalid when an infinitesimally small change to the constants occurring in the argument appears, are at least doubtful, if not even useless. Hence, we define a formula to be *robustly valid* iff it remains valid under some small variation of constants:

Definition 1 (Robust validity). *A DC formula ϕ is robustly valid over time domain T iff there is $\varepsilon > 0$ such that $\models_T \phi'$ holds for each $\phi' \in \mathcal{N}(\phi, \varepsilon)$, where $\mathcal{N}(\phi, \varepsilon)$ is the set of all DC formulae that are structurally equal to ϕ, yet may differ from ϕ in the constants of the individual atomic formulae by at most ε.*

I.e., $\mathcal{N}(\phi, \varepsilon)$ is the ε-neighborhood of ϕ with respect to the following recursively defined metrics on DC formulae:

$$\begin{aligned}
d(\textstyle\int S_1 \geq k, \int S_2 \geq l) &= \begin{cases} |k - l| & \text{if } S_1 = S_2, \\ \infty & \text{otherwise;} \end{cases} \\
d(\textstyle\int S_1 > k, \int S_2 > l) &= \begin{cases} |k - l| & \text{if } S_1 = S_2, \\ \infty & \text{otherwise;} \end{cases} \\
d(\neg\phi, \neg\psi) &= d(\phi, \psi) \ ; \\
d(\phi_1 \wedge \phi_2, \psi_1 \wedge \psi_2) &= \max\{d(\phi_1, \psi_1), d(\phi_2, \psi_2)\} \ ; \\
d(\phi_1 \frown \phi_2, \psi_1 \frown \psi_2) &= \max\{d(\phi_1, \psi_1), d(\phi_2, \psi_2)\} \ ; \\
d(\phi, \psi) &= \infty \text{ if } \phi \text{ and } \psi \text{ disagree on the} \\
&\qquad \text{outermost operator.}
\end{aligned}$$

In analogy to robust validity, we define *robust satisfaction* of formulae by observations and by trajectories as follows:

Definition 2 (Robust satisfaction).

1. *A formula ϕ is robustly satisfied (over time domain T) by an observation $obs \in Obs_T$ iff there is $\varepsilon > 0$ such that $obs \models_T \phi'$ holds for each $\phi' \in \mathcal{N}(\phi, \varepsilon)$.*
2. *A formula ϕ is robustly satisfied (over time domain T) by a trajectory $tr \in \mathit{Traj}_T$ iff there is $\varepsilon > 0$ such that $tr \models_T \phi'$ holds for each $\phi' \in \mathcal{N}(\phi, \varepsilon)$.*

Note that this definition in fact yields a three-valued interpretation of satisfaction by observations, as an observation may fail to robustly satisfy both ϕ and $\neg\phi$, while in classical DC, exactly one of $obs \models_T \phi$ or $obs \not\models_T \phi$ does inevitably hold. On the levels of satisfaction by trajectories or of validity, no fundamental differences do arise. It is, however, a consequence of the definitions that robust validity is more discriminative than classical validity: classical validity is a necessary, yet not sufficient, condition for robust validity.

Unfortunately, the existential quantification of ε in the three definitions yields that the relation between satisfaction by an observation, satisfaction by a trajectory, and validity is different from the classical setting. Thus, the following statements (which follow immediately from the definitions) are just single-sided implications, while they are equivalences in the classical setting:

Lemma 1 (Satisfaction vs. validity).

1. *For each trajectory $tr \in Traj_T$ it holds that ϕ is robustly satisfied (over time domain T) by all observations of the form $(tr, [0, e])$ if ϕ is robustly satisfied (over time domain T) by tr.*
2. *ϕ is robustly satisfied (over time domain T) by all trajectories tr if ϕ is robustly valid (over time domain T).*

4 Multi-valued Interpretation

As the definition of robust satisfaction or validity has an extra quantification over formula neighborhoods, the robust interpretation is structurally more complex than the standard semantics of DC. Fortunately, an equivalent semantics can be derived by more direct means, namely by a multi-valued interpretation of DC. The idea is to assign to each (sub-)formula a real-number denoting its *slackness* in the following sense: each formula is mapped to the upper bound of variation in constants it can take on the current observation without changing its truth value. Such slackness information can be lumped together with the formula's truth value by mapping it to a signed slackness value: if the formula is satisfied by the observation then we assign the slackness as its multi-valued "truth" value; otherwise we assign minus its slackness. We will now define a truth-functional version of this multi-valued interpretation and will then show that it coincides with the robust interpretation.

In a first step, we define a real-valued interpretation $\mathcal{M}_T[\![\cdot]\!] : DC \to Obs_T \to \mathbb{R}$ of formulae on observations $obs \in Obs_T$ and over time domain T as follows:

$$
\begin{aligned}
\mathcal{M}_T[\![\textstyle\int S \geq k]\!](tr, [a, b]) &= \int_{t=a}^{b} \chi \circ [\![S]\!] \circ tr(t)\,\mathrm{d}t - k \\
\mathcal{M}_T[\![\textstyle\int S > k]\!](tr, [a, b]) &= \int_{t=a}^{b} \chi \circ [\![S]\!] \circ tr(t)\,\mathrm{d}t - k \\
\mathcal{M}_T[\![\neg\phi]\!]\,obs &= -\mathcal{M}_T[\![\phi]\!](obs) \\
\mathcal{M}_T[\![\phi \wedge \psi]\!]\,obs &= \min\{\mathcal{M}_T[\![\phi]\!](obs), \mathcal{M}_T[\![\psi]\!](obs)\} \\
\mathcal{M}_T[\![\phi \frown \psi]\!](tr, [a, b]) &= \sup_{m \in T \cap [a,b]} \min\{\mathcal{M}_T[\![\phi]\!](tr, [a, m]), \mathcal{M}_T[\![\psi]\!](tr, [m, b])\} \ .
\end{aligned}
$$

In fact, the supremum operator in $\mathcal{M}_T[\![\phi \frown \psi]\!](tr, [a, b])$ could be replaced by the maximum over interval $[a, b]$, as Corollary 3 below shows the semantics to be continuous such that closedness of the observation interval $[a, b]$ implies that the maximum exists (and trivially coincides with the supremum).

Finally, we overload the symbol $\mathcal{M}_T[\![\cdot]\!]$ by defining the multi-valued interpretations $\mathcal{M}_T[\![\cdot]\!] : DC \to Traj_T \to \mathbb{R}$ over individual trajectories and $\mathcal{M}_T[\![\cdot]\!] : DC \to \mathbb{R}$ over the universe of trajectories to be

$$\mathcal{M}_T[\![\phi]\!](tr) = \inf_{e \in T} \mathcal{M}_T[\![\phi]\!](tr, [0, e]),$$
$$\mathcal{M}_T[\![\phi]\!] = \inf_{tr \in Traj_T} \mathcal{M}_T[\![\phi]\!](tr)$$

This multi-valued semantics corresponds closely to the standard semantics:

Lemma 2 (Multi-valued semantics vs. classical semantics).

1. *If* $\mathcal{M}_T[\![\phi]\!](obs) > 0$ *then* $obs \models_T \phi$;
2. *if* $\mathcal{M}_T[\![\phi]\!](obs) < 0$ *then* $obs \not\models_T \phi$;
3. *if* $\mathcal{M}_T[\![\phi]\!](tr) > 0$ *then* $tr \models_T \phi$;
4. *if* $\mathcal{M}_T[\![\phi]\!](tr) < 0$ *then* $tr \not\models_T \phi$;
5. *if* $\mathcal{M}_T[\![\phi]\!] > 0$ *then* $\models_T \phi$;
6. *if* $\mathcal{M}_T[\![\phi]\!] < 0$ *then* $\not\models_T \phi$.

I.e., positivity of the multi-valued semantics is a sufficient, yet not necessary, condition for satisfaction or validity (depending on the variant of $\mathcal{M}_T[\![\phi]\!]$ used), while negativity is a sufficient, yet not necessary, condition for dissatisfaction or invalidity. Despite this close correspondence, the multi-valued interpretation has a number of interesting properties that distinguish it from the standard interpretation:

Lemma 3 (Lipschitz-continuity). *For any DC formula ϕ, the semantic mapping $\mathcal{M}_T[\![\phi]\!] : Obs_T \to \mathbb{R}$ is Lipschitz continuous with constant 1 with respect to the metrics*

$$d\left((tr_1, [b_1, e_1]), (tr_2, [b_2, e_2])\right) \stackrel{\text{def}}{=} \max \left\{ \begin{array}{l} |b_1 - b_2|, \\ |e_1 - e_2|, \\ \int_{t=\max\{b_1,b_2\}}^{\min\{e_1,e_2\}} \chi \circ (tr_1 \neq tr_2)(t)\, \mathrm{d}t \end{array} \right\}$$

on observations.

This Lipschitz continuity, together with the following linearity properties, will allow us to develop approximation schemes for $\mathcal{M}_T[\![\phi]\!]$.

Lemma 4 (Linearity of multi-valued semantics). *Let $obs = (tr, [b, e])$ be an observation, let $c \in \mathbb{R}$ and $d \in \mathbb{R}_{>0}$. If $\mathcal{M}_T[\![\phi]\!](obs) = x$ then*

1. $\mathcal{M}_T[\![\phi_{+c}]\!](obs) = x + c$, *where ϕ_{+c} is the formula obtained from ϕ by replacing each positive occurrence of an atomic formula $\int S \geq k$ (or $\int S > k$) by $\int S \geq k - c$ (by $\int S > k - c$, resp.) and each negative occurrence by $\int S \geq k + c$ (by $\int S > k + c$, resp.),*

2. *$\mathcal{M}_{d\cdot T}[\![\phi_{\cdot d}]\!](obs') = xd$, where $d \cdot T = \{dt \mid t \in T\}$ and $\phi_{\cdot d}$ is the formula obtained from ϕ by replacing each occurrence of $\int S \geq k$ by $\int S \geq kd$ and each occurrence of $\int S > k$ by $\int S > kd$, and observation $obs' = \left(t \mapsto tr\left(\frac{t}{d}\right), [bd, ed]\right)$.*

Given these properties, which help in building verification support, as e.g. the continuity property allows to remove whole parts (namely a ball of radius δ in the observation space around obs) from the search space of a satisfiability search once an observation obs with truth value $\mathcal{M}_T[\![\phi]\!](obs) = -\delta$ has been found, it is interesting to see that the multi-valued semantics is in fact tightly linked to the robust interpretation:

Theorem 1 (Robustness vs. multi-valued).

1. *$\mathcal{M}_T[\![\phi]\!](obs) > 0$ iff obs robustly satisfies ϕ;*
2. *$\mathcal{M}_T[\![\phi]\!](tr) > 0$ iff tr robustly satisfies ϕ;*
3. *$\mathcal{M}_T[\![\phi]\!] > 0$ iff ϕ is robustly valid.*

Proof. We show only (1.); the other cases are analogous:

As $\mathcal{M}_T[\![\phi]\!](obs)$ assigns the slackness of the constants, i.e. corresponds to the amount of variation of constants that can be applied without invalidating satisfaction by obs, it is straightforward to show by induction on the structure of ϕ that $\mathcal{M}_T[\![\phi]\!](obs) > 0$ implies that all formulae ϕ' with $d(\phi, \phi') < \mathcal{M}_T[\![\phi]\!](obs)$ are satisfied by obs. I.e., $\mathcal{M}_T[\![\phi]\!](obs) > 0$ implies that obs robustly satisfies ϕ.

Vice versa, if $\mathcal{M}_T[\![\phi]\!](obs) \leq 0$ then $\mathcal{M}_T[\![\phi_{+(-\varepsilon)}]\!](obs) < 0$ for each $\varepsilon > 0$. I.e., according to Lemma 2, $obs \not\models \phi_{+(-\varepsilon)}$ for all $\varepsilon > 0$. As $d(\phi, \phi_{+(-\varepsilon)}) = \varepsilon$, this shows that obs does not robustly satisfy ϕ. □

5 Approximability

Due to the Lipschitz continuity of the multi-valued semantics and due to its correspondence to the robust interpretation, it turns out that the robust interpretation is approximable in a variety of ways. E.g., we find that the discrete-time interpretation approximates the real-time interpretation with a quantifiable tolerance. Note that such results do inherently build on the multi-valued interpretation.

5.1 Real Time Versus Rational Time

Before we can start with discrete-time approximation, we show that robust DC cannot distinguish between real-valued and rational-valued time in the sense that a robustly satisfying observation over real-valued time exists iff a robustly satisfying observation over rational time exists:[2]

[2] The same is, btw., true for the standard interpretation, yet for different reasons: for every $n \in \mathbb{N}$, existence of an observation with n discontinuities satisfying ϕ can be expressed as a formula in FOL$(\mathbb{R}, +, <)$. As FOL$(\mathbb{R}, +, <)$ cannot distinguish between rationals and reals, ϕ has a rational-time model with n state changes iff it has a real-time model with n state changes.

Lemma 5 (Rational time vs. real time). $\mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!] = \mathcal{M}_{\mathbb{Q}\geq 0}[\![\phi]\!]$.

Proof. Let $tr \in Traj_{\mathbb{R}\geq 0}$ and $e \in \mathbb{R}_{\geq 0}$. Due to density of $\mathbb{Q}$ in $\mathbb{R}$,

$$\inf_{tr' \in Traj_{\mathbb{Q}\geq 0}, e' \in \mathbb{Q}_{\geq 0}} d((tr, [0, e]), (tr', [0, e'])) = 0 \ .$$

Similarly, real-valued chop points can be arbitrarily closely approximated by rational ones. Given the continuity of $\mathcal{M}_T[\![\phi]\!]$, as expressed in Lemma 3, an easy induction over the structure of ϕ thus shows

$$\begin{aligned}
&\mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!] \\
&= \inf_{tr \in Traj_{\mathbb{R}\geq 0}, e \in \mathbb{R}} \mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!](tr, [0, e]) && [\text{Def. of } \mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!]] \\
&= \inf_{tr \in Traj_{\mathbb{Q}\geq 0}, e \in \mathbb{Q}} \mathcal{M}_{\mathbb{Q}\geq 0}[\![\phi]\!](tr, [0, e]) && [\text{Density of } \mathbb{Q} \text{ in } \mathbb{R}] \\
&= \mathcal{M}_{\mathbb{Q}\geq 0}[\![\phi]\!] && [\text{Def. of } \mathcal{M}_{\mathbb{Q}\geq 0}[\![\phi]\!]]
\end{aligned}$$

□

5.2 Approximation of Real Time Interpretation by the Discrete Time Interpretation

Given the equivalence of the real-valued time and the rational-time interpretation expressed by Lemma 5, we can proceed towards approximation of real time by discrete time:

Lemma 6 (Upper approximation by discrete time). *Let ϕ be a DC formula and let $depth(\phi)$ denote the nesting depth of chop operators in ϕ. Then*

$$\mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!] \leq \mathcal{M}_{\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2} \ .$$

Proof. Let $obs = (tr, [a, b]) \in Obs_{\mathbb{N}}$ be a discrete-time (and hence also a real-time) observation. We show by induction on the structure of ϕ that

$$\mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!](obs) \in \mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) \pm \frac{depth(\phi)}{2} \ ,$$

where $x \pm y$ denotes the set $[x - y, x + y]$.

Base case: $\phi = \int S \geq k$ or $\phi = \int S > k$. Is simple as $depth(\phi) = 0$ and $\mathcal{M}_{\mathbb{R}\geq 0}[\![\phi]\!](obs) = \int_{t=a}^{b} \chi \circ [\![S]\!] \circ tr(t)\, \mathrm{d}t - k = \mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs)$.

Induction steps $\phi = \neg\psi_1$ and $\phi = \psi_1 \wedge \psi_2$ follow from the corresponding properties of ψ_i.

Induction step: $\phi = \psi_1 \frown \psi_2$. We establish the upper bound for $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!](obs)$ below. The lower bound is established similarly.

$$\begin{aligned}
&\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!](obs) \\
&= \sup_{m\in[a,b]} \min \left\{ \begin{array}{l} \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\psi_1]\!](tr,[a,m]), \\ \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\psi_2]\!](tr,[m,b]) \end{array} \right\} && [\text{Def. } \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]] \\
&\leq \sup_{m\in\mathbb{N}\cap[a,b]} \min \left\{ \begin{array}{l} \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\psi_1]\!](tr,[a,m]), \\ \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\psi_2]\!](tr,[m,b]) \end{array} \right\} + \frac{1}{2} && [\text{Lemma 3, } d(\mathbb{N},\mathbb{R}_{\geq 0}) = \tfrac{1}{2}] \\
&\leq \sup_{m\in\mathbb{N}\cap[a,b]} \min \left\{ \begin{array}{l} \mathcal{M}_{\mathbb{N}}[\![\psi_1]\!](tr,[a,m]) + \frac{depth(\psi_1)}{2}, \\ \mathcal{M}_{\mathbb{N}}[\![\psi_2]\!](tr,[m,b]) + \frac{depth(\psi_2)}{2} \end{array} \right\} + \frac{1}{2} && [\text{Induction}] \\
&\leq \sup_{m\in\mathbb{N}\cap[a,b]} \min \left\{ \begin{array}{l} \mathcal{M}_{\mathbb{N}}[\![\psi_1]\!](tr,[a,m]) + \frac{depth(\phi)}{2}, \\ \mathcal{M}_{\mathbb{N}}[\![\psi_2]\!](tr,[m,b]) + \frac{depth(\phi)}{2} \end{array} \right\} && [depth(\psi_i) + 1 \leq depth(\phi)] \\
&= \mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) + \frac{depth(\phi)}{2} && [\text{Def. } \mathcal{M}_{\mathbb{N}}[\![\phi]\!]]
\end{aligned}$$

Thus, $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!](obs) \in \mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) \pm \frac{depth(\phi)}{2}$ holds for $\phi = \psi_1 \frown \psi_2$, which ends the induction.

As a consequence, $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!](obs) \leq \mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) + \frac{depth(\phi)}{2}$ holds for arbitrary formulae ϕ and arbitrary discrete-time observations $obs \in Obs_{\mathbb{N}}$. As the universe $Traj_{\mathbb{N}}$ of discrete-time trajectories is properly included in the universe $Traj_{\mathbb{R}_{\geq 0}}$ of real-time trajectories, we have:

$$\begin{aligned}
&\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!] \\
&= \inf_{tr\in Traj_{\mathbb{R}_{\geq 0}}, e\in\mathbb{R}_{\geq 0}} \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!](tr,[0,e]) && [\text{Def. } \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]] \\
&\leq \inf_{tr\in Traj_{\mathbb{N}}, e\in\mathbb{N}} \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!](tr,[0,e]) && [\mathbb{N} \subset \mathbb{R}_{\geq 0}] \\
&\leq \inf_{tr\in Traj_{\mathbb{N}}, e\in\mathbb{N}} \mathcal{M}_{\mathbb{N}}[\![\phi]\!](tr,[0,e]) + \frac{depth(\phi)}{2} && [\text{above induction}] \\
&= \mathcal{M}_{\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2} && [\text{Def. } \mathcal{M}_{\mathbb{N}}[\![\phi]\!]]
\end{aligned}$$

□

Therefore, dense-time formulae can be falsified using discrete-time reasoning: if $\mathcal{M}_{\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2}$ is negative then ϕ is certainly robustly invalid, as $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!] < 0$ follows.

In case above approximation is too inexact, linearity of the multi-valued semantics allows for scaling, thus yielding tighter approximation by using higher "sampling rates":

Corollary 1 (Discr. approx. with higher sampling rate). *For any* $n \in \mathbb{N} \setminus \{0\}$*,*

$$\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!] \leq \mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2n} \quad .$$

Proof. Follows directly from the previous lemma together with Lemma 4 and the fact that $depth(\phi) = depth(\phi_{\cdot n})$:

$$\begin{aligned}
&\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!] \\
&= \frac{1}{n}\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi\cdot n]\!] && \text{[Lemma 4]} \\
&\leq \frac{1}{n}\left(\mathcal{M}_{\mathbb{N}}[\![\phi\cdot n]\!] + \frac{depth(\phi\cdot n)}{2}\right) && \text{[Lemma 6]} \\
&= \frac{1}{n}\mathcal{M}_{\mathbb{N}}[\![\phi\cdot n]\!] + \frac{depth(\phi)}{2n} && [depth(\phi) = depth(\phi\cdot n)] \\
&= \mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2n} && \text{[Lemma 4]}
\end{aligned}$$

□

Unfortunately, the previous lemma and its corollary do only provide *upper* approximations of the real-valued time interpretation $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]$ by discrete time with arbitrary sampling rates $\mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!]$. Yet, these upper approximations are complemented by a tightness result concerning rational time:

Lemma 7. $\inf_{k\geq l, k\in\mathbb{N}} \mathcal{M}_{\frac{1}{k!}\cdot\mathbb{N}}[\![\phi]\!] \leq \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!]$ *holds for each DC formula* ϕ *and each* $l \in \mathbb{N}$.

Proof. Assume, on the contrary, that $x \stackrel{\text{def}}{=} \inf_{k\geq l, k\in\mathbb{N}} \mathcal{M}_{\frac{1}{k!}\cdot\mathbb{N}}[\![\phi]\!] > \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!]$. Then there is a rational-time observation $obs \in Obs_{\mathbb{Q}_{\geq 0}}$ with $x > \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!](obs)$. But as $obs = (tr, [a, b])$ is a rational-time observation, there is $m \in \mathbb{N}$ with $m \geq l$ such that $a, b \in \frac{1}{m}\cdot\mathbb{N}$ and tr is constant on $[\frac{i}{m}, \frac{i+1}{m})$ for each $i \in \mathbb{N}$ and that, furthermore, all chop points characterizing (i.e., yielding the suprema in) $\mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!]$ are in $\frac{1}{m}\cdot\mathbb{N}$. Therefore, $\mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!](obs_n) = \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!](obs)$ holds for all multiples n of m, where $obs_n = (tr_n, [a, b])$ is the natural restriction of obs to over-sampled discrete time obtained using the restriction tr_n of tr to domain $\frac{1}{n}\cdot\mathbb{N}$. With $n = m!$, this yields the contradiction $x > \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!](obs) = \mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!](obs_n) \geq \inf_{obs'\in Obs_{\frac{1}{n}\cdot\mathbb{N}}} \mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!](obs') = \mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!] \geq \inf_{k\geq l, k\in\mathbb{N}} \mathcal{M}_{\frac{1}{k!}\cdot\mathbb{N}}[\![\phi]\!] = x$. Consequently, the assumption that $\inf_{k\geq l, k\in\mathbb{N}} \mathcal{M}_{\frac{1}{k!}\cdot\mathbb{N}}[\![\phi]\!] > \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!]$ must be wrong, which proves $\inf_{k\geq l, k\in\mathbb{N}} \mathcal{M}_{\frac{1}{k!}\cdot\mathbb{N}}[\![\phi]\!] \leq \mathcal{M}_{\mathbb{Q}_{\geq 0}}[\![\phi]\!]$. □

However, using Lemma 5, this tightness result carries over to real-valued time:

Corollary 2 (Asymptotic tightness of disc.-time approx.).
$\inf_{k\geq l, k\in\mathbb{N}} \mathcal{M}_{\frac{1}{k!}\cdot\mathbb{N}}[\![\phi]\!] \leq \mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]$ *holds for each DC formula* ϕ *and each* $l \in \mathbb{N}$.

5.3 Discrete Time with Different Sampling Rates

Given above approximation results between discrete time and real-valued time, the rate of convergence of the discrete time interpretation when using increasingly larger sampling rates becomes interesting. A close look at the proofs of Lemma 6 and Corollary 1 reveals that they carry over from real-valued time to using discrete time (with different sampling rates) on both sides. When replacing $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]$ by $\mathcal{M}_{\frac{1}{k}\cdot\mathbb{N}}[\![\phi]\!]$ for some arbitrary $k \in \mathbb{N} \setminus \{0\}$, we obtain

Lemma 8 (Approximation by sub-sampling). *Let ϕ be a DC formula and let $k \in \mathbb{N} \setminus \{0\}$. Then*

$$\mathcal{M}_{\frac{1}{k}\cdot\mathbb{N}}[\![\phi]\!] \leq \mathcal{M}_{\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2} \ .$$

Proof. Substitute $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]$ with $\mathcal{M}_{\frac{1}{k}\cdot\mathbb{N}}[\![\phi]\!]$ in the proof of Lemma 6. □

Again, we can scale this result using the linearity properties from Lemma 4, thus obtaining a discrete-time variant of Corollary 1:

Corollary 3 (Sampling-rate conversion). *For any $m, n \in \mathbb{N} \setminus \{0\}$,*

$$\mathcal{M}_{\frac{1}{mn}\cdot\mathbb{N}}[\![\phi]\!] \leq \mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!] + \frac{depth(\phi)}{2n} \ .$$

Proof. Repeat the proof of Corollary 1 with $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!]$ replaced by $\mathcal{M}_{\frac{1}{mn}\cdot\mathbb{N}}[\![\phi]\!]$ and Lemma 6 substituted with Lemma 8. □

Note that this implies that independently of the formula structure, finer sampling cannot yield arbitrary changes in the multi-valued truth value. When moving to an over-sampling, the possible increase in truth value is bounded by $\frac{depth(\phi)}{2n}$, where n is the base sampling rate. In particular, the possible increase converges against 0 for growing sampling rates.

6 Decidability

We will now turn to decidability and semi-decidability results over integer and real-valued time.

6.1 Decidability over Discrete Time

In order to obtain a decision procedure for robust validity over discrete time, we present a reduction of robust validity over discrete time to conventional validity over discrete time. A simple induction shows

Lemma 9 (Robust vs. classical satisfaction). *For each DC formula ϕ and each observation $obs \in Obs_{\mathbb{N}}$, the equivalence $\mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) > 0$ iff $obs \models_{\mathbb{N}} \phi^\circ$ holds, where ϕ° is the formula ϕ with all positive occurrences of $\int S \geq k$ replaced by $\int S > k$ and all negative occurrences of $\int S > k$ replaced by $\int S \geq k$.*

As $\mathcal{M}_{\mathbb{N}}[\![\cdot]\!]$ maps formulae to integers, a corresponding reduction of robust validity to classical validity can be derived.

Lemma 10 (Robust vs. classical validity). *For a DC formula ϕ with integer constants, $\mathcal{M}_{\mathbb{N}}[\![\phi]\!] > 0$ iff $\models_{\mathbb{N}} \phi^\circ$. I.e., ϕ is robustly valid over discrete time iff ϕ° is valid over discrete time in the classical sense.*

Proof. It follows from the definition of $\mathcal{M}_T[\![\cdot]\!]$ that $\mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) \in \mathbb{Z} \pm C$ for each $obs \in Obs_{\mathbb{N}}$, where C is the set of constants occurring in ϕ and $M \pm N = \{m + n \mid m \in M, n \in N\} \cup \{m - n \mid m \in M, n \in N\}$. Therefore,

$$\begin{aligned}
&\mathcal{M}_{\mathbb{N}}[\![\phi]\!] > 0 \\
\text{iff}\ &\inf_{tr \in Traj_{\mathbb{N}}, e \in \mathbb{N}} \mathcal{M}_{\mathbb{N}}[\![\phi]\!](tr, [0,e]) > 0 && [\text{Def. } \mathcal{M}_T[\![\phi]\!]] \\
\text{iff}\ &\forall\, tr \in Traj_{\mathbb{N}}, e \in \mathbb{N}\,.\ \big(\mathcal{M}_{\mathbb{N}}[\![\phi]\!](tr, [0,e]) > 0\big) \\
& && [\mathcal{M}_{\mathbb{N}}[\![\phi]\!](obs) \in \mathbb{Z} \pm C, \text{ which has no accumulation point}] \\
\text{iff}\ &\forall\, tr \in Traj_{\mathbb{N}}, e \in \mathbb{N}\,.\ \big((tr, [0,e]) \models_{\mathbb{N}} \phi^\circ\big) && [\text{Lemma 9}] \\
\text{iff}\ &\models_{\mathbb{N}} \phi^\circ && [\text{Def. of classical validity}]
\end{aligned}$$

□

Thus, robust validity of ϕ over discrete time can be reduced to classical validity of ϕ° over discrete time.

Theorem 2 (Decidability of robust validity over discrete time). *It is decidable whether a DC formula ϕ with integer constants is robustly valid over discrete time.*

Proof. According to Lemma 10 it suffices to decide classical validity of ϕ° instead. This problem is known to be decidable via a reduction to an emptiness problem of extended regular expressions; see [7] for details. [3] □

6.2 Semi-Decidability Over Dense Time

Using the approximation scheme between discrete and dense time exposed in Section 5, above discrete-time decidability result does immediately generalize to a dense-time semi-decision procedure:

Theorem 3 (Semi-decidab. of dense time rob. invalidity). *If ϕ contains rational constants only then it is semi-decidable whether $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!] < 0$, i.e. whether ϕ is* robustly *invalid over real-valued time.*

Proof. W.l.o.g. we may assume that ϕ contains integer constants only[4] such that $\mathcal{M}_{\mathbb{N}}[\![\phi_{\cdot n}]\!] \in \mathbb{Z}$ for each $n \in \mathbb{N}$. According to Corollaries 1 and 2, inequation $\mathcal{M}_{\mathbb{R}_{\geq 0}}[\![\phi]\!] < 0$ holds iff $\mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!] < -\frac{depth(\phi)}{2n}$ for some $n \in \mathbb{N} \setminus \{0\}$. However,

$$\begin{aligned}
&\mathcal{M}_{\frac{1}{n}\cdot\mathbb{N}}[\![\phi]\!] < -\frac{depth(\phi)}{2n} \\
\text{iff}\ &\mathcal{M}_{\mathbb{N}}[\![\phi_{\cdot n}]\!] < -\frac{depth(\phi)}{2} && [\text{Lemma 4}]
\end{aligned}$$

[3] Strictly speaking, we need to extend the procedure from reference [7] to handle arbitrary integer constants in duration inequations $\int S \sim k$, as [7] deals with non-negative constants only. However, given that durations $\int S$ can only yield non-negative values, this extension is straightforward: validity of an arbitrary formula ϕ is equivalent to validity of its variant $\phi_{\mathbb{N}}$, where $\phi_{\mathbb{N}}$ is derived from ϕ by replacing each occurrence of $\int S \geq k$ or $\int S > k$ with $k < 0$ by $\int S \geq 0$.

[4] If ϕ contains non-integer rational constants then we can use $\phi_{\cdot d}$, with d being a common denominator of all constants in ϕ, instead. According to Lemma 4, the formulae ϕ and $\phi_{\cdot d}$ are equivalent wrt. robust validity over dense time.

iff $\mathcal{M}_{\mathbb{N}}[\![\phi{\cdot}n]\!] + 1 \leq -\left\lfloor \frac{depth(\phi)}{2} \right\rfloor$ [$\mathcal{M}_{\mathbb{N}}[\![\phi{\cdot}n]\!] \in \mathbb{Z}$]

iff $\mathcal{M}_{\mathbb{N}}[\![(\phi{\cdot}n)_{+\left(1+\left\lfloor \frac{depth(\phi)}{2} \right\rfloor\right)}]\!] \leq 0$ [Lemma 4]

iff $(\phi{\cdot}n)_{+\left(1+\left\lfloor \frac{depth(\phi)}{2} \right\rfloor\right)}$ is not robustly valid over discrete time.

[Def. of robust validity]

The latter is decidable according to Theorem 2. Hence, in order to semi-decide whether ϕ is robustly invalid over real-valued time, it suffices to decide robust validity of $(\phi{\cdot}n)_{+\left(1+\left\lfloor \frac{depth(\phi)}{2} \right\rfloor\right)}$ over discrete time for successively larger $n \in \mathbb{N}\backslash\{0\}$ until an invalid instance is found. □

7 Discussion

We have developed the concept of robust interpretation for the interval temporal logic Duration Calculus, and we have shown an equivalence result relating robust interpretation to a multi-valued semantics, where real numbers is used as semantic domain and Lipschitz continuous functions are associated with the operators of Duration Calculus.

The multi-valued semantics provides insight concerning robustness of the formula, as the meaning of a formula describes how much the constants in the formula may be varied without changing the truth value of the formula. Furthermore, this semantics was shown to provide a nice framework for studying the relationship between different time domains.

Based on the multi-valued semantics, we have studied how a real-time semantics of Duration Calculus can be approximated by a discrete-time semantics. This extends dicrete-time approximation, as suggested by Chakravorty and Pandya [2], to an interval-based temporal logic featuring accumulated durations. In our setting, an asymptotically tight upper-bound approximation constitutes the basis for a semi-decision procedure. A similar lower-bound approximation would give a decidability result. Unfortunately we do not have a corresponding lower-bound approximation result yet, although it is likely that such do at least hold for those fragments of Duration Calculus, where chop is confined to occur in only one polarity (i.e., either in only positive or in only negative contexts).

Acknowledgements. The authors would like to thank Stefan Ratschan for his detailed comments on an earlier draft of this paper. Work of the first author was partly supported by the German Research Council (DFG) as part of the Transregional Collaborative Research Center "Automatic Verification and Analysis of Complex Systems" (SFB/TR 14 AVACS, `www.avacs.org`).

References

1. Eugene Asarin and Ahmed Bouajjani. Perturbed turing machines and hybrid systems. In *Proceedings of the Sixteenth Annual IEEE Symposium on Logic in Computer Science (LICS 2001)*. IEEE, 2001.

2. G. Chakravorty and P. K. Pandya. Digitizing Interval Duration Logic. In *Proceedings of CAV 2003*, LNCS 2725, pages 167–179, Springer-Verlag 2003.
3. Martin Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In Jörg Flum and Mario Rodríguez-Artalejo, editors, *Computer Science Logic (CSL'99)*, LNCS 1683, pages 126–140. Springer-Verlag, 1999.
4. Martin Fränzle. What will be eventually true of polynomial hybrid automata. In Naoki Kobayashi and Benjamin C. Pierce, editors, *Theoretical Aspects of Computer Software (TACS 2001)*, LNCS 2215, pages 340–359. Springer-Verlag, 2001.
5. Martin Fränzle and Michael R. Hansen. A Robust Interpretation of Duration Calculus (Extended abstract). In Paul Pettersson and Wang Yi, editors, *Nordic Workshop on Programming Theory*, Technical report 2004-041, Department of Information Technology, Uppsala University, pages 83–85, 2004.
6. Vineet Gupta, Thomas A. Henzinger, and Radha Jagadeesan. Robust timed automata. In Oded Maler, editor, *Proceedings of the First International Workshop on Hybrid and Real-Time Systems (HART 97)*, LNCS 1201, pages 331–345. Springer-Verlag, 1997.
7. Michael R. Hansen. Model-checking discrete duration calculus. *Formal Aspects of Computing*, 6(6A):826–845, 1994.
8. Anuj Puri. Dynamical properties of timed automata. In Ravn and Rischel [12], pages 210–227.
9. Stefan Ratschan. Continuous first-order constraint satisfaction. In J. Calmet, B. Benhamou, O. Caprotti, L. Henocque, and V. Sorge, editors, *Artificial Intelligence, Automated Reasoning, and Symbolic Computation*, LNCS 2385, pages 181–195. Springer, 2002.
10. Stefan Ratschan. Quantified constraints under perturbations. *Journal of Symbolic Computation*, 33(4):493–505, 2002.
11. Stefan Ratschan. Search heuristics for box decomposition methods. *Journal of Global Optimization*, 24(1):51–60, 2002.
12. A. P. Ravn and H. Rischel, editors. *Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT'98)*, LNCS 1486, Springer-Verlag, 1998.
13. Anders P. Ravn, Hans Rischel, and Kirsten M. Hansen. Specifying and verifying requirements of real-time systems. *IEEE Transactions on Software Engineering*, 19(1):41–55, January 1993.
14. Alfred Tarski. A decision method for elementary algebra and geometry. RAND Corporation, Santa Monica, Calif., 1948.
15. Zhou Chaochen and Michael R. Hansen. *Duration Calculus — A Formal Approach to Real-Time Systems.* EATCS monographs on theoretical computer science. Springer-Verlag, 2004.
16. Zhou Chaochen, Michael R. Hansen, and Peter Sestoft. Decidability and undecidability results for duration calculus. In P. Enjalbert, A. Finkel, and K. W. Wagner, editors, *Symposium on Theoretical Aspects of Computer Science (STACS 93)*, LNCS 665, pages 58–68. Springer-Verlag, 1993.
17. Zhou Chaochen, C. A. R. Hoare, and Anders P. Ravn. A calculus of durations. *Information Processing Letters*, 40(5):269–276, 1991.