

Article

A Truly Robust Signal Temporal Logic: Monitoring Safety Properties of Interacting Cyber-Physical Systems under Uncertain Observation

Bernd Finkbeiner ¹ , Martin Fränzle ^{2,*} , Florian Kohn ¹  and Paul Kröger ²

- ¹ CISPA Helmholtz Center for Information Security, Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany; finkbeiner@cispa.de (B.F.); florian.kohn@cispa.de (F.K.)
- ² Department of Computing Science, Carl von Ossietzky Universität, Ammerländer Heerstraße 114-118, 26129 Oldenburg, Germany; paul.kroeger@uni-oldenburg.de
- * Correspondence: martin.fraenzle@uol.de; Tel.: +49-441-9722-500

Abstract: Signal Temporal Logic is a linear-time temporal logic designed for classifying the time-dependent signals originating from continuous-state or hybrid-state dynamical systems according to formal specifications. It has been conceived as a tool for systematizing the monitoring of cyber-physical systems, supporting the automatic translation of complex safety specifications into monitoring algorithms, faithfully representing their semantics. Almost all algorithms hitherto suggested do, however, assume perfect identity between the sensor readings, informing the monitor about the system state and the actual ground truth. Only recently have Visconti et al. addressed the issue of inexact measurements, taking up the simple model of interval-bounded per-sample error that is unrelated, in the sense of chosen afresh, across samples. We expand their analysis by decomposing the error into an unknown yet fixed offset and an independent per-sample error and show that in this setting, monitoring of temporal properties no longer coincides with collecting Boolean combinations of state predicates evaluated in each time instant over best-possible per-sample state estimates, but can be genuinely more informative in that it infers determinate truth values for monitoring conditions that interval-based evaluation remains inconclusive about. For the model-free as well as for the linear model-based case, we provide optimal evaluation algorithms based on affine arithmetic and SAT modulo theory, solving over linear arithmetic. The resulting algorithms provide conclusive monitoring verdicts in many cases where state estimations inherently remain inconclusive. In their model-based variants, they can simultaneously address the issues of uncertain sensing and partial observation.

Keywords: signal temporal logic; online monitoring; uncertain information; partial observation



Citation: Finkbeiner, B.; Fränzle, M.; Kohn, F.; Kröger, P. A Truly Robust Signal Temporal Logic: Monitoring Safety Properties of Interacting Cyber-Physical Systems under Uncertain Observation. *Algorithms* **2022**, *15*, 126. <https://doi.org/10.3390/a15040126>

Academic Editors: Andreas Rauh, Luc Jaulin and Julien Alexandre dit Sandretto

Received: 15 March 2022

Accepted: 9 April 2022

Published: 11 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Precise and automatic monitoring of the satisfaction of safety constraints imposed on cyber-physical systems is of utmost importance in a variety of settings: traditionally, it facilitates offline or, if supported by the monitoring algorithm, online system debugging as well as, if pursued online in real-time, the demand-driven activation of safety and fallback mechanisms in safety-oriented architectures as soon as a safety-critical system leaves its operational domain or exposes unexpected behavior. An application domain of growing importance is the safety assurance of autonomous systems, such as unmanned aircraft. Such systems are increasingly equipped with decision-making components that carry out complex missions in areas such as transport, mapping and surveillance, and agriculture. In such applications the monitor plays a critical role in assessing system health conditions (such as sensor cross-validation) and regulatory constraints like geo-fencing, which prevents the aircraft from entering protected airspace [1]. More recently, continuous diagnosis in continuous agile development processes like DevOps has caught interest

and provides a further field of application [2]. Of special interest here is the provisioning of flexible languages for the specification of monitors, as the pertinent safety constraints vary tremendously across systems and application domains. Answering this quest, Signal Temporal Logic (STL) [3] and similar linear-time temporal logics have been designed for classifying the time-dependent signals originating from continuous-state or hybrid-state dynamical systems according to formal specifications, alongside efficient stream processing languages targeted towards online monitoring [1]. These highly expressive specification languages do, however, induce the follow-up quest for efficient automatic implementation of monitoring algorithms by means of translation from the formal safety or monitoring specifications.

There consequently is a rich body of work on synthesis of monitors from logical specifications of temporal or spatio-temporal type (cf. [4] for an overview), with nowadays even robust industrial tools being available [5], as well as hard real-time capable stream-based execution mechanisms for on-line monitoring of even more expressive monitoring languages [1]. Most of the suggested algorithms do, however, not address the problem of epistemic uncertainty due to environmental sensing, with the monitoring algorithms rather taking sensor values and timestamps as is and ignoring their inherent imprecision. Such imprecisions are unavoidable in applications such as autonomous aircraft due to wind and other external influences. A notable exception is provided by robust quantitative interpretations of temporal logic, which can cope with inaccuracy in timestamps [6] as well as in sensor values [7]. The corresponding robust monitoring approaches [8] support a metric, yet not stochastic, error model, and consequently ignore the fact that repeated measurements provide additional evidence, thus ignoring the wisdom and toolset from metrology concerning state estimation [9,10], consequently providing extremely pessimistic verdicts [11]. Overcoming the latter problem would require equipping the pertinent logics, like Signal Temporal Logic [7], with a truly stochastic (i.e., reporting a likelihood of satisfaction over a stochastic model) rather than a trace-based metric semantics (reporting slackness of the signal values observed across a single trace towards change of truth value of the formula). This remains the subject of our further research.

In this article, we do nevertheless show that already in a metric setting of interval-bounded measurement error, as employed in [12], refined algorithms addressing the relation between successive measurements are possible. Visconti et al. [12] have previously addressed the issue of inexact measurements metrically, taking up the simple model of interval-bounded independent per-sample error which is unrelated across samples in the sense of chosen afresh upon every sample. We expand their analysis by decomposing the error into an unknown yet fixed offset and an independent per-sample error and show that in this setting, monitoring of temporal properties no longer coincides with collecting Boolean combinations of predicates evaluated pointwise over best-possible per-sample state estimates, but can be genuinely more informative in that it infers determinate truth values for monitoring conditions that interval-based evaluation remains inconclusive about. For the model-free as well as for the (certain or uncertain) linear model-based case, we provide optimal evaluation algorithms based on affine arithmetic [13] and SAT modulo theory solving over linear arithmetic [14,15]. Beyond uncertain sensing, we also address the issues of partial observation (w.r.t. both state variables and time instants) in uncertain linear systems. In all these cases, the reductions to proof obligations in affine arithmetic provide conclusive monitoring verdicts in many cases where interval-valued state estimations and subsequent interval-based evaluation of temporal monitoring properties inherently remains inconclusive, which we demonstrate by means of examples. We furthermore prove that our affine-arithmetic reductions are optimal in that they are as precise as a monitor operating under metric uncertainty can possibly be: they do not only provide sound verdicts throughout, but are also optimally informed in that they always yield a conclusive verdict whenever this is justified by the formula semantics. Any reduction to even richer extensions of interval arithmetic, like [16], would consequently fail to provide additional gains in precision.

To achieve these results, we first in Section 2 review the definition of Signal Temporal Logic [7], which we use as the formalism of choice for illustration. We then provide the metric error model for measurements (Section 3) and based on it define the monitoring problem under metric uncertainty (Section 4) including rigorous criteria for soundness, completeness, and precision of monitoring algorithms. The subsequent two sections develop optimal monitoring algorithms based on reductions to affine arithmetic, where Section 5 covers the model-free case and Section 6 treats optimal monitoring when a (potentially uncertain) affine model of system dynamics is given. Both sections provide illustrative examples of the constructions. Section 7, finally, investigates the worst-case complexity of the monitoring problem under uncertainty.

2. Signal Temporal Logic

Signal temporal logic (STL) [3] is a linear-time temporal logic designed as a formal specification language for classifying the time-dependent signals originating from continuous-state or hybrid-state dynamical systems. Its development has been motivated by a need for a flexible yet rigorous language systematising the monitoring of cyber-physical systems. Especially relevant to such monitoring applications is the bounded-time fragment of STL defined as follows.

Definition 1. *Formulae ϕ of bounded-time STL are defined by the Backus-Naur form*

$$\begin{aligned} \phi & := \top \mid g \geq c \mid \neg\phi \mid \phi \vee \phi \mid \phi \mathbf{U}_{[t,t']}\phi \\ g & := cx \mid cx + g \\ c & \in \mathbb{Q} \\ x & \in \text{Var} \\ t & \in \mathbb{N} \end{aligned}$$

where *Var* is a predefined set of signal names. We demand that $t \leq t'$ in $\mathbf{U}_{[t,t']}\phi$.

The constant \perp , further Boolean connectives like \wedge or \Rightarrow , and further modalities $\mathbf{F}_{[t,t']}\phi$ or $\mathbf{G}_{[t,t']}\phi$ can be defined as usual: for example, $\mathbf{F}_{[t,t']}\phi$ is an abbreviation for $\top \mathbf{U}_{[t,t']}\phi$ and $\mathbf{G}_{\leq t}\phi$ is an abbreviation for $\phi \mathbf{U}_{[t+1,t+1]}\top$ given the discrete nature of the time model.

Note that the above definition confines state expressions g to be linear combinations of signals, in contrast to the standard definition [3] of STL, which permits more general state expressions. The reason for adopting this restriction is that it permits exact results in monitoring, whereas more general state expressions can well be treated in our framework by exploiting standard affine-arithmetic approximations [13], yet completeness would be lost due to overapproximations induced by a strife for soundness.

For the same reasons, we adopt a discrete-time semantics, as issues of continuous interpolation between time instants of measurements have been addressed before in [17]. Adopting those mechanisms, continuous-time dynamic systems and continuous-time interpretation of STL can be treated as well, yet would again resort to affine approximations at the price of sacrificing exactness of the monitoring algorithm.

The semantics of STL builds on the notion of a trajectory:

Definition 2. *A state valuation σ is a mapping of signal names $x \in \text{Var}$ to real values, i.e., a function $\sigma : \text{Var} \rightarrow \mathbb{R}$. The set of all state valuations is denoted by Σ . A (discrete time) trajectory $\tau : \mathbb{N} \rightarrow \Sigma$ is a mapping from time instants, where time is identified with the natural numbers \mathbb{N} , to state valuations.*

Satisfaction of an STL formula ϕ by a (discrete-time) trajectory τ at time instant $t \in \mathbb{N}$, denoted as $\tau, t \models \phi$, is defined recursively as

$$\begin{aligned}
 \tau, t \models \top & \quad \text{holds,} \\
 \tau, t \models g \geq c & \quad \text{iff } G(\tau(t)) \geq c, \text{ where } G \text{ is the linear function defined by expression } g, \\
 \tau, t \models \neg\phi & \quad \text{iff } \tau, t \not\models \phi, \\
 \tau, t \models \phi \vee \psi & \quad \text{iff } \tau, t \models \phi \text{ or } \tau, t \models \psi, \\
 \tau, t \models \phi \mathbf{U}_{[t_1, t_2]} \psi & \quad \text{iff } \exists k \in \{t + t_1, \dots, t + t_2\} : (\tau, k \models \psi) \wedge \forall l \in \{t, \dots, k - 1\} : (\tau, l \models \phi).
 \end{aligned}$$

Note that the truth value of an STL formula ϕ over a trajectory τ at time t thus can be decided at time $t + \text{duration}(\phi)$ if the values $\tau(k)(x)$ are known for all time instants $k \in \{t, \dots, t + \text{duration}(\phi)\}$ and all variable names x occurring in ϕ , where $\text{duration}(\phi)$ is defined as follows:

$$\begin{aligned}
 \text{duration}(\top) & = 0, \\
 \text{duration}(g \geq c) & = 0, \\
 \text{duration}(\neg\phi) & = \text{duration}(\phi), \\
 \text{duration}(\phi \vee \psi) & = \max(\text{duration}(\phi), \text{duration}(\psi)), \\
 \text{duration}(\phi \mathbf{U}_{[t_1, t_2]} \psi) & = \max(t_2 - 1 + \text{duration}(\phi), t_2 + \text{duration}(\psi)).
 \end{aligned}$$

Unfortunately, the ground-truth values of $\tau(k)(x)$ are frequently not directly accessible and have to be retrieved via environmental sensing, which is bound to be inexact due to measurement error and partial due to economic and physical constraints on sensor deployment and capabilities. Inaccessibility of the ground truth renders direct decision of STL properties based on the above semantics elusive; we rather need to infer, as far as this is possible, the truth value of an STL monitoring condition ϕ from the vague evidence provided by mostly partial and inexact sensing.

3. Imperfect Information Due to Noisy Sensing

The simplest metric model of measurement error is obtained by assuming the error to be interval-bounded and independent across sensors as well as across time instants of measurements, thus pretending that the error incurred when measuring the same physical quantity by the same sensor at different times is uncorrelated. Sensor-based monitoring under such a model of measurement uncertainty can be realized by an appropriate interval lifting of the STL semantics [12], as standard interval arithmetic (IA) [18] underlying this lifting reflects an analogous independence assumption.

This independence assumption, however, is famously known as the dependency (or alias) problem of interval arithmetic in cases where the independence assumption does not actually apply and IA consequently yields an overly conservative approximation instead [18]. Such overapproximation will obviously also arise when the interval-based monitoring algorithm [12] is applied in cases where the per-sample error of multiple measurements is not fully independent; the overapproximation then shows by reporting inconclusive monitoring verdicts (due to the interval embedding encoded as the inconclusive truth value interval $\{\perp, \top\}$) rather than a conclusive truth value

Dependencies between per-sample measurement errors are, however, the rule and not the exception. As a typical example take the usual decomposition of measurement error into a confounding unknown yet fixed sensor offset that remains constant across successive measurements taken by the same sensor, and a random measurement error that varies uncorrelated between samples at different time instants. The upper bounds of these two values refer directly to the two terms “trueness” and “precision” used by the pertinent ISO norm 5725 to describe the accuracy of a measurement method. They are consequently found routinely in data sheets of sensor devices, which we consider to be the contracts between component (i.e., sensor) manufacturer and component user (i.e., the monitor designer) in the sense of contract-based design [19], implying that all subsequent logical inferences we pursue are relative to satisfaction of the contract by the actual sensor. Within the ISO parlance, precision identifies the grouping or closeness of multiple readings,

i.e., the portion of the total error that varies in an unpredictable way between tests or measurements. In contrast, trueness indicates the closeness of the average test results to a reference or true value in the sense of the deviation or offset of the arithmetic mean of a large number of repeated measurements and the true or accepted reference value.

Definition 3. Let S be a sensor observing a signal $\sigma \in Var$ at times $T \subseteq \mathbb{N}$ with a maximal sensor offset of $\varepsilon \geq 0$ and a maximal random measurement error of $\delta \geq 0$. Let τ be a (ground-truth) trajectory. Then $m_S : T \rightarrow \mathbb{R}$ is a possible S time series over τ iff

$$\exists o \in [-\varepsilon, \varepsilon] : \forall t \in T : \exists e \in [-\delta, \delta] : \tau(\sigma)(t) + o + e = m_S(t). \tag{1}$$

If m_S is an S time series over τ , then we symmetrically say that the trajectory τ is consistent with m_S and denote this fact by $m_S \vdash \tau$. This notion immediately extends to simultaneous consistency with a set of time series $m_{S_1}, m_{S_2}, \dots, m_{S_n}$: we denote the fact that trajectory τ satisfies $m_{S_i} \vdash \tau$ for each $i \in \{1, \dots, n\}$ by $m_{S_1}, \dots, m_{S_n} \vdash \tau$.

Note that the above definition features two additive offsets affecting measurements, the first of which (namely the sensor offset) is uniformly chosen for the whole time series while the second one (the random noise) is chosen independently upon every sample. These errors are absolute in that their magnitude does not depend on the magnitude of the ground truth value, which is a standard model of measurement errors appropriate for many simple sensor designs. In specific settings, e.g., when the dynamic range of a sensor is extended by variable-gain pre-amplification as usual in seismology [20] or by regulating light flow to optical sensors via an automatically controlled optical aperture, relative error or similar error models may be more appropriate. These can be formulated analogously. For the combination of an absolute offset and a relative per-sample error, e.g., the characteristic Equation (1) would have to be replaced by

$$\exists o \in [-\varepsilon, \varepsilon] : \forall t \in T : \exists e \in \left[(1 + \delta)^{-1}, 1 + \delta \right] : \tau(\sigma)(t) \cdot e + o = m_S(t). \tag{2}$$

4. The Monitoring Problem

Assume that we want to continuously monitor truth of a safety requirement ϕ stated as a bounded-time STL formula. In reality, we can only do so based on a set m_{S_1} to m_{S_n} of time series of measurements obtained through different sensors S_1 to S_n . Each of these sensors is inexact, none can predict the future, and even together they provide only partial introspection into the set Var of signals generated by the system under monitoring. The problem at hand is to, at any time $t \in \mathbb{N}$, generate as precise as possible verdicts about the truth of the monitoring condition ϕ at time $t - \text{duration}(\phi)$ given the imprecise measurements provided by the sensor array S_1 to S_n up to time t .

Doing so requires identifying the full set of ground-truth signals possible given a set of inexact measurements. This, however, coincides with the notion of consistency stated in Definition 3.

Definition 4. Let S_1 to S_n be a set of sensors, each qualified by an individual maximum sensor offset ε_{S_i} and an individual maximum random error δ_{S_i} , which observe (not necessarily different) signals $\sigma_{S_i} \in Var$ at (potentially diverse) time instants $T_{S_i} \subseteq \mathbb{N}$. Let $t \in \mathbb{N}$ be the current time and $m_{S_i} : T_{S_i} \cap \mathbb{N}_{\leq t} \rightarrow \mathbb{R}$ be the time series representing measurements obtained by the different sensors S_i up to time t .

The possible ground truth associated to the time series m_{S_1} to m_{S_n} is the set of all trajectories τ satisfying $m_{S_1}, \dots, m_{S_n} \vdash \tau$, i.e., being consistent with all available measurements simultaneously. We signify the set of all possible ground truth trajectories corresponding to a set of measurements m_{S_1}, \dots, m_{S_n} by

$$GT(m_{S_1}, \dots, m_{S_n}) = \{ \tau : \mathbb{N} \rightarrow \Sigma \mid m_{S_1}, \dots, m_{S_n} \vdash \tau \}.$$

The monitoring problem now is to characterize the possible ground truth exactly and to determine the possible truth values of the monitoring condition ϕ across the possible ground truth:

Definition 5. Let ϕ be a bounded-time STL formula according to the syntax from Definition 1, $t \in \mathbb{N}$ be the current time, and $m_{S_i} : T_{S_i} \cap \mathbb{N}_{\leq t} \rightarrow \mathbb{R}$, for S_1 to S_n , be time series representing measurements obtained by the different sensors S_i up to time t .

Let M be an algorithm taking as arguments a current time t , a vector of time series $m_{S_i} : T_{S_i} \cap \mathbb{N}_{\leq t} \rightarrow \mathbb{R}$ and computing a verdict in $\mathbb{B}^+ = \mathbb{B} \cup \{\text{inconclusive}\}$. In the sequel, we denote termination of M with verdict x by $M(t, m_{S_1}, \dots, m_{S_n}) = x$.

We say that M is sound iff

(a) $M(t, m_{S_1}, \dots, m_{S_n}) = \top$ implies that $\forall \tau \in GT(m_{S_1}, \dots, m_{S_n}) : \tau, t - \text{duration}(\phi) \models \phi$ and

(b) $M(t, m_{S_1}, \dots, m_{S_n}) = \perp$ implies that $\forall \tau \in GT(m_{S_1}, \dots, m_{S_n}) : \tau, t - \text{duration}(\phi) \models \neg\phi$ holds for all t and m_{S_i} .

M is complete iff M terminates on all t and m_{S_i} .

M is conclusive iff

(c) $M(t, m_{S_1}, \dots, m_{S_n}) = \text{inconclusive}$ implies that $\exists \tau, \tau' \in GT(m_{S_1}, \dots, m_{S_n}) : \tau, t - \text{duration}(\phi) \models \phi \wedge \tau', t - \text{duration}(\phi) \models \neg\phi$

holds for all t and m_{S_i} .

We call M exact iff M is sound, conclusive, and complete.

A sound monitor thus provides correct verdicts only, but may refuse decisive verdicts by non-termination or by reporting inconclusive. A complete monitor always provides some verdict, including inconclusive. A sound and complete monitor may thus still be uninformative by delivering sound but vacuous inconclusive verdicts. A conclusive monitor, in contrast, reports inconclusive only when the evidence provided by the uncertain sensors factually is too weak to determine an actual truth value. An exact monitor, consequently, always provides an as precise verdict as possible.

When striving for such an exact monitoring algorithm, the problem is that the set $GT(m_{S_1}, \dots, m_{S_n})$ of ground-truth trajectories corresponding to a given time series of measurements is uncountable in general, namely as soon as $\varepsilon > 0$ or $\delta > 0$, i.e., whenever measurements are imprecise. An enumeration of $GT(m_{S_1}, \dots, m_{S_n})$, and thereby a straightforward lifting of the standard monitoring algorithms is impossible. Any algorithmic approach to STL monitoring under imprecise observation consequently has to resort to a non-trivial finite computational representation of $GT(m_{S_1}, \dots, m_{S_n})$, which is the issue of the next two sections.

5. Exact Monitoring under Imperfect Information: The Model-Free Case

As a motivating example consider the time series of inexact measurements depicted in Figure 1, where

- t denotes time instant of the measurement (for simplicity considered to be exactly known and to coincide with the time of its associated ground truth values—both simplifications can be relaxed),
- x is the unknown ground-truth value of the physical quantity x under observation,
- black dots denote inexact measurements m_i taken at time instances $i = 1 \dots 14$,
- perpendicular intervals attached to measurements indicate error margins: measurements may deviate by ± 1 from ground truth; ± 0.5 thereof can be attributed to an unknown constant sensor offset, leaving another ± 0.5 to random measurement noise,
- the red areas, corresponding to the state predicate $x < 2 \vee x > 5$, indicate critical values for x , e.g., a geo-fencing condition not to be violated,

- the monitoring condition $\phi = \mathbf{G}_{\leq 12}(x \geq 2 \wedge x \leq 5)$ is to be decided at time $t = 13$ for time $t' = t - \text{duration}(\phi) = t - 12 = 1$, i.e., whether $x \in [2, 5]$, avoiding the red range, holds throughout the depicted time interval I .

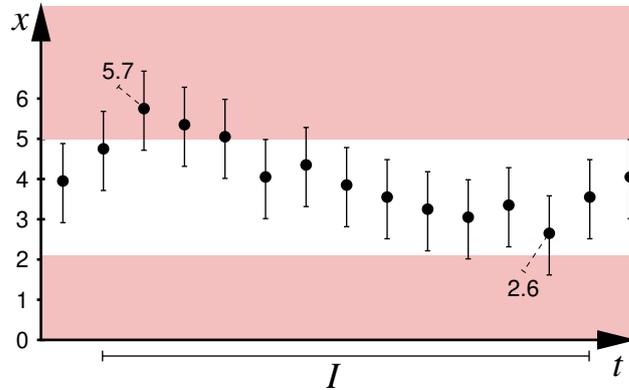


Figure 1. Model-free monitoring of temporal conditions under metric interval-type uncertainty.

The uncertainty intervals depicted are tight insofar that, first, their width is ± 1 and thus coincides with the sum of the two errors sensor offset and random noise and, second, that in the absence of any known model of the system dynamics, no reach-set propagation across time instances is possible. Evaluation of ϕ based on interval arithmetic [12] therefore remains inconclusive, given that some uncertainty intervals (namely the ones at times $t = 3$ and $t = 12$) overlap with the red areas, yet none falls completely into this forbidden range. As the intervals depicted represent the sharpest possible state estimates w.r.t. the metric error model discussed here, monitoring approaches based on first applying best-possible state estimation and subsequently evaluation of the monitoring condition are equally prone to remaining inconclusive.

Using affine arithmetic [13] and SAT modulo theory solving over linear arithmetic (SMT-LA) [14], we will, however, be able to decide that ϕ is violated at time $t' = 1$. The core argument in the detailed, general construction to follow is that we can represent the possible ground truth values $x_i = \tau(i)(x)$ relating to the measurements m_i as $x_i + o + e_i = m_i$ with $o \in [-0.5, 0.5]$ representing the unknown, yet bounded sensor offset and $e_i \in [-0.5, 0.5]$ for $i = 1 \dots 13$ representing per-sample independent error. Now observe that $m_3 = 5.7 \wedge m_{12} = 2.6 \wedge x_3 + o + e_3 = m_3 \wedge x_{12} + o + e_{12} = m_{12} \wedge o, e_3, e_{12} \in [-0.5, 0.5] \wedge x_3, x_{12} \in [2, 5]$ is unsatisfiable. The latter can be decided with SMT-LA solving. The unsatisfiability proves that at least one of x_3, x_{12} definitely falls into the red range due to the dependence introduced by the sensor offset.

For the full construction let us assume that

1. ϕ mentions the state variables $V \subset \text{Var}$;
2. for each $v \in V$ we are having a sensor with maximal offset $\epsilon_v \geq 0$ and maximum random per-sample error $\delta_v \geq 0$; (We will later relax the assumption that all variables in ϕ be directly observable through a sensor. To be meaningful, such partial observation does, however, require a system model permitting to infer information over unobservable variables, which is subject of the next section.)
3. that these sensors have provided measurements $m_v(i)$ for each variable $v \in V$ and each time instant $i \in \{t - \text{duration}(\phi), \dots, t\}$. (We will likewise relax the assumption that each time point be observed by the sensors in the section to follow.)

We then build a linear constraint system, i.e., a Boolean combination of linear constraints as follows:

1. For each $v \in V$ and each $i \in \{t - \text{duration}(\phi), \dots, t\}$, we declare a constant

$$m_v_i = m_v(i).$$

2. For each $v \in V$, we declare a variable o_v of type real and generate the bound constraints

$$o_v \geq -\epsilon_v \wedge o_v \leq \epsilon_v$$

representing the sensor offset for measuring v .

3. For each $v \in V$ and each $i \in \{t - \text{duration}(\phi), \dots, t\}$, we declare a variable e_{v_i} of type real and generate the bound constraints

$$e_{v_i} \geq -\delta_v \wedge e_{v_i} \leq \delta_v$$

representing the per-sample independent error.

4. For each $v \in V$ and each $i \in \{t - \text{duration}(\phi), \dots, t\}$, we declare a variable v_i of type real and generate a linear constraint

$$v_i + o_v + e_{v_i} = m_{v_i}$$

representing consistency between measurements and ground truth values as stated in Definition 3.

5. Using standard constructions of SMT-based bounded model checking, we add an SMT-LA encoding for validity of ϕ at time $t' = t - \text{duration}(\phi)$ to the constraint system as follows:

- For each subformula ψ of ϕ and each time instant $k \in \{t - \text{duration}(\phi), \dots, t - \text{duration}(\psi)\}$ we add a Boolean variable ψ_k ,
- if $\psi = \top$ then we assert constraints ψ_k stating that ψ is invariantly true for each $k \in \{t - \text{duration}(\phi), \dots, t\}$,
- if $\psi = g \geq c$ then we add constraints $\psi_k \Leftrightarrow g[\vec{v}_k/\vec{v}] \geq c$ for each $k \in \{t - \text{duration}(\phi), \dots, t\}$,
- if $\psi = \neg\psi'$ then we add $\psi_k \Leftrightarrow \neg\psi'_k$ to the constraint system for each $k \in \{t - \text{duration}(\phi), \dots, t - \text{duration}(\psi)\}$,
- if $\psi = \psi' \vee \psi''$ then we add constraints $\psi_k \Leftrightarrow (\psi'_k \vee \psi''_k)$ for each $k \in \{t - \text{duration}(\phi), \dots, t - \text{duration}(\psi)\}$,
- if $\psi = \psi' \mathbf{U}_{[t_1, t_2]} \psi''$ then we add constraints

$$\psi_k \Leftrightarrow \left(\bigwedge_{i=k}^{k+t_1-1} \psi'_i \right) \wedge \bigvee_{i=k+t_1}^{k+t_2} \left(\psi''_i \wedge \bigwedge_{j=k+t_1}^{i-1} \psi'_j \right)$$

for each $k \in \{t - \text{duration}(\phi), \dots, t - \text{duration}(\psi)\}$,

$\phi_{t'}$ consequently is the root variable representing validity of ϕ at time $t' = t - \text{duration}(\phi)$.

6. We finally add one of the two conjuncts

- (a) $\neg\phi_{t'}$ or
- (b) $\phi_{t'}$ alternatively,

where $t' = t - \text{duration}(\phi)$, to the resultant constraint system and check both variants for their satisfiability using an SMT-LA solver.

Depending on the results of the two satisfiability checks, we report

- inconclusive if both systems are found to be satisfiable,
- \top if the system (a) containing $\neg\phi_{t'}$ is unsatisfiable,
- \perp if the system (b) containing $\phi_{t'}$ is unsatisfiable,

The resulting STL monitoring algorithm is best possible in that it is sound, conclusive, and complete:

Lemma 1. *The above algorithm M constitutes an exact monitor in the sense of Definition 5.*

Proof. In order to show that M is exact, we have to prove that it is complete, conclusive, and sound.

Completeness is straightforward, as the constraint system generated in steps 1 to 6 is finite. Its generation hence terminates, as do the subsequent satisfiability checks because SMT-LA is decidable.

For soundness and conclusiveness note that the constraint system generated by steps 1 to 4 constitute a Skolemized version of the equation (1) defining consistency and that satisfiability of $\neg\phi_{t'}$ (or of $\phi_{t'}$ alternatively) corresponds to invalidity of $\forall\tau \in \text{GT}(m_{S_1}, \dots, m_{S_n}) : \tau, t' \models \phi$ (of $\forall\tau \in \text{GT}(m_{S_1}, \dots, m_{S_n}) : \tau, t' \models \neg\phi$, resp.) with $t' = t - \text{duration}(\phi)$. The subproblems decided within algorithm M thus directly match the conditions used in Definition 5 to characterize soundness and being conclusive. \square

Note that the above encoding can easily be adjusted to other metric error models beyond additive absolute error simply by changing the characteristic formula applied in step 4 and adjusting the bounds for the errors o_v and e_{v_i} accordingly. The relative per-sample error from Equation (2) would, for example, be encoded by $v_i * e_{v_i} + o_v = m_{v_i}$. The subsequent SMT solving would then, however, require a constraint solver addressing a more general fragment of arithmetic than SMT-LA due to the bilinear term $v_i * e_{v_i}$.

6. Exact Monitoring under Imperfect Information Given Uncertain Linear Dynamics

Additional inferences about the correlation between systems states at different time instants, and consequently additional evidence refining monitoring verdicts, are available when we have access to a model of system dynamics. Beyond refined arguments concerning feasible ground-truth value ranges within the error margins, such a model also allows to bridge gaps in sensor information, like time instants missing in a time series or references to unobservable signals. As a motivating example consider the time series of inexact measurements depicted in Figure 2, where

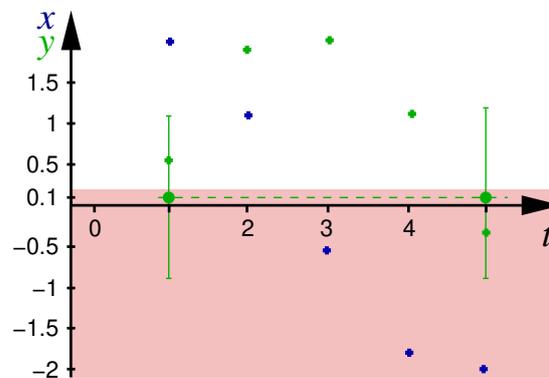


Figure 2. Model-based monitoring of temporal conditions under interval-type uncertainty and partial observation.

- t denotes time of measurement,
- x and y constitute the (mostly unobservable) systems state, which is subject to uncertain linear dynamics $x' = \frac{x}{\sqrt{2}} - \frac{y}{\sqrt{2}}$ and $y' = \frac{x}{\sqrt{2}} + \frac{y}{\sqrt{2}} \pm 0.1$,
- blue (green, resp.) crosses denote the unknown actual values of x (y , resp.) along a system evolution,
- green dots denote two inexact measurements taken on y at time instants 1 and 5, which are the only measurements available for the system,
- perpendicular intervals of width ± 1 denote the error margins of these measurements, consisting of ± 0.5 independent per-measurement error and ± 0.5 unknown constant sensor offset,
- the red area indicates critical values for y , namely $y < 0.2$,

- the monitoring condition to be decided at $t = 5$ for $t' = t - \text{duration}(\phi) = t - 4 = 1$ is $\phi = \mathbf{G}_{\leq 4}y \geq 0.2$, i.e., to decide whether the red area is avoided throughout time instants $1, \dots, 5$.

Evaluation of the monitoring condition over the uncertainty intervals remains inconclusive due to both the overlap of the given uncertainty intervals at times 1 and 5 with the red area and the lack of any information for the other times. Note that even most precise state estimation, while being able to deduce intervals for the possible ground truth values of y at time instants 2 to 4, cannot narrow down the intervals for y at time instants 1 and 5. Any monitoring approach based on a sequence of best-in-class state estimation and subsequent evaluation by a monitor thus is bound to remain inconclusive. Holistic treatment of the STL monitoring condition by affine arithmetic, however, can decide violation of the monitoring condition ϕ : the conjunction of the affine form representations of the relation between measurements and ground truth values with the equations for the system dynamics and with the monitoring condition constitutes an unsatisfiable linear constraint system (shown later in full detail).

The formal construction relies on the encoding from the previous section and conjoins it with the equations characterizing the system dynamics. It is generated as follows:

- 1–5 Identical to steps 1 to 5 from Section 5, with the slight variation that constants representing measurements (step 1), slack variables for random noise (step 3) and constraints $v_i + o_v + e_v = m_v$ encoding consistency with measurements (second half of step 4) are only generated for time instants where measurements are available.
- 6 For each $v \in V$ and each $i \in \{t - \text{duration}(\phi), \dots, t - 1\}$, declare a real variable u_v_i and generate the linear constraints

$$\begin{aligned} v_{i+1} &= c_1x_i + c_2y_i + \dots + c_nz_i + c + u_v_i \\ \wedge \quad u_v_i &\geq -\gamma \\ \wedge \quad u_v_i &\leq \gamma \end{aligned}$$

when the dynamics of v is given by the uncertain equation $v' = c_1x + c_2y + \dots + c_nz + c \pm \gamma$. The uncertain offset u_v_i can be dropped when the dynamic equation is certain.

- 7 We finally add one of the two conjuncts

- (a) $-\phi_{t'}$ or
- (b) $\phi_{t'}$ alternatively

to the resultant constraint system and check both variants for their satisfiability using an SMT-LA solver.

For the example from Figure 2, that encoding (shown in iSAT [21] syntax; a complete overview over the iSAT syntax is available from https://projects.informatik.uni-freiburg.de/attachments/download/189/isat3_manual-0.02-20140409.pdf, accessed on 14 March 2022) reads as follows for variant 7(b) (an equivalent encoding in the SMT-Lib format can be found in Appendix A):

```
DECL
-- Ground-truth state variables
float [-100,100] x1, x2, x3, x4, x5;
float [-100,100] y1, y2, y3, y4, y5;

-- Actual measurements
define my1 = 0.1;
define my5 = 0.1;

-- Uncertainties in measurements
float [-0.5,0.5] oy, ey1, ey5;
```

```

-- Uncertainties in system dynamics
float [-0.1,0.1] uy1, uy2, uy3, uy4;

-- Helper variables for BMC encoding
boole p1, p2, p3, p4, p5, q1;

define s = 0.707106781; -- 1/sqrt(2)

EXPR
-- Uncertain linear system dynamics
x2 = s*x1 - s*y1;
y2 = s*x1 + s*y1 + uy1;
x3 = s*x2 - s*y2;
y3 = s*x2 + s*y2 + uy2;
x4 = s*x3 - s*y3;
y4 = s*x3 + s*y3 + uy3;
x5 = s*x4 - s*y4;
y5 = s*x4 + s*y4 + uy4;

-- Relations between measurements and states
-- reflecting an absolute error of +/-0.5 both as offset and random
y1 + 0.5*oy + 0.5*ey1 = my1;
y5 + 0.5*oy + 0.5*ey5 = my5;

-- BMC encoding of monitoring condition
-- p_ represents satisfaction of y >= 0.2 at time instant _
p1 <-> y1 >= 0.2;
p2 <-> y2 >= 0.2;
p3 <-> y3 >= 0.2;
p4 <-> y4 >= 0.2;
p5 <-> y5 >= 0.2;

-- q_ represents validity of G <=5 p at time instant _
q1 <-> p1 and p2 and p3 and p4 and p5;

-- Goal, namely satisfaction of q at time 1
q1;

```

Note that the above encoding employs the slightly optimized BMC encoding

$$\psi_k \Leftrightarrow \bigwedge_{i=k}^{k+d} \psi'_i$$

for subformulae $\psi = \mathbf{G}_{\leq d} \psi'$ at each $k \in \{t - \text{duration}(\phi), \dots, t - \text{duration}(\psi)\}$.

The above constraint system is unsatisfiable, confirming the verdict \perp for the monitoring condition $\phi = \mathbf{G}_{\leq 4} y \geq 0.2$ at time $t' = 1$. Its unsatisfiability can automatically be decided by any satisfiability modular theory (SMT) solver addressing SMT-LA, i.e., Boolean combinations of linear inequalities. Likewise, its variant encoding the relative error model from Equation (2) can be decided by any SMT solver solving Boolean combinations of polynomial constraints. Such solvers do in general rely on solving a Boolean abstraction of the SMT formula, where all theory atoms (linear or polynomial inequalities in our case) are replaced by Boolean literals by a CDCL (conflict-driven clause learning) propositional satisfiability (SAT) solver [22,23] in order to resolve the Boolean structure. As this SAT solving incrementally instantiates the Boolean literals in the abstraction, a conjunctive constraints system in the theory underlying the SMT problem (e.g., linear arithmetic) is

incrementally built by collecting the theory constraints that have been abbreviated by the Boolean literals. These conjunctive systems of theory constraints are then solved by a subordinate theory solver, which blocks further expansion of the partial truth assignment to the literals in the Boolean abstraction when the associated theory-related constraint system becomes unsatisfiable. The reasons for unsatisfiability are usually reported back to the SAT solver in form of a corresponding conflict clause over the abstracting Boolean literals, where the conflict clause reflects a minimal (or, in cases of undecidability of high computational cost, small) infeasible core of the unsatisfiable theory constraint system. This conflict clause is added to the Boolean SAT problem and forces the SAT solver into (usually non-chronological) backtracking, thus searching for a different resolution of the Boolean structure of the SMT problem. A thorough description of the algorithmic principles underlying this so-called lazy theorem proving approach to SMT can be found in [24,25]. iSAT is an industrial-strength SMT solver that is commercially available [26] and covers a very general fragment of arithmetic, covering linear, polynomial, and transcendental functions over the integers, the mathematical reals, and (in bit-precise form) the computational floats [27].

Although iSAT [21,28,29] is by no means optimized for solving linear constraint systems—its primary field is non-linear arithmetic involving transcendental functions, the above monitoring condition can be checked in approximately 300 ms on a single core of a Core i7 10th generation running at 1.8 to 2.4 GHz. iSAT would, with essentially unaltered performance, be able to also check error models whose encoding requires non-linear arithmetic, like the mixed absolute-relative error model of Equation (2). In the above case of absolute error, we may equally well apply the dedicated SMT-LA solver MathSAT 5 [15] to the equivalent SMT-lib encoding shown in Appendix A, as only linear arithmetic is involved. The runtime then amounts to just 9.4 ms on an eight-core AMD Ryzen 7 5800X running at 4.4 GHz. As these runtimes have been observed on general-purpose SMT solvers devoid of any particular optimization for the formula structures arising in the monitoring problem, we deem online monitoring in real-time practical even for more complex (deeper nesting of sub-formulae, larger duration(ϕ)) monitoring conditions and system models (higher dimensionality especially), given the proven scalability of SMT to large-scale industrial problems.

For the above model-based monitoring procedure, akin to Lemma 1, we obtain

Lemma 2. *For systems featuring uncertain affine dynamics, the above monitoring algorithm is exact, where exactness in this setting refers to exact characterization, in the sense of Definition 5, of the truth values possible over $GT(m_{S_1}, \dots, m_{S_n}) \cap D$ with D being the set of possible trajectories of the system according to its uncertain linear dynamics.*

7. Computational Worst-Case Complexity

The aforementioned computation times indicate that the procedure is feasible in practice, notwithstanding the fact that the monitoring problem under metric uncertainty actually is NP-complete:

Lemma 3. *The model-free exact monitoring problem under imperfect information (given as interval-bounded additive absolute measurement error) is NP-complete.*

Proof. The linear reduction of the model-free monitoring problem to SMT-LA exposed in Section 5 shows that the monitoring problem is in NP, as SMT-LA is NP-complete.

NP-hardness follows from a straightforward reduction of the NP-complete problem of propositional satisfiability solving (SAT) [30] to model-free monitoring: Consider a propositional SAT formula ϕ . From ϕ derive an STL monitoring condition ϕ' by replacing each positive literal x from ϕ by $x > 0$ and each negative literal $\neg x$ by $x < 0$. Then the SAT formula ϕ is satisfiable if the monitoring verdict for the STL formula ϕ' is different from

\perp when applied to a measurement where all observed variables x obtain a measurement $m_x = 0$ under a non-zero random measurement error $\delta_v > 0$ for all $v \in \text{Var}$. \square

Remark 1. *As the above reduction of SAT only requires a positive noise margin δ_v w.r.t. random measurement error and is independent from any assumption concerning the offset ϵ_v , it applies to Visconti et al.'s noise model [12] as well. Exact monitoring for the error model from [12] consequently also is NP-complete.*

NP-completeness thus seems to be the inherent price to pay for uncertain information: bounded STL monitoring under certain observation, in contrast, is polynomial in the discrete-time case, as it only has to check an existing valuation given by the measurements for satisfaction of the (bounded) monitoring condition.

Remark 2. *The NP-completeness result for the model-free case expressed in Lemma 3 transfers to the case of model-based monitoring problem under metric imperfect information. NP-hardness can be shown by considering a discrete-time dynamical system with constant state 0 throughout within the very same SAT reduction as in the proof of Lemma 3. The reduction of the monitoring problem to SMT-LA from Section 6 again proves the linear model-based monitoring problem to be in NP.*

For linear uncertain discrete-time models, model-based monitoring under uncertainty consequently is NP-complete as well.

Note that the above NP-hardness results only apply to situations where measurements remain completely uninformative due to the measurement error, whereas more informed cases converge, depending on their level of informedness, towards checking assignments rather than finding satisfying assignments. The hardness results consequently are of limited relevance to actual applications, as these are extremely unlikely to feature an investment into completely uninformative sensor equipment.

8. Conclusions

In this article we have shown that the monitoring under uncertain environmental observation of properties expressed in linear-time temporal logic is fundamentally different from state estimation under uncertainty. While accurate state estimation followed by evaluation of the monitoring property provides a sound mechanism, this two-step algorithm may remain unnecessarily inconclusive. We have exposed two sample cases where a direct evaluation of the temporal logic property, for which we gave the formal constructions via a reduction to SAT modulo theory solving over linear arithmetic, yields definite results, whereas the two-step algorithm based on state estimation remains inconclusive. The reason is that durational properties expressed by temporal logic induce rather complex relations between successive values of signals and that these relations overlap and interfere with the cross-measurement relations induced by measurements of dynamically related variables as well as by dependencies between measurements. The single-step reduction exposed in this article encodes both the specification formula to be monitored and the error model for measurements into a common logical representation such that the interaction between these two cross-time-instant relations can be analyzed and exploited for more informed verdicts.

In the present article, we have analyzed these effects theoretically and on small, prototypic examples, within a setting of non-stochastic, metrically constrained error, where the different types of measurement error are interval-bounded. Future work will address real-life benchmark applications from the air taxi domain and extend the theory to a stochastic setting, where both measurement errors and uncertain system dynamics are described by distributions rather than metric intervals. Furthermore, we will address runtime efficiency by devising structural SMT approaches exploiting the particular problem structure rather than using problem-agnostic general purpose SMT solvers. Where this does not suffice to obtain real-time capabilities suitable for online monitoring, we will reduce computational complexity by appropriate approximation algorithms providing

real-time capabilities in settings where the exact reductions and the SAT modulo theory algorithms used herein do not feature sufficient performance.

A further issue of interest could be the handling of outliers in the measured time series, where tolerance of the monitoring verdict against $k \in \mathbb{N}$ outliers would constitute a useful relaxation of the monitoring requirement. In such a relaxation, a monitor alarm would be suppressed if, at most, k measurements can be replaced by (arbitrarily different or bounded-offset) valuations that render the monitoring condition true when combined with the ground-truth of the remaining noisy measurements. Such tolerance against a fixed number of outliers can well be encoded and solved via SMT, as has been demonstrated in [31].

Author Contributions: Conceptualization, B.F., M.F., F.K. and P.K.; Formal analysis, B.F., M.F. and P.K.; Funding acquisition, B.F. and M.F.; Investigation, M.F. and P.K.; Methodology, B.F., M.F., F.K. and P.K.; Project administration, B.F., M.F. and P.K.; Software, M.F. and F.K.; Supervision, B.F. and M.F.; Visualization, M.F.; Writing—original draft, M.F.; Writing—review & editing, B.F., M.F., F.K. and P.K. All authors have read and agreed to the published version of the manuscript.

Funding: The research herein has been supported by Deutsche Forschungsgemeinschaft under grant DFG FR 2715/5-1 “Konfliktresolution und kausale Inferenz mittels integrierter sozio-technischer Modellbildung” and as part of the Collaborative Research Center Foundations of “Perspicuous Software Systems” (TRR 248, 389792660) as well as by the State of Lower Saxony within the collaborative research scheme Zukunftslabor Mobilität.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. SMT-LIB Encoding of the Model-Based Monitoring Example

```
(set-logic QF-LRA)
(set-option :print-success false)

; Ground-truth state variables
(declare-const x1 Real)
(assert (and (<= (- 100) x1) (<= x1 100)))
(declare-const x2 Real)
(assert (and (<= (- 100) x2) (<= x2 100)))
(declare-const x3 Real)
(assert (and (<= (- 100) x3) (<= x3 100)))
(declare-const x4 Real)
(assert (and (<= (- 100) x4) (<= x4 100)))
(declare-const x5 Real)
(assert (and (<= (- 100) x5) (<= x5 100)))

(declare-const y1 Real)
(assert (and (<= -100 y1) (<= y1 100)))
(declare-const y2 Real)
(assert (and (<= -100 y2) (<= y2 100)))
(declare-const y3 Real)
(assert (and (<= -100 y3) (<= y3 100)))
(declare-const y4 Real)
(assert (and (<= -100 y4) (<= y4 100)))
(declare-const y5 Real)
(assert (and (<= -100 y5) (<= y5 100)))
```

```
; Uncertainties in measurements
(declare-const oy Real)
(assert (and (<= (- 0.5) oy) (<= oy 0.5)))
(declare-const ey1 Real)
(assert (and (<= (- 0.5) ey1) (<= ey1 0.5)))
(declare-const ey5 Real)
(assert (and (<= (- 0.5) ey5) (<= ey5 0.5)))

; Uncertainties in system dynamics
(declare-const uy1 Real)
(assert (and (<= (- 0.1) uy1) (<= uy1 0.1)))
(declare-const uy2 Real)
(assert (and (<= (- 0.1) uy2) (<= uy2 0.1)))
(declare-const uy3 Real)
(assert (and (<= (- 0.1) uy3) (<= uy3 0.1)))
(declare-const uy4 Real)
(assert (and (<= (- 0.1) uy4) (<= uy4 0.1)))

; Actual measurements
(declare-const my1 Real)
(assert (= my1 0.1))
(declare-const my5 Real)
(assert (= my5 0.1))

; Helper variables for BMC encoding
(declare-const p1 Bool)
(declare-const p2 Bool)
(declare-const p3 Bool)
(declare-const p4 Bool)
(declare-const p5 Bool)
(declare-const q1 Bool)

(declare-const s Real)
(assert (= s 0.707106781)) ; 1/sqrt(2)

; Uncertain linear system dynamics
(assert (= x2 (- (* s x1) (* s y1))))
(assert (= y2 (+ (* s x1) (* s y1) uy1)))
(assert (= x3 (- (* s x2) (* s y2))))
(assert (= y3 (+ (* s x2) (* s y2) uy2)))
(assert (= x4 (- (* s x3) (* s y3))))
(assert (= y4 (+ (* s x3) (* s y3) uy3)))
(assert (= x5 (- (* s x4) (* s y4))))
(assert (= y5 (+ (* s x4) (* s y4) uy4)))

; Relations between measurements and states
; reflecting an absolute error of +/-0.5 both as offset and random
(assert (= (+ y1 (* 0.5 oy) (* 0.5 ey1)) my1))
(assert (= (+ y5 (* 0.5 oy) (* 0.5 ey5)) my5))

; BMC encoding of monitoring condition
; p_ represents satisfaction of y >= 0.2 at time instant _
(assert (= p1 (>= y1 0.2)))
(assert (= p2 (>= y2 0.2)))
```

```

(assert (= p3 (>= y3 0.2)))
(assert (= p4 (>= y4 0.2)))
(assert (= p5 (>= y5 0.2)))

; q_ represents validity of G <=5 p at time instant _
(assert (= q1 (and p1 p2 p3 p4 p5)))

; Goal, namely satisfaction of q at time 1
(assert q1)

(check-sat)

```

References

- Baumeister, J.; Finkbeiner, B.; Schirmer, S.; Schwenger, M.; Torens, C. RTLola Cleared for Take-Off: Monitoring Autonomous Aircraft. In Proceedings of the 32nd International Conference, CAV 2020 Part II, Los Angeles, CA, USA, 21–24 July 2020; Lahiri, S.K., Wang, C., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12225, pp. 28–39. [\[CrossRef\]](#)
- Gautham, S.; Jayakumar, A.V.; Rajagopala, A.; Elks, C. Realization of a Model-Based DevOps Process for Industrial Safety Critical Cyber Physical Systems. In Proceedings of the 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), Victoria, BC, Canada, 10–12 May 2021; pp. 597–604.
- Maler, O.; Nickovic, D. Monitoring Temporal Properties of Continuous Signals. In *Joint International Conferences on Formal Modelling and Analysis of Timed Systems, Proceedings of the FORMATS 2004 and Formal Techniques in Real-Time and Fault-Tolerant Systems, FTRFT 2004, Grenoble, France, 22–24 September 2004*; Lakhnech, Y., Yovine, S., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3253, pp. 152–166. [\[CrossRef\]](#)
- Bartocci, E.; Deshmukh, J.V.; Donzé, A.; Fainekos, G.; Maler, O.; Nickovic, D.; Sankaranarayanan, S. Specification-Based Monitoring of Cyber-Physical Systems: A Survey on Theory, Tools and Applications. In *Lectures on Runtime Verification—Introductory and Advanced Topics*; Bartocci, E., Falcone, Y., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2018; Volume 10457, pp. 135–175. [\[CrossRef\]](#)
- Holberg, H.J.; Häusler, S. *From Safety Requirements to Safety Monitors—Automatic Synthesis in Compliance with ISO 26262*; Embedded World: Nuremberg, Germany, 2012.
- Fränzle, M.; Hansen, M.R. A Robust Interpretation of Duration Calculus. In Proceedings of the Second International Colloquium on Theoretical Aspects of Computing—ICTAC 2005, Hanoi, Vietnam, 17–21 October 2005; Hung, D.V., Wirsing, M., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3722, pp. 257–271. [\[CrossRef\]](#)
- Donzé, A.; Maler, O. Robust Satisfaction of Temporal Logic over Real-Valued Signals. In Proceedings of the 8th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS 2010, Klosterneuburg, Austria, 8–10 September 2010; Chatterjee, K., Henzinger, T.A., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6246, pp. 92–106. [\[CrossRef\]](#)
- Donzé, A.; Ferrère, T.; Maler, O. Efficient Robust Monitoring for STL. In Proceedings of the 25th International Conference on Computer Aided Verification, CAV 2013, Saint Petersburg, Russia, 13–19 July 2013; Sharygina, N.; Veith, H., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8044, pp. 264–279. [\[CrossRef\]](#)
- Maybeck, P.S. Stochastic models, estimation, and control. In *Mathematics in Science and Engineering*; Academic Press: New York, NY, USA; San Francisco, CA, USA; London, UK, 1979; Volume 141.
- Junges, S.; Torfah, H.; Seshia, S.A. Runtime Monitors for Markov Decision Processes. In *Computer Aided Verification*; Silva, A., Leino, K.R.M., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland 2021; Volume 12760, pp. 553–576.
- Fränzle, M.; Kröger, P. The Demon, the Gambler, and the Engineer—Reconciling Hybrid-System Theory with Metrology. In *Symposium on Real-Time and Hybrid Systems—Essays Dedicated to Professor Chaochen Zhou on the Occasion of His 80th Birthday*; Jones, C.B., Wang, J., Zhan, N., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2018; Volume 11180, pp. 165–185. [\[CrossRef\]](#)
- Visconti, E.; Bartocci, E.; Loret, M.; Nenzi, L. Online monitoring of spatio-temporal properties for imprecise signals. In Proceedings of the 19th ACM-IEEE International Conference on Formal Methods and Models for System Design, Virtual Event, 20–22 November 2021; Arun-Kumar, S., Méry, D., Saha, I., Zhang, L., Eds.; ACM: New York, NY, USA, 2021; pp. 78–88. [\[CrossRef\]](#)
- de Figueiredo, L.H.; Stolfi, J. Affine Arithmetic: Concepts and Applications. *Numer. Algorithms* **2004**, *37*, 147–158. [\[CrossRef\]](#)

14. Wolfman, S.A.; Weld, D.S. The LPSAT Engine & Its Application to Resource Planning. In Proceedings of the 16th International Joint Conference on Artificial Intelligence—Volume 1, IJCAI'99, Stockholm, Sweden, 31 July–6 August 1999; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 1999; pp. 310–316.
15. Cimatti, A.; Griggio, A.; Schaafsma, B.; Sebastiani, R. The MathSAT5 SMT Solver. In Proceedings of the 19th International Conference, TACAS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, 16–24 March 2013; Piterman, N., Smolka, S., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7795.
16. Jiang, C.; Fu, C.M.; Ni, B.Y.; Han, X. Interval arithmetic operations for uncertainty analysis with correlated interval variables. *Acta Mech. Sin.* **2016**, *32*, 743–752. [\[CrossRef\]](#)
17. Jha, S.; Tiwari, A.; Seshia, S.A.; Sahai, T.; Shankar, N. TeLEx: Learning signal temporal logic from positive examples using tightness metric. *Form. Methods Syst. Des.* **2019**, *54*, 364–387. [\[CrossRef\]](#)
18. Moore, R.E. *Interval Analysis*; Prentice-Hall: Upper Saddle River, NJ, USA, 1966; pp. 11 + 145.
19. Benveniste, A.; Caillaud, B.; Nickovic, D.; Passerone, R.; Raclet, J.; Reinkemeier, P.; Sangiovanni-Vincentelli, A.L.; Damm, W.; Henzinger, T.A.; Larsen, K.G. Contracts for System Design. *Found. Trends Electron. Des. Autom.* **2018**, *12*, 124–400. [\[CrossRef\]](#)
20. Loper, G.B. Variable Gain Voltage Amplifier. U.S. Patent No. 2,497,835, 14 February 1950. Available online: <https://patentimages.storage.googleapis.com/52/a3/32/2fca1a6d25a758/US2497835.pdf> (accessed on 5 April 2022).
21. Fränzle, M.; Herde, C.; Teige, T.; Ratschan, S.; Schubert, T. Efficient Solving of Large Non-linear Arithmetic Constraint Systems with Complex Boolean Structure. *J. Satisf. Boolean Model. Comput.* **2007**, *1*, 209–236. [\[CrossRef\]](#)
22. Silva, J.P.M.; Sakallah, K.A. Conflict Analysis in Search Algorithms for Satisfiability. In Proceedings of the Eighth International Conference on Tools with Artificial Intelligence, ICTAI '96, Toulouse, France, 16–19 November 1996; pp. 467–469. [\[CrossRef\]](#)
23. Bayardo, R.J., Jr.; Schrag, R. Using CSP Look-Back Techniques to Solve Real-World SAT Instances. In Proceedings of the Fourteenth National Conference on Artificial Intelligence and Ninth Innovative Applications of Artificial Intelligence Conference, AAAI 97, IAAI 97, Providence, RI, USA, 27–31 July 1997; Kuipers, B., Webber, B.L., Eds.; AAAI Press/The MIT Press: Palo Alto, CA, USA, 1997; pp. 203–208.
24. Sebastiani, R. Lazy Satisfiability Modulo Theories. *J. Satisf. Boolean Model. Comput.* **2007**, *3*, 141–224. [\[CrossRef\]](#)
25. Barrett, C.; Tinelli, C. Satisfiability Modulo Theories. In *Handbook of Model Checking*; Clarke, E.M., Henzinger, T.A., Veith, H., Bloem, R., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 305–343. [\[CrossRef\]](#)
26. Teige, T.; Eggers, A.; Scheibler, K.; Stasch, M.; Brockmeyer, U.; Holberg, H.J.; Bienmüller, T. Two Decades of Formal Methods in Industrial Products at BTC Embedded Systems. In Proceedings of the 24th International Symposium on Formal Methods, FM 2021, Virtual Event, 20–26 November 2021; Huisman, M., Pasareanu, C.S., Zhan, N., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2021; Volume 13047, pp. 725–729. [\[CrossRef\]](#)
27. Scheibler, K.; Neubauer, F.; Mahdi, A.; Fränzle, M.; Teige, T.; Bienmüller, T.; Fehrer, D.; Becker, B. Accurate ICP-based floating-point reasoning. In Proceedings of the 2016 Formal Methods in Computer-Aided Design, FMCAD 2016, Mountain View, CA, USA, 3–6 October 2016; Piskac, R., Talupur, M., Eds.; IEEE: New York, NY, USA, 2016; pp. 177–184. [\[CrossRef\]](#)
28. Herde, C. Efficient Solving of Large Arithmetic Constraint Systems with Complex Boolean Structure: Proof Engines for the Analysis of Hybrid Discrete-Continuous Systems. Ph.D. Thesis, Carl von Ossietzky University of Oldenburg, Oldenburg, Germany, 2010.
29. Scheibler, K.; Kupferschmid, S.; Becker, B. Recent Improvements in the SMT Solver iSAT. In Proceedings of the Workshop Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV), Warnemünde, Germany, 12–14 March 2013; Haubelt, C., Timmermann, D., Eds.; Institut für Angewandte Mikroelektronik und Datentechnik, Fakultät für Informatik und Elektrotechnik, Universität Rostock: Rostock, Germany, 2013; pp. 231–241.
30. Cook, S.A. The Complexity of Theorem-Proving Procedures. In Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, Shaker Heights, OH, USA, 3–5 May 1971; Harrison, M.A., Banerji, R.B., Ullman, J.D., Eds.; ACM: New York, NY, USA, 1971; pp. 151–158. [\[CrossRef\]](#)
31. Amri, M.; Becis, Y.; Aubry, D.; Ramdani, N.; Fränzle, M. Robust indoor location tracking of multiple inhabitants using only binary sensors. In Proceedings of the IEEE International Conference on Automation Science and Engineering, CASE 2015, Gothenburg, Sweden, 24–28 August 2015; pp. 194–199. [\[CrossRef\]](#)