System Analysis and Robustness

Eugenio Moggi[1], Amin Farjudian[2], and Walid Taha[3]

[1] DIBRIS, Genova Univ., Genova, Italy, moggi@unige.it
[2] Univ. of Nottingham Ningbo China, amin.farjudian@nottingham.edu.cn
[3] Halmstad Univ., Halmstad, Sweden, walid.taha@hh.se

Abstract. Software is increasingly embedded in a variety of physical contexts. This imposes new requirements on tools that support the design and analysis of systems. For instance, modeling embedded and cyber-physical systems needs to blend discrete mathematics, which is suitable for modeling digital components, with continuous mathematics, used for modeling physical components. This blending of continuous and discrete creates challenges that are absent when the discrete or the continuous setting are considered in isolation. We consider robustness, that is, the ability of an analysis of a model to cope with small amounts of imprecision in the model. Formally, we identify analyses with monotonic maps between complete lattices (a mathematical framework used for abstract interpretation and static analysis) and define robustness for monotonic maps between complete lattices of closed subsets of a metric space.

Keywords: Analyses; Robustness; Domain theory.

1 Introduction

The following considerations are taken from the paper "Continuous modeling of real-time and hybrid systems: from concepts to tools" [12] by Berhard Steffen et al., which was published in a special section on timed and hybrid systems. They provide the context and motivations for the issues addressed in this short paper.

1. Having served as a successful paradigm in physics and engineering for more than 300 years, starting with the discovery of the differential calculus by Leibniz and Newton at the end of the seventeenth century, **the continuous interpretation of time was overwhelmed by the digital revolution**.
2. The key point of formal description techniques is their mathematical exactness: it is unambiguous how the specified system is going to behave. **Exactness should, however, not be confused with precision**: "the system must respond within at least 1 and up to 20 seconds" is exact, although one might argue that it is not precise. **Exact specifications make the amount of imprecision explicit**.
3. Typically the behavior of the controlled system is given a priori, while the controlling system still needs to be designed in a way guaranteeing a correct overall behavior. . . . , for most embedded systems the open system approach is insufficient as **the correctness of the controlling system depends on properties of the environment. Capturing these situations requires modeling the environment as well**.

Imprecision. In a discrete setting one can achieve absolute precision[4], in a continuous setting there are two pervasive and unavoidable sources of imprecision:

1. imprecision in measurements, namely predictions based on a mathematical model and observations on a *real system* can be compared only up to the precision of instruments used for measurements on the real system, and
2. imprecision in representing continuous quantities in computer-assisted tools for modeling and analyzing hybrid/continuous systems.

Thus, a real number $x{:}\,\mathbb{R}$ in mathematics, becomes $x \pm \epsilon$ in physics, with $\epsilon > 0$ *measurement error*, in theory of computation becomes an interval $[\underline{x}, \overline{x}]$ with $\underline{x}$ and $\overline{x}$ belonging to a subset of $\mathbb{R}$ with exact finite representations (e.g., floating-point or rational numbers) [14][5]. However, any $x{:}\,\mathbb{R}$ can be **approximated** by *proper rational intervals* $[\underline{x}, \overline{x}]$ with **arbitrarily small imprecision**, i.e., for any $\delta > 0$ there are rational numbers $\underline{x}$ and $\overline{x}$ such that $\underline{x} < x < \overline{x}$ and $0 < \overline{x} - \underline{x} < \delta$.

Approximability extends to continuous maps on $\mathbb{R}$. First, a continuous map f on $\mathbb{R}$ has a Scott continuous *natural extension* $\overline{f}(I) \stackrel{\Delta}{=} \{f(x) | x{:}\,I\}$ on the cpo $\mathbb{IR}$ of intervals ordered by reverse inclusion. Scott continuity implies that the imprecision of $\overline{f}(I)$ goes to 0 when the imprecision of I goes to 0. Second, $\overline{f}$ can be replaced by a Scott continuous F mapping proper rational intervals to proper rational intervals such that $F([x]) = [f(x)] = \overline{f}([x])$, thus $\overline{f}(I) \subseteq F(I)$. When f is not continuous, one must give up something. Namely, one can find a monotonic F on $\mathbb{IR}$ such that:

1. $\forall x{:}\,\mathbb{R}.F([x]) = [f(x)]$, but F fails to be Scott continuous, or
2. F is Scott continuous, $\forall I{:}\,\mathbb{IR}.\overline{f}(I) \subseteq F(I)$, but $\forall x{:}\,\mathbb{R}.F([x]) = [f(x)]$ fails.

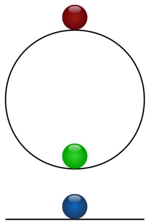
In both cases the property "$F(I)$ converges to $f(x)$ when I converges to x" fails.

Robustness. In [13], we introduced **robustness**, a property of monotonic maps between complete lattices of (closed) subsets in metric spaces. Intuitively, robustness requires that *small changes* to the input I of a map F cause small changes to its output, where the definition of small relies on the metrics. Often, analyses can be identified with monotonic maps between complete lattices. For instance, reachability analysis can be cast as a monotonic map F on the complete lattice $\mathbb{P}(\mathbb{S})$ of subsets of the state space $\mathbb{S}$, that takes a set I of initial states and outputs the set $R(I)$ of states reachable from I, thus $I \subseteq R(I) = R^2(I)$.

If $\mathbb{S}$ is a metric space, then one has the mathematical framework to measure imprecision. The picture below shows the initial state s of three systems (red, green and blue) consisting of a ball that can move (in a one-dimensional space) under the effect of gravity. We assume that initially the speed is 0, thus from s only s is reachable, i.e., $R_r(\{s\}) = R_g(\{s\}) = R_b(\{s\}) = \{s\}$, but:

[4] This does not exclude the possibility of using *imprecise* (aka loose) specifications.

[5] Representing a real with a float, as done in traditional numerical methods, means that the imprecision in computations is either ignored or is tracked manually.



- the red ball (top) is *unstable*, i.e., a small change s' to s means that $R_r(\{s'\})$ includes some states far from s;
- the green ball (middle) is *stable*, i.e., a small change s' to s implies that all states in $R_g(\{s'\})$ are close to s;
- the blue ball (bottom) is stable, if a small change s' affects only the position (while the speed remains 0); it is unstable, if the speed can change (and there is no friction).

These claims on s can be recast as follows: R_g is *robust at* $\{s\}$, R_r is not.

Background. We assume familiarity with metric/topological spaces, the notions of open/closed/compact subset of a space [4,10], and make limited use of Category Theory [2,3] and Domain Theory [8]. We may write $x{:}\, X$ for $x \in X$.

- Every metric space is a topological space whose open subsets are given by unions of open balls $B(x,\delta) \stackrel{\Delta}{=} \{y|d(x,y) < \delta\}$.
- $\mathsf{O}(\mathbb{S})$ is the set of open subsets of a metric/topological space $\mathbb{S}$, $\mathsf{C}(\mathbb{S})$ is the set of closed subsets, and $\mathsf{P}(\mathbb{S})$ is the set of all subsets.
- $\mathbb{P}(\mathbb{S})$ is the complete lattice of all subsets of $\mathbb{S}$ ordered by reverse inclusion, which is the natural *information order* on over-approximations (thus, sups are given by intersections and infs by unions). Similarly, $\mathbb{C}(\mathbb{S})$ is the complete lattice of closed subsets of $\mathbb{S}$ ordered by reverse inclusion (sups are given by intersections, but only finite infs are given by unions).

Contributions. The contributions of this short paper are:

1. A definition of imprecision in the context of metric spaces (Sec 2), related to the *noise model* in [7] and δ-safety in [11]. The main point is that imprecision makes a subset S of a metric space $\mathbb{S}$ indistinguishable from its closure $\overline{S}$.
2. A notion of robustness [13] (Sec 3) for monotonic maps $A{:}\, \mathbb{C}(\mathbb{S}_1) \to \mathbb{C}(\mathbb{S}_2)$, the restriction to closed subsets is due to indistinguishability of S and $\overline{S}$.
3. Results about existence of *best* robust approximations [13] (Sec 4).

2 Imprecision in Metric Spaces

Definition 1. *Given a metric space $\mathbb{S}$, with distance function d, we define:*

1. *$B(S,\delta) \stackrel{\Delta}{=} \{y|\exists x{:}\, S.d(x,y) < \delta\}$, where $S{:}\, \mathsf{P}(\mathbb{S})$ and $\delta > 0$. Intuitively, $B(S,\delta)$ is the set of points in S with imprecision $< \delta$. $B(S,\delta)$ is open, because it is the union of open balls $B(s,\delta)$ with $s{:}\, S$, moreover $B(B(S,\delta),\delta') \subseteq B(S,\delta+\delta')$.*
2. *$\overline{S}{:}\, \mathsf{C}(\mathbb{S})$ is the **closure** of $S{:}\, \mathsf{P}(\mathbb{S})$, i.e., the smallest $C{:}\, \mathsf{C}(\mathbb{S})$ such that $S \subseteq C$. For $S{:}\, \mathsf{P}(\mathbb{S})$ and $\delta > 0$ the following holds: $S \subseteq \overline{S} \subseteq B(S,\delta) = B(\overline{S},\delta)$. Thus, in the presence of imprecision, S and $\overline{S}$ are **indistinguishable**.*
3. *$S_\delta \stackrel{\Delta}{=} \overline{B(S,\delta)}$ is the δ**-fattening** of $S{:}\, \mathsf{P}(\mathbb{S})$. Intuitively, S_δ is the set of points in S with imprecision $\leq \delta$. In fact, $B(S,\delta) \subseteq S_\delta \subseteq B(S,\delta')$ when $0 < \delta < \delta'$. For $S{:}\, \mathsf{P}(\mathbb{S})$ the following holds: $\overline{S} = \bigcap_{\delta>0} B(S,\delta) = \bigcap_{\delta>0} S_\delta$. Thus, the closure $\overline{S}$ is the set of points that are in S with arbitrarily small imprecision.*

We consider some examples of metric spaces motivated by applications.

Example 1 (Discrete). A set $\mathbb{S}$ can be viewed as a **discrete** metric space, i.e., $d(s,s')=1$ when $s\neq s'$. Any subset S of $\mathbb{S}$ is closed and open. Thus, $\mathsf{C}(\mathbb{S})=\mathsf{P}(\mathbb{S})$, and $S_\delta=S$ for $\delta\leq 1$. More generally, if $\forall s,s'{:}\,\mathbb{S}.s\neq s' \implies \delta\leq d(s,s')$, then $\forall S{:}\,\mathsf{P}(\mathbb{S}).S_\delta=S$, i.e., an imprecision $\leq\delta$ amounts to absolute precision.

Example 2 (Euclidean). Euclidean spaces $\mathbb{R}^n$ (and Banach spaces) are used for modeling continuous and hybrid systems [9]. For $C{:}\,\mathsf{C}(\mathbb{R}^n)$, δ-fattening has a simpler alternative definition, namely $C_\delta=\{y|\exists x{:}\,C.d(x,y)\leq\delta\}$.

Example 3 (Products, sub-spaces, sums). The product $\mathbb{S}_0\times\mathbb{S}_1$ of two metric spaces is the product of the underlying sets with metric $d(x,y)\stackrel{\Delta}{=}\max\limits_{i:2} d_i(x_i,y_i)$.

A subset S' of $\mathbb{S}$ inherits the metric, thus can be considered a metric space $\mathbb{S}'$. If S' is also closed, then $\mathsf{C}(\mathbb{S}')\subseteq\mathsf{C}(\mathbb{S})$ and the δ-fattening of $S{:}\,\mathsf{P}(\mathbb{S}')$ is $S_\delta\cap S'$.

The sum $\coprod_{i:I}\mathbb{S}_i$ of an I-indexed family of metric spaces is $\{(i,x)|i{:}\,I\wedge x{:}\,\mathbb{S}_i\}$ with metric $d((i,x),(j,y))\stackrel{\Delta}{=}$ if $i=j$ then $d_i(x,y)$ else 1. The following hold: $\mathsf{P}(\coprod_{i:I}\mathbb{S}_i)\cong\prod_{i:I}\mathsf{P}(\mathbb{S}_i)$, i.e., a subset in the sum *is* a sum $\coprod_{i:I}S_i$ of subsets. Similarly, $\mathsf{C}(\coprod_{i:I}\mathbb{S}_i)\cong\prod_{i:I}\mathsf{C}(\mathbb{S}_i)$. Moreover, $(\coprod_{i:I}S_i)_\delta=\coprod_{i:I}(S_i)_\delta$ for $\delta\leq 1$.

Remark 1. Usually the state space of a hybrid automaton [1] is a (finite) sum of closed sub-spaces of Euclidean spaces. A hybrid system on a Euclidean space $\mathbb{S}$ is a pair $\mathcal{H}=(F,G)$ of relations on $\mathbb{S}$. Equivalently, $\mathcal{H}$ is a subset $F+G$ of the metric space $\mathbb{S}^2+\mathbb{S}^2$. Therefore, closure and δ-fattening are applicable to hybrid systems on $\mathbb{S}$ as well as to subsets of $\mathbb{S}$.

3 Analyses and Robustness

We identify analyses with arrows $A{:}\,\mathbf{Po}(X,Y)$ in the category $\mathbf{Po}$ of complete lattices and monotonic maps between them. The partial order $\leq$ allows to define over-approximations and compare them. We consider $\leq$ as an information order, thus: $x_0\leq x$ means that x_0 is an over-approximation of x, $x_1\leq x_0$ means that x_1 is a bigger over-approximation than x_0 (hence, less informative).

The complete lattice $\bot<\top$ of truth values, usually denoted Σ, is isomorphic to $\mathbb{P}(1)$ with 1 being the singleton set $\{\mathsf{fail}\}$, namely $\top$ (true) corresponds to $\emptyset$ (cannot fail), while $\bot$ (false) corresponds to $\{\mathsf{fail}\}$ (may fail). Safety analyses are arrows $A{:}\,\mathbf{Po}(X,\Sigma)$, and over-approximations may give false negatives.

Example 4. Safety analysis for transition systems on $\mathbb{S}$ corresponds to the arrow $\mathsf{Sf}{:}\,\mathbf{Po}(\mathbb{P}(\mathbb{S}^2)\times\mathbb{P}(\mathbb{S})\times\mathbb{P}(\mathbb{S}),\Sigma)$ such that $\mathsf{Sf}(R,I,B)=\top\stackrel{\Delta}{\iff}R^*(I)$ and B are disjoint, i.e., the set $R^*(I)$ of states reachable from the set I of initial states by (finitely many) R-transitions is disjoint from the set B of bad states.

Complete lattices do not have the structure to *quantify* imprecision. Thus, we restrict to complete lattices of the form $\mathbb{C}(\mathbb{S})$, with $\mathbb{S}$ a metric space, and use δ-fattening (Sec 2) to bound imprecision. Namely, given an over-approximation

C' of $C\colon \mathbb{C}(\mathbb{S})$, i.e., $C \subseteq C'$ (or equivalently $C' \leq C$), we say that the imprecision of C' in over-approximating C is $\leq \delta \overset{\Delta}{\iff} C \subseteq C' \subseteq C_\delta$.

For a metric space $\mathbb{S}$, there is an adjunction in **Po** (Galois connection) between $\mathbb{P}(\mathbb{S})$ and $\mathbb{C}(\mathbb{S})$. In particular, every $S\colon \mathbb{P}(\mathbb{S})$ has a *best over-approximation* $\overline{S}\colon \mathbb{C}(\mathbb{S})$. In other words, $\mathbb{C}(\mathbb{S})$ is an *abstract interpretation* of $\mathbb{P}(\mathbb{S})$ [5].

Definition 2 (Robustness [13]). *Given* $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ *with* $\mathbb{S}_1$ *and* $\mathbb{S}_2$ *metric spaces, we say that:*

- A *is* ***robust*** *at* $C \overset{\Delta}{\iff} \forall \epsilon > 0. \exists \delta > 0. A(C_\delta) \subseteq A(C)_\epsilon$.
- A *is* ***robust*** $\overset{\Delta}{\iff}$ A *is robust at every* C.

Robustness is a trivial property of analyses in a discrete setting (Ex 1).

Proposition 1. *If* $\mathbb{S}_1$ *is discrete, then every* $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ *is robust.*

Most analyses are not cast in the right form to ask whether they are robust, but usually one can show that they have the right form up to isomorphisms in **Po**.

Example 5. We consider analyses for (topological) transition systems [6].

1. Reachability $\mathsf{Rf}_R\colon \mathbf{Po}(\mathbb{P}(\mathbb{S}), \mathbb{P}(\mathbb{S}))$ for a transition system R on $\mathbb{S}$ is not a map on closed subsets, but can be replaced by the arrow $C \mapsto \overline{\mathsf{Rf}_R(C)}$ on $\mathbb{C}(\mathbb{S})$. This is the canonical way to turn arrows on $\mathbb{P}(\mathbb{S})$ into arrows on $\mathbb{C}(\mathbb{S})$, but it may fail to be idempotent. A better choice is the *best* idempotent arrow on $\mathbb{C}(\mathbb{S})$ over-approximating Rf_R, denoted Rs_R and called **safe reachability** in [13], i.e., $\mathsf{Rs}_R(C) \overset{\Delta}{=}$ the smallest $C'\colon \mathbb{C}(\mathbb{S})$ such that $C \subseteq C'$ and $R(C') \subseteq C'$.
2. Reachability $\mathsf{Rf}\colon \mathbf{Po}(\mathbb{P}(\mathbb{S}^2) \times \mathbb{P}(\mathbb{S}), \mathbb{P}(\mathbb{S}))$ for transition systems on $\mathbb{S}$. First, we replace $\mathbb{P}(\mathbb{S}^2) \times \mathbb{P}(\mathbb{S})$ with the isomorphic $\mathbb{P}(\mathbb{S}^2 + \mathbb{S})$ (see Ex 3). Second, we proceed as done for Rf_R. In particular, we can replace Rf with safe reachability $\mathsf{Rs}\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}^2) \times \mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$ for *closed* transition systems on $\mathbb{S}$.
3. Safety $\mathsf{Sf}\colon \mathbf{Po}(\mathbb{P}(\mathbb{S}^2) \times \mathbb{P}(\mathbb{S}) \times \mathbb{P}(\mathbb{S}), \Sigma)$ is definable in terms of reachability Rf, namely $\mathsf{Sf}(R, I, B) \overset{\Delta}{\iff} \mathsf{Rf}(R, I) \# B$, where $\#$ is the disjointness predicate. Any replacement for Rf induces a corresponding notion of safety, e.g., safe safety $\mathsf{Ss}\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}^2) \times \mathbb{C}(\mathbb{S}) \times \mathbb{C}(\mathbb{S}), \Sigma)$ is $\mathsf{Ss}(R, I, B) \overset{\Delta}{\iff} \mathsf{Rs}(R, I) \# B$.

Remark 2. An analysis $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ is often robust at some $C\colon \mathbb{C}(\mathbb{S}_1)$, but it is rarely robust at every C. For instance, let R_C be the diagonal relation on $C\colon \mathbb{C}(\mathbb{R})$, which is a closed transition system on $\mathbb{R}$, then

- Rs_{R_C} is robust, since $\mathsf{Rs}_{R_C}(I) = I$ for every $I\colon \mathbb{C}(\mathbb{R})$;
- Rs is robust at $(R_\mathbb{N}, I)$ for every $I\colon \mathbb{C}(\mathbb{R})$, but
- Rs is not robust at $(R_\mathbb{R}, I)$ when $\emptyset \subset I \subset \mathbb{R}$, because $\mathsf{Rs}((R_\mathbb{R})_\delta, I) = \mathbb{R}$.

Time automata are a special case of hybrid automata (e.g., see [12]), and the latter are subsumed by hybrid systems [9]. **Timed transition systems** are an abstraction for all these systems. In particular, there is an abstraction map $\alpha\colon \mathbf{Po}(\mathbb{P}(\mathbb{S}^2 + \mathbb{S}^2), \mathbb{P}(\mathbb{T} \times \mathbb{S}^2))$ from hybrid systems on (the Euclidean space) $\mathbb{S}$ to timed transition systems on (the topological space) $\mathbb{S}$, where $\mathbb{T}$ is the continuous time line, i.e., the space of non negative reals $[0, +\infty)$.

Example 6. Reachability is not appropriate when time matters. For a timed transition system R on $\mathbb{S}$, a better analysis is **evolution** $\mathsf{Ef}_R\colon \mathbf{Po}(\mathbb{P}(\mathbb{S}), \mathbb{P}(\mathbb{T}\times\mathbb{S}))$, which gives the time at which a state is reached, namely $\mathsf{Ef}_R(I) \triangleq$ the smallest $E\colon \mathbb{P}(\mathbb{T}\times\mathbb{S})$ such that $\{0\}\times I \subseteq E$ and $\{(t+d, s')|(t,s)\colon E \wedge (d,s,s')\colon R\} \subseteq E$. By analogy with reachability, one can define $\mathsf{Ef}\colon \mathbf{Po}(\mathbb{P}(\mathbb{T}\times\mathbb{S}^2)\times\mathbb{P}(\mathbb{S}), \mathbb{P}(\mathbb{T}\times\mathbb{S}))$ and safe variants $\mathsf{Es}\colon \mathbf{Po}(\mathbb{C}(\mathbb{T}\times\mathbb{S}^2)\times\mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{T}\times\mathbb{S}))$, and cast them in the form required by robustness. Safe evolution can be extended to include asymptotically reachable states $\mathsf{Es}\colon \mathbf{Po}(\mathbb{C}(\mathbb{T}\times\mathbb{S}^2)\times\mathbb{C}(\mathbb{S}), \mathbb{C}(\overline{\mathbb{T}}\times\mathbb{S}))$, where $\overline{\mathbb{T}}$ is $[0,+\infty]$.

4 Best Robust Approximations

Intuitively, when an analysis $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ is robust at C, $A(C)$ is *useful* also in the presence of small amounts of imprecision. This is obvious for analyses $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \Sigma)$, where robustness at C means $A(C_\delta) = A(C)$ when δ is *small.*

Definition 3. *Given $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$, we say that:*

- *$A'\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ is a robust approximation of A $\overset{\triangle}{\iff}$ A' is robust and $\forall C. A'(C) \leq A(C)$.*
- *$A^{\boxdot}\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ is a **best robust approximation** of A $\overset{\triangle}{\iff}$ $A^{\boxdot}$ is a robust approximation of A such that $A'(C) \leq A^{\boxdot}(C)$ for every robust approximation A' of A and C.*

Every arrow has a *worst* robust approximation, namely the map $C \mapsto \bot$, where $\bot$ is the least element in $\mathbb{C}(\mathbb{S}_2)$. There are $A\colon \mathbf{Po}(\mathbb{C}([0,1]), \mathbb{C}(\mathbb{R}))$ that do not have a best robust approximation (see [13, Ex 4.6]). When $\mathbb{S}_1$ and $\mathbb{S}_2$ are discrete metric spaces, every $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ is robust, thus $A^{\boxdot} = A$. We give conditions on metric spaces implying existence of best robust approximations. The first result applies to safety analyses and is related to the notion of robustness in [7, Def 2].

Theorem 1. *If $\mathbb{S}_2$ is a finite metric space, then $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ has a best robust approximation $A^{\boxdot}$ given by $A^{\boxdot}(C) = \bigcap\{A(C_\delta)|\delta > 0\}$.*

Proof. $\mathbb{C}(\mathbb{S}_2) = \mathbb{P}(\mathbb{S}_2) \cong \Sigma^n$ is a finite complete lattice, when $\mathbb{S}_2$ is a finite (and necessarily discrete) metric space with n points. Therefore, $A'\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ robust at C means that there exists $\delta > 0$ such that $A'(C) = A'(C_\delta)$.

Since $\{A(C_\delta)|\delta > 0\}$ is a chain in a finite lattice, there exists $\delta > 0$ such that $A(C_{\delta'}) = A(C_\delta)$ when $\delta' < \delta$. Let $\delta(C)$ be the biggest element in $(0,+\infty]$ such that $A(C_{\delta'}) = A(C_\delta)$ when $\delta' < \delta < \delta(C)$. Define $A^{\boxdot}(C) \triangleq A(C_\delta)$ for $\delta < \delta(C)$, then $A^{\boxdot}$ is monotonic, since $A^{\boxdot}(C) = A(C_\delta) \leq A(C'_\delta) \leq A^{\boxdot}(C')$ when $C \leq C'$ and $\delta < \delta(C)$, and $A^{\boxdot}$ is a robust approximation of A, since

- $A^{\boxdot}(C) = A(C_\delta) \leq A(C)$ when $\delta < \delta(C)$, and
- $A^{\boxdot}(C) = A(C_\delta) = A^{\boxdot}(C_{\delta'})[= A(C_{\delta'})]$ when $\delta' < \delta < \delta(C)$.

Finally, $A^{\boxdot}$ is the best robust approximation of A, because $A'(C) = A'(C_\delta) \leq A(C_\delta) = A^{\boxdot}(C)$ when A' is a robust approximation of A and δ is small. $\square$

$\mathcal{H}$	S_0	s	S_f	S_s	S_r	S_R	
$\mathcal{H}_E$	$[0,1]$	0	$[0]$	S_f	$\mathbf{S_0}$	S_0	
		$0 < s \leq 1$	$[s,1]$	S_f	S_f	S_f	
$\mathcal{H}_D$	$[0,1]$	0	S_0	S_0	S_0	S_0	
		$0 < s \leq 1$	$(0,s]$	$\mathbf{S_0}$	S_0	S_0	
$\mathcal{H}_T$	$\{(x,y) \vert 0 \leq x \leq y \leq 1\}$	$(0,1)$	$S^*(0)$	S_f	S_f	S_f	$b=0$
		$(0,1)$	$S^*(b)$	$\mathbf{S_f} \uplus \mathbf{S(0)}$	S_s	S_s	$0 < b < 1$
		$(0,1)$	$S(1)$	S_f	S_f	$\mathbf{S_0}$	$b=1$

For $\mathcal{H}_E$ and $\mathcal{H}_D$ we take $\mathcal{H}_0 = (F_0, G_0)$ with $F_0 = [0,1] \times [-1,1]$ and $G_0 = [0,1]^2$.
For $\mathcal{H}_T = (F,G)$ we take $\mathcal{H}_0 = (\overline{F}, G_0)$ with $G_0 = \{(y,y) | y\colon [0,1]\} \times \{(0,y) | y\colon [0,1]\}$,
and we use the notation $S(b) \triangleq [0,b] \times [b]$ and $S^*(b) \triangleq \cup_n S(b^n)$ for subsets of S_0.
The differences in the approximations of the reachable states are highlighted in **bold.**
Table 1. Safe and robust over-approximations of the set of reachable states.

Theorem 2. *If $\mathbb{S}_1$ and $\mathbb{S}_2$ are compact metric spaces, then $A\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ has a best robust approximation $A^{\boxdot}$ given by $A^{\boxdot}(C) = \bigcap \{A(C_\delta) | \delta > 0\}$.*

Proof. We refer to [13] for details of the proof. The key points are:

- if $\mathbb{S}$ is a compact metric space, then $\mathbb{C}(\mathbb{S})$ is a continuous lattice;
- if $\mathbb{S}_1$ and $\mathbb{S}_2$ are compact metric spaces, then a map $A'\colon \mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ is robust exactly when it is Scott continuous. □

5 Examples

We conclude by comparing different reachability analyses for three *deterministic* hybrid systems $\mathcal{H}$ [9]:

$\mathcal{H}_E$ a quantity x grows according to ODE $\dot{x} = x$ when $0 \leq x < 1$, and stays constant when it reaches the threshold 1, i.e., $\dot{x} = 0$ when $x = 1$.

$\mathcal{H}_D$ a quantity x decreases according to ODE $\dot{x} = -x$ when $0 < x \leq 1$, and it is *instantaneously* reset to 1 when it is 0, i.e., $x^+ = 1$ when $x = 0$.

$\mathcal{H}_T$ a timer x grows while the timeout y stays constant, i.e., $\dot{x} = 1 \& \dot{y} = 0$ when $0 \leq x < y \leq 1$, when x reaches y it is reset and the timeout updated, i.e., $x^+ = 0 \& y^+ = by$ when $0 < x = y \leq 1$ (with b constant in the interval $[0,1]$), moreover $x^+ = 0 \& y^+ = 1$ when $0 = x = y \leq 1$, i.e., y is reset to 1.

Table 1 gives for each $\mathcal{H}$ above (and initial state s) the following sets:

- $S_f \triangleq \mathsf{Rf}_{\mathcal{H}}(s)$ set of states reachable (from s) in finitely many transitions, S_f is always a subset of the set S of the states reachable in finite time;
- $S_s \triangleq \mathsf{Rs}_{\mathcal{H}}(s)$ superset of S computed by safe reachability;
- $S_r \triangleq \mathsf{Rs}^{\boxdot}_{\mathcal{H}}(s)$ superset of S_s robust w.r.t. over-approximations of s;
- $S_R \triangleq \mathsf{Rs}^{\boxdot}(\overline{\mathcal{H}}, s)$ superset of S_s robust w.r.t. over-approximations of $\overline{\mathcal{H}}$ & s.

Note that S_r depends on a compact subset S_0 (over-approximating s and the *support* of $\mathcal{H}$), and S_R depends also on a compact hybrid system $\mathcal{H}_0$ (with support S_0 and over-approximating $\mathcal{H}$). In particular, $\mathcal{H}_0$ constrains the over-approximations of $\mathcal{H}$. The inclusions $[s \in] S_f [\subseteq S] \subseteq S_s \subseteq S_r \subseteq S_R [\subseteq S_0]$ hold always. We explain why some of these inclusions are strict.

- $\mathcal{H} = \mathcal{H}_E$ & $s = 0$: $S_f = S = S_s \subset S_r$, because any small positive change to s causes the quantity to grow and eventually reach the threshold.
- $\mathcal{H} = \mathcal{H}_D$ & $s > 0$: $S_f = S \subset S_s$, because safe reachability includes 0, which is reachable only asymptotically (not in finite time), and any state in $\mathsf{Rf}_{\mathcal{H}}(0)$.
- $\mathcal{H} = \mathcal{H}_T$ & $s = (0, 1)$ & $0 < b < 1$: $S_f \subset S = S_s$, because the system has a *Zeno behaviour*, namely the state $x = y = 0$ is reachable from $x = y = 1$ in time $b/(1-b)$, but it requires infinitely many updates to the timeout y. Thus S_f computes an under-approximation of what is reachable in finite time.
- $\mathcal{H} = \mathcal{H}_T$ & $s = (0, 1)$ & $b = 1$: $S_f = S = S_r \subset S_R$, because the imprecision in $\mathcal{H}_\delta$ means that y can be updated with any value y^+ in $[\max(0, y - \delta), y]$ when $0 < x = y \leq 1$. Therefore, $x = y = 0$ is reachable in $O(\delta^{-1})$ transitions.

References

1. R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical computer science*, 138(1):3–34, 1995.
2. A. Asperti and G. Longo. *Categories, Types and Scructures: an Introduction to Category Theory for the working Computer Scientist.* MIT Press, 1991.
3. S. Awodey. *Category theory.* Oxford University Press, 2010.
4. J. B. Conway. *A Course in Functional Analysis.* Springer, 2nd edition, 1990.
5. P. Cousot and R. Cousot. Abstract interpretation frameworks. *Journal of logic and computation*, 2(4):511–547, 1992.
6. P. J. L. Cuijpers and M. A. Reniers. Topological (bi-) simulation. *Electronic Notes in Theoretical Computer Science*, 100:49–64, 2004.
7. M. Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In *Computer Science Logic*, pages 126–139. Springer, 1999.
8. G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. W. Mislove, and D. S. Scott. *Continuous Lattices and Domains*, volume 93 of *Encycloedia of Mathematics and its Applications.* Cambridge University Press, 2003.
9. R. Goebel, R. G. Sanfelice, and A. Teel. Hybrid dynamical systems. *Control Systems, IEEE*, 29(2):28–93, 2009.
10. J. L. Kelley. *General topology.* Springer, 1975.
11. S. Kong, S. Gao, W. Chen, and E. Clarke. dreach: δ-reachability analysis for hybrid systems. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 200–205. Springer, 2015.
12. K. G. Larsen, B. Steffen, and C. Weise. Continuous modeling of real-time and hybrid systems: from concepts to tools. *International Journal on Software Tools for Technology Transfer*, 1(1-2):64–85, 1997.
13. E. Moggi, A. Farjudian, A. Duracz, and W. Taha. Safe & robust reachability analysis of hybrid systems. *Theoretical Computer Science*, 2018. Open access DOI 10.1016/j.tcs.2018.06.020.
14. R. E. Moore. *Interval Analysis.* Prentice-Hall, 1966.