Safe & Robust Reachability Analysis of Hybrid Systems

Eugenio Moggi[1a], Amin Farjudian[2b], Adam Duracz[3c], Walid Taha[4d]

[a] *DIBRIS, Genova Univ., v. Dodecaneso 35, 16146 Genova, Italy, Email: moggi@unige.it*
[b] *University of Nottingham Ningbo, China, Email: Amin.Farjudian@gmail.com*
[c] *Rice University, Houston, TX, USA, Email: adam.duracz@rice.edu*
[d] *Halmstad University, Halmstad, Sweden, Email: Walid.Taha@hh.se*

Abstract

Hybrid systems—more precisely, their mathematical models—can exhibit behaviors, like *Zeno behaviors*, that are absent in purely discrete or purely continuous systems. First, we observe that, in this context, the usual definition of *reachability*—namely, the reflexive and transitive closure of a transition relation—can be *unsafe*, i. e., it may compute a proper subset of the set of states *reachable in finite time* from a set of initial states. Therefore, we propose *safe reachability*, which always computes a super-set of the set of reachable states.

Second, in safety analysis of hybrid and continuous systems, it is important to ensure that a reachability analysis is also *robust* w. r. t. small perturbations to the set of initial states and to the system itself, since discrepancies between a system and its mathematical models are unavoidable. We show that, under certain conditions, the *best Scott continuous approximation* of an analysis A is also its *best robust approximation*. Finally, we exemplify the gap between the set of reachable states and the supersets computed by safe reachability and its best robust approximation.

Keywords: Hybrid systems; Reachability; Robustness; Domain theory.

Introduction

In a transition system—i. e., a relation $\rightarrow$ on a set of states—reachability is a clearly defined notion, namely, the reflexive and transitive closure $\rightarrow^*$ of $\rightarrow$. Reachability analysis plays an important role in computer-assisted verification and analysis [2], since **safety** (a key system requirement) is usually formalized in terms of **reachability**, namely:

[1] Research partially supported by the Swedish Knowledge Foundation.
[2] Work done while the author was a researcher at Halmstad University.
[3] Work done while the author was a PhD student at Halmstad University.
[4] Research partially supported by US NSF award #1736754 "A CPS Approach to Robot Design", the ELLIIT 7Swedish Strategic Area initiative, and the Swedish Knowledge Foundation project "AstaMoCA: Model-based Communications Architecture for the AstaZero Automotive Safety Facility".

state s is safe $\iff$ it is not possible to reach a bad state from s.

For a hybrid system one can define a transition relation $\to$ on a *continuous and uncountable* state space, but $\to^*$ captures only the states reachable in finitely many transitions, and they can be a proper subset of those reachable in finite time! Hybrid systems with *Zeno behaviors*—where infinitely many events occur in finite time—are among the systems in which the two notions of reachability differ. Zeno behaviors arise naturally when modeling rigid body dynamics with impacts, as illustrated by the system consisting of a bouncing ball (Example 2.8), whose Zeno behavior is due to the modeling of impacts as discrete events.

Contributions

The first contribution of this paper is the notion of **safe reachability** (Def 3.6), which gives an over-approximation—i. e., a superset—of the states reachable in finite time, including the case where the hybrid system has Zeno behaviors. Mathematical models are always *simplifications*, through abstractions and approximations, of *real systems*. Simplifications are essential to making analyses manageable. In safety analysis, over-approximations are acceptable, since they can only lead to false negatives, i. e., the analysis may wrongly conclude that (a state s of) the system in unsafe, because the over-approximation includes some unreachable bad states.

The second contribution is to show, under certain assumptions, that the *best Scott continuous approximation* of safe reachability coincides with its *best robust approximation*. In safety analysis robust over-approximations are important, because inaccuracies in the modeling of a cyber-physical system (as well as in its building and testing) are unavoidable, as convincingly argued in [13].

Background

We build directly on the following papers.

- [15] is an excellent tutorial on hybrid systems, from which we borrow the definition of a hybrid system (Def 2.1), but we do not use hybrid arcs (and related notions), since they cannot reach nor go beyond *Zeno points*.
- [10, 9] introduce topological transition systems (TTS), which we use for defining safe reachability (Def 3.6). In TTSs on discrete spaces, standard reachability (Def 3.1) and safe reachability (Def 3.6) coincide.
- [12] is one among several papers, where Edalat recasts mainstream mathematics in Domain Theory, and shows what is gained by doing so. In the context of this paper, Domain Theory becomes relevant when the Scott and Upper Vietoris topologies on certain *hyperspaces* coincide.

The reachability maps we introduce are arrows in the category of complete lattices and monotonic maps, which is the standard setting for defining and comparing abstract interpretations [8]. Our notion of robustness is related to δ-*safety*, i. e., safety of a system subject to noise up to δ. [13, 19] argue that δ-safety makes the verification task easier, and excludes systems that are safe only under unrealistic assumptions.

Summary

The rest of the paper is organized as follows:

- Sec 2 recalls the definition of a hybrid system from [15], defines the corresponding transition relation (Def 2.3), and gives some examples.
- Sec 3 introduces two reachability maps Rf and Rs (Def 3.1 and 3.6, respectively), establishes their properties and how they relate to each other.
- Sec 4 introduces the notion of robustness (see Def 4.1) and states two results on the existence of best robust approximations (Corr 4.4 and 4.5), that follow from more general results on Scott continuous maps.
- Sec 5 uses the category of complete lattices and monotonic maps (see Def 5.2) as a framework to discuss approximations and relate reachability maps defined on different complete lattices. In this framework we give a general definition of *best approximation* (Thm 5.11), and in particular a systematic way to turn a monotonic map f between complete lattices into its best Scott continuous approximation $f^{\boxdot}$ (see Prop 5.15).
- Sec 6 recalls and assesses the most relevant notions in [15], mainly to justify in retrospect the approach taken in this paper.
- Sec 7 analyses (with the aid of pictures) the differences between the under-approximation Rf and several over-approximations (from Rs to $\mathsf{Rs}^{\boxdot}$) of sets of reachable states, for the hybrid systems introduced in Sec 2.

Appendix A contains proofs that were too long to inline and a section relating robustness and Scott continuity (see Appendix A.1).

1. Mathematical preliminaries

We assume familiarity with the notions of Banach, metric, and topological space, and the definitions of open, closed, and compact subset of a topological space (see, e. g., [7, 18]). The relations among spaces are:

- Every Banach space is a *Cauchy complete* metric space whose distance is $d(x, y) \triangleq |y - x|$, where $|x|$ is the norm of x;
- Every metric space is a topological space whose open subsets are given by unions of open balls $B(x, \delta) \triangleq \{y | d(x, y) < \delta\}$.

For the sake of simplicity, one may replace Banach spaces with Euclidean spaces $\mathbb{R}^n$. For membership we may write $x{:}X$ instead of $x \in X$, and we use the following notations:

- $\mathbb{R}$ denotes the Euclidean space of the real numbers;
- $\mathbb{N}$ denotes the set of natural numbers, while ω is the poset of natural numbers with the usual linear order;

- $\mathsf{P}(\mathbb{S})$ is the set of subsets of a set $\mathbb{S}$ (the notation is used also when $\mathbb{S}$ is a set with additional structure, e. g., a Banach or topological space);
- $\mathsf{O}(\mathbb{S})$ is the set of open subsets of a topological space $\mathbb{S}$, and $\mathsf{C}(\mathbb{S})$ is the set of closed subsets (the notation is used also when $\mathbb{S}$ is a set with additional structure that induces a topology, e. g., a Banach or metric space).

Except for Sec 5, we make limited use of Category Theory ([3, 4]).

- If $\mathbb{A}$ is a category and $X, Y{:}\mathbb{A}$ are two of its *objects*, then $\mathbb{A}(X, Y)$ denotes the set of *arrows* from X to Y.
- Products and coproducts in $\mathbb{A}$ are denoted by $\prod$ and $\coprod$, they are *defined* by the properties (where $\prod$ on the right-hand side is a product of sets)

$$\mathbb{A}(X, \prod i{:}I.Y_i) \cong \prod i{:}I.\mathbb{A}(X, Y_i) \quad \mathbb{A}(\coprod i{:}I.X_i, Y) \cong \prod i{:}I.\mathbb{A}(X_i, Y).$$

- **Set** is the category of sets and (total) maps. It has both products and coproducts, in particular $\coprod i{:}I.X_i$ is (up to iso) the set $\{(i, x)|i{:}I \wedge x{:}X_i\}$.
- $\mathbf{Set}_p$ is the category of sets and partial maps. It has both products and coproducts, but only coproducts are computed as in **Set**.
- **Top** is the category of topological spaces and continuous maps.

Finally, we recall some definitions and their basic properties:

- x is a **limit** of a sequence $(x_n|n{:}\omega)$ in the topological space $\mathbb{S} \stackrel{\Delta}{\iff} \forall O{:}\mathsf{O}(\mathbb{S}).x{:}O \implies \exists m.\forall n > m.x_n{:}O$.

  The limits of a sequence form a closed subset of $\mathbb{S}$. In a metric space a sequence has at most one limit.

- x is an **accumulation point** of a sequence $(x_n|n{:}\omega)$ in the topological space $\mathbb{S} \stackrel{\Delta}{\iff} \forall O{:}\mathsf{O}(\mathbb{S}).x{:}O \implies \forall m.\exists n > m.x_n{:}O$.

  The accumulation points of a sequence form a closed subset of $\mathbb{S}$, every limit is also an accumulation point, and every accumulation point is a limit of a sub-sequence $(x_{f(n)}|n{:}\omega)$ for some strictly increasing $f{:}\mathbf{Set}(\omega, \omega)$, i. e., $\forall n.f(n) < f(n+1)$. In a metric space, if a sequence has a limit, then the limit is the only accumulation point.

- The **derivative** $\dot{f}{:}\mathbf{Set}_p(\mathbb{R}, \mathbb{S})$ of a partial map $f{:}\mathbf{Set}_p(\mathbb{R}, \mathbb{S})$ from $\mathbb{R}$ to a Banach space $\mathbb{S}$ is given by $\dot{f}(x) = v \stackrel{\Delta}{\iff} \exists \delta > 0$ s. t. $B(x, \delta)$ is included in the domain of f, and if x is the limit in $\mathbb{R}$ of a sequence $(x_n|n{:}\omega)$ in $B(x, \delta) - \{x\}$, then v is the limit of the sequence $(\frac{f(x_n)-f(x)}{x_n-x}|n{:}\omega)$ in $\mathbb{S}$.

  If $\dot{f}(x)$ is defined, then f must be defined in an open ball $B(x, \delta)$ and continuous at x. If $\dot{f}$ is defined and continuous in $B(x, \delta)$, then f is called *continuously differentiable* in $B(x, \delta)$.

2. Hybrid Systems and Topological Transition Systems

In this section, we define what is a hybrid system (cf. [15]), i. e., a mathematical model suitable for describing cyber-physical systems [20, 22]; what is a topological timed transition system (cf. [10]), i. e., an abstraction of hybrid systems useful for defining various reachability maps; finally we introduce some examples of hybrid systems that will be used throughout the paper.

Definition 2.1. A **Hybrid System** (HS for short) $\mathcal{H}$ on a Banach space $\mathbb{S}$ is a pair (F, G) of binary relations on $\mathbb{S}$, i. e., $F, G{:}\mathsf{P}(\mathbb{S} \times \mathbb{S})$, respectively called **flow** and **jump** relation. We say that $\mathcal{H}$ is **open/closed/compact**, when the relations F and G—as subsets of the topological space $\mathbb{S} \times \mathbb{S}$—are open/closed/compact.

Remark 2.2. In [15], the authors restrict $\mathbb{S}$ to a Euclidean space $\mathbb{R}^n$, and show that HS subsume Hybrid Automata [2] and Switching Systems.

The flow and jump relations are constraints for the *trajectories* describing how the HS evolves over time (see the notion of solution in [15, page 39-40]). Trajectories are not needed to define reachability (see Sec 3), since a simpler notion of *transition* suffices (see also [2, Sec 2] and [21, Def 5]).

Definition 2.3. A **Topological Timed Transition System** (TTTS) is a pair $(\mathbb{S}, \longrightarrow)$ consisting of a topological space $\mathbb{S}$ and a timed transition relation $\longrightarrow {:}\mathsf{P}(\mathbb{S} \times \mathbb{T} \times \mathbb{S})$, where $\mathbb{T} \triangleq \{d{:}\mathbb{R} | d \geq 0\}$ is the **continuous time line**. Its corresponding transition relation on $\mathbb{S}$ is given by $s \longrightarrow s' \overset{\Delta}{\iff} \exists d.s \xrightarrow{d} s'$.

A HS $\mathcal{H} = (F, G)$ on $\mathbb{S}$ induces a TTTS $(\mathbb{S}, \xrightarrow[\mathcal{H}]{})$ s. t. $s \xrightarrow[\mathcal{H}]{d} s' \overset{\Delta}{\iff}$

1. $d = 0$ and $s\, G\, s'$, or,
2. $d > 0$ and there exists a continuous map $f{:}\mathbf{Top}([0, d], \mathbb{S})$ s. t.:
   - the derivative $\dot{f}$ of f is defined and continuous in $(0, d)$;
   - $s = f(0)$, $s' = f(d)$ and $\forall t{:}(0, d).f(t)\, F\, \dot{f}(t)$.

   In this case we say that f *realizes* the transition.

Remark 2.4. Hybrid arcs (cf. [15]) could be defined in term of a transition relation where the labels $d > 0$ are replaced by their realizer maps f.

- In [15] the requirements on f are more relaxed than ours, namely: f must be *absolutely continuous* (which, in our case, is implied by the continuity of $\dot{f}$), and the flow relation must hold *almost everywhere* in $(0, d)$. However, the safe evolution and safe reachability maps (see Def 3.6) are insensitive to these changes. Thus, we have adopted the requirements on f that are mathematically simpler to express.

- In [16] the requirements on f are stricter than ours, namely: $\dot{f}$ must extend continuously to $[0, d]$, and the flow relation must hold also at the end-points. For instance, the map $f(t) = \sqrt{t}$ is continuous in $[0, d]$, its derivative $\dot{f}(t) = \frac{1}{2*\sqrt{t}}$ is continuous in $(0, d)$, but it cannot be extended continuously to 0. The main rationale for the stricter requirements is that a transition $s \xrightarrow{d} s'$ with $d > 0$ can only start from a state in the domain of the flow relation F.

Notation 2.5. Given a first-order language with an interpretation in a Banach space $\mathbb{S}$, a HS on $\mathbb{S}$ can be described by two formulas, a flow formula $F(x, \dot{x})$ and a jump formula $G(x, x^+)$, with two free variables each: x denotes the current state, $\dot{x}$ denotes the derivative of a trajectory flowing through x, and x^+ denotes a state reachable from x with one jump.

Similarly, given a two sorted language, with one sort interpreted in $\mathbb{R}$ and the other in a topological space $\mathbb{S}$, a timed transition relation can be described by a formula $T(x, d, x')$ with three free variables: x denotes the starting state, d:$\mathbb{R}$ the duration of the transition, and x' the final state.

We introduce some hybrid systems, and give explicit descriptions of their timed transition relations (see also the Figures in Sec 7).

Example 2.6 (Expand). The HS $\mathcal{H}_E$ on $\mathbb{R}$ describes the expansion of a quantity m until it reaches a threshold $M > 0$. Its flow and jump relations are:

$$F = \{(m, \dot{m}) | 0 \leq m = \dot{m} \leq M\}, \qquad G = \emptyset.$$

It has two kinds of trajectories depending on the start state m_0 (see Fig 1).

1. When $m_0 = 0$, the quantity remains 0 forever, i. e., $f(t) = 0$ when $t \geq 0$.
2. When m_0:$(0, M)$, there is an exponential growth $f(t) = m_0 * e^t$ until $f(t)$ becomes M, then the trajectory cannot progress further.

The timed transition relation $\xrightarrow[\mathcal{H}_E]{}$ consists of the transitions

- $m \xrightarrow{d} m'$ with $0 < d$ and $0 \leq m \leq m' = m * e^d \leq M$.

Removing (M, M) from F does not change the timed transitions, while adding $(M, 0)$ to F entails the addition of the transitions $M \xrightarrow{d} M$ with $d > 0$.

Example 2.7 (Decay). The HS $\mathcal{H}_D$ on $\mathbb{R}$ describes the decay of a quantity $m > 0$, and a *refill* to $M > 0$ when $m = 0$. Its flow and jump relations are:

$$F = \{(m, \dot{m}) | m > 0 \wedge \dot{m} = -m\}, \qquad G = \{(0, M)\}.$$

It has two kinds of trajectories, depending on the start state m_0 (see Fig 2):

1. When $m_0 = 0$, there is a refill followed by a decay $f(t) = M * e^{-t}$.
2. When $m_0 > 0$, there is a decay $f(t) = m_0 * e^{-t}$. Thus, $f(t) > 0$ when $t \geq 0$, and $f(t) \to 0$ as $t \to +\infty$.

The timed transition relation $\xrightarrow[\mathcal{H}_D]{}$ consists of the transitions

- $0 \xrightarrow{0} M$, and
- $m \xrightarrow{d} m'$ with $0 < d$ and $m > m' = m * e^{-d} > 0$.

Adding $(0,0)$ to F entails the addition of the transitions $0 \xrightarrow{d} 0$ with $d > 0$.

Example 2.8 (Bouncing ball). The HS $\mathcal{H}_B$ on $\mathbb{R}^2$ describes a bouncing ball with height $h \geq 0$ and velocity v, which is kicked when it stops, i. e., when $h = v = 0$. Its flow and jump relations depend on a coefficient of restitution b (we do not restrict its value, but $b{:}[-1, 0]$ would be the obvious restriction), and a velocity $V > 0$ given to the ball when it is kicked. We assume the force of gravity to be -1 (for the sake of simplicity). Formally:

- $F = \{((h, v), (\dot{h}, \dot{v}))|h > 0 \wedge \dot{h} = v \wedge \dot{v} = -1\}$.
- $G = \{((0, v), (0, v^+))|v < 0 \wedge v^+ = b * v\} \uplus \{((0, 0), (0, V))\}$.

It has seven kinds of trajectories starting from $(h = 0, v > 0)$, depending on the value of b (see Fig 3).

1. When $b < -1$, the ball never stops (its energy increases at each bounce).
2. When $b = -1$, the ball never stops (its energy remains constant).
3. When $b{:}(-1, 0)$, the ball stops in finite time, but after infinitely many bounces (this is a **Zeno behavior**), then it is kicked, i. e., $(h = 0, v = V)$.
4. When $b = 0$, the ball stops as it hits the ground, then it is kicked.
5. When $b{:}(0, 1)$, as the ball hits the ground, it stops after infinitely many instantaneous slowdowns $0 > b^n * v \to 0$ (this is a **chattering Zeno behavior**), then it is kicked.
6. When $b = 1$, as the ball hits the ground, the trajectory cannot progress further in time.
7. When $b > 1$, as the ball hits the ground, its velocity drifts to $-\infty$ after an infinite sequence of instantaneous accelerations $0 > b^n * v \to -\infty$, and the trajectory cannot progress further in time.

The timed transition relation $\xrightarrow[\mathcal{H}_B]{}$ consists of the following transitions:

- $(0, v) \xrightarrow{0} (0, v')$ with $v < 0$ and $v' = b * v$, this is a bounce;
- $(0, 0) \xrightarrow{0} (0, V)$, this is when the ball is kicked;
- $(h, v) \xrightarrow{d} (h', v')$, with $0 < d$ and $0 \leq h, h' = h + v * d - \frac{d^2}{2} \wedge v' = v - d$, this is when the ball moves while the energy $E(h, v) = h + \frac{v^2}{2}$ stays constant.

In particular, $(0, v) \xrightarrow{2*v} (0, -v)$ is the transition between two bounces. Adding $\{((0, v), (\dot{h}, \dot{v}))|\dot{h} = v \wedge \dot{v} = -1\}$ to F does not change the timed transitions, while adding $((0, 0), (0, 0))$ to G entails the addition of $(0, 0) \xrightarrow{0} (0, 0)$.

The following construction adds a clock to a HS to record the passing of time.

Definition 2.9. Given a HS $\mathcal{H} = (F, G)$ on $\mathbb{S}$, the derived HS $t(\mathcal{H}) = (F', G')$ on $\mathbb{R} \times \mathbb{S}$ *adds* a clock to $\mathcal{H}$, namely:

- $F' \triangleq \{((t, s), (1, \dot{s})) \mid s\, F\, \dot{s}\}$, because $dt/dt = 1$;
- $G' \triangleq \{((t, s), (t, s^+)) \mid s\, G\, s^+\}$, because jumps are instantaneous.

Proposition 2.10. $(t, s) \xrightarrow[t(\mathcal{H})]{d} (t', s') \iff t' = t + d \wedge s \xrightarrow[\mathcal{H}]{d} s'$.

Proof. Only the case $d > 0$ is non-trivial.

- If f':**Top**$([0, d], \mathbb{R} \times \mathbb{S})$ realizes the transition $(t, s) \xrightarrow[t(\mathcal{H})]{d} (t', s')$, then $f'(x) = (t + x, f(x))$ for a unique f:**Top**$([0, d], \mathbb{S})$, and moreover this f realizes the transition $s \xrightarrow[\mathcal{H}]{d} s'$.
- Conversely, if f:**Top**$([0, d], \mathbb{S})$ realizes $s \xrightarrow[\mathcal{H}]{d} s'$, then $f'(x) = (t + x, f(x))$ realizes $(t, s) \xrightarrow[t(\mathcal{H})]{d} (t', s')$. □

3. Evolution and Reachability

Transition systems (TS for short) provide the main formalism for modeling discrete systems. The formalism does not mention time explicitly, but it assumes that time is discrete, and each transition takes one time unit (or alternatively, it abstracts from time and describes only the order of discrete state changes).

Given a TS $(\mathbb{S}, \to)$, i. e., a binary relation $\to$ on a set $\mathbb{S}$ (aka a directed graph), we identify the *discrete time line* with the set $\mathbb{N}$ of natural numbers and define the following notions related to the TS.

- A trajectory (called trace in a discrete setting) is a map f:**Set**$([0, n], \mathbb{S})$ s. t. $\forall i < n.f(i) \to f(i + 1)$ for some n:$\mathbb{N}$, or equivalently, a path f:$\mathbb{S}^+$ in the graph. The length of f is n and $f(0)$ is its starting state.
- The evolution map Ef:$\mathsf{P}(\mathbb{S}) \to \mathsf{P}(\mathbb{N} \times \mathbb{S})$ is $\mathsf{Ef}(I) \triangleq \{(n, s') | \exists s{:}I.s \to^n s'\}$, or equivalently the union of (the graphs of) all trajectories starting from the set I of initial states. Therefore, $\mathsf{Ef}(I)$ says at what time a state is reached, but forgets the trajectories used to reach it. However, when $\to$ is deterministic, there is at most one trajectory of length n from s to s', which can be recovered from $\mathsf{Ef}(\{s\})$.
- The reachability map Rf:$\mathsf{P}(\mathbb{S}) \to \mathsf{P}(\mathbb{S})$ is $\mathsf{Rf}(I) \triangleq \{s' | \exists s{:}I.s \to^* s'\}$, or equivalently $\{s' | \exists n.(n, s'){:}\mathsf{Ef}(I)\}$. Therefore, $\mathsf{Rf}(I)$ says whether a state is reachable from I, but forgets at which time instances it is reached.

For TTTS (and HS) one would like to reuse as much as possible the theory available for TS. The main point of this section is that naive reuse can result under-approximating what is reachable in finite time. To address this problem, we present a solution that computes an over-approximation (see Sec 3.1). This solution exploits the topological structure of the state space $\mathbb{S}$ and the continuous time line $\mathbb{T}$.

We choose to cast analyses (like reachability) as monotonic maps (like Rf) rather than as relations (like $\rightarrow^*$). This becomes essential in Def 3.6 and for defining approximability (Sec 5) and robustness (Sec 4) of an analysis.

Definition 3.1. The **evolution** map $\mathsf{Ef}{:}\mathsf{P}(\mathbb{S}) \to \mathsf{P}(\mathbb{T}\times\mathbb{S})$ and the **reachability** map $\mathsf{Rf}{:}\mathsf{P}(\mathbb{S}) \to \mathsf{P}(\mathbb{S})$ for a TTTS $(\mathbb{S}, \longrightarrow)$ are:

- $\mathsf{Ef}(I) \triangleq$ the smallest $S{:}\mathsf{P}(\mathbb{T}\times\mathbb{S})$ s. t. $\{0\}\times I \subseteq S$ and S is *closed* w. r. t. timed transitions, i. e., $(t,s){:}S \wedge s \xrightarrow{d} s' \implies (t+d, s'){:}S$.
- $\mathsf{Rf}(I) \triangleq$ the smallest $S{:}\mathsf{P}(\mathbb{S})$ s. t. $I \subseteq S$ and S is *closed* w. r. t. transitions, i. e., $s{:}S \wedge s \longrightarrow s' \implies s'{:}S$.

We denote with $\mathsf{Ef}_{\mathcal{H}}$ and $\mathsf{Rf}_{\mathcal{H}}$ the evolution and reachability maps for the TTTS induced by the HS $\mathcal{H}$.

Remark 3.2. The f in Ef and Rf stands for finite, because these maps consider only states that are reachable in **finitely many** transitions. There is an important difference between discrete systems and continuous/hybrid systems. In a discrete (time) system the transition relation suffices to define trajectories, the evolution, and the reachability maps. In a continuous (time) system: to define trajectories, the structure of a HS is needed; to define the evolution map, the timed transition relation suffices; and to define the reachability map, the transition relation suffices.

Theorem 3.3. *The following properties hold:*

1. Ef *is monotonic, i. e.,* $I_0 \subseteq I_1 \implies \mathsf{Ef}(I_0) \subseteq \mathsf{Ef}(I_1)$*, and preserves unions, i. e.,* $\forall K \subseteq \mathsf{P}(\mathbb{S}).\mathsf{Ef}(\cup K) = \cup\{\mathsf{Ef}(I) | I{:}K\}$.
2. Rf *is monotonic, preserves unions, is a closure, i. e.,* $I \subseteq \mathsf{Rf}(I) = \mathsf{Rf}^2(I)$*, and* $\pi(\mathsf{Ef}(I)) = \mathsf{Rf}(I)$.
3. *If* $\mathcal{H}$ *is a HS on* $\mathbb{S}$*, then* $\forall I{:}\mathsf{P}(\mathbb{S}).\mathsf{Ef}_{\mathcal{H}}(I) = \mathsf{Rf}_{t(\mathcal{H})}(\{0\}\times I)$ *and* $\forall J{:}\mathsf{P}(\mathbb{R}\times\mathbb{S}).\pi(\mathsf{Rf}_{t(\mathcal{H})}(J)) = \mathsf{Rf}_{\mathcal{H}}(\pi(J))$.

Here, $\pi{:}\mathbb{R}\times\mathbb{S} \longrightarrow \mathbb{S}$ *is* $\pi(t,s) \triangleq s$*, and* $\pi(J)$ *is the image of* $J \subseteq \mathbb{R}\times\mathbb{S}$.

Proof. See Appendix A.

A pair (t, s') is in $\mathsf{Ef}_{\mathcal{H}}(I)$ exactly when s' is reached at time t in finitely many transitions starting from some $s{:}I$. In *Zeno systems* there are states that are reached at a finite time t, but not in a finite number of transitions. Therefore, $\mathsf{Ef}_{\mathcal{H}}$ and $\mathsf{Rf}_{\mathcal{H}}$ may under-approximate what we would like to compute.

Definition 3.4. A **Zeno behavior** of $\mathcal{H}$ is a sequence $((d_n, s_n)|n{:}\omega)$ in $\mathbb{T} \times \mathbb{S}$ s. t. :

1. $\forall n.s_n \xrightarrow[\mathcal{H}]{d_n} s_{n+1}$,
2. $d \triangleq \sum_{n:\omega} d_n$ is defined and finite, and,
3. the sequence has infinitely many jumps, i. e., $\{n|d_n = 0\}$ is infinite.

The last requirement excludes *fragmentation* of a flow transition $s \xrightarrow[\mathcal{H}]{d} s'$, i. e., sequences $((f(t_n), t_{n+1} - t_n)|n{:}\omega)$, where $f{:}\mathbf{Top}([0,d], \mathbb{S})$ realizes $s \xrightarrow[\mathcal{H}]{d} s'$, and $(t_n|n{:}\omega)$ is a strictly increasing sequence with $t_0 = 0$ and $\sup_{n:\omega} t_n = d$.

The accumulation points of $(s_n|n{:}\omega)$ in the topological space $\mathbb{S}$ are called the **Zeno points**, and d is called the **Zeno time**, since it is the time needed to reach a Zeno point from s_0.

$\mathcal{H}_B$ of Example 2.8 is the classical case of a HS with Zeno behavior. When b is in the interval $(-1, 0)$, the stop state $s = (0, 0)$ is reached in finite time from $s_0 = (0, v)$ with $v < 0$, but after infinitely many bounces (see Fig 3 in Sec 7). When b is in the interval $(0, 1)$, $\mathcal{H}_B$ has a chattering Zeno behavior, i. e., the stop state is reached after infinitely many instantaneous slowdowns. On the other hand, Prop 3.5 shows that the stop state is not in $\mathsf{Rf}_{\mathcal{H}_B}(\{s_0\})$ when $b \neq 0$.

Proposition 3.5. *Let* $S \triangleq \{(h, v)|h \geq 0 \wedge E(h, v) > 0\}$*, where* $E(h, v) = h + \frac{v^2}{2}$ *is the energy in state* (h, v)*. Then,* $\mathsf{Rf}_{\mathcal{H}_B}(S) = S$*, provided that* $b \neq 0$*.*

Proof. We prove that S is closed w. r. t. the transition relation $\xrightarrow[\mathcal{H}_B]{}$ by case analysis. There are three cases:

- bounce, i. e., $(0, v) \longrightarrow (0, b * v)$ with $v < 0$: $(0, v){:}S$, because $E(0, v) = \frac{v^2}{2} > 0$, and $(0, b * v){:}S$, because $E(0, b * v) > 0$ when $b \neq 0$;
- ball kicked, i. e., $(0, 0) \longrightarrow (0, V)$: there is nothing to prove, as $(0, 0) \notin S$;
- move, i. e., $(h, v) \longrightarrow (h', v')$ with $h, h' \geq 0 \wedge v > v' \wedge E(h, v) = E(h', v')$: $(h, v){:}S \implies (h', v'){:}S$ holds, because the energy stays constant. □

We propose a key change to Def 3.1 that exploits the topology on $\mathbb{S}$ and $\mathbb{T}$ by considering reachable also a state that is *arbitrarily close* to reachable states.

Definition 3.6 (Safe maps). Let $\mathsf{C}(\mathbb{S})$ be the set of **closed subsets** of a topological space $\mathbb{S}$. The **safe evolution** map $\mathsf{Es}{:}\mathsf{C}(\mathbb{S}) \to \mathsf{C}(\mathbb{T} \times \mathbb{S})$ and the **safe reachability** map $\mathsf{Rs}{:}\mathsf{C}(\mathbb{S}) \to \mathsf{C}(\mathbb{S})$ for a TTTS $(\mathbb{S}, \longrightarrow)$ are:

- $\mathsf{Es}(I) \triangleq$ the smallest $S{:}\mathsf{C}(\mathbb{T} \times \mathbb{S})$ s. t. $\{0\} \times I \subseteq S$ and *closed* w. r. t. timed transitions.
- $\mathsf{Rs}(I) \triangleq$ the smallest $S{:}\mathsf{C}(\mathbb{S})$ s. t. $I \subseteq S$, and *closed* w. r. t. transitions.

We denote with $\mathsf{Es}_{\mathcal{H}}$ and $\mathsf{Rs}_{\mathcal{H}}$ the safe evolution and safe reachability maps for the TTTS induced by the HS $\mathcal{H}$, respectively.

Remark 3.7. If $s_0{:}I$ and $((d_n, s_n)|n{:}\omega)$ is a Zeno behavior of $\mathcal{H}$, then the set $S = \mathsf{Rs}_{\mathcal{H}}(I)$ includes every Zeno point s. In fact, the sequence $(s_n|n{:}\omega)$ is included in S, and all its accumulation points must be in S, because S is closed. More generally, $S = \mathsf{Rs}_{\mathcal{H}}(I)$ and $E = \mathsf{Es}_{\mathcal{H}}(I)$ have the following properties:

- If $s_0{:}I$, $\forall n.s_n \xrightarrow[\mathcal{H}]{d_n} s_{n+1}$ and s is an accumulation point of $(s_n|n{:}\omega)$, then $s{:}S$, moreover $(d, s){:}E$ when $d = \sum_{n:\omega} d_n < +\infty$. We call this property of S *path completion* and $d = \sum_{n:\omega} d_n$ the *duration* of the path. When $d = +\infty$, the states added by path completion are *asymptotically reachable*, but may not be reachable in finite time.

- If $s_0{:}I$, $\forall n.s_0 \xrightarrow[\mathcal{H}]{d_n} s_{n+1}$ and s is an accumulation point of $(s_n|n{:}\omega)$, then $s{:}S$, moreover $(d, s){:}E$ when d is an accumulation point of $(d_n|n{:}\omega)$. We call this property of S *non-deterministic completion*.

Among the states added by these two forms of completions, only those added by path completion of a path of finite duration should be considered reachable, the others are spurious additions due to the definition of safe reachability. The two completions can occur also in purely continuous systems.

1. Let $f{:}\mathbf{Top}([0, d), \mathbb{R})$ be the map $f(t) = \sin(\frac{1}{t-d})$, then
   - the derivative $\dot{f}$ of f is defined and continuous in $(0, d)$, but
   - there is no way to extend f to a continuous map on $[0, d]$.

   If $\mathcal{H}$ on $\mathbb{R}^2$ has flow relation $F = \{((x, f(x)), (1, \dot{f}(x)))|0 < x < d\}$, then $\mathsf{Rs}_{\mathcal{H}}(\{(0, f(0))\}) = \{(x, f(x))|0 \leq x < d\} \uplus \{(d, y)| - 1 \leq y \leq 1\}$, where path completion adds the states (d, y).
2. If $\mathcal{H}$ on $\mathbb{R}^2$ has flow relation $F = \{((x, y), (1, v))|0 \leq x, y < d \wedge 0 \leq v < 1\}$, then $\mathsf{Rs}_{\mathcal{H}}(\{(0, 0)\}) = \{(x, y)|0 \leq y \leq x \leq d\}$, where non-deterministic completion adds the states (x, x) for $x > 0$.

There is an analogue of Thm 3.3 for the safe maps, but with weaker properties, mainly because the set of closed subsets is closed only w. r. t. finite unions.

Theorem 3.8. *The following properties hold:*

1. Es *is monotonic and preserves finite unions.*
2. Rs *is monotonic, preserves finite unions, is a closure, and* $\pi(\mathsf{Es}(I)) \subseteq \mathsf{Rs}(I)$.
3. $\forall I{:}\mathsf{P}(\mathbb{S}).\mathsf{Ef}(I) \subseteq \mathsf{Es}(\overline{I})$, *and* $\forall I{:}\mathsf{P}(\mathbb{S}).\mathsf{Rf}(I) \subseteq \mathsf{Rs}(\overline{I})$.
4. *If* $\mathcal{H}$ *is a HS on* $\mathbb{S}$, *then* $\forall I{:}\mathsf{C}(\mathbb{S}).\mathsf{Es}_{\mathcal{H}}(I) = \mathsf{Rs}_{t(\mathcal{H})}(\{0\} \times I)$, *and* $\forall J{:}\mathsf{C}(\mathbb{R} \times \mathbb{S}).\pi(\mathsf{Rs}_{t(\mathcal{H})}(J)) \subseteq \mathsf{Rs}_{\mathcal{H}}(\overline{\pi(J)})$.

Here, $\overline{S}{:}\mathsf{C}(\mathbb{S})$ *is the* ***closure*** *of* $S{:}\mathsf{P}(\mathbb{S})$, *i. e., the smallest* $S'{:}\mathsf{C}(\mathbb{S})$ *s. t.* $S \subseteq S'$.

Proof. See Appendix A.

3.1. Summary of inclusion relations

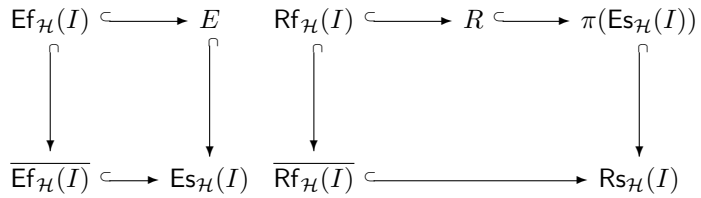
We give a summary of the inclusion relations among the sets computed by the four maps defined in this section. Given a HS $\mathcal{H}$ on $\mathbb{S}$ and a set $I{:}\mathsf{C}(\mathbb{S})$ of initial states, there are two *informally defined* subsets $E{:}\mathsf{P}(\mathbb{T}\times\mathbb{S})$ and $R{:}\mathsf{P}(\mathbb{S})$:

- E set of (t,s) s. t. s is reached at time t, i. e., there is a *trajectory* of $\mathcal{H}$ starting from a state in I and reaching s at time t.
- R set of states reachable (from I) in finite time, i. e., $R=\pi(E)$.

The monotonic maps in Def 3.1 and 3.6 allow to define four subsets:

- $\mathsf{Ef}_{\mathcal{H}}(I)$: set of (t,s) s. t. s is reached at time t in finitely many transitions.
- $\mathsf{Rf}_{\mathcal{H}}(I)$: set of states reachable in finitely many transitions, i. e., $\pi(\mathsf{Ef}_{\mathcal{H}}(I))$.
- $\mathsf{Es}_{\mathcal{H}}(I){:}\mathsf{C}(\mathbb{T}\times\mathbb{S})$ a closed over-approximation of E.
- $\mathsf{Rs}_{\mathcal{H}}(I){:}\mathsf{C}(\mathbb{S})$ a closed over-approximation of R.

The inclusion relations among these six subsets are:



By suitable choices of closed HS $\mathcal{H}$ on $\mathbb{R}$ and singletons I we show that no other inclusion holds. In particular, $\mathsf{Ef}_{\mathcal{H}}$ and $\mathsf{Rf}_{\mathcal{H}}$ may compute proper under-approximations, while $\mathsf{Es}_{\mathcal{H}}$ and $\mathsf{Rs}_{\mathcal{H}}$ may compute proper over-approximations.

1. $\mathsf{Ef}_{\mathcal{H}}(I)\subset\overline{\mathsf{Ef}_{\mathcal{H}}(I)}\subset E=\mathsf{Es}_{\mathcal{H}}(I)$ and $\mathsf{Rf}_{\mathcal{H}}(I)\subset\overline{\mathsf{Rf}_{\mathcal{H}}(I)}\subset R=\mathsf{Rs}_{\mathcal{H}}(I)$.
   Take $\mathcal{H}=(\emptyset,G)$ with $G\triangleq\{(x,x/2)|0\le x\}\uplus\{(0,2)\}$ and $I=\{1\}$, then
   - $\mathsf{Rf}_{\mathcal{H}}(I)=\{2^{-n}|n{:}\mathbb{N}\}$ and $\mathsf{Ef}_{\mathcal{H}}(I)=\{0\}\times\mathsf{Rf}_{\mathcal{H}}(I)$
   - $\overline{\mathsf{Rf}_{\mathcal{H}}(I)}=\{2^{-n}|n{:}\mathbb{N}\}\uplus\{0\}$ and $\overline{\mathsf{Ef}_{\mathcal{H}}(I)}=\{0\}\times\overline{\mathsf{Rf}_{\mathcal{H}}(I)}$
   - $\mathsf{Rs}_{\mathcal{H}}(I)=\{2^{-n}|n{:}\mathbb{N}\}\uplus\{0,2\}$ and $\mathsf{Es}_{\mathcal{H}}(I)=\{0\}\times\mathsf{Rs}_{\mathcal{H}}(I)$
2. $\mathsf{Ef}_{\mathcal{H}}(I)=E\subset\overline{\mathsf{Ef}_{\mathcal{H}}(I)}\subset\mathsf{Es}_{\mathcal{H}}(I)$ and $\mathsf{Rf}_{\mathcal{H}}(I)=R\subset\overline{\mathsf{Rf}_{\mathcal{H}}(I)}\subset\pi(\mathsf{Es}_{\mathcal{H}}(I))$.
   Take $\mathcal{H}=(\emptyset,G)$ with $G\triangleq\{(2,x)|x\ge 2\}\uplus\{(x,1/x)|x\ge 2\}\uplus\{(0,1)\}$ and $I=\{2\}$, then
   - $\mathsf{Rf}_{\mathcal{H}}(I)=[2,+\infty)\uplus(0,1/2]$ and $\mathsf{Ef}_{\mathcal{H}}(I)=\{0\}\times\mathsf{Rf}_{\mathcal{H}}(I)$
   - $\overline{\mathsf{Rf}_{\mathcal{H}}(I)}=[2,+\infty)\uplus[0,1/2]$ and $\overline{\mathsf{Ef}_{\mathcal{H}}(I)}=\{0\}\times\overline{\mathsf{Rf}_{\mathcal{H}}(I)}$
   - $\mathsf{Rs}_{\mathcal{H}}(I)=[2,+\infty)\uplus[0,1/2]\uplus\{1\}$ and $\mathsf{Es}_{\mathcal{H}}(I)=\{0\}\times\mathsf{Rs}_{\mathcal{H}}(I)$
3. $\mathsf{Rf}_{\mathcal{H}}(I)=R=\pi(\mathsf{Es}_{\mathcal{H}}(I))\subset\overline{\mathsf{Rf}_{\mathcal{H}}(I)}\subset\mathsf{Rs}_{\mathcal{H}}(I)$.
   Take $\mathcal{H}=(F,\{(0,2)\})$ with $F\triangleq\{(x,-x)|0\le x\}$ and $I=\{1\}$, then
   - $\mathsf{Ef}_{\mathcal{H}}(I)=E=\mathsf{Es}_{\mathcal{H}}(I)=\{(t,e^{-t})|0\le t\}$
   - $\mathsf{Rf}_{\mathcal{H}}(I)=(0,1]$
   - $\overline{\mathsf{Rf}_{\mathcal{H}}(I)}=[0,1]$
   - $\mathsf{Rs}_{\mathcal{H}}(I)=[0,2]$

4. Robustness

In this section we define when an analysis is robust (Def 4.1). The definition assumes that the analysis is cast as a monotonic map $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$ between *hyper-spaces* consisting of closed subsets of a metric space. Intuitively, A is *robust* at C when *small extensions* to the subset C cause small extensions to $A(C)$. When an analysis is not robust, and this is often the case, one may want to replace it with a robust over-approximation. We give sufficient conditions on the underlying metric spaces, which ensure that every monotonic map has a *best robust approximation* (Corr 4.4). There are two problems in relation to the reachability (and evolution) maps defined in Sec 3:

- Robustness of $\mathsf{Rs}_{\mathcal{H}}$ says only that small extensions to the set of initial states cause small extensions to the set of reachable states, but it does not say what happens when *small extensions* to $\mathcal{H}$ are allowed.
- Corr 4.4 is not directly applicable to $\mathsf{Rs}_{\mathcal{H}}$, because the only Banach space satisfying its conditions is the trivial one, i. e., $\mathbb{R}^0$.

These problems are better addressed by moving to the category **Po** of complete lattices and monotonic maps (Sec 5). In fact, reachability maps are arrows in **Po**, and within **Po** one can easily derive other arrows, to which Corr 4.4 applies.

Definition 4.1 (Robustness). Given a metric space $(\mathbb{S}, d)$ the **δ-fattening** $S_\delta{:}\mathsf{C}(\mathbb{S})$ of $S{:}\mathsf{P}(\mathbb{S})$ is the closure of the open set $B(S,\delta) \triangleq \{y | \exists x{:}S.d(x,y) < \delta\}$. Given a monotonic map $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$ with $\mathbb{S}_1$ and $\mathbb{S}_2$ metric spaces

- A is **robust** at $C{:}\mathsf{C}(\mathbb{S}_1) \stackrel{\triangle}{\iff} \forall \epsilon > 0. \exists \delta > 0. A(C_\delta) \subseteq A(C)_\epsilon$
- A is **robust** $\stackrel{\triangle}{\iff}$ A is robust at every $C{:}\mathsf{C}(\mathbb{S}_1)$.

Robustness becomes trivial when $\mathbb{S}_1$ is *discrete* (i. e., $d(x,y) = 1$ when $x \neq y$), because $\mathsf{C}(\mathbb{S}_1) = \mathsf{P}(\mathbb{S}_1)$ and any monotonic map $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$ is robust.

Remark 4.2. The subset $B(S,\delta)$ is the semantic counterpart of the formula $\phi_\delta(x) \triangleq (\exists y.\phi(y) \wedge d(x,y) < \delta)$, which adds noise up to δ to a formula $\phi(x)$ with one free variable x, where $d(x,y)$ is a term defining a distance (see [13]). There is no reason for the interpretation of formulas to be closed, and we could define robustness also for monotonic maps $A{:}\mathsf{P}(\mathbb{S}_1) \to \mathsf{P}(\mathbb{S}_2)$ on subsets, namely A is **robust** at $S{:}\mathsf{P}(\mathbb{S}_1) \stackrel{\triangle}{\iff} \forall \epsilon > 0. \exists \delta > 0. A(S_\delta) \subseteq A(S)_\epsilon$. However, the main reasons to focus on maps acting only on closed subsets are:

1. The notion of δ-fattening cannot distinguish two subsets of $\mathbb{S}$ with the same closure, namely $B(S,\delta) = B(\overline{S},\delta)$ and $S_\delta = \overline{S}_\delta$.
2. One can replace A with the map $\overline{A}{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$ given by $\overline{A}(C) \triangleq \overline{A(C)}$, that satisfies $\forall S{:}\mathsf{P}(\mathbb{S}_1).\overline{A(S)} = \overline{A}(\overline{S})$ when A is robust.

In safety analysis one has also a subset U of *unsafe* states, and *safety* means that $A(S)$ and U are disjoint. By analogy with [19], we define δ-*safety* to mean that $A(S_\delta)$ and U_δ are disjoint. Since A is monotonic, δ-safety implies safety. If A is robust at S and U is compact, then the converse hold, namely, safety implies δ-safety for some δ.

Example 4.3. One may ask whether the safe reachability map $\mathsf{Rs}_{\mathcal{H}}$ or the safe evolution map $\mathsf{Es}_{\mathcal{H}}$ for a HS $\mathcal{H}$ on the Banach space $\mathbb{S}$ are robust. More generally, the question makes sense for safe reachability Rs and safe evolution Es (see Def 3.6) for a TTTS $\longrightarrow$ on a metric space $\mathbb{S}$. With the definition of robustness in Remark 4.2 the question makes sense also for reachability Rf and evolution Ef (see Def 3.1) for a TTTS $\longrightarrow$ on a metric space $\mathbb{S}$. We check robustness of $\mathsf{Rs}_{\mathcal{H}}$ and $\mathsf{Rf}_{\mathcal{H}}$ for the HS on $\mathbb{R}$ introduced in Sec 2:

- for $\mathcal{H}_E$ of Example 2.6 $\mathsf{Rf}_{\mathcal{H}}$ and $\mathsf{Rs}_{\mathcal{H}}$ are not robust at $[0]$, since $\mathsf{Rf}_{\mathcal{H}}([0]) = \mathsf{Rs}_{\mathcal{H}}([0]) = [0]$ and $\mathsf{Rf}_{\mathcal{H}}([0]_\delta) = \mathsf{Rs}_{\mathcal{H}}([0]_\delta) = [-\delta, M]$ when $\delta \leq M$.
- for $\mathcal{H}_D$ of Example 2.7 $\overline{\mathsf{Rf}_{\mathcal{H}}}$ and $\mathsf{Rs}_{\mathcal{H}}$ are robust, but $\mathsf{Rf}_{\mathcal{H}}$ is not robust at $(0, m]$ when $0 < m < M$, since $\mathsf{Rf}_{\mathcal{H}}((0, m]) = (0, m]$ and $\mathsf{Rf}_{\mathcal{H}}((0, m]_\delta) = [-\delta, M]$ when $m + \delta \leq M$.

Robustness is a desirable property, but it does not come for free. We state a useful corollary, whose proof hinges on two more general results:

1. The first result (Thm A.4) states that, under certain assumptions, robustness is equivalent to *Scott continuity*. This equivalence is crucial to recasting order-theoretic results in term of robustness.
2. The second result (Thm 5.15) states that every monotonic map $A{:}X \to Y$ between complete lattices has a *best Scott continuous approximation* $A^{\boxdot}$. Moreover, $A^{\boxdot}(x) = \bigsqcup\{A(b) | b \ll_X x\}$ (Thm 5.20), when X is a *continuous lattice*, and $\ll_X$ is its *way-below* relation.

Corollary 4.4. *If $\mathbb{S}_1$ and $\mathbb{S}_2$ are compact metric spaces, then any monotonic map $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$ has a* ***best robust approximation*** *$A^{\boxdot}{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$. That is $A^{\boxdot}$ is the smallest, w. r. t. the point-wise inclusion order $A_1 \subseteq A_2$, among the monotonic maps A' that are robust and approximate A (i. e., $A \subseteq A'$).*

Moreover, $A^{\boxdot}(C) = \bigcap\{A(C_\delta) | \delta > 0\}$, and $A^{\boxdot}(C) \subseteq A'(C)$ when A' is a monotonic map, which is robust at C and approximates A.

Proof. See Appendix Appendix A.1. □

Every reachability map $R{:}\mathsf{C}(\mathbb{S}) \to \mathsf{C}(\mathbb{S})$ is idempotent, i. e., $R = R^2$, but for $R^{\boxdot}$ one has only that $R \subseteq R^{\boxdot} \subseteq R^{\boxdot} \circ R^{\boxdot}$. However, another general result on Scott continuous maps (Thm 5.15) ensures the existence of a robust approximation of R, which is also idempotent.

Corollary 4.5. *If $\mathbb{S}$ is a compact metric space, then every monotonic map $A{:}\mathsf{C}(\mathbb{S}) \to \mathsf{C}(\mathbb{S})$ has a* ***best approximation*** *$A_{\boxplus}{:}\mathsf{C}(\mathbb{S}) \to \mathsf{C}(\mathbb{S})$ among the approximations A_+ of A that are robust and satisfy $\forall C{:}\mathsf{C}(\mathbb{S}).C \subseteq A_+(C) = A_+^2(C)$.*

PROOF. See Appendix Appendix A.1. □

For discrete metric spaces the notion of robustness is not interesting, because every monotonic map is robust. In the case of compact metric spaces Corr 4.4 provides a systematic way of getting the best robust approximation of a monotonic map. In all other cases robustness is an interesting notion, but a best robust approximation may not exist, as shown by the following example.

Example 4.6. Consider the non-compact metric space $\mathbb{R}$ and the monotonic map $A{:}\mathsf{C}(\mathbb{R}) \to \mathsf{C}(\mathbb{R})$ given by $A(C) \triangleq \{x | \exists n.x_n{:}C \wedge x \geq n\}$, where $(x_n|n{:}\omega)$ is a sequence in $\mathbb{R}$ with limit 0 s. t. $\forall n.0 < x_{n+1} < x_n$, e. g., $x_n = 2^{-n}$, then

- $A([0]_{x_n}) = A([x_n]) = \{x | x \geq n\}$
- $A([0]) = \emptyset$, thus A is not robust at $[0]$
- $\bigcap\{A([0]_\delta)|\delta > 0\} = \emptyset$.

Let $A_n{:}\mathsf{C}(\mathbb{R}) \to \mathsf{C}(\mathbb{R})$ be the monotonic map $A_n(C) \triangleq A([x_n]) \cup A(C)$, then

- $A(C) \subseteq A_{n+1}(C) \subseteq A_n(C)$, thus $(A_n|n{:}\omega)$ is a decreasing sequence of monotonic maps approximating A
- A_n is robust, since $A(C)$ depends only on which x_i with $i < n$ are in C
- $A_n([0]) = A_n([0]_{x_n}) = A([0]_{x_n}) = \{x | x \geq n\}$
- $A([0]) = \bigcap\{A_n([0])|n{:}\omega\}$.

If A' were a best robust approximation of A, then we get a contradiction. In fact, every A_n approximates A', thus $A'([0]) = \emptyset$, moreover A' approximates A, thus $\{x | x \geq n\} \subseteq A'([0]_{x_n})$.

5. A Framework for Approximability

This section introduces the category **Po** of complete lattices and monotonic maps, and uses it as a framework for a number of purposes. We present only the category-theoretic and order-theoretic background needed for establishing the relevant results, but we illustrate the intuition behind formal definitions through informal prose and appropriate examples.

Notation 5.1. Complete lattices are posets, and a poset X is a pair (S, R), in which S is the underlying set, and $R \subseteq S \times S$ is a reflexive, anti-symmetric, and transitive binary relation on S. We usually denote R as $\leq_X$, or $\leq$ when X is clear from the context, while for S we use the notation $|X|$.

The main reasons for choosing **Po** as framework are:

Abstraction. Po allows to cast definitions and prove results at the appropriate level of abstraction, focusing on the bare essentials needed, thus avoiding the reworking of concrete instances of more abstract and general theorems.

For instance, the appropriate level of abstraction to define reachability maps and prove their properties is that of (topological) transition systems.

By composition with a monotonic map (Def 5.7) from a complete lattice $\mathbb{H}(\mathbb{S})$ of hybrid systems (on a Banach space) to a complete lattice $\mathbb{P}(\mathbb{S}^2)$ of (topological) transition systems (on a topological space), one can turn definitions on $\mathbb{P}(\mathbb{S}^2)$ into definitions on $\mathbb{H}(\mathbb{S})$.

Approximation. The order relation (on a complete lattice) allows to express when something is an over- or under-approximation of something else, and one can choose different order relations on the same underlying set.

For instance, on the set $\mathsf{P}(\mathbb{S})$ of subsets of $\mathbb{S}$ the obvious order relation is subset inclusion, but we choose reverse inclusion to express that a smaller over-approximation is *more informative* than a bigger one.

Optimality. Po is the natural setting for defining and comparing *abstract interpretations* [8]. In particular, adjunctions (aka Galois connections) give a systematic way to move from a concrete to a more abstract *semantic domain* and back. When the abstract domain is identified with a subset of the concrete domain, adjunctions provide a rigorous formalization of *best approximation*.

Generality. Category theory provides general machinery, like cartesian closed categories, for interpreting simply typed lambda-calculus, and the dual concepts of initial algebra and final co-algebra, for interpreting inductive and co-inductive definitions. Posets amount to categories where there is at most one arrow between two objects. Thus, category-theoretic concepts and results apply both to the category **Po** and to its objects.

Several maps can be viewed as arrows in **Po**. For instance, adding a clock to a HS (Def 2.9) is a monotonic map from $\mathbb{H}(\mathbb{S})$ to $\mathbb{H}(\mathbb{R} \times \mathbb{S})$.

The evolution and reachability maps in Def 3.1 and 3.6 are monotonic maps between complete lattices of (closed) subsets of a topological space. It is not difficult to see the inductive nature of their definitions, thus in **Po** they can be defined from more elementary arrows and a fix-point operator.

Since **Po** is cartesian closed, one can use the simply typed lambda-calculus for defining more complex arrows from simpler ones.

Definition 5.2 (Po, dual, adjunction, algebra, co-algebra).

1. The category **Po** is defined as follows:
   - Objects X:**Po** are **complete lattices**, i. e., posets $(|X|, \leq_X)$ s. t. each subset S of $|X|$ has a **sup**, denoted by $\bigsqcup S$. In particular, $\bot_X \triangleq \bigsqcup \emptyset$ denotes the least element of X.

- Arrows $f{:}\mathbf{Po}(X,Y)$ from X to Y, denoted $X \xrightarrow{f} Y$, are **monotonic** maps $f{:}|X| \to |Y|$, i. e., $\forall x_0, x_1{:}|X|.x_0 \leq_X x_1 \implies f(x_0) \leq_Y f(x_1)$.

2. Given $X = (|X|, \leq_X){:}\mathbf{Po}$, its **dual** X^{op} is $(|X|, \geq_X)$, i. e., the poset X with the order reversed.
3. An **adjunction** $f \dashv g$ is a pair of maps $X \underset{g}{\overset{f}{\leftrightarrows}} Y$ s. t.

$$\forall x{:}|X|.\forall y{:}|Y|.x \leq_X g(y) \iff f(x) \leq_Y y.$$

   We call g a **right adjoint** to f, and f a **left adjoint** to g.
4. Given $h{:}\mathbf{Po}(X,X)$ we say that
   - $x{:}|X|$ is an **algebra** (aka prefix-point) for $h \iff^{\triangle} h(x) \leq_X x$.
   - $x{:}|X|$ is a **co-algebra** (aka postfix-point) for $h \iff^{\triangle} x \leq_X h(x)$.
   - an algebra μ is **initial** $\iff^{\triangle} \forall x{:}|X|.h(x) \leq_X x \implies \mu \leq_X x$.
   - a co-algebra $\nu{:}|X|$ is **final** $\iff^{\triangle} \forall x{:}|X|.x \leq_X h(x) \implies x \leq_X \nu$.

In the definition of complete lattice we require only the existence of all sups, but it is well-known that a poset that has all sups necessarily has all infs (and conversely). Sups are irrelevant for defining the other notions, that make sense in the bigger category of posets and monotonic maps. However, the restriction to complete lattices is essential for proving some of the properties stated in Prop 5.4.

Example 5.3. We define some objects and arrows in **Po** by equipping sets introduced in previous sections with a partial order and by showing that certain maps are monotonic w. r. t. such partial orders.

1. $\mathbb{P}(\mathbb{S}) \triangleq (\mathsf{P}(\mathbb{S}), \leq)$ is the complete lattice of subsets of a set $\mathbb{S}$ ordered by reverse inclusion $U \leq V \iff^{\triangle} U \supseteq V$, where $\bigsqcup S = \bigcap S$.
   The dual $\mathbb{P}(\mathbb{S})^{op}$ is the complete lattice $(\mathsf{P}(\mathbb{S}), \subseteq)$, where $\bigsqcup S = \bigcup S$.
   Specific instances are the complete lattices $\mathbb{P}(\mathbb{S} \times \mathbb{T} \times \mathbb{S})$ of timed transition systems on $\mathbb{S}$ and $\mathbb{P}(\mathbb{S}^2)$ of transition systems (relations) on $\mathbb{S}$.
2. $\mathbb{C}(\mathbb{S}) \triangleq (\mathsf{C}(\mathbb{S}), \leq)$ is the complete lattice of closed subsets of a topological space $\mathbb{S}$ ordered by reverse inclusion $\leq$, and $\bigsqcup S = \bigcap S$, because the intersection of a set of closed subsets is closed.
   $\mathbb{P}(\mathbb{S}) = \mathbb{C}(\mathbb{S})$ when $\mathbb{S}$ is discrete, thus results on $\mathbb{C}(\mathbb{S})$ apply also to $\mathbb{P}(\mathbb{S})$.
3. A binary relation $R{:}\mathsf{P}(\mathbb{S}_1 \times \mathbb{S}_2)$ induces two arrows

$$\mathbb{P}(\mathbb{S}_1) \underset{R^*}{\overset{R_*}{\rightleftarrows}} \mathbb{P}(\mathbb{S}_2)$$

   the direct image $R_*(S) \triangleq \{s_2 | \exists s_1{:}S.R(s_1, s_2)\}$ and the inverse image $R^*(S) \triangleq \{s_1 | \exists s_2{:}S.R(s_1, s_2)\}$. Since $R^* = (R^{op})_*$ and $R_* = (R^{op})^*$, every result on R_* can be turned into a result on R^* (and conversely).
4. If R is (the graph of) $f{:}\mathbf{Set}(\mathbb{S}_1, \mathbb{S}_2)$, then we have an adjunction $f^* \dashv f_*$.

5. If R is the graph of $f{:}\mathbf{Top}(\mathbb{S}_1, \mathbb{S}_2)$, then the inverse image R^* restricts to an arrow $f^*{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_2), \mathbb{C}(\mathbb{S}_1))$, but the direct image R_* may fail to map closed subsets to closed subsets.
   The direct image of a compact subset along a continuous map is always compact, thus when compact subsets and closed subsets coincide, as in compact Hausdorff spaces, R_* restricts to an arrow $f_*{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$. In any case, $f^*{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_2), \mathbb{C}(\mathbb{S}_1))$ has a right adjoint (see Example 5.5).
6. If $R{:}\mathsf{P}(\mathbb{S}^2)$, then one can consider algebras and co-algebras for R_*
   - $S{:}\mathsf{P}(\mathbb{S})$ is an algebra when $R_*(S) \supseteq S$
   - $S{:}\mathsf{P}(\mathbb{S})$ is a co-algebra when $S \supseteq R_*(S)$.

   The initial algebra is the biggest $S{:}\mathsf{P}(\mathbb{S})$ w. r. t. $\subseteq$ s. t. $R_*(S) = S$, the final co-algebra is the smallest $S{:}\mathsf{P}(\mathbb{S})$ s. t. $R_*(S) = S$, namely the empty set.

We recall some key properties of **Po**. In particular, the construction $(-)^{op}$ is a *functor* on **Po**, which turns *automatically* definitions and results (expressed in a certain language) into their *duals*. For instance, it turns left into right adjoints, algebras into co-algebras, and the characterization of the right adjoint to f into a dual characterization for its left adjoint (where sups become infs).

Proposition 5.4 (Basic properties).

1. *The category* **Po** *is* ***cartesian closed****, more precisely*
   - *The product* $\prod i{:}I.X_i$ *of the* I*-indexed family* $(X_i{:}\mathbf{Po} | i{:}I)$ *is the poset* $(\prod i{:}I.|X_i|, \leq)$*, where* $\leq$ *is defined point-wise. The terminal object* 1 *is product of the* $\emptyset$*-indexed family, and the binary product* $X_0 \times X_1$ *is the product of the* 2*-indexed family* (X_0, X_1)*.*
   - *The exponential* Y^X *of* $X, Y{:}\mathbf{Po}$ *is the poset* $(\mathbf{Po}(X, Y), \leq)$*, where* $\leq$ *is defined point-wise.*
2. *If* $f{:}\mathbf{Po}(X, Y)$*, then* $f^{op} \triangleq f{:}\mathbf{Po}(X^{op}, Y^{op})$*. Moreover,* $X = (X^{op})^{op}$*, and:*
   - $\forall f{:}\mathbf{Po}(X, Y).\forall g{:}\mathbf{Po}(Y, X).f \dashv g \iff g^{op} \dashv f^{op}$*.*
   - $\forall h{:}\mathbf{Po}(X, X).\forall x{:}|X|.h(x) \leq_X x \iff x \leq_{X^{op}} h^{op}(x)$*.*
3. $f{:}\mathbf{Po}(X, Y)$ *has at most one right adjoint, and the following are equivalent:*
   - f *preserves all sups, i. e.,* $f(\bigsqcup S) = \bigsqcup f(S)$ *for all* $S \subseteq |X|$*.*
   - f *has a right adjoint, namely,* $f^R(y) \triangleq \bigsqcup\{x | f(x) \leq_Y y\}$*.*
4. $h{:}\mathbf{Po}(X, X)$ *has a unique initial algebra* μ_h *and final co-algebra* ν_h*, there are monotonic maps* $\mu, \nu{:}\mathbf{Po}(X^X, X)$ *s. t.* $\mu(h) = \mu_h$ *and* $\nu(h) = \nu_h$*, and moreover* $h(\mu_h) = \mu_h \leq_X \nu_h = h(\nu_h)$*.*

Example 5.5. We use Prop 5.4 to define arrows as left/right adjoint.

1. Given $R{:}\mathsf{P}(\mathbb{S}_1 \times \mathbb{S}_2)$ the arrow $R_*{:}\mathbf{Po}(\mathbb{P}(\mathbb{S}_1), \mathbb{P}(\mathbb{S}_2))$ preserves unions (same for R^*), thus R_* has a left adjoint $R_*^L(S) \triangleq \{s_1{:}\mathbb{S}_1 | \{s_2 | R(s_1, s_2)\} \subseteq S\}$. If R is (the graph of) a map f, then $f^{*L} \dashv f^* = f_*^L \dashv f_*$.

2. Given f:$\mathbf{Top}(\mathbb{S}_1, \mathbb{S}_2)$, the arrow f^*:$\mathbf{Po}(\mathbb{C}(\mathbb{S}_2), \mathbb{C}(\mathbb{S}_1))$ preserves all sups, thus it has a right adjoint, which is given by $\overline{f_*}(C_1) \triangleq \overline{f_*(C_1)}$.
   In particular, for any $\mathbb{S}$:$\mathbf{Top}$ consider ι:$\mathbf{Top}(|\mathbb{S}|, \mathbb{S})$, where $|\mathbb{S}|$:$\mathbf{Top}$ is the set $|\mathbb{S}|$ with the discrete topology and ι is the identity map on $|\mathbb{S}|$. Clearly, $\mathbb{C}(|\mathbb{S}|) = \mathbb{P}(|\mathbb{S}|)$, the arrow ι^*:$\mathbf{Po}(\mathbb{C}(\mathbb{S}), \mathbb{C}(|\mathbb{S}|))$ is the inclusion of $\mathsf{C}(\mathbb{S})$ into $\mathsf{P}(\mathbb{S})$ and its right adjoint is given by closure $\overline{\iota_*}(S) = \overline{S}$.

All objects relevant for (topological) transition systems and hybrid systems are either exponentials or complete lattices of the form $\mathbb{C}(\mathbb{S})$, where $\mathbb{S}$ is a topological space. We state some properties of the *functor* $\mathbb{C}$:$\mathbf{Top} \longrightarrow \mathbf{Po}$.

Proposition 5.6. *The construction* $\mathbb{C}$:$\mathbf{Top} \longrightarrow \mathbf{Po}$ *has the properties:*

1. *Binary union* $\cup$:$\mathbf{Po}(\mathbb{C}(\mathbb{S}) \times \mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$ *is* natural *in* f:$\mathbf{Top}(\mathbb{S}, \mathbb{S}')$*, namely* $f^*(C_1' \cup C_2') = f^*(C_1') \cup f^*(C_2')$ *and* $\overline{f_*(C_1 \cup C_2)} = \overline{f_*(C_1)} \cup \overline{f_*(C_2)}$.
2. $\mathbb{C}(-)$ *turns co-products into products, namely* $\prod i{:}I.\mathbb{C}(\mathbb{S}_i) \cong \mathbb{C}(\coprod i{:}I.\mathbb{S}_i)$ *with isomorphism* $(C_i | i{:}I) \mapsto \{(i, s) | i{:}I \wedge s{:}C_i\}$ *natural in* f_i:$\mathbf{Top}(\mathbb{S}_i.\mathbb{S}_i')$.

We recast previous definitions as objects and arrows in **Po**, and introduce the transition and support maps.

- The transition map allows to define the (safe) reachability maps in terms of final co-algebras. Def 3.1 and 3.6 are cast as initial algebras for certain monotonic maps on complete lattices of subsets ordered by inclusion, and the proofs of Thm 3.3 and 3.8 use systematically the universal property of initial algebras. However, the order on $\mathbb{C}(\mathbb{S})$ is reverse inclusion, thus algebras turn into co-algebras.

- The support of a relation R on $\mathbb{S}$ gives the *biggest* subset of $\mathbb{S}$, to which the (safe and robust) reachability map for R can be restricted (see Def 5.9). The support of a HS (F, G) serves a similar purpose, and ignores the image of the flow relation F, because it consists of velocities.

Definition 5.7 (Revised definitions).

1. $\mathbb{H}(\mathbb{S}) \triangleq \mathbb{P}(\mathbb{S}^2) \times \mathbb{P}(\mathbb{S}^2)$ is the object of HS on a Banach space $\mathbb{S}$, similarly $\mathbb{H}_c(\mathbb{S}) \triangleq \mathbb{C}(\mathbb{S}^2) \times \mathbb{C}(\mathbb{S}^2)$ is the object of closed HS on $\mathbb{S}$ (Def 2.1).
2. α:$\mathbf{Po}(\mathbb{H}(\mathbb{S}), \mathbb{P}(\mathbb{S}^2))$ maps a HS $\mathcal{H}$ to its transition relation $\xrightarrow[\mathcal{H}]{}$ (Def 2.3)
3. t:$\mathbf{Po}(\mathbb{H}(\mathbb{S}), \mathbb{H}(\mathbb{R} \times \mathbb{S}))$ maps a HS $\mathcal{H}$ to $\mathcal{H}$ with a clock added (Def 2.9)
4. T:$\mathbf{Po}(\mathbb{P}(\mathbb{S}^2) \times \mathbb{P}(\mathbb{S}), \mathbb{P}(\mathbb{S}))$ given by $\mathsf{T}(R, S) \triangleq R_*(S)$ is the **transition map**, which maps a transition system (relation) R on $\mathbb{S}$ and a set S of states to the set of states reachable from S in one step. Its *currying* $\mathsf{curry}(\mathsf{T})$:$\mathbf{Po}(\mathbb{P}(\mathbb{S}^2), \mathbb{P}(\mathbb{S})^{\mathbb{P}(\mathbb{S})})$ maps a relation R to its direct image R_*.
5. The **reachability** and **safe reachability** maps are
   - Rf:$\mathbf{Po}(\mathbb{P}(\mathbb{S}^2) \times \mathbb{P}(\mathbb{S}), \mathbb{P}(\mathbb{S}))$ given by $\mathsf{Rf}(R, I) \triangleq \nu(\lambda S{:}\mathbb{P}(\mathbb{S}).I \cup \mathsf{T}(R, S))$
   - Rs:$\mathbf{Po}(\mathbb{P}(\mathbb{S}^2) \times \mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$ given by $\mathsf{Rs}(R, I) \triangleq \nu(\lambda S{:}\mathbb{C}(\mathbb{S}).I \cup \overline{\mathsf{T}(R, S)})$

where ν:$\mathbf{Po}(X^X, X)$ computes the final co-algebra of a monotonic map.

6. The **support** maps for transition systems and hybrid systems are
   - S:$\mathbf{Po}(\mathbb{P}(\mathbb{S}^2), \mathbb{C}(\mathbb{S}))$ given by $\mathsf{S}(R) \triangleq \overline{\{s | \exists s'. s\, R\, s' \vee s'\, R\, s\}}$
   - S:$\mathbf{Po}(\mathbb{H}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$ given by $\mathsf{S}(F, G) \triangleq \overline{\{s | \exists v. s\, F\, v\}} \cup \mathsf{S}(G)$.

Remark 5.8. Prop 5.6 implies that $\mathbb{H}(\mathbb{S}) \cong \mathbb{P}(\mathbb{S}')$ and $\mathbb{H}_c(\mathbb{S}) \cong \mathbb{C}(\mathbb{S}')$, where $\mathbb{S}'$ is the topological space $\mathbb{S}^2 + \mathbb{S}^2$, and $\mathbb{S}'$ can be equipped with a metric, when $\mathbb{S}$ has one. The currying of the transition and reachability maps are arrows from $\mathbb{P}(\mathbb{S}^2)$, thus by composing them with α one gets arrows from $\mathbb{H}(\mathbb{S})$, by further composing with the inclusion of $\mathbb{H}_c(\mathbb{S})$ into $\mathbb{H}(\mathbb{S})$ one restricts these arrows to closed hybrid systems on $\mathbb{S}$. The map $\mathsf{Rf}_R = \lambda I.\mathsf{Rf}(R, I)$ is an instance of a general construction $\Box$:$\mathbf{Po}(X^X, X^X)$, which maps f:$\mathbf{Po}(X, X)$ to the biggest h:$\mathbf{Po}(X, X)$ s. t. $\forall x$:$X.h(x) \leq x, f(x), h^2(x)$, namely $h(x) \triangleq \nu(\lambda y$:$X.x \sqcap f(y))$. Categorically h is the *co-monad* generated by f. Rf_R is $\Box(R_*)$, since $S_1 \sqcap S_2$ in $\mathbb{P}(\mathbb{S})$ is given by union, similarly Rs_R is $\Box(f)$ for a simple tweak f of R_*.

Robustness (Def 4.1) has been defined for arrows between objects of the form $\mathbb{C}(\mathbb{S})$ with $\mathbb{S}$ metric space, but existence of best robust approximations (Corr 4.4) is guaranteed only when $\mathbb{S}$ is compact. Refinement is a way to shrink a complete lattice, and on $\mathbb{C}(\mathbb{S})$ it amounts to replace $\mathbb{S}$ with a closed sub-space.

Proposition 5.9 (Refinement). *The object $X \uparrow x_0$ of **refinements** of x_0:X, given by the set $\{x | x_0 \leq_X x\}$ ordered by $\leq_X$, has the properties:*

1. *$\mathbb{C}(\mathbb{S}) \uparrow C$ coincides with $\mathbb{C}(C)$, when C is viewed as a sub-space of $\mathbb{S}$.*
2. *$X \uparrow x_0 \hookrightarrow X$ preserves infs, and its left adjoint is $x \mapsto x \sqcup x_0$.*
3. *If f:$\mathbf{Po}(X, Y)$ and $y_0 \leq_Y f(x_0)$, then f restricts to $\mathbf{Po}(X \uparrow x_0, Y \uparrow y_0)$.*

Remark 5.10. We use refinement mainly to restrict reachability maps, such as Rs:$\mathbf{Po}(\mathbb{H}_c(\mathbb{S}) \times \mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$, in fact

- $S \leq \mathsf{Rs}(\mathcal{H}_0, S)$ when $\mathcal{H}_0$:$\mathbb{H}_c(\mathbb{S})$ and $S \leq S_0 \triangleq \mathsf{S}(\mathcal{H}_0)$:$\mathbb{C}(\mathbb{S})$, therefore
- Rs restricts to an arrow Rs_0:$\mathbf{Po}(\mathbb{H}_c(\mathcal{H}_0) \times \mathbb{C}(S_0), \mathbb{C}(S_0))$, where we have exploited the isomorphism $\mathbb{H}_c(\mathbb{S}) \times \mathbb{C}(\mathbb{S}) \cong \mathbb{C}(\mathbb{S}^2 + \mathbb{S}^2 + \mathbb{S})$ and with abuse of notation write $\mathbb{H}_c(\mathcal{H}_0) \times \mathbb{C}(S_0)$ for $\mathbb{C}(\mathcal{H}_0 + S_0)$.

If $\mathcal{H}_0$ is compact, then S_0 is compact and Corr 4.4 becomes applicable to Rs_0. However, $\mathsf{Rs}_0^{\boxdot}$ is robust w. r. t. small extensions of $\mathcal{H} \geq \mathcal{H}_0$ and $S \geq S_0$, as far as they are refinements of $\mathcal{H}_0$ and S_0, respectively. In other words, $\mathcal{H}_0$ and S_0 represent hard constraints, thus the δ-fattening of S in $\mathsf{C}(S_0)$ is given by $S_\delta \cap S_0$, where S_δ is the δ-fattening of S in $\mathsf{C}(\mathbb{S})$. Similarly, for the δ-fattening in $\mathbb{H}(\mathcal{H}_0)$.

We are interested in correct analyses, and we reuse the conceptual framework adopted in *static program analysis* to relate the analysis $A(p)$ of a program p to its semantics $[\![p]\!]$. Program semantics usually interprets programs in an infinite poset X, while static analysis relies on a finite poset F to achieve decidability

(which is not an issue we address in this paper). Most program properties are undecidable, so analyses can only provide conservative answers. For instance, in the case of safety properties, a program must be safe when a *correct* analysis says so, but it can be safe also when the analysis says that it could be unsafe.

- First, F should be (up to isomorphisms) the restriction of X to a subset, so one can say that $A(p)$ is *correct* when $A(p) \leq_X [\![p]\!]$.
- Second, F must be able to approximate every element in X, namely for every $x{:}X$ there exists $\Box_F(x){:}F$ s. t. $\Box_F(x) \leq_X x$.

A third requirement is that $\Box_F$ must be a monotonic and idempotent map on X. For complete lattices there are simpler ways to capture these requirements.

Proposition 5.11 (Best approximation). *Given $X{:}\mathbf{Po}$ and $F \subseteq |X|$, the following properties are equivalent*

1. *F is closed w. r. t. sups computed in X.*
2. *$F = f(Y)$ for some $f{:}\mathbf{Po}(Y, X)$ preserving all sups.*
3. *$F = \{x | x = h(x)\}$ for some $h{:}\mathbf{Po}(X, X)$ s. t. $h(x) \leq x$ and $h(x) \leq h^2(x)$.*

*Moreover, h is uniquely determined by F, namely $h(x) = \bigsqcup\{y{:}F | y \leq_X x\}$, thus we write $\Box_F$ for the unique h and call $\Box_F(x)$ the **best F-approximation** of x.*

Proof. We prove a sequence of implications.

- (1) $\Longrightarrow$ (2). Let $Y{:}\mathbf{Po}$ be the subset F with the order inherited from X and $f{:}\mathbf{Po}(Y, X)$ the inclusion of F into $|X|$, then f preserves sups, by the assumption (1).
- (2) $\Longrightarrow$ (3). Let f^R be the right adjoint to f, which exists by Prop 5.4, and $h \triangleq f \circ f^R{:}\mathbf{Po}(X, X)$. We prove $h(x) \leq_X x$ and $h(x) \leq_X h^2(x)$. Clearly, $f^R(x) \leq_Y f^R(x)$ is true, therefore

  $$\begin{array}{ll} \Longrightarrow & f(f^R(x)) \leq_X x \quad \text{by } f \dashv f^R \\ \Longleftrightarrow & h(x) \leq_X x \quad \text{by definition of } h \end{array}$$

  By duality $y \leq_Y f^R(f(y))$ is true, therefore

  $$\begin{array}{lll} \Longrightarrow & f^R(x) \leq_Y f^R(f(f^R(x))) & \text{by taking } y = f^R(x) \\ \Longrightarrow & f(f^R(x)) \leq_Y f(f^R(f(f^R(x)))) & \text{by monotonicity of } f \\ \Longleftrightarrow & h(x) \leq_X h^2(x) & \text{by definition of } h. \end{array}$$

- (3) $\Longrightarrow$ (1). Suppose that $\forall i{:}I.h(x_i) = x_i$ and that $x = \bigsqcup\{x_i | i{:}I\}$, we have to prove $h(x) = x$. Clearly, $h(x) \leq x$ is one of the properties of h, thus it suffices to prove $x \leq h(x)$.

  $$\begin{array}{lll} & \forall i.x_i \leq h(x_i) & \text{by assumption on } x_i \\ \Longrightarrow & \forall i.x_i \leq h(x) & \text{by } x_i \leq x \text{ and monotonicity of } h \\ \Longleftrightarrow & x \leq h(x) & \text{by definition of sup.} \end{array}$$

  □

Example 5.12, 5.13 and 5.14 give sets of *approximants* for objects of the form $\mathbb{C}(\mathbb{S})$ and Y^X, including the set of Scott continuous maps. Scott continuity is an important property because of its relation to robustness (Thm A.4) and computability (*computable* maps must be Scott continuous).

Example 5.12. Let X be $\mathbb{P}(\mathbb{R})$, we give a decreasing sequence of subsets of $\mathsf{P}(\mathbb{R})$ satisfying the properties in Prop 5.11.

1. $\mathsf{C}(\mathbb{R}) \subset \mathsf{P}(\mathbb{R})$, the cardinality of $\mathsf{C}(\mathbb{R})$ is $2^{\aleph_0}$, while that of $\mathsf{P}(\mathbb{R})$ is $2^{2^{\aleph_0}}$. However, the rationale for using $\mathsf{C}(\mathbb{R})$, is that in the presence of *noise* it is impossible to distinguish a subset from its closure.
2. $\mathbb{IR}_\bot^\top \subset \mathsf{K}(\mathbb{R})_\bot \subset \mathsf{C}(\mathbb{R})$, these subsets have the same cardinality.
   - $\mathsf{K}(\mathbb{S})$ is the set of compact subsets of the topological space $\mathbb{S}$. When $\mathbb{S}$ is Hausdorff $\mathsf{K}(\mathbb{S}) \subseteq \mathsf{C}(\mathbb{S})$, when $\mathbb{S}$ is compact $\mathsf{C}(\mathbb{S}) \subseteq \mathsf{K}(\mathbb{S})$. Since $\mathbb{R}$ is Hausdorff but not compact, we add $\bot$ (i. e., $\mathbb{R}$ in $\mathbb{P}(\mathbb{R})$) to get a complete lattice.
   - $\mathbb{IR}$ is the set of intervals $[x, x']$ with $x \leq x'$. Topologically they are the non-empty connected compact subsets of $\mathbb{R}$, thus $\mathbb{IR} \subset \mathsf{K}(\mathbb{R})$. To get a complete lattice, we add also $\top$ (i. e., $\emptyset$ in $\mathbb{P}(\mathbb{R})$).
3. $\mathbb{IF}_\bot^\top \subset_f \mathbb{IR}_\bot^\top$, where $\mathbb{IF}$ is the set of intervals with endpoints in a finite subset $\mathbb{F} \subset_f \mathbb{R}$, thus $\mathbb{IF}$ is finite.

Similar subsets of $\mathsf{P}(\mathbb{R}^n)$ can be defined for any Euclidean space $\mathbb{R}^n$.

Example 5.13. Consider the subset $\Box(X) \triangleq \{f | f^2 = f \leq \mathrm{id}_X\}$ of $\mathbf{Po}(X, X)$, which is isomorphic to the set of all $F \subseteq |X|$ satisfying one of the properties in Prop 5.11. Categorically $\Box(X)$ is the set of *co-monads*. Co-monads require only $f \leq f^2$ and $f \leq \mathrm{id}_X$, but in a poset this implies $f = f^2$. We show that co-monads on a complete lattice X are closed w. r. t. sups computed in X^X, i. e., if $(f_i{:}\Box(X) | i{:}I)$ and $f = \bigsqcup\{f_i | i{:}I\}$, then $f \leq f^2$ ($f \leq \mathrm{id}_X$ is immediate). In fact

$$\begin{array}{ll} f = \bigsqcup\{f_i | i{:}I\} & \text{by definition of } f \\ \leq \bigsqcup\{f_i^2 | i{:}I\} & \text{by the assumption } f_i{:}\Box(X) \\ \leq \bigsqcup\{f^2 | i{:}I\} & \text{because } f_i \leq f \text{ by definition of } f \\ \leq f^2 & \text{by definition of sup.} \end{array}$$

Besides the adjunction given by Prop 5.11, there is another adjunction involving the object $\Box(X){:}\mathbf{Po}$, i. e., the subset $\Box(X)$ with the order inherited from X^X, namely $(\mathsf{P}(|X|), \subseteq) \underset{p}{\overset{p^R}{\leftrightarrows}} \Box(X)$, where

- $p^R(f) \triangleq \{x | x = f(x)\}$ is the set of fix-points (the image) of $f{:}\Box(X)$. The image of p^R is the set of $F \subseteq |X|$ closed w. r. t. sups (computed in X).
- $p(S) \triangleq \lambda x{:}X.\bigsqcup\{x'{:}S | x' \leq x\}$ is $\Box_F{:}\Box(X)$ for the closure F of S w. r. t. sups.

Example 5.14. We consider subsets $F \subseteq \mathbf{Po}(X,Y) = |Y^X|$ consisting of monotonic maps preserving sups of certain *shapes*, and prove that all of them satisfy the properties in Prop 5.11. More formally, we identify a shape with a poset D and define

- The object X^D:**Po** of D-**diagrams** (i. e., diagrams of shape D) in X:**Po** is the set of monotonic maps from D to X with the point-wise order. Since sups are computed point-wise, X^D is a complete lattice.
- The arrow $\sqcup_D$:$\mathbf{Po}(X^D, X)$ computing D-**sups** (i. e., sups of D-diagrams) is x:$X^D \mapsto \bigsqcup\{x_d | d{:}D\}$. If D is empty, then $X^D = \{\emptyset\}$ and $\sqcup_D \emptyset = \bot_X$. If D has a maximum $\top$, then $\sqcup_D x = x(\top)$.
- The subset Y_D^X of $\mathbf{Po}(X,Y)$ consisting of the maps preserving D-sups, i. e., the f:$\mathbf{Po}(X,Y)$ s. t. $\forall x{:}X^D. f(\sqcup_D x) = \sqcup_D(f \circ x)$. For instance, f:$Y_\emptyset^X$ means that $f(\bot_X) = \bot_Y$, f:Y_ω^X means that f preserves sups of ω-chains.

One can consider maps preserving D-sups for more than one shape by taking the intersection of Y_D^X for different D. For instance, **additive maps** preserve sups of every shape (but it suffices to consider flat posets), **Scott continuous maps** preserve sups of **directed posets** (but it suffices to consider posets that have sups of finite subsets). One can also consider the intersection of the set $\Box(X)$ of co-monads on X with X_D^X. It is obvious that maps preserving D-sups form a sub-category of **Po**, because id_X:X_D^X and $g \circ f$:Z_D^X when f:Y_D^X and g:Z_D^Y.

We conclude the example by showing that Y_D^X is closed w. r. t. sups in Y^X, namely if $(f_i{:}Y_D^X | i{:}I)$, $f = \bigsqcup\{f_i | i{:}I\}$ and x:X^D, then $f(\sqcup_D x) = \sqcup_D(f \circ x)$:

$$
\begin{array}{rll}
f(\sqcup_D x) = \bigsqcup\{f_i(\bigsqcup\{x_d | d{:}D\}) | i{:}I\} & & \text{by definition of } f \text{ and } \sqcup_D \\
= \bigsqcup\{\bigsqcup\{f_i(x_d) | d{:}D\} | i{:}I\} & & \text{by the assumption } f_i{:}Y_D^X \\
= \bigsqcup\{\bigsqcup\{f_i(x_d) | i{:}I\} | d{:}D\} & & \text{by associativity and commutativity of } \bigsqcup \\
= \bigsqcup\{f(x_d)) | d{:}D\} & & \text{by definition of } f \\
= \sqcup_D(f \circ x) & & \text{by definition of } \sqcup_D.
\end{array}
$$

The following theorem gives the properties of two best approximations involving Scott continuous maps, which underpin the results in Sec 4 on the existence of best robust approximations.

Theorem 5.15. *Every f:$\mathbf{Po}(X,Y)$ has a* ***best continuous approximation*** *$f^\boxdot$:$\mathbf{Po}(X,Y)$, namely the biggest Scott continuous map in Y^X s. t. $f^\boxdot \leq f$. Moreover, $id^\boxdot = id$ and $(g^\boxdot \circ f^\boxdot)^\boxdot = g^\boxdot \circ f^\boxdot \leq (g \circ f)^\boxdot$.*

Every h:$\mathbf{Po}(X,X)$ has a ***best continuous co-monad approximation*** *$h_\boxplus$:$\mathbf{Po}(X,X)$, namely the biggest Scott continuous map in X^X s. t. $h_\boxplus \leq h$ and $h_\boxplus \circ h_\boxplus = h_\boxplus \leq id_X$. Moreover, $id_\boxplus = id$ and $h_\boxplus \leq h^\boxdot$.*

Proof. The existence of $f^\boxdot$ and $h_\boxplus$ follows from the fact that the subsets satisfying the properties in Thm 5.11 are closed w. r. t. intersections, therefore one can intersect the subsets Y_D^X and $\Box(X)$ given in Example 5.14 and 5.13. Their properties are easy consequences of their definitions, and the fact that Scott continuous maps form a sub-category of **Po**. □

We conclude this section with some basic notions and results on *continuous lattices* (see [17]) culminating in Thm 5.20, which provides a simple way for *computing* $f^{\boxdot}$ of $f{:}\mathbf{Po}(X,Y)$ when X is a continuous lattice.

First we need to define the way-below relation and give its basic properties (for more details on the concepts introduced referred to [14, 1]).

Proposition 5.16. *Given a complete lattice X, define*

1. *x is **way-below** y (written $x \ll_X y$) $\stackrel{\triangle}{\iff}$ for any directed poset D and $z{:}X^D$, if $y \leq_X \sqcup_D z$, then $\exists d{:}D.x \leq_X z_d$.*
2. *$\mathop{\downarrow\!\!\!\downarrow}_X y \stackrel{\triangle}{=} \{x | x \ll_X y\}$ denotes the set of elements that are way-below y.*

The following properties hold (and are easy to prove):

1. *$\mathop{\downarrow\!\!\!\downarrow} y$ is downward closed, i. e., $x_0 \leq x_1 \ll y \implies x_0 \ll y$.*
2. *$\mathop{\downarrow\!\!\!\downarrow} y$ is closed w. r. t. finite sups, i. e., $x_0, x_1 \ll x \implies x_0 \sqcup x_1 \ll x$ and $\bot \ll x$, and therefore is a directed subset of X.*
3. *if $x \leq y$, then $\mathop{\downarrow\!\!\!\downarrow} x \subseteq \mathop{\downarrow\!\!\!\downarrow} y$.*

Definition 5.17 (Continuous Lattice).
A complete lattice X is **continuous** $\stackrel{\triangle}{\iff} \forall x{:}X.x = \bigsqcup \mathop{\downarrow\!\!\!\downarrow} x$.

[12] advocates the use of Domain Theory for the study of dynamical systems. In this context, when $\mathbb{S}$ is a compact Hausdorff space the complete lattice $\mathbb{C}(\mathbb{S})$ is continuous, and moreover the Scott topology coincides with the Upper topology (see Thm A.4 and [12, Prop 3.2 and 3.3]).

Example 5.18. In general $\ll$ on $\mathbb{C}(\mathbb{S})$ is given by $C' \ll C \iff C \subseteq K^c \subseteq C'$ for some compact subset K of $\mathbb{S}$, where K^c denotes the complement of K.

1. If $\mathbb{S}$ is a compact metric space, then $\mathbb{C}(\mathbb{S})$ is a continuous lattice and $\ll$ is definable in terms of fattening, namely $C' \ll C \iff \exists \delta > 0. C_\delta \subseteq C'$.
2. If $\mathbb{S}$ is locally compact, then $\mathbb{C}(\mathbb{S})$ is a continuous lattice. Euclidean spaces $\mathbb{R}^n$ are locally compact, but not compact, and the relation between $\ll$ and fattening is more subtle, i. e., $C' \ll C \iff \exists \delta > 0. C_\delta \cup B(0, 1/\delta)^c \subseteq C'$.
3. An infinite dimensional Banach space $\mathbb{S}$ is not locally compact and $\mathbb{C}(\mathbb{S})$ is not a continuous lattice, because its compact subsets have empty interior, and therefore $C' \ll C \iff C' = \mathbb{S}$.

It is easy to show that every $f{:}\mathbf{Po}(X,Y)$ is the sup $\bigsqcup\{[x, f(x)] | x{:}X\}$ in Y^X of *monotonic step maps* $[x,y] \stackrel{\triangle}{=} \begin{cases} y & \text{if } x \leq_X x' \\ \bot_Y & \text{otherwise} \end{cases}$.

When X is a continuous lattice, there is a similar result for Scott continuous maps, namely every Scott continuous $f{:}\mathbf{Po}(X,Y)$ is the sup $\bigsqcup\{[\![x, f(x)]\!] | x{:}X\}$ of *continuous step maps* $[\![x,y]\!] \stackrel{\triangle}{=} \begin{cases} y & \text{if } x \ll_X x' \\ \bot_Y & \text{otherwise} \end{cases}$.

In general $[\![x,y]\!] \leq [x,y]$ in Y^X, and the equality holds exactly when $x \ll_X x$ (in this case $[x,y]$ is also Scott continuous). The following result shows that every continuous step map is Scott continuous, when X is a continuous lattice.

Proposition 5.19. *Given a continuous lattice X and a complete lattice Y*

1. *If D is a directed poset, $z{:}X^D$ and $x \leq_X \sqcup_D z$, then $\exists d{:}D.x \ll_X z_d$.*
2. *Continuous step maps $[\![x,y]\!] \triangleq \begin{cases} y & \text{if } x \ll_X x' \\ \bot_Y & \text{otherwise} \end{cases}$ are Scott continuous.*

Proof.

1. [14, Thm I-1.9].
2. If D is a directed poset, $z{:}X^D$ and $[\![x,y]\!](\sqcup_D z) = y$, then $[\![x,y]\!](z_d) = y$ for some $d{:}D$, by $x \ll_X \sqcup_D z$ and the previous property. □

Theorem 5.20. *If X is a continuous lattice and Y is a complete lattice, then $f^{\boxdot}(x) = \bigsqcup\{f(b) | b \ll_X x\}$ for every $f{:}\mathbf{Po}(X,Y)$ and $x{:}X$.*

Proof. Since X is a continuous lattice, the continuous step maps $[\![b, f(b)]\!]$ are Scott continuous. Scott continuous maps are closed w. r. t. sups computed in Y^X, thus $f' \triangleq \bigsqcup\{[\![b, f(b)]\!] | b{:}X\}$ is Scott continuous and $f'(x) = \bigsqcup\{f(b) | b \ll_X x\}$. Finally, $f' = f^{\boxdot}$ because f' has the properties characterizing $f^{\boxdot}$, namely

- $f' \leq f$. In fact, $f'(x) = \bigsqcup\{f(b) | b \ll x\} \leq \bigsqcup\{f(x) | b \ll x\} = f(x)$.
- If g Scott continuous and $g \leq f$ in Y^X, then $g \leq f'$. In fact,

$$\begin{array}{lll} g(x) = g(\bigsqcup {\downarrow\!\!\!\downarrow} x) & & \text{because } X \text{ is continuous} \\ \quad = \bigsqcup\{g(b) | b \ll x\} & & \text{by } g \text{ Scott continuous and } {\downarrow\!\!\!\downarrow} x \text{ directed} \\ \quad \leq \bigsqcup\{f(b) | b \ll x\} & & \text{by the assumption } g \leq f \\ \quad = f'(x) & & \text{by definition of } f'. \end{array}$$

□

6. Related Notions

This section compares notions used in [15]—that are more familiar to the hybrid systems research community—with those used in this paper, where we favour an *abstract/qualitative* view, based on topological spaces and posets, over a *concrete/quantitative* one, based on Euclidean or metric spaces.

We also favour a category-theoretic view, which focuses on arrows, mainly $A{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}'))$, rather than elements, $C{:}|\mathbb{C}(\mathbb{S})| \cong \mathbf{Po}(1, \mathbb{C}(\mathbb{S}))$. This allows: to decouple a hybrid system from arrows related to it (see Def 3.1 and 3.6); to consider arrows defined on complete lattices of hybrid systems (see Def 5.7); to define notions, like robustness (Def 4.1), with a broader scope than [15].

For each notion in [15] that we deem relevant, we say on which page it is introduced, whether there is a corresponding definition in [23] (for hybrid automata), and how it relates to notions used or introduced in this paper.

At the end of this section, we show how the construction $\Box{:}\mathbf{Po}(X^X, X^X)$ in Remark 5.8 allows to define an arrow computing the smallest closed subset $C \supseteq I$ *safely stable* for $\mathcal{H}$.

Solution (to a HS) [15, page 39-40]. After defining a HS (Def 2.1) we say that for defining reachability its transition relation suffices.

If $s \xrightarrow[\mathcal{H}]{d} s'$ is a timed transition, then there exists a solution $x{:}D \to \mathbb{S}$ to $\mathcal{H}$ with *hybrid time domain* $D = [0,d] \times \{0\}$ s. t. $s = x(0,0)$ and $s' = x(d,0)$.

In comparison to (timed) transition relation (Def 2.3), the definitions of hybrid time domain D, hybrid arc $x{:}D \to \mathbb{S}$, and when x is a solution to the HS $\mathcal{H}$, are clumsy (and also inadequate to cope with Zeno behaviors).

A hybrid time domain is called *hybrid time trajectory* in [23, Def 2], and a solution corresponds to an *execution* in [23, Def 3].

Basic assumptions [15, page 43]. Most theorems in [15] are on HS satisfying the *basic assumptions*. If the convexity requirement is ignored, then $\mathcal{H}$ is compact $\Longrightarrow$ $\mathcal{H}$ satisfies the basic assumptions $\Longrightarrow$ $\mathcal{H}$ is closed.

We never use the basic assumptions. For our purposes, compact HS and closed HS on $\mathbb{S}$ suffice, and they correspond to the standard notions of compact and closed subset (of the topological space $\mathbb{S}^2 + \mathbb{S}^2$).

Forward invariant set [15, page 48], *invariant set* in [23, Def 8]. A subset S is *forward invariant* for $\mathcal{H}$ on $\mathbb{S}$ when every solution $x{:}D \to \mathbb{S}$ to $\mathcal{H}$ starting in S (i. e., $x(t_0,0){:}S$) stays in S (i. e., $\forall(t,j){:}D.x(t,j){:}S$).

If S is forward invariant, then it is closed w. r. t. the transition relation $\xrightarrow[\mathcal{H}]{}$. The reverse implication holds, when S is a closed subset of $\mathbb{S}$.

Thus, for closed subsets forward invariance can be defined in terms of the more elementary transition relation, in particular: $\mathsf{Rs}_{\mathcal{H}}(I)$ is the smallest closed forward invariant subset S containing I, and the closed forward invariant subsets for $\mathcal{H}$ are exactly the fix-points of the safe reachability map $\mathsf{Rs}_{\mathcal{H}}$, i. e., the sets S s. t. $S = \mathsf{Rs}_{\mathcal{H}}(S)$.

Perturbation (of a HS) [15, page 49, 56]. The definition of $\mathcal{H}_\sigma$ (page 56), which subsumes that of $\mathcal{H}_{\delta\sigma}$ (page 49), uses the closed convex hull, in order to satisfy the convexity requirement on the flow relation.

If we ignore the convexity requirement, take as σ the constant map $s \mapsto \delta$, and assume that $\mathcal{H}$ is compact, then $\mathcal{H}_\sigma$ will be the δ-fattening of $\mathcal{H}$ in $\mathcal{H}_c(\mathbb{S})$, provided one chooses a suitable metric on $\mathbb{S}^2 + \mathbb{S}^2$.

δ-fattening (Def 4.1) is defined in any metric space, and allows to define perturbations of other entities besides HS, while perturbations of a HS rely on more structure (because of the convexity requirement).

Stable subset [15, page 49], see also [23, Def 9]. [9, Def 6] defines stable subsets for topological transition systems. A subset S of $\mathbb{S}$ is *stable* for $\mathcal{H}$ when for every ϵ there exists δ s. t. every solution $x{:}D \to \mathbb{S}$ starting in $B(S,\delta)$ stays in $B(S,\epsilon)$. One has that:

- S stable $\iff$ $\overline{S}$ stable

- S stable and closed $\implies$ S forward invariant.

The safe reachability map $\mathsf{Rs}_{\mathcal{H}}$ allows to define the stronger property, i. e., S *safely stable* for $\mathcal{H}$ $\overset{\Delta}{\iff}$ $\forall\epsilon.\exists\delta.\mathsf{Rs}_{\mathcal{H}}(S_\delta) \subseteq S_\epsilon$, equivalently $S = \mathsf{Rs}_{\mathcal{H}}(S)$ and $\mathsf{Rs}_{\mathcal{H}}$ is robust at S. When S is closed, one has a chain of implications:

- S safely stable $\implies$ S stable $\implies$ $\forall\epsilon.\exists\delta.\mathsf{Rf}_{\mathcal{H}}(S_\delta) \subseteq S_\epsilon$.

The reverse implications fail. For instance, consider the HS $\mathcal{H}_X$ on $\mathbb{R}$ with empty flow relation and jump relation $G = \{(x_{m,n}, x_{m,n+1}) | m, n{:}\omega\}$, where the double sequence $x_{m.n}$ satisfies the properties

1. $0 < x_{m,n} < x_{m,n+1} < 1$
2. $x_{m,0}$ is the limit of $(x_{m+1,n}|n{:}\omega)$, thus $x_{m+1,n} < x_{m,0}$
3. 0 is the limit of $(x_{m,0}|m{:}\omega)$ and 1 is the limit of $(x_{0,n}|n{:}\omega)$.

$S \triangleq \{0\}$ is not safely stable, since $\mathsf{Rs}_{\mathcal{H}_X}(S_\delta) = S_\delta \cup \{x_{m,n} | m, n{:}\omega\} \cup \{1\}$, but it is stable, since all *nontrivial* solutions have the form $x(0, j) = x_{i,n+j}$, thus $x(0, 0) = x_{i,n} < \delta \triangleq x_{m,0}$ implies $x(0, j) < \delta$. Therefore, stability fails to detect that there is a sequence of $m + 1$ Zeno behaviors starting from $x_{m,0}$ and eventually reaching 1.

Pre-attractive subset [15, page 49]. A subset S is *pre-attractive* for $\mathcal{H}$ when there exists δ s. t. every solution $x{:}D \to \mathbb{S}$ to $\mathcal{H}$ starting in $B(S, \delta)$ tends towards S, i. e., $\forall\epsilon.\exists n.\forall(t, j){:}D.t + j > n \implies x(t, j){:}B(S, \epsilon)$.

If the hybrid time domain of the solution x is *bounded*, i. e., there exists n_0 s. t. $\forall(t, j){:}D.t + j \leq n_0$, then x tends towards S for trivial reasons. For this definition a Zeno behavior x has an unbounded D, because there is no bound on j (while t has a bound).

The map $\mathsf{Es}_{\mathcal{H}}$ allows to define an analog of the pre-attractive property, i. e., S *eventually attractive* $\overset{\Delta}{\iff}$ $\exists\delta.\forall\epsilon.\exists n.\forall t > n.\mathsf{Es}_{\mathcal{H}}(S_\delta)(t) \subseteq S_\epsilon$.

Eventually attractive is not implied nor implies pre-attractive. Every S is eventually attractive for $\mathcal{H}_X$ above, because $\mathsf{Es}_{\mathcal{H}_X}(I) = \{0\} \times \mathsf{Rs}_{\mathcal{H}_X}(I)$, while $\{0\}$ is not pre-attractive. On the other hand, $\{0\}$ is eventually attractive, but not pre-attractive, for the HS $\mathcal{H}_Y$ on $\mathbb{R}$ with flow relation $F = \{(0, 0)\}$ and jump relation $G = \{(y_{m,n}, y_{m,n+1}) | m, n{:}\omega\}$, where the double sequence $y_{m.n}$ satisfies the properties

1. $0 < y_{m,n+1} < y_{m,n}$
2. $y_{m+1,0}$ is the limit of $(y_{m,n}|n{:}\omega)$, thus $y_{m+1,0} < y_{m,n}$
3. 0 is the limit of $(y_{m,0}|m{:}\omega)$.

Starting from any $y_{m,n}$ there is a cascade of Zeno behaviours leading to 0, but a solution can only approach the first Zeno point $y_{m+1,0}$.

Robustness (w. r. t. perturbations of a HS) [15, page 56]. We could find only informal definitions of robustness, or theorems where the notion is made precise but too specific (robustness of pre-asymptotic stability):

1. "One way to characterize robustness of pre-asymptotic stability of a compact set is to study the effect of state-dependent perturbations on the hybrid system and show that, when the perturbations are small enough, the pre-asymptotic stability is preserved" [15, Thm 15].
2. "Another way is to consider constant perturbations and show that they lead to *practical* pre-asymptotic stability" [15, Thm 17].

If one considers stability instead of pre-asymptotic stability, then the safe reachability map $\mathsf{Rs}{:}\mathbf{Po}(\mathbb{H}_c(\mathbb{S}) \times \mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$ allows to define S is *robustly stable* for $\mathcal{H} \stackrel{\Delta}{\iff} \forall\epsilon.\exists\delta.\mathsf{Rs}(\mathcal{H}_\delta, S_\delta) \subseteq S_\epsilon$, equivalently $S = \mathsf{Rs}(\mathcal{H}, S)$ and Rs is robust at $(\mathcal{H}, S)$. Clearly, S robustly stable $\implies$ S safely stable.

In general, it may not exist the smallest closed subset containing I and safely stable for $\mathcal{H}$. However, one could consider the restriction $A{:}\mathbf{Po}(\mathbb{C}(S_0), \mathbb{C}(S_0))$ of $\mathsf{Rs}_{\mathcal{H}}{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}), \mathbb{C}(\mathbb{S}))$ to a compact subset S_0 s. t. $S_0 = \mathsf{Rs}_{\mathcal{H}}(S_0)$, and re-define S *safely stable* for $\mathcal{H}$ to mean $S = A^{\boxdot}(S)$, where $A^{\boxdot}{:}\mathbf{Po}(\mathbb{C}(S_0), \mathbb{C}(S_0))$ is the best robust approximation of A given by Corr 4.4.

There is an alternative characterization of A, namely $A = \Box(T)$, where $\Box{:}\mathbf{Po}(X^X, X^X)$ is the map $\Box(f) \stackrel{\Delta}{=} \lambda x{:}X.\nu(\lambda y{:}X.x \sqcap f(y))$ given in Remark 5.8, and $T{:}\mathbf{Po}(\mathbb{C}(S_0), \mathbb{C}(S_0))$ is the transition map $T(C) \stackrel{\Delta}{=} \overline{\{s'{:}S_0 | \exists s{:}C.s \xrightarrow[\mathcal{H}]{} s'\}}$.

One can apply $\Box$ to other maps in $\mathbf{Po}(\mathbb{C}(S_0), \mathbb{C}(S_0))$. For instance, $\Box(A^{\boxdot})$ computes the smallest closed subset containing I and safely stable for $\mathcal{H}$. By applying $\Box$ to yet another map one can compute also the smallest closed subset containing I and robustly stable for $\mathcal{H}$.

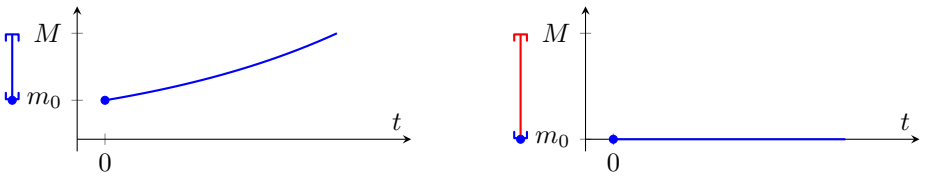
7. Figures and Examples

We go through the hybrid systems introduced in Sec 2 and for each of them we compare the sets computed by different analyses. More precisely, given a HS $\mathcal{H}$ on $\mathbb{S}$ and a state s_0 in the support $\mathsf{S}(\mathcal{H})$ of $\mathcal{H}$, take as set of initial states $I = \{s_0\}$, then define four subsets $S_f \subseteq S_s \subseteq S_r \subseteq S_R$ of $\mathbb{S}$:

- $S_f \stackrel{\Delta}{=} \mathsf{Rf}_{\mathcal{H}}(I)$ set of states reachable in finitely many transitions.
- $S_s \stackrel{\Delta}{=} \mathsf{Rs}_{\mathcal{H}}(I)$ safe approximation of the set of states reachable in finite time. One should use $\overline{I}$ in place of I, but a singleton is already closed.

  To define S_r one must restrict $\mathsf{Rs}_{\mathcal{H}}$ to a map in $\mathbf{Po}(\mathbb{C}(S_0), \mathbb{C}(S_0))$, where S_0 is a *sufficiently large* compact subset of $\mathbb{S}$. When $\overline{\mathcal{H}}$ is compact, the canonical choice for S_0 is $\mathsf{S}(\overline{\mathcal{H}}) = \mathsf{S}(\mathcal{H})$.
- $S_r \stackrel{\Delta}{=} \mathsf{Rs}^{\boxdot}_{\mathcal{H}}(I)$ approximation of S_s robust w. r. t. perturbations to I.

  To define S_R one must restrict Rs to a map in $\mathbf{Po}(\mathbb{H}_c(\mathcal{H}_0) \times \mathbb{C}(S_0), \mathbb{C}(S_0))$, where $\mathcal{H}_0$ is a *sufficiently large* compact HS on $\mathbb{S}$ and $S_0 = \mathsf{S}(\mathcal{H}_0)$. The role of $\mathcal{H}_0$ is to capture the *allowed* perturbations to $\mathcal{H}$, thus $\mathcal{H}_0 \leq \overline{\mathcal{H}}$ in $\mathbb{H}_c(\mathbb{S})$, where $\overline{\mathcal{H}}$ is the closure of $\mathcal{H}$.



(a) $m_0 > 0$ (b) $m_0 = 0$

Figure 1: Trajectories and reachable states of $\mathcal{H}_E$ (Expand). In each case the set of states reachable from $I = \{m_0\}$ is on the left of the trajectory starting from m_0.

- $S_R \triangleq \mathsf{Rs}^{\boxdot}(\overline{\mathcal{H}}, I)$ approximation of $S'_r \triangleq \mathsf{Rs}^{\boxdot}_{\overline{\mathcal{H}}}(I)$ robust w. r. t. perturbations to $\mathcal{H}$ & I *allowed* by $\mathcal{H}_0$.

In the figures we adopt the following color coding for states and trajectories:

- a bullet • indicates the initial state s_0
- blue - S_f and the part of a trajectory reachable in finitely many transitions
- green - $S_s - S_f$ and the rest of a trajectory not reachable in finitely many transitions, like Zeno points and beyond
- red - $S_r - S_s$, there is no analogue for a trajectory starting from s_0.

7.1. Expand

$\mathcal{H}_E = (F, G)$ of Example 2.6 is a compact *deterministic* HS on $\mathbb{R}$

$$F = \{(m, \dot{m}) | 0 \leq m = \dot{m} \leq M\} \qquad G = \emptyset$$

whose behavior is depicted in Fig 1. Let $S_0 = [0, M]$ and $\mathcal{H}_0 = (F_0, G_0)$ with $F_0 = S_0 \times [-M, M]$ and $G_0 = \emptyset$, then

- $S_f = S_s = S_r = S_R = [m_0, M]$ when $0 < m_0 \leq M$
- $S_f = S_s = [0] \subset [0, M] = S_r = S_R$ when $0 = m_0$.

We now explain why making the set of reachable states robust w. r. t. perturbations to $\mathcal{H}$ does not make a difference in the case $0 < m_0 \leq M$. To approximate S_R we take a small $\delta > 0$ and define $I_\delta \ll I$ in $\mathbb{C}(S_0)$ and $\mathcal{H}_\delta \ll \mathcal{H}$ in $\mathbb{H}_c(\mathcal{H}_0)$.

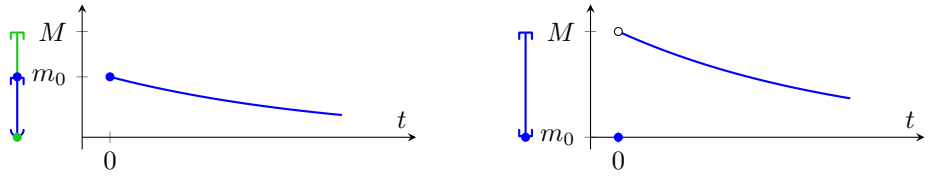
Let $I_\delta = [m_0 - \delta, M]$ and $F_\delta = \{(m, \dot{m}) | 0 \leq m \leq M \wedge m - \delta \leq \dot{m} \leq M\}$. By taking $2 * \delta < m_0$ we can ensure that $F_\delta(m) \subset (0, M]$ for any $m{:}I_\delta$, therefore $S_R = \mathsf{Rs}^{\boxdot}(\overline{\mathcal{H}}, I) \subseteq \mathsf{Rs}(\mathcal{H}_\delta, I_\delta) = [m_0 - \delta, M] \to S_r$ when $\delta \to 0$.

7.2. Decay

$\mathcal{H}_D = (F, G)$ of Example 2.7 is a deterministic HS on $\mathbb{R}$

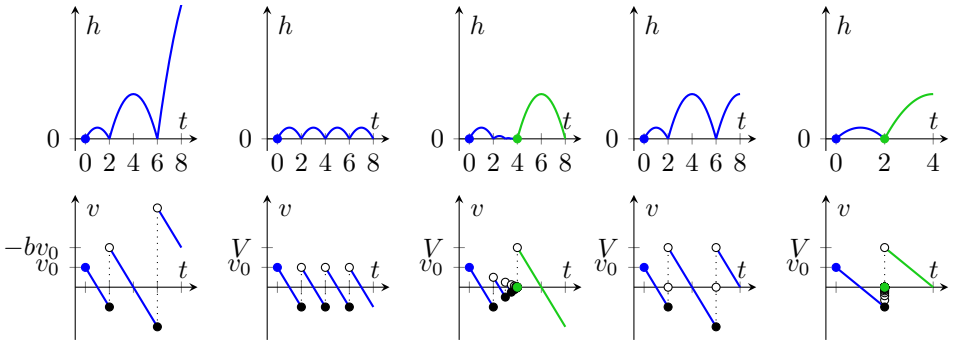
$$F = \{(m, \dot{m}) | m > 0 \wedge \dot{m} = -m\} \qquad G = \{(0, M)\}$$

whose behavior is depicted in Fig 2. Its closure is compact but it is no longer deterministic. Let $S_0 = [0, M]$ and $\mathcal{H}_0 = (F_0, G_0)$ with $F_0 = S_0 \times [-M, M]$ and $G_0 = S_0 \times S_0$, then



(a) $m_0 > 0$ (b) $m_0 = 0$

Figure 2: Trajectories and reachable states of $\mathcal{H}_D$ (Decay). In each case the set of states reachable from $I = \{m_0\}$ is on the left of the trajectory starting from m_0.



(a) $b < -1$ (b) $b = -1$ (c) $-1 < b < 0$ (d) $b = 0$ (e) $0 < b < 1$

Figure 3: Trajectories of $\mathcal{H}_B$ (Bouncing ball). All trajectories start from $(h = 0, v = v_0)$.

- $S_f = (0, m_0] \subset [0, M] = S_s = S_r = S_R$ when $0 < m_0 \leq M$
- $S_f = S_s = S_r = S_R = [0, M]$ when $0 = m_0$.

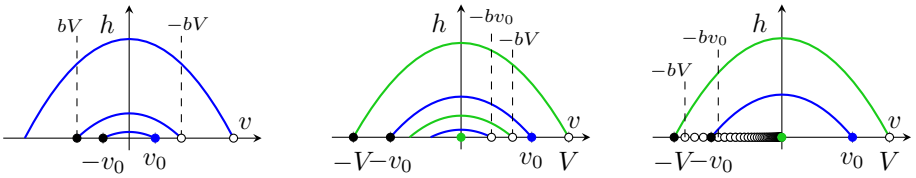
$S_s = S_r = S_R = S_0$, because $S_s = S_0$ and these subsets cannot be bigger than the support of $\mathcal{H}_0$. This result does not change, when $\mathcal{H}_0$ is replaced with a HS with a bigger support, but the proof is not as simple (see Sec 7.1).

7.3. Bouncing Ball

$\mathcal{H}_B = (F, G)$ of Example 2.8 is a deterministic HS on $\mathbb{R}^2$

- $F = \{((h, v), (\dot{h}, \dot{v}))|h > 0 \wedge \dot{h} = v \wedge \dot{v} = -1\}$
- $G = \{((0, v), (0, v^+))|v < 0 \wedge v^+ = b * v\} \uplus \{((0, 0), (0, V))\}$

its behavior depends on the coefficient of restitution b (see Fig 3). The closure of $\mathcal{H}_B$ is not compact and its support is the closed subset $\{(h, v)|0 \geq h\}$. However, compactness is irrelevant to define and compare S_f and S_s. Let $s_0 = (0, v_0)$ with $0 < v_0 < V$ and $S(u) \triangleq \{(h, v)|0 \geq h \wedge E(h, v) = E(0, u)\}$ be the set of states whose energy $E(h, v) = h + \frac{v^2}{2}$ is exactly $E(0, u)$, then the sets S_f and S_s are (see Fig 4):



(a) $b < -1$ (b) $-1 < b < 0$ (c) $0 < b < 1$

Figure 4: Set of reachable states of $\mathcal{H}_B$ (Bouncing ball). The set I is always $\{(h = 0, v = v_0)\}$. In case (a) there is an expanding sequence of parabolas $(-b)^n v_0 \to +\infty$. In case (b) there are two shrinking sequences of parabolas $(-b)^n v_0 \to 0$ and $(-b)^n V \to 0$.

1. $S_f = S_s = \bigcup_n S(b^n v_0)$ when $b < -1$
2. $S_f = S_s = S(v_0)$ when $b = -1$ (elastic bounce)
3. $S_f = \bigcup_n S(b^n v_0) \subset S_f \cup S(0) \cup (\bigcup_n S(b^n V)) = S_s$ when $-1 < b < 0$
4. $S_f = S_s = S(v_0) \cup S(0) \cup S(V)$ when $b = 0$ (inelastic bounce)
5. $S_f = S(v_0) \cup S'(b, v_0) \subset S_f \cup S(0) \cup S(V) \cup S'(b, V) = S_s$ when $0 < b < 1$, with $S'(b, u) \triangleq \{(0, -b^n u) | 0 \leq n\}$ sequence of instantaneous slowdowns
6. $S_f = S_s = S(v_0)$ when $b = 1$
7. $S_f = S_s = S(v_0) \cup S'(b, v_0)$ when $1 < b$, now $S'(b, u)$ is a sequence of instantaneous accelerations.

To make $\mathcal{H}_B$ compact, the simplest is to put an upper bound to the energy of the system, say $E_0 = E(0, V_0)$ with $V_0 > V$, and allow only b s. t. $|b| \leq 1$, so that the energy cannot increase when the ball bounces. More precisely, we make $\mathcal{H}_B$ compact with support $S_0 = \{(h, v) | 0 \leq h \wedge E(h, v) \leq E_0\}$ by taking

- $F = \{((h, v), (\dot{h}, \dot{v})) | (h, v) : S_0 \wedge \dot{h} = v \wedge \dot{v} = -1\}$
- $G = \{((0, v), (0, v^+)) | 0 \leq -v \leq V_0 \wedge v^+ = b * v\} \uplus \{((0, 0), (0, V))\}$.

To define S_R we fix another compact HS $\mathcal{H}_0 = (F_0, G_0)$ with support S_0. The simplest is to take $F_0 = F$ and replace G with a G_0 independent from b, namely

- $G_0 = \{((0, v), (0, v^+)) | 0 \leq -v \leq V_0 \wedge |v^+| \leq -v\} \uplus \{((0, 0), (0, V))\}$.

The relations among S_s, S_r and S_R, when $|b| \leq 1$ and $0 < v_0 < V < V_0$, are

1. $S_s = S_r = S(v_0) \subset \bigcup \{S(v) | v : [0, V]\} = S_R$ when $b = -1$ (elastic bounce)
2. $S_f = S_r = S_R = \bigcup_n S(b^n v_0) \cup S(0) \cup (\bigcup_n S(b^n V))$ when $-1 < b < 0$
3. $S_s = S_r = S_R = S(v_0) \cup S(0) \cup S(V)$ when $b = 0$ (inelastic bounce)
4. $S_s = S_r = S_R = S(v_0) \cup S'(b, v_0) \cup S(0) \cup S(V) \cup S'(b, V)$ when $0 < b < 1$
5. $S_s = S_r = S(v_0) \subset S(v_0) \cup S(V) \cup \{(0, v) | -v : [0, V]\} = S_R$ when $b = 1$.

There is an informal explanation for S_R in the case $b = -1$ (elastic bounce). After each bounce the ball may lose a bit of energy, thus after sufficiently many bounces it may stop (minimum energy). After a kick the energy will reach the maximum value allowed, and then it may decrease again after each bounce.

Thus any level of energy in $[0, E(0,V)]$ is reachable, assuming $0 < v_0 < V$. More formally we define $\mathcal{H}_\delta \ll \mathcal{H}$ in $\mathbb{H}_c(\mathcal{H}_0)$ s. t. $\mathcal{H}_\delta \to \mathcal{H}$ when $\delta \to 0$. Since $\mathcal{H}_0$ allows only perturbations in G, we define G_δ (for $\delta > 0$) as

$$\{((0,v),(0,v^+))|0 \leq -v \leq V_0 \wedge |v^+| \leq -v \wedge -v - \delta \leq v^+\} \uplus \{((0,0),(0,V))\}$$

When $-v$ is small, i. e., $0 \leq -v \leq \delta \leq V$, $|v^+| \leq -v$ and the energy is $\leq \frac{\delta^2}{2}$. Otherwise, $0 < \delta < -v$, v^+:$[-v-\delta, -v]$ and the energy loss is $\leq V\delta - \frac{\delta^2}{2}$.

Remark 7.1. It is important what $\mathcal{H}_0$ is chosen to capture the hard constraints of interest, because it can affect how S_R is computed. For instance, for the bouncing ball one may replace $\mathcal{H}_0$ with a *more relaxed* $\mathcal{H}'_0$

- $G'_0 = \{((0,v),(0,v^+))|0 \leq -v \leq V_0 \wedge |v^+| \leq V_0\} \uplus \{((0,0),(0,V))\}$

$\mathcal{H}'_0$ has the same support of $\mathcal{H}_0$, but $\mathcal{H}'_0 < \mathcal{H}_0$, because after a bounce the ball can increase its energy as far as it stays below the upper bound $E(0,V_0)$. This change results in a bigger subset S_R when $|b| = 1$, namely

- $S_0 = S_R$ when $b = -1$, i. e., any state in the support of $\mathcal{H}$ is reachable because of the more permissive perturbations
- $S(v_0) \cup S(V) \cup \{(0,v)| - v{:}[0,V_0]\} = S_R$ when $b = 1$.

Conclusions and Future Work

The main contributions of this paper concern reachability analysis in the context of hybrid (and continuous) systems.

First, we have proposed safe reachability $\mathsf{Rs}_{\mathcal{H}}(I)$, which computes an over-approximation of the set of states reachable in finite time from the set I of initial states by the HS $\mathcal{H}$, and compared it with the more naive reachability $\mathsf{Rf}_{\mathcal{H}}(I)$, which computes only an under-approximation.

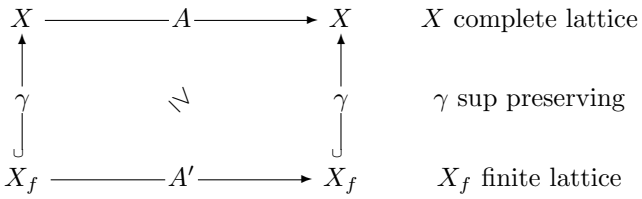
Second, and more importantly, we have addressed the issue of *robustness* of an analysis A cast as a monotonic map between complete lattices of a particular form (namely hyperspaces of metric spaces). In some cases robustness amounts to Scott continuity, and one can exploit the following facts:

- Every monotonic map A:$\mathbf{Po}(X,Y)$ between complete lattices has a best Scott continuous approximation $A^{\boxdot} \leq A$:$\mathbf{Po}(X,Y)$.
- When X is a continuous lattice, $A^{\boxdot}(x)$ is the sup of $\{A(b)|b \ll_X x\}$, i. e., it is computed by applying A to *way-below* approximations of x.

While the importance of safe/sound analyses is widely recognized, the issue of robustness is mostly overlooked (one reason being that for discrete systems it is not an issue). In our view, robustness has at least two immediate implications:

Modeling languages. There should be syntactic support to distinguish between hard and soft constraints on a HS $\mathcal{H}$. Hard constraints must be satisfied also by small perturbations $\mathcal{H}_\delta$. Thus, they identify the complete lattice (hyperspace) X where $\mathcal{H}$ is placed, while soft constraints provide the additional information to identify $\mathcal{H}$ uniquely within X. The distinction would be needed by tools that implement a robust analysis and can be ignored by other tools. In [11, 19] there is no explicit annotation for soft constraints, instead there is a re-interpretation of logical formula, which injects noise up to δ in specific sub-formulas.

Finite model checking. Counterexample-guided Abstraction & Refinement (CEGAR) is a general way of analyzing a system $\mathcal{H}$ with an infinite state space by leveraging finite model checking tools (see [6, 5]). In the setting of abstract interpretation, CEGAR amounts to approximating an analysis A:$\mathbf{Po}(X, X)$ with a *finite* analysis A':$\mathbf{Po}(X_f, X_f)$, i. e.,



Among these A':$\mathbf{Po}(X_f, X_f)$ there is a best one given by $A_f \triangleq \gamma^R \circ A \circ \gamma$.

If $\mathcal{H}$ is a HS on $\mathbb{R}^n$ with support included in a compact subset K, then there are at least three reachability analyses $\mathsf{Rs}^{\boxdot}_{\mathcal{H}} \leq \mathsf{Rs}_{\mathcal{H}} \leq \mathsf{Rf}_{\mathcal{H}}$:$\mathbf{Po}(X, X)$, where X is the continuous lattice $\mathbb{C}(K)$. In general, these analyses differ, and so do their best approximations on some finite lattice (counterexamples can be given using $\mathcal{H}_E$ and $\mathcal{H}_D$ in Examples 2.6 and 2.7).

However, when X is a continuous lattice and X_f is finite, an approximation A':$\mathbf{Po}(X_f, X_f)$ of A:$\mathbf{Po}(X, X)$ can be turned into an approximation of $A^{\boxdot}$, namely $A''(x) \triangleq A'(b)$ with b biggest element in X_f s. t. $\gamma(b) \ll_X \gamma(x)$.

As future work we plan to address **computability** issues. More specifically, given a compact HS $\mathcal{H}_0$ on $\mathbb{S}$ with support S_0, is $\mathsf{Rs}^{\boxdot}$:$\mathbf{Po}(\mathbb{H}_c(\mathcal{H}_0) \times \mathbb{C}(S_0), \mathbb{C}(S_0))$ computable? When $\mathbb{S}$ has a countable dense subset, all continuous lattices involved have a countable base, and the question is mathematically well-posed.

References

[1] S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Clarendon Press, Oxford, 1994.

[2] 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.

[3] A. Asperti and G. Longo. *Categories, Types and Scructures: an Introduction to Category Theory for the working Computer Scientist*. MIT Press, 1991.

[4] S. Awodey. *Category theory*. Oxford University Press, 2010.

[5] E. Clarke, A. Fehnker, Z. Han, B. Krogh, O. Stursberg, and M. Theobald. Verification of hybrid systems based on counterexample-guided abstraction refinement. In *TACAS*, volume 3, pages 192–207. Springer, 2003.

[6] E. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement. In *Computer aided verification*, pages 154–169. Springer, 2000.

[7] J. B. Conway. *A Course in Functional Analysis*. Springer, 2nd edition edition, 1990.

[8] P. Cousot and R. Cousot. Abstract interpretation frameworks. *Journal of logic and computation*, 2(4):511–547, 1992.

[9] P. J. L. Cuijpers. On bicontinuous bisimulation and the preservation of stability. In A. Bemporad, A. Bicchi, and G. Buttazzo, editors, *Hybrid Systems: Computation and Control*, volume 4416 of *Lecture Notes in Computer Science*, pages 676–679. Springer, 2007.

[10] P. J. L. Cuijpers and M. A. Reniers. Topological (bi-) simulation. *Electronic Notes in Theoretical Computer Science*, 100:49–64, 2004.

[11] W. Damm, G. Pinto, and S. Ratschan. Guaranteed termination in the verification of ltl properties of non-linear robust discrete time hybrid systems. *International Journal of Foundations of Computer Science*, 18(01):63–86, 2007.

[12] A. Edalat. Dynamical systems, measures and fractals via domain theory. *Information and Computation*, 120(1):32–48, July 1995.

[13] 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.

[14] 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.

[15] R. Goebel, R. G. Sanfelice, and A. Teel. Hybrid dynamical systems. *Control Systems, IEEE*, 29(2):28–93, 2009.

[16] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. Algorithmic analysis of nonlinear hybrid systems. *IEEE transactions on automatic control*, 43(4):540–554, 1998.

[17] K. Keimel. Domain theory its ramifications and interactions. *Electronic Notes in Theoretical Computer Science*, 333(Supplement C):3–16, 2017. The Seventh International Symposium on Domain Theory and Its Applications (ISDT).

[18] J. L. Kelley. *General topology*. Springer, 1975.

[19] 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.

[20] E. A. Lee. Cyber physical systems: Design challenges. In *Object oriented real-time distributed computing (isorc), 2008 11th ieee international symposium on*, pages 363–369. IEEE, 2008.

[21] A. Platzer. Differential dynamic logic for hybrid systems. *Journal of Automated Reasoning*, 41(2):143–189, 2008.

[22] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th design automation conference*, pages 731–736. ACM, 2010.

[23] J. Zhang, K. H. Johansson, J. Lygeros, and S. Sastry. Dynamical systems revisited: Hybrid systems with zeno executions. In *International Workshop on Hybrid Systems: Computation and Control*, pages 451–464. Springer, 2000.

Appendix A. Proofs

PROOF (**of Thm 3.3**). $\mathsf{Ef}(I)$ and $\mathsf{Rf}(I)$ are the least prefix-points of some monotonic maps on complete lattices of the form $(\mathsf{P}(\mathbb{S}), \subseteq)$. Thus, we can exploit the universal property of the least prefix-point X for a monotonic map F, i. e., $F(Y) \leq Y \implies X \leq Y$.

1. Consider the monotonic maps F and F_I on $\mathsf{P}(\mathbb{T} \times \mathbb{S})$:

$$F(S) \triangleq \{(t+d, s') | \exists s.(t,s){:}S \wedge s \xrightarrow{d} s'\}, \quad F_I(S) \triangleq (\{0\} \times I) \cup F(S).$$

   $\mathsf{Ef}(I)$ is the least prefix-point of F_I. Since $F_{I_0}(S) \subseteq F_{I_1}(S)$ when $I_0 \subseteq I_1$, a prefix-point for F_{I_1} is also a prefix-point for F_{I_0}. Hence, we conclude that $\mathsf{Ef}(I_0) \subseteq \mathsf{Ef}(I_1)$.
   Since $I \subseteq \cup K$ when $I{:}K$, then $\mathsf{Ef}(I) \subseteq \mathsf{Ef}(\cup K)$. Now, let $U = \{\mathsf{Ef}(I) | I{:}K\}$. To prove $\mathsf{Ef}(\cup K) \subseteq \cup U$, observe that:

   - F preserves unions, thus $F(\cup U) = \cup\{F(S) | S{:}U\}$;
   - $\forall S{:}U.F(S) \subseteq S$, thus $F(\cup U) = \cup U$;
   - $\forall I{:}K.\exists S{:}U.\{0\} \times I \subseteq S$, thus $\{0\} \times (\cup K) \subseteq \cup U$.

   Therefore, $\cup U$ is a prefix-point for $F_{\cup K}$.
2. Consider the monotonic maps G and G_I on $\mathsf{P}(\mathbb{S})$:

$$G(S) \triangleq \{s' | \exists s{:}S.s \longrightarrow s'\}, \quad G_I(S) \triangleq I \cup G(S).$$

   $\mathsf{Rf}(I)$ is the least prefix-point of G_I. By analogy with the previous point, one can prove that Rf is monotonic and preserves unions.
   Let S be a prefix-point of G_I, i. e., $G_I(S) \subseteq S$. Then:

   - $I \subseteq S$, because $I \subseteq G_I(S)$.
   - $G_S(S) \subseteq S$, because $G(S) \subseteq G_I(S)$ and $G_S(S) = S \cup G(S)$.

   By taking $S = \mathsf{Rf}(I)$, we conclude $I \subseteq \mathsf{Rf}(I) \subseteq \mathsf{Rf}(\mathsf{Rf}(I)) \subseteq \mathsf{Rf}(I)$.
   To prove $\pi(\mathsf{Ef}(I)) = \mathsf{Rf}(I)$, observe that:

   - $\forall E{:}\mathsf{P}(\mathbb{T} \times \mathbb{S}).\pi(F_I(E)) = G_I(\pi(E))$. Hence, $\pi(\mathsf{Ef}(I)) \supseteq \mathsf{Rf}(I)$.
   - $\forall S{:}\mathsf{P}(\mathbb{S}).G_I(S) \subseteq S \implies F_I(\mathbb{T} \times S) \subseteq \mathbb{T} \times S$.

   Therefore, $\mathsf{Ef}(I) \subseteq \mathbb{T} \times \mathsf{Rf}(I)$, and consequently, $\pi(\mathsf{Ef}(I)) \subseteq \mathsf{Rf}(I)$.
3. Consider the monotonic maps F_I on $\mathsf{P}(\mathbb{T} \times \mathbb{S})$, G_I on $\mathsf{P}(\mathbb{S})$, G^t_J on $\mathsf{P}(\mathbb{R} \times \mathbb{S})$, whose least prefix-points are $\mathsf{Ef}_{\mathcal{H}}(I)$, $\mathsf{Rf}_{\mathcal{H}}(I)$, and $\mathsf{Rf}_{t(\mathcal{H})}(J)$, respectively.
   Since $(t,s) \xrightarrow[t(\mathcal{H})]{} (t+d, s') \iff 0 \leq d \wedge s \xrightarrow[\mathcal{H}]{d} s'$, by Prop 2.10, these maps are related as follows:

   - $\forall E{:}\mathsf{P}(\mathbb{T} \times \mathbb{S}).F_I(E) = G^t_{\{0\} \times I}(E)$, so $\mathsf{Ef}_{\mathcal{H}}(I) = (\mathsf{Rf}_{t(\mathcal{H})}(\{0\} \times I)$.
   - $\forall S{:}\mathsf{P}(\mathbb{R} \times \mathbb{S}).\pi(G^t_J(S)) = G_{\pi(J)}(\pi(S))$, so $\pi(\mathsf{Rf}_{t(\mathcal{H})}(J)) \supseteq \mathsf{Rf}_{\mathcal{H}}(\pi(J))$.
   - $\forall S{:}\mathsf{P}(\mathbb{S}).G_{\pi(J)}(S) \subseteq S \implies G^t_J(\mathbb{R} \times S) \subseteq \mathbb{R} \times S$.

As a result, $\mathsf{Rf}_{t(\mathcal{H})}(J) \subseteq \mathbb{R} \times \mathsf{Rf}_{\mathcal{H}}(\pi(J))$, and $\pi(\mathsf{Rf}_{t(\mathcal{H})}(J)) \subseteq \mathsf{Rf}_{\mathcal{H}}(\pi(J))$. □

Proof (**of Thm 3.8**). $\mathsf{Es}(I)$ and $\mathsf{Rs}(I)$ are defined as least prefix-points of monotonic maps on complete lattices of the form $(\mathsf{C}(\mathbb{S}), \subseteq)$, $\mathsf{C}(\mathbb{S})$ is closed w. r. t. arbitrary intersections and finite unions computed in $\mathsf{P}(\mathbb{S})$, and the monotonic map $S \mapsto \overline{S}$ from $\mathsf{P}(\mathbb{S})$ to $\mathsf{C}(\mathbb{S})$ preserves finite unions.

1. $\mathsf{Es}(I)$ is the least prefix-point of a monotonic map F'_I on $\mathsf{C}(\mathbb{T} \times \mathbb{S})$ given by:
$$F'_I(S) \triangleq (\{0\} \times I) \cup \overline{\{(t+d, s') | \exists s.(t,s){:}S \wedge s \xrightarrow{d} s'\}},$$
and the properties of Es are proved similar to those of Ef, except for the need to restrict to finite unions.
2. $\mathsf{Rs}(I)$ is the least prefix-point of a monotonic map G'_I on $\mathsf{C}(\mathbb{S})$ given by:
$$G'_I(S) \triangleq I \cup \overline{\{s' | \exists s{:}S.s \longrightarrow s'\}},$$
and the properties of Rs are proved by analogy with those of Rf. In particular, $\pi(\mathsf{Es}(I)) \subseteq \mathsf{Rs}(I)$ follows from:
$$\forall S{:}\mathsf{C}(\mathbb{S}).G'_I(S) \subseteq S \implies F'_I(\mathbb{T} \times S) \subseteq \mathbb{T} \times S.$$
As a result, $\mathsf{Es}(I) \subseteq \mathbb{T} \times \mathsf{Rs}(I)$, and consequently $\pi(\mathsf{Es}(I)) \subseteq \mathsf{Rs}(I)$.
3. If $I{:}\mathsf{P}(\mathbb{S})$ and $S{:}\mathsf{P}(\mathbb{T} \times \mathbb{S})$, then $I \subseteq \overline{I}{:}\mathsf{C}(\mathbb{S})$ and $F_I(S) \subseteq F'_{\overline{I}}(S){:}\mathsf{C}(\mathbb{T} \times \mathbb{S})$. Hence, $\mathsf{Ef}(I) \subseteq \mathsf{Es}(\overline{I}){:}\mathsf{C}(\mathbb{T} \times \mathbb{S})$, and consequently $\mathsf{Ef}(I) \subseteq \mathsf{Es}(\overline{I})$.
The inclusion $\mathsf{Rf}(I) \subseteq \mathsf{Rs}(\overline{I})$ follows from $\mathsf{Ef}(I) \subseteq \mathsf{Es}(\overline{I})$, since:
   - $\mathsf{Rf}(I) = \pi(\mathsf{Ef}(I))$, by Thm 3.3.
   - $\pi(\mathsf{Es}(\overline{I})) \subseteq \mathsf{Rs}(\overline{I})$, by the previous point.
4. Consider the monotonic maps F'_I on $\mathsf{C}(\mathbb{T} \times \mathbb{S})$, G'_I on $\mathsf{C}(\mathbb{S})$, and G^t_J on $\mathsf{C}(\mathbb{R} \times \mathbb{S})$, whose least prefix-points are $\mathsf{Es}_{\mathcal{H}}(I)$, $\mathsf{Rs}_{\mathcal{H}}(I)$ and $\mathsf{Rs}_{t(\mathcal{H})}(J)$, respectively. Since $(t,s) \xrightarrow[t(\mathcal{H})]{} (t+d, s') \iff 0 \leq d \wedge s \xrightarrow[\mathcal{H}]{d} s'$, by Prop 2.10, these maps are related as follows:
   - $\forall E{:}\mathsf{C}(\mathbb{T} \times \mathbb{S}).F'_I(E) = G^t_{\{0\} \times I}(E)$, so $\mathsf{Es}_{\mathcal{H}}(I) = (\mathsf{Rs}_{t(\mathcal{H})}(\{0\} \times I)$.
   - $\forall S{:}\mathsf{C}(\mathbb{S}).G'_{\overline{\pi(J)}}(S) \subseteq S \implies G^t_J(\mathbb{R} \times S) \subseteq \mathbb{R} \times S$.

   Hence, $\mathsf{Rs}_{t(\mathcal{H})}(J) \subseteq \mathbb{R} \times \mathsf{Rs}_{\mathcal{H}}(\overline{\pi(J)})$, and $\pi(\mathsf{Rs}_{t(\mathcal{H})}(J)) \subseteq \mathsf{Rs}_{\mathcal{H}}(\overline{\pi(J)})$. □

Appendix A.1. Proofs related to Robustness

In order to relate different properties of monotonic maps $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$, where $\mathbb{S}_1$ and $\mathbb{S}_2$ are metric spaces, we move to the category **Top** of topological spaces, by considering suitable topologies on $\mathsf{C}(\mathbb{S})$.

Definition A.1 (Topologies). Given a metric space $\mathbb{S}$, let $\mathsf{O}(\mathbb{S}) \subseteq \mathsf{P}(\mathbb{S})$ be the topology induced by the metric, namely $O{:}\mathsf{O}(\mathbb{S}) \iff \forall x{:}O.\exists \delta > 0.B(x,\delta) \subseteq O$, and for $S{:}\mathsf{P}(\mathbb{S})$ $B(S,\delta) \triangleq \bigcup\{B(x,\delta) | s{:}S\}{:}\mathsf{O}(\mathbb{S})$ and let $\uparrow S \triangleq \{C{:}\mathsf{C}(\mathbb{S}) | C \subseteq S\}$. We define four topologies on $\mathsf{C}(\mathbb{S})$, namely given $U \subseteq \mathsf{C}(\mathbb{S})$ we say that

- U is **Alexandrov open** $\stackrel{\triangle}{\iff} \forall C{:}U.\uparrow C \subseteq U$.
- U is **Upper open** $\stackrel{\triangle}{\iff} \forall C{:}U.\exists O{:}\mathsf{O}(\mathbb{S}).C \in \uparrow O \subseteq U$.
- U is **Robust open** $\stackrel{\triangle}{\iff} \forall C{:}U.\exists \delta > 0.\uparrow B(C,\delta) \subseteq U$.
- U is **Scott open** $\stackrel{\triangle}{\iff} \forall D \subseteq \mathsf{C}(\mathbb{S}).(\bigcap D){:}U \implies \exists D_0 \subset_f D.\uparrow(\bigcap D_0){:}U$, where $\bigcap D$ is the intersection of all subsets in D, and $D_0 \subset_f D$ means that D_0 is a finite subset of D.

Alexandrov and Scott topologies are order-theoretic: Alexandrov topology is definable on (the carrier of) any poset $X = (|X|, \leq_X)$ and the monotonic maps between two posets are exactly the continuous maps w. r. t. the corresponding Alexandrov topologies; Scott topology (in the form given above) is definable on any complete lattice. We have specialized their definitions to the complete lattice $\mathbb{C}(\mathbb{S})$ with carrier $\mathsf{C}(\mathbb{S})$ and $\leq$ given by reverse inclusion.

Vietoris topology, which can be decomposed in upper and lower Vietoris topologies, is definable on $\mathsf{C}(\mathbb{S})$ for any topological space $\mathbb{S}$. We consider only the upper Vietoris topology and call it Upper topology for short.

Among the four topologies, the Robust topology is the only one which depends on the metric on $\mathbb{S}$, the other depend only on the topology on $\mathbb{S}$ induced by the metric. We show that the robust monotonic maps (Def 4.1) are exactly the continuous maps for the robust topology.

Theorem A.2. *Given a map $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$ with $\mathbb{S}_1$ and $\mathbb{S}_2$ metric spaces, the following properties are equivalent:*

1. *A is monotonic and robust.*
2. *A is continuous w. r. t. the Robust topologies.*

Proof. We exploit the following facts valid in any metric space:

(F1) $B(B(S,\delta),\delta') \subseteq B(S,\delta+\delta')$.

(F2) $S \subseteq \overline{S} = \bigcap\{B(S,\delta) | \delta > 0\}$.

(F3) $B(S,\delta) \subseteq S_\delta \stackrel{\triangle}{=} \overline{B(S,\delta)} \subseteq B(S,\delta')$ when $\delta < \delta'$.

(1) $\implies$ (2). Given $U_2 \subseteq \mathsf{C}(\mathbb{S}_2)$ open (for the Robust topology), we have to prove that $U_1 \stackrel{\triangle}{=} A^{-1}(U_2) \subseteq \mathsf{C}(\mathbb{S}_1)$ is open. U_1 is downward closed, because U_2 is downward closed and A is monotonic. Moreover, for every $C{:}U_1$ we have to find $\delta > 0$ such that $\uparrow B(C,\delta) \subseteq U_1$:

- $A(C){:}U_2$ and U_2 open imply that $\uparrow B(A(C),\delta') \subseteq U_2$ for some $\delta' > 0$.
- Let ϵ be in $(0,\delta')$. By (F3), we get $A(C)_\epsilon \subseteq B(A(C),\delta')$.
- By robustness of A, there exists $\delta > 0$ such that $A(C_\delta) \subseteq A(C)_\epsilon$.
- If $C'{:}\uparrow B(C,\delta)$, then $C' \subseteq C_\delta$, thus $A(C') \subseteq A(C_\delta)$ by monotonicity of A.

- Therefore $C'{:}U_1$, i. e., $A(C'){:}U_2$, because $A(C'){:}\uparrow B(A(C),\delta') \subseteq U_2$.

$(2) \Longrightarrow (1)$. First we prove that A is monotonic. More precisely, we show that $C \subseteq D$ and $A(C) \not\subseteq A(D)$ leads to a contradiction. In fact, take $s{:}A(C) - A(D)$ and let $U_2 = \{D'{:}\mathsf{C}(\mathbb{S}_2) | s \notin D'\}$, then

- U_2 is open, because $s \notin D'$ implies $s \notin B(D',\epsilon)$ for some $\epsilon > 0$.
- $U_1 \triangleq A^{-1}(U_2)$ is open, because A is continuous and U_2 is open.
- $D \in U_1$ and $C \notin U_1$, by definition of U_1.
- But U_1 is downward closed, thus one get the contradiction $C \in U_1$.

Then we show that A is robust at $C{:}\mathsf{C}(\mathbb{S}_1)$, i. e., $\forall\epsilon > 0.\exists\delta > 0.A(C_\delta) \subseteq A(C)_\epsilon$. Let $U_2 \triangleq \{C'{:}\mathsf{C}(\mathbb{S}_2) | \exists\epsilon' > 0.B(C',\epsilon') \subseteq B(A(C),\epsilon)\}$, then $U_2 \subseteq\uparrow B(A(C),\epsilon)$. We prove that U_2 is open, i. e., $\forall C'{:}U_2.\exists\delta > 0.\uparrow B(C',\delta) \subseteq U_2$:

- $C'{:}U_2$ implies $B(C',\epsilon') \subseteq B(A(C),\epsilon)$ for some $\epsilon' > 0$.
- By (F1), $B(B(C',\delta),\delta) \subseteq B(C',\epsilon')$ when $\delta = \epsilon'/2$.
- Therefore, $\uparrow B(C',\delta) \subseteq U_2$.

$U_1 \triangleq A^{-1}(U_2)$ is open, because A is continuous and U_2 is open. But $C{:}U_1$. Therefore, there exists $\delta' > 0$ such that $\uparrow B(C,\delta') \subseteq U_1$. If δ is in $(0,\delta')$, then (F3) implies that $C_\delta \subseteq B(C,\delta')$. Hence, $C_\delta{:}U_1$ and $A(C_\delta){:}U_2$, which implies $A(C_\delta) \subseteq B(A(C),\epsilon) \subseteq A(C)_\epsilon$. □

Lemma A.3. *In a metric space the following implications hold:*

1. *U Scott open* $\Longrightarrow$
2. *U Robust open* $\Longrightarrow$
3. *U Upper open* $\Longrightarrow$
4. *U Alexandrov open.*

Proof. We rely on (F1-F3), see the proof of Thm A.2, to prove the implications:

- $(1) \Longrightarrow (2)$. If U is Scott open and $C{:}U$, let $O_n \triangleq B(C,2^{-n})$, we prove that $\uparrow O_n \subseteq U$ for some n.

  Let $C_n \triangleq \overline{O_n}$ and $D \triangleq \{C_n | n{:}\omega\}$, then $C_n \supseteq O_n \supseteq C_{n+1}$ and $C = \bigcap D{:}U$, thus $\uparrow C_n \subseteq U$, for some n.

  Since $O_n \subseteq C_n{:}U$, then $\uparrow O_n \subseteq\uparrow C_n \subseteq U$.

- $(2) \Longrightarrow (3)$. If U is robust open and $C{:}U$, then there exists $\delta > 0$ for which $\uparrow B(C,\delta) \subseteq U$. Thus, $O = B(C,\delta){:}\mathsf{O}(\mathbb{S})$ is such that $C \in\uparrow O \subseteq U$.

- $(3) \Longrightarrow (4)$. If U is upper open, then U is the union of subsets of the form $\uparrow O$, thus it is Alexandrov open. □

Theorem A.4. *In a compact metric space the Upper topology is included in the Scott topology. Therefore, Scott, Robust and Upper topologies coincide.*

PROOF. When $\mathbb{S}$ is a compact metric space, the closed subsets coincide with the compact subsets. To prove that the Upper topology is included in the Scott topology, it suffices to show that for any open subset O of $\mathbb{S}$, the subset $\uparrow O$ of $\mathsf{C}(\mathbb{S})$ is Scott open. Let C be the complement of O and $D = \{K_i|i{:}I\}$ an I-indexed family of closed subsets such that $K = (\bigcap\{K_i|i{:}I\} \subseteq O$, then $K'_i = K_i \cap C$ is another I-indexed family D' of closed subsets whose intersection is $\emptyset$. Since compact subsets have the *finite intersection property*, there is $J \subset_f I$ such that $\bigcap\{K'_i|i{:}J\} = \emptyset$, or equivalently, $\bigcap\{K_i|i{:}J\}{:}\uparrow O$.

The coincidence of the three topologies (Scott, Robust and Upper) follows immediately from the inclusions established in Lemma A.3. □

Example A.5. We give a metric space $\mathbb{S}$ where the four topologies on $\mathsf{C}(\mathbb{S})$ differ. Let $\mathbb{S} = \{x|x > 0\}$ be the set of positive reals with the usual metric $d(x, y) = |y - x|$, and define $x_n \triangleq 2^{-n}$ and $\delta_n \triangleq x_{n+1}$. Then, $C = \{x_n|n{:}\omega\}$ is a closed subset of $\mathbb{S}$, $O = \cup_n B(x_n, \delta_n)$ is an open subset of $\mathbb{S}$, and the following counter-examples show that the four topologies differ:

- $\uparrow C$ is Alexandrov open, but it is not open in the other topologies.
- $\uparrow O$ is upper open, but it is not robust open, because $C{:}\uparrow O$ but there is no $\delta > 0$ such that $B(C, \delta) \subseteq O$, because $(0, \delta) \subseteq B(C, \delta)$ but $(0, \delta) \not\subseteq O$.
- $\uparrow \emptyset = \{\emptyset\}$ is robust open, because $B(\emptyset, \delta) = \emptyset$, but it is not Scott open, because $C_n = \{x|x \geq 2^n\}$ are closed subsets of $\mathbb{S}$ such that $\emptyset \subset C_{n+1} \subset C_n$, whose intersection is $\emptyset$.

PROOF (**of Corr 4.4 and 4.5**). If $\mathbb{S}_1$ and $\mathbb{S}_2$ are compact metric spaces, then Thm A.4 implies that a monotonic map $A{:}\mathsf{C}(\mathbb{S}_1) \to \mathsf{C}(\mathbb{S}_2)$, or equivalently an arrow $A{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$, is robust exactly when it is Scott continuous.

- By Thm 5.15 every $A{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$ has a best continuous approximation $A^{\boxdot}{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_2))$.
- $\mathbb{C}(\mathbb{S}_1)$ is a continuous lattice with way-below relation $\ll$ definable in terms of fattening, as shown in Example 5.18. Therefore, one can use the characterization of $A^{\boxdot}$ in Thm 5.20 and replace $\{b|b \ll C\}$ with $\{C_\delta|\delta > 0\}$.
- By Thm 5.15 every $A{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_1))$, has a best continuous co-monad approximation $A_{\boxplus}{:}\mathbf{Po}(\mathbb{C}(\mathbb{S}_1), \mathbb{C}(\mathbb{S}_1))$. Since the order on $\mathbb{C}(\mathbb{S}_1)$ is reverse inclusion, the co-monad properties become $C \subseteq A_{\boxplus}(C) = A^2_{\boxplus}(C)$. □