University of Pennsylvania
ScholarlyCommons

Technical Reports (CIS) | Department of Computer & Information Science

January 2005

Approximation Metrics for Discrete and Continuous Systems

Antoine Girard
University of Pennsylvania

George J. Pappas
University of Pennsylvania, pappasg@seas.upenn.edu

Follow this and additional works at: http://repository.upenn.edu/cis_reports

Recommended Citation
Girard, Antoine and Pappas, George J., "Approximation Metrics for Discrete and Continuous Systems" (2005). *Technical Reports (CIS)*. Paper 54.
http://repository.upenn.edu/cis_reports/54

University of Pennsylvania Department of Computer and Information Science Technical Report No. MS-CIS-05-10.

This paper is posted at ScholarlyCommons. http://repository.upenn.edu/cis_reports/54
For more information, please contact repository@pobox.upenn.edu.

Approximation Metrics for Discrete and Continuous Systems

Abstract
Established system relationships for discrete systems, such as language inclusion, simulation, and bisimulation, require system observations to be identical. When interacting with the physical world, modeled by continuous or hybrid systems, exact relationships are restrictive and not robust. In this paper, we develop the first framework of system approximation that applies to both discrete and continuous systems by developing notions of approximate language inclusion, approximate simulation, and approximate bisimulation relations. We define a hierarchy of approximation pseudo-metrics between two systems that quantify the quality of the approximation, and capture the established exact relationships as zero sections. Our approximation framework is compositional for synchronous composition operators. Algorithms are developed for computing the proposed pseudo-metrics, both exactly and approximately. The exact algorithms require the generalization of the fixed point algorithms for computing simulation and bisimulation relations, or dually, the solution a static game whose cost is the so-called branching distance between the systems. Approximations for the pseudo-metrics can be obtained by considering Lyapunov-like functions called simulation and bisimulation functions. We illustrate our approximation framework in reducing the complexity of safety verification problems for both deterministic and nondeterministic continuous systems.

Comments
University of Pennsylvania Department of Computer and Information Science Technical Report No. MS-CIS-05-10.

This technical report is available at ScholarlyCommons: http://repository.upenn.edu/cis_reports/54

APPROXIMATION METRICS FOR DISCRETE AND CONTINUOUS SYSTEMS

ANTOINE GIRARD AND GEORGE J. PAPPAS

Abstract. Established system relationships for discrete systems, such as language inclusion, simulation, and bisimulation, require system observations to be identical. When interacting with the physical world, modeled by continuous or hybrid systems, exact relationships are restrictive and not robust. In this paper, we develop the first framework of system approximation that applies to both discrete and continuous systems by developing notions of approximate language inclusion, approximate simulation, and approximate bisimulation relations. We define a hierarchy of approximation pseudo-metrics between two systems that quantify the quality of the approximation, and capture the established exact relationships as zero sections. Our approximation framework is compositional for synchronous composition operators. Algorithms are developed for computing the proposed pseudo-metrics, both exactly and approximately. The exact algorithms require the generalization of the fixed point algorithms for computing simulation and bisimulation relations, or dually, the solution a static game whose cost is the so-called branching distance between the systems. Approximations for the pseudo-metrics can be obtained by considering Lyapunov-like functions called simulation and bisimulation functions. We illustrate our approximation framework in reducing the complexity of safety verification problems for both deterministic and nondeterministic continuous systems.

1. Introduction

Compositional modeling in concurrency theory [Mil89], and complexity reduction in the formal verification of discrete systems [CGP00] have resulted in a wealth of system relationships, including the established notions of language inclusion, simulations and bisimulations [CGP00]. These notions have had great impact in not only reducing the complexity of discrete systems [BCM$^+$90], but also in reducing problems for continuous and hybrid systems to purely discrete problems [AHP00]. Much more recently, the notions of simulation and bisimulation have resulted in new equivalence notions for nondeterministic continuous [Pap03, TP04, vdS04] and hybrid systems [HTP05, JvdS04, PvdSB04].

The notions of language inclusion, simulation, and bisimulation for both discrete and continuous systems are all *exact*, requiring external behavior of two systems to be identical. As exact relationships between discrete systems do not permit any error, there are clear limitations in the amount of system compression that can be achieved. Approximate relationships which do allow for the possibility of error, will certainly allow for more dramatic system compression. Even though this has been the tradition for deterministic continuous systems [ASG00], it has been recently argued convincingly [CB02, PHW03, vBMOW03], that even for more quantitative classes of finite transition systems, such as labeled Markov processes [DGJP04], probabilistic automata [vBMOW03], and quantitative transition systems [dAFS04], notions of system approximation are not only better candidates for complexity reduction but also provide more robust relationships between systems. The challenge in developing approximate system relationships is the quantification of the quality of the approximation.

This research is partially supported by the Région Rhône-Alpes (Projet CalCel) and the National Science Foundation Presidential Early CAREER (PECASE) Grant 0132716.

The goal of this paper is to provide a theory of system approximation that applies to both finite (discrete) and infinite (continuous) transition systems by providing approximate generalizations of language inclusion, simulation, and bisimulation. By generalizing the exact notions we ensure that our framework captures the traditional exact notions for finite systems as a special case, while developing more robust notions of system approximation for infinite transition systems.

To technically achieve our goal, we consider metric transition systems, which are transition systems equipped with metrics on the state space and the observation space. Based on observation metric, we develop a hierarchy of approximation pseudo-metrics between two metric transition systems measuring the distance from reachable set inclusion and equivalence, language inclusion and equivalence, simulation and bisimulation relations. For a large subclass of systems, the notions of exact language inclusion, simulation, and bisimulation are naturally captured as the zero sections of the pseudo-metrics. Furthermore, the relationship among the various approximation metrics is analogous to the relationship among the exact notions. For synchronous composition of metric transition systems, we show that the language, simulation and bisimulation metrics are compositional.

We then propose algorithms for computing the proposed pseudo-metrics, both exactly and approximately. Algorithms for exact computation require the generalization of the fixed point algorithms for computing simulation and bisimulation relations [KS90], or dually, the solution a static game whose cost is the so-called branching distance between the systems [dAFS04]. Algorithmic relaxations for computing approximations of the pseudo-metrics can be obtained by considering Lyapunov-like functions called simulation and bisimulation functions, which are also shown to be compositional.

This line of research has been motivated by the algorithmic verification of hybrid systems. The significant progress in the formal verification of discrete systems [BCM$^+$90], has inspired a plethora of sophisticated methods for safety verification of continuous and hybrid systems. The approaches range from discrete and predicate abstraction methods [AHP00, ADI02, TK02], to reachability computations [ABDM00, ADG03, CK99, KV00, MT00, Gir05], to Lyapunov-like barriers [PJ04]. However, progress on continuous (and thus hybrid) systems has been limited to systems of small continuous dimension, motivating research on model reduction [HK04], and projection based methods [AD04] for safety verification.

Since the results of this paper could be of great use in the above methods, we conclude this paper with two continuous examples that illustrate how our framework can be used in computing an over-approximation of the distance between two systems, and in reducing the complexity of safety verification for both deterministic and nondeterministic continuous systems. These examples, even though they illustrate the power of our approximation framework, are simple cases of a more systematic computational framework that is currently under development for linear systems [GP05a] and nonlinear systems [GP05b], and will be part of a future publication.

2. Exact Relationships for Transition Systems

2.1. **Transition systems.** In this paper, we will consider the framework of transition systems which enable us to model in a unified way both discrete and continuous systems with either deterministic or nondeterministic dynamics (see *e.g.* [Pap03]). The results in this section can be reviewed in much greater detail in [CGP00].

Definition 2.1 (Transition system)**.** A (labeled) transition system with observations is a tuple $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\langle . \rangle\rangle)$ that consists of:

- a (possibly infinite) set Q of states,
- a (possibly infinite) set Σ of labels,
- a transition relation $\rightarrow \subseteq Q \times \Sigma \times Q$,
- a (possibly infinite) set $Q^0 \subseteq Q$ of initial states,
- a (possibly infinite) set Π of observations,
- an observation map $\langle\langle . \rangle\rangle : Q \rightarrow \Pi$.

The set of labeled transition systems associated to a set of labels Σ and a set of observations Π is denoted $\mathcal{T}(\Sigma, \Pi)$.

A transition $(q, \sigma, q') \in \rightarrow$ will be denoted $q \xrightarrow{\sigma} q'$. We assume that the systems we consider are *non-blocking* so that for all $q \in Q$, there exists at least one transition $q \xrightarrow{\sigma} q'$ of T. If for any state $q \in Q$ and any label $\sigma \in \Sigma$, there exists at most a unique transition $q \xrightarrow{\sigma} q'$ of T and, in addition, the set of initial states Q^0 contains a single element, then T is called *deterministic*. Transition system T is called *finite* if Q and Σ are finite sets, and *infinite* otherwise. For all labels $\sigma \in \Sigma$, the σ-successor is defined as the set valued map given by

$$\forall q \in Q,\ \mathrm{Post}^{\sigma}(q) = \left\{ q' \in Q |\ q \xrightarrow{\sigma} q' \right\}.$$

We denote with $\mathrm{Supp}(\mathrm{Post}^{\sigma})$ the support of the σ-successor which is the subset of elements $q \in Q$ such that $\mathrm{Post}^{\sigma}(q)$ is not empty. A state trajectory of T is an infinite sequence of transitions,

$$q^0 \xrightarrow{\sigma^0} q^1 \xrightarrow{\sigma^1} q^2 \xrightarrow{\sigma^2} \ldots, \text{ where } q^0 \in Q^0.$$

An external trajectory is a sequence of elements of $\Pi \times \Sigma \times \Pi$ of the form $\pi^0 \xrightarrow{\sigma^0} \pi^1 \xrightarrow{\sigma^1} \pi^2 \xrightarrow{\sigma^2} \ldots$. The set of all external trajectories associated to a set of labels Σ and a set of observations Π is denoted $\mathcal{E}(\Sigma, \Pi)$. An external trajectory is accepted by transition system T if there exists a state trajectory of T, such that for all $i \in \mathbb{N}$, $\pi^i = \langle\langle q^i \rangle\rangle$. The set of external trajectories accepted by transition system T is called the language of T, and is denoted by $L(T)$. The reachable set of T is the subset of Π defined by:

$$\mathrm{Reach}(T) = \left\{ \pi \in \Pi |\ \exists \{\pi^i \xrightarrow{\sigma^i} \pi^{i+1}\}_{i \in \mathbb{N}} \in L(T),\ \exists j \in \mathbb{N},\ \pi^j = \pi \right\}.$$

One of the most important problems for transition systems is the safety verification problem. The *safety verification problem* asks whether the intersection of $\mathrm{Reach}(T)$ with an unsafe set $\Pi_U \subseteq \Pi$ is empty or not. The verification of finite transition systems of very high cardinality has motivated the development of various notion of system equivalence and system refinement that potentially reduce the complexity of safety verification [CGP00].

2.2. **Exact transition system relationships.** For complexity reduction as well as for enabling compositional modeling and analysis, various notions of *exact* system equivalence and refinement have been established in the formal methods community [CGP00]. In this section, we quickly review the established exact relationships in order to develop approximate versions in the subsequent sections.

Let $T_1 = (Q_1, \Sigma_1, \rightarrow_1, Q_1^0, \Pi_1, \langle\langle . \rangle\rangle_1)$ and $T_2 = (Q_2, \Sigma_2, \rightarrow_2, Q_2^0, \Pi_2, \langle\langle . \rangle\rangle_2)$ be two labeled transition systems with the same set of labels ($\Sigma_1 = \Sigma_2 = \Sigma$) and the same set of observations ($\Pi_1 = \Pi_2 = \Pi$) (*i.e.* T_1 and T_2 are elements of $\mathcal{T}(\Sigma, \Pi)$).

If $L(T_1) \subseteq L(T_2)$, then it is clear from the definition of the reachable set that $\mathrm{Reach}(T_1) \subseteq \mathrm{Reach}(T_2)$. Thus, given an unsafe set Π_U, if T_2 is safe then T_1 is safe, since if the intersection of $\mathrm{Reach}(T_2)$ and

Π_U is empty then it follows that the intersection of $\mathrm{Reach}(T_1)$ and Π_U is also empty. Similarly, we obtain that if $L(T_1) = L(T_2)$ then $\mathrm{Reach}(T_1) = \mathrm{Reach}(T_2)$. However, given two transition systems T_1 and T_2, checking *language inclusion* ($L(T_1) \subseteq L(T_2)$) and *language equivalence* ($L(T_1) = L(T_2)$) is computationally demanding for finite transition systems, and infeasible for most infinite transition systems. This has motivated the development of stronger notions of system refinement and equivalence, namely simulation and bisimulation.

Definition 2.2 (Simulation)**.** A relation $\mathcal{S} \subseteq Q_1 \times Q_2$ is called a simulation relation (of T_1 by T_2) if for all $(q_1, q_2) \in \mathcal{S}$:

(1) $\langle\langle q_1 \rangle\rangle_1 = \langle\langle q_2 \rangle\rangle_2$,
(2) for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}$.

For transition systems with a finite number of states and a finite number of labels, checking whether a relation $\mathcal{S}$ is a simulation relation is much easier (polynomial) than checking language inclusion [CGP00].

Definition 2.3. T_2 simulates T_1 (denoted $T_1 \preceq T_2$) if there exists $\mathcal{S}$, a simulation relation of T_1 by T_2, such that for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{S}$.

Note that the relation $\preceq$ is a preorder on the set $\mathcal{T}(\Sigma, \Pi)$ of transition systems. An interesting case is when a relation is a simulation of T_1 by T_2 as well as a simulation of T_2 by T_1. Such a relation is called a bisimulation.

Definition 2.4 (Bisimulation)**.** A relation $\mathcal{B} \subseteq Q_1 \times Q_2$ is a bisimulation relation between T_1 and T_2 if for all $(q_1, q_2) \in \mathcal{B}$:

(1) $\langle\langle q_1 \rangle\rangle_1 = \langle\langle q_2 \rangle\rangle_2$,
(2) for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{B}$,
(3) for all $q_2 \xrightarrow{\sigma}_2 q_2'$, there exists $q_1 \xrightarrow{\sigma}_1 q_1'$ such that $(q_1', q_2') \in \mathcal{B}$.

If any initial state of T_1 can be related to an initial state of T_2 and conversely, then T_1 and T_2 simulate each other. We say that T_1 and T_2 are bisimilar.

Definition 2.5. T_1 and T_2 are bisimilar (denoted $T_1 \cong T_2$) if there exists $\mathcal{B}$, a bisimulation relation between T_1 and T_2 such that, for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{B}$ and conversely.

The relation $\cong$ is an equivalence relation on the set of transition systems $\mathcal{T}(\Sigma, \Pi)$. Bisimulations have been vital in collapsing infinite transition systems to bisimilar finite transition systems, especially in the context of timed and hybrid systems [AHP00]. The different relationships between transition systems are summarized in the following classical result:

Theorem 2.6 (Hierarchy of system relationships)**.** *For all T_1, $T_2 \in \mathcal{T}(\Sigma, \Pi)$,*

$$\begin{array}{ccccc} T_1 \cong T_2 & \Rightarrow & L(T_1) = L(T_2) & \Rightarrow & \mathrm{Reach}(T_1) = \mathrm{Reach}(T_2) \\ \Downarrow & & \Downarrow & & \Downarrow \\ T_1 \preceq T_2 & \Rightarrow & L(T_1) \subseteq L(T_2) & \Rightarrow & \mathrm{Reach}(T_1) \subseteq \mathrm{Reach}(T_2). \end{array}$$

Let us remark that if T_1 and T_2 are bisimilar then solving the reachability problem for T_1 is equivalent to solving the reachability problem for T_2. Even though from a verification perspective we would

like to relate the reachable sets of transition systems, complexity considerations force us to consider stronger relationships between transition systems. However, it is well known that the notions of simulation and bisimulation are different than language inclusion or language equality only for non-deterministic transition systems [Mil89]. For deterministic labeled transition systems, the notions become equivalent.

Theorem 2.7. *If T_1 and T_2 are deterministic then the following equivalences hold:*

$$\begin{array}{lcl} T_1 \cong T_2 & \Longleftrightarrow & L(T_1) = L(T_2), \\ T_1 \preceq T_2 & \Longleftrightarrow & L(T_1) \subseteq L(T_2). \end{array}$$

The fact that, in the presence of nondeterminism, simulation and bisimulation are stronger than language (or trajectory) equivalence has resulted in novel notions of exact system equivalence for nondeterministic dynamical, control, and hybrid systems [Pap03, TP04, vdS04, HTP05].

3. Metric Transition Systems

As exact relationships between transition systems do not permit any error, there are clear limitations in the amount of system compression that can be achieved. Approximate relationships which do allow for the possibility of error, will certainly allow for more dramatic system compression. Even though this has been the tradition for deterministic continuous systems [ASG00], it has been recently argued convincingly that even for more quantitative classes of finite transition systems, such as labeled Markov processes [DGJP04], probabilistic automata [vBMOW03], and quantitative transition systems [dAFS04], notions of system approximation are not only better candidates for complexity reduction but also provide more robust relationships between systems. The challenge of approximate system relationships is the quantification of the quality of the approximation.

The goal of this paper is to provide a theory of system approximation that applies to both finite (discrete) and infinite (continuous) transition systems, by providing approximate generalizations of the exact relationships of Section 2.2. By generalizing the exact notions we ensure that our framework captures the traditional exact notions for finite systems as a special case, while developing more robust notions of system approximation for infinite transition systems. To technically achieve our goal, we must equip the transition systems we consider with some topological structure that is induced by metrics on the state space and the observation space.

Definition 3.1 (Metric transition systems)**.** A transition system $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\langle . \rangle\rangle)$ is called a metric transition system if (Q, d_Q) and (Π, d_Π) are metric spaces. The set of metric transition systems associated to a set of labels Σ and a set of observations Π is denoted $\mathcal{T}_M(\Sigma, \Pi)$.

Note that, in this paper, we do not equip the set of labels Σ with any metric (equivalently we consider Σ with the trivial discrete metric). In this paper, we also need to distinguish a special class of metric transition systems that enjoy some additional regularity assumptions.

Definition 3.2 (Regular metric transition systems)**.** A metric transition system $T \in \mathcal{T}_M(\Sigma, \Pi)$ is called regular if

(1) its set of initial values Q_0 is compact,
(2) its observation map $\langle\langle . \rangle\rangle$ is continuous,
(3) its transition relation satisfies the following properties:

(a) for all $\sigma \in \Sigma$, the set valued map Post^σ is continuous[1],
(b) for all $\sigma \in \Sigma$, $\mathrm{Supp}(\mathrm{Post}^\sigma)$ is an open subset of Q,
(c) for all $\sigma \in \Sigma$, for all $q \in \mathrm{Supp}(\mathrm{Post}^\sigma)$, $\mathrm{Post}^\sigma(q)$ is a compact subset of Q,
(d) for all $\sigma \in \Sigma$, for all $q \in \mathrm{Supp}(\mathrm{Post}^\sigma)$, $\mathrm{Post}^\sigma(q)$ has a compact neighborhood.

The set of regular metric transition systems is denoted $\mathcal{T}_M^*(\Sigma, \Pi)$.

Remark 3.3. For usual metric spaces such as finite dimensional vector spaces, property (3.d) is a direct consequence of the property (3.c). However, as noted in [Wei05], it is not necessarily the case when we consider some infinite dimensional metric spaces such as the functional space L^2. Such metric spaces arise if the set of states is derived from partial differential equations.

Let us present some broad classes of regular metric transition systems that are of great interest in this paper. In particular, we are interested in finite transition systems as models of discrete systems, and infinite transition systems as models of continuous systems.

3.0.1. *Finite transition systems.* If Q is a finite set, then for any metrics defined on Q and Π, it is easy to check that the properties of Definition 3.2 hold. This example, although trivial, ensures that the framework developed in this paper will apply and capture the existing exact relationships for purely discrete systems.

3.0.2. *Continuous dynamical systems.* Let us consider the following differential inclusion

$$\begin{cases} \dot{x}(t) \in F(x(t)), & x(0) \in I,\ x(t) \in \mathbb{R}^n, \\ y(t) = g(x(t)), & y(t) \in \mathbb{R}^p \end{cases}$$

where F is a set valued map. This framework includes ordinary differential equations as well as control systems [Aub91]. Following [Pap03], we can derive a nondeterministic labeled transition system $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\langle . \rangle\rangle)$ from this differential inclusion by the following procedure:

- the set of states is $Q = \mathbb{R}^n$,
- the set of labels is $\Sigma = \mathbb{R}^+$,
- the transition relation is given by $q \xrightarrow{t} q'$ if and only if there exists a function $x(.)$ such that

$$x(0) = q,\ x(t) = q' \text{ and for almost all } s \in [0, t],\ \dot{x}(s) \in F(x(s)),$$

- the set of initial values is $Q^0 = I$,
- the set of observations is $\Pi = \mathbb{R}^p$,
- the observation map is given by $\langle\langle x \rangle\rangle = g(x)$.

Let us assume that I is compact and g is continuous. If in addition the set valued map F is continuous, has compact convex images and linear growth, that is

$$\exists c,\ \forall x \in \mathbb{R}^n,\ \forall y \in F(x),\ \|y\| \leq c(\|x\| + 1)$$

then we can show that the defined transition system satisfies the conditions of Definition 3.2.

[1]Set-valued continuity concepts are stated in Appendix.

4. Approximation Metrics for Metric Transition Systems

Metric transition systems have enough structure to develop a hierarchy of system approximation metrics, eventually resulting in an approximate version of Theorem 2.6. We begin with notions of approximate reachability and approximate language inclusion, and continue with the stronger notions of approximate simulation and bisimulation.

4.1. **Reachability and Language Metrics.** Since the set of observations is now a metric space (Π, d_Π), we can denote by $h_\Pi^{\rightarrow}$ and h_Π respectively the directed and undirected Hausdorff distances (see Appendix for a quick review) associated to the metric d_Π. The reachability metric between T_1 and T_2 is naturally defined as the Hausdorff distance between $\mathrm{Reach}(T_1)$ and $\mathrm{Reach}(T_2)$.

Definition 4.1 (Reachability metrics)**.** The directed and undirected reachability metrics are defined respectively as

$$\begin{aligned} d_{\mathcal{R}}^{\rightarrow}(T_1, T_2) &= h_\Pi^{\rightarrow}\left(\mathrm{Reach}(T_1), \mathrm{Reach}(T_2)\right), \\ d_{\mathcal{R}}(T_1, T_2) &= h_\Pi\left(\mathrm{Reach}(T_1), \mathrm{Reach}(T_2)\right). \end{aligned}$$

Since the reachability metrics are Hausdorff distances, the following result is a direct consequence of the well-known properties of Hausdorff distances.

Theorem 4.2. *The reachability metrics are pseudo-metrics on the set of metric transition systems $\mathcal{T}_M(\Sigma, \Pi)$ and*

$$\begin{aligned} d_{\mathcal{R}}^{\rightarrow}(T_1, T_2) = 0 \quad &\Longleftrightarrow \quad cl\left(\mathrm{Reach}(T_1)\right) \subseteq cl\left(\mathrm{Reach}(T_2)\right), \\ d_{\mathcal{R}}(T_1, T_2) = 0 \quad &\Longleftrightarrow \quad cl\left(\mathrm{Reach}(T_1)\right) = cl\left(\mathrm{Reach}(T_2)\right). \end{aligned}$$

For safety verification, the reachability metric is of great interest. Indeed, if we could compute $d_{\mathcal{R}}^{\rightarrow}(T_1, T_2)$ we would have that

$$\mathrm{Reach}(T_1) \subseteq N(\mathrm{cl}(\mathrm{Reach}(T_2)), d_{\mathcal{R}}^{\rightarrow}(T_1, T_2)) \tag{4.1}$$

where $N(\pi, \delta)$ denotes the δ neighborhood of $\pi \in \Pi$. Hence, if the distance separating $\mathrm{Reach}(T_2)$ and the unsafe set Π_U is strictly greater than $d_{\mathcal{R}}^{\rightarrow}(T_1, T_2)$, then the intersection of $\mathrm{Reach}(T_1)$ and Π_U is empty and therefore T_1 is safe.

Unfortunately the reachability metric is impossible to compute exactly for most infinite metric transition systems, and extremely difficult for most finite transition systems. We will therefore develop a hierarchy of *stronger* metrics, starting with two metrics that measure the distance between the languages between two systems. In order to define a distance between two languages, we first have to consider a metric in the space of external trajectories. Let s_1 and s_2 be two elements of $\mathcal{E}(\Sigma, \Pi)$:

$$s_1 = \{\pi_1^i \xrightarrow{\sigma_1^i} \pi_1^{i+1}\}_{i \in \mathbb{N}}, \; s_2 = \{\pi_2^i \xrightarrow{\sigma_2^i} \pi_2^{i+1}\}_{i \in \mathbb{N}}.$$

Since we are interested in safety verification problems, it makes sense to define the distance between s_1 and s_2 as

$$d_{\mathcal{E}}(s_1, s_2) = \begin{cases} \sup_{i \in \mathbb{N}} d_\Pi(\pi_1^i, \pi_2^i) & \text{if } \forall j \in \mathbb{N}, \; \sigma_1^j = \sigma_2^j \\ +\infty & \text{otherwise.} \end{cases}$$

Proposition 4.3. *$d_{\mathcal{E}}$ is a metric on the set of external trajectories $\mathcal{E}(\Sigma, \Pi)$.*

Proof. Let s_1, s_2, s_3 be elements of $\mathcal{E}(\Sigma,\Pi)$:

$$s_1 = \{\pi_1^i \xrightarrow{\sigma_1^i} \pi_1^{i+1}\}_{i\in\mathbb{N}},\ s_2 = \{\pi_2^i \xrightarrow{\sigma_2^i} \pi_2^{i+1}\}_{i\in\mathbb{N}},\ s_3 = \{\pi_3^i \xrightarrow{\sigma_3^i} \pi_3^{i+1}\}_{i\in\mathbb{N}}.$$

If there exists $j \in \mathbb{N}$ such that $\sigma_1^j \neq \sigma_2^j$ or $\sigma_2^j \neq \sigma_3^j$ then the triangular inequality trivially holds since the righthand side of the inequality is equal to $+\infty$. Moreover, if there exists $j \in \mathbb{N}$ such that $\sigma_1^j \neq \sigma_3^j$, then we have either $\sigma_1^j \neq \sigma_2^j$ or $\sigma_2^j \neq \sigma_3^j$. Hence, the triangular inequality holds as well. Therefore, let us assume that for all $j \in \mathbb{N}$, $\sigma_1^j = \sigma_2^j = \sigma_3^j$. Then,

$$\begin{aligned} d_{\mathcal{E}}(s_1,s_3) &= \sup_{i\in\mathbb{N}} d_\Pi(\pi_1^i,\pi_3^i) \leq \sup_{i\in\mathbb{N}}(d_\Pi(\pi_1^i,\pi_2^i) + d_\Pi(\pi_2^i,\pi_3^i)) \\ &\leq \sup_{i\in\mathbb{N}} d_\Pi(\pi_1^i,\pi_2^i) + \sup_{i\in\mathbb{N}} d_\Pi(\pi_2^i,\pi_3^i) = d_{\mathcal{E}}(s_1,s_2) + d_{\mathcal{E}}(s_2,s_3). \end{aligned}$$

The second property ($d_{\mathcal{E}}(s_1,s_2) = 0 \iff s_1 = s_2$) and the third property ($d_{\mathcal{E}}(s_1,s_2) = d_{\mathcal{E}}(s_2,s_1)$) are quite obvious. □

Let $h_{\overrightarrow{\mathcal{E}}}$ and $h_{\mathcal{E}}$ denote respectively the directed and undirected Hausdorff distance associated to the metric $d_{\mathcal{E}}$. Since $L(T_1)$ and $L(T_2)$ are subsets of $\mathcal{E}(\Sigma,\Pi)$, the language metric between T_1 and T_2 can then be defined as the Hausdorff distance between the languages $L(T_1)$ and $L(T_2)$.

Definition 4.4 (Language metrics)**.** The directed and undirected language metrics are defined respectively as

$$\begin{aligned} d_{\overrightarrow{\mathcal{L}}}(T_1,T_2) &= h_{\overrightarrow{\mathcal{E}}}\left(L(T_1),L(T_2)\right), \\ d_{\mathcal{L}}(T_1,T_2) &= h_{\mathcal{E}}\left(L(T_1),L(T_2)\right). \end{aligned}$$

The meaning of the directed language metric is the following. For any external trajectory of the system T_1, we can find an external trajectory of the system T_2, with the same sequence of labels, such that the distance between the observations of the two systems remains bounded by $d_{\overrightarrow{\mathcal{L}}}(T_1,T_2)$.

Similar to the reachability metrics, the following result follows as a consequence of the properties of Hausdorff distances.

Theorem 4.5. *The language metrics are pseudo-metrics on the set of metric labeled transition systems $\mathcal{T}_M(\Sigma,\Pi)$ and*

$$\begin{aligned} d_{\overrightarrow{\mathcal{L}}}(T_1,T_2) = 0 &\iff cl(L(T_1)) \subseteq cl(L(T_2)), \\ d_{\mathcal{L}}(T_1,T_2) = 0 &\iff cl(L(T_1)) = cl(L(T_2)). \end{aligned}$$

The following inequalities hold between the reachability and language metrics.

Theorem 4.6. *For all T_1, $T_2 \in \mathcal{T}_M(\Sigma,\Pi)$, $d_{\overrightarrow{\mathcal{R}}}(T_1,T_2) \leq d_{\overrightarrow{\mathcal{L}}}(T_1,T_2)$ and $d_{\mathcal{R}}(T_1,T_2) \leq d_{\mathcal{L}}(T_1,T_2)$.*

Proof. Let $\varepsilon > 0$. Let π_1 be an element of $\mathrm{Reach}(T_1)$. There exists an external trajectory of T_1,

$$s_1 = \{\pi_1^i \xrightarrow{\sigma_1^i} \pi_1^{i+1}\}_{i\in\mathbb{N}}$$

such that $\pi_1^j = \pi_1$ for some $j \in \mathbb{N}$. There also exists an external trajectory of T_2,

$$s_2 = \{\pi_2^i \xrightarrow{\sigma_2^i} \pi_2^{i+1}\}_{i\in\mathbb{N}}$$

such that $d_{\mathcal{E}}(s_1, s_2) < d_{\overrightarrow{\mathcal{L}}}(T_1, T_2) + \varepsilon$. Particularly, this means that $d_{\Pi}(\pi_1^j, \pi_2^j) < d_{\overrightarrow{\mathcal{L}}}(T_1, T_2) + \varepsilon$. Since π_2^j is an element of $\mathrm{Reach}(T_2)$, we have $d_{\overrightarrow{\mathcal{R}}}(T_1, T_2) < d_{\overrightarrow{\mathcal{L}}}(T_1, T_2) + \varepsilon$. This holds for all $\varepsilon > 0$, hence $d_{\overrightarrow{\mathcal{R}}}(T_1, T_2) \leq d_{\overrightarrow{\mathcal{L}}}(T_1, T_2)$. The inequality for the undirected metrics is straightforward. □

The computation of $d_{\overrightarrow{\mathcal{L}}}(T_1, T_2)$ and $d_{\mathcal{L}}(T_1, T_2)$ is also extremely difficult (but feasible in the case of quantitative, finite transition systems [dAFS04]). We will therefore consider approximate versions of the stronger notions of simulation and bisimulation.

4.2. **Approximate simulation and simulation metric.**

4.2.1. *Approximate simulation.* We introduce a notion of approximate simulation that is obtained by relaxing the *exact* observational equivalence required by exact simulation relations. Instead of requiring that the observations of two systems start and remain identical, we require that they start and remain close.

Definition 4.7 (Approximate simulation)**.** Let T_1, $T_2 \in \mathcal{T}_M(\Sigma, \Pi)$. A relation $\mathcal{S}_\delta \subseteq Q_1 \times Q_2$ is called a δ-approximate simulation relation (of T_1 by T_2) if for all $(q_1, q_2) \in \mathcal{S}_\delta$:

(1) $d_{\Pi}\left(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2\right) \leq \delta$,
(2) for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta$.

Since d_{Π} is a metric, for $\delta = 0$ we recover the established definition of exact simulation relation. Parameter δ can serve as a measure of simulation precision.

Definition 4.8. Transition system T_2 approximately simulates T_1 with precision δ (noted $T_1 \preceq_\delta T_2$), if there exists $\mathcal{S}_\delta$, a δ-approximate simulation relation of T_1 by T_2 such that for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{S}_\delta$.

The following results ensure that the set of δ-approximate simulation relations has a maximal element.

Lemma 4.9. *Let $\{\mathcal{S}_\delta^i\}_{i \in I}$ be a (possibly nondenumerable) family of δ-approximate simulation relations of T_1 by T_2. Then, $\bigcup_{i \in I} \mathcal{S}_\delta^i$ is a δ-approximate simulation relation of T_1 by T_2.*

Proof. Let $(q_1, q_2) \in \bigcup_{i \in I} \mathcal{S}_\delta^i$, there exists $i \in I$ such that $(q_1, q_2) \in \mathcal{S}_\delta^i$. Then, $d_{\Pi}\left(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2\right) \leq \delta$. Moreover, for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta^i \subseteq \bigcup_{i \in I} \mathcal{S}_\delta^i$. □

Given a precision parameter δ, Lemma 4.9 allows us to define the largest simulation relation between two systems.

Definition 4.10. Let $\{\mathcal{S}_\delta^i\}_{i \in I}$ be the set of δ-approximate simulation relations of T_1 by T_2. The maximal δ-approximate simulation relation of T_1 by T_2 is defined by

$$\mathcal{S}_\delta^{\max} = \bigcup_{i \in I} \mathcal{S}_\delta^i.$$

It is clear that T_2 approximately simulates T_1 with precision δ if and only if for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{S}_\delta^{\max}$. Approximate simulation relations define a parameterized family of relations on the set of metric transition systems $\mathcal{T}_M(\Sigma, \Pi)$. These relations satisfy the following properties:

Proposition 4.11. *Let T_1, T_2 and $T_3 \in \mathcal{T}_M(\Sigma, \Pi)$:*

(1) *For all* $\delta \geq 0$, $T_1 \preceq_\delta T_1$,
(2) *For all* $\delta \geq 0$, *if* $T_1 \preceq_\delta T_2$, *then for all* $\delta' \geq \delta$, $T_1 \preceq_{\delta'} T_2$,
(3) *For all* $\delta \geq 0$, $\delta' \geq 0$, *if* $T_1 \preceq_\delta T_2$ *and* $T_2 \preceq_{\delta'} T_3$, *then* $T_1 \preceq_{\delta+\delta'} T_3$.

Proof. The first property is obvious. Let us remark that a δ-approximate simulation relation of T_1 by T_2 is also a δ'-approximate simulation relation of T_1 by T_2 (for $\delta' \geq \delta$); the second property is straightforward. $T_1 \preceq_\delta T_2$, let $S_\delta^{\max}$ be the maximal δ-approximate simulation relation of T_1 by T_2. $T_2 \preceq_{\delta'} T_3$, let $S_{\delta'}^{\max}$ be the maximal δ'-approximate simulation relation of T_2 by T_3. Let us define the following relation $\mathcal{S}_{\delta+\delta'} \subseteq Q_1 \times Q_3$:

$$\mathcal{S}_{\delta+\delta'} = \{(q_1, q_3),\ \exists q_2 \in Q_2,\ (q_1, q_2) \in \mathcal{S}_\delta^{\max} \text{ and } (q_2, q_3) \in \mathcal{S}_{\delta'}^{\max}\}.$$

Let $(q_1, q_3) \in \mathcal{S}_{\delta+\delta'}$, let q_2 be the corresponding element of Q_2,

$$d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_3\rangle\rangle_3\right) \leq d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right) + d_\Pi\left(\langle\langle q_2\rangle\rangle_2, \langle\langle q_3\rangle\rangle_3\right) \leq \delta + \delta'.$$

For all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta^{\max}$, there also exists $q_3 \xrightarrow{\sigma}_3 q_3'$ such that $(q_2', q_3') \in \mathcal{S}_{\delta'}^{\max}$. Hence, $(q_1', q_3') \in \mathcal{S}_{\delta+\delta'}$. Therefore, $\mathcal{S}_{\delta+\delta'}$ is a $(\delta+\delta')$-approximate simulation relation of T_1 by T_3. Moreover, for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{S}_\delta^{\max}$, there also exists $q_3 \in Q_3^0$ such that $(q_2, q_3) \in \mathcal{S}_{\delta'}^{\max}$. Therefore, $T_1 \preceq_{\delta+\delta'} T_2$. □

Let us remark that contrary to the relation $\preceq$, the relation $\preceq_\delta$ (for $\delta > 0$) is not a preorder[2] on the set of metric transition systems $\mathcal{T}_M(\Sigma, \Pi)$. Indeed, the third property of Proposition 4.11 is not a transitivity property. However, it can be interpreted as a triangular inequality and therefore the precision of the approximate simulation of T_1 by T_2 appears to be a good criterion to define a distance between the two systems.

4.2.2. *Simulation metric.* The simulation metric is defined as the tightest precision δ with which T_2 approximately simulates T_1.

Definition 4.12 (Simulation metric)**.** The simulation metric is defined by

$$d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) = \inf\{\ \delta \ \mid\ T_1 \preceq_\delta T_2\}.$$

Theorem 4.13. *The simulation metric is a directed pseudo metric on the set of metric labeled transition systems* $\mathcal{T}_M(\Sigma, \Pi)$ *and*

$$T_1 \preceq T_2 \implies d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) = 0.$$

Proof. Let T_1, T_2 and T_3 be elements of $\mathcal{T}_M(\Sigma, \Pi)$. Let us remark that from Proposition 4.11, we have the following inclusion:

$$\left\{\delta + \delta' |\ T_1 \preceq_\delta T_2 \text{ and } T_2 \preceq_{\delta'} T_3\right\} \subseteq \{\delta |\ T_1 \preceq_\delta T_3\}.$$

Hence,

$$\begin{aligned} d_{\overrightarrow{\mathcal{S}}}(T_1, T_3) &= \inf\{\delta |\ T_1 \preceq_\delta T_3\} \leq \inf\left\{\delta + \delta' |\ T_1 \preceq_\delta T_2 \text{ and } T_2 \preceq_{\delta'} T_3\right\} \\ &\leq \inf\{\delta |\ T_1 \preceq_\delta T_2\} + \inf\{\delta |\ T_2 \preceq_\delta T_3\} = d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) + d_{\overrightarrow{\mathcal{S}}}(T_2, T_3). \end{aligned}$$

Therefore, the triangular inequality holds. The second part of the proposition is obvious. □

The following example shows that the converse direction of Theorem 4.13 does not hold for the general class of metric transition systems $\mathcal{T}_M(\Sigma, \Pi)$.

[2]However, the relation $T_1 \lessapprox T_2$ defined as $\exists\delta :\ T_1 \preceq_\delta T_2$ is a preorder in $\mathcal{T}_M(\Sigma, \Pi)$.

Example 4.14. Let us consider two labeled transition systems $T_1 = (Q_1, \Sigma_1, \rightarrow_1, Q_1^0, \Pi_1, \langle\langle . \rangle\rangle_1)$ and $T_2 = (Q_2, \Sigma_2, \rightarrow_2, Q_2^0, \Pi_2, \langle\langle . \rangle\rangle_2)$ where $Q_1 = Q_2 = \mathbb{R}$, $\Sigma_1 = \Sigma_2 = \{\tau\}$, $Q_1^0 = Q_2^0 = \mathbb{R}$, $\Pi_1 = \Pi_2 = \mathbb{R}$, and $\langle\langle q_1 \rangle\rangle_1 = q_1$, $\langle\langle q_2 \rangle\rangle_2 = q_2$. The transition relation of T_1 is given by $q_1 \xrightarrow{\tau}_1 q_1'$ where

$$q_1' = \begin{cases} q_1 + 1, \text{ if } q_1 < 0 \\ q_1 - 1, \text{ if } q_1 \geq 0 \end{cases}$$

The transition relation of T_2 is given by $q_2 \xrightarrow{\tau}_2 q_2'$ where

$$q_2' = \begin{cases} q_2 + 1, \text{ if } q_2 \leq 0 \\ q_2 - 1, \text{ if } q_2 > 0 \end{cases}$$

Let us remark that both successor maps Post_1^τ and Post_2^τ are discontinuous. Let $\mathcal{S}$ be an exact simulation relation of T_1 by T_2, then necessarily $\mathcal{S}$ is a subset of $\{(q_1, q_2) \in \mathbb{R}^2 |\ q_1 = q_2\}$. It is easy to check that $(0, 0)$ cannot be in $\mathcal{S}$. Therefore, T_2 does not exactly simulate T_1. Now let $\delta > 0$, let us define the following relation

$$\mathcal{S}_\delta = \left\{(q_1, q_2) \in \mathbb{R}^2 |\ |q_1 - q_2| \leq \delta \text{ and } q_1 < q_2 \leq \lfloor q_1 \rfloor + 1\right\}.$$

Let us prove that $\mathcal{S}_\delta$ is a δ-approximate simulation relation of T_1 by T_2. Let $(q_1, q_2) \in \mathcal{S}_\delta$, then $|q_1 - q_2| \leq \delta$. Let $q_1 \xrightarrow{\tau}_1 q_1'$, if $q_1 < 0$ then $q_1' = q_1 + 1$. $q_1 < 0$ implies that $q_2 \leq 0$. Thus, $q_2 \xrightarrow{\tau}_2 q_2'$ with $q_2' = q_2 + 1$. Then, $|q_1' - q_2'| = |q_1 - q_2| \leq \delta$ and $q_1' < q_2' \leq \lfloor q_1 \rfloor + 2 = \lfloor q_1 + 1 \rfloor + 1 = \lfloor q_1' \rfloor + 1$. Hence, (q_1', q_2') is in $\mathcal{S}_\delta$. Similarly, if $q_1 \geq 0$ then $q_1' = q_1 - 1$. $q_1 \geq 0$ implies that $q_2 > 0$. Then, $q_2 \xrightarrow{\tau}_2 q_2'$ with $q_2' = q_2 - 1$. Then, $|q_1' - q_2'| = |q_1 - q_2| \leq \delta$ and $q_1' < q_2' \leq \lfloor q_1 \rfloor = \lfloor q_1 - 1 \rfloor + 1 = \lfloor q_1' \rfloor + 1$. Therefore, (q_1', q_2') is in $\mathcal{S}_\delta$. We proved that for all $\delta > 0$, $\mathcal{S}_\delta$ is a δ-approximate simulation relation of T_1 by T_2. Let $q_1 \in \mathbb{R}$, let $q_2 = \min(q_1 + \delta, \lfloor q_1 \rfloor + 1)$, then $(q_1, q_2) \in \mathcal{S}_\delta$. Therefore, for all $\delta > 0$ $T_1 \preceq_\delta T_2$ and hence $d_{\mathcal{S}}^{\rightarrow}(T_1, T_2) = 0$. This is an example where a system T_1 is not exactly simulated by a system T_2 but the simulation metric between the two systems is equal to zero.

The above example illustrates that the converse direction of Theorem 4.13 will require the development of some topological results about simulation relations that will require the additional structure of regular metric transitions systems $\mathcal{T}_M^*(\Sigma, \Pi)$.

Lemma 4.15. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$, let $\mathcal{R} \subseteq Q_1 \times Q_2$ be a closed subset then*

$$\mathcal{R}' = \left\{(q_1, q_2) \in \mathcal{R} |\ \forall q_1 \xrightarrow{\sigma}_1 q_1', \exists q_2 \xrightarrow{\sigma}_2 q_2', (q_1', q_2') \in \mathcal{R}\right\}$$

is a closed subset as well.

Proof. Let $(q_1, q_2) \in \mathrm{cl}(\mathcal{R}')$, there exists a sequence $\{(q_1^i, q_2^i)\}_{i \in \mathbb{N}}$ of elements of $\mathcal{R}'$ converging to (q_1, q_2). First, let us remark that since $\mathcal{R}$ is closed, $(q_1, q_2) \in \mathcal{R}$. Let $q_1 \xrightarrow{\sigma}_1 q_1'$ (*i.e.* $q_1' \in \mathrm{Post}_1^\sigma(q_1)$), since the support of the σ-successor is open, there exists $n \in \mathbb{N}$, such that for all $i \geq n$, $q_1^i \in \mathrm{Supp}(\mathrm{Post}_1^\sigma)$. The set valued map Post_1^σ is lower semicontinuous, hence there exists a sequence $\{q_1'^i\}_{i \geq n}$ such that for all $i \geq n$, $q_1'^i \in \mathrm{Post}_1^\sigma(q_1^i)$ and which converges to q_1'. Since (q_1^i, q_2^i) is in $\mathcal{R}'$, then for all $i \geq n$, there exists $q_2'^i \in \mathrm{Post}_2^\sigma(q_2^i)$ such that $(q_1'^i, q_2'^i) \in \mathcal{R}$. By assumption, the set $\mathrm{Post}_2^\sigma(q_2)$ has a compact neighborhood V. Since Post_2^σ is upper semicontinuous and since $\{q_2^i\}_{i \in N}$ converges to q_2, there exists $m \geq n$ such that for all $i \geq m$, $q_2'^i \in \mathrm{Post}_2^\sigma(q_2^i) \subseteq V$. V is a compact, hence there exists a subsequence of the sequence $\{q_2'^i\}_{i \geq m}$ which we will also note $\{q_2'^i\}_{i \geq m}$ and which converges to a limit $q_2' \in V$. Now, for all neighborhood W of $\mathrm{Post}_2^\sigma(q_2)$ ($W \subseteq V$), there exists $p \geq m$ such that for all $i \geq p$, $q_2'^i \in \mathrm{Post}_2^\sigma(q_2^i) \subseteq W$. Hence $q_2' \in \mathrm{cl}(W)$. Since this holds for all neighborhood of $\mathrm{Post}_2^\sigma(q_2)$ we have $q_2' \in \mathrm{cl}\left(\mathrm{Post}_2^\sigma(q_2)\right) = \mathrm{Post}_2^\sigma(q_2)$ because $\mathrm{Post}_2^\sigma(q_2)$ is compact. Hence, we have

$q_2 \xrightarrow{\sigma}_2 q_2'$. (q_1', q_2') is the limit of a sequence of elements of the closed subset $\mathcal{R}$, therefore $(q_1', q_2') \in \mathcal{R}$. Hence, $(q_1, q_2) \in \mathcal{R}'$ which is consequently closed. □

A consequence of Lemma 4.15 is the following.

Proposition 4.16. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$, and let $\mathcal{S}_\delta$ be a δ-approximate simulation relation of T_1 by T_2. Then cl($\mathcal{S}_\delta$) is also a δ-approximate simulation relation of T_1 by T_2.*

Proof. It is easy to see that we have

$$\mathcal{S}_\delta \subseteq \left\{(q_1, q_2) \in \mathrm{cl}(\mathcal{S}_\delta) |\ \forall q_1 \xrightarrow{\sigma}_1 q_1', \exists q_2 \xrightarrow{\sigma}_2 q_2', (q_1', q_2') \in \mathrm{cl}(\mathcal{S}_\delta)\right\} \subseteq \mathrm{cl}(\mathcal{S}_\delta).$$

Then, from Lemma 4.15, it follows that

$$\left\{(q_1, q_2) \in \mathrm{cl}(\mathcal{S}_\delta) |\ \forall q_1 \xrightarrow{\sigma}_1 q_1', \exists q_2 \xrightarrow{\sigma}_2 q_2', (q_1', q_2') \in \mathrm{cl}(\mathcal{S}_\delta)\right\} = \mathrm{cl}(\mathcal{S}_\delta). \tag{4.2}$$

Let $(q_1, q_2) \in \mathrm{cl}(\mathcal{S}_\delta)$, there exists a sequence $\{(q_1^i, q_2^i)\}_{i\in\mathbb{N}}$ of elements of $\mathcal{S}_\delta$ converging to (q_1, q_2). Since the observation maps $\langle\langle . \rangle\rangle_1$ and $\langle\langle . \rangle\rangle_2$ are continuous,

$$d_\Pi(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) = \lim_{i\to+\infty} d_\Pi(\langle\langle q_1^i \rangle\rangle_1, \langle\langle q_2^i \rangle\rangle_2) \leq \delta.$$

Together with equation (4.2), this allows to conclude that cl($\mathcal{S}_\delta$) is also a δ-approximate simulation relation of T_1 by T_2. □

Corollary 4.17. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$, and let $S_\delta^{\max}$ be the maximal δ-approximate simulation relation of T_1 by T_2. Then $S_\delta^{\max}$ is a closed subset of $Q_1 \times Q_2$.*

Proof. $S_\delta^{\max}$ is a δ-approximate simulation relation of T_1 by T_2, so is cl($S_\delta^{\max}$). Hence, since $S_\delta^{\max}$ is the maximal δ-approximate simulation relation of T_1 by T_2, we have cl($S_\delta^{\max}$) $\subseteq S_\delta^{\max}$. □

Before we can state the main result about the simulation metric, we will require the following lemma.

Lemma 4.18. *Let $\{\mathcal{R}_\varepsilon\}_{\varepsilon>0}$ be a family of closed subsets of $Q_1 \times Q_2$ indexed over the strictly positive real numbers and such that for all $\varepsilon_1 \leq \varepsilon_2$, $\mathcal{R}_{\varepsilon_1} \subseteq \mathcal{R}_{\varepsilon_2}$. Let $q_1 \in Q_1$ and let C_2 be a compact subset of Q_2:*

$$\forall \varepsilon > 0,\ \exists q_2 \in C_2,\ \textit{such that } (q_1, q_2) \in \mathcal{R}_\varepsilon \implies \exists q_2 \in C_2,\ \textit{such that } \forall \varepsilon > 0,\ (q_1, q_2) \in \mathcal{R}_\varepsilon.$$

Proof. Let $\{\varepsilon_i\}_{i\in\mathbb{N}}$ be a decreasing sequence of reals converging to 0. Then, for all $i \in \mathbb{N}$, there exists $q_2^i \in C_2$ such that $(q_1, q_2^i) \in \mathcal{R}_{\varepsilon_i}$. Since C_2 is compact, there exists a subsequence of $\{q_2^i\}_{i\in\mathbb{N}}$ which we will also note $\{q_2^i\}_{i\in\mathbb{N}}$ and which converges to a limit $q_2 \in C_2$. Let $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that for all $i \geq n$, $\varepsilon_i \leq \varepsilon$ and hence $\mathcal{R}_{\varepsilon_i} \subseteq \mathcal{R}_\varepsilon$. Therefore, for all $i \geq n$, $(q_1, q_2^i) \in \mathcal{R}_\varepsilon$ which is closed. Hence, $(q_1, q_2) \in \mathcal{R}_\varepsilon$. □

The main result about simulation metrics states that for regular metric labeled transition systems, the zero section of the simulation metric coincides with the exact simulation relation $\preceq$ of Section 2.2.

Theorem 4.19. *For all T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$,*

$$T_1 \preceq T_2 \iff \overrightarrow{d_{\mathcal{S}}}(T_1, T_2) = 0.$$

Proof. Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$, such that $d_{\mathcal{S}}^{\rightarrow}(T_1, T_2) = 0$. This implies that for all $\delta > 0$, $T_1 \preceq_\delta T_2$. Equivalently, for all $q_1 \in Q_1^0$, for all $\delta > 0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{S}_\delta^{\max}$. From Corollary 4.17, for all $\delta > 0$, $\mathcal{S}_\delta^{\max}$ is closed. Moreover, since Q_2^0 is compact, it follows from Lemma 4.18 that for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that for all $\delta > 0$, $(q_1, q_2) \in \mathcal{S}_\delta^{\max}$. Let us define the relation $\mathcal{S} = \bigcap_{\delta > 0} \mathcal{S}_\delta^{\max}$, we have

$$\forall q_1 \in Q_1^0,\ \exists q_2 \in Q_2^0 \text{ such that } (q_1, q_2) \in \mathcal{S}. \tag{4.3}$$

Let us prove that $\mathcal{S}$ is an exact simulation relation. Let $(q_1, q_2) \in \mathcal{S}$,

$$\forall \delta > 0,\ d_\Pi(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) \leq \delta \iff d_\Pi(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) = 0 \iff \langle\langle q_1 \rangle\rangle_1 = \langle\langle q_2 \rangle\rangle_2.$$

Let $q_1 \xrightarrow{\sigma}_1 q_1'$. For all $\delta > 0$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta^{\max}$. Since $\mathrm{Post}_2^\sigma(q_2)$ is compact, it follows from Lemma 4.18 that there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that for all $\delta > 0$, $(q_1', q_2') \in \mathcal{S}_\delta^{\max}$. Equivalently,

$$\forall q_1 \xrightarrow{\sigma}_1 q_1',\ \exists q_2 \xrightarrow{\sigma}_2 q_2' \text{ such that } (q_1', q_2') \in \mathcal{S}.$$

Hence $\mathcal{S}$ is an exact simulation relation. Equation (4.3) allows to conclude that $T_1 \preceq T_2$. □

The relationship between the simulation metric and the language metric is captured by the following result which holds for all metric transition systems, not necessarily regular.

Theorem 4.20. *For all T_1, $T_2 \in \mathcal{T}_M(\Sigma, \Pi)$, $d_{\mathcal{L}}^{\rightarrow}(T_1, T_2) \leq d_{\mathcal{S}}^{\rightarrow}(T_1, T_2)$.*

Proof. Let $\delta > d_{\mathcal{S}}^{\rightarrow}(T_1, T_2)$, then $T_1 \preceq_\delta T_2$. Let $s_1 = \{\pi_1^i \xrightarrow{\sigma_1^i} \pi_1^{i+1}\}_{i \in \mathbb{N}} \in L(T_1)$, there exists a state trajectory of T_1:

$$\{q_1^i \xrightarrow{\sigma_1^i}_1 q_1^{i+1}\}_{i \in \mathbb{N}} \text{ such that } \forall i \in \mathbb{N},\ \langle\langle q_1^i \rangle\rangle_1 = \pi_1^i.$$

$q_1^0 \in Q_1^0$ then there exists $q_2^0 \in Q_2^0$ such that (q_1^0, q_2^0) is in $\mathcal{S}_\delta^{\max}$, the maximal δ-approximate simulation relation of T_1 by T_2. Using the second property of Definition 4.7 it can be shown by induction that there exists a state trajectory of T_2,

$$\{q_2^i \xrightarrow{\sigma_2^i}_2 q_2^{i+1}\}_{i \in \mathbb{N}} \text{ such that } \forall i \in \mathbb{N},\ \sigma_1^i = \sigma_2^i \text{ and } (q_1^i, q_2^i) \in \mathcal{S}_\delta^{\max}.$$

Let $s_2 = \{\pi_2^i \xrightarrow{\sigma_2^i} \pi_2^{i+1}\}_{i \in \mathbb{N}}$ be the associated external trajectory accepted by T_2 (for all $i \in \mathbb{N}$, $\langle\langle q_2^i \rangle\rangle_2 = \pi_2^i$). Then, we have for all $i \in \mathbb{N}$, $d_\Pi(\pi_1^i, \pi_2^i) = d_\Pi(\langle\langle q_1^i \rangle\rangle_1, \langle\langle q_2^i \rangle\rangle_2) \leq \delta$. Therefore, since the external trajectories s_1 and s_2 share the same sequence of labels, $d_{\mathcal{E}}(s_1, s_2) \leq \delta$. Hence, $d_{\mathcal{L}}^{\rightarrow}(T_1, T_2) \leq \delta$. This holds for all $\delta > d_{\mathcal{S}}^{\rightarrow}(T_1, T_2)$, therefore $d_{\mathcal{L}}^{\rightarrow}(T_1, T_2) \leq d_{\mathcal{S}}^{\rightarrow}(T_1, T_2)$. □

For deterministic transition systems, the equivalence between exact language inclusion and exact simulation has an approximate analogue, as the following result shows.

Lemma 4.21. *If T_2 is deterministic then $d_{\mathcal{L}}^{\rightarrow}(T_1, T_2) = d_{\mathcal{S}}^{\rightarrow}(T_1, T_2)$.*

Proof. Let $\mathcal{L}_\delta$ be the subset of $Q_1 \times Q_2$ defined by the following: $(q_1^0, q_2^0) \in \mathcal{L}_\delta$ if for all sequence of transitions of T_1 starting in q_1^0, $q_1^0 \xrightarrow{\sigma^0}_1 q_1^1 \xrightarrow{\sigma^1}_1 q_1^2 \xrightarrow{\sigma^2}_1 \ldots$, there exists a sequence of transitions of T_2 with the same sequence of labels and starting in q_2^0, $q_2^0 \xrightarrow{\sigma^0}_2 q_2^1 \xrightarrow{\sigma^1}_2 q_2^2 \xrightarrow{\sigma^2}_2 \ldots$, such that for all $i \in \mathbb{N}$, $d_\Pi(\langle\langle q_1^i \rangle\rangle_1, \langle\langle q_2^i \rangle\rangle_2) \leq \delta$. Let us prove that $\mathcal{L}_\delta$ is a δ-approximate simulation relation of T_1 by T_2. Let $(q_1^0, q_2^0) \in \mathcal{L}_\delta$, first it is clear that we have $d_\Pi(\langle\langle q_1^0 \rangle\rangle_1, \langle\langle q_2^0 \rangle\rangle_2) \leq \delta$. Let $q_1^0 \xrightarrow{\sigma^0}_1 q_1^1$, since $(q_1^0, q_2^0) \in \mathcal{L}_\delta$ then there exists a transition $q_2^0 \xrightarrow{\sigma^0}_2 q_2^1$. Note that since T_2 is deterministic, any sequence of transitions

of T_2 starting in q_2^0 with the label σ^0 begins with the transition $q_2^0 \xrightarrow{\sigma^0}_2 q_2^1$. Let us consider a sequence of transitions of T_1 starting in q_1^1, $q_1^1 \xrightarrow{\sigma^1}_1 q_1^2 \xrightarrow{\sigma^2}_1 q_1^3 \xrightarrow{\sigma^3}_1 \ldots$, then $q_1^0 \xrightarrow{\sigma^0}_1 q_1^1 \xrightarrow{\sigma^1}_1 q_1^2 \xrightarrow{\sigma^2}_1 \ldots$ is a sequence of transitions of T_1 as well. Since $(q_1^0, q_2^0) \in \mathcal{L}_\delta$, there exists a sequence of transitions of T_2 with the same sequence of labels and starting in q_2^0 and therefore beginning by the transition $q_2^0 \xrightarrow{\sigma^0}_2 q_2^1$: $q_2^0 \xrightarrow{\sigma^0}_2 q_2^1 \xrightarrow{\sigma^1}_2 q_2^2 \xrightarrow{\sigma^2}_2 \ldots$, such that for all $i \in \mathbb{N}$, $d_\Pi(\langle\langle q_1^i \rangle\rangle_1, \langle\langle q_2^i \rangle\rangle_2) \leq \delta$. Thus, $(q_1^1, q_2^1) \in \mathcal{L}_\delta$ and therefore $\mathcal{L}_\delta$ is a δ-approximate simulation relation of T_1 by T_2. Let $\delta > d_{\overrightarrow{\mathcal{L}}}(T_1, T_2)$, let $q_0^1 \in Q_1^0$. Since T_2 is deterministic then, there exist a unique initial state $q_2^0 \in Q_2^0$. Moreover, since $\delta > d_{\overrightarrow{\mathcal{L}}}(T_1, T_2)$, it is clear that $(q_1^0, q_2^0) \in \mathcal{L}_\delta$. Hence, $T_1 \preceq_\delta T_2$. Since this holds for all $\delta > d_{\overrightarrow{\mathcal{L}}}(T_1, T_2)$, $d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) \leq d_{\overrightarrow{\mathcal{L}}}(T_1, T_2)$. Lemma 4.20 allows to conclude. □

The fact that the simulation metric is stronger (for nondeterministic systems) than the language inclusion metric will result in algorithms for its computation, which are advantageous especially in the context of infinite metric transition systems. Before we discuss their computation in Sections 6 and 7, we present similar results for approximate bisimulations.

4.3. **Approximate bisimulations and bisimulation metric.** The development of approximate bisimulation is similar to the development of approximate simulation. We therefore state all results without their conceptually and technically similar proofs.

4.3.1. *Approximate bisimulation.* If a relation is a δ-approximate simulation relation of T_1 by T_2 as well as a δ-approximate simulation relation of T_2 by T_1, then it is called a δ-approximate bisimulation relation.

Definition 4.22 (Approximate bisimulation)**.** Let T_1, $T_2 \in \mathcal{T}_M(\Sigma, \Pi)$. A relation $\mathcal{B}_\delta \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$ is a δ-approximate bisimulation relation between T_1 and T_2 if for all $(q_1, q_2) \in \mathcal{B}_\delta$:

(1) $d_\Pi(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) \leq \delta$,
(2) for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{B}_\delta$,
(3) for all $q_2 \xrightarrow{\sigma}_2 q_2'$, there exists $q_1 \xrightarrow{\sigma}_1 q_1'$ such that $(q_1', q_2') \in \mathcal{B}_\delta$.

Definition 4.23. T_1 and T_2 are said to be approximately bisimilar with the precision δ (denoted $T_1 \cong_\delta T_2$), if there exists $\mathcal{B}_\delta$, a δ-approximate bisimulation relation between T_1 and T_2 such that for all $q_1 \in \mathcal{Q}_1^0$, there exists $q_2 \in \mathcal{Q}_2^0$ such that $(q_1, q_2) \in \mathcal{B}_\delta$, and conversely.

Similar to approximate simulation relations, we can show that the union of a (possibly nondenumerable) family of δ-approximate bisimulation relations between T_1 and T_2 is a δ-approximate bisimulation relation between T_1 and T_2. It follows that there exists a maximal δ-approximate bisimulation relation between T_1 and T_2.

Definition 4.24. Let $\{\mathcal{B}_\delta^i\}_{i \in I}$ be the set of δ-approximate bisimulation relations between T_1 and T_2. The maximal δ-approximate bisimulation relation between T_1 and T_2 is defined by

$$\mathcal{B}_\delta^{\max} = \bigcup_{i \in I} \mathcal{B}_\delta^i.$$

Clearly, T_1 and T_2 are approximately bisimilar with precision δ if and only if for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{B}_\delta^{\max}$, and conversely. Approximate bisimulation relations for metric transition systems satisfy the following properties.

Proposition 4.25. *Let T_1, T_2 and $T_3 \in \mathcal{T}_M(\Sigma, \Pi)$:*

(1) *For all $\delta \geq 0$, $T_1 \cong_\delta T_1$,*
(2) *For all $\delta \geq 0$, if $T_1 \cong_\delta T_2$, then for all $\delta' \geq \delta$, $T_1 \cong'_\delta T_2$,*
(3) *For all $\delta \geq 0$, $\delta' \geq 0$, if $T_1 \cong_\delta T_2$ and $T_2 \cong_{\delta'} T_3$, then $T_1 \cong_{\delta+\delta'} T_3$.*

Contrarily to $\cong$, the relation $\cong_\delta$ (for $\delta > 0$) is not an equivalence relation[3] on the set of metric labeled transition systems $\mathcal{T}_M(\Sigma, \Pi)$. But the above properties enable us to define a bisimulation metric in $\mathcal{T}_M(\Sigma, \Pi)$.

4.3.2. *Bisimulation metric.*

Definition 4.26 (Bisimulation metric)**.** The bisimulation metric is the function defined by

$$d_{\mathcal{B}}(T_1, T_2) = \inf \{\delta \mid T_1 \cong_\delta T_2\}.$$

Theorem 4.27. *The bisimulation metric is a pseudo metric on the set of metric transition systems $\mathcal{T}_M(\Sigma, \Pi)$ and*

$$T_1 \cong T_2 \implies d_{\mathcal{B}}(T_1, T_2) = 0.$$

Theorem 4.28. *For all T_1, $T_2 \in \mathcal{T}_M(\Sigma, \Pi)$, $d_{\mathcal{L}}(T_1, T_2) \leq d_{\mathcal{B}}(T_1, T_2)$ and $d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) \leq d_{\mathcal{B}}(T_1, T_2)$.*

Proof. The proof of the first inequality is similar to the proof of Lemma 4.20. However, let us remark that a δ-approximate bisimulation relation is also a δ-approximate simulation relation. Hence, $T_1 \cong_\delta T_2$ implies that $T_1 \preceq_\delta T_2$ and therefore $d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) \leq d_{\mathcal{B}}(T_1, T_2)$. □

If we assume that the metric transition systems we consider are also regular, then, similar to the simulation metric, we obtain that the zero section of the bisimulation metric coincides with the exact equivalence relation $\cong$ from Section 2.2.

Theorem 4.29. *For all T_1, $T_2 \in \mathcal{T}^*_M(\Sigma, \Pi)$,*

$$T_1 \cong T_2 \iff d_{\overrightarrow{\mathcal{B}}}(T_1, T_2) = 0.$$

For deterministic systems, the notions of language equivalence and exact bisimulation holds also between the approximate versions of these notions. It implies that for deterministic systems the language and the bisimulation metrics are equal.

Theorem 4.30. *If T_1 and T_2 are deterministic then $d_{\mathcal{L}}(T_1, T_2) = d_{\mathcal{B}}(T_1, T_2)$.*

4.4. **Hierarchy of system approximations.** The results of Theorem 4.6, 4.20 and 4.28 can be summarized in the following theorem which is the analog of Theorem 2.6 for our approximation metrics.

Theorem 4.31 (Hierarchy of system approximations)**.** *For all metric transition system T_1, $T_2 \in \mathcal{T}_M(\Sigma, \Pi)$, the following relationships hold (where $\to$ stands for $\geq$)*

$$\begin{array}{ccccc} d_{\mathcal{B}}(T_1, T_2) & \to & d_{\mathcal{L}}(T_1, T_2) & \to & d_{\mathcal{R}}(T_1, T_2) \\ \downarrow & & \downarrow & & \downarrow \\ d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) & \to & d_{\overrightarrow{\mathcal{L}}}(T_1, T_2) & \to & d_{\overrightarrow{\mathcal{R}}}(T_1, T_2) \end{array}$$

[3]However, the relation $T_1 \approx T_2$ defined as $\exists \delta : T_1 \cong_\delta T_2$ is an equivalence relation in $\mathcal{T}_M(\Sigma, \Pi)$.

All the metrics defined in this section provide an over-approximation of the directed reachability metric which is useful for reducing the complexity of the safety verification problem (see equation (4.1)). Let us remark that for regular metric labeled transition systems, a slightly weaker version of Theorem 2.6 is obtained by considering the zero sections of the different metrics:

$$\begin{array}{ccccc} T_1 \cong T_2 & \Rightarrow & \mathrm{cl}(L(T_1)) = \mathrm{cl}(L(T_2)) & \Rightarrow & \mathrm{cl}(\mathrm{Reach}(T_1)) = \mathrm{cl}(\mathrm{Reach}(T_2)) \\ \Downarrow & & \Downarrow & & \Downarrow \\ T_1 \preceq T_2 & \Rightarrow & \mathrm{cl}(L(T_1)) \subseteq \mathrm{cl}(L(T_2)) & \Rightarrow & \mathrm{cl}(\mathrm{Reach}(T_1)) \subseteq \mathrm{cl}(\mathrm{Reach}(T_2)). \end{array}$$

For deterministic labeled transition systems, according to Lemmas 4.21 and 4.30, some of the approximation metrics are equal. The following theorem summarizes these results:

Theorem 4.32. *If T_1 and T_2 are deterministic then the following equalities hold:*

$$\begin{array}{rcl} d_{\mathcal{B}}(T_1, T_2) & = & d_{\mathcal{L}}(T_1, T_2), \\ d_{\mathcal{S}}^{\rightarrow}(T_1, T_2) & = & d_{\mathcal{L}}^{\rightarrow}(T_1, T_2). \end{array}$$

5. Compositional Approximations

One of the most powerful features of simulation and bisimulation is that they allow compositional reasoning. In fact, simulation and bisimulation have their origins in concurrency theory [Mil89], before impacting formal verification [CGP00]. In this section, we show that the approximate metrics we developed in the previous section are also compositional, in an approximate sense.

We illustrate the compositionality of our metrics for synchronous composition. The composition of two metric transition systems $T_1 = (Q_1, \Sigma_1, \rightarrow_1, Q_1^0, \Pi_1, \langle\langle . \rangle\rangle_1)$ and $T_2 = (Q_2, \Sigma_2, \rightarrow_2, Q_2^0, \Pi_2, \langle\langle . \rangle\rangle_2)$ is denoted $T_1 || T_2$ and is defined by $T_1 || T_2 = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\langle . \rangle\rangle)$ where:

- the set of states $Q = Q_1 \times Q_2$,
- the set of labels $\Sigma = \Sigma_1 \cap \Sigma_2$,
- the transition relation is given by
$$(q_1, q_2) \xrightarrow{\sigma} (q_1', q_2') \iff q_1 \xrightarrow{\sigma}_1 q_1' \text{ and } q_2 \xrightarrow{\sigma}_2 q_2',$$
- the set of initial states $Q^0 = Q_1^0 \times Q_2^0$,
- the set of observations $\Pi = \Pi_1 \times \Pi_2$,
- the observation map is given by $\langle\langle (q_1, q_2) \rangle\rangle = (\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2)$.

Therefore the systems synchronize on common events[4], and we assume that the composition is non-blocking. Since (Π_1, d_{Π_1}) and (Π_2, d_{Π_2}) are metric spaces, we consider the metric space (Π, d_Π) where the metric d_Π is defined by

$$d_\Pi\left((\pi_1, \pi_2), (\pi_1', \pi_2')\right) = d_{\Pi_1}\left(\pi_1, \pi_1'\right) + d_{\Pi_2}\left(\pi_2, \pi_2'\right).$$

If $U_1 = (P_1, \Sigma_1, \rightarrow_1, P_1^0, \Pi_1, \langle\langle . \rangle\rangle_1)$ is an approximation of T_1, and $U_2 = (P_2, \Sigma_2, \rightarrow_2, P_2^0, \Pi_2, \langle\langle . \rangle\rangle_2)$ is an approximation of T_2, we show that $U_1 || U_2$ is an approximation of $T_1 || T_2$, from the perspective of our language metrics.

Theorem 5.1. *For all T_1, $U_1 \in \mathcal{T}_M(\Sigma_1, \Pi_1)$, T_2, $U_2 \in \mathcal{T}_M(\Sigma_2, \Pi_2)$,*

$$\begin{array}{rcl} d_{\mathcal{L}}^{\rightarrow}(T_1 || T_2, U_1 || U_2) & \leq & d_{\mathcal{L}}^{\rightarrow}(T_1, U_1) + d_{\mathcal{L}}^{\rightarrow}(T_2, U_2), \\ d_{\mathcal{L}}(T_1 || T_2, U_1 || U_2) & \leq & d_{\mathcal{L}}(T_1, U_1) + d_{\mathcal{L}}(T_2, U_2). \end{array}$$

[4]More general composition operators can and will be considered in future work.

Proof. Let s be an element of $L(T_1||T_2)$, $s = (\pi_1^0, \pi_2^0) \xrightarrow{\sigma^0} (\pi_1^1, \pi_2^1) \xrightarrow{\sigma^1} (\pi_1^2, \pi_2^2) \xrightarrow{\sigma^2} \dots$. It is clear from the definition of the composition that $s_1 = \pi_1^0 \xrightarrow{\sigma^0}_1 \pi_1^1 \xrightarrow{\sigma^1}_1 \pi_1^2 \xrightarrow{\sigma^2} \dots$ is an element of $L(T_1)$ and that $s_2 = \pi_2^0 \xrightarrow{\sigma^0}_2 \pi_2^1 \xrightarrow{\sigma^1}_1 \pi_2^2 \xrightarrow{\sigma^2} \dots$ is an element of $L(T_2)$. Let $\delta_1 > d_{\mathcal{L}}^{\rightarrow}(T_1, U_1)$, $\delta_2 > d_{\mathcal{L}}^{\rightarrow}(T_2, U_2)$, then there exists an element of $L(U_1)$ with the same sequence of labels than s_1, $r_1 = \rho_1^0 \xrightarrow{\sigma^0}_1 \rho_1^1 \xrightarrow{\sigma^1}_1 \rho_1^2 \xrightarrow{\sigma^2} \dots$ such that for all $i \in \mathbb{N}$, $d_{\Pi_1}(\pi_1^i, \rho_1^i) \leq \delta_1$. Similarly, there exists an element of $L(U_2)$ with the same sequence of labels than s_2, $r_2 = \rho_2^0 \xrightarrow{\sigma^0}_2 \rho_2^1 \xrightarrow{\sigma^1}_2 \rho_2^2 \xrightarrow{\sigma^2} \dots$ such that for all $i \in \mathbb{N}$, $d_{\Pi_2}(\pi_2^i, \rho_2^i) \leq \delta_2$. Note that r_1 and r_2 share the same sequence of labels, therefore $r = (\rho_1^0, \rho_2^0) \xrightarrow{\sigma^0} (\rho_1^1, \rho_2^1) \xrightarrow{\sigma^1} (\rho_1^2, \rho_2^2) \xrightarrow{\sigma^2} \dots$ is an element of $L(U_1||U_2)$. Moreover, for all $i \in \mathbb{N}$,

$$d_{\Pi}\left((\pi_1^i, \pi_2^i), (\rho_1^i, \rho_2^i)\right) = d_{\Pi_1}(\pi_1^i, \rho_1^i) + d_{\Pi_2}(\pi_2^i, \rho_2^i) \leq \delta_1 + \delta_2.$$

Hence, since s and r share the same sequence of labels, $d_{\mathcal{E}}(s, r) \leq \delta_1 + \delta_2$. Therefore, for all $\delta_1 > d_{\mathcal{L}}^{\rightarrow}(T_1, U_1)$ and $\delta_2 > d_{\mathcal{L}}^{\rightarrow}(T_2, U_2)$, $d_{\mathcal{L}}^{\rightarrow}(T_1||T_2, U_1||U_2) \leq \delta_1 + \delta_2$ which leads to the first inequality. The second inequality is obtained by symmetry. □

Therefore approximate language inclusion is compositional. The following results show that it is also the case for approximate simulation and approximate bisimulation.

Proposition 5.2. *Let T_1, $U_1 \in \mathcal{T}_M(\Sigma_1, \Pi_1)$, T_2, $U_2 \in \mathcal{T}_M(\Sigma_2, \Pi_2)$, then*

$$\begin{aligned} T_1 \preceq_{\delta_1} U_1 \text{ and } T_2 \preceq_{\delta_2} U_2 &\implies T_1||T_2 \preceq_{\delta_1+\delta_2} U_1||U_2, \\ T_1 \cong_{\delta_1} U_1 \text{ and } T_2 \cong_{\delta_2} U_2 &\implies T_1||T_2 \cong_{\delta_1+\delta_2} U_1||U_2, \end{aligned}$$

Proof. $T_1 \preceq_{\delta_1} U_1$, let $\mathcal{S}_1$ be the corresponding δ_1-approximate simulation relation of T_1 by U_1. Similarly, $T_2 \preceq_{\delta_2} U_2$, let $\mathcal{S}_2$ be the corresponding δ_2-approximate simulation relation of T_2 by U_2. Let $\mathcal{S}$ be the subset of $Q_1 \times Q_2 \times P_1 \times P_2$ defined by

$$\mathcal{S} = \{(q_1, q_2, p_1, p_2) \in Q_1 \times Q_2 \times P_1 \times P_2 |\ (q_1, p_1) \in \mathcal{S}_1 \text{ and } (q_2, p_2) \in \mathcal{S}_2\}.$$

Let $(q_1, q_2, p_1, p_2) \in \mathcal{S}$, then since $(q_1, p_1) \in \mathcal{S}_1$ and $(q_2, p_2) \in \mathcal{S}_2$:

$$d_{\Pi}\left(\langle\langle(q_1, q_2)\rangle\rangle, \langle\langle(p_1, p_2)\rangle\rangle\right) = d_{\Pi_1}\left(\langle\langle q_1\rangle\rangle_1, \langle\langle p_1\rangle\rangle_1\right) + d_{\Pi_2}\left(\langle\langle q_2\rangle\rangle_2, \langle\langle p_2\rangle\rangle_2\right) \leq \delta_1 + \delta_2.$$

Let $(q_1, q_2) \xrightarrow{\sigma} (q_1', q_2')$, then $q_1 \xrightarrow{\sigma}_1 q_1'$ and $q_2 \xrightarrow{\sigma}_2 q_2'$. Since $(q_1, p_1) \in \mathcal{S}_1$ and $(q_2, p_2) \in \mathcal{S}_2$, there exist $p_1 \xrightarrow{\sigma}_1 p_1'$ and $p_2 \xrightarrow{\sigma}_2 p_2'$ such that $(q_1', p_1') \in \mathcal{S}_1$ and $(q_2', p_2') \in \mathcal{S}_2$. Hence, $(p_1, p_2) \xrightarrow{\sigma} (p_1', p_2')$ and $(q_1', q_2', p_1', p_2') \in \mathcal{S}$. Therefore, $\mathcal{S}$ is a $(\delta_1 + \delta_2)$-approximate simulation relation of $T_1||T_2$ by $U_1||U_2$. Let $(q_1, q_2) \in Q_1^0 \times Q_2^0$, there exists $p_1 \in P_1^0$ such that $(q_1, p_1) \in \mathcal{S}_1$. There also exists $p_2 \in P_2^0$ such that $(q_2, p_2) \in \mathcal{S}_2$. Hence, $(q_1, q_2, p_1, p_2) \in \mathcal{S}$. Therefore, $T_1||T_2 \preceq_{\delta_1+\delta_2} U_1||U_2$. The second part of the proposition is proved using a symmetrical reasoning. □

Theorem 5.3. *For all T_1, $U_1 \in \mathcal{T}_M(\Sigma_1, \Pi_1)$, T_2, $U_2 \in \mathcal{T}_M(\Sigma_2, \Pi_2)$,*

$$\begin{aligned} d_{\mathcal{S}}^{\rightarrow}(T_1||T_2, U_1||U_2) &\leq d_{\mathcal{S}}^{\rightarrow}(T_1, U_1) + d_{\mathcal{S}}^{\rightarrow}(T_2, U_2), \\ d_{\mathcal{B}}(T_1||T_2, U_1||U_2) &\leq d_{\mathcal{B}}(T_1, U_1) + d_{\mathcal{B}}(T_2, U_2). \end{aligned}$$

Proof. Let $\delta_1 > d_{\mathcal{S}}^{\rightarrow}(T_1, U_1)$, $\delta_2 > d_{\mathcal{S}}^{\rightarrow}(T_2, U_2)$, then $T_1 \preceq_{\delta_1} U_1$ and $T_2 \preceq_{\delta_2} U_2$. Therefore, from Proposition 5.2, $T_1||T_2 \preceq_{\delta_1+\delta_2} U_1||U_2$ and $d_{\mathcal{S}}^{\rightarrow}(T_1||T_2, U_1||U_2) \leq \delta_1 + \delta_2$. Since this holds for all $\delta_1 > d_{\mathcal{S}}^{\rightarrow}(T_1, U_1)$, $\delta_2 > d_{\mathcal{S}}^{\rightarrow}(T_2, U_2)$, then $d_{\mathcal{S}}^{\rightarrow}(T_1||T_2, U_1||U_2) \leq d_{\mathcal{S}}^{\rightarrow}(T_1, U_1) + d_{\mathcal{S}}^{\rightarrow}(T_2, U_2)$. The proof of the second inequality is similar. □

In this part, we showed that our approximation framework allows compositional reasoning. Indeed, the composition of approximations is an approximation of the composition. Note that even though our compositionality results hold for the language, simulation, and bisimulation metric, they do not hold for the reachability metric. This is further evidence that for safety verification, overapproximating the reachability metric with the language, simulation, or bisimulation metric, can further decompose safety analysis by exploiting the above compositionality results.

6. Exact Metric Computation

In the previous sections, we presented a compositional theory of system approximation for metric transition systems. In this section, we focus on the computation of the simulation and bisimulation metrics since the language (and hence reachability) metrics are either impossible to compute for infinite transition systems, or computationally demanding for finite quantitative transition systems [dAFS04].

We propose two approaches for computing the simulation and bisimulation metric. The first approach, described in this Section, focuses on computing *exactly* the metrics using a natural generalization of the fixed-point (or game-theoretic) interpretations of simulation and bisimulation. The second approach, described in Section 7, is a relaxation of the first approach, offering *approximate* upper bounds for the metrics at a reduced computational cost.

6.1. **Maximal approximate simulations.** For the established exact simulations of Section 2.2, a computable characterization of the maximal exact simulation relation is often given in terms of the fixed point of a decreasing sequence of subsets of $\mathcal{Q}_1 \times \mathcal{Q}_2$. A similar approach can be used for the maximal δ-approximate simulation relation. We assume that the metric transition systems we consider are regular. Let us consider the following algorithm whose goal is to search for such relations.

Algorithm 6.1. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$. For a given $\delta \geq 0$, define the following sequence $\{\mathcal{S}_\delta^i\}_{i\in\mathbb{N}}$ of subsets of $\mathcal{Q}_1 \times \mathcal{Q}_2$:*

$$\begin{array}{rcl} \mathcal{S}_\delta^0 & = & \{(q_1, q_2) \in \mathcal{Q}_1 \times \mathcal{Q}_2 |\ d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right) \leq \delta\} \\ \mathcal{S}_\delta^{i+1} & = & \{(q_1, q_2) \in \mathcal{S}_\delta^i |\ \forall q_1 \xrightarrow{\sigma}_1 q_1', \exists q_2 \xrightarrow{\sigma}_2 q_2', (q_1', q_2') \in \mathcal{S}_\delta^i\},\ i \in \mathbb{N}. \end{array}$$

Lemma 6.2. *For all $\delta \geq 0$, for all $i \in \mathbb{N}$, the subset $\mathcal{S}_\delta^i$ is closed.*

Proof. Since the observation maps $\langle\langle . \rangle\rangle_1$ and $\langle\langle . \rangle\rangle_2$ are continuous, it is clear that the subset $\mathcal{S}_\delta^0$ is closed. Assuming that the subset $\mathcal{S}_\delta^i$ is closed for some $i \in \mathbb{N}$, then, according to Lemma 4.15, $\mathcal{S}_\delta^{i+1}$ is closed as well. □

For metric transition systems with a finite number of states, it is clear that Algorithm 6.1 reaches a fixed point in a finite number of steps. For infinite transition systems, Algorithm 6.1 may not reach a fixed point in a finite number steps. However, the sequence $\{\mathcal{S}_\delta^i\}_{i\in\mathbb{N}}$ does approach a fixed point as i goes to $+\infty$. This fixed point is the maximal δ-approximate simulation relation of T_1 by T_2.

Theorem 6.3. *Let $\{\mathcal{S}_\delta^i\}_{i\in\mathbb{N}}$ be the decreasing sequence of sets defined by Algorithm 6.1 and $\mathcal{S}_\delta^{\max}$ be the maximal δ-approximate simulation relation of T_1 by T_2. Then, the following properties hold:*

$$\forall i \in \mathbb{N}, \mathcal{S}_\delta^{\max} \subseteq \mathcal{S}_\delta^i,$$
$$\bigcap_{i=0}^{i=+\infty} \mathcal{S}_\delta^i = \mathcal{S}_\delta^{\max}.$$

Proof. It is clear that $\mathcal{S}_\delta^{\max} \subseteq \mathcal{S}_\delta^0$. Hence, let us assume that $\mathcal{S}_\delta^{\max} \subseteq \mathcal{S}_\delta^i$, for some $i \in \mathbb{N}$. Let $(q_1, q_2) \in \mathcal{S}_\delta^{\max} \subseteq \mathcal{S}_\delta^i$, for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta^{\max} \subseteq \mathcal{S}_\delta^i$. Hence, $(q_1, q_2) \in \mathcal{S}_\delta^{i+1}$. By induction, the first part of the theorem is proved. Now, let us show that $\bigcap_{i=0}^{i=+\infty} \mathcal{S}_\delta^i$ is a δ-approximate simulation relation of T_1 by T_2. Let $(q_1, q_2) \in \bigcap_{i=0}^{i=+\infty} \mathcal{S}_\delta^i$, then particularly $(q_1, q_2) \in \mathcal{S}_\delta^0$. Hence, $d_\Pi(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2) \leq \delta$. Let $q_1 \xrightarrow{\sigma}_1 q_1'$, from the construction of the sequence $\{\mathcal{S}_\delta^i\}_{i\in\mathbb{N}}$, for all $i \in \mathbb{N}$, there exists $q_2'^i \in \mathrm{Post}_2^\sigma(q_2)$ such that $(q_1', q_2'^i) \in \mathcal{S}_\delta^i$. Since $\mathrm{Post}_2^\sigma(q_2)$ is compact, there exists $\{q_2'^{i_k}\}_{k\in\mathbb{N}}$ a subsequence of $\{q_2'^i\}_{i\in\mathbb{N}}$ converging to an element q_2' in $\mathrm{Post}_2^\sigma(q_2)$. Let $i \in N$, there exists $n \in \mathbb{N}$ such that for all $k \geq n$, $i_k \geq i$ and hence $\mathcal{S}_\delta^{i_k} \subseteq \mathcal{S}_\delta^i$ because the sequence $\{\mathcal{S}_\delta^i\}_{i\in\mathbb{N}}$ is decreasing. Thus, for all $k \geq n$, $(q_1', q_2'^{i_k})$ is an element of $\mathcal{S}_\delta^i$ which is closed. Hence, (q_1', q_2') is in $\mathcal{S}_\delta^i$ for all $i \in \mathbb{N}$. It follows that $\bigcap_{i=0}^{i=+\infty} \mathcal{S}_\delta^i$ is a δ-approximate simulation of T_1 by T_2. From the first part of the theorem, it is clear that $\mathcal{S}_\delta^{\max} \subseteq \bigcap_{i=0}^{i=+\infty} \mathcal{S}_\delta^i$ which allows to conclude. □

6.2. **Directed branching distance.** A dual approach to Algorithm 6.1 consists in characterizing the maximal approximate simulation relations of T_1 by T_2 as the level sets of a function. Let us consider the following algorithm.

Algorithm 6.4. *Let $T1$, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$. Define the following sequence $\{f_\mathcal{S}^i\}_{i\in\mathbb{N}}$ of functions from $\mathcal{Q}_1 \times \mathcal{Q}_2$ to $\mathbb{R}^+ \cup \{+\infty\}$:*

$$\begin{aligned} f_\mathcal{S}^0(q_1, q_2) &= d_\Pi(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2) \\ f_\mathcal{S}^{i+1}(q_1, q_2) &= \max\left(d_\Pi(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_\mathcal{S}^i(q_1', q_2') \right), \ i \in \mathbb{N}. \end{aligned}$$

For transition systems with a finite number of states, it is shown in [dAFS04], that Algorithm 6.4 reaches a fixed point in a finite (polynomial) number of steps. In the more general case of metric transition systems, the following lemma shows that the sequence of functions $\{f_\mathcal{S}^i\}_{i\in\mathbb{N}}$ converges in a pointwise sense.

Lemma 6.5. *Let $\{f_\mathcal{S}^i\}_{i\in\mathbb{N}}$ be the sequence of functions defined by Algorithm 6.4. For all $(q_1, q_2) \in Q_1 \times Q_2$, the sequence $\{f_\mathcal{S}^i(q_1, q_2)\}_{i\in\mathbb{N}}$ is increasing.*

Proof. For all $(q_1, q_2) \in Q_1 \times Q_2$, it is clear that $f_\mathcal{S}^0(q_1, q_2) \leq f_\mathcal{S}^1(q_1, q_2)$. Let us assume that for some $i \in \mathbb{N}$, for all $(q_1, q_2) \in Q_1 \times Q_2$, $f_\mathcal{S}^i(q_1, q_2) \leq f_\mathcal{S}^{i+1}(q_1, q_2)$. Let $(q_1, q_2) \in Q_1 \times Q_2$, then it is clear that

$$\sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_\mathcal{S}^i(q_1', q_2') \leq \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_\mathcal{S}^{i+1}(q_1', q_2').$$

Hence, it is straightforward that $f_\mathcal{S}^{i+1}(q_1, q_2) \leq f_\mathcal{S}^{i+2}(q_1, q_2)$. □

As a consequence of Lemma 6.5, for all $(q_1, q_2) \in Q_1 \times Q_2$, the sequence $\{f_\mathcal{S}^i(q_1, q_2)\}_{i\in\mathbb{N}}$ converges in $\mathbb{R}^+ \cup \{+\infty\}$. Hence, the sequence of functions $\{f_\mathcal{S}^i\}_{i\in\mathbb{N}}$ converges pointwise to a limit introduced in [dAFS04] for transition systems with a finite set of states as the *branching distance*.

Definition 6.6. Let $\{f_\mathcal{S}^i\}_{i\in\mathbb{N}}$ be the sequence of functions defined by Algorithm 6.4. The directed *branching distance* [dAFS04] between T_1 and T_2 is the function defined by

$$\forall (q_1, q_2) \in Q_1 \times Q_2, \ f_\mathcal{S}^{\min}(q_1, q_2) = \lim_{i\to\infty} f_\mathcal{S}^i(q_1, q_2).$$

Before giving the main result on the duality between the approach using relations and the approach using functions, we will need the following lemma.

Lemma 6.7. *Let $f : Q_1 \times Q_2 :\to \mathbb{R} + \cup\{+\infty\}$ be a function with closed level sets:*

$$\text{For all } \delta \geq 0,\ \mathcal{V}_\delta(f) = \{(q_1, q_2) \in Q_1 \times Q_2 |\ f(q_1, q_2) \leq \delta\} \text{ is a closed subset.}$$

Let $\delta \geq 0$, $q_1 \in Q_1$ and let C_2 be a compact subset of Q_2, then

$$\forall \varepsilon > 0,\ \exists q_2 \in C_2,\ \text{such that } f(q_1, q_2) \leq \delta + \varepsilon \implies \exists q_2 \in C_2,\ \text{such that } f(q_1, q_2) \leq \delta.$$

Proof. Let us remark that the family of sets $\{\mathcal{V}_{\delta+\varepsilon}(f)\}_{\varepsilon>0}$ satisfies the assumptions of Lemma 4.18. Hence, if for all $\varepsilon > 0$ there exists $q_2 \in C_2$ such that $f(q_1, q_2) \leq \delta + \varepsilon$ (*i.e.* $(q_1, q_2) \in \mathcal{V}_{\delta+\varepsilon}(f)$), then from Lemma 4.18, there exists $q_2 \in C_2$ such that for all $\varepsilon > 0$, $(q_1, q_2) \in \mathcal{V}_{\delta+\varepsilon}(f)$ (*i.e.* $f(q_1, q_2) \leq \delta + \varepsilon$). Since this holds for all $\varepsilon > 0$, it follows that $f(q_1, q_2) \leq \delta$. □

Theorem 6.8. *Let $\{\mathcal{S}^i_\delta\}_{i\in\mathbb{N}}$ be the sequence of sets defined by Algorithm 6.1 and $\{f^i_{\mathcal{S}}\}_{i\in\mathbb{N}}$ be the sequence of functions defined by Algorithm 6.4. Then, for all $i \in N$,*

$$\forall \delta \geq 0,\ \mathcal{S}^i_\delta = \left\{(q_1, q_2) \in Q_1 \times Q_2 |\ f^i_{\mathcal{S}}(q_1, q_2) \leq \delta\right\}. \tag{6.1}$$

Let $\mathcal{S}^{\max}_\delta$ be the maximal δ-approximate simulation relation of T_1 by T_2 and $f^{\min}_{\mathcal{S}}$ be the directed branching distance between T_1 and T_2. Then,

$$\forall \delta \geq 0,\ \mathcal{S}^{\max}_\delta = \left\{(q_1, q_2) \in Q_1 \times Q_2 |\ f^{\min}_{\mathcal{S}}(q_1, q_2) \leq \delta\right\}.$$

Proof. Let us prove the first part of the theorem. For $i = 0$, it is clear that equation (6.1) holds. Let us assume that equation (6.1) holds, for some $i \in \mathbb{N}$. Let $\delta \geq 0$, let $(q_1, q_2) \in \mathcal{S}^{i+1}_\delta$, then for all $q_1 \xrightarrow{\sigma}_1 q'_1$, there exists $q_2 \xrightarrow{\sigma}_2 q'_2$ such that $(q'_1, q'_2) \in \mathcal{S}^i_\delta$ (*i.e.* $f^i_{\mathcal{S}}(q'_1, q'_2) \leq \delta$). Therefore, we have

$$\sup_{q_1 \xrightarrow{\sigma}_1 q'_1} \inf_{q_2 \xrightarrow{\sigma}_2 q'_2} f^i_{\mathcal{S}}(q'_1, q'_2) \leq \delta.$$

In addition, since $(q_1, q_2) \in \mathcal{S}^{i+1}_\delta \subseteq \mathcal{S}^i_\delta$, we have $d_\Pi(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2) \leq f^i_{\mathcal{S}}(q_1, q_2) \leq \delta$. Hence, $f^{i+1}_{\mathcal{S}}(q_1, q_2) \leq \delta$. Reciprocally, let (q_1, q_2) be an element of $Q_1 \times Q_2$, such that $f^{i+1}_{\mathcal{S}}(q_1, q_2) \leq \delta$. Let $q_1 \xrightarrow{\sigma}_1 q'_1$, then for all $\varepsilon > 0$, there exists $q'_2 \in \mathrm{Post}^\sigma_2(q_2)$, such that $f^i_{\mathcal{S}}(q'_1, q'_2) \leq \delta + \varepsilon$. From Lemma 6.2, for all $\varepsilon > 0$, $\mathcal{S}^i_{\delta+\varepsilon}$ is a closed subset, hence $f^i_{\mathcal{S}}$ has closed level sets. It follows from Lemma 6.7 that there exists $q'_2 \in \mathrm{Post}^\sigma_2(q_2)$ such that $f^i_{\mathcal{S}}(q'_1, q'_2) \leq \delta$ (*i.e.* $(q'_1, q'_2) \in \mathcal{S}^i_\delta$). Now let us remark that $f^i_{\mathcal{S}}(q_1, q_2) \leq f^{i+1}_{\mathcal{S}}(q_1, q_2) \leq \delta$, hence $(q_1, q_2) \in \mathcal{S}^i_\delta$. Therefore, $(q_1, q_2) \in \mathcal{S}^{i+1}_\delta$. Hence, the first part of the theorem is proved by induction. The second part of the theorem is straightforward from the following sequence of equivalences:

$$f^{\min}_{\mathcal{S}}(q_1, q_2) \leq \delta \iff \forall i \in \mathbb{N},\ f^i_{\mathcal{S}}(q_1, q_2) \leq \delta \iff \forall i \in \mathbb{N},\ (q_1, q_2) \in \mathcal{S}^i_\delta \iff (q_1, q_2) \in \mathcal{S}^{\max}_\delta.$$

□

Let us remark that particularly, the zero set of the directed *branching distance* between T_1 and T_2 is the maximal exact simulation relation of T_1 by T_2. Another interesting fact is that the level sets of the functions $\{f^i_{\mathcal{S}}\}_{i\in\mathbb{N}}$ and $f^{\min}_{\mathcal{S}}$ are closed subsets.

For metric transition systems with an infinite set of states, the fixed point iteration of Algorithm 6.4 may not be an efficient way to compute the directed *branching distance*. An alternative method is to solve the following fixed-point equation.

Theorem 6.9. *The directed branching distance between T_1 and T_2 is the smallest function defined on $Q_1 \times Q_2$ with values in $\mathbb{R}^+ \cup \{+\infty\}$ satisfying the following functional equation:*

$$f_{\mathcal{S}}^{\min}(q_1, q_2) = \max\left(d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^{\min}(q_1', q_2') \right). \tag{6.2}$$

Proof. Let $(q_1, q_2) \in Q_1 \times Q_2$, for all $i \in \mathbb{N}$, we have $f_{\mathcal{S}}^i(q_1, q_2) \leq f_{\mathcal{S}}^{\min}(q_1, q_2)$. Hence, for all $i \in \mathbb{N}$,

$$\sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^i(q_1', q_2') \leq \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^{\min}(q_1', q_2').$$

Therefore, for all $i \in \mathbb{N}$, we have

$$f_{\mathcal{S}}^{i+1}(q_1', q_2') \leq \max\left(d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^{\min}(q_1', q_2') \right).$$

When i tends to $+\infty$, this inequality becomes

$$f_{\mathcal{S}}^{\min}(q_1, q_2) \leq \max\left(d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^{\min}(q_1', q_2') \right).$$

Since for all $(q_1, q_2) \in Q_1 \times Q_2$, the sequence $\{f_{\mathcal{S}}^i(q_1, q_2)\}_{i \in \mathbb{N}}$ is increasing, then the sequence

$$\left\{ \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^i(q_1', q_2') \right\}_{i \in \mathbb{N}}$$

is increasing as well. Let $l(q_1, q_2) \in \mathbb{R}^+ \cup \{+\infty\}$ denote the limit of this sequence. For all $i \in \mathbb{N}$,

$$\sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^i(q_1', q_2') \leq l(q_1, q_2).$$

Let $q_1 \xrightarrow{\sigma}_1 q_1'$, for all $i \in \mathbb{N}$, for all $\varepsilon > 0$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'^i$, such that $f_{\mathcal{S}}^i(q_1', q_2') \leq l(q_1, q_2) + \varepsilon$. From Lemma 6.7, it follows that for all $i \in \mathbb{N}$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'^i$, such that $f_{\mathcal{S}}^i(q_1', q_2'^i) \leq l(q_1, q_2)$. $\mathrm{Post}_2^\sigma(q_2)$ is compact, then there exists $\{q_2'^{i_k}\}_{k \in \mathbb{N}}$ a subsequence of $\{q_2'^i\}_{i \in \mathbb{N}}$ which converges to $q_2' \in \mathrm{Post}_2^\sigma(q_2)$. Let $i \in \mathbb{N}$, there exists $n \in \mathbb{N}$, such that for all $k \geq n$, $i_k \geq i$. Hence for all $k \geq n$, $f_{\mathcal{S}}^i(q_1', q_2'^{i_k}) \leq f_{\mathcal{S}}^{i_k}(q_1', q_2'^{i_k}) \leq l(q_1, q_2)$. Since this holds for all $k \geq n$, we have $f_{\mathcal{S}}^i(q_1', q_2') \leq l(q_1, q_2)$. This holds for all $i \in \mathbb{N}$ and hence, $f_{\mathcal{S}}^{\min}(q_1', q_2') \leq l(q_1, q_2)$. We proved that for all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$, such that $f_{\mathcal{S}}^{\min}(q_1', q_2') \leq l(q_1, q_2)$. Therefore,

$$\sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^{\min}(q_1', q_2') \leq l(q_1, q_2).$$

Hence,

$$\max\left(d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}^{\min}(q_1', q_2') \right) \leq f_{\mathcal{S}}^{\min}(q_1, q_2).$$

Now, let us prove that $f_{\mathcal{S}}^{\min}$ is the smallest function satisfying equation (6.2). Let f be a solution of (6.2), then for all $(q_1, q_2) \in Q_1 \times Q_2$, $f(q_1, q_2) \geq d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right) = f_{\mathcal{S}}^0(q_1, q_2)$. By induction, it is easy to show that for all $i \in \mathbb{N}$ $f(q_1, q_2) \geq f_{\mathcal{S}}^i(q_1, q_2)$ and hence $f(q_1, q_2) \geq f_{\mathcal{S}}^{\min}(q_1, q_2)$. □

Let us remark that the directed *branching distance* $f_{\mathcal{S}}^{\min}$ is the smallest solution of the fixed-point equation (6.2) in the sense that for all solution f of (6.2), for all $(q_1, q_2) \in Q_1 \times Q_2$, $f_{\mathcal{S}}^{\min}(q_1, q_2) \leq f(q_1, q_2)$.

We now arrive to the main result of this section which states that for regular metric transition systems, the simulation metric can be computed by solving a static game where the cost function of the game is the directed *branching distance*.

Theorem 6.10. *Let $f_{\mathcal{S}}^{\min}$ be the directed branching distance between T_1 and T_2. Then,*

$$d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) = \sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{S}}^{\min}(q_1, q_2). \tag{6.3}$$

Proof. Let $\delta > d_{\overrightarrow{\mathcal{S}}}(T_1, T_2)$, then $T_1 \preceq_\delta T_2$. Hence, for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$, such that $(q_1, q_2) \in \mathcal{S}_\delta^{\max}$. From Theorem 6.8, it follows that $f_{\mathcal{S}}^{\min}(q_1, q_2) \leq \delta$. Consequently,

$$\sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{S}}^{\min}(q_1, q_2) \leq \delta.$$

Since this holds for all $\delta > d_{\overrightarrow{\mathcal{S}}}(T_1, T_2)$,

$$\sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{S}}^{\min}(q_1, q_2) \leq d_{\overrightarrow{\mathcal{S}}}(T_1, T_2).$$

Conversely, let

$$\delta = \sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{S}}^{\min}(q_1, q_2).$$

Let $q_1 \in Q_1^0$, then for all $\varepsilon > 0$, there exists $q_2 \in Q_2^0$ such that, $f_{\mathcal{S}}^{\min}(q_1, q_2) \leq \delta + \varepsilon$. From Lemma 6.7, there exists $q_2 \in Q_2^0$ such that, $f_{\mathcal{S}}^{\min}(q_1, q_2) \leq \delta$. Hence, for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$, such that $(q_1, q_2) \in \mathcal{S}_\delta^{\max}$. Consequently, $T_1 \preceq_\delta T_2$ and therefore $d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) \leq \delta$. □

To summarize, in order to exactly compute the simulation metric, one must solve equation (6.2) in order to obtain the branching distance, and then solve the much easier static game (6.3). In Section 7, we will consider relaxations of equation (6.2), but we first develop analogous results for exactly computing the bisimulation metric.

6.3. **Maximal approximate bisimulations.** The development of this section is similar to the exact computation of the simulation metric and therefore the proofs in this section are omitted. The well known bisimulation algorithm [KS90], can be generalized for approximate bisimulations as follows.

Algorithm 6.11. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$. For $\delta \geq 0$, define the following sequence $\{\mathcal{S}_\delta^i\}_{i \in \mathbb{N}}$ of subsets of $\mathcal{Q}_1 \times \mathcal{Q}_2$:*

$$\begin{aligned} \mathcal{B}_\delta^0 &= \{(q_1, q_2) \in \mathcal{Q}_1 \times \mathcal{Q}_2 |\ d_\Pi(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) \leq \delta\} \\ \mathcal{B}_\delta^{i+1} &= \left\{ (q_1, q_2) \in \mathcal{B}_\delta^i \;\middle|\; \begin{array}{l} \forall q_1 \xrightarrow{\sigma}_1 q_1', \exists q_2 \xrightarrow{\sigma}_2 q_2', (q_1', q_2') \in \mathcal{B}_\delta^i \text{ and} \\ \forall q_2 \xrightarrow{\sigma}_2 q_2', \exists q_1 \xrightarrow{\sigma}_1 q_1', (q_1', q_2') \in \mathcal{B}_\delta^i \end{array} \right\}, \ i \in \mathbb{N}. \end{aligned}$$

The above algorithm approaches the maximal (coarsest) approximate bisimulation relation $\mathcal{B}_\delta^{\max}$.

Theorem 6.12. *Let $\{\mathcal{B}_\delta^i\}_{i\in\mathbb{N}}$ be the decreasing sequence of sets defined by Algorithm 6.11 and $\mathcal{B}_\delta^{\max}$ be the maximal δ-approximate bisimulation relation between T_1 and T_2. Then, the following properties hold:*

$$\forall i \in \mathbb{N}, \mathcal{B}_\delta^{\max} \subseteq \mathcal{B}_\delta^i,$$
$$\bigcap_{i=0}^{i=+\infty} \mathcal{B}_\delta^i = \mathcal{B}_\delta^{\max}.$$

6.4. **Branching distance.** If we represent approximate simulation relations as levels sets of functions, then the following dual approach based on functions can be used for fixed-point computation.

Algorithm 6.13. *Let $T1$, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$. Define the following sequence $\{f_\mathcal{B}^i\}_{i\in\mathbb{N}}$ of functions from $\mathcal{Q}_1 \times \mathcal{Q}_2$ to $\mathbb{R}^+ \cup \{+\infty\}$:*

$$\begin{aligned} f_\mathcal{B}^0(q_1, q_2) &= d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right) \\ f_\mathcal{B}^{i+1}(q_1, q_2) &= \max\left(d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_\mathcal{B}^i(q_1', q_2'), \sup_{q_2 \xrightarrow{\sigma}_2 q_2'} \inf_{q_1 \xrightarrow{\sigma}_1 q_1'} f_\mathcal{B}^i(q_1', q_2')\right), \ i \in \mathbb{N}. \end{aligned}$$

As for the case of approximate simulation, we can show that for all $(q_1, q_2) \in Q_1 \times Q_2$, the series $\{f_\mathcal{B}^i(q_1, q_2)\}_{i\in\mathbb{N}}$ is increasing. Hence, the sequence of functions $\{f_\mathcal{B}^i\}_{i\in\mathbb{N}}$ converges pointwise in $\mathbb{R}^+ \cup \{+\infty\}$.

Definition 6.14. Let $\{f_\mathcal{B}^i\}_{i\in\mathbb{N}}$ be the sequence of functions defined by Algorithm 6.13. The *branching distance* [dAFS04] between T_1 and T_2 is the function defined by

$$\forall (q_1, q_2) \in Q_1 \times Q_2, \ f_\mathcal{B}^{\min}(q_1, q_2) = \lim_{i\to\infty} f_\mathcal{B}^i(q_1, q_2).$$

The duality between the approach using relations and the approach using functions is captured by the following result.

Theorem 6.15. *Let $\{\mathcal{B}_\delta^i\}_{i\in\mathbb{N}}$ be the sequence of sets defined by Algorithm 6.11 and $\{f_\mathcal{B}^i\}_{i\in\mathbb{N}}$ be the sequence of functions defined by Algorithm 6.13. Then, for all $i \in N$,*

$$\forall \delta \geq 0, \ \mathcal{B}_\delta^i = \left\{(q_1, q_2) \in Q_1 \times Q_2 |\ f_\mathcal{B}^i(q_1, q_2) \leq \delta\right\}.$$

Let $\mathcal{B}_\delta^{\max}$ be the maximal δ-approximate bisimulation relation between T_1 and T_2 and $f_\mathcal{B}^{\min}$ be the branching distance between T_1 and T_2. Then,

$$\forall \delta \geq 0, \ \mathcal{B}_\delta^{\max} = \left\{(q_1, q_2) \in Q_1 \times Q_2 |\ f_\mathcal{B}^{\min}(q_1, q_2) \leq \delta\right\}.$$

The branching distance is the smallest solution of the fixed-point equation given by the following theorem.

Theorem 6.16. *The branching distance between T_1 and T_2 is the smallest function defined on $Q_1 \times Q_2$ with values in $\mathbb{R}^+ \cup \{+\infty\}$ satisfying the following functional equation:*

$$f_\mathcal{B}^{\min}(q_1, q_2) = \max\left(d_\Pi\left(\langle\langle q_1\rangle\rangle_1, \langle\langle q_2\rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_\mathcal{B}^{\min}(q_1', q_2'), \sup_{q_2 \xrightarrow{\sigma}_2 q_2'} \inf_{q_1 \xrightarrow{\sigma}_1 q_1'} f_\mathcal{B}^{\min}(q_1', q_2')\right).$$

Finally, similar to the simulation metric, for regular metric transition systems, the bisimulation metric can computed by solving a static game where the cost function of the game is the *branching distance.*

Theorem 6.17. *Let $f_{\mathcal{B}}^{\min}$ be the branching distance between T_1 and T_2. Then,*

$$d_{\overrightarrow{\mathcal{B}}}(T_1, T_2) = \max\left(\sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{B}}^{\min}(q_1, q_2),\ \sup_{q_2 \in Q_2^0} \inf_{q_1 \in Q_1^0} f_{\mathcal{B}}^{\min}(q_1, q_2)\right).$$

In this section, we proposed a method for the exact computation of the simulation and the bisimulation metrics between regular metric transition systems. It consists in solving a static game where the cost function is the branching distance (see Theorems 6.10 and 6.17). For systems with a finite number of states, fixed point Algorithms 6.4 and 6.13 for the computation of the branching distance are guaranteed to terminate within a finite number of states. For systems with an infinite number of states, these algorithms do not necessarily reach a fixed point in a finite number of iterations. Then, an alternative approach is to solve directly the functional equations given by Theorems 6.9 and 6.16. However, in cases where the equations given by Theorems 6.9 and 6.16 are difficult to solve, one can consider the relaxation that are proposed in the following section.

7. Approximate Metric Computation

One of the great advantages of having metric structure on transition systems, is that metrics enable us to consider relaxations. If the equations given by Theorems 6.9 and 6.16 are difficult to solve, then we can consider relaxations that will result in computing an over-approximation of the simulation or the bisimulation metrics. The relaxations we propose are based on classes of functions that we call simulation and bisimulation functions.

7.1. Simulation Functions.

Let $T_1 = (Q_1, \Sigma, \rightarrow_1, Q_1^0, \Pi, \langle\langle . \rangle\rangle_1)$ and $T_2 = (Q_2, \Sigma, \rightarrow_2, Q_2^0, \Pi, \langle\langle . \rangle\rangle_2)$ be two elements of $\mathcal{T}_M^*(\Sigma, \Pi)$[5]. A simulation function between T_1 and T_2 is a positive function defined on $Q_1 \times Q_2$, bounding the distance between the observations associated to the couple (q_1, q_2) and non increasing under the dynamics of the systems.

Definition 7.1 (Simulation function)**.** A function $f_{\mathcal{S}} : Q_1 \times Q_2 \rightarrow \mathbb{R}^+ \cup \{+\infty\}$ is called a simulation function between T_1 and T_2 if its level sets are closed, and for all $(q_1, q_2) \in Q_1 \times Q_2$:

$$f_{\mathcal{S}}(q_1, q_2) \geq \max\left(d_{\Pi}\left(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2\right),\ \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{S}}(q_1', q_2')\right).$$

For regular metric labeled transition systems, simulation functions are reminiscent of (robust) Lyapunov functions and can be seen as relaxations of the directed *branching distance*. In fact, the directed *branching distance* is a simulation function itself:

Theorem 7.2. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$ and let $f_{\mathcal{S}}^{\min}$ be the directed branching distance between T_1 and T_2. Then, $f_{\mathcal{S}}^{\min}$ is the smallest simulation function between T_1 and T_2.*

Proof. We know that $f_{\mathcal{S}}^{\min}$ has closed level sets. From Theorem 6.9, it is clear that $f_{\mathcal{S}}^{\min}$ is a simulation function. Let $f_{\mathcal{S}}$ be a simulation function between T_1 and T_2, let $\{f_{\mathcal{S}}^i\}_{i \in \mathbb{N}}$ be the sequence of functions defined by Algorithm 6.4. We have, for all $(q_1, q_2) \in Q_1 \times Q_2$, $f_{\mathcal{S}}(q_1, q_2) \geq d_{\Pi}\left(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2\right) = f_{\mathcal{S}}^0(q_1, q_2)$. By induction, it is easy to show that for all $(q_1, q_2) \in Q_1 \times Q_2$, for all $i \in \mathbb{N}$, $f_{\mathcal{S}}(q_1, q_2) \geq f_{\mathcal{S}}^i(q_1, q_2)$ and hence $f_{\mathcal{S}}(q_1, q_2) \geq f_{\mathcal{S}}^{\min}(q_1, q_2)$. □

[5]Even though we do not need to assume that T_1 and T_2 are regular, we do have to assume that for all labels $\sigma \in \Sigma$, the successor maps Post_1^{σ} and Post_2^{σ} have compact images.

As in Theorem 6.9, the directed *branching distance* $f_{\mathcal{S}}^{\min}$ is the smallest simulation function between T_1 and T_2 in the sense that for all simulation function $f_{\mathcal{S}}$, for all $(q_1, q_2) \in Q_1 \times Q_2$, $f_{\mathcal{S}}^{\min}(q_1, q_2) \leq f_{\mathcal{S}}(q_1, q_2)$. Thus, the directed *branching distance* between T_1 and T_2 will be also called minimal simulation function between T_1 and T_2.

A simulation function between T_1 and T_2 is a convenient way to define a family $\{\mathcal{S}_\delta\}_{\delta \geq 0}$ of approximate simulation relations of T_1 by T_2.

Theorem 7.3. *Let $f_{\mathcal{S}}$ be a simulation function between T_1 and T_2. Then for all $\delta \geq 0$,*

$$\mathcal{S}_\delta = \{(q_1, q_2) \in Q_1 \times Q_2 |\ f_{\mathcal{S}}(q_1, q_2) \leq \delta\}$$

is a δ-approximate simulation relation of T_1 by T_2.

Proof. Let $(q_1, q_2) \in \mathcal{S}_\delta$, then $d_\Pi(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) \leq f_{\mathcal{S}}(q_1, q_2) \leq \delta$. Let $q_1 \xrightarrow{\sigma}_1 q_1'$, then for all $\varepsilon > 0$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $f_{\mathcal{S}}(q_1', q_2') \leq f_{\mathcal{S}}(q_1, q_2) + \varepsilon \leq \delta + \varepsilon$. From Lemma 6.7, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $f_{\mathcal{S}}(q_1', q_2') \leq \delta$. Hence $\mathcal{S}_\delta$ is a δ-approximate simulation relation of T_1 by T_2. □

Let us remark that particularly the zero set of a simulation function is an exact simulation relation. We can now state the following result which shows that an over-approximation of the simulation metric can be computed by solving a game where the cost function is a simulation function.

Theorem 7.4. *Let $f_{\mathcal{S}}$ be any simulation function between T_1 and T_2. Then,*

$$d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) \leq \sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{S}}(q_1, q_2).$$

Proof. Let

$$\delta = \sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{S}}^{\min}(q_1, q_2).$$

Let $q_1 \in Q_1^0$, then for all $\varepsilon > 0$, there exists $q_2 \in Q_2^0$ such that, $f_{\mathcal{S}}^{\min}(q_1, q_2) \leq \delta + \varepsilon$. Hence, for all $\varepsilon > 0$, $T_1 \preceq_{\delta+\varepsilon} T_2$. Therefore, $d_{\overrightarrow{\mathcal{S}}}(T_1, T_2) \leq \delta$. □

The above theorem enables us to over-approximate the simulation metric by relaxing the solution of equation (6.2) with Lyapunov-like simulation functions. In addition to this relaxation, the following result shows that, for the synchronous composition defined in Section 5, simulation functions are also compositional.

Theorem 7.5. *Let $f_{\mathcal{S}_1}$ be a simulation function of T_1 by U_1 and $f_{\mathcal{S}_2}$ be a simulation function of T_2 by U_2, then $f_{\mathcal{S}} = f_{\mathcal{S}_1} + f_{\mathcal{S}_2}$ is a simulation function of $T_1 || T_2$ by $U_1 || U_2$.*

Proof. Let $(q_1, q_2, p_1, p_2) \in Q_1 \times Q_2 \times P_1 \times P_2$, then

$$\begin{aligned} f_{\mathcal{S}}(q_1, q_2, p_1, p_2) &= f_{\mathcal{S}_1}(q_1, p_1) + f_{\mathcal{S}_2}(q_2, p_2) \\ &\geq = d_{\Pi_1}(\langle\langle q_1 \rangle\rangle_1, \langle\langle p_1 \rangle\rangle_1) + d_{\Pi_2}(\langle\langle q_2 \rangle\rangle_2, \langle\langle p_2 \rangle\rangle_2) = d_\Pi(\langle\langle (q_1, q_2) \rangle\rangle, \langle\langle (p_1, p_2) \rangle\rangle). \end{aligned}$$

Let $(q_1, q_2) \xrightarrow{\sigma} (q_1', q_2')$, then $q_1 \xrightarrow{\sigma}_1 q_1'$ and $q_2 \xrightarrow{\sigma}_2 q_2'$. Let $\varepsilon > 0$, there exist $p_1 \xrightarrow{\sigma}_1 p_1'$ and $p_2 \xrightarrow{\sigma}_2 p_2'$ such that $f_{\mathcal{S}_1}(q_1', p_1') \leq f_{\mathcal{S}_1}(q_1, p_1) + \varepsilon$ and $f_{\mathcal{S}_2}(q_2', p_2') \leq f_{\mathcal{S}_2}(q_2, p_2) + \varepsilon$. Hence, for all $\varepsilon > 0$, there exists $(p_1, p_2) \xrightarrow{\sigma} (p_1', p_2')$ such that $f_{\mathcal{S}}(q_1', q_2', p_1', p_2') \leq f_{\mathcal{S}}(q_1, q_2, p_1, p_2) + 2\varepsilon$. Therefore,

$$f_{\mathcal{S}}(q_1, q_2, p_1, p_2) \geq \sup_{(q_1, q_2) \xrightarrow{\sigma} (q_1', q_2')} \inf_{(p_1, p_2) \xrightarrow{\sigma} (p_1', p_2')} f_{\mathcal{S}}(q_1', q_2', p_1', p_2')$$

which leads to the expected result. □

7.2. **Bisimulation Functions.** We now consider similar relaxations for the bisimulation metric. Bisimulation functions are defined in a similar way to simulation functions. The proofs of the results of this part are omitted because they are similar to the proofs for simulation functions.

Definition 7.6 (Bisimulation functions)**.** A function $f_{\mathcal{B}} : Q_1 \times Q_2 \to \mathbb{R}^+ \cup \{+\infty\}$ is a bisimulation function between T_1 and T_2 if its level sets are closed and for all $(q_1, q_2) \in Q_1 \times Q_2$:

$$f_{\mathcal{B}}(q_1, q_2) \geq \max \left(d_{\Pi}\left(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2\right), \sup_{q_1 \xrightarrow{\sigma}_1 q_1'} \inf_{q_2 \xrightarrow{\sigma}_2 q_2'} f_{\mathcal{B}}(q_1', q_2'), \sup_{q_2 \xrightarrow{\sigma}_2 q_2'} \inf_{q_1 \xrightarrow{\sigma}_1 q_1'} f_{\mathcal{B}}(q_1', q_2') \right).$$

For regular metric labeled transition systems, we can show that the *branching distance* is a bisimulation function.

Theorem 7.7. *Let T_1, $T_2 \in \mathcal{T}_M^*(\Sigma, \Pi)$, let $f_{\mathcal{B}}^{\min}$ be the branching distance between T_1 and T_2. Then, $f_{\mathcal{B}}^{\min}$ is the smallest bisimulation function between T_1 and T_2.*

Thus, the directed *branching distance* between T_1 and T_2 will be also called minimal bisimulation function between T_1 and T_2.

Theorem 7.8. *Let $f_{\mathcal{B}}$ be a bisimulation function between T_1 and T_2, then for all $\delta \geq 0$,*

$$\mathcal{B}_\delta = \{(q_1, q_2) \in Q_1 \times Q_2 |\ f_{\mathcal{B}}(q_1, q_2) \leq \delta\}$$

is a δ-approximate bisimulation relation of T_1 by T_2.

Particularly the zero set of a bisimulation function is an exact bisimulation relation.

Theorem 7.9. *Let $f_{\mathcal{B}}$ be a bisimulation function between T_1 and T_2. Then,*

$$d_{\mathcal{B}}^{\rightarrow}(T_1, T_2) \leq \max \left(\sup_{q_1 \in Q_1^0} \inf_{q_2 \in Q_2^0} f_{\mathcal{B}}(q_1, q_2), \sup_{q_2 \in Q_2^0} \inf_{q_1 \in Q_1^0} f_{\mathcal{B}}(q_1, q_2) \right).$$

The following theorem states that bisimulation functions are compositional.

Theorem 7.10. *Let $f_{\mathcal{B}_1}$ be a bisimulation function between T_1 and U_1 and $f_{\mathcal{B}_2}$ be a bisimulation function between T_2 and U_2, then $f_{\mathcal{B}} = f_{\mathcal{B}_1} + f_{\mathcal{B}_2}$ is a simulation function of $T_1 || T_2$ by $U_1 || U_2$.*

In this section, we proposed Lyapunov-like relaxations for computing over-approximations of the simulation and the bisimulation metrics, which can further overapproximate the language and reachability metric between two transition systems. In the final section, we illustrate how these computations could be used for reducing the complexity of safety verification problems for continuous systems.

8. Verification Illustration

Despite significant progress in the formal verification of discrete systems [BCM+90], the progress for continuous (and thus hybrid) systems has been limited to systems of small continuous dimension. The Lyapunov-like relaxations of Section 7 allow us to use a wealth of Lyapunov techniques for approximating simulation and bisimulation functions. We present two examples, one simply illustrating the steps of our framework for nondeterministic linear systems, and one showing how Lyapunov equations can dramatically reduce the complexity of safety verification problems for deterministic linear systems with an approximation error that is easily computable and acceptable.

8.1. **Nondeterministic Continuous Systems.** Consider the following continuous-time linear system with bounded disturbances:

$$\left\{\begin{array}{lllllllll} \dot{x}_1(t) & = & - & 2x_1(t) & + & y_1(t) & + & z_1(t) & + & d_1(t) \\ \dot{y}_1(t) & = & - & x_1(t) & & & + & z_1(t) & + & d_1(t) \\ \dot{z}_1(t) & = & & x_1(t) & - & y_1(t) & - & 2z_1(t) & & \end{array}\right.$$

The system is observed through the variable $\pi_1(t) = x_1(t)$. The values of the disturbance $d_1(.)$ is constrained in the set $[-1, 1]$. The initial state lies in the polytope I_1 given by:

$$I_1 = \left\{(x_1, y_1, z_1) \in \mathbb{R}^3 \mid -1 \leq x_1 - y_1 - z_1 \leq 1,\ 8 \leq y_1 \leq 9,\ -6 \leq z_1 \leq -4\right\}.$$

As stated previously, we can derive a regular metric transition system $T_1 \in \mathcal{T}_M^*(\mathbb{R}^+, \mathbb{R})$ which is also nondeterministic. We want to show that T_1 can be approximated by the regular metric labeled transition system $T_2 \in \mathcal{T}_M^*(\mathbb{R}^+, \mathbb{R})$ generated by the following linear system:

$$\dot{x}_2(t) = -x_2(t) + d_2(t).$$

The system is observed through the variable $\pi_2(t) = x_2(t)$. The values of the disturbance $d_2(.)$ are constrained in the set $[-1, 1]$. The initial value of the state variable lies in the interval $I_2 = [2, 5]$. Let us show that

$$f_{\mathcal{B}}(x_1, y_1, z_1, x_2) = |x_1 - y_1 - z_1| + |y_1 + z_1 - x_2|$$

is a bisimulation function between T_1 and T_2. First, let us remark that from the triangular inequality

$$|x_1 - x_2| \leq f_{\mathcal{B}}(x_1, y_1, z_1, x_2).$$

Hence, $f_{\mathcal{B}}(x_1, y_1, z_1, x_2)$ bounds the distance between the observations of T_1 and T_2. Moreover, we can check that

$$\begin{aligned} \frac{\partial f_{\mathcal{B}}}{\partial x_1}\dot{x}_1 + \frac{\partial f_{\mathcal{B}}}{\partial y_1}\dot{y}_1 + \frac{\partial f_{\mathcal{B}}}{\partial z_1}\dot{z}_1 + \frac{\partial f_{\mathcal{B}}}{\partial x_2}\dot{x}_2 &= -2|x_1 - y_1 - z_1| - |y_1 + z_1 - x_2| \\ &\quad + (d_1 - d_2)\,\mathrm{sgn}(y_1 + z_1 - x_2)\,. \end{aligned}$$

Hence, for all disturbance $d_1(t)$ (respectively $d_2(t)$) there exists a disturbance $d_2(t)$ (respectively $d_1(t)$) such that $df_{\mathcal{B}}(x_1(t), y_1(t), z_1(t), x_2(t))/dt$ is negative. Therefore, $f_{\mathcal{B}}$ is non increasing under the dynamics of the systems. Hence, it is clear that $f_{\mathcal{B}}$ is a bisimulation function between T_1 and T_2.

¿From Theorem 7.9, an over-approximation of the bisimulation metric between T_1 and T_2 can be computed by solving a game. We can check that

$$\sup_{(x_1,y_1,z_1)\in I_1} \inf_{x_2 \in I_2} f_{\mathcal{B}}(x_1, y_1, z_1, x_2) = \sup_{(x_1,y_1,z_1)\in I_1} |x_1 - y_1 - z_1| = 1$$

and that

$$\sup_{x_2 \in I_2} \inf_{(x_1,y_1,z_1)\in I_1} f_{\mathcal{B}}(x_1, y_1, z_1, x_2) = 0.$$

Hence, $d_{\mathcal{B}}(T_1, T_2) \leq 1$. The systems T_1 and T_2 are approximately bisimilar with the precision 1. We now propose to use this result to compute an over-approximation of the reachable set of T_1. From Theorem 4.31, we know that the distance between the reachable sets of T_1 and T_2 (*i.e.* the reachability metric) is bounded by $d_{\mathcal{B}}(T_1, T_2)$ and hence by 1. It is easy to compute the reachable set of T_2 which is equal to $(-1, 5]$. Then, from Theorem 4.31, we obtain that $Reach(T_1) \subseteq [-2, 6]$. The systematic computation of such approximations for nondeterministic linear systems using robust Lyapunov techniques is the focus of current research for both linear [GP05a] and nonlinear systems [GP05b].

8.2. **Deterministic Continuous Systems.** The second example we consider consists in the approximation of a high dimensional deterministic linear system of the form:

$$\left\{ \begin{array}{rcl} \dot{x}_1(t) & = & A_1 x_1(t),\ x_1(t) \in \mathbb{R}^{100},\ x_1(0) \in I_1, \\ \pi_1(t) & = & C_1 x_1(t),\ \pi_1(t) \in \mathbb{R}^2 \end{array} \right. \tag{8.1}$$

where I_1 is a bounded polytope of $\mathbb{R}^{100}$. The unstable subspace of the system is of dimension 6. The dynamics on the 94 dimensional stable subspace was chosen at random. We want to verify that the system is safe, that is if the intersection of its reachable set with an unsafe set Π_U, shown in Figure 1, is empty. We approximated this system with two different deterministic linear systems of smaller dimension.

The first approximation we considered is six dimensional and consists of simply projecting the original system on its unstable subspace. Similar to the previous example, we computed a (quadratic) bisimulation function between the two systems by solving a Lyapunov equation (see [GP05a] for more details). Then, an upper bound of the bisimulation metric between the two systems was computed by solving the game given by Theorem 7.9. The second approximation is a ten dimensional approximation consisting of the projection of the original system on the subspace spanned by the eigenvectors associated to the eigenvalues with the largest real part.

Figure 1 shows reachable sets of the hundred dimensional system, its six dimensional approximation, and its ten dimensional approximation and the associated approximation errors. We can see that the six dimensional approximation does not allow us to conclude that the system is safe, even though the original system is actually safe. However, by adding slightly more modeling detail, the ten dimensional approximation allows to conclude that the original system is safe.

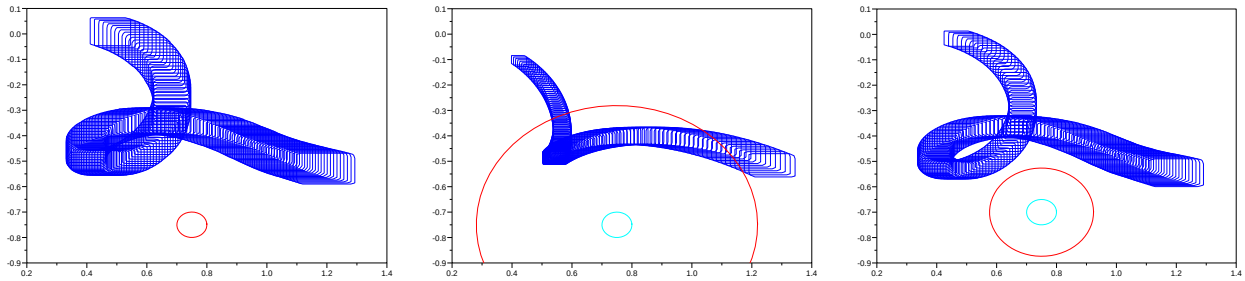

FIGURE 1. Reachable sets of the original hundred dimensional system (left) and of its six dimensional and ten dimensional approximations (center and right). The circle on the left figure and the inner circle on the others represent the unsafe set Π_U. The outer circle on the center and right figure consists of the set of points whose distance to Π_U is smaller than the upper bound of the bisimulation metric.

The reachable sets were computed using the very recent zonotope techniques [Gir05]. The system (Pentium 3, 700 MHz, Scilab) needed 51 seconds to compute the reachable set of the hundred dimensional system. It needed less than 1 second to process the six dimensional approximation, including the computation of the reachable set, the computation of a bisimulation function and the computation of an upper bound of the bisimulation metric. It needed about 4 seconds to process the same tasks for the ten dimensional approximation. This is strong evidence, that approximate bisimulations allow to significantly reduce the computation time of the verification process. In [GP05a, GP05b], we propose systematic methods for the computation of simulation and bisimulation functions for

linear systems and nonlinear systems, that could be used for reducing the complexity of most safety verification approaches for continuous and hybrid systems.

The example also illustrates the important point that robustness simplifies verification. Indeed, if the distance between the reachable set of the original system and the set of unsafe states would have been larger then the approximation of the original system by its unstable subsystem might have been sufficient to check the safety. Generally, the more robustly safe a system is, the larger the distance from the unsafe safe, resulting in larger model compression and easier safety verification.

9. Conclusion

In this paper, we have developed a framework of system approximation for metric transition systems by developing a hierarchy of metrics for reachable set inclusion, language inclusion and simulation and bisimulation relations. Our framework is compositional and captures the established exact relationships for discrete systems, and enables approximate relationships for deterministic and nondeterministic continuous systems. The exact computation of the metrics, which requires the branching distance and solving a static game, can be relaxed in a Lyapunov-like manner using simulation and bisimulations functions.

Future research includes developing algorithmic methods for computing such functions for linear, nonlinear, and hybrid systems. Even though we considered synchronous composition in this paper, more general composition operators will also be considered. Finally, for sophisticated verification properties expressible in temporal logics, an exciting direction emerges in understanding the relationship between approximation metrics and more robust semantics of spatial and temporal logics [DCMM04].

References

[ABDM00] E. Asarin, O. Bournez, T. Dang, and O. Maler. Approximate reachability analysis of piecewise linear dynamical systems. In *Hybrid Systems: Computation and Control*, volume 1790 of *LNCS*, pages 21–31. Springer, 2000.

[AD04] E. Asarin and T. Dang. Abstraction by projection and application to multi-affine systems. In *Hybrid Systems: Computation and Control*, volume 2993 of *LNCS*, pages 32–47. Springer, 2004.

[ADG03] E. Asarin, T. Dang, and A. Girard. Reachability of non-linear systems using conservative approximations. In *Hybrid Systems: Computation and Control*, volume 2623 of *LNCS*, pages 22–35. Springer, 2003.

[ADI02] R. Alur, T. Dang, and F. Ivancic. Reachability analysis of hybrid systems via predicate abstraction. In *Hybrid Systems: Computation and Control*, volume 2289 of *LNCS*, pages 35–48. Springer, 2002.

[AHP00] R. Alur, T.A. Henzinger, and G. Lafferriere G.J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(7):971–984, July 2000.

[ASG00] A. C. Antoulas, D. C. Sorensen, and S. Gugercin. A survey of model reduction methods for large-scale systems. *Contemporary Mathematics*, 280:193–219, 2000.

[Aub91] J. P. Aubin. *Viability Theory*. Birkhauser, 1991.

[BCM+90] J.R. Burch, E.M. Clarke, K.L. McMillan, D.L. Dill, and L.J. Hwang. Symbolic Model Checking: 10^{20} States and Beyond. In *Proceedings of the Fifth Annual IEEE Symposium on Logic in Computer Science*, pages 1–33, Washington, D.C., 1990.

[CB02] P. Caspi and A. Benveniste. Toward an approximation theory for computerized control. In *Embedded Software (EMSOFT)*, volume 2491 of *LNCS*, pages 294–304. Springer, 2002.

[CGP00] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. MIT Press, 2000.

[CK99] A. Chutinan and B.H. Krogh. Verification of polyhedral invariant hybrid automata using polygonal flow pipe approximations. In *Hybrid Systems: Computation and Control*, volume 1569 of *LNCS*, pages 76–90. Springer, 1999.

[dAFS04] L. de Alfaro, M. Faella, and M. Stoelinga. Linear and branching metrics for quantitative transition systems. In *ICALP'04*, volume 3142 of *LNCS*, pages 1150–1162. Springer, 2004.

[DCMM04] J.M. Davoren, V. Coulthard, N. Markey, and T. Moor. Non-deterministic temporal logics for general flow systems. In *Hybrid Systems: Computation and Control*, volume 2993 of *Lecture Notes in Computer Science*, pages 280–295. Springer-Verlag, 2004.

[DGJP04] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Metrics for labelled markov processes. *Theoretical Computer Science*, 318(3):323–354, June 2004.

[Ewa96] G. Ewald. *Combinatorial convexity and algebraic geometry*. Springer, 1996.

[Gir05] A. Girard. Reachability of uncertain linear systems using zonotopes. In *Hybrid Systems: Computation and Control*, volume 3414 of *Lecture Notes in Computer Science*, pages 291–305. Springer, 2005.

[GP05a] A. Girard and G. J. Pappas. Approximate bisimulations for constrained linear systems. submitted, February 2005.

[GP05b] A. Girard and G. J. Pappas. Approximate bisimulations for nonlinear dynamical systems. submitted, February 2005.

[HK04] Z. Han and B. H. Krogh. Reachability of hybrid control systems using reduced-order models. In *Proceedings of the American Control Conference*, Boston, MA, July 2004.

[HTP05] E. Haghverdi, P. Tabuada, and G. J. Pappas. Bisimulation relations for dynamical, control, and hybrid systems. *Theoretical Computer Science*, 2005. In press.

[JvdS04] A.A. Julius and A.J. van der Schaft. A behavioral framework for compositionality: linear systems, discrete event systems and hybrid systems. In *Proceedings of the Sixteenth International Symposium on Mathematical Theory of Networks and Systems*, Leuven, Belgium, July 2004.

[KS90] P.C. Kanellakis and S.A. Smolka. CCS expressions, finite-state processes, and three problems of equivalence. *Information and Computation*, 86:43–68, 1990.

[KV00] A. Kurzhanski and P. Varaiya. Ellipsoidal tehcniques for reachability analysis. In *Hybrid Systems: Computation and Control*, volume 1790 of *LNCS*. Springer, 2000.

[Mil89] R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

[MT00] I. Mitchell and C. Tomlin. Level set methods for computation in hybrid systems. In *Hybrid Systems: Computation and Control*, volume 1790 of *LNCS*. Springer, 2000.

[Pap03] G. J. Pappas. Bisimilar linear systems. *Automatica*, 39(12):2035–2047, December 2003.

[PHW03] A. Di Pierro, C. Hankin, and H. Wiklicky. Quantitative relations and approximate process equivalences. In *CONCUR 2003*, volume 2761 of *LNCS*, pages 508–522. Springer, 2003.

[PJ04] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems: Computation and Control*, volume 2993 of *Lecture Notes in Computer Science*, pages 477 – 492. Springer, 2004.

[PvdSB04] G. Pola, A.J. van der Schaft, and M. D. Di Benedetto. Bisimulation theory for switching linear systems. In *Proceedings of the 43rd IEEE Conference on Decision and Control*, pages 555–569, Nassau, Bahamas, December 2004.

[TK02] A. Tiwari and G. Khanna. Series of abstractions for hybrid automata. In *Hybrid Systems: Computation and Control*, volume 2289 of *LNCS*, pages 465–478. Springer, 2002.

[TP04] P. Tabuada and G. J. Pappas. Bisimilar control affine systems. *Systems and Control Letters*, 52:49–58, 2004.

[vBMOW03] F. van Breugel, M. Mislove, J. Ouaknine, and J. Worrell. An intrinsic characterization of approximate probabilistic bisimilarity. In *Foundations of Software Science and Computation Structures*, volume 2620 of *LNCS*, pages 200–215. Springer, 2003.

[vdS04] A. van der Schaft. Equivalence of dynamical systems by bisimulation. *IEEE Transactions on Automatic Control*, 49(12):2160–2172, December 2004.

[Wei05] E. W. Weisstein et al. Locally compact. *From MathWorld–A Wolfram Web Resource*, 2005.

Appendix

Set Valued Continuity. Following [Aub91] , the set valued map Post^σ is called:

- upper semicontinuous at $q \in Q$ if for any neighborhood V of $\mathrm{Post}^\sigma(q)$,

$$\exists \eta > 0 \text{ such that } \forall q' \in Q,\ d_Q(q, q') \leq \eta \implies \mathrm{Post}^\sigma(q') \subset V.$$

- lower semicontinuous at $q \in \mathrm{Supp}(\mathrm{Post}^\sigma)$ if for any $q' \in \mathrm{Post}^\sigma(q)$ and for any sequence of elements $q_n \in \mathrm{Supp}(\mathrm{Post}^\sigma)$ converging to q, there exists a sequence of elements $q'_n \in \mathrm{Post}^\sigma(q_n)$ converging to q'.
- continuous at $q \in \mathrm{Supp}(\mathrm{Post}^\sigma)$ if it is both upper semicontinuous and lower semicontinuous at q. If Post^σ is continuous at all $q \in \mathrm{Supp}(\mathrm{Post}^\sigma)$ then we say that it is continuous.

Metrics, Hausdorff distance.

Definition 9.1 (Metric)**.** A metric on a set E is a positive function $d : E \times E \to \mathbb{R} \cup \{+\infty\}$, such that the three following properties hold:

(1) for all $e_1 \in E$, $e_2 \in E$, $e_3 \in E$, $d(e_1, e_3) \leq d(e_1, e_2) + d(e_2, e_3)$,
(2) for all $e_1 \in E$, $e_2 \in E$, $d(e_1, e_2) = 0 \iff e_1 = e_2$,
(3) for all $e_1 \in E$, $e_2 \in E$, $d(e_1, e_2) = d(e_2, e_1)$.

We say that (E, d) is a metric space. If the second property is replaced by $e_1 = e_2 \implies d(e_1, e_2) = 0$ then d is called a pseudo-metric. If the third property is dropped, then d is called a directed metric.

A metric on a set E induces a natural metric on the set of subsets of E known as the Hausdorff distance (see *e.g.* [Ewa96]).

Definition 9.2 (Hausdorff distance)**.** Let E_1 and E_2 be two subsets of E. The directed Hausdorff distance associated to the metric d is defined by

$$h^{\rightarrow}(E_1, E_2) = \sup_{e_1 \in E_1} \inf_{e_2 \in E_2} d(e_1, e_2).$$

The Hausdorff distance associated to the metric d is then

$$h(E_1, E_2) = \max\left(h^{\rightarrow}(E_1, E_2), h^{\rightarrow}(E_2, E_1)\right).$$

We have the following classical theorem.

Theorem 9.3. *The (directed) Hausdorff distance is a (directed) pseudo-metric on the set of subsets of E and*

$$h^{\rightarrow}(E_1, E_2) = 0 \quad \textit{if and only if} \quad cl(E_1) \subseteq cl(E_2)$$
$$h(E_1, E_2) = 0 \quad \textit{if and only if} \quad cl(E_1) = cl(E_2)$$

where $cl(E_i)$ denotes the closure of the set E_i.

Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104

E-mail address: agirard@seas.upenn.edu

Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104

E-mail address: pappasg@ee.upenn.edu