Least-violating symbolic controller synthesis for safety, reachability and attractivity specifications

Antoine Girard, Alina Eqtami

LEAST-VIOLATING SYMBOLIC CONTROLLER SYNTHESIS FOR SAFETY, REACHABILITY AND ATTRACTIVITY SPECIFICATIONS

A. GIRARD AND A. EQTAMI

Abstract. Specifications considered in symbolic control are often interpreted qualitatively and controllers are usually classified as correct if they enforce the specification or as incorrect if they do not. In practice, a given ideal specification might be impossible to meet. In that case, it is interesting for the system designer to be able to quantify the distance between achievable behaviors and the specification, and to synthesize the least-violating controller enforcing the closed-loop behavior that is the closest to a correct one. In this paper, we develop such an approach for three types of specifications: safety, uniform reachability and uniform attractivity. We define controllability measures associated to these properties. For finite transition systems, we present dynamic programming algorithms for the computation of these measures and of the associated least-violating controllers. We discuss how these results can be used to synthesize controllers for infinite transition systems via symbolic control techniques. To demonstrate the relevance of our approach, we show an application to adaptive cruise control.

1. Introduction

Symbolic or abstraction-based control is a computational approach to controller synthesis for general nonlinear systems with state and input constraints, where the continuous dynamics of the system is approximated using a finite-state dynamical system called finite or symbolic abstraction (see e.g. [36, 4]). The main advantage of using symbolic abstractions is that it makes it possible to use algorithmic techniques for the automatic synthesis of controllers to enforce various types of specifications such as safety and reachability [14], specifications described by other dynamical systems [36], by finite-state automata [26], or by linear temporal logic formulas [4]. When the dynamics of the system and of its abstraction are related by some formal behavioral relationship such as alternating simulation relations [36] or feedback refinement relations [31], then a controller for the original system can be obtained from that synthesized for the abstraction. In this case, this controller is said to be "correct by design" since the specification is guaranteed to hold for the original system.

The specifications considered in symbolic control are often interpreted qualitatively in the sense that a controller is classified as correct if it enforces the specification or as incorrect if it does not. However, in practice, a given ideal specification might be impossible to enforce. In that case, the system designer would be interested in quantifying the distance between achievable behaviors and the specification, and in synthesizing the least-violating controller enforcing the closed-loop behavior that is the closest to a correct one. Indeed, the system designer may decide that the distance to the ideal specification is after all acceptable. For specifications given under the form of a dynamical system or of a linear temporal logic formula, this could be formulated as finding the controller that minimizes the behavioral distance between the system and the specification [15], or that maximizes the robustness of the satisfaction of the temporal logic formula as measured by a quantitative semantics (see e.g. [13, 11]).

In this paper, we develop such an approach for three common types of specifications: safety, uniform reachability and uniform attractivity. The main contributions of the paper are as follows. Firstly, we first define

*This research was partially supported by Labex DigiCosme (project ANR-11-LABEX-0045-DIGICOSME) operated by ANR as part of the program "Investissement d'Avenir" Idex Paris-Saclay (ANR-11-IDEX-0003-02). This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 725144).

controllability measures associated to these properties: evaluated at a given initial state, these measures quantify how close to correct behaviors the system can be controlled. Secondly, we show for finite-state systems that these controllability measures can be computed using dynamic programming and we provide explicit construction of associated least-violating controllers. Thirdly, we discuss how to lift these results to infinite-state systems using abstraction-based techniques relying on alternating simulation relations or feedback refinement relations. Finally, we show the relevance of the studied problem by applying it to a numerical case study inspired by adaptive cruise control in autonomous vehicles.

The notion of least-violating controller has been introduced in [38] for safety properties where the synthesized controller seeks to minimize the time spent outside the safe set. In comparison, in the current work, the least-violating controller aims at minimizing over all time the distance to a correct trajectory, similar to the approach presented in [33] where such objectives are considered for temporal logic specifications, though only on bounded time-horizons and for linear systems. Quantitative approaches to controller synthesis can also be related to robustness, see e.g. [37, 8, 24]. In [37], the synthesis of robust controllers is considered where one of the robustness requirement is that the deviation from the correct behavior should be proportional to the amplitude of disturbances. The problem considered in the current paper for safety specifications can actually be recasted in the framework of [37]. However, the proposed solutions for controller synthesis follow slightly different approaches. Synthesis of robust controllers is also considered in [8, 24] for safety and general omega-regular specifications where the robustness requirement is to maximize the number of disturbance introductions required to violate the specification. While also based on quantitative synthesis and dynamic programming, this work appears to address objectives and to use formulations that are different from ours.

While classical dynamic programming theory [6, 5] often deals with cumulative costs, discounted or not, on bounded or unbounded time-horizons, the problems formulated in this paper have non-cumulative costs and aim at minimizing minimum or maximum costs over unbounded time-horizons. However, such costs have already been considered in the literature, e.g. in [3, 10, 29, 18, 1], sometimes in relations with safety [20] or reachability [19, 23] specifications. These works deal with systems described by differential equations and mostly focus on the bounded time-horizon case, since the work on unbounded horizons [10] is based on bounded horizon relaxations. In comparison, in the current work, we consider unbounded horizon problems and dynamic programming is applied to discrete-time, finite-state transition systems, which make it possible to consider potentially blocking, non-deterministic and discontinuous infinite-state behaviors, through symbolic control techniques. Symbolic control has been used to tackle a number of optimal control problems involving either cumulative costs such as minimal-time [21, 14], entry-time problems [9], finite [22] or infinite [17] horizon problems, or average costs [32]. The research that is the most closely related to the present work are [7] and [30, 39]. In [7], the authors study dynamic programming formulations that are similar to those characterizing safety and uniform reachability controllability measures. However, in this work, the characterization of the level sets of the value function in terms of controllability measures is not established, and the synthesis of controllers is not discussed. In [30] and [39], the authors study a large class of optimal control problems, which can capture our dynamic programming formulation to synthesize least-violating controllers for uniform reachability, but not for safety. Finally, uniform attractivity specifications are not covered by these papers.

Some of the results on safety specifications have been presented in preliminary form in the conference paper [12]. The present paper gives a deeply reworked presentation of these results and provides characterization of the value function in terms of the controllability measure, which was not introduced in this work. Moreover, the results related to uniform reachability and uniform attractivity, and the application to adaptive cruise control are new. Finally, while the focus of the paper is on the synthesis of least-violating controllers, it is straightforward to adapt the approach to synthesize maximally satisfying controllers, which aim, when a specification can be met, at maximizing over all time the distance to incorrect trajectories.

The remainder of the paper is organized as follows. Section 2 introduces preliminary definitions and defines controllability measures for safety, uniform reachability and uniform attractivity specifications. Section 3 provides algorithms based on dynamic programming for the computation of these measures and for the synthesis of the associated least-violating controllers, for finite transition systems. In Section 4, we lift these results to

infinite transition systems using symbolic control techniques. Finally, Section 5 shows an application of our framework to adaptive cruise control.

2. Preliminaries

In this section, after defining some notations, we introduce the classes of systems and of controllers considered in the paper. Then, we present the three types of specifications under study (safety, uniform reachability and uniform attractivity) and define the associated controllability measures.

Notations: $\mathbb{R}$, $\mathbb{R}_0^+$ and $\mathbb{N}$ denote the sets of real, nonnegative real and natural numbers, respectively. For $K \in \mathbb{N} \cup \{+\infty\}$, we define the following sets of integers $\mathbb{N}_{<K} = \{k \in \mathbb{N} |\ k < K\}$ and $\mathbb{N}_{\leq K} = \{k \in \mathbb{N} |\ k \leq K\}$. The lexicographic order over $\mathbb{R}^2$ is defined by $(v_1, v_2) \leq_{lex} (w_1, w_2)$ if and only if $v_1 < w_1$, or $v_1 = w_1$ and $v_2 \leq w_2$. If $(v_1, v_2) \leq_{lex} (w_1, w_2)$ and $(v_1, v_2) \neq (w_1, w_2)$, then we denote $(v_1, v_2) <_{lex} (w_1, w_2)$. $\overline{\mathbb{R}}$ denotes the set of extended real numbers, i.e. $\overline{\mathbb{R}} = [-\infty, +\infty]$. For an extended real-valued function $V : X \to \overline{\mathbb{R}}$, the lower level sets of function V are defined as $L_\delta(V) = \{x \in X |\ V(x) \leq \delta\}$ where $\delta \in \overline{\mathbb{R}}$. A relation $R \subseteq X \times Y$ is identified with the set-valued map $R : X \rightrightarrows Y$ where $R(x) = \{y \in Y |\ (x, y) \in R\}$. The domain of R is $\mathrm{dom}(R) = \{x \in X |\ R(x) \neq \emptyset\}$. The inverse relation of R is $R^{-1} = \{(y, x) \in Y \times X |\ (x, y) \in R\}$. Given $X' \subseteq X$, we have $R(X') = \bigcup_{x \in X'} R(x)$. Given two set-valued maps $R_1 : X \rightrightarrows Y$ and $R_2 : Y \rightrightarrows Z$, the set valued-map $R_2 \circ R_1 : X \rightrightarrows Z$ is given for all $x \in X$, by $R_2 \circ R_1(x) = R_2(R_1(x))$. Given a metric space (X, d), we define the ball centered at $x \in X$ of radius $\delta \in \mathbb{R}_0^+$ as $B(x, \delta) = \{x' \in X |\ d(x, x') \leq \delta\}$. Given a finite set X, $|X|$ denotes the number of elements of X.

2.1. Transition systems.

In this paper, we focus on the following class of transition systems [36]:

Definition 2.1. A *transition system* Σ is a tuple $\Sigma = (X, U, Y, F, H)$, consisting of a set of states X; a set of inputs U; a set of outputs Y; a transition relation $F : X \times U \rightrightarrows X$; and an output map $H : X \to Y$. Σ is *finite* if X and U are finite.

An input $u \in U$ is called *enabled* at $x \in X$ if $F(x, u) \neq \emptyset$. Let $\mathrm{enab}_F(x) \subseteq U$ denote the set of all inputs enabled at x. If $\mathrm{enab}_F(x) = \emptyset$, then the state x is called *blocking*, otherwise it is non-blocking. The set of non-blocking states is denoted nbs_F. Σ is said to be *deterministic*, if for all $x \in X$, for all $u \in \mathrm{enab}_F(x)$, $F(x, u)$ is a singleton.

Within the framework of transition systems, we can define (memoryless state-feedback) controllers as follows:

Definition 2.2. A *controller* for system Σ is a set-valued map $C : X \rightrightarrows U$ such that $C(x) \subseteq \mathrm{enab}_F(x)$, for all $x \in X$.

Closed-loop trajectories are then defined as follows:

Definition 2.3. A sequence $(x_t)_{t=0}^T$, where $T \in \mathbb{N} \cup \{+\infty\}$, $x_t \in X$, for $t \in \mathbb{N}_{\leq T}$, is called a *closed-loop trajectory* of system Σ with controller C if and only if

$$\forall t \in \mathbb{N}_{<T},\ x_{t+1} \in F(x_t, C(x_t)).$$

A trajectory is called *maximal* if either $T = +\infty$ or $C(x_T) = \emptyset$, it is *complete* if $T = +\infty$. The set of maximal closed-loop trajectories starting from a given initial state $x_0 \in X$ is denoted by $\mathcal{T}_{\max}(\Sigma, C, x_0)$.

2.2. Specifications.

Consider a system $\Sigma = (X, U, Y, F, H)$ and a subset of states $X^* \subseteq X$. In the following, we define three basic types of specifications: safety, uniform reachability and uniform attractivity.

Definition 2.4. A state $x_0 \in X$ is *safety controllable* to X^*, if there exists a controller C such that all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy $x_t \in X^*$, for all $t \in \mathbb{N}$. The set of safety controllable states is denoted by $\text{S-cont}(\Sigma, X^*)$.

Intuitively, a state is safety controllable if all maximal closed-loop trajectories initiating from that state stay in X^* forever.

Definition 2.5. A state $x_0 \in X$ is *uniform reachability controllable* to X^*, if there exist a controller C and $T_0 \in \mathbb{N}$, such that for all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$, there exists $t \in \mathbb{N}_{\leq \min(T,T_0)}$, such that $x_t \in X^*$. The set of uniform reachability controllable states is denoted by R-cont(Σ, X^*).

Essentially, a state is reachability controllable if all maximal closed-loop trajectories initiating from that state reach X^* in finite time. The term "uniform" refers to the fact that the time to reach X^* is uniformly bounded by T_0, which depends on the initial state x_0 but not on the trajectory. It is easy to show that reachability and uniform reachability coincides for deterministic systems and for finite systems. The following example illustrates this notion of uniformity.

Example 2.6. Consider a transition system $\Sigma = (X, U, Y, F, H)$ where $X = \mathbb{N}$, $U = \{0\}$ and F is given by $F(0,0) = \{x \in \mathbb{N} |\ x \geq 1\}$ and $F(x,0) = \{x-1\}$ for all $x \geq 1$. The value of Y and H is not relevant for the subsequent discussion. A pictural representation of Σ is shown in Figure 1. Let us remark that Σ is not deterministic nor finite. Let us consider the controller C given by $C(x) = \{0\}$, for all $x \in \mathbb{N}$. Finally, let $X^* = \{1\}$ and $x_0 = 0$. For all $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$, it is clear that $x_t \in X^*$ for the first time at time $t = x_1$ so all closed-loop trajectories initiating in x_0 reach X^* in finite time. However, this time cannot be uniformly bounded since $x_1 \in \{x \in \mathbb{N} |\ x \geq 1\}$, which is an unbounded set. $\diamond$

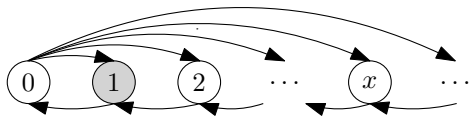

FIGURE 1. Illustration of Example 2.6: all trajectories starting in 0 reach 1 at some finite time. However this time cannot be uniformly bounded.

Definition 2.7. A state $x_0 \in X$ is *uniform attractivity controllable* to X^*, if there exist a controller C and $T_0 \in \mathbb{N}$, such that all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy $x_t \in X^*$, for all $t \geq T_0$. The set of uniform attractivity controllable states is denoted by A-cont(Σ, X^*).

Essentially, a state is attractivity controllable if all maximal closed-loop trajectories initiating from that state eventually reach X^* and stay therein forever. Again, the term "uniform" refers to the fact that the time after which trajectories do not leave X^* is uniformly bounded by T_0, which depends on the initial state x_0 but not on the trajectory. It is straightforward to show that attractivity and uniform attractivity coincides for deterministic systems. We provide the following example to illustrate the notion of uniform attractivity.

Example 2.8. Consider a transition system $\Sigma = (X, U, Y, F, H)$ where $X = \{0,1,2\}$, $U = \{0\}$ and F is given by $F(0,0) = \{0\}$, $F(1,0) = \{1,2\}$, $F(2,0) = \{0\}$. The value of Y and H is not relevant for the subsequent discussion. A pictural representation of Σ is shown in Figure 2. Let us remark that Σ is not deterministic. Let us consider the controller C given by $C(x) = \{0\}$, for all $x \in \{1,2,3\}$. Finally, let $X^* = \{0,1\}$ and $x_0 = 1$. Let $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$, we have either $x_t = 1$, for all $t \in \mathbb{N}$ or there exists $T_0 \in \mathbb{N}$, $T_0 \geq 2$ such that $x_t = 1$ for all $t \in \mathbb{N}_{\leq T_0 - 2}$, $x_{T_0-1} = 2$ and $x_t = 0$, for all $t \geq T_0$. So, all maximal closed-loop trajectories initiating from 1 do not leave X^* after some finite time T_0. However, this time cannot be uniformly bounded and depends on the trajectory. More precisely, it depends on the instant when the non-deterministic transition from state 1 to state 2 occurs, if such transition occurs. Let us remark, that this example shows that, unlike for reachability, even for finite transition systems there is a fundamental difference between attractivity and uniform attractivity. $\diamond$

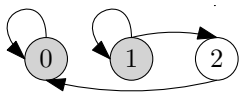

FIGURE 2. Illustration of Example 2.8: all trajectories starting in 1 stay in $\{0,1\}$ after some finite time. However this time cannot be uniformly bounded.

Remark 2.9. A comparison with some specifications written in Linear Temporal Logic [2] (LTL) is in order. The notion of safety provided in Definition 2.4 corresponds to the LTL formula $\Box X^*$. However, the uniformity requirement for reachability and attractivity in Definitions 2.5 and 2.7 make them semantically different from, and actually stronger than the LTL formulas $\Diamond X^*$ and $\Diamond\Box X^*$. In fact, the uniformity requirement cannot be expressed in LTL, since LTL formulas are evaluated on single trajectories while the uniformity requirement refers to the set of trajectories $\mathcal{T}_{\max}(\Sigma, C, x_0)$.

We now show the following relation between the three notions defined above:

Proposition 2.10. *The following equality holds:* $\text{A-cont}(\Sigma, X^*) = \text{R-cont}(\Sigma, \text{S-cont}(\Sigma, X^*))$.

Proof. Let $x_0 \in \text{A-cont}(\Sigma, X^*)$, then there exist a controller C and $T_0 \in \mathbb{N}$, such that all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy $x_{T_0} \in \text{S-cont}(\Sigma, X^*)$. Hence, $x_0 \in \text{R-cont}(\Sigma, \text{S-cont}(\Sigma, X^*))$. Now, let $x_0 \in \text{R-cont}(\Sigma, \text{S-cont}(\Sigma, X^*))$, there exist a controller C_{R} and $T_0 \in \mathbb{N}$, such that for all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C_{\text{R}}, x_0)$, there exists $t \in \mathbb{N}_{\leq \min(T, T_0)}$, such that $x_t \in \text{S-cont}(\Sigma, X^*)$. For all $x \in \text{S-cont}(\Sigma, X^*)$, there exists a controller C_{S}^x such that all trajectories in $\mathcal{T}_{\max}(\Sigma, C_{\text{S}}^x, x)$ are complete and stay in X^* forever. Let us consider the controller C defined as follows

$$C(x) = \begin{cases} C_{\text{R}}(x) & \text{if } x \notin \text{S-cont}(\Sigma, X^*); \\ C_{\text{S}}^x(x) & \text{if } x \in \text{S-cont}(\Sigma, X^*) \end{cases}$$

Then, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy $x_t \in X^*$ for all $t \geq T_0$. Hence, $x_0 \in \text{A-cont}(\Sigma, X^*)$. □ □

2.3. **Controllability measures.** From now on, let us assume that the output set $Y = \overline{\mathbb{R}}$ and $H : X \to Y$ is given by

$$H(x) = \inf\{\delta \in \mathbb{R}_0^+ |\ B(x, \delta) \cap X^* \neq \emptyset\} \tag{2.1}$$

where (X, d) is a metric space. Essentially, $H(x)$ represents the distance of state x to the set X^*. Then, for $\delta \in \mathbb{R}$, let us consider the lower level-sets $X_\delta^* = L_\delta(H)$. We can then define quantitative measures of controllability for a state $x \in X$ as follows:

Definition 2.11. The *safety, uniform reachability, uniform attractivity controllability measures* of a state $x \in X$ are respectively defined as

$$V_{\text{S}}(x) = \inf\{\delta \in \mathbb{R} |\ x \in \text{S-cont}(\Sigma, X_\delta^*)\} \tag{2.2}$$

$$V_{\text{R}}(x) = \inf\{\delta \in \mathbb{R} |\ x \in \text{R-cont}(\Sigma, X_\delta^*)\} \tag{2.3}$$

$$V_{\text{A}}(x) = \inf\{\delta \in \mathbb{R} |\ x \in \text{A-cont}(\Sigma, X_\delta^*)\} \tag{2.4}$$

A simple intuitive explanation of the controllability measures can be given for finite transition systems as follows. For safety specifications, if $V_{\text{S}}(x) = 0$ then $x \in \text{S-cont}(\Sigma, X^*)$. If $V_{\text{S}}(x) > 0$ then $x \notin \text{S-cont}(\Sigma, X^*)$, nonetheless there exists a least-violating controller which keeps the closed loop-trajectories initiating from x less than $V_{\text{S}}(x)$ away from X^*. Similarly, for reachability specifications, if $V_{\text{R}}(x) = 0$ then $x \in \text{R-cont}(\Sigma, X^*)$, if $V_{\text{R}}(x) > 0$ then $x \notin \text{R-cont}(\Sigma, X^*)$, nonetheless there exists a least-violating controller which drives the closed loop-trajectories initiating from x less than $V_{\text{R}}(x)$ away from X^*. Finally, for attractivity specifications, if

$V_{\mathrm{A}}(x) = 0$ then $x \in \text{A-cont}(\Sigma, X^*)$, if $V_{\mathrm{A}}(x) > 0$ then $x \notin \text{A-cont}(\Sigma, X^*)$, nonetheless there exists a least-violating controller which eventually keeps the closed loop-trajectories initiating from x less than $V_{\mathrm{A}}(x)$ away from X^*.

In the following, we consider the problem of computing these controllability measures and of synthesizing least-violating controllers achieving these fundamental limits. These are of particular interest to the system designer when a given "ideal" specification cannot be met. Indeed, in that case the controllability measure provides the information on how close we can get to the specification. The designer may then decide that this deviation is acceptable and use the associated least-violating controller. Such a situation will be shown in Section 5 on a numerical example inspired by adaptive cruise control in autonomous vehicles. Before that, we develop approaches in Section 3, to compute these controllability measures for finite transition systems based on dynamic programming. In Section 4, we lift these methods to compute approximate solutions for infinite transition systems, using finite state abstractions.

Remark 2.12. The paper focuses on the synthesis of least-violating controllers that correspond to H given by (2.1). However, all the results can be adapted to other choices for H. In particular, by considering the signed distance to the set X^*, given by

$$H(x) = \begin{cases} -\sup\{\delta \in \mathbb{R}_0^+ |\ B(x,\delta) \subseteq X^*\} & \text{if } x \in X^*; \\ \inf\{\delta \in \mathbb{R}_0^+ |\ B(x,\delta) \cap X^* \neq \emptyset\} & \text{otherwise} \end{cases}$$

the synthesized controller is at the same time least-violating at uncontrollable states and maximally satisfying at controllable states, in the sense that it maximizes the distance to incorrect behaviors.

3. A dynamic programming approach for finite systems

In this section, we consider a finite transition system Σ and provide fixed-point characterizations of the safety, uniform reachability and uniform attractivity controllability measures. We also give explicit constructions of the least-violating controllers.

3.1. Safety specifications.

Let us consider the following dynamic programming fixed-point iteration:

$$\begin{aligned} W_{\mathrm{S}}^0(x) &= H(x) \\ W_{\mathrm{S}}^{k+1}(x) &= \begin{cases} \max\Big(H(x), \min\limits_{u \in \mathrm{enab}_F(x)} \max\limits_{x^+ \in F(x,u)} W_{\mathrm{S}}^k(x^+)\Big) & \\ & \text{if } x \in \mathrm{nbs}_F; \\ +\infty & \text{if } x \notin \mathrm{nbs}_F \end{cases} \end{aligned} \tag{3.1}$$

(3.2)

for $x \in X$, $k \in \mathbb{N}$.

Proposition 3.1. *For a finite transition system Σ, there exists $K \in \mathbb{N}_{<|X|\times(|H(X)|+1)}$ such that for all $k \geq K$, $W_{\mathrm{S}}^k(x) = W_{\mathrm{S}}^K(x)$, for all $x \in X$.*

Proof. First, we are going to prove that for all $x \in X$, the sequence $(W_{\mathrm{S}}^k(x))_{k\in\mathbb{N}}$ is nondecreasing. This is obviously the case if $x \notin \mathrm{nbs}_F$. When $x \in \mathrm{nbs}_F$, we have the following

$$\begin{aligned} W_{\mathrm{S}}^1(x) &= \max\Big(H(x), \min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{S}}^0(x^+)\Big) \\ &\geq H(x) = W_{\mathrm{S}}^0(x) \end{aligned}$$

Assume now, that for some $k \geq 1$, $W_{\mathrm{S}}^k(x) \geq W_{\mathrm{S}}^{k-1}(x)$ for all $x \in X$. Then, for all $x \in \mathrm{nbs}_F$,

$$\begin{aligned} W_{\mathrm{S}}^{k+1}(x) &= \max\Big(H(x), \min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{S}}^k(x^+)\Big) \\ &\geq \max\Big(H(x), \min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{S}}^{k-1}(x^+)\Big) \\ &= W_{\mathrm{S}}^k(x) \end{aligned}$$

Note that for all $x \notin \mathrm{nbs}_F$, we also have $W_{\mathrm{S}}^{k+1}(x) \geq W_{\mathrm{S}}^k(x)$. Thus, by induction, it follows that for all $k \in \mathbb{N}$, for all $x \in X$, we have $W_{\mathrm{S}}^{k+1}(x) \geq W_{\mathrm{S}}^k(x)$, i.e. the sequence $(W_{\mathrm{S}}^k(x))_{k\in\mathbb{N}}$ is nondecreasing.

To show that the fixed point is reached in a finite number of steps, let us remark that for all $x \in X$, for all $k \in \mathbb{N}$, $W_{\mathrm{S}}^k(x) \in H(X) \cup \{+\infty\}$, which is finite from the finiteness of X. Together with the fact that for all $x \in X$, the sequence $(W_{\mathrm{S}}^k(x))_{k\in\mathbb{N}}$ is nondecreasing, this shows that there exists $K \in \mathbb{N}_{<|X|\times(|H(X)|+1)}$, such that for all $k \geq K$, for all $x \in X$, $W_{\mathrm{S}}^k(x) = W_{\mathrm{S}}^K(x)$. □ □

We denote the fixed-point of (3.1), (3.2) by $W_{\mathrm{S}}^\star$. It follows from Proposition 3.1 and (3.2) that for all $x \in \mathrm{nbs}_F$,

$$W_{\mathrm{S}}^\star(x) = \max\Big(H(x), \min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{S}}^\star(x^+)\Big). \tag{3.3}$$

We define the following controller for Σ:

$$C_{\mathrm{S}}^\star(x) = \begin{cases} \arg\min_{u \in \mathrm{enab}_F(x)} \Big(\max_{x^+ \in F(x,u)} W_{\mathrm{S}}^\star(x^+)\Big) & \\ \qquad\qquad\qquad\qquad \text{if } x \in \mathrm{nbs}_F; \\ \emptyset \qquad\qquad\qquad\qquad \text{if } x \notin \mathrm{nbs}_F \end{cases} \tag{3.4}$$

Theorem 3.2. *Let Σ be a finite transition system, let $W_{\mathrm{S}}^\star$ be the fixed-point of (3.1), (3.2) and let $C_{\mathrm{S}}^\star$ be given by (3.4). Then, for all $\delta \in \mathbb{R}$, for all $x_0 \in L_\delta(W_{\mathrm{S}}^\star)$, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{S}}^\star, x_0)$ are complete and satisfy $x_t \in X_\delta^*$, for all $t \in \mathbb{N}$. Moreover, for all $\delta \in \mathbb{R}$, $L_\delta(W_{\mathrm{S}}^\star) = \text{S-cont}(\Sigma, X_\delta^*)$.*

Proof. Let $\delta \in \mathbb{R}$, $x_0 \in L_\delta(W_{\mathrm{S}}^\star)$ and $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{S}}^\star, x_0)$. By (3.3), we get $W_{\mathrm{S}}^\star(x) \geq H(x)$ for all $x \in X$, then $L_\delta(W_{\mathrm{S}}^\star) \subseteq L_\delta(H) = X_\delta^*$. By (3.3) and (3.4), we get for all $t \in \mathbb{N}_{<T}$, $W_{\mathrm{S}}^\star(x_{t+1}) \leq W_{\mathrm{S}}^\star(x_t)$. Hence, since $x_0 \in L_\delta(W_{\mathrm{S}}^\star)$, we get for all $t \in \mathbb{N}_{\leq T}$, $x_t \in L_\delta(W_{\mathrm{S}}^\star) \subseteq X_\delta^*$. Let us assume that $T < +\infty$, then by maximality $C_{\mathrm{S}}^\star(x_T) = \emptyset$, which from (3.4) means that $x_T \notin \mathrm{nbs}_F$. From (3.2), we get that $W_{\mathrm{S}}^\star(x_T) = +\infty$, which contradicts the fact that $x_T \in L_\delta(W_{\mathrm{S}}^\star)$ with $\delta \in \mathbb{R}$. Hence, $T = +\infty$, and the trajectory $(x_t)_{t=0}^T$ is complete.

From above, it follows directly that $L_\delta(W_{\mathrm{S}}^\star) \subseteq \text{S-cont}(\Sigma, X_\delta^*)$. We now prove the reverse inclusion. Let $\delta \in \mathbb{R}$, from Definition 2.4, $\text{S-cont}(\Sigma, X_\delta^*) \subseteq X_\delta^*$ and therefore, for all $x \in \text{S-cont}(\Sigma, X_\delta^*)$, $H(x) \leq \delta$. Let us assume that for some $k \in \mathbb{N}$, we have for all $x \in \text{S-cont}(\Sigma, X_\delta^*)$, $W_{\mathrm{S}}^k(x) \leq \delta$. Note that this is true for $k = 0$. Let $x \in \text{S-cont}(\Sigma, X_\delta^*)$, from Definition 2.4, it follows that $x \in \mathrm{nbs}_F$ and that there exists $\tilde{u} \in \mathrm{enab}_F(x)$ such that $F(x, \tilde{u}) \subseteq \text{S-cont}(\Sigma, X_\delta^*)$. Hence, for all $x^+ \in F(x, \tilde{u})$, $W_{\mathrm{S}}^k(x^+) \leq \delta$. It follows that

$$\min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{S}}^k(x^+) \leq \max_{x^+ \in F(x,\tilde{u})} W_{\mathrm{S}}^k(x^+) \leq \delta.$$

This, together with $H(x) \leq \delta$ and (3.2), implies that $W_{\mathrm{S}}^{k+1}(x) \leq \delta$. Hence, by induction, we get that for all $k \in \mathbb{N}$, for all $x \in \text{S-cont}(\Sigma, X_\delta^*)$, $W_{\mathrm{S}}^k(x) \leq \delta$. Thus by Proposition 3.1, it follows that for all $x \in \text{S-cont}(\Sigma, X_\delta^*)$, $W_{\mathrm{S}}^\star(x) \leq \delta$. Then, $\text{S-cont}(\Sigma, X_\delta^*) \subseteq L_\delta(W_{\mathrm{S}}^\star)$. □ □

We would like to highlight some features of our approach. Let us point out that by computing the fixed-point of (3.1), (3.2), one can compute the sets of safety controllable states for a family of specification sets X_δ^* parameterized by $\delta \in \mathbb{R}$. Moreover, it is interesting to remark that the proposed controller (3.4) is independent of the parameter δ and will automatically enforce the safety specification for the smallest possible value of the

parameter. For H given by (2.1), the distance to a safe set X^*, controller (3.4) is the least-violating controller, which keeps trajectories as close as possible to the safe set.

Corollary 3.3. *Let Σ be a finite transition system, let V_{S} be given by (2.2), and let $W_{\mathrm{S}}^\star$ be the fixed-point of (3.1), (3.2). Then, $V_{\mathrm{S}} = W_{\mathrm{S}}^\star$.*

Proof. If $W_{\mathrm{S}}^\star(x) = +\infty$, then from Theorem 3.2, for all $\delta \in \mathbb{R}$, $x \notin \text{S-cont}(\Sigma, X_\delta^*)$ and $V_{\mathrm{S}}(x) = +\infty$. If $W_{\mathrm{S}}^\star(x) < +\infty$, then let $\delta = W_{\mathrm{S}}^\star(x)$. From Theorem 3.2, it follows that $x \in \text{S-cont}(\Sigma, X_\delta^*)$. Therefore, $V_{\mathrm{S}}(x) \leq W_{\mathrm{S}}^\star(x)$.

If $V_{\mathrm{S}}(x) = +\infty$, then for all $\delta \in \mathbb{R}$, $x \notin \text{S-cont}(\Sigma, X_\delta^*)$ and from Theorem 3.2, $W_{\mathrm{S}}^\star(x) > \delta$. Hence $W_{\mathrm{S}}^\star(x) = +\infty$. If $V_{\mathrm{S}}(x) < +\infty$, then let $\delta > V_{\mathrm{S}}(x)$. Then, $x \in \text{S-cont}(\Sigma, X_\delta^*)$, which implies from Theorem 3.2 that $x \in L_\delta(W_{\mathrm{S}}^\star)$. Hence, $W_{\mathrm{S}}^\star(x) \leq \delta$ for all $\delta > V_{\mathrm{S}}(x)$. It follows that $W_{\mathrm{S}}^\star(x) \leq V_{\mathrm{S}}(x)$. □ □

3.2. **Reachability specifications.** Similar to safety, we consider the following dynamic programming fixed-point iteration:

$$W_{\mathrm{R}}^0(x) = H(x) \tag{3.5}$$

$$W_{\mathrm{R}}^{k+1}(x) = \begin{cases} \min\Big(H(x), \min\limits_{u \in \mathrm{enab}_F(x)} \max\limits_{x^+ \in F(x,u)} W_{\mathrm{R}}^k(x^+)\Big) & \\ & \text{if } x \in \mathrm{nbs}_F; \\ H(x) & \text{if } x \notin \mathrm{nbs}_F \end{cases} \tag{3.6}$$

for $x \in X$, $k \in \mathbb{N}$.

Remark 3.4. It is important to mention that the dynamic programming fixed point (3.5), (3.6) can be seen as a special case of the one considered in the work [30, 39]. Some of the results below can be obtained using results of [30]. However, we decided to include the proofs for self-containment of the paper and because these are instrumental for the case of uniform attractivity specifications considered in the next section. Interestingly, in [30, 39], efficient algorithms a la Dijkstra are presented for computing the fixed-point of (3.5), (3.6).

Proposition 3.5. *For a finite transition system Σ, there exists $K \in \mathbb{N}_{<|X|\times|H(X)|}$ such that for all $k \geq K$, $W_{\mathrm{R}}^k(x) = W_{\mathrm{R}}^K(x)$, for all $x \in X$.*

Proof. The proof follows the same lines as that of Proposition 3.1 with, in the present case the sequence $(W_{\mathrm{R}}^k(x))_{k\in\mathbb{N}}$ being non-increasing for all $x \in X$ with values in $H(X)$. □ □

We denote the fixed-point of (3.5), (3.6) by $W_{\mathrm{R}}^\star$. It follows from Proposition 3.5 and (3.6) that for all $x \in \mathrm{nbs}_F$,

$$W_{\mathrm{R}}^\star(x) = \min\Big(H(x), \min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{R}}^\star(x^+)\Big). \tag{3.7}$$

Let the function $k^\star : X \to \mathbb{N}$ be defined as follows for all $x \in X$

$$k^\star(x) = \min\{k \in \mathbb{N} |\ W_{\mathrm{R}}^k(x) = W_{\mathrm{R}}^\star(x)\}. \tag{3.8}$$

From Proposition 3.5, it follows that $k^\star$ is well-defined and that for all $x \in X$, $0 \leq k^\star(x) \leq K$. Moreover, it is clear that if $k^\star(x) \neq 0$, then $x \in \mathrm{nbs}_F$. From this observation, and by (3.6) and (3.8), we have that the following equation holds for all $x \in X$, such that $k^\star(x) \neq 0$:

$$W_{\mathrm{R}}^\star(x) = \min\Big(H(x), \min_{u \in \mathrm{enab}_F(x)} \max_{x^+ \in F(x,u)} W_{\mathrm{R}}^{k^\star(x)-1}(x^+)\Big). \tag{3.9}$$

We define the following controller for Σ:

$$C_{\mathrm{R}}^\star(x) = \begin{cases} \arg\min\limits_{u \in \mathrm{enab}_F(x)} \Big(\max\limits_{x^+ \in F(x,u)} W_{\mathrm{R}}^{k^\star(x)-1}(x^+)\Big) & \\ & \text{if } k^\star(x) \geq 1; \\ \emptyset & \text{if } k^\star(x) = 0 \end{cases} \tag{3.10}$$

We start with some preliminary result before stating the main results of the section.

Lemma 3.6. *For all $x_0 \in X$, for all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C^\star_{\mathrm{R}}, x_0)$, for all $t \in \mathbb{N}_{<T}$ it holds that $k^\star(x_t) \neq 0$ and $(W^\star_{\mathrm{R}}(x_{t+1}), k^\star(x_{t+1})) <_{lex} (W^\star_{\mathrm{R}}(x_t), k^\star(x_t))$.*

Proof. Let $t \in \mathbb{N}_{<T}$, then $C^\star_{\mathrm{R}}(x_t) \neq \emptyset$, which from (3.10) implies that $k^\star(x_t) \neq 0$. Then, by (3.8), $W^\star_{\mathrm{R}}(x_t) \neq H(x_t)$, and from (3.9), it follows that

$$W^\star_{\mathrm{R}}(x_t) = \min_{u \in \mathrm{enab}_F(x_t)} \max_{x^+ \in F(x_t,u)} W_{\mathrm{R}}^{k^\star(x_t)-1}(x^+)$$

Then by (3.10), we have $W^\star_{\mathrm{R}}(x_t) \geq W_{\mathrm{R}}^{k^\star(x_t)-1}(x_{t+1})$. Since the sequence $(W^k_{\mathrm{R}}(x_{t+1}))_{k\in\mathbb{N}}$ is non-increasing with its infimum given by $W^\star_{\mathrm{R}}(x_{t+1})$. We get that $W_{\mathrm{R}}^{k^\star(x_t)-1}(x_{t+1}) \geq W^\star_{\mathrm{R}}(x_{t+1})$ and therefore $W^\star_{\mathrm{R}}(x_t) \geq W^\star_{\mathrm{R}}(x_{t+1})$. Moreover, if $W^\star_{\mathrm{R}}(x_t) = W^\star_{\mathrm{R}}(x_{t+1})$, then we get $W_{\mathrm{R}}^{k^\star(x_t)-1}(x_{t+1}) = W^\star_{\mathrm{R}}(x_{t+1})$. Then by (3.8), we have $k^\star(x_{t+1}) \leq k^\star(x_t)-1$. Hence, either $W^\star_{\mathrm{R}}(x_{t+1}) < W^\star_{\mathrm{R}}(x_t)$, or $W^\star_{\mathrm{R}}(x_{t+1}) = W^\star_{\mathrm{R}}(x_t)$ and $k^\star(x_{t+1}) < k^\star(x_t)$. Therefore, $(W^\star_{\mathrm{R}}(x_{t+1}), k^\star(x_{t+1})) <_{lex} (W^\star_{\mathrm{R}}(x_t), k^\star(x_t))$. □ □

Theorem 3.7. *Let Σ be a finite transition system, let $W^\star_{\mathrm{R}}$ be the fixed-point of (3.5), (3.6), let $C^\star_{\mathrm{R}}$ be given by (3.10), and let $T_0 = |H(X)| \times (K+1) - 1$. Then, for all $\delta \in \mathbb{R}$, for all $x_0 \in L_\delta(W^\star_{\mathrm{R}})$, for all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C^\star_{\mathrm{R}}, x_0)$, $T \leq T_0$ and $x_T \in X^*_\delta$. Moreover, for all $\delta \in \mathbb{R}$, $L_\delta(W^\star_{\mathrm{R}}) = \text{R-cont}(\Sigma, X^*_\delta)$.*

Proof. Let $\delta \in \mathbb{R}$, $x_0 \in L_\delta(W^\star_{\mathrm{R}})$ and $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C^\star_{\mathrm{R}}, x_0)$. From Lemma 3.6, we get that the sequence $(W^\star_{\mathrm{R}}(x_t), k^\star(x_t))_{t\in\mathbb{N}_{\leq T}}$ is strictly decreasing for the lexicographic order. Moreover, for all $t \in \mathbb{N}_{\leq T}$, $(W^\star_{\mathrm{R}}(x_t), k^\star(x_t)) \in H(X) \times \mathbb{N}_{\leq K}$. It follows that T is bounded by T_0. By maximality of $(x_t)_{t=0}^T$, we have $C^\star_{\mathrm{R}}(x_T) = \emptyset$. From (3.10), this implies that $k^\star(x_T) = 0$ and (3.8) gives $W^\star_{\mathrm{R}}(x_T) = H(x_T)$. From Lemma 3.6, we also get that $W^\star_{\mathrm{R}}(x_T) \leq W^\star_{\mathrm{R}}(x_0) \leq \delta$. Hence, $x_T \in X^*_\delta$.

From above, it follows directly that $L_\delta(W^\star_{\mathrm{R}}) \subseteq \text{R-cont}(\Sigma, X^*_\delta)$. We now prove the reverse inclusion. We proceed by contradiction, let us assume that there exists $x_0 \in \text{R-cont}(\Sigma, X^*_\delta)$ such that $x_0 \notin L_\delta(W^\star_{\mathrm{R}})$. Then, $W^\star_{\mathrm{R}}(x_0) > \delta$. Let $C : X \rightrightarrows U$ be a controller as in Definition 2.5. Let us assume that for some $T \in \mathbb{N}$, there exists $(x_t)_{t=0}^T$, a closed-loop trajectory of system Σ with controller C, such that for all $t \in \mathbb{N}_{\leq T}$, $W^\star_{\mathrm{R}}(x_t) > \delta$. Note that this is true for $T = 0$. If $C(x_T) = \emptyset$, then the trajectory is maximal and from (3.9) we have for all $t \in \mathbb{N}_{\leq T}$, $H(x_t) \geq W^\star_{\mathrm{R}}(x_t) > \delta$, which contradicts the fact that $x_0 \in \text{R-cont}(\Sigma, X^*_\delta)$. If $C(x_T) \neq \emptyset$, then let $u_T \in C(X_T)$ and let

$$x_{T+1} = \arg \max_{x^+ \in F(x_T, u_T)} W^\star_{\mathrm{R}}(x^+).$$

Then by (3.7), we get

$$\begin{aligned} W^\star_{\mathrm{R}}(x_{T+1}) &\geq \min_{u \in \mathrm{enab}_F(x_T)} \max_{x^+ \in F(x_T,u)} W^\star_{\mathrm{R}}(x^+) \\ &\geq W^\star_{\mathrm{R}}(x_T) > \delta. \end{aligned}$$

Hence, we get by induction that there exists a closed-loop trajectory of system Σ with controller C, $(x_t)_{t=0}^T$ with $T = +\infty$ such that for all $t \in \mathbb{N}$, $W^\star_{\mathrm{R}}(x_t) > \delta$. Then from (3.9), we get for all $t \in \mathbb{N}$, $H(x_t) \geq W^\star_{\mathrm{R}}(x_t) > \delta$ which contradicts the fact that $x_0 \in \text{R-cont}(\Sigma, X^*_\delta)$. □ □

Similar to the case of safety specifications, computing the fixed-point of (3.5), (3.6) allows one to compute the sets of uniform reachability controllable states for the family of specification sets X^*_δ parameterized by $\delta \in \mathbb{R}$. Similarly, the proposed controller (3.10) is independent of the parameter δ and automatically enforces the reachability specification for the smallest possible value of the parameter. If H is the distance to a target set X^*, given by (2.1), controller (3.10) is the least-violating controller, which drives trajectories as close as possible to the target set. However, a significant difference with the case of safety specifications is that the controller (3.10) is not obtained from the fixed-point $W^\star_{\mathrm{R}}$ only, but from the iterates $(W^k_{\mathrm{R}})_{k\in\mathbb{N}}$. Actually, there are cases where the fixed-point $W^\star_{\mathrm{R}}$ carries no information on the way to reach the target as shown in the following example:

Example 3.8. Consider a transition system $\Sigma = (X, U, Y, F, H)$ where $X = \{0, 1, 2\}$, $U = \{0, 1\}$ and F is given by $F(0,0) = \{0\}$, $F(1,0) = \{0\}$, $F(1,1) = \{2\}$, $F(2,0) = \{1\}$, $Y = X$ and $H(x) = x$ for all $x \in X$. A pictural representation of Σ is shown in Figure 3. The fixed-point of (3.5), (3.6) in this case is flat and given by $W^\star_{\rm R}(x) = 0$, for all $x \in X$. In particular, it does not allow to decide that input $u = 0$ should be taken in $x = 1$ since the value of $W^\star_{\rm R}$ at the successor for all inputs is identical. $\diamond$

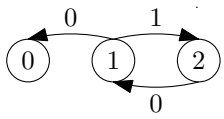

FIGURE 3. Illustration of Example 3.8: for $H(x) = x$ for all $x \in X$, the fixed-point of (3.5), (3.6) is flat, $W^\star_{\rm R}(x) = 0$, for all $x \in X$.

We can then state the following corollary whose proof is along the same lines as that of Corollary 3.3.

Corollary 3.9. *Let Σ be a finite transition system, let $V_{\rm R}$ be given by (2.3), and let $W^\star_{\rm R}$ be the fixed-point of (3.5), (3.6). Then, $V_{\rm R} = W^\star_{\rm R}$.*

3.3. **Attractivity specifications.** Let $W^\star_{\rm S}$ be the fixed-point of (3.1), (3.2) associated to safety specifications and consider the following dynamic programming fixed-point iteration:

$$W^0_{\rm A}(x) = W^\star_{\rm S}(x) \tag{3.11}$$

$$W^{k+1}_{\rm A}(x) = \begin{cases} \min\Big(W^\star_{\rm S}(x), \min\limits_{u \in {\rm enab}_F(x)} \max\limits_{x^+ \in F(x,u)} W^k_{\rm A}(x^+)\Big) & \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } x \in {\rm nbs}_F; & \\ W^\star_{\rm S}(x) \qquad\qquad\qquad\qquad \text{if } x \notin {\rm nbs}_F \end{cases} \tag{3.12}$$

for $x \in X$, $k \in \mathbb{N}$. Let us remark that (3.11) and (3.12) are similar to (3.5), (3.6) where H is replaced by $W^\star_{\rm S}$. Then, from Proposition 3.5, for finite transition systems, there exists $K \in \mathbb{N}_{<|X|\times(|H(X)|+1)}$, such that for all $k \geq K$, $W^k_{\rm A}(x) = W^K_{\rm A}(x)$, for all $x \in X$. We denote the fixed-point of (3.11), (3.12) by $W^\star_{\rm A}$.

Proposition 3.10. *Let Σ be a finite transition system, let $W^\star_{\rm A}$ be the fixed-point of (3.11), (3.12), then, for all $\delta \in \mathbb{R}$, $L_\delta(W^\star_{\rm A}) = {\rm A\text{-}cont}(\Sigma, X^*_\delta)$. Moreover, let $V_{\rm A}$ be given by (2.4), then $V_{\rm A} = W^\star_{\rm A}$.*

Proof. From Theorems 3.7 and 3.2, it follows that $L_\delta(W^\star_{\rm A}) = {\rm R\text{-}cont}(\Sigma, L_\delta(W^\star_{\rm S})) = {\rm R\text{-}cont}(\Sigma, {\rm S\text{-}cont}(\Sigma, X^*_\delta))$. Then, from Proposition 2.10, we get $L_\delta(W^\star_{\rm A}) = {\rm A\text{-}cont}(\Sigma, X^*_\delta)$. The second part of the proposition is proved along the same lines as Corollary 3.3. □ □

Similar to the case of safety and reachability specifications, computing the fixed-point of (3.11), (3.12) allows one to compute the sets of uniform attractivity controllable states for the parameterized family of specification sets X^*_δ.

We now focus on the synthesis of controllers enforcing the attractivity specification. Let the function $k^\star : X \to \mathbb{N}$ be defined as follows for all $x \in X$

$$k^\star(x) = \min\{k \in \mathbb{N} |\ W^k_{\rm A}(x) = W^\star_{\rm A}(x)\}. \tag{3.13}$$

Let us remark that $k^\star$ is well-defined and for all $x \in X$, $0 \leq k^\star(x) \leq K$.

For $\delta \in \mathbb{R}$, let us define the controller C_{A}^{δ} as follows:

$$C_{\mathrm{A}}^{\delta}(x) = \begin{cases} \arg\min\limits_{u \in \mathrm{enab}_F(x)} \Big(\max\limits_{x^+ \in F(x,u)} W_{\mathrm{A}}^{k^\star(x)-1}(x^+) \Big) \\ \qquad\qquad \text{if } W_{\mathrm{A}}^{\star}(x) \leq \delta < W_{\mathrm{S}}^{\star}(x); \\ \arg\min\limits_{u \in \mathrm{enab}_F(x)} \Big(\max\limits_{x^+ \in F(x,u)} W_{\mathrm{S}}^{\star}(x^+) \Big) \\ \qquad\qquad \text{if } W_{\mathrm{S}}^{\star}(x) \leq \delta; \\ \emptyset \qquad\qquad \text{if } \delta < W_{\mathrm{A}}^{\star}(x) \end{cases} \tag{3.14}$$

From (3.12), we have for all $x \in X$, $W_{\mathrm{A}}^{\star}(x) \leq W_{\mathrm{S}}^{\star}(x)$. Hence, the three cases in (3.14) cover all possible position of δ relatively to $W_{\mathrm{A}}^{\star}(x)$ and $W_{\mathrm{S}}^{\star}(x)$. If $W_{\mathrm{A}}^{\star}(x) \leq \delta < W_{\mathrm{S}}^{\star}(x)$, then from (3.11) and (3.13), we get that $k^\star(x) \geq 1$, which also implies that $x \in \mathrm{nbs}_F$ and therefore the first case in (3.14) is well-defined. If $W_{\mathrm{S}}^{\star}(x) \leq \delta$, then $x \in \mathrm{nbs}_F$ (otherwise we would have $W_{\mathrm{S}}^{\star}(x) = +\infty$) and the second case in (3.14) is also well-defined.

Theorem 3.11. *Let Σ be a finite transition system, let $W_{\mathrm{S}}^{\star}$ and $W_{\mathrm{A}}^{\star}$ be the fixed-points of (3.1), (3.2) and (3.11), (3.12), respectively, let $T_0 = |H(X)| \times (K+1) - 1$. Let $\delta \in \mathbb{R}$ and let C_{A}^{δ} be given by (3.14). Then, for all $x_0 \in L_\delta(W_{\mathrm{A}}^{\star})$, all maximal trajectories $(x_t)_{t=0}^{T} \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{A}}^{\delta}, x_0)$ are complete and satisfy $x_t \in X_\delta^*$, for all $t \geq T_0$.*

Proof. Let $\delta \in \mathbb{R}$, $x_0 \in L_\delta(W_{\mathrm{A}}^{\star})$ and $(x_t)_{t=0}^{T} \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{A}}^{\delta}, x_0)$.

For all $t \in \mathbb{N}_{<T}$, such that $W_{\mathrm{A}}^{\star}(x_t) \leq \delta < W_{\mathrm{S}}^{\star}(x_t)$, then $k^\star(x_t) \geq 1$ and similar to the proof of Lemma 3.6 we can show that $(W_{\mathrm{A}}^{\star}(x_{t+1}), k^\star(x_{t+1})) <_{lex} (W_{\mathrm{A}}^{\star}(x_t), k^\star(x_t))$. Then, if $W_{\mathrm{A}}^{\star}(x_0) \leq \delta < W_{\mathrm{S}}^{\star}(x_0)$, it follows that either there exists $t \in \mathbb{N}_{\leq \min(T,T_0)}$ such that $W_{\mathrm{S}}^{\star}(x_t) \leq \delta$, or $T \leq T_0$ and $W_{\mathrm{A}}^{\star}(x_T) \leq \delta < W_{\mathrm{S}}^{\star}(x_T)$. In the second case, we have from (3.14) that $C_{\mathrm{A}}^{\delta}(x_T) \neq \emptyset$, which contradicts the maximality of $(x_t)_{t=0}^{T}$.

Moreover, for all $t \in \mathbb{N}_{<T}$, such that $W_{\mathrm{S}}^{\star}(x_t) \leq \delta$ it follows similar to the proof of Theorem 3.2 that $W_{\mathrm{S}}^{\star}(x_{t+1}) \leq W_{\mathrm{S}}^{\star}(x_t)$. Hence, it follows that for all $t \in \mathbb{N}_{\leq T}$, such that $t \geq \min(T, T_0)$, $W_{\mathrm{S}}^{\star}(x_t) \leq \delta$. If $T < +\infty$, then $W_{\mathrm{S}}^{\star}(x_T) \leq \delta$ implies that $C_{\mathrm{A}}^{\delta}(x_T) \neq \emptyset$, which contradicts the maximality of $(x_t)_{t=0}^{T}$. Therefore, $(x_t)_{t=0}^{T}$ is complete and for all $t \geq T_0$, $W_{\mathrm{S}}^{\star}(x_t) \leq \delta$. Since $H(x) \leq W_{\mathrm{S}}^{\star}(x)$ for all $x \in X$, we get the statement of the theorem. □ □

We would like to highlight here an important difference with safety and reachability specifications. Indeed, the proposed controller (3.14) depends on the value of the parameter δ when safety and reachability controllers (3.4) and (3.10) are independent from the value of δ. Actually, it is in general impossible to find a controller of the class introduced in Definition 2.2 that enforces uniform attractivity of X_δ^* from all initial states in A-cont(Σ, X_δ^*), for all possible value of δ at the same time. This is shown by the following example:

Example 3.12. Consider a transition system $\Sigma = (X, U, Y, F, H)$ where $X = \{0,1,2,3\}$, $U = \{0,1\}$ and F is given by $F(0,0) = \{0\}$, $F(1,0) = \{3\}$, $F(1,1) = \{2\}$, $F(2,0) = \{1,2\}$, $F(3,0) = \{0\}$, $Y = X$ and $H(x) = x$ for all $x \in X$. A pictural representation of Σ is shown in Figure 4. For this system, we have $X_0^* = \{0\}$, $X_2^* = \{0,1,2\}$, A-cont$(\Sigma, X_0^*) = \{0,1,3\}$ and A-cont$(\Sigma, X_2^*) = X$. Let us show that there is no controller of the class introduced in Definition 2.2 that enforces at the same time uniform attractivity of X_0^* from all initial states in A-cont(Σ, X_0^*), and of X_2^* from all initial states in A-cont(Σ, X_2^*). Indeed, to enforce uniform attractivity of X_0^* from state $x_0 = 1$ it is necessary to choose $C(1) = \{0\}$. From other states, only input 0 is enabled and therefore we have to choose $C(x) = \{0\}$, for all $x \in X$. Let us emphasize that this is the unique controller enforcing uniform attractivity of X_0^* from all states in A-cont(Σ, X_0^*). However, this controller does not enforce uniform attractivity of X_2^* from state $x_0 = 2$ that belongs to A-cont(Σ, X_2^*). Indeed, for $x_0 = 2$, for any $\tau \in \mathbb{N}$, $\tau \geq 2$, there exists $(x_t)_{t=0}^{T} \in \mathcal{T}_{\max}(\Sigma, C, x_0)$, such that $x_\tau = 3$. Hence, for $x_0 = 2$, it is not possible to find $T_0 \in \mathbb{N}$, such that for all $(x_t)_{t=0}^{T} \in \mathcal{T}_{\max}(\Sigma, C, x_0)$, $x_t \in X_2^*$, for all $t \geq T_0$. Hence, C does not enforce uniform attractivity of X_2^* from all initial states in A-cont(Σ, X_2^*). Since C is the unique controller enforcing uniform attractivity of X_0^* from all initial states in A-cont(Σ, X_0^*), there does not exist any controller enforcing uniform attractivity of X_0^* and X_2^* at the same time. ⋄

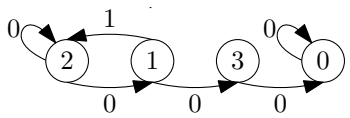

FIGURE 4. Illustration of Example 3.12: there does not exist a memoryless controller that enforces uniform attractivity of $X_0^* = \{0\}$ and $X_2^* = \{0, 1, 2\}$ at the same time.

If we relax the uniformity requirement for some of the states, the following controller, which is independent of δ can be used.

$$C_{\mathrm{A}}^\star(x) = \begin{cases} \arg \min\limits_{u \in \mathrm{enab}_F(x)} \Big(\max\limits_{x^+ \in F(x,u)} W_{\mathrm{A}}^{k^\star(x)-1}(x^+) \Big) \\ \qquad\qquad \text{if } k^\star(x) \geq 1; \\ \arg \min\limits_{u \in \mathrm{enab}_F(x)} \Big(\max\limits_{x^+ \in F(x,u)} W_{\mathrm{S}}^\star(x^+) \Big) \\ \qquad\qquad \text{if } k^\star(x) = 0 \text{ and } x \in \mathrm{nbs}_F; \\ \emptyset \qquad\qquad \text{if } x \notin \mathrm{nbs}_F \end{cases} \tag{3.15}$$

If $k^\star(x) \geq 1$, then $x \in \mathrm{nbs}_F$ and therefore the first case in (3.15) is well-defined. Also, let us remark that for $x \notin \mathrm{nbs}_F$ then by (3.2), (3.12), we get that $W_{\mathrm{A}}^\star(x) = W_{\mathrm{S}}^\star(x) = +\infty$. Therefore, it follows that for all $x \in X$, such that $W_{\mathrm{A}}^\star(x) < +\infty$, $x \in \mathrm{nbs}_F$ and $C_{\mathrm{A}}^\star(x) \neq \emptyset$.

Theorem 3.13. *Let Σ be a finite transition system, let $W_{\mathrm{S}}^\star$ and $W_{\mathrm{A}}^\star$ be the fixed-points of (3.1), (3.2) and (3.11), (3.12), respectively. Let $C_{\mathrm{A}}^\star$ be given by (3.15). Then, the following holds:*

- *For all $\delta \in \mathbb{R}$, for all $x_0 \in L_\delta(W_{\mathrm{A}}^\star)$, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{A}}^\star, x_0)$ are complete and there exists $T_0 \in \mathbb{N}$ such that $x_t \in X_\delta^*$, for all $t \geq T_0$.*
- *For all $x_0 \in L_{\delta_0}(W_{\mathrm{A}}^\star)$, with $\delta_0 = \min_{x \in X} W_{\mathrm{S}}^\star(x)$, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{A}}^\star, x_0)$ are complete and satisfy $x_t \in X_{\delta_0}^*$, for all $t \geq K$.*

Proof. Let $\delta \in \mathbb{R}$, let us consider $x_0 \in L_\delta(W_{\mathrm{A}}^\star)$ and $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma, C_{\mathrm{A}}^\star, x_0)$.

For all $t \in \mathbb{N}_{<T}$, such that $k^\star(x_t) \geq 1$, we can show similar to the proof of Lemma 3.6 that $(W_{\mathrm{A}}^\star(x_{t+1}), k^\star(x_{t+1})) <_{lex} (W_{\mathrm{A}}^\star(x_t), k^\star(x_t))$.

For all $t \in \mathbb{N}_{<T}$, such that $k^\star(x_t) = 0$, and we have from (3.3) and (3.15) that $W_{\mathrm{S}}^\star(x_{t+1}) \leq W_{\mathrm{S}}^\star(x_t)$. Since $k^\star(x_t) = 0$, we have $W_{\mathrm{S}}^\star(x_t) = W_{\mathrm{A}}^\star(x_t)$. Moreover, we have from (3.12) that $W_{\mathrm{A}}^\star(x_{t+1}) \leq W_{\mathrm{S}}^\star(x_{t+1})$. Therefore, $W_{\mathrm{A}}^\star(x_{t+1}) \leq W_{\mathrm{A}}^\star(x_t)$. Moreover, if $W_{\mathrm{A}}^\star(x_{t+1}) = W_{\mathrm{A}}^\star(x_t)$, we get that $W_{\mathrm{A}}^\star(x_{t+1}) = W_{\mathrm{S}}^\star(x_{t+1})$ and therefore $k^\star(x_{t+1}) = 0$. Hence, for all $t \in \mathbb{N}_{<T}$, such that $k^\star(x_t) = 0$, we have $(W_{\mathrm{A}}^\star(x_{t+1}), k^\star(x_{t+1})) \leq_{lex} (W_{\mathrm{A}}^\star(x_t), k^\star(x_t))$.

If $T < +\infty$, then from above we get that $W_{\mathrm{A}}^\star(x_T) \leq \delta$, which implies that $C_{\mathrm{A}}^\star(x_T) \neq \emptyset$ and contradicts the maximality of $(x_t)_{t=0}^T$. Hence $T = +\infty$, and $(x_t)_{t=0}^T$ is complete. Moreover from above, we get that there exists $T_0 \in \mathbb{N}$, such that for all $t \geq T_0$, $W_{\mathrm{A}}^\star(x_t) = W_{\mathrm{A}}^\star(x_{T_0})$ and $k^\star(x_t) = 0$. Hence, for all $t \geq T_0$, $W_{\mathrm{S}}^\star(x_t) = W_{\mathrm{A}}^\star(x_t) = W_{\mathrm{A}}^\star(x_{T_0}) \leq \delta$. Since $H(x) \leq W_{\mathrm{S}}^\star(x)$ for all $x \in X$, we get the first statement of the theorem.

Let us assume that $x_0 \in L_{\delta_0}(W_{\mathrm{A}}^\star)$. For all $x \in X$, we have $W_{\mathrm{A}}^\star(x) \geq \delta_0$. Then, from above we have for all $t \in \mathbb{N}$, $W_{\mathrm{A}}^\star(x_t) = \delta_0$. Moreover, when $k^\star(x_t) \geq 1$, it follows that $k^\star(x_{t+1}) < k^\star(x_t)$ and when $k^\star(x_t) = 0$, it follows that $k^\star(x_{t+1}) = 0$. Since $k^\star(x_0) \leq K$, we have for all $t \geq K$ that $k^\star(x_t) = 0$. Then, for all $t \geq K$, $W_{\mathrm{S}}^\star(x_t) = W_{\mathrm{A}}^\star(x_t) = \delta_0$. Since $H(x) \leq W_{\mathrm{S}}^\star(x)$ for all $x \in X$, we get the second statement of the theorem. □ □

Hence, the previous theorem shows that there exists a controller given by (3.15), independent from the parameter δ, and such that for all $\delta \in \mathbb{R}$, all maximal closed-loop trajectories initiating in A-cont(Σ, X^*_δ) do not leave X^*_δ after some finite time, though it is not possible to provide a uniform bound on that time. Nonetheless, the controller (3.15) enforces uniform attractivity of $X^*_{\delta_0}$ from all initial states in A-cont$(\Sigma, X^*_{\delta_0})$.

4. Abstraction-based synthesis for infinite systems

In this section, we show how to lift our approach from finite state systems to infinite state systems by using abstraction techniques. Let consider us consider two transition systems $\Sigma_1 = (X_1, U_1, Y_1, F_1, H_1)$ and $\Sigma_2 = (X_2, U_2, Y_2, F_2, H_2)$ sharing the same set of outputs $Y_1 = Y_2 = \overline{\mathbb{R}}$. In the following discussion, Σ_1 represents the concrete system and is generally an infinite transition system while Σ_2 is the finite abstraction. Hence, safety, uniform reachability and uniform attractivity controllability measures and the associated least-violating controllers can be computed for Σ_2 using the techniques presented in the previous section. To be able to lift these results to Σ_1 we need to assume that some formal behavioral relationship holds between Σ_1 and Σ_2. We consider the following notion of approximate alternating simulation relation, which is adapted from [36].

Definition 4.1. Let $\varepsilon \in \mathbb{R}^+_0$, a relation $R \subseteq X_1 \times X_2$ is an *ε-approximate alternating simulation relation* from Σ_1 to Σ_2 if for all $(x_1, x_2) \in R$, the following conditions hold:

(1) $H_1(x_1) \leq H_2(x_2) + \varepsilon$
(2) for all $u_2 \in \text{enab}_{F_2}(x_2)$, there exists $u_1 \in \text{enab}_{F_1}(x_1)$, such that $F_1(x_1, u_1) \subseteq R^{-1}(F_2(x_2, u_2))$.

R is said to be an *ε-approximate alternating bisimulation relation* between Σ_1 and Σ_2 if R and R^{-1} are ε-approximate alternating simulation relation from Σ_1 to Σ_2 and from Σ_2 to Σ_1 respectively.

There exist techniques for computing finite abstractions of nonlinear systems provided these satisfy some assumptions. Under the mild assumption of incremental forward completeness, finite abstractions can be computed that are related by ε-approximate alternating simulation relations [40]. When considering the much stronger assumption of incremental stability, finite abstractions can be related by ε-approximate alternating bisimulation relations [27, 16, 28]. Finally, if the system satisfies some incremental stabilizability assumption, finite abstractions can be computed that are related by ε-approximate alternating simulation relations [35]. Let us remark that while the abstractions obtained in [40] are non-deterministic, those of [35] are deterministic. Note that in all these techniques, the parameter ε determining the accuracy of the abstraction can be chosen arbitrarily small. Of course, more accurate abstractions require more states.

The following result establishes relations between the controllability measures of Σ_1 and Σ_2:

Theorem 4.2. *Let $V_{\mathrm{S},i}$, $V_{\mathrm{R},i}$ and $V_{\mathrm{A},i}$ denote the safety, uniform reachability, uniform attractivity controllability measures for system Σ_i, $i = 1, 2$:*

- *If $R \subseteq X_1 \times X_2$ is an ε-approximate alternating simulation relation from Σ_1 to Σ_2, then for all $(x_1, x_2) \in R$*

$$V_{\mathrm{S},1}(x_1) \leq V_{\mathrm{S},2}(x_2) + \varepsilon,$$
$$V_{\mathrm{R},1}(x_1) \leq V_{\mathrm{R},2}(x_2) + \varepsilon,$$
$$V_{\mathrm{A},1}(x_1) \leq V_{\mathrm{A},2}(x_2) + \varepsilon.$$

- *If $R \subseteq X_1 \times X_2$ is an ε-approximate alternating bisimulation relation between Σ_1 and Σ_2, then for all $(x_1, x_2) \in R$*

$$|V_{\mathrm{S},1}(x_1) - V_{\mathrm{S},2}(x_2)| \leq \varepsilon,$$
$$|V_{\mathrm{R},1}(x_1) - V_{\mathrm{R},2}(x_2)| \leq \varepsilon,$$
$$|V_{\mathrm{A},1}(x_1) - V_{\mathrm{A},2}(x_2)| \leq \varepsilon.$$

Proof. Let $R \subseteq X_1 \times X_2$ be an ε-approximate alternating simulation relation from Σ_1 to Σ_2, and let us consider $(x_1, x_2) \in R$. With only minor modifications to the proofs of Theorems 1 and 3 in [14], it is possible to show that the following implication holds for all $\delta \in \mathbb{R}$:

$$\begin{aligned} x_2 \in \text{S-cont}(\Sigma_2, &L_\delta(H_2)) \\ &\implies x_1 \in \text{S-cont}(\Sigma_1, L_{\delta+\varepsilon}(H_1)) \\ x_2 \in \text{R-cont}(\Sigma_2, &L_\delta(H_2)) \\ &\implies x_1 \in \text{R-cont}(\Sigma_1, L_{\delta+\varepsilon}(H_1)) \end{aligned}$$

This implies that $V_{\mathrm{S},1}(x_1) \leq V_{\mathrm{S},2}(x_2) + \varepsilon$ and $V_{\mathrm{R},1}(x_1) \leq V_{\mathrm{R},2}(x_2) + \varepsilon$ for all $(x_1, x_2) \in R$. Similarly, we can show that for all $\delta \in \mathbb{R}$, for all $(x_1, x_2) \in R$:

$$\begin{aligned} x_2 \in \text{R-cont}(\Sigma_2, &L_\delta(V_{\mathrm{S},2})) \\ &\implies x_1 \in \text{R-cont}(\Sigma_1, L_{\delta+\varepsilon}(V_{\mathrm{S},1})). \end{aligned}$$

This, together with Proposition 2.10, allows us to conclude that for all $\delta \in \mathbb{R}$, for all $(x_1, x_2) \in R$:

$$\begin{aligned} x_2 \in \text{A-cont}(\Sigma_2, &L_\delta(H_2)) \\ &\implies x_1 \in \text{A-cont}(\Sigma_1, L_{\delta+\varepsilon}(H_1)). \end{aligned}$$

Hence $V_{\mathrm{A},1}(x_1) \leq V_{\mathrm{A},2}(x_2) + \varepsilon$ for all $(x_1, x_2) \in R$. The second item of the theorem is a straightforward consequence of the first one. □ □

Let us now move to controller refinement. Namely, given the least-violating controllers for Σ_2 as defined in the previous section, we address the question about how one can obtain safety, reachability and attractivity controllers for Σ_1. For systems related by ε-approximate alternating simulation relation, there exists a canonical controller refinement procedure described e.g. in [36]. However, this procedure does not allow to produce memoryless controllers for Σ_1 even when memoryless controllers are given for the abstraction Σ_2. However, specific refinement procedures can be designed for safety and reachability specifications, which result in memoryless controllers, see [14] for the qualitative case, and [12] for the quantitative case. Note that all these controllers allow to achieve the bounds established in Theorem 4.2. In the following, for the sake of simplicity and brevity, we will discuss controller refinement only in the specific case of feedback refinement relations [31].

Definition 4.3. A relation $R \subseteq X_1 \times X_2$ is a *feedback refinement relation* from Σ_1 to Σ_2 if $\mathrm{dom}(R) = X_1$ and for all $(x_1, x_2) \in R$, the following conditions hold:

(1) $H_1(x_1) \leq H_2(x_2)$
(2) $\mathrm{enab}_{F_2}(x_2) \subseteq \mathrm{enab}_{F_1}(x_1)$
(3) for all $u \in \mathrm{enab}_{F_2}(x_2)$, $R(F_1(x_1, u)) \subseteq F_2(x_2, u)$.

While all feedback refinement relations are 0-approximate alternating simulation relation the converse is not true. The main advantage of feedback refinement relations is that they have a very simple canonical controller refinement procedure, which in particular preserves the memoryless property from the abstract to the concrete controller. Techniques for computing finite abstractions of nonlinear systems related by feedback refinement relations are described in [31]. For our setting, we can state the following result, which is a straightforward consequence of Theorems 3.2, 3.7, 3.13 and Theorem V.4 in [31]:

Theorem 4.4. *Let $R \subseteq X_1 \times X_2$ be a feedback refinement relation from Σ_1 to Σ_2:*

(1) *For Σ_2, let $W^\star_{\mathrm{S},2}$ be the fixed-point of (3.1), (3.2), and let $C^\star_{\mathrm{S},2}$ be given by (3.4). Then, for all $\delta \in \mathbb{R}$, for all $x_0 \in X_1$ with $R(x_0) \subseteq L_\delta(W^\star_{\mathrm{S},2})$, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma_1, C^\star_{\mathrm{S},2} \circ R, x_0)$ are complete and satisfy $x_t \in L_\delta(H_1)$, for all $t \in \mathbb{N}$.*
(2) *For Σ_2, let $W^\star_{\mathrm{R},2}$ be the fixed-point of (3.5), (3.6), let $C^\star_{\mathrm{R},2}$ be given by (3.10). Then, there exists $T_0 \in \mathbb{N}$, such that for all $\delta \in \mathbb{R}$, for all $x_0 \in X_1$ with $R(x_0) \subseteq L_\delta(W^\star_{\mathrm{R},2})$, for all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma_1, C^\star_{\mathrm{R},2} \circ R, x_0)$, $T \leq T_0$ and $x_T \in L_\delta(H_1)$.*

(3) *For Σ_2, let $W^\star_{\mathrm{S},2}$ and $W^\star_{\mathrm{A},2}$ be the fixed-points of (3.1), (3.2) and (3.11), (3.12), respectively and let $C^\star_{\mathrm{A},2}$ be given by (3.15). Then, the following holds:*
   - *For all $\delta \in \mathbb{R}$, for all $x_0 \in X_1$ with $R(x_0) \subseteq L_\delta(W^\star_{\mathrm{A},2})$, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma_1, C^\star_{\mathrm{A},2} \circ R, x_0)$ are complete and there exists $T_0 \in \mathbb{N}$ such that $x_t \in L_\delta(H_1)$, for all $t \geq T_0$.*
   - *There exists $T_0 \in \mathbb{N}$, such that for all $x_0 \in X_1$ with $R(x_0) \subseteq L_{\delta_0}(W^\star_{\mathrm{A},2})$, with $\delta_0 = \min_{x_2 \in X_2} W^\star_{\mathrm{S},2}(x_2)$, all maximal trajectories $(x_t)_{t=0}^T \in \mathcal{T}_{\max}(\Sigma_1, C^\star_{\mathrm{A},2} \circ R, x_0)$ are complete and satisfy $x_t \in L_\delta(H_1)$, for all $t \geq T_0$.*

5. Application to adaptive cruise control

In this section, we show an application of our approach to adaptive cruise control. We consider the following set-up with two vehicles. Vehicle 1 is following vehicle 2, the relative position of the former with respect to the latter is given by $d \in (-\infty, 0]$. Vehicles are driving at velocities v_1 and v_2 respectively. In the following, the dynamics of vehicle 1 is controlled while that of vehicle 2 is considered as a disturbance. We consider the following discrete-time model with sampling period τ derived from [25] :

$$\left\{ \begin{array}{lcl} d_{t+1} & = & d_t + \tau(v_{1,t} - v_{2,t}) \\ v_{1,t+1} & = & v_{1,t} + \tau f(v_{1,t}, u_t) \\ v_{2,t+1} & = & \sigma_{[v_2^{\min}, v_2^{\max}]}(v_{2,t} + \tau a_{2,t}) \end{array} \right. \tag{5.1}$$

where $f(v,u) = u - (f_0 + f_1 v + f_2 v^2)/M$ and $\sigma_{[a,b]}$ is a saturation function defined by $\sigma_{[a,b]}(v) = \max(a, \min(v, b))$, which guarantees that $v_{2,t} \in [v_2^{\min}, v_2^{\max}]$ for all time. The control input $u_t \in [u^{\min}, u^{\max}]$ represents the contribution of braking and engine torque to the acceleration of vehicle 1. M denotes the mass of the vehicle 1, while the vector of parameters $f = (f_0, f_1, f_2)$ describes road friction and vehicle aerodynamics. The disturbance $a_{2,t} \in [a_2^{\min}, a_2^{\max}]$ represents the acceleration of vehicle 2.

We consider the problem of designing an adaptive cruise control system. For that purpose, we define the time headway $\omega_t = -d_t/v_{1,t}$. The requirements for adaptive cruise control, parameterized by a target velocity v^* and a target time headway ω^*, are formulated as follows. We must either:

- keep the time headway $\omega_t \geq \omega^*$ and maintain the velocity $v_{1,t}$ at the desired value v^*, or
- keep velocity $v_{1,t} \leq v^*$ and maintain the time headway ω_t at the desired value ω^*.

We formalize this specification as synthesizing a controller enforcing uniform attractivity of

$$X^* = \{(d, v_1, v_2) \in \mathbb{R}^3 |\ (-d/v_1, v_1) \in Z_a^* \cup Z_b^*\}$$

where

$$Z_a^* = \{(\omega, v_1) \in \mathbb{R}^2 |\ \omega \geq \omega^*,\ v_1 = v^*\},$$
$$Z_b^* = \{(\omega, v_1) \in \mathbb{R}^2 |\ \omega = \omega^*,\ v_1 \leq v^*\}.$$

Actually, this specification cannot be enforced so we aim at synthesizing the least-violating controller with respect to the following distance function:

$$H(d, v_1, v_2) = \min_{(\omega', v_1') \in Z_a^* \cup Z_b^*} \max(|-d/v_1 - \omega'|, \alpha |v_1 - v_1'|)$$

where $\alpha > 0$ is a design parameter defining the relative tolerance to deviations from the desired velocity and from the desired time headway. In addition, we specify strong safety requirements regarding collision avoidance and conformance to speed limitations. We must at all time:

- keep the distance $d_t \leq 0$, and
- keep velocity $v_{1,t} \in [v_1^{\min}, v_1^{\max}]$.

To enforce these specifications by design, we disable in system (5.1) the inputs leading to states violating such constraints. Note that this may introduce some blocking states in (5.1), which can be handled by our approach. Values of parameters, compatible with empirical measurements are taken from [25] and given in Table 1.

M	1370	kg
f_0	51	N
f_1	1.2567	Ns/m
f_2	0.4342	$\mathrm{Ns}^2/\mathrm{m}^2$
τ	0.5	s
g	9.82	$\mathrm{m/s}^2$

$u^{\min}$	-0.3g	$\mathrm{m/s}^2$
$u^{\max}$	0.2g	$\mathrm{m/s}^2$
$v_2^{\min}$	12	m/s
$v_2^{\max}$	28	m/s
$a_2^{\min}$	-3	$\mathrm{m/s}^2$
$v_2^{\max}$	2	$\mathrm{m/s}^2$

v^*	20	m/s
ω^*	1.5	s
$v_1^{\min}$	10	m/s
$v_1^{\max}$	30	m/s
α	0.5	

TABLE 1. Parameter values

We propose to solve the problem using the abstraction-based approach presented in the paper. For that purpose, we build a symbolic abstraction of system (5.1). We use a covering of the state space $(-\infty, 0] \times [v_1^{\min}, v_1^{\max}] \times [v_2^{\min}, v_2^{\max}]$, given by the Cartesian product of coverings of the three intervals defined as follows:

$$\begin{cases} (-\infty, 0] &= (-\infty, d_0 + \theta_d] \cup \\ & \qquad \bigcup_{i=1}^{n_d - 1} [d_0 + i\theta_d, d_0 + (i+1)\theta_d], \\ [v_1^{\min}, v_1^{\max}] &= \bigcup_{i=0}^{n_{v_1} - 1} [v_1^{\min} + i\theta_{v_1}, v_1^{\min} + (i+1)\theta_{v_1}], \\ [v_2^{\min}, v_2^{\max}] &= \bigcup_{i=0}^{n_{v_2} - 1} [v_2^{\min} + i\theta_{v_2}, v_2^{\min} + (i+1)\theta_{v_2}], \end{cases}$$

where $\theta_d = -d_0/n_d$, $\theta_{v_1} = (v_1^{\max} - v_1^{\min})/n_{v_1}$, $\theta_{v_2} = (v_2^{\max} - v_2^{\min})/n_{v_2}$. We also use a subset of the input set given by $\{u^{\min} + i\theta_u |\ i = 0, \ldots, n_u - 1\}$ where $\theta_u = (u^{\max} - u^{\min})/(n_u - 1)$. The symbolic abstraction is computed using an approach similar to [31, 34] and is related to the system (5.1) by a feedback refinement relation. Note that the function H needs also to be over-approximated on each element of the covering. For the numerical results reported below the following abstraction parameter where chosen: $d_0 = -100$ m, $n_d = 50$, $n_{v_1} = 50$, $n_{v_2} = 40$, $n_u = 10$.

For the abstraction, we used the approach presented in Section 3 to compute $W^\star_{\mathrm{S},2}$ and $W^\star_{\mathrm{A},2}$ the fixed-points of (3.1), (3.2) and (3.11), (3.12), respectively and the associated least-violating controller $C^\star_{\mathrm{A},2}$ given by (3.15). Then, we used Theorem 4.4 to obtain a controller for system (5.1). The overall computation took about 3 hours (CPU: 2.2 GHz Intel Core i7, RAM: 16 Go 1600 MHz DDR3, Matlab R2015a). The computed minimal safety controllability measure is $\delta_0 = \min_{x_2 \in X_2} W^\star_{\mathrm{S},2}(x_2) = 0.9118$.

In Figure 5, we show slices of the computed sets represented at different values of v_2:

- The red line represents the target set X^*.
- The white set represents the set $L_{\delta_0}(W^\star_{\mathrm{S},2})$. All trajectories starting in this set stay there forever. It is the set of safety controllable states that is the closest to X^* as measured by distance H. This set is also shown in full dimension in Figure 6.
- The light grey set represents the set $L_{\delta_0}(W^\star_{\mathrm{A},2})$. All trajectories starting in this set will reach the white set before a uniformly bounded finite time (here 10 s).
- The dark grey represents the set $\bigcup_{\delta < +\infty} L_\delta(W^\star_{\mathrm{A},2})$. All trajectories starting in this set stay there forever, without guarantees of ever reaching the white set.

- The black set consists of the uncontrollable states from which the strong safety requirements cannot be guaranteed.

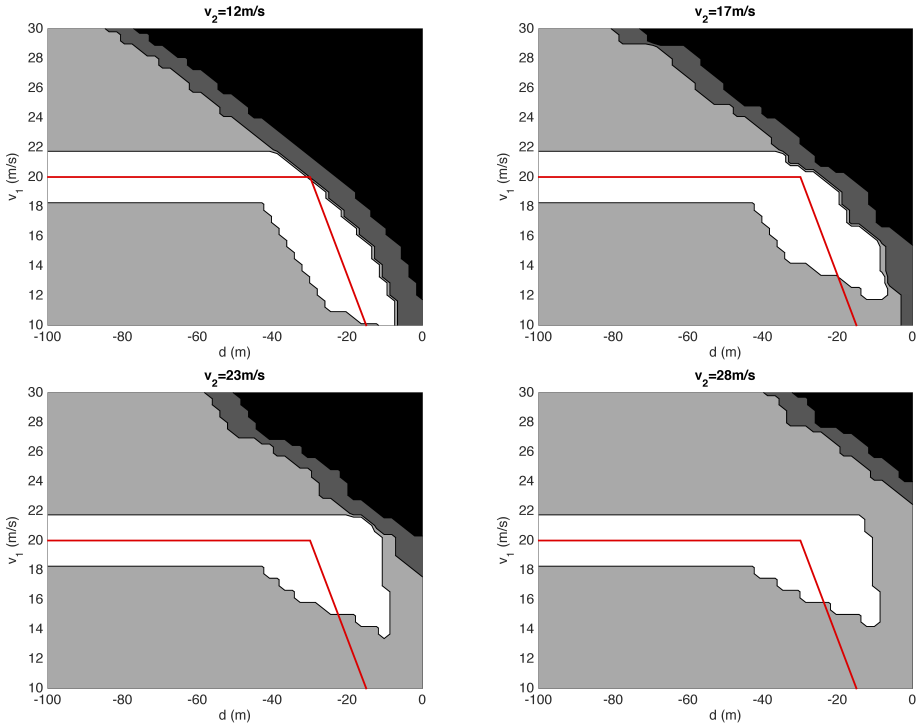

FIGURE 5. Sets of safety controllable states (white), of uniform attractivity controllable states (light and dark grey) and of uncontrollable states (black) computed by the algorithm (detailed description in the text).

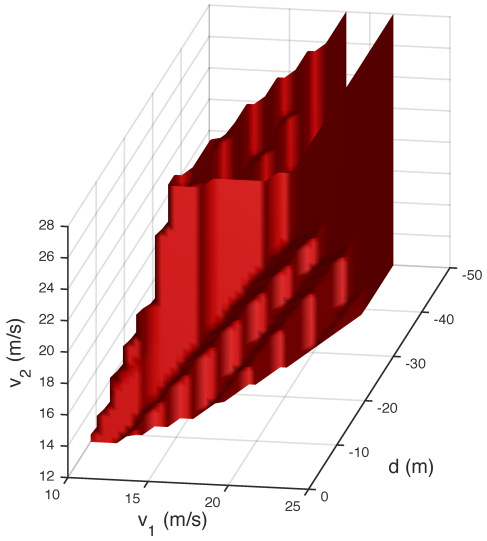

FIGURE 6. Boundary of $L_{\delta_0}(W^{\star}_{\mathrm{S},2})$, the set of safety controllable states that is the closest to X^* as measured by distance H.

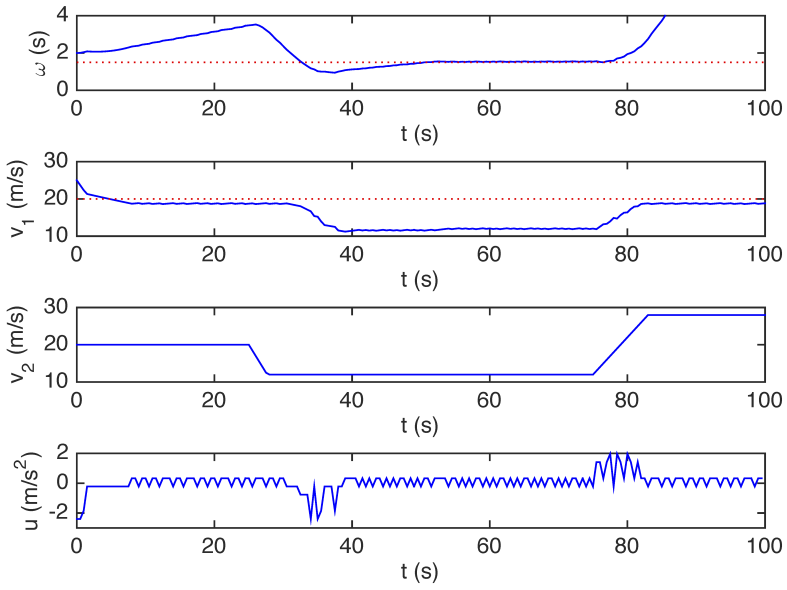

FIGURE 7. Simulated trajectories of system (5.1) using the synthesized controllers: evolution of the time headway, of the velocities of vehicle 1 and vehicle 2 and the control input of vehicle 1; The values of the target velocity v^* and the target time headway ω^* are represented by dashed lines.

In Figure 7, we show a simulation of system (5.1) using the controller given in Theorem 4.4. We consider the following scenario, the initial value of (d, v_1, v_2) is $(-50, 25, 20)$. The leading vehicle (vehicle 2) drives at constant speed for the first 25 s, then applies maximal deceleration until reaching minimal speed for the next 50 s, and maximal acceleration until reaching maximal speed for the last 25 s. The plots represent the evolution of the time headway, of the velocities of vehicle 1 and vehicle 2 and the control input of vehicle 1. The values of the target velocity v^* and the target time headway ω^* are represented by dashed lines. Initially the time headway is greater than ω^* so vehicle 1 regulates its speed around v^*. After vehicle 2 decelerates, the time headway reduces and drops below ω^*, then vehicle 1 stops regulating its speed to regulate its time headway around ω^*. When vehicle 2 accelerates, the time headway increases again and becomes larger than ω^*, then vehicle 1 restarts regulating its speed around v^*. We can see on this simulation, that the system behaves as expected.

6. Conclusion

In this paper, we presented an approach to synthesize least-violating controllers for safety, uniform reachability and uniform attractivity specifications. Our approach is based on quantitative controllability measures. For finite systems, we showed how these measures and the associated controllers can be computed using dynamic programming. For infinite systems, abstraction based techniques allow to lift these results with strong guarantees. An application to adaptive cruise control shows promising results and proves the relevance of our approach, when ideal specifications cannot be enforced. Future work should focus on extending these results to other types of specifications such as those expressed in Linear Temporal Logic or given under the form of a dynamical system. We will also consider extensions of this work enabling to cope with robustness with respect to unmodelled disturbances.

References

[1] M. Assellaou, O. Bokanowski, A. Desilles, and H. Zidani. Value function and optimal trajectories for a maximum running cost control problem with state constraints. application to an abort landing problem. *ESAIM: Mathematical Modelling and Numerical Analysis*, 52(1):305–335, 2018.

[2] C. Baier and J.-P. Katoen. *Principles of model checking*. MIT press, 2008.

[3] E. Barron. Differential games with maximum cost. *Nonlinear Analysis: Theory, Methods & Applications*, 14(11):971–989, 1990.

[4] C. Belta, B. Yordanov, and E. A. Gol. *Formal methods for discrete-time dynamical systems*. Springer, 2017.

[5] D. P. Bertsekas. *Dynamic programming and optimal control*, volume 2. Athena Scientific, 4th edition, 2012.

[6] D. P. Bertsekas. *Dynamic programming and optimal control*, volume 1. Athena Scientific, 4th edition, 2017.

[7] K. Chatterjee and T. A. Henzinger. Value iteration. In *25 Years of Model Checking*, pages 107–138. Springer, 2008.

[8] E. Dallal, D. Neider, and P. Tabuada. Synthesis of safety controllers robust to unmodeled intermittent disturbances. In *IEEE Conference on Decision and Control*, pages 7425–7430, 2016.

[9] F. de Roo and M. Mazo. On symbolic optimal control via approximate simulation relations. In *IEEE Conference on Decision and Control*, pages 3205–3210, 2013.

[10] S. Di Marco and R. Gonzalez. Relaxation of minimax optimal control problems with infinite horizon. *Journal of Optimization Theory and Applications*, 101(2):285–306, 1999.

[11] A. Donzé and O. Maler. Robust satisfaction of temporal logic over real-valued signals. In *International Conference on Formal Modeling and Analysis of Timed Systems*, pages 92–106. Springer, 2010.

[12] A. Eqtami and A. Girard. Safety control, a quantitative approach. In *IFAC Conference on Analysis and Design of Hybrid System*, 2018.

[13] G. E. Fainekos and G. J. Pappas. Robustness of temporal logic specifications for continuous-time signals. *Theoretical Computer Science*, 410(42):4262–4291, 2009.

[14] A. Girard. Controller synthesis for safety and reachability via approximate bisimulation. *Automatica*, 48(5):947–953, 2012.

[15] A. Girard and G. J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5):782–798, 2007.

[16] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1):116–126, 2009.

[17] L. Grüne and O. Junge. Global optimal control of perturbed systems. *Journal of Optimization Theory and Applications*, 136(3):411–429, 2008.

[18] A. Kurzhanski and P. Varaiya. On some nonstandard dynamic programming problems of control theory. In *Variational Analysis and Applications*, pages 589–603. Springer, 2005.

[19] J. Lygeros. On reachability and minimum cost optimal control. *Automatica*, 40(6):917–927, 2004.

[20] K. Margellos and J. Lygeros. Viable set computation for hybrid systems. *Nonlinear Analysis: Hybrid Systems*, 10:45–62, 2013.

[21] M. Mazo Jr and P. Tabuada. Symbolic approximate time-optimal control. *Systems & Control Letters*, 60(4):256–263, 2011.

[22] P.-J. Meyer, A. Girard, and E. Witrant. Safety control with performance guarantees of cooperative systems using compositional abstractions. *IFAC-PapersOnLine*, 48(27):317–322, 2015.

[23] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin. A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 50(7):947–957, 2005.

[24] D. Neider, A. Weinert, and M. Zimmermann. Synthesizing optimally resilient controllers. *Acta Informatica*, 57(1):195–221, 2020.

[25] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A. D. Ames, J. W. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Correct-by-construction adaptive cruise control: Two approaches. *IEEE Transactions on Control Systems Technology*, 24(4):1294–1307, 2015.

[26] G. Pola and M. D. Di Benedetto. Control of cyber-physical-systems with logic specifications: a formal methods approach. *Annual Reviews in Control*, 2019.

[27] G. Pola, A. Girard, and P. Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10):2508–2516, 2008.

[28] G. Pola and P. Tabuada. Symbolic models for nonlinear control systems: Alternating approximate bisimulations. *SIAM Journal on Control and Optimization*, 48(2):719–733, 2009.

[29] M. Quincampoix and O.-S. Serea. A viability approach for optimal control with infimum cost. *Annals. Stiint. Univ. Al. I. Cuza Iasi, sI a, Mat*, 48:113–132, 2002.

[30] G. Reissig and M. Rungger. Symbolic optimal control. *IEEE Transactions on Automatic Control*, 64(6):2224–2239, 2018.

[31] G. Reissig, A. Weber, and M. Rungger. Feedback refinement relations for the synthesis of symbolic controllers. *IEEE Transactions on Automatic Control*, 62(4):1781–1796, 2016.

[32] M. Rungger, G. Reissig, and M. Zamani. Symbolic synthesis with average performance guarantees. In *IEEE Conference on Decision and Control*, pages 7404–7410, 2016.

[33] S. Sadraddini and C. Belta. Robust temporal logic model predictive control. In *Annual Allerton Conference on Communication, Control, and Computing*, pages 772–779. IEEE, 2015.

[34] A. Saoud, A. Girard, and L. Fribourg. Contract based design of symbolic controllers for interconnected multiperiodic sampled-data systems. In *IEEE Conference on Decision and Control*, pages 773–779, 2018.
[35] P. Tabuada. An approximate simulation approach to symbolic control. *IEEE Transactions on Automatic Control*, 53(6):1406–1418, 2008.
[36] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.
[37] P. Tabuada, S. Y. Caliskan, M. Rungger, and R. Majumdar. Towards robustness for cyber-physical systems. *IEEE Transactions on Automatic Control*, 59(12):3151–3163, 2014.
[38] J. Tumova, G. C. Hall, S. Karaman, E. Frazzoli, and D. Rus. Least-violating control strategy synthesis with safety rules. In *International Conference on Hybrid Systems: Computation and Control*, pages 1–10, 2013.
[39] A. Weber, M. Kreuzer, and A. Knoll. A generalized Bellman-Ford algorithm for application in symbolic optimal control. In *European Control Conference*, 2020.
[40] M. Zamani, G. Pola, M. Mazo, and P. Tabuada. Symbolic models for nonlinear control systems without stability assumptions. *IEEE Transactions on Automatic Control*, 57(7):1804–1809, 2011.

Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, 91190, Gif-sur-Yvette, France

Email address: {antoine.girard,alina.eqtami}@l2s.centralesupelec.fr