Synthesis of Input-to-State Safety and Attractivity Controllers using Nested Sequences of Abstractions

W. A. Apaza-Perez, Antoine Girard

Synthesis of Input-to-State Safety and Attractivity Controllers using Nested Sequences of Abstractions

W. Alejandro Apaza-Perez, Antoine Girard

***Abstract*— In this paper, we introduce a notion of input-to-state safety (ISSf) and input-to-state attractivity (ISA) controllers for finite state dynamical systems. Using such controllers, the deviation of the closed-loop trajectories from a safe or from a target set can be bounded by a gain function that is increasing with respect to the amplitude of the disturbances. We show the existence of controllers that are least violating (LV) in the sense that their gain function is minimal (with respect to a certain order on the set of gain functions) over all possible ISSf and ISA controllers. Then, we consider the problem of synthesizing these LV-ISSf and LV-ISA controllers for the colexicographic order on gain functions. We present an approach that is based on successive refinements of controllers: starting from a controller synthesized against worst-case disturbances, the controller is iteratively refined in order to improve the closed-loop behavior under disturbances of lower amplitude. We prove that our method makes it possible to synthesize a LV-ISSf controller, and an ISA controller that is shown to be a LV-ISA controller when an easily checkable condition is satisfied. We discuss how these results can be used to synthesize robust controllers for nonlinear continuous-time systems via symbolic control techniques. Finally, we show an application to adaptive cruise control to demonstrate the effectiveness of our approach.**

***Index Terms*— Symbolic control; Input-to-sate stability; Safety; Attractivity; Quantitative synthesis.**

I. INTRODUCTION

The field of symbolic control (see e.g. [21], [1], [13]) deals with computational approaches to synthesize controllers for nonlinear dynamical systems subject to state and input constraints and bounded disturbances. Symbolic control techniques rely on the use of symbolic models, also called discrete abstractions, which are finite-state approximations of the dynamical system under consideration [6], [25], [2]. The use of symbolic models makes it possible to use automated discrete controller synthesis techniques for enforcing specifications such as safety or reachability [21], [4], or more complex ones given under the form of dynamical systems [13], [19] or of temporal logic formulas [9], [1]. When the behaviors of the symbolic model and of the original system can be related by some formal relationship, such as alternating simulation relations [14] or feedback refinement relations [16], controllers synthesized for the symbolic model can be used to control the system with formal guarantees of correctness.

However, in practice, it is often the case that a given ideal specification cannot be enforced. In that case, one may be interested in designing the controller that enforces the closed-loop behavior which is the closest possible to the specification, and in providing certificates on the distance to that specification. Such controllers are called least violating since they achieve the minimal violation of the specification according to a certain distance. In [23], controllers for unsatisfiable safety specifications are synthesized in such a way that the closed-loop trajectories spend a minimal amount of time outside the safe set. Another possibility is to synthesize controllers such that the distance between closed-loop trajectories and the set of trajectories satisfying the specification is minimal. This is the approach taken in [17] for bounded-time specifications given by temporal logic formulas and in [5] for unbounded-time specifications such as safety, reachability and uniform attractivity. In all these approaches, the closed-loop behavior is optimized over worst-case disturbances.

In this paper, we go one step further by synthesizing controllers that can adapt the degree of violation of the specification to the amplitude of disturbances. We introduce notions of input-to-state safety (ISSf) controllers and of input-to-state attractivity (ISA) controllers for a class of finite state dynamical systems where the effect of disturbances of varying amplitude is modeled by nested sequences of subsystems. Such controllers are associated to gain functions that quantify the distance between closed-loop trajectories and the safe set or the target set as a function of the amplitude of disturbances. Using such controllers, low amplitude disturbances result in small deviations from the specified behavior, while larger deviations can be expected for disturbances of higher amplitude. While the ISSf property has been introduced recently in [8] for continuous systems, the ISA property is new but directly inspired by the celebrated input-to-state stability (see e.g. [7], [20]).

The first main contribution of this paper is to show the existence ISSf and ISA controllers that are least violating (LV), meaning that their gain function is minimal (with respect to a certain order on the set of gain functions) over all possible ISSf and ISA controllers. As a second contribution, we present algorithms to synthesize LV-ISSf and LV-ISA controllers for the colexicographic order on gain functions. The algorithms are based on successive refinements of least violating (not input-to-state) safety or attractivity controllers that were introduced in [5]. Starting from a least violating controller synthesized against worst-case disturbances, the controller is iteratively refined in order to improve the closed-loop behavior under disturbances of lower amplitude. Each iteration involves solving dynamic programming fixed-points for which efficient algorithms can be found e.g. in [15], [24]. We prove that our method makes it possible to synthesize LV-ISSf controllers and ISA controllers that are shown to be least violating when an easily checkable condition is satisfied. As a third contribution, we demonstrate that our results developed for finite-sate systems can be lifted to nonlinear continuous-time dynamical systems with bounded disturbances using symbolic control techniques. For that purpose, we provide a method for computing nested sequences of abstractions approximating the dynamics of the system subject to disturbances of varying amplitude. Finally, we show an application of our techniques by synthesizing an ISA controller for an adaptive cruise control problem inspired from [12].

Our work partially builds on the results of [5], where the notion of least violating safety and attractivity controllers were introduced and algorithms for their computation were presented. The current paper extends these notions for systems with disturbances of varying amplitude by introducing the LV-ISSf and LV-ISA properties. The algorithms presented in this paper use those presented in [5] as building blocks in an iterative refinement procedure. The main results of the present paper, showing that the synthesized controllers are

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).

W. A. Apaza-Perez and A. Girard are with the Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, 91190, Gif-sur-Yvette, France. {willy-alejandro.apaza-perez; antoine.girard}@l2s.centralesupelec.fr

LV-ISSf or LV-ISA, require non-trivial proof techniques and are not straightforward consequences of the results in [5].

Other closely related works include [22], [3], [11], [18]. In [22], the synthesis of robust controllers is considered where the requirements are firstly that the deviation from the correct behavior (modeled as an automaton) should be proportional to the amplitude of the disturbances and secondly that the effect of sporadic disturbances vanishes after some time. This problem can actually be related to that of synthesizing ISA-controllers. In our approach, the gain functions are not limited to be linear and we introduce the concept of least violating controllers for arbitrary gain functions. Also, the proposed solutions for controller synthesis are different. Synthesis of robust controllers is also considered in [3], [11] for safety and omega-regular specifications. In these works, the controller needs not to adapt its performance to the level of disturbances but instead seeks to maximize the number of disturbed transitions that can occur before the specification is violated. Let us remark that these approaches have also been used with symbolic control techniques in [18] to synthesize resilient controllers. While addressing different objectives and using different formulations, these works share some similarities with our approach in the sense that they are based on controller refinement and dynamic programming.

The rest of the paper is organized as follows. Section II presents some preliminary definitions and introduces the notions of ISSf and ISA controllers. The section ends with the proof of the existence of LV-ISSf and LV-ISA controllers. Sections III and IV present algorithms to compute these controllers and provide proofs of correctness of the proposed algorithms. In section V, we show how our results developed for finite-state systems can be lifted to continuous-time nonlinear systems using the symbolic control approach. Finally, section VI shows an application to the adaptive cruise control problem.

II. PRELIMINARIES

In this section, after defining some notations used in the paper, we present the class of systems under consideration and the types of controllers we aim at synthesizing.

Notations: $\mathbb{R}$, $\mathbb{R}_{>0}$, $\mathbb{R}_{\geq 0}$ and $\mathbb{N}$ denote the sets of real, positive real, non negative real numbers, and non negative integers, respectively. For $J \subseteq \mathbb{R}$ and $K \in \mathbb{R}$, we define the following sets $J_{<K} = \{k \in J | k < K\}$ and $J_{\leq K} = \{k \in J | k \leq K\}$. $\overline{\mathbb{R}}_{\geq 0}$ denotes the set of non negative extended real numbers, i.e. $\overline{\mathbb{R}}_{\geq 0} = [0, +\infty]$. Given a function $V : X \to \overline{\mathbb{R}}_{\geq 0}$, the lower level sets of function V are defined as $L_\delta(V) = \{x \in X | \, V(x) \leq \delta\}$ where $\delta \in \overline{\mathbb{R}}_{\geq 0}$. The power set of a set X is denoted by 2^X and when X is a finite set, $|X|$ denotes the number of elements of X. Given sets X_1, X_2, a relation $R \subseteq X_1 \times X_2$ is identified with the set valued map $R : X_1 \to 2^{X_2}$ defined by $R(x_1) = \{x_2 \in X_2 | \, (x_1, x_2) \in R\}$. The identity relation over X is $I_X = \{(x, x') \in X \times X \, | \, x = x'\}$. Given $x \in \mathbb{R}^n$ and $A \subseteq \mathbb{R}^n$, $\|x\|$ is the Euclidean norm of x, and $\|x\|_A$ is the Euclidean distance between x and A defined by $\|x\|_A = \inf_{x' \in A} \|x - x'\|$.

A. Transition systems.

In this paper, we consider the general framework of transition systems (see e.g. [21]):

Definition 1: A *transition system* Σ is a tuple (X, U, F), where X is a set of states, U is a set of control inputs, $F \subseteq X \times U \times X$ is a transition relation. Σ is *finite* if X and U are finite sets.

A transition $(x, u, x^+) \in F$ is also denoted by $x^+ \in F(x, u)$. An input $u \in U$ is called *enabled* at $x \in X$ if $F(x, u) \neq \emptyset$. Let $\text{enab}_F(x) \subseteq U$ denote the set of all inputs enabled at x. If $\text{enab}_F(x) = \emptyset$, then the state x is called *blocking*, otherwise it is *non-blocking*. The set of non-blocking states is denoted by nbs_F.

Within the framework of transition systems, we consider memoryless state-feedback controllers:

Definition 2: A *controller* for system $\Sigma = (X, U, F)$ is a set-valued map $C : X \to 2^U$ such that $C(x) \subseteq \text{enab}_F(x)$, for all $x \in X$.

The *domain* of C is $\text{dom}(C) = \{x \in X | \, C(x) \neq \emptyset\}$. Given a system and a controller, we can define closed-loop trajectories as follows:

Definition 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

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

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

We then define closed-loop reachable sets and closed-loop attractor sets as follows:

Definition 4: Given a set of states $X^0 \subseteq X$, the *closed-loop reachable set* of system Σ with controller C from X^0 is

$$\text{reach}(\Sigma, C, X^0) = \left\{ x \in X \middle| \begin{array}{c} \exists (x_t)_{t=0}^T \in \mathscr{T}(\Sigma, C, x_0), T \in \mathbb{N} \\ \text{such that } x_0 \in X^0 \text{ and } x_T = x \end{array} \right\}.$$

Definition 5: Given a set of states $X^0 \subseteq X$, the *closed-loop attractor set* of system Σ with controller C from X^0 is

$$\text{attr}(\Sigma, C, X^0) = \bigcap_{\tau \in \mathbb{N}} \left\{ x \in X \middle| \begin{array}{c} \exists (x_t)_{t=0}^T \in \mathscr{T}(\Sigma, C, x_0), T \geq \tau \\ \text{such that } x_0 \in X^0 \text{ and } x_T = x \end{array} \right\}.$$

We also define the notion of controlled invariant set:

Definition 6: A set of states $X^0 \subseteq X$ is a *controlled invariant set* of system Σ if there exists a controller C such that for all $x_0 \in X^0$, all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy $x_t \in X^0$, for all $t \geq 0$.

It is well-known (see e.g. [4], [21]) that X^0 is a controlled invariant set if and only if for all $x \in X^0$, there exists $u \in \text{enab}_F(x)$ such that $F(x, u) \subseteq X^0$. We state the following instrumental result relating closed-loop reachable/attractor sets and controlled invariant sets.

Lemma 1: Let $X^0 \subseteq X$ and a controller C, then

(i) $\forall x \in \text{reach}(\Sigma, C, X^0) \cap \text{dom}(C), \forall u \in C(x), \; F(x, u) \subseteq \text{reach}(\Sigma, C, X^0)$.

(ii) $\forall x \in \text{attr}(\Sigma, C, X^0) \cap \text{dom}(C), \; \forall u \in C(x), \; F(x, u) \subseteq \text{attr}(\Sigma, C, X^0)$.

Moreover, if for all $x_0 \in X^0$, all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ are complete, then $\text{reach}(\Sigma, C, X^0)$ and $\text{attr}(\Sigma, C, X^0)$ are controlled invariant sets of Σ.

Proof: Let us prove assertion (i). Let $x \in \text{reach}(\Sigma, C, X^0) \cap \text{dom}(C)$, then there exists $(z_t)_{t=0}^T \in \mathscr{T}(\Sigma, C, z_0)$, $T \in \mathbb{N}$, with $z_0 \in X^0$ and $z_T = x$. Let $u \in C(x)$ and $x^+ \in F(x, u)$, then $(z_t)_{t=0}^{T+1} \in \mathscr{T}(\Sigma, C, z_0)$ with $z_{T+1} = x^+$. Therefore, $x^+ \in \text{reach}(\Sigma, C, X^0)$ and (i) holds.

To prove (ii), let $x \in \text{attr}(\Sigma, C, X^0) \cap \text{dom}(C)$, then for all $\tau \in \mathbb{N}$, there exists $(z_t)_{t=0}^T \in \mathscr{T}(\Sigma, C, z_0)$, $T \geq \tau$, with $z_0 \in X^0$ and $z_T = x$. Let $u \in C(x)$ and $x^+ \in F(x, u)$, then $(z_t)_{t=0}^{T+1} \in \mathscr{T}(\Sigma, C, z_0)$, $T + 1 \geq \tau$, with $z_0 \in X^0$ and $z_{T+1} = x^+$. Then, $x^+ \in \text{attr}(\Sigma, C, X^0)$ and (ii) holds.

Now, let us assume that for all $x_0 \in X^0$, all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ are complete. Then, $\text{reach}(\Sigma, C, X^0) \cap \text{dom}(C) = \text{reach}(\Sigma, C, X^0)$ and $\text{attr}(\Sigma, C, X^0) \cap \text{dom}(C) = \text{attr}(\Sigma, C, X^0)$ hold. Therefore, it follows from (i) and (ii) that $\text{reach}(\Sigma, C, X^0)$ and $\text{attr}(\Sigma, C, X^0)$ are controlled invariant sets of Σ. ■

A feedback refinement relation [16] is a formal behavioral relationship between two transition systems Σ_a and Σ_b, which guarantees that a controller designed for Σ_b can be also used for Σ_a.

Definition 7: Given two transition systems $\Sigma_a = (X_a, U_a, F_a)$ and $\Sigma_b = (X_b, U_b, F_b)$ with $U_b \subseteq U_a$. A relation $R \subseteq X_a \times X_b$ is a *feedback refinement relation* from Σ_a to Σ_b if for all $x_a \in X_a$, there exists $x_b \in X_b$ such that $(x_a, x_b) \in R$ and the following hold for all $(x_a, x_b) \in R$:

$$\begin{aligned} &\text{enab}_{F_b}(x_b) \subseteq \text{enab}_{F_a}(x_a);\\ &u \in \text{enab}_{F_b}(x_b) \Longrightarrow R(F_a(x_a,u)) \subseteq F_b(x_b,u). \end{aligned}$$

In this paper, we consider transition systems with a particular hierarchical structure:

Definition 8: Given a system $\Sigma = (X, U, F)$, a *nested sequence of subsystems* of Σ is a family of systems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ with $\Sigma_\alpha = (X, U, F_\alpha)$, $N \in \mathbb{N}$, and such that

- $\Sigma_N = \Sigma$ and
- the identity relation I_X is a feedback refinement relation from Σ_α to $\Sigma_{\alpha+1}$ for all $\alpha \in \mathbb{N}_{<N}$.

In other words, a nested sequence of subsystems satisfies for all $x \in X$ and $\alpha \in \mathbb{N}_{<N}$:

$$\begin{aligned} &\text{enab}_{F_{\alpha+1}}(x) \subseteq \text{enab}_{F_\alpha}(x);\\ &u \in \text{enab}_{F_{\alpha+1}}(x) \Longrightarrow F_\alpha(x,u) \subseteq F_{\alpha+1}(x,u). \end{aligned}$$

Thus, higher values of α correspond to fewer enabled inputs and increased non-determinism of the transition relation F_α. Intuitively, $\alpha \in \mathbb{N}_{\leq N}$ can be thought about as a level of disturbance, $\alpha = 0$ corresponding to the minimal level (i.e. the nominal behavior) and $\alpha = N$ corresponding to the maximal level of disturbance.

Then, given a trajectory $(x_t)_{t=0}^T \in \mathscr{T}(\Sigma, C, x_0)$, the associated *level of disturbances* is the sequence $(\alpha_t)_{t=0}^{T-1}$ defined for all $t \in \mathbb{N}_{<T}$ by

$$\alpha_t = \min\{\, \alpha \in \mathbb{N}_{\leq N} | \, \exists u_t \in C(x_t), \text{ such that } x_{t+1} \in F_\alpha(x_t, u_t)\}. \quad (1)$$

The goal of this paper is to synthesize safety and attractivity controllers which can optimally adapt their performance to the level of disturbances. Note that the level of disturbances is assumed to be time-varying and unknown to the controller.

B. least violating input-to-state safety and attractivity

Consider a finite transition system $\Sigma = (X, U, F)$ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ of Σ and a reference set $X^* \subseteq X$. Let $H : X \to \mathbb{R}_{\geq 0}$ be a function such that $H(x) = 0$ if and only if $x \in X^*$. An example of such function is given by

$$H(x) = \min_{x' \in X^*} d(x, x')$$

where d is a metric on X.

In this paper, we are interested in designing controllers for safety and (uniform) attractivity specifications. The problem of synthesizing least violating controllers for such specifications has been considered in [5]. A least violating safety controller for Σ is a controller C that keeps the trajectories of Σ as close as possible to the reference set X^*. In contrast, a least violating attractivity controller for Σ is a controller C that drives and then keeps the trajectories of Σ as close as possible to X^*. In this paper, we want to synthesize least violating controllers which additionally adapt their performance to the level of disturbances by enforcing an input-to-state safety or attractivity property.

To define formally the problem under consideration, let us introduce *gain functions*, which are non-decreasing maps from $\mathbb{N}_{\leq N}$ to $\mathbb{R}_{\geq 0}$. The set of gain functions is denoted Γ_N. In this paper, Γ_N is equipped with the *colexicographic order* $\preceq$ defined as follows. For $\gamma_1, \gamma_2 \in \Gamma_N$, we write $\gamma_1 \prec \gamma_2$ if there exists $k \in \mathbb{N}_{\leq N}$ such that $\gamma_1(k) < \gamma_2(k)$ and for all $l \in \mathbb{N}_{\leq N}$ with $l > k$, $\gamma_1(l) = \gamma_2(l)$. Then, we note $\gamma_1 \preceq \gamma_2$ if $\gamma_1 \prec \gamma_2$ or if $\gamma_1 = \gamma_2$. The colexicographic order is a total order on Γ_N. We can now define the notions of least violating input to state safety and attractivity controllers.

Definition 9: Let us consider a finite transition system Σ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. A controller C is an *input-to-state safety controller* if there exist:

- a non-empty set of initial states $X_C^0 \subseteq X$;
- a gain function $\gamma_C \in \Gamma_N$;

such that for all $x_0 \in X_C^0$, all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy

$$H(x_0) \leq \gamma_C(0) \text{ and } \forall t \geq 1,\, H(x_t) \leq \gamma_C\Big(\max_{0 \leq s < t} \alpha_s\Big) \quad (2)$$

where $(\alpha_t)_{t=0}^{T-1}$ is the level of disturbances given by (1) associated to $(x_t)_{t=0}^T$. We say that C is an ISSf controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

In addition, C is *least violating* if there is a gain function γ_C satisfying (2) such that for any other input-to-state safety controller C', it holds $\gamma_C \preceq \gamma_{C'}$. We say that C is a LV-ISSf controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

Definition 10: Let us consider a finite transition system Σ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. A controller C is an *input-to-state attractivity controller* if there exist:

- a non-empty set of initial states $X_C^0 \subseteq X$;
- a time bound $T_C \in \mathbb{N}_{>0}$;
- a gain function $\gamma_C \in \Gamma_N$;

such that for all $x_0 \in X_C^0$, all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ are complete and satisfy

$$\forall t \geq T_C,\, H(x_t) \leq \gamma_C\Big(\max_{t - T_C \leq s < t} \alpha_s\Big) \quad (3)$$

where $(\alpha_t)_{t=0}^{T-1}$ is the level of disturbances given by (1) associated to $(x_t)_{t=0}^T$. We say that C is an ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

In addition, C is *least violating* if there is a gain function γ_C satisfying (3) such that for any other input-to-state attractivity controller C', it holds $\gamma_C \preceq \gamma_{C'}$. We say that C is a LV-ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

Remark 1: In this paper, we deal with finite time attractivity. Since Σ is a finite transition system, it is straightforward to show that finite time and asymptotic attractivity are equivalent. Also, it should be noticed that we deal with uniform attractivity as the time bound T_C is valid for all maximal trajectories. Note that even for finite transition systems, there is a difference between uniform attractivity and (non-uniform) attractivity (see [5] for more details).

Following Definitions 9 and 10, it is important to emphasize the following features of LV-ISSf and LV-ISA controllers:

- The fact that these controllers are defined using the colexicographic order induces that the primarily objective is to minimize the input-to-state gain for the worst case disturbances, that is $\gamma(N)$, and then try to minimize the gains for lower levels of disturbances, i.e. $\gamma(N-1),\ldots,\gamma(0)$ in that order. A consequence is that a LV-ISSf or a LV-ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ is also a least violating safety or a least violating attractivity controller for Σ in the sense of [5].
- It is generally not required that $\gamma(0) = 0$, which allows us to deal with cases when the reference set X^* cannot be made safe or attractive, even in the nominal case, the objective being to stay as close as possible to X^*.
- A fundamental difference between the notions of LV-ISSf and LV-ISA controllers is that while in (2) the bound on $H(x_t)$ depends on all past values of the disturbance levels, in (3) it

only depends on the past values of the disturbance levels over the last T_C time steps, where T_C is a finite time bound. Hence, LV-ISA controllers are more resilient than LV-ISSf controllers since when the disturbance level decreases and remains at the minimal level, the nominal behavior is restored in finite time for the former but not for the latter.

In the following sections, we present a computational approach for synthesizing LV-ISSf and LV-ISA controllers for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$. In the remaining of the paper, we will make the following assumption:

Assumption 1: There exists a controller C and an initial state x_0 such that all maximal trajectories $(x_t)_{t=0}^{T} \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ are complete.

It is clear that if Assumption 1 does not hold then there does not exists any ISSf nor ISA controllers, so it is pointless to try to synthesize such controllers. We will provide in the following an algorithm to check Assumption 1. Assumption 1 also guarantees the existence of LV-ISSf and of LV-ISA controllers.

Theorem 1: Under Assumption 1, there exist a LV-ISSf controller and a LV-ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$.

Proof: Let us consider a controller C as in Assumption 1. Consider the set of initial states $X_c^0 = \{x_0\}$ and the gain function given for all $k \in \mathbb{N}_{\leq N}$, by $\gamma_c(k) = \max_{x\in X} H(x)$. Then (2) holds and therefore C is an ISSf controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$. Moreover, (3) holds for the time bound $T_C = 1$ and therefore C is also an ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$. So the sets of ISSf and ISA controllers are both non-empty.

To show the existence of LV-ISSf controllers, let us remark that since Σ is finite there exist only finitely many controllers for Σ. There are only finitely many subsets of X. Also, for any controller C and set of initial states X_C^0 such that all maximal trajectories $(x_t)_{t=0}^{T} \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ with $x_0 \in X_C^0$ are complete, the minimal (with respect to $\preceq$) gain function such that (2) holds has values in $H(X)$, which is a finite set. Hence, there are finitely many candidates (C, X_C^0, γ_C) for the LV-ISSf controller. From existence of an ISSf controller, we know that the set of candidates is also not-empty. Then, the LV-ISSf controller exists and can be obtained by selecting from this set of candidates a triple with minimal γ_C with respect to the total order $\preceq$.

For showing the existence of LV-ISA controllers, we use similar arguments to show the finiteness of possible C, X_C^0 and γ_C. However, we additionally need to show that it is sufficient to consider time bounds $T_C \leq |X|+1$. Let C be an ISA controller with set of initial states X_C^0, time bound T_C, and gain function γ_C. Let us assume that $T_C > |X|+1$, we want to show that (3) holds for time bound $T_C' = |X|+1$. Hence, let $(x_t)_{t=0}^{+\infty} \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ with $x_0 \in X_C^0$ and let $(\alpha_t)_{t=0}^{+\infty}$ be the associated the level of disturbances. Let $\tau \geq T_C' = |X|+1$, then there exists $\tau - T_C' \leq s_1 < s_2 < \tau$ such that $x_{s_1} = x_{s_2}$. Let $l = s_1 - s_2$ and $m \in \mathbb{N}_{>0}$ such that $T_C' + ml \geq T_C$. Consider the sequence $(\tilde{x}_t)_{t=0}^{+\infty}$ given by

$$\begin{cases} \tilde{x}_t &= x_t, & t = 0,\dots,s_1; \\ \tilde{x}_{s_1+kl+s} &= x_{s_1+s}, & s = 1,\dots,l;\ k = 0,\dots,m-1; \\ \tilde{x}_t &= x_{t-ml} & t \geq s_1 + ml + 1. \end{cases} \tag{4}$$

Then, it can be easily checked that $(\tilde{x}_t)_{t=0}^{+\infty} \in \mathscr{T}_{\max}(\Sigma, C, x_0)$ and that the associated level of disturbances $(\tilde{\alpha}_t)_{t=0}^{+\infty}$ can be defined from $(\alpha_t)_{t=0}^{+\infty}$ in the same way as in (4). By construction of the sequences $(\tilde{x}_t)_{t=0}^{+\infty}$ and $(\tilde{\alpha}_t)_{t=0}^{+\infty}$, we obtain $x_\tau = \tilde{x}_{\tau+ml}$ and

$$\max_{\tau+ml-T_C\leq s<\tau+ml} \tilde{\alpha}_s \leq \max_{\tau-T_C'\leq s<\tau} \alpha_s.$$

Then, it follows from above and from (3) that

$$\begin{aligned} H(x_\tau) &= H(\tilde{x}_\tau) \\ &\leq \gamma_C\Big(\max_{\tau+ml-T_C\leq s<\tau+ml} \tilde{\alpha}_s\Big) \\ &\leq \gamma_C\Big(\max_{\tau-T_C'\leq s<\tau} \alpha_s\Big). \end{aligned}$$

Therefore, one can always find a time bound $T_C \leq |X|+1$. It follows that there are finitely many candidates $(C, X_C^0, T_C, \gamma_C)$ for the LV-ISA controller. From existence of an ISA controller, we know that the set of candidates is also not-empty. Then, the LV-ISA controller exists and can be obtained by selecting from this set of candidates one with minimal γ_C with respect to the total order $\preceq$. ■

Remark 2: In this paper, we deal with controllers that are least violating with respect to the colexicographic order. However, similar to Definitions 9 and 10, one can define LV-ISSf and LV-ISA controllers for other ordering relations on Γ_N. Actually, it follows from the proof of Theorem 1 that LV-ISSf and LV-ISA controllers also exist for any total preorder $\preceq_*$ on Γ_N satisfying for all $\gamma_1, \gamma_2 \in \Gamma_N$:

$$\forall k \in \mathbb{N}_{\leq N}, \gamma_1(k) \leq \gamma_2(k) \implies \gamma_1 \preceq_* \gamma_2.$$

Examples of such total preorders on Γ_N are as follows:

- *Lexicographic order* $\preceq_{lex}$: for $\gamma_1, \gamma_2 \in \Gamma_N$, we write $\gamma_1 \prec_{lex} \gamma_2$ if there exists $k \in \mathbb{N}_{\leq N}$ such that $\gamma_1(k) < \gamma_2(k)$ and for all $l \in \mathbb{N}_{\leq N}$ with $l < k$, $\gamma_1(l) = \gamma_2(l)$. Then, we note $\gamma_1 \preceq_{lex} \gamma_2$ if $\gamma_1 \prec_{lex} \gamma_2$ or if $\gamma_1 = \gamma_2$.
- *Summation order* $\preceq_{sum}$: for $\gamma_1, \gamma_2 \in \Gamma_N$, we write $\gamma_1 \preceq_{sum} \gamma_2$ if $\gamma_1(0) + \cdots + \gamma_1(N) \leq \gamma_2(0) + \cdots + \gamma_2(N)$.

III. Synthesis of LV-ISSf controllers

In this section, we present an approach to synthesize LV-ISSf controllers. The approach consists of two main steps: firstly we synthesize a least violating safety controller for Σ following the approach in [5]; secondly the controller is iteratively refined into a LV-ISSf controller using the nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$.

A. Synthesis of least violating safety controllers

We briefly recall the main results of [5] on synthesis of least violating safety controllers for a transition system $\tilde{\Sigma} = (X, U, \tilde{F})$. Let us consider the following dynamic programming fixed-point iteration:

$$W_S^0(x) = H(x), \tag{5}$$

$$W_S^{k+1}(x) = \begin{cases} \max\left(H(x), \min\limits_{u\in \mathrm{enab}_{\tilde{F}}(x)} \max\limits_{x^+\in\tilde{F}(x,u)} W_S^k(x^+)\right) & \\ \qquad\qquad \text{if } x \in \mathrm{nbs}_{\tilde{F}}; & \\ +\infty \qquad\qquad \text{if } x \notin \mathrm{nbs}_{\tilde{F}} \end{cases} \tag{6}$$

for $x \in X$, $k \in \mathbb{N}$. We denote the fixed-point of (5), (6) by W_S^*. It can be shown that for finite transition systems, there exists $K \in \mathbb{N}$ such that for all $k \geq K$, for all $x \in X$, $W_S^k(x) = W_S^*(x)$.

A least violating safety (LV-Sf) controller $C : X \to 2^U$ for the system $\tilde{\Sigma}$, which keeps trajectories as close as possible to the reference set $X^* \subseteq X$, is given for all $x \in X$ by:

$$C(x) = \left\{ u \in \mathrm{enab}_{\tilde{F}}(x) \,\middle|\, \max_{x^+\in\tilde{F}(x,u)} W_S^*(x^+) \leq W_S^*(x) \right\} \tag{7}$$

It is worth noting that C is a set valued-controller that may enable more than one input at a given state. Moreover, considering (6) for $k \geq K$, we get that $\mathrm{dom}(C) = \mathrm{nbs}_{\tilde{F}}$. The next result is a direct consequence of Theorem 3.2 in [5] and is stated without proof.

Proposition 1 (Theorem 3.2 in [5]): For all $\beta \in \mathbb{R}_{\geq 0}$, for all $x_0 \in X$, it holds that $W_S^*(x_0) \leq \beta$ if and only if there exists a controller C such that all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\tilde{\Sigma}, C, x_0)$ are complete and satisfy

$$\forall t \geq 0,\ H(x_t) \leq \beta.$$

Moreover, for all $x_0 \in L_\beta(W_S^*)$, such a controller C is given by (7).

Let us remark that Proposition 1 implies that for any $X^0 \subseteq L_\beta(H)$, such that X^0 is a controlled invariant set of Σ, it holds $X^0 \subseteq L_\beta(W_S^*)$. Another consequence of Proposition 1 is that Assumption 1 is a necessary and sufficient condition for W_S^* to have finite values.

Corollary 1: There exists $x \in X$ such that $W_S^*(x) < +\infty$ if and only if Assumption 1 holds for system $\tilde{\Sigma}$.

Proof: Let us assume that Assumption 1 holds. Then, there exists a controller C and a state x_0 such that all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\tilde{\Sigma}, C, x_0)$ are complete. Moreover,

$$\forall t \geq 0,\ H(x_t) \leq \max_{x \in X} H(x).$$

Then, from Proposition 1, $W_S^*(x_0) \leq \max_{x \in X} H(x) < +\infty$ where the last inequality follows from X being a finite set.

For the converse result, let us assume that there exists $x_0 \in X$ such that $W_S^*(x_0) < +\infty$. Let C be given by (7), then it follows from Proposition 1 that all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\tilde{\Sigma}, C, x_0)$ are complete. ∎

Let us remark that the previous result provides an algorithm to check whether Assumption 1 holds.

B. Input-to-state safety via refinements

We present an approach to synthesize a LV-ISSf controller for a system Σ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. The approach is based on iterative refinements of least violating safety controllers.

Let us define $X_{N+1}^0 = X$ and $C_{N+1}(x) = \mathrm{enab}_{F_N}(x)$, for all $x \in X$. Then, let us consider the following iterative refinement procedure. For $\alpha \in \mathbb{N}_{\leq N}$, let $\Sigma_\alpha^c = (X, U, F_\alpha^c)$ where F_α^c is defined by

$$F_\alpha^c(x,u) = \begin{cases} F_\alpha(x,u) & \text{if } u \in C_{\alpha+1}(x); \\ \emptyset & \text{if } u \notin C_{\alpha+1}(x) \end{cases} \tag{8}$$

Intuitively Σ_α^c describes the dynamics of Σ_α constrained by the controller $C_{\alpha+1}$ (note that $\Sigma_N^c = \Sigma_N = \Sigma$). Then, let $W_{S,\alpha}^*$ and C_α be given by (5)-(6) and by (7) for the system $\tilde{\Sigma} = \Sigma_\alpha^c$, and let

$$\beta_\alpha = \min_{x \in X_{\alpha+1}^0} W_{S,\alpha}^*(x),\ X_\alpha^0 = L_{\beta_\alpha}(W_{S,\alpha}^*) \cap X_{\alpha+1}^0. \tag{9}$$

Intuitively, C_N corresponds to the LV-Sf controller for Σ given by (7) and thus guarantees the minimal deviation from X^* for the worst case disturbances. Then, for $\alpha \in \mathbb{N}_{<N}$, C_α is a refinement of $C_{\alpha+1}$ aiming at improving the performances of the closed-loop system for the level of disturbance α. Let us prove the following instrumental properties:

Lemma 2: The following assertions hold:

(i) $\forall \alpha \in \mathbb{N}_{\leq N},\ \forall x \in X,\ C_\alpha(x) \subseteq C_{\alpha+1}(x)$;
(ii) $\forall \alpha \in \mathbb{N}_{\leq N},\ \forall x \in X,\ \mathrm{enab}_{F_\alpha^c}(x) = C_{\alpha+1}(x)$;
(iii) $\forall \alpha \in \mathbb{N}_{\leq N},\ X_\alpha^0 \neq \emptyset$ and $X_\alpha^0 \subseteq X_{\alpha+1}^0$;
(iv) $\forall \alpha \in \mathbb{N}_{\leq N},\ X_\alpha^0 = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0)$;
(v) $\forall \alpha \in \mathbb{N}_{<N},\ \forall x \in X_{\alpha+1}^0,\ W_{S,\alpha}^*(x) \leq \beta_{\alpha+1}$;
(vi) $\forall \alpha \in \mathbb{N}_{\leq N},\ \mathrm{dom}(C_\alpha) = \mathrm{nbs}_{F_N}$.

Proof: Let us prove the different assertions above.

(i): Let $x \in X$, from (7) we have $C_\alpha(x) \subseteq \mathrm{enab}_{F_\alpha^c}(x)$, and from (8), we have $\mathrm{enab}_{F_\alpha^c}(x) \subseteq C_{\alpha+1}(x)$.

(ii): Let $x \in X$, we have $C_{\alpha+1}(x) \subseteq \mathrm{enab}_{F_{\alpha+1}^c}(x)$ by (7) and $\mathrm{enab}_{F_{\alpha+1}^c}(x) \subseteq \mathrm{enab}_{F_{\alpha+1}}(x)$ by (8). Moreover, by Definition 8, we have $\mathrm{enab}_{F_{\alpha+1}}(x) \subseteq \mathrm{enab}_{F_\alpha}(x)$. Therefore, $C_{\alpha+1}(x) \subseteq \mathrm{enab}_{F_\alpha}(x)$. By (8), we have $\mathrm{enab}_{F_\alpha^c}(x) = \mathrm{enab}_{F_\alpha}(x) \cap C_{\alpha+1}(x)$ and hence $\mathrm{enab}_{F_\alpha^c}(x) = C_{\alpha+1}(x)$.

(iii): Let us remark that $X_{N+1}^0 = X$ is non-empty. Then, from (9), we obtain assertion (iii) by induction.

(iv): We proceed by induction. By the second equality in (9), we get that $X_N^0 = L_{\beta_N}(W_{S,N}^*)$. Then, it follows from (7) that $X_N^0 = \mathrm{reach}(\Sigma_N, C_N, X_N^0)$. Then, let us assume that for some $\alpha \in \mathbb{N}_{<N}$, $X_{\alpha+1}^0 = \mathrm{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X_{\alpha+1}^0)$. Then, from Definition 8, (i) and (iii), we get that $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0) \subseteq \mathrm{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X_{\alpha+1}^0)$. Hence, $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0) \subseteq X_{\alpha+1}^0$, by the induction hypothesis. Moreover, from the second equality in (9), $X_\alpha^0 \subseteq L_{\beta_\alpha}(W_{S,\alpha}^*)$. Then, it follows from (7) that $\mathrm{reach}(\Sigma_\alpha^c, C_\alpha, X_\alpha^0) \subseteq L_{\beta_\alpha}(W_{S,\alpha}^*)$. From (i) and (8), we get that $\mathrm{reach}(\Sigma_\alpha^c, C_\alpha, X_\alpha^0) = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0)$. Hence, it follows that $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0) \subseteq L_{\beta_\alpha}(W_{S,\alpha}^*) \cap X_{\alpha+1}^0$. Then, by the second equality in (9), we get $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0) \subseteq X_\alpha^0$. We always have the converse inclusion $X_\alpha^0 \subseteq \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0)$ and therefore $X_\alpha^0 = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^0)$.

(v): Consider $\alpha \in \mathbb{N}_{<N}$, $x_0 \in X_{\alpha+1}^\infty$ and let us assume that $\beta_{\alpha+1} < +\infty$. From (ii), we can consider $C_{\alpha+1}$ as a controller for Σ_α^c. Then, let us consider a maximal trajectory $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha^c, C_{\alpha+1}, x_0)$. By (8) and Definition 8 we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}^c, C_{\alpha+1}, x_0)$. By the second equality in (9) we get that $W_{S,\alpha+1}^*(x_0) \leq \beta_{\alpha+1}$. Then, from Proposition 1 applied to $\Sigma_{\alpha+1}^c$, $(x_t)_{t=0}^T$ is complete and for all $t \geq 0$, $H(x_t) \leq \beta_{\alpha+1}$. From Proposition 1 applied this time to Σ_α^c, we get that $W_{S,\alpha}^*(x_0) \leq \beta_{\alpha+1}$. Clearly, this inequality holds also if $\beta_{\alpha+1} = +\infty$ and thus (v) is proved.

(vi): Let us consider $\alpha \in \mathbb{N}_{\leq N}$. From (ii), we have $\mathrm{dom}(C_{\alpha+1}) = \mathrm{nbs}_{F_\alpha^c}$. From (6), (7), we get that $\mathrm{dom}(C_\alpha) = \mathrm{nbs}_{F_\alpha^c}$. Hence, $\mathrm{dom}(C_\alpha) = \mathrm{dom}(C_{\alpha+1})$. Then, for all $\alpha \in \mathbb{N}_{\leq N}$, $\mathrm{dom}(C_\alpha) = \mathrm{dom}(C_{N+1}) = \mathrm{nbs}_{F_N^c} = \mathrm{nbs}_{F_N}$, because $F_N^c = F_N$. ∎

Under Assumption 1, we get the following additional property:

Lemma 3: Under Assumption 1 for system Σ, the following assertion holds:

(vii) $\forall \alpha \in \mathbb{N}_{\leq N},\ \beta_\alpha < +\infty$ and $\forall \alpha \in \mathbb{N}_{<N},\ \beta_\alpha \leq \beta_{\alpha+1}$.

Proof: Under Assumption 1, we get from Corollary 1 and the first equality in (9) that $\beta_N < +\infty$. Then for $\alpha \in \mathbb{N}_{<N}$, we have from (iii) and (v) in Lemma 2 that

$$\beta_\alpha = \max_{x \in X_{\alpha+1}^0} W_{S,\alpha}^*(x) \leq \beta_{\alpha+1}.$$

Thus, (vii) is proved. ∎

We can now state the main result of the section:

Theorem 2: Under Assumption 1 for system Σ, the controller $C = C_0$ is a LV-ISSf controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ with associated set of initial states $X_C^0 = X_0^0$ and gain function γ_C given by

$$\forall \alpha \in \mathbb{N}_{\leq N},\ \gamma_C(\alpha) = \beta_\alpha. \tag{10}$$

Moreover, for any other LV-ISSf controller C' with associated set of initial states $X_{C'}^0$ and gain function $\gamma_{C'}$ it holds $\gamma_{C'} = \gamma_C$, $X_{C'}^0 \subseteq X_C^0$, and $C'(x) \subseteq C(x)$, for all $x \in \mathrm{reach}(\Sigma_0, C', X_{C'}^0)$.

Proof: From (iii) in Lemma 2, we have $X_C^0 = X_0^0 \neq \emptyset$. Also from (vii) in Lemma 3, we get that γ_C is a non-decreasing function.

Let $x_0 \in X_C^0$, then from the second equality in (9), $W_{S,0}^*(x_0) \leq \beta_0$. From (6), we get that $H(x_0) \leq W_{S,0}^*(x_0)$. Hence, $H(x_0) \leq \beta_0$. Now, let $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$, then from (i) and (vi) in Lemma 2 and (8) we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_N^c, C_N, x_0)$. By (iii) in Lemma 2, $x_0 \in X_N^0$, then, it follows from (9) that $W_{S,N}^*(x_0) \leq \beta_N$. By (vii) in Lemma 3,

$\beta_N < +\infty$. Then, from Proposition 1, $(x_t)_{t=0}^{T}$ is complete and for all $t \in \mathbb{N}$, $H(x_t) \leq \beta_N$. Let $(\alpha_t)_{t=0}^{T-1}$ be the level of disturbances associated to $(x_t)_{t=0}^{T}$. Let $t \in \mathbb{N}$ and let $\bar{\alpha} = \max_{0 \leq s < t} \alpha_s$. Then, from (i) in Lemma 2 and (8), $(x_s)_{s=0}^{t} \in \mathscr{T}(\Sigma_{\bar{\alpha}}^{c}, C_{\bar{\alpha}}, x_0)$. By (iii) in Lemma 2, $x_0 \in X_{\bar{\alpha}}^{0}$, then, it follows from (9) that $W_{S,\bar{\alpha}}^{*}(x_0) \leq \beta_{\bar{\alpha}}$. By (vii) in Lemma 3, $\beta_{\bar{\alpha}} < +\infty$. Then, from Proposition 1, we get that $H(x_t) \leq \beta_{\bar{\alpha}}$. Therefore C is an ISSf controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

Let C' be a LV-ISSf controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. Let us prove by induction on α, that for all $\alpha \in \mathbb{N}_{\leq N}$:

$$\begin{aligned} &\gamma_{C'}(\alpha) = \beta_\alpha, \\ &X_{C'}^{0} \subseteq X_\alpha^{0}, \\ &C'(x) \subseteq C_\alpha(x),\ \forall x \in \mathrm{reach}(\Sigma_\alpha, C', X_{C'}^{0}). \end{aligned} \tag{11}$$

We start with the case $\alpha = N$. Since C' is an ISSf controller, it follows from Proposition 1 that $X_{C'}^{0} \subseteq L_{\gamma_{C'}(N)}(W_{S,N}^{*})$. Then, since $X_{C'}^{0} \neq \emptyset$ and by the first equality in (9), we get that $\beta_N \leq \gamma_{C'}(N)$. Moreover, since C' is a LV-ISSf controller, we also have $\beta_N \geq \gamma_{C'}(N)$, which gives $\beta_N = \gamma_{C'}(N)$. Hence, $X_{C'}^{0} \subseteq L_{\beta_N}(W_{S,N}^{*}) = X_N^{0}$ by the second equality in (9). Since C' is an ISSf controller we have $\mathrm{reach}(\Sigma_N, C', X_{C'}^{0}) \subseteq L_{\gamma_{C'}(N)}(H)$. Moreover from Lemma 1, we get that $\mathrm{reach}(\Sigma_N, C', X_{C'}^{0})$ is a controlled invariant of Σ_N. Hence, it follows from Proposition 1 that $\mathrm{reach}(\Sigma_N, C', X_{C'}^{0}) \subseteq L_{\gamma_{C'}(N)}(W_{S,N}^{*})$. From $\gamma_{C'}(N) = \beta_N$ we get that $\mathrm{reach}(\Sigma_N, C', X_{C'}^{0}) \subseteq L_{\beta_N}(W_{S,N}^{*})$. Then, let $x \in \mathrm{reach}(\Sigma_N, C', X_{C'}^{0})$ and $u \in C'(x)$, then by (i) in Lemma 1, $F_N(x,u) \subseteq \mathrm{reach}(\Sigma_N, C', X_{C'}^{0}) \subseteq L_{\beta_N}(W_{S,N}^{*})$. Moreover $W_{S,N}^{*}(x) \leq \beta_N$, then $u \in C_N(x)$ by (7). Therefore, (11) holds for $\alpha = N$.

Now let $\alpha \in \mathbb{N}_{<N}$, and let us assume that (11) holds for $\alpha + 1$. We show that (11) holds for α. Since C' is an ISSf controller, it follows from Proposition 1 that $X_{C'}^{0} \subseteq L_{\gamma_{C'}(\alpha)}(W_{S,\alpha}^{*})$. Moreover, $X_{C'}^{0} \neq \emptyset$ and $X_{C'}^{0} \subseteq X_{\alpha+1}^{0}$ by the induction hypothesis. Then, by the first equality in (9), we get that $\beta_\alpha \leq \gamma_{C'}(\alpha)$. Moreover, since C' is a LV-ISSf controller, we also have $\beta_\alpha \geq \gamma_{C'}(\alpha)$, which gives $\beta_\alpha = \gamma_{C'}(\alpha)$. Hence, $X_{C'}^{0} \subseteq L_{\beta_\alpha}(W_{S,\alpha}^{*}) \cap X_{\alpha+1}^{0} = X_\alpha^{0}$ by the second equality in (9). The proof that $C'(x) \subseteq C_\alpha(x)$, for all $x \in \mathrm{reach}(\Sigma_\alpha, C', X_{C'}^{0})$ is identical to the case $\alpha = N$. Hence, (11) holds for all $\alpha \in \mathbb{N}_{\leq N}$, which proves the Theorem. ∎

To summarize, our approach, based on iterative refinements of least violating controllers, allows us to compute a LV-ISSf controller. Moreover, we have shown that the computed controller is valid for the largest possible set of initial states and that it is maximally permissive on the reachable set of the nominal system.

IV. Synthesis of ISA controllers

In this section, we apply an approach similar to that of the previous section to synthesize ISA controllers. The obtained controller are generally not least violating. However, we provide a sufficient condition that is easily checkable a posteriori and that guarantees that synthesized controller is a LV-ISA controller.

A. Synthesis of least violating attractivity controllers

We briefly recall the main results of [5] on synthesis of least violating attractivity controllers for a transition system $\tilde{\Sigma} = (X, U, \tilde{F})$. Let W_S^{*} be the fixed point of (5), (6). Let us consider the following dynamic programming fixed-point iteration:

$$W_A^{0}(x) = W_S^{*}(x), \tag{12}$$

$$W_A^{k+1}(x) = \begin{cases} \min\left(W_S^{*}(x), \min\limits_{u \in \mathrm{enab}_{\tilde{F}}(x)} \max\limits_{x^+ \in \tilde{F}(x,u)} W_A^{k}(x^+)\right) & \\ \qquad\qquad \text{if } x \in \mathrm{nbs}_{\tilde{F}}; & \\ +\infty \qquad \text{if } x \notin \mathrm{nbs}_{\tilde{F}} \end{cases} \tag{13}$$

for $x \in X$, $k \in \mathbb{N}$. We denote the fixed-point of (12), (13) by W_A^{*}. It can be shown that for finite transition systems, there exists $K \in \mathbb{N}$ such that for all $k \geq K$, for all $x \in X$, $W_A^{k}(x) = W_A^{*}(x)$. Let the function $k^{*} : X \to \mathbb{N}$ be defined as follows for all $x \in X$

$$k^{*}(x) = \min\{k \in \mathbb{N} \,|\, W_A^{k}(x) = W_A^{*}(x)\}. \tag{14}$$

A least violating attractivity (LV-A) controller for the system $\tilde{\Sigma}$, which drives and then keeps trajectories as close as possible to the reference set $X^{*} \subseteq X$ can then be defined as follows. For $\beta \in \overline{\mathbb{R}}_{\geq 0}$, let the controller $C_\beta : X \to 2^{U}$ be given for all $x \in X$ by:

$$C_\beta(x) = \begin{cases} \arg\min\limits_{u \in \mathrm{enab}_{\tilde{F}}(x)} \left(\max\limits_{x^+ \in \tilde{F}(x,u)} W_A^{k^{*}(x)-1}(x^+)\right) & \\ \qquad\qquad \text{if } W_A^{*}(x) \leq \beta < W_S^{*}(x); & \\ \left\{u \in \mathrm{enab}_{\tilde{F}}(x) \,\middle|\, \max\limits_{x^+ \in \tilde{F}(x,u)} W_S^{*}(x^+) \leq W_S^{*}(x)\right\} & \\ \qquad\qquad \text{if } W_S^{*}(x) \leq \beta; & \\ \emptyset \qquad \text{if } \beta < W_A^{*}(x). \end{cases} \tag{15}$$

Let us remark that for $\beta < +\infty$, $\mathrm{dom}(C_\beta) = L_\beta(W_A^{*})$. The next result is a direct consequence of Proposition 3.10 and Theorem 3.11 in [5] and is stated without proof.

Proposition 2 (Proposition 3.10 and Theorem 3.11 in [5]): Let $\beta \in \mathbb{R}_{\geq 0}$, the following assertions hold:

(a) For all $x_0 \in X$, if there exist $T_{x_0} \in \mathbb{N}$ and a controller C such that all maximal trajectories $(x_t)_{t=0}^{T} \in \mathscr{T}_{\max}(\tilde{\Sigma}, C, x_0)$ are complete and satisfy
$$\forall t \geq T_{x_0},\ H(x_t) \leq \beta,$$
then $x_0 \in L_\beta(W_A^{*})$.

(b) There exists $T_0 \in \mathbb{N}$, such that for all $x_0 \in L_\beta(W_A^{*})$, all maximal trajectories $(x_t)_{t=0}^{T} \in \mathscr{T}_{\max}(\tilde{\Sigma}, C_\beta, x_0)$ are complete and satisfy
$$\forall t \geq T_0,\ H(x_t) \leq W_S^{*}(x_t) \leq \beta.$$

Let us emphasize that in (a), the time bound T_{x_0} and the controller C may depend on the initial state x_0 while in (b), the time bound T_0 and the controller C_β are valid for all $x_0 \in L_\beta(W_A^{*})$. A consequence of Proposition 2 is that Assumption 1 is a necessary and sufficient condition for W_A^{*} to have finite values.

Corollary 2: There exists $x \in X$ such that $W_A^{*}(x) < +\infty$ if and only if Assumption 1 holds for system $\tilde{\Sigma}$.

Proof: The proof is similar to that of Corollary 1 and is therefore ommitted. ∎

B. Input-to-state attractivity via refinements

We present an approach to synthesize a LV-ISA controller for a system Σ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. The approach is based on iterative refinements of least violating attractivity controllers.

Let $W_{S,N}^{*}$, $W_{A,N}^{*}$ be given by (5)-(6) and by (12)-(13) for the system $\tilde{\Sigma} = \Sigma_N$. Then, let us define

$$\beta_N = \min_{x \in X} W_{A,N}^{*}(x),\ X_N^{0} = L_{\beta_N}(W_{A,N}^{*}),\ X_N^{\infty} = L_{\beta_N}(W_{S,N}^{*}). \tag{16}$$

Let C_N be given by (15) for the system $\tilde{\Sigma} = \Sigma_N$ and $\beta = \beta_N$. Let T_N be the associated time bound as in item (b) of Proposition 2.

Note that C_N corresponds to the LV-A controller for Σ given by (15) and thus guarantees the minimal asymptotic deviation from X^{*} for the worst case disturbances. Then, for $\alpha \in \mathbb{N}_{<N}$, we define an iterative refinement procedure aiming at improving the performances of the closed-loop system for the level of disturbance α.

For $\alpha \in \mathbb{N}_{<N}$, let $\Sigma^c_\alpha = (X, U, F^c_\alpha)$ where F^c_α is defined by

$$F^c_\alpha(x,u) = \begin{cases} F_\alpha(x,u) & \text{if } u \in C_{\alpha+1}(x); \\ \emptyset & \text{if } u \notin C_{\alpha+1}(x) \end{cases} \tag{17}$$

Intuitively Σ^c_α describes the dynamics of Σ_α constrained by the controller $C_{\alpha+1}$. Let $W^*_{S,\alpha}$, $W^*_{A,\alpha}$ be given by (5)-(6) and by (12)-(13) for the system $\tilde{\Sigma} = \Sigma^c_\alpha$, and let

$$\beta_\alpha = \max_{x \in X^\infty_{\alpha+1}} W^*_{A,\alpha}(x),\ X^\infty_\alpha = L_{\beta_\alpha}(W^*_{S,\alpha}) \cap X^\infty_{\alpha+1}. \tag{18}$$

Let C_α be given by (15) for the system $\tilde{\Sigma} = \Sigma^c_\alpha$ and $\beta = \beta_\alpha$. Let T_α be the associated time bound as in item (b) of Proposition 2.

We define also the following convention $\Sigma^c_N = \Sigma_N$. We first prove the following instrumental properties:

Lemma 4: The following assertions hold:

(i) $\forall \alpha \in \mathbb{N}_{<N},\ \forall x \in X,\ C_\alpha(x) \subseteq C_{\alpha+1}(x)$;
(ii) $\forall \alpha \in \mathbb{N}_{<N},\ \forall x \in X,\ \text{enab}_{F^c_\alpha}(x) = C_{\alpha+1}(x)$;
(iii) $\forall \alpha \in \mathbb{N}_{\leq N},\ X^\infty_\alpha \neq \emptyset$ and $\forall \alpha \in \mathbb{N}_{<N},\ X^\infty_\alpha \subseteq X^\infty_{\alpha+1}$;
(iv) $\forall \alpha \in \mathbb{N}_{\leq N},\ X^\infty_\alpha = \text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha)$;
(v) $\forall \alpha \in \mathbb{N}_{<N},\ \forall x \in X^\infty_{\alpha+1},\ W^*_{A,\alpha}(x) \leq \beta_{\alpha+1}$;

Proof: The proofs of assertions (i) and (ii) are similar to that of Lemma 2. We prove the other assertions in the following.

(iii) and (iv): We proceed by induction. From (12) and (13), one can show that

$$\min_{x \in X} W^*_{S,N}(x) = \min_{x \in X} W^*_{A,N}(x) = \beta_N.$$

Hence, from the third equality in (16), we get that $X^\infty_N \neq \emptyset$. Moreover, we get by (15) and the third equality in (16) that $X^\infty_N = \text{reach}(\Sigma_N, C_N, X^\infty_N)$. Then, let us assume that for some $\alpha \in \mathbb{N}_{<N}$, $X^\infty_{\alpha+1} \neq \emptyset$ and $X^\infty_{\alpha+1} = \text{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X^\infty_{\alpha+1})$.

We first prove that $X^\infty_\alpha \neq \emptyset$. Let us first assume that $\beta_\alpha < +\infty$. Then, let $x_0 \in X^\infty_{\alpha+1}$, and let us consider a maximal trajectory $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_\alpha, x_0)$. Since $W^*_{A,\alpha}(x_0) \leq \beta_\alpha < +\infty$ by the first equality in (18), we get from item (b) in Proposition 2 applied to Σ^c_α that $(x_t)_{t=0}^T$ is complete and that for all $t \geq T_\alpha$, $W^*_{S,\alpha}(x_t) \leq \beta_\alpha$. From (17), Definition 8 and (i), we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_0)$. Then, since $X^\infty_{\alpha+1} = \text{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X^\infty_{\alpha+1})$ and $x_0 \in X^\infty_{\alpha+1}$, we get that for all $t \geq 0$, $x_t \in X^\infty_{\alpha+1}$. It follows that

$$\forall t \geq T_\alpha, x_t \in L_{\beta_\alpha}(W^*_{S,\alpha}) \cap X^\infty_{\alpha+1}.$$

This implies that $L_{\beta_\alpha}(W^*_{S,\alpha}) \cap X^\infty_{\alpha+1} \neq \emptyset$ and thus by the second equality in (18) we get that $X^\infty_\alpha \neq \emptyset$. Assuming now that $\beta_\alpha = +\infty$, we get from the second equality in (18) that $X^\infty_\alpha = X^\infty_{\alpha+1} \neq \emptyset$, by the induction hypothesis.

We now prove that $X^\infty_\alpha = \text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha)$. From Definition 8, (i) and the second equality in (18) we get that $\text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha) \subseteq \text{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X^\infty_{\alpha+1})$, which from the induction hypothesis gives $\text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha) \subseteq X^\infty_{\alpha+1}$. From the second equality in (18), we also get that $X^\infty_\alpha \subseteq L_{\beta_\alpha}(W^*_{S,\alpha})$. Then, from (15), we get that $\text{reach}(\Sigma^c_\alpha, C_\alpha, X^\infty_\alpha) \subseteq L_{\beta_\alpha}(W^*_{S,\alpha})$. From (i) and (17), we get that $\text{reach}(\Sigma^c_\alpha, C_\alpha, X^\infty_\alpha) = \text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha)$. Hence, we get that $\text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha) \subseteq L_{\beta_\alpha}(W^*_{S,\alpha}) \cap X^\infty_{\alpha+1}$. Then by the second equality in (18), we get $\text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha) \subseteq X^\infty_\alpha$. Since we always have $X^\infty_\alpha \subseteq \text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha)$, it follows that $X^\infty_\alpha = \text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha)$.

Hence, we have proved by induction that for all $\alpha \in \mathbb{N}_{\leq N}$, $X^\infty_\alpha \neq \emptyset$ and $X^\infty_\alpha = \text{reach}(\Sigma_\alpha, C_\alpha, X^\infty_\alpha)$. The fact that for all $\alpha \in \mathbb{N}_{<N}$, $X^\infty_\alpha \subseteq X^\infty_{\alpha+1}$ follows directly from the second equality in (18). Hence (iii) and (iv) are proved.

(v): Consider $\alpha \in \mathbb{N}_{<N}$, $x_0 \in X^\infty_{\alpha+1}$ and let us assume that $\beta_{\alpha+1} < +\infty$. From (ii), we can consider $C_{\alpha+1}$ as a controller for Σ^c_α. Then, let us consider a maximal trajectory $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_{\alpha+1}, x_0)$. By (17), Definition 8 and (ii) we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_{\alpha+1}, C_{\alpha+1}, x_0)$. Moreover, we have from (12), (13) and the second inequality in (18) that $W^*_{A,\alpha+1}(x_0) \leq W^*_{S,\alpha+1}(x_0) \leq \beta_{\alpha+1}$. Then, from item (b) of Proposition 2 applied to $\Sigma^c_{\alpha+1}$, $(x_t)_{t=0}^T$ is complete and for all $t \geq T_{\alpha+1}$, $H(x_t) \leq \beta_{\alpha+1}$. From item (a) of Proposition 2 applied this time to Σ^c_α, we get that $W^*_{A,\alpha}(x_0) \leq \beta_{\alpha+1}$. Clearly, this inequality holds also if $\beta_{\alpha+1} = +\infty$ and thus (v) is proved. ∎

Under Assumption 1, we get the following additional properties:

Lemma 5: Under Assumption 1 for system Σ, the following assertions hold:

(vi) $\forall \alpha \in \mathbb{N}_{\leq N},\ \beta_\alpha < +\infty$ and $\forall \alpha \in \mathbb{N}_{<N},\ \beta_\alpha \leq \beta_{\alpha+1}$;
(vii) $\forall \alpha \in \mathbb{N}_{\leq N},\ \text{dom}(C_\alpha) = X^0_N \neq \emptyset$;
(viii) $\forall \alpha \in \mathbb{N}_{\leq N},\ \exists T'_\alpha \in \mathbb{N}$, such that any $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha, C_\alpha, x_0)$ with $x_0 \in X^0_N$ is complete and satisfies

$$\forall t \geq T'_\alpha,\ x_t \in X^\infty_\alpha;$$

(ix) $X^0_N = \text{reach}(\Sigma_N, C_N, X^0_N)$.

Proof: Let us prove the different assertions.

(vi): Under Assumption 1, we get from Corollary 2 and the first equality in (16) that $\beta_N < +\infty$. Then for $\alpha \in \mathbb{N}_{<N}$, we have from (iii) and (v) in Lemma 4 that

$$\beta_\alpha = \max_{x \in X^\infty_{\alpha+1}} W^*_{A,\alpha}(x) \leq \beta_{\alpha+1}.$$

Thus, (vi) is proved.

(vii) and (viii): We proceed by induction. From (15), (vi), we get that $\text{dom}(C_N) = L_{\beta_N}(W^*_{A,N})$ and from the first and second equalities in (16), we get that $X^0_N = L_{\beta_N}(W^*_{A,N}) \neq \emptyset$. Moreover, from the item (b) of Proposition 2 applied to Σ_N, we get that any $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_N, C_N, x_0)$ with $x_0 \in X^0_N$ is complete and satisfies for all $t \geq T_N$, $x_t \in L_{\beta_N}(W^*_{S,N}) = X^\infty_N$, by the third equality in (16). Hence, (vii) and (viii) hold for $\alpha = N$ with $T'_N = T_N$. Then, let us assume that (vii) and (viii) hold for $\alpha + 1$ for some $\alpha \in \mathbb{N}_{<N}$.

We already have from (i) in Lemma 4 that $\text{dom}(C_\alpha) \subseteq \text{dom}(C_{\alpha+1}) = X^0_N$. Let us prove the converse inclusion. Let us consider a controller $\tilde{C}_\alpha$ defined for all $x \in X$ as follows:

$$\tilde{C}_\alpha(x) = \begin{cases} C_{\alpha+1}(x) & \text{if } x \in X \setminus X^\infty_{\alpha+1}; \\ C_\alpha(x) & \text{if } x \in X^\infty_{\alpha+1}. \end{cases} \tag{19}$$

From (ii) in Lemma 4, we can consider $\tilde{C}_\alpha$ as a controller for Σ^c_α. Then, let $x_0 \in X^0_N$, and $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, \tilde{C}_\alpha, x_0)$. Let us assume that for all $t \in \mathbb{N}_{\leq T}$, $x_t \notin X^\infty_{\alpha+1}$. Then, $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_{\alpha+1}, x_0)$. From (17) and Definition 8, it follows that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_0)$. Then, from the induction hypothesis, $(x_t)_{t=0}^T$ is complete and satisfies $x_t \in X^\infty_{\alpha+1}$, for all $t \geq T'_{\alpha+1}$, a contradiction. Hence, there exists $\tau \in \mathbb{N}_{\leq T}$, such that $x_\tau \in X^\infty_{\alpha+1}$. Then, $(x_t)_{t=\tau}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, \tilde{C}_\alpha, x_\tau)$. From (17) and Definition 8 and (i) in Lemma 4, we have that $(x_t)_{t=\tau}^T \in \mathscr{T}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_\tau)$, which together with (iv) in Lemma 4 gives that $x_t \in X^\infty_{\alpha+1}$, for all $\tau \leq t \leq T$. Then, $(x_t)_{t=\tau}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_\alpha, x_\tau)$. Moreover,

$$W^*_{A,\alpha}(x_\tau) \leq \max_{x \in X^\infty_{\alpha+1}} W^*_{A,\alpha}(x) = \beta_\alpha < +\infty.$$

It follows from item (b) of Proposition 2 applied to Σ^c_α that $(x_t)_{t=\tau}^T$ is complete and for all $t \geq \tau + T_\alpha$, $H(x_t) \leq \beta_\alpha$. Then, from item (a) of Proposition 2 applied to Σ^c_α, we get that $W^*_{A,\alpha}(x_0) \leq \beta_\alpha$. Hence, $x_0 \in L_{\beta_\alpha}(W^*_{A,\alpha}) = \text{dom}(C_\alpha)$ by (15) and (vi). Thus, $X^0_N \subseteq \text{dom}(C_\alpha)$ and (vii) holds for α.

Let $x_0 \in X^0_N$ and $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha, C_\alpha, x_0)$. Then, from (17) and (i) in Lemma 4, $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_\alpha, x_0)$. Since $X^0_N = \text{dom}(C_\alpha) =$

$L_{\beta_\alpha}(W^*_{A,\alpha})$, we get from item (b) of Proposition 2 applied to Σ^c_α that $(x_t)_{t=0}^T$ is complete and satisfies $x_t \in L_{\beta_\alpha}(W^*_{S,\alpha})$, for all $t \geq T_\alpha$. Moreover, by Definition 8 and (i) in Lemma 4, $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_0)$. Then, by the induction hypothesis, we get that $x_t \in X^\infty_{\alpha+1}$, for all $t \geq T'_{\alpha+1}$. Then, it follows from the second equality in (18) that $x_t \in X^\infty_\alpha$, for all $t \geq T'_\alpha$ where $T'_\alpha = \max(T'_{\alpha+1}, T_\alpha)$. Hence (viii) holds for α, and (vii) and (viii) are proved.

(ix): We already have $X^0_N \subseteq \text{reach}(\Sigma_N, C_N, X^0_N)$. We prove the converse inclusion. From item (b) of Proposition 2, we get that for any $x_0 \in X^0_N$, all maximal trajectories $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_N, C_N, x_0)$ are complete. This implies that $\text{reach}(\Sigma_N, C_N, X^0_N) \subseteq \text{dom}(C_N)$. Since by (vii), $\text{dom}(C_N) = X^0_N$ we get that $\text{reach}(\Sigma_N, C_N, X^0_N) \subseteq X^0_N$. ∎

We can now state the main result of this section:

Theorem 3: Under Assumption 1 for system Σ, the controller $C = C_0$ is an ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ with associated set of initial states $X^0_C = X^0_N$, time bound $T_C = \max(T_0, \ldots, T_N) + 1$ and gain function γ_C given by

$$\forall \alpha \in \mathbb{N}_{\leq N},\ \gamma_C(\alpha) = \beta_\alpha. \tag{20}$$

Moreover, C is an LV-ISA controller if the following holds:

$$\forall \alpha \in \mathbb{N}_{<N},\ \max_{x \in X^\infty_{\alpha+1}} W^*_{A,\alpha}(x) = \min_{x \in X^\infty_{\alpha+1}} W^*_{A,\alpha}(x). \tag{21}$$

In that case, for any other LV-ISA controller C' with associated set of initial states $X^0_{C'}$ and gain function $\gamma_{C'}$ it holds $\gamma_{C'} = \gamma_C$, $X^0_{C'} \subseteq X^0_C$ and $C'(x) \subseteq C(x)$, for all $x \in \text{attr}(\Sigma_0, C', X^0_{C'})$.

Proof: From (vii) in Lemma 5, we have $X^0_C = X^0_N \neq \emptyset$. Also from (vi) in Lemma 5, we get that γ_C is a non-decreasing function. Let us also remark that for all $\alpha \in \mathbb{N}_{\leq N}$, $T_C \geq T'_\alpha$ where T'_α are the time bounds as in (viii) in Lemma 5.

Let $x_0 \in X^0_C$ and $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma, C, x_0)$, then from (i) in Lemma 4 and (vii) in Lemma 5, we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_N, C_N, x_0)$. Then, by (viii) in Lemma 5, we get that $(x_t)_{t=0}^T$ is complete and by (ix) in Lemma 5, $x_t \in X^0_N$, for all $t \geq 0$. Let $(\alpha_t)_{t=0}^{T-1}$ be the level of disturbances associated to $(x_t)_{t=0}^T$. Let $t \geq T_C$ and $\tilde{\alpha} = \max_{t-T_C \leq s < t} \alpha_s$. Then, from (i) in Lemma 4 and Definition 8, we get that $(x_s)_{s=t-T_C}^t \in \mathscr{T}(\Sigma_{\tilde{\alpha}}, C_{\tilde{\alpha}}, x_{t-T_C})$. Moreover, by (viii) in Lemma 5, since $x_{t-T_C} \in X^0_N$ and $T_C \geq T_{\tilde{\alpha}}$, we get that $x_t \in X^\infty_{\tilde{\alpha}}$. Then, from the third equality in (16), the second equality in (18) and by (5), (6), we get that $H(x_t) \leq W_{S,\tilde{\alpha}}(x_t) \leq \beta_{\tilde{\alpha}}$. Therefore C is an ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

Let C' be a LV-ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. First, we are going to prove that $X^0_{C'} \subseteq X^0_N$. Because C' is an ISA controller, we get by item (a) in Proposition 2, that $X^0_{C'} \subseteq L_{\gamma_{C'}(N)}(W^*_{A,N})$. Then, since $X^0_{C'} \neq \emptyset$ and by the first equality in (16), we get that $\beta_N \leq \gamma_{C'}(N)$. Moreover, since C' is a LV-ISA controller, we also have $\beta_N \geq \gamma_{C'}(N)$, which gives $\beta_N = \gamma_{C'}(N)$. Hence, $X^0_{C'} \subseteq L_{\beta_N}(W^*_{A,N}) = X^0_N$ by the second equality in (16).

Now, let us prove by induction on α, that for all $\alpha \in \mathbb{N}_{\leq N}$:

$$\begin{aligned} \gamma_{C'}(\alpha) &= \beta_\alpha, \\ \text{attr}(\Sigma_\alpha, C', X^0_{C'}) &\subseteq X^\infty_\alpha, \\ C'(x) &\subseteq C_\alpha(x),\ \forall x \in \text{attr}(\Sigma_\alpha, C', X^0_{C'}). \end{aligned} \tag{22}$$

We start with the case $\alpha = N$. We already proved that $\gamma_{C'}(N) = \beta_N$. Since C' is an ISA controller we have $\text{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\gamma_{C'}(N)}(H)$. Moreover from Lemma 1, we get that $\text{attr}(\Sigma_N, C', X^0_{C'})$ is a controlled invariant of Σ_N. Hence, it follows from Proposition 1 that $\text{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\gamma_{C'}(N)}(W^*_{S,N})$. From $\gamma_{C'}(N) = \beta_N$ and the third equality of (16), we get that $\text{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\beta_N}(W^*_{S,N}) = X^\infty_N$. Then, let $x \in \text{attr}(\Sigma_N, C', X^0_{C'})$ and $u \in C'(x)$, then by (ii) in Lemma 1, $F_N(x,u) \subseteq \text{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\beta_N}(W^*_{S,N})$. Morever $W^*_{S,N}(x) \leq \beta_N$, then $u \in C_N(x)$ by (15). Therefore, (22) holds for $\alpha = N$.

Now let $\alpha \in \mathbb{N}_{<N}$, and let us assume that (22) holds for $\alpha+1$. We show that (22) holds for α. Let $x_0 \in \text{attr}(\Sigma_\alpha, C', X^0_{C'})$, and $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha, C', x_0)$. Then, from Definition 5, there exists $\tilde{x}_0 \in X^0_{C'}$, $(\tilde{x}_t)_{t=0}^{\tilde{T}} \in \mathscr{T}_{\max}(\Sigma_\alpha, C', \tilde{x}_0)$ and $\tau \geq T_{C'}$ such that $\tilde{x}_\tau = x_0$. Consider the trajectory $(\bar{x}_t)_{t=0}^{T+\tau}$ where $\bar{x}_t = \tilde{x}_t$ if $t \leq \tau$ and $\bar{x}_t = x_{t-\tau}$ if $t > \tau$. Then, $(\bar{x}_t)_{t=0}^{T+\tau} \in \mathscr{T}_{\max}(\Sigma_\alpha, C', \tilde{x}_0)$. Since C' is an ISA controller we get that $(\bar{x}_t)_{t=0}^{T+\tau}$ is complete and for all $t \geq T_{C'}$, $H(\bar{x}_t) \leq \gamma_{C'}(\alpha)$. Since $\tau \geq T_{C'}$, we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha, C', x_0)$ is complete and for all $t \geq 0$, $H(x_t) \leq \gamma_{C'}(\alpha)$. Moreover, by (ii) in Lemma 1, we get that $x_t \in \text{attr}(\Sigma_\alpha, C', X^0_{C'})$, for all $t \geq 0$. Then let us consider the controller $\tilde{C}_\alpha$ defined for all $x \in X$ as follows:

$$\tilde{C}_\alpha(x) = \begin{cases} \emptyset & \text{if } x \in X \setminus \text{attr}(\Sigma_\alpha, C', X^0_{C'}); \\ C'(x) & \text{if } x \in \text{attr}(\Sigma_\alpha, C', X^0_{C'}). \end{cases}$$

Then, $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha, \tilde{C}_\alpha, x_0)$. By Definition 8, we have $\text{attr}(\Sigma_\alpha, C', X^0_{C'}) \subseteq \text{attr}(\Sigma_{\alpha+1}, C', X^0_{C'})$. Then from the induction hypothesis, we obtain that for all $x \in \text{attr}(\Sigma_\alpha, C', X^0_{C'})$, $C'(x) \subseteq C_{\alpha+1}(x)$. This implies that for all $x \in X$, $\tilde{C}_\alpha(x) \subseteq C_{\alpha+1}(x)$ and therefore $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma^c_\alpha, \tilde{C}_\alpha, x_0)$. We finally get from Proposition 1 and from item (a) in Proposition 2 that $W^*_{S,\alpha}(x_0) \leq \gamma_{C'}(\alpha)$ and $W^*_{A,\alpha}(x_0) \leq \gamma_{C'}(\alpha)$. Since $x_0 \in \text{attr}(\Sigma_\alpha, C', X^0_{C'}) \subseteq \text{attr}(\Sigma_{\alpha+1}, C', X^0_{C'}) \subseteq X^\infty_{\alpha+1}$ by the induction hypothesis, we get from the first equality in (18) and by (21) that $W^*_{A,\alpha}(x_0) = \beta_\alpha$. This gives us $\beta_\alpha \leq \gamma_{C'}(\alpha)$. Since C' is a LV-ISA controller, we get $\gamma_{C'}(\alpha) \leq \beta_\alpha$. Hence $\beta_\alpha = \gamma_{C'}(\alpha)$.

From above it follows that $\text{attr}(\Sigma_\alpha, C', X^0_{C'}) \subseteq X^\infty_{\alpha+1}$ and $\text{attr}(\Sigma_\alpha, C', X^0_{C'}) \subseteq L_{\gamma_{C'}(\alpha)}(W^*_{S,\alpha})$. From $\gamma_{C'}(\alpha) = \beta_\alpha$ and the second equality of (18), we get that $\text{attr}(\Sigma_\alpha, C', X^0_{C'}) \subseteq L_{\beta_\alpha}(W^*_{S,\alpha}) \cap X^\infty_{\alpha+1} = X^\infty_\alpha$. Then, let $x \in \text{attr}(\Sigma_\alpha, C', X^0_{C'})$ and $u \in C'(x) \subseteq C_{\alpha+1}(x)$, then by (ii) in Lemma 1, $F^c_\alpha(x,u) = F_\alpha(x,u) \subseteq \text{attr}(\Sigma_\alpha, C', X^0_{C'}) \subseteq L_{\beta_\alpha}(W^*_{S,\alpha})$. Morever $W^*_{S,\alpha}(x) \leq \beta_\alpha$, then $u \in C_\alpha(x)$ by (15). Therefore, (22) holds for α. Hence, (22) holds for all $\alpha \in \mathbb{N}_{\leq N}$ and the theorem is proved. ∎

Hence, our approach, based on iterative refinements of least violating controllers, allows us to compute an ISA controller. Under condition (21), we proved that the synthesized controller is a LV-ISA controller. In that case, we have shown that the computed controller is valid for the largest possible set of initial states and that it is maximally permissive on the attractor set of the nominal system. Note that condition (21), can be easily checked a posteriori. Intuitively, this condition states that $X^\infty_{\alpha+1}$ should be included in the basin of attraction of the smallest closed-loop attractor of Σ^c_α.

We end the section with a simple illustrative example that shows that condition (21) is indeed necessary to ensure that the synthesized ISA controller is least violating.

Example 1: Consider a system $\Sigma = (X, U, F)$ where the set of states $X = \{x_0, x_1, x'_1, x_2, x'_2\}$ and the set of inputs $U = \{a, b\}$. $(\Sigma_\alpha)_{\alpha \in \mathbb{N}_{\leq 1}}$ is a nested sequence of subsystems of Σ. The transition relation F is represented in Figure 1, where plain transitions represent the nominal behavior F_0 and the dashed transition is the additional transition in the perturbed behavior F_1. Let the reference set $X^* = \{x_0\}$ and let the function $H : X \to \mathbb{R}_{\geq 0}$ be defined as $H(x_0) = 0$ and $H(x_i) = H(x'_i) = i$ for $i = 1, 2$.

We synthesize an ISA controller using the approach presented in the section. The LV-A controller for the perturbed system Σ_1 is C_1 given by $C_1(x_0) = \{a, b\}$ and $C_1(x) = \{a\}$ for all $x \neq x_0$. Then the ISA controller for $(\Sigma_\alpha)_{\alpha \in \mathbb{N}_{\leq 1}}$ is $C = C_0$ given by $C(x) = \{a\}$ for all $x \in X$. The associated set of initial states is $X^0_C = X$ and the gain function γ_C given by $\gamma_C(0) = \gamma_C(1) = 1$.

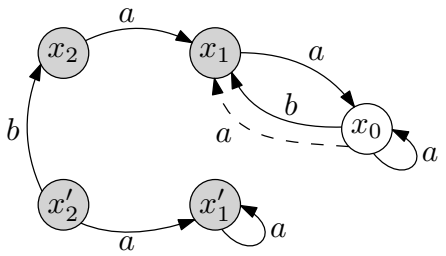

Fig. 1. Transition relation of the system in Example 1. Plain transitions represent the nominal behavior F_0 and the dashed transition is the additional transition in the perturbed behavior F_1.

The function $W^*_{A,0}$ is given by $W^*_{A,0}(x_i) = 0$ for $i = 0,1,2$ and $W^*_{A,0}(x'_i) = 1$ for $i = 1,2$. The set $X_1^\infty = \{x_0, x_1, x_{1'}\}$, thus condition (21) is not satisfied since

$$\max_{x \in X_1^\infty} W^*_{A,0}(x) = 1 \text{ and } \min_{x \in X_1^\infty} W^*_{A,0}(x) = 0.$$

In that case, C is not least violating. Indeed, a LV-ISA controller C' is given by $C'(x_i) = \{a\}$, for $i = 0,1,2$, $C'(x'_1) = \emptyset$ and $C'(x'_2) = \{b\}$, with associated set of initial states is $X^0_{C'} = X \setminus \{x'_1\}$ and the gain function $\gamma_{C'}$ given by $\gamma_{C'}(0) = 0$ and $\gamma_{C'}(1) = 1$.

Therefore, this example shows that condition (21) is necessary for ensuring the ISA controllers synthesized using our approach are least violating. ◇

V. Abstraction-based control synthesis for infinite systems with disturbances

In this section, we show how to lift our approach from finite systems to infinite systems using abstraction techniques. Let us consider the following system with disturbances:

$$\dot{\xi}(t) = f(\xi(t), \upsilon(t), \omega(t)) \tag{23}$$

where $\xi(t) \in \mathcal{X} \subseteq \mathbb{R}^n$, $\upsilon(t) \in \mathcal{U} \subseteq \mathbb{R}^p$ and $\omega(t) \in \mathcal{W} \subseteq \mathbb{R}^n$ denote the state, the control input and the unknown disturbance at time $t \in \mathbb{R}_{\geq 0}$, respectively. We are interested in controlling the system (23) towards a reference set $\mathcal{X}^* \subseteq \mathcal{X}$ through a digital controller. We assume that $\mathcal{W}$ contains the origin and that there exists $b_{\mathcal{W}} \in \mathbb{R}_{\geq 0}$ such that for all $w \in \mathcal{W}$, $\|w\| \leq b_{\mathcal{W}}$. We also assume that there exists $b_f \in \mathbb{R}_{\geq 0}$ such that for all $(z,u,w) \in \mathcal{X} \times \mathcal{U} \times \mathcal{W}$, $\|f(z,u,w)\| \leq b_f$.

Let us consider a sequence $0 \leq b_0 \leq b_1 \leq \cdots \leq b_N = b_{\mathcal{W}}$ and let $\mathcal{W}_\alpha = \{w \in \mathcal{W} \mid \|w\| \leq b_\alpha\}$. Let $\tau \in \mathbb{R}_{>0}$ be the sampling period, then for $\alpha \in \mathbb{N}_{\leq N}$, we denote by $\mathscr{M}([0,\tau], \mathcal{W}_\alpha)$ the set of measurable functions $\omega : [0,\tau] \to \mathcal{W}_\alpha$. We define an infinite transition system $\tilde{\Sigma}_\alpha = (\mathcal{X}, \mathcal{U}, \mathcal{F}_\alpha)$ describing the sampled dynamics of (23) subject to disturbances bounded by b_α, with the transition relation $\mathcal{F}_\alpha \subseteq \mathcal{X} \times \mathcal{U} \times \mathcal{X}$ given for $z \in \mathcal{X}$ by

$$\text{enab}_{\mathcal{F}_\alpha}(z) = \left\{ u \in \mathcal{U} \;\middle|\; \begin{array}{c} \forall \omega \in \mathscr{M}([0,\tau], \mathcal{W}_\alpha), \\ \exists \xi : [0,\tau] \to \mathcal{X} \text{ solution of (23)} \\ \text{with } \xi(0) = z,\ \upsilon(t) = u, \forall t \in [0,\tau] \end{array} \right\}, \tag{24}$$

and for all $u \in \text{enab}_{\mathcal{F}_\alpha}(z)$ by

$$\mathcal{F}_\alpha(z,u) = \left\{ z' \in \mathcal{X} \;\middle|\; \begin{array}{c} \exists \omega \in \mathscr{M}([0,\tau], \mathcal{W}_\alpha), \\ \exists \xi : [0,\tau] \to \mathcal{X} \text{ solution of (23) with} \\ \xi(0) = z,\ \xi(\tau) = z',\ \upsilon(t) = u, \forall t \in [0,\tau] \end{array} \right\}. \tag{25}$$

To be able to lift the results developed in the previous sections to (23), we use finite abstractions. Let us consider a finite partition $\{Q_x\}_{x \in X}$ of $\mathcal{X}$ and a finite subset $U \subseteq \mathcal{U}$. We use quantizers $\theta_\mathcal{X} : \mathcal{X} \to X$ and $\theta_\mathcal{W} : \mathcal{W} \to \mathbb{N}_{\leq N}$ defined as follows:

$$\theta_\mathcal{X}(z) = x \iff z \in Q_x,$$
$$\theta_\mathcal{W}(w) = \min\{\alpha \in \mathbb{N}_{\leq N} \mid w \in \mathcal{W}_\alpha\}.$$

Then, for $\alpha \in \mathbb{N}_{\leq N}$, we define a finite transition system $\Sigma_\alpha = (X, U, F_\alpha)$, where the transition relation $F_\alpha \subseteq X \times U \times X$ is given for $x \in X$ by

$$\text{enab}_{F_\alpha}(x) = \bigcap_{z \in Q_x} \text{enab}_{\mathcal{F}_\alpha}(z), \tag{26}$$

and for $u \in \text{enab}_{F_\alpha}(x)$ by

$$F_\alpha(x,u) = \left\{ x' \in X \mid \mathcal{F}_\alpha(Q_x, u) \cap Q_{x'} \neq \emptyset \right\}. \tag{27}$$

In the following, we use the notation $\Sigma = \Sigma_N$.

Proposition 3: For $\alpha \in \mathbb{N}_{\leq N}$, the relation

$$R = \{(z,x) \in \mathcal{X} \times X \mid \theta_\mathcal{X}(z) = x\}$$

is a feedback refinement relation from $\tilde{\Sigma}_\alpha$ to Σ_α. Moreover, $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ is a nested sequence of subsystems of Σ.

Proof: Let $\alpha \in \mathbb{N}_{\leq N}$, it follows from (26) that for all $(z,x) \in R$, $\text{enab}_{F_\alpha}(x) \subseteq \text{enab}_{\mathcal{F}_\alpha}(z)$. Then, let $u \in \text{enab}_{F_\alpha}(x)$, from (27), we get that $\theta_\mathcal{X}(\mathcal{F}_\alpha(z,u)) \subseteq F_\alpha(x,u)$. Finally, for all $z \in \mathcal{X}$, $(z, \theta_\mathcal{X}(z)) \in R$. Then, R is a feedback refinement relation from $\tilde{\Sigma}_\alpha$ to Σ_α.

Let $\alpha \in \mathbb{N}_{<N}$, we have $\mathcal{W}_\alpha \subseteq \mathcal{W}_{\alpha+1}$. Then, from (24), it follows that for all $z \in \mathcal{X}$, $\text{enab}_{\mathcal{F}_{\alpha+1}}(z) \subseteq \text{enab}_{\mathcal{F}_\alpha}(z)$. Then, from (26), we get that for all $x \in X$, $\text{enab}_{F_{\alpha+1}}(x) \subseteq \text{enab}_{F_\alpha}(x)$. Let $x \in X$ and $u \in \text{enab}_{F_{\alpha+1}}(x)$, we get from (25) that for all $z \in Q_x$, $\mathcal{F}_\alpha(z,u) \subseteq \mathcal{F}_{\alpha+1}(z,u)$. It follows from (27) that $F_\alpha(x,u) \subseteq F_{\alpha+1}(x,u)$. Hence, $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ is a nested sequence of subsystems of Σ. ■

Remark 3: In the construction described above, it is assumed that the map $\mathcal{F}_\alpha$ can be computed exactly, which is often not the case. It should be noted that the result presented in Proposition 3 still holds if one uses over-approximations of $\mathcal{F}_\alpha$. There are many methods for computing such over-approximations (see e.g. [10] and the references therein).

In the following, we show how controllers synthesized using the nested sequence of abstractions $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ can be used to design controllers for (23). Let us consider a function $h : \mathcal{X} \to \mathbb{R}_{\geq 0}$ such that $h(z) = 0$ if and only if $z \in \mathcal{X}^*$. We assume that h is Lipschitz with constant l_h. Such a function can be given e.g. by $h(z) = \|z\|_{\mathcal{X}^*}$ with Lipschitz constant $l_h = 1$. Then, to design ISSf and ISA controllers for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ we use the function $H : X \to \mathbb{R}_{\geq 0}$ given by

$$H(x) = \sup_{z \in Q_x} h(z).$$

Given a controller $C : X \to 2^U$ for Σ, let us consider the following sampled and quantized controller for (23):

$$u(t) = C \circ \theta_\mathcal{X}(\xi(k\tau)),\ \forall t \in [k\tau, (k+1)\tau),\ k \in \mathbb{N}. \tag{28}$$

We can now state the main results of the section.

Proposition 4: Let C be an ISSf controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ with associated set of initial states X^0_C and gain function γ_C. Then, all trajectories ξ of (23)-(28) with $\theta_\mathcal{X}(\xi(0)) \in X^0_C$ are defined on $\mathbb{R}_{\geq 0}$ and satisfy

$$\forall t \geq 0,\ h(\xi(t)) \leq \gamma_C\Big(\max_{0 \leq s < t} \theta_\mathcal{W}(\omega(s))\Big) + l_h b_f \tau.$$

Proof: Let us consider a trajectory ξ of (23)-(28) with $\theta_\mathcal{X}(\xi(0)) \in X^0_C$. Then, from (25), there exists $K \in \mathbb{N} \cup \{+\infty\}$, such that $(\xi(k\tau))_{k=0}^K \in \mathscr{T}_{\max}(\tilde{\Sigma}_N, C \circ \theta_\mathcal{X}, \xi(0))$. From Proposition 3, we get that $(\theta_\mathcal{X}(\xi(k\tau)))_{k=0}^K \in \mathscr{T}_{\max}(\Sigma_N, C, \theta_\mathcal{X}(\xi_0))$ where $\theta_\mathcal{X}(\xi_0) \in X^0_C$.

Since C is an ISSf controller, it follows from Definition 9 that $(\theta_{\mathcal{X}}(\xi(k\tau)))_{k=0}^{K}$ is complete, therefore $K=+\infty$, and

$$\forall k\in\mathbb{N},\ H(\theta_{\mathcal{X}}(\xi(k\tau)))\leq\gamma_C\left(\max_{0\leq j<k}\alpha_j\right) \tag{29}$$

where

$$\alpha_j=\min\left\{\alpha\in\mathbb{N}_{\leq N}\ \middle|\ \begin{array}{c}\exists\, u_j\in C(\theta_{\mathcal{X}}(\xi(j\tau))),\ \text{such that}\\ \theta_{\mathcal{X}}(\xi(j\tau+\tau))\in F_\alpha(\theta_{\mathcal{X}}(\xi(j\tau)),u_j)\end{array}\right\}.$$

From Proposition 3, we have for all $j\in\mathbb{N}$, $\alpha_j\leq\tilde{\alpha}_j$ where

$$\tilde{\alpha}_j=\min\left\{\alpha\in\mathbb{N}_{\leq N}\ \middle|\ \begin{array}{c}\exists\, u_j\in C(\theta_{\mathcal{X}}(\xi(j\tau))),\ \text{such that}\\ \xi(j\tau+\tau)\in\mathcal{F}_\alpha(\xi(j\tau),u_j)\end{array}\right\}.$$

Let $t\in\mathbb{R}_{\geq 0}$, and let $k\in\mathbb{N}$ such that $t\in[k\tau,(k+1)\tau)$. Then, from (25), we have

$$\max_{0\leq j<k}\alpha_j\leq\max_{0\leq j<k}\tilde{\alpha}_j\leq\max_{0\leq s<t}\theta_{\mathcal{W}}(\omega(s)). \tag{30}$$

Then, by definition of H, l_h and b_f, we get

$$\begin{aligned}h(\xi(t))&\leq h(\xi(k\tau))+l_h\|\xi(t)-\xi(k\tau)\|\\&\leq H(\theta_{\mathcal{X}}(\xi(k\tau)))+l_h b_f\tau.\end{aligned}$$

Then, (29) and (30) allow us to reach the conclusion. ∎

Proposition 5: Let C be an ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$ with associated set of initial states X_C^0, time bound K_C and gain function γ_C. Then, all trajectories ξ of (23)-(28) with $\theta_{\mathcal{X}}(\xi(0))\in X_C^0$ are defined on $\mathbb{R}_{\geq 0}$ and satisfy

$$\forall t\geq T,\ h(\xi(t))\leq\gamma_C\left(\max_{t-T\leq s<t}\theta_{\mathcal{W}}(\omega(s))\right)+l_h b_f\tau.$$

where $T=(K_C+1)\tau$.

The proof of Proposition 5 for ISA controllers is analogous to the proof of Proposition 4 taking into account that the bound on $h(\xi(t))$ only depends on the past values of the disturbance levels over last K_C+1 sampling periods. It is therefore omitted.

In this section, we have shown how the ISSf and ISA controllers designed using the approach presented in the previous sections can be used for infinite systems using carefully defined nested sequences of finite abstractions.

VI. Numerical Example

In this section, we show an application of our approach to adaptive cruise control which is a driver assistance system that seeks to combine safe following distance with speed regulation.

A. Mathematical model

We consider a set-up with two vehicles. Vehicle 1 is following vehicle 2, the relative position of vehicle 1 w.r.t the vehicle 2 is given by $d\in(-\infty,0]$. In the following, vehicles are driving at velocities v_1 (follower) and v_2 (leader), where the dynamics of vehicle 1 is controlled while that of vehicle 2 is considered as a disturbance. We consider the following continuous-time model adapted from [12]:

$$\begin{cases}\dot{d} &= v_1-v_2\\ \dot{v}_1 &= u-\frac{f_0+f_1v_1+f_2v_1^2}{M}\\ \dot{v}_2 &= \Gamma(v_2,w)\end{cases} \tag{31}$$

where the function Γ is given by

$$\Gamma(v_2,w)=\begin{cases}w & \text{if } v_2\in(v_2^{\min},v_2^{\max})\\ \max(0,w) & \text{if } v_2=v_2^{\min}\\ \min(0,w) & \text{if } v_2=v_2^{\max}\end{cases}$$

The choice of Γ saturates the value of v_2 so 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. The parameter M represents the mass of vehicle 1, while the vector of parameters $f=(f_0,f_1,f_2)$ describes the road friction and vehicle aerodynamics. The disturbance $w(t)\in[w^{\min},w^{\max}]$ represents the acceleration of vehicle 2.

B. Specifications

We consider the problem of designing an adaptive cruise control system. Let us define the time headway $\vartheta(t)=-d(t)/v_1(t)$. The requirements for adaptive cruise control, parameterized by a target velocity v^* and a target time headway ϑ^*, are formulated as follows. We must either:

- keep the time headway $\vartheta(t)\geq\vartheta^*$ 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 $\vartheta(t)$ at the desired value ϑ^*.

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

$$\mathcal{X}^*=\left\{(d,v_1,v_2)\in\mathbb{R}^3\mid(-d/v_1,v_1)\in\mathcal{Y}_a^*\cup\mathcal{Y}_b^*\right\} \tag{32}$$

where

$$\begin{aligned}\mathcal{Y}_a^*&=\{(\vartheta,v_1)\in\mathbb{R}^2\mid\vartheta\geq\vartheta^*,v_1=v^*\},\\ \mathcal{Y}_b^*&=\{(\vartheta,v_1)\in\mathbb{R}^2\mid\vartheta=\vartheta^*,v_1\leq v^*\}.\end{aligned}$$

Actually, this specification cannot be enforced so we aim at synthesizing a controller enforcing the closed-loop behavior that is the closest to a correct one with respect to the following distance function:

$$h(d,v_1,v_2)=\min_{(\vartheta',v_1')\in\mathcal{Y}_a^*\cup\mathcal{Y}_b^*}\max\left(|-d/v_1-\vartheta'|,\alpha|v_1-v_1'|\right)$$

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 $v_1(t)\in[v_1^{\min},v_1^{\max}]$.

Values of parameters, compatible with empirical measurements are taken from [12] and given in Table I.

TABLE I
Model and Specification Parameter Values

M	1370	kg	u^{min}	$-0.3g$	m/s^2
f_0	51	N	$u^{\max}$	$0.2g$	m/s^2
f_1	1.2567	Ns/m	$w^{\min}$	-3.2	m/s^2
f_2	0.4342	Ns^2/m^2	$w^{\max}$	3.2	m/s^2
g	9.82	m/s^2	$v_1^{\min}$	5	m/s
v^*	20	m/s	$v_1^{\max}$	30	m/s
ϑ^*	1.5	s	$v_2^{\min}$	12	m/s
α	1.5		$v_2^{\max}$	28	m/s

C. Synthesis of an ISA controller

We aim at computing an ISA controller for our system using a symbolic abstraction. We use a sampling period $\tau=0.5\,s$. For the set of relative positions, we use the partition of $(-\infty,0]$ consisting of the unbounded interval $(-\infty,60)$ with a uniform partition of $[-60,0]$ in

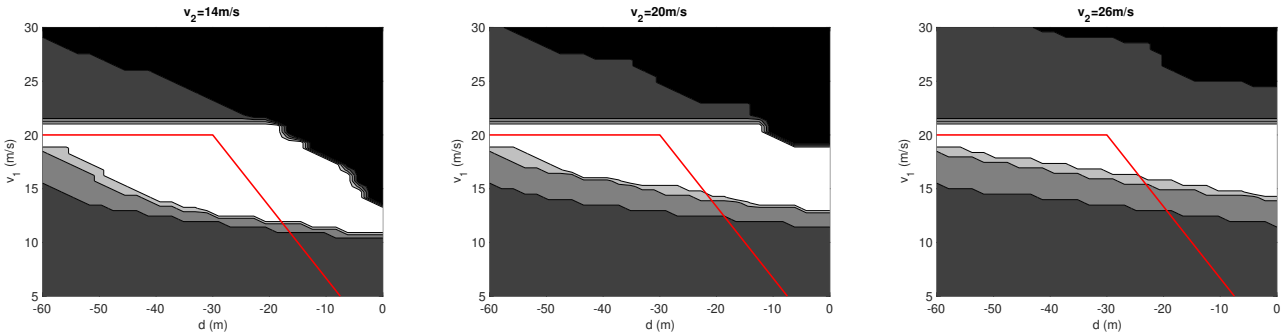

Fig. 2. ISA controller for system (31): red line represents the target set $\mathcal{X}^*$; black set consists of the states that are outside of the domain of the controller; dark grey set consists of the states that are inside the domain of the controller; medium grey / light grey / white sets correspond to the attractors for the different levels of disturbances.

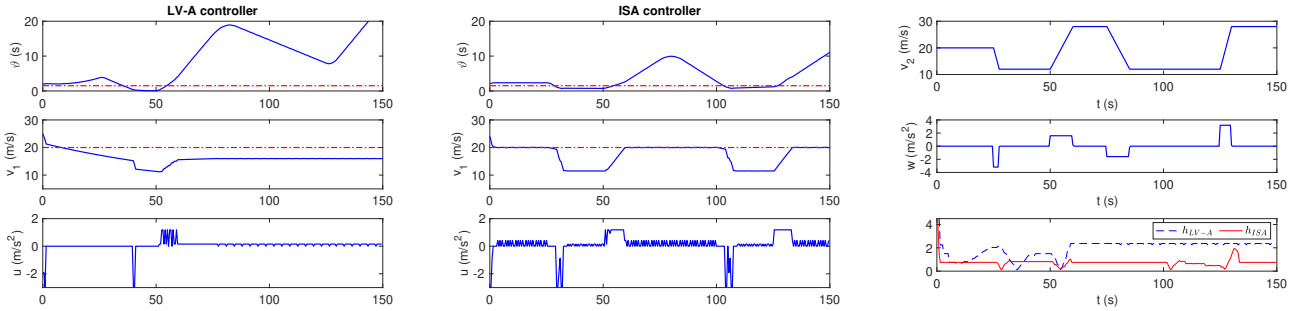

Fig. 3. Simulated trajectories of system (31) using a LV-A controller proposed in [5] (left) and our proposed ISA controller (center): evolution of the time headway, of the velocity of vehicle 1 and control input are represented in the plots where the target time headway ϑ^* and target velocity v^* are represented by dashed lines; velocity and acceleration of vehicle 2 and distance between the target set and the trajectories using a LV-A controller and an ISA controller (right).

30 sub-intervals. For the sets of velocities, we consider uniform partitions of $[5,30]$ and $[12,28]$ in 50 and 40 sub-intervals, respectively. For the control inputs, we choose a finite set of 21 elements consisting of 0 and 20 other values separated by $(u^{\max}-u^{\min})/20$. We consider three levels of disturbances given by the bounds $b_0=0.8$, $b_1=1.6$, $b_2=3.2$. A nested sequence of abstractions $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq 2}}$ is then computed using the approach presented in Section V. Then, we used the approach presented in Section IV to synthesize an ISA controller C for the nested sequence of abstractions $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq 2}}$. Note that the strong safety requirements are satisfied by construction since inputs potentially leading to relative positions $d\geq 0$ or to velocities $v_1\in[v_1^{\min},v_1^{\max}]$ are disabled in the abstraction.

The overall computation took about 1 hour 35 minutes (CPU: 2.8 GHz Intel Core i7, RAM: 16 Go 2133 MHz LPDDR3, Matlab R2019b), with 68 minutes spent on computing the first abstraction Σ_2 and synthesizing the controller C_2; 17 minutes spent on computing the abstraction Σ_1^c and synthesizing the controller C_1; 10 minutes spent on computing the abstraction Σ_0^c and synthesizing the ISA controller $C=C_0$. We can see that the overhead of computing the ISA controller C in comparison to computing the LV-A C_2 is not so much. The associated gain function γ_C is given by $\gamma_C(0)=1.50$, $\gamma_C(1)=1.74$, $\gamma_C(2)=2.37$. We check that the sufficient condition (21) of Theorem 3 is satisfied for $\alpha=1$ but not for $\alpha=0$ since

$$\max_{x\in X_2^\infty} W^*_{A,1}(x)=\min_{x\in X_2^\infty} W^*_{A,1}(x)=1.74.$$

and

$$\max_{x\in X_1^\infty} W^*_{A,0}(x)=1.50 \text{ and } \min_{x\in X_1^\infty} W^*_{A,0}(x)=1.11.$$

Therefore, C is an ISA controller but may not be a LV-ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq 2}}$. However, since (21) is satisfied for $\alpha=1$, C is a LV-ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\{1,2\}}$.

In Figure 2, we show slices of the computed sets which are represented by colors white, light gray, dark gray and black at different values of v_2:

- The red line represents the target set $\mathcal{X}^*$ in (32);
- The black set consists of the states that are outside of the domain of the controller $\mathrm{dom}(C\circ\theta_{\mathcal{X}})=\theta_{\mathcal{X}}^{-1}(X_C^0)$;
- The dark grey set consists of the states that are inside the domain of the controller $\mathrm{dom}(C\circ\theta_{\mathcal{X}})=\theta_{\mathcal{X}}^{-1}(X_C^0)$;
- The medium grey / light grey / white sets correspond to the attractors for the different levels of disturbances $\theta_{\mathcal{X}}^{-1}(X_\alpha^\infty)$, for $\alpha\in\mathbb{N}_{\leq 2}$.

In Figure 3, we show a simulation of system (31) using a LV-A controller synthesized using the approach in [5] and the proposed ISA controller in the following scenario. The initial value of (d,v_1,v_2) is $(-50,24,20)$. The leading vehicle (vehicle 2) drives at constant speed for the first $25s$, then at time 25 it applies maximal deceleration $-b_2$ until it reaches the velocity $v_2^{\min}$, at time 50 it applies acceleration b_1 until it reaches velocity $v_2^{\max}$, at time 75 it applies deceleration $-b_1$ until it reaches velocity $v_2^{\min}$, and at time 125 it applies maximal acceleration b_2 until it reaches the velocity $v_2^{\max}$. The profiles of velocity $v_2(t)$ and acceleration $w(t)$ are shown on the right figure. The plots in the left and center figures represent the evolution of the time headway $\vartheta(t)$, of the velocity $v_1(t)$, the control input $u(t)$ for the LV-A controller proposed in [5] (left figure) and the proposed ISA controller (center figure). The values of the target velocity v^* and the target time headway ϑ^* are represented by dashed lines. We can see from these plots that the ISA controller does a much better job in regulating both the time headway and the velocity. Quantitatively, the performances of the LV-A controller and of the ISA controller

can be compared through the distance h evaluated on trajectories: h_{LV-A} for the LV-A controller and h_{ISA} for the ISA controller on the right figure. We can see on the simulation that the system behaves as expected and that the *ISA* controller outperforms the LV-A controller.

VII. CONCLUSIONS

In this paper, we introduced the notion of LV-ISSf and of LV-ISA controllers for finite state systems subject to disturbances of various levels. We have developed algorithms for computing such controllers and we have shown how these can be used in combination with symbolic control techniques. An application to adaptive cruise control shows the performance improvement of LV-ISA controllers compared to LV-A controllers. In the future, we plan to work on developing other algorithms for the synthesis of LV-ISA controllers when the condition (21) is not satisfied. We would also like to develop algorithms for synthesizing ISSf and ISA controllers that are least violating for the lexicographic and the summation orders.

REFERENCES

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

[2] S. Coogan and M. Arcak. Finite abstraction of mixed monotone systems with discrete and continuous inputs. *Nonlinear Analysis: Hybrid Systems*, 23:254–271, 2017.

[3] 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.

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

[5] A. Girard and A. Eqtami. Least-violating symbolic controller synthesis for safety, reachability and attractivity specifications. *Automatica*, 127:109543, 2021.

[6] 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.

[7] Z.-P. Jiang and Y. Wang. Input-to-state stability for discrete-time nonlinear systems. *Automatica*, 37(6):857–869, 2001.

[8] S. Kolathaya and A. D. Ames. Input-to-state safety with control barrier functions. *IEEE control systems letters*, 3(1):108–113, 2018.

[9] J. Liu and N. Ozay. Finite abstractions with robustness margins for temporal logic-based control synthesis. *Nonlinear Analysis: Hybrid Systems*, 22:1–15, 2016.

[10] P.-J. Meyer, A. Devonport, and M. Arcak. *Interval Reachability Analysis: Bounding Trajectories of Uncertain Systems with Boxes for Control and Verification*. Springer, 2021.

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

[12] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A. Ames, J. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Correct-by-construction adaptive cruise control: Two approaches. *IEEE Trans. on Cont. Syst. Technol.*, 24(4):1294–1307, 2016.

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

[14] 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.

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

[16] 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.

[17] 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.

[18] S. Samuel, K. Mallik, A.-K. Schmuck, and D. Neider. Resilient abstraction-based controller design. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 2123–2129. IEEE, 2020.

[19] V. Sinyakov and A. Girard. Formal controller synthesis from specifications given by discrete-time hybrid automata. *Automatica*, 131:109768, 2021.

[20] E. D. Sontag. Input to state stability: Basic concepts and results. In *Nonlinear and optimal control theory*, pages 163–220. Springer, 2008.

[21] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[22] 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.

[23] 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.

[24] A. Weber, M. Kreuzer, and A. Knoll. A generalized Bellman-Ford algorithm for application in symbolic optimal control. In *European Control Conference*, 2020.

[25] 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.