Synthesis of Input-to-State Attractivity Controllers for Transition Systems with Disturbances

W. A. Apaza-Perez, Antoine Girard

Synthesis of Input-to-State Attractivity Controllers for Transition Systems with Disturbances

W. Alejandro Apaza-Perez, Antoine Girard

***Abstract*— In this paper, we introduce a notion of input-to-state attractivity (ISA) controllers for a class of finite transition systems with disturbances. The performances of an ISA controller are characterized by a gain function that quantifies the deviation of closed-loop trajectories from the target set as a function of the amplitude of past disturbances on a bounded time window. We prove the existence of controllers that are gain-optimal (GO) in the sense that their gain function is minimal (with respect to a given order on the set of gain functions) over all possible ISA controllers. Then, we consider the problem of synthesizing ISA controllers. We present an approach 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 lower disturbances. We prove that our method makes it possible to synthesize an ISA controller that is shown to be a GO-ISA controller (for the colexicographic order) when a condition, which can be easily checked a posteriori, is satisfied. Finally, an application to adaptive cruise control demonstrates the effectiveness of our approach.**

I. INTRODUCTION

Formal synthesis (see e.g. [19], [1], [11]) refers to a collection of algorithmic approaches for automatically designing controllers enforcing various specifications such as safety or reachability [19], [4], or more complex ones given in the form of dynamical systems [11], [17] or of temporal logic formulas [8], [1]. The algorithms for controller synthesis usually apply to finite-state dynamical systems but can be lifted to handle infinite-state dynamics via the use of symbolic models, also called discrete abstractions, which are finite-state approximations of the dynamical system under consideration [6], [23], [2]. When the behaviors of the symbolic model and of the original system can be related by some formal relationship, such as alternating simulation relations [12] or feedback refinement relations [14], controllers synthesized for the symbolic model can be used to control the system with 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. A 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 [15] 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 an attractivity specification to the amplitude of disturbances. We introduce a notion of input-to-state attractivity (ISA) controllers for a class of finite transition systems where the effect of disturbances of varying amplitude is captured by nested sequences of subsystems. The performances of an ISA controller can be measured by a gain function that quantifies the distance between closed-loop trajectories and the target set as a function of the amplitude of past disturbances on a bounded time window: low disturbances result in small deviations from the target set, while larger deviations can be expected for higher disturbances. In the framework of transition systems, the ISA property is new. However, it is directly inspired by the celebrated input-to-state stability (see e.g. [7], [18]).

The first main contribution of this paper is to show the existence ISA controllers that are gain-optimal (GO), meaning that their gain function, and hence the deviation from the target set, is minimal (with respect to a certain order on the set of gain functions) over all possible ISA controllers. As a second contribution, we present an algorithm to synthesize ISA controllers for the colexicographic order on gain functions. The algorithms are based on successive refinements of least-violating 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 lower disturbances. Each iteration involves solving dynamic programming fixed-points for which efficient algorithms can be found e.g. in [13], [21]. We prove that our method makes it possible to synthesize an ISA controller that is shown to be a GO-ISA controller when a condition, which can easily be checked a posteriori, is satisfied. Finally, we use our approach in combination with symbolic models to synthesize an ISA controller for an adaptive cruise control problem [10].

Our work partially builds on the results of [5], where the

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 is with the Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, 91190, Gif-sur-Yvette, France, and also with the Universidad Mayor de San Andrés, FCPN, Carrera de Matemática, Av. Villazón 1995, La Paz, Bolivia. waapaza@umsa.bo

A. Girard is with the Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, 91190, Gif-sur-Yvette, France. antoine.girard@l2s.centralesupelec.fr

notion of least-violating 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 GO-ISA property. The algorithms presented in this paper use those presented in [5] as building blocks in an iterative refinement procedure. However, the main results of the present paper require non-trivial proof techniques and are not straightforward consequences of the results in [5]. Other closely related works include [20], [3], [9], [16]. In [20], 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], [9] 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 models in [16] 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. In [22], a robust synthesis problem is also considered where one tries to maximize the disturbances that can be tolerated for a given performance level. This can be viewed as a dual approach to that considered in this paper, resulting in different dynamic programming fixed points. Moreover, while the present paper considers attractivity, [22] deals with safety properties.

The rest of the paper is organized as follows. Section II introduces the notion of (GO)-ISA controllers, provides a formal problem statement, and presents some preliminary results. Section III presents an algorithm to synthesize such controllers and provide proofs of correctness of the proposed algorithms. Finally, section IV shows an application to the adaptive cruise control problem.

Notations: $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, $\mathbb{R}_{>0}$, $\mathbb{N}$ and $\mathbb{N}_{>0}$ denote the sets of real, non negative real, positive real numbers, non negative integers and positive 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 $R(x_1) = \{x_2 \in X_2 |\, (x_1, x_2) \in R\}$.

II. PROBLEM FORMULATION

In this section, we first provide a description of the setup of transition systems with disturbances. Then, we give a precise statement of the problem considered in the paper. Finally, preliminary results that will be useful for subsequent discussions are presented.

A. Transition systems with disturbances

In this paper, we consider the general framework of transition systems (see e.g. [19]):

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.

In this paper, we will refer to transition systems simply as systems. 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. The non-determinism in the transition relation F is often used to model the effect of disturbances. However, such modelling fails to capture the fact that disturbances can be of varying amplitude. For that purpose, we consider systems with a particular structure reflecting the effect of disturbances of various amplitudes:

Definition 2: Given $\Sigma = (X, U, F)$, a *nested sequence of subsystems* of Σ is a finite sequence of systems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ with $N \in \mathbb{N}$, $\Sigma_\alpha = (X, U, F_\alpha)$, $\Sigma_N = \Sigma$, and such that for all $x \in X$ and $\alpha \in \mathbb{N}_{<N}$,

- $\text{enab}_{F_{\alpha+1}}(x) \subseteq \text{enab}_{F_\alpha}(x)$,
- for all $u \in \text{enab}_{F_{\alpha+1}}(x)$, $F_\alpha(x, u) \subseteq F_{\alpha+1}(x, u)$.

Intuitively, $\alpha \in \mathbb{N}_{\leq N}$ can be thought about as a disturbance, $\alpha = 0$ corresponding to the lowest disturbance (i.e. the nominal behavior) and $\alpha = N$ corresponding to the highest disturbance (i.e. worst-case behavior). Then, higher values of α naturally correspond to fewer enabled inputs and increased non-determinism. Specifying the transition relations F_α is part of the modelling. In the following, we assume these transition relations to be given.

In this paper, we consider memoryless state-feedback controllers:

Definition 3: 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 4: 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 a *closed-loop trajectory* of system Σ with controller C if and only if for all $t \in \mathbb{N}_{<T}$, there exists $u_t \in C(x_t)$ 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.

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

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

where F_α, $\alpha \in \mathbb{N}_{\leq N}$ in (1) correspond to the transition relations of the nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ of Σ as defined in Definition 2. The goal of this paper is to synthesize controllers that can optimally adapt their performance to disturbances. Note that the disturbance can be time-varying and is assumed to be unmeasured and thus unknown to the controller.

B. Gain-optimal controllers for input-to state attractivity

Consider a target set $X^* \subseteq X$ and 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 $H(x) = \min_{x' \in X^*} d(x, x')$ where d is a metric on X. We are interested in designing controllers for uniform attractivity specifications. Uniform attractivity requires the existence of a uniform time bound after which all closed-loop trajectories stay in X^*. It was shown in [5] that this property differs from the temporal logic specification *eventually always* even in the case of finite transition systems. The problem of synthesizing least-violating controllers for uniform attractivity was considered in [5]. 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 attractivity property.

To formally define 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 denote by $\inf_{\preceq}(\Gamma)$ the infimum of a set $\Gamma \subseteq \Gamma_N$ with respect to $\preceq$.

Definition 5: Let us consider a system Σ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. An *input-to-state attractivity* (ISA) controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ is a tuple $(C, X_C^0, T_C, \gamma_C)$ where $C : X \to 2^U$ is a controller, $X_C^0 \subseteq X$ is a non-empty set of initial states, $T_C \in \mathbb{N}_{>0}$ is a time bound and $\gamma_C \in \Gamma_N$ is a gain function, 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

$$\forall t \geq T_C,\, H(x_t) \leq \gamma_C\Big(\max_{t - T_C \leq s < t} \alpha_s\Big) \tag{2}$$

where $(\alpha_t)_{t=0}^{T-1}$ is the disturbance given by (1) associated to $(x_t)_{t=0}^{T}$. Moreover, ISA controller $(C, X_C^0, T_C, \gamma_C)$ is *gain-optimal* (GO-ISA) if

$$\gamma_C = \inf_{\preceq}\big\{\, \gamma_{C'} \in \Gamma_N | \; (C', X_{C'}^0, T_{C'}, \gamma_{C'}) \text{ is an ISA controller}\big\}.$$

Gain functions allow us to measure the deviation of closed-loop trajectories from the target set as a function of the amplitude of past disturbances on a bounded time window. As such, gain functions can be seen as a performance index of the ISA controller. Then, GO-ISA controllers are controllers that are optimal with respect to that performance index. Following Definitions 5, it is important to emphasize the following features of GO-ISA controllers:

- The fact that these controllers are defined using the colexicographic order induces that the primary 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. $\gamma(N-1)$,...,$\gamma(0)$ in that order. A consequence is that a GO-ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$ is also 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 attractive, even in the nominal case, the objective being to stay as close as possible to X^*.

Remark 1: We only consider state-feedback memoryless controllers (i.e. $C : X \to 2^U$). It is clearly possible to design controllers with best performances if the disturbance α_t is measured and known to the controller (i.e. with $C : X \times \mathbb{N}_{\leq N} \to 2^U$). The question whether it is possible to obtain better performances with state-feedback controllers with memory is open and left for future investigations.

Throughout 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 ISA controllers, so it is pointless to try to synthesize such controllers.

Theorem 1: Let Σ be a finite system with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. Under Assumption 1, there exists a GO-ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

Proof: Let C be a controller 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 for the time bound $T_C = 1$ and therefore $(C, X_C^0, T_C, \gamma_C)$ is an ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$. So the set of ISA controllers is non-empty.

Let us denote by Γ_N^* the subset of gain functions γ such that for all $k \in \mathbb{N}_{\leq N}$, $\gamma(k) \in H(X)$. Let us remark that since X is finite, Γ_N^* is also finite. Moreover, it is easy to see for any ISA controller $(C, X_C^0, T_C, \gamma_C)$, there exists a gain function $\gamma_C^* \in \Gamma_N^*$ such that $\gamma_C^* \preceq \gamma_C$ and $(C, X_C^0, T_C, \gamma_C^*)$ is an ISA controller. From Definition 5 and from above it follows that an ISA controller $(C, X_C^0, T_C, \gamma_C)$ is (GO-ISA) if and only if $\gamma_C = \inf_{\preceq} \Gamma'_N$ where $\Gamma'_N = \big\{\, \gamma_{C'} \in \Gamma_N^* | \; (C', X_{C'}^0, T_{C'}, \gamma_{C'}) \text{ is an ISA controller}\big\}$. Γ'_N is a

non-empty subset of Γ_N^*, which is finite. Hence, there exists a minimal element γ_C of Γ'_N for the total order $\preceq$. Then, $\gamma_C \in \Gamma'_N$ gives us the existence of controller C, set of initial states X_0^C, and time bound T_C such that $(C, X_C^0, T_C, \gamma_C)$ is an ISA controller. Since $\gamma_C = \inf_{\preceq} \Gamma'_N$, it is also GO-ISA. ■

Remark 2: In this paper, we deal with controllers that are gain-optimal with respect to the colexicographic order. However, similar to Definitions 5, one can define GO-ISA controllers for other ordering relations on Γ_N. Actually, it follows from the proof of Theorem 1 that GO-ISA controllers also exist for any total preorder $\preceq_*$ on Γ_N such that for any $\gamma_1, \gamma_2 \in \Gamma_N$, $\gamma_1 \preceq_* \gamma_2$ if $\gamma_1(k) \leq \gamma_2(k)$ for all $k \in \mathbb{N}_{\leq N}$. 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 $\gamma_1(0) + \cdots + \gamma_1(N) \leq \gamma_2(0) + \cdots + \gamma_2(N)$.

It should be noticed that GO-ISA controllers generally depend on the chosen order on gain functions. Also, for a given order, they are generally not unique, as shown by the following example.

Example 1: Consider the transition system Σ presented in Figure 1 with two levels of disturbances (i.e. $N = 1$). Plain edges represent the transitions in F_0 and dashed edges represent the additional transitions in F_1. Let $H(x) = x$ for all $x \in X = \{0,1,2,3\}$ and let us consider the controllers C_a and C_b given by $C_a(x) = \{a\}$ and $C_b(x) = \{b\}$ for all $x \in X$. It can be easily shown that $(C_a, X_{C_a}^0, T_{C_a}, \gamma_{C_a})$ is a GO-ISA controller with set of initial states $X_{C_a}^0 = X$, time bound $T_{C_a} = 2$ and gain function $\gamma_{C_a}(0) = 1$, $\gamma_{C_a}(1) = 2$. To illustrate the influence of the set of initial states and of the time bound, let us consider the set of initial states $X_{C_a}^{0\prime} = \{0,1,2\}$, time bound $T'_{C_a} = 1$ and gain function $\gamma'_{C_a}(0) = 2$, $\gamma'_{C_a}(1) = 2$. One can check that $(C_a, X_{C_a}^0, T'_{C_a}, \gamma'_{C_a})$ is an ISA controller but is not GO-ISA since $\gamma_{C_a} \preceq \gamma'_{C_a}$. One can also check that $(C_a, X_{C_a}^{0\prime}, T'_{C_a}, \gamma_{C_a})$ is a GO-ISA controller, which however applies to a strictly smaller set of initial states. Finally, $(C_b, X_{C_b}^0, T_{C_b}, \gamma_{C_b})$ is an ISA controller with set of initial states $X_{C_b}^0 = X$, time bound $T_{C_b} = 3$ and gain function $\gamma_{C_b}(0) = 0$, $\gamma_{C_b}(1) = 3$. C_a performs better for the worst-case disturbances ($\gamma_{C_a}(1) < \gamma_{C_b}(1)$), while C_b performs better in nominal conditions ($\gamma_{C_b}(0) < \gamma_{C_a}(0)$). Actually, $(C_b, X_{C_b}^0, T_{C_b}, \gamma_{C_b})$ can be shown to be a GO-ISA controller for the lexicographic order. Both $(C_a, X_{C_a}^0, T_{C_a}, \gamma_{C_a})$ and $(C_b, X_{C_b}^0, T_{C_b}, \gamma_{C_b})$ are GO-ISA controllers for the summation order.

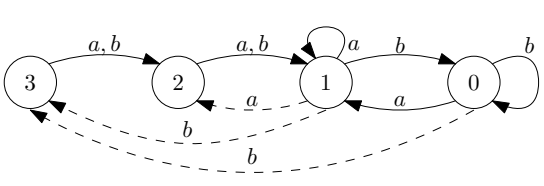

Fig. 1: Transition system Σ in Example 1. Plain edges represent the transitions in F_0 and dashed edges represent the additional transitions in F_1.

We can now provide a formal statement of the problem under consideration in this paper:

Problem 1: Given a finite system $\Sigma = (X, U, F)$ with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$, and a function $H : X \to \mathbb{R}_{\geq 0}$, synthesize a GO-ISA controller for $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq N}}$.

In this paper, we provide a partial solution to Problem 1. We provide an approach to synthesize ISA controllers using successive refinements. These ISA controllers are shown to be GO-ISA when a condition, which can be easily checked a posteriori, is satified.

C. Preliminary results

In this section, we introduce some notions and results that will be instrumental for further discussions.

Definition 6: Given a set of states $X^0 \subseteq X$, the *closed-loop reachable set* of system Σ with controller C from X^0 is

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

Definition 7: Given a set of states $X^0 \subseteq X$, the *closed-loop attractor set* of system Σ with controller C from X^0 is

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

We also define the notion of controlled invariant set:

Definition 8: 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], [19]) that X^0 is a controlled invariant set if and only if for all $x \in X^0$, there exists $u \in \mathrm{enab}_F(x)$ such that $F(x,u) \subseteq X^0$. It can be easily seen that Assumption 1 is actually equivalent to the existence of a non-empty controlled invariant set, which can be checked using standard algorithms (see e.g. [4], [19]). We state the following instrumental result relating closed-loop attractor sets and controlled invariant sets.

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

$$\forall x \in \mathrm{attr}(\Sigma, C, X^0) \cap \mathrm{dom}(C),\ \forall u \in C(x),\ F(x,u) \subseteq \mathrm{attr}(\Sigma, C, X^0). \tag{3}$$

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 $\mathrm{attr}(\Sigma, C, X^0)$ is a controlled invariant set of Σ.

Proof: Let $x \in \mathrm{attr}(\Sigma, C, X^0) \cap \mathrm{dom}(C)$, 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, $x^+ \in \mathrm{attr}(\Sigma, C, X^0)$ and (3) 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, $\mathrm{attr}(\Sigma, C, X^0) \cap \mathrm{dom}(C) = \mathrm{attr}(\Sigma, C, X^0)$. Therefore, it follows from (3) that $\mathrm{attr}(\Sigma, C, X^0)$ is a controlled invariant set of Σ. ■

III. Synthesis of ISA controllers

In this section, we present an approach to synthesize ISA controllers. The approach consists of two main steps: firstly we synthesize a least-violating attractivity controller for Σ following the approach in [5]; secondly the controller is iteratively refined into an ISA controller using the nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$. The obtained controller are generally not gain-optimal. However, we provide a sufficient condition that is easily checkable a posteriori and that guarantees that the synthesized controller is a GO-ISA controller.

A. Synthesis of least-violating attractivity controllers

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

$$W_S^0(x) = H(x), \tag{4}$$

$$W_S^{k+1}(x) = \begin{cases} \max\left(H(x), \min\limits_{u\in \mathrm{enab}_{\tilde{F}}(x)} \max\limits_{x^+\in\tilde{F}(x,u)} W_S^k(x^+)\right) \\ \qquad\qquad \text{if } x \in \mathrm{nbs}_{\tilde{F}}; \\ +\infty \qquad\qquad \text{if } x \notin \mathrm{nbs}_{\tilde{F}} \end{cases} \tag{5}$$

for $x \in X$, $k \in \mathbb{N}$. Let W_S^* be the fixed-point of (4)-(5). Then, let

$$W_A^0(x) = W_S^*(x), \tag{6}$$

$$W_A^{k+1}(x) = \begin{cases} \min\left(W_S^*(x), \min\limits_{u\in \mathrm{enab}_{\tilde{F}}(x)} \max\limits_{x^+\in\tilde{F}(x,u)} W_A^k(x^+)\right) \\ \qquad\qquad \text{if } x \in \mathrm{nbs}_{\tilde{F}}; \\ +\infty \qquad\qquad \text{if } x \notin \mathrm{nbs}_{\tilde{F}} \end{cases} \tag{7}$$

for $x \in X$, $k \in \mathbb{N}$. Let W_A^* be the fixed-point of (6), (7) 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 $x \in X$, $W_S^k(x) = W_S^*(x)$ and $W_A^k(x) = W_A^*(x)$. Let the function $k^* : X \to \mathbb{N}$ be defined as follows for all $x \in X$

$$k^*(x) = \min\{k \in \mathbb{N} \,|\, W_A^k(x) = W_A^*(x)\}. \tag{8}$$

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:

$$C_\beta(x) = \begin{cases} \arg\min\limits_{u\in \mathrm{enab}_{\tilde{F}}(x)} \left(\max\limits_{x^+\in\tilde{F}(x,u)} W_A^{k^*(x)-1}(x^+)\right) \\ \qquad\qquad \text{if } W_A^*(x) \leq \beta < W_S^*(x); \\ \left\{u \in \mathrm{enab}_{\tilde{F}}(x) \,\middle|\, \max\limits_{x^+\in\tilde{F}(x,u)} W_S^*(x^+) \leq W_S^*(x)\right\} \\ \qquad\qquad \text{if } W_S^*(x) \leq \beta; \\ \emptyset \qquad\qquad \text{if } \beta < W_A^*(x). \end{cases} \tag{9}$$

Let us remark that for $\beta < +\infty$, $\mathrm{dom}(C_\beta) = L_\beta(W_A^*)$. The next results are direct consequences of Theorem 3.2, Proposition 3.10 and Theorem 3.11 in [5] and are 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 for all $t \geq 0$, $H(x_t) \leq \beta$.

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 for all $t \geq T_{x_0}$, $H(x_t) \leq \beta$, 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 for all $t \geq T_0$, $H(x_t) \leq W_S^*(x_t) \leq \beta$.

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 $x_0 \in L_\beta(W_A^*)$.

B. Input-to-state attractivity via refinements

We present an approach to synthesize an 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 (4)-(5) and by (6)-(7) for the system $\tilde{\Sigma} = \Sigma_N$. Then, let us define

$$\beta_N = \min_{x\in X} W_{A,N}^*(x),\ X_N^0 = L_{\beta_N}(W_{A,N}^*),\ X_N^\infty = L_{\beta_N}(W_{S,N}^*). \tag{10}$$

Let C_N be given by (9) 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 (9) and thus guarantees the minimal asymptotic deviation from X^* for the worst case disturbance. 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 disturbance α.

For $\alpha \in \mathbb{N}_{<N}$, let $\Sigma_\alpha^c = (X, U, F_\alpha^c)$ where F_α^c is defined by

$$F_\alpha^c(x,u) = \begin{cases} F_\alpha(x,u) & \text{if } u \in C_{\alpha+1}(x); \\ \emptyset & \text{if } u \notin C_{\alpha+1}(x) \end{cases} \tag{11}$$

Intuitively Σ_α^c describes the dynamics of Σ_α constrained by the controller $C_{\alpha+1}$. Let $W_{S,\alpha}^*$, $W_{A,\alpha}^*$ be given by (4)-(5) and by (6)-(7) for the system $\tilde{\Sigma} = \Sigma_\alpha^c$, and let

$$\beta_\alpha = \max_{x\in X_{\alpha+1}^\infty} W_{A,\alpha}^*(x),\ X_\alpha^\infty = L_{\beta_\alpha}(W_{S,\alpha}^*) \cap X_{\alpha+1}^\infty. \tag{12}$$

Let C_α be given by (9) for the system $\tilde{\Sigma} = \Sigma_\alpha^c$ and $\beta = \beta_\alpha$. Let T_α be the associated time bound as in item (b) of Proposition 2. We also define the following convention $\Sigma_N^c = \Sigma_N$. We can now state our main result:

Theorem 2: Let Σ be a finite system with a nested sequence of subsystems $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$. Under Assumption 1, $(C, X_C^0, T_C, \gamma_C)$ is an ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$, with controller $C = C_0$, set of initial states $X_C^0 = X_N^0$, time bound $T_C = \max(T_0, \ldots, T_N) + 1$ and gain function γ_C given by

$$\forall \alpha \in \mathbb{N}_{\leq N},\ \gamma_C(\alpha) = \beta_\alpha. \tag{13}$$

Moreover, $(C, X_C^0, T_C, \gamma_C)$ is GO-ISA if the following holds:

$$\forall \alpha \in \mathbb{N}_{<N},\ \max_{x\in X_{\alpha+1}^\infty} W_{A,\alpha}^*(x) = \min_{x\in X_{\alpha+1}^\infty} W_{A,\alpha}^*(x). \tag{14}$$

In that case, for any other GO-ISA controller $(C', X_{C'}^0, T_{C'}, \gamma_{C'})$, it holds $\gamma_{C'} = \gamma_C$, $X_{C'}^0 \subseteq X_C^0$ and $C'(x) \subseteq C(x)$, for all $x \in \mathrm{attr}(\Sigma_0, C', X_{C'}^0)$.

The proof of Theorem 2 is presented in the next section. Our approach, based on iterative refinements of least-violating controllers, allows us to compute an ISA controller. Under condition (14), the synthesized controller is a GO-ISA controller. In that case, the computed controller is valid for the largest possible set of initial states and is maximally permissive on the attractor set of the nominal system. Note that condition (14), can be easily checked a posteriori. Intuitively, this condition states that $X_{\alpha+1}^\infty$ should be included in the basin of attraction of the smallest closed-loop attractor of Σ_α^c. Let us remark that even if condition (14) does not hold, our approach has an optimal gain for the worst case disturbance and allows to improve the behavior for lower disturbances. Finally, we would like to emphasize that, even though our approach produces several controllers C_α for $\alpha \in \mathbb{N}_{\leq N}$, only the controller $C = C_0$ is actually applied to the system Σ. In particular, the knowledge of the disturbance is not required by the controller C, which is a state-feedback memoryless controller.

C. Proof of Theorem 2

We start by proving several instrumental results:

Lemma 2: The following assertions hold:

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

Proof: Let us prove the different assertions above.

(i): Let $x \in X$, from (9) we have $C_\alpha(x) \subseteq \mathrm{enab}_{F_\alpha^c}(x)$, and from (11), 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 (9) and $\mathrm{enab}_{F_{\alpha+1}^c}(x) \subseteq \mathrm{enab}_{F_{\alpha+1}}(x)$ by (11). Moreover, by Definition 2, 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 (11), 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) and (iv): We proceed by induction. From (6) and (7), 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 (10), we get that $X_N^\infty \neq \emptyset$. Moreover, we get by (9) and the third equality in (10) that $X_N^\infty = \mathrm{reach}(\Sigma_N, C_N, X_N^\infty)$. Then, let us assume that for some $\alpha \in \mathbb{N}_{<N}$, $X_{\alpha+1}^\infty \neq \emptyset$ and $X_{\alpha+1}^\infty = \mathrm{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X_{\alpha+1}^\infty)$.

We first prove that $X_\alpha^\infty \neq \emptyset$. Let us first assume that $\beta_\alpha < +\infty$. Then, let $x_0 \in X_{\alpha+1}^\infty$, and let us consider a maximal trajectory $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_\alpha^c, C_\alpha, x_0)$. Since $W_{A,\alpha}^*(x_0) \leq \beta_\alpha < +\infty$ by the first equality in (12), we get from item (b) in Proposition 2 applied to Σ_α^c 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 (11), Definition 2 and (i), we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_0)$. Then, since $X_{\alpha+1}^\infty = \mathrm{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X_{\alpha+1}^\infty)$ and $x_0 \in X_{\alpha+1}^\infty$, we get that for all $t \geq 0$, $x_t \in X_{\alpha+1}^\infty$. It follows that for all $t \geq T_\alpha$, $x_t \in L_{\beta_\alpha}(W_{S,\alpha}^*) \cap X_{\alpha+1}^\infty$. This implies that $L_{\beta_\alpha}(W_{S,\alpha}^*) \cap X_{\alpha+1}^\infty \neq \emptyset$ and thus by the second equality in (12) we get that $X_\alpha^\infty \neq \emptyset$. Assuming now that $\beta_\alpha = +\infty$, we get from the second equality in (12) that $X_\alpha^\infty = X_{\alpha+1}^\infty \neq \emptyset$, by the induction hypothesis.

We now prove that $X_\alpha^\infty = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty)$. From Definition 2, (i) and the second equality in (12) we get that $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty) \subseteq \mathrm{reach}(\Sigma_{\alpha+1}, C_{\alpha+1}, X_{\alpha+1}^\infty)$, which from the induction hypothesis gives $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty) \subseteq X_{\alpha+1}^\infty$. From the second equality in (12), we also get that $X_\alpha^\infty \subseteq L_{\beta_\alpha}(W_{S,\alpha}^*)$. Then, from (9), we get that $\mathrm{reach}(\Sigma_\alpha^c, C_\alpha, X_\alpha^\infty) \subseteq L_{\beta_\alpha}(W_{S,\alpha}^*)$. From (i) and (11), we get that $\mathrm{reach}(\Sigma_\alpha^c, C_\alpha, X_\alpha^\infty) = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty)$. Hence, we get that $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty) \subseteq L_{\beta_\alpha}(W_{S,\alpha}^*) \cap X_{\alpha+1}^\infty$. Then by the second equality in (12), we get $\mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty) \subseteq X_\alpha^\infty$. Since we always have $X_\alpha^\infty \subseteq \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty)$, it follows that $X_\alpha^\infty = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty)$.

Hence, we have proved by induction that for all $\alpha \in \mathbb{N}_{\leq N}$, $X_\alpha^\infty \neq \emptyset$ and $X_\alpha^\infty = \mathrm{reach}(\Sigma_\alpha, C_\alpha, X_\alpha^\infty)$. The fact that for all $\alpha \in \mathbb{N}_{<N}$, $X_\alpha^\infty \subseteq X_{\alpha+1}^\infty$ follows directly from the second equality in (12). Hence (iii) and (iv) are proved.

(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 (11), Definition 2 and (ii) we get that $(x_t)_{t=0}^T \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}^c, C_{\alpha+1}, x_0)$. Moreover, we have from (6), (7) and the second inequality in (12) 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 $\Sigma_{\alpha+1}^c$, $(x_t)_{t=0}^T$ 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_α^c, 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 3: 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) $\forall \alpha \in \mathbb{N}_{\leq N},\ \mathrm{dom}(C_\alpha) = X_N^0 \neq \emptyset$;
(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 $x_0 \in X_N^0$ is complete and satisfies for all $t \geq T'_\alpha$, $x_t \in X_\alpha^\infty$;
(ix) $X_N^0 = \mathrm{reach}(\Sigma_N, C_N, X_N^0)$.

Proof: Let us prove the different assertions above.

(vi): Under Assumption 1, 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, for all $t \geq 0$,

$H(x_t) \leq \max_{x\in X} H(x)$. Then, from Proposition 2, $W^*_A(x_0) \leq \max_{x\in X} H(x) < +\infty$ where the last inequality follows from X being a finite set. Then, we get from the first equality in (10) that $\beta_N < +\infty$. Then for $\alpha \in \mathbb{N}_{<N}$, we have from (iii) and (v) in Lemma 2 that $\beta_\alpha = \max_{x\in X^\infty_{\alpha+1}} W^*_{A,\alpha}(x) \leq \beta_{\alpha+1}$. Thus, (vi) is proved.

(vii) and (viii): We proceed by induction. From (9), (vi), we get that $\mathrm{dom}(C_N) = L_{\beta_N}(W^*_{A,N})$ and from the first and second equalities in (10), 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 $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_N, C_N, x_0)$ 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 (10). 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 2 that $\mathrm{dom}(C_\alpha) \subseteq \mathrm{dom}(C_{\alpha+1}) = X^0_N$. Let us prove the converse inclusion. Let us consider a controller $\tilde{C}_\alpha$ defined for all $x \in X$ as follows:

$$\tilde{C}_\alpha(x) = \begin{cases} C_{\alpha+1}(x) & \text{if } x \in X \setminus X^\infty_{\alpha+1}; \\ C_\alpha(x) & \text{if } x \in X^\infty_{\alpha+1}. \end{cases} \tag{15}$$

From (ii) in Lemma 2, we can consider $\tilde{C}_\alpha$ as a controller for Σ^c_α. Then, let $x_0 \in X^0_N$, and $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma^c_\alpha, \tilde{C}_\alpha, x_0)$. Let us assume that for all $t \in \mathbb{N}_{\leq T}$, $x_t \notin X^\infty_{\alpha+1}$. Then, $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_{\alpha+1}, x_0)$. From (11) and Definition 2, it follows that $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_0)$. Then, from the induction hypothesis, $(x_t)^T_{t=0}$ 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, $(x_t)^T_{t=\tau} \in \mathscr{T}_{\max}(\Sigma^c_\alpha, \tilde{C}_\alpha, x_\tau)$. From (11) and Definition 2 and (i) in Lemma 2, we have that $(x_t)^T_{t=\tau} \in \mathscr{T}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_\tau)$, which together with (iv) in Lemma 2 gives that $x_t \in X^\infty_{\alpha+1}$, for all $\tau \leq t \leq T$. Then, $(x_t)^T_{t=\tau} \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_\alpha, x_\tau)$. 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 $(x_t)^T_{t=\tau}$ 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, $x_0 \in L_{\beta_\alpha}(W^*_{A,\alpha}) = \mathrm{dom}(C_\alpha)$ by (9) and (vi). Thus, $X^0_N \subseteq \mathrm{dom}(C_\alpha)$ and (vii) holds for α.

Let $x_0 \in X^0_N$ and $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_\alpha, C_\alpha, x_0)$. Then, from (11) and (i) in Lemma 2, $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma^c_\alpha, C_\alpha, x_0)$. Since $X^0_N = \mathrm{dom}(C_\alpha) = L_{\beta_\alpha}(W^*_{A,\alpha})$, we get from item (b) of Proposition 2 applied to Σ^c_α that $(x_t)^T_{t=0}$ is complete and satisfies $x_t \in L_{\beta_\alpha}(W^*_{S,\alpha})$, for all $t \geq T_\alpha$. Moreover, by Definition 2 and (i) in Lemma 2, $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_{\alpha+1}, C_{\alpha+1}, x_0)$. 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 (12) 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 $X^0_N \subseteq \mathrm{reach}(\Sigma_N, C_N, X^0_N)$. 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 $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_N, C_N, x_0)$ are complete. This implies that $\mathrm{reach}(\Sigma_N, C_N, X^0_N) \subseteq \mathrm{dom}(C_N)$. Since by (vii), $\mathrm{dom}(C_N) = X^0_N$ we get that $\mathrm{reach}(\Sigma_N, C_N, X^0_N) \subseteq X^0_N$. ∎

We can now provide the core proof of Theorem 2:

Proof: From (vii) in Lemma 3, we have $X^0_C = X^0_N \neq \emptyset$. Also from (vi) in Lemma 3, 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 3.

Let $x_0 \in X^0_C$ and $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma, C, x_0)$, then from (i) in Lemma 2 and (vii) in Lemma 3, we get that $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_N, C_N, x_0)$. Then, by (viii) in Lemma 3, we get that $(x_t)^T_{t=0}$ is complete and by (ix) in Lemma 3, $x_t \in X^0_N$, for all $t \geq 0$. Let $(\alpha_t)^{T-1}_{t=0}$ be the level of disturbances associated to $(x_t)^T_{t=0}$. Let $t \geq T_C$ and $\tilde{\alpha} = \max_{t-T_C \leq s < t} \alpha_s$. Then, from (i) in Lemma 2 and Definition 2, we get that $(x_s)^t_{s=t-T_C} \in \mathscr{T}(\Sigma_{\tilde{\alpha}}, C_{\tilde{\alpha}}, x_{t-T_C})$. Moreover, by (viii) in Lemma 3, 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 (10), the second equality in (12) and by (4), (5), we get that $H(x_t) \leq W_{S,\tilde{\alpha}}(x_t) \leq \beta_{\tilde{\alpha}}$. Therefore $(C, X^0_C, T_C, \gamma_C)$ is an ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq N}}$.

Let $(C', X^0_{C'}, T_{C'}, \gamma_{C'})$ be a GO-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 $(C', X^0_{C'}, T_{C'}, \gamma_{C'})$ 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 (10), we get that $\beta_N \leq \gamma_{C'}(N)$. Moreover, since $(C', X^0_{C'}, T_{C'}, \gamma_{C'})$ is a GO-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 (10).

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

$$\begin{aligned} \gamma_{C'}(\alpha) &= \beta_\alpha, \\ \mathrm{attr}(\Sigma_\alpha, C', X^0_{C'}) &\subseteq X^\infty_\alpha, \\ C'(x) &\subseteq C_\alpha(x),\ \forall x \in \mathrm{attr}(\Sigma_\alpha, C', X^0_{C'}). \end{aligned} \tag{16}$$

We start with the case $\alpha = N$. We already proved that $\gamma_{C'}(N) = \beta_N$. Since $(C', X^0_{C'}, T_{C'}, \gamma_{C'})$ is an ISA controller we have $\mathrm{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\gamma_{C'}(N)}(H)$. Moreover from Lemma 1, we get that $\mathrm{attr}(\Sigma_N, C', X^0_{C'})$ is a controlled invariant of Σ_N. Hence, it follows from Proposition 1 that $\mathrm{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\gamma_{C'}(N)}(W^*_{S,N})$. From $\gamma_{C'}(N) = \beta_N$ and the third equality of (10), we get that $\mathrm{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\beta_N}(W^*_{S,N}) = X^\infty_N$. Then, let $x \in \mathrm{attr}(\Sigma_N, C', X^0_{C'})$ and $u \in C'(x)$, then by (3) in Lemma 1, $F_N(x,u) \subseteq \mathrm{attr}(\Sigma_N, C', X^0_{C'}) \subseteq L_{\beta_N}(W^*_{S,N})$. Morever $W^*_{S,N}(x) \leq \beta_N$, then $u \in C_N(x)$ by (9). Therefore, (16) holds for $\alpha = N$.

Now let $\alpha \in \mathbb{N}_{<N}$, and let us assume that (16) holds for $\alpha+1$. We show that (16) holds for α. Let $x_0 \in \mathrm{attr}(\Sigma_\alpha, C', X^0_{C'})$, and $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_\alpha, C', x_0)$. Then, from Definition 7, there exists $\tilde{x}_0 \in X^0_{C'}$, $(\tilde{x}_t)^{\tilde{T}}_{t=0} \in \mathscr{T}_{\max}(\Sigma_\alpha, C', \tilde{x}_0)$ and $\tau \geq T_{C'}$ such that $\tilde{x}_\tau = x_0$. Consider the trajectory $(\bar{x}_t)^{T+\tau}_{t=0}$ where $\bar{x}_t = \tilde{x}_t$ if $t \leq \tau$ and $\bar{x}_t = x_{t-\tau}$ if $t > \tau$. Then, $(\bar{x}_t)^{T+\tau}_{t=0} \in \mathscr{T}_{\max}(\Sigma_\alpha, C', \tilde{x}_0)$. Since $(C', X^0_{C'}, T_{C'}, \gamma_{C'})$ is an ISA controller we get that $(\bar{x}_t)^{T+\tau}_{t=0}$ 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 $(x_t)^T_{t=0} \in \mathscr{T}_{\max}(\Sigma_\alpha, C', x_0)$ is complete and for all $t \geq 0$, $H(x_t) \leq \gamma_{C'}(\alpha)$. Moreover, by (3) in Lemma 1, we get that $x_t \in \mathrm{attr}(\Sigma_\alpha, C', X^0_{C'})$, 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 2, 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 (12) and by (14) that $W^*_{A,\alpha}(x_0) = \beta_\alpha$. This gives us $\beta_\alpha \leq \gamma_{C'}(\alpha)$. Since $(C', X^0_{C'}, T_{C'}, \gamma_{C'})$ is a GO-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 (12), 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 (3) 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 (9). Then, (16) holds for α. Hence, (16) holds for all $\alpha \in \mathbb{N}_{\leq N}$ and the theorem is proved. ■

IV. Numerical example

In this section, we use our approach for adaptive cruise control.

A. Mathematical model, specification and abstraction

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 $v_1 \in [v_1^{\min}, v_1^{\max}]$ and $v_2 \in [v_2^{\min}, v_2^{\max}]$, 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 [10]:

$$\begin{cases} \dot{d} & = v_1 - v_2 \\ \dot{v}_1 & = u - \frac{f_0 + f_1 v_1 + f_2 v_1^2}{M} \\ \dot{v}_2 & = \Gamma(v_2, w) \end{cases} \tag{17}$$

where the function Γ ensures that $v_2 \in [v_2^{\min}, v_2^{\max}]$ at all time: $\Gamma(v_2, w) = w$ if $v_2 \in (v_2^{\min}, v_2^{\max})$; $\Gamma(v_2, w) = \max(0, w)$ if $v_2 = v_2^{\min}$; $\Gamma(v_2, w) = \min(0, w)$ if $v_2 = v_2^{\max}$. The control input $u \in [u^{\min}, u^{\max}]$ accounts for the contribution of braking and engine torque to the acceleration of vehicle 1. M is 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 $w \in [w^{\min}, w^{\max}]$ represents the acceleration of vehicle 2. Values of parameters, compatible with empirical measurements are taken from [10] and given in Table I. We consider the sampled version of (17) with time step $\tau = 0.5\,s$.

We consider the problem of designing an adaptive cruise control system. Let us define the time headway $\vartheta = -d/v_1$. 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 $\vartheta \geq \vartheta^*$ and maintain the velocity v_1 at the desired value v^*, or
- keep velocity $v_1 \leq v^*$ and maintain the time headway ϑ at the desired value ϑ^*.

We formalize this specification as synthesizing a controller enforcing uniform attractivity of the set $\mathcal{X}^* = \left\{(d, v_1, v_2) \in \mathbb{R}^3 \mid (-d/v_1, v_1) \in \mathcal{Y}^*\right\}$ where $\mathcal{Y}^* = [\vartheta^*, +\infty) \times \{v^*\} \cup \{\vartheta^*\} \times (-\infty, v^*]$. One can check that there does not exist a controller rendering $\mathcal{X}^*$ invariant. Hence, uniform attractivity of $\mathcal{X}^*$ 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:

$$h(d, v_1, v_2) = \min_{(\vartheta', v_1') \in \mathcal{Y}^*} \max\left(|-d/v_1 - \vartheta'|, \alpha|v_1 - v_1'|\right) \tag{18}$$

where $\alpha > 0$ is a design parameter defining the relative tolerance to deviations from the desired velocity and from the desired time headway. The parameter values of the specification are as follows: $\vartheta^* = 1.5\,s$, $v^* = 20\,m/s$, $\alpha = 1.5$.

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

We compute a symbolic model of (17) in the form of a transition system Σ using the approach described in [2]. To define the set of symbolic states, 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 30 sub-intervals; and for the sets of velocities, we use 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 separated by $(u^{\max} - u^{\min})/20$. A nested sequence of abstractions $\{\Sigma_\alpha\}_{\alpha \in \mathbb{N}_{\leq 2}}$ is computed corresponding to increasing intervals of disturbances $[2^{\alpha-2} w^{\min}, 2^{\alpha-2} w^{\max}]$ for $\alpha = 0, 1, 2$. To guarantee that the transition relations F_α satisfy the property of Definition 2 (i.e. larger values of α produce increased non-determinism), it is sufficient when computing the abstraction to use a method that produces larger over-approximations of the reachable set for larger sets of disturbances. Note that is the case of the method in [2] that is used in the following. We also lift the distance function (18) to the symbolic model by defining H as the maximal value of h on the element of the partition associated to a given symbolic state.

TABLE I: Model and specification parameter values

M	1370	kg	u^{min}	-3	m/s^2	$v_1^{\min}$	5	m/s
f_0	51	N	$u^{\max}$	2	m/s^2	$v_1^{\max}$	30	m/s
f_1	1.257	Ns/m	$w^{\min}$	-3.2	m/s^2	$v_2^{\min}$	12	m/s
f_2	0.434	Ns^2/m^2	$w^{\max}$	3.2	m/s^2	$v_2^{\max}$	28	m/s

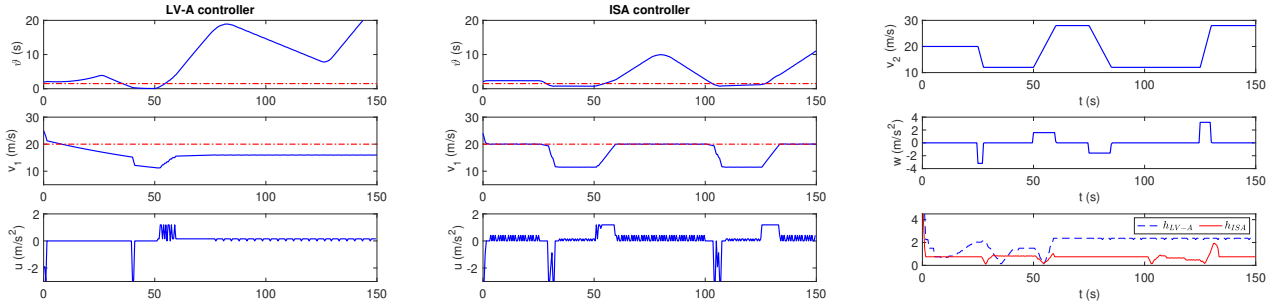

Fig. 2: Trajectories of system (17) using a LV-A controller proposed in [5] (left) and our proposed ISA controller (center): evolution of the time headway, of the velocity of vehicle 1 and control input are represented in the plots where the target time headway ϑ^* and target velocity v^* are represented 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).

B. Synthesis of an ISA controller

We used the approach presented in Section III to synthesize an ISA controller $(C, X_C^0, T_C, \gamma_C)$ for the nested sequence of abstractions $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq 2}}$. Note that the strong safety requirements can be satisfied by disabling in the abstraction all inputs potentially leading to relative positions $d \geq 0$ or to velocities $v_1 \in [v_1^{\min}, v_1^{\max}]$.

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 controller $C = C_0$. We can see that the overhead of computing the ISA controller $(C, X_C^0, T_C, \gamma_C)$ in comparison to computing the LV-A C_2 is not so much. The 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 (14) of Theorem 2 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 $\max_{x\in X_1^\infty} W_{A,0}^*(x) = 1.50$ when $\min_{x\in X_1^\infty} W_{A,0}^*(x) = 1.11$. Therefore, $(C, X_C^0, T_C, \gamma_C)$ is an ISA controller but may not be a GO-ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\mathbb{N}_{\leq 2}}$. However, since (14) is satisfied for $\alpha = 1$, $(C, X_C^0, T_C, \gamma_C)$ is a GO-ISA controller for $\{\Sigma_\alpha\}_{\alpha\in\{1,2\}}$.

In Figure 2, we show a simulation of system (17) using a least-violating attractivity 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.

V. CONCLUSIONS

In this paper, we introduced the notion of GO-ISA controllers for finite state systems subject to disturbances of varying levels. We have developed algorithms for computing such controllers, these algorithms can be used in combination with symbolic control techniques. An application to adaptive cruise control shows the performance improvement of ISA controllers compared to LV-A controllers. In the future, we plan to work on developing other algorithms for the synthesis of GO-ISA controllers when the condition (14) is not satisfied. We would also like to develop algorithms for synthesizing ISA controllers that are gain-optimal 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] J. Liu and N. Ozay. Finite abstractions with robustness margins for temporal logic-based control synthesis. *Nonlinear Analysis: Hybrid Systems*, 22:1–15, 2016.

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

[10] 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.

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

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

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

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

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

[20] 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.

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

[22] L. Yang, D. Rizzo, M. Castanier, and N. Ozay. Parameter sensitivity analysis of controlled invariant sets via value iteration. In *American Control Conference*, pages 4737–4744. IEEE, 2020.

[23] 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.