



HAL
open science

Symbolic observer-based controller for uncertain nonlinear systems

W. A. Apaza-Perez, Antoine Girard, Christophe Combastel, Ali Zolghadri

► **To cite this version:**

W. A. Apaza-Perez, Antoine Girard, Christophe Combastel, Ali Zolghadri. Symbolic observer-based controller for uncertain nonlinear systems. *IEEE Control Systems Letters*, 2021, 5 (4), pp.1297-1302. 10.1109/LCSYS.2020.3034274 . hal-02995397

HAL Id: hal-02995397

<https://hal.science/hal-02995397v1>

Submitted on 9 Nov 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Symbolic observer-based controller for uncertain nonlinear systems*

W.A. Apaza-Perez¹, A. Girard¹, C. Combastel², A. Zolghadri²

Abstract—Symbolic control is an approach to the control of continuous or hybrid systems with specifications expressed in a logic form. This approach is based on the use of symbolic models describing the dynamical system behavior with a finite description of the transition relation between its states. In the literature, many results using this approach assume the availability of full and exact information about the system states to compute the control actions. In this paper, we consider a more realistic scenario where only partial information about the plant states is available. This paper proposes an abstraction that makes it possible to synthesize output-feedback controllers. The presence of disturbances and output noise is also considered. A direct path between observer designs in the classical theory and control synthesis in formal methods is established and a numerical example is provided to illustrate the results.

I. INTRODUCTION

Over the last decades, the problem of control design for systems with complex specifications has spurred on substantial research efforts that have been developing along several major lines. One appealing direction takes advantage of the so-called *formal methods* and is based on symbolic models. These models are abstractions which are related to the dynamics of the system by some formal behavioral relationship such as alternating simulations [1] or feedback refinement relations [2]. This allows to capture aspects of the system being analyzed explaining how the results of analysis/design for the symbolic model can be used in the system, see for example [1], [3], [4], [5]. Finite state models are especially well suited for automated analysis and offer a common language to describe an abstract view of continuous dynamics as well as the software implementation of control algorithms [6]. It is, therefore, possible to formally reason about the behavior of the interconnection between continuous dynamics and software which has been one of the main thrusts behind the research area of hybrid systems. Classical control theory provides a wide range of results to control of continuous or hybrid systems where control objectives are usually aimed at satisfying specifications such as stabilization, output tracking or disturbance rejection; while symbolic control and systems allow us to consider more complex specifications expressed in some formal syntax (e.g. linear temporal logic LTL,

computational tree logic). The use of symbolic models for control design purposes has been investigated, among many others, in the following papers: LTL specifications for linear control systems by [7], [8], and for discrete time piecewise affine systems by [9], [10]; nonlinear control systems with general specifications in a behavioral framework by [1], [11], [2], and with specifications expressed as nondeterministic transition systems by [12]; nonlinear switched systems and safety and reachability specifications were considered in [13], [14]; networked nonlinear control systems and specifications expressed as nondeterministic transition systems in [15], [16]. [17] considers safety specifications and overlapping symbolic models. Along theoretical results, computational tools have also been developed to compute abstractions and control synthesis PESSOA [18], CoSyMa [19], TuLiP [20], SCOTS [21], pFaces [22], or Mascot [23]. Apart from differences in the classes of specifications and of plants considered, the common denominator of the papers above is in assuming full information on the state of the plant for control purposes. The issue is that this assumption may become very restrictive in many real applications where only output variables, or sensor measurements of them, are available.

The aim of the paper is to overcome the crucial assumption about full and exact knowledge of the states of the system for the controller synthesis. We use observers to define an abstraction, which allows us to cover a wide class of systems (linear and nonlinear) due to the extensive literature on observer design in the classical control theory for continuous or hybrid systems [24], [25], and complex specifications can be considered [26]. The proposed observer-based approach to synthesize symbolic controllers for systems with partial information and bounded disturbances has some important features: i) The abstraction is related to a feedback refinement relation of the system formed by the plant and the observer, ii) Computing the abstraction is solely based on the dynamics of the plant and only requires the knowledge of some bounds on the estimation error of the observer, iii) Controller refinement only requires feeding the obtained symbolic controller with the state estimate of the observer.

Some recent works on observer/estimator-based abstractions for control with partial information can be found in [27], [28], [29], [30], [31]. The observer design can be realized from the initial dynamic system as it is done in [27] and [28] where discrete-time linear systems with LTL specifications, and a class of discrete-time piecewise-affine systems with a robust interpretation of LTL were considered respectively. In comparison, in the current work, the approach allows considering linear and non-linear systems with uncertainties. In another way, the estimation of the non-measurable states can also be done at the symbolic level as it has been done works [29], [30], [31] but this demands the use of more computational

*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); and the French State, managed by the French National Research Agency (ANR) in the frame of the "Investments for the future" Programme IdEx Bordeaux - SysNum (ANR-10-IDEX-03-02).

¹W.A. Apaza-Perez, 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

²C. Combastel, A. Zolghadri are with the Univ. of Bordeaux, CNRS, IMS, UMR 5218, 33405 Talence, France {christophe.combastel, ali.zolghadri}@u-bordeaux.fr

resources due to the handling of sets of symbolic states as estimators.

The remainder of the paper is organized as follows. Section II presents some preliminary notions. The problem is formally stated and the main results are presented in section III. In section IV, a numerical example is presented to illustrate technical results. Finally, section V concludes the paper with some remarks.

II. PRELIMINARIES

Notations. $\mathbb{R}, \mathbb{R}_{>0}, \mathbb{R}_{\geq 0}$, and \mathbb{N}_0 denote the set of real, positive real, non negative real numbers, and non negative integers, respectively. Given $a, b \in \mathbb{N}_0$ such that $a \leq b$, we denote by $[a; b]$ a closed interval in \mathbb{N}_0 . Given a relation $R \subseteq X \times Y$ and $X' \subseteq X$, we have $R(X') = \{y \in Y \mid \exists x \in X', (x, y) \in R\}$. Consider a vector $x \in \mathbb{R}^n$, we denote by x_i the i -th component of x and by $\|x\|$ the Euclidean norm of x . For $\varepsilon \in \mathbb{R}_{\geq 0}^n$, $x \in \mathbb{R}^n$ and $A \subseteq \mathbb{R}^n$, define the ε -expansion of A as the set $N_\varepsilon(A) = \{y \in \mathbb{R}^n \mid \exists x \in A, \forall i \in [1; n], |y_i - x_i| \leq \varepsilon_i\}$, and a hyper rectangle with center x and radius ε as $N_\varepsilon(x) = \{y \in \mathbb{R}^n \mid \forall i \in [1; n], |y_i - x_i| \leq \varepsilon_i\}$. Given a function $V : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$ and $k \in \mathbb{R}_{\geq 0}$, its gradient is denoted by ∇V and $V^{-1}(\leq k) = \{x \in X \mid V(x) \leq k\}$. A continuous function $\gamma : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is said to belong to class κ (resp. κ_∞) if it is strictly increasing and $\gamma(0) = 0$ (and $\gamma(r) \rightarrow \infty$ when $r \rightarrow \infty$). X^+ denotes the set of finite sequences of elements in X .

A. Transition systems.

Abstractions are dynamical systems with finitely many states and input values, each of which symbolizes aggregates of states and inputs of the original system. Abstractions are mathematically modeled as transition systems [1].

Definition 1 (Transition system): A transition system S 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*.

The notation $F(x, u) = \{x' \in X \mid (x, u, x') \in F\}$ denotes the set of successors of x upon control input u . Since $F(x, u)$ may be empty, we denote $U(x) = \{u \in U \mid F(x, u) \neq \emptyset\}$. A system is called *nonblocking* if the set $U(x)$ of every $x \in X$ is nonempty. A transition $(x, u, x') \in F$ is also denoted by $x \xrightarrow{u} x'$ and an infinite sequence of transitions $x_0 \xrightarrow{u_0} x_1 \xrightarrow{u_1} x_2 \xrightarrow{u_2} \dots$ by $(x_i^{u_i})_{i \in \mathbb{N}_0}$, where the set of all infinite sequences of transitions in X is denoted by $(X \times U)^\omega$. A *state-feedback control* C is a partial function on non-empty sequences of states of the system

$$C : X \times (U \times X)^+ \rightarrow 2^U \quad (1)$$

$$(x_0, u_0, x_1, u_1, \dots, u_{k-1}, x_k) \mapsto U_k$$

where U_k is a set of admissible inputs to be used in the subsequent k -step. The behaviour generated by a system S and a state-feedback control C is denoted as $\mathcal{B}(S, C)$ and consists of all infinite sequences $(x_i^{u_i})_{i \in \mathbb{N}_0} \in (X \times U)^\omega$ that satisfies $u_i \in C(x_0, u_0, \dots, u_{i-1}, x_i)$ and $x_i \xrightarrow{u_i} x_{i+1}$ for all $i \in \mathbb{N}_0$. Given $\varepsilon \in \mathbb{R}_{>0}^n$, the ε -expansion of $\mathcal{B}(S, C)$ is defined as $N_\varepsilon(\mathcal{B}(S, C)) = \{(y_i^{u_i})_{i \in \mathbb{N}_0} \in (X \times U)^\omega \mid \exists (x_i^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}(S, C) \wedge \forall i \in \mathbb{N}_0, |x_i - y_i| \leq \varepsilon_i\}$.

Consider a transition system $S = (X, U, F)$, where $X \subseteq X_1 \times X_2$, and a state-feedback control C in the system S . The projection of $\mathcal{B}(S, C)$ over X_1 , denoted by $\mathcal{B}_{X_1}(S, C)$, is defined as $\mathcal{B}_{X_1}(S, C) = \{(x_i^{u_i})_{i \in \mathbb{N}_0} \in (X \times U)^\omega \mid \exists (\tilde{x}_i, z_i^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}(S, C) \wedge \forall i \in \mathbb{N}_0, x_i = \tilde{x}_i\}$, and the projection over X_2 is defined analogously.

Definition 2: Given two transition systems $S_a = (X_a, U_a, F_a)$ and $S_b = (X_b, U_b, F_b)$ with $U_b \subseteq U_a$. A relation $R \subseteq X_a \times X_b$ is a *feedback refinement relation* from S_a to S_b if $\forall x_a \in X_a, \exists x_b \in X_b, (x_a, x_b) \in R$ and the following holds for all $(x_a, x_b) \in R$:

$$U_b(x_b) \subseteq U_a(x_a); \quad (2)$$

$$u \in U_b(x_b) \implies R(F_a(x_a, u)) \subseteq F_b(x_b, u).$$

Feedback refinement relation allows the designer to work with the abstract system S_b instead of the concrete system S_a . Under conditions in (2), a controller for the abstract system S_b can be used on the concrete system S_a , see [2].

III. PROBLEM STATEMENT

Consider the following nonlinear continuous-time system

$$\begin{cases} \dot{\xi}(t) = f(\xi(t), u(t), w(t)) \\ y(t) = h(\xi(t), \delta(t)) \end{cases} \quad (3)$$

where $\xi(t) \in \mathcal{X} \subseteq \mathbb{R}^n$, $u(t) \in \mathcal{U} \subseteq \mathbb{R}^p$, $y(t) \in \mathcal{Y} \subseteq \mathbb{R}^m$ denote the state, the control input, the measured output at time $t \in \mathbb{R}_{\geq 0}$, respectively. The uncertainties denoted by $w(t) \in \mathcal{W} \subseteq \mathbb{R}^{r_1}$ and $\delta(t) \in \mathcal{D} \subseteq \mathbb{R}^{r_2}$ are bounded, i.e. there exist $b_1, b_2 \in \mathbb{R}_{\geq 0}$ such that $\forall t \in \mathbb{R}_{\geq 0}, \|w(t)\| \leq b_1, \|\delta(t)\| \leq b_2$.

The problem considered in the paper can be roughly formulated as follows: how to build abstractions which take into account disturbances and partial information of the system and how to synthesize output feedback controllers.

A. Observer and discrete abstraction

Assume there exist:

- i) An observer for the system (3), which is expressed by

$$\dot{\hat{\xi}}(t) = g(\hat{\xi}(t), u(t), y(t)), \quad (4)$$

where $\hat{\xi}(t) \in \hat{\mathcal{X}} \subseteq \mathbb{R}^n$. It is assumed that the observer has been synthesized by some method, e.g. [32], [33].

- ii) class- κ_∞ functions $\underline{\alpha}, \bar{\alpha}$, class- κ functions $\beta, \gamma_1, \gamma_2$, and a positive-definite function $V : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$ such that into the dynamic of the estimation error

$$\dot{z}(t) = G(z(t), \xi(t), u(t), w(t), \delta(t)), \quad (5)$$

where $z(t) = \hat{\xi}(t) - \xi(t)$, the following conditions hold

$$\underline{\alpha}(\|z\|) \leq V(z) \leq \bar{\alpha}(\|z\|) \quad (6)$$

$$\begin{aligned} \nabla V(z(t)) \cdot G(z(t), \xi(t), u(t), w(t), \delta(t)) \leq & (7) \\ -\beta(V(z(t))) + \gamma_1(\|w(t)\|) + \gamma_2(\|\delta(t)\|). & \end{aligned}$$

Consider the composition of system (3) and the observer (4) given by

$$\begin{cases} \dot{\xi}(t) = f(\xi(t), u(t), w(t)), \\ \dot{\hat{\xi}}(t) = g(\hat{\xi}(t), u(t), h(\xi(t), \delta(t))), \end{cases} \quad (8)$$

where forward completeness is assumed, and define the state space \mathcal{J} as

$$\mathcal{J} = \{(x, \hat{x}) \in \mathcal{X} \times \hat{\mathcal{X}} \mid V(x - \hat{x}) \leq \beta^{-1}(\gamma_1(b_1) + \gamma_2(b_2))\}. \quad (9)$$

Note that condition (7) ensures that \mathcal{J} is a forward invariant set. Since we are interested in controlling the system (3) through a digital and quantized controller, the controls are assumed piecewise constant functions from R_0^+ to \mathcal{U} such that given $\tau \in \mathbb{R}_{>0}$, $u(t) = u(k\tau)$ for all $t \in [k\tau, (k+1)\tau[$ and $k \in \mathbb{N}_0$. The τ -sampled system from (8) is given as

$$S_1 = (X_1, U_1, F_1) \quad (10)$$

with state space $X_1 = \mathcal{J}$, input space $U_1 = \mathcal{U}$ and a transition function $F_1((x, \hat{x}), u) := \{(x', \hat{x}') \mid \exists (\xi, \hat{\xi}) \text{ a solution of (8) with } u \in U_1 \wedge (\xi(0), \hat{\xi}(0)) = (x, \hat{x}) \wedge (\xi(\tau), \hat{\xi}(\tau)) = (x', \hat{x}')\}$.

Consider uniform grids

$$\begin{aligned} \eta\mathbb{Z}^n &= \{q \in \mathbb{R}^n \mid \exists k \in \mathbb{Z}^n, \forall i \in [1; n] q_i = k_i \eta_i\}, \\ \mu\mathbb{Z}^p &= \{u \in \mathbb{R}^p \mid \exists k \in \mathbb{Z}^p, \forall i \in [1; p] u_i = k_i \mu_i\}, \end{aligned}$$

with $\eta \in \mathbb{R}_{>0}^n$ and $\mu \in \mathbb{R}_{>0}^p$. Given $\varepsilon \in \mathbb{R}_{\geq 0}^n$, define a system

$$S_2 = (X_2, U_2, F_2) \quad (11)$$

with $X_2 = 2\eta\mathbb{Z}^n \cap \hat{\mathcal{X}}$, $U_2 = \mu\mathbb{Z}^p \cap U_1$, and

$$F_2(q, u) = \{q' \in X_2 \mid N_\varepsilon(F_0(N_{\varepsilon+\eta}(q), u)) \cap N_\eta(q') \neq \emptyset\},$$

where given a set $A \subseteq \mathcal{X}$,

$$F_0(A, u) := \left\{ x' \in \mathcal{X} \mid \begin{array}{l} \exists x \in A, \exists \xi \text{ a solution of (3) with} \\ u \in U_2 \wedge \xi(0) = x \wedge \xi(\tau) = x' \end{array} \right\}.$$

The quantizer map from $\hat{\mathcal{X}}$ to X_2 is denoted Q and defined as $Q(\hat{x}) = \{q \in X_2 \mid \hat{x} \in N_\eta(q)\}$. The behavior of the transition relation F_2 defined in (11) is illustrated in Figure 1.

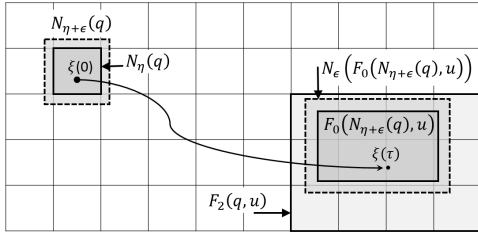


Fig. 1. Transition relation F_2 defined in S_2 : if the estimation error between ξ and $\hat{\xi}$ is included in the ε -expansion of $N_\eta(q)$, then its effect on the dynamics F_0 under u is included in ε -expansion of $F_0(N_{\varepsilon+\eta}(q), u)$.

The following theorem allows us to define a feedback refinement relation between S_1 and S_2 .

Theorem 3: Consider the systems (10) and (11), then the relation

$$R = \{((x, \hat{x}), q) \in X_1 \times X_2 \mid \hat{x} \in N_\eta(q)\}, \quad (12)$$

defines a *feedback refinement relation* from S_1 to S_2 if $V^{-1}(\leq \beta^{-1}(\gamma_1(b_1) + \gamma_2(b_2))) \subseteq N_\varepsilon(0)$. \triangle

Proof. Let $((x, \hat{x}), q) \in R$, $u \in U_2(q) \subseteq U_1((x, \hat{x}))$. The proof is reduced to guarantee the following inclusion $R(F_1((x, \hat{x}), u)) \subseteq F_2(q, u)$. Consider $\tilde{q} \in R(F_1((x, \hat{x}), u))$, then there exists $(x', \hat{x}') \in F_1((x, \hat{x}), u)$ such that

$$\hat{x}' \in N_\eta(\tilde{q}), \quad (13)$$

by (12). As \mathcal{J} is a forward invariant set from (6)-(7), then $F_1((x, \hat{x}), u) \subseteq \mathcal{J}$. Consequently, $V(x' - \hat{x}') \leq \beta^{-1}(\gamma_1(b_1) + \gamma_2(b_2))$, which implies

$$\forall i \in [1; n], |x'_i - \hat{x}'_i| \leq \varepsilon_i, \quad (14)$$

by $V^{-1}(\leq \beta^{-1}(\gamma_1(b_1) + \gamma_2(b_2))) \subseteq N_\varepsilon(0)$. From (14), we obtain

$$\hat{x}' \in N_\varepsilon(F_0(x, u)). \quad (15)$$

As $((x, \hat{x}), q) \in R$, then $(x, \hat{x}) \in \mathcal{J}$ which implies $x - \hat{x} \in V^{-1}(\leq \beta^{-1}(\gamma_1(b_1) + \gamma_2(b_2)))$ by (9). Consequently,

$$\forall i \in [1; n], |x_i - \hat{x}_i| \leq \varepsilon_i. \quad (16)$$

As $\hat{x} \in N_\eta(q)$, then $x \in N_{\varepsilon+\eta}(q)$ by (16), and $F_0(x, u) \subseteq F_0(N_{\varepsilon+\eta}(q), u)$. Thus, $N_\varepsilon(F_0(x, u)) \subseteq N_\varepsilon(F_0(N_{\varepsilon+\eta}(q), u))$ holds. From (15), it is ensured that $\hat{x}' \in N_\varepsilon(F_0(N_{\varepsilon+\eta}(q), u))$ which implies with (13) that $N_\eta(\tilde{q}) \cap N_\varepsilon(F_0(N_{\varepsilon+\eta}(q), u)) \neq \emptyset$, i.e. $R(F_1((x, \hat{x}), u)) \subseteq F_2(q, u)$. \square

The idea behind the hyper rectangle containing the invariant set is to better manage the precision of the observer which is affected by different disturbances. If a controller can be designed satisfying some specifications based on abstraction (11), then an output feedback controller based on chosen observer can be used to compute controls driving the initial system consistently with the specifications.

Proposition 4: Assume that conditions on Theorem 3 hold, and let $C_2 : X_2 \times (U_2 \times X_2)^+ \rightarrow U_2$ be a control defined in the system (11). If a control $C_1 : X_1 \times (U_2 \times X_1)^+ \rightarrow U_2$ in (10) is defined as $C_1(x_0, \hat{x}_0, u_0, x_1, \hat{x}_1, u_1, \dots, x_k, \hat{x}_k) := C_2(Q(\hat{x}_0), u_0, Q(\hat{x}_1), u_1, \dots, Q(\hat{x}_k))$, then

$$\mathcal{B}_X(S_1, C_1) \subseteq N_{\varepsilon+\eta}(\mathcal{B}(S_2, C_2)). \quad (17)$$

Proof. The proof is reduced to two claims:

Claim 1. $\mathcal{B}_X(S_1, C_1) \subseteq N_\varepsilon(\mathcal{B}_{\hat{\mathcal{X}}}(S_1, C_1))$.

Let $(x_i^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}_X(S_1, C_1)$ then $\exists (\hat{x}_i^{u_i})_{i \in \mathbb{N}_0} \in (\hat{\mathcal{X}} \times U_2)^\omega$,

$$((x_i, \hat{x}_i)^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}(S_1, C_1). \quad (18)$$

From (18) and its projection over $\hat{\mathcal{X}}$, $(\hat{x}_i^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}_{\hat{\mathcal{X}}}(S_1, C_1)$ holds, and $\forall i \in [1; n]$, $|\hat{x}_i - x_i| \leq \varepsilon_i$ by (8)-(9). Consequently, $(x_i^{u_i})_{i \in \mathbb{N}_0} \in N_\varepsilon(\mathcal{B}_{\hat{\mathcal{X}}}(S_1, C_1))$.

Claim 2. $N_\varepsilon(\mathcal{B}_{\hat{\mathcal{X}}}(S_1, C_1)) \subseteq N_{\varepsilon+\eta}(\mathcal{B}(S_2, C_2))$.

Let $(x_i^{u_i})_{i \in \mathbb{N}_0} \in N_\varepsilon(\mathcal{B}_{\hat{\mathcal{X}}}(S_1, C_1))$, then $\exists (\hat{x}_i^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}_{\hat{\mathcal{X}}}(S_1, C_1)$ such that $\forall i \in [1; n]$, $|\hat{x}_i - x_i| \leq \varepsilon_i$. Since control C_1 is defined from C_2 and applying the quantizer Q to the states of $(\hat{x}_i^{u_i})_{i \in \mathbb{N}_0}$, then there exists $(q_i^{u_i})_{i \in \mathbb{N}_0} \in \mathcal{B}(S_2, C_2)$ such that $\forall i \in [1; n]$, $\hat{x}_i \in N_\eta(q_i)$. Consequently $(x_i^{u_i})_{i \in \mathbb{N}_0} \in N_{\varepsilon+\eta}(\mathcal{B}(S_2, C_2))$. \square

Theorem 3 provides an abstraction design which is related by a feedback refinement relation of the system formed by the plant and the observer. It should be pointed out that this abstraction computation is solely based on the dynamics of the plant and only requires the knowledge of some bound ε on the estimation error of the observer, see system S_2 in (11). Proposition 4 allows us to refine a controller C_1 which only requires feeding the obtained symbolic controller C_2 with the state estimate of the observer through the quantizer map Q .

IV. EXAMPLE: ADAPTIVE CRUISE CONTROL

Adaptive cruise control is a driver assistance system that seeks to combine safe following distance with speed regulation. We consider a set-up with two vehicles. Vehicle 2 is following vehicle 1, the relative position of vehicle 2 w.r.t the vehicle is given by $d \in (-\infty, 0]$.

The dynamic of vehicle 2 is controlled while that of vehicle 1 is considered as a disturbance. Consider the following continuous-time model adapted from [34]:

$$\begin{cases} \dot{d} &= v_1 - v_2; & y_d &= d + \delta_1; \\ \dot{v}_2 &= \frac{u - h(v_2)}{M}; & y_{v_2} &= v_2 + \delta_2; \\ \dot{v}_1 &= \Gamma(v_1, w); \end{cases} \quad (19)$$

where $h(v_2) = f_0 + f_1 v_2 + f_2 v_2^2$, and the function Γ as

$$\Gamma(v_1, w) = \begin{cases} w & \text{if } v_1 \in (v_1^{\min}, v_1^{\max}) \\ \max(0, w) & \text{if } v_1 = v_1^{\min} \\ \min(0, w) & \text{if } v_1 = v_1^{\max} \end{cases}$$

which gives $v_1(t) \in [v_1^{\min}, v_1^{\max}]$ for all time. The states d and v_2 are measured through the outputs y_d and y_{v_2} , while v_1 is not measured. The control input $u \in [u^{\min}, u^{\max}]$ represents the contribution of braking and engine torque to the acceleration of vehicle 2. $M > 0$ represents the mass of vehicle 2, 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 1, and δ_1, δ_2 denote bounded disturbances in the measured variables of the system.

The problem of designing an adaptive cruise control system is considered with a time headway defined as $\vartheta(t) = -d(t)/v_2(t)$. The requirements for adaptive cruise control are parameterized by a target velocity v^* and a target time headway ϑ^* . They are formulated as synthesizing a controller enforcing uniform attractivity of

$$X^* = \{(d, v_2) \in \mathbb{R}^2 \mid (-d/v_2, v_2) \in Z_a^* \cup Z_b^*\}, \quad (20)$$

where $Z_a^* = \{(\vartheta, v_2) \in \mathbb{R}^2 \mid \vartheta \geq \vartheta^*, v_2 = v^*\}$, $Z_b^* = \{(\vartheta, v_2) \in \mathbb{R}^2 \mid \vartheta = \vartheta^*, v_2 \leq v^*\}$.

Actually, this specification cannot be enforced so we aim at synthesizing a least-violating controller, according to [35], enforcing the closed-loop behavior whose attractor is the closest to X^* in (20) with respect to the following distance function:

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

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: *i*) keep the distance $d(t) \leq 0$, and *ii*) keep velocity $v_2(t) \in [v_2^{\min}, v_2^{\max}]$.

Values of parameters, compatible with empirical measurements are taken from [34] and given in Table I.

Consider the observer

$$\begin{cases} \dot{\hat{d}} &= \hat{v}_1 - \hat{v}_2 + l_1 (\hat{d} - y_d) + l_2 (\hat{v}_2 - y_{v_2}), \\ \dot{\hat{v}}_2 &= \frac{u - h(y_{v_2})}{M} + l_3 (\hat{d} - y_d) + l_4 (\hat{v}_2 - y_{v_2}) \\ \dot{\hat{v}}_1 &= l_5 (\hat{d} - y_d) + l_6 (\hat{v}_2 - y_{v_2}) \end{cases} \quad (21)$$

TABLE I
PARAMETER VALUES

M	1370	Kg	u^{\max}	0.2	g	m/s^2	w^{\max}	3	m/s^2
f_0	51	N	v_2^{\min}	10	m/s		ϑ^*	1.5	s
f_1	1.2567	Ns/m	v_2^{\max}	30	m/s		v^*	20	m/s
f_2	0.4342	Ns^2/m^2	v_1^{\min}	12	m/s		τ	0.5	s
g	9.82	m/s^2	v_1^{\max}	28	m/s		α	0.5	
u^{\min}	-0.3	g	w^{\min}	-1.7	m/s^2				

which is similar to (19) with linear correction terms; the parameters l_1, \dots, l_6 will be designed to ensure that trajectories $(\hat{d}, \hat{v}_2, \hat{v}_1)$ converge to a neighborhood of (d, v_2, v_1) (related to the considered disturbances).

Defining estimation errors as $e_d = \hat{d} - d$, $e_{v_1} = \hat{v}_1 - v_1$, $e_{v_2} = \hat{v}_2 - v_2$, the estimation error dynamics is defined as:

$$\begin{cases} \dot{e}_d &= e_{v_1} - e_{v_2} + l_1 e_d + l_2 e_{v_2} - l_1 \delta_1 - l_2 \delta_2 \\ \dot{e}_{v_2} &= \frac{h'(v_2^0)}{M} \delta_2 + l_3 e_d + l_4 e_{v_2} - l_3 \delta_1 - l_4 \delta_2 \\ \dot{e}_{v_1} &= l_5 e_d + l_6 e_{v_2} - l_5 \delta_1 - l_6 \delta_2 - \Gamma(v_1, w) \end{cases} \quad (22)$$

where v_2^0 is an unknown value inside $[v_2^{\min}, v_2^{\max}]$ but $|h'(v_2^0)| \leq \bar{h} = f_1 + 2f_2 v_2^{\max}$ holds (locally Lipschitz). Since the disturbances considered in the system (19) are bounded, there are constants $\bar{\delta}_1, \bar{\delta}_2, \bar{\Gamma} \in \mathbb{R}_{>0}$ such that $|\delta_1| \leq \bar{\delta}_1$, $|\delta_2| \leq \bar{\delta}_2$, $|\Gamma(v_1, w)| \leq \bar{\Gamma}$ are satisfied.

In matrix terms, the system (22) can be expressed as

$$\dot{e} = (A + LC)e + (LC + B_1)\Delta\tilde{\delta} + B_2 W \tilde{w}, \quad (23)$$

where $e = [e_d, e_{v_2}, e_{v_1}]^T$, $\Delta = \sqrt{3} \text{diag}(\bar{\delta}_1, \bar{\delta}_2, \frac{\bar{h}}{M} \bar{\delta}_2)$, $W = \bar{\Gamma}$, $A = \begin{bmatrix} 0 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $L = \begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \\ l_5 & l_6 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, $B_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, $B_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, $\tilde{\delta} = \Delta^{-1} [-\delta_1, -\delta_2, \frac{h'(v_2^0)}{M} \delta_2]^T$, $\tilde{w} = -W^{-1} \Gamma(v_1, w)$. The disturbances in terms of $\tilde{\delta}, \tilde{w}$ allows to satisfy $\|\tilde{\delta}\|, \|\tilde{w}\| \leq 1$.

We propose a quadratic Lyapunov function $V(e) = e^T P e$ for the system (22), where $P \in \mathbb{R}^{3 \times 3}$ is a positive definite matrix which will be obtained through the next matrix inequality¹:

$$\begin{bmatrix} A^T P + PA + C^T Z^T + ZC + \lambda P & * & * \\ \Delta^T (C^T Z^T + B_1^T P) & -\rho_1 I_3 & * \\ W^T B_2^T P & 0 & -\rho_2 \end{bmatrix} \leq 0, \quad (24)$$

where $Z = PL$, and $\lambda, \rho_1, \rho_2 \in \mathbb{R}_{>0}$ are design parameters.

The derivative of Lyapunov function along the trajectories of the system (23) is given by

$$\begin{aligned} \dot{V}(e(t)) &= e^T (A^T P + PA + C^T Z^T + ZC) e + \\ &\quad + 2e^T (ZC + PB_1)\Delta\tilde{\delta} + 2e^T PB_2 W \tilde{w} \\ &\leq -\lambda e^T P e + \rho_1 \|\tilde{\delta}\|^2 + \rho_2 \|\tilde{w}\|^2, \end{aligned} \quad \text{from (24).}$$

Thus, all trajectories of (23) converge to the invariant set $V^{-1}(\leq \frac{\rho_1 + \rho_2}{\lambda})$, which is contained in a hyper rectangle $N_\varepsilon(0)$, with $\forall i \in [1; 3]$, $\varepsilon_i = \sqrt{\frac{\rho_1 + \rho_2}{\lambda} (P^{-1})_{i,i}}$, see Proposition 1 in [36].

For the numerical results reported below the following parameters were chosen: $\bar{\delta}_1 = \bar{\delta}_2 = 0.01$ and notice that $\Gamma(v_1, w) \in [w^{\min}, w^{\max}]$, obtaining from (24): $l_1 = -28.51$, $l_2 = 0.96$, $l_3 = -3.01$, $l_4 = -24.91$, $l_5 = -270.11$, $l_6 = 3.08$,

¹The symbol $*$ refers to symmetric terms and I_3 is the identity matrix of dimension 3.

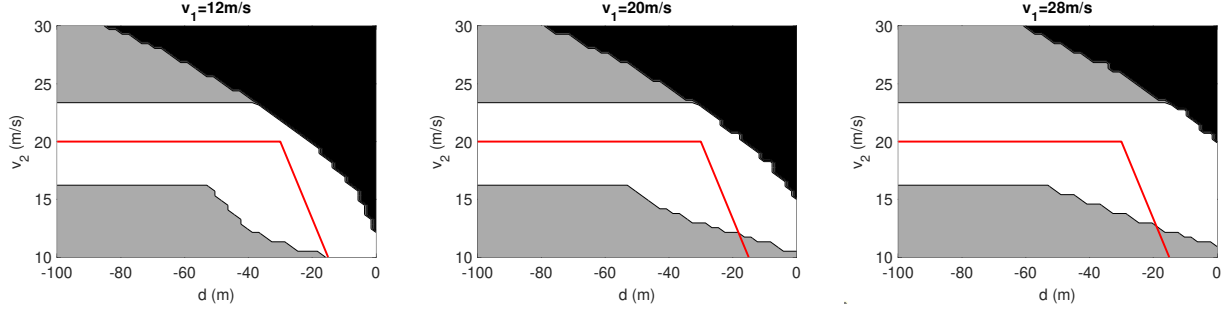


Fig. 2. Set of safety controllable states (white); set of states which will reach the white set (light grey); set of uncontrollable states (black).

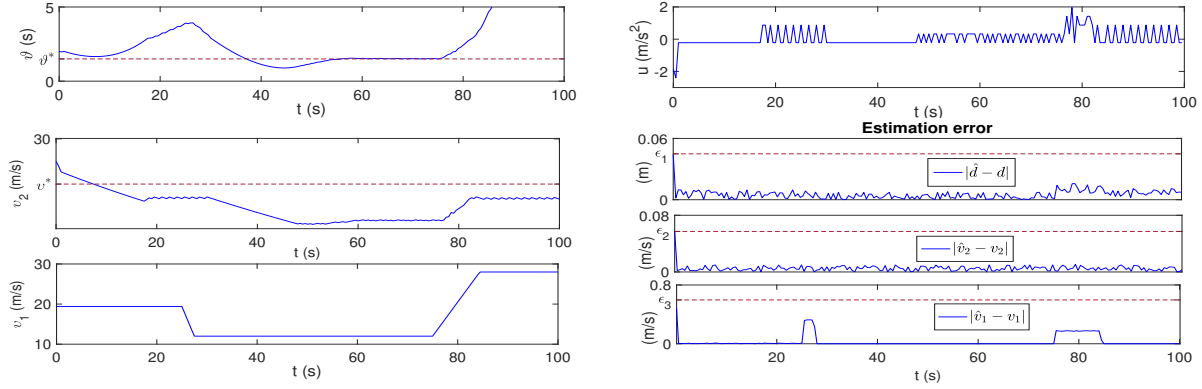


Fig. 3. Simulated trajectories of system (19) using the observer-based controller: (left side) evolution of the time headway, of the velocities of vehicle 2 and vehicle 1 where the target time headway ϑ^* and the values of the target velocity v^* are represented by dashed lines; (right side) the control input of vehicle 2 and estimation errors between real and observer states.

$$\lambda = 10.95, \rho_1 = 1.59, \rho_2 = 2.31, \varepsilon = [0.04 \ 0.06 \ 0.59]^T, P = \begin{bmatrix} 353.23 & * & * \\ -6.34 & 109.09 & * \\ -18.73 & 0.23 & 1.99 \end{bmatrix}.$$

The parameter ε is used to define S_2 in (11) with the abstraction parameters $\eta = (\eta_d, \eta_{v_2}, \eta_{v_1})$ and μ which were chosen as: $d_0 = -100m$, $\eta_d = -d_0/100$, $\eta_{v_2} = (v_2^{\max} - v_2^{\min})/100$, $\eta_{v_1} = (v_1^{\max} - v_1^{\min})/80$, $\mu = (u^{\max} - u^{\min})/10$. Theorem 3, using ε and $V(e) = e^T P e$, guarantees a feedback refinement relation between the τ -sampled system of (19)-(21) and S_2 . We have synthesized a least-violating controller C_2 for S_2 according to [35]. It is shown in Figure 2, where the slices are computed at different values of v_1 :

- The red line represents the target set X^* in (20), and the white set represents the attractor of the closed-loop dynamics that is the closer to the target set as measured by distance H . All trajectories starting in this set stay there forever.
- In the light grey set, all trajectories starting in this set will reach the attractor while still enforcing the strong safety requirements.
- The black set consists of the uncontrollable states from which the strong safety requirements cannot be guaranteed.

The implementation of the least-violating controller for system (19) is done through the controller C_1 defined in Proposition 4 which depends solely on the information of the observer. In Figure 3, we show a simulation of system (19) using the observer-based controller in the following scenario: the initial value of (d, v_2, v_1) and $(\hat{d}, \hat{v}_2, \hat{v}_1)$ are $(-50 + \varepsilon_1, 25 + \varepsilon_2, 20 + \varepsilon_3)$ and $(-50, 25, 20)$, respectively. The leading vehicle

(vehicle 1) drives at constant speed for the first 25s, then applies maximal deceleration until reaching minimal speed for the next 50s, and maximal acceleration until reaching maximal speed for the last 25s. The plots represent the evolution of the time headway, of the velocities of vehicle 2 and vehicle 1, the control input of vehicle 2 and estimation errors. The values of the target velocity v^* and the target time headway ϑ^* are represented by dashed lines in left side. Initially the time headway is greater than ϑ^* so vehicle 2 regulates its speed around v^* . After vehicle 1 decelerates, the time headway reduces and drops below ϑ^* , then vehicle 2 stops regulating its speed to regulate its time headway around ϑ^* . When vehicle 1 accelerates, the time headway increases again and becomes larger than ϑ^* , then vehicle 2 restarts regulating its speed around v^* . The error magnitudes never exceed their bound values $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$, due to stability and reduce to the magnitude of the measurement noises δ_1, δ_2 (white noise of magnitude 0.01) and the disturbance term w during the simulation. Numerically, $|\hat{d}(t) - d(t)| \leq 0.05$, $|\hat{v}_2(t) - v_2(t)| \leq 0.06$, $|\hat{v}_1(t) - v_1(t)| \leq 0.59$ for all time. Note that the estimation error in v_1 is greater than other states, this is due to the effect of the disturbance w for which the observer cannot compensate between a time step and the next. We can see on the simulation that the system behaves as expected. The performance degradation of the observer-based controller compared to a state-based controller can be evaluated through the value $\varsigma = \max_{t \geq t_s} H(d(t), v_2(t), v_1(t))$, which is the maximal

value reached by the distance function H after the trajectory reaches the attractor. In the simulation, $\zeta = 1.8286$ (observer) is reduced to 1.1 (state), which appears acceptable in view of the observer precision given by ε .

V. CONCLUSIONS

In this paper, an abstraction design which is related by a feedback refinement relation of the system formed with the plant and a chosen observer was proposed. This approach allows us to use results in the observer design from classical control theory, which covers a wide class of systems (linear and nonlinear), while being able to deal with complex specifications and disturbances. The controller refinement only requires feeding the obtained symbolic controller with the state estimate of the observer, which provides an output-feedback controller. An application to adaptive cruise control illustrates our results. Further investigations are necessary to cope with the transient behaviour of the observer before reaching the forward invariant set.

REFERENCES

- [1] P. Tabuada. *Verification and Control of Hybrid Systems*. Springer, New York, NY, USA, 2009.
- [2] G. Reissig, A. Weber, and M. Rungger. Feedback refinement relations for the synthesis of symbolic controllers. *IEEE Trans. Autom. Control*, 62(4):1781–1796, Apr. 2017.
- [3] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas. Discrete abstractions of hybrid systems. *Proc. IEEE*, 88(7):971–984, Jul. 2000.
- [4] G. Reissig. Computing abstractions of nonlinear systems. *IEEE Trans. Autom. Control*, 56(11):2583–2598, Nov. 2011.
- [5] C. Belta, B. Yordanov, and E. A. Gol, editors. *Formal Methods for Discrete-Time Dynamical Systems*, volume 89. Springer, Cham, Switzerland, 2018.
- [6] E. A. Lee and S. A. Seshia. *Introduction to embedded systems: A cyber-physical systems approach*. MIT Press, Cambridge, MA, USA, 2016.
- [7] E. A. Gol, M. Lazar, and C. Belta. Language-guided controller synthesis for linear systems. *IEEE Trans. Autom. Control*, 59(5):1163–1176, May. 2014.
- [8] P. Tabuada and G. J. Pappas. Linear time logic control of discrete-time linear systems. *IEEE Trans. Autom. Control*, 51(12):1862–1877, Dec. 2006.
- [9] B. Yordanov, J. Tumova, I. Cerna, J. Barnat, and C. Belta. Temporal logic control of discrete-time piecewise affine systems. *IEEE Trans. Autom. Control*, 57(6):1491–1504, Jun. 2012.
- [10] G. Pola, P. Pepe, and M.D. Di Benedetto. Symbolic models for networks of discrete-time nonlinear control systems. In *American Control Conf.*, pages 1787–1792, 2014.
- [11] G. Pola, A. Borri, and M. D. Di Benedetto. On symbolic control design of discrete-time nonlinear systems with state quantized measurements. In *Proc. 55th IEEE Conf. Decis. Control*, pages 6571–6576, Las Vegas, NV, USA, 2016.
- [12] G. Pola, A. Borri, and M. D. Di Benedetto. Integrated design of symbolic controllers for nonlinear systems. *IEEE Trans. Autom. Control*, 57(2):534–539, Feb. 2012.
- [13] A. Girard. Controller synthesis for safety and reachability via approximate bisimulation. *Automatica*, 48(5):947–953, 2012.
- [14] A. Girard. Low-complexity quantized switching controllers using approximate bisimulation. *Nonlinear Anal. Hybrid Syst.*, 10:34–44, Nov. 2013.
- [15] A. Borri, G. Pola, and M. D. Di Benedetto. Integrated symbolic design of unstable nonlinear networked control systems. In *Proc. 51st IEEE Conf. Decis. Control*, pages 1374–1379, Maui, HI, USA, 2012.
- [16] A. Borri, G. Pola, and M. D. Di Benedetto. Design of symbolic controllers for networked control systems. *IEEE Trans. Autom. Control*, 64(3):1034–1046, 2019.
- [17] P. Meyer, A. Girard, and E. Witrant. Compositional abstraction and safety synthesis using overlapping symbolic models. *IEEE Trans. Autom. Control*, 63(6):1835–1841, Jun. 2018.
- [18] M. Mazo, A. Davitian, and P. Tabuada. Pessoa: A tool for embedded controller synthesis. In T. Touili, B. Cook, and P. Jackson, editors, *Computer Aided Verification*, pages 566–569, Heidelberg, Germany, 2010. Springer.
- [19] S. Mouelhi, A. Girard, and G. Gössler. Cosyma: A tool for controller synthesis using multi-scale abstractions. In *Proc. 16th Int. Conf. Hybrid Syst. Comput. Control*, pages 83–88, 2013.
- [20] T. Wongpiromsarn, U. Topcu, N. Ozay, H. Xu, and R.M. Murray. Tulip: A software toolbox for receding horizon temporal logic planning. In *Proc. 14th Int. Conf. Hybrid Syst. Comput. Control*, pages 313–314, 2011.
- [21] M. Rungger and M. Zamani. Scots: A tool for the synthesis of symbolic controllers. In *Proc. 19th Int. Conf. Hybrid Syst. Comput. Control*, pages 99–104, 2016.
- [22] M. Khaled and M. Zamani. Pfaces: An acceleration ecosystem for symbolic control. In *Proc. 22nd Int. Conf. Hybrid Syst. Comput. Control*, page 252–257, 2019.
- [23] K. Hsu, R. Majumdar, K. Mallik, and A. K. Schmuck. Multi-layered abstraction-based controller synthesis for continuous-time systems. In *Proc. 21st Int. Conf. Hybrid Syst. Comput. Control*, page 120–129, 2018.
- [24] D. Luenberger. An introduction to observers. *IEEE Trans. Autom. Control*, 16(6):596–602, Dec. 1971.
- [25] J.S. Shamma and T. Kuang-Yang. Set-valued observers and optimal disturbance rejection. *IEEE Trans. Autom. Control*, 44(2):253–264, Feb. 1999.
- [26] C. Belta, B. Yordanov, and E. A. Gol. *Formal Methods for Discrete-Time Dynamical Systems*. Springer, Cham, Switzerland, 2017.
- [27] S. Haesaert, A. Abate, and P. M. J. Van den Hof. Correct-by-design output feedback of lti systems. In *Proc. 54th IEEE Conf. Decis. Control*, pages 6159–6164, Osaka, Japan, 2015.
- [28] O. Mickelin, N. Ozay, and R. M. Murray. Synthesis of correct-by-construction control protocols for hybrid systems using partial state information. In *Proc. Amer. Control Conf.*, pages 2305–2311, Portland, OR, USA, 2014.
- [29] M. Mizoguchi and T. Ushio. Deadlock-free output feedback controller design based on approximately abstracted observers. *Nonlinear Anal. Hybrid Syst.*, 30:58–71, Nov. 2018.
- [30] G. Pola, M. D. Di Benedetto, and A. Borri. Symbolic control design of nonlinear systems with outputs. *Automatica*, 109:108511, Nov. 2019.
- [31] R. Majumdar, N. Ozay, and A.-K. Schmuck. On abstraction-based controller design with output feedback. In *Proc. 23rd Int. Conf. Hybrid Syst. Comput. Control*, pages 1–11, 2020.
- [32] A. Martinelli. Nonlinear unknown input observability: Extension of the observability rank condition. *IEEE Trans. Autom. Control*, 64(1):222–237, Jan. 2019.
- [33] E. Rocha-Cózatl and J.A. Moreno. Dissipative design of unknown input observers for systems with sector nonlinearities. *Int. J. Robust Nonlinear Control*, 21(14):1623–1644, 2011.
- [34] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A.D. Ames, J.W. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Correct-by-construction adaptive cruise control: Two approaches. *IEEE Trans. Control Syst. Technol.*, 24(4):1294–1307, Jul. 2016.
- [35] A. Girard and A. Eqtami. Least-violating symbolic controller synthesis for safety, reachability and attractivity specifications. [Online]. Available: <https://hal.archives-ouvertes.fr/hal-02533407>, Apr 2020.
- [36] C. Le Guernic and A. Girard. Reachability analysis of linear systems using support functions. *Nonlinear Anal. Hybrid Syst.*, 4(2):250–262, 2010.