INTERNATIONAL JOURNAL OF ROBUST AND NONLINEAR CONTROL
Int. J. Robust. Nonlinear Control (2013)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/rnc.3033

Model falsification using set-valued observers for a class of discrete-time dynamic systems: a coprime factorization approach

Paulo Rosa[1,*,†], Carlos Silvestre[2,3] and Michael Athans[4]

[1]*Deimos Engenharia, Av. D. João II, Lt 1.17.01, Andar 10, 1998-023 Lisboa, Portugal*
[2]*Institute for Systems and Robotics, Instituto Superior Tecnico, Lisboa, Portugal*
[3]*Department of Electrical and Computer Engineering, Faculty of Science and Technology, University of Macau, Taipa, Macau*
[4]*Professor of EECS (emeritus), M.I.T., USA*

SUMMARY

This article introduces a new method for model falsification using set-valued observers, which can be applied to a class of discrete linear time-invariant dynamic systems with time-varying model uncertainties. In comparison with previous results, the main advantages of this approach are as follows: The computation of the convex hull of the set-valued estimates of the state can be avoided under certain circumstances; to guarantee convergence of the set-valued estimates of the state, the required number of previous steps is at most as large as the number of states of the nominal plant; and it provides a straightforward *nonconservative* method to falsify uncertain models of dynamic systems, including open-loop unstable plants. The results obtained are illustrated in simulation, emphasizing the advantages and shortcomings of the suggested method. Copyright © 2013 John Wiley & Sons, Ltd.

Received 2 January 2012; Revised 12 April 2013; Accepted 10 May 2013

KEY WORDS: system model validation; uncertain linear systems; coprime factorization; fault detection; identification methods

1. INTRODUCTION

The problem of *model falsification* or *model invalidation* is relevant in a wide range of applications, such as fault detection and isolation, multiple-model adaptive control and model identification methodologies. In any of these situations, as stressed in [1], the key aspect to take into account is the fact that a model can never be *validated* in practice. Indeed, a given dynamic model being compatible with the input/output data sequence up to time t does not imply that it is compatible with the measurements at time $t + \delta$, where $\delta > 0$. Therefore, one can only say that a given model is not falsified (or invalidated) by the current input/output data sequence. On the other hand, a model is obviously invalidated or falsified once it is not compatible with the observations.

As a typical framework, one considers the problem of selecting an appropriate model for a given dynamic system, among a set of predefined *eligible models*. However, unmodeled and/or unknown dynamics (present in virtually every physical system) and adverse exogenous disturbances can result in the invalidation of models that would be valid if such perturbations were taken into account. Hence, it is imperative that the formulation of the problem takes into account these uncertainty terms, to avoid undue invalidation of models. As an example, the solution proposed in [1] for uncertain linear time-invariant (LTI) systems, and later on extended to linear parameter-varying (LPV) systems [2], assumes that the system is described by an LTI nominal model interconnected with an LTI or linear time-varying unknown system, which can be used, for instance, to describe

*Correspondence to: Paulo Rosa, Deimos Engenharia, Av. D. João II, Lt 1.17.01, Andar 10, 1998-023 Lisboa, Portugal.
†E-mail: paulo.rosa@deimos.com.pt

unmodeled dynamics and parametric uncertainty. However, the methods provided in [1, 2] are not recursive, which means that, after a given amount of input/output data is obtained, we verify whether or not the data sequence is compatible with the model of the system. Hence, the complexity of the algorithms grows with the number of measurements.

A different approach to model falsification can be found in the fault detection and isolation literature – see, for instance, [3]. The main idea in such architectures stems from the designing of filters that are more reactive to faults than to disturbances and model uncertainty. This can be achieved, for instance, by using geometric considerations regarding the plant ([4–7]), or by optimizing a particular norm minimization objective, such as the $\mathcal{H}_\infty$-norm or ℓ_1-norm ([8–12]). The latter approach provides, in general, important robustness properties, as stressed in [8, 13–15], by explicitly accounting for model uncertainty. After synthesizing the filters, a set of residuals is then generated by comparing the actual output of the plant with the ones estimated by each filter. A model is thereafter invalidated if the corresponding residual is greater than a given threshold, which may be time-varying and that, in general, depends on the model uncertainty and on the amplitude of the disturbances. As a caveat, these methodologies are typically conservative or can only be applied to a particular class of systems.

A novel model falsification strategy was proposed in [16–19], which relies on set-valued observers (SVOs) – see [20–22] and references therein – to invalidate discrete-time LPV models of dynamic systems. The reasoning behind this approach is similar to that of [1, 2], but a recursive algorithm is proposed instead, allowing it to run in real time. Because of the properties inherited from the SVOs, this model falsification method guarantees that valid models of the plant are never invalidated. Moreover, under certain distinguishability conditions briefly discussed in the sequel, it can also be shown that the *correct* model of the plant is selected. Other set-membership approaches to model falsification in the literature include [23] and [24], where set-valued estimates of unknown parameters of the plant are computed.

In [16, 17, 19], an extension of the SVOs introduced in [25] to LPV uncertain systems is presented. The proposed solution is able to cope with descriptions of the plant that can be time-varying and partially unknown. To constrain the number of faces of the set-valued estimate of the state of the system, an overbound was proposed, which is guaranteed not to grow unbounded, under certain assumptions on the plant. Nevertheless, a few questions regarding the implementation of these SVOs were left unresolved. In particular, to guarantee a bounded set-valued estimate of the state, an arbitrarily large number of previous state estimates was required, possibly leading to excessive computational requirements. Furthermore, it was assumed that the plant (at least in closed-loop) was asymptotically stable.

This paper proposes a new SVO-based strategy to invalidate a class of discrete-time dynamic systems, guaranteeing that the set-valued estimates of the state remain bounded under mild assumptions, and requiring at most the n previous state estimates, where n is the number of states of the model of the system. We stress that this is the main contribution of this work because it shows that the conservatism added by the suggested SVO-based approach does not lead to the unbounded growth of the set-valued state estimates of the system. Moreover, the proposed solution can be applied to a class of dynamic systems described by (possibly unstable) LTI models with time-varying input and output uncertainties.

The remainder of this paper is organized as follows. We start by introducing the notation used in this work and describing some of the techniques available in the literature for the design of SVOs in Section 2. In Section 3, the main results of this article regarding the convergence of the SVOs and its applicability to a class of dynamic systems are presented. The theory is illustrated by means of a simulation example in Section 4. Finally, some conclusions regarding this work are discussed in Section 5.

2. PRELIMINARIES AND NOTATION

2.1. Notation

The set of all integers and the set of all strictly positive integers are denoted by $\mathbb{Z}$ and $\mathbb{Z}^+$, respectively. The subspace of all proper and real rational stable transfer matrices is denoted by

DOI: 10.1002/rnc

$\mathcal{RH}_\infty$. We represent the elements of $v(k) \in \mathbb{R}^m$, for some $m, k \in \mathbb{Z}$, $m > 0$, as $v_i(k)$, so that $v(k) = [v_1(k),\ v_2(k),\ \cdots,\ v_m(k)]^{\mathrm{T}}$. The concatenation of vectors $v(k), v(k-1), \cdots, v(k-N+1)$, for $N \in \mathbb{Z}^+$ is denoted as

$$v_N = \begin{bmatrix} v(k) \\ \vdots \\ v(k-N+1) \end{bmatrix}.$$

For the sake of simplicity, v is used instead of v_N whenever N can be inferred from the context. For $a, b \in \mathbb{R}^n$, we say that $a \leqslant b$ if $a_i \leqslant b_i$ for all $i \in \{1, \cdots, n\}$. For a discrete-time signal, $r(\cdot)$, we define $|r(\cdot)| := \max_{i,k} |r_i(k)|$. The $\mathcal{L}_2$-induced norm of a system $G \in \mathcal{RH}_\infty$ is denoted by $\|G\|$. For a matrix A, the largest singular value is denoted by $|A| := \sigma_{\max}(A)$.

2.2. *Set-valued observers for linear time-invariant systems*

Consider an LTI system described by

$$\begin{cases} \tilde{x}(k+1) = \tilde{A}\tilde{x}(k) + \tilde{B}\tilde{u}(k) + \tilde{L}\tilde{d}(k), \\ \quad\ \tilde{x}(k) \in \tilde{Y}(k), \end{cases} \tag{1}$$

with bounded exogenous disturbances, $\tilde{d}(\cdot)$, uncertain initial state, $\tilde{x}(0) \in X(0)$, and control input, $\tilde{u}(\cdot)$. It is also assumed that, without loss of generality, $\left|\tilde{d}(\cdot)\right| \leqslant 1$. At each time, k, the vector of states is denoted by $\tilde{x}(k)$, and we define

$$X(0) := \mathrm{Set}(M_0, m_0),$$

where

$$\mathrm{Set}(M, m) := \{q : Mq \leqslant m\} \tag{2}$$

represents a convex polytope. Moreover, $\tilde{Y}(k)$, for each time k, is a measured uncertainty set where the state, $\tilde{x}(k)$, is contained – see Remark 1. In particular, $\tilde{Y}(k)$ is assumed to be described as

$$\tilde{Y}(k) = \mathrm{Set}\left(\tilde{M}(k-1), \tilde{m}(k-1)\right),$$

for a matrix $\tilde{M}(k-1)$ and a vector $\tilde{m}(k-1)$ with appropriate dimensions. Furthermore, let $\tilde{x}(k) \in \mathbb{R}^{n_x}$, $\tilde{d}(k) \in \mathbb{R}^{n_d}$, and $\tilde{u}(k) \in \mathbb{R}^{n_u}$.

Remark 1
In case the following vector measurements are available

$$\tilde{y}(k) = \tilde{C}\tilde{x}(k) + \tilde{n}(k),$$

with bounded measurement noise $\tilde{n}(k)$, $|\tilde{n}(\cdot)| \leqslant \bar{n}$, and $\tilde{y}(k) \in \mathbb{R}^{n_y}$, then one can write

$$\tilde{x}(k) \in \tilde{Y}(k) = \mathrm{Set}\left(\tilde{M}(k-1), \tilde{m}(k-1)\right),$$

with

$$\tilde{M}(k-1) = \tilde{M} = \begin{bmatrix} \tilde{C} \\ -\tilde{C} \end{bmatrix}, \quad \tilde{m}(k-1) = \begin{bmatrix} \bar{n} + \tilde{y}(k) \\ \bar{n} - \tilde{y}(k) \end{bmatrix}.$$

Let $X(k+1)$ represent the set of possible states at time $k+1$, that is, the state $\tilde{x}(k+1)$ satisfies (1) with $\tilde{x}(k) \in X(k)$ if and only if $\tilde{x}(k+1) \in X(k+1)$. An SVO aims to find $X(k+1)$, based upon (1) and with the additional knowledge that $\tilde{x}(k) \in X(k)$, $\tilde{x}(k-1) \in X(k-1), \cdots, \tilde{x}(k-n_o) \in X(k-n_o)$ for some finite n_o. Furthermore, we want $X(k+1)$ to be the smallest set containing all the solutions to (1). A procedure for time-varying discrete-time linear systems was introduced in [25], and a preliminary extension to uncertain plants is presented in [16, 17, 19].

DOI: 10.1002/rnc

The computation of $X(k+1)$ based upon $X(k)$ for systems with no model uncertainty can be performed by using the technique described in [25]. Indeed, let the system be described by (1). Then, as shown in [25], $\tilde{x}(k+1) \in X(k+1)$ if and only if there exist $\tilde{x}(k)$, and $\tilde{d}(k)$, such that

$$P(k)\begin{bmatrix}\tilde{x}(k+1)\\ \tilde{x}(k)\\ \tilde{d}(k)\end{bmatrix} \leqslant \begin{bmatrix}\tilde{B}\tilde{u}(k)\\ -\tilde{B}\tilde{u}(k)\\ \mathbf{1}\\ \mathbf{1}\\ \tilde{m}(k)\\ m(k-1)\end{bmatrix} =: p(k) \tag{3}$$

where the inequality is taken element-wise,

$$P(k) := \begin{bmatrix} I & -\tilde{A} & -\tilde{L}\\ -I & \tilde{A} & \tilde{L}\\ 0 & 0 & I\\ 0 & 0 & -I\\ \tilde{M}(k) & 0 & 0\\ 0 & M(k\text{-}1) & 0\end{bmatrix},$$

with $M(k-1)$ and $m(k-1)$ defined such that

$$X(k) = \mathrm{Set}(M(k-1), m(k-1)).$$

The inequality in (3) provides a description of a set in $\mathbb{R}^{2n_x+n_d}$, denoted by

$$\Gamma(k+1) = \mathrm{Set}(P(k), p(k)).$$

Therefore, it is straightforward to conclude that

$$\hat{x} \in X(k+1) \Leftrightarrow \underset{\tilde{x}\in\mathbb{R}^{n_x}, \tilde{d}\in\mathbb{R}^{n_d}}{\exists} : \begin{bmatrix}\hat{x}\\ \tilde{x}\\ \tilde{d}\end{bmatrix} \in \Gamma(k+1)$$

Hence, the set $X(k+1)$ can be obtained by projecting $\Gamma(k+1)$ onto the subspace of the first n_x coordinates, as illustrated in Figure 1.

The projection of $\Gamma(k+1)$ onto $\mathbb{R}^{n_x}$ can be performed resorting to the *Fourier–Motzkin elimination method* ([25, 26]). Therefore, we obtain a description of all the admissible $\tilde{x}(k+1)$ that does not depend upon specific $\tilde{x}(k)$ nor $\tilde{d}(k)$.

The formulation in (3) can be easily extended, in case it is convenient to compute $X(k+1)$ not only based upon $X(k)$ but also upon $X(k-1), \cdots, X(k-n_o)$. Indeed, $\tilde{x}(k+1) \in X(k+1)$ if and only if there exist $\tilde{x}(k+1), \cdots, \tilde{x}(k-n_o+1)$, $\tilde{y}(k)$, and $\tilde{d}(k), \cdots, \tilde{d}(k-n_o+1)$, such that,

$$P_{n_o}(k)\left[\tilde{x}(k+1)^{\mathrm{T}} \quad \tilde{x}_{n_o}^{\mathrm{T}} \quad \tilde{d}_{n_o}^{\mathrm{T}}\right]^{\mathrm{T}} \leqslant p_{n_o}(k) \tag{4}$$

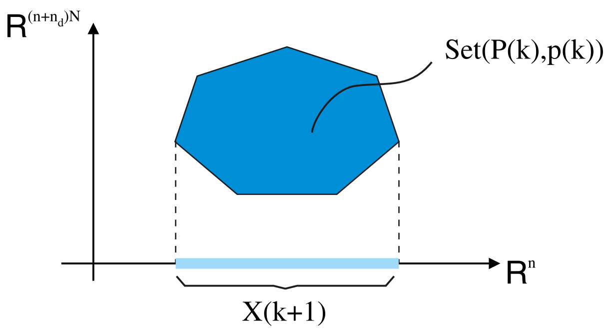


Figure 1. Projection of the set $\Gamma(k+1)$ onto $\mathbb{R}^{n_x}$.

DOI: 10.1002/rnc

where

$$P_{n_o}(k) := \begin{bmatrix} I & -\tilde{A} & \cdots & 0 & -\tilde{L} & 0 & \cdots & 0 \\ -I & \tilde{A} & \cdots & 0 & \tilde{L} & 0 & \cdots & 0 \\ I & 0 & \cdots & 0 & -\tilde{L} & -\tilde{A}\tilde{L} & \cdots & 0 \\ -I & 0 & \cdots & 0 & \tilde{L} & \tilde{A}\tilde{L} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ I & 0 & \cdots & -\tilde{A}^{n_o} & -\tilde{L}^k & \cdots & \cdots & -\tilde{A}^{n_o\text{-}1}\tilde{L} \\ -I & 0 & \cdots & \tilde{A}^{n_o} & \tilde{L}^k & \cdots & \cdots & \tilde{A}^{n_o\text{-}1}\tilde{L} \\ 0 & \cdots & \cdots & 0 & I & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & -I & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & I \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & -I \\ \tilde{M}(k) & 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 \\ 0 & M(k\text{-}1) & \cdots & 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & M(k\text{-}n_o) & 0 & \cdots & \cdots & 0 \end{bmatrix}$$

and $p_{n_o}(k)$ can be inferred from (1).

For plants with uncertainties, the set $X(k+1)$ is, in general, nonconvex, even if $X(k)$ is convex. Thus, it cannot be represented by a linear inequality as in (2). The approach suggested in [16] is to overbound this set by a convex polytope, therefore adding some conservatism to the solution. A generalization of this result is presented in [18, 19]. An alternative in the literature to the design of SVOs uses Luenberger observers to provide bounded errors for the estimates of the states – see [27] and references therein.

2.3. *Coprime factorization of linear time-invariant systems*

The so-called *left-coprime factorization of discrete-time LTI systems* will be used in the following section and is introduced next.

Definition 1
Let $M, N \in \mathcal{RH}_\infty$. Then, M and N are *left-coprime over* $\mathcal{RH}_\infty$ if there exist $X, Y \in \mathcal{RH}_\infty$ such that

$$\begin{bmatrix} M & N \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = MX + NY = I.$$

Moreover, if P is a proper real-rational matrix, then a *left-coprime factorization* of P is a factorization

$$P = N^{-1}M,$$

where N and M are left-coprime over $\mathcal{RH}_\infty$.

The conditions for the existence of a left-coprime factorization are mild, and only the observability of the pair (A, C) is required. Indeed, we recover the following result (see, for instance, [28, p. 554]).

Proposition 1
Let

$$P(z) := D + C(zI - A)^{-1}B := \left[\begin{array}{c|c} zI - A & B \\ \hline C & D \end{array}\right]$$

DOI: 10.1002/rnc

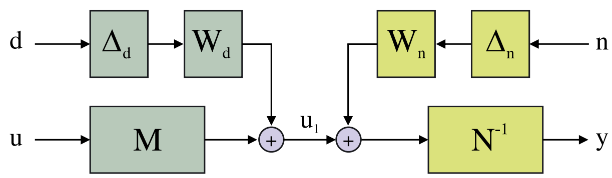


Figure 2. Block diagram of a class of discrete-time LTI dynamic systems with time-varying uncertainties and unknown disturbances.

be observable and define

$$\begin{bmatrix} N & M \end{bmatrix} = \left[\begin{array}{c|cc} zI - A + KC & -K & B - KD \\ \hline RC & R & RD \end{array}\right],$$

where R is any nonsingular matrix and K is such that $A - KC$ is stable. Then,

$$P = N^{-1} M.$$

3. MAIN RESULTS

We are now in conditions of stating the main results in this paper. We will start by addressing the use of the SVOs in the context of model falsification. Thereafter, guarantees of convergence of the SVOs are provided, and finally, we illustrate how to use these methods to falsify a class of models with uncertain dynamics.

3.1. Model falsification using set-valued observers

In [16, 18], the main idea was to invalidate dynamic models associated with SVOs whose state estimate, at a given time, is the empty set. Thus, as long as a given SVO provides nonempty set-valued estimates for the state of the plant, the corresponding dynamic model cannot be discarded. However, several assumptions – including open-loop stability – are posed regarding the structure of the dynamic models in [16, 18]. Hence, the first part of this subsection is devoted to the development of a method to invalidate dynamic models with a more general structure, whereas in the second part, we show how to use this method on a model selection architecture.

The class of discrete-time dynamic systems considered is described by LTI models driven by unknown but bounded disturbances, connected to time-varying uncertainties, as in [1], and as depicted in Figure 2.

We assume that M, N, W_d and W_n are LTI dynamic systems and that Δ_d, Δ_n are uncertain (possibly) time-varying matrices, with the appropriate dimensions and with $|\Delta_d| \leqslant 1$, $|\Delta_n| \leqslant 1$. Moreover, the control input, $u(\cdot)$, and noisy measurements, $y(\cdot)$, are assumed known, and $|d| \leqslant 1$, $|n| \leqslant 1$.

Notice that

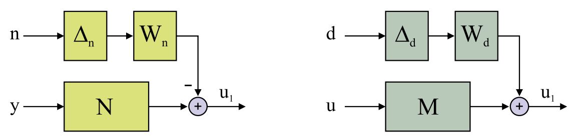
$$\begin{aligned} y &= N^{-1}(u_1 + W_n \Delta_n n) \\ \Leftrightarrow u_1 &= Ny - W_n \Delta_n n, \end{aligned} \tag{5}$$

and

$$u_1 = Mu + W_d \Delta_d d. \tag{6}$$

Therefore, u_1 can be estimated by using (5) or (6). Because of the uncertainties and to the exogenous disturbances, the value of $u_1(k)$ for each k is also, in general, uncertain. Thus, an SVO as in [16, 25] and as described in Section 2, referred to as SVO_A and depicted in Figure 3(a), can be designed to generate the set-valued estimates of u_1 based upon (5), whereas an SVO, designated by SVO_B and illustrated in Figure 3(b), can be synthesized to obtain the set-valued estimates of u_1 based upon (6).

DOI: 10.1002/rnc



(a) Block-diagram used by SVO$_A$ to obtain u_1 based on u and on the bounds on m.

(b) Block-diagram used by SVO$_B$ to obtain u_1 based on y and on the bounds on n.

Figure 3. Block diagrams used to compute the set-valued estimates of u_1. (a) Block diagram used by SVO$_A$ to obtain u_1 based on u and on the bounds on m. (b) Block diagram used by SVO$_B$ to obtain u_1 based on y and on the bounds on n.

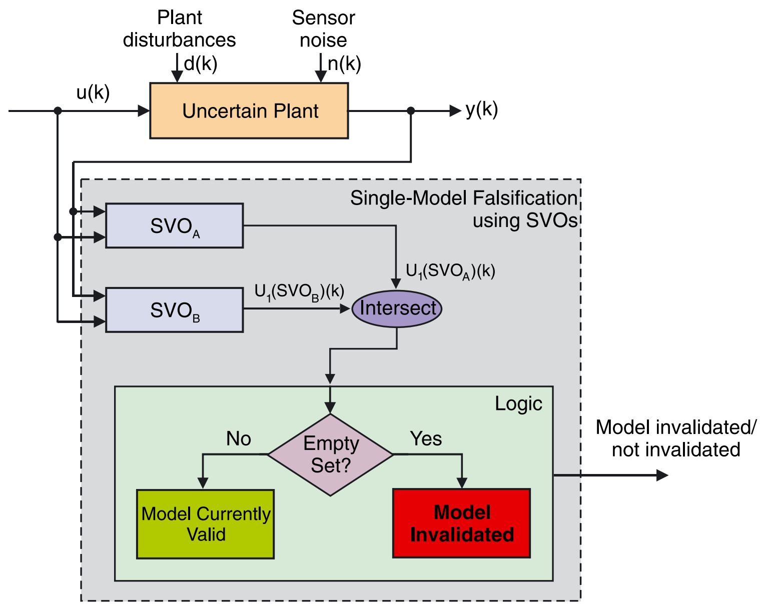


Figure 4. Architecture for single-model falsification using SVOs, including the interconnection between the *true* plant, SVO$_A$ and SVO$_B$.

Remark 2

It is straightforward to conclude that system S_A (Figure 3(a)) can be described by (1) with the change of variables

$$\tilde{u} = y, \tilde{d} = \Delta_n n,$$

and with the appropriate definition of the matrices of the dynamics. Similarly, system S_B (Figure 3(b)) can be described by (1) with the change of variables

$$\tilde{u} = u, \tilde{d} = \Delta_d d.$$

Therefore, in both cases, the measured variable is the set-valued estimate of u_1, provided by the other SVO.

Using this line of thought, the architecture depicted in Figure 4 is proposed for single-model falsification using SVOs, as described in the sequel.

The set-valued estimates of $u_1(k)$, generated by SVO$_A$ and SVO$_B$, denoted by $U_1(\text{SVO}_A)(k)$ and $U_1(\text{SVO}_B)(k)$, respectively, are obtained by driving the SVOs with the (noisy) measurements output, $y(\cdot)$, and with the control inputs, $u(\cdot)$, respectively. If, at a given time k, the set-valued estimate of $u_1(k)$, obtained with SVO$_A$, that is, $U_1(\text{SVO}_A)(k)$, does not intersect with the set-valued estimate of $u_1(k)$, obtained with SVO$_B$, that is, $U_1(\text{SVO}_B)(k)$, the model of the system is not compatible with the true dynamics. Hence, such a model is falsified (i.e., invalidated).

DOI: 10.1002/rnc

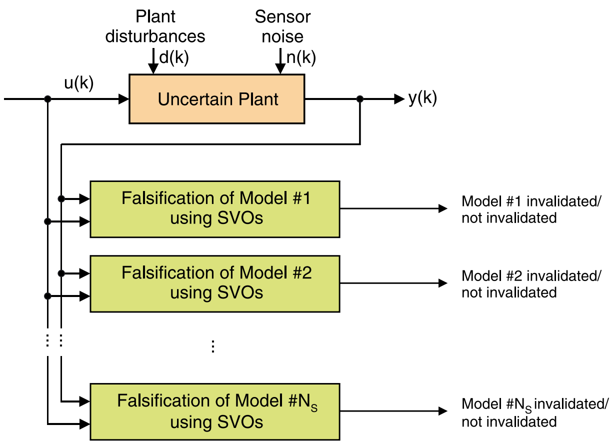


Figure 5. Multiple-model falsification architecture using SVOs.

Remark 3
The initial set-valued state estimates, as well as the set-valued estimates of $U_1(\mathrm{SVO}_A)(0)$ and $U_1(\mathrm{SVO}_B)(0)$, may, in general, be very conservative, if no information is available *a priori* regarding these variables. Nevertheless, as illustrated in the example of Section 4, this issue does not degrade the performance of the algorithm, as the impact of the knowledge regarding those initial values tends to decrease as time goes on.

In summary, one concludes that

- If $\underset{k_o \geqslant 0}{\exists} : U_1(\mathrm{SVO}_A)(k_o) \bigcap U_1(\mathrm{SVO}_B)(k_o) = \emptyset$, then the model of the plant is *not* compatible with the observations and input commands, for $k \geqslant k_o$;
- If $\underset{k \leqslant k_o}{\forall} : U_1(\mathrm{SVO}_A)(k) \bigcap U_1(\mathrm{SVO}_B)(k) \neq \emptyset$, then the model of the plant *is* compatible with the observations and input commands, at least up to $k \leqslant k_o$.

Therefore, if a set of *plausible* dynamic models of a given plant is available, then a couple of SVOs can be designed for each of these models, to invalidate them or not. Thus, the architecture in Figure 5 is proposed as a model selection approach, where N_S denotes the number of considered dynamic models.

In Figure 5, each *model falsification block* is composed of the architecture in Figure 4. Once $N_S - 1$ dynamic models have been invalidated, one concludes that models remaining valid (if any) are the only ones that are able to describe the observed behavior of the plant.

Remark 4
The architecture in Figure 5 does not guarantee that only a single model is not going to be invalidated. Indeed, as shown in [17], this approach only guarantees that the "correct" model of the plant is not falsified. It does not, however, provide any guarantees in terms of invalidating all the other *plausible* models of the plant. These topics are still under research, and some preliminary results are presented in [29]. The interested reader is further referred to [30–34].

3.2. *Guarantees of convergence*

As stated in [16], one possible shortcoming of the SVOs is related to the numerical approximations used during the computation of the set-valued estimates. In other words, because we do not have infinite precision in the computations that have to be carried out at every sampling time to obtain the set-valued estimate $\hat{X}(k)$, the actual set where the state can take value, $X(k)$, need not be entirely contained inside $\hat{X}(k)$ – see Figure 6. Therefore, it may happen that the true state does not belong to $\hat{X}(k)$, and hence, we may end up by discarding the 'correct' model of the plant.

DOI: 10.1002/rnc

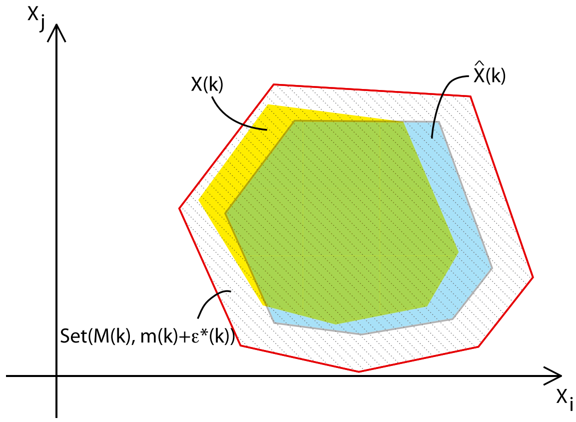


Figure 6. Overbound of set $\hat{X}(k)$ to include $X(k)$.

The solution proposed in [16] is to 'robustify' the algorithm by slightly enlarging the set $\hat{X}(k)$, as illustrated in Figure 6. As long as the maximum error in the computation of the set $X(k)$ is known, we have, for every time k, a vector $\epsilon^\star(k)$ such that $X(k) \subseteq \text{Set}(M(k), m(k) + \epsilon^\star(k))$.

Moreover, it may happen that, from time-step to time-step, the number of faces of the polytope containing the set-valued estimate of the state of the system increases exponentially. Hence, it is useful to overbound, in such circumstances, that polytope by another one, with a constrained number of faces.

Nonetheless, using an overbound to guarantee that we do not discard valid states of the plant also has its shortcomings. Besides adding conservatism to the solution, it may be responsible for the unbounded increase with time of the area of the polytope of the set-valued estimate.

Remark 5

One of the first algorithms developed to compute (ellipsoidal) set-valued estimates of the state of a system was presented in [20] and [35]. Using ellipsoids to describe the set-valued estimates of the state is an alternative method to the one discussed in this article, with the advantage of having less computationally demanding calculations. However, unlike the convex polytope-based approach presented herein, the ellipsoid-based approach does not guarantee convergence of the set of state estimates, even if the system at hand is stable.

The solution proposed in this paper to both problems is to use the left-coprime factorization (Definition 1) of the dynamic model of the system, together with the model falsification architecture depicted in Figure 4.

Theorem 1

Consider a system described by the observable realization

$$P(z) := D + C(zI - A)^{-1}B := \left[\begin{array}{c|c} zI - A & B \\ \hline C & D \end{array}\right],$$

with state $x(k) \in \mathbb{R}^{n_x}$, actuated by control input $u(k)$, $|u(k)| \leqslant \bar{u} < \infty$, with exogenous disturbances $d(k)$, and with measurements $y(k)$, $|y(k)| \leqslant \bar{y} < \infty$, corrupted by additive noise $n(k)$, such that $|d(\cdot)| \leqslant 1$ and $|n(\cdot)| \leqslant 1$. Then, there exist $M(z)$ and $N(z)$ such that

(i) $P(z) = N(z)^{-1}M(z)$;

ii) The set-valued estimates of the states of N and M, respectively, $\hat{\Psi}(\text{SVO}_A)(k)$ and $\hat{\Psi}(\text{SVO}_B)(k)$, obtained from the overbounding of (4), are bounded, for $n_o \geqslant n_x$, provided that the maximal numeric error $\epsilon_j(k)$ of SVO_j, with $j \in \{A, B\}$, satisfies $\epsilon_j(k) \leqslant \epsilon_j^\star \left| x_i^j(k) \right|$,

DOI: 10.1002/rnc

for some $0 \leqslant \epsilon_j^\star < 1$ and for every $x^j(k) \in X^j(k)$, and where $X^j(k)$ denotes the set-valued state estimate of SVO_j.

Proof
The first part of the proof comes directly from Proposition 1. In particular, let K in Proposition 1 satisfy

$$(A - KC)^{n_x} = 0.$$

It should be noticed that the existence of such K is guaranteed, from the existence of a *deadbeat* observer for any observable LTI system – see, for instance, Theorem 5.3 in [36]. We now show that the set-valued estimates of the state of system $N(z)$ are bounded. For the sake of simplicity, the index A is omitted in the proof because all the quantities are related to SVO_A.

Consider the smallest hypercubes, denoted by $\hat{\Psi}(k)$, $\hat{\Psi}(k+1)$, $\cdots$, $\hat{\Psi}(k+n_o)$, that contain the sets $\hat{X}(k)$, $\hat{X}(k+1)$, $\cdots$, $\hat{X}(k+n_o)$, respectively, plus the maximal numeric error at each sampling time, $\epsilon(k)$, with $\epsilon(k) \leqslant \epsilon^\star |x_i(k)|$, for some $0 \leqslant \epsilon^\star < 1$ and for every $x(k) \in X(k)$. Then, for $n_o \geqslant n_x$, an overly conservative SVO can be synthesized to generate the sets $\hat{\Psi}(k)$, $\hat{\Psi}(k+1)$, $\cdots$, $\hat{\Psi}(k+n_o)$, using the following inequality:

$$|x(k+n_o)| \leqslant |(A-KC)^{n_o} x(k)| + \epsilon^\star |x(k)| + \delta_{n_o} = \epsilon^\star |x(k)| + \delta_{n_o},$$

because $(A - KC)^{n_o} = 0$, for $n_o \geqslant n_x$, and where

$$\delta_{n_o} = \max_{y(k),\cdots,y(k+n_o-1)} \left| (A-KC)^{n_o-1} K y(k) + \cdots + K y(k+n_o-1) \right|.$$

Notice that, because the sequence $\hat{\Psi}(k)$, $\hat{\Psi}(k+1)$, $\cdots$, $\hat{\Psi}(k+n_o)$ contains the sequence of set-valued estimates provided by an SVO as described in Section 2, it now suffices to show that the former does not grow without bound. However, given that

- $\epsilon^\star < 1$, by assumption,
- and, because $|y| \leqslant \bar{y} < \infty$, there exists $\bar{\delta}$ such that $|\delta_{n_o}| \leqslant \bar{\delta} < \infty$,

we conclude that the sets defined by (4) for system $N(z)$, with maximal numeric error at each sampling time, $\epsilon(k)$, are bounded.

A similar result can be obtained for the set-valued estimates of the state of $M(z)$ (provided by SVO_B), thus concluding the proof. □

Remark 6
The deadbeat observer was selected to compute the value of K, as it takes the size of the initial set-valued estimate of the state to zero in n_x steps. However, for sufficiently small $\epsilon^\star$, any other value of K can be used, as long as $|(A - KC)^{n_x}| < 1$. Indeed, let K be selected such that

$$|A - KC| = \delta,$$

with $\delta < 1$. By using the approach in the proof of Theorem 1, an SVO with these dynamics is guaranteed to be stable if

$$\delta + \epsilon^\star < 1.$$

Therefore, there is no particular *optimal* value for $\epsilon^\star$, as long as the aforementioned constraint is satisfied. However, for systems with higher complexity, that is, a larger number of states, the set-valued estimates are also of higher dimension. Therefore, it is more likely to run into numerical errors in these situations, which suggests the use of larger values for $\epsilon^\star$, to avoid erroneous invalidation of models.

Remark 7
The choice of K does not impact on the invalidation of the dynamic model. Indeed, we have

$$P(z) = N(z)^{-1} M(z),$$

which means that, for each K, we have a different representation of the same input/output behavior.

DOI: 10.1002/rnc

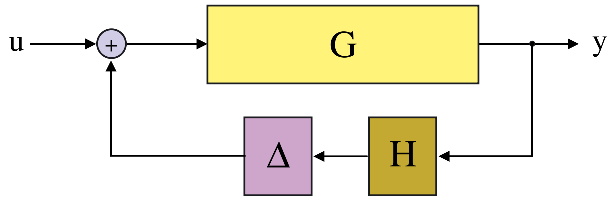


Figure 7. Feedback interconnection between the nominal plant and the uncertainty in A.

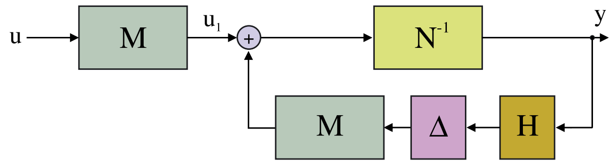


Figure 8. Feedback interconnection between the nominal plant and the uncertainty in A, using the left-coprime decomposition.

3.3. *Model uncertainty in the dynamics*

Notice that the model in Figure 2 can be used to represent not only dynamic systems with exogenous disturbances and measurement noise but also models with uncertainty in the input and in the outputs. Moreover, this technique can also be used to model uncertainty in matrix A, if the linear combination of states multiplying this uncertainty can be obtained by the measured outputs.

To see this, assume that

$$A = A_o + \Delta A_1,$$

where $\operatorname{rank}(A_1) = 1$ and with $|\Delta| \leqslant 1$. Hence, there exist vectors e_1 and f_1 such that

$$A_1 = e_1 f_1^{\mathrm{T}}.$$

Now, suppose that the signal $f_1^{\mathrm{T}} x(\cdot)$ can be obtained from the outputs of the plant, assuming no measurement noise[‡], that is,

$$f_1^{\mathrm{T}} x(\cdot) = h^{\mathrm{T}} y(\cdot),$$

for some vector h, with the appropriate length. Also, let $H = e_1 h^{\mathrm{T}}$. Then, as described in [28], we can obtain a feedback description of the uncertain plant, where Δ is interconnected with the nominal plant, that is, the plant for $\Delta = 0$ – see Figure 7.

Using the left-coprime decomposition, this interconnection can be transformed into the one depicted in Figure 8. Hence, we can use the results in the previous subsection to assess whether or not the model with uncertain A matrix can describe a given input/output sequence.

In comparison with the previous results [16, 19], we are now able of handling uncertainties in matrix A, without using the convex hull of the set-valued state estimates obtained at the vertices of the uncertainty parameter sets. Nevertheless, this is only true if the linear combination of the states that multiplies the uncertainty can be recovered from the outputs of the plant.

4. SIMULATIONS

In this section, some advantages of the methods described in Section 3 are illustrated by means of an example. We consider a plant with a continuous-time realization

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Ld(t), \\ y(t) = Cx(t) + n(t), \end{cases} \tag{7}$$

[‡]The measurement noise will impact the estimate of the state by the SVO as a bounded disturbance. Therefore, it can be considered as such during the design of the SVO.

DOI: 10.1002/rnc

where $x(t) \in \mathbb{R}^5$ denotes the state of the system, $y(t) \in \mathbb{R}$ is the measured output, corrupted by noise $n(t)$, $u(t)$ is the control input and $d(t)$ is an exogenous disturbance. Moreover, we have that

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -2 & 2 & -0.2 & 0.2 & 0 \\ 2 & -2.15 & 0.2 & -0.3 & 1 \\ 0 & 0 & 0 & 0 & -10 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad L = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -10 \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

There are several real life applications that share the dynamics of the aforementioned equation, for instance in seismic and vibration models [37], automotive suspension systems [38] and flexible space structures [39], among others. In particular, these dynamics have been used in our previous studies, to describe a double mass-spring-dashpot plant, where the control input is noncollocated with the measured output – see, for example, [40, 41]. In this case, the output of the plant is the position of mass m_2, whereas the control input is the force applied to mass m_1.

The system in (7) was discretized using a sampling period of $T = 300$ ms. Moreover, the disturbances and measurement noise are assumed to follow a uniform distribution, with zero mean, and maximum absolute values of $\bar{d} := 1$ N and $\bar{n} := 0.001$ m, respectively. For the sake of simplicity, the control signal is defined as

$$u(k) := u(kT) := A_s \sin(\omega kT),$$

where $A_s = 2$ N and $\omega = 2$ rad/s. Hence, the state of the system at time kT can be described by

$$\begin{cases} x(k+1) = A_d x(k) + B_d u(k) + L_d d(k), \\ y(k) = C_d x(k) + n(k), \end{cases} \tag{8}$$

where the matrices A_d, B_d, L_d and C_d are straightforwardly obtained from the discretization of (7).

The model falsification architecture depicted in Figure 5 was adopted, using a set of three plausible models of the plant, described by (8), but with different C_d matrices:

- Model $M\#1$: $C_d = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix}$;
- Model $M\#2$: $C_d = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \end{bmatrix}$;
- Model $M\#3$: $C_d = \begin{bmatrix} 0 & 0.5 & 0 & 0 & 0 \end{bmatrix}$.

As a physical interpretation, these models represent different gains in the sensor that measures the position of mass m_2. For each of these models, a pair of SVOs for the corresponding coprime factorization was designed, as illustrated in Figure 5.

Notice that, if an SVO is designed for (8) as in [17], then the convergence of the set-valued estimate of the state would only be guaranteed if $N > 177$ in (4), because there are $k \in \mathbb{N}$ with $k \leqslant 177$ such that

$$\left\| A_d^k \right\| > 1.$$

However, by using the coprime factorization-based approach introduced in this paper, we guarantee the convergence of the set-valued estimates of the state for any $N \geqslant 5$ in (4). Hence, the computational burden associated with the implementation of the SVOs is significantly decreased.

The results obtained for a typical Monte–Carlo run of the aforementioned scenario are depicted in Figure 9. Here, it was considered that the initial state of the system is zero, whereas the set-valued initial state estimate is given by

$$\hat{X}(0) = \{x \in \mathbb{R}^5 : |x_i| \leqslant 0.1\}.$$

DOI: 10.1002/rnc

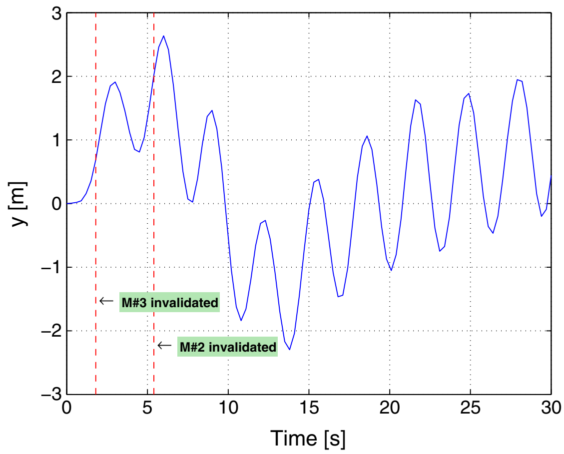


Figure 9. Output of the plant for a typical Monte–Carlo run. The time instants where the models were invalidated are also pointed out in the figure.

In reference to Figure 2, W_d and W_n are (constant) unit gains. In this example, model $M\#3$ was falsified in 1.8 s. Therefore, after six sampling periods, the input/output sequences are not compatible with the ones obtained from a dynamic system described by model $M\#3$. Nevertheless, models $M\#1$ and $M\#2$ are both valid, in the sense that the observed input/output sequences are compatible with such dynamics. At time $t = 5.4$ s, model $M\#2$ is invalidated. Hence, the only remaining model is the one compatible with (8) and with the observations. This model remains valid, as expected, throughout the simulation.

Remark 8
Each iteration requires between 1 and 3 s, to perform all the necessary computations, using an Intel Xeon CPU @2.6 GHz (Intel, Santa Clara, CA, USA). Notice that, for this case, the processing time required per sampling period is above the sampling period itself, thus jeopardizing the practical implementability of the technique. Such an issue can be circumvented by the following: (i) increasing the computational power; (ii) increasing the sampling period; or (iii) decreasing the horizon N. Indeed, the proposed structure can take advantage of parallel processing units because each SVO is independent from the other. Nevertheless, such practical improvements are out of the scope of this paper. For an experimental evaluation of SVOs, the reader is referred to [42].

5. CONCLUSIONS

A coprime factorization-based approach was proposed in this article to address the problem of model falsification of dynamic systems, using SVOs. The results presented indicate that using SVOs as a means of model invalidation is possible, not only for stable but also for unstable systems. Moreover, in terms of implementability, using the coprime factors of a transfer function matrix, rather than the 'original' transfer function matrix, may also have its own advantages. In particular, this method allows us to bound the number of required previous estimates of the state not to be larger than the number of states of the system. This particular benefit of the proposed methodology was also illustrated in simulation.

As a caveat, SVO-based model falsification is a *worst case* approach, in the sense that a model can only be invalidated if none of the allowable sequences of disturbances and measurement noise explains the measured output sequence.

DOI: 10.1002/rnc

ACKNOWLEDGEMENTS

This work was partially supported by Fundação para a Ciência e a Tecnologia (ISR/IST pluriannual funding) through the POS_Conhecimento Program that includes FEDER funds, and by the PTDC/EEA-ACR/72853/2006 OBSERVFLY Project.

REFERENCES

1. Poolla K, Khargonekar P, Tikku A, Krause J, Nagpal K. A time-domain approach to model validation. *IEEE Transactions on Automatic Control* 1994; **39**(5):951–959.
2. Bianchi F, Sánchez-Peña R. Robust identification/invalidation in an LPV framework. *International Journal of Robust and Nonlinear Control* 2010; **20**:301–312.
3. Blanke M, Kinnaert M, Lunze J, Staroswiecki M, Schröder J. *Diagnosis and Fault-Tolerant Control*, (2nd edn). Springer: Berlin, Germany, 2006.
4. Massoumnia M-A. A geometric approach to failure detection and identification in linear systems. *Ph.D. Dissertation*, Massachusetts Institute of Technology, 1986.
5. Massoumnia MA. Geometric approach to the synthesis of failure detection filters. *IEEE Transactions on Automatic Control* 1986; **31**(9):839–846.
6. Longhi S, Moteriù A. Fault detection for linear periodic systems using a geometric approach. *IEEE Transactions on Automatic Control* 2009; **54**(7):1637–1643.
7. Bokor J, Balas G. Detection filter design for LPV systems – a geometric approach. *Automatica* 2004; **40**:511–518.
8. Edelmayer A, Bokor J, Keviczky L. An $\mathcal{H}_\infty$ approach to robust detection of failures in dynamical systems. *Proceedings of the 33rd Conference on Decision and Control*, Vol. 3, Lake Buena Vista, FL, USA, 1994; 3037–3039.
9. Frank P, Ding X. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of Process Control* 1997; **7**(6):403–424.
10. Niemann H, Stoustrup J. Fault diagnosis for non-minimum phase systems using H_∞ optimization. *Proceedings of the American Control Conference*, Arlington, VA, USA, June 2001; **6**:4432–4436.
11. Marcos A, Ganguli S, Balas G. An application of $\mathcal{H}_\infty$ fault detection and isolation to a transport aircraft. *Control Engineering Practice* 2005; **13**:105–119.
12. Collins EGJ, Tinglun S. Robust l_1 estimation using the Popov–Tsypkin multiplier with application to robust fault detection. *International Journal of Control* 2001; **74**(3):303–313.
13. Mangoubi R, Appleby B, Verghese G, Vander Velde W. A robust failure detection and isolation algorithm. *Proceedings of the 34th Conference on Decision and Control*, Vol. 3, New Orleans, USA, 1995; 2377–2382.
14. Patton R, Chen J. Observer-based fault detection and isolation: robustness and applications. *Control Engineering Practice* 1997; **5**(5):671–682.
15. Esteban AM. Aircraft applications of fault detection and isolation techniques. *Ph.D. Dissertation*, University of Minnesota, 2004.
16. Rosa P, Silvestre C, Shamma J, Athans M. Multiple-model adaptive control with set-valued observers. *Proceedings of the 48th IEEE Conference on Decision and Control*, Shanghai, China, December 2009; 2441–2447.
17. Rosa P, Silvestre C, Shamma J, Athans M. Fault detection and isolation of LTV systems using set-valued observers. *Proceedings of the 49th IEEE Conference on Decision and Control*, Atlanta, GA, USA, December 2010; 768–774.
18. Rosa P, Silvestre C, Athans M. Model falsification of LPV systems using set-valued observers. *Proceedings of the 18th IFAC World Congress*, Milan, Italy, August–September 2011; **18**(1):1546–1551.
19. Rosa P, Silvestre C. Multiple-model adaptive control using set-valued observers. *International Journal of Robust and Nonlinear Control* (in press) 2013. DOI: 10.1002/rnc.3005.
20. Schweppe F. Recursive state estimation: unknown but bounded errors and system inputs. *IEEE Transactions on Automatic Control* 1968; **13**(1):22–28.
21. Bertsekas D, Rhodes I. Recursive state estimation for a set-membership description of uncertainty. *IEEE Transactions on Automatic Control* 1971; **16**(2):117–128.
22. Blanchini F, Miani S. *Set-Theoretic Methods in Control*. Birkhäuser: Basel, 2007.
23. Kosut R, Lau M, Boyd S. Set-membership identification of systems with parametric and nonparametric uncertainty. *IEEE Transactions on Automatic Control* 1992; **37**(7):929 –941.
24. Cabral FB, Safonov MG. Unfalsified model reference adaptive control using the ellipsoid algorithm. *International Journal of Adaptive Control and Signal Processing* 2004; **18**(8):683–696.
25. Shamma J, Tu K-Y. Set-valued observers and optimal disturbance rejection. *IEEE Transactions on Automatic Control* 1999; **44**(2):253–264.
26. Keerthi S, Gilbert E. Computation of minimum-time feedback control laws for discrete-time systems with state-control constraints. *IEEE Transactions on Automatic Control* 1987; **32**(5):432–435.
27. Blanchini F, Sznaier M. A convex optimization approach to synthesizing bounded complexity ℓ^∞ filters. *Proceedings of the 48th IEEE Conference on Decision and Control*, Shanghai, China, December 2009; 217–222.
28. Zhou K, Doyle J, Glover K. *Robust Optimal Control*. Prentice Hall: New Jersey, 1996.
29. Rosa P, Silvestre C. On the distinguishability of discrete linear time-invariant dynamic systems. *Proceedings of the 50th IEEE Conference on Decision and Control*, Orlando, FL, USA, December 2011; 3356–3361.

30. Grewal M, Glover K. Identifiability of linear and nonlinear dynamical systems. *IEEE Transactions on Automatic Control* 1976; **21**(6):833–837.
31. DiStefano J, III, Cobelli C. On parameter and structural identifiability: nonunique observability/reconstructibility for identifiable systems, other ambiguities and new definitions. *IEEE Transactions on Automatic Control* 1980; **25**(4):830–833.
32. Walter E, Lecourtier Y, Happel J. On the structural output distinguishability of parametric models, and its relations with structural identifiability. *IEEE Transactions on Automatic Control* 1984; **29**(1):56–57.
33. Lou H, Si P. The distinguishability of linear control systems. *Nonlinear Analysis: Hybrid Systems* 2009; **3**:21–38.
34. Johansson A. A sufficient condition for invalidation of linear state-space systems with uncertain time-varying parameters. *IEEE Transactions on Automatic Control* 2009; **54**(12):2915–2920.
35. Schweppe F. *Uncertain Dynamic Systems*. Prentice-Hall: USA, 1973.
36. O'Reilly J. *Observers for Linear Systems*. Academic Press Inc. (London) Ltd.: USA edition published by Academic Press Inc., New York, 1983.
37. Hergarten S, Jansen F. On the separation of timescales in spring-block earthquake models. *Nonlinear Processes in Geophysics* 2005; **12**:83–88.
38. Gaspar P, Szaszi I, Bokor J. Design of robust controllers for active vehicle suspension using the mixed μ synthesis. *Vehicle System Dynamics* 2003; **40**(4):193–228.
39. Balas G, Young P, Doyle J. μ based control design as applied to a large space structure: control design for the minimast facility. *Technical Report*, NASA CSI/GI final report, 1992.
40. Athans M, Fekri S, Pascoal A. Issues on robust adaptive feedback control. *Preprints of the 16th IFAC World Congress*, Prague, Czech Republic, 2005; 9–39.
41. Rosa P, Shamma J, Silvestre C, Athans M. Stability overlay for linear and nonlinear time-varying plants. *Proceedings of the 48th IEEE Conference on Decision and Control*, Shanghai, China, December 2009; 2435–2440.
42. Rosa P, Simao T, Lemos J, Silvestre C. Multiple-model adaptive control of an air heating fan using set-valued observers. *20th Mediterranean Conference on Control & Automation (MED)*, Barcelona, Spain, 2012; 469–474.

DOI: 10.1002/rnc