Active Fault Isolation: A Duality-Based Approach via Convex Programming

Franco Blanchini, Daniele Casagrande, Giulia Giordano, Stefano Miani, Sorin Olaru, Vasso Reppa

ACTIVE FAULT ISOLATION: A DUALITY-BASED APPROACH VIA CONVEX PROGRAMMING

FRANCO BLANCHINI[†], DANIELE CASAGRANDE[‡], GIULIA GIORDANO[§], STEFANO MIANI[‡], SORIN OLARU[¶], AND VASSO REPPA[‖]

Abstract. This paper presents the mathematical conditions and the associated design methodology of an active fault diagnosis technique for continuous-time linear systems. Given a set of faults known a priori, the system is modeled by a finite family of linear time-invariant systems, accounting for one healthy and several faulty configurations. By assuming bounded disturbances and using a residual generator, an invariant set and its projection in the residual space (*i.e.*, its limit set) are computed for each system configuration. Each limit set, related to a single system configuration, is parameterized with respect to the system input. Thanks to this design, active fault isolation can be guaranteed by the computation of a test input, either constant or periodic, such that the limit sets associated with different system configurations are separated, and the residual converges towards one limit set only. In order to alleviate the complexity of the explicit computation of the limit set, an implicit dual representation is adopted, leading to efficient procedures, based on quadratic programming, for computing the test input. The developed methodology offers a competent continuous-time solution to the optimization-based computation of the test input via Hahn-Banach duality. Simulation examples illustrate the application of the proposed active fault diagnosis methods and its efficiency in providing a solution, even in relatively large state-dimensional problems.

Key words. Active fault isolation, residual, limit set, support functional, separating hyperplane, convex programming, duality

AMS subject classifications. 49N15, 90C25, 93E10, 94C12

1. Introduction.

The occurrence of faults is unavoidable in the operational life of control processes, making indispensable the application of fault detection and isolation (FDI) mechanisms that monitor the system status [6]. In the last twenty years, model-based or analytical redundancy-based approaches became very popular for tackling the FDI problem [4, 10]. The FDI decision making process becomes challenging due to the presence of modeling errors, system disturbances, and measurement noise, which can mask the effects of faults [11]. When assuming stochastic uncertainties, the robustness of the FDI mechanism is defined with respect to an acceptable small rate of false alarms [12, 13]. On the other hand, when assuming bounded uncertainties, robustness entails that the FDI mechanism is insensitive to uncertainties (no false alarms). In both cases the fault detection rate should be maximized [9]. The boundedness assumption on the uncertainties, including faults, offers a particularly attractive framework for FDI guarantees.

The role of a FDI mechanism in the system supervision can be either passive or active. A passive FDI mechanism only monitors the input and output data of the system, and obtains a decision based on the processed information. Assuming bounded uncertainties, several researchers have developed passive FDI methods, where sets in

[†]Dipartimento di Matematica e Informatica, Università degli Studi di Udine, 33100 Udine, Italy. blanchini@uniud.it

[‡]Dipartimento di Ingegneria Elettrica, Gestionale e Meccanica, Università degli Studi di Udine, 33100 Udine, Italy. daniele.casagrande@uniud.it, miani.stefano@uniud.it

[§]Department of Automatic Control and LCCC Linnaeus Center, Lund University, 223 63 Lund, Sweden. giulia.giordano@control.lth.se

[¶]Laboratory of Signals and Systems (L2S, UMR 8506), CentraleSupélec-CNRS-U. Paris-Sud, U. Paris-Saclay, 91192, Gif-sur-Yvette, France. sorin.olaru@supelec.fr

[‖]KIOS Research and Innovation Center of Excellence, Department of Electrical & Computer Engineering, University of Cyprus, Nicosia, 1678, Cyprus. reppavasso@gmail.com

the parameter or residual space are generated on-line [33, 34, 30, 7, 31]. A fault is detected when either the parameter set is empty, or the inclusion of the residual within the corresponding set does not hold. In general, if the trajectories of the system states belong to sets or tubes [32, 5], then fault detection can be translated into an inclusion test [41]. Alternatively, several passive set-theoretic FDI methods aim at the off-line separation of healthy and faulty sets [38, 37] by exploiting the existence of *limit sets*, where the residuals are guaranteed to converge under healthy conditions and various fault scenarios.

If the FDI mechanism can step in the (closed-loop) system operation (e.g., there are no security or safety reasons that forbid the access to the system, or there is information related to the control design), its role becomes active. Active FDI can offer more design freedom to ensure the diagnosis of faults, which may be affected by the closed-loop system operation [2]. There are two main approaches to active fault diagnosis. (1) The FDI mechanism can intervene to the system operation by inducing an auxiliary input signal that can stimulate the system to make the effects of faults detectable [24, 8, 43, 35, 3, 28, 29]. Following this approach, the auxiliary signal can be designed based on the open-loop operation of the system [24, 8, 35], or the closed-loop operation [3, 43, 28, 29]. (2) The FDI can activate the reconfiguration of the control scheme, aiming to increase the detectability and the isolability of the faults [23, 44, 27, 42]. The design of active fault diagnosis methods depends also on the type of uncertainties and the associated assumptions. There is a significant research activity in the case of bounded uncertainties, e.g. [24, 35, 44, 43], while new methods were recently developed for stochastic disturbances [27], probabilistic parametric uncertainties [22], or both stochastic and bounded uncertainties [21]. Most of active fault diagnosis methods consider discrete-time systems, e.g. [24, 3, 35, 42, 28, 43, 29], and there are very few for continuous-time systems [23, 44, 25]. To the best of our knowledge, the auxiliary signal design of continuous-time systems with persistent-but-bounded disturbances is a challenging problem [40].

In this research work, we present an active observer-based FDI technique for continuous-time linear systems affected by norm-bounded disturbances. We take into account one healthy and several faulty system configurations, and seek suitable test signals that guarantee separation of the limit sets via hyperplanes in the residual space [24, 26, 28]. In contrast to [24], a finite isolation window can be obtained based on a positive answer for the asymptotic separation conditions. When compared to [26], the online monitoring is reduced to a simple positioning with respect to separating hyperplanes. Also, the forward set propagation and projection in [28] are avoided.

From a technical point of view, our contribution is twofold. Firstly, we propose a framework for obtaining a continuous-time solution to active FDI based on the Hahn-Banach theorem. Minimum norm duality allows us to show that the problem is convex; its domain is the unit ball of the residual space, which is typically of low (output-space) dimension. Secondly, since the explicit computation of limit sets is a complex task, we apply a *dual* implicit representation of limit sets for continuous time systems. Given a constant test signal u, we show that the distance between two limit sets can be obtained without explicitly computing the sets and requires quadratic programming in the case of the Euclidean norm. This design feature allows us to handle efficiently *large scale dimensions*. For constant test signals u bounded in a polytope, since the distance between limit sets is a convex function of u [19], the values that offer the best discrimination (maximizing the distance) are achieved on the vertices. For periodic test signals, a frequency sweeping procedure is proposed to

select the suitable frequencies for set-separation.

2. Problem Formulation. Consider the family of linear time invariant systems

$$\dot{x}(t) = A_h x(t) + B_h u(t) + E_h d(t) \tag{2.1}$$

$$y(t) = C_h x(t) + D_h w(t) \tag{2.2}$$

where $x(t) \in \mathbb{R}^n$ is the state, $u(t) \in \mathbb{R}^m$ is a controlled input signal, $y(t) \in \mathbb{R}^p$ is the measured output, while $d(t) \in \mathbb{R}^q$ and $w(t) \in \mathbb{R}^p$ are noise signals; A_h, B_h, C_h, D_h and E_h are matrices of appropriate dimensions. The index h is associated with the configuration (healthy or faulty) in which the system is operating:

$$[A_h, B_h, C_h, D_h, E_h], \qquad h \in \mathcal{H},$$

where $\mathcal{H} = \{0, 1, \ldots, N\}$ is a discrete and finite set of indices. Index $h = 0$ corresponds to the healthy configuration $[A_0, B_0, C_0, D_0, E_0] \doteq [A, B, C, D, E]$, while any other $h \geq 1$ corresponds to a faulty configuration. Note that matrices D_h and E_h are indexed as well, since a fault may alter the effect of the disturbances on the system. The disturbances $d(t) \in \mathbb{R}^q$ and $w(t) \in \mathbb{R}^p$ are unknown, but subject to the bounds

$$d(t) \in \mathcal{B}_q, \qquad w(t) \in \mathcal{B}_p,$$

where $\mathcal{B}_k \doteq \{v \in \mathbb{R}^k : \quad \|v\|_\infty \leq 1\}$ is the unit ball of the ∞-norm. Any weight concerning the components of d and w, respectively, is absorbed in the matrix E_h and in the square, possibly diagonal matrix D_h.

Note that all of the $N + 1$ system modes, corresponding to healthy and faulty configurations, can be known *a priori*, based on historical data used to create a fault dictionary [1], which is a common fault diagnosis tool for electric circuits [45].

The objective of this work is to determine suitable test signals u that guarantee the distinguishability of the system configurations $[A_h, B_h, C_h, D_h, E_h]$, $h \in \mathcal{H}$. If the system configurations are distinguishable for a specific test signal, then at each time instant we can check whether the system is operating in a non-healthy configuration, thus yielding to a finite-time fault detection, and even specify the exact faulty configuration (fault isolation).

3. Active Fault Isolation Based on Set Separation. In order to detect a fault and isolate it (namely, to establish the actual configuration h in which the system is operating), we can adopt an observer:

$$\frac{d}{dt}\hat{x}(t) = (A + LC)\hat{x}(t) + Bu(t) - Ly(t), \tag{3.1}$$

$$\hat{y}(t) = C\hat{x}(t). \tag{3.2}$$

The detection and isolation will rely on the monitoring of the *residual* signal:

$$r(t) = y(t) - \hat{y}(t), \tag{3.3}$$

which converges to zero in the absence of disturbances and in healthy conditions, provided that the observer is properly designed (*i.e.*, $(A+LC)$ is Hurwitz). Conversely, in faulty conditions and in the presence of noise this convergence is not ensured and r can be used as an indicator for fault diagnosis. The overall system dynamics is

$$\begin{aligned} \frac{d}{dt}\begin{bmatrix} x(t) \\ \hat{x}(t) \end{bmatrix} &= \begin{bmatrix} A_h & 0 \\ -LC_h & (A+LC) \end{bmatrix}\begin{bmatrix} x(t) \\ \hat{x}(t) \end{bmatrix} \\ &+ \begin{bmatrix} B_h \\ B \end{bmatrix} u(t) + \begin{bmatrix} E_h & 0 \\ 0 & -LD_h \end{bmatrix}\begin{bmatrix} d(t) \\ w(t) \end{bmatrix}, \end{aligned} \tag{3.4}$$

with residual output equation

$$r(t) = \begin{bmatrix} C_h & -C \end{bmatrix} \begin{bmatrix} x(t) \\ \hat{x}(t) \end{bmatrix} + \begin{bmatrix} 0 & D_h \end{bmatrix} \begin{bmatrix} d(t) \\ w(t) \end{bmatrix}. \tag{3.5}$$

We adopt the new state space representation

$$\dot{z}(t) = F_h z(t) + G_h u(t) + P_h v(t), \tag{3.6}$$

$$r(t) = M_h z(t) + Q_h v(t), \tag{3.7}$$

where $z(t) = \begin{bmatrix} x(t)^\top & \hat{x}(t)^\top \end{bmatrix}^\top \in \mathbb{R}^{2n}$, $v(t) = \begin{bmatrix} d(t)^\top & w(t)^\top \end{bmatrix}^\top \in \mathbb{R}^a$, $a = q+p$, and the matrices $F_h \in \mathbb{R}^{2n\times 2n}$, $G_h \in \mathbb{R}^{2n\times m}$, $P_h \in \mathbb{R}^{2n\times a}$, $M_h \in \mathbb{R}^{p\times 2n}$ and $Q_h \in \mathbb{R}^{p\times a}$ are those appearing in (3.4) and (3.5). Note that $v(t)$ is in the unit ball of the ∞-norm:

$$v(t) \in \mathcal{B}_a.$$

We make the following assumptions.

ASSUMPTION 1. *Matrices A_h are Hurwitz $\forall h \in \mathcal{H}$.*

ASSUMPTION 2. *Matrix L is given such that $(A + LC)$ is Hurwitz.*

REMARK 1. *The choice of an observer gain L such that $(A + LC)$ is Hurwitz requires the detectability of the pair (A, C). The observer gain L may be designed under observability conditions,* e.g.*, to optimize nominal (healthy) working conditions. Being a free design parameter, L can also be chosen so as to facilitate fast and effective FDI.* We assume that a test signal u of bounded magnitude is available for active fault detection and isolation. The essential idea is to choose u appropriately, to ensure that the limit sets to which the residual converges when the system is operating in different configurations can be separated by suitable hyperplanes.

In the residual space, let us define the convex and compact sets $\mathcal{R}_h(u) \subset \mathbb{R}^p$, $h \in \mathcal{H}$, each associated with one of the system configurations. We denote these limit sets as $\mathcal{R}_h(u)$ because, as we will see, they can be determined based on (3.6) and (3.7), hence their computation depends on the test signal u. In this work, the system configuration is inferred by validating, for all $k = 0, \ldots, N$, the hypothesis:

Hypothesis k: if $r(t) \in \mathcal{R}_k(u)$, the system configuration is $[A_k, B_k, C_k, D_k, E_k]$.

The healthy or a faulty configuration i is guaranteed to be isolated at a certain time instant t^* if and only if a single hypothesis (hypothesis i) is validated at time t^*. This can be achieved if we determine a test signal u such that $\mathcal{R}_h(u) \cap \mathcal{R}_l(u) = \emptyset$ for each pair $h, l \in \mathcal{H}$, $h \neq l$. However, the explicit computation of the sets $\mathcal{R}_h(u)$ and of their intersection can be intractable. We can deal with the problem by considering that two sets are separated (*i.e.*, have an empty intersection) if their distance is positive. Since the two limit sets $\mathcal{R}_h(u)$ and $\mathcal{R}_l(u)$ are convex, it is known that they are separated if and only if there exists a separating hyperplane

$$\mathcal{S}_{hl} = \left\{ r \in \mathbb{R}^p : \langle s_{hl}, r \rangle = \rho_{hl} \right\} \tag{3.8}$$

with $s_{hl} \in \mathbb{R}^p$ and $\rho_{hl} \in \mathbb{R}$ (we denote by $\langle \cdot, \cdot \rangle$ the scalar product) such that:

$$\begin{aligned} \langle s_{hl}, r \rangle &< \rho_{hl}, \qquad \text{for any } r \in \mathcal{R}_h(u), \\ \langle s_{hl}, r \rangle &> \rho_{hl}, \qquad \text{for any } r \in \mathcal{R}_l(u). \end{aligned}$$

Based on the concept of separating hyperplane, different system configurations can be distinguished, according the following definition.

DEFINITION 3.1. *Assume that a ball $\mathcal{A}$ of admissible initial conditions, centered in the origin, is given*[1] *and a test signal $u(\cdot)$ is assigned. Then, configurations h and l are* distinguishable *in the interval $[\bar{t}_1, \bar{t}_2]$ (possibly with $\bar{t}_2 = \infty$) if their corresponding sets $\mathcal{R}_h(u)$ and $\mathcal{R}_l(u)$, $h \neq l$, $h, l \in \mathcal{H}$ are separated in the interval $[\bar{t}_1, \bar{t}_2]$ by the hyperplane $\mathcal{S}_{hl}$ in* (3.8)*; namely if, for all $t \in [\bar{t}_1, \bar{t}_2]$, we have*

$$\begin{aligned} \langle s_{hl}, r \rangle &< \rho_{hl}, \qquad \text{if the configuration is } h, \\ \langle s_{hl}, r \rangle &> \rho_{hl}, \qquad \text{if the configuration is } l, \end{aligned}$$

for all initial conditions $x(0) \in \mathcal{A}$ and all $v(t) \in \mathcal{B}_a$.

In order to achieve separation between limit sets in the residual space (by providing suitable separating hyperplanes), two types of test signals will be considered.

- Constant $u(t) = u \in \mathbb{R}^m$: the separation interval will be open, $[\bar{t}_1, \infty)$.
- Sinusoidal $u(t) = \gamma \bar{u} \cos(\omega t)$, with constant $\bar{u} \in \mathbb{R}^m$: after some $\bar{t}$, the separation intervals $[\bar{t}_1 + k(2\pi/\omega), \bar{t}_2 + k(2\pi/\omega)]$, $k \in \mathbb{N}$, $\bar{t}_2 - \bar{t}_1 < (2\pi/\omega)$, will be repeated periodically.

Once proper separating hyperplanes are found off-line, active fault isolation requires monitoring on-line the signals

$$\sigma_{hl}(t) = \langle s_{hl}, r(t) \rangle, \tag{3.9}$$

for each pair $h, l \in \mathcal{H}$ and checking at each time instant if the signal σ_{hl} is greater or smaller than the corresponding threshold ρ_{hl}. As shown in the following sections, for each pair of configurations, finding the separating hyperplane, as well as checking whether the distance is positive, can efficiently be performed by exploiting duality.

REMARK 2. *A popular approach in fault diagnosis is based on the use of multiple models describing the healthy mode and various faulty modes of a system, and the generation of several residual filters associated with each model: using the available input and output data, fault diagnosis logic then checks which of the available known models matches the dynamical behavior of the system subject to faults. Due to the presence of uncertainties, the exact matching is unrealistic and optimization criteria are applied. In a bounded-uncertainty framework, the model that best matches the real system behavior is the one whose corresponding residual norm is less than a threshold, or the one with the smaller distance-like metric [47]. In a stochastic-uncertainty framework, the model that best matches the real system behavior is the one with the highest probability [50, 17]. In this work, instead of using a bank of dynamical residual filters (see e.g. Chapter 4 in [1]), we consider only one residual generator and check in which limit set the residual resides, taking into account the hyperplanes that separate the limit sets. Each limit set corresponds to a single system configuration, and their separation can be guaranteed by the proper auxiliary signal that is designed.*

In the following sections we will consider the continuous-time case; yet, we point out that the development of the theory would be unchanged in the discrete-time case, except for the fact that we need to consider series rather than integrals.

4. Set Separation via Constant Test Signals. We first consider constant signals, and present some preliminaries from convex analysis and duality theory.

[1] Assuming that the initial conditions are bounded in a ball is fundamental to ensure that separation actually occurs after a *finite* time instant $\bar{t}_1$. In general, the system state converges to a ball, but no guaranteed lower bound for the time can be provided if the initial conditions are arbitrary.

4.1. Separation of Convex Sets: Some Preliminaries. Given two convex and compact sets $\mathcal{R}_1$ and $\mathcal{R}_2$ in $\mathbb{R}^p$, we define their distance as

$$\text{dist}\,(\mathcal{R}_1, \mathcal{R}_2) \doteq \inf_{r_1 \in \mathcal{R}_1,\, r_2 \in \mathcal{R}_2} \|r_2 - r_1\|_2, \tag{4.1}$$

where $\|\cdot\|_2$ denotes the Euclidean norm. Since $\mathcal{R}_1$ and $\mathcal{R}_2$ are compact, the infimum is actually a minimum. The two sets are separated, i.e. $\mathcal{R}_1 \bigcap \mathcal{R}_2 = \emptyset$, if their distance is (strictly) positive: $\text{dist}\,(\mathcal{R}_1, \mathcal{R}_2) > 0$.

Determining the distance between two convex and compact sets is a convex optimization problem that is typically tractable when the representation of the sets $\mathcal{R}_1$ and $\mathcal{R}_2$ is simple enough. Unfortunately, this is not necessarily true in our setup.[2] However, we will show that the problem becomes tractable if we resort to duality, since an explicit computation of the limit sets is no more necessary.

The main idea is simple and is the following. The distance between $\mathcal{R}_1$ and $\mathcal{R}_2$ is equivalent to the distance of their difference $\mathcal{R} = \mathcal{R}_2 - \mathcal{R}_1$ from the origin. To explicitly represent $\mathcal{R}$ one has, in principle, to consider all possible realizations of the disturbances. Yet, the explicit representation of $\mathcal{R}$ can be avoided: it is enough to characterize **only** the disturbance function that realizes the distance by solving the (convex) dual problem. To this aim, we need the concept of support functional [20, 5].

DEFINITION 4.1. *Given a convex and compact set $\mathcal{R} \in \mathbb{R}^p$, the* support functional $\phi_{\mathcal{R}} : \mathbb{R}^p \to \mathbb{R}$ *is*

$$\phi_{\mathcal{R}}(s) \doteq \sup_{r \in \mathcal{R}} \langle s, r \rangle.$$

By duality [20], the distance (4.1) can be expressed as follows.

PROPOSITION 4.2. *Given two convex and compact sets $\mathcal{R}_1$ and $\mathcal{R}_2$ in $\mathbb{R}^p$, consider their distance, defined in* (4.1)*. Then*

$$dist\,(\mathcal{R}_1, \mathcal{R}_2) = \max_{\|s\|_2 \le 1} \big\{ -[\phi_{\mathcal{R}_1}(-s) + \phi_{\mathcal{R}_2}(s)] \big\}. \tag{4.2}$$

Proof. Let $r = r_2 - r_1$ and write (4.1) as

$$\text{dist}\,(\mathcal{R}_1, \mathcal{R}_2) \doteq \inf_{r \in \mathcal{R}_{21}} \|r\|_2, \tag{4.3}$$

where $\mathcal{R}_{21}$ is the Minkowski sum of $\mathcal{R}_2$ and $-\mathcal{R}_1$ defined as

$$\mathcal{R}_{21} = \{r = r_2 - r_1, \quad r_1 \in \mathcal{R}_1, \quad r_2 \in \mathcal{R}_2\}.$$

In view of the Hahn-Banach duality theorem (see [20], Th. 1, pag. 136), we have

$$\text{dist}\,(\mathcal{R}_1, \mathcal{R}_2) = \max_{\|s\|_2 \le 1} \quad -\phi_{\mathcal{R}_{21}}(s),$$

where $\phi_{\mathcal{R}_{21}}$ is the support functional of $\mathcal{R}_{21}$. By definition

$$\begin{aligned}\phi_{\mathcal{R}_{21}}(s) &= \max_{r \in \mathcal{R}_{21}} \langle s, r \rangle = \max_{r_1 \in \mathcal{R}_1,\ r_2 \in \mathcal{R}_2} \langle s, r_2 - r_1 \rangle = \left\{ \max_{r_1 \in \mathcal{R}_1} \langle s, -r_1 \rangle + \max_{r_2 \in \mathcal{R}_2} \langle s, r_2 \rangle \right\} \\ &= \left\{ \max_{r_1 \in \mathcal{R}_1} \langle -s, r_1 \rangle + \max_{r_2 \in \mathcal{R}_2} \langle s, r_2 \rangle \right\} = \{\phi_{\mathcal{R}_1}(-s) + \phi_{\mathcal{R}_2}(s)\}.\end{aligned}$$

[2] For instance, in the case of bounded-energy disturbances, the reachability sets would be ellipsoids and explicit computation would be feasible [18, 25, 5]. However, this is not the case for pointwise in time bounded disturbances.

Note that the supremum is indeed a maximum due to continuity and compactness of the sets $\mathcal{R}_1$ and $\mathcal{R}_2$. □

REMARK 3. *If in (4.1) a generic norm $\|\cdot\|_X$ is used, then the duality still holds if the Euclidean norm in (4.2) is replaced by $\|\cdot\|_{X^*}$, the dual norm of $\|\cdot\|_X$.*

Once we have established that the sets are separated, *i.e.*, that their distance is (strictly) positive, we need to find a separating hyperplane. We can take the half-way separating plane, as follows.

PROPOSITION 4.3. *If dist$(\mathcal{R}_1, \mathcal{R}_2) > 0$, then a separating hyperplane is*

$$\mathcal{S}_{12} = \left\{ r \in \mathbb{R}^p : \langle \hat{s}, r \rangle = \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2} \right\},$$

where $\hat{s}$ is the maximizer of (4.2)*. The distance of the hyperplane from both the sets $\mathcal{R}_1$ and $\mathcal{R}_2$ is equal to dist$(\mathcal{R}_1, \mathcal{R}_2)/2$.*

Proof. We show that $\langle \hat{s}, r_1 \rangle > \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2}$ for any $r_1 \in \mathcal{R}_1$. Indeed

$$\begin{aligned}\langle \hat{s}, r_1 \rangle &= -\langle -\hat{s}, r_1 \rangle \geq -\phi_{\mathcal{R}_1}(-\hat{s}) = \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2} - \frac{\phi_{\mathcal{R}_2}(\hat{s}) + \phi_{\mathcal{R}_1}(-\hat{s})}{2} \\ &= \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2} + \frac{\text{dist}\,(\mathcal{R}_1, \mathcal{R}_2)}{2} > \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2}.\end{aligned}$$

With an analogous reasoning, $\langle \hat{s}, r_2 \rangle < \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2}$ for any $r_2 \in \mathcal{R}_2$:

$$\begin{aligned}\langle \hat{s}, r_2 \rangle &\leq \phi_{\mathcal{R}_2}(\hat{s}) = \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2} - \left[-\frac{\phi_{\mathcal{R}_2}(\hat{s}) + \phi_{\mathcal{R}_1}(-\hat{s})}{2} \right] \\ &= \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2} - \frac{\text{dist}\,(\mathcal{R}_1, \mathcal{R}_2)}{2} < \frac{\phi_{\mathcal{R}_2}(\hat{s}) - \phi_{\mathcal{R}_1}(-\hat{s})}{2}.\end{aligned}$$

The hyperplane is at the same distance dist$(\mathcal{R}_1, \mathcal{R}_2)/2$ from both the sets, which is the quantity that we are neglecting, in both cases, to get a strict inequality. □

4.2. Asymptotic Separation of Limit Sets. Given system (3.6)–(3.7), we first deal with asymptotic separation of limit sets by means of constant test signals.

ASSUMPTION 3. *The test signal u is constant and lies in the polytope $\mathcal{U} \subset \mathbb{R}^m$.*

In view of asymptotic stability, in the absence of noise ($v \equiv 0$) the residual would converge asymptotically to the point

$$r_h(\infty) \doteq -M_h F_h^{-1} G_h u = -C_h A_h^{-1} B_h u + C(A + LC)^{-1}[LC_h A_h^{-1} B_h u + Bu].$$

In healthy conditions ($h = 0$), $r(t)$ converges to $r_0(\infty) = 0$. In the presence of noise, $r(t)$ converges to a set (limit set), which in healthy conditions is centered in the origin.

Under these assumptions, discriminating two configurations h and l in finite time (according to Definition 3.1) is possible if we know a separating hyperplane between $r_h(t)$ and $r_l(t)$. If we take the noise into account, a necessary and sufficient condition for the system trajectories to ultimately cross the separating hyperplane is that the limit sets for h and for l lie on opposite sides of the hyperplane [25].

By denoting by $\mathcal{Z}_h(0)$ the infinite-time reachable set for the input-free h system configuration (i.e. described by (3.6) with $u = 0$)

$$\dot{z} = F_h z(t) + P_h v(t), \tag{4.4}$$

the limit set $\mathcal{R}_h(u)$ associated with the h configuration can be expressed as

$$\mathcal{R}_h(u) = \{-M_h F_h^{-1} G_h u\} \oplus M_h \mathcal{Z}_h(0) \oplus Q_h \mathcal{B}_a, \tag{4.5}$$

where $\oplus$ is the Minkowski sum for sets. The residual $r(t)$ described by (3.3) is guaranteed to converge to a limit set $\mathcal{R}_h(u)$. The goal of this work is to compute, if possible, an input signal u that guarantees that the residual r converges to a separable limit set. If finding such a u is not possible, then the residual might converge to the non-empty intersection of two limit sets associated with two different configurations (e.g. the healthy limit set and a faulty limit set), leading to missed fault detection or non-isolation of the actual system configuration.

A crucial condition for the existence of u suitable for discriminating configurations h and l in finite time [24] is that $\mathcal{R}_h(u) \bigcap \mathcal{R}_l(u) = \emptyset$, *i.e.*, the distance $\delta_{hl}(u)$ between the two sets is positive:

$$\delta_{hl}(u) = \operatorname{dist}\left(\mathcal{R}_h(u), \mathcal{R}_l(u)\right) > 0. \tag{4.6}$$

Hence, the active fault isolation is realized based on the following definition.

DEFINITION 4.4. *Configurations l and h are* distinguishable *if there exists $u \in \mathcal{U}$ such that $\delta_{hl}(u) > 0$.*

PROBLEM 1. *Given the matrices F_h, G_h, M_h, Q_h P_h, $h \in \mathcal{H}$, the matrices F_l, G_l, M_l, Q_l P_l, $l \in \mathcal{H}$, $l \neq h$, and the polytope $\mathcal{U}$, find constant values $u_{hl} \in \mathcal{U}$ such that $\delta_{hl}(u) > 0$.*

REMARK 4. *The approach that employs constant test signals to find a separating hyperplane fails when the distance conditions* (4.6) *are not met. This happens for LTI system configurations* (2.1) *with similar static gains, a class of systems that can be efficiently handled with frequency-based tests, as described in Section 5. However, the general hyperplane method with constant test signals can be efficiently used for high dimensional systems, hence it is to be privileged in applications whenever* (4.6) *holds.*

The distance function $\delta_{hl}(u)$ has the following useful properties.

PROPOSITION 4.5. *[19] Function $\delta_{hl}(u)$ is convex.*

PROPOSITION 4.6. *[19] The maximum of $\delta_{hl}(u)$ is reached on the set of vertices of $\mathcal{U}$, vert($\mathcal{U}$).* Hence configurations h and l are distinguishable iff $\delta_{hl}(u) > 0$ for some $u \in \operatorname{vert}(\mathcal{U})$. Checking this condition thus requires solving a finite number of convex optimization problems.

The limit set for the residual is given by the projection $M_h\mathcal{Z}(0)$ of the infinite-time reachable set $\mathcal{Z}(0)$ for the state. In our case, we need a suitable external approximation of $M_h\mathcal{Z}(0)$ as a projection of an external approximation of $\mathcal{Z}(0)$. The difficulty, in view of (4.5), is that we would need evaluating the set

$$M_h\mathcal{Z}_h(0) = \left\{ r \in \mathbb{R}^p : r = \int_0^\infty \; M_h e^{F_h\sigma} P_h v(\sigma) d\sigma,\, v(\sigma) \in \mathcal{B}_a \right\}, \tag{4.7}$$

which is the image of the set of all functions v of bounded magnitude. Techniques based on support hyperplanes have been discussed in [36, 14]. Still, the problem is that this computation in the overall state-space would be prohibitive.

Moreover, if we establish that, for a certain u, $\delta_{hl}(u) > 0$, namely $\mathcal{R}_h(u)$ and $\mathcal{R}_l(u)$ are separated, the active fault isolation requires finding a separating hyperplane $\mathcal{S}_{hl} = \{r \in \mathbb{R}^p : \langle s_{hl}, r\rangle = \rho_{hl}\}$. Based on this hyperplane, configurations l and h can be distinguished on-line by monitoring the signal

$$\sigma_{hl}(t) = \langle s_{hl}, r(t)\rangle$$

and checking whether it is greater or smaller than the threshold ρ_{hl}. By adopting duality, we can simultaneously assess whether the distance is positive and find the separating hyperplane.

REMARK 5. *The separation between a certain pair of configurations is, in general, obtained with a constant signal different from the one needed to separate another pair. One could argue if, to distinguish multiple fault pairs at the same time, a single signal can be used. In most of the practical situations this is possible; however, the signal needed to make the separation detectable is much larger in magnitude than the signal needed to separate two configurations only.*

4.3. A Solution Based on Hahn-Banach Duality. We propose a solution that is based on duality in minimum distance problems and is quite efficient, since the residual space is typically low dimensional (at least, its dimension is usually lower than the state-space dimension). For the sake of generality, we now assume that

$$v(t) \in \mathcal{B}$$

where $\mathcal{B}$ is the unit (closed) ball of any norm $\|\cdot\|$. Denote by $\|\cdot\|_*$ the dual norm.

If we consider system (3.6)–(3.7), the limit set is

$$\mathcal{R}_h(u) = \left\{ r \in \mathbb{R}^p : r = -M_h F_h^{-1} G_h u + \int_0^\infty M_h e^{F_h \sigma} P_h v(\sigma) d\sigma + Q_h v_Q, \right. \\ \left. v(\sigma) \in \mathcal{B}, \quad v_Q \in \mathcal{B} \right\},$$

where we denote by v_Q the disturbance directly affecting the residual r, to discriminate it from the function $v(\sigma)$ in the integral. We need to assess whether $\delta_{hl}(u) = \mathrm{dist}(\mathcal{R}_h(u), \mathcal{R}_l(u)) > 0$. As shown in Section 4.1, the minimum-norm problem can be dualized by considering the support functional of $\mathcal{R}_h(u)$. For simplicity in the notation, we write $\phi_h = \phi_{\mathcal{R}_h(u)}$. Then we have

$$\begin{aligned} \phi_h(s) &= \sup_{r \in \mathcal{R}_h(u)} \langle s, r \rangle = \\ &= \sup_{v(\sigma) \in \mathcal{B}, v_Q \in \mathcal{B}} s^\top \left\{ -M_h F_h^{-1} G_h u + \int_0^\infty M_h e^{F_h \sigma} P_h v(\sigma) d\sigma + Q_h v_Q \right\} \\ &= -s^\top M_h F_h^{-1} G_h u + \sup_{v(\sigma) \in \mathcal{B}} \int_0^\infty s^\top M_h e^{F_h \sigma} P_h v(\sigma) d\sigma + \sup_{v_Q \in \mathcal{B}} s^\top Q_h v_Q. \end{aligned}$$

The supremum of the integral is achieved by selecting at each time

$$v(\sigma) = \frac{[s^\top M_h e^{F_h \sigma} P_h]^\top}{\|s^\top M_h e^{F_h \sigma} P_h\|_*}$$

(componentwise), so that the integrand function becomes $\|s^\top M_h e^{F_h \sigma} P_h\|_*$. Similarly, the supremum in the last term is $\|s^\top Q_h\|_*$. Then we get the following explicit expression for the support functional

$$\phi_h(s) = -s^\top M_h F_h^{-1} G_h u + \int_0^\infty \|s^\top M_h e^{F_h \sigma} P_h\|_* d\sigma + \|s^\top Q_h\|_*. \tag{4.8}$$

The support functional of a convex and compact set is convex [20] and locally bounded. We can then formulate the main result of the section.

PROPOSITION 4.7. *The distance function $\delta_{hl}(u)$ can be computed by solving the convex optimization problem*

$$\delta_{hl}(u) = -\min_{\|s\|_2 \le 1} \quad \{\phi_l(-s) + \phi_h(s)\}.$$

Once the problem is solved and the optimizer $\hat{s}$ is found, if the distance is positive, according to Proposition 4.3 a separating hyperplane is given by

$$\mathcal{S}_{hl} = \left\{ r \in \mathbb{R}^p : \langle \hat{s}, r \rangle = \frac{\phi_{\mathcal{R}_l}(\hat{s}) - \phi_{\mathcal{R}_h}(-\hat{s})}{2} \right\}.$$

The considered problem requires solving a convex optimization program in the unit ball of the Euclidean norm in $\mathbb{R}^p$ (formally, the dual of the residual space). This space is typically low dimensional and the solution can be found via standard software.

The only issue left is the evaluation of the integral. This is a straightforward task, which can be accomplished via numerical integration. If the time horizon is large enough, depending on the eigenvalues of F_h, the integral can be evaluated with arbitrary approximation. If the integration interval is $[0, T]$, then an upper bound for the truncation error:

$$\mathrm{err}(T) = \int_0^\infty \|s^\top M_h e^{F_h \sigma} P_h\|_* dt - \int_0^T \|s^\top M_h e^{F_h \sigma} P_h\|_* dt = \int_T^\infty \|s^\top M_h e^{F_h \sigma} P_h\|_* dt$$

is provided by the following result.

PROPOSITION 4.8. *Assume that matrix F_h has N distinct eigenvalues λ_k, with $k = 1, \dots, N$. Then*

$$err(T) \le \sum_{k=1}^{N} \quad \|\bar{R}_k\|_* \frac{e^{-\xi_k T}}{\xi_k},$$

where $\bar{R}_k = |R_k|$ are the componentwise magnitudes of vectors R_k (suitable complex residuals of the decomposition $s^\top M_h e^{F_h \sigma} P_h = \sum_{k=1}^{N} \quad R_k \; e^{\lambda_k \sigma}$) and $-\xi_k < 0$ is the real part of λ_k.

Proof. We have

$$\mathrm{err}(T) = \int_T^\infty \quad \|s^\top M_h e^{F_h \sigma} P_h\|_* d\sigma = \int_T^\infty \quad \| \sum_{k=1}^{N} \quad R_k \; e^{\lambda_k \sigma} \|_* d\sigma$$

$$\le \int_T^\infty \quad \sum_{k=1}^{N} \quad \|\bar{R}_k\|_* |e^{\lambda_k \sigma}| d\sigma = \sum_{k=1}^{N} \quad \|\bar{R}_k\|_* \int_T^\infty \quad |e^{\lambda_k \sigma}| d\sigma = \sum_{k=1}^{N} \quad \|\bar{R}_k\|_* \frac{e^{-\xi_k T}}{\xi_k}. \qquad \square$$

REMARK 6. *The error in the computation of the integral leads to overestimating the distance between the two sets: truncating the integral at time T is equivalent to neglecting the noise after T, hence considering smaller reachability sets. This consideration suggests to compute $err(T)$ once the procedure has given the "optimal" s.*

5. Set Separation via Frequency-Based Test Signals. In the following we assume that u is a scalar (hence, $m = 1$) frequency test signal of a fixed amplitude, injected in the system for detection purposes.

ASSUMPTION 4. *Signal u is sinusoidal, $u(t) = \gamma \cos(\omega t) \in \mathbb{R}$, with γ constant.*

We analyze the scalar case for simplicity and without restriction, since $u \in \mathbb{R}$ is enough to provide the fundamental principles of set separation via periodic signals. In fact, given the system (3.6), considering the test signal $u(t) = \gamma \bar{u} \cos(\omega t) \in \mathbb{R}^m$, with $\bar{u} \in \mathbb{R}^m$ a constant vector, and the matrix $G_h \in \mathbb{R}^{2n \times m}$, is equivalent to considering the scalar test signal $\tilde{u}(t) = \gamma \cos(\omega t)$ and the vector $\tilde{G}_h = G_h \bar{u} \in \mathbb{R}^{2n}$.

When considering sinusoidal test signals, the scenario changes with respect to Section 4, since in general the residual $r(t)$ of system (3.6)–(3.7) will converge asymptotically not to a fixed set, but to a "periodically evolving set" centered on a periodic orbit around the origin. Denoting by $\bar{\mathcal{R}}_h$ the limit set with no test signal ($u = 0$),

$$\bar{\mathcal{R}}_h = R_h(0) = \left\{ r \in \mathbb{R}^p : r = \int_0^\infty \quad M_h e^{F_h \sigma} P_h v(\sigma) d\sigma + Q_h v_Q, \qquad v(\sigma) \in \mathcal{B}, v_Q \in \mathcal{B} \right\},$$

the periodic limit set is

$$\mathcal{R}_h(\gamma, \omega t) = \bar{\mathcal{R}}_h \oplus \{ r = \gamma H_h(\omega) \nu(\omega t) \}, \tag{5.1}$$

where

$$\nu(\omega t) = [\ \cos(\omega t) \quad \sin(\omega t)\ ]^\top$$

and

$$H_h(\omega) = \left[\mathrm{Re}\left[M_h (j\omega I - F_h)^{-1} G_h \right] \quad - \mathrm{Im}\left[M_h (j\omega I - F_h)^{-1} G_h \right] \right].$$

Since we are dealing with periodically fluctuating sets, separation cannot be persistent, but just periodically occurring. With the support of Fig. 1, we now introduce the notions of weak and strong separation.

Definition 5.1. *Configurations h and l are* weakly separated by the test signal $u(t) = \gamma \cos(\omega t)$ *if there exist a hyperplane $\mathcal{S}_{hl} = \{ r \in \mathbb{R}^p : \langle s, r \rangle = \rho \}$ (which we call* weakly separating hyperplane*) and a time instant t_0 such that, for $t = t_0 + k(2\pi/\omega), \quad k \in \mathbb{N}$,*
i) $\langle s, r \rangle < \rho$ for all $r \in \mathcal{R}_h(\gamma, \omega t)$;
ii) $\langle s, r \rangle > \rho$ for all $r \in \mathcal{R}_l(\gamma, \omega t)$.

Remark 7. *Definitions 3.1 and 5.1 are concordant and can be related by the restriction $t = t_0 + k(2\pi/\omega) \in [\bar{t}_1 + k(2\pi/\omega), \bar{t}_2 + k(2\pi/\omega)], \ k \in \mathbb{N}$.*

A stronger notion of separation requires that one of the sets never crosses the hyperplane, while the other periodically does.

Definition 5.2. *Configuration l is* strongly separated by the test signal $u(t) = \gamma \cos(\omega t)$ from configuration h *if there exists a hyperplane $\mathcal{S}_{lh} = \{ r \in \mathbb{R}^p : \langle s, r \rangle = \rho \}$ (which we call* strongly separating hyperplane*) such that*
i) $\langle s, r \rangle < \rho$ for all $r \in \mathcal{R}_l(\gamma, \omega t)$;
ii) there exists t_0 such that $\langle s, r \rangle > \rho$ for $r \in \mathcal{R}_h(\gamma, \omega t)$ and $t = t_0 + k(2\pi/\omega), \quad k \in \mathbb{N}$.[3]

Each strongly separating hyperplane is obviously a weak separating hyperplane, but the other way round is not true. Two configurations may admit a weakly, but not a strongly, separating hyperplane; this happens, *e.g.*, when the two sets follow the same orbit with different phase.

[3]Equivalently, we may have that $\langle s, r \rangle > \rho$ for all $r \in \mathcal{R}_l(\gamma, \omega t)$ and there exists t_0 such that $\langle s, r \rangle < \rho$ for $r \in \mathcal{R}_h(\gamma, \omega t)$ and $t = t_0 + k(2\pi/\omega), \quad k \in \mathbb{N}$.

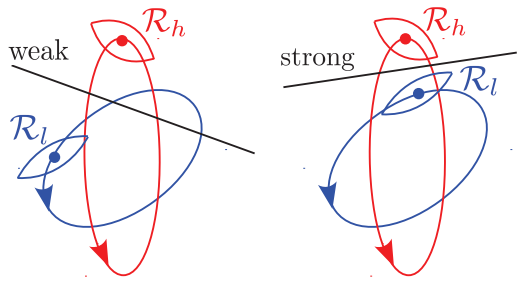

Fig. 1: Left: configurations h and l are (periodically) *weakly separated* by the hyperplane. Right: configuration l is *strongly separated* from configuration h.

Weak separation is equivalent to the fact that at some points $t = t_0 + k(2\pi/\omega)$, $k \in \mathbb{N}$, the distance between the limit sets is positive. It can be easily detected by means of a phase sweep, by checking whether

$$\max_{0 \le \theta \le 2\pi} \operatorname{dist}\left(\mathcal{R}_h(\gamma,\theta), \mathcal{R}_l(\gamma,\theta)\right) > 0\,,$$

where $\theta \doteq \omega t$, which reduces to solving a parameterized convex optimization problem.

REMARK 8. *Unlike weak separation, strong separation is an asymmetric concept: the strongly separating hyperplane can be crossed by one and only one of the two sets, which we call* external set *(set $\mathcal{R}_h$ in Fig. 1, right). The other one, we call* internal set*, always remains on one side of the hyperplane (set $\mathcal{R}_l$ in Fig. 1, right). The internal set is both strongly and weakly separated from the external set, while the external set is weakly separated from the internal set. Hopefully, for an efficient diagnosis, we might find other planes for which the situation is reversed ($\mathcal{R}_h$ is internal and $\mathcal{R}_l$ esternal).*

To handle the strong separation case, we need a preliminary lemma.

LEMMA 5.3. *The hyperplane $\mathcal{S}_{12} = \{r \in \mathbb{R}^p : \langle s, r\rangle = \rho\}$ separates two compact sets $\mathcal{R}_1$ and $\mathcal{R}_2$ in $\mathbb{R}^p$* (i.e., *$\langle s, r\rangle < \rho \;\forall\; r \in \mathcal{R}_1$ and $\langle s, r\rangle > \rho \;\forall\; r \in \mathcal{R}_2$) if and only if it separates conv$\{\mathcal{R}_1\}$ and conv$\{\mathcal{R}_2\}$, where conv$\{\cdot\}$ denotes the convex hull.*

Proof. The convex hull of the set $\mathcal{R}_i$, conv$\{\mathcal{R}_i\}$, is the intersection of all half-spaces including $\mathcal{R}_i$. Therefore, if $\mathcal{R}_1$ and $\mathcal{R}_2$ are on opposite sides of the hyperplane $\mathcal{S}_{12}$, so are their convex hulls, and vice-versa. □

The following theorem establishes the condition for strong separation.

THEOREM 5.4. *A strong separating hyperplane between $\mathcal{R}_h(\gamma,\theta)$ (external set) and $\mathcal{R}_l(\gamma,\theta)$ (internal set) exists if and only if the distance between $\mathcal{R}_h(\gamma,\theta)$ and*

$$\mathcal{C}_l(\gamma) \doteq \mathit{conv}\{\mathcal{R}_l(\gamma,\theta), \quad \theta \in [0, 2\pi]\}$$

is positive for some $\theta \in [0, 2\pi]$.

Proof. The thesis follows from Lemma 5.3, since strong separation of l from h is equivalent to the following two conditions.
i) $\mathcal{R}_l(\gamma,\theta)$ is on one side of a separating hyperplane for all t, hence for all $\theta = \omega t$. In view of Lemma 5.3, this is equivalent to the fact that the convex hull $\mathcal{C}_l(\gamma)$ of the floating set is always on one side of the hyperplane.
ii) $\mathcal{R}_h(\gamma,\theta)$ (which, being convex, is equal to conv $\{\mathcal{R}_h(\gamma,\theta)\}$) is on the opposite side of the hyperplane for some θ. □

Strong separation can be assessed by checking whether a periodic orbit, namely the ellipse of all points of the form $\gamma H_h(\omega)\nu(\theta)$, intersects a convex and compact set, as shown in the next theorem.

THEOREM 5.5. *A strongly separating hyperplane between configuration $\mathcal{R}_h(\gamma,\theta)$ (external set) and $\mathcal{R}_l(\gamma,\theta)$ (internal set) exists if and only if, for some $\theta \in [0,2\pi]$:*

$$\gamma H_h(\omega)\nu(\theta) \notin \bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma).$$

Proof. Assume that, for some $\theta \in [0,2\pi]$, $\mathcal{R}_h(\gamma,\theta)$ and $\mathcal{C}_l(\gamma)$ are separated by the hyperplane $\mathcal{S} = \{r \in \mathbb{R}^p : \langle s, r\rangle = \rho\}$. This is true if and only if $\langle s, r\rangle < \rho$ for all $r \in \mathcal{C}_l(\gamma)$ and $\langle s, r\rangle > \rho$ for all $r \in \mathcal{R}_h(\gamma,\theta)$. Hence, in view of (5.1),

$$\max_{r\in\mathcal{C}_l(\gamma)} \langle s, r\rangle < \rho < \min_{r\in\mathcal{R}_h(\gamma,\theta)} \langle s, r\rangle = \langle s, \gamma H_h(\omega)\nu(\theta)\rangle + \min_{r\in\bar{\mathcal{R}}_h} \langle s, r\rangle.$$

Equivalently, for such a θ,

$$\langle s, \gamma H_h(\omega)\nu(\theta)\rangle > \max_{r\in\mathcal{C}_l(\gamma)} \langle s, r\rangle - \min_{r\in\bar{\mathcal{R}}_h} \langle s, r\rangle = \max_{r\in\mathcal{C}_l(\gamma)} \langle s, r\rangle + \max_{r\in\bar{\mathcal{R}}_h} \langle s, r\rangle.$$

In the last equality, we exploited the fact that $-\min_{r\in\bar{\mathcal{R}}_h} \langle s, r\rangle = \max_{r'\in-\bar{\mathcal{R}}_h} \langle s, r'\rangle$ and the fact that $\mathcal{R}_h$ is 0-symmetric (due to the symmetry of the disturbance set, which is the unit ball of the ∞-norm), so that $\mathcal{R}_h = -\mathcal{R}_h$. Then, we have that

$$\begin{aligned}\langle s, \gamma H_h(\omega)\nu(\theta)\rangle &> \max_{r''\in\mathcal{C}_l(\gamma)} \langle s, r''\rangle + \max_{r'\in\bar{\mathcal{R}}_h} \langle s, r'\rangle = \max_{r'\in\bar{\mathcal{R}}_h,\ r''\in\mathcal{C}_l(\gamma)} \langle s, r' + r''\rangle \\ &= \max_{r\in\bar{\mathcal{R}}_h\oplus\mathcal{C}_l(\gamma)} \langle s, r\rangle.\end{aligned}$$

The proof is concluded by observing that the last condition is equivalent to saying that point $\gamma H_h(\omega)\nu(\theta)$ is outside the set $\bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma)$. Note that, since all the implications can be reversed, the provided condition is necessary and sufficient. □

The theorem signifies that, to find the value $\theta \in [0,2\pi]$ for which the point $\gamma H_h(\omega)\nu(\theta)$ has maximum distance from the set $\bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma)$, we can sweep over the phase θ. Also this problem can be solved by adopting duality, which leads to a convex optimization problem in the unit ball of $\mathbb{R}^p$.

PROPOSITION 5.6. *For any θ, the distance of $\gamma H_h(\omega)\nu(\theta)$ from $\bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma)$ is*

$$dist\big(\gamma H_h(\omega)\nu(\theta), \bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma)\big) = \max_{\|s\|_2\le 1} \ \langle s, \gamma H_h(\omega)\nu(\theta)\rangle - \phi_{lh}(s), \tag{5.2}$$

where

$$\begin{aligned}\phi_{lh}(s) = &\int_0^\infty \|s^\top M_h e^{F_h\sigma} P_h\|_* d\sigma + \|s^\top Q_h\|_* \\ &+ \int_0^\infty \|s^\top M_l e^{F_l\sigma} P_l\|_* d\sigma + \|s^\top Q_l\|_* + \gamma\|s^\top H_l(\omega)\|.\end{aligned} \tag{5.3}$$

Proof. The result follows by noting that

$$\bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma) = \bar{\mathcal{R}}_h \oplus \bar{\mathcal{R}}_l \oplus \{r \in \mathbb{R}^p : r = \gamma H_l(\omega)\nu(\theta), \quad \|\nu(\theta)\| \le 1\},$$

where the last set is an elliptical disk. Hence, the support functional of $\bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma)$ is exactly $\phi_{lh}(s)$ in (5.3) and the result in [20] (Th. 1, pag. 136) immediately applies. □

Once the optimal $\hat{s}$ is found, and also the frequency $\hat{\theta}$ that maximizes the distance of $\gamma H_h(\omega)\nu(\theta)$ from $\bar{\mathcal{R}}_h \oplus \mathcal{C}_l(\gamma)$, a separating hyperplane between the two configurations h and l can be found as follows.

COROLLARY 5.7. *A separating hyperplane between* $\mathcal{R}_h(\gamma,\hat{\theta})$ *and* $\mathcal{C}_l(\gamma)$ *is*

$$\mathcal{S}_{lh} = \left\{ r \in \mathbb{R}^p : \langle \hat{s}, r \rangle = \frac{\rho_1 + \rho_2}{2} \right\},$$

where

$$\rho_1 = \int_0^\infty \|\hat{s}^\top M_l e^{F_l \sigma} P_l\|_* d\sigma + \|\hat{s}^\top Q_l\|_* + \gamma \|\hat{s}^\top H_l(\omega)\|$$

and

$$\rho_2 = \gamma \langle \hat{s}, H_h(\omega)\nu\hat{\theta} \rangle - \int_0^\infty \|\hat{s}^\top M_h e^{F_h \sigma} P_h\|_* d\sigma - \|\hat{s}^\top Q_h\|_*.$$

Proof. The proof follows from Proposition 4.3. Indeed ρ_1 and ρ_2 are, respectively, the support functional of $\mathcal{C}_l(\gamma)$ evaluated in $\hat{s}$ and the opposite of the support functional of $\mathcal{R}_h(\gamma,\hat{\theta})$ evaluated in $-\hat{s}$. □

REMARK 9. *There are cases in which there exists a hyperplane that strongly separates* l *from* h*, where* $\mathcal{R}_h(\gamma,\theta)$ *is the external set and* $\mathcal{R}_l(\gamma,\theta)$ *the internal set, while the other way around is not possible. This happens, for instance, in the case of a damped oscillator, frequency tested: the failure of the damper can lead to a situation in which the faulty orbits in the position-speed plane encircle the healthy orbits. Therefore, only the healthy set can be internal.*

Since the amplitude of the periodic orbit is a monotone function of the amplitude of the test signal, the larger γ is chosen (compatibly with the given bounds), the better set separation is achieved. However, we are interested in finding the smallest γ for which set separation is ensured. Conversely, for a fixed amplitude, a possibility is to choose the frequency that provides the best separation (in terms of maximum distance between the sets). This can be done as follows.

PROCEDURE 1. **Inputs:** *frequency range* $[\omega_1, \omega_2]$*, frequency step* $\delta\omega > 0$*, phase step* $\delta\theta > 0$*, indices* l *and* h*.*
Outputs: s_{sep} *and* ρ_{sep} *of the separating hyperplane* $\mathcal{S} = \{r \in \mathbb{R}^p : \langle s_{sep}, r \rangle = \rho_{sep}\}$*.*
Set $\omega_{sep} := \omega_1$*,* $dist_{sep} := 0$*,* $s_{sep} = [0\ 0]^\top$*.*
– *FOR* $\omega := \omega_1 : \delta\omega : \omega_2$
  – *FOR* $\theta := 0 : \delta\theta : \pi$
    – *Solve the dual convex optimization problem* (5.2)*.*
    – *IF* $dist >$ $dist_{max}$*, THEN* $dist_{max} := dist$*,* $\omega_{sep} := \hat{\omega}$*,* $\theta_{sep} := \hat{\theta}$*,* $s_{sep} := \hat{s}$*.*
  – *End FOR*
– *End FOR*
– *Given* s_{sep}*, compute* ρ_{sep} *as in Corollary 5.7, so that* $\mathcal{S} = \{r \in \mathbb{R}^p : \langle s_{sep}, r \rangle = \rho_{sep}\}$ *is the separating hyperplane.* As previously observed, in general at each frequency there exists an infimum $\hat{\gamma}(\omega)$ such that separation can be achieved for $\gamma > \hat{\gamma}(\omega)$. We now discuss conditions ensuring that weak or strong separation is possible (i.e. $\gamma(\omega)$ is finite). The following proposition is a generalization of the condition in [25].

PROPOSITION 5.8. *Weak separation between configurations* h *and* l *is possible at some frequency* ω *if and only if the transfer functions* H_h *and* H_l *are distinct:*

$$H_h(\omega) \neq H_l(\omega). \tag{5.4}$$

Strong separation (either of configuration h *from* l *or vice-versa) is possible at some frequency* ω *if and only if the transfer functions* H_h *and* H_l *are distinct even under a*

phase shift:

$$H_h(\omega) \neq H_l(\omega)\Xi(\theta), \quad \forall \;\; 0 \leq \theta \leq 2\pi, \tag{5.5}$$

where $\Xi(\theta)$ *is the rotation matrix*

$$\Xi(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}.$$

Proof. Weak separation requires that $\mathcal{R}_h(\gamma, \omega t)$ and $\mathcal{R}_l(\gamma, \omega t)$ are disjoint at some t. Since the size of the noise-dependent component of the set is independent of the testing signal u, we can scale the condition as

$$\frac{1}{\gamma}\mathcal{R}_h(\gamma, \omega t) \bigcap \frac{1}{\gamma}\mathcal{R}_l(\gamma, \omega t) = \emptyset$$

and then, from (5.1), we get

$$\frac{1}{\gamma}\bar{\mathcal{R}}_h \oplus \{r = H_h(\omega)\nu(\omega t)\} \bigcap \frac{1}{\gamma}\bar{\mathcal{R}}_l \oplus \{r = H_l(\omega)\nu(\omega t)\} = \emptyset.$$

The size of the two sets $\bar{\mathcal{R}}_h/\gamma$ and $\bar{\mathcal{R}}_l/\gamma$ decreases with γ, so the intersection becomes empty for large enough γ if and only if (5.4) holds.

For the strong separation condition (5.5) the proof is almost identical. The only difference is that we might have two periodic orbits which are identical up to a phase shift: in this case, strong separation would be impossible. □

REMARK 10. *The constant signal is a particular case of periodic test signal and the separability condition* (5.4) *has to be satisfied for* $\omega = 0$ *leading to a simple interpretation: the distinguishability in this case is related to the static gain which has to be different. More general signal could be considered. Periodic signals (e.g. square or saw waves) could be handled by means of a Fourier analysis without conceptual difficulties. From a practical standpoint, however, the overall scheme would be much more involved. Non-periodic signal would not lead to theoretical difficulties, but they would require recording all possible trajectories on an infinite horizon, for all possible configuration: this is practically unrealistic.*

6. Examples.

6.1. Electrical Network. Consider the network with capacitors and resistors shown in Fig. 2, where the connections with the four marked resistors can be fully interrupted. Three voltage generators, each with maximum voltage V_{max}, can be applied in points A, B or C. Then $|V_A| + |V_B| + |V_C| \leq 3V_{max}$. According to Proposition 4.6, the best discriminating property is achieved by applying the series of all the generators at the maximum voltage in one of the points (A, B or C). We assume each capacitor of $1\mu F$ and each resistor of $1k\Omega$, with the exception of the load resistors $R_{C2} = R_{C4} = R_{C6} = 20k\Omega$. A disturbance d of amplitude $1A$ acts on capacitor 2 and the available measurements are the voltages on capacitors 4 and 6.

Being the system stable, we could use a trivial observer $L = 0$. Next we report the (symmetric) tables Δ_A, Δ_B, Δ_C of the distances among the residual sets, achieved by applying a voltage of $250V = 3V_{max}$ at the points A, B and C, respectively. The healthy condition is in the last row/column. For instance, in Δ_A, entry 1–2 represents the distance between limit sets associated with faulty configurations 1 and 2, while

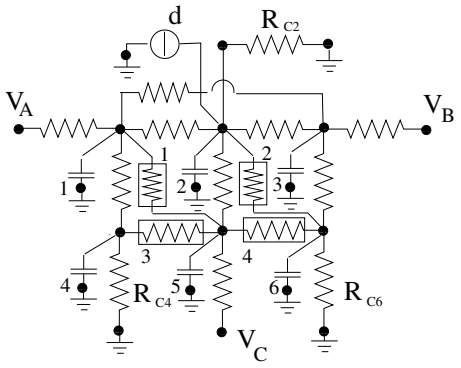

Fig. 2: The electric circuit.

entry 3–5 is the distance between limit sets associated with the faulty condition 3 and the healthy condition ($h = 0$). Quite surprisingly, in general the trivial observer $L = 0$ works much better than the "optimal observer" in terms of guaranteed distances: this is most probably due to a "stabilizing effect" of the filter with respect to the test input u, which makes fault isolation more difficult.

$\Delta_A =$

	1	2	3	4	0
1	0	0	9.8045	11.6363	1.2015
2	0	0	8.8918	12.3898	1.8044
3	9.8045	8.8918	0	22.9829	11.4089
4	11.6363	12.3898	22.9829	0	12.5671
0	1.2015	1.8044	11.4089	12.5671	0

$\Delta_B =$

	1	2	3	4	0
1	0	0.2998	8.9882	16.0927	0
2	0.2998	0	6.7890	14.5159	0
3	8.9882	6.7890	0	7.0741	8.5654
4	16.0927	14.5159	7.0741	0	15.8557
0	0	0	8.5654	15.8557	0

$\Delta_C =$

	1	2	3	4	0
1	0	0.1783	63.9698	52.3798	1.6246
2	0.1783	0	61.8821	49.9311	0
3	63.9698	61.8821	0	18.9248	61.0577
4	52.3798	49.9311	18.9248	0	48.8082
0	1.6246	0	61.0577	48.8082	0

These tests are typically performed when the circuit is not normally operated and under the assumption that the testing signal maximum value V_{max} is considerably smaller than the maximum voltage admissible in the circuit. Testing the circuit under normal operations is clearly possible: for instance, one can assume that the same voltage is applied to all points V_A, V_B and V_C. With our method, we can numerically compute the minimum effective signal: the minimal voltage to be applied to all generators, to ensure overall pairwise separation, is around $5000V$, roughly 20 time the intensity required if the diagnosis is performed separately. Hence, the application of the same voltage to all points has a very limited diagnosis sensibility.

6.2. Elastic System. Consider the 5-degree-of-freedom oscillating system depicted in Fig. 3, with a persistent noise d affecting mass 3. The state variables are the positions and their derivatives (velocities). An auxiliary input u consisting of a force is applied to mass 5, while the outputs y_1 and y_2 are the positions of masses 1

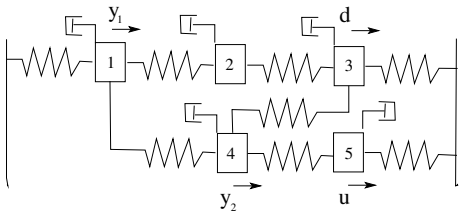

Fig. 3: The oscillating system.

and 4. We assume that a complete failure of the springs connecting masses 1-4 and 3-4 can occur. The model of the system is

$$M\ddot{q}(t) = -K_h^{EL} q(t) - D^{DA}\dot{q}(t) + B_q u(t) + E_q d(t)$$
$$y(t) = [\ q_1(t)\ \ q_4(t)\ ]^\top + w(t)$$

where $y, w \in \mathbb{R}^2$, $\|w\|_\infty \leq 1$, $|d(t)| \leq 1$, the mass diagonal matrix is the identity matrix, the nominal damping matrix is $D^{DA}_{nom} = 0.3I$, while the stiffness matrix and the actual damping matrix are, respectively,

$$K_h^{EL} = \begin{bmatrix} 4 & -1 & 0 & -1 & 0 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 3 & -1 & 0 \\ -1 & 0 & -1 & 3 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{bmatrix} \text{ and } D^{DA} = \begin{bmatrix} 0.3 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & \beta & 0 & 0 \\ 0 & 0 & 0 & 0.3 & 0 \\ 0 & 0 & 0 & 0 & 0.3 \end{bmatrix}.$$

We assume that some dumpers can fail. For brevity, we consider two of them: damper 2 and damper 3. The possible configurations are

$$\begin{array}{lll} h = 0: & \{\alpha = 0.3,\ \beta = 0.3\}, & \text{healthy}, \\ h = 1: & \{\alpha = 0,\ \beta = 0.3\}, & \text{faulty}, \\ h = 2: & \{\alpha = 0.3,\ \beta = 0\}, & \text{faulty}. \end{array}$$

From physical considerations, we see that a constant test signal would be of no use, because the system steady state does not depend on the damper values. Here a frequency test is fundamental. We have computed the function

- $\rho_{lh}(\gamma, \omega)$ = distance for the strong separation of l from h.

and such values are depicted in Figs. 4. We remind that whenever such index is greater than 0 there exists a separation hyperplane periodically crossed by residual l, but never crossed by the residual h.

It is apparent there are three ranges of frequencies, centered around about 0.81 rad/sec, 1.20 rad/s and 1.8 rad/sec at which the indexes ρ_{lh} attain their maxima. We point out that the proper undamped frequencies of the elastic system are $\omega_1 = 0.8132$, $\omega_2 = 1.2446$, $\omega_3 = 1.7321$, $\omega_4 = 1.8759$, $\omega_5 = 2.2958$, and as expected the good ranges enclose some of them. However, quite unexpectedly, the good range at which all the three indexes are significantly high is located between ω_3 and ω_4. The optimal separating hyperplanes at $\omega = 1.816$ rad/s are depicted in Fig. 4 bottom right, where $s_{21}^\top = [0.969\ 0.245]$, $s_{20}^\top = [1\ 0]$ and $s_{10}^\top = [0.411\ \ -0.911]$. The distance is quite modest or null at the other frequencies, including the second. This definitely depends on the placement of the sensors and actuator: a different topology could clearly give a completely different result.

In Fig. 5, the periodic orbits with the effect of the noise corresponding to $\gamma = 100$ and $\omega = 1.816$ are depicted, along with the strongly separating hyperplane $s_{21}^\top x = 14.86$. The worst case phase is about $\theta = 2.4$.

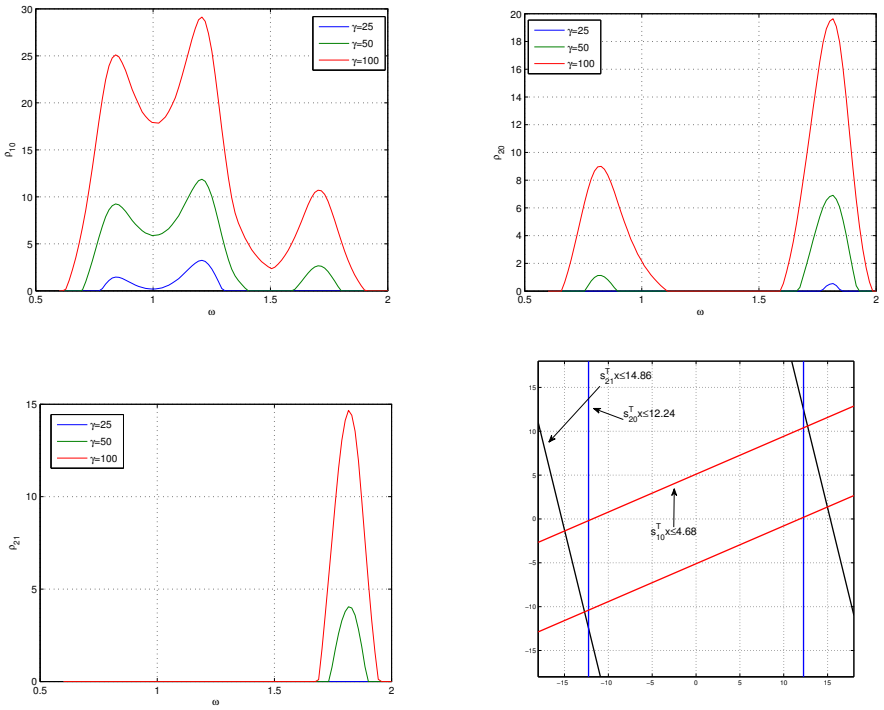

Fig. 4: Separation distances between pairs of configurations: top left, distance $\rho_{10}(\gamma, \omega)$ between configuration $l = 1$ (faulty with $\alpha = 0$) and $h = 0$ (healthy); top right, distance $\rho_{20}(\gamma, \omega)$ between configuration $l = 2$ (faulty with $\beta = 0$) and $h = 0$; bottom left, distance $\rho_{21}(\gamma, \omega)$ between configuration $h = 2$ (faulty with $\beta = 0$) and $h = 1$ (faulty with $\alpha = 0$). Bottom right: the separating hyperplanes at $\omega = 1.816$ rad/s; for each pair of configurations (s_{21}, s_{20} and s_{10}) a hyperplane, as well as its symmetric counterpart, is found.

Given the existence of non null separation values for all the three indexes around $\omega = 1.8$ for $\gamma = 100$, a single exciting signal with $\gamma = 100$ and $\omega = 1.816$ is sufficient to exactly determine the current configuration. It is apparent that two different exciting frequencies and amplitudes might have been used, e.g. $\gamma = 25$ at $\omega = 0.84$ to verify whether the system is working in the faulty configuration 1 or the healthy, $\gamma = 25$ at $\omega = 1.816$ to verify configuration 2 vs configuration 0, etc.

This example and the associated discussion on the exciting frequencies can be linked to the analysis in [8] (section 3.8, page 111) on the asymptotic behavior of the excitation signals, although the assumption on the disturbances are slightly different. In [8], a dominant frequency appears in the auxiliary excitation signals; we can interpret this observation in light of the parameterization of separation distance between limit sets, which depends on the frequency.

As a final comment, Fig. 5 shows that, for some noise realizations, the residual can periodically intersect the orbit associated with a different configuration. In these cases, a (complete) separation is not performed and there might be false alarms/diagnosis.

7. Concluding Remarks. We have described the design of an active fault detection and isolation (FDI) method for continuous-time linear systems. Using known

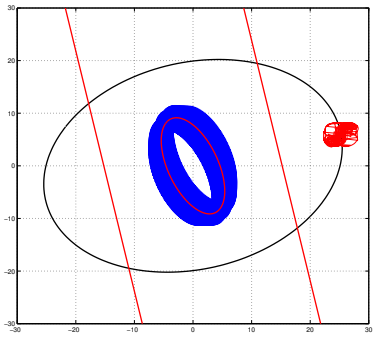

Fig. 5: The periodic residual orbits for configurations 2 (blue) and 1 (red) and the plane $s_{21}^{\top} x = 14.86$ that strongly separates 2 from 1.

bounds for the disturbances and a linear residual generator, we consider the limit sets associated with different faults, towards which the residual is guaranteed to converge. Every limit set is parameterized with respect to a single system configuration and an auxiliary signal. Active FDI could be performed by computing an auxiliary signal that separates the limit sets making detection possible by monitoring the residual. However, the separation of limit sets is a cumbersome problem when the explicit description of the limit sets, which is rather complex, is required. The auxiliary input is either a constant or a sinusoidal signal.

To overcome this problem, instead of explicitly determining or approximating the limit sets, we use duality to compute of the distance between two limit sets, based on the their support functionals, by solving a convex optimization problem. We can guarantee that the isolation window is finite by checking if the distance is positive. In addition, separating hyperplanes are easily computed. The approach allows us to decide off-line which are the optimal input signals to apply in order to guarantee fault isolation, while the on-line decision is simply made by checking if the residual is to the left or to the right of the separating hyperplanes (which requires a negligible computational effort). We believe that the proposed approach can be fruitfully combined with previous methods, *e.g.* [25, 43, 35], providing *a priori* separation guarantees. Our approach, based on the separation of sets, shares some weakness with the existing methods because its efficiency could be compromised in the case of large model uncertainties, a problem which also arises when explicitly computing reachable sets.

The added value of the suggested methodology is that it works in continuous-time as well and drastically reduces complexity. In practice, the technique can be applied by considering a set of *a priori* known faults which can be determined form historical data, or after a vulnerability analysis, the developed methodology can be used for preventive maintenance. Specifically, by regularly applying the proposed methods with different auxiliary signals, we may be able to localize a fault before it becomes a failure. Furthermore, through this technique we can determine the input signal that will drive the system to a safe configuration. Ideally, the safe configuration is the healthy configuration; in practice, it can be a faulty configuration with minimal consequences in order to increase the remaining useful life of the system. The active fault isolation problem can be investigated in relation to a sensor placement problem,

aiming at enhancing the separability of the limit sets by a proper selection of sensors.

REFERENCES

[1] C. Alippi, M. Catelani, A. Fort, and M. Mugnaini, *Automated selection of test frequencies for fault diagnosis in analog electronic circuits*, IEEE Trans. Instrum. Meas., 54 (2005), pp. 1033–1044.

[2] A. E. Ashari, R. Nikoukhah, and S. L. Campbell, *Effects of feedback on active fault detection*, Automatica, 48 (2012), pp. 866–872.

[3] A. E. Ashari, R. Nikoukhah, and S. L. Campbell, *Active Robust Fault Detection in Closed-Loop Systems: Quadratic Optimization Approach*, IEEE Transaction on Automatic Control, 51 (2012), pp. 2532–2544.

[4] M. Basseville and I. V. Nikiforov, *Detection of abrupt changes: theory and application*, vol. 104, Prentice Hall Englewood Cliffs, 1993.

[5] F. Blanchini and S. Miani, *Set-theoretic methods in control*, Systems & Control: Foundations & Applications, Birkhäuser, Basel, 2015.

[6] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and fault-tolerant control*, Springer-Verlag Berlin Heidelberg, 2016.

[7] J. Blesa, V. Puig, J. Saludes, and R. M. Fernndez-Cant, *Set-membership parity space approach for fault detection in linear uncertain dynamic systems*, Int. J. Adaptive Control and Signal Processing, (2014). doi: 10.1002/acs.2476.

[8] S. La Vern Campbell and R. Nikoukhah, *Auxiliary signal design for failure detection*, Princeton University Press, 2004.

[9] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*, Springer Publishing Company, Incorporated, 2012.

[10] S. X. Ding, *Model-based fault diagnosis techniques*, Springer, 2008.

[11] P. M. Frank, *Handling modelling uncertainty in fault detection and isolation systems*, J. Control Engineering and Applied Informatics, 4 (2002), pp. 29–46.

[12] P. Goupil, and A. Marcos, *ndustrial Review*, In Fault Tolerant Flight Control,Springer Berlin Heidelberg, pp. 521–536.

[13] P. Goupil, *AIRBUS state of the art and practices on FDI and FTC in flight control system, Control Engineering Practice*, Control Engineering Practice, 19 (2011), pp. 524–539.

[14] T. J. Graettinger and B. H. Krogh, *Hyperplane method for reachable state estimation for linear time-invariant systems*, J. Optimization Theory and Applications, 69 (1991), pp. 555–587.

[15] P. Gurfil, *Relative motion between elliptic orbits: generalized boundedness conditions and optimal formation keeping*, J. Guidance, Control, and Dynamics, 28 (2005), pp. 761–767.

[16] D. Henry and A. Zolghadri, *Design and analysis of robust residual generators for systems under feedback control*, Automatica, 41 (2005), pp. 251–264.

[17] S. Kim, J. Choi, and Y. Kim, *Fault detection and diagnosis of aircraft actuators using fuzzy-tuning IMM filter*, IEEE Trans. Aerosp. Electron. Syst., 44 (2008), pp. 940–952.

[18] A. Kurzhanski and I. Valyi, *Ellipsoidal Calculus for Estimation and Control*, Birkhäuser Mathematics, 1994.

[19] K. K. Kwang-Ki, D. M. Raimondo, and R. D. Braatz, *Optimum input design for fault detection and diagnosis: Model-based prediction and statistical distance measures*, in Proc. European Control Conference (ECC), 2013, pp. 1940–1945.

[20] D. G. Luenberger, *Optimization by vector space methods*, John Wiley & Sons Inc., New York, New York, USA, 1969.

[21] G. R. Marseglia, J. K. Scott, L. Magni, R.D. Braatz, and D. M. Raimondo, , *A hybrid stochastic-deterministic approach for active fault diagnosis using scenario optimization*, IFAC Proc. Volumes, 47 (2014), pp. 1102–1107

[22] A. Mesbah, S. Streif, R. Findeisen, and R.D. Braatz, , *Active fault diagnosis for nonlinear systems with probabilistic uncertainties*, IFAC Proc. Volumes, 47 (2014), pp. 7079–7084.

[23] H. Niemann, *A setup for active fault diagnosis*, IEEE Trans. Autom. Control, 51 (2006), pp. 1572–1578.

[24] R. Nikoukhah, *Guaranteed active failure detection and isolation for linear dynamical systems*, Automatica, 34 (1998), pp. 1345–1358.

[25] R. Nikoukhah, S. L. Campbell, K. G. Horton, and F. Delebecque, *Auxiliary signal design for robust multimodel identification*, IEEE Trans. Autom. Control, 47 (2002), pp. 158–164.

[26] S. Olaru, J. A. De Doná, M. M. Seron, and F. Stoican, *Positive invariant sets for fault tolerant multisensor control schemes*, Int. J. Control, 83 (2010).

[27] I. Punčochář, J. Širokỳ, and M. Šimandl,, *Constrained active fault detection and control*, IEEE Trans. Autom. Control, 60 (2015), pp. 253–258.
[28] D. M. Raimondo, R. D. Braatz, and J. K. Scott, *Active fault diagnosis using moving horizon input design*, in Proc. European Control Conference (ECC), 2013, pp. 3131–3136.
[29] D. M. Raimondo, G. R. Marseglia, J. K. Scott, and R.D. Braatz, , *Closed-loop input design for guaranteed fault diagnosis using set-valued observers*, Automatica, 74 (2016), pp. 107–117.
[30] T. Raïssi, G. Videau, and A. Zolghadri, *Interval observer design for consistency checks of nonlinear continuous-time systems*, Automatica, 46 (2010), pp. 518–527.
[31] S.-A. Raka and C. Combastel, *Fault detection based on robust adaptive thresholds: A dynamic interval approach*, Annual Reviews in Control, 37 (2013), pp. 119–128.
[32] S. V. Raković and K. I. Kouramas, *Invariant approximations of the minimal robust positively invariant set via finite time Aumann integrals*, in Proc. IEEE Conf. Decision and Control, 2007, pp. 194–199.
[33] V. Reppa and A. Tzes, *Fault detection and diagnosis based on parameter set estimation*, IET Control Theory & Applications, 5 (2011), pp. 69–83.
[34] V. Reppa and A. Tzes, *Fault diagnosis based on set membership identification using output-error models*, Int. J. Adaptive Control and Signal Processing, (2015).
[35] J. K. Scott, R. Findeisen, R. D. Braatz, and D. M. Raimondo, *Input design for guaranteed fault diagnosis using zonotopes*, Automatica, 50 (2014), pp. 1580–1589.
[36] E. I. Senin and V. A. Soldunov, *Attainable estimates of sets of feasible states of linear systems under limited disturbances*, Autom. Remote Control, 50 (1990), pp. 1513–1521.
[37] M. M. Seron, J. A. De Doná, and S. Olaru, *Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions*, IEEE Trans. Autom. Control, 57 (2012), pp. 1657–1669.
[38] M. M. Seron, X. W. Zhuo, J. A. De Doná, and J. Martinez, *Multisensor switching control strategy with fault tolerance guarantees*, Automatica, 44 (2008), pp. 88–97.
[39] M. M. Seron, X. W. Zhuo, J. A. De Doná, and J. Richter, *Fault tolerant control using virtual actuators and set-separation detection principles*, Int. J. Robust and Nonlinear Control, 22 (2012), pp. 709–742.
[40] K. Severson, C. Paphonwit, and R. D. Braatz, *Perspectives on process monitoring of industrial systems*, in Proc. 9th IFAC SAFEPROCESS, Paris, France, 2015.
[41] F. Stoican and S. Olaru, *Set-theoretic Fault-tolerant Control in Multisensor Systems*, John Wiley & Sons, 2013.
[42] F. Stoican, S. Olaru, and G. Bitsoris, *Controlled invariance-based fault detection for multisensory control systems*, IET Control Theory & Applications, 7 (2013), pp. 606–611.
[43] F. Stoican, S. Olaru, M. M. Seron, and J. A. De Doná, *Reference governor design for tracking problems with fault detection guarantees*, J. Process Control, 22 (2012), pp. 829–836.
[44] J. Stoustrup, and H. Niemann,, *Active fault diagnosis by controller modification*, Int. J. Systems Science, 41 (2010), pp. 925–936.
[45] M. Tadeusiewicz, S. Hałgas, and M. Korzybski, *Multiple catastrophic fault diagnosis of analog circuits considering the component tolerances*, Int. J. Circuit Theory and Applications, 40 (2012), pp. 1041–1052.
[46] A. Tanwani, A. D. Domínguez-García, and D. Liberzon, *An inversion-based approach to fault detection and isolation in switching electrical networks*, IEEE Trans. Control Syst. Technol., 19 (2011), pp. 1059–1074.
[47] A. Varga, *Solving Fault Diagnosis Problems: Linear Synthesis Techniques*, vol. 84, Springer, 2017.
[48] L. Vu and D. Liberzon, *Invertibility of switched linear systems*, Automatica, 44 (2008), pp. 949–958.
[49] F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru, *Actuator-fault detection and isolation based on set-theoretic approaches*, J. Process Control, (2014).
[50] Y. Zhang, and X. Li, *Detection and diagnosis of sensor and actuator failures using IMM estimator*, IEEE Trans. Aerosp. Electron. Syst., 34 (1998), pp. 1293-1313.