2018 European Control Conference (ECC)
June 12-15, 2018. Limassol, Cyprus

Fault Isolation for Large Scale Discrete-Time Systems Based on Implicit Set Representation

Franco Blanchini[1], Daniele Casagrande[2], Giulia Giordano[3], Stefano Miani[2], Sorin Olaru[4] and Vasso Reppa[5]

Abstract— **To detect faults in a system we can adopt an observer, designed for the healthy system, and monitor the discrepancy between actual and expected behaviour of the *residual* (difference between the system output and its estimate). To isolate faults, we can compute the invariant sets associated with each fault, and their projection in the residual space (*limit set*): faults can be isolated if the associated limit sets are separated when a (constant) test input is applied. However, the explicit computation of limit sets can be hard even for low-dimensional systems. As a main contribution, we show that, by adopting an implicit representation of limit sets, very efficient procedures can be used to solve the problem, based on convex quadratic programming or linear programming. Simulations show that the approach is effective in solving even large dimensional problems, which makes it suitable for large-scale networked systems.**

I. Introduction

The real-time operation of control processes relies on the monitoring of the global functioning as well as the health of the sub-components [14]. The diagnosis is implemented by means of a fault detection and isolation (FDI) mechanism that can be further related to re-design or reconfiguration of the feedback control system [6]. Consequently, the FDI block is a fundamental component, whose design principles commonly exploit either analytical redundancy of the available data from the process or the abstraction leading to model-based tests [36], [3]. The FDI decision making process is challenging due to the presence of modeling simplifications and omissions, system disturbances, and measurement noise, which can mask the effects of malfunctioning [9]. FDI mechanisms can have either a *passive* or an *active* role in the system supervision.

A *passive* FDI mechanism monitors just the input and output data of the system: the decision is then based on the processed information. Several studies developed passive FDI methods in the presence of bounded uncertainties, which generate on-line sets in the parameter [13], [26], [27] or residual space [23], [7], [24], [11]. A fault is detected when either the parameter set is empty, or the inclusion of the residual within the corresponding set does not hold. Alternatively, the real-time trajectories of the system states can be analysed in terms of inclusion within sets or tubes [25], [5], which are characterised off-line explicitly or via parameterisations. Consequently, fault detection can be performed on-line via an inclusion test [32]. Other passive set-theoretic FDI methods aim at the off-line separation of healthy and faulty sets [31], [30] by exploiting the existence of *limit sets*, where the residuals are guaranteed to converge under healthy conditions and various fault scenarios.

In the absence of security or safety reasons that forbid the access to the system or its excitation, the FDI mechanism can become *active* and step in the (closed-loop) system operation. This gives more design freedom and helps diagnose faults that may be affected by the closed-loop system operation [2]. In active fault diagnosis, the FDI mechanism can either steer the reconfiguration of the control scheme so as to increase fault detectability and isolability [16], [35], [20], [33], or stimulate the system, to make the effects of faults detectable [17], [8], [34], [28], [1], [21], [22], by generating an auxiliary input signal (which can be designed based on the open-loop [17], [8], [28] or the closed-loop [1], [34], [21], [22] operation of the system).

This paper follows the latter approach and focuses on the design of an *active model-based* FDI mechanism that guarantees set separation via an auxiliary input signal, chosen off-line based on an optimisation mechanism. Given a set of pre-defined fault scenarios, the scalability advantages of the procedure make it suitable for large-scale dynamical systems (such as networked systems with a large number of components). Results for continuous-time FDI design [4] have recently shown that the fault isolation problem can be solved for continuous-time linear systems based on the Hahn-Banach theorem and a duality approach; the present results, conversely, specifically deal with discrete-time systems.

We consider linear dynamics and develop an active observer-based FDI technique to reconstruct the state information affected by norm-bounded disturbances. We take into account one healthy and a finite number of faulty system configurations, and seek suitable test signals that guarantee separation of the limit sets via hyperplanes in the residual space [17], [19], [21]. Since the explicit computation of limit sets is a hard task, we propose an approach that avoids it and exploits an implicit representation [12], [29]. Given a constant test signal u chosen to ensure set separation, we show that the distance between two limit sets can be obtained

[1] F. Blanchini is with Dipartimento di Matematica, Informatica e Fisica, Università degli Studi di Udine, 33100 Udine, Italy blanchini@uniud.it

[2] D. Casagrande and S. Miano are with the Dipartimento Politecnico di Ingegneria e Architettura, Università degli Studi di Udine, 33100 Udine, Italy {daniele.casagrande,miani.stefano}@uniud.it

[3] G. Giordano is with the Delft Center for Systems and Control, Delft University of Technology, 2628 CD Delft, The Netherlands. g.giordano@tudelft.nl

[4] S. Olaru is with the 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

[5] V. Reppa is with the KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, 1678, Cyprus. reppavasso@gmail.com

978-3-9524-2699-9 ©2018 EUCA

without explicitly computing the sets, via convex quadratic programming in the case of the Euclidean norm and linear programming in the case of ∞-norm. The problem domain is the unit ball of the residual space, which is typically of low (output-space) dimension. When the distance between two limit sets is positive (separation condition), we provide the expression of a separating hyperplane. If the test signal u is bounded in a polytope, the values of u that maximise the distance, and offer the best discrimination, are achieved on the vertices, since the distance is a convex function of u. The approach allows us to efficiently handle *large scale systems* and networked systems with many components.

In contrast to [17], isolation in finite time can be achieved based on a positive answer for the asymptotic separation conditions. When compared to [19], the on-line monitoring reduces to a simple positioning with respect to separating hyperplanes, having lower computational complexity. Also, the forward set propagation and projection in [21] are avoided.

From a broader point of view, the present work can be interpreted as an active-mode detection technique for discrete-time linear systems affected by bounded disturbances [37].

The paper is organised in two main parts, one devoted to the problem statement and the theoretical results on active fault isolation, and one that illustrates the results by means of a numerical example with complete state and observer space dimension 20, for which no explicit computation is practically possible: our method, based on an implicit representation, assures fault isolation. A series of conclusions and remarks complete this study.

II. Active fault isolation for discrete-time systems based on implicit set representation

Consider the family of linear time invariant discrete-time systems

$$\begin{aligned} x(k+1) &= A_h x(k) + B_h u(k) + E_h d(k) && (1)\\ y(k) &= C_h x(k) + D_h w(k) && (2)\end{aligned}$$

where $x(k) \in \mathbb{R}^n$ is the state, $u(k) \in \mathbb{R}^m$ is a controlled input, $y(k) \in \mathbb{R}^p$ is the measured output, while $d(k) \in \mathbb{R}^q$ and $w(k) \in \mathbb{R}^p$ represent disturbance and noise, respectively. A_h, B_h, C_h, D_h and E_h are matrices of appropriate dimensions. For the sake of simplicity, the state dimension is considered as constant for all h. The signals $d(k) \in \mathbb{R}^q$ $w(k) \in \mathbb{R}^p$ are unknown and subject to the bounds

$$\|d(k)\|_\infty \leq 1,$$

$$\|w(k)\|_\infty \leq 1.$$

Any weight concerning the components of d and w is absorbed in the matrix E_h and in the square, possibly diagonal matrix D_h. The index h is associated with the configuration in which the system is actually 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. We will assume that $h = 0$ corresponds to the healthy condition $[A_0, B_0, C_0, D_0, E_0] \doteq [A, B, C, D, E]$, while any other $h \geq 1$ corresponds to a faulty condition. To detect a fault and to isolate it (namely, to establish the actual active configuration h of the system), we can adopt an observer:

$$\begin{aligned} \hat{x}(k+1) &= (A+LC)\hat{x}(k) + Bu(k) - Ly(k), && (3)\\ \hat{y}(k) &= C\hat{x}(k). && (4)\end{aligned}$$

Under observability assumptions, in healthy conditions and in the absence of disturbance and noise, with an appropriate choice of the gain L, the residual variable $r(k) = y(k) - \hat{y}(k)$ converges to zero. Conversely, in faulty conditions and in the presence of disturbance and noise, this convergence is not ensured and r can be used as a fault detection indicator. The overall system dynamics obey to

$$\begin{aligned} \begin{bmatrix} x(k+1) \\ \hat{x}(k+1) \end{bmatrix} &= \begin{bmatrix} A_h & 0 \\ -LC_h & (A+LC) \end{bmatrix} \begin{bmatrix} x(k) \\ \hat{x}(k) \end{bmatrix} \\ &+ \begin{bmatrix} B_h \\ B \end{bmatrix} u(k) + \begin{bmatrix} E_h & 0 \\ 0 & -LD_h \end{bmatrix} \begin{bmatrix} d(k) \\ w(k) \end{bmatrix}, \qquad (5)\end{aligned}$$

with residual output equation

$$r(k) = \begin{bmatrix} C_h & -C \end{bmatrix} \begin{bmatrix} x(k) \\ \hat{x}(k) \end{bmatrix} + \begin{bmatrix} 0 & D_h \end{bmatrix} \begin{bmatrix} d(k) \\ w(k) \end{bmatrix}. \qquad (6)$$

We will adopt the new state space representation

$$\begin{aligned} z(k+1) &= F_h z(k) + G_h u(k) + P_h v(k), && (7)\\ r(k) &= M_h z(k) + Q_h v(k), && (8)\end{aligned}$$

where $z(k) = \begin{bmatrix} x(k)^\top & \hat{x}(k)^\top \end{bmatrix}^\top$, $v(k) = \begin{bmatrix} d(k)^\top & w(k)^\top \end{bmatrix}^\top$ and the matrices F_h, G_h, P_h, M_h and Q_h are those appearing in (5) and (6). Note that $v(k) \in \mathbb{R}^s$, $s = q + p$, is in the unit ball of the ∞-norm:

$$v(k) \in \mathcal{B} \doteq \{v \in \mathbb{R}^s : \ \|v\|_\infty \leq 1\}.$$

We make the following assumptions.

Assumption 1: Matrices A_h are Schur for all $h \in \mathcal{H}$. Matrix L is given[1] and such that $(A + LC)$ is Schur.

Without any further assumption on v, it is in general impossible to detect any fault unless we provide more hypotheses on the input. We assume thus that a test signal u of bounded magnitude can be adopted.

Assumption 2: The test signal u is constant and $u \in \mathcal{U}$, where $\mathcal{U}$ is a polytope.

In the absence of v in (7) and (8), and in view of asymptotic stability, the residual converges asymptotically to the point

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

Note that $r_\infty(0) = 0$. Under these assumptions, distinguishing two faults, h and l, in finite time is possible if we know a separating hyperplane between $r_\infty(h)$ and $r_\infty(l)$. But even if $r_\infty(h)$ and $r_\infty(l)$ are separable, the noise v may prevent the system trajectories from ultimately crossing the barrier

[1] L may be designed *e.g.* to optimise nominal (healthy) working conditions.

that discriminates the configurations h and l. A necessary and sufficient condition for ultimately crossing this barrier is that the limit sets for h and l are on opposite sides of the plane [18].

To distinguish two faults, we need to find an input u assuring the existence of proper separating hyperplanes between the limit sets. Denoting by $\mathcal{Z}_h(0)$ the minimal robustly invariant set for the system (7) with $u = 0$,

$$z(k+1) = F_h z(k) + P_h v(k), \tag{9}$$

the limit set for the residual r is

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

where $\oplus$ is the Minkowski sum for sets. Therefore a crucial condition for the existence of u that discriminates between configurations h and l in finite time T [17] is $\mathcal{R}_h(u) \bigcap \mathcal{R}_l(u) = \emptyset$, *i.e.*, the distance between the two sets is positive:

$$\delta_{hl}(u) = \text{dist}\left(\mathcal{R}_h(u), \mathcal{R}_l(u)\right) > 0, \tag{10}$$

with

$$\text{dist}\left(\mathcal{Q}, \mathcal{R}\right) \doteq \inf_{q \in \mathcal{Q},\, r \in \mathcal{R}} \quad \|r - q\|, \tag{11}$$

where $\|r - q\|$ can denote *any relevant norm* (typically the Euclidean norm or the ∞-norm).

Definition 1: 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 $\delta_{hl}(u_{hl}) > 0$.

Remark 1: Considering a separating hyperplane might be conservative for simple (*e.g.*, first or second order) systems, where faults can be isolated simply by examining the transient even when the distance conditions (10) are not met. However, the general hyperplane method can be efficiently used for high dimensional systems, as we will see later.

Some preliminary results are the following.

Proposition 1: [15] Function $\delta_{hl}(u)$ is convex; hence, its maximum is reached on the set of vertices of $\mathcal{U}$, vert($\mathcal{U}$).

It follows that configurations h and l are distinguishable if and only if $\delta_{hl}(u) > 0$ for some $u \in$ vert($\mathcal{U}$). Therefore, checking if configurations l and h are distinguishable requires solving a finite number of convex optimisation problems.

In principle, to compute the limit set for the residual, we would need to compute the minimal robustly invariant set $\mathcal{Z}_h(0)$ and to evaluate its projection $M_h\mathcal{Z}_h(0)$. In [5] it is shown how to compute an external invariant approximation of $\mathcal{Z}_h(0)$. In our case, we need a suitable external approximation of $M_h\mathcal{Z}_h(0)$ as a projection of an external approximation of $\mathcal{Z}_h(0)$. Precisely, we wish to approximate the set

$$\mathcal{R}(0) = \left\{ r \in \mathbb{R}^p : r = \sum_{k=0}^{\infty} \quad MF^k P v_k,\, v_k \in \mathcal{B} \right\} \tag{12}$$

by the set

$$\mathcal{R}^T(0) \doteq \left\{ r \in \mathbb{R}^p : r = \sum_{k=0}^{T} \quad MF^k P v_k,\, v_k \in \mathcal{B} \right\}. \tag{13}$$

Indeed, the following approximation result holds.

Proposition 2: Define

$$\nu(M, F, P) \doteq \max_i \quad \sum_{k=0}^{\infty} \quad \sum_j \left| [MF^{k+T+1}P]_{ij} \right|,$$

where $[\cdot]_{ij}$ are the elements of matrix $\cdot$, and

$$\mu(T) = \min\{\mu > 0 : \quad \nu(M, F, P)\mathcal{B} \subset \mu\mathcal{R}^T(0)\}, \tag{14}$$

where $\mathcal{B}$ is the unit ball of the ∞-norm. Then

$$\mathcal{R}(0) \subseteq (1 + \mu(T))\mathcal{R}^T(0).$$

Proof: We have that

$$\mathcal{R}(0) \quad = \quad \mathcal{R}^T(0) \oplus \underbrace{\left\{ r = \sum_{k=0}^{\infty} \quad MF^{k+T+1}Pv'_k,\, v'_k \in \mathcal{B} \right\}}_{\doteq \mathcal{S}^T(0)}.$$

The maximum $\|\cdot\|_\infty$ norm of the elements of the set denoted by $\mathcal{S}^T$ is the ∞-to-∞ induced norm of the operator

$$[MF^{T+1}P \; MF^{T+2}P \; MF^{T+3}P \ldots],$$

which is given by [10]

$$\begin{aligned} \nu(M, F, P) \quad &\doteq \max\nolimits_{r \in \mathcal{S}^T} \quad \|r\|_\infty \\ &= \max\nolimits_i \quad \sum\nolimits_{k=0}^{\infty} \quad \sum\nolimits_j \left| [MF^{k+T+1}P]_{ij} \right|. \end{aligned}$$

Therefore $\mathcal{S}^T \subseteq \mu\mathcal{R}^T$ if the unit ball of the ∞-norm multiplied by $\nu(M, F, P)$ is a subset of $\mu\mathcal{R}^T$, exactly as required by condition (14). ■

Checking condition (14) requires the solution of some Linear Programming problems. For each vertex b of the unit ball of the infinity norm multiplied by $\nu(M, F, P)$, $\nu(M, F, P)b$, we need to minimise μ such that $\nu(M, F, P)b$ can be expressed by a finite sum of the form (13), with vectors v_k whose component absolute value is less or equal to 1.

The complexity of the *explicit representation* of the set $\mathcal{R}^T(0)$ can be too high anyway [5]. To compute the set, we have to generate the candidate vertices, which are $\sum_{k=0}^{T} \; MF^k P\hat{v}_k$, with $\hat{v}_k \in$ vert($\mathcal{B}$). Their number grows exponentially: there are $(\#\text{vert}(\mathcal{B}))^{T+1}$ vertices to be projected in the p-dimensional residual space. Yet, we can solve the problem efficiently by providing an implicit representation as follows.

Consider the lower bound

$$\delta^T_{hl}(u) = \text{dist}\left(\mathcal{R}^T_h(u), \mathcal{R}^T_l(u)\right) \leq \delta_{hl}(u),$$

where

$$\mathcal{R}^T_h(u) \doteq \{M_h[I - F_h]^{-1}G_h u\} \oplus (1 + \mu(T))\mathcal{R}^T_h(0) \oplus Q_h\mathcal{B}.$$

This lower bound can be computed as the solution of the minimisation problem:

$$\begin{aligned}\delta_{hl}^{T}(u) &= \min_{v'_Q,\, v''_Q,\, v'_k,\, v''_k} \|r_h - r_l\| && (15)\\ &\text{s.t.} && \\ r_h &= M_h[I-F_h]^{-1}G_h u + && \\ &+ \quad (1+\mu(T))\sum_{k=0}^{T} M_h F_h^k P_h v'_k + Q_h v'_Q && (16)\\ r_l &= M_l[I-F_l]^{-1}G_l u + && \\ &+ \quad (1+\mu(T))\sum_{k=0}^{T} M_l F_l^k P_l v''_k + Q_l v''_Q && (17)\\ & v'_Q,\, v''_Q,\, v'_k,\, v''_k \in \mathcal{B}. && (18)\end{aligned}$$

Computationally, this is a substantial improvement. Consider, e.g., $n = 10$, $m = 2$, $p = 3$, $q = 1$ (hence $s = 4$) and $T = 10$. There are $(\#\text{vert}(\mathcal{B}))^{T+1} = [2^s]^{T+1} = 2^{44}$, more than 16×10^{12}, candidate vertices. Most of these would be redundant, but the elimination procedure would be intractable and practically unfeasible. Then we should solve a minimum-distance problem between two sets of such a complexity in dimension $p = 3$. Yet, in the Euclidean norm case, the quadratic minimisation problem has $2[(T+1)*s+s] = 96$ variables (each upper and lower bounded, which requires $96 * 2$ inequality constraints) and $p * 2 = 6$ equality constraints, and is solvable via standard software.

If in (15) we take the infinity norm (possibly weighted), we obtain a Linear Programming (LP) problem

$$\min\ \delta : \quad -\delta\bar{1} \leq r_h - r_l \leq \delta\bar{1}, \quad \text{subject to } (16)\,(17)\,(18),$$

where $\bar{1} = [1\ 1\ 1 \ldots 1]^\top$ and the inequalities have to be intended component-wise. LP problems with thousands of variables are standard in optimisation.

An important role in fault isolation is played by the distance matrix, defined as follows. For any input u we have seen how to approximate $\delta_{hl}(u)$, the distance between limit sets. Since the distance is a convex function, it reaches its maximum on the vertices of $\mathcal{U}$. Then, for any vertex u_j of $\mathcal{U}$, one can consider the distance matrices

$$[\Delta(u_j)]_{hl} = \delta_{hl}(u_j),$$

which are nonnegative and symmetric. Distance matrices suggest which signal u is the most appropriate for distinguishing between pairs of configurations.

Hence, to decide *off-line* if two configurations h and l are distinguishable, separation between two sets in the residual space can be checked via the following procedure.
1) Compute $\nu(M_h, F_h, P_h)$ and $\nu(M_l, F_l, P_l)$ (compute the sums of series and take the maximum).
2) Compute the value of μ for a given T, which can be fixed depending on the complexity of $\mathcal{R}_h^T(0)$ and $\mathcal{R}_l^T(0)$.
3) For each vertex u of the set $\mathcal{U}$, solve the problem (15)–(18) and check whether the resulting $\delta_{hl}^T(u)$ is positive.

In order to isolate *on-line* the failures, once we have established that the distances among limit sets associated with the test signal u are positive, we need to find *separation hyperplanes* among these sets. For instance, in Fig. 1, if u is applied, we can distinguish between failures 2 and 1 since the residual, in finite time, will be confined to the left or to the right of the hyperplane Π_{12}. If we consider the Euclidean norm, a separation hyperplane between a pair of sets $\mathcal{R}_h^T(0)$ and $\mathcal{R}_l^T(0)$ can be taken as

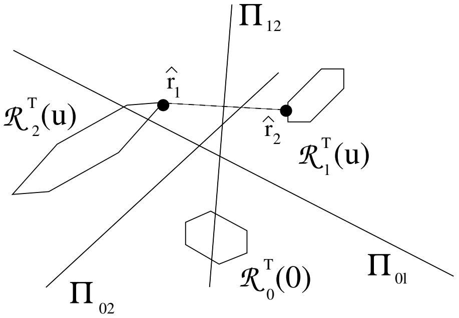


Fig. 1: Separation hyperplanes between pairs of sets.

$$\Pi_{hl} = \left\{ r : \quad (\hat{r}_h - \hat{r}_l)^\top r = \frac{(\hat{r}_h - \hat{r}_l)^\top(\hat{r}_h + \hat{r}_l)}{2} \right\},$$

where $\hat{r}_h \in \mathcal{R}_h^T(0)$ and $\hat{r}_l \in \mathcal{R}_l^T(0)$ are the two points at minimum Euclidean distance from Π_{hl}. Again, we do not need the explicit representation of the two sets: $\hat{r}_h$ and $\hat{r}_l$ are achieved for free from the quadratic optimisation problem. If the distance among sets is based on a different norm, the expression is different, but still a separation hyperplane can be determined for any pair of convex sets having positive distance. Note that a single hyperplane can separate several pairs of sets: this can be useful for *detecting* a fault.

Hence, to distinguish between two configurations h and l, we just need to compute the discriminant function

$$\text{discr}(h,l) \doteq \text{sign}\left[(\hat{r}_h - \hat{r}_l)^\top r - \frac{(\hat{r}_h - \hat{r}_l)^\top(\hat{r}_h + \hat{r}_l)}{2} \right],$$

which is positive for configuration h and negative for configuration l. Since we have $N + 1$ possible operating modes (including the healthy one), this requires checking at most $(N+1)N/2$ linear functions. *Only discriminant functions are needed for the on-line decision making*, since the sets $\mathcal{R}_h^T(0)$ are used exclusively off-line, for design purposes.

Remark 2: After switching from configuration l to configuration h, given a constant input $u = \bar{u}$ and the distance $\delta_{hl}(\bar{u})/2$ of the separating hyperplane from the set $\mathcal{R}_h(\bar{u})$, the time necessary for the residual trajectory to ultimately cross the separating hyperplane between the two sets can be estimated along the lines suggested in [30, Appendix A]. The finite-time detection will be effective provided that no supplementary configuration switch happens in this time interval (*i.e.*, under the assumption of persistence of fault).

III. Example

Consider the 5-degree-of-freedom oscillating system depicted in Fig. 2, with a persistent disturbance affecting mass 3. Two control forces are applied to masses 2 and 5, while the outputs are the positions of masses 1 and 4. We assume

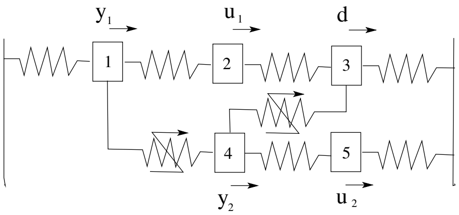


Fig. 2: The oscillating system: the springs connecting masses 1-4 and 3-4 may be broken (meaning that their elastic constant becomes 0).

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

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

where $q \in \mathbb{R}^5$ (hence, the system state has size 10), $y, w \in \mathbb{R}^2$, $\|w\|_\infty \leq 1$, $|d(t)| \leq 1$, the mass diagonal matrix is $M = I$, the damping matrix is $D = 0.3I$ and the stiffness matrix is

$$
K_h = \begin{bmatrix} 2+\alpha & -1 & 0 & -\alpha & 0 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 2+\beta & -\beta & 0 \\ -\alpha & 0 & -\beta & 1+\alpha+\beta & -1 \\ 0 & 0 & 0 & -1 & 2 \end{bmatrix}.
$$

The test input u and the disturbance d affect the system through matrices B_q and E_q, respectively.

The possible configurations are

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

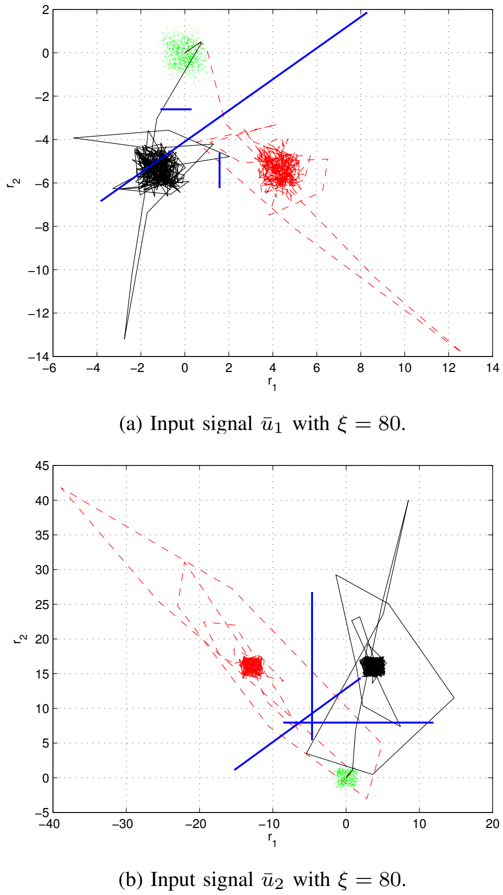
We considered the sampling time $\tau = 1$ and computed the optimal filter whose gains are reported in Table I[2]. The overall state and observer space dimension is $n = 20$. Computing the reachable and limit set is just hopeless.

We considered a test signal u subject to $\|u\|_\infty \leq \xi$, where $\xi > 0$ is an amplitude parameter. According to Proposition 1, the "best" discrimination value is found on one of the four vertices of this set. By symmetry we can check two vertices:

$$
\bar{u}_1 = [\ \xi \quad \xi\ ]^\top, \qquad \bar{u}_2 = [\ \xi \quad -\xi\ ]^\top.
$$

We chose a time horizon $T = 30$ and, by evaluating the series, we computed the values of $\mu(30)$ corresponding to the above values of h: $\mu(30)|_{h=0} = 0.5822$, $\mu(30)|_{h=1} = 0.6890$ and $\mu(30)|_{h=2} = 0.4915$. In Table II we reported the distances between pairs of sets as functions of the intensity ξ of the signal for both vertices $\bar{u}_1$ and $\bar{u}_2$. It turns out that $\bar{u}_2$ has much better discriminating properties than $\bar{u}_1$, since it assures greater distances.

We show the transient generated with a random signal v assuming values at the extrema $\{-1, 1\}$, starting from the healthy configuration ($h = 0$) in presence of a constant input of magnitude $\xi = 80$ corresponding to $\bar{u}_1$ in Fig. 3 (a) and to $\bar{u}_2$ in Fig. 3 (b). We have also represented the separation lines by segments whose length is proportional to the distance between the sets. According to Table II, there is only one separation line for $\bar{u}_1$, which discriminates 0 and 1. It is worth pointing out that the "simulated" limit sets seem to be quite far from the separation lines. To solve the optimisation problem that provides δ_{hl} with the MATLAB® function `quadprog`, the required computational time amounts to tens of milliseconds (using a 2.3 GHz Intel Core i7 processor).



(a) Input signal $\bar{u}_1$ with $\xi = 80$.

(b) Input signal $\bar{u}_2$ with $\xi = 80$.

Fig. 3: The simulations and the separation lines (blue); the evolution of system configuration $h = 0$ is shown with a green dotted line, $h = 1$ with a red dashed line, $h = 2$ with a black line.

IV. Concluding Remarks and Discussion

We have proposed a numerically efficient approach to fault isolation based on limit set separation. The limit sets for the residuals under faults are implicitly handled, by formulating a linear-quadratic constrained problem that can be easily solved, even for large scale systems.

Separation between configurations h and l_1 might be obtained with a constant signal different from the one needed to separate configurations h and l_2. To distinguish multiple fault pairs, we can seek a signal that concurrently separates all the limit sets, or we can first inject a signal that separates the first pair, then switch to a different signal. As a further extension, we could consider the discrete-time counterpart of the periodic excitation signals discussed in [4].

[2] The code for the example is available online at the URL http://users.dimi.uniud.it/~franco.blanchini/fault.zip.

$$L = \begin{bmatrix} -0.0393 & -0.0436 & -0.0455 & -0.0467 & -0.0424 & 0.1232 & 0.0602 & -0.0528 & -0.0134 & 0.0495 \\ -0.0834 & -0.0834 & -0.0217 & -0.0565 & -0.0565 & -0.0093 & 0.0589 & 0.0288 & 0.0674 & -0.0008 \end{bmatrix}^\top$$

TABLE I: The observer gain for the discrete-time example.

ξ	20	40	60	80	100	120	140
$\delta_{01}(\bar{u}_1)$	0	0	0.1581	1.8658	3.5734	5.2811	6.9888
$\delta_{02}(\bar{u}_1)$	0	0	0	0.7094	2.0447	3.3799	4.7152
$\delta_{12}(\bar{u}_1)$	0	0	0	0.8110	2.1920	3.5730	4.9541
$\delta_{01}(\bar{u}_2)$	0.1581	5.2811	10.4065	15.5354	20.6653	25.7957	30.9262
$\delta_{02}(\bar{u}_2)$	0	3.3799	7.3857	11.3915	15.4210	19.4814	23.5590
$\delta_{12}(\bar{u}_2)$	0	3.5730	7.7161	11.8592	16.0023	20.1454	24.2885

TABLE II: The distances among sets as a function of ξ and of the vertex $\bar{u}_k$.

Our approach allows us to decide off-line which are the best signals to adopt, 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.* [18], [34], [28], providing *a priori* separation guarantees.

References

[1] A. E. Ashari, R. Nikoukhah, and S. L. Campbell, "Active Robust Fault Detection in Closed-Loop Systems: Quadratic Optimization Approach", *IEEE Trans. Autom. Control*, 51, pp. 2532–2544, 2012.

[2] A. E. Ashari, R. Nikoukhah, and S. L. Campbell, "Effects of feedback on active fault detection", *Automatica*, 48(5), pp. 866–872, 2012.

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

[4] F. Blanchini, D. Casagrande, G. Giordano, S. Miani, S. Olaru, V. Reppa, "Active fault isolation: a duality-based approach via convex programming", *SIAM J. Control Optim.*, 55(3), pp. 1619-1640, 2017.

[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. Fernández-Cantí, "Set-membership parity space approach for fault detection in linear uncertain dynamic systems", *Int. J. Adapt. Control Signal Process.*, 2014.

[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] M. A. Dahleh and I. D. Diaz-Bobillo, *Control of Uncertain Systems: A Linear Programming Approach*, Englewood Cliffs, New Jersey, USA: Prentice-Hall, 1995

[11] D. Efimov, T. Raïssi, and A. Zolghadri, "Set adaptive observers for linear parameter-varying systems: Application to fault detection", *J. Dynamic Systems, Measurement, and Control*, 136, p. 021006, 2014.

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

[13] A. Ingimundarson, J. M. Bravo, V. Puig, T. Alamo, and P. Guerra, "Robust fault detection using zonotope-based set-membership consistency test", *Int. J. Adapt. Control Signal Process.*, 23, pp. 311–330, 2009.

[14] R. Isermann, *Fault-diagnosis systems*, Springer, 2006.

[15] 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*, 2013, pp. 1940–1945.

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

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

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

[19] 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.

[20] I. Punčochář, J. Širokỳ, and M. Šimandl, "Constrained active fault detection and control", *IEEE Trans. Autom. Control*, 60, pp. 253–258, 2015.

[21] D. M. Raimondo, R. D. Braatz, and J. K. Scott, "Active fault diagnosis using moving horizon input design", in *Proc. European Control Conference*, 2013, pp. 3131–3136.

[22] 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, pp. 107–117, 2016.

[23] T. Raïssi, G. Videau, and A. Zolghadri, "Interval observer design for consistency checks of nonlinear continuous-time systems", *Automatica*, 46, pp. 518–527, 2010.

[24] S.-A. Raka and C. Combastel, "Fault detection based on robust adaptive thresholds: A dynamic interval approach", *Annual Reviews in Control*, 37, pp. 119–128, 2013.

[25] 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. Dec. Control*, 2007, pp. 194–199.

[26] V. Reppa and A. Tzes, "Fault detection and diagnosis based on parameter set estimation", *IET Control Theory & Applications*, 5, pp. 69–83, 2011.

[27] V. Reppa and A. Tzes, "Fault diagnosis based on set membership identification using output-error models", *Int. J. Adapt. Control Signal Process.*, 30, pp. 224-255, 2016.

[28] J. K. Scott, R. Findeisen, R. D. Braatz, and D. M. Raimondo, "Input design for guaranteed fault diagnosis using zonotopes", *Automatica*, 50, pp. 1580–1589, 2014.

[29] E. I. Senin and V. A. Soldunov, "Attainable estimates of sets of feasible states of linear systems under limited disturbances", *Autom. Remote Control*, 50, pp. 1513–1521, 1990.

[30] 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, pp. 1657–1669, 2012.

[31] M. M. Seron, X. W. Zhuo, J. A. De Doná, and J. Martinez, "Multisensor switching control strategy with fault tolerance guarantees", *Automatica*, 44, pp. 88–97, 2008.

[32] F. Stoican and S. Olaru, *Set-theoretic Fault-tolerant Control in Multisensor Systems*, John Wiley & Sons, 2013.

[33] F. Stoican, S. Olaru, and G. Bitsoris, "Controlled invariance-based fault detection for multisensory control systems", *IET Control Theory & Applications*, 7, pp. 606–611, 2013.

[34] 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, pp. 829–836, 2012.

[35] J. Stoustrup, and H. Niemann, "Active fault diagnosis by controller modification", *Int. J. Systems Science*, 41, pp. 925–936, 2010.

[36] A. Varga, *Solving Fault Diagnosis Problems: Linear Synthesis Techniques*, Springer, 2017.

[37] L. Vu and D. Liberzon, "Invertibility of switched linear systems", *Automatica*, 44, pp. 949–958, 2008.