Fault Isolation for Large Scale Discrete-Time Systems Based on Implicit Set Representation
Franco Blanchini, Daniele Casagrande, Giulia Giordano, Stefano Miani, Sorin Olaru, Vasso Reppa

To cite this version:
Franco Blanchini, Daniele Casagrande, Giulia Giordano, Stefano Miani, Sorin Olaru, et al.. Fault Isolation for Large Scale Discrete-Time Systems Based on Implicit Set Representation. 16th European Control Conference (ECC 2018), Jun 2018, Limassol, Cyprus. pp.1-6. hal-01720264

HAL Id: hal-01720264
https://hal-centralesupelec.archives-ouvertes.fr/hal-01720264
Submitted on 1 Mar 2018

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

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Fault Isolation for Large Scale Discrete-Time Systems
Based on Implicit Set Representation

Franco Blanchini¹, Daniele Casagrande², Giulia Giordano³, Stefano Miano², Sorin Olaru⁴ and Vasso Reppa⁵

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 signal 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.
without explicitly computing the sets, via convex quadratic programming in the case of the Euclidean norm and linear programming in the case of \( \infty \)-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

\[
\begin{align*}
    x(k+1) &= A_h x(k) + B_h u(k) + E_h d(k) \\
    y(k) &= C_h x(k) + D_h w(k)
\end{align*}
\]

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 \( d(k) \in \mathbb{R}^q \) and \( w(k) \in \mathbb{R}^p \) are unknown and subject to the bounds

\[
\|d(k)\|_\infty \leq 1, \quad \|w(k)\|_\infty \leq 1.
\]

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:

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

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 \( [A_0, B_0, C_0, D_0, E_0] \cong [A, B, C, D, E] \), while any other \( h \geq 1 \) corresponds to a faulty condition. To detect a fault and isolate it, we will establish the actual active configuration \( h \) of the system, and we adopt the observer:

\[
\begin{align*}
    \hat{x}(k+1) &= (A + LC)\hat{x}(k) + Bu(k) - Ly(k), \quad (3) \\
    \hat{y}(k) &= C\hat{x}(k).
\end{align*}
\]

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

\[
\begin{align*}
    \begin{bmatrix}
        x(k+1) \\
        \hat{x}(k+1)
    \end{bmatrix} &= \begin{bmatrix}
        A_h & 0 \\
        -LC_h & (A + LC)
    \end{bmatrix} \begin{bmatrix}
        x(k) \\
        \hat{x}(k)
    \end{bmatrix} \\
    &\quad + \begin{bmatrix}
        B_h \\
        B
    \end{bmatrix} u(k) + \begin{bmatrix}
        E_h & 0 \\
        0 & -LD_h
    \end{bmatrix} \begin{bmatrix}
        d(k) \\
        w(k)
    \end{bmatrix},
\end{align*}
\]

with residual output equation

\[
\begin{align*}
    r(k) &= \begin{bmatrix}
        C_h & -C
    \end{bmatrix} \begin{bmatrix}
        x(k) \\
        \hat{x}(k)
    \end{bmatrix} + \begin{bmatrix}
        0 & D_h
    \end{bmatrix} \begin{bmatrix}
        d(k) \\
        w(k)
    \end{bmatrix}.
\end{align*}
\]

We will adopt the new state space representation

\[
\begin{align*}
    z(k+1) &= F_h z(k) + G_h u(k) + P_h v(k), \quad (7) \\
    r(k) &= M_h z(k) + Q_h v(k), \quad (8)
\end{align*}
\]

where \( z(k) = [x(k)^T, \hat{x}(k)^T]^T \), \( v(k) = [d(k)^T, w(k)^T]^T \), 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 \( \infty \)-norm:

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

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

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

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

\(^1\) \text{\( l \) 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 \( u \) assuming 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 \( u = 0 \),

\[
z(k + 1) = F_h z(k) + P_h v(k),
\]

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 \( \mathcal{R}_h(u) \cap \mathcal{R}_l(u) = \emptyset \), i.e., the distance between the two sets is positive:

\[
\delta_{hl}(u) = \text{dist}(\mathcal{R}_h(u), \mathcal{R}_l(u)) > 0,
\]

with

\[
\text{dist}(Q, \mathcal{R}) = \inf_{q \in Q, r \in \mathcal{R}} \| r - q \|,
\]

where \( \| r - q \| \) can denote any relevant norm (typically the Euclidean norm or the \( \infty \)-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 \( \delta_{hl} \) is convex; hence, its maximum is reached on the set of vertices of \( \mathcal{U} \), \( \text{vert}(\mathcal{U}) \). It follows that configurations \( h \) and \( l \) are distinguishable if and only if \( \delta_{hl}(u) > 0 \) for some \( u \in \text{vert}(\mathcal{U}) \). 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

\[
\mathcal{R}(0) = \left\{ r \in \mathbb{R}^p : r = \sum_{k=0}^{\infty} M F_h^k P v_k, v_k \in \mathcal{B} \right\}.
\]

by the set

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

Indeed, the following approximation result holds.

Proposition 2: Define

\[
\nu(M, F, P) = \max_{i} \sum_{k=0}^{\infty} \sum_{j} ||M F_h^{k+T+1} P||_{ij},
\]

where \( [i,j] \) are the elements of the matrix \( \cdot \), and

\[
\mu(T) = \min \{ \mu > 0 : \nu(M, F, P) B \subseteq \mu \mathcal{R}^T(0) \}, \tag{14}
\]

where \( B \) is the unit ball of the \( \infty \)-norm. Then

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

Proof: We have that

\[
\mathcal{R}(0) = \mathcal{R}^T(0) \oplus \left\{ r = \sum_{k=0}^{\infty} M F_h^{k+T+1} P v_k, v_k \in \mathcal{B} \right\}_{\pm \mathcal{S}^T(0)}.
\]

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

\[
[M F_h^{T+1} P M F_h^{T+2} P M F_h^{T+3} P \ldots],
\]

which is given by [10]

\[
\nu(M, F, P) = \max_{r \in \mathcal{S}^T} \| r \|_\infty = \max_{i} \sum_{k=0}^{\infty} \sum_{j} ||M F_h^{k+T+1} P||_{ij}.
\]

Therefore \( \mathcal{S}^T \subseteq \mu \mathcal{R}^T \) if the unit ball of the \( \infty \)-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 \( \mu \) 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 \( \sum_{k=0}^{\infty} M F_h^k \tilde{v}_k \), with \( \tilde{v}_k \in \text{vert}(\mathcal{B}) \). 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

\[
\delta_{hl}(u) = \text{dist}(\mathcal{R}_h^T(u), \mathcal{R}_l^T(u)) \leq \delta_{hl}(u),
\]

where

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

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

\[
\delta_{hl}^T(u) = \min_{v_Q', v_L', v_R'} \| r_h - r_l \|
\]

\[
\text{s.t.}
\]

\[
r_h = M_h [I - F_h]^{-1} G_h u + (1 + \mu(T)) \sum_{k=0}^{T} M_h F_h^k P_h v_k' + Q_h v_Q'
\]

\[
r_l = M_l [I - F_l]^{-1} G_l u + (1 + \mu(T)) \sum_{k=0}^{T} M_l F_l^k P_l v_l' + Q_l v_Q'
\]

\[
v_Q', v_L', v_R' \in \mathcal{B}. \quad (16)
\]

\[
\delta_{hl}^T(u) = \min_{\bar{\delta} \in \mathbb{R}^+} \bar{\delta} \quad \text{subject to } (16) \quad (17) \quad (18),
\]

where \( \bar{\delta} = [1 \ 1 \ 1 \ldots 1]^T \) 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 converges 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 \( \mu \) 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 \( \Pi_{12} \). 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

\[
\Pi_{hl} = \left\{ r : (\hat{r}_h - \hat{r}_l)^T r = \frac{(\hat{r}_h - \hat{r}_l)^T (\hat{r}_h + \hat{r}_l)}{2} \right\},
\]

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 \( \Pi_{hl} \). 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

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

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...
that a complete failure of the springs connecting masses 1-4 and 3-4 can occur. The model of the system is
\[
M \ddot{y}(t) = -K_h \dot{y}(t) - D \dot{y}(t) + B_q u(t) + E_q d(t)
\]
\[
y(t) = [q_1(t) \ q_2(t)]^T + w(t)
\]
where \( q \in \mathbb{R}^3 \) (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
\[
K_h = \begin{bmatrix}
2 + \alpha & -1 & 0 & -\alpha & 0 \\
-1 & 2 - \alpha & -1 & 0 & 0 \\
0 & -1 & 2 + \beta & -\beta & 0 \\
-\alpha & 0 & -\beta & 1 + \alpha + \beta & -1 \\
0 & 0 & 0 & -1 & 2
\end{bmatrix}
\]
The test input \( u \) and the disturbance \( d \) affect the system through matrices \( B_q \) and \( E_q \), respectively.

The possible configurations are
\[
h = 0 : \{ \alpha = 1, \beta = 1 \}, \quad \text{healthy},
\]
\[
h = 1 : \{ \alpha = 0, \beta = 1 \}, \quad \text{faulty},
\]
\[
h = 2 : \{ \alpha = 1, \beta = 0 \}, \quad \text{faulty}.
\]

We considered the sampling time \( \tau = 1 \) and computed the optimal filter whose gains are reported in Table II. 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:
\[
\bar{u}_1 = [\xi \ \xi]^T, \quad \bar{u}_2 = [\xi \ -\xi]^T.
\]

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 \( \xi \) 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 \( \delta_{hl} \) with the MATLAB® function \texttt{quadprog}, the required computational time amounts to tens of milliseconds (using a 2.3 GHz Intel Core i7 processor).

**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].
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


