Automatica 50 (2014) 1580–1589

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Input design for guaranteed fault diagnosis using zonotopes[☆]

Joseph K. Scott[a,1], Rolf Findeisen[b], Richard D. Braatz[a], Davide M. Raimondo[c]

[a] Department of Chemical Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA

[b] Institute for Automation Engineering, Laboratory for Systems Theory and Automatic Control, Otto-von-Guericke University Magdeburg, Germany

[c] Identification and Control of Dynamic Systems Laboratory, University of Pavia, Italy

ARTICLE INFO

Article history:
Received 26 February 2013
Received in revised form
7 February 2014
Accepted 26 February 2014
Available online 24 April 2014

Keywords:
Fault diagnosis
Input design
Reachability analysis
Zonotopes

ABSTRACT

An input design method is presented for guaranteeing the diagnosability of faults from the outputs of a system. Faults are modeled by discrete switches between linear models with bounded disturbances and measurement errors. Zonotopes are used to efficiently characterize the set of inputs that are guaranteed to lead to outputs that are consistent with at most one fault scenario. Provided that this set is nonempty, an element is then chosen that is minimally harmful with respect to other control objectives. This approach leads to a nonconvex optimization problem, but is shown to be equivalent to a mixed-integer quadratic program that can be solved efficiently. Methods are given for reducing the complexity of this program, including an observer-based method that drastically reduces the number of binary variables when many sampling times are required for diagnosis.

1. Introduction

In many industries (chemical (Venkatasubramanian, Rengaswamy, Yin, & Kavuri, 2003), aerospace (Zolghadri, 2010), etc.), the trend toward increasing complexity and automation has made component malfunctions and other abnormal events (i.e., faults) increasingly frequent. At the same time, economic considerations have led to the use of inexpensive and unreliable components in many mass market applications. Accordingly, achieving safe and reliable operation for many systems now requires fast and accurate methods for detecting and diagnosing faults on the basis of process measurements. These tasks are rendered difficult by the confounding effects of disturbances, measurement uncertainty, and the compensatory actions of the control system.

Fault detection and diagnosis methods can be categorized as either passive or active. Passive approaches attempt to diagnose faults by comparing the available input–output data for the process to models or historical data (Chiang, Russell, & Braatz, 2001; Venkatasubramanian et al., 2003). Often, however, faults may not be detectable in the available measurements, or cannot be diagnosed without exciting the system. Accordingly, the active approach involves injecting a signal into the system to improve detectability of the fault (Blackmore, Rajamanoharan, & Williams, 2008; Campbell & Nikoukhah, 2004; Esna Ashari, Nikoukhah, & Campbell, 2012; Niemann, 2006; Nikoukhah, 1998; Simandl & Puncochar, 2009).

This article presents a set-based approach for active fault diagnosis. The process of interest, under nominal and various faulty conditions, is described by a set of linear discrete-time models subject to bounded disturbances and measurement errors. Faults are modeled by discrete switches between these models. The proposed framework permits multiple faults occurring either sequentially or simultaneously, although computational complexity ultimately limits the number of scenarios considered (see Section 2). Given a set of scenarios, the objective is to compute an input that is guaranteed to generate outputs consistent with at most one scenario, thereby providing a complete fault diagnosis. Such inputs are referred to as *separating inputs*. In addition to this diagnosis condition, the computed input is further required to be minimally harmful with respect to other control objectives.

This problem was first considered in Nikoukhah (1998). In the case of two models (one nominal and one faulty), the set of separating inputs was shown to be the complement of a projection of a high-dimensional polytope. Unfortunately, polytope projection is computationally intensive and numerically unstable in the required dimensions. The book (Campbell & Nikoukhah,

[☆] The material in this paper was partially presented at the 2013 American Control Conference (ACC 2013), June 17–19, 2013, Washington, DC, USA. This paper was recommended for publication in revised form by Associate Editor Michele Basseville under the direction of Editor Torsten Söderström. BP is acknowledged for financial support of this project.

E-mail addresses: jkscott@mit.edu (J.K. Scott), rolf.findeisen@ovgu.de (R. Findeisen), braatz@mit.edu (R.D. Braatz), davide.raimondo@unipv.it (D.M. Raimondo).

[1] Tel.: +1 8646560997; fax: +1 8646560784.

http://dx.doi.org/10.1016/j.automatica.2014.03.016
0005-1098/

2004) proposes an active input design method for the case where the disturbances and measurement errors are energy bounded rather than pointwise bounded. The input is chosen as the solution of a bilevel optimization problem in which the outer program searches for a minimum two-norm input and the inner program restricts the feasible set to separating inputs. This optimization problem is nonconvex and is solved in the two-model case by a specialized algorithm. Various extensions of this approach have been investigated, including methods for continuous-time and nonlinear systems (Andjelkovic, Sweetingham, & Campbell, 2008; Campbell & Nikoukhah, 2004), asymptotically optimal implementations (Nikoukhah & Campbell, 2006; Nikoukhah, Campbell, & Delebecque, 2000), and methods for systems under linear feedback control (Ashari, Nikoukhah, & Campbell, 2009, 2012; Esna Ashari et al., 2012). A more general optimization formulation has also been proposed that permits multiple fault models and arbitrary objectives and constraints (Campbell, Horton, & Nikoukhah, 2002; Campbell & Nikoukhah, 2004). However, the structure of the two-model formulation is lost and the method instead relies on general-purpose software to solve difficult optimal control problems constrained by two-point boundary-value problems.

This article treats the case where the disturbances and measurement errors are pointwise bounded rather than energy bounded, and uses zonotopes rather than polytopes or ellipsoids. After a formal problem statement and some preliminary developments in Sections 2 and 3, the set of separating inputs is characterized using efficient zonotope computations in Section 4, effectively eliminating the polytope projection problem in Nikoukhah (1998). This result is then used to pose a bilevel optimization problem for choosing an optimal separating input in Section 5, similar to the approach in Nikoukhah and Campbell (2006). The use of zonotopes here permits a reformulation as a mixed-integer quadratic program (MIQP) for which the number of integer variables can be controlled using zonotope order reduction techniques. The resulting optimization problem is simple to implement and practically solvable, while being flexible with respect to the choice of objective, the presence of state and control constraints, the possibility of multiple fault models, and the possibility of multiple faults occurring simultaneously or sequentially in the time interval of interest. Techniques for reducing the computational complexity of the approach are discussed in Section 6, and an approximate implementation of the approach using set-valued observers is proposed in Section 7 to reduce the complexity when many sampling times are required for diagnosis. Numerical examples are presented in Section 8, and Section 9 contains concluding remarks. This article extends the preliminary results in Scott, Findeisen, Braatz, and Raimondo (2013) by providing a more general theoretical development, an improved optimization formulation, a treatment of state constraints, several new methods for reducing computational complexity, and extended numerical results.

2. Problem formulation

Consider a discrete-time system with time k, state $\mathbf{x}_k \in \mathbb{R}^{n_x}$, output $\mathbf{y}_k \in \mathbb{R}^{n_y}$, input $\mathbf{u}_k \in \mathbb{R}^{n_u}$, disturbance $\mathbf{w}_k \in \mathbb{R}^{n_w}$, and measurement error $\mathbf{v}_k \in \mathbb{R}^{n_v}$. In each interval $[k, k+1]$, $k = 0, 1, \ldots$, the system evolves according to one of n_m possible linear models. The matrices of these models are distinguished by the argument $i \in \mathbb{I} \equiv \{1, \ldots, n_m\}$:

$$\mathbf{x}_{k+1} = \mathbf{A}(i_k)\mathbf{x}_k + \mathbf{B}(i_k)\mathbf{u}_k + \mathbf{r}(i_k) + \mathbf{B}_w(i_k)\mathbf{w}_k, \tag{1}$$

$$\mathbf{y}_k = \mathbf{C}(i_k)\mathbf{x}_k + \mathbf{s}(i_k) + \mathbf{D}_v(i_k)\mathbf{v}_k. \tag{2}$$

The model $i = 1$ is nominal, and the rest are faulty. Models representing multiple, simultaneous faults can be included in $\mathbb{I}$ if desired. The constant vectors $\mathbf{r}(i)$ and $\mathbf{s}(i)$ are used to model additive faults such as sensor and actuator bias. It is assumed that $\mathbf{x}_0 \in X_0$, and $(\mathbf{w}_k, \mathbf{v}_k) \in W \times V$, $\forall k \in \mathbb{N}$, where X_0, W and V are zonotopes (see Section 3.1).

A fault at time k is modeled by a transition from one model in $\mathbb{I}$ to another; i.e., $i_k \neq i_{k-1}$. Given a time interval $[0, N]$, a *fault scenario* on $[0, N]$ is defined as a sequence $(i_0, \ldots, i_N) \in \mathbb{I}^N$. Let $\tilde{\mathbb{I}} \subset \mathbb{I}^N$ denote a set of permissible fault scenarios on $[0, N]$. Given $\tilde{\mathbb{I}}$, the goal is to compute an open-loop input sequence $\tilde{\mathbf{u}} = (\mathbf{u}_0, \ldots, \mathbf{u}_{N-1})$ such that any observed sequence of outputs $\tilde{\mathbf{y}} = (\mathbf{y}_0, \ldots, \mathbf{y}_N)$ is consistent with at most one fault scenario in $\tilde{\mathbb{I}}$, regardless of the exact values of the initial condition, disturbances, and measurement errors in the sets X_0, W, and V. Such input sequences are referred to as *separating inputs* (see Section 4). Ideally, $\tilde{\mathbf{u}}$ should be *minimal* in some sense (e.g., length, norm). We assume that N is specified and focus on the computation of a separating input sequence that minimizes a quadratic objective subject to input and state constraints. This computation can be iterated with N increasing from 1 until the problem becomes feasible.

Requiring that $\tilde{\mathbf{u}}$ is a separating input is equivalent to requiring that every distinct pair of scenarios $\tilde{i}, \tilde{j} \in \tilde{\mathbb{I}}$ can be distinguished. Thus, $\tilde{\mathbf{u}}$ must satisfy $Q = \binom{s}{2}$ conditions, where s is the number of scenarios in $\tilde{\mathbb{I}}$ (see (19) in Section 5). Despite the computational advantages of the proposed methods, this combinatorial dependence demands a parsimonious selection of permissible scenarios. If every scenario is permissible, then $s = (n_m)^N$. However, many scenarios will be nonsensical (e.g., spontaneously corrected faults) or very unlikely (e.g., multiple unrelated faults). Further reductions can be achieved by limiting the frequency of faults (i.e., imposing a minimum number of repeats $i_k = i_{k+1} = \cdots = i_{k+d}$ after a transition). Effectively choosing scenarios for a given application is not considered here; $\tilde{\mathbb{I}}$ is assumed given.

3. Preliminaries

3.1. Zonotopes and set operations

The methods in this article involve computations with *zonotopes*, which are centrally symmetric convex polytopes that can be described as Minkowski sums of line segments (Kuhn, 1998). In *generator representation*, a zonotope Z is prescribed by its *center* $\mathbf{c} \in \mathbb{R}^n$ and *generators* $\mathbf{g}_1, \ldots, \mathbf{g}_{n_g} \in \mathbb{R}^n$ as $Z = \{\mathbf{G}\boldsymbol{\xi} + \mathbf{c} : \boldsymbol{\xi} \in \mathbb{R}^{n_g}, \ \|\boldsymbol{\xi}\|_\infty \leq 1\}$, where $\mathbf{G} \equiv [\mathbf{g}_1 \ \ldots \ \mathbf{g}_{n_g}]$. We use the notation $Z = \{\mathbf{G}, \mathbf{c}\}$. The *order* of a zonotope is n_g/n. A first-order zonotope with linearly independent generators is a parallelotope.

Let $Z, Y \subset \mathbb{R}^n$, $\mathbf{R} \in \mathbb{R}^{m \times n}$, and define the operations

$$\mathbf{R}Z \equiv \{\mathbf{R}\mathbf{z} : \mathbf{z} \in Z\}, \tag{3}$$

$$Z \oplus Y \equiv \{\mathbf{z} + \mathbf{y} : \mathbf{z} \in Z, \ \mathbf{y} \in Y\}, \tag{4}$$

$$Z \ominus Y \equiv \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} + Y \subset Z\}. \tag{5}$$

When $Z = \{\mathbf{G}_z, \mathbf{c}_z\}$ and $Y = \{\mathbf{G}_y, \mathbf{c}_y\}$ are zonotopes, (3)–(4) are also zonotopes and can be computed efficiently (Kuhn, 1998):

$$\mathbf{R}Z = \{\mathbf{R}\mathbf{G}_z, \mathbf{R}\mathbf{c}_z\}, \qquad Z \oplus Y = \{[\mathbf{G}_z \ \mathbf{G}_y], \mathbf{c}_z + \mathbf{c}_y\}. \tag{6}$$

In contrast, when Z and Y are general convex polytopes, the Minkowski sum (4) and the linear mapping (3) with singular $\mathbf{R}$ (e.g., polytope projection) both become extremely computationally demanding and numerically unstable in dimensions greater than about 10 (Althoff & Krogh, 2011; Fukuda, 2004). However, the results of the operations in (6) can be higher order than Z and Y. To avoid increasing orders, techniques for enclosing a given zonotope within a zonotope of lower order must be used. For the computations presented in Section 8, Method C in Althoff, Stursberg, and Buss (2010) is used.