Preprints of the 10th IFAC International Symposium on Dynamics and Control of Process Systems
The International Federation of Automatic Control
December 18-20, 2013. Mumbai, India

Certifying Robustness of Separating Inputs and Outputs in Active Fault Diagnosis for Uncertain Nonlinear Systems

Stefan Streif [*,**] **Daniel Hast** [*] **Richard D. Braatz** [**]
Rolf Findeisen [*]

[*] *Institute for Automation Engineering, Laboratory Systems Theory and Control, Otto-von-Guericke University Magdeburg, Germany*
[**] *Massachusetts Institute of Technology, Cambridge, MA, USA*

Abstract: To ensure safe operation of technical processes, faults have to be reliably detected and isolated to provide information for process maintenance, shutdown, or reconfiguration. Fault detection and isolation can be achieved by invalidation of fault candidates, i.e. models of the system in fault-free and faulty condition. In order to enhance the performance of fault detection and isolation, so-called *active approaches* use input signals with the objective that the resulting system outputs are consistent with at most one fault candidate. Guaranteeing or analyzing robustness of active fault diagnosis with respect to input, output, and process uncertainties and nonlinearities is challenging. This paper provides certificates of robustness of input sequences with respect to the aforementioned uncertainties and nonlinearities. The certificates enable the determination of input and output uncertainties for which unique fault diagnosis results can still be guaranteed. In addition, a method is presented to select a minimal number of outputs that still guarantee robust fault diagnosis, thus reducing the measurement setup and cost. The approach employs nonlinear mixed-integer feasibility problems and a relaxation framework and does not require the explicit computation of reachable sets. The approach is applicable to polynomial discrete-time systems and is demonstrated for a numerical example.

Keywords: Fault detection and isolation; Nonlinear systems; Process control applications.

1. INTRODUCTION

Fault detection and isolation (FDI) is becoming increasingly important in chemical plants due to growing requirements for safety and availability. FDI approaches have to cope with uncertain measurements (Blanke et al., 2006), which impede making conclusive statements. An important class of FDI methods are so-called *active* approaches in which auxiliary input signals are used to enhance the FDI performance (Niemann and Poulsen, 2005; Ungermann et al., 2012; Campbell and Nikoukhah, 2004; Zhang, 1989). Active diagnosis becomes important if faults are not detectable or isolable during nominal plant operation, in particular, if the reachable output sets for different faults and the nominal behavior overlap, or if the control actions mask the effects of faults.

Finding input signals that ensure guaranteed FDI is challenging, because the signals should not influence the system performance and safety. To this end, several approaches have been proposed, mainly focusing on excitation design and robustness against uncertainties (Blanke et al., 2006). Campbell and Nikoukhah (2004) present a comprehensive methodology for the design of active inputs for FDI over finite and infinite intervals. Recently, a computationally efficient approach for active and guaranteed FDI using zonotopes and optimization has been proposed (Scott et al., 2013). However, with few exceptions (Andjelkovic et al., 2008), most methods allow only for linear models or analysis methods, or focus on discrete-event systems (Sampath et al., 1998).

This paper considers (polynomial) nonlinear discrete-time models and addresses robustness of fault diagnosis with respect to process uncertainties and nonlinearities (Sec. 2). The presented methods are based on set-based invalidation methods employing convex relaxations (Rumschinski et al., 2012; Savchenko et al., 2011, 2012; Streif et al., 2012). These methods allow guaranteed statements on model consistency and inconsistency in the presence of uncertainties. Based on this framework, Sec. 3 derives certificates that enable robustness checks of fault diagnosis subject to disturbances and measurement uncertainties. In contrast to most other works that employ set-based approaches (e.g. Savchenko et al. (2012)), the presented approach does not explicitly compute reachable ouput sets to check diagnosability and uses a mixed-integer formulation instead. Sec. 4 outlines different solutions to reduce the problem size and the presented approach. An algorithm in Sec. 5 reduces the number of required measurement outputs. The proposed greedy algorithm allows the selection of a minimum number of outputs such that robust FDI is still guaranteed and measurement cost is reduced. Sec. 6 gives an example illustrating the robustness certificates for separating inputs. Overall, the results enable robustness analysis of active fault diagnosis signals, redesign of the inputs, and selection of outputs if robustness cannot be certified.

2. PROBLEM FORMULATION

Given a process subject to faults, consider explicit discrete-time models of the nominal and faulty process of the form:

$$\begin{aligned} x(k+1) &= g\big(x(k), u(k), \delta_g(k), p, s\big), \\ y(k) &= h\big(x(k), u(k), p, s\big). \end{aligned} \tag{1}$$

The functions g and h represent the aggregated hybrid dynamics and the model output, respectively. The functions g and h are assumed to be polynomial. The time index is $k \in \mathbb{N}$ and $x(k) \in \mathbb{R}^{n_x}$, $p \in \mathbb{R}^{n_p}$, $\delta_g(k) \in \mathbb{R}^{n_g}$, $u(k) \in \mathbb{R}^{n_u}$, and $y(k) \in \mathbb{R}^{n_y}$ are the system states, time-invariant parameters, time-variant disturbances, inputs, and outputs available for fault diagnosis, respectively.

The binary variables $s \in \{0,1\}^{d_s} \subset \mathbb{Z}^{d_s}$ model the *faults* $\mathcal{F} := \{f^{[0]}, f^{[1]}, \ldots, f^{[n_f]}\}$. The value $s = s^{[i]}$, $i \in \mathcal{J} := \{0, 1, \ldots, n_f\}$ provides an appropriate unique *fault signature*, where n_f is the number of faults. A model of the form (1) is called a fault candidate for $s^{[i]}$. The fault is denoted by the superscript $^{[i]}$ on the variables, where $i = 1, \ldots, n_f$. The nominal fault-free case is denoted by the superscript $^{[0]}$.

This paper considers different types of process and measurement uncertainties. The model parameters p are uncertain and described by a bounded set $\mathcal{P} \subset \mathbb{R}^{n_p}$. Similarly, time-varying process disturbances $\delta_g(k)$ are assumed to be uncertain but bounded, $\delta_g(k) \in \mathcal{D}_g \subset \mathbb{R}^{n_g}, \forall k$.

Active fault diagnosis relies on measurements and auxiliary input signals. We assume n_t+1 output measurements while the system is excited by a given input sequence at consecutive time instances $t_0, t_1, \ldots, t_{n_t}$ with corresponding time-index set $\mathcal{T} := \{0, 1, \ldots, n_t\}$. Measurement uncertainties are modeled as

$$\hat{y}_i(k) - \delta_{y,i} \le y_i(k) \le \hat{y}_i(k) + \delta_{y,i}, \qquad i = 1, 2, \ldots, n_y, \quad k \in \mathcal{T}, \tag{2}$$

where $y_i(k)$ is the true but unknown output value, $\hat{y}_i(k)$ is the measured output value, and $\delta_y \in \mathbb{R}^{n_y}$ denotes the measurement uncertainty.

Uncertainties in the input sequence $\hat{u} := \{\hat{u}(0), \hat{u}(1), \ldots, \hat{u}(n_t)\}$, with $\hat{u}(k) \in \mathbb{R}^{n_u}$, are modeled by

$$\hat{u}_i(k) - \delta_{u,i} \le u_i(k) \le \hat{u}_i(k) + \delta_{u,i}, \qquad i = 1, 2, \ldots, n_u, \quad k \in \mathcal{T}, \tag{3}$$

where $u(k)$ is the input of the model (1) and $\delta_u \in \mathbb{R}^{n_u}$ is the time-independent input uncertainty. These uncertanties may be due to actuator or controller uncertainty. To shorten the notation, we write $u \in \mathcal{U}$ (respectively, $y \in \mathcal{Y}$) instead of (3) (respectively (2)).

Relaxation and Set-based Fault Diagnosis. This paper uses the notion of *consistency* for fault diagnosis. For this purpose, a feasibility problem is constructed to check the consistency of a fault $f^{[i]}$ with measurement data (2) and input data (3):

$$\mathrm{FP}^{[i]}: \begin{cases} \text{find } \xi^{[i]} \\ \text{s.t. } x(k+1) = \\ \qquad g\big(x(k), u(k), \delta_g(k), p, s^{[i]}\big), & \forall k \in \mathcal{T} \setminus n_t \\ \quad y(k) = h\big(x(k), u(k), p, s^{[i]}\big), & \forall k \in \mathcal{T} \\ \quad x(k) \in \mathcal{X}, y \in \mathcal{Y}, u \in \mathcal{U}, & \forall k \in \mathcal{T} \\ \quad \delta_g \in \mathcal{D}_g, p \in \mathcal{P}, \end{cases}$$

where the vector $\xi^{[i]} := [x(0), \ldots, x(n_t), u(0), \ldots, u(n_t), \delta_g(0), \ldots, \delta_g(n_t), y(0), \ldots, y(n_t), s^{[i]}, p]^\top$ lumps all variables in $\mathrm{FP}^{[i]}$, and $\mathcal{X}$ denotes given convex sets bounding the states for all $k \in \mathcal{T}$. To simplify notation, the variable superscript $^{[i]}$ is dropped in the constraints of $\mathrm{FP}^{[i]}$, except for $\xi^{[i]}$.

Based on the $\mathrm{FP}^{[i]}$ and its solution set, one can define:

Definition 1. (Consistent fault candidate). The fault candidate $f^{[i]}$ is consistent, if the $\mathrm{FP}^{[i]}$ admits a solution.

Model-based fault diagnosis can be subdivided into two tasks. The first task, *fault detection*, is to determine if the nominal case $f^{[0]}$ is consistent with the measurements, i.e., if the associated $\mathrm{FP}^{[0]}$ admits a solution for actual measurements. The second task, *fault isolation*, is to determine which fault candidates are consistent with the measurements. Ideally, the aim is to achieve complete fault isolation, which means that only one fault candidate is uniquely and unambiguously determined.

Solving the tasks of fault detection and isolation is non-trivial, especially for nonlinear and uncertain systems. However, for the considered polynomial model class, the feasibility problem $\mathrm{FP}^{[i]}$ can be relaxed into a semidefinite or linear program. With these convex relaxations, outer approximations can be derived of the possibly nonconvex solution set (see Fig. 1). The outer approximations are guaranteed enclosures of all solutions consistent with the $\mathrm{FP}^{[i]}$. The Lagrangian dual of the convex relaxation can be used to check whether a consistent solution exists, i.e., checking whether the solution set is empty. The used weak duality theorem and the relaxation process guarantee that, if the objective of the dual program is unbounded, then the feasibility problem $\mathrm{FP}^{[i]}$ does not admit a solution. Feasibility of the resulting relaxed problems can be checked efficiently for moderate-size systems with available solvers. Due to space limitations, readers are referred to (Rumschinski et al., 2010; Savchenko et al., 2011; Rumschinski et al., 2012) for theoretical and numerical details of the set-based framework, and to the free Matlab toolbox ADMIT (Streif et al., 2012) that performs all of the reformulation steps in the set-based framework.

Separating Inputs and Output Selection. The aforementioned methods allow the guaranteed invalidation of fault candidates. Diagnosability of a system requires that the output sets of different fault models do not overlap for all possible uncertainties at least at one measurement time-point, see Fig. 1. Measurements will then allow one to decide which fault has occurred. However, the faults may not be detectable or isolable under all operating conditions and inputs, particularly in a closed-loop system in which a fault-tolerant controller compensates for the faults. To overcome this, input sequences can be computed such that any observed sequence of outputs is consistent with at most one fault candidate in $\mathcal{F}$. Such input sequences are referred to as *separating inputs*, see Scott et al. (2013). By definition, if a separating input is injected into the system, then all faults in $\mathcal{F}$ are diagnosable from output measurements provided that the actual fault scenario is in $\mathcal{F}$, that is, the reachable sets (for all possible uncertainties) of the fault candidate models $\mathrm{FP}^{[i]}$ are disjoint sets, see Fig. 1 for an illustration.

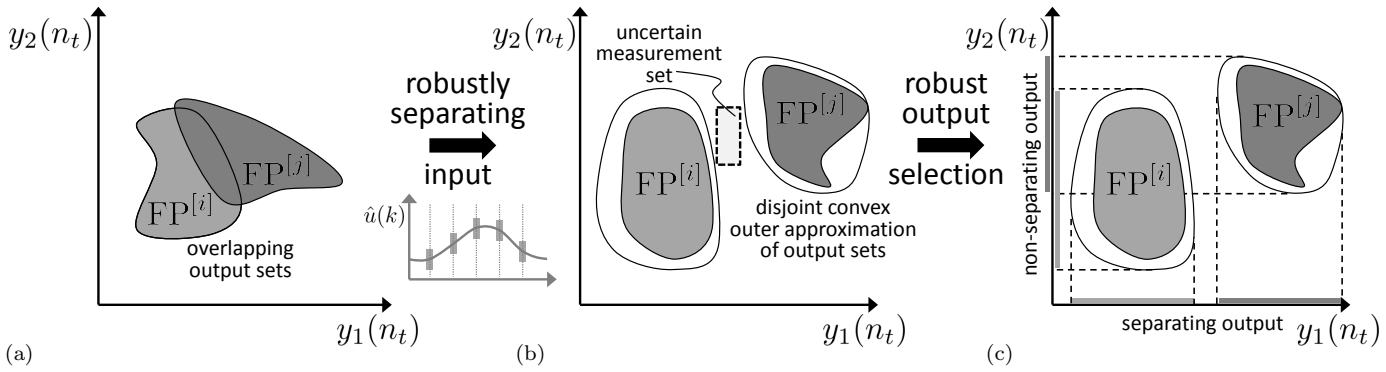

Fig. 1. Illustration of Problems 1 and 2. (a) The projection of the solution sets onto the output space (y_1,y_2) at time t_{n_t} of the fault models $\mathrm{FP}^{[i]}$ and $\mathrm{FP}^{[j]}$ overlap, which then prevents unique diagnosis. (b) The application of a separating input $\hat{u}$ leads to non-overlapping output sets that are separated (in a maximum norm sense) by at least the measurement uncertainty (dashed box). The plot between (a) and (b) shows the set of separating input $\hat{u}$ in which, for any input value within the uncertainty set, output set separation is guaranteed. (c) Measuring output y_1 is sufficient to isolate the faults, since the projection of the output sets onto subspace y_1 results in disjoint sets. Output y_2 alone does not guarantee output separation due to overlapping sets in the projection.

Assume that a potential separating input sequence $\hat{u}$ has been determined with one of the methods referenced in Sec. 1. Such an input sequence could have been computed either by means of structural analysis, optimization or stochastic approaches, without guaranteed certificates for robustness. To guarantee that the potential input sequence allows the isolation of all faults regardless of model nonlinearities and uncertainties, consider the problem:

Problem 1. (Robustly separating inputs). Certify that the uncertain input signal $u \subseteq \mathcal{U}$ robustly separates outputs within a finite number of n_t time steps for the input uncertainties δ_u, output uncertainties δ_y, and for process uncertainties $\mathcal{D}_g$, $\mathcal{P}$, $\mathcal{X}$.

In principle, one can measure all outputs of and also inject all inputs to the system with the best accuracy that is technically possible to achieve best fault diagnosis results. This however is expensive in practical applications and not desirable. This motivates the determination of those measurement outputs and corresponding maximally tolerable measurement uncertainty together with a minimal desired input precision that allows unique fault detection and isolation. The precision of the input signal is determined within the solution of Problem 1; Problem 2 considers the determination of a minimal set of measured outputs:

Problem 2. (Robust output selection). Determine a subset of outputs $\mathcal{O} \subseteq \{1, 2, \ldots, n_y\}$ for a given accuracy $\delta_{y,j}, j \in \mathcal{O}$ that enables robust and guaranteed fault detection and isolation despite input uncertainties δ_u and process uncertainties $\mathcal{D}_g$, $\mathcal{P}$, $\mathcal{X}$.

The next sections address the stated problems.

3. SEPARATING INPUTS

This section provides certificates for robust diagnosis despite input uncertainties δ_u and output uncertainties δ_y. The problem is approached by starting with the rigorous requirement for diagnosability using an associated mixed-integer formulation. While this approach is very flexible and also allows the incorporation of qualitative fault descriptions (see Rumschinski et al. (2012)), it also leads to a computationally demanding problem. In the subsequent Sec. 4, possible means for problem size reduction are discussed. Note that the presented approach does not require the explicit computation of reachable sets as done e.g. in Savchenko et al. (2012).

Constraints for Output Set Separation. As the first step, define the requirements and constraints for separation of the output sets of two faults $f^{[i]}$ and $f^{[j]}$ with $i, j \in \mathcal{J}$, $i \neq j$, leading to the feasibility problems $\mathrm{FP}^{[i]}$ and $\mathrm{FP}^{[j]}$. For unique fault diagnosis, every possible pairwise comparison of two faults must have separated output sets, at least at one time-point. This requires to check a large number of different combinations. To simplify the presentation, this section considers only a single fault pair $[i, j]$, with $i, j \in \mathcal{J}$, $i \neq j$ including the nominal case. The extension to the full case where all pairwise combinations are considered in a single feasibility problem $\mathrm{FP}^{[\mathcal{J}]}$ is straightforward. It can, however, lead to a large and possibly intractable problem. Without loss of generality, the full-case feasibility problem is tackled in Sec. 4.

Since the outputs of the system are uncertain, the minimum distance between the outputs $y_l^{[i]}$ and $y_l^{[j]}$ must be larger than the output uncertainty $2\delta_{y,l}$, cf. (2). Define

$$\sigma_l^{[i,j]}(k) := \left(y_l^{[i]}(k) - y_l^{[j]}(k)\right)^2 - \left(2\delta_{y,l}\right)^2,\ l \in \mathcal{O}, \qquad (4)$$

and demand that $\sigma_l^{[i,j]}(k) \geq 0$ at least for one $k \in \mathcal{T}$ and one $l \in \mathcal{O}$ (cf. Fig. 1). For this purpose, reformulate condition (4) by binary variables that are constrained to be one if condition (4) holds:

$$\beta_l^{[i,j]}(k) \geq \frac{\sigma_l^{[i,j]}(k)}{M} \quad \text{and} \quad \beta_l^{[i,j]}(k) \leq \frac{\sigma_l^{[i,j]}(k)}{M} + 1. \qquad (5)$$

The constant M is large enough to ensure $-1 \leq \frac{\sigma^{[i,j]}(k)}{M} \leq 1$ for all admissible values of $\sigma_l^{[i,j]}(k)$; M can be computed by preprocessors using interval arithmetic (Streif et al., 2012). The binary variable $\beta_l^{[i,j]}(k)$ can take the values of 0 or 1 if $\sigma_l^{[i,j]}(k) = 0$. However, this does not restrict further reasoning and can be avoided in practice by adding a small enough number to either equation in (5), see references in Rumschinski et al. (2012).

The binary variables $\beta_l^{[i,j]}(k)$ indicate whether the two faults $\mathrm{FP}^{[i]}$ and $\mathrm{FP}^{[j]}$ have disjoint output sets with respect to the measurement uncertainties at time index k (cf. Fig. 1). The constraint

$$\sum_{l\in\mathcal{O}}\sum_{k\in\mathcal{T}}\beta_l^{[i,j]}(k)\geq 1, \tag{6}$$

demands that output sets are disjoint at least at one time instance $k\in\mathcal{T}$.

Robustness Certificate for Separating Input Sets. With the above equations, the feasibility problem

$$\mathrm{FP}^{[i,j]}:\begin{cases}\text{find } \xi^{[i]},\xi^{[j]},\beta_l^{[i,j]}(k),k\in\mathcal{T},l\in\mathcal{O}\\ \text{s.t. constraints in } \mathrm{FP}^{[i]}\\ \quad\text{constraints in } \mathrm{FP}^{[j]}\\ \quad\text{constraints } (4),(5),(6),\end{cases}$$

combines the feasibility problems $\mathrm{FP}^{[i]}$, $\mathrm{FP}^{[j]}$, and the constraints for separated output sets. The combined feasibility problem contains $(n_t+1)n_y$ additional binary variables and $2(n_t+1)n_y+1$ additional constraints due to the requirements for output set separation. The input uncertainty δ_u is assumed to satisfy (3), i.e., $u\in\mathcal{U}$.

The feasibility problem $\mathrm{FP}^{[i,j]}$ is used to check if there exists any input sequence $u\in\mathcal{U}$ that separates the outputs. However, the resulting problem is a nonlinear mixed-integer problem that is challenging to solve. Convex relaxations are applied as presented in the previous section, with use of infeasibility certificates provided by the Lagrangian dual. This allows the determination of outer approximations of separating input sets. Also, if the feasibility problem $\mathrm{FP}^{[i,j]}$ can be shown to be inconsistent, then it can be certified that no separating input exist. However, the outer approximations do not ensure that all input sequence parameterized by the set $\mathcal{U}$ guarantees output set separation. Therefore we modify $\mathrm{FP}^{[i,j]}$ to be able to derive certificates that guarantee output set separation.

We approach the problem from the opposite direction and determine the solution sets for which all outputs overlap at all time-points, which introduces the constraint

$$\sum_{l\in\mathcal{O}}\sum_{k\in\mathcal{T}}\beta_l^{[i,j]}(k)=0, \tag{7}$$

which is the inversion of constraint (6). If the solution set can be proved to be empty, then the output sets are disjoint at least at one time point. To determine the solution set, the constraint (7) instead of (6) is incorporated into the feasibility problem $\mathrm{FP}^{[i,j]}$, to obtain:

$$\widehat{\mathrm{FP}}^{[i,j]}:\begin{cases}\text{find } \xi^{[i]},\xi^{[j]},\beta_l^{[i,j]}(k),k\in\mathcal{T},l\in\mathcal{O}\\ \text{s.t. constraints in } \mathrm{FP}^{[i]}\\ \quad\text{constraints in } \mathrm{FP}^{[j]}\\ \quad\text{constraints } (4),(5),(7).\end{cases}$$

The solution set of $\widehat{\mathrm{FP}}^{[i,j]}$ gives the input values for which the outputs overlap at all time instances. If it can be shown that $\widehat{\mathrm{FP}}^{[i,j]}$ does not admit a solution for a given input uncertainty $\mathcal{U}$, then all inputs robustly separate the outputs. As above, it is difficult to check that $\widehat{\mathrm{FP}}^{[i,j]}$ admits a solution. However, convex linear relaxations can be used to show that there exists no solution using the Lagrangian dual. This analysis allows the statement of the following theorem:

Theorem 1. (Certificate for separation of output sets). If the solution set of the convex relaxation of $\widehat{\mathrm{FP}}^{[i,j]}$ is empty, then it is guaranteed that any realization $u\in\mathcal{U}$ leads to separated outputs $y\in\mathcal{Y}$ at least for one $k\in\mathcal{T}$ and one $l\in\mathcal{O}$.

Proof: Follows directly from the construction of $\widehat{\mathrm{FP}}^{[i,j]}$.

Note that constraints on the inputs or states can be added straightforwardly to $\widehat{\mathrm{FP}}^{[i,j]}$. However, to guarantee robustness with respect to these constraints, constraints have to be included in a similar manner as above in (4)–(7).

Thm. 1 enables one to check for robustness of a precomputed input sequence with uncertainties δ_u with respect to process uncertainties and nonlinearities. The computationally demanding determination of reachable output sets to analyze diagnosability is avoided by using a single mixed-integer problem. It is also possible to search for a maximal input uncertainty for which output set separation can be guaranteed by iteratively and heuristically increasing δ_u, to reformulate $\mathrm{FP}^{[i,j]}$ as an optimization that minimizes an affine function of δ_u, or to test different uncertainty combinations as demonstrated for the example in Sec. 6.

4. PROBLEM SIZE REDUCTION

The presented mixed-integer formulation can account for the combinatorial problem of comparison of different fault outputs at different time-steps and avoids the explicit computation of reachable sets by solving a single feasibility problem. In addition, it allows for the incorporation of qualitative fault descriptions (Rumschinski et al., 2012). However, it might suffer from a large number of binary variables. This section discusses two solutions to reduce the problem size even in the case when many faults are considered.

Reformulation and simplifications. Constraint (7) imposes all $\beta_l^{[i,j]}(k)$ to be zero, which allows to simplify Eq. (5). This yields a computationally simpler problem with fewer binary variables. Note that this can result in a simple feasibility problem if the FP does not contain integer variables.

Reduction for more than two faults. For unique FDI, all faults in $\mathcal{F}$ have to be considered. One way to do this is to compare all faults in a pairwise manner using Thm. 1, which would require solving $\binom{n_f+1}{2}$ problems $\widehat{\mathrm{FP}}^{[i,j]}$. An alternative way is to add equations for all faults in $\mathcal{F}$ and the corresponding pairwise comparisons to obtain a single feasibility problem that comprises all faults, $\mathrm{FP}^{[\mathcal{J}]}$. Even for small models, however, this might lead to an intractable problem.

Here a different approach is proposed that considers all possible fault combinations at once with only slight increase of the problem size compared to the case with only two faults $[i,j]$. The basic idea is to consider the

combined feasibility problem $\widehat{\text{FP}}^{[i,j]}$ as given above, but without fixing the fault signature variables $s^{[i]}$ and $s^{[j]}$ to their respective values. Rather, we keep the (binary) fault signature variables as decision variables and search for a pair of fault signatures that violate the output separation constraints. If no solution is found, then Thm. 1 certifies that the output sets are separated.

To derive the required constraints on $s^{[i]}$ and $s^{[j]}$, note that $s^{[i]}$ and $s^{[j]}$ are not fixed, but are rather decision variables. Demand that

$$\sum_{l=1}^{d_s} s_l^{[i]} = 1, \quad \sum_{l=1}^{d_s} s_l^{[j]} = 1, \quad s_l^{[i]} + s_l^{[j]} \leq 1, \quad l = 1, 2, \ldots, d_s. \tag{8}$$

The first two equations in (8) imply that each fault is represented by a single binary variable, which is mild assumption and is often the case or can be achieved by introducing additional binary variables and suitable rewriting of (1). The last constraint in (8) ensures that no two faults are the same.

Eq. (8) introduce $d_s + 2$ additional integral constraints that are *special ordered sets of type one*, which are usually dealt with efficiently by mixed-integer solvers during the branch-and-bound method. Eq. (8) can be used to build a feasibility problem $\text{FP}^{[\mathcal{J}]}$ that combines all faults in $f \in \mathcal{F}$ simultaneously. Thm. 1 can be used to certify that all inputs parameterized from the set $\mathcal{U}$ robustly separate the outputs of all faults.

5. OUTPUT SELECTION

It is intuitively clear that more outputs and more accurate measurements can improve the performance of FDI. However, accurate measurements of all available outputs might not be necessary for unique FDI. To reduce costs, it is of interest to use a minimum number of sensors such that faults can still be robustly detected and isolated. To this end, Problem 2 is addressed next.

Define the cost $c_i \in \mathbb{R}_+, i = 1, \ldots, n_y$, for measuring the output y_i at the given accuracy $\delta_{y,l}$. Then the following greedy algorithm can be used to select a minimum number of outputs for which the cost is locally minimized.

Algorithm 1. (Output selection).

```
Input:   output index set 𝒪
         cost vector c ∈ ℝ^{n_y}
Returns: selected output index set 𝒪 which minimizes cost

SORT 𝒪 w.r.t. descending cost c
WHILE 𝒪 is not empty
  FOR i = 1 TO LENGTH(𝒪)
    SET 𝒪* ← 𝒪
    REMOVE ith elements from 𝒪*
    IF Lagrangian dual of FP^[i,j] with selected outputs 𝒪*
          is unbounded
      SET 𝒪 ← 𝒪*
      BREAK for-loop
    END
    IF i = LENGTH(𝒪)
      BREAK while-loop
    END
  END
END
```

Algorithm 1 returns a subset of the outputs $\mathcal{O}$ for which robust FDI is guaranteed, and can be extended straightforwardly to incorporate more than two faults as described in the previous section.

6. EXAMPLE

Due space limitations, the approach is demonstrated for an academic example. Consider a nonlinear discrete-time system with three fault candidates given by

$$f^{[0]} : x(k+1) = u(k) + \left(p_1 x^2(k) - x(k)\right) p_2, \tag{9}$$

$$f^{[1]} : x(k+1) = u(k) + \left(p_1 x^2(k) - x(k)\right) (p_2 + 0.5), \tag{10}$$

$$f^{[2]} : x(k+1) = (u(k) + 0.5) + \left(p_1 x^2(k) - x(k)\right) p_2, \tag{11}$$

where $f^{[0]}$ is the nominal case, $f^{[1]}$ is a sensor-offset fault, and $f^{[2]}$ is an actuator-gain fault. The parameters p_1, p_2 and the initial condition x_0 are unknown but bounded in

$$\mathcal{P} = \{0.098 \leq p_1 \leq 0.102, 0.495 \leq p_2 \leq 0.505\},$$
$$\mathcal{X} = \{0.95 \leq x(0) \leq 1.05\}.$$

Consider that an input sequence, leading to disjoint outputs is known for the arithmetic mean values of the parameters and initial conditions (i.e., $p_1 = 0.1$, $p_2 = 0.5$, and $x_0 = 1$). In Fig. 2, the considered sequence and appropriate output sequences for the mean-value case of the fault candidates (9)–(11) are shown. The aim is to certify robustness of output set separation with respect to the uncertainties of the parameters and initial condition, and to obtain suitable measurement and input uncertainties.

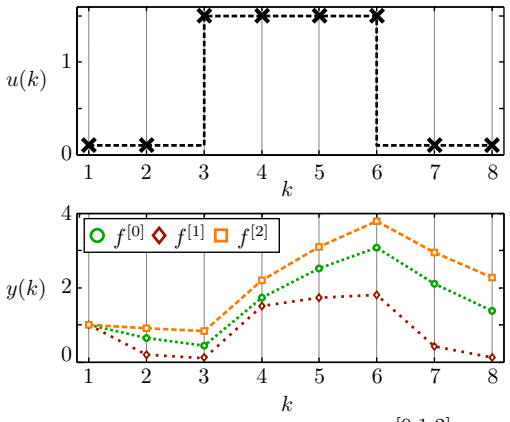

Fig. 2. Input and output signals of $f^{[0,1,2]}$ for the arithmetic mean of the parameters and initial conditions.

The consistency approach in Sec. 3 and Thm. 1 incorporating the uncertainties $\mathcal{X}$, $\mathcal{U}$, δ_u, and δ_y is employed to determine if robust diagnosis can be certified for a combination of input and output uncertainties. The results were obtained with the Matlab toolbox ADMIT (Streif et al., 2012) using the mixed-integer solver CPLEX.

The results are summarized in Table 1, where the considered input and output uncertainties are shown together with the information if a certificate for the robustness of diagnosis can be given (✓) or not (✗).

Fig. 3 provides more insight on the certificates for robust diagnosis by showing the outer boundings of the reachable outputs for (a) $\delta_u = 0.1$, $\delta_y = 0.1$ (not certified) and (b) $\delta_u = 0.05$, $\delta_y = 0.1$ (certified) from Tab. 1. Fig. 3 also shows measurements that were randomly sampled from a uniform distribution with width δ_y centered at values

δ_u \ δ_y	0.005	0.01	0.05	0.1
0.05	✓	✓	✓	X
0.10	✓	✓	✓	X
0.20	✓	✓	X	X
0.30	✓	X	X	X

Table 1. Certified (✓) and not certified (X) robustness for diagnosis.

obtained from a Monte Carlo simulation, which indicates that the outer boundings of $y(k)$ are quite tight in this problem. The time bases of the fault candidates are slightly shifted for plotting purposes. Note here that the reachable sets are shown for ease of presentation here. However, their time-consuming computation is not required for the presented analysis.

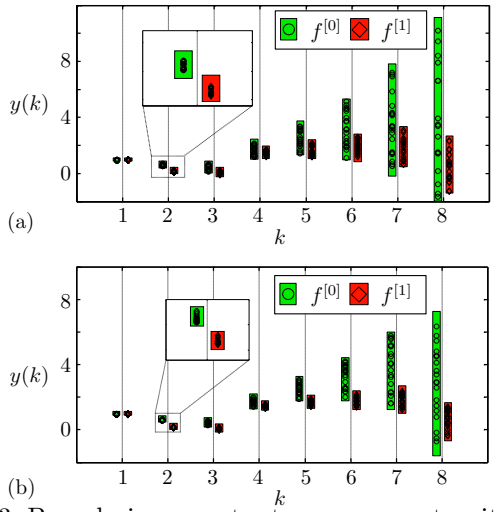

Fig. 3. Boundaries on output measurements with 20 samples of a Monte Carlo simulation with $f^{[0]}$ and $f^{[1]}$ for: (a) a non-certified case ($\delta_u = 0.1$, $\delta_y = 0.1$) and (b) a certified case ($\delta_u = 0.05$, $\delta_y = 0.1$).

Enlarged samples for $k = 2$ are shown in Fig. 3 that clarify whether the output sets of the nominal and faulty case can be separated. The output sets overlap in Case a, but not in Case b. It is evident that the Case a leads to a feasible solution for the inverted feasibility problem $\widehat{\text{FP}}^{[i,j]}$. In contrast, a certificate for robust diagnosis can be given in Case b.

7. CONCLUSIONS

While active FDI methods for linear systems are well established and computationally efficient (see e.g. Scott et al. (2013), Campbell and Nikoukhah (2004), and references within), it is not necessarily guaranteed that the obtained input sequences are robust with respect to process uncertainties and nonlinearities. This paper presents a method that can be applied directly to polynomial systems with defined uncertainties to certify robustness of fault separation with respect to nonlinearities or uncertainties for given input sequences. The approach also enables the redesign of active FDI. If robustness cannot be certified, then the engineer can choose different input sequences, improve the precision of measurement or actuation devices, or refine the fault or process models.

The certificates can also be used in a heuristic search for separating input sets that guarantee fault diagnosis, by using Monte Carlo sampling to determine separating inputs and to then expand the uncertainties locally around the sample. Furthermore, the determined uncertainty bounds can be used as constraints in nonlinear optimization to choose the best input sequences that minimize input energy or cost, while diagnosability is still guaranteed.

The presented approach can be computationally costly and may not be applicable in all real-time applications. However, in many applications, only fault detection is performed online, and fault isolation is done offline. When faults are suspected, separating inputs can then be designed offline for diagnosis. Then, enough time and computational power is available to apply the results of this work and determine robustly separating inputs.

REFERENCES

Andjelkovic, I., Sweetingham, K., and Campbell, S.L. (2008). Active fault detection in nonlinear systems using auxiliary signals. In *Proc. American Control Conference (ACC)*, 2142–2147.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006). *Diagnosis and Fault-Tolerant Control*. Springer, Heidelberg, Berlin.

Campbell, S. and Nikoukhah, R. (2004). *Auxilary Signal Design for Failure Detection*. Princeton Univ. Press.

Niemann, H.H. and Poulsen, N.K. (2005). Active fault diagnosis in closed-loop systems. In *Proc. IFAC World Congress*, 6 pp.

Rumschinski, P., Borchers, S., Bosio, S., Weismantel, R., and Findeisen, R. (2010). Set-base dynamical parameter estimation and model invalidation for biochemical reaction networks. *BMC Syst. Biol.*, 4:69, online.

Rumschinski, P., Streif, S., and Findeisen, R. (2012). Combining qualitative information and semi-quantitative data for guaranteed invalidation of biochemical network models. *Int. J. Robust Nonlin. Control*, 22, 1157–1173.

Sampath, M., Lafortune, S., and Teneketzis, D. (1998). Active diagnosis of discrete-event systems. *IEEE T. Automat. Contr.*, 43, 908–929.

Savchenko, A., Rumschinski, P., and Findeisen, R. (2011). Fault diagnosis for polynomial hybrid systems. In *Proc. IFAC World Congress*, 2755–2760.

Savchenko, A., Rumschinski, P., Streif, S., and Findeisen, R. (2012). Complete diagnosability of abrupt faults using set-based sensitivities. In *Proc. IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS)*, 860–865.

Scott, J.K., Findeisen, R., Braatz, R.D., and Raimondo, D.M. (2013). Design of active inputs for set based fault diagnosis. In *Proc. American Control Conference (ACC)*, 3567–3572.

Streif, S., Savchenko, A., Rumschinski, P., Borchers, S., and Findeisen, R. (2012). ADMIT: A toolbox for guaranteed model invalidation, estimation and qualitative-quantitative modeling. *Bioinformatics*, 28, 1290–1291.

Ungermann, M., Lunze, J., and Schwarzmann, D. (2012). Test signal generation for service diagnosis based on local structural properties. *Int. J. Appl. Math. Comp. Sci.*, 22, 55–65.

Zhang, X.J. (1989). *Auxiliary Signal Design in Fault Detection and Diagnosis*, volume 134 of *Lecture notes in control and information sciences*. Springer, Heidelberg, Berlin.