Proceedings of the 9th International Symposium on
Dynamics and Control of Process Systems (DYCOPS 2010),
Leuven, Belgium, July 5-7, 2010
Mayuresh Kothare, Moses Tade, Alain Vande Wouwer, Ilse Smets (Eds.)

Complete Fault Diagnosis Of Uncertain Polynomial Systems

Philipp Rumschinski * **Jan Richter** ** **Anton Savchenko** *
Steffen Borchers * **Jan Lunze** *** **Rolf Findeisen** *,[1]

* *Institute of Automation Engineering, Otto-von-Guericke Universität Magdeburg, Germany*
** *Siemens AG, Industry Sector, Gleiwitzer Str. 555, 90475 Nuremberg, Germany*
*** *Institute of Automation and Computer Control, Ruhr-Universität Bochum, Germany*

Abstract: The increase in complexity in process control goes along with an increasing need for complete and guaranteed fault diagnosis. In this contribution, we propose a set-based method for complete fault diagnosis for polynomial systems. It is based on a reformulation of the diagnosis problem as a nonlinear feasibility problem, which is subsequently relaxed into a semidefinite program. This is done by exploiting the polynomial/rational structure of the discrete-time model equations. We assume the measurements of the output and the input to be available as uncertain, but bounded convex sets. The applicability of the method is demonstrated considering a two-tank system subject to multiple faults.

1. INTRODUCTION

Fault diagnosis methods aim at deciding whether a fault has occurred or not, given some measured information. The result of the diagnosis is then either used for monitoring purposes only, or to inform a subsequent control re-adjustment step. Introductions to the most common approaches for fault diagnosis are provided by books Blanke et al. [2006], Ding [2008], Gertler [1998], Isermann [2006]. In literature fault diagnosis is subdivided in methods relying on the analysis of signals (*signal-based*) and methods incorporating a model of the considered process (*model-based*). The latter methods are often founded on consistency tests. Here the measurement data is compared with the ability of a system model to reproduce exactly those measurements Blanke et al. [2006] or on consistency tests based on identified system parameters Isermann [2006].

In both cases the goal is to determine the set of models consistent with the measurements (*fault candidates*). Assuming that for all faults a corresponding model is known (*closed-world assumption*), a fault diagnosis algorithm is said to be *complete* if the true fault is never excluded from the set of fault candidates. Every complete consistency-based fault diagnosis method, starting from an initial fault candidate set, seeks to iteratively exclude fault scenarios that are inconsistent with the observations. If only one fault remains, it is uniquely diagnosed. In general, it is not possible to uniquely distinguish between all faults due to some overlap in the input-output behavior of the corresponding models. However, it is clear that if two behaviors belonging to these fault scenarios differ from another, then there exists an input-sequence that permits distinction between them (*active fault diagnosis*). This dependence is intimately linked to the persistence of excitation condition encountered in system identification, which is however out of the scope of this work.

Consistency-based approaches for fault diagnosis are available for linear parameter varying systems Blesa et al. [2007], for uncertain linear systems Combastel and Raka [2009], Tornil et al. [2003], and for nonlinear systems subject to biased uncertain measurements Planchon [2007]. Other approaches are based on residuals generated by means of observers or Kalman filters and compared to a threshold Theilliol et al. [2008], Videau et al. [2009], Zhang et al. [2008]. Further fault diagnosis methods for nonlinear systems are available in Aßfalg and Allgöwer [2006], Selmic et al. [2009], Zhang et al. [2002].

In this work, we propose a set-based approach for fault diagnosis for polynomial and rational systems in which we directly aim to classify what fault situations are consistent with the taken measurements. Our framework derives from a parameter estimation and model invalidation approach presented in Borchers et al. [2009], which is based on formulating the regarded problem in terms of a nonlinear feasibility problem. We extend this technique to fault diagnosis, by reformulating the fault detection and fault isolation problems in a similar way. Coupled with an efficient semidefinite solution strategy of the feasibility problem, we are able to provide conclusive proofs on inconsistency of certain fault situations with respect to the measurements. Under the assumption of a complete description of the set of possible faults we can furthermore isolate the corresponding fault candidates and guarantee completeness of our method.

2. PROBLEM SETUP

In this contribution, we consider discrete-time systems $\mathcal{M}_f$ subject to a specific fault $f \in \mathcal{F} = \{f_0, f_1, \ldots, f_{n_f}\}$, where f_0 is associated with the nominal (fault free) system. The

[1] Corresponding author `rolf.findeisen@ovgu.de`

behavior of these systems is described by polynomial or rational difference equations of the form

$$G^f(x_{k+1}, x_k, w_k, p) = 0, \tag{1}$$

$$H^f(y_k, x_k, w_k, p) = 0. \tag{2}$$

Here $x_k \in \mathbb{R}^{n_x}$ denotes the system states, $p \in \mathbb{R}^{n_p}$ the model parameters and $w_k \in \mathbb{R}^{n_w}$, $y_k \in \mathbb{R}^{n_y}$ denote the measured input and output respectively.

For simplicity of presentation, we assume throughout the paper that only a single fault affects the considered process in the time horizon of interest and that for all faults a corresponding model is known. Furthermore, we assume the measurements to be unknown-but-bounded and to be given as convex sets such that measurement uncertainties can be taken into account.

Definition 1. (Consistency). Consider a measurement $\mathcal{W}_k$ of the applied input taken at time-index k and a measurement $\mathcal{Y}_k$ of the output of the considered process. A model $\mathcal{M}_f$ is said to be consistent with the measurements if $w_k \in \mathcal{W}_k$ and $y_k \in \mathcal{Y}_k$.

With Definition 1 we can state the following problems:

Problem 1. (Fault detection). A fault has occurred if the model of the nominal case $\mathcal{M}_{f_0}$ is inconsistent with the measurements.

Problem 2. (Fault isolation). A fault f is a fault candidate, if the model $\mathcal{M}_f$ is consistent with the measurements.

Note that consistency can on-line only be checked in a necessary manner since only past measurements can be taken into account, but not future ones.

3. FAULT DIAGNOSIS AS A FEASIBILITY PROBLEM

In this section, we propose a reformulation of Problem 1 and Problem 2 as a nonlinear feasibility problem. Therefore, assume the following collections of measurements $\mathcal{Y} = \{\mathcal{Y}_k \subset \mathbb{R}^{n_y}, k \in T\}$ and $\mathcal{W} = \{\mathcal{W}_k \subset \mathbb{R}^{n_w}, k \in T\}$ in a certain time window $T = \{t_0, \ldots, t_e\}$. This time window just specifies the time instances when a measurement was taken. Furthermore, assume a candidate fault model $\mathcal{M}_f$ to be given, as described in the previous section. We can then gather all information in the following semi-algebraic equations

$$F_f(\mathcal{P}) : \begin{cases} G^f(x_{k+1}, x_k, w_k, p) = 0, & k \in T, \\ H^f(y_k, x_k, w_k, p) = 0, & k \in T, \\ p \in \mathcal{P}, & \\ x_k \in \mathcal{X}_k, & k \in T, \\ w_k \in \mathcal{W}_k, & k \in T, \\ y_k \in \mathcal{Y}_k, & k \in T, \end{cases} \tag{3}$$

where $\mathcal{P}, \mathcal{X}_k$ denote some given convex sets bounding the parameters and the states, respectively. For instance such bounds can be derived from the physical meaning of the parameters or states (e.g. concentrations have to be non-negative), or from conservation principles. Note that these bounds can be in general arbitrary large, but from a practical perspective tighter bounds are preferable for the proposed relaxation procedure.

Recall that the goal of the fault detection problem is to show that under the allowed variations in p the measurements are not reproducible by the nominal model $\mathcal{M}_{f_0}$.

We denote therefore as feasibility problem the problem of checking whether $F_f(\mathcal{P})$ admits a solution or not.

If the feasibility problem does not admit a solution, then there exists no input for which the model $\mathcal{M}_f$ is consistent with the measurements $\mathcal{Y}, \mathcal{W}$.

Problem 1 and Problem 2 are transfered to

Proposition 1. (Fault detection/Fault isolation). If $F_f(\mathcal{P})$ does admit a solution, the fault f is a fault candidate, i.e. $\mathcal{M}_f$ is consistent with the measurements.

However, it is in general not possible to determine an exact solution of the feasibility problem $F_f(\mathcal{P})$, due to the nonlinearities of the model equations. But we will show in the next section that it is possible to address a relaxed version instead of the original feasibility problem for polynomial/rational systems to give conclusive answers to the problems included in Proposition 1. Note that as a consequence of the relaxation the fault candidates will be determined by elimination of all other possibilities.

4. PROBLEM RELAXATION

As shown in Kuepfer et al. [2007], Borchers et al. [2009] for polynomial/rational systems it is possible to relax $F_f(\mathcal{P})$ into a convex semidefinite program. The method used is based on an image convexification described in Lasserre [2001], Ramana [1994]. Semidefinite programs as a generalization of linear programs can then be efficiently solved via interior point methods, e.g. with Sturm [1999]. In literature several approaches for reformulating $F_f(\mathcal{P})$ are known, i.a. Lasserre [2001], Parrilo [2003]. For the purpose of this work a quadratic reformulation is chosen, as it leads to *SDPs* of moderate size. For the sake of completeness, we present a short overview of the necessary relaxation steps following Borchers et al. [2009].

As a first step the original feasibility problem $F_f(\mathcal{P})$ is rewritten as a quadratic feasibility problem (QP). Therefore, we introduce a vector $\xi \in \mathbb{R}^{n_\xi}$, consisting of a minimal basis of monomials of the model and output equations (1)-(2), in the form

$$\xi = (1,\ x_i,\ p_j,\ w_l,\ y_m,\ x_i p_j,\ x_i w_l,\ \ldots)^T,$$

where the indexes i, j, l, m correspond to the respective number of states x, parameters p, inputs w and outputs y. Equations (1) can be transformed to

$$G_i^f(x_{k+1}, x_k, p, w) = \xi^T Q_k^i \xi = 0, \tag{4}$$

in which $Q_k^i \in \mathbb{R}^{n_\xi \times n_\xi}$ is a symmetric matrix and the index i is again the number of states. Apparently the same is possible for (2) whereas i takes values in $\{1, \ldots, n_y\}$. Note that if the model equations (1)-(2) contain higher order terms (products of lower degree monomials), additional equality constraints of the form (4) have to be introduced.

For simplicity of notation we redefine the index i such that it covers the number of states n_x, the number of output equations n_y and the number of additional constraints n_d as $i \in \mathcal{I} = \{1, \ldots, n_x + n_y + n_d\}$.

The bounds describing the subsets $\mathcal{P}, \mathcal{X}_k, \mathcal{W}_k, \mathcal{Y}_k$ appearing in $F_f(\mathcal{P})$ can be described as linear constraints

$$B\xi \geq 0.$$

Here $B \in \mathbb{R}^{2(n_\xi - 1)\times n_\xi}$ provides explicit upper and lower bounds on all components of ξ except the first one.

Then $F_f(\mathcal{P})$ can be rewritten as

$$QP_f(\mathcal{P}) : \begin{cases} \text{find } \xi \in \mathbb{R}^{n_\xi} \\ \text{subject to} \quad \xi^T Q_k^i \xi = 0, \; i \in \mathcal{I}, k \in T, \\ \qquad\qquad\quad\; \xi_1 = 1, \\ \qquad\qquad\quad\; B\xi \geq 0. \end{cases}$$

Such a quadratic decomposition can always be found for a polynomial/rational system (1)-(2), but $QP_f(\mathcal{P})$ is of course still non-convex. However, by introducing $X = \xi\xi^T$ and relaxing the $rank(X) = 1$ and $tr(X) \geq 1$ condition into the weaker constraint $X \succeq 0$, see e.g. Parrilo [2003], we get the convex semidefinite program

$$SDP_f(\mathcal{P}) : \begin{cases} \text{find} \qquad\quad X \in \mathbb{R}^{n_\xi \times n_\xi} \\ \text{subject to } tr(Q_k^i X) = 0, \quad i \in \mathcal{I}, k \in T, \\ \qquad\qquad\quad tr(ee^T X) = 1, \\ \qquad\qquad\quad BXe \geq 0, \\ \qquad\qquad\quad BXB^T \geq 0, \\ \qquad\qquad\quad X \succeq 0, \end{cases}$$

where $e = (1, 0, \ldots, 0)^T \in \mathbb{R}^{n_\xi}$. The relaxation process will increase in general the solution space of $F_f(\mathcal{P})$ and therefore a fault could be wrongly included in the fault candidate set. However, the true fault will never be excluded from the fault candidates. Note that the redundant constraints $BXB^T \geq 0$ were added to reduce this effect Lasserre [2001].

Since we are only interested in proving infeasibility of $F_f(\mathcal{P})$, an efficient approach is to consider the Lagrangian dual L_f of the semidefinite relaxation.

$$L_f(\mathcal{P}) : \begin{cases} \max \omega \\ \text{subject to} \\ \displaystyle\sum_{k\in T}\sum_{j\in\mathcal{I}} \nu_k^j Q_k^j + \omega ee^T + e\lambda_1^T B + \\ +B^T\lambda_1 e^T + B^T\lambda_2 B + \lambda_3 = 0, \\ \lambda_1 \geq 0, \; \lambda_2 \geq 0, \; \lambda_3 \succeq 0, \end{cases} \tag{5}$$

where ν_k^j, ω are the Lagrangian multipliers corresponding to the equality constraints in the semi definite program, and $\lambda_1 \in \mathbb{R}^{2n_\xi - 1}, \lambda_2 \in \mathbb{R}^{(2n_\xi-1)\times(2n_\xi-1)}$, $\lambda_3 \in \mathbb{R}^{n_\xi \times n_\xi}$ those corresponding to the remaining constraints.

Theorem 1. If the Lagrangian dual $L_f(\mathcal{P})$ is unbounded, then $\mathcal{M}_f$ is inconsistent with the measurements.

The Lagrangian weak-duality property and the relaxation process guarantee that if the Lagrangian dual is unbounded, then $F_f(\mathcal{P})$ does not admit a solution Waldherr et al. [2008].

5. PARAMETER ESTIMATION

Recall that a way for proving inconsistency of a model $\mathcal{M}_f$ is to verify that the Lagrangian dual $L_f(\mathcal{P})$ is unbounded. But since we allow uncertainties in the parameters as well as in the measurements it is very likely for a fault resulting in a slow change in the system dynamics, that the corresponding model $\mathcal{M}_f$ cannot be excluded immediately. In such a case it might be necessary to estimate the system parameters from the measurements. The same is true for a fault resulting in a slow drift in one of the parameters. The goal is then to approximate the subset $\mathcal{P}_c \subseteq \mathcal{P}$ of consistent parameters. We denote this approximation as $\hat{\mathcal{P}}_c$. Therefore, a subregion $\mathcal{Q} \subseteq \mathcal{P}$ is tested via the Lagrangian dual whether a consistent parameterization is contained or not. The subset $\mathcal{P}_c$ is approximated by systematically exploring subregions of $\mathcal{P}$ and cutting out those that lead to an unbounded $L_f(\mathcal{P})$, i.e.

$$\hat{\mathcal{P}}_c := \mathcal{P} \setminus \bigcup_{\mathcal{Q}\subseteq\mathcal{P} \,:\, L_f(\mathcal{Q})\to\infty} \mathcal{Q}. \tag{6}$$

A possible way of systematically investigating the parameter space is using a recursive bisection algorithm.

Algorithm 1. ($\mathcal{Q}^* = Outer - approximate(\mathcal{M}_f, \mathcal{Q})$).
if $L_f(\mathcal{Q})$ *is unbounded*
  then **return** $\mathcal{Q}^* = \emptyset$
  else if $volume(\mathcal{Q}) \leq precision\ threshold\ \delta$
    then **return** $\mathcal{Q}^* = \mathcal{Q}$
    else *partition* $\mathcal{Q}$ *into* $\mathcal{Q}_1$ *and* $\mathcal{Q}_2$,
      i.e. $\mathcal{Q}_1 \cup \mathcal{Q}_2 = \mathcal{Q}$ *and* $\mathcal{Q}_1 \cap \mathcal{Q}_2 = \emptyset$
      $\mathcal{Q}_1' := Outer - approximate(\mathcal{Q}_1)$
      $\mathcal{Q}_2' := Outer - approximate(\mathcal{Q}_2)$
      return$\mathcal{Q}^* = \mathcal{Q}_1' \cup \mathcal{Q}_2'$
  fi
fi

In Figure 1 the outcome of Algorithm 1 is depicted. The quality of the outer-approximation is directly dependent on the chosen precision threshold δ, whereas a decrease of δ results of course in an increase of computational effort.

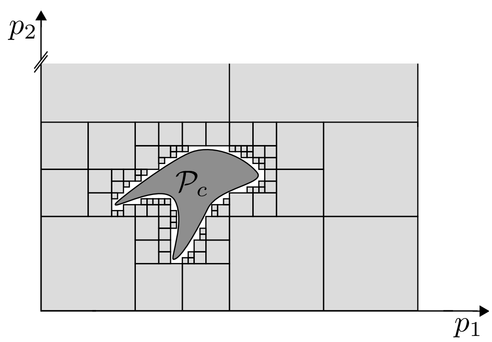

Fig. 1. Result of the outer-approximation algorithm for a consistent parameter region $\mathcal{P}_c$ (dark gray area). Light gray areas do not contain consistent parameterizations.

Note that in the case when the applied solver is not well tuned, e.g. the solution is not converging fast enough and the number of allowed iterations is too low, it might also be necessary to implement this algorithm for proving inconsistency.

6. FAULT DIAGNOSIS ALGORITHM

In the previous section, we have shown, that the set of parameters $\mathcal{P}_c$ leading to a consistent behavior of a model

$\mathcal{M}_f$ can be approximated. In this section we want to show how the parameter estimation algorithm can be extended to a complete fault diagnosis algorithm. As a first step we have to introduce a way of dividing the measurement collections $\mathcal{Y}$ and $\mathcal{W}$ into subsequences. This derives from Borchers et al. [2009], but is used here for formalizing the fault diagnosis algorithm and not only for reducing the computational complexity.

We split the collection of measurements $\mathcal{Y}$ and $\mathcal{W}$ into smaller collections

$$\mathcal{S} = \{\mathcal{S}^j \subseteq \mathcal{Y}, j = 1, \ldots, n_{\mathcal{S}}\} \tag{7}$$

with a corresponding shortened time window $T_j \subseteq T$ as depicted in Figure 2.

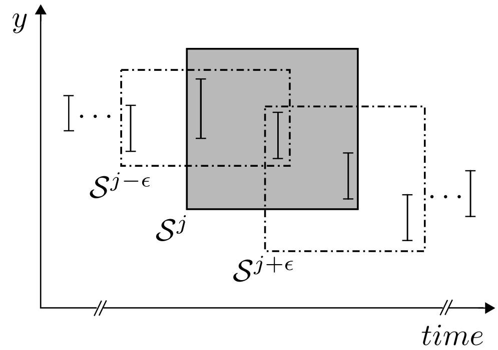

Fig. 2. Split collection of measurements.

The consistent parameters $\mathcal{P}_c$ can then be bounded by intersecting the estimates obtained for each individual subsequence, i.e.

$$\mathcal{P}_c \subseteq \bigcap_{j=1\ldots n_{\mathcal{S}}} \hat{\mathcal{P}}_c^j, \tag{8}$$

where $\hat{\mathcal{P}}_c^j$ denotes the result of Algorithm 1 for one subsequence j. A direct consequence is of course that a model $\mathcal{M}_f$ can only be consistent with the measurements if for all subsequences $\mathcal{S}^j$ a non-empty consistent parameter set $\hat{\mathcal{P}}_c^j$ can be found.

Hence it is sufficient to prove that one subsequence leads to the empty set. In the case that only one subsequence is considered the detectability of a fault consequently depends on the size of the regarded subsequence.

If we now specify the starting point of a shortened time-window with k and the length of the time-window with j, the fault diagnosis is given by

Algorithm 2. ($\hat{\mathcal{F}}$ =*Fault-Diagnosis*$(\mathcal{F}, k, j)$).
initialize $\hat{\mathcal{F}} = \mathcal{F}$
if $Fault-Detection(\mathcal{M}_{f_0}, k, j) ==$ **false**
  then $\hat{\mathcal{F}} = \hat{\mathcal{F}} \setminus f_0$
    display *a fault has occurred* fi
for $f_i \in \hat{\mathcal{F}}$
  if $Fault-Detection(\mathcal{M}_{f_i}, k, j) ==$ **false**
    then $\hat{\mathcal{F}} = \hat{\mathcal{F}} \setminus f_i$ fi
end
return $\hat{\mathcal{F}}$

function $consistent = Fault-Detection(\mathcal{M}_f, k, j)$
$\mathcal{Q} := Outer-approximate(\mathcal{M}_f, \mathcal{P})$
if $\mathcal{Q} == \emptyset$ then **return** $consistent =$ **false** fi
if $\mathcal{Q} \subseteq \mathcal{P}$ then **return** $consistent =$ **true** fi

Theorem 2. Algorithm 2 is a complete fault diagnosis algorithm, since the true fault f^* is never excluded from the initial fault set $\mathcal{F}$, i.e. $f^* \in \hat{\mathcal{F}}$.

The completeness of Algorithm 2 results directly from Theorem 1. If we consider an initial fault set $\mathcal{F}$ a fault f will only be excluded if and only if $F_f(\mathcal{P})$ is infeasible. At the same time $\mathcal{M}_f$ might be considered as consistent due to the relaxation, even though $F_f(\mathcal{P})$ does not admit a solution. In other words if we denote the best possible diagnostic result as $\mathcal{F}^*$ then

$$\mathcal{F}^* \subseteq \hat{\mathcal{F}}.$$

7. EXAMPLE

In this section we will show the applicability of our method considering the simple two-tank system as described in Blanke et al. [2006] and depicted in Figure 3.

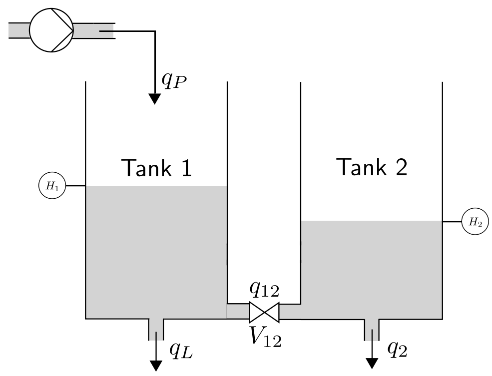

Fig. 3. Two-tank system.

We only consider the case that H_1, H_2 are measurable, because, as demonstrated in Blanke et al. [2006], measuring only one of the heights results in a loss of diagnosability.

7.1 System description

The system consists of two tanks connected by a valve, an inflow q_P, an outflow q_2 and a possible leakage q_L. H_1, H_2 denote the measured water-levels. the maximum allowed height h_{max} for H_1 is reached q_P will be set to zero. All parameters are given in Table 1 and are taken from Blanke et al. [2006]. We assume for reasons of simplicity in the remainder of this work that under operating conditions the fill level H_1 will always be greater or equal to H_2. If one would want to incorporate the case that $H_1 < H_2$ than one could apply a strategy similar to Hasenauer et al. [2009] by adding some discrete switching conditions. A mathematical description of the system is then given by the following nonlinear differential equations

$$\dot{H}_1(t) = \frac{1}{A}(q_P(t) - q_L(t) - q_{12}(t)), \tag{9}$$

$$\dot{H}_2(t) = \frac{1}{A}(q_{12}(t) - q_2(t)), \tag{10}$$

with

$$q_p(t) = \begin{cases} \bar{q}_p, & H_1(t) \leq h_{max}, \\ 0, & H_1(t) > h_{max}, \end{cases} \quad (11)$$

$$q_L(t) = \begin{cases} c_L\sqrt{H_1(t)}, & H_1(t) > 0, \\ 0, & H_1(t) \leq 0, \end{cases} \quad (12)$$

$$q_{12}(t) = \begin{cases} c_{12}\sqrt{H_1(t) - H_2(t)}, & V_{12} \text{ is open}, \\ 0, & V_{12} \text{ is closed}, \end{cases} \quad (13)$$

$$q_2(t) = \begin{cases} c_2\sqrt{H_2(t)}, & H_2(t) > 0, \\ 0, & H_2(t) \leq 0. \end{cases} \quad (14)$$

The equations (12)-(14) contain non-polynomial parts, therefore, we extend the model with three additional states and three additional constraints

$$\Delta H^2(t) = H_1(t) - H_2(t), \quad (15)$$

$$H_1^2(t) = H_1(t)H_1(t), \quad (16)$$

$$H_2^2(t) = H_2(t)H_2(t). \quad (17)$$

This approach of approximating the nonlinearities might not be suited for other nonlinearities (e.g. exponential functions) or for other measurement setups. In such cases stricter constraints have to be applied, e.g. enveloping the nonlinearities by means of polynomial functions, for further details see Hasenauer et al. [2009].

As our method requires the considered models to be in discrete-time, we apply Euler discretization to the equations (12)-(14) with a step size of 2 seconds.

Table 1. Nominal parameters

Parameter:	Value:	Description:
A	$1.54 \cdot 10^{-2}\text{m}^2$	Area of both tanks
h_{max}	0.6m	Height of both tanks
u_{nom}	1	Nominal pump velocity
c_{12}	$6 \cdot 10^{-4}\text{m}^{5/2}\text{s}^{-1}$	Flow constant valve V_{12}
c_2	$2 \cdot 10^{-4}\text{m}^{5/2}\text{s}^{-1}$	Flow constant of the outflow
c_L	$2.6 \cdot 10^{-4}\text{m}^{5/2}\text{s}^{-1}$	Flow constant of the leakage
$\bar{q}_P$	$1.5 \cdot 10^{-4}\text{m}^3\text{s}^{-1}$	Flow constant of pump

7.2 Scenario and Setup

We study the presented approach in a series of simulation studies. To get a realistic setup the parameters are not assumed to be known a priori, but are first estimated following the algorithm proposed in Section 5. The considered case is depicted in Figure 4, we performed it by simulating the temporal evolution of the two states with two slightly different initial conditions for the lower and upper bound ($\underline{H}_1(0) = 0.275\text{m}, \underline{H}_2(0) = 0.0375\text{m}$, and $\overline{H}_1(0) = 0.325\text{m}, \overline{H}_2(0) = 0.0625\text{m}$). We also added to the bounds an additional absolute error of 1.2cm. The results of the parameter estimation are given in Table 2.

Table 2. Achieved parameter bounds

Parameter:	Lower bound:	Upper bound:
c_{12}	$5 \cdot 10^{-4}$	$7 \cdot 10^{-4}$
c_2	$1 \cdot 10^{-4}$	$3 \cdot 10^{-4}$
$\bar{q}_P$	$0.5 \cdot 10^{-4}$	$2.5 \cdot 10^{-4}$

In the following, we consider four different scenarios concerning the measurements. For this reason, let us consider the measurement collection $\mathcal{Y}^* := \{\mathcal{Y}_k = (H_1^k, H_2^k), 0 \leq k \leq 300\}$, with each measurement providing information on both states. If we split the measurement collection,

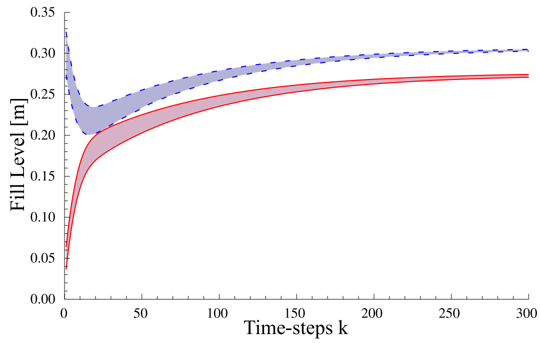

Fig. 4. Measurements taken of the two states from the faultless model. The red lines give the upper and lower bounds on the measurements of H_1 and the dashed blue lines the bounds on the measurements of H_2.

following (7), into subsequences $\mathcal{S}^j = \{\mathcal{Y}_j, \ldots, \mathcal{Y}_{j+\epsilon}\}$ with $\epsilon \in \{1, 2, 4, 9\}$, we can investigate how many time-steps after a fault f has occurred the fault can be detected/isolated. Two different fault scenarios are considered: First (f_1), the valve V_{12} gets stuck in the closed position or the flow through it is obstructed suddenly at time-step $k = 150$ (Figure 5) and second (f_2) the leakage q_L occurs at time-step $k = 50$ (Figure 6).

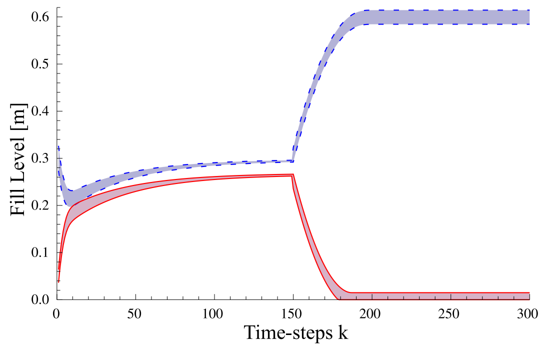

Fig. 5. Fault f_1 occurs on time step 150.

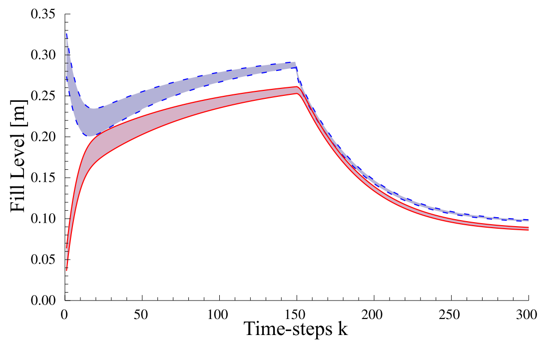

Fig. 6. Fault f_2 occurs on time step 150.

7.3 Simulation results

Table 3 shows the number of time-steps until a fault is detected and isolated. The number of considered measurements is apparently deciding the time necessary for detecting/isolating the fault. An interesting observation is that if only 2 measurements are considered at once, a detection of the second fault is not possible before the

Table 3. Necessary time steps

Fault:	Number of time-steps k:				Description of faults:
	$\epsilon = 1$	$\epsilon = 2$	$\epsilon = 4$	$\epsilon = 9$	
f_1	9	2	1	1	Valve V_{12} is closed
f_2	-	-	2	1	Tank 1 is leaking

new steady-state is reached. This implies that one has to carefully choose the amount of considered measurements. Also, as noted in Blanke et al. [2006], the detection of f_2 is more difficult then the detection of f_1. This seems to be a result of the less drastic change in the output measurements. In addition fault f_1 can still be detected when even larger errors in the measurements are assumed (results not shown). One can conclude that if the measurements would not allow a certain precision, i.e. the error is (very) large, a detection/isolation is not possible.

8. CONCLUSIONS AND OUTLOOK

We have studied in this contribution fault diagnosis for a quite general class of process control models. Based on an existing set-based parameter estimation, we proposed a solution method to the fault detection and isolation problems that is complete under the closed-world assumption. The method furthermore provides conclusive results even if the measurements and the model parameters admit uncertainties. We demonstrated for the well-known two tank example, that our approach is capable of determining which of the considered fault situations are exhibited by the plant.

For the considered class of uncertain polynomial/rational systems we were able to show that the fault detection/isolation tasks can be reformulated as a non-convex feasibility problem. Additionally, we have shown that it is sufficient to address a relaxed convex version of this feasibility problem and still achieve conclusive results. With the help of this so-called semidefinite program we could derive an efficient algorithm for fault diagnosis. This algorithm is complete since the true fault is never excluded from the set of fault candidates. Furthermore, we proposed a method for reducing the computational complexity.

In practice, even with the proposed reduction technique, the number of resulting problems might be too large for very complex processes, especially if the direct diagnosability of the faults cannot be guaranteed. A combination of the method with a state prediction scheme could then be used to limit the number of fault models which has to be addressed simultaneously. For instance, if more than one fault model is consistent with the measurements a investigation of the reachable state sets for all models could help discarding models as soon as the next measurement arrives and thus reducing immediately the number of possible fault situations. Such a prediction could also be used for finding a specific input sequence that allows to discriminate fault alternatives (active diagnosis). Both extensions will be subject of future work. Furthermore, it might be possible to extend the proposed framework to continuous-time models as shown in Lasserre et al. [2008].

REFERENCES

J. Aßfalg and F. Allgöwer. Fault diagnosis with structured augmented state models: modeling, analysis, and design. In *Proc. of IEEE Conf. on Dec. and Contr., CDC'06*, pages 1165–1170, San Diego, USA, 2006.

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer, 2nd edition, 2006.

J. Blesa, Y. Bolea, and Y. Puig. Robust fault detection using interval LPV models. In *Proc. of IEEE Eur. Contr. Conf., ECC'07*, pages 1618–1625, Kos, Greece, 2007.

S. Borchers, P. Rumschinski, S. Bosio, R. Weismantel, and R. Findeisen. A set-based framework for coherent model invalidation and parameter estimation of discrete time nonlinear systems. In *Proc. IEEE Conf. on Dec. and Contr., CDC '09*, pages 6786–6792, Shanghai, China, 2009.

C. Combastel and S. A. Raka. A set-membership fault detection test with guaranteed robustness to parametric uncerties in continuous time linear systems. In *Proc. of IFAC Symp. on Fault Det., Superv. and Saf. of Techn. Proc., SAFEPROCESS'09*, pages 1192–1197, Barcelona, Spain, 2009.

S. X. Ding. *Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*. Springer, 2008.

J. Gertler. *Fault Detection and Diagnosis in Engineering Systems*. Marcel Dekker, New York, 1998.

J. Hasenauer, P. Rumschinski, S. Waldherr, S. Borchers, F. Allgöwer, and R. Findeisen. Guaranteed steady-state bounds for uncertain chemical processes. In *Proc. Int. Symp. Adv. Contr. of Chem. Proc., ADCHEM'09*, pages 674–679, Istanbul, Turkey, 2009.

R. Isermann. *Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance*. Springer, 2006.

L. Kuepfer, U. Sauer, and P. A. Parrilo. Efficient classification of complete parameter regions based on semidefinite programming. *BMC Bioinformatics*, 8:12, 2007.

J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. on Optimization*, 11(3):796–817, 2001.

J.B. Lasserre, D. Henrion, C. Prieur, and E. Trelat. Nonlinear optimal control via opccupation measures and lmi relaxations. *SIAM J. on Contr. and Opt.*, 47:1643–1666, 2008.

P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Math. Program.*, 96(2):293–320, 2003.

P. Planchon. *Guaranteed diagnosis of uncertain linear systems using state-set observation*. Logos-Verlag, 2007.

M. V. Ramana. *An algorithmic analysis of multiquadratic and semidefinite programming problems*. PhD thesis, John Hopkins University, 1994.

R. R. Selmic, M. M. Polycarpou, and T. Parisini. Actuator fault detection in nonlinear uncertain systems using neural on-line approximation models. *Eur. J. of Control*, 15(1):29–44, 2009.

J.F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Opt. Meth. and Soft.*, 11(1):625–653, 1999.

D. Theilliol, J.-C. Ponsart, M. Rodrigues, S. Aberkane, and J. Yamé. Design of sensor fault diagnosis method for nonlinear systems described by linear polynomial matrices formulation: application to a winding machine. In *Proc. of IFAC World Congress*, pages 1890–1895, Seoul, Korea, 2008.

S. Tornil, T. Excobet, and L. Trave-Massuyes. Robust fault detection using interval methods. In *Proc. of IEEE Eur. Contr. Conf., ECC'03*, Cambridge, United Kingdom, 2003.

G. Videau, R. Raissi, and A. Zolghadri. Set-observer design for consistency checks of nonlinear systems. In *Proc. of Symp. of Fault Det., Superv. and Saf. of Tech. Proc., SAFEPROCESS'09*, pages 1210–1215, Barcelona, Spain, 2009.

S. Waldherr, R. Findeisen, and F. Allgöwer. Global sensitivity analysis of biochemical reaction networks via semidefinite programming. In *Proc. of IFAC World Congress*, pages 9701–9706, Seoul, Korea, 2008.

X. Zhang, M. M. Polycarpou, and T. Parisini. A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems. *IEEE Trans. on Autom. Control*, 47(4):576–593, 2002.

Y. Zhang, N. E. Wu, and B. Jiang. Fault detection and isolation applied to a ship propulsion benchmark. In *Proc. of IFAC World Congress*, pages 1908–1913, Seoul, Korea, 2008.