Proceedings of the 18th World Congress
The International Federation of Automatic Control
Milano (Italy) August 28 - September 2, 2011

Fault Diagnosis for Polynomial Hybrid Systems

Anton Savchenko [*,1] Philipp Rumschinski [*,1]
Rolf Findeisen [*,**]

[*] *Institute of Automation Engineering, Otto-von-Guericke University, Magdeburg, Germany.*
[**] *Corresponding author (e-mail: rolf.findeisen@ovgu.de)*

Abstract: Safety requirements of technological processes trigger an increased demand for elaborate fault diagnosis tools. However, abrupt changes in system behavior are hard to formulate with continuous models but easier to represent in terms of hybrid systems. Therefore, we propose a set-based approach for complete fault diagnosis of hybrid polynomial systems formulated as a feasibility problem. We employ mixed-integer linear program relaxation of this formulation to exploit the presence of discrete variables. We improve the relaxation with additional constraints for the discrete variables. The efficiency of the method is illustrated with a simple two-tank example subject to multiple faults.

Keywords: Estimation and fault detection; Parameter estimation based methods for FDI; Process control applications.

1. INTRODUCTION

The goal of fault diagnosis is to isolate possible faults that have occurred in a system, given some measured information. This knowledge can then be used either for monitoring and safety purposes, or for changing the control scheme that will counteract the impact of the faults. An introduction to the most common fault diagnosis approaches can be found in Blanke et al. [2006], Ding [2008], Gertler [1998], Isermann [2006]. Although physical processes are mostly continuous, a system might also possess discrete changes in its dynamics, e.g. due to a fault, phase changes, flow limitation through a valve or discontinuous input signals (Branicky et al. [1998]). In many cases such processes are described in terms of *hybrid systems* (Hofbaur and Williams [2004]).

We focus in this work on *model-based* fault diagnosis methods for such hybrid systems. These methods are typically based on *consistency tests*, which compare measurement data with the capability of a model to reproduce those measurements. The goal is to determine the set of models that are consistent with the measurements. We refer to this set also as *fault candidates.* Typically, those fault candidates are determined by excluding all fault models that are not consistent with the observations. Assuming the initial set of fault candidates describes all possible faults that can occur, a fault diagnosis method is said to be *complete* if the true fault is never excluded from the fault candidates. In practice, this does not necessarily lead to a single fault candidate due to some overlap in the input-output behavior of the considered fault models.

In literature there are several model-based fault diagnosis methods available for hybrid systems. For instance, in Bayoudh et al. [2008] a state tracking algorithm was employed. An observer-based approach was presented in Narasimhan and Biswas [2007] and a stochastic hypothesis testing based method in Fourlas et al. [2003].

In this contribution we present a set-based approach for polynomial hybrid systems. The proposed approach extends Rumschinski et al. [2010], where the fault diagnosis task is formulated in terms of a nonlinear feasibility problem and relaxed to a convex semidefinite program. The main advantages of such a formulation are the incorporation of uncertainty as for instance resulting from noise or model-plant mismatch and the achievable rigorous proof of model inconsistency. To be able to account for hybrid phenomena as e. g. non-smooth or discontinuous dynamics, we introduce integer switches into the feasibility formulation of Rumschinski et al. [2010]. Furthermore, we propose an aggregate model formulation for faults that affect only subsystems to reduce possible redundancy in the system formulation of different faults. In contrast to the semidefinite relaxation used in our previous work, here we employ linear relaxations that allow us to consider larger systems due to the effective use of mixed-integer linear solvers (e. g. Gur [2010]). In addition, we comment on the relaxation gaps in connection to the discrete variables, which in some special cases are less conservative than the ones with continuous variables.

2. PROBLEM SETUP

Given a process we consider discrete time hybrid models $\mathcal{M}_f$ that correspond to specific system faults

$$f \in \mathcal{F} = \{f_0, \dots, f_{n_f}\},$$

where f_0 is associated with the nominal system (faultless case). The behavior of these systems is described by polynomial or rational difference equations of the form

[1] The researchers were supported in part by the International Max Plank Research School, Magdeburg.

$$\mathcal{M}_f : \begin{cases} G_f(x_{k+1}, x_k, w_k, p) = 0, \\ H_f(y_k, x_k, w_k, p) = 0. \end{cases} \tag{1}$$

Here $x_k \in \mathbb{R}^{n_x} \times \mathbb{Z}^{d_x}$ denotes the system states, $p \in \mathbb{R}^{n_p} \times \mathbb{Z}^{d_p}$ the model parameters and $w_k \in \mathbb{R}^{n_w} \times \mathbb{Z}^{d_w}$, $y_k \in \mathbb{R}^{n_y} \times \mathbb{Z}^{d_y}$ denote the measured input and output respectively. This notation is used to allow for both continuous variables and discrete variables in the model formulation.

We assume that models corresponding to all faults in $\mathcal{F}$ are known. Additionally, the measurements are assumed to be unknown-but-bounded and their real subspaces to be given as convex sets so that measurement uncertainties can be taken into account. We collect them in the form

$$\mathcal{Y} = \{\ \mathcal{Y}_k \ \subset \mathbb{R}^{n_y} \times \mathbb{Z}^{d_y},\ \ k \in T\},$$
$$\mathcal{W} = \{\ \mathcal{W}_k \ \subset \mathbb{R}^{n_w} \times \mathbb{Z}^{d_w},\ k \in T\}$$

within a certain time window $T = \{t_0, t_1, \ldots, t_e\}$. This time window denotes the time instances when the measurements were taken.

The method for fault diagnosis that we employ checks consistency of the models with the measurement data. We formalize the notion of consistency in the following way:

Definition 1. (Consistency). Consider the collection of measurements $\mathcal{W}$ of the applied input and the measurements $\mathcal{Y}$ 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 $y_k \in \mathcal{Y}_k$ for all $k \in T$.

With Definition 1 we can state the following:

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

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

2.1 Aggregated Model

For numerous systems that occur in practice the expressions G_f that correspond to different faults are quite similar. We can reduce this redundancy in formulation (1) by merging the models using a set of integer variables that correspond to each of the faulty scenarios. Formally speaking we introduce one model of the form

$$\mathcal{M} : \begin{cases} G(x_{k+1}, x_k, w_k, p, s) = 0, \\ H(y_k, x_k, w_k, p, s) = 0, \end{cases} \tag{2}$$

where the variables x_k, w_k, y_k and p are as defined before, and the variables $s \in \mathbb{Z}^{d_s}$ correspond to the faults that occur in the model. Namely, we introduce a set

$$\mathbb{S} = \{s_f \in \mathbb{Z}^{d_s} \mid f \in \mathcal{F}\},$$

such that for every system fault $f \in \mathcal{F}$ the following holds

$$G(x_{k+1}, x_k, w_k, p, s_f) = G_f(x_{k+1}, x_k, w_k, p),$$
$$H(y_k, x_k, w_k, p, s_f) = H_f(y_k, x_k, w_k, p).$$

Hence, every model $\mathcal{M}_f$ is represented by the system (2) when the variable s is set to s_f.

2.2 Feasibility Problem Formulation

Next we formulate Proposition 1 and Proposition 2 as nonlinear feasibility problems. The goal of the fault detection problem is to show that under the allowed variations of system parameters the measurements are not reproducible by the model $\mathcal{M}_{f_0}$.

As in Rumschinski et al. [2010], we introduce a set of semialgebraic equations, that represent the system in terms of the equations (2):

$$F(\mathcal{S}) : \begin{cases} G(x_{k+1}, x_k, w_k, p, s) = 0, & k \in T, \\ H(y_k, x_k, w_k, p, s) = 0, & k \in T, \\ \ p \ \in \mathcal{P}, \quad s \ \in \mathcal{S}, & \\ w_k \ \in \mathcal{W}_k,\ y_k \ \in \mathcal{Y}_k, & k \in T, \\ x_k \ \in \mathcal{X}_k, & k \in T \cup \{t_{e+1}\}, \end{cases}$$

where $\mathcal{P}$, $\mathcal{X}_k$ denote given sets with convex real subspaces, bounding the parameters and the states, respectively.

Remark 1. These bounds can be either derived from the physical meaning of the parameters and states, or from conservation principles. Theoretically, the bounds can be arbitrary large, but tighter bounds are preferable in practice for the employed relaxation procedure that will be explained in the following section.

The set $\mathcal{S} \subset \mathbb{Z}^{d_s}$ denotes a collection of admissible values for the variables s and the feasibility problem is formulated as the problem of checking whether $F(\mathcal{S})$ admits a solution with $s = s_f$ for model $\mathcal{M}_f$. Naturally, the value s_f has to be included in $\mathcal{S}$ to do so.

Theorem 1. If the feasibility problem does not admit a solution for $s = s_f$, then the model $\mathcal{M}_f$ is inconsistent with the measurements $\mathcal{Y}$, $\mathcal{W}$.

The proof follows directly from the construction of $F(\mathcal{S})$.

Using Theorem 1 we can formulate fault detection and fault isolation in the following way.

Proposition 3. (Fault detection/isolation). If $F(\mathcal{S})$ does admit a solution with $s = s_f$, the fault f is a fault candidate, i.e. $\mathcal{M}_f$ is consistent with the measurements.

Remark 2. For fault detection it suffices to set $\mathcal{S} = \{s_{f_0}\}$ and check if $F(\mathcal{S})$ admits a solution or not. However if we include all values s_f corresponding to the models $\mathcal{M}_f$ (i. e. $\mathbb{S} \subseteq \mathcal{S}$), we can check consistency of every faulty model once we obtain the projection of the feasible region of $F(\mathcal{S})$ onto the subspace $\mathbb{Z}^{d_s}$.

Remark 3. The variables s in this formulation are time-invariant, so our method will not be suited for fault isolation in cases when the measurement data are taken both before and after the fault occurs. Even though in this situation we still can detect the appearance of the fault, isolation is in general only possible if all of the employed measurements correspond to the same faulty case.

In practice it is not always possible to determine an exact solution of the feasibility problem $F(\mathcal{S})$, due to the nonlinearities of the model equations. However, 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 3. Note that as a consequence of the relaxation the fault candidates will be determined by elimination of all other possibilities.

3. PROBLEM RELAXATION

For the considered system class it is possible to relax $F(\mathcal{S})$ into a convex semidefinite or linear program Fujie and Kojima [1997], Lasserre [2001], Parrilo [2003]. Although in Rumschinski et al. [2010] the semidefinite formulation was employed for fault diagnosis, we propose here the use of a mixed-integer linear relaxation. The linear relaxation allows us to handle significantly larger problems than the semidefinite formulation, besides efficient mixed-integer linear solvers are available nowadays (i. a. Gur [2010]). For a comparison of continuous variables in LP and SDP relaxations for polynomial programs we refer to Anstreicher [2009] and handling of discrete variables will be addressed in Section 4. 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 $F(\mathcal{S})$ is rewritten in form of a mixed-integer quadratic feasibility problem ($MIQP$). Therefore, we introduce a vector $\xi \in \mathbb{R}^{n_\xi}$, consisting of a minimal basis of monomials of the model and output equations (2), in the form

$$\xi_i \in \{1,\ x_j,\ p_l,\ w_m,\ y_n,\ s_r,\ x_jp_l,\ x_jw_m,\ \ldots\},$$
$$I_\xi \subseteq \{1,\ldots,n_\xi\},\ \xi_{I_\xi} \in \mathbb{Z}^{d_\xi},$$

where indices j,l,m,n,r correspond to the respective number of states x, parameters p, inputs w, outputs y and model variables s. We treat the products of the discrete variables as discrete entries of ξ, whereas products of the continuous variables, as well as mixed products, are treated as continuous entries.

Using the vector ξ, equations (2) can be transformed to

$$\mathcal{M}: \begin{cases} G_i(x_{k+1},x_k,w_k,p,s) = \xi^T Q_k^i \xi = 0, \\ H_j(y_k,x_k,w_k,p,s) = \xi^T Q_k^{j+n_G} \xi = 0, \end{cases} \qquad (3)$$

where $Q_k^i \in \mathbb{R}^{n_\xi \times n_\xi}$ is a symmetric matrix and the range of index i corresponds to the number of equations $n_G + n_H$. Apart from that, if ξ contains n_A higher order terms (products of first degree monomials), n_A additional equality constraints of the form (3) have to be introduced.

To simplify the notation we define the range of index i such that it covers the number of equations (2) as well as the number of additional constraints, i. e.

$$i \in \mathcal{I} = \{1,\ldots,n_G+n_H+n_A\}.$$

The bounds that describe the subsets $\mathcal{P}$, $\mathcal{S}$, $\mathcal{X}_k$, $\mathcal{W}_k$, $\mathcal{Y}_k$ in $F(\mathcal{S})$ can be formulated as linear constraints

$$B\xi \geq 0.$$

In the most trivial case $B \in \mathbb{R}^{2(n_\xi-1)\times n_\xi}$ provides explicit upper and lower bounds on all components of ξ except for the first one. However, one can employ any valid constraint that is linear in the basis ξ.

Then the feasibility problem $F(\mathcal{S})$ can be rewritten as

$$MIQP(\mathcal{S}): \begin{cases} \text{find} & \xi \in \mathbb{R}^{n_\xi} \\ \text{subject to} & \xi^T Q_k^i \xi = 0,\ i \in \mathcal{I}, k \in T, \\ & \xi_1 = 1, \\ & B\xi \geq 0, \\ & \xi_{I_\xi} \in \mathbb{Z}^{d_\xi}. \end{cases}$$

Such a quadratic decomposition can always be found for a polynomial/rational system (2), although its continuous relaxation is still not convex. We obtain a convex semidefinite program (with non-convex integrality constraints) by introducing the variable matrix $X = \xi\xi^T$ and relaxing the conditions $rank(X) = 1$ and $tr(X) \geq 1$ with the weaker constraint $X \succeq 0$, see e. g. Parrilo [2003]. To simplify the notation we will denote the space of the matrix variable X as $\mathbb{X} \subset \mathbb{R}^{n_\xi \times n_\xi}$, where entries that correspond to the products of the discrete variables of ξ will be treated as discrete variables.

The semidefinite program is then represented as

$$SDP(\mathcal{S}): \begin{cases} \text{find} & X \in \mathbb{X} \\ \text{subject to} & tr(Q_k^i X) = 0, \quad i \in \mathcal{I}, k \in T, \\ & tr(ee^T X) = 1, \\ & BXe \geq 0, \\ & BXB^T \geq 0, \\ & X \succeq 0, \end{cases}$$

where $e = (1,0,\ldots,0)^T \in \mathbb{R}^{n_\xi}$.

Remark 4. Due to the relaxation the solution space will increase compared to $F(\mathcal{S})$ which might lead to the wrong inclusion of a faulty model in the fault candidate set. However, as the relaxation is conservative, the true fault will never be excluded from the fault candidates. Additionally, the introduction of the constraints $BXB^T \geq 0$ aims at reducing this conservatism (see Lasserre [2001]).

The mixed-integer linear relaxation of the SDP program is obtained by substituting the constraint $X \succeq 0$ with $X \geq 0$. After the relaxation of the SDP-constraint the mixed-integer linear program is formulated as

$$MILP(\mathcal{S}): \begin{cases} \text{find} & X \in \mathbb{X} \\ \text{subject to} & tr(Q_k^i X) = 0, \quad i \in \mathcal{I}, k \in T, \\ & tr(ee^T X) = 1, \\ & BXe \geq 0, \\ & BXB^T \geq 0, \\ & X \geq 0. \end{cases}$$

As stated in Theorem 1, we are interested in proving infeasibility of $F(\mathcal{S})$. An efficient approach in this case is to consider the dual formulation $D(\mathcal{S})$ of the mixed-integer relaxation:

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

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

Theorem 2. If the dual program $D(\mathcal{S})$ is unbounded, then for all faults f with $s_f \in \mathcal{S}$, $\mathcal{M}_f$ is inconsistent with the measurements.

The weak-duality theorem and the relaxation process guarantee that if the dual program is unbounded, then $F(\mathcal{S})$ does not admit a solution.

4. REDUCING THE RELAXATION ERROR FOR INTEGER VARIABLES

The relaxation technique, introduced in the previous section, allows us to approximate the non-convex feasibility problem $F(\mathcal{S})$ with another type of problem (either semidefinite or linear), that is non-convex only due to the integrality conditions. These can be efficiently solved with the help of mixed-integer solvers, so we are able to find globally optimal solutions. However, those solutions will not always be feasible for $F(\mathcal{S})$. By relaxing non-convex constraints we introduce "spurious" solutions, that are valid for the modified problem, but violate the nominal model constraints.

As mentioned in Remark 4, the SDP formulation can be strengthened with the constraint $BXB^T \geq 0$ that originates from the reformulation-linearization technique Sherali and Adams [1999]. The effect of this strengthening was studied for the continuous case in Anstreicher [2009]. We now employ a similar notation to study the effect of additional constraints, that can be introduced to both SDP and $MILP$ relaxations due to the presence of the discrete variables in our system. We concentrate on binary ($\{0,1\}$) variables as they represent the most common type of discrete variables, that can be employed to model fault switches and discontinuity of the models.

Notice, that we only relax equalities of the type

$$X_{ij} = \xi_i \xi_j \tag{4}$$

for the matrix X, written in form of the $rank$ constraint

$$rank(X) = 1.$$

In case of the SDP formulation we relax the constraint to $X \succeq 0$, and for $MILP$ it is further relaxed to $X \geq 0$.

Lemma 1. For $MILP$ and SDP formulations the relaxation error for the elements of X that involve binary variables can be avoided.

Proof. We show that equality (4) can be reformulated via a set of linear constraints if ξ_i or ξ_j is binary. As equality (4) only affects pairs of variables ξ_i, ξ_j, we can restrict ourselves to submatrices of X of size 3×3. Larger matrices will not provide any additional information for strengthening the relaxation:

$$rank \begin{pmatrix} 1 & \xi_2 & \xi_3 \\ \xi_2 & X_{22} & X_{23} \\ \xi_3 & X_{23} & X_{33} \end{pmatrix} = 1. \tag{5}$$

Depending on the number of binary variables in (5), two cases are possible. The first case, when ξ_2 and ξ_3 are both binary variables, leads to the following additional constraints:

$$\begin{cases} X_{ij} \in \{0,1\}, & \forall i,j \in \{2,3\}, \\ X_{ii} = \xi_i^2 = \xi_i, & \forall i \in \{2,3\}, \\ X_{23} = \xi_2\xi_3 = min\{\xi_2, \xi_3\}, & \end{cases} \tag{6}$$

where the last equation can be represented via the following set of linear inequalities:

$$\begin{cases} X_{23} \leq \xi_2, \\ X_{23} \leq \xi_3, \\ X_{23} \geq \xi_2 + \xi_3 - 1. \end{cases} \tag{7}$$

As the introduced constraints (6) can be written in linear form using (7), the lemma holds for this case. Namely, any combination of binary variables that satisfies (6) will automatically satisfy the $rank$ constraint (5).

Without loss of generality we consider as the second case the case when ξ_2 is binary and ξ_3 continuous. The set of additional constraints is

$$\begin{cases} X_{22} \in \{0,1\}, \\ X_{22} = \xi_2, \\ X_{23} \leq u_3\xi_2, \\ X_{23} \geq l_3\xi_2, \\ X_{23} \leq \xi_3 + (\xi_2 - 1)l_3, \\ X_{23} \geq \xi_3 + (\xi_2 - 1)u_3, \end{cases} \tag{8}$$

where $l_3 \leq \xi_3 \leq u_3$ are the bounds on the corresponding monomial of ξ. In this case we can not introduce additional constraints on the variable X_{33}, as it is the product of two continuous variables. So the $rank$ constraint (5) will not be satisfied by just adding (8) to the relaxation. Nevertheless, for any binary value of ξ_2 the constraints on X_{23} will be equivalent to (4), so we avoid its relaxation. Naturally, as in the previous case, the constraint on the variable X_{22} is also tight for any binary value of ξ_2. $\square$

Corollary 1. Aggregation of the faulty models $\mathcal{M}_f$ in form (2) does not introduce any additional relaxation error if all of the variables s are binary.

Remark 5. We should point out that the constraints are tight when integrality conditions are in place, but they do not represent convex hulls of the feasible points. Therefore, if one considers the linear relaxation with all the binary variables relaxed to continuous variables in $[0,1]$, fractional solutions might appear. We rely therefore on mixed-integer solvers, that can efficiently produce valid cuts if the linear relaxation of the mixed-integer problem produces infeasible result.

We showed that binary variables that appear in the system do not add relaxation errors for both semidefinite and mixed-integer linear relaxations of the initial feasibility problem. Also by merging the models (1) into one model (2) we do not increase conservatism of the obtained relaxation compared to the relaxation of each of the feasibility problems (as it was done in Rumschinski et al. [2010]).

5. EXAMPLE

In this section we illustrate the fault diagnosis method considering the simple two-tank system as described in Blanke et al. [2006] and depicted in Figure 1. We consider first the case when both H_1 and H_2 are measured and compare the result with the result from Rumschinski et al.

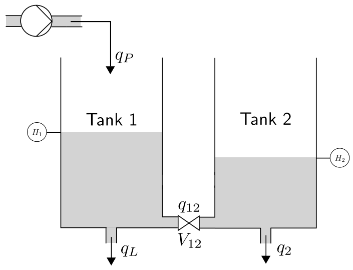

Fig. 1. Two-tank system.

[2010]. Secondly, we assume that one can only measure the outflow from the second tank and investigate the diagnosability of the obtained system.

5.1 System Description

The system consists of two tanks with the area $A = 1.54 \cdot 10^{-2}\text{m}^2$ 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. If the maximum allowed height $h_{max} = 0.6\text{m}$ for H_1 is reached, q_P will be set to zero. The switching conditions for differential equations are modeled using state-dependent binary variables. 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. Incorporating the case for $H_1 < H_2$ can be done with additional discrete switching conditions. We consider two fault scenarios, first when the valve V_{12} gets stuck in the closed position, and second when the leakage q_L occurs. These scenarios are embedded in the aggregated model using a pair of binary parameters $s \in \{0, 1\}^2$.

5.2 State Measurement Scenario

A mathematical description of the system is 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

$$\begin{aligned} q_P(t) &= \bar{q}_p d_p(t)(1 - \sqrt{H_1(t)/h_{max}}), \\ q_L(t) &= c_L d_L(t)\sqrt{H_1(t)}, \\ q_{12}(t) &= c_{12} s_1 \sqrt{H_1(t) - H_2(t)}, \\ q_2(t) &= c_2 d_2(t)\sqrt{H_2(t)}. \end{aligned} \tag{11}$$

The binary variables can be described in the following form

$$\begin{aligned} d_p(t) &= \begin{cases} 1, \ H_1(t) \le h_{max}, \\ 0, \ H_1(t) > h_{max}, \end{cases} & s_1 &= \begin{cases} 1, \ V_{12} \text{ open}, \\ 0, \ V_{12} \text{ closed}, \end{cases} \\ d_L(t) &= \begin{cases} s_2, \ H_1(t) > 0, \\ 0, \ \ H_1(t) \le 0, \end{cases} & s_2 &= \begin{cases} 1, \ \text{Tank 1 leaking}, \\ 0, \ \text{Tank 1 sealed}, \end{cases} \\ d_2(t) &= \begin{cases} 1, \ H_2(t) > 0, \\ 0, \ H_2(t) \le 0. \end{cases} \end{aligned}$$

that can be easily represented via a set of mixed-integer linear constraints.

Note that the equations (11) contain non-polynomial parts, that can be reformulated by introducing three additional states with constraints

$$\begin{aligned} \Delta H^2(t) &= H_1(t) - H_2(t), \\ SqrtH_1^2(t) &= H_1(t), \\ SqrtH_2^2(t) &= H_2(t), \end{aligned} \tag{12}$$

and placing $SqrtH_1$, $SqrtH_2$ and ΔH in (11) instead of the corresponding square root terms.

As our method requires usage of discrete-time models, we apply Euler discretization to the equations (9)–(10) with a step size of 1 second.

To get a realistic setup the parameters are not assumed to be known a priori but chosen to be bounded (see Table 1).

Table 1. Reference Parameter Values

Parameter [Unit]	Lower bound	Nominal value	Upper bound
c_{12} $[\text{m}^{5/2}\text{s}^{-1}]$	$5.75 \cdot 10^{-4}$	$6 \cdot 10^{-4}$	$6.25 \cdot 10^{-4}$
c_2 $[\text{m}^{5/2}\text{s}^{-1}]$	$1.75 \cdot 10^{-4}$	$2 \cdot 10^{-4}$	$2.25 \cdot 10^{-4}$
c_L $[\text{m}^{5/2}\text{s}^{-1}]$	$2.35 \cdot 10^{-4}$	$2.6 \cdot 10^{-4}$	$2.85 \cdot 10^{-4}$
$\bar{q}_P$ $[\text{m}^{5/2}\text{s}^{-1}]$	$4.25 \cdot 10^{-4}$	$4.5 \cdot 10^{-4}$	$4.75 \cdot 10^{-4}$

5.3 Output Measurement Scenario

The second setup relies on partial knowledge of the states of the system. We consider a measured signal proportional to the outflow q_2 and for simplicity we assume it to be the additional state $SqrtH_2(t) = \sqrt{H_2(t)}$. Additionally, we use the measured data to define the inflow q_P in the form

$$q_P(t) = \bar{q}_p d_p(t)(1 - \sqrt{H_2(t)/h_{max}}).$$

5.4 Experimental Setup

The simulation data employed for fault diagnosis was obtained using initial conditions $H_1(0) = 0.325\text{m}$ and $H_2(0) = 0.0625\text{m}$ for 300s with the stepsize 1s. Nominal parameter values were taken from the Table 1. An absolute error (5% of the maximal value of H_1 and H_2) was added to the states to simulate the output disturbances.

In the formulation (9)–(11) the nominal behavior of the system is described by setting the variables $s_{f_0} = \{1, 0\}$, i. e. when the valve V_{12} is open and the Tank 1 is not leaking. The fault scenarios are similarly represented by $s_{f_1} = \{0, 0\}$ for the stuck valve and $s_{f_2} = \{1, 1\}$ for the leaking tank. We set

$$S = \{s_{f_0}, s_{f_1}, s_{f_2}\}$$

and estimate admissible values of S considering sets of measurements taken at specific time ranges.

The faults are assumed to occur at time-step 150s (cf. Figure 2), and we perform the fault diagnosis procedure with the measurements taken right after this time-step. According to Remark 3, we cannot isolate the fault for the time range that includes measurements before and after this time step. We discuss a possible solution in Section 6.

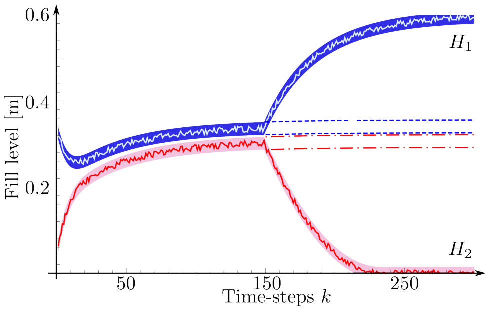

Fig. 2. Simulated measurements of the valve stuck at 150s. Dashed lines correspond to nominal case.

5.5 Computational Results and Discussion

State Measurement Scenario Taking measurements from the point 150s, we are able to uniquely diagnose the occurrence of the stuck valve fault considering 4 time-steps. The occurrence of the leakage in the first tank can be diagnosed with only 2 time-steps.

Although we used a slightly different experimental setup compared to Rumschinski et al. [2010], we showed that its results can be reproduced.

Output Measurement Scenario For the output measurement scenario the fault diagnosis is much harder. Due to the absence of the bounds on the water level of the first tank the measurement data are less informative. Both faults result in a decreasing water level of the second tank and these measurements alone can correspond to the nominal trajectory for some allowed parameter combination. It requires 9 time-steps to detect the occurrence of the stuck valve fault, but we were unable to uniquely diagnose it. To detect the leakage in the first tank we need 16 time-steps, although in this scenario we also discriminate the other fault and, hence, the diagnosis is unique.

Compared to the state measurement scenario the leakage is harder to detect here, as it mainly results in the drop of the water level in the first tank. On the other hand, the water level of the second tank decreases less steep compared to the stuck valve case, which makes it possible to distinguish between the two fault behaviors.

The above result shows that our method can be applied for the output measurement scenario, providing useful information on the faulty behavior of the system.

6. CONCLUSIONS AND OUTLOOK

In this contribution we have studied fault diagnosis for a class of hybrid systems. We extended the approach presented in Rumschinski et al. [2010] to handle discrete variables and to suppress model redundancy by aggregating the models corresponding to the different fault scenarios. 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 hybrid systems we were able to show that the fault detection/isolation tasks can be reformulated as a nonconvex feasibility problem. Additionally, we have shown that it is sufficient to address a relaxed version of this feasibility problem and still achieve conclusive results. A mixed-integer linear formulation was chosen because of highly efficient $MILP$-solvers that are available nowadays. We derived that the relaxation gaps can be avoided for binary variables present in the system formulation and hence the proposed aggregation of the models does not increase the conservatism of the relaxation.

Integer switches that are employed by our aggregation approach are treated as time invariant parameters. This prevents us from isolating the fault if it occurs within the considered time range, however, the fault detection is still possible for such a setup. One possible way to overcome this restriction is to employ time variant switches instead. The drawback of this solution lies in a significant increase of model variables leading to an increase of solving time.

The proposed linear relaxation is advantageous in terms of computation speed, but might be too conservative for a different class of hybrid systems. The presented semidefinite formulation is fully applicable with our method and the corresponding study should take place as soon as efficient mixed-integer semidefinite solvers are available.

REFERENCES

Gurobi optimizer 3.0 reference manual, 2010. URL `http://www.gurobi.com`.

M. Anstreicher. Semidefinite programming versus the reformulation-linearization technique for nonconvex quadratically constrained quadratic programming. *J. of Glob. Opt.*, 43(2-3):471–484, 2009.

M. Bayoudh, L. Travé-Massuyes, X. Olive, and T.A. Space. Hybrid systems diagnosis by coupling continuous and discrete event techniques. In *Proc. of the IFAC World Congress, Seoul, Korea*, pages 7265–7270, 2008.

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

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.

M.S. Branicky, V.S. Borkar, and S.K. Mitter. A unified framework for hybrid control: Model and optimal control theory. *IEEE Trans. on Auto. Contr.*, 43(1):31, 1998.

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

G.K. Fourlas, K.J. Kyriakopoulos, and N.J. Krikelis. Model based fault diagnosis of hybrid systems based on hybrid structure hypothesis testing. *J. of Appl. Sys. Studies*, 4(3), 2003.

T. Fujie and M. Kojima. Semidefinite programming relaxation for nonconvex quadratic programs. *J. of Glob. Opt.*, 10(4):367–380, 1997.

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

M.W. Hofbaur and B.C. Williams. Hybrid estimation of complex systems. *IEEE Trans. on Sys., Man, and Cybern., Part B*, 34(5):2178–2191, 2004.

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

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

S. Narasimhan and G. Biswas. Model-based diagnosis of hybrid systems. *IEEE Trans. on Sys., Man and Cyber., Part A*, 37(3):348–361, 2007.

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

P. Rumschinski, J. Richter, A. Savchenko, S. Borchers, J. Lunze, and R. Findeisen. Complete fault diagnosis of uncertain polynomial systems. In *Proc. 9th IFAC Symp. on Dyn. and Contr. of Process Sys., DYCOPS-9*, pages 127–132, Leuven, Belgium, 2010.

H.D. Sherali and W.P. Adams. *A reformulation-linearization technique for solving discrete and continuous nonconvex problems.* Kluwer Academic Publishers, 1999.