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

Structural Problem Reduction for Set-based Fault Diagnosis

Anton Savchenko, Philipp Rumschinski, Stefan Streif, Rolf Findeisen

Institute of Automation Engineering, Otto-von-Guericke University, Magdeburg, Germany

{anton.savchenko, philipp.rumschinski, stefan.streif, rolf.findeisen}@ovgu.de

Abstract:
Complex technical systems, e. g. chemical plants, are prone to equipment failures. To ensure the safe operation of such systems, the occurrence of a fault has to be reliably detected. Set-based validation and identification methods are well suited for this problem as they are flexible with respect to modeling uncertainties and as they can provide guaranteed results. One of the main challenges of set-based approaches is, however, the complexity of underlying computations. Simplifying the problem formulation via a suitable approximation of the model is one way to reduce the computational effort. However, to retain the ability to diagnose faults, the underlying structure of the model has to be taken into account. We present a method to reduce the problem formulation based on causal reasoning and lifting technique that orders the system states according to the effects of occurring faults. We present an approach to derive such a reduction and illustrate its application considering two 5-tank configurations.

Keywords: Estimation and fault detection; Problem reduction; Fault detection and isolation; Process control applications.

1. INTRODUCTION

Fault diagnosis is important to ensure a satisfactory and safe operation of complex technical processes in many application fields. In chemical plants, for instance, fault diagnosis can prevent failures or the shutdown of the complete plant or its parts. The task of fault diagnosis has been studied extensively in the last decades, surveys of commonly used detection and diagnosis methods can be found i. a. in (Patton et al., 1989; Blanke et al., 2006).

In addition to ease design and guaranteed diagnosis results, fault diagnosis approaches need to be robust against uncertainties. Furthermore, fault diagnosis methods have to be fast enough to be able to initiate counter measures in time. The increase of safety or precision requirements on process control typically leads also to an increase in the model complexity. Thus fault diagnosis becomes even more difficult. We propose a method to reduce the complexity of fault diagnosis within the set-based framework presented in (Rumschinski et al., 2010; Savchenko et al., 2011) for polynomial hybrid discrete-time systems.

The proposed reduction is related to two concepts that have been successfully employed in the context of fault diagnosis: *residual generation* and *causal relations*.

Residual generation, clearly a corner stone of model-based fault diagnosis, provides the criterion to decide whether a process behaves fault-free or faulty. In the simplest case this criterion (or *residual*) is a comparison of the measurements and the model output (Gertler, 1991). There are several methods available in literature to generate residuals appropriate for fault diagnosis. For instance, in (Frisk, 2000) a residual generator for polynomial systems based on elimination theory and Gröbner bases was proposed, see (Staroswiecki and Comtet-Varga, 2001) for a discussion of diagnosability issues related to polynomial systems. For a comparison of knowledge-based residuals and residuals derived from analytical redundancies see (Frank, 1990).

Causal relations are an abstract description of the influence of model variables, e. g. states and inputs, on other model variables (Fagarasan et al., 2004). There are basically two different approaches to define such relations, taking either the faulty model or the fault-free model as a point of reference. If the faulty system is considered, the faults are connected to observable changes in the system dynamics. For this reason, a model of the process is constructed that includes the relationship between a fault and its symptoms. Such a model is typically expressed as a fault-symptom tree and diagnosis consists of connecting the observed symptoms backwards to their possible causes. Alternatively, causal relations are defined starting with the nominal system behavior as for most classical diagnostic approaches. A structured way of building such relations was presented e. g. in (Heim et al., 2002). In (Aslund et al., 2011), diagnosability of continuous-time systems was investigated based on the concept of causal relations.

In this contribution, we present a problem reduction method for the set-based approach for polynomial hybrid discrete-time systems presented in (Rumschinski et al., 2010; Savchenko et al., 2011). The fault diagnosis task is formulated in terms of a nonlinear (mixed-integer) feasibility problem and relaxed into a convex semidefinite or linear program. The main advantages of such a formulation are the easy incorporation of unknown-but-bounded uncertainties as, for instance, resulting from noise

or model-plant mismatch, and rigorous proof of model inconsistency. The major drawback of the approach is the increasing computational effort for larger model sizes. To limit the needed effort to solve the diagnosis problem, we propose a procedure based on the concepts of causal reasoning and residual generation to reduce the size of the feasibility problem. At first, we determine the causal relations of the fault signatures and the model variables based on the model description. Then, using projections similar to residual generation, we define a smaller set of variables by aggregating the variables that are not needed to diagnose a specific fault. This approach differs from standard model reduction approaches, (Antoulas et al., 2001; Moore, 1981), since we employ the information on the states of the system in form of uncertain bounds instead of truncating (almost) unobservable/uncontrollable states. In principle, this procedure is an alternative relaxation based on the model structure. We illustrate the approach considering two 5-tank configurations and give a detailed comparison between the results achieved with the complete and reduced feasibility formulations.

2. FAULT DIAGNOSIS

Given a process subject to a number of abrupt faults, we consider an implicit discrete-time model of the form

$$M : \begin{cases} g(x(k+1), x(k), w(k), p, s) = 0, \\ h(y(k), x(k), w(k), p, s) = 0. \end{cases}$$

representing the faulty and nominal cases. 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, $w(k) \in \mathbb{R}^{n_w} \times \mathbb{Z}^{d_w}$ the measured inputs and $y(k) \in \mathbb{R}^{n_y} \times \mathbb{Z}^{d_y}$ the outputs. Note that all these variables can contain continuous and discrete parts. The time index is denoted by $k \in \mathbb{N}$.

The functions g and h represent the aggregated hybrid dynamics and the model output, respectively. The variable $s \in \mathbb{Z}^{d_s}$ links the models of all considered *fault scenarios* $\mathcal{F} = \{f_0, f_1, \ldots, f_{n_f}\}$, where f_0 corresponds to the faultless case. For each fault scenario the value $s = s_f$, $f \in \mathcal{F}$ provides a unique *fault signature*. We assume the functions g and h to be polynomial or rational. Note that other nonlinearities can be approximated by such functions to an arbitrary precision, see (Hasenauer et al., 2010) and references therein. Note also that we use here for notational simplicity an implicit discrete-time model formulation, however, considering instead explicit integration schemes is straightforward.

To account for process uncertainty, we assume the parameters p to be unknown-but-bounded, i. e. $p \in \mathcal{P} \subseteq \mathbb{R}^{n_p} \times \mathbb{Z}^{d_p}$. We also assume to have prior knowledge on the unknown-but-bounded states of the system derived from initial conditions, physical meaning of the states, or from conservation principles. Furthermore, the measurements are assumed to be unknown-but-bounded and we collect all information in the form

$$\begin{aligned} \mathcal{X} &= \{\ \mathcal{X}_k \subset \mathbb{R}^{n_x} \times \mathbb{Z}^{d_x}, t_k \in \mathcal{T}\}, \\ \mathcal{Y} &= \{\ \mathcal{Y}_k \subset \mathbb{R}^{n_y} \times \mathbb{Z}^{d_y}, t_k \in \mathcal{T}\}, \\ \mathcal{W} &= \{\, \mathcal{W}_k \subset \mathbb{R}^{n_w} \times \mathbb{Z}^{d_w}, t_k \in \mathcal{T}\}, \end{aligned}$$

within a certain time window $\mathcal{T} = \{t_0, t_1, \ldots, t_e\}$. This time window denotes the time instances at which a measurement is taken. We denote with $\mathcal{T}^-$ the set of all time instances except the last one, i. e. $\mathcal{T}^- = \mathcal{T} \setminus \{t_e\}$.

For shorthand of notation, we write $x \in \mathcal{X}$ (resp. $y \in \mathcal{Y}$, $w \in \mathcal{W}$) meaning $x(k) \in \mathcal{X}_k$ (resp. $y(k) \in \mathcal{Y}_k$, $w(k) \in \mathcal{W}_k$) for each $t_k \in \mathcal{T}$. Also, with some abuse of notation, we will write $k \in \mathcal{T}$ meaning $t_k \in \mathcal{T}$.

The employed fault diagnosis method checks consistency of the model with the measurement data, which can be formalized in the following way:

Definition 1. (Consistency). The model M for the fault scenario f is said to be consistent with the input measurements $\mathcal{W}$ and the output measurements $\mathcal{Y}$ if there exists $p \in \mathcal{P}$, $x \in \mathcal{X}$ such that $w \in \mathcal{W}$, $y \in \mathcal{Y}$ and $s = s_f$. ■

Definition 2. (Fault candidate). A fault scenario $f \in \mathcal{F}$ is said to be a *fault candidate* if M is consistent for $s = s_f$. ■

Essentially the goal of model-based fault diagnosis is to determine possible fault candidates, or more formally:

Problem 1. (Fault detection). Determine if M is consistent for f_0. ■

Problem 2. (Fault isolation). Determine all fault candidates within $\mathcal{F} \setminus \{f_0\}$. ■

Clearly, solving Problem 1 and 2 is challenging, especially in the considered unknown-but-bounded case. We proposed in (Rumschinski et al., 2010; Savchenko et al., 2011) a set-based approach to solve these problems based on (mixed-integer) nonlinear feasibility problems. For the sake of completeness, we provide next a short review of the approach as the basis for our later considerations.

Guaranteed set-based fault diagnosis via relaxation

Problem 1 and 2 can be addressed by determining for which fault signatures s_f the following (semi-)algebraic equations admit a solution.

$$F(\mathcal{T}, \mathcal{S}) : \begin{cases} g(x(k+1), x(k), w(k), p, s) = 0, k \in \mathcal{T}^-, \\ h(y(k), x(k), w(k), p, s) = 0, \quad k \in \mathcal{T}, \\ (x, y, w) \in (\mathcal{X}, \mathcal{Y}, \mathcal{W}), \\ p \in \mathcal{P}, \quad s \in \mathcal{S}. \end{cases}$$

Here, $\mathcal{P}$, $\mathcal{X}$, $\mathcal{W}$ and $\mathcal{Y}$ correspond to the unknown-but-bounded data as defined before, and the set $\mathcal{S} = \{s_f \in \{0,1\}^{d_s} \mid f \in \tilde{\mathcal{F}} \subseteq \mathcal{F}\}$ denotes the subset of fault signatures corresponding to fault scenarios $\tilde{\mathcal{F}}$.

Checking whether $F(\mathcal{T}, \mathcal{S})$ admits a solution is a nonlinear mixed-integer feasibility problem. The solution set of $F(\mathcal{T}, \mathcal{S})$ consists of all values of the variables that satisfy the given constraints. The projection of this set onto the subspace of variables s provides a set of its admissible values, hence solving Problem 1 and 2. In other words, if this projection does not include a specific fault signature then the corresponding fault is not a fault candidate. The set of fault candidates is, therefore, determined by excluding all faults that are inconsistent with the data.

Determining the solution set of $F(\mathcal{T}, \mathcal{S})$ is generally a difficult task. For systems of moderate size it can be efficiently approximated by semidefinite or linear relaxations (Rumschinski et al., 2010; Savchenko et al., 2011). However, for larger systems the corresponding relaxed problems become computationally demanding. For this reason, we present in this work a suitable problem reduction approach. We formalize the requirements for such a reduction next.

Problem reduction for set-based fault diagnosis

The needed computational effort to solve the semidefinite or linear relaxation of $F(\mathcal{T},\mathcal{S})$ scales with the number of variables (or *monomials*) and the number of associated constraints in $F(\mathcal{T},\mathcal{S})$. Thus we introduce the following concept of problem reduction for fault diagnosis.

Problem 3. (Problem reduction). Find a feasibility formulation equivalent to $F(\mathcal{T},\mathcal{S})$ that allows solving Problem 1 and 2 with less computational effort. ■

The presented approach is based on projections similar to the idea of *residual generation*, see e. g. (Frisk, 2000). However, instead of generating residuals solely to solve the fault diagnosis problems, we employ them to simplify the problem structure and, thus, limit the needed computational effort. We choose appropriate residuals based on the concept of *causality relationships* (also called parity relations or relevance relations), see e. g. (Svärd and Nyberg, 2008; Aslund et al., 2011).

3. REDUCED FEASIBILITY FORMULATION

In this section we present an adapted concept of causal relations and residuals to reduce the amount of variables in the feasibility problem discussed in the previous section.

Causal reasoning

To derive a simpler representation of the feasibility problem that estimates the admissible values of the fault signatures s, we have to determine which parts of the model M are affected by a specific fault.

The idea of *causal reasoning* from the field of Artificial Intelligence provides the means to analyze relations between variables within a system. It was employed for the problem of fault diagnosis e. g. in (Travé-Massuyès and Pons, 1997; Fagarasan et al., 2004). We propose here a framework adjusted to our setup.

Definition 3. (Causal relation). In the model M the change in the state $x_i(k)$ is said to be *causally related* to the variable σ (e. g. another state or an input) if there is an equality g_j that contains both $x_i(k)$ and σ. ■

This definition is the discrete-time analog to the notion of differential causality used in (Aslund et al., 2011).

To determine the states of the model M that are affected by the occurrence of the fault $f \in \mathcal{F}\setminus\{f_0\}$ according to Definition 3, we consider only the subspace of variables $s \in \mathbb{Z}^{d_s}$ for which the values of fault signatures s_f and s_{f_0} differ. In more technical terms, we introduce two sets of indices $\hat{J}$ and $\tilde{J}$ such that

$$\hat{J} = \{j \in \{1,\dots,d_s\} \mid s_{fj} \neq s_{f_0 j}\}, \quad \tilde{J} = \{1,\dots,d_s\}\setminus\hat{J}.$$

Therefore, we can split the vector s into two parts: $\hat{s} = \{s_j \mid j \in \hat{J}\}$ and $\tilde{s} = \{s_j \mid j \in \tilde{J}\}$, where s_j denotes the j-th element of s. To simplify notation we define

$$\hat{\mathcal{S}} = \{\hat{s}_f, \hat{s}_{f_0}\}.$$

This means, by setting $\tilde{s}_f \equiv \tilde{s}_{f_0}$ we obtain the restriction of $F(\mathcal{T},\mathcal{S})$ to the fault f as follows

$$F_f(\mathcal{T},\hat{\mathcal{S}}):\begin{cases} g(x(k+1),x(k),w(k),p,\tilde{s}_{f_0},\hat{s}) = 0, & k \in \mathcal{T}^-,\\ h(y(k),x(k),w(k),p,\tilde{s}_{f_0},\hat{s}) = 0, & k \in \mathcal{T},\\ (x,y,w) \in (\mathcal{X},\mathcal{Y},\mathcal{W}),\\ p \in \mathcal{P}, \quad \hat{s} \in \hat{\mathcal{S}}. \end{cases}$$

Furthermore, based on the notion of causal relations we introduce the term causal order.

Definition 4. (Causal order). The state $x_i(k)$ is called a state of *first causal order* for the fault $f \in \mathcal{F}\setminus\{f_0\}$, if it is causally related to $\hat{s}$. The state $x_i(k)$ is called a state of *n-th causal order* (for $n > 1$), if it is causally related to any state of $(n-1)$-th causal order. ■

Assuming that in the model M no decoupled dynamics are present, we clearly have for $n \geq n_x$ all states included in the n-th causal order.

Next we show how to employ the notion of causal order to generate a feasibility formulation that estimates the values of fault signature $\hat{s}$, but is of smaller size with respect to $F(\mathcal{T},\mathcal{S})$. To provide complete fault diagnosis (under the assumption that all faults are known), we must ensure that no actual fault is excluded from the list of fault candidates. In other words, the estimates of admissible values of the variables in $\hat{s}$ should relate to the estimates of $F(\mathcal{T},\mathcal{S})$. Hence our goal is to ensure that the resulting estimates outer approximate the solution obtained by solving $F(\mathcal{T},\mathcal{S})$. To do so we employ a method similar to lift-and-project algorithms widely used in mixed-integer linear programming (Balas et al., 1991).

Lifting of the variable space

For a given fault f and chosen causal order n we divide the variables $(x(k), x(k+1), w(k), y(k), p)$ for a single time step $k \in \mathcal{T}$ into two vectors. Note, that it is sufficient to consider a single time step for the proposed relaxation procedure since the model M is time-invariant. The vector ξ consists of variables up to n -th causal order, while the rest form the vector ζ. In these terms the problem $F(\{k\},\{s_{f_0}, s_f\})$ can be written as

$$F_f(\{k\},\hat{\mathcal{S}}) : \begin{cases} a(\xi,\zeta,\hat{s}) = 0,\\ (\xi,\zeta) \in (\mathcal{X}_1,\mathcal{X}_2),\\ \hat{s} \in \hat{\mathcal{S}}, \end{cases}$$

where a represents the constraints equivalent to g and h in the new variables ξ, ζ.

Next we introduce a new set of lifting variables η, the lift function $\eta = l(\xi,\zeta)$ and the constraints $\hat{a}$, such that we can reformulate the feasibility problem in the form

$$\hat{F}_f(\{k\},\hat{\mathcal{S}}) : \begin{cases} \hat{a}(\xi,\eta,\hat{s}) = 0,\\ \eta = l(\xi,\zeta),\\ (\xi,\zeta) \in (\mathcal{X}_1,\mathcal{X}_2),\\ \hat{s} \in \hat{\mathcal{S}}. \end{cases}$$

One possibility to ensure that the formulation $\hat{F}_f(\{k\},\hat{\mathcal{S}})$ is equivalent to $F_f(\{k\},\hat{\mathcal{S}})$ is to demand the following equivalence relation to hold $\hat{a}(\xi,l(\xi,\zeta),\hat{s}) \equiv a(\xi,\zeta,\hat{s})$. Throughout the rest of this paper we only consider lifting procedures that satisfy this relation. There are numerous ways for creating suitable lift functions. In this work we use a method similar to the *aggregation* of variables, introduced in (Simon and Ando, 1961).

We express $a_i(\xi,\zeta,\hat{s})$ via a sum of its monomials

$$a_i(\xi,\zeta,\hat{s}) = \textstyle\sum_{j=1}^{n_i} m_{i,j}(\xi,\zeta,\hat{s}).$$

We write $\sigma | m_{i,j}$ if $m_{i,j}$ depends on σ. If $m_{i,j}$ only depends on σ, we write $m_{i,j}(\sigma)$.

As stated in Problem 3, we are interested in lift functions, that simplify the structure of the polynomials in $\hat{a}$ compared to a. An adequate measure of complexity/simplicity for general polynomial problems is the overall amount of involved variables or monomials and the polynomial degree. To ensure the former we require that the dimension of η is smaller than the dimension of ζ. For the latter, we pose the following constraint on each monomial $\hat{m}_{i,j}$ of $\hat{a}$:

$$\deg(\hat{m}_{i,j}(\xi,\eta,\hat{s})) \leq \deg(\hat{m}_{i,j}(\xi,l(\xi,\zeta),\hat{s})).$$

The construction of appropriate lift functions can then be done with the help of Algorithm 1. The variables η created this way only depend on ζ, however, depending on the structure of the system, including elements of ξ can lead to a more significant size reduction.

Algorithm 1 Lifting using first causal order

in ξ place the states x_i of first causal order w.r.t. $\hat{s}$; in ζ the remaining variables of $(x(k), x(k+1), w(k), y(k), p)$
set $\hat{a} = a$
while $\exists \hat{a}_i$ with $\hat{m}_{i,j}(\zeta)$ **do**
  set $\eta_i = \sum_{j\in J} \hat{m}_{i,j}(\zeta)$ for $J = \{j \mid \hat{m}_{i,j}(\zeta)\}$,
  replace $\sum_{j\in J} \hat{m}_{i,j}(\zeta)$ with η_i in $\hat{a}$
end while
if $\exists r_0, r_1, \ldots, r_n$, $n \geq 1$ such that for each monomial $\hat{m}$ of $\hat{a}$ $\quad \zeta_{r_0} | \hat{m} \Rightarrow \zeta_{r_i} | \hat{m} \quad \forall i = \{1, \ldots, n\}$ **then**
  set $\eta_r = \zeta_{r_0} \cdot \zeta_{r_1} \cdot \ldots \cdot \zeta_{r_n}$
  replace $\zeta_{r_0} \cdot \zeta_{r_1} \cdot \ldots \cdot \zeta_{r_n}$ with η_r in $\hat{a}$
end if
for each ζ_j that still exists in $\hat{a}$ set $\eta_i = \zeta_j$ and replace them in $\hat{a}$

Remark 1. Note that the introduced lift functions l can be viewed as residuals, however for the proposed approach they do not immediately indicate a fault. Rather, they are employed to simplify the model structure. ■

Problem reduction

After the lifting variables η are chosen, we divide the feasibility problem into two parts. This procedure is called a projection, since we effectively restrict the space of the problem to only include variables ξ, η and $\hat{s}$.

From the formulation $\hat{F}_f(\{k\}, \hat{\mathcal{S}})$ we construct two problems of the form:

$$Lift(\mathcal{X}_1, \mathcal{X}_2): \begin{cases} \eta = l(\xi,\zeta), \\ \hat{a}_2(\eta) = 0, \\ (\xi,\zeta) \in (\mathcal{X}_1, \mathcal{X}_2), \end{cases}$$

$$Proj(\mathcal{Z}, \hat{\mathcal{S}}): \begin{cases} \hat{a}_1(\xi,\eta,s) = 0, \\ (\xi,\eta) \in (\mathcal{X}_1, \mathcal{Z}), \\ \hat{s} \in \hat{\mathcal{S}}. \end{cases}$$

Only those constraints $\hat{a}$ appear in $Proj(\mathcal{Z}, \hat{\mathcal{S}})$, that depend on ξ. Notice, that by definition of causal order, $\hat{a}_2$ does not contain elements of $\hat{s}$. The set $\mathcal{Z}$ represents the feasible set corresponding to η.

The following theorem connects these problems to the original feasibility formulation.

Theorem 1. (Reduced feasibility problem). For the presented reduction procedure the following inclusion holds

$$\hat{F}_f(\{k\}, \hat{\mathcal{S}}) \subseteq Proj(Lift(\mathcal{X}_1, \mathcal{X}_2)_\eta, \hat{\mathcal{S}}).$$ ■

Proof: Let $(\xi^*, \zeta^*, \eta^*, \hat{s}^*) \in \hat{F}_f(\{k\}, \hat{\mathcal{S}})$. Then $(\xi^*, \zeta^*, \eta^*) \in Lift(\mathcal{X}_1, \mathcal{X}_2)$ by construction, as its constraints are taken directly from $\hat{F}_f(\{k\}, \hat{\mathcal{S}})$.

If we now define $\mathcal{Z} = Lift(\mathcal{X}_1, \mathcal{X}_2)_\eta$, the point $(\xi^*, \eta^*, \hat{s}^*)$ is a valid solution of $Proj(\mathcal{Z}, \hat{\mathcal{S}})$, since $\hat{a}_1(\xi^*, \eta^*, \hat{s}^*) = 0$, $\hat{s} \in \hat{\mathcal{S}}$ and $\xi \in \mathcal{X}_1$ for $\hat{F}_f(\{k\}, \hat{\mathcal{S}})$, and we have already shown that $\eta^* \in \mathcal{Z}$. □

The problem $Lift(\mathcal{X}_1, \mathcal{X}_2)$ is structurally simpler, and the problem $Proj(\mathcal{Z}, \hat{\mathcal{S}})$ is of lower dimension compared to $F(\{k\}, \mathcal{S})$. Therefore, Theorem 1 implies a less computationally demanding solution for estimating the set of admissible fault signatures s_f for one time step. Since the model M is time-invariant, we can extend Theorem 1 to the whole time-window $\mathcal{T}$, hence solving Problem 3.

Remark 2. The computational effort can be further reduced, as the explicit formulation of l allows the use of computationally inexpensive methods for outer approximating the feasible set $\mathcal{Z}$, e. g. via interval arithmetics. It easily follows from Theorem 1 that $Proj(\mathcal{Z}, \hat{\mathcal{S}})$ provides an outer approximation of the set $\hat{F}_f(\{k\}, \hat{\mathcal{S}})$. ■

Remark 3. Theorem 1 guarantees that each solution of the initial problem is also a solution of the reduced problem. However, solving $Lift(\mathcal{X}_1, \mathcal{X}_2)$ first might increase the solution space of $Proj(\mathcal{Z}, \hat{\mathcal{S}})$. ■

Remark 4. If the reduced problem leads to unsatisfactory results, one can choose a higher causal order at the initial step of Algorithm 1 or increase the length of the considered time window $\mathcal{T}$. ■

4. EXAMPLES

We illustrate the presented reduction method considering two 5-tank system configurations, depicted in Fig. 1 and 2.

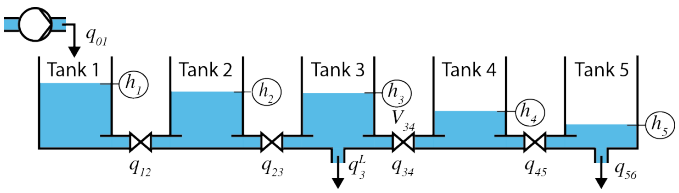

Fig. 1. Sequential 5-tank system.

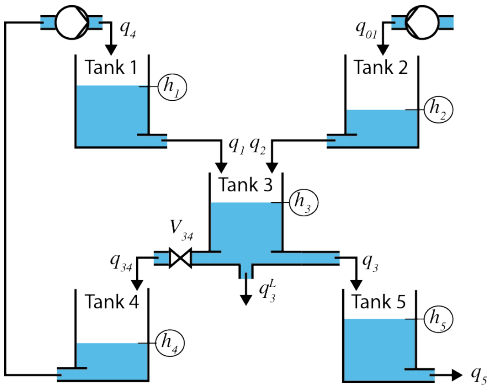

Fig. 2. Interconnected 5-tank system.

Sequential 5-tank system (Fig. 1)

System description: The system consists of five tanks with areas A connected by valves with the inflow q_{01} and the outflow q_{56}. h_1, h_2, h_3, h_4 and h_5 denote the measured water-levels. If the maximum allowed height $h_{\max} = 1\text{m}$ for h_1 is reached, q_{01} is set to zero. This switching condition is modeled using the state-dependent binary variable d_{01}. For this setup we assume that under operating conditions and all fault scenarios the plant is in a state where $h_1 \geq h_2 \geq h_3 \geq h_4 \geq h_5$.

We consider two fault scenarios, first when valve V_{34} gets clogged and its throughput is reduced by 50 percent. The second fault is a leakage in the third tank q_3^L. These scenarios are embedded in the aggregated model using the binary vector $s \in \{0,1\}^2$.

The discrete-time model of the system is given by the following nonlinear difference equations

$$\begin{aligned} h_i(k+1) &= h_i(k) + \Delta t(q_{i-1i}(k) - q_{ii+1}(k))/A, \\ h_3(k+1) &= h_3(k) + \Delta t(q_{23}(k) - q_{34}^*(k) - q_3^L(k))/A, \end{aligned} \tag{1}$$

with $i \in \{1,2,4,5\}$, $\Delta t = 5\text{s}$ and

$$\begin{aligned} q_{ii+1}(k) &= c_{ii+1}\sqrt{h_i(k) - h_{i+1}(k)},\ i \in \{1,2,3,4\}, \\ q_{01}(k) &= \bar{q}_{01} d_{01}(k),\ q_3^L(k) = c_3^L d_3^L(k)\sqrt{h_3(k)}, \\ q_{56}(k) &= c_{56}\sqrt{h_5(k)}, q_{34}^*(k) = q_{34}(k)(1 - 0.5 s_1). \end{aligned} \tag{2}$$

The binary variables are defined as follows

$$d_{01}(k) = \begin{cases} 1, & h_1(k) \leq h_{max}, \\ 0, & h_1(k) > h_{max}, \end{cases} \quad s_1 = \begin{cases} 1, & V_{34} \text{ clogged}, \\ 0, & V_{34} \text{ open}, \end{cases}$$

$$d_3^L(k) = \begin{cases} s_2, & h_3(k) > 0, \\ 0, & h_3(k) \leq 0, \end{cases} \quad s_2 = \begin{cases} 1, & \text{Tank 3 leaking}, \\ 0, & \text{Tank 3 sealed}. \end{cases}$$

Note that it can be represented via a set of mixed-integer linear constraints (Savchenko et al., 2011).

As (2) contains non-polynomial parts, we reformulate them by introducing virtual states and new constraints:

$$\begin{aligned} (\Delta h_{i,i+1}(k))^2 &= h_i(k) - h_{i+1}(k),\ i \in \{1,2,3,4\} \\ (Sqh_i(k))^2 &= h_i(k),\ i \in \{3,5\}. \end{aligned} \tag{3}$$

Placing $Sqh_i(k)$ and $\Delta h_{i,i+1}(k)$ in (2) instead of appropriate square root terms results in a polynomial model.

Problem reduction: We reduce next the diagnosis problem for the leakage fault. To do so, we restrict the set of fault switches to s_2, setting s_1 to zero. The elements of ξ are then taken from the third equation of (1), so $\xi = (h_3(k), \Delta h_{2,3}(k), \Delta h_{3,4}(k), Sqh_3(k))$.

These elements appear in equations $2-4$ of (1) and (3), and following Algorithm 1 we substitute the rest of the elements with new variables

$$\begin{aligned} &\eta^1 = c_{23}/A,\ \eta^2 = c_{34}/A,\ \eta^3 = c_3^L/A, \\ &\eta^4(k) = h_2(k),\ \eta^5(k) = h_4(k), \\ &\eta^6(k) = h_2(k+1) - h_2(k) - \Delta t c_{12} \Delta h_{1,2}(k)/A, \\ &\eta^7(k) = h_4(k+1) - h_4(k) + \Delta t c_{45} \Delta h_{4,5}(k)/A. \end{aligned} \tag{4}$$

The initial uncertain bounds on the parameters and the uncertain data for $h_i(k)$ are employed to estimate the feasible bounds on every element of η using interval arithmetics (cf. Remark 2). These bounds are used as uncertain initial data to estimate admissible values of s_2.

Simulation: We compare the quality of fault diagnosis and the speed differences between the initial formulation (1) and the reduced formulation. We relax both problems following (Savchenko et al., 2011), which results in a mixed-integer linear formulation. The implementation is done in the Matlab toolbox *ADMIT* (Streif et al., 2012).

For simulation we use parameter values $c_{ij} = 1.232 \cdot 10^{-4}\text{m}^{5/2}\text{s}^{-1}$, $c_3^L = 6.16 \cdot 10^{-5}\text{m}^{5/2}\text{s}^{-1}$, $\bar{q}_{01} = 1.5 \cdot 10^{-4}\text{m}^3\text{s}^{-1}$ and $A = 1.54 \cdot 10^{-2}\text{m}^2$ and relative tolerance of ± 1 percent is added to represent the unknown-but-bounded data. Initial water tank levels are chosen as $h_0 = (0.6, 0.5, 0.4, 0.3, 0.2)$ and the relative tolerance of ± 5 percent is added to the simulated data.

After 10 time steps the leakage in the third tank is introduced, and for either model we find the minimal amount of time steps to uniquely diagnose the fault.

Results: The resulting problem sizes as well as the time needed for the fault diagnosis are reported in Table 1. Both

Table 1. Results of the first setup

Problem	Simulation	N Var.	N Cons.	Time steps	Time [s]
Full	Faultless	94	259	4	158
	Leakage	94	259	4	159
Reduced	Faultless	52	134	5	40
	Leakage	43	110	4	32

formulations uniquely diagnose both cases in not more than 5 time steps, and the reduced problem is around 50 percent smaller in size, which leads to a speedup of $75-80$ percent. Although not shown, similar results were achieved for the clogging fault.

Interconnected 5-tank system (Fig. 2)

System Description: The parameters of the tanks as well as the throughput of the connecting pipes are as for the previous example. The pump connecting tank 4 to tank 1 is chosen to not prevent the free water flow.

We consider two fault scenarios, first when valve V_{34} gets clogged and its throughput is reduced by 50 percent. The second fault is a leakage in the third tank q_3^L. These scenarios are embedded in the aggregated model using the binary vector $s \in \{0,1\}^2$.

Similarly, the discrete-time model of the system is given by the following nonlinear difference equations

$$\begin{aligned} &h_1(k+1) - h_1(k) - \Delta t(q_4(k) - q_1(k))/A = 0, \\ &h_2(k+1) - h_2(k) - \Delta t(q_{01}(k) - q_2(k))/A = 0, \\ &h_3(k+1) - h_3(k) - \Delta t(q_1(k) + q_2(k) - q_3(k) - q_f(k))/A = 0, \\ &h_4(k+1) - h_4(k) - \Delta t(q_{34}(k) - q_4(k))/A = 0, \\ &h_5(k+1) - h_5(k) - \Delta t(q_3(k) - q_5(k))/A = 0, \end{aligned}$$

with $\Delta t = 5\text{s}$ and

$$\begin{aligned} q_{01}(k) &= \bar{q}_{01} d_{01}(k),\ q_i(k) = c_i\sqrt{h_i(k)},\ i \in \{1,\ldots,5\} \\ q_{34}(k) &= c_{34}(1 - 0.5 s_1)\sqrt{h_3(k)}, \\ q_f(k) &= c_3^L d_3^L(k)\sqrt{h_3(k)} + q_{34}(k). \end{aligned}$$

Binary variables $d_{01}(k)$ and $d_3^L(k)$ as well as additional virtual states for $\sqrt{h_i(k)}$ are defined as before.

Problem reduction and simulation: Due to a higher number of connections between the tanks in this setup, the reduction procedure did not decrease the problem size as much as for the first setup.

The unknown-but-bounded parameter values are specified in the appendix, and the initial water tank levels are $h_0 = (0.9, 0.7, 0.5, 0.4, 0.3)$. The simulation data was acquired using average values of the parameter bounds, and the relative tolerance of ± 5 percent was added to the simulated water levels data.

Results: The resulting problem sizes as well as the computation times are provided in Table 2. Both formulations uniquely diagnose both cases in not more than 6 time steps, however the reduced model is only 35 percent smaller in size, which shows, that the second setup is more interconnected. Nevertheless, the performance improvement of the reduced problem was $65 - 75$ percent.

Table 2. Results of the second setup

Problem	Simulation	N Var.	N Cons.	Time steps	Time [s]
Full	Faultless	114	284	5	153
	Leakage	114	284	5	165
Reduced	Faultless	75	198	6	38
	Leakage	75	198	6	71

5. CONCLUSIONS

In this contribution, we proposed an approach to reduce the complexity of the set-based fault diagnosis framework presented in Savchenko et al. (2011). The proposed approach employs the notion of causal order to determine the states of the model primarily affected by the occurrence of a fault. This knowledge is then used to relax the dynamics and structure of the full model, reducing its size without proportionally increasing the relaxation error.

We presented an approach to construct a relaxed model formulation. By employing a higher causal order this approach allows a trade-off between model complexity and model accuracy. We illustrated the algorithm with two 5-tank configurations, comparing the resulting model sizes, execution times and amount of data required for unique diagnosis of a specific fault.

Although, the relaxed models required generally more time steps until unique diagnosis of the faults was achieved, the overall solution time was substantially smaller than that of the full model with fewer time steps.

Overall, this method is well suited for processes that contain sequentially connected parts, or if the occurring faults only affect subsystems.

As the proposed approach introduces an additional layer of relaxation of the problem formulation, the obtained results can be conservative. Future research will address the impact on the quality of the proposed relaxations, as well as the possibility to retain the property of diagnosability.

REFERENCES

Antoulas, A.C., Sorensen, D.C., and Gugercin, S. (2001). A survey of model reduction methods for large-scale systems. *Contemporary Math.*, 280, 193–220.

Aslund, J., Bregon, A., Krysander, M., Frisk, E., Pulido, B., and Biswas, G. (2011). Structural diagnosability analysis of dynamic models. In *Proc. IFAC World Congress*, 4082–4088. Milan, Italy.

Balas, E., Ceria, S., and Cornuéjols, G. (1991). A lift-and-project cutting plane algorithm for mixed 0-1 programs. *Math. Programming*, 58(1).

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006). *Diagnosis and fault-tolerant control*. Springer, 2nd edition.

Fagarasan, I., Ploix, S., and Gentil, S. (2004). Causal fault detection and isolation based on a set-membership approach. *Automatica*, 40(12), 2099–2110.

Frank, P.M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. *Automatica*, 26(3), 459–474.

Frisk, E. (2000). Residual generator design for non-linear, polynomial systems: a Gröbner basis approach. In *Proc. Symp. Fault Det. Superv. Saf. Tech. Proc. (SAFEPROCESS)*. Budapest, Hungary.

Gertler, J. (1991). Analytical redundancy methods in fault detection and isolation. In *Proc. Symp. Fault Det. Superv. Saf. Tech. Proc. (SAFEPROCESS)*, 9–21. Baden-Baden, Germany.

Hasenauer, J., Rumschinski, P., Waldherr, S., Borchers, S., Allgöwer, F., and Findeisen, R. (2010). Guaranteed steady state bounds for uncertain (bio-) chemical processes using infeasibility certificates. *J. Process Control*, 20(9), 1076–1083.

Heim, B., Gentil, S., Cauvin, S., Travé-Massuyès, L., and Braunschweig, B. (2002). Fault diagnosis of a chemical process using causal uncertain model. In *Prestigious App. Int. Sys., 15th Eur. Conf. AI (ECAI)*. Lyon, France.

Moore, B. (1981). Principal component analysis in linear systems: controllability, observability, and model reduction. *IEEE Trans. Automatic Control*, 26(1), 17–32.

Patton, R.J., Frank, P.M., and Clarke, R.N. (1989). *Fault diagnosis in dynamic systems: theory and application*. Prentice-Hall, Inc.

Rumschinski, P., Richter, J., Savchenko, A., Borchers, S., Lunze, J., and Findeisen, R. (2010). Complete fault diagnosis of uncertain polynomial systems. In *Proc. IFAC Symp. Dyn. Control Proc. Syst. (DyCoPs)*, 127–132. Leuven, Belgium.

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

Simon, H.A. and Ando, A. (1961). Aggregation of variables in dynamic systems. *Econometrica*, 111–138.

Staroswiecki, M. and Comtet-Varga, G. (2001). Analytical redundancy relations for fault detection and isolation in algebraic dynamic systems. *Automatica*, 37(5), 687–699.

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(9), 1290–1291.

Svärd, C. and Nyberg, M. (2008). A mixed causality approach to residual generation utilizing equation system solvers and differential-algebraic equation theory. In *Proc. 19th Int. Workshop Princ. Diagn. (DX-08)*. Blue Mountains, Australia.

Travé-Massuyès, L. and Pons, R. (1997). Causal ordering for multiple mode systems. In *Proc. 11th Int. Workshop Qual. Reas.*, 203–214. Cortona, Italy.