Diagnosis of Linear Systems with Structured Uncertainties based on Guaranteed State Observation

Philippe Planchon and Jan Lunze

Abstract: Reaching fault tolerance in technological systems requires to detect malfunctions. This paper presents a diagnostic method that is robust with respect to unknown-but-bounded uncertainties of the dynamical model and the measurements. By using models of the faultless and the faulty behaviours, a state-set observer computes polyhedral sets from which the consistency of the models with the interval measurements is determined. The diagnostic result is proven to be complete, i.e., the set of faults obtained by the diagnostic algorithm includes the actual fault. The algorithm is illustrated by an application example.

Keywords: Fault diagnosis, guaranteed state observation, linear uncertain systems, polytopic sets.

1. INTRODUCTION

1.1. Diagnosis

Fault diagnosis aims at determining whether a fault is affecting a dynamical process (Fig. 1). Model-based diagnostic methods compare the *actual behaviour* of the process represented by measurement sequences of the inputs and the outputs with the *expected behaviour* that is given by a mathematical model.

As the model and the measurements used for diagnostic purposes are usually subject to uncertainties, the diagnoses have to be robust with respect to these uncertainties. The challenge is to determine which faults are affecting the process with an acceptable ratio of false alarms to missed alarms. False alarms happen when a fault is indicated that did not occur, missed alarms when a fault occurs without being detected.

In this paper the process is represented in each fault situation by a linear state-space model whose parameters may have unknown-but-bounded uncertainties. Furthermore, the measurements may also be subject to an unknown-but-bounded error. Under these conditions, a *complete diagnostic result* is sought, meaning that the diagnosis yields a set which includes all faults, for which the model and the measurement sequences match (within the given uncertainty assumption). Such model and measurements are said to be *consistent*.

This paper proposes to verify this consistency by pursuing set-membership observations. It is shown that, in order to attain a completeness of the diagnostic result, the set-observers must compute over-approximations of the set of possible current states. The observer is then said to be *guaranteed*, i.e., it describes a set of states which includes the actual state of the system. The guaranteed observation results are then interpreted in the framework of *consistency-based diagnosis*, yielding the desired completeness.

1.2. Literature overview

The monographs [1-3] present thorough surveys about existing diagnostic methods. In this paper, an observer-based approach to diagnosis is described, in which uncertainties are explicitly taken into account, both in the parameters used for the modeling and in the input-output measurement signals.

As opposed to numerous studies, the present approach does not rely on a stochastic consideration of uncertainties - in which these have a probability distribution - but merely considers the uncertainties to lie within given bounds (deterministic uncertainties). While it is possible to deal with such unknown-but-

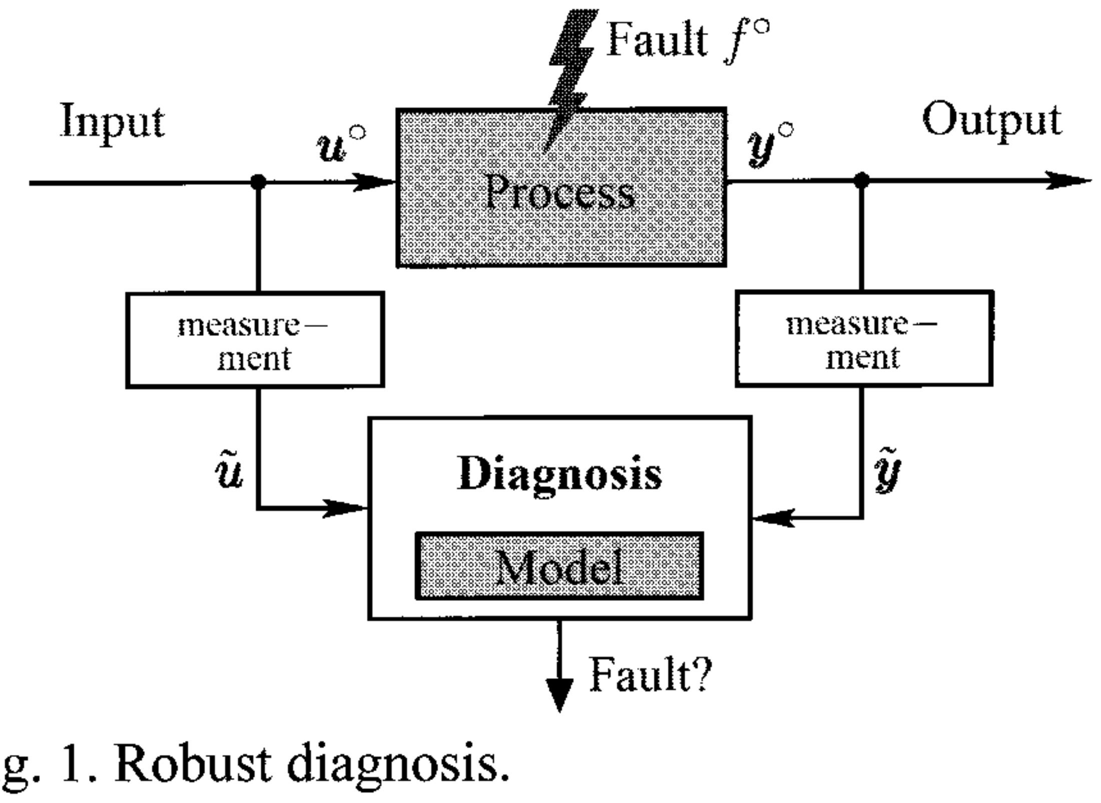


Fig. 1. Robust diagnosis.

Manuscript received September 15, 2007; accepted April 21, 2008. Recommended by Guest Editors Marcel Staroswiecki and Bin Jiang.

Philippe Planchon is working for BMW Group in Munich, Germany (e-mail: philippe_planchon@yahoo.com).

Jan Lunze is head of the Institute of Automation and Computer Control in Bochum, Germany (e-mail: lunze@atp.rub.de).

bounded uncertainties using approaches from optimal control theory, e.g., with H_2 or H_∞ filtering techniques [4,5], the present solution uses a set-membership approach. The advantage of the method described in this paper over these approaches is the fact that no fault can be overseen and a complete diagnostic result is obtained.

Using an observer-based diagnosis, the method relies on two main steps. First, the state-observation is solved in a set-theoretic sense for each model of the possible process behaviours. Second, the results of these set-observers are evaluated into a diagnostic result. In order to achieve completeness in an acceptable computing time, the set-valued observations must be guaranteed, i.e., they over-approximate the true result.

Several such guaranteed observers have been developed in the past for linear discrete-time state-space models. These distinguish themselves mainly in the type of geometry used: ellipsoids [6,7], polytopes [8,9] or intervals [10,11]. Fewer methods are known which also consider model uncertainty [12-14]. While these set-theoretic observers may appear formally very different from standard stochastic observers, their algorithmic similarity with the extended Kalman filter is interestingly discussed in [15].

Much research in this field has also been conducted using approaches based on interval arithmetic, [11,16-18]. The achieved algorithms for state observation (or parameter estimation) is generally intrinsically different from the above mentioned works. Furthermore, the models used to describe the process are often either static or based on an input to output relationship, not on state-space formalism. An original method combining residual generation and parameter estimation using intervals is found in [19], but it does not pursue completeness. An unknown-input observer may also be used to consider the model uncertainty, e.g., in [20] using parallelotopes and in [21] using ellipsoids. This leads of course to different observation algorithms and, most of all, requires a different modeling. Further set-theoretical diagnostic methods that consider model uncertainties exist based on frequency-domain models, [22,23].

This paper describes a diagnosis for processes subject to unknown-but-bounded measurement and parameter uncertainties based on polyhedral-set observation. To the authors' knowledge, it presents a novel approach in considering (structured) parameter uncertainties and in not requiring to "guess" an bounded initial state-set. Furthermore, the paper emphasises the causality between the aim to obtain complete diagnosis and the necessity to solve the set-observation task using over-approximations. The reason to use over-approximation (and not any other kind of approximation) is often unclear in the literature for similar diagnostic methods.

1.3. Assumptions

Throughout this paper the following assumptions are made:

Assumption 1: A finite number of faults may affect the process. The set of all faults is denoted by $\mathbb{F} = \{f_0, f_1, \ldots, f_N\}$. By convention, the faultless behaviour is represented by f_0 and the faulty behaviours by f_i, $i > 0$. The fault truly occurring in the process is denoted by f°, such that at every time instant $\exists j \in \{0, \ldots, N\}, f^\circ \equiv f_j$.

Assumption 2: The set $\mathbb{F}$ is known and the process is represented for all faults by a linear state-space model (closed-world assumption, *cf.* [24]). These models may include unknown-but-bounded parameter uncertainties.

Assumption 3: A constant fault $f^\circ \in \mathbb{F}$ affects the process during the entire time horizon of the diagnosis, hence $f^\circ(k) \equiv f^\circ$ (time-invariant fault). Extensions to time-varying faults are possible but not described in this paper.

Assumption 4: At all time instances k an upper bound on the measurement error is available, such that two vectors $\boldsymbol{e}_u(k)$ and $\boldsymbol{e}_y(k)$ are known for which

$$|\boldsymbol{u}^\circ(k) - \tilde{\boldsymbol{u}}(k)| \leq \boldsymbol{e}_u(k) \quad \text{and} \quad |\boldsymbol{y}^\circ(k) - \tilde{\boldsymbol{y}}(k)| \leq \boldsymbol{e}_y(k)$$

hold, with $\boldsymbol{u}^\circ$ the true input and $\tilde{\boldsymbol{u}}$ the measured input and with $\boldsymbol{y}^\circ$ and $\tilde{\boldsymbol{y}}$ the true and measured outputs.

While Assumption 1 may seem very restrictive, it is in general necessary to have a model of each fault behaviour which must be *identified.* However, unknown faults may still be successfully *detected* if the generated behaviour sufficiently differs from the faultless one. This comment also holds true for faults which vary during the time horizon of the diagnosis, as shown by an example in [25].

Assumption 4 is well-suited to consider offsets (e.g., induced from improper calibration). The time dependence may be used, for example, when a sensor's precision depends on other values of its environment (e.g., a rotational speed sensor with poor precision in its lower RPM range). As the considered uncertainties $\boldsymbol{e}_u(k)$ and $\boldsymbol{e}_y(k)$ do not assume the measurement errors to have a zero mean value, perturbations such as noise must be filtered-out before applying the presented diagnostic method. Similarly, there is no handling of outliers such that these must be removed from the signals. Alternatively if a signal processing method is known to detect outliers and if these only occur in the output signals of the system, the observation algorithm presented here (Algorithm 1) can be made to skip the corresponding measurement step, using only the predicted set. This, of course, worsens the observation's accuracy (and hence the diagnostic accuracy) but would not impair with the completeness property. In practice, the values of the error bounds $\boldsymbol{e}_u(k)$ and $\boldsymbol{e}_y(k)$ can be found in the technical specification of the sensors and actuators, or can be determined empirically. In the latter case, it may be difficult to assure that Assumption 4 always holds true.

2. DIAGNOSTIC METHOD

2.1. Measurements and process model

2.1.1 Measurements

At each time instant *k*, the real-valued measurements $\tilde{\boldsymbol{u}}(k)$ and $\tilde{\boldsymbol{y}}(k)$ are converted into two sets $\mathcal{U}(k)$ and $\mathcal{Y}(k)$ using the two time-varying upper bounds $\boldsymbol{e}_u(k)$ and $\boldsymbol{e}_y(k)$ of the measurement error. The sequence of inputs

$$\boldsymbol{U}(0\ldots\bar{k}) = (\boldsymbol{u}(0),\ldots,\boldsymbol{u}(\bar{k}))$$

yields, at each time k, the set $\mathcal{U}(k)$ of input values that may have occurred

$$\mathcal{U}(k) := \{\boldsymbol{u}\in\mathbb{R}^m \mid |\boldsymbol{u}-\tilde{\boldsymbol{u}}(k)| \le \boldsymbol{e}_u(k)\} \tag{1}$$

and for the time horizon $0\ldots\bar{k}$ the sequence

$$\mathcal{U}(0\ldots\bar{k}) = (\mathcal{U}(0),\ldots,\mathcal{U}(\bar{k})).$$

The fact that a sequence $\boldsymbol{U}(0\ldots\bar{k})$ of real-valued inputs belongs to the sequence $\mathcal{U}(0\ldots\bar{k})$ of set-valued inputs is described by the notation

$$\begin{aligned}&\boldsymbol{U}(0\ldots\bar{k}) \in \mathcal{U}(0\ldots\bar{k})\\ &\qquad\Leftrightarrow \boldsymbol{u}(k)\in\mathcal{U}(k),\ 0\le k\le\bar{k}.\end{aligned} \tag{2}$$

Similarly, the output measurement sequence results in sets of output values

$$\mathcal{Y}(k) := \{\boldsymbol{y}\in\mathbb{R}^r \mid |\boldsymbol{y}-\tilde{\boldsymbol{y}}(k)| \le \boldsymbol{e}_y(k)\}. \tag{3}$$

By construction the sets $\mathcal{U}(k)$ and $\mathcal{Y}(k)$ are hyper-cubes and, therefore, describe intervals in each dimension of the input and output spaces. By Assumption 4, these sets are guaranteed to contain the true input $\boldsymbol{u}^\circ(k)$ and the true output $\boldsymbol{y}^\circ(k)$:

$$\boldsymbol{u}^\circ(k) \in \mathcal{U}(k) \quad\text{and}\quad \boldsymbol{y}^\circ(k) \in \mathcal{Y}(k).$$

Hence, by treating all vectors within these sets, the state observation and thus the subsequent diagnosis are intrinsically robust against the considered error.

2.1.2 Process models

A linear state-space model $\mathcal{M}_f$ with time-varying parameter uncertainties is associated to each fault $f\in\mathbb{F}$:

$$\boldsymbol{x}(k+1) = \boldsymbol{A}_f(\boldsymbol{p}(k))\boldsymbol{x}(k) + \boldsymbol{B}_f\boldsymbol{u}(k) \tag{4}$$

$$\boldsymbol{y}(k) = \boldsymbol{C}_f\boldsymbol{x}(k) + \boldsymbol{D}_f\boldsymbol{u}(k) \tag{5}$$

$$\boldsymbol{p}(k)\in\mathbb{P}\subset\mathbb{R}^{N_p}. \tag{6}$$

The state, input and output vectors are $\boldsymbol{x}\in\mathbb{R}^n$, $\boldsymbol{u}\in\mathbb{R}^m$ or $\boldsymbol{y}\in\mathbb{R}^r$, respectively, and the matrices $\boldsymbol{A}_f$, $\boldsymbol{B}_f$, $\boldsymbol{C}_f$ and $\boldsymbol{D}_f$ are of corresponding sizes. The model uncertainties are *structured*, i.e., the dependency of the system matrix upon the uncertain parameters can be represented in the form

$$\boldsymbol{A}_f(\boldsymbol{p}) := \boldsymbol{A}_{f,0} + \sum_{i=1}^{N_p}(p_i\,\boldsymbol{A}_{f,i}). \tag{7}$$

The interval set $\mathbb{P}$ in which the model parameter $\boldsymbol{p} = (p_1,\ldots,p_{N_p})^T$ varies is defined by

$$\mathbb{P} := \{\boldsymbol{p}\in\mathbb{R}^{N_p} \mid p_i^{\min} \le p_i \le p_i^{\max},\ \ 1\le i\le N_p\}.$$

For simplicity and brevity, this paper only considers uncertainties in the system matrix $\boldsymbol{A}_f$. However, the method used to take into account these uncertainties can be transposed in the exact same way to deal with uncertainties in the input matrix $\boldsymbol{B}_f$ (cf. Section 4).

Uncertainties in the output matrix $\boldsymbol{C}_f$, however, cannot be considered as is done with $\boldsymbol{A}_f$ and $\boldsymbol{B}_f$. Fortunately there are few applications which truly require such consideration (the output $\boldsymbol{y}$ is often a subset of the state $\boldsymbol{x}$). Very few methods are known from the authors which do consider such uncertainties (e.g., [12]).

Definition 1 (Input-to-output operator)**:** The operator $\psi_{y,f}$ describing the achievable output of the model $\mathcal{M}_f$ for a given initial state $\boldsymbol{x}(0)$ and a sequence of inputs $\boldsymbol{U}(0\ldots\bar{k})$ is called the input-to-output operator.

If the parameters are known and time-invariant ($\forall k,\ \ \boldsymbol{p}(k)=\boldsymbol{0}$), the input-to-output operator is real-valued and has a well-known form in the control community:

$$\begin{aligned}&\psi_{y,f}(\boldsymbol{x}(0),\boldsymbol{U}(0\ldots\bar{k})) := \boldsymbol{y}(\bar{k})\\ &= \boldsymbol{C}_f\left(\boldsymbol{A}_{f,0}^{\bar{k}}\boldsymbol{x}(0) + \sum_{j=1}^{\bar{k}}\boldsymbol{A}_{f,0}^{\bar{k}-j}\boldsymbol{B}_f\boldsymbol{u}(j-1)\right) + \boldsymbol{D}_f\boldsymbol{u}(\bar{k}).\end{aligned}$$

For a model with uncertain parameters in $\mathbb{P} \subset \mathbb{R}^{N_p}$, the operator is set-valued and described by

$$\psi_{y,f}(\boldsymbol{x}(0),\boldsymbol{U}(0\ldots\bar{k})) := \mathcal{Y}(\bar{k}) = \bigcup_{\boldsymbol{P}\in\mathbb{P}^{\bar{k}}} \{\boldsymbol{C}_f \psi_{x,f,\boldsymbol{P}}(\boldsymbol{x}(0),\boldsymbol{U}(0\ldots\bar{k})) + \boldsymbol{D}_f \boldsymbol{u}(\bar{k})\},$$

where $\psi_{x,f,\boldsymbol{P}}$ is the input-to-state operator of the exact model corresponding to a specific sequence of parameters $\boldsymbol{P} = \boldsymbol{P}(0\ldots\bar{k}-1) = (\boldsymbol{p}(0),\ldots,\boldsymbol{p}(\bar{k}-1)) \in \mathbb{P}^{\bar{k}}$. An analytical expression of the $\psi_{x,f,\boldsymbol{P}}$ operator is found in [26] to be

$$\psi_{x,f,\boldsymbol{P}}(x_0,\boldsymbol{U}(0\ldots\bar{k}-1)) = \left(\prod_{k=0}^{\bar{k}-1} A_f(\boldsymbol{p}(k))\right) x_0 + \sum_{j=1}^{\bar{k}} \left(\prod_{q=j}^{\bar{k}-1} A_f(\boldsymbol{p}(q))\right) \boldsymbol{B}_f \boldsymbol{u}(j-1),$$

when the following matrix product definitions are used, for $k' \geq k$:

$$\prod_{q=k}^{k'} A_f(\boldsymbol{p}(q)) := A_f(\boldsymbol{p}(k')) \cdot A_f(\boldsymbol{p}(k'-1)) \cdot \ldots \cdot A_f(\boldsymbol{p}(k))$$

and for $k' = k-1$:

$$\prod_{q=k}^{k-1} A_f(\boldsymbol{p}(q)) := \boldsymbol{I}.$$

2.2. Consistency-based diagnosis

The main idea of the diagnostic method proposed in this paper consists in testing the consistency of the models $\mathcal{M}_f$ and the measured set-valued input and output sequences. Consistency means that there exists an initial state as well as real-valued input and output sequences within the given set-valued sequences such that for this initial state and this input sequence the model yields this output sequence. The notion of consistency can be formalised using the input-to-state operator as follows.

Definition 2 (Model consistency)**:** The model $\mathcal{M}_f$ is said to be consistent with a sequence of measurements $U(0\ldots\bar{k})$ and $Y(0\ldots\bar{k})$ if there exists an initial state $\boldsymbol{x}(0)$ such that, for a model with exact parameters:

$$\boldsymbol{Y}(k) = \psi_{y,f}(\boldsymbol{x}(0),\boldsymbol{U}(0\ldots k)), \ \forall k \in \{0,\ldots,\bar{k}\},$$

and for a model with uncertain parameters:

$$\boldsymbol{Y}(k) \in \psi_{y,f}(\boldsymbol{x}(0),\boldsymbol{U}(0\ldots k)), \ \forall k \in \{0,\ldots,\bar{k}\}. \quad (8)$$

Using the symbol "$\models$", the model consistency is represented as follows:

$$\mathcal{M}_f \models (\boldsymbol{U}(0\ldots\bar{k}),\boldsymbol{Y}(0\ldots\bar{k})).$$

The definition of model consistency is extended to consider the sequence of set-valued input and output sets:

$$\mathcal{M}_f \models (\mathcal{U}(0\ldots\bar{k}),\mathcal{Y}(0\ldots\bar{k}))$$

if $\exists \breve{\boldsymbol{U}}(0\ldots\bar{k}) \in \mathcal{U}(0\ldots\bar{k})$ and $\exists \breve{\boldsymbol{Y}}(0\ldots\bar{k}) \in \mathcal{Y}(0\ldots\bar{k})$ such that $\mathcal{M}_f \models (\breve{\boldsymbol{U}}(0\ldots\bar{k}),\breve{\boldsymbol{Y}}(0\ldots\bar{k}))$.

The consistency of a model $\mathcal{M}_f$ with a sequence of inputs and outputs (either real or set-valued) indicates that a process behaves like the model $\mathcal{M}_f$. Hence, this implies that the fault f may have occurred and leads to the following definition of the set of fault candidates.

Definition 3 (Fault candidates)**:** The set of fault candidates is defined by

$$\mathcal{F}^*(\bar{k}) \equiv \mathcal{F}^*(\bar{k} \mid 0\ldots\bar{k}) := \{f \in \mathbb{F} \mid \mathcal{M}_f \models (\mathcal{U}(0\ldots\bar{k}),\mathcal{Y}(0\ldots\bar{k}))\}. \quad (9)$$

Consequently, a fault candidate describes a fault situation in which the measured input and output sequences are consistent with the model of this fault situation. Hence, the set of fault candidates $\mathcal{F}^*(\bar{k})$ represents the best achievable diagnostic result[1]. With these notations and definitions the diagnostic problem can be formally described as follows:

Diagnostic problem:

Given:

- the sequence of set-valued inputs and outputs $\mathcal{U}(0\ldots\bar{k})$ and $\mathcal{Y}(0\ldots\bar{k})$.
- the process model $\mathcal{M}_f$, for all faults $f \in \mathbb{F}$.

Find:

- the set of *fault candidates*, Eq. (9).

An obvious consequence of the assumptions described earlier is given in the following proposition:

Proposition 1: The true fault is a fault candidate: $f^\circ \in \mathcal{F}^*(k), \ \forall k \leq \bar{k}$.

As mentioned in the introduction, the aim of the presented diagnosis is to be *complete*. Using the above notation a formal definition of completeness can now be given:

Definition 4 (Complete diagnosis)**:** A diagnosis is said to be complete if its result - described by a set

[1] The "best" means that no method to verify consistency may lead to a finer diagnosis than $\mathcal{F}^*$ while preserving completeness and using the same information (models and measurement sets).

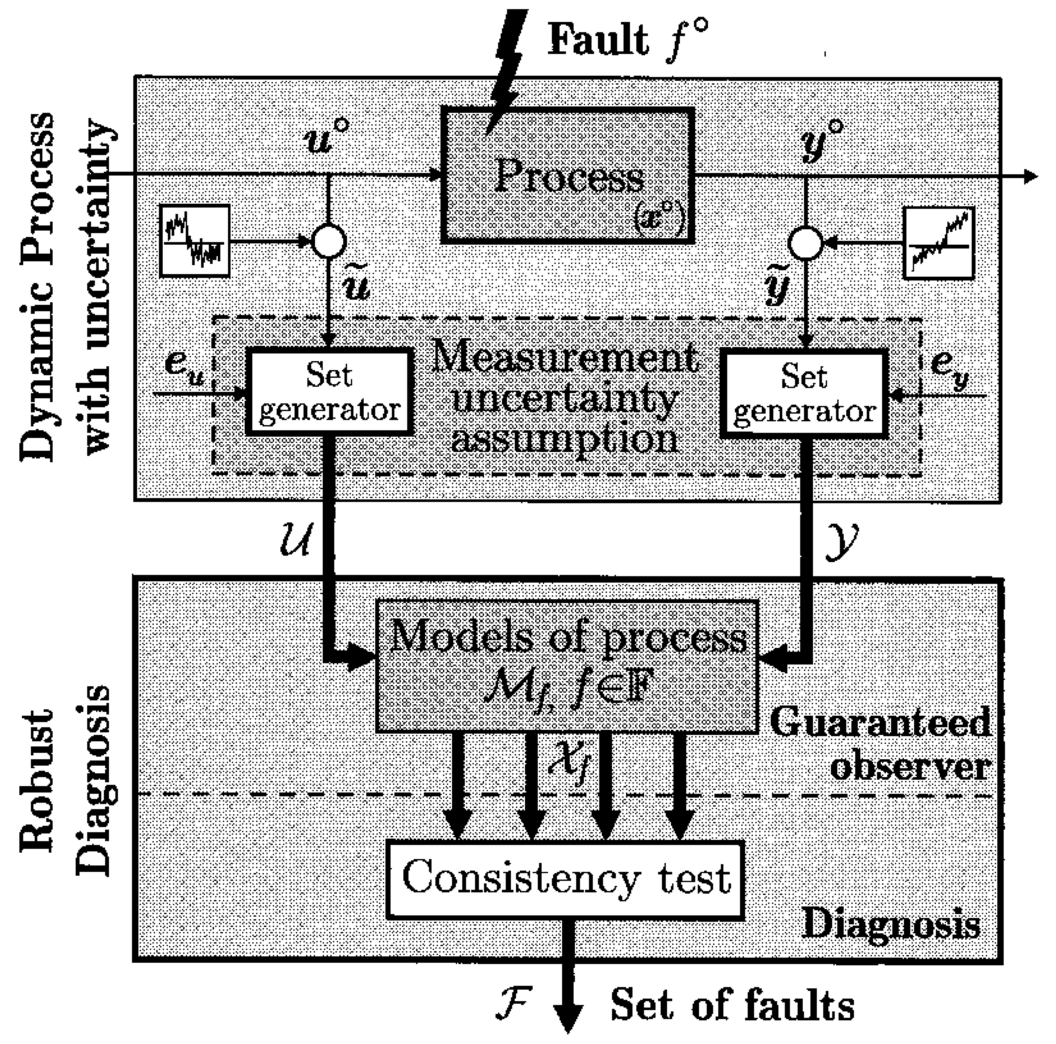


Fig. 2. Robust diagnosis using guaranteed observation.

$\mathcal{F}$ of faults - contains all fault candidates: $\mathcal{F}(k) \supseteq \mathcal{F}^*(k), \ \forall k \le \bar{k}$.

Following Proposition 1, the result of a complete diagnosis always contains the true fault. Hence, the complete diagnosis is also said to be *guaranteed*, meaning it cannot cause missed alarms.

2.3. Overview of the proposed diagnostic method

To solve the diagnostic problem, a method to check the consistency of a model with sequences of input and output sets is needed. Based on Definition 2, the consistency is proven if an initial state $x(0)$ is found which verifies (8). Therefore, by solving a state-observation problem for a model $\mathcal{M}_f$ and a sequence of input and output data, the (in)consistency of the model with the data can be checked.

Because of the set-valued nature of the data, it is proposed to use a set-membership state-observation to verify the consistencies. In the general case, such an observer yields a set $\mathcal{X}(\bar{k} \,|\, 0 \ldots \bar{k})$ representing the states $x(\bar{k})$ possibly reached by the system, given the measurement horizon of the sequences $\mathcal{U}(0 \ldots \bar{k})$ and $\mathcal{Y}(0 \ldots \bar{k})$.[2] Verifying the consistency then simplifies to a verification whether $\mathcal{X}(\bar{k} \,|\, 0 \ldots \bar{k})$ is an empty set or not. More specifically, as the diagnostic result should be complete, a *guaranteed state-observation* is considered: if no exact representation of the sets $\mathcal{X}$ is possible, these are then to be over-approximated. This implies that only inconsistencies can be proven but, most of all, this assures that no fault is wrongly excluded from the diagnostic result, hence its completeness.

In the following section, a diagnostic algorithm is derived which is shown to result in a *complete* and *guaranteed* diagnosis. Furthermore, the diagnosis is robust since the completeness is achieved for an explicit consideration of modeling and measurement errors. The algorithm is based on two consecutive steps (Fig. 2):

1. a *guaranteed state observation* of all models $\mathcal{M}_f$ and $f \in \mathbb{F}$ (see Sections 3 and 4).
2. the *consistency check* of all models (see Section 5).

3. GUARANTEED STATE-SET OBSERVATION

A set-observer constructs the set of all states which may be reached by a process described by model $\mathcal{M}_f$ and for the measured sequences of inputs $\mathcal{U}(0 \ldots \bar{k})$ and outputs $\mathcal{Y}(0 \ldots \bar{k})$. The resulting set of states is said to be *minimal* - and is denoted by $\mathcal{X}^*(\bar{k} \,|\, 0 \ldots \bar{k})$ - if it contains all the reachable states, and only these states. In the general case, the minimal state-set corresponding to a model $\mathcal{M}_f$ and a set-valued sequence of inputs $\mathcal{U}(0 \ldots \bar{k})$ and of outputs $\mathcal{Y}(0 \ldots \bar{k})$ is given by:

$$\begin{aligned} &\mathcal{X}^*(\bar{k} \,|\, 0 \ldots \bar{k}) := \{ \boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \,|\, \boldsymbol{x} := \psi_{x,f,\boldsymbol{P}}(\boldsymbol{x}(0), \boldsymbol{U}(0 \ldots \bar{k})), \\ &\boldsymbol{P} \in \mathbb{P}^{N_P}, \boldsymbol{x}(0) \in \mathbb{R}^{\mathrm{n}}, \boldsymbol{U}(0 \ldots \bar{k}) \in \mathcal{U}(0 \ldots \bar{k}), \\ &\text{for which } \psi_{y,f}(\boldsymbol{x}(0), \boldsymbol{U}(0 \ldots k)) \in \mathcal{Y}(k), 0 \le k \le \bar{k} \}. \end{aligned}$$

Computing $\mathcal{X}^*$ is a very complex task which can be numerically computed only for special cases. In the case of a model with no feedthrough ($\boldsymbol{D}_f = \boldsymbol{0}$), the above expression is equivalently obtained using a recursion over the given time-horizon as follows:

$$\mathcal{X}^*(0 \,|\, 0 \ldots 0) := \{ \boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \,|\, (\boldsymbol{C}_f \boldsymbol{x}) \in \mathcal{Y}(0) \}, \qquad (10)$$

and for $0 \le k \le \bar{k}$,

$$\begin{aligned} &\mathcal{X}^*(k \,|\, 0 \ldots k) := \{ \boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \,|\, \boldsymbol{x} := \boldsymbol{A}_f(\hat{\boldsymbol{p}})\hat{\boldsymbol{x}} + \boldsymbol{B}_f \hat{\boldsymbol{u}}, \\ &\hat{\boldsymbol{x}} \in \mathcal{X}^*(k-1 \,|\, 0 \ldots k-1), \hat{\boldsymbol{p}} \in \mathbb{P}, \hat{\boldsymbol{u}} \in \mathcal{U}(k-1), \qquad (11) \\ &\text{for which } (\boldsymbol{C}_f \boldsymbol{x}) \in \mathcal{Y}(k) \}. \end{aligned}$$

This operation can be further decomposed into three independent operations, which form the basis for most set-membership observation algorithms found in the literature, e.g., [7,8]. The recursion then becomes:

$$\mathcal{X}^*(k \,|\, 0 \ldots k) := \mathcal{X}_p^*(k) \cap \mathcal{X}_m^*(k), \qquad (12)$$

[2] Even when considering a *known* model together with *real-valued* measurement sequences, the result of such an observer can be a *set* of states.

with $\mathcal{X}_p^*(k)$ and $\mathcal{X}_m^*(k)$ defined as

$$\mathcal{X}_p^*(k) := \{\boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \mid \boldsymbol{x} := \boldsymbol{A}_f(\hat{\boldsymbol{p}})\hat{\boldsymbol{x}} + \boldsymbol{B}_f\hat{\boldsymbol{u}},\ \hat{\boldsymbol{u}} \in \mathcal{U}(k-1),$$
$$\hat{\boldsymbol{x}} \in \mathcal{X}^*(k-1 \mid 0\ldots k-1),\ \hat{\boldsymbol{p}} \in \mathbb{P}\} \qquad (13)$$

$$\mathcal{X}_m^*(k) = \{\boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \mid (\boldsymbol{C}_f\boldsymbol{x}) \in \mathcal{Y}(k)\}. \qquad (14)$$

Even in this form, the minimal state-sets are difficult to compute in practice. Indeed, for linear models with uncertainties, the one-step prediction described by $\mathcal{X}_p^*$ does not even result in a convex set. Therefore, research has focused not on computing $\mathcal{X}^*$ but an under-approximation or over-approximations of these minimal sets, [10].

As a complete diagnosis is desired based on the set-observation results, an *over*-approximation of these sets is chosen as derived using the following algorithm (The operators $F_{f,p}$, $F_{f,m}$ and $F_{\supseteq}$ used in the algorithm are explained afterward). The computation steps necessary within one recursion of such a guaranteed observer are illustrated for a two-dimensional system in Fig. 3. An implementation of this algorithm using polyhedra is given in Section 4.

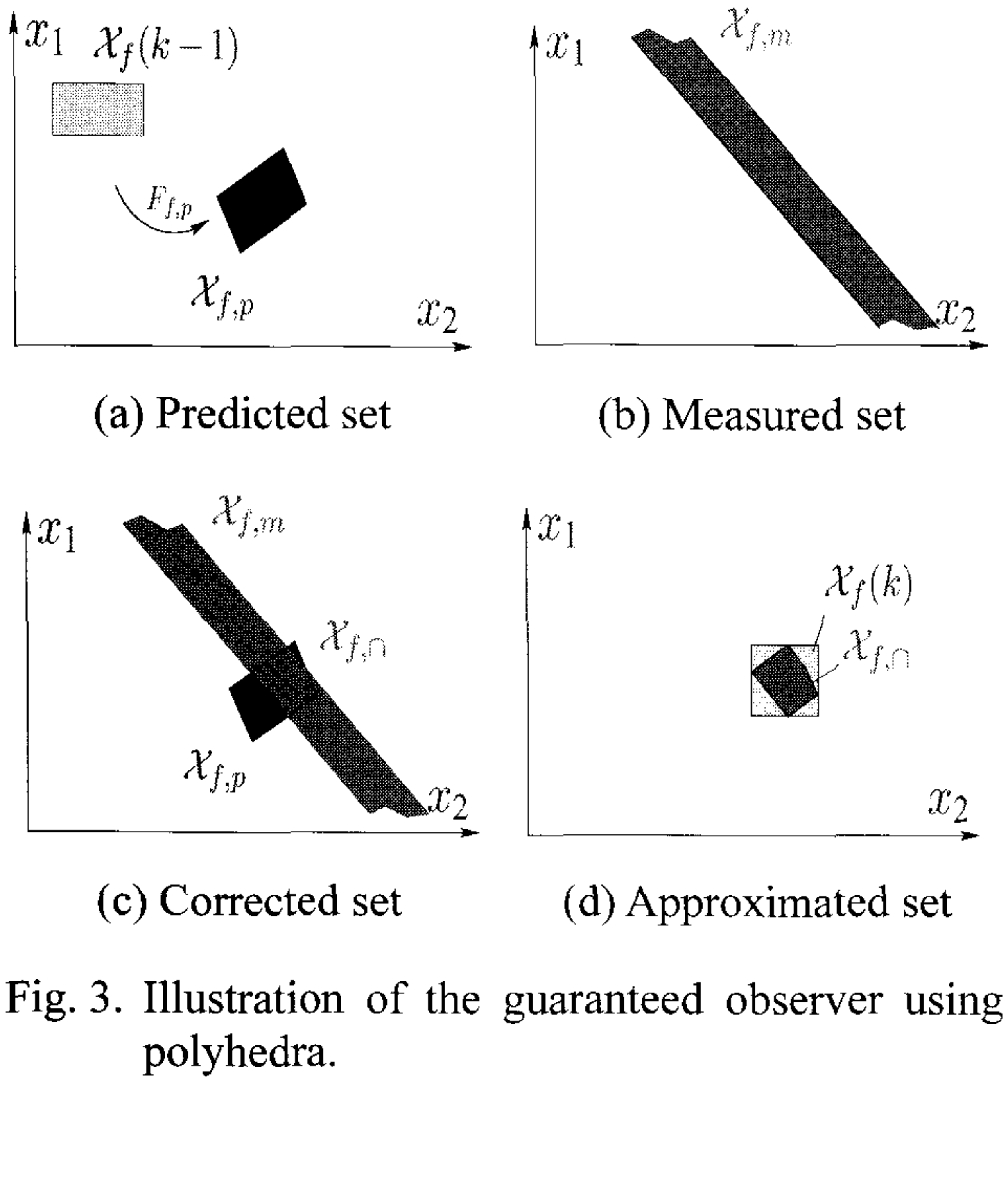
Algorithm 1 (Guaranteed Observation):

GIVEN:

- a model $\mathcal{M}_f$ as in (4)-(6)
- a sequence of input and output sets $\mathcal{U}(0\ldots\bar{k})$ and $\mathcal{Y}(0\ldots\bar{k})$

INITIALISATION: $(k := 0)$

$$\mathcal{X}_f(0) = F_{f,m}(\mathcal{Y}(0), \mathcal{U}(0))$$



(a) Predicted set (b) Measured set

(c) Corrected set (d) Approximated set

Fig. 3. Illustration of the guaranteed observer using polyhedra.

LOOP: (until $k = \bar{k}$)

$$\mathcal{X}_f(k-1) \rightarrow \mathcal{X}_f(k)$$

1. Compute the predicted set

$$\mathcal{X}_{f,p} = F_{f,p}(\mathcal{X}_f(k-1), \mathcal{U}(k-1))$$

2. Compute the measured set

$$\mathcal{X}_{f,m} = F_{f,m}(\mathcal{Y}(k), \mathcal{U}(k))$$

3. Compute the corrected set

$$\mathcal{X}_{f,\cap} = \mathcal{X}_{f,p} \cap \mathcal{X}_{f,m}$$

4. Compute the approximated set

$$\mathcal{X}_f(k) = F_{\supseteq}(\mathcal{X}_{f,\cap}) \supseteq \mathcal{X}_{f,\cap}$$

RESULT: A sequence of current-state sets

$$\mathcal{X}_f(k) \equiv \mathcal{X}_f(k \mid 0\ldots k), \quad 0 \le k \le \bar{k}.$$

In Step 1, the operator $F_{f,p}$ is introduced as an over-approximation of the one-step prediction from (13). It encloses, the possibly non-convex set $\mathcal{X}_p^*$ into a convex set:

$$F_{f,p}(\mathcal{X}_f(k-1), \mathcal{U}(k-1)) \supseteq$$
$$\{\boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \mid \boldsymbol{x} = \boldsymbol{A}_f(\hat{\boldsymbol{p}})\hat{\boldsymbol{x}} + \boldsymbol{B}_f\hat{\boldsymbol{u}}, \qquad (15)$$
$$\hat{\boldsymbol{x}} \in \mathcal{X}_f(k-1),\ \hat{\boldsymbol{u}} \in \mathcal{U}(k-1),\ \hat{\boldsymbol{p}} \in \mathbb{P}\}.$$

In Step 2, the operator $F_{f,m}$ yields the set $\mathcal{X}_m^*$ of states that are consistent with the measurements. Its representation is extended from (14) for models with feedthrough:

$$F_{f,m}(\mathcal{Y}(k), \mathcal{U}(k)) = \{\boldsymbol{x} \in \mathbb{R}^{\mathrm{n}} \mid$$
$$(\boldsymbol{C}_f\boldsymbol{x} + \boldsymbol{D}_f\hat{\boldsymbol{u}}) \in \mathcal{Y}(k),\ \hat{\boldsymbol{u}} \in \mathcal{U}(k)\}. \qquad (16)$$

In Step 4, an operator $F_{\supseteq}$ is used to keep the mathematical representation of the sets - and hence the numerical burden of the algorithm - equally complex over time. For example, using ellipsoidal sets, the corrected set (an intersection of two ellipsoids) must be over-approximated to an ellipsoid to make the recursion possible. Using polyhedral sets, the corrected set remains a polyhedron but of increased complexity, such that a new and simpler polyhedron is sought. This step is decisive in determining either how fast or how precise the observation runs, which are two contradictory aims.

Theorem 1 (Complete Observation): The sets $\mathcal{X}_f$ reconstructed by Algorithm 1 verify

$$\mathcal{X}_f(k) \supseteq \mathcal{X}^*_f(k \mid 0 \ldots k).$$

Proof 1: The theorem is a direct consequence of the structure of the algorithm which is an implementation of the recursion from (12)-(14), using solely over-approximations. Hence, the proof is given here by recursion. For simplicity a model with no feedthrough is considered, but the result is true in general as shown in [27].

The verification for $k = 0$ is trivial by comparison of (10) with the initialisation of the Algorithm 1 using (16).

It is now assumed that the theorem's result holds true at time $k-1$. Consequently, the right hand-side of (15) is an over-approximation of $\mathcal{X}^*_p$ from (13) and, therefore, so is $\mathcal{X}_{f,p}$ computed in the Step 1.

The set $\mathcal{X}_{f,m}$ obtained within the algorithm is identical to $\mathcal{X}^*_m$ from (14). Hence, the intersection described in Step 3 remains an over-approximation of $\mathcal{X}^*(k \mid 0 \ldots k)$, and so is the set $\mathcal{X}_f(k)$ computed in Step 4. Therefore, $\mathcal{X}_f(k) \supseteq \mathcal{X}^*_f(k \mid 0 \ldots k)$ holds, which proves the theorem.

4. IMPLEMENTATION OF THE OBSERVER FOR POLYHEDRAL SETS

This section shows how the observation algorithm can be implemented using polyhedral state sets. A polyhedral set $\mathcal{X} \subset \mathbb{R}^n$ describes a convex region delimited by s linear inequalities. Let $\boldsymbol{m}_i^T$ be the rows of a matrix $\boldsymbol{M} \in \mathbb{R}^{s \times n}$ (the *faces* of the set) and q_i the elements of a vector $\boldsymbol{q} \in \mathbb{R}^s$. The facial description of a polyhedron is given by

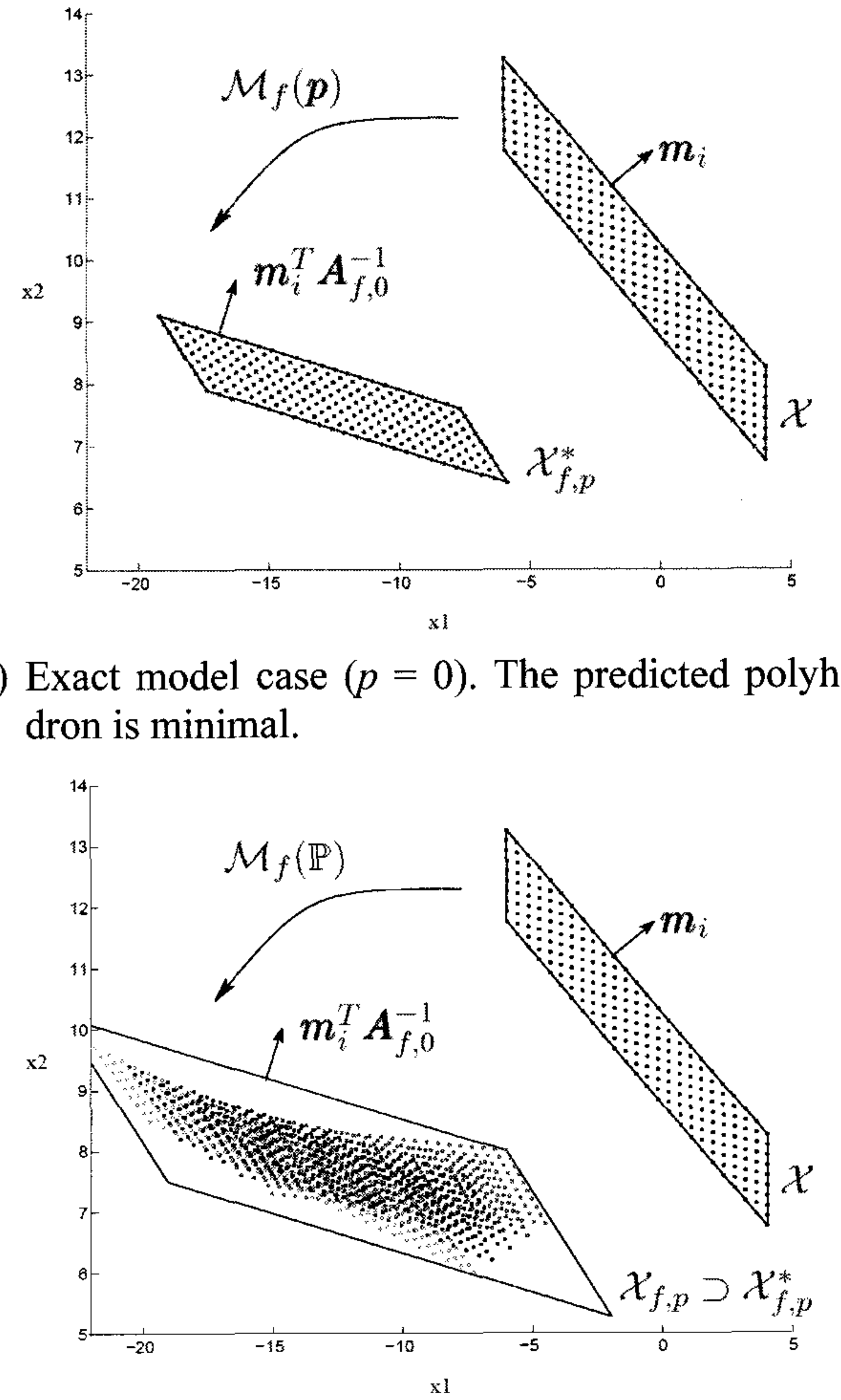
$$\mathcal{X} = \{\boldsymbol{x} \in \mathbb{R}^n \mid \boldsymbol{Mx} \leq \boldsymbol{q}\}. \tag{17}$$

4.1. Predicted set

The computation of the predicted set $\mathcal{X}_{f,p} = F_{f,p}(\mathcal{X},\mathcal{U})$ is the most complex task of the algorithm when considering model uncertainties. In the following, a conceptual description of the solution is given. The reader can find a detailed proof of the result in [27, Prop. 3.4].

In Fig. 4 the approach to compute the prediction step is graphically illustrated. The polyhedral sets thus obtained are compared to the prediction of a mesh of vectors spread over $\mathcal{X}$. If no parameter uncertainties are considered ($\boldsymbol{p} = \boldsymbol{0}$ in Fig. 4(a)), the prediction set can be exactly represented by a polyhedron, which faces are given by $(\boldsymbol{M}\boldsymbol{A}_{f,0}^{-1})$.[3] If parameter uncertainties are considered ($\boldsymbol{p} \in \mathbb{P}$ in Fig. 4(b)), the minimal predicted set represented by the mesh of vectors is not convex. The idea pursued to solve the prediction, is to enclose this non-convex set into a polyhedra, using the faces obtained if no parameter uncertainties existed. In practice, this is pertinent if one assumes that most of the model information is "contained" in $A_{f,0}$ while the uncertainty-driven information ($A_{f,j}$, $j > 0$) is of smaller magnitude.

Therefrom, the predicted set is described by



(a) Exact model case (p = 0). The predicted polyhedron is minimal.

(b) Model with uncertainty ($p \in \mathbb{P}$). The predicted polyhedron is complete.

Fig. 4. Predicted set for models without and with uncertainty.

[3] Actually, if the system is subject to an uncertain input ($e_u \neq 0$), a further set of faces must be considered to describe the minimal set. These result from a Fourier-Motzkin elimination, see [27,28]. However, it is possible not to consider these additional faces, which further over-approximates the set.

$$\mathcal{X}_{f,p} = \{x \in \mathbb{R}^n \mid MA_{f,0}^{-1}x \le h\} \tag{18}$$

with, for all $i \in \{1,\ldots,s\}$,

$$\begin{aligned} h_i := q_i &+ \max_{u \in \mathcal{U}}(m_i^T A_{f,0}^{-1} B_f u) \\ &+ \sum_{j=1}^{N_p} \max[p_j^{min} \min_{x \in \mathcal{X}}(m_i^T A_{f,0}^{-1} A_{f,j} x), \\ &\qquad p_j^{min} \max_{x \in \mathcal{X}}(m_i^T A_{f,0}^{-1} A_{f,j} x), \\ &\qquad p_j^{max} \min_{x \in \mathcal{X}}(m_i^T A_{f,0}^{-1} A_{f,j} x), \\ &\qquad p_j^{max} \max_{x \in \mathcal{X}}(m_i^T A_{f,0}^{-1} A_{f,j} x)]. \end{aligned} \tag{19}$$

The explanation of this result is given here for an autonomous system $(u = 0)$. Having imposed the faces of the sought polyhedron (18), one solely needs to determine an appropriate value for h. This value must assure an inclusion of the minimal predicted set, i.e., it must enclose all possible vectors $\hat{x} = A_f(p)x$, $\forall p \in \mathbb{P}$ and $\forall x \in \mathcal{X}$. Hence, for all $i = \{1,\ldots,s\}$, let

$$\begin{aligned} h_i^* &:= \max_{\substack{p \in \mathbb{P} \\ \hat{x} \in \mathcal{X}_{f,p}}} (MA_{f,0}^{-1}\hat{x}) = \max_{\substack{p \in \mathbb{P} \\ \hat{x} \in \mathcal{X}}} (MA_{f,0}^{-1} A_f(p) x) \\ &= \max_{\substack{p \in \mathbb{P} \\ \hat{x} \in \mathcal{X}}} MA_{f,0}^{-1}(A_{f,0}x + \sum_{j=1}^{N_p}(p_j A_{f,j} x)). \end{aligned}$$

This optimisation cannot be easily solved, but an overapproximation of the solution is derived using the expansion rule $\max(a + b) \le (\max(a) + \max(b))$, such that:

$$\begin{aligned} h_i^* \le h_i &:= \max_{x \in \mathcal{X}}(MA_{f,0}^{-1} A_{f,0} x) \\ &+ \sum_{j=1}^{N_p}(\max_{\substack{p_j^{\min} \le p_j \le p_j^{\max} \\ x \in \mathcal{X}}} (p_j MA_{f,0}^{-1} A_{f,j} x)). \end{aligned}$$

The consideration of an input signal does not change the above approximation concept, since the expansion of the max-operator can be done in the same way. The first term is exactly q_i as defined in (17) and each summand in the second term can be expanded by further over approximation, resulting in (19).

Using this approach, it is then possible to compute an over-approximation of (13), without having to explicitly compute the product $A_f(p)x$, $\forall x \in \mathcal{X}$, $\forall p \in \mathbb{P}$. Furthermore, uncertainties in the input matrix may be considered in the exact same way, using a structural decomposition of the term $B_f(p)u$.

4.2. Measured set

The measured set $\mathcal{X}_{f,m} = F_{f,m}(\mathcal{Y},\mathcal{U})$ can always be described using polyhedra, since no parameter uncertainties occur in (5). It is given by

$$\mathcal{X}_{f,m}^* = \{x \in \mathbb{R}^n \mid Nx \le h\}$$

with $N := \begin{bmatrix} C_f \\ -C_f \end{bmatrix} \in \mathbb{R}^{2r \times n}$ and the vector $h = (h_1, \ldots, h_{2r})^T \in \mathbb{R}^{2r}$ defined as

$$\begin{aligned} h_i &:= y_i^{\max} - \min_{u \in \mathcal{U}}(d_{f,i}^T u), \\ h_{r+i} &:= -(y_i^{\min} - \max_{u \in \mathcal{U}}(d_{f,i}^T u)) \end{aligned}$$

for $i = 1,\ldots,r$ and with $d_{f,i}^T$ the i-th row of D_f.

4.3. Corrected set

The computation of the corrected set $\mathcal{X}_{f,\cap} = \mathcal{X}_{f,p} \cap \mathcal{X}_{f,m}$ is straightforward: using the facial description of the polyhedra, the intersection is obtained by appending all inequalities of one set to another. (This is not an efficient implementation but is sufficient because of the later approximation step.)

4.4. Approximated set

The approximated set $F_{\supset}(\mathcal{X}_{f,\cap})$ is determined to avoid that the number of constraints describing the set of states increases with each loop. This is made necessary since the intersection operation (and possibly the Fourier-Motzkin elimination, cf. Footnote 3) results in many redundant inequalities. These increase the complexity of the state set description in each recursion loop, although not modifying its geometric shape. A removal of these redundant constraints is possible, as described in [29], however this step is very time consuming and is not necessary since we now search an inclusion of the corrected set in a polyhedron of fixed size (with μ faces).

Let $W = \begin{bmatrix} w_1^T \\ w_\mu^T \end{bmatrix}$ be some chosen faces. An over-approximation of $\mathcal{X}_{f,\cap}$ is obtained as

$$F_{\supset}(\mathcal{X}_{f,\cap}) = \{x \in \mathbb{R}^n \mid Wx \le z\}$$

with, for all $i \in \{1,\ldots,\mu\}$

$$z_i := \max_{x \in \mathcal{X}_{f,\cap}} (w_i^T x).$$

The approximated set can only be computed if $\mathcal{X}_{f,\cap}$ is a bounded polyhedron (i.e., a polytope). Hence, the computation of the approximated set is skipped in the first loops of the algorithm until the state sets are bounded. As shown in [27], this is generally achieved after v loops, where $v \leq n$ is the observability index of model $\mathcal{M}_f$. It is emphasized that this permits to use the algorithm without any (bounded) initial state-set to begin the recursion. This is an important prerequisite for completeness (although, in practice, an initial set could be chosen extremely large). Instead, this approach uses the first measurements of the output sequence to construct a bounded state-set over a finite number of recursions.

A trivial choice for the over-approximation faces is $\boldsymbol{W} = \begin{bmatrix} \boldsymbol{I}_n \\ -\boldsymbol{I}_n \end{bmatrix}$, with $\boldsymbol{I}_n$ the n-dimensional identity matrix. In this case, the resulting polytope is enclosed between axis-parallel faces, i.e., it is a hypercube or interval set. As shown in [27], a further choice could be to define $\boldsymbol{W}$ using the observability matrix

$$\boldsymbol{S}_f = \begin{bmatrix} \boldsymbol{C}_f \\ \boldsymbol{C}_f \boldsymbol{A}_{f,0}^{-1} \\ \vdots \\ \boldsymbol{C}_f \boldsymbol{A}_{f,0}^{-n+1} \end{bmatrix},$$

letting $\boldsymbol{W} = \begin{bmatrix} \boldsymbol{S}_f \\ -\boldsymbol{S}_f \end{bmatrix}$ and pursuing the over-approximation only every n-steps.

4.5. Computational burden

An overview of the computational burden implied by the proposed algorithm is presented in Table 1. Noticeably the linear programs over the set $\mathcal{U}$ may be solved explicitly, since the set is an hypercube, which further improves the proposed implementation.

One advantage of using a polyhedral implementation is the possibility *not* to compute an over-approximated set in each recursion. This greatly increases the accuracy of the observation, while remaining within a possibly acceptable computational cost. In such a case, the computational burden is not constant in each recursion, but increases until the next fixed-size over-approximation is determined. Since the observation is more precise, so may be the underlying diagnosis described in the next section. Pursuing such a moving horizon strategy is dependent both on the available resources as well as on the currently investigated system.

Table 1. Computational burden for guaranteed observation. (The notation q-LP($\mathcal{X}$) indicates q linear programs have to be solved over the constraints describing $\mathcal{X}$.)

Set	Faces	Optimisations
$\mathcal{X}_f(k)$	s	None, the set is given
$\mathcal{X}_{f,p}(k+1)$	s	s-LP($\mathcal{U}$)+2N_p-LP($\mathcal{X}_f$)
$\mathcal{X}_{f,m}(k+1)$	$2r$	$2r$-LP($\mathcal{U}$)
$\mathcal{X}_{f,\cap}(k+1)$	$s+2r$	None, trivial intersection
$\mathcal{X}_f(k+1)$	$\mu = s$	μ-LP($\mathcal{X}_{f,\cap}$)

5. DIAGNOSIS BASED ON GUARANTEED OBSERVATION

5.1. Consistency and diagnosis

Using the following theorem, the result of the guaranteed observation is used to verify the consistency of models with set-valued input and output measurements.

Theorem 2 (Consistency and observation)**:** A model that is consistent with a sequence of input and output sets yields a non-empty guaranteed state-observation result:

$$\mathcal{M}_f \vDash (\mathcal{U}(0\ldots\bar{k}), \mathcal{Y}(0\ldots\bar{k})) \Rightarrow \mathcal{X}_f(\bar{k}) \neq \varnothing.$$

Proof 2: According to Definition 2, the model is consistent if $\exists \boldsymbol{x}(0)$ such that (8) holds. Hence, the relation $\mathcal{X}_f^*(0\,|\,0\ldots\bar{k}) \neq \varnothing$ holds. From Theorem 1, the relation $\mathcal{X}_f(\bar{k}) \neq \varnothing$ follows, which proves the theorem.

Clearly, based on a non-empty set-observation result, it cannot be assured that a model is consistent with the measurements (this would be the opposite of the theorem!). However, an *empty state-set* does prove the *inconsistency* of the model. Consequently, the result of the guaranteed observation can be interpreted for diagnosis using the emptiness criteria as follows.

Definition 5 (Induced set of faults)**:** Let $\mathcal{X}_f$ be the sets resulting from a guaranteed observation using different models $\mathcal{M}_f, f \in \mathbb{F}$. The set of faults induced by the observer is $\mathcal{F}(k) := \{f \in \mathbb{F} \,|\, \mathcal{X}_f(k) \neq \varnothing\}$.

Theorem 3 (Complete Diagnosis)**:** The set of faults induced by a guaranteed observer is complete: $\mathcal{F}(\bar{k}) \supseteq \mathcal{F}^*(0\ldots\bar{k})$.

Proof 3: From the description of the diagnostic problem in (9) it is known that for all $f \in \mathcal{F}^*(0\ldots\bar{k})$ the relation $\mathcal{M}_f \vDash (\mathcal{U}(0\ldots\bar{k}), \mathcal{Y}(0\ldots\bar{k}))$ holds. Theorem 2 implies $\mathcal{X}_f(\bar{k}) \neq \varnothing$ and hence, based on Definition 5, $f \in \mathcal{F}(\bar{k})$.

5.2. Diagnostic algorithm

By using the notion of consistency and the guaranteed state-set observation to test the consistency, the following diagnostic algorithm is obtained.

Algorithm 2 (Diagnostic algorithm):

GIVEN:

- the models $\mathcal{M}_f, f \in \mathbb{F}$ as (4)-(6)
- the sequence of input and output sets $\mathcal{U}(0\ldots\bar{k})$ and $\mathcal{Y}(0\ldots\bar{k})$

INITIALISATION: $(k := 0)$

$$\mathcal{X}_f(0) = F_{f,m}(\mathcal{Y}(0), \mathcal{U}(0)), \ \forall f \in \mathbb{F}$$

$$\mathcal{F}(0) := \{f \in \mathbb{F} | \mathcal{X}_f(0) \neq \varnothing\}$$

LOOP: (until $k = \bar{k}$)

$$\mathcal{X}_f(k-1), \mathcal{F}(k-1) \to \mathcal{X}_f(k), \mathcal{F}(k)$$

1. Compute the state sets $\mathcal{X}_f(k)$, for all $f \in \mathcal{F}(k-1)$, using Algorithm 1 recursively with $\mathcal{X}_f(k-1)$ and the measurement sets $\mathcal{U}(k-1)$, $\mathcal{U}(k)$ and $\mathcal{Y}(k)$.
2. Determine the induced set of faults

$$\mathcal{F}(k) := \{f \in \mathcal{F}(k-1) | \mathcal{X}_f(k) \neq \varnothing\}.$$

RESULT: The sequence of induced fault sets $\mathcal{F}(k)$, $0 \le k \le \bar{k}$.

The diagnostic algorithm yields the following diagnostic results:

Proposition 2: The result of Algorithm 2 is interpreted as follows:

- A fault is *detected* at time k, if and only if the model of the faultless behaviour is inconsistent with the measurements, hence if and only if $\exists k \le \bar{k}$ such that $f_0 \notin \mathcal{F}(k)$.
- A fault f_i is *unambiguously identified* at time k, if and only if $\exists k \le \bar{k}$ such that $\mathcal{F}(k) = \{f_i\}$. In this case the true fault is exactly known: $f^\circ \equiv f_i$.

The success of the diagnosis is of course relative to the given information. First, just as for any diagnosis, the considered measurement signals must capture a behaviour of the system which allows a distinction. An actuator failure can never be detected, if the given measurements do not include an excitation of this actuator. Second, since uncertainties are considered, the fault behaviour must be "sufficiently different" from the faultless behaviour such that the fault may be identified, despite the uncertainties. Therefore, while the bounds $e_u(k)$ and $e_y(k)$ - which account for the size of the sets $\mathcal{U}$ and $\mathcal{Y}$ - must be sufficiently large for Assumption 4 to hold true, setting these bounds too conservatively may prevent to detect inconsistencies, and hence the faults. The same holds true for the modeling uncertainties.

The length of the given input and output sequences also plays a role in the diagnosis. For example, if a fault distinguishes itself only in its dynamical behaviour, then the sequences should be long enough (with respect to the time constants) to capture the characteristic differences in the behaviours. Long sequences tend to lead to good diagnostic results since the underlying state-sets tend to converge[4] over time for stable models (i.e., $|\det(A_f)| < 1$). Shorter sequences, however, are more prone to respect Assumption 3.

5.3. Implementation of the diagnostic algorithm

Based on the guaranteed observation algorithm from Section 4, the implementation of the proposed diagnosis only needs one additional operation: an emptiness criterion (cf. the consistency check in Step 2 of Algorithm 2). A polyhedron (17) is empty if and only if

$$\alpha_{\min} := \min_{Mx \le q + 1\alpha} \alpha$$

has a strictly positive solution ($\alpha_{\min} > 0$), cf. [30]. This test is a linear program in the variable (αx^T).

In each step of the diagnostic algorithm, it is verified which models lead to a non-empty state-set observation result. The faults corresponding to these models cannot be asserted not to have occurred and, hence, are kept in the set of faults, which represent the (complete) diagnostic result.

6. NUMERICAL EXAMPLE

The guaranteed diagnoser is demonstrated by the following example in which a motor brings a rod to a desired angular position using a proportional controller (Fig. 5). The process is described by the second order differential equation

$$J\ddot{\theta} = -k_v\dot{\theta} - k_p\theta + k(\theta_{ref} - \theta), \tag{20}$$

with θ, $\dot{\theta}$ and $\ddot{\theta}$ the angular position and its derivatives, θ_{ref} the angular set-point. The process parameters J, k_v, k_p and k are given for four distinct fault behaviours in Table 2.

The state-space models $\mathcal{M}_f$, $f \in \mathbb{F} = \{f_0, f_1, f_2, f_3\}$ needed to apply Algorithm 2 are obtained by discretising the continuous-time model (20) for the different parameters and the sampling time

[4] The convergence is not necessarily true in case of non-zero input or parameter uncertainties.

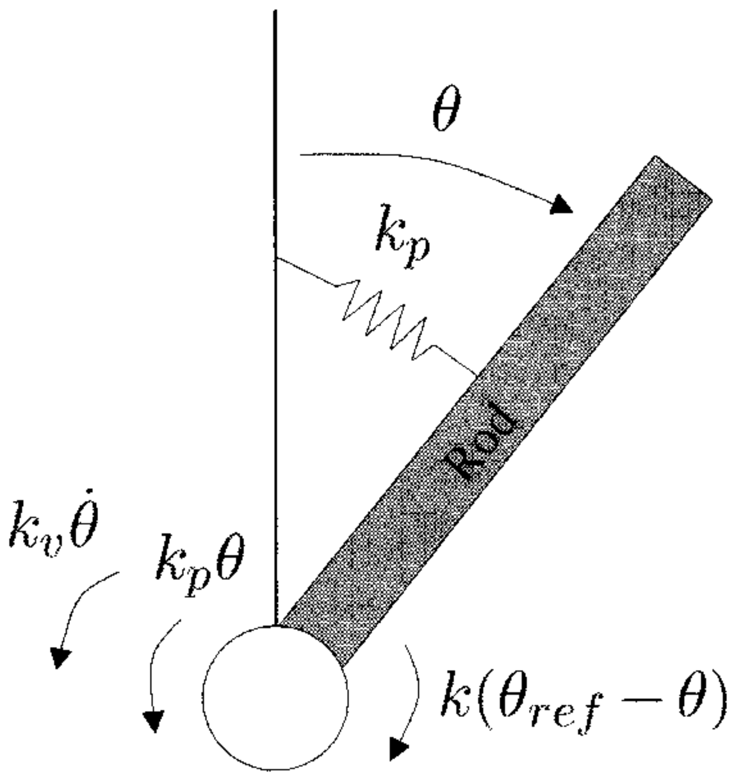


Fig. 5. Example of rotating rod.

Table 2. Process true parameters (S.I. units).

Parameter	Description
$k = 10$	Controller gain
$k_p = 0.02$	Friction in the position
$k_v = 0.90$	Friction in the velocity ($f_i, i \neq 3$)
$k_v = 1.60$	Friction in the velocity (f_3)
$J = 0.7$	Inertia (f_0, f_3)
$J = 1.3$	Inertia (f_1)
$J = 2.0$	Inertia (f_2)

$T_s = 0.02s$. The state vector $x = (\theta\ \dot{\theta})^T$, the input $u = \theta_{ref}$ and the output $y = \theta$ are used. The model of the faultless behaviour $\mathcal{M}_{f_0}$ is given here:

$$A_{f_0} = \begin{bmatrix} 0.997 & 0.020 \\ -0.282 & 0.972 \end{bmatrix}, \quad \mathbb{P}=\{\mathbf{0}\},$$

$$B_{f_0} = \begin{bmatrix} 0.003 \\ 0.281 \end{bmatrix},$$

$$C_{f_0} = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

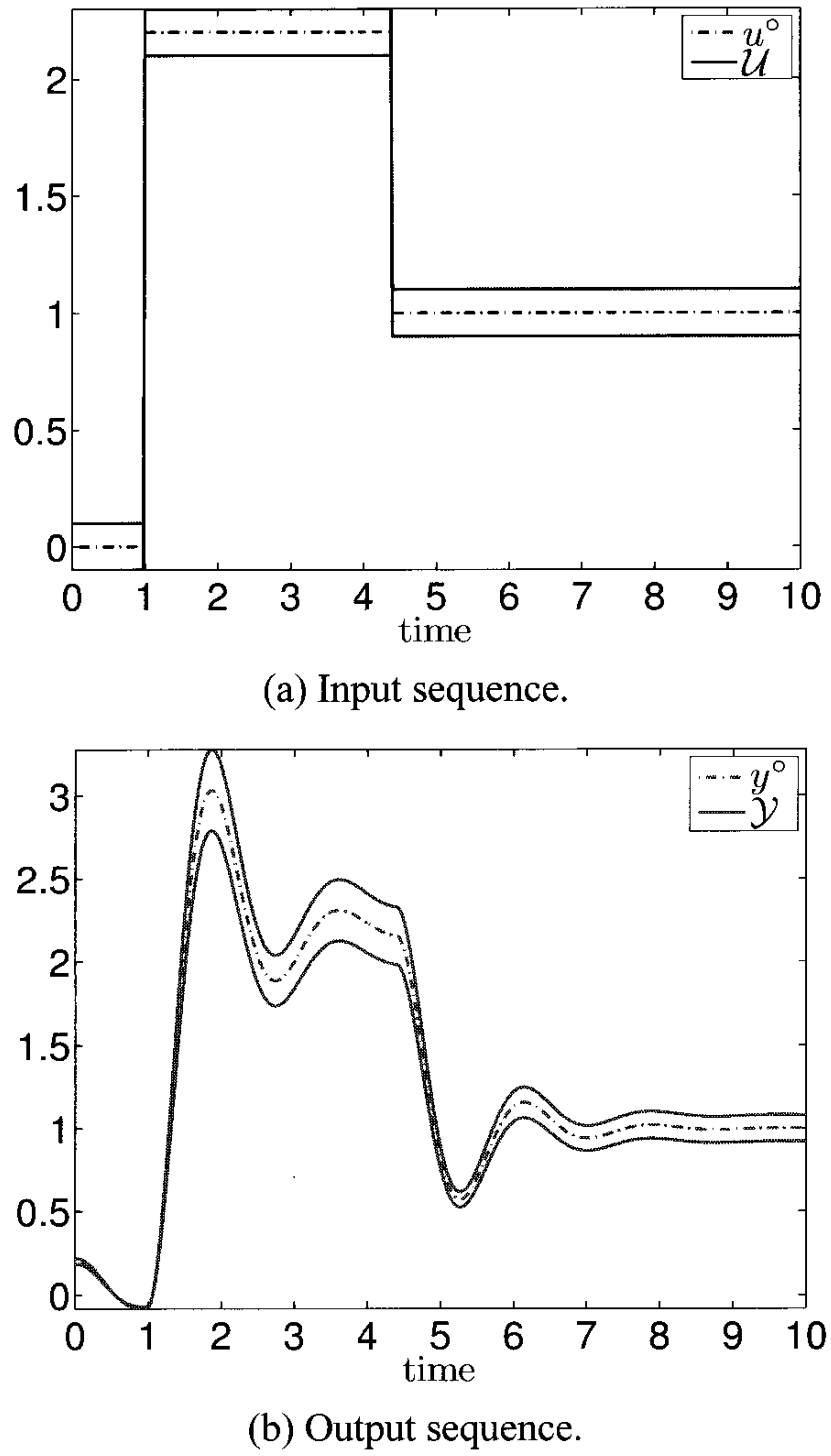
$$D_{f_0} = 0.$$

For simplicity the behaviours of faults f_0, f_2 and f_3 are assumed exactly known ($\mathbb{P}=\{\mathbf{0}\}$). The behaviour for fault f_1 is known except for an uncertainty in the process inertia $J \in [0.9, 1.3]\mathrm{kg\,m}^2$. Note that this interval includes the true value $J = 1.3$.

An experiment is considered for which the given input and output data are plotted in Fig. 6. Applying Algorithm 2 yield both an observation result for each model and a diagnosis. The sequences of sets $\mathcal{X}_f$, $f \in \mathbb{F}$, resulting from the guaranteed observation are drawn in Fig. 7. By projecting the sets on each dimension of the state-space $\mathbb{R}^2$, the polyhedra are represented in a simplified manner as intervals.

The diagnostic result is shown in Fig. 8. The interruption of the bars in the diagram emphasises at what time a given model becomes inconsistent with the input and output measurements. For example, the model of the faultless behaviour f_0 becomes inconsistent with the measurements at time $t' = 1.66s$ and, hence, a fault is detected ($f_0 \notin \mathcal{F}$). As the model of two other fault situations are likewise proven to be inconsistent with the measurements, the fault f_3 is unambiguously identified.

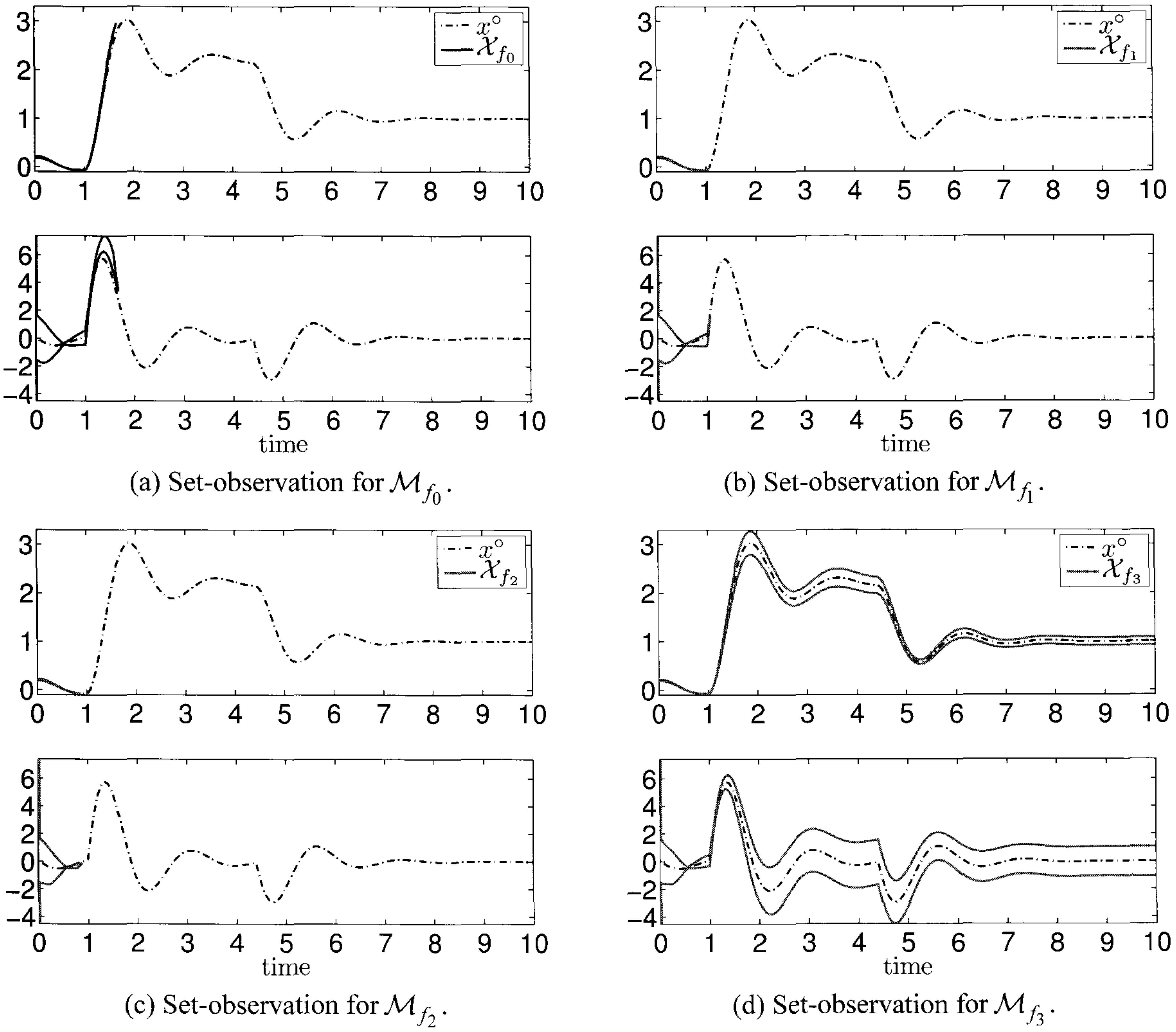
The computation effort needed for this solution is manageable. Using MATLAB on a Pentium IV 1500MHz with 512Mb of memory, this example requires roughly 80ms to compute each time step for each considered model.



(a) Input sequence.

(b) Output sequence.

Fig. 6. Input and output sets for an experiment under fault behaviour $f^\circ = f_3$ (solid lines: edges of the interval sets, dashed lines: true measurements).



(a) Set-observation for $\mathcal{M}_{f_0}$.

(b) Set-observation for $\mathcal{M}_{f_1}$.

(c) Set-observation for $\mathcal{M}_{f_2}$.

(d) Set-observation for $\mathcal{M}_{f_3}$.

Fig. 7. State-set observations for all fault models $\mathcal{M}_{f_i}, i \geq 0$. All faults, except f_3, become inconsistent with the measurements.

While the graphical representation of the observation results in Fig. 7 causes the proposed approach to look similar to an interval-based method, this is not exact. Indeed, in each recursion of the observer, the predicted set $\mathcal{X}_{f,p}$ is a polyhedron and, in general, not a hypercube. If this intermediary set would have been represented by means of an interval set, it would have lead to further over-approximations (cf. Figs. 3(a) or 4). Using the proposed approach, the only over-approximations which occur are in the consideration of model uncertainties (predicted set) and in the final simplification (approximated set). While the former cannot be avoided using this method - or any other method based on convex sets - the latter effect may be diminished by not over-approximating in every recursion of the algorithm. Nevertheless, an actual comparison of this method with an interval-based approach remains open.

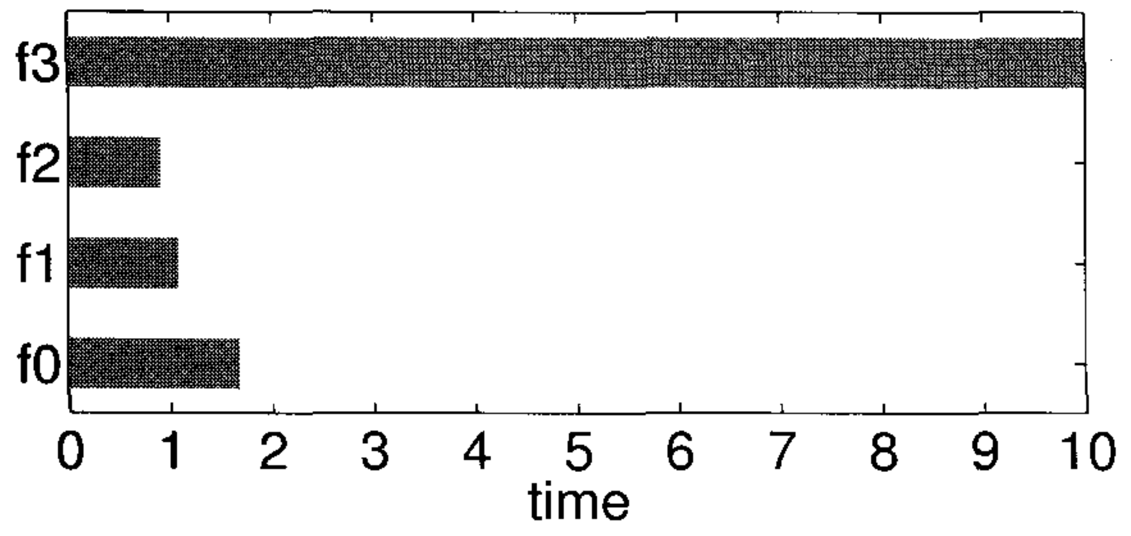


Fig. 8. Consistency of fault models over time.

7. CONCLUSIONS

A method for fault diagnosis based on a guaranteed state observer is presented. The observation allows to verify the consistency of uncertain state-space models with sequences of set-valued input and output measurements. The set-valued approach offers robustness of the diagnostic result with respect to explicitly described measurement and modeling errors.

To the author's knowledge, the approach to consider structured model uncertainties and the diagnosis derived therefrom are new. The solution is based on the decomposition of the uncertainties in the system and input matrices such that an over-approximation using a polyhedral state observer is found. This approach allows to derive a set of faults which represents a complete diagnosis.

While a resemblance seems to exist with methods based on interval analysis, a more precise result can be expected using a polyhedral set-valued method since the underlying computations are less conservative.

REFERENCES

[1] R. J. Patton, P. M. Frank, and R. N. Clark, *Issues of Fault Diagnosis for Dynamic Systems*, Springer, 2000.

[2] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, Springer, Heidelberg, 2006.

[3] R. Isermann, "Modellgestützte Überwachung und Fehlerdiagnose technischer Systeme, Teil 1," *Automatisierungstechnische Praxis*, vol. 5, pp. 9-20, 1996.

[4] J. J. Gertler, *Fault Detection and Diagnosis in Engineering Systems*, Marcel Dekker, 1998.

[5] J. C. Geromel and M. C. de Oliveira, "H2 and H∞ robust filtering for convex bounded uncertain systems," *IEEE Trans. on Automatic Control*, vol. 46, no. 1, pp. 100-107, 2001.

[6] F. C. Schweppe, "Recursive state estimation: Unknown but bounded errors and system inputs," *IEEE Trans. on Automatic Control*, vol. 13, no. 1, pp. 22-28, February 1968.

[7] F. L. Chernousko, *State Estimation for Dynamic Systems*, CRC Press, 1994.

[8] H. S. Witsenhausen, "Sets of possible states of linear systems given perturbed observations," *IEEE Trans. on Automatic Control*, vol. 13, no. 5, pp. 556-558, October 1968.

[9] L. Chisci, A. Garulli, and G. Zappa, "Recursive state bounding by parallelotopes," *Automatica*, vol. 32, no. 7, pp. 1049-1055, 1996.

[10] L. Jaulin, M. Kieffer, O. Didrit, and E. Walter, *Applied Interval Analysis*, Springer-Verlag, London, 2001.

[11] V. Puig, J. Quevedo, T. Escobet, and S. de las Heras, "Passive robust fault detection approaches using interval models," *Proc. of the 15th IFAC World Congress*, Barcelona, 2002.

[12] B. T. Polyak, S. A. Nazin, C. Durieu, and E. Walter, "Ellipsoidal parameter or state estimation under model uncertainty," *Automatica*, vol. 40, no. 7, pp. 1171-1179, 2004.

[13] T. Alamo, J. M. Bravo, and E. F. Camacho, "Guaranteed state estimation by zonotopes," *Automatica*, vol. 41, no. 6, pp. 1035-1043, 2005.

[14] P. Guerra, V. Puig, and A. Ingimundarson, "Robust fault detection using a consistency-based state estimation test considering unknown but bounded noise and parametric uncertainty," *Proc. of European Control Conference*, pp. 1595-1601, Kos, Greece, 2007.

[15] J. S. Shamma and K.-Y. Tu, "Approximate setvalued observers for nonlinear systems," *IEEE Trans. on Automatic Control*, vol. 42, no. 5, pp. 648-658, May 1997.

[16] V. Puig, A. Stancu, and J. Quevedo, "Passive robust fault detection using a forward-backward test," *Proc. of SAFEPROCESS*, Beijing, China, 2006.

[17] H. Janati Idrissi, F. Kratz, and J. Ragot, "Fault detection and isolation for uncertain systems," *Proc. of IEEE Conference and Decision and Control*, pp. 4748-4753, Las Vegas, 2002.

[18] H. Janati Idrissi, O. Adrot, and J. Ragot, "Residual generation for uncertain models," *Proc. of IEEE Conference and Decision and Control*, pp. 590-595, Orlando, 2001.

[19] A. Tzes and K. Le, "Fault detection for jump discrete systems," *Proc. of American Control Conference*, pp. 4496-4500, San Diego, 1999.

[20] P. Kesavan and H. J. Lee, "A set based approach to detection and isolation of faults in multivariable systems," *Computers and Chemical Engineering*, vol. 25, pp. 925-940, 2001.

[21] M. Witczak, J. Korbicz, and R. J. Patton, "A bounded-error approach to designing unknown input observers," *Proc. of the 15th IFAC World Congress*, Barcelona, 2002.

[22] F. Hamelin and T. Boukhobza, "Geometric-based approach to fault detection for multilinear affine systems," *Proc of the 16th IFAC World Congress*, Prag, 2005.

[23] F. Hamelin, H. Noura, and D. Sauter, "Fault detection method of uncertain system using interval model," *Proc. of European Control Conference*, pp. 826-831, Porto, 2001.

[24] B. J. Kuipers, *Qualitative Reasoning. Modeling and Simulation with Incomplete Knowledge*, The MIT Press, 1994.

[25] P. Planchon and J. Lunze, "Robust diagnosis using state-set observation," *Proc. of SAFEPROCESS*, Beijing, China, 2006.

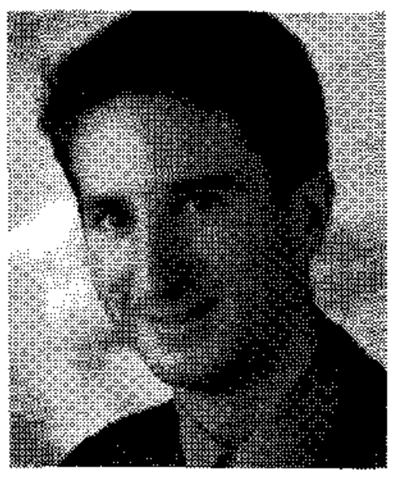
[26] J. S. Bay, *Fundamentals of Linear State Space Systems*, McGraw-Hill, 1999.

[27] P. Planchon, *Guaranteed Diagnosis of Uncertain Linear Systems using State-set Observation*, Ph.D. Thesis, Ruhr-Universität Bochum, Logos-Verlag, Berlin 2007.

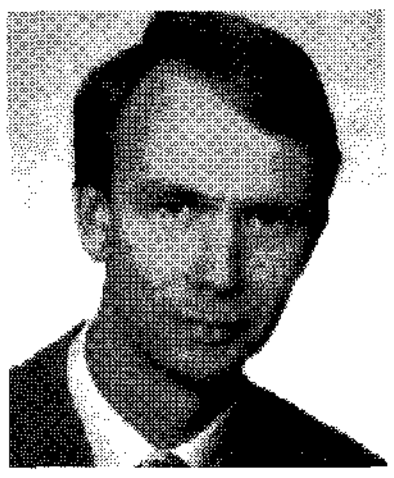
[28] S. S. Keerthi and E. G. Gilbert, "Computation of minimum-time feedback control laws for discrete time systems with state-control constraints," *IEEE Trans. on Automatic Control*, vol. 32, no. 5, pp. 432-435, May 1987.

[29] M. H. Karwan, V. Lotfi, J. Telgen, and S. Zionts, editors, *Redundancy in Mathematical Programming*, Springer, Berlin, 1983.

[30] E. C. Kerrigan, *Robust Constraint Satisfaction: Invariant Sets and Predictive Control*, Ph.D. Thesis, University of Cambridge, Available online, November 2000.



Philippe Planchon obtained his mechanical engineering degree from the University of Technology in Compiègne (France) in 2001, and was student at the University of Illinois in Urbana-Champaign (USA). He obtained his PhD degree from the Ruhr-University Bochum (Germany) in 2007. Since 2006 he is working for the Service department of BMW Group in Munich towards improving the overall quality and coordination of the offboard diagnosis. His research interests include diagnosis of dynamic processes, set-valued state-observation - especially polyhedric based methods - and the diagnosis of highly interconnected systems.



Jan Lunze obtained the diploma in Automatic Control at the Technical University Ilmenau in 1974. From 1974 until 1992 he was research associate and later Professor of Automatic Control at the Academy of Sciences in Dresden. 1980 and 1983 he obtained the PhD and the DrSc. degrees (Habilitation) both from the Technical University Ilmenau. From 1992 until 2001 he was Professor of Control Engineering at the Technical University Hamburg-Harburg and since 2002 he is head of the Institute of Automation and Computer Control of the Ruhr-University Bochum, where he teaches systems and control theory. Professor Lunze's research interest are in linear control theory, particularly in the fields of robust control and large-scale systems, in hybrid systems, discrete-event systems and in applications of knowledge processing to dynamical systems. Currently, his research is focused on qualitative modeling, fault diagnosis and process control applications of robust and decentralised control. He is author and co-author of numerous papers and of several books including *Regelungstechnik* (Springer 1996) and *Automatisierungstechnik* (Oldenbourg 2003) and co-author of *Diagnosis and Fault-Tolerant Control* (Springer 2003, 2006).