**Proceedings of the 13th IFAC Symposium on
Information Control Problems in Manufacturing
Moscow, Russia, June 3-5, 2009**

Component Group Diagnosability via Directional Resolution

Ivan Havel *

* *Department of Cybernetics, Faculty of Electrical Engineering, Czech Technical University, Karlovo náměstí 13, 121 35 Prague 2, Czech Republic, (e-mail: havel@labe.felk.cvut.cz)*

Abstract: This paper addresses simplification of diagnostic models of systems that can be described in propositional logic. Performing diagnostics on the entire model of a system when only a few variables are expected to be observed, is not efficient. If we know the limited set of variables which might appear in the observation, then we can simplify the diagnostic model before the diagnosis inference takes place. An extended model pruning procedure was proposed which systematically removes parts of a model that do not contribute to the overall system diagnosis. It employs an algorithm deciding component group diagnosability based on directional resolution. The paper analyses behavior of group diagnosability for different component groupings in a model. A set of general rules capturing the diagnosability changes for growing groups is derived. The pruning procedure is modified on the basis of these rules.

Keywords: diagnosability, incomplete-observation, model-based diagnostics, propositional logic, directional resolution, model simplification.

1. INTRODUCTION

The framework for this paper is *model-based diagnostics*, whose goal is to determine health of system components based on a system description and an observation of system variables. The focus is on *structured systems* which can be described within *propositional logic* (e.g. logical circuits). These systems are described by system topology and the behavior of the components.

The aim of this work is to *simplify the diagnostic model* of a system for some given conditions of observation. Suppose that we plan to diagnose a system and we already know that we cannot observe all its variables; (it is either expensive or not feasible). With such limitations, it is possible that all obtainable diagnoses claim the behavior of a certain system part is normal. Thus, this part of the system cannot ever be diagnosed as faulty. There is no point in computing diagnoses from the complete model and this knowledge should be utilized to adjust the model.

A procedure for model simplification (model pruning) which systematically removes segments of a model that do not contribute to the overall system diagnosis was proposed in Havel (2007). It uses an algorithm for deciding *component diagnosability* based on directional resolution, which was described in Havel (2006), to find a new simplified model of a system while preserving the ability to obtain all possible diagnoses of the system for a given set of observed system variables.

The weak point of the original procedure is that it examines diagnosability of only one component at a time. This way, not all models can be simplified. The extended pruning procedure was proposed in Havel (2008). It performs diagnosability examination on more incident components at once and therefore it is able to prune the model not only from its dead-ends but from inside too. This paper focuses on the concept of component-group diagnosability employed in the pruning procedure and analyses its behavior. It proposes a slight modification of the procedure on the basis of the rules derived from the analysis.

The paper is structured as follows: An introduction to component diagnosability within model-based diagnostics and the algorithm description is given in section 2. Both the original and extended model pruning procedures are discussed in section 3. In section 4, the concept of component-group diagnosability is described together with the algorithm deciding the problem. Behavior of diagnosability over all possible component groupings in a model is analysed and rules for growing groups are stated in section 5. Finally, outcomes of the analysis are summarized in section 6 and concluding remarks are given in section 7.

2. COMPONENT DIAGNOSABILITY

This section introduces the fundamentals of model-based diagnostics. Then, the concept of *component diagnosability* is explained. After that, a description of *directional resolution* is given, which is later used to construct an algorithm for deciding the diagnosability.

2.1 Model-based Diagnostics

Reiter (1987) laid the foundations for model-based diagnostics. His *diagnosis from first principles* acts on a logic-based description of a system and an observation of its behavior. It attempts to find a set of components in the system which, when assumed to be faulty, explains the abnormal behavior of the system. Reiter suggests a procedure that computes *minimal diagnoses*, i.e. diagnoses containing minimal subsets of faulty components. Together with the assumption-based truth maintenance system (ATMS) by de Kleer and Williams (1987) it can be classified among *consistency-based approaches* which compute minimal diagnoses from conflicts. The following definitions are variations of those from Darwiche (1998) adapted for diagnosis of components in Havel (2006).

Definition 1. (Component description). Description of a component X is a triple $(\mathbf{P}, \mathbf{A}, \mathbf{\Delta_X})$, where $\mathbf{P}$ and $\mathbf{A}$ are sets of atomic propositions such that $\mathbf{P} \cap \mathbf{A} = \emptyset$, and Δ_X is a set of propositional sentences constructed from atoms in $\mathbf{P}$ and $\mathbf{A}$. Here, $\mathbf{P}$ is called the set of non-assumables; $\mathbf{A}$ is called the set of assumables; Δ_X is called a database. It is required that Δ_X be consistent with every $\mathbf{A}$-instantiation.

The propositional sentences in Δ_X describe normal component behavior. The set of assumables $\mathbf{A} = \{ok1, ok2, \ldots\}$ represents the health of the component. Variables $ok1, ok2$ are called assumables since they are initially assumed to be true, i.e. the component is initially assumed to be healthy. $\mathbf{P}$ is a set of the component ports (non-assumables). Ports are the inputs and outputs of a component.

Definition 2. (Observation). Given a component X description $(\mathbf{P}, \mathbf{A}, \mathbf{\Delta_X})$, a component observation is a consistent conjunction of $\mathbf{P}$-literals.

An observation of component behavior is a sentence containing a conjunction of a subset (not necessarily all variables) of non-assumable literals, e.g. $A \wedge \neg C$.

A component is considered faulty when true valuation of assumables can no longer be justified or – the observation ϕ is inconsistent with $\Delta_X \cup \mathbf{A}$. In that case, it is necessary to relax some assumables (i.e. replace some instances of ok with $\neg ok$) in order to restore consistency. Such relaxation is called *diagnosis* providing it is consistent with the component description and observation.

Definition 3. (Diagnosis). Given a component description $(\mathbf{P}, \mathbf{A}, \mathbf{\Delta_X})$ and a component observation ϕ, a diagnosis is an $\mathbf{A}$-instantiation that is consistent with $\Delta_X \cup \{\phi\}$.

The strongest conclusion that can be drawn concerning the health of a component for a given state of its ports is called *component consequence*.

Theorem 1. (Component consequence). Let X be a component with a set of ports $\mathbf{P}$ and description Δ_X (in clausal form). If ϕ is an instantiation of atoms $\mathbf{P}$, then

$$Cons_{\mathbf{A}}^{\Delta_X}(\phi) = \bigwedge_{\alpha \in \Delta_X, \phi \models \neg \alpha_{\mathbf{P}}} \alpha_{\mathbf{A}}.$$

2.2 Component Diagnosability Definition

Diagnosability answers the question whether it is worthy to diagnose a component when we already know which of its ports can only be observed – Havel (2006).

Definition 4. (Component diagnosability). Given a component description Δ, set of component health variables $\mathbf{H}$, set of observed component ports $\mathbf{P_o}$, and set of unobserved component ports $\mathbf{P_u}$, $\mathbf{P_o} \cap \mathbf{P_u} = \emptyset$, one can state that component is diagnosable iff

$$\exists \phi_o \forall \phi_u \quad Cons_{\mathbf{H}}^{\Delta}(\phi_o \wedge \phi_u) \neq true.$$

Given the ports we cannot observe, the definition claims that if there is at least one combination of values for the remaining (observed) ports which implies abnormal behavior of the component, no matter what the values of the unobserved ports may be, the *component is diagnosable.*

■ *Example 1.* If we observe all its ports, the AND gate from figure 1a) is obviously diagnosable. When we observe only one of its ports, the component is not diagnosable. The question is, are two ports still enough for diagnosability? We may either happen to observe the output and one of the inputs (figure 1b) or only the inputs (figure 1c).

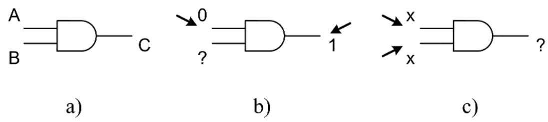

Fig. 1. An AND gate example.

The first observation case is preferable since there exists a combination (input A at zero, output C at one) that proves the component is faulty no matter what the state of the input B is. Therefore, an AND gate *is diagnosable* when observing its output and one of the inputs.

In the other case, no combination of A and B values exists that may evince component malfunction. Therefore, an AND gate *is not diagnosable* when observing only inputs.

2.3 Directional Resolution

Davis and Putnam (1960) came up with a uniform proof procedure for quantification theory. Their so-called *'refutation algorithm'*, referred to as *DP-resolution* or *directional resolution* by Rish and Dechter (2000), is an algorithm deciding propositional satisfiability. It performs resolution along a given ordering of propositional variables. Each clause is put into a bucket according to the index of its literal highest in the ordering. Resolution is always applied to clauses within one bucket and only on its respective literal. The algorithm processes the buckets starting from the highest literals. If an empty resolvent is found, i.e. there is a contradiction in the theory φ, the algorithm claims the theory is *unsatisfiable.* Otherwise, *directional extension* $E_o(\varphi)$ of φ along o is returned which contains the original buckets extended with the newly resolved clauses.

2.4 Diagnosability via Resolution

The idea behind deciding component diagnosability is based on *proof by contradiction.* Instead of looking for a specific combination of port values proving a component's malfunction, *unsatisfiability* of the theory claiming the opposite, i.e. that the component is healthy, is examined.

The theory is therefore extended with one positive literal for each component's health variable (typically one). On this extended theory, we resolve first over the health variable(s) and over the unobserved port variables (note that we are not interested in the distinction between input and output ports, the relation among them is the only thing that matters). The remaining buckets, which have not been resolved yet, belong to the observed port variables. Now, there are only two possibilities – these buckets are either empty or they contain some clauses.