

An Integration of FDI and DX Techniques for Determining the Minimal Diagnosis in an Automatic Way

Rafael Ceballos, Sergio Pozo, Carmelo Del Valle, and Rafael M. Gasca

Departamento de Lenguajes y Sistemas Informáticos, Universidad de Sevilla,
Escuela Técnica Superior de Ingeniería Informática,
Avenida Reina Mercedes s/n 41012 Sevilla, Spain

Abstract. Two communities work in parallel in model-based diagnosis: FDI and DX. In this work an integration of the FDI and the DX communities is proposed. Only relevant information for the identification of the minimal diagnosis is used. In the first step, the system is divided into clusters of components, and each cluster is separated into nodes. The minimal and necessary set of contexts is then obtained for each cluster. These two steps automatically reduce the computational complexity since only the essential contexts are generated. In the last step, a signature matrix and a set of rules are used in order to obtain the minimal diagnosis. The evaluation of the signature matrix is on-line, the rest of the process is totally off-line.

1 Introduction

Diagnosis allows us to determine why a correctly designed system does not work as expected. Diagnosis is based on a set of integrated sensors which obtain a set of observations. The aim of diagnosis is to detect and identify the reason for any unexpected behaviour, and to isolate the parts which fail in a system. The behaviour of components is stored by using constraints. Inputs and outputs of components are represented as variables of the component constraints. These variables can be observable and non-observable depending on the allocation of the sensors.

Two communities work in parallel, although separately, in model-based diagnosis: FDI (from Automatic Control) and DX (from Artificial Intelligence). Nevertheless, the integration of FDI with DX theories has been shown in recent work [1],[2]. Within the DX community the work of Reiter [3] and De Kleer and Williams [4] introduce the basic definitions and foundations of diagnosis. A general theory was proposed to explain the discrepancies between the observed and the correct behaviour by using a logical-based diagnosis process. In the FDI community, [5] and [6] presented the formalization of structural analysis, the process to obtain the ARRs (Analytical Redundancy Relation) of the system.

In this work an integration of FDI theories with the DX community is proposed, in order to improve the minimal diagnosis determination. This integration has three phases. The structural pre-treatment in the first phase and the

reduction of the model in the second phase enables the improvement of the computational complexity. The minimal diagnosis is obtained by applying an observational model to a signature matrix together with a set of compilation rules. The evaluation of the signature matrix is on-line, however the rest of the process is totally off-line.

Our paper has been organized as follows. First, definitions and notations are established in order to clarify concepts. Section 3 shows an example of the validation of this approach. Section 4 describes the advantages of the structural pretreatment. After that, in Section 5, the process for the definition of the context network is explained. Section 6 describes the determination of the minimal diagnosis. Finally, conclusions are drawn and future work is outlined.

2 Definitions and Notation

In order to clarify the diagnosis process some definitions must be established.

Definition 2.1. *System Model:* A finite set of polynomial equality constraints (P) which determine the system behaviour. This is done by means of the relations between non-observable (V_i) and observable variables (sensors) of the system (O_j).

Definition 2.2. *Observational Model:* A tuple of values for the observable variables.

Definition 2.3. *Context:* A collection of components of the system, and their associated constraints. The number of possible contexts is $2^{nComp} - 1$, where $nComp$ is the number of components of the system.

Definition 2.4. *Context Network:* A graph formed by all the contexts of the system in accordance with the way proposed by ATMS[7]. The context network has a natural structure of a directed graph for set inclusion.

Definition 2.5. *Diagnosis Problem:* A tuple formed by a system model and an observational model. The solution to this problem is a set of possible failed components.

3 Example

Figure 1a shows a polybox system. This polybox system is derived from the standard problem used in the diagnosis community [4]. The system consists of fifteen components: nine multipliers, and six adders. The observable variables are represented by shaded circles in Figure 1a.

4 Structural Pretreatment

The first part of this section shows the way to divide the diagnosis problem into independent diagnosis subproblems. The second part of this section explains the

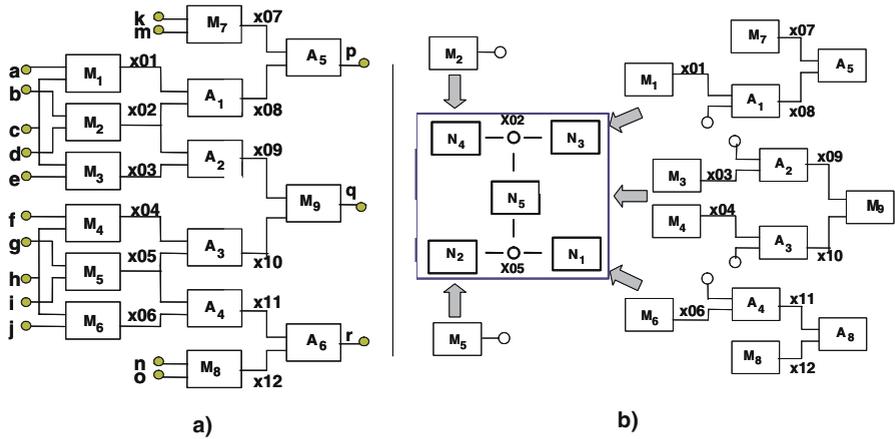


Fig. 1. a) Polybox example b) Nodes of the polybox example

way of grouping the components into nodes in order to reduce the number of non-observable variables to be considered in the system.

4.1 Identification of the Clusters

The objective of this section is the partition of the system into independent subsets of components. This partition reduces the computational complexity of the diagnosis process since it enables the generation of the diagnosis of the whole system based on the diagnosis of the subsystems.

Definition 4.1. *Cluster of components:* A set of components T is a cluster, if it does not exist a common non-observable variable of any component of the cluster with any component outside the cluster, and if for all $T' \subset T$, T' is not a cluster of components. In a cluster, all common non-observable variables among

the components belong to the same cluster, therefore all the connections with components which are outside the cluster are monitored. A cluster of components is totally monitored, and for this reason the detection of faults inside the cluster is possible without information from other components which do not belong to the cluster. A more detailed explanation and the cluster detection algorithm appears in [2].

The diagnosis space for a system initially consists of $2^{n_{Comp}}$ diagnoses [4], where n_{Comp} is the number of components of the system. Therefore the computational complexity for the diagnosis process is always smaller for an equivalent system divided into clusters, due to the reduced number of possible diagnoses.

4.2 Obtaining Relations Without Non-observable Variables

In the diagnosis process it is necessary to produce new relations without non-observable variables, in order to monitor the system behaviour by using only the

observational model. Our approach uses a function named *NewRelations* (NR) which takes a set of constraints and obtains a set of new constraints without a set of non-observable variables. Example: $\text{NR}(\{x-a-c, y-b-d, f-x-y\}, \{x, y\}) = \{a-c + b-d - f = 0\}$.

This function can be implemented using different techniques. The Gröbner Basis algorithm [8] is used here. Gröbner basis theory is the origin of many symbolic algorithms used to manipulate equality polynomials. It is a combination of Gaussian elimination (for linear systems) and the Euclidean algorithm (for univariate polynomials over a field). The Gröbner basis can be used to produce an equivalent system which has the same solution as the original, and without having non-observable variables.

4.3 Obtaining the Nodes of Each Cluster

The main assumption in this paper is to suppose that only one constraint is associated to each component. If it is necessary to apply this methodology to components with n constraints (where $n > 1$), it is then possible decoupling the component x into n virtual components x_i with one constraint each.

Our approach provides the minimal set of constraints to detect all the possible diagnoses of a system. The introduction of new definitions is necessary in order to efficiently generate this set of constraints:

Definition 4.2. *Dispensable variable:* A non-observable variable v_i is dispensable if there exist only two components x_i and x_j which include this variable in their related constraints. In the polybox example the variable x04 and the variable x08 are dispensable variables.

Definition 4.3. *Node of components:* A single component could be a node of components if none of its non-observable variables is a dispensable variable. Two components, or, a component and a node of components, belong to the same node of components if they have a common dispensable variable.

Algorithm: The algorithm for the identification of the nodes of a cluster begins by creating n nodes, where n is the number of components of the cluster. All these nodes have initially one component. When a dispensable variable v is detected, the two nodes, which include v in their constraints, are merged into one node. The process ends when all the dispensable variables are detected. Each node contains a set of constraints and a set of dispensable variables.

When all the nodes are identified, new set of constraints, without the dispensable variables is obtained, by applying the *NewRelations* function to the set of constraints of each node. If the node of components have no dispensable variables it is not necessary to apply the *NewRelations* function.

In the DX community diagnoses are determined by conflicts. Many methodologies try to use the structural description of the system, those methods are known as compilation methods. In [9] the Possible Conflicts (PCs) concept is proposed as a compilation technique. Each PC represents a subsystem within system description containing minimal analytical redundancy and being capable

Table 1. Improvements obtained using structural pretreatment in the examples

			No pretreatment		With pretreatment		
Example	Clusters	Nodes	Vars.	Ctxs. Elapsed time	Vars.	Ctxs.	Elapsed time
Polybox	1	5	12	$2^{15}-1$ 32 seconds	2	31	31 milliseconds

of becoming a conflict. Computing Analytical Redundancy Relations (ARRs)[5] is the compilation technique of FDI methodology.

Our approach provide the minimal set of contexts which include an overdetermined system of constraints that can detect a conflict in a cluster. The contexts are built by using nodes of components instead of components, since it is impossible to generate constraints without non-observable variables by using a subset of a node, because it will be impossible to substitute a dispensable variable of the node, which only appears in one component of the context.

Example: Figure 1b shows the partition of the polybox example into nodes. Table 1 shows the results obtained in the proposed example. The column *Nodes* shows the addition of all the nodes included in the clusters of the system. The column *Vars* shows the initial number of non-observable variables, and the final number of non-observable variables after the structural pretreatment. The column *Ctxs* shows the total number of possible contexts of the system, and the final number of possible contexts by using the structural pretreatment. The column elapsed time shows the necessary time to process the set of contexts of the system if the time to process one context is supposed to be 1 millisecond. In the polybox example 1 cluster is obtained. The non-observable variables are reduced from 12 to 2. Table 2 shows the list of nodes of the polybox example, and the constraint obtained in each node by eliminating the dispensable variables.

5 Determination of the Context Network

Our approach provide the minimal set of contexts which can detect a conflict in a cluster. The minimality issue was not guaranteed in the original ARR approach, but its guaranteed in our approach. In [9] approach the PCs are obtained directly by using components, but our approach use nodes instead of components,

Table 2. Nodes for the polybox example

Nodes	Components	Constraints	Dispensable var.	Non-Obs var.
N_1	$M_6M_8A_4A_6$	$h-j + n \cdot o - r + x05$	{x06, x11, x12}	{x05}
N_2	M_5	$g \cdot i - x05$	{}	{x05}
N_3	$M_1M_7A_1A_5$	$a \cdot c + k \cdot m - p + x02$	{x01, x07, x08}	{x02}
N_4	M_2	$b \cdot d - x02$	{}	{x02}
N_5	$M_3M_4M_9A_2A_3$	$q - (f \cdot h + x05) \cdot (x02 + c \cdot e)$	{x03, x04, x09, x10}	{x02, x05}

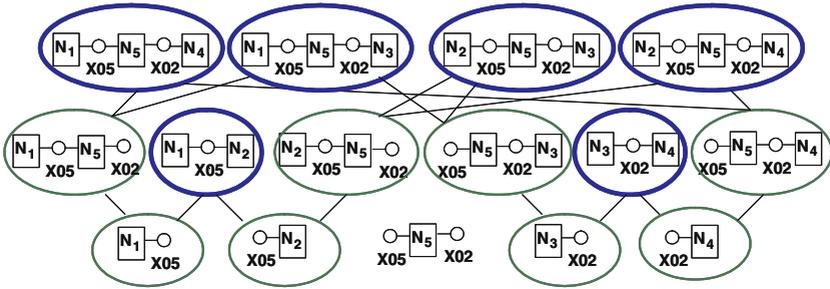


Fig. 2. Context network of the polybox example

therefore the size of the problem is reduced from 2^c , where c is the number of components, to 2^n , where n is the number of nodes.

A context network, in accordance with the way proposed by ATMS[7], is generated in order to obtain all the relevant contexts for the diagnosis process. In order to establish the smallest set of contexts it is necessary to introduce the following definitions.

Definition 5.1. *Structural context:* This is a context where all the nodes are connected, that is, they compose a connected graph, and all the non-observable variables appear in at least two constraints. The function to determine which are structural contexts is named *isAStructural* and takes a context C and returns a true value if it is a structural context.

Definition 5.2. *Minimal completed context:* A structural context C is a completed context if the set of constraints of the nodes of the context is an overdetermined system of constraints, and, if it is possible to generate new constraints without non-observable variables by using the set of constraints of the context. A completed context is minimal if no context $C' \subset C$ exists such that C' is a completed context.

If C is a minimal completed context then all the context C' exists, where $C \subset C'$, can only generate constraints which can be generated with context that contains fewer nodes. Therefore, if a context C is a minimal completed context it

Table 3. CARCs obtained in the polybox example

Index	Context	CARC
1	N_1N_2	$h \cdot j + n \cdot o - r + g \cdot i$
2	N_3N_4	$a \cdot c + k \cdot m - p + b \cdot d$
3	$N_1N_3N_5$	$q - (f \cdot h - h \cdot j - n \cdot o + r) \cdot (-a \cdot c - k \cdot m + p + c \cdot e)$
4	$N_1N_4N_5$	$q - (f \cdot h - h \cdot j - n \cdot o + r) \cdot (b \cdot d + c \cdot e)$
5	$N_2N_3N_5$	$q - (f \cdot h + g \cdot i) \cdot (-a \cdot c - k \cdot m + p + c \cdot e)$
6	$N_2N_4N_5$	$q - (f \cdot h + g \cdot i) \cdot (b \cdot d + c \cdot e)$

is not necessary to process contexts C' such that $C \subset C'$, since it is not possible to generate new relevant constraints for the diagnosis process.

The algorithm which generates the contexts of each cluster has n stages, first the context with 1 node are obtained, then the context with 2 nodes, until it reaches the context with n nodes, where n is the number of nodes. The function *NewRelations* is only applied to the contexts which are structural contexts. When a minimal completed context C is found, the new constraints without non-observable variables are stored, and no contexts C' , such that $C \subset C'$, are generated. These new constraints are named Context Analytical Redundancy Constraint.

Definition 5.3. *Context Analytical Redundancy Constraint (CARC):* A constraint obtained from a minimal completed context in such a way that only the observed variables are related.

Example: In order to clarify this section, Tables 2 and 3 shows the results obtained for the polybox example. This system includes only one cluster with 15 components. The number of possible contexts is reduced from $2^{15}-1$ to 2^5-1 . By applying the rules and the algorithm proposed in this section, 14 contexts of the possible 31 (2^5-1) are generated, however only 6 are minimal completed contexts. These 6 contexts generate 6 CARCs. Figure 2 shows the context network of the polybox example. Only the treated contexts are circled. The minimal completed contexts are circled in bold.

6 Determination of the Minimal Diagnoses

The last step is the determination of the minimal diagnoses using the set of CARCs. In order to clarify the methodology, we suppose that the sensor observations are correct. We propose using a signature matrix as in FDI, but in order to obtain the same minimal diagnoses as in DX approach, it is necessary to apply a set of rules which guarantee the no-exoneration case in the solution.

Definition 6.1. *Fault signature:* Given a set of n CARCs, denoted $CARC = \{CARC_1, CARC_2, \dots, CARC_n\}$, and a set of m faults denoted $F = \{F_1, \dots, F_m\}$, the signature of a fault F_j is given by $FS_j = [s_{1j}, \dots, s_{nj}]^T$ in which $s_{ij} = 1$ if the context which generated the $CARC_i$ involves the nodes included in the fault F_j , and $s_{ij} = 0$ otherwise.

Definition 6.2. *Signature matrix:* All the signatures for the set of possible faults constitute the signature matrix.

Definition 6.3. *Signature of an observation:* This is given by $OS = [OS_1, \dots, OS_n]$ where $OS_i = 0$ if the $CARC_i$ is satisfied, and $OS_i = 1$ otherwise.

Definition 6.4. *Diagnosis set:* The set of faults whose signatures are consistent with the signature of the observational model. Our approach assumes that an observation signature OS is consistent with another signature FS_j if $OS_i = s_{ij} \forall i$.

Definition 6.5. *Minimal diagnosis:* A fault F_j is a minimal diagnosis if F_k is not a diagnosis \forall faults $F_k \subset F_j$.

Table 4 shows the signature matrix for the polybox example in order to clarify these definitions and the process to obtain the minimal diagnoses. The signature $OK = [0, \dots, 0]^T$ represents the no-fault case. The signature matrix is very similar to the corresponding matrix in the FDI methodology. However in our approach, the faults involve nodes instead of components.

In this example it is necessary to expand the number of columns of the signature matrix in order to consider multiple faults. Each fault F_j , which involves n nodes, is obtained using a fault F_k , which involves $n-1$ nodes, and a simple fault F_s which is not involved in F_k . The multiple fault signature F_j is given by $FS_j = [s_{1j}, \dots, s_{nj}]^T$ in which $s_{ij} = 0$ if $s_{ik} = s_{is}$, and $s_{ij} = 1$ otherwise. The multiple fault signature F_j is not added to the signature matrix if $\forall s_{ij} : s_{ij} = 1 \rightarrow s_{ij} = s_{ik}$, due to the implication that the new multiple fault is a superset of a previously obtained fault which involves fewer nodes, and therefore cannot be part of a minimal diagnosis. The generation of the signature matrix stops when it is impossible to generate new signatures of faults which involve n nodes, with the faults which involve $n-1$ nodes.

In FDI, the exoneration assumption [1] is implied, that is, given an observational model, each component of the support of a satisfied CARC is considered as functioning correctly, that is, it is exonerated. In the DX approach, the exoneration is not considered by default.

In order to obtain the same results as in the DX approach by using a signature matrix, it is necessary to apply a new definition of consistency. In the no-exoneration case an observation signature OS is consistent with another signature FS_j if $\forall OS_i = 1$ then $s_{ij} = 1$. That is, only the non-satisfied CARCs are used, and F_j must have the value 1 in each non-satisfied CARC. When the diagnosis set is obtained by using the new definition of consistency, we propose the application of a set of rules in order to detect which of the faults are minimal diagnoses, since many faults will be consistent with the observational model although they are not a minimal diagnosis. The following algorithm generates the rules to obtain the minimal diagnoses.

Algorithm: Let $CS(OS,FS)$ be a function which evaluates whether the signature OS is consistent with signature FS. For each possible fault F_j in the signature matrix, let MD_{F_j} be a Boolean variable which holds information on whether a fault F_j is a minimal diagnosis, and let VC_{F_j} be a Boolean variable which holds information on whether a fault F_j is a valid candidate for the generation of new faults that could be a minimal diagnosis. For each possible fault F_j it is initially supposed that $VC_{F_j} = \text{true}$.

The first step is to validate if the OK (no fault case) is a minimal diagnosis: $MD_{OK} = CS(OS,OKS)$, and, for any simple fault F_j , the equality $VC_{F_j} = \neg MD_{OK}$ must be satisfied.

If OK is not a minimal diagnosis, the following rules must be evaluated for all the possible faults (except OK) in the same sequential order as they appear in

Table 4. The signature matrix of the polybox example

CARC	OK	F ₁	F ₂	F ₃	F ₄	F ₅	F ₁₂	F ₁₃	F ₁₄	F ₁₅	F ₂₃	F ₂₄	F ₂₅	F ₃₄	F ₃₅	F ₄₅	F _{xxx}
1	0	1	1	0	0	0	1	1	1	1	1	1	1	0	0	0	1
2	0	0	0	1	1	0	0	1	1	0	1	1	0	1	1	1	1
3	0	1	0	1	0	1	1	1	1	1	1	0	1	1	1	1	1
4	0	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1
5	0	0	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1
6	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1

$$F_{xxx} \subset \{F_{123}, F_{124}, F_{134}, F_{135}, F_{145}, F_{234}, F_{235}, F_{245}\}$$

	OK	F ₁	F ₂	F ₃	F ₄	F ₅	F ₁₂	F ₁₃	F ₁₄	F ₁₅	F ₂₃	F ₂₄	F ₂₅	F ₃₄	F ₃₅	F ₄₅	F _{xxx}
VC	1	1	1	1	1	1	1	1	1	0	1	1	0	1	0	0	0
MD	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0

VC and MD values for the observation signature OS = [0, 0, 1, 1, 1, 1]^T

Table 5. A subset of the rules for the polybox example

MD _{OK} = CS(OS,OKS)	MD _{F1} ⇒ VC _{F14} = false	MD _{F13} ⇒ VC _{F123} = false
VC _{F1} = ¬ MD _{OK}	...	MD _{F13} ⇒ VC _{F134} = false
...	MD _{F1} ⇒ VC _{F15} = false	MD _{F13} ⇒ VC _{F135} = false
VC _{F5} = ¬ MD _{OK}	MD _{F2} = VC _{F2} ∧ CS(OS,FS ₂)	MD _{F14} = VC _{F14} ∧ CS(OS,FS ₁₄)
MD _{F1} = VC _{F1} ∧ CS(OS,FS ₁)
MD _{F1} ⇒ VC _{F12} = false	MD _{F13} = VC _{F13} ∧ CS(OS,FS ₁₃)	MD _{F245} = VC _{F245} ∧ CS(OS,FS ₂₄₅)

the signature matrix. These rules guarantee the correct detection of the minimal diagnoses for an observational model:

- For each fault F_j with the signature FS_j, the equality MD_{F_j} = VC_{F_j} ∧ CS(OS,FS_j) must be satisfied.
- For each fault F_k which involves n + 1 nodes, where n ≥ 0, and which can be obtained using the fault F_j(that involves n nodes) and a simple fault F_s(which is not involved in F_j) then MD_{F_j} ⇒ VC_{F_k} = false.

Example: Table 5 shows a subset of the rules for the polybox example. The generation of the rules for the verification of whether a fault is a minimal diagnosis can be done off-line, because these rules are the same for all the observational models. The bottom of Table 4 shows the VC and MD evaluation results for the observation signature OS = [0, 0, 1, 1, 1, 1]^T. Only the evaluation of the rules must be done on-line. This part of the process is a simple propagation of Boolean values.

The evaluation of the signature matrix is very similar to the FDI methodology. However in our approach, the faults involve nodes instead of components. Hence, the last step is the substitution of each node with one of its components. In the polybox example, fault F₃ is equivalent to the faults in {{M₁}, {M₇}},

$\{A_1\}$, $\{A_5\}$ }; fault F_{12} is equivalent to faults $\{\{M_6M_5\}, \{M_8M_5\}, \{A_4M_5\}, \{A_6M_5\}\}$; and so on.

The information of all the possible minimal diagnoses is stored in a matrix and as a set of rules. Therefore, it is only necessary to calculate this matrix and rules once. As happens in FDI methodology, this work can be done off-line, only the evaluation of the signature matrix and rules is on-line. Our approach provide always the minimal diagnoses set of the system by using an observational model. The minimality issue was not guaranteed in the original FDI approach since only the signature matrix is used, but it is guaranteed in our approach since the compilation rules are added to the diagnosis process.

7 Conclusions and Future Work

This paper proposes a new approach to automation of and improvement in the determination of minimal diagnosis. The approach is based on FDI and DX theories. The structural pre-treatment in the first phase and the reduction of the model in the second phase enable improvement in the computational complexity. All the possible minimal diagnoses are represented as a signature matrix and as a set of rules. It is only necessary to calculate this matrix and rules once. The minimal diagnosis is obtained by using an observational model, the signature matrix and a set of compilation rules. Only the evaluation of the compilation rules and signature matrix is on-line, the rest of the process can be done off-line.

The methodology was applied to an standard example, and the results were very promising. As future work we suggest extending the methodology to include dynamic systems and to include more complex and real problems, where the application of the methodology could be more complicated.

Acknowledgment

This work has been funded by the M. de Ciencia y Tecnología of Spanish (DPI2003-07146-C02-01) and the European Regional Development Fund.

References

1. Cordier, M., Lévy, F., Montmain, J., Travé-Massuyés, L., Dumas, M., Staroswiecki, M., Dague, P.: A comparative analysis of AI and control theory approaches to model-based diagnosis. In: 14th European Conference on Artificial Intelligence. (2000) 136–140
2. Ceballos, R., Gómez López, M. T., Gasca, R., Pozo, S.: Determination of Possible Minimal Conflict Sets using Components Clusters and Grobner Bases. In: DX04, 15th International Workshop on Principles of Diagnosis, Carcassonne, France (2004) 21–26
3. Reiter, R.: A theory of diagnosis from first principles. *Artificial Intelligence* 32 1 (1987) 57–96

4. de Kleer, J., Mackworth, A., Reiter, R.: Characterizing diagnoses and systems. *Artificial Intelligence* **2-3** (1992) 197–222
5. Staroswiecki, M., Declerk, P.: Analytical redundancy in non linear interconnected systems by means of structural analysis. In: *IFAC Advanced Information Processing in Automatic Control (AIPAC-89)*, Nancy, France (1989) 51–55
6. Cassar, J., Staroswiecki, M.: A structural approach for the design of failure detection and identification systems. In: *IFAC-IFIP-IMACS Conf. on Control of Industrial Processes*, Belfort, France. (1997)
7. de Kleer, J.: An assumption-based truth maintenance system. *Artificial Intelligence* **2** (1986) 127–161
8. Buchberger, B.: Gröbner bases: An algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory*, N. K. Bose, ed. (1985) 184–232
9. Pulido, B., González, C.A.: Possible conflicts: A compilation technique for consistency-based diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics* **34** (2004) 2192–2206