# **Qualitative Faults Diagnosis Algorithm: Theory and Detection**

He-xuan Hu<sup>1,2</sup>

Agricultural and Animal Husbandry College of Tibet University <sup>1</sup> Lin-zhi, Tibet, P.R. China College of Energy and Electrical Engineering Hohai University <sup>2</sup> Nanjing, Jiangsu Province, P.R. China hexuan\_hu@hhu.edu.cn

Hao-hua Li College of Energy and Electrical Engineering Hohai University Nanjing, Jiangsu Province, P.R. China haohuali@163.com

Abstract—This paper presents a qualitative theory for faults diagnosis. We extend Reiter's [1] theory to deal with the dynamic and continuous systems and offer a necessary assumption and the corresponding propositions. Then we propose an algorithm of detection of faults and extend it to the multi-faults case. As there is not enough information about multi-faults, multi-faults diagnosis is usually a partially observable problem. The STRIPS [2], a classic technique of automated planning, is chosen to build the system model in which the cause-effect information required to process the diagnosis has been integrated. It provides the reasoning ability for the multi-faults diagnosis when diagnosis is formalized as reasoning from effects to causes with causal knowledge. The advantages are that this approach allows building the model gradually with the information received instead of fully in one time and provides a corresponding diagnostic search strategy that has the powerful reasoning ability.

*Keywords-qualitative; multi-faults; diagnosis; cause-effect; reasoning ability* 

# I. INTRODUCTION

The qualitative faults diagnosis has been developed extensively since its introduction several decades ago. There are two principle reasons of using qualitative model: one is that it is very difficult to obtain or develop an accurate quantitative model when there is not enough information about system. The second reason is that the decisions and inferences of engineers and scientists are not only referring to differential equations or numerical values. Mathematical calculations are a small part of diagnosing a fault in a complex industrial plant. Even when mathematical representations are used, there is a large amount of qualitative knowledge needed to set up equations and interpret the results of calculations. Furthermore, numerical descriptions fail to produce insight into why a system behaves as it does. The relationships between variables which represent the

Shi-ping Huang College of Energy and Electrical Engineering Hohai University Nanjing, Jiangsu Province, P.R. China sph2014@126.com

Ye Zhang College of Computer and Information Engineering Hohai University Nanjing, Jiangsu Province, P.R. China silve fox@hotmail.com

physical laws to which a system conforms are only a representation in mathematics. The operators can obtain the numerical results calculated by those mathematical equations, but cannot directly obtain the meaningful explanation from these results of complex mathematical analysis. Multi-faults diagnosis is such a partially observable problem because firstly there is not enough information about the relationships between the faults, and secondly there is not a model for some fault, for example, in the case of the leakage of tank (the parameter of flow constant depends on the diameter of the hole, but it is impossible to know the diameter of the hole before we have detected the leakage.).

Various formal theories of employing causal knowledge have been studied in the literature to solve the problems of multi-fault diagnosis. In the 1980s, Reiter proposed a logic-based theory of diagnosis, aiming at formally capturing diagnosis of abnormal behavior in a device or system, using a model of normal structure and behavior [1]. This approach is called consistency-based approach. Basically, consistency-based diagnosis amounts to finding faulty device components that account for a discrepancy between predicted normal behavior and actually observed behavior. The discrepancy is formalized as logical inconsistency; a diagnosis is established when assuming particular components to be faulty and others to be normally functioning and restores the consistency of the observed system. Approximately at the same time, De Kleer and Williams have independently implemented General Diagnostic Engine (GDE) which also realizes the above ideas [3]. A lot of good practical works have been developed from their theory, [4], [5] and [6]. There is a review about all these diagnostic notions in [7]. We don't list the references here again.

However, Reiter's theory is only applied to diagnosing digital circuits, which are representative only of physical devices with static, persistent states. Dvorak [8] and Ng [9] use the theory of qualitative simulation [10], a semi-

quantitative method called –qualitative physics", to extend the Reiter's theory to deal with the dynamic and continuous system. Qualitative physics does not require detailed information. An order of magnitude information about the normal operating values of process parameters and variables is sufficient. The advantage is that it does not depend on an accurate mathematical model. But qualitative physics predicts qualitative behavior by using qualitative differential equations (QDEs) that are an abstraction of the ordinary differential equations (ODEs) used to represent the state of the system.

In addition, for achieving multi-faults (including sensor faults) diagnosis under partially knowledge, we need a model that can describe the dynamic and continuous system and a corresponding diagnostic search strategy that has the powerful reasoning ability.

To describe dynamic and continuous system with an efficient cause-effect diagnostic search strategy, we propose -automata" as the form of model and -STRIPS" (STanford Research Institute Problem Solver, [2]), a classic technique of automated planning [11], as the means of building model. The idea to use automata to describe dynamic systems is not new. -Automata" have been largely applied in the discrete event systems (DES) [12]. But the DES builds the system model through composing the various pre-designed component models with controller models by parallel composition. The diagnosis is performed by a large diagnoser into which all possible diagnoses are embedded [13]. The drawback is that the means of building model in DES is neither flexible nor practical to update its own model in a reasoning situation. Moreover, it is not practical to list all possible diagnoses in advance, especially considering the combinations of multi-faults. The STRIPS language is very suitable to generate the system model since it integrates the cause-effect information required to process the diagnosis. Indeed, with the STRIPS language, actions are described in terms of their preconditions and effects and states are formulated as conjunctions of positive literals. The precondition states what must be true in a state before an action can be executed. The effect describes how the state changes when the action is executed. An action is -applicable" in any state that satisfies the precondition; otherwise, the action has no effect. This allows building the model gradually with the information received instead of fully in one time. This is a precious advantage.

The fault diagnosis process we propose rests on the three following steps which are running at receiving each new observation set.

- 1. Identification of the system current state from the system observations and comparison with the predicted states by using the flexible STRIPS model.
- 2. Using Reiter's theory with fault models to identify not only faulty components themselves but also their faulty modes (for example, stuck open or stuck close for a valve).
- 3. According the result of the step 2, determination of the possible future system states using the flexible STRIPS model.

The rest of this paper is organized as follows. Reiter's theory of diagnosis is briefly introduced in section II. The

fault detection process is described in section III. Section IV summarizes the work done and discusses directions for future research.

# II. REITER'S THEORY OF DIAGNOSIS

In Reiter's theory of diagnosis, a diagnosis problem consists of a system description (*SD*), a set of system components (*COMP*), and observations of the system (*OBS*). The system description specifies the general rules that must be obeyed for the system to function normally. His diagnostic algorithm computes all diagnoses which explain the differences between the predicted and observed behavior of a given system. We will present a brief review of the definitions and the algorithm proposed by Reiter.

**Definition 1**: System: A system is a pair (*SD, COMP, OBS*) where: (1) *SD*, the system description; (2) *COMP*, the system components; (3) *OBS*, the observations of a system.

**Definition 2**: Hitting set: A hitting set for a collection of sets *C* is a set  $H \subseteq Y_{S \in C}S$  such that  $H \cap S \neq \{\}$  for each  $S \in C$ . A hitting set for *C* is minimal if and only if no proper subset of it is a hitting set for *C*.

**Definition 3**: Diagnosis: A diagnosis for (*SD*, *COMP*, *OBS*) is a minimal set  $\Delta \subseteq COMP$  such that:  $SD \cup OBS \cup \{AB(c) | c \in \Delta\} \cup \{\neg AB(c) | c \in COMP - \Delta\}$  is consistent, where *AB* is a predicate indicating that a component is abnormal.

The Principle of Parsimony: A diagnosis is a conjecture that some minimal set of components are faulty. Intuitively, a diagnosis is a conjecture that certain of the components are faulty (abnormal) and the rest normal. According to the principle of Parsimony, a diagnosis is determined by a smallest set of components with the following property: the assumption that each of these components is faulty (abnormal), together with the assumption that all other components are behaving correctly (not abnormal), is consistent with the system description and the observation.

**Definition 4**: Conflict set: A conflict set for (*SD*, *COMP*, *OBS*) is a set  $\{c_1, ..., c_k\} \subseteq COMP$  such that:

 $SD \cup OBS \cup \{\neg AB(c_1), \dots, \neg AB(c_k)\}$  is inconsistent. A conflict set for (*SD*, *COMP*, *OBS*) is minimal iff. no proper subset of it is a conflict set for (*SD*, *COMP*, *OBS*).

**Theorem 1**:  $\Delta \subseteq COMP$  is a diagnosis for (*SD*, *COMP*, *OBS*) iff  $\Delta$  is a minimal hitting set for the collection of conflict sets for (*SD*, *COMP*, *OBS*).

Based on the above definitions and theorem, there is a direct generate-and-test mechanism which rests on three steps: systematically generate subsets  $\Delta$  of *COMP*, generate  $\Delta$ s with the smallest subset and test each one for the consistency of  $SD \cup OBS \cup \{\neg AB(c) | c \in COMP - \Delta\}$ .

The sub-algorithm of computing hitting sets is firstly introduced. Suppose F is a collection of sets. An edge-labelled and node-labelled tree T is an HS-tree for F *iff* it is a smallest tree with the following properties:

(1) Its root is labelled by  $\neg \varphi^n$  if F is empty. Otherwise, its root is labelled by a set of F.

(2) If n is a node of T, define H(n) to be the set of edge labels on the path in T from the root node to n. If n is labelled by  $\rightarrow^{n}$ , it has no successor nodes in T. If n is

labelled by a set  $\sum$  of F, then for each  $\sigma \in \sum$ , n has a successor node  $n_{\sigma}$  joined to n by an edge labelled by  $\sigma$ . The label for  $n_{\sigma}$  is a set  $S \in F$  such that  $S \cap H(n_{\sigma}) = \{\}$  if such a set S exists. Otherwise,  $n_{\sigma}$  is labelled by  $\neg r$ .

In diagnosis, F is the set of all conflict set for (*SD*, *COMP*, *OBS*). These sets are not explicitly known in advance and are calculated as needed by an underlying consistency-checking module. Each access to F is very expensive because an access to F will require a call to a consistency-checker. Clearly, it is better to access to F as few as possible. Reiter proposed several pruning heuristics to reduce access to F by reusing node labels which have already been found. Greiner et al. [14] proposed the corrected version of Reiter's algorithm.

The sub-algorithm HS- $DAG_0$  is used to construct the HS-dag (it is a directed graph) for a collection of sets - F, without pruning:

(1) Let D represent the growing HS-dag. Generate a node which will be the root of the HS-dag. This node will be processed in step 2 below.

(2) Process the nodes in D in a breadth first order. To process a node n:

- (a) Define *H*(*n*) to be the set of edge labels on the path in *D* from the root down to node *n*.
- (b) If a set S ∈ F, such that S ∩ H(n<sub>σ</sub>) = {}, exists, then label node n by the set S where S is the first member of F. Otherwise, n is labelled by -√<sup>n</sup>.
- (c) If n is labelled by a set S∈ F, then for each σ∈ ∑, generate a new downward arc labelled by σ. This arc leads to a new node m with H(m) = H(n) ∪ {σ}. The new node m will be processed (labelled and expanded) after all nodes in the same generation as n have been processed.
- (3) Return the resulting HS-dag. D.

Following the Reiter's basic algorithm, there are three pruning enhancements to the  $HS-DAG_0$  algorithm to reduce the size of the HS-dag and also improve the algorithm's efficiency:

(1) Reusing Nodes: This algorithm will not always generate a new node m as a descendant of node n. There are two cases to consider:

- (a) If there is a node n' in D such that  $H(n') = H(n) \cup \{\sigma\}$ , then let the  $\sigma$ -arc under n point to this existing node n'. Hence, n' will have more than one parent.
- (b) Otherwise, generate a new node, m, at the end of this  $\sigma$ -arc as described in the basic HS-DAG<sub>0</sub> algorithm.

(2) Closing: If there is node n' which is labelled by  $\neg$  and  $H(n') \subset H(n)$ , then close node n. A label is not computed for node n and no any successor nodes are generated.

(3) Pruning: If the set  $\Sigma$  is to label a node and it has not been used before, then attempt to prune D as described in the following.

(a) If there is a node n' which has been labelled by the set S' of F where Σ⊂S', then re-label n' with Σ. For any σ in S'-Σ, the σ-arc under n' is no longer allowed. The node connected by this arc and all of its descendants are removed, except for those nodes with another ancestor

which is not being removed. Note that this step may eliminate the node that is currently being processed.

(b) Interchange the sets S' and Σ in the collection. (Note that this has the same effect as eliminating S' from F).

The set of all diagnoses can now be read from the generated graph *D*. Each the set of edge labels on the path in *D* from the root node to any leaf node which is labelled by  $-\sqrt{2^{n}}$  is a diagnosis for the current system state.

#### III. EXTEND TO DYNAMIC SYSTEM

We make an assumption that a fault is permanent not intermittent. It means that the effects of a fault exist continuously, not repeatedly for short periods and that the information expressed by a conflict set is cumulative, in other words, once a conflict set is detected in some state, then the information that at least one of its components must be faulty would be still valid in the successor states. Based on this assumption, we extend the definitions of Reiter to deal with these continuously new observations.

**Definition 5**: A diagnosis  $\Delta$  for (*SD, COMP, OBS*) predicts *New-OBS* (the new observations) iff

 $SD \cup OBS \cup \{AB(c) | c \in \Delta\} \cup \{\neg AB(c) | c \in COMP - \Delta\}$ 

 $\models$  New-OBS, that is to say that if all the components of  $\varDelta$  are faulty, and the remaining components are all functioning normally, the New-OBS must be hold.

**Proposition 1** is immediate consequences of definition 5.

(1) Every diagnosis for (SD, COMP, OBS) which predicts New-OBS is a diagnosis for (SD, COMP, OBS  $\cup$  New-OBS), i.e. diagnoses are preserved under confirming the new observations.

(2) No diagnosis for (*SD*, *COMP*, *OBS*) which predicts  $\neg New-OBS$  is a diagnosis for (*SD*, *COMP*, *OBS* $\cup New-OBS$ ), i.e. the new observations rejects the diagnoses which it disconfirms.

**Proposition 2**: A conflict set for (*SD*, *COMP*, *OBS*) is still a conflict for (*SD*, *COMP*, *OBS*  $\cup$  *New-OBS*).

As the limitation of paper space, we ignore the proofs of these two propositions. Moreover, the details of the method of modeling by STRIPS have been presented in [15-18]. The readers can be referenced it.

#### IV. THE FAULT DETECTION ALGORITHM

The basic idea of fault detection in this paper is very simple: determine the current state in which the system is, predict the normal successive possible states, and compare these predictive states with those observed (these steps are all based on the normal system model generated by the method based on STRIPS [15-18]). If there are differences between these predictive and observed effects, the fault symptoms are detected. This basic idea is also used in the consistency-checking module. The difference is that we compute the predictive states using the fault STRIPS actions but not only using the normal STRIPS actions with the observations. The details will be presented in the consistency-checking module. The fault detection algorithm is now given as following.

## Algorithm 1: Fault detection

Init: Determine the initial state  $s_0$  from the current observation; i = 0; Predict the possible successive possible states  $S_{np0}$  of  $s_0$ ;

```
While (receiving new observations) Do
```

```
Determine the current state s_i;

Predict the normal successive possible states S_{npi} for next iteration;

If s_i \notin S_{np(i-1)} then { The fault symptoms are detected and returned; <sup>1</sup>

Call the principle diagnostic process;

Diagnose = Return of the principle diagnostic process

(s_i)}

End If;

Wait for (new observations);

i = i+1;
```

End While

The fault detection algorithm rests on the following steps:

(1) Determination of the current state  $s_i$  (based on the modeling by STRIPS):

Determination of the current state  $s_i$  depends on the available information:

- the values from sensors: the values observed are the sensor readings and are displayed as numerical numbers. But in qualitative model, these values are expressed as numeric ranges and each range is characterized by two landmarks which are decided in the design. The number of landmarks is fixed to avoid an uncertainty explosion. The direction of a value's change is also the useful qualitative information. So a value is represented as a couple elements (range, Direction).
- the status of components: -the status of components" are represented as some logic atoms, for example, a valve is opened as On (Valve) or a pump is closed as Off (Pump).
- the state space is constructed by these observed values and the status of components. As the status of components and landmarks are limited, the state space is also limited.
- (2) Predict the normal successive possible states:
- The normal effects of possible control actions are predicted by using the STRIPS actions defined as before. Then the possible normal states are determined as the step 1 by using the new values and status of components, and then they are stored in a normal predictive state set  $S_{npi}$ .
- (3) Compare these predictive states with observed ones: After receiving new observed values, the current system state is determined and then compare it with the ones in  $S_{np(i-1)}$  which is determined at the last time of receiving new observed values. The comparison between two states includes two respects: firstly check every value's ranges and direction, and then check status of components. If all of things are consistent, then these two states are equivalent, otherwise these two states are not equivalent. If the current system state belongs to the last normal predictive states  $S_{np(i-1)}$ , then we say that the system is normal, otherwise we say that it is abnormal. The fault symptoms are detected and returned. The corresponding state of these fault symptoms will be marked. A call to the principle diagnostic process is done.

#### V. CONCLUSION

This paper is first part of a two part effort that is

intended to present a qualitative theory of multi-faults diagnosis and propose an algorithm of detection of faults. Reiter [1] has proposed a consistency-based approach for multi-faults diagnosis, but his theory is only applied to diagnosing digital circuits, which are representative only of physical devices with static, persistent states. We extend his theory to deal with the dynamic and continuous systems and offer a necessary assumption and the corresponding propositions. Multi-faults diagnosis is a partially observable problem as there is usually not enough information about faults. The reasoning ability is required to make up for this shortcoming. So the STRIPS, a classic technique of automated planning, is chosen to build the system model. It provides great support for the multi-faults diagnosis when diagnosis is formalized as reasoning from effects to causes with causal knowledge. The detail process of multi-faults diagnosis will be presented in the companion of this paper.

## ACKNOWLEDGMENT

This work is supported by —The Nature Science Foundation of Tibet", —A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions (Coastal Development Conservancy)", —Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China", "the Fundamental Research Funds for the Central Universities", and —he Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry".

## REFERENCES

- R. Reiter, -A theory of diagnosis from first principles," Artificial Intelligence, Vol.32, No. 1, pp. 57-95, 1987.
- [2] R. E. Fikes and N. J. Nilsson, -STRIPS: a new approach to the application of theorem proving to problem solving," Artificial Intelligence, Vol. 2, Issues 3-4, pp. 189-208, 1971.
- [3] J. De Kleer and B. C. Williams, Dignosing multiple faults," Artificial Intelligence, Vol. 32 (1), pp. 97-130, 1987.
- [4] A. Malik, P. Struss and M. Sachenbacher, "Case studies in modelbased diagnosis and fault Analysis of car-subsystems," Proceedings of the European Conference on Artificial Intelligence (ECAI), 1996.
- [5] B. Williams and P. Nayak, —Amodel-based approach to reactive self-configuring systems," Proceedings of Thirteenth National Conference on Artificial Intelligence (AAAI'96), Portland, Oregon, 1996.
- [6] A. Ligeza and J. M. Kościelny, —Anew approach to multiple fault diagnosis: A combination of diagnostic matrices, graphs, algebraic and rule-based models. The case of two-layer models, "Int. J. Appl. Math. Comput. Sci., Vol. 18, No. 4, pp. 465–476, 2008.
- [7] Peter J.F. Lucas, —Aalysis of notions of diagnosis," Artificial Intelligence, Vol. 105, pp. 295-343, 1998.
- [8] D. Dvorak and B. Kuipers, -Process monitoring and diagnosis: A model-based approach," IEEE Expert: Intelligent Systems and Their Applications, Vol. 6, no. 3, pp. 67-74, 1991.
- [9] H. T. Ng, -Model-based multi-fault diagnosis of dynamic, continuous physical devices," IEEE Expert, Vol. 6, No. 6, pp. 38-43, 1991.
- [10] B. Kuipers, -Qualitative Simulation," Artificial Intelligence, Vol. 29, No. 3, pp. 289-338, 1986.
- [11] M. Ghallab, D. Nau and P. Traverso, Automated Planning: Theory and Practice, Morgan Kaufmann Publishers, 2004.
- [12] C. G. Cassandras and S. Lafortune, Introduction to Discrete Event Systems (Second Version), Kluwer Academic Publishers, 2007.

<sup>&</sup>lt;sup>1</sup>  $S_{np(i-1)}$  is the set of predictive states for state  $s_i$ , but it is determined at the time of  $s_{i-1}$ .

- [13] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis, — Dignosability of discrete-event systems," IEEE Trans. Automatic Control, Vol. 40, No. 9, pp. 1555–1575, 1995.
- [14] R. Greiner, B. A. Smith and R. W. Wilkerson, —ACorrection to the Algorithm in Reiter's Theory of Diagnosis," Artificial Intelligence, Vol. 41, No. 1, pp. 79-88, 1989.
- [15] H. X. Hu, A. L. Gehin, and M. Bayart, -A Formal Framework of Reconfigurable Control Based on Model Checking," in American Control Conference, Seattle, Washington, USA, 2008.
- [16] H. X. Hu, A. L. Gehin, and M. Bayart, -An extended qualitative multi-faults diagnosis from first principles I: theory and modelling", in 48th IEEE Conference on Decision and Control, China, 2009.
- [17] H. X. Hu, A. L. Gehin, and M. Bayart, -An extended qualitative multi-faults diagnosis from first principles II: algorithm and case study," in 48th IEEE Conference on Decision and Control, China, 2009.
- [18] A. L. Gehin, H. X. Hu, and M. Bayart, -A self-updating model for analysing system reconfigurability", Engineering Applications of Artificial Intelligence, Vol.25, Issue 1, pp.20-30, 2012.