Generalizing diagnosability definition and checking for open systems: a Game structure approach

Tarek Melliti [1], **Philippe Dague** [2]

[1] *IBISC, Univ. d'Evry Val d'Essonne, France*
(Tel: 33 1 60 87 39 36; e-mail: tmelliti@ibisc.fr)

[2] *LRI, Univ. Paris-Sud, CNRS, and INRIA Saclay-Ile de France*
(Tel: 33 1 69 72 92 59 93; e-mail: philippe.dague@lri.fr).

Abstract

In Model Based Diagnosis, diagnosing a situation consists in comparing the behavior of the system within its fault (or correct) model in order to find explanation(s). In the case of discrete systems, the model is usually an automaton labeled by two types of actions: the observed ones and the unobserved ones. When dealing with fault model we distinguish among the unobserved events a set of fault events. Diagnosability is the study of the capability of the model to detect faults and also discriminate between different types of faults within. Let we consider A system and its fault model A depicted in the figure 1.

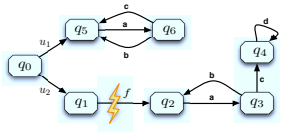

Figure 1: A system containing one fault f

The observation of an infinite iteration of (ab) on the system, can be explained,according to the model A, either by the run u_1 or by $u_2 f$ followed by an infinity of (ab). We can deduce that this model do not have the capability to discriminate between a correct execution and a faulty execution (two ambiguous runs), we say that the fault f is nondiagnosable in A. A formal definition of diagnosability was given in (Sampath *et al.*, 1995). The definition stands that a fault in a system is diagnosable if and only if, we can not find two infinite runs that produces the same observable and one contains the fault on other not. Many works other than (Sampath *et al.*, 1995) proposed solutions to check the diagnosability, (Cimatti *et al.*, 2003)etc.

Let we now consider the same fault model but we change slightly the meaning of the events. All the internal events are considered controllable by the system. A part of the observable ones are no longer controlled by the system (e.g commands)[1]. Let we consider that b and c are now uncontrollable. Even by making this modification, the classical diagnosability definition and methods still considers f as non diagnosable. But, we can observe that infinitely often, for the ambiguous observation $(ab)^\infty$, one can give the system the event c instead of b and then within finite steps of observations (here one) we can say without ambiguity that f did (by observing d) or did not (by observing a) happen. In fact f is diagnosable. This toy example shows the limit of the classical definition of diagnosability to cover some types of systems.

Let $A_\mathcal{E}$ be a transition system which has the same observable events as A but with inverse controllability labels, call $A_\mathcal{E}$ an environment of A. Let we consider a synchronous interaction between the system and the environment on the observable events. We can consider this interaction as a game between the two systems. The system wins if it has a strategy (by choosing its controllable moves) to control the interaction in order to keep infinitely the ambiguity. In the opposite the environment wins if each time an ambiguity appears then it has a strategy to resolve it within a finite set of moves.

In this work we generalize the definition of diagnosability by using game structures and strategies framework. We give a method to synthesis the environment and generate the game structure. Then we use Alternating-Time Temporal Logic to check the existence of wining strategies for the environment in order to decide whether a system is diagnosable or not.

REFERENCES

(Cimatti *et al.*, 2003) A. Cimatti, C. Pecheur, and R. Cavada. Formal verification of diagnosability via symbolic model checking. In *In Proceedings of the 18th International Joint Conference on Artificial Intelligence IJCAI03*, pages 363–369, 2003.

(Sampath *et al.*, 1995) M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete event systems. *IEEE Trans. on Automatic Control*, 40(9):1555–1575, September 1995.

[1] Note here that A as interpreted before is a system where every event is controllable (a spacial case).