A probabilistic analysis of diagnosability in discrete event systems

Farid Nouioua and **Philippe Dague**[1]

Abstract. This paper shows that we can take advantage of information about the probabilities of the occurrences of events, when this information is available, to refine the classical results of diagnosability: instead of giving a binary answer, the approach we propose allows one to quantify, in particular, the degree of non-diagnosability in case of negative answer. The dynamics of the system is modelled by a reducible Markov chain. A state of this chain contains information about whether it is faulty (resp. ambiguous) or not. The useful refinements of the decision about diagnosability are then obtained from the asymptotic analysis of this Markov chain. This analysis may be very useful in practice since it may lead to take the decision of tolerating some non-diagnosable systems, if their non-diagnosability is not critical, and thus allows one saving the cost of additional sensors necessary to make these systems diagnosable. [2].

1 MOTIVATION

One major requirement in designing today's real-life complex systems, is to ensure for them a high level of autonomy. Studying the diagnosability of a system is one of the key issues in this context. The problem of diagnosability drew the attention of many researchers from both the discrete-event and the control communities. A formal definition of diagnosability has been introduced first in [7]. This work provides also an algorithm to verify diagnosability in discrete event systems (DES) represented by finite automata. The proposed method is based on the so-called diagnoser which is an automaton with only observable events and which allows one to estimate the state of the system after the observation of a sequence of events. Other verification algorithms with polynomial complexity (the previous one is exponential in the states number) have been then proposed and are based on the twin plant approach which uses a synchronized product of two automata [3][9]. Adaptations of these algorithms have been also proposed to deal with the distributed case [5][8]. Another approach to solve diagnosability problem in DESs is based on model-checking [1] where the verification of diagnosability is reduced to the verification of a formula, often expressed in temporal logic, by using efficient tools developed in the model-checking community. We find also methods that use algebraic language [2] and more recently SAT formalism to express and solve diagnosability [6].

However, all these approaches give a binary answer to the question of whether the system is diagnosable or not. But, one can easily remark that there is no single level in non-diagnosability of a system, i.e., in case of a non-diagnosable system we would like to quantify the degree of this non-diagnosability. The practical importance of such a refinement is that it could allow the tolerance of a system with, say, a low level or controllable form of non-diagnosability, if the cost necessary to making it diagnosable by adding observable events and thus sensors is very high. This paper shows that this objective can be achieved by enhancing the transitions of a DES with their probabilities. The method consists in extracting a Markov chain that explains the dynamics of the system and provides probabilities of the different observable traces leading it to faulty/normal and/or ambiguous/unambiguous states. Some probability measures can then be derived from the asymptotic analysis of this Markov chain and provides useful conclusions that go further than simply deciding if the system is or is not diagnosable.

In section 2, we define a probabilistic discrete event model, we show its relationship to a classical DES and we recall some basic definitions useful to define diagnosability. In section Section 3, we start by recalling the algorithm used in [7] to verify diagnosability in case of possible multiple faults, we show after that how to use the diagnoser in the case of probabilistic transitions to construct a so-called estimator (which can be thought of as a probabilistic diagnoser) and how to extract from it a Markov chain and we explain how we can use the results of the asymptotic behavior of the Markov chain to draw the wished conclusions. Section 4 is devoted to some examples that illustrate different cases one can encounter. Finally we conclude and give some perspectives of future work in section 5.

2 PROBABILISTIC DISCRETE EVENT MODEL

This section introduces the notion of a probabilistic discrete event model which simply corresponds to a classical DES enriched by information about probabilities of the transitions between its states.

Definition 1 *We model a probabilistic discrete event system $(PDES)$ by the structure $\Gamma = (X, E, \theta, x_0)$ where $X = \{x_0, ..., x_{n-1}\}$ is a finite set of states ($|X| = n$), $E = \{e_0, ..., e_{m-1}\}$ is a finite set of events occurring on Γ ($|E| = m$), x_0 is the initial state and $\theta : X \times E \times X \longrightarrow [0..1]$ is a probabilistic transition function defined such that $\theta(x, e, x') = \alpha$ $(0 \leq \alpha \leq 1)$ is the probability that the event e occurs in x and causes the transition of the system from state x to state x'.*

Definition 2 *To a PDES $\Gamma = (X, E, \theta, x_0)$ we associate a discrete event system (DES) $G = (X, E, \delta, x_0)$ having the same states set X, events set E and initial state x_0. The transitions of G are defined by $\delta \subseteq X \times E \times X$ where $(x, e, x') \in \delta \Leftrightarrow \theta(x, e, x') > 0$.*

The DES G is simply the automaton obtained by removing from Γ the information about the probabilities of its transitions.

[1] LRI, Univ. Paris-Sud and CNRS, and INRIA Saclay-Ile-de-France, Parc Club Orsay Universit, 4 rue J. Monod, 91893 Orsay Cedex, FRANCE, email: {Farid.Nouioua, Philippe.Dague}@lri.fr

[2] This work is part of DIAFORE project supported by ANR under grant ANR-05-PDIT-016-05.

The probabilistic transition function can be generalized to a word s of E^* (the Kleene closure of E). $\theta(x_1, s, x_2)$ is the probability that the system transits from x_1 to x_2 following the word s. Since a transition between two states following a word can in general be performed by following different paths, this probability is the sum of probabilities of all paths leading from x_1 to x_2. Formally, let us consider that $s = e_1, \dots e_p$ and let $C^s_{x_1,x_2}$ be the set of state sequences between x_1 and x_2 by which the system may transit to generate s:

$$C^s_{x_1,x_2} = \{(y_1, \dots y_{p+1}) | x_1 = y_1, x_2 = y_{p+1}, (y_i, e_i, y_{i+1}) \in \delta\}$$

We have: $\theta(x_1, s, x_2) = \sum_{(y_1,\dots,y_{p+1}) \in C^s_{x_1,x_2}} \prod_{i=1}^{p} \theta(y_i, e_i, y_{i+1})$. $\theta(x_1, s, x_2)$ can also be defined recursively by:

$\theta(x_1, s, x_2) = \sum_{j=0}^{n-1} \theta(x_1, e_1, x_j).\theta(x_j, e_2 \dots e_p, x_2)$.

Let us now recall some basic definitions and notations relative to G and useful in the study of diagnosability.

We denote by L the language generated by G. L is a subset of E^* and is prefix closed. $E = E_o \cup E_{uo}$ where E_o (resp. E_{uo}) contains the observable (resp. unobservable) events. $E_f \subseteq E_{uo}$ is a subset of unobservable events containing the faults. Moreover, faults are partitioned into disjoint sets corresponding to the different fault types: $E_f = E_{f_1} \cup \dots \cup E_{f_p}$. In what follows, we will focus on one fault type as in [9][5][8]. This is justified as the system is diagnosable if and only if it is diagnosable for each fault type. Thus, to check the diagnosability of a syetem with several faults, one must check in turn its diagnosability w.r.t each fault type by considering all the other faults as non observables.

For the sake of simplicity, we will denote by f each occurrence of the fault type for which we want to verify the diagnosability. We suppose also that L is live, that there is no cycle in G with only unobservable events and that we represent in the model all the possible transitions of the system in each state. Thus, we have for each x in X: $\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \theta(x, e_i, x_j) = 1$.

Example 1 *Figure 1 shows an example of a PDES* $\Gamma = (X, E, \theta, x_0)$ *and its corresponding DES* $G = (X, E, \delta, x_0)$ *where:* $X = \{x_0, x_1\}$, $E = E_o \cup E_{uo}$ *with* $E_o = \{a, b, c\}$ *and* $E_{uo} = \{f, uo\}$*, the set of fault events is* $E_f = \{f\}$*, the initial state for the two systems is* x_0 *and the transition functions are defined by:*

- $\theta(x_0, uo, x_1) = 1/6$, $\theta(x_0, f, x_1) = 1/2$, $\theta(x_0, c, x_1) = 1/3$, $\theta(x_1, a, x_1) = 1/3$ *and* $\theta(x_1, b, x_0) = 2/3$. *For the other possible combinations of the source state* x*, target state* y *and the event* e*,* $\theta(x, e, y) = 0$.
- $\delta(x_0, uo) = x_1$, $\delta(x_0, f) = x_1$, $\delta(x_0, c) = x_1$, $\delta(x_1, a) = x_1$ *and* $\delta(x_1, b) = x_0$.

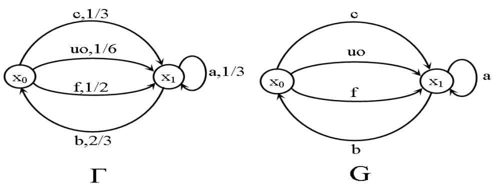

Figure 1. A PDES and the corresponding simple DES

A word of the language L is also called trace. The empty trace is denoted by ϵ. The postlanguage of L after s is denoted by L/s: $L/s = \{t \in E^* | st \in L\}$. $P : E^* \longrightarrow E^*$ is a projection function that erases from any trace its unobservable events : $P(\sigma) = \epsilon$ if $\sigma = \epsilon$ or $\sigma \in E_{uo}$, $P(\sigma) = \sigma$ if $\sigma \in E_o$ and $P(s\sigma) = P(s)P(\sigma)$ for $s \in E^*$ and $\sigma \in E$.

P_L^{-1} is the inverse projection: for any $w \in E_o^*$, $P_L^{-1}(w) = \{s \in L | P(s) = w\}$. It provides for an observable trace w, all traces of L whose projection is w. We denote by s_f the final event of a trace s and by $\Psi(f)$ all traces ending in the fault event f: $\Psi(f) = \{s \in L | s_f = f\}$ and we define: $X_o = \{x_0\} \cup \{x \in X \,|\exists y \in X, \exists e \in E_o, (y, e, x) \in \delta\}$. Let $L(G, x)$ denote the set of traces originating from x, $L_o(G, x)$ denotes the set of traces originating from x and ending at the first observable event and $L_\sigma(G, x)$ the subset of $L_o(G, x)$ containing traces that end at the observable event σ: $L_o(G, x) = \{s \in L(G, x) \mid s = u\sigma, u \in E_{uo}^*, \sigma \in E_o\}$, $L_\sigma(G, x) = \{s \in L_o(G, x) \mid s_f = \sigma\}$.

3 DIAGNOSABILITY

Intuitively, a system is said to be diagnosable if we can deduce without confusion after a finite delay of observations whether a fault occurred or not in the system. Let us recall here the formal definition given in [7] adapted to our assumption that only one fault type is considered. The system is diagnosable if the following holds: $(\exists n \in N)[\forall s \in \Psi(f)](\forall t \in L/s)[\|t\| \geq n \Rightarrow D])$, where the diagnosability condition D is: $w \in P_L^{-1}[P(st)] \Rightarrow f \in w$.

3.1 Checking the “binary” diagnosability

We start by checking the ”binary” diagnosability of the system. We use for that the algorithm of Sampath and al. [7] whose diagnoser is well adapted to be used for a probabilistic analysis (see below). We consider the case of possible multiple faults. In what follows we recall briefly the construction of the generator G' and the diagnoser G_d before giving (without technical details) the necessary and sufficient condition on G' and G_d for the binary diagnosability of L.

The generator G' is defined by $G' = (X_o, E_o, \delta_{G'}, x_0)$ where X_o, E_o and x_0 have already been defined. $\delta_{G'}$ is such that: $(x, \sigma, x') \in \delta_{G'}\ if\ (x, s, x') \in \delta\ for\ some\ s \in L_\sigma(G, x)$. The corresponding probabilistic generator is defined by $\Gamma' = (X_o, E_o, \theta_{\Gamma'}, x_0)$ where X_o, E_o and x_0 are the same as in G' and the probabilistic transition function $\theta_{\Gamma'} : X_o \times E_o \times X_o \longrightarrow [0, 1]$ is defined by: $\theta_{\Gamma'}(x, \sigma, x') = \sum_{s \in L_\sigma(G,x)} \theta(x, s, x')$.

Proposition 1 *The sum of the probabilities of all transitions issued from each state of* Γ' *equals 1. Formally:*

$$\sum_{\sigma \in E_o} \sum_{x' \in X_0} \theta_{\Gamma'}(x, \sigma, x') = 1\ \ for\ each\ x\ in\ X_0$$

.

The diagnoser is a deterministic automaton which is defined by $G_d = (Q_d, E_o, \delta_d, q_0)$ where:

- $Q_d \subseteq 2^{X_o \times \{N,F\}}$. A state q_d of Q_d is of the form: $q_d = \{(x_1, l_1), \dots, (x_k, l_k)\}$ where $x_i \in X_o$ and $l_i \in \{N, F\}$.
- E_o is the set of the observable events.
- $\delta_d : Q_d \times E_o \longrightarrow Q_d$ is the transition function of the diagnoser defined by: $q_2 = \delta_d(q_1, \sigma) \Leftrightarrow q_2 = R(q_1, \sigma)$ with:
  - $\sigma \in e_d(q_1)$ where $e_d(q_1) = \bigcup_{(x,l) \in q_1} \{P(s) | s \in L_o(G, x)\}$
  - $R : Q_d \times E_o \longrightarrow Q_d$ is a range function defined by: $R(q, \sigma) = \bigcup_{(x,l) \in q} \bigcup_{s \in L_\sigma(G,x)} \bigcup_{(x,s,x') \in \delta} \{(x', LP(x, l, s))\}$

- $LP : X_o \times \{N, F\} \times E^* \longrightarrow \{N, F\}$ is a label propagation function defined by:

$$LP(x, l, s) = \begin{cases} N & if \quad l = N \ and \ f \notin s \\ F & else \end{cases}$$

- $q_0 = \{(x_0, N)\}$ is the initial state of the diagnoser G_d.

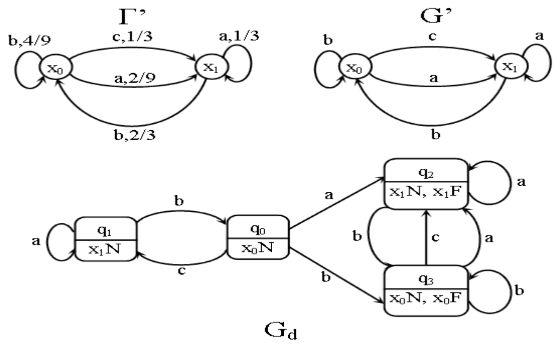

Figure 2. The probabilistic generator Γ', the simple generator G' and the diagnoser G_d

Figure 2 represents the probabilistic generator, the simple generator and the diagnoser of the system described in example 1.

A state q of G_d is said to be f-uncertain if $\exists(x, l), (x', l') \in q$ such that $l \neq l'$, i.e., $l = N$ and $l' = F$ or vice versa. Informally, a set of f-uncertain states $q_1, \ldots q_n$ is said to form an f-indeterminate cycle if $q_1, \ldots q_n$ form a cycle in G_d to which correspond in G' a cycle involving only states with label F and a cycle involving only states with label N. Finally, L is diagnosable if and only if its diagnoser G_d contains no f-indeterminate cycle.

3.2 Constructing the estimator

The diagnoser gives us a general information about the state of the system after the observation of a sequence of observable events. For example, let us suppose that we have, in the diagnoser, a path from the initial state $q_0 = \{(x_0, N)\}$ to some f-uncertain state q and that this path is labeled by the observable trace w. Let us suppose for instance that q corresponds to two different states x_1 and x_2 with no fault in the first state and with a fault in the second one, i.e., $q = \{(x_1, N), (x_2, F)\}$. If we observe the trace w, we can deduce that the system is either in state x_1 and no fault occurred or in state x_2 with the occurrence of a fault. In a probabilistic framework, the probabilities to be in state x_1 or in state x_2 are not necessarily the same. However, the probability to observe w, independently from the target state represents the probability to be in a f-uncertain state.

The estimator is a PDES which makes explicit this piece of information: a state of the estimator is composed of a state name from the original system, a fault label (N or F) and a new attribute which indicates if we can decide or not that a fault occurred when the system arrives to this state, i.e., this attribute indicates simply if the state belongs to some f-uncertain state or not. The transitions of the estimators correspond to a refinement of those of the diagnoser. Indeed, if we have a transition in the diagnoser from a state q_1 to a state q_2 by means of an observable σ then for each sub-state in q_2, we have at least one sub-state in q_1 which transits to it by σ, of course, with some probability. The estimator makes explicit these internal transitions and their corresponding probabilities. Formally, the estimator is defined by $\Delta = (Z, E_o, \varphi, z_0)$ where:

- Let $q_0, \ldots, q_k$ be the states of the diagnoser G_d such that $q_0 = \{(x_0, N)\}$. The set of the states of Δ is $Z \subseteq X \times \{N, F\} \times \{NA, A\} \times \{0, \ldots, k\}$ where NA (resp. A) is a new label standing for non ambiguous (resp. ambiguous). The initial state of Δ is $z_0 = (x_0, N, NA, 0)$ and each sub-state (x, l) of a state q_i of G_d corresponds to a state $z = (x, l, Att, i)$ of Δ where:

$$Att = \begin{cases} A & if \quad q_i \ is \ an \ f-uncertain \ state \\ NA & else \end{cases}$$

- E_o is the set of observable events.
- $\varphi : Z \times E_o \times Z \longrightarrow [0..1]$ is the probabilistic transition function of Δ. Let $z = (x, l, Att, i)$ and $z' = (x', l', Att', i')$ be two states of Z and σ be an observable event. The transition probability $\varphi(z, \sigma, z')$ can be different from 0 only if there is a possible transition from z to z'. From the construction of the diagnoser G_d, this corresponds to the case where there is at least some trace $s \in L_\sigma(G, x)$ such that $l' = LP(x, l, s)$ and $(x, s, x') \in \delta$. Let S be the set of all such traces: $S = \{s \in L_\sigma(G, x) | l' = LP(x, l, s) \quad and \quad (x, s, x') \in \delta\}$. The transition probability $\varphi(z, \sigma, z')$ is then the sum of the probabilities of transitions from x to x' by the different traces of S: $\varphi(z, \sigma, z') = \sum_{s \in S} \theta(x, s, x')$.

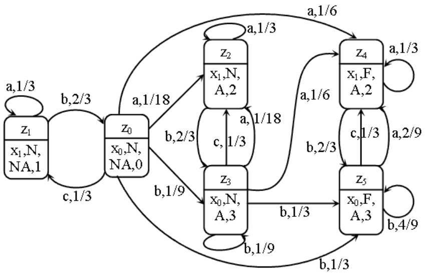

Figure 3. The estimator

Figure 3 shows the estimator of the system presented in example 1.

Remark 1 *It can be easily shown that the maximum number of states in the estimator is exponential on the number of states in the system and since we consider one fault at a time this number is linear on the number of fault types.*

Proposition 2 *The sum of the probabilities of all transitions issued from each state of* Δ *equals 1:*

$$\sum_{\sigma \in E_o} \sum_{z' \in Z} \varphi(z, \sigma, z') = 1 \ \ for \ each \ z \ in \ Z$$

3.3 Probabilistic analysis

In this section, we show how to extract from the estimator an homogeneous and discrete Markov chain and then to exploit the well known results about the asymptotic behaviors of such chains (for more details about that, see for example [4]) to provide some refinement to the classical binary diagnosability. We think that such a refinement can be, in practice, very useful in taking decisions about what adaptations have to be done on a non diagnosable system.

3.3.1 The Markov chain associated with the estimator

To an estimator $\Delta = (Z, E_o, \varphi, z_0)$, we associate the homogeneous and discrete time Markov chain $\{M_i, i = 0, 1...\}$ where M_i is a random variable whose value is the state of the system after the observation of the i^{th} event occurring in the system. Z is the state space of our Markov chain. Its transition matrix tr is defined by:

$$\forall (z_1, z_2) \in Z^2, tr_{z_1,z_2} = \sum_{\sigma \in E_o} \varphi(z_1, \sigma, z_2).$$

Figure 4 illustrates graphically the Markov chain of the system presented in example 1. The corresponding transition matrix is:

$$tr = \begin{array}{c} \\ z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{array} \begin{array}{c} \begin{array}{cccccc} z_0 & z_1 & z_2 & z_3 & z_4 & z_5 \end{array} \\ \begin{pmatrix} 0 & 1/3 & 1/18 & 1/9 & 1/6 & 1/3 \\ 2/3 & 1/3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/3 & 2/3 & 0 & 0 \\ 0 & 0 & 7/18 & 1/9 & 1/6 & 1/3 \\ 0 & 0 & 0 & 0 & 1/3 & 2/3 \\ 0 & 0 & 0 & 0 & 5/9 & 4/9 \end{pmatrix} \end{array}$$

A Markov chain is said to be irreducible if its representative graph represents one strongly connected component. In the general case a Markov chain is reducible and its representative graph contains more than one strongly connected component. This is the case for Markov chains associated with the estimators described in this work.

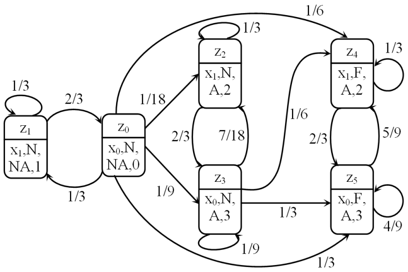

Figure 4. The representative graph of the Markov chain associated with the estimator

Proposition 3 *Under the assumption that there is at least one occurrence of a fault in the system, the Markov chain $\{M_i\}$ associated with the estimator Δ is reducible*[3].

3.3.2 The asymptotic behavior

In addition to the information about the binary diagnosability property of a system, the transition probabilities provide further useful information especially when the system is not diagnosable. By studying the asymptotical behavior of the Markov chain associated with the estimator, we can compute relevant probability measures concerning the possible infinite observable traces of the system. The fact that we consider infinite traces is not disadvantageous in practice because this study allows also one to estimate the average number of steps after which the system converges to a stage where it is or not diagnosable. After an arbitrary infinite execution of G, we focus on three probability measures that we think important in this context: the probability p^G_{Nd} that the observed infinite trace (projection of the execution onto the set of observable events) is non-diagnosable, i.e., we cannot decide if the fault occurred or not; the probability p^G_F that a fault occurred and the probability $p^G_{F/Nd}$ that a fault occurred known that the observed trace is non-diagnosable. To perform our analysis, we apply the following procedure:

1. Classify the states of the chain $\{M_i\}$. We recall that: a class is simply a strongly connected component in the representative graph of $\{M_i\}$; a persistent class is a class whose states have no successor outside it; if a persistent class contains only one state, then it is said to be absorbent and a class which is not persistent is said to be transitory. Let $\zeta = \{C_1, \dots, C_h\}$ be the set of the persistent classes of $\{M_i\}$ and $\mu = \{\mu_1, \dots, \mu_r\}$ be the set of transitory states, i.e., which do not belong to persistent classes.
2. Put the transition matrix in the canonical form in which: persistent classes are put in the first and the states of each persistent class are put together. We obtain the transition matrix:

   $$tr = \begin{pmatrix} Tr_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & Tr_h & 0 \\ R_1 & \cdots & R_h & Q \end{pmatrix}$$

   Tr_i is the stochastic matrix containing the transition probabilities inside the persistent class C_i. The matrix $R = [R_1, \dots, R_h]$ (resp. the matrix Q) contains the transition probabilities from transitory states to persistent states (resp. to transitory states).
3. Compute the fundamental matrix of the Markov chain given by: $N = (I - Q)^{-1}$ (I is the unit matrix of size r) and the absorption matrix given by $B = N.R$. We have the following results: the probability to be in a transitory state after an infinite number of steps is 0; the average number of steps (observed events) before absorption (reaching a persistent class) starting from a transitory state i is given by the sum of the terms of the i^{th} row of the fundamental matrix N and the probability of absorption in the persistent state j when we start from state i is given by the term b_{ij} of the matrix B. The absorption probability of a persistent class is then the sum of the absorption probabilities of its states. The starting point for us is always the initial state $z_0 = (x_0, N, NA, 0)$ that we suppose without loss of generality be the first transitory state[4] which corresponds to the first row of N and B.

Let ζ_{Nd} (resp. ζ_F) be the subset of persistent classes containing only ambiguous states (resp. states with the fault label), i.e. states $z = (x, l, Att, i)$ where $Att = A$ (resp. $l = F$) and let $\zeta_{Nd \wedge F}$ be the subset of persistent classes containing only ambiguous states with the fault label: $\zeta_{Nd \wedge F} = \zeta_{Nd} \cap \zeta_F$. Then we can define the probabilities p^G_{Nd}, p^G_F and $p^G_{F/Nd}$ as follows:

- p^G_{Nd} is the probability to be absorbed in one of the classes of ζ_{Nd} starting from z_0. It is given by: $p^G_{Nd} = \sum_{c \in \zeta_{Nd}} \sum_{z \in c} b_{1z}$.
- p^G_F is the probability to be absorbed in one of the classes of ζ_F starting from z_0. It is given by: $p^G_F = \sum_{c \in \zeta_F} \sum_{z \in c} b_{1z}$.
- $p^G_{Nd \wedge F}$ is the probability to be absorbed in one of the classes of $\zeta_{Nd \wedge F}$ starting from z_0. Using the Bayes formulae, we obtain: $p^G_{F/Nd} = \dfrac{\sum_{c \in \zeta_{Nd \wedge F}} \sum_{z \in c} b_{1z}}{\sum_{c \in \zeta_{Nd}} \sum_{z \in c} b_{1z}}$.
- In addition to these probability measures, we can obtain the average number of steps before absorption starting from state z_0 by the relation: $\overline{Nb}^G_{Abs} = \sum_{j=1}^{r} (N)_{1j}$.

[3] Supposing that there is at least one fault occurrence in the system, the estimator must contain at least one state whose fault label is F and it is easy to prove that from such a state we can never come back to the initial state z_0 whose fault label is N.

[4] z_0 is always transitory. See the explanation given in the previous footnote.

Let us now come back to our example (see the transition matrix in the previous section and the representative graph in figure 4). We have one persistent class $C = \{z_4, z_5\}$ and two transitory classes: the first one contains the states z_0 and z_1 and the other one contains the states z_2 and z_3. After putting the transition matrix in the canonical form we compute the matrices N and B. The first rows (corresponding to z_0) of these matrices are:

$$N_1 = \begin{array}{c} \begin{array}{cccc} z_0 & z_1 & z_2 & z_3 \end{array} \\ \begin{pmatrix} 3/2 & 3/4 & 5/12 & 1/2 \end{pmatrix} \end{array} \text{ and } B_1 = \begin{array}{c} \begin{array}{cc} z_4 & z_5 \end{array} \\ \begin{pmatrix} 1/3 & 2/3 \end{pmatrix} \end{array}$$

From N_1 we obtain that: $\overline{Nb}^{G}_{Abs} = 3/2 + 3/4 + 5/12 + 1/2 = 3.16 \;\; steps$. Moreover, we have: $\zeta_{Nd} = \zeta_F = \zeta_{Nd \wedge F} = C$. Thus, we obtain : $p^G_{Nd} = p^G_F = p^G_{F/Nd} = 1$. This means that, in average, after the observation of 3 to 4 events, we are almost sure that the trace observed corresponds to a non-diagnosable trace theoretically, but we are also almost sure that a fault has occurred.

4 EXAMPLES

The figures 5 shows four examples of PDES. The lack of space prevents us to examine in detail, for these examples, the whole of the analysis procedure described in this paper. So, we only comment briefly the final results that are summed up in table 1.

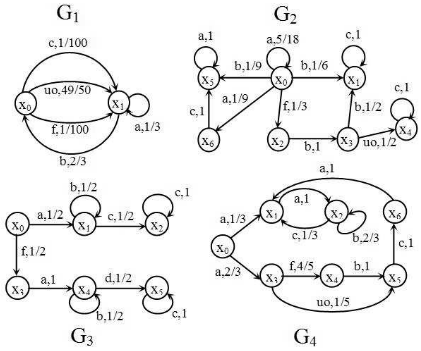

Figure 5. Examples

G_1 has exactly the same structure that the system discussed in this paper but with different probability transitions: we put a very small probability in the transition containing the fault. We obtain the same probabilities: $p_{Nd} = p_F = p_{F/Nd} = 1$ but the average number of steps before being absorbed passes from 3.16 to 150.5. In G_2, we have the probability of $6/13$ that an arbitrary infinite trace observed in the system be non-diagnosable and the same probability that it contains a fault (the probability to be in a diagnosable trace (resp. in a trace without fault) is then $1 - 6/13 = 7/13$). We have the probability of $1/2$ that a non-diagnosable trace contains a fault. Even if G_3 is theoretically non-diagnosable, the probability to observe a non-diagnosable trace tends to 0 when the length of this trace tends to ∞. In addition, in average, we must not wait for a long time before obtaining a diagnosable trace ($\overline{Nb}^{G_3}_{Abs} = 3$) in which the probabilities of having or not a fault are here equal. Finally G_4 is diagnosable, it is then obvious to obtain that $p_{Nd} = 0$ as in G_3. However, the difference between the two cases is that the estimator of G_3 contains at least one ambiguous state (with $Att = A$) but that is transitory, whereas all states in G_4 are unambiguous (with $Att = NA$).

G_1 and G_2 are examples where the probability of non diagnosability tends to a strictly positive value when the length of the observed trace tends to ∞. But, even in this case, the knowledge about the fault probability in an arbitrary infinite trace can be significant for taking decisions: in G_1 even if we are sure that all infinite traces are ”theoretically” not diagnosable, we know that the probability that a fault occurs tends to 1. The situation is completely different in G_2 in which the non diagnosability of the system is more ”effective”. G_3 is an example of a system which can be kept unchanged even if not diagnosable unless the average time before absorption is judged very long, because the probability to stay in a non-diagnosable trace tends to 0 when the length of the observed trace tends to ∞.

Table 1. Results for the PDESs G_1 to G_4.

	# pers. classes	p_{Nd}	p_F	$p_{F/Nd}$	$\overline{Nb}^{G_i}_{Abs}$
G_1	1	1	1	1	150.5
G_2	4	$6/13$	$6/13$	$1/2$	2.38
G_3	2	0	$1/2$	no	3
G_4	2	0	$8/15$	no	3.2

5 CONCLUSION

We have shown that using probabilistic information about the transitions of a DES, when available, can provide useful refinement of the binary decision about the diagnosability of the system. Especially, this refinement can lead in practice to tolerate non-diagnosability in cases where it is not persistent, i.e., in cases where it suffices to let the system run for enough long time to be almost sure that the observed trace will allow one to decide if a fault occurred or not.

Different perspectives are open from this first investigation. We want to generalize this work to other DES formalisms like Petri nets and symbolic transition systems, to the distributed case, and to the case where reparability actions are also available, in order to study global self-healability in a probabilistic framework.

REFERENCES

[1] A. Cimatti, C. Pecheur, and R. Cavada, ‘Formal verification of diagnosability via symbolic model checking’, in *18th International Joint Conference on Artificial Intelligence (IJCAI’2003)*, pp. 363–369.

[2] L. Console, C Picardi, and M. Ribaudo, ‘Diagnosis and diagnosability analysis using PEPA’, in *14th European Conference on Artificial Intelligence (ECAI’2000)*, pp. 131–136.

[3] S. Jiang, Z. Huang, V. Chandra, and R. Kumar, ‘A polynomial algorithm for testing diagnosability of discrete event systems’, *IEEE Transactions On Automatic Control*, **46**(8), 1318–1321, (2001).

[4] J.G. Kemeny and J.L. Snell, *Finite Markov Chains*, Springer-Verlag, 1983.

[5] Y. Pencole, ‘Diagnosability analysis of distributed discrete event systems’, in *16th European Conference on Artificial Intelligence (ECAI’2004)*, pp. 173–178.

[6] J. Rintanen and A. Grastien, ‘Diagnosability testing with satisfiability algorithms’, in *20th International Joint Conference on Artificial Intelligence (IJCAI’2007)*, pp. 532–537.

[7] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, ‘Diagnosability of discrete-event systems’, *IEEE Transactions On Automatic Control*, **40**(9), 1555–1575, (1995).

[8] A. Schumann and Y. Pencole, ‘Scalable diagnosability checking of event-driven systems’, in *20th International Joint Conference on Artificial Intelligence (IJCAI’2007)*, pp. 575–580.

[9] T. Yoo and S. Lafortune, ‘Polynomial-time verification of diagnosability of partially-observed discrete-event systems’, *IEEE Transactions On Automatic Control*, **47**(9), 1491–1495, (2002).