People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Mohamed Khider University - Biskra

Order Number: ....
Series: ....

Faculty of Exact Sciences and Sciences of Nature and Life
Computer Science Department

THESIS

In Candidacy for the Degree of

DOCTOR 3^{rd} CYCLE IN COMPUTER SCIENCE
Option: Artificial Intelligence

By

SOUMIA MANCER

TITLE

A CPN-Approach for Distributed Abductive Reasoning

Application to Causal Model-Based Diagnosis

Defended on: 29/06/2020
in front of the jury composed of:

Mr. Laid Kahloul	Professor at the University of Biskra	President
Mr. Hammadi Bennoui	Professor at the University of Biskra	Supervisor
Mr. Allaoua Chaoui	Professor at the University of Constantine 2	Examiner
Mr. Mustapha Bourahla	Professor at the University of M'sila	Examiner
Mr. Abdelhamid Djeffal	Associate Professor at the University of Biskra	Examiner

Abstract

This thesis deals with fault diagnosis of distributed systems from a model-based view where Coloured Petri Nets are used to describe the system behaviour. The systems concerned here are those comprising different interacting subsystems. Coloured Behavioural Petri Nets are defined as a particular CPN intended for the description of a system's causal behaviour, where each transition is labelled with a matrix describing explicitly its firing ways. The use of such matrices helps in tackling the problem of complexity during backward analysis, and gives rise to a very specific technique based on reachability of CBPNs called CW-analysis. CBPNs together with the CW-analysis are used to develop a distributed model-based diagnosis approach. The diagnostic system is defined as set of diagnostic agents where each is assigned to diagnose a subsystem. Accordingly, the system model consists of a set of place-bordered CBPNs, whereas CW-analysis is exploited to implement a local diagnosis scheme. Once local diagnoses are obtained by the different agents, a cooperation process should be initiated to ensure global consistency of such diagnoses.

key-words: Model-based diagnosis, Causal models, Petri nets, Reachability analysis, CW-analysis.

RÉSUME

Cette thèse traite le problème du diagnostic des pannes dans les systèmes distribués à partir d'une approche basée-modèle où les réseaux de Petri colorés (CPNs) sont utilisés pour décrire le comportement du système. Les systèmes concernés ici sont ceux comprenant différents sous-systèmes en interaction. Les réseaux de Petri colorés comportementaux (CBPNs) sont définis comme un CPN particulier destiné à la déscription du comportement causal d'un système, où chaque transition est étiquetée avec une matrice décrivant explicitement ses modes de franchissement. L'utilisation de telles matrices aide à résoudre le problème de la complexité lors de l'analyse en arrière et donne lieu à une technique très spécifique basée sur l'accessibilité des CBPNs, appelée CW-analysis. Les CBPNs et la CW-analysis sont utilisés pour développer une approche de diagnostic basée-modèle distribué. Le système de diagnostic est défini comme un ensemble d'agents où chacun est chargé de diagnostiquer le sous-système associé. En conséquence, le modèle du système consiste en un ensemble de CBPNs avec places de frontières, tandis que la CW-analysis est exploitée pour realiser le diagnostic local. Une fois les diagnostics locaux obtenus par les différents agents, un processus de coopération doit être engagé pour assurer la cohérence globale de ces diagnostics.

Mots-clés: Diagnostic basé-modèle, Modèles causaux, Réseaux de Petri, Analyse d'accessibilité, CW-analysis.

ACKNOWLEDGEMENTS

Firstly, and foremost, I would like to thank God for giving me the strength, knowledge, ability and opportunity to undertake this research study and to persevere and complete it satisfactorily.

I would like to take this opportunity to express my gratitude to my supervisor professor Hammadi Bennoui for the continuous support of my PhD study, for his patience and motivation. Thank you Sir for encouragement, advice, and support through ups and downs all those years.

I also thank those who agreed to be the referees of this thesis and allocated their valuable time in order to evaluate the quality of this work: Prof. Laid Kahloul, Prof. Allaoua Chaoui, Prof. Mustapha Bourahla and Dr. Abdelhamid Djeffal for their examination of the report and their valuable comments.

Special thank is dedicated to Prof. Kazar Okba, director of LINFI laboratory. Also, I express my very special appreciation to Mr. M'hamed Mancer (my brother), Mr. Abd Alhakim Cheriet and Mrs. Amira Mohammedi for the consistent support along my study years, and for the hand giving to me each time I get stacked.

My sincere thanks go to my best family ever, my parents, my brothers, and my sisters for their deep love and sincere support for me. Thank you so much.

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE **Page**

Chapter 1

Introduction

Ever since humans have been developing systems where an increasing number of them are dedicated, of course, for the facilities of daily life. For instance, there are many well-known examples in application areas such as medical devices, aircraft flight control, nuclear systems, household appliances, and so on. For such systems, high performance, product quality, and cost-efficiency are continuously required, besides the insistent demands for more system reliability, availability, security, and safety. Unfortunately, the fact is *"any human-made system is prone to fail"*, system failures are relatively common. On average, these failures cause inconvenience but no serious, long-term damage. However, this would not be the case all the time, some failures result in loss of life, significant property damage, or damage to the environment. Concerning such undesirable effects, the need for effective means to deal with them is quite apparent. For this very issue, fault diagnosis has been extensively appreciated in both industry and academia.

Global Overview and Motivation

From a general perspective, fault diagnosis can be explained as follows. Any designed system has a behaviour, obviously defined in terms of its observed variables, for which it is known a priori when it is normal (often called the *expected behaviour*). At some point in time, an observation over the system is made, *e.g.*, checking the temperature degree. When the made observation does not coincide with what is expected, it indicates a symptom, and so a system failure (usually, a system failure is defined to be any deviation of the system from its normal behaviour). The task of fault diagnosis is to, given such a symptom, generate a diagnosis statement, thus to determine the causes leading the system to misbehave, which helps effectively to get the system back to well-functioning. Therefore, different branches of science have carried out the problem of fault diagnosis such as mechanical engineering, electronics, automatic control, and computer science. A great deal of research effort has been spent on the design and development of efficient diagnostic systems, which gives rise to a variety of approaches and schemes.

Model-based diagnosis (MBD) is a general approach, whose efficiency in dealing with system failures has been demonstrated by a great number of successful applications in different sectors. Here, the diagnosis is performed on the basis of a mathematical model of the system behaviour. The main idea consists in the comparison between the observed behaviour and the one which can be predicted using the system model. It has been adopted practically in two distinct and parallel research communities. The Fault Detection and Isolation (FDI) community has evolved in the automatic control field from the seventies and uses techniques from control theory and statistical analysis. The DX community emerged more recently, with foundations in the fields of computer science and artificial intelligence (AI).[1]

Generally, the diagnostic activity comprises two components: the system model and the diagnosis process itself (*i.e.*, the search strategy). Along the line of AI, qualitative causal models with logic are used to describe the system behaviour, while the search for the cause of a system failure is abductive reasoning. For the sake of simplicity, the system model is qualitative because it uses a particular terminology such as "high/low temperature". In this case, the system variables (states) are characterized by a *few discrete values*. On the other hand, the model

[1] While the FDI approach focuses on fault detection in dynamical systems, the DX approach focuses on diagnosis reasoning. A discussion of a common approach for methods used by the FDI and DX communities has been investigated not very early ([16], [17]).

is causal because it describes the *cause-effect relationships* generally between symptoms and failures. Concerning the reasoning, abduction is a non-monotonic reasoning paradigm that explains hypothetically what has been observed. In other words, it generates hypotheses for the sources (causes) of faults.

Up to here, the most important distinguishing feature in diagnostic systems is the modelling formalism, which even the reasoning task rests on. Originated in the late 80's, the foundations and basic notions for the MBD approach were logically introduced [44]. Since then, different approaches have been developed for different purposes by means of different formalisms. Petri nets, among others, have been widely used in this area, they have been proved well-suited formalism that provides, other than modelling, effective analysis and verification tool. While the net model represents the system behaviour, the classical analysis techniques of PNs can be exploited to perform the diagnostic reasoning scheme. Such techniques can be classified as behavioural, relying on net reachability; or structural, based on the incidence matrix and state equation.

Although being useful for a very wide variety of application areas (due to the generality and permissiveness inherent in such nets), the major weakness of Petri nets lies in the complexity problem. A PN-based model tends to become too large and so hard to be analysed even for modest-size systems. The main reason behind that is the use of one kind of tokens (all tokens are black), which can be quite clear when dealing with systems composed of a number of different processes with similar structure and behaviour. A conceivable dealing, here, in order to face such a problem could be that, folding the net model structurally while preserving its proprieties. That is why the focus is turned specifically to Coloured Petri nets, as a high class of Petri nets, where the similar processes are described in a uniform and succinct way without losing the ability to distinguish between them by introducing the notion of *a token with a colour*. Therefore, the net places are attached to colour sets to determine the kind of tokens they can hold; the transitions are characterized by several firing ways (one at a time); while the arcs are associated with expressions to determine the involved token colours (to be consumed or produced) when the corresponding transition fires. Thereby, the net model becomes more reducible.

Here is a significant aspect to discuss. Since diagnosis adopts abductive reasoning on the one hand; and the notions of, let us say, the *logical diagnostic problem* are redefined in terms of reachability in PNs on the other hand, the system model analysis needs to be performed in a backward fashion, which corresponds to a backward reachability analysis. In a few words, given a marking, the backward reachability analysis allows us to compute the set of possible initial markings from which that marking could be reachable. For diagnosis, the marking to start from corresponds to a symptom, while the initial ones represent the possible causes leading the system to misbehave. Practically, the backward reachability analysis is the dual concept of the forward one. Thus, it can be performed as a forward analysis, obviously, on the reversed net model. For classical PNs, such a reversing can be done just by reversing the direction of arcs where the inputs become outputs and vice-versa.

The disappointing thing when using CPNs instead of classical PNs, especially for the tasks requiring backward reasoning such as diagnosis, is that the backward reachability analysis of CPNs could not be that ease, as for PNs. More accurately, in the CPN model, a transition may fire in several ways, which are implicitly determined by the related arcs expressions. Besides reversing the arcs' direction, the process needs an inversion of the arc expressions. Mathematically, an expression inversion is considered a cumbersome task generally for the case of multi-input arguments (of course, we exclude the case of one-input argument because it is so trivial). For the case we deal with, it often leads to a state-space explosion. The reasoning, here, considers all arguments as constants, except one for which the calculation would be performed. Such a process would be accomplished for each argument each time the transition needs to fire backwardly. It is easy to be figured out that it is difficult and also an inadequate way for reasoning.

Summing up. A couple of quite apparent issues have been discussed so far. The first concerns the PN-based approaches. Despite the suitability of PNs for modelling and analysis, the system representation becomes fairly complex. The second lies in the backward analysis based on reachability of CPNs. These issues motivate the work of this thesis: introduce efficient net models help in describing systems in a more reducible way, besides simplifying the analysis process.

Main Objectives

The goal of this thesis is to develop a distributed approach based on Coloured Petri Nets for causal model-based diagnosis of large and concurrent systems. The systems concerned by this approach are those consisting of a collection of interacting subsystems.

The first objective of the thesis is to define a particular CPN model called Coloured Behavioural Petri Net that allows describing the causal behaviour of the system under study. The concept of FW-matrix is introduced as a transition matrix representing the possible ways it may fire. The main concepts and related notions are formally defined.

The second objective is to define a method devoted for the analysis of such net models. The *CW-analysis* is introduced as a backward analysis technique based on reachability of CBPNs. Particularly, the concept of *inhibited colour* is defined as the main feature of CW-analysis, where the production of certain colours can take place.

With the two objectives fulfilled, the main goal is to develop a CBPN-based diagnosis approach, from centralized then distributed views, where the diagnostic problem is formulated in terms of reachability in CBPNs. The system model is given in terms of CBPNs, while the diagnostic reasoning is performed using the CW-analysis.

Main Contributions

The main contributions of this thesis can be summarized as follows:

- The Coloured Behavioural Petri Net model is introduced to represent a system's causal behaviour. The use of FW-matrices allows us to describe explicitly the different firing ways of transitions. Each row-vector of the matrix corresponds to a firing way, and so it determines the involved colours when the transition gets fired. In this case, an arc expression becomes a typed variable for an input arc and a selective function (which determines the corresponding colour to each output place) for the output one.

- As a second contribution, we first set the different concepts related to the CW-analysis technique. The technique can be performed by exploiting the FW-matrices with the help of *inhibited colours* (when dealing with conditions unsatisfied in the case under examination). Instead of inverting an arc expression during the backfiring of a transition (as usually do in CPNs), the process needs simple manipulation of its matrix where the input block becomes output and vice-versa. Secondly, we develop a CBPN-based approach where the formal notions concerning diagnostic problem and its solution can be re-formulated in terms of CBPNs, whereas the reasoning task can be implemented using the CW-analysis.
- The last contribution concerns the development of a distributed CBPN-based diagnosis approach. In this approach, the diagnostic system itself is defined as multiagent system where each agent is devoted to diagnose a subsystem. Therefore, the system model consists of a collection of place-bordered CBPNs.

Thesis Structure

This thesis is organized as follows::

Chapter 2 is dedicated to the preliminary concepts concering the model-based diagnosis, Petri nets and, in particular, Coloured Petri nets (CPNs) that will be used through the thesis. It ends by surveying the use of PNs for model-based diagnosis.

Chapter 3 provides a full description of the Coloured Behavioural Petri Nets class, citing the formal definitions and an illustrative example. At the end of the chapter a translation procedure from BPNs to CBPNs is detailed.

Chapter 4 introduces the CW-analysis and details the use of CBPNs for centralized model-based diagnosis.

Chapter 5 presents the distributed CBPN-based diagnosis approach for large and concurrent systems.

Chapter 6 outlines the concluding remarks and draws some future works.

Publications

As a result of this thesis the following publications were produced:

- Mancer, S., & Bennoui, H. (2017). Coloured Petri Nets Based Diagnosis on Causal Models. In PNSE@ Petri Nets (pp. 123-136).
- Mancer, S., & Bennoui, H. (2019). Distributed Diagnostic Problem Solving With Colored Behavioral Petri Nets. IEEE Transactions on Systems, Man, and Cybernetics: Systems.

Part I

Preliminaries

CHAPTER 2

MODEL-BASED DIAGNOSIS & PETRI NETS

Model-based diagnosis (MBD) is a general approach based on a model of the system behaviour for reasoning. Petri nets (PNs) and Coloured Petri Nets, on the other hand, are powerful and recognized tools that offer a clear and precise language for modelling and analysis. This chapter is dedicated to recall the basic concepts and notions related to model-based diagnosis, PNs, and CPNs, which are known useful throughout the thesis. It will be followed by a brief survey concerning the use of PNs/CPNs in the area of model-based diagnosis with a particular emphasise on the BPN-based diagnosis approach.

2.1 Introduction

With the aim of developing methods and techniques help in discovering automatically and effectively the causes leading a system to misbehave, a prominent concern of research effort has been and is being oriented towards fault diagnosis problem. A general investigation of such a problem considers the type of knowledge available. In fact, there are two kinds of diagnostic knowledge, shallow knowledge and the so-called deep knowledge. Shallow knowledge refers to empirical knowledge that can be gleaned from past experience with the meant system. It consists of a set of observations of faults assigned to them diagnoses and generally takes the form of an expert system (it is usually acquired by interviewing domain experts and encoded as if-then rules). On the other hand, deep knowledge refers to the knowledge about the system internal structure, components, and their interactions. It may be developed from a fundamental understanding of the system in the form of a mathematical model, which allows us predicting its behaviour for any admissible input condition. Up to here, the approaches making use of shallow knowledge are classified as expert-system approaches and model-based approaches in the case of deep knowledge.

Early in the previous century, diagnosis occurred as one of the most common domains where the expert-system approach was applied; unfortunately, using it for diagnosis of artefacts rather than medical diagnosis became a bottleneck. The acquiring and maintenance of the required knowledge represent cumbersome tasks in the deployment of diagnostic systems. In the late 70's and instead of using such expert or shallow knowledge (which could be regarded as the experts' subjective view of the system), the use of deep knowledge (as the objective view of the system) for diagnosis started to be investigated. Since then model-based diagnosis has become a general approach adopted successfully in a variety of application domains, *e.g.*, aerospace, military, transportation, manufacturing and production, ... etc. In this approach, the reasoning process is performed based on a mathematical model of the system behaviour, together with an observation of how the system actually behaves. A problem of diagnosis is then pointed out when there are discrepancies between the gotten observation and the predicted behaviour (using the system model), the idea of the approach is fully presented in

Fig. 2.1.

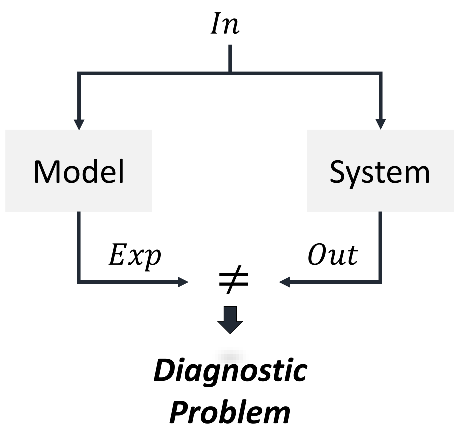


Figure 2.1: A presentation of diagnostic activity

Given the same input value for both the real system and its model. The output of the system (gotten by observation) is compared to the expected one (generated using the system model). For the case of no differences between the obtained results (outputs), it may be assumed that the system works correctly. In case some significant difference of the observed behaviour from the predicted one takes place, it must be stated an inconsistency between the system real behaviour and its model. Here, system misbehaviour is detected, which implies the occurrence of a fault (when assuming the system model is correct).

A model is some description of a system given, in our case, in a formal manner by using a modelling language. For diagnosis, this model can describe the system behaviour in the fault-free case ($i.e$, correct behaviour), as it can give knowledge about which fault can occur and the consequences it may provoke ($i.e$, faulty behaviour), and possibly both. A system model is usually component-oriented, where the corresponding system can be viewed as a set of components interacting among each other. This is the case when the model is not designed specifically for diagnosis purposes, thus no information about the system behaviour in the presence of faults is given. Here, a system diagnosis consists of identifying the parts of the system responsible for some unexpected behaviour. Another possible view of the system model could be that describing the causal relationships between faults and symptoms, it exploits by that the system causal behaviour.

2.2 Principles of Model-Based Diagnosis

In this section, a short overview of model-based diagnosis is given. In particular, it reviews the most popular approaches to diagnosis the abductive and the consistency-based. Then, it details a unified framework based on the integration of both approaches for centralized and distributed systems. Here, the first-order logic will be used to formalize the main notions and concepts related to each approach.

2.2.1 Approaches to model-based diagnosis

According to the representation of knowledge about the normality and faults, and then how diagnoses are defined and computed, there are two prevailing approaches to model-based diagnosis, consistency-based [44] and abductive [39].

Consistency-based diagnosis

Back to the seminal paper *"A Theory of Diagnosis from First Principles"* of *Raymond Reiter*, where he has set the basic notions of diagnostic reasoning based on analysis of inconsistency between the system real behaviour and the predicted one (using its model). In this theory, the system model is already available, it may be constructed for reasons other than diagnosis, as the case of an artefact where the created models during its designing could be exploited for diagnosis.

In this approach, the system description SD can be defined by the pair $(BM, COMPS)$. BM, for Behavioural Model, is a set of first-order formulas defining how the system components are connected and how they normally behave. $COMPS = \{c_1, ..., c_n\}$ is a set of constants listing the system components. By assuming that all of these components behave correctly, $\forall c \in COMPS\ \neg AB(c)$ (AB for abnormal), the correct behaviour of the system can be formalized as:

$$BM \cup \{\neg AB(c_1), ..., \neg AB(c_n)\}$$

On the other hand, the current behaviour of the system can be obtained by measuring the values of its observed variables as an observation. This observation can be given as a set of first-order formulas too, let it be OBS. When the system acts correctly, then it fulfills the consistency of

$$BM \cup \{\neg AB(c_1), ..., \neg AB(c_n)\} \cup OBS$$

Whereas, if at least one of the system components becomes faulty, $\exists c \in COMPS$ $AB(c)$, it turns out to be inconsistent. In this case, we have a problem of diagnosis, the observation on the system is inconsistent with the assumption above (all components work as expected). A diagnostic problem is then given by

$$DP = (BM, COMPS, OBS)$$

It should be noted that the resulted inconsistency is caused by assuming that all components behave correctly, which is in fact wrong. Therefore, the diagnostic process consists in searching for some set of components, a subset of $COMPS$, that when assumed to be faulty, it brings consistency back explaining the system misbehaviour.

Definition 2.1. A diagnosis for a system with observation, given by (BM, $COMPS$, OBS), is a minimal set $\Delta \subseteq COMPS$ such that

$$BM \cup OBS \cup \{AB(c)|c \in \Delta\} \cup \{\neg AB(c)|c \in \{COMPS - \Delta\}\} \text{ is consistent}$$

The minimality requirement is strictly necessary, here, to avoid redundant diagnoses. Notice that by changing the assumption $\neg AB(c)$ to $AB(c)$ for certain component c, it leads to regaining consistency between the observed behaviour of the system and the one predicted using its model. In this case, c is assumed to be broken, then $\Delta = \{c\}$ is a diagnosis to DP. It is a *consistency-based diagnosis*, by which explaining inconsistent observations corresponds to restoring consistency.

Before moving on, it is worthy to outline the notion of a *conflict set*, as the key idea of the theory of consistency-based diagnostic reasoning. A conflict set is any subset of components $\{c_1, ..., c_k\} \subseteq COMPS$ that, given the observations, cannot be claimed to be simultaneously correct (at least one of them must be faulty), *i.e.*,

$$BM \cup OBS \cup \{\neg AB(c_1), ..., \neg AB(c_k)\}$$

is inconsistent, besides it is said to be *minimal* if any of its proper subsets is not a conflict set. Up to here, consistency-based diagnoses can be built by combining elements from different conflict sets, each diagnosis should have at least a component in common with each conflict set, which leads us to another important concept, that is, a *hitting set*. We say that H is a hitting set for a collection of sets C if $H \subseteq \cup_{S \in C} S$ such that $H \cap S \neq \emptyset \ \forall S \in C$. Again, a hitting set is minimal if any of its proper subsets is not a hitting set. We end by presenting the basic theorem of Reiter's theory [44].

Theorem 2.1. *$\Delta \subseteq COMPS$ is a diagnosis for $DP = (BM, COMPS, OBS)$ if and only if Δ is a minimal hitting set for the collection of conflict sets for DP.*

Abductive diagnosis

The abductive diagnosis approach generally considers the faulty behaviour of the system. In fact, such reasoning is usually adopted in the medical domain. In this case, explaining misbehaviour or a symptom means finding a set of causes that implies logically the symptom itself and not just by being consistent with it, as the case of *consistency-based approach*. In this respect, the behavioural model of the system describes what happens in case of faults, when the system deviates from its correct behaviour. Therefore, we introduce a set of faulty behaviour modes for each component c as follows: $mode(c) = \{m_1, ..., m_n\}$, where $m_1, ..., m_n$ denote the possible failure modes. Here, the BM of the system contains, besides the structure of the system, a description for each faulty behaviour mode of each component (one of these modes could be the *unknown* mode with which no model is associated [36]), it is given as implications describing causal relationships between faults and their causes. Notice that due to the absence of the correct behaviour, no discrepancies between the observed and the predicted behaviours could be detected (there is no expected outputs to be predicted). Thus, $BM \cup OBS \cup \{\neg AB(c)\}$ remains consistent, unlike the previous approach.

Note that $OBS \equiv I \Rightarrow O$, where I denotes the inputs and O denotes the outputs. Since there is no inconsistency to be explained when the expected normal manifestations are unavailable, diagnostic reasoning is confined to give some account for some observed manifestations. Let $CO \subseteq O$ be a combination of outputs to be explained. An abductive diagnosis for CO is given by Δ such that:

$$BM \cup I \cup \Delta \vdash CO \text{ and}$$

$BM \cup I \cup \Delta$ is consistent.

*** Furthur remarks**

As discussed before, consistency-based and abductive diagnosis differ in the representation of normality and faults and in the meaning they give to the term *explain*. Instead of the abductive view where a component is abnormal if it manifests as it is described in the behavioural model[1], in the consistency-based view, a component is abnormal if its observed behaviour deviates from the expected one. that makes the difference between explanations very obvious. In the first approach, a solution attempts to explain why the system reacts as it is observed; while in the second a solution explains why the system exhibits a malfunction. In other words, any computed diagnosis does not exactly explain the observed behaviour of the system. The observed behaviour itself is not important, the significance lies in being different from what is expected. That explains some of the undesirable results when using such an approach (as illustrated in the domain of digital circuits by [23]).

An idea concerning both approaches consists in exploiting knowledge about faults in the consistency-based approach, and knowledge about correct behaviour in abductive approach. In other words, extending component-oriented models to describe the possible faults of the system and their consequences, as well as including descriptions of nominal behaviour in causal models ([38], [51]). In fact, the two approaches were integrated ([22], [13], [18]) and shown to be the extremes of a wide spectrum of possible definitions of diagnosis ranging from a pure consistency-based diagnosis to a pure abductive diagnosis [15].

2.2.2 Unified framework for MBD

In the framework proposed in [15], the diagnostic problem is defined as an abduction problem with consistency constraints, where an observation must be entailed by a diagnosis with the satisfaction of some consistency constraints.

[1] In fact, BM describes, according to the abductive approach, different faulty behavioural modes. In the discussion above we have assumed, for reasons of simplicity, that only one faulty behavioural mode, noted AB, is modelled.

Here, the correct and faulty behaviours of a system have been represented in a uniform way. As already known, a model of the investigated system is of crucial importance in order to perform a model-based diagnosis. Usually, such a model is developed based on a deep understanding of the system. This understanding can be generally expressed in terms of relationships between the different units or variables of the system. In fact, qualitative models are widely used essentially for diagnostic reasoning, which does not require precise measures over the system, but rather it works in broad ranges of values like absent/present, high/low and so on. In this case, the system variables are characterized by a *few discrete values*. When such relationships describe the cause-effect transformations among system variables, the system model, besides being qualitative, becomes causal. Indeed, causal knowledge is very useful for diagnosis, in particular, it helps to discover the causal path explaining the made observation.

In terms of causal models, system behaviour can be viewed as a set of states (also entities), describing partially the situations in which the system can be at a given time, connected among them by means of cause-effect relationships. Each of these states ranges over a finite set of values often referred to as admissible-values. According to [14], the system states can be classified, for diagnostic purposes, into:

- Initial-causes: represent system states from which any evolution begins;
- Internal-states: represent non-observable states, usually, as consequences of initial-causes;
- Manifestations: are observable and measured states by which observations would be made.

When dealing with faulty models, initial-causes represent initial perturbations leading the system to misbehave, whereas manifestations represent expected symptoms. In this case, explaining a symptom, an observation in general, consists of finding a set of initial causes implying it.

Up to here, a diagnostic problem consists of the triple $DP = (BM, INIT, OBS)$, for which BM is the causal model describing the system behaviour, while $INIT$ denotes the set of initial-causes instances in terms of which an observation OBS would be explained. A solution to DP must predict the observation OBS, as well as satisfy some consistency constraints. By the way, as already said, according to the unified framework, there is a spectrum of diagnostic problem definitions depending on the selected (sub-)observations to be covered (directly supported) by a diagnosis. A diagnostic problem DP is then defined as an abduction problem as follows.

Definition 2.2. The abduction problem corresponding to DP is given by

$$AP = (BM, INIT, \langle \Psi^+, \Psi^- \rangle)$$

such that: $\Psi^+ \subseteq OBS$ and $\Psi^- = \{m(x) | m(y) \in OBS, x \neq y\}$ (m is a manifestation and $x, y \in admissible\_values(m)$).

By considering OBS to be the made observations. Ψ^+ is a subset of observations to be entailed (covered) by a solution of AP. Ψ^- is the set of all possible values that conflict with the made observation (which are known to be absent in the case under examination). It is typically used for consistency checking. A solution to AP is then defined as $\Delta \subseteq INIT$ for which

$$\begin{array}{ll} \forall x \in \Psi^+ & BM \cup \Delta \vdash x \\ \forall y \in \Psi^- & BM \cup \Delta \nvdash y \end{array}$$

Δ must predict each parameter in Ψ^+ and no parameter in Ψ^-. In other words, a solution to AP must be consistent with all observable parameters while covering a selected group of them.

2.2.3 Distributed Model-Based Diagnosis

Generally, when designing a fault diagnosis system one can pursue a centralized, decentralized, or distributed architecture. With the fact that an increasing number of nowadays built systems are concurrent and often distributed, the most suitable architecture when constructing a diagnostic system would be the distributed one. Practically, a distribution of the system model over the diagnosis system can be (referring to [48]):

* *spatially* according to the spatial distribution of the system's components;

* *semantically* according to the type of knowledge, e.g. a separate model of the electrical and of the thermodynamical behaviour of the system.

In this thesis, we focus on the spatially distributed one.

A distributed system S (the one to be diagnosed) is characterized by its structure, it consists of a collection of interacting subsystems $S_1,...,S_n$ (each of which represents a part of S), that do communicate and cooperate among each other. And with that, a distributed approach of multiple diagnostic agents, where each agent is associated with a specific subsystem, has been argued appropriate [46]. In such an approach, the system model is distributed over the agents, the diagnosis is locally generated and the consistency between the subsystems should be satisfied, by means of communication among agents (agents derive the distributed diagnosis by local calculations and by information exchanges, e.g., [25], [24], [26], [29], [4], [31], [43], [52], and [53]). In that case, each agent A_i is in charge of a subsystem S_i, has its local model, receives the local observations and can exchange limited information with the adjacent agents for consistency checking.

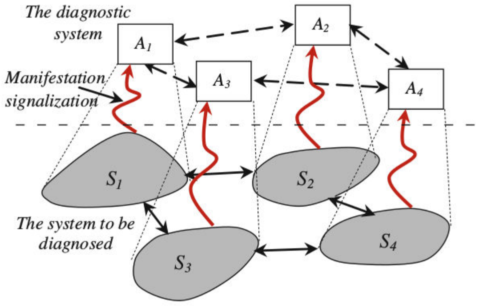


Figure 2.2: A diagnostic system architecture.

Within this view, the initial DP can be formalized as a conjunction of n local diagnostic problems $DP = \bigcup_{i=1}^{n} DP_i$. Each of these DP_i corresponds to a particular subsystem S_i. Notice that each subsystem S_i can not be fully independent from the other system parts. It interacts with them through different connection elements. By considering these connection elements, a local diagnostic problem DP_i would be given by $DP_i = (BM_i, INIT_i, In_i, Out_i, < \Psi_i^+, \Psi_i^- >)$. Here, $(BM_i, INIT_i, < \Psi_i^+, \Psi_i^- >)$ can be viewed similar to the initial diagnostic problem.

In_i and Out_i correspond to connection elements that are classified into inputs to S_i, that are determined from other subsystems S_j, and outputs from S_i to S_j.

Definition 2.3. Given a local diagnosis problem $DP_i = (BM_i, INIT_i, In_i, Out_i, < \Psi_i^+, \Psi_i^- >)$, a *consistent local solution* to DP_i is a set of assumptions $\Delta_i \subseteq INIT_i$, such that:

$$\forall m \in Out_i^+ \cup \Psi_i^+ : \; BM_i \cup In_i \cup \Delta_i \vdash m$$

$$\forall n \in Out_i^- \cup \Psi_i^- : \; BM_i \cup In_i \cup \Delta_i \nvdash n$$

In order to determine a solution to DP that is globally consistent, the reasoning task needs to be performed in two steps. At first, the agent A_i defines a preliminary local diagnosis to DP_i in absence of any external information from neighbouring agents. The step that follows consists of checking consistency with neighbouring agents. Each agent A_i must discard its own diagnoses that are not consistent with those of the neighbourhood. Starting from Δ_i, agent A_i deduces the instances of the states corresponding to outputs of S_i to be compared with values requested by neighbouring agents as their inputs. Note that, analogously to the gotten observation, Out_i is classified into two subsets Out_i^+ and Out_i^-. Out_i^+ denotes the output values that are modelled in BM_i and are deduced from Δ_i; whereas Out_i^- holds the modelled values in contradiction with the deduced ones.

2.3 Petri Nets

In about the 1960's, Petri nets were introduced by Carl Adam Petri in his PhD dissertation as bipartite directed graphs intended for modelling concurrent, asynchronous, distributed and/or parallel systems. Petri nets are well-suited tools that offer a clear and precise description of the system's static structure besides its dynamics in one net model via the graph structure and the token game respectively. Another interesting aspect about them is that they are designed to assist system analysis, and so different techniques, reachability-based and algebraic-based, have been developed for studying them. Side by side to the formal description and analysis, such nets provide a convenient graphical representation of the investigated system that comprises: *places* (circles), *transitions* (rectangles), *tokens* (black dots) assigned to places, and *arcs* as relationships between places and transitions. The formal definition of Petri net and the relevant concepts are presented in what follows, for further details we address the reader to [35].

Definition 2.4. A Petri net is a 4-tuple $N = (P,T,A,W)$ where:

- $P \cap T = \emptyset$,
- $P \cup T \neq \emptyset$.
- $A \subseteq (P \times T) \cup (T \times P)$.

P is a set of places, T is a set of transitions, A is a set of arcs, and W is a weight function such that $\forall a \in A : W(a) \geq 1$. In case $\forall a \in A : W(a) = 1$, N is said to be an ordinary PN. In what follows, let $X = P \cup T$ be the set of nodes (elements) of a Petri net.

Definition 2.5. Given a net $N = (P,T,A,W)$ and $x \in X$. ${}^\bullet x = \{y|yAx\}$ and $x^\bullet = \{y|xAy\}$ are called the *pre* and *post* sets of the node x respectively. The node x is a source if ${}^\bullet x = \emptyset$, while it is a sink if $x^\bullet = \emptyset$.

Definition 2.6. Given a net $N = (P,T,A,W)$. A marking of N is a function $\mu : P \to \mathbb{N}$ representing the number of tokens into places. An initial marking is singled out and denoted μ_0.

A marked Petri net (N,μ) denotes a Petri net together with its marking.

Definition 2.7. Given a marked Petri net (N,μ). A transition $t \in T$ is enabled at a marking μ iff

$$\forall p \in {}^\bullet t : \mu(p) \geq 1.$$

Once t is enabled at μ, it may fire producing a new marking μ' (we write $\mu[t\rangle\mu'$) such that $\forall p \in P$:

$$\mu'(p) = \mu(p) - W(p,t) + W(t,p).$$

Example 2.1. *As an example, let us consider the logical expression $a \wedge b \equiv c$, where a, b and c assume boolean values (T for true and F for false) and $\wedge$ is the logical connective* and*; c is true only when both a and b are true, it is false otherwise. The expression c can be described by the Petri net shown in Fig. 2.3. Since a and b can* *be set in four different ways, the PN corresponding to c has four transitions, e.g.* t_1 *represents the setting when both a and b are true (given by the places* a_T *and* b_T *respectively), and so the value of c is also true (given by the places* c_T*).*

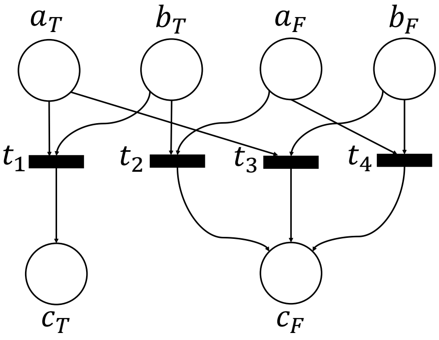


Figure 2.3: Petri net corresponding to $a \wedge b \rightarrow c$

A very useful tool for Petri nets analysis is the *reachability graph*. As an oriented graph, a reachability graph describes the state space of the system, that means the possible states the system could be in during execution. In fact, reachability can be considered as a fundamental basis for studying the dynamic properties of any system [35]. The firing of an enabled transition will change the token distribution (marking) in a net according to the transition rule. A sequence of firings will result in a sequence of markings. A marking μ is said to be reachable from a marking μ_0 if there exists a sequence of firings that transforms $\mu_0 \rightarrow \mu$.

Definition 2.8. Given a marked Petri net (N, μ_0), the reachability set from a marking μ_0, indicated as $R(N, \mu_0)$ (also $[\mu_0\rangle$), is the smallest set of markings such that:

- $\mu_0 \in R(N, \mu_0)$;
- if $\mu_1 \in R(N, \mu_0)$ and $\mu_1[t\rangle\mu_2$ for some $t \in T$, then $\mu_2 \in R(N, \mu_0)$.

At the end, we consider the following features:

- A safe marking is a marking such that $\forall p \in P : \mu(p) \leq 1$.

- Two transitions are said to be concurrent if and only if each time they are both enabled, the firing of one does not prevent the other from being enabled.
- A marked Petri net (N, μ_0) is deterministic if and only if $\forall \mu \in R(N, \mu_0)$ $\forall t_1, t_2 \in T$: if $\mu[t_1\rangle$ and $\mu[t_2\rangle$ then t_1 and t_2 are concurrent.
- Given a place $p \in P$, and a marking μ'. The situation where $\mu'(p)$ is said to be reachable from a marked Petri net (N, μ), write $(N, \mu) \vdash \mu'(p)$, iff

$$\mu' \in R(N, \mu) \text{ and } \mu'(p) \neq 0$$

Coloured Petri Nets

Coloured Petri Net is the expanded form of Classical Petri Net that has the ability of programming with ML programming language. ML is the programming language for AI whose composition with coloured Petri net modelling made it useful for creating recursive functions and different commands on the edges of models. By using Coloured Petri Net, adding operators and multi-set marking is possible, and the best tool for modelling and verification of models is CPN tools (CPN), used in the cases such as security and database systems and also in smart algorithms. In general, the CPN model is a formal model as a mathematical description of syntax and semantics model.

In [28], a full description of CPNs has been provided. In fact, such nets have been introduced in order to address the complexity problem of classical Petri nets (a PN model of a given system tends to become too complex, whether the model size or the analysis, even for a modest-size system). The principle of a CPN model is to extend the notion of token with a colour, we use the notation *token colour* by convenience. That allows describing similar processes in a uniform and succinct way without losing the ability to distinguish between them. Before giving the formal definition of CPNs we need to know about multi-sets. A multi-set is a set where individual elements may occur more than once.

Definition 2.9. A multi-set m over a set S is a function $m \in [S \to \mathbb{N}]$ denoted $\sum_{s \in S} m(s)'s$ where:

- $\forall s \in S : s \in m \ iff \ m(s) \neq 0$.
- S_{MS} is the set of all finite multi-sets over S.

We can therefore define the following operations to deal with mutlisets. Thus, $\forall m, m_1, m_2 \in S_{MS}$ and $\forall n \in \mathbb{N}$:

$$\begin{array}{lcl} |m| & = & \sum_{s\in S} m(s). \\ m_1 + m_2 & = & \sum_{s\in S}(m_1(s) + m_2(s))'s. \\ m_1 \neq m_2 & = & \exists s \in S : m_1(s) \neq m_2(s). \\ m_1 \leqslant m_2 & = & \forall s \in S : m_1(s) \leqslant m_2(s) \\ & & \text{(defined analogously to } \geqslant). \end{array}$$

Note. *In the CPN definition below, we set only the needed parts.*

Definition 2.10. A CPN is a 5-tuple $N = (\Sigma, P, T, A, C)$ where:

- $P \cap T = \emptyset, P \cup T \neq \emptyset$.
- $A \subseteq (P \times T) \cup (T \times P)$.
- $C \in [P \rightarrow 2^{\Sigma}]$.

The definition of the sets P, T and A for a CPN is analogous to that for Petri nets. Σ is the set of colour sets. C is a colour function that associates to each place p a colour set (denoted $C(p) \in \Sigma$). That means each place p may hold one or more tokens, each of which carries a colour (data value) belonging to p's colour set. A *marking* is a function μ such that $\forall p \in P : \mu(p) \in C(p)_{MS}$ which defines for each place a *multi-set* of colours that are presented into. The firing of a transition leads to moving tokens in the net model. Such tokens are determined by the arc expressions (which consist of typed variables, constants, functions or even operators). The evaluation of an arc expression is a multi-set of colours. Moreover, it can be attached to each transition a boolean expression (with variables) called a guard which specifies the bindings for which it evaluates to true. A binding is an assignment of data values to the free variables appearing in the expression of an incoming arc or a guard of a transition. A binding of a transition can be written in the form: $(v_1 = d_1, v_2 = d_2, ..., v_n = d_n)$ where $for \ i \in 1..n : v_i$ is a variable and

d_i is the value assigned to v_i. We denote by $Expr < b >$ the evaluation of the expression $Expr$ with the binding b.

A transition t is enabled if there is a binding such that:

1. The evaluation result of each of the input arc expressions is present on the corresponding input place;
2. The guard (if any) is satisfied.

When a transition t is enabled at a marking μ such that $\mu[t\rangle\mu'$, the new marking μ' is calculated as follows

$$\forall p \in P : \mu'(p) = \mu(p) - E(p,t) < b > +E(t,p) < b >$$

where $E(x_1,x_2)$ refers to the expression of the arc (x_1,x_2).

Example 2.2. *Back to the previous example. The CPN model corresponding to the same expression is displayed in Fig. 2.4, where $C(a) = C(b) = C(c) = \{T,F\}$, an expression is attached to each arc remembering that the x and y are variables on a multi-set. Thus the expression $x \wedge y$ states that in case transition t fires, a token of colour x and a token of colour y are destroyed on a and b respectively. Accordingly, the possible settings of the arc expression $x \wedge y$ are $T \wedge T$, $T \wedge F$, $F \wedge T$ and $F \wedge F$.*

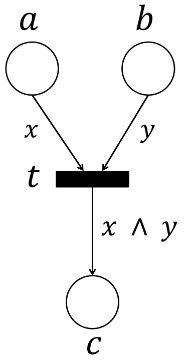


Figure 2.4: CPN corresponding to Example. 2.1

2.4 PN-Based Diagnosis

It is worth knowing that a system model is of crucial importance in the MBD approaches, thus the use of precise language plays a major role. Petri nets have become very well-known tools in this area due to their ability of modelling, validating and verifying a wide range of systems, all in a uniform language. Solving diagnostic problems using PNs has already been investigated by several researchers, we mention in this regard the works of [8], [47], [3], [42], [33], [54], [2], where the reasoning task is captured by exploiting the classical analysis techniques of PNs.

2.4.1 Brief survey

In fact, several approaches and frameworks have been proposed depending on the system nature and the used formalisms. In the context of Petri Nets, discrete event systems (DES) have gained big efforts. We mention in this regard the work of [6] on the problem of identification and synthesis of the faulty model of a PN in such a way the fault-free system is supposed to be known. The work of [34] investigates the effect of fluidization of PNs on fault diagnosis focusing particularly on untimed continuous PNs. As well, [49] provides a discussion of an online approach for DES fault diagnosis in basis of labelled PNs (an overview of the historical development of DES within PNs can be found in [27]). The work in [7] presents a decentralized approach based on labelled PNs for diagnosing discrete-event systems (DES). It extends the communication protocols defined in [19] for automata to the PN-based approach introduced in [9]. In the same field, the work in[12] deals with the problem of diagnosing DESs based on PNs by introducing an on-line decentralized approach, where the system to be diagnosed is assumed to be observed by a set of sites. Each site is informed with the system structure and the initial marking, whereas the observation is done locally. At the level of each site, a local diagnosis is performed by making use of some integer linear programming (ILP) problem solutions [21]. The work in [54] concerns the identification problem of faulty behaviour in a DES. Based on PNs, the identification process starts by extracting the abnormal behaviour from a given observed sequence, building a non-linear integer programming, then converting it to an ILP, whose solutions identify the set of faults leading the system to misbehave. We can mention also the work of [37] where a CPN version of the diagnoser introduced in [47] is presented. Such a diagnoser is constructed on the basis of a labelled PN model of the system to be diagnosed. The approach is, then, extended to implement a modular diagnoser for large distributed systems. The work of [32], as an earlier work, exploits CPNs as well for modelling, then diagnosing a BPEL web service, the diagnosis problem is given as inequations system constructed using the evolution equation of PNs, whereas to solve such a problem an algebra algorithm is proposed.

The work with the largest point of contact with this thesis is one quite early published by [42] (then extended by [3]), which addresses the problem of the application of PNs approach to model-based diagnosis. Such a work uses a specific class of PNs called Behavioural Petri Net (BPN), introduced in [1] to represent a system given by its causal behaviour. Moreover, it defines a particular backward reachability analysis method called BW-Analysis to perform the reasoning (diagnosis) scheme. It exploits two different kinds of tokens, *normal* and *inhibitor*, aimed at modelling the truth or falsity of the condition associated with a marked place. A formal description of the approach is as follows.

2.4.2 BPN-based diagnosis

Behavioural Petri Nets

The idea of using PNs to represent a causal model, then verify it, was introduced by Portinale in [40]. It resulted in defining a specific class of PNs, referred to as Behavioural Petri Nets [1], to describe particularly a system's causal behaviour. One of the main features for which such a net model is defined is that finding an alternative to logical formalisms in such a way that the precise semantics of a causal model can be given in terms of Petri net structure and behaviour. For further discussion about BPNs, a full description can be found in [1].

Definition 2.11. A BPN is a 4-tuple $N = (P, T_N, T_{OR}, A)$ such that $(P, T_N \cup T_{OR}, A)$ is an acyclic ordinary Petri net with:

- $\forall p \in P(|^\bullet p| \leq 1 \wedge |p^\bullet \leq 1|)$
- $\forall p_1, p_2 \in P((^\bullet p_1 = {}^\bullet p_2) \wedge (p_1^\bullet = p_2^\bullet) \rightarrow p_1 = p_2)$

- $\forall t \in T_N(|^\bullet t| = 1 \wedge |t^\bullet| > 0) \vee (|^\bullet t| > 0 \wedge |t^\bullet| = 1)$
- $\forall t \in T_{OR}(|^\bullet t| \geq 2 \wedge |t^\bullet| = 1)$

It should be noticed that a BPN model is safe; that is, any place can hold at most one token[2]. A transition can be either an *And-transition* (T_N) or an *Or-transition* (T_{OR}). *And-transitions* are intended in the usual way (as conjunctions of causes); while, *Or-transitions* are intended to represent the logical connective *OR*. Thus, an *Or-transition* has a concession in a marking iff at least one of its input places is marked. The initial marking of a BPN is a safe marking μ_0 by which only source places can be marked.

BW-Analysis

Given a BPN, a particular analysis technique called BW-analysis is defined in [1] as a backward analysis method based on reachability. As said previously, such a method uses two different kinds of tokens, *normal* and *inhibitor*, aimed at modelling the truth or falsity of the condition associated with a marked place. Thus a marking of a place $\mu(p)$ ranged in $\{b, w, 0\}$. If $\mu(p) = b$ then the place p is marked with a normal (black) token, if $\mu(p) = w$ then it is marked with an inhibitor token (white), and if $\mu(p) = 0$ then it is empty, here no constraint is imposed on the condition associated to p (it is *unknown*).

Starting from a marking μ where only sink places are marked $\mu(p) \neq 0 \Rightarrow p^\bullet = \emptyset$, the BW-analysis makes use of a set of backward firing rules, as illustrated in Fig. 2.5, to determine the set of initial markings from which μ could be reached. The application of such a method results in a graph whose root node is the marking μ, the leaves are whether initial markings or inconsistent ones, whereas the arcs are labelled with fired transitions. Notice that some of the rules are indeterministic, by that the graph.

Applying BW-analysis to diagnostic problem solving

In terms of BPNs, system behaviour can be represented as follows. Each state's instance is modelled by a place. Initial-causes instances are represented by source

[2] By ignoring the temporal aspect of the system evolution.

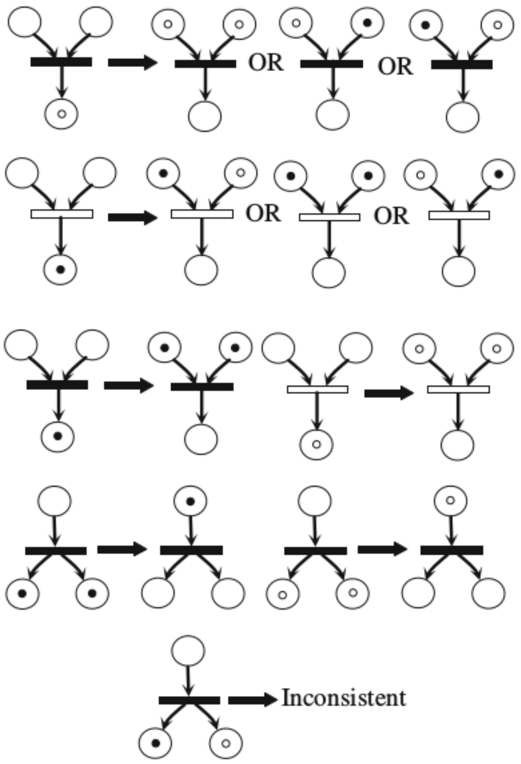


Figure 2.5: Backward firing rules of a BPN.

places, while manifestations instances are represented by sink ones. Concerning the cause-effect relationships among these instances, they are described by means of transitions. In this case, observation over the system can be described by a final marking by which only sink places, corresponding to manifestations, can be marked.

The BPN diagnostic problem $BPNDP$ corresponding to the logical DP is defined as $BPNDP = (N, P^{Init}, \langle P^{+}, P^{-} \rangle)$ where N is the BPN representation of the causal BM, P^{Init} denotes the set of source places corresponding to initial causes of BM, P^{+}, P^{-} are two sets of sink places representing the observations and thus corresponding respectively to Ψ^{+} and Ψ^{-}. The following concepts need to be recalled.

- a marking μ of a BPN is called a final marking if and only if no transition is enabled at μ;

- it is said that μ *covers* a set of places Q if and only if $\forall p \in Q \rightarrow \mu(p) = 1$;
- while μ *zero-covers* the set Q if and only if $\forall p \in Q \rightarrow \mu(p) = 0$

Now the concept of diagnostic solution can be captured by the following theorem whose proof can be found in [41].

Theorem 2.2. *Given a $BPNDP = (N, P^{Init}, \langle P^+, P^- \rangle)$, an initial marking μ^{Init} is a solution to $BPNDP$ if and only if the final marking μ of (N, μ^{Init}) covers P^+ and zero-covers P^-.*

Up to here, what has been presented is a centralized approach for diagnostic problem solving. In fact, the distributed version of the BPN-based approach has been already investigated by Bennoui in [3] where the system model is given by a set of place-bordered BPNs and the global diagnosis can be achieved through communication between agents each time they accomplish a local diagnosis.

2.5 Discussion

Indeed, BPNs offer a clear and precise language for system description, besides capturing all aspects concerning causal models validation. Nevertheless and as we pointed out in the introduction, a Petri net representation, in general, becomes fairly complex when dealing with real-life systems (even with the smallest size of them). The main reason is that we only have one type of token. As an example, in a mechanical domain, let us consider a state representing *an engine temperature*. This one can assume *high*, *medium*, or *low* value at a given time. In the corresponding BPN model, each of these values is represented by a place. Furthermore, for each one there is an execution path as a subnet to deal with. Notice that the mentioned problem comes up with places and also with transitions. On the one hand, a subset of places belongs to the same modelled state. On the other hand, a subset of transitions shares the same *place_domains* (both inputs and outputs) and performs the same action with them. Here, we use the term *place_domain* to denote the set of places corresponding to a state's values.

Usually, such kind of problems can be faced by turning to high-level net classes, and particularly the Coloured Petri Net one, since it represents the structural folding of classical PNs (of course, when the places' colour-sets are finite). Hence, a mapping between a BPN and a CPN can be informally defined as follows.

- We replace a set of places $\{p_1,...,p_n\}$ belonging to the same *place_domain* by a single place p, as long as, we attach to p the colour set $\{c_1,...,c_n\}$ in such a way that each colour c_i refers to a place p_i. Here, a token in the place p represents the fact that the corresponding state to p assumes the value modelled by the colour carried by such token.

- We replace a set of transitions $\{t_1,...,t_m\}$ having the same *place_domains* for both inputs and outputs by a single transition t, which may fire in m different ways each of which corresponds to a transition t_i.

- Again, a marking μ of a CPN is a safe marking, each place can hold at most one token at a time. Obviously, within an initial marking μ_0, only the source places can be marked.

Unfortunately, such criteria are still deficient. They lack a full representation of *Or-transitions*. Recall that an *Or-transition* is enabled in a marking if at least one of its input places is marked. An all set proposal consists of adding new transitions and inhibitor arcs[3] for that, however, we get again involved in the complexity problem, getting more places and transitions.

Taking up the diagnostic problem again where the reasoning task should be accomplished by a backward analysis, which can be seen as a forward one on the inverted net model. Instead of classical PNs where such a process needs only an inversion of the arcs' direction, in terms of CPNs, it can be realized in two steps:

1. Inversion of arcs' direction; and

2. CPN expressions (guards or those associated with arcs) inversion.

In this respect, many attempts have been made such as [11], [20] and not very earlier [5]. The work presented in [5] consists in proposing a backward reachability analysis based on an inverted CPN, which can be obtained by means of structural

[3] An inhibitor arc connects a place p to a transition t in such a way that it disables the transition t when the input place p is marked. Notice that no tokens can move through an inhibitor arc when the transition fires.

transformations on the original net model. Here, let us get to a significant issue concerning the analysis task within CPNs. We have mentioned that a transition may fire in several ways, besides the use of arc expressions to determine the involved token colours when it fires. Although such expressions are linear functions in general, the inversion process may be impossible for some cases and hard for others. Of course, we do not account the trivial cases where functions are of one input argument. Rather, the complexity arises in case of multi-input arguments, the reasoning process needs generally exponential time, besides being not adequate to our aims.

To simplify the analysis task, we propose using matrices as labels for transitions where the different firing ways are determined with. Each line of the matrix corresponds to a way of firing and determines the involved token colours. As well, each column corresponds to a place and shows the meant token colours (whether consumed or produced) by this transition. In fact, this proposal is the key feature of a particular class of CPNs called CBPNs, as a folding of BPNs introduced in [42]. It should be noticed that we do not intend to neglecting the arc expressions, but they will be used as *typed variables* and *selective expressions*.

2.6 Conclusion

This chapter has reviewed the main concepts and notations related to fault diagnosis problem within a model-based reasoning view for centralized and distributed systems, as will be used in this thesis. Also, some definitions concerning Petri nets that would be useful throughout the thesis have been recalled. Then, and since we are inspired by the works presented in [42] and [3], they are both detailed to some extent; whereas a brief survey is considered for the use of PNs in the general context of model-based diagnosis.

The chapter has ended by discussing the major weakness related to PN-based approaches in general that is the complexity problem in terms of net representation when dealing with real systems. As well as, the problem concerning the backward analysis of a CPN model where an inversion of the net expressions (the ones attached to arcs) is recommended.

The following chapter aims at presenting the first contribution of this thesis, in which we make use of the CPN models to tackle the first problem, so the system model becomes more reducible. Besides, using matrices attached to transitions to describe explicitly their firing ways instead of being implicit in arcs expressions. In fact, this gives rise to a particular model based on CPNs named Coloured Behavioural Petri Net.

Part II

Contributions

CHAPTER 3

COLOURED BEHAVIOURAL PETRI NETS

This chapter provides a full description about the structure and dynamics of Coloured Behavioural Petri Nets in order to represent the causal behaviour of the system under study. As well as, an illustrative example is discussed to touch on the very related concepts. The chapter ends by a BPN-CBPN translation procedure together with an application example and a proof of correctness.

3.1 Introduction

Petri net models are well-known useful tools that offer a clear and precise description of the system under study. However, the use of one type of token provokes a salient problem that is the net representation, which becomes fairly complex even for small systems. Coloured Petri Nets have been introduced, as high-level net models, to simplify the PN model structure. Generally, high-level Petri nets have been widely used in both theoretical analysis and practical modelling of various systems. The main reason for the success of this class of net models is that they make it possible to obtain much more succinct and manageable descriptions than can be obtained by means of classical Petri nets. Besides, they still offer a wide range of analysis methods and tools.

3.2 Coloured Behavioural Petri Net models

Coloured Behavioural Petri Nets (CBPNs) denote a particular class of CPNs with the following features. Each place describes a system state, and so its colour set corresponds to the set of such a state admissible values, provided that being marked with one token colour at a time. A token colour in a place means that the state corresponding to such a place assumes the value described by such a colour. A matrix is attached to each transition to define the different ways the transition may fire, and so each row corresponds to a classical PN transition; while each column corresponds to a connected place and shows the involved token colours when it gets fired. Accordingly, a transition input arc is labelled with a typed variable, while with a selective function if it is an output one. Generally, this is all about the static structure of a CBPN, whereas its dynamic behaviour or the token game can be expressed via the following rules:

Enabling of a transition:
A transition is enabled if a combination of its input places markings formalizes a sub-row (by considering only the columns of these places) of its firing ways matrix.

Firing of an enabled transition:
An enabled transition may fire. If a transition fires, it destroys one token colour on each of its input places and creates one token colour on each of its output places according to a certain row of its firing ways matrix.

3.2.1 Structure of CBPNs

Definition 3.1. A Coloured Behavioural Petri Net is a 6-tuple $N = (\Sigma, P, T, A, C, FW)$ where:

- (Σ, P, T, A, C) is a Coloured Petri Net.
- $FW : T \longrightarrow MAT_{n,m}(\Sigma \cup \{\varepsilon\})$.
- A^+ (transitive closure of A) is irreflexive.

Since CBPN models can be considered as the CPN-version of causal models, the set of places can be partitioned into three subsets: Initial causes Ic, Manifestations Mn, and Internal states Is. Thus,

$$P = Ic \uplus Mn \uplus Is$$

such that:

* $Ic = \{p | p \in P, \ ^{\bullet}p = \emptyset\}$,

* $Mn \subseteq \{p | p \in P, \ p^{\bullet} = \emptyset\}$, and

* $Is = P \setminus (Ic \cup Mn)$.

Given a transition $t \in T$ with n firing ways, that means the number of transitions for which t may be unfolded in a classical PN, and m places with which it is connected ($m = |^{\bullet}t| + |t^{\bullet}|$).

Firing ways matrix:
A t's Firing Ways matrix $FW = [c_{ij}]$ is an $n \times m$ matrix of colours $c_{ij} \in \bigcup_{\omega \in \Sigma} \omega$ including the *empty colour* ε. The FW matrix contains a row for each firing way and a column for each connected place. Thus, the c_{ij} consists of the colour removed from (added to) the place j when t fires with respect to the i^{th} firing way.

Empty colour ε:

Since the FW matrix contains only colours, while a place may have an empty marking*the empty set*, which is actually a set, can not be included. Thus, we are imposed on introducing a particular colour ε that we call *empty colour* to stand for *the empty set* inside a matrix (its utility will be shown later).

A transition t, besides being associated with a firing ways matrix, can be ranged as a fork transition if $|t^{\bullet}| > 1$; or a join transition if $|^{\bullet}t| \geqslant 1$. In case t is a fork transition then it is intended to split the meant input token colour (where multiple consequences are present). Here, the colours belonging to the same row must be similar.

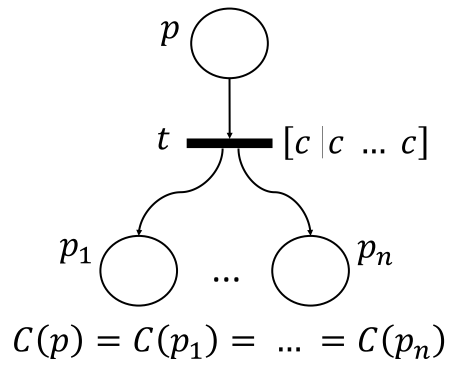


Figure 3.1: Fork transition

While if it is join, we meet three possible cases of use.

- The first is as usual when t is a conjunction of causes. In this case, t becomes enabled if all its input places are marked (empty markings are excluded).

- The second consists of the logical Or where t becomes enabled if at least one of its input places is marked. For the sake of simplicity, we often suppose that t has at most two input places. The use of such kind of transitions allows us to model situations in which a particular instance of a state can be determined by alternative causes while keeping safeness.

- The last one is a particular case of the second, it consists of the exclusive Or, where t becomes enabled if and only if just one of its input places is marked.

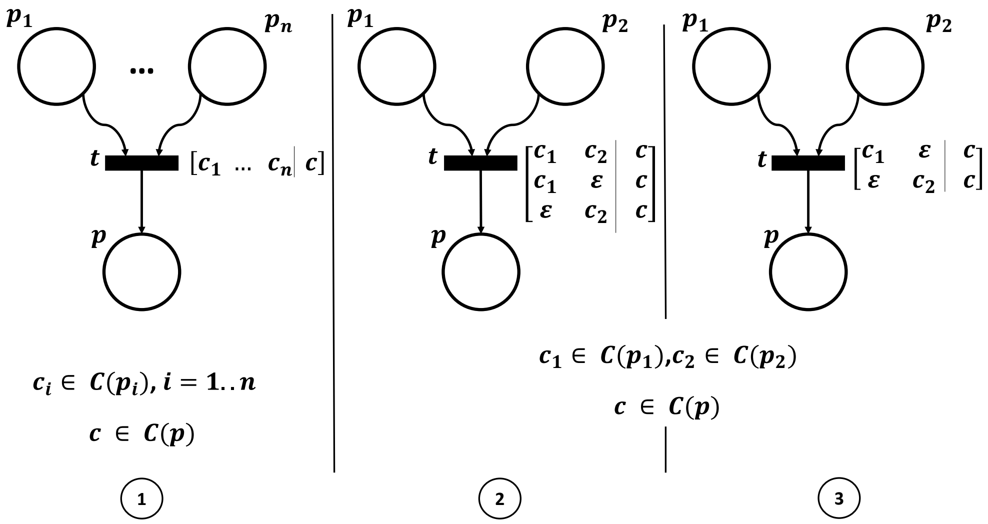

p_1
p_n
t
$[c_1 \dots c_n | c]$
p
$c_i \in C(p_i), i = 1..n$
$c \in C(p)$
1
p_1
p_2
t
$\begin{bmatrix} c_1 & c_2 & c \\ c_1 & \varepsilon & c \\ \varepsilon & c_2 & c \end{bmatrix}$
p
$c_1 \in C(p_1), c_2 \in C(p_2)$
$c \in C(p)$
2
p_1
p_2
t
$\begin{bmatrix} c_1 & \varepsilon & c \\ \varepsilon & c_2 & c \end{bmatrix}$
p
3

Figure 3.2: Possible cases of join transition

Finally, the $FW(t)$ can be decomposed into $FWin_{n\times|{}^\bullet t|}$ and $FWout_{n\times|t^\bullet|}$ as the input and output sub-matrices respectively. Such a decomposition is quite useful in the analysis phase.

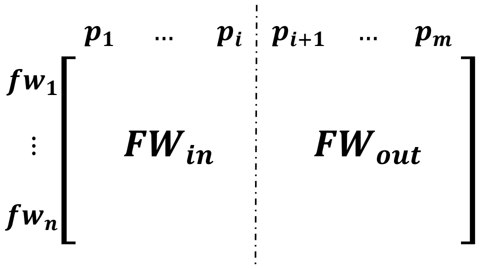


Figure 3.3: FW-matrix decomposition

Note. *The irreflexivity of A^+ is reasonable since we are dealing with the causal behaviour of a system without considering temporal aspects.*

Example 3.1. *In terms of the previous example, Fig. 3.4 depicts the CBPN version of the PN and CPN of Fig. 2.3. Notice that each of the possible ways that a and b* *can be set in (which means the four transitions of the PN, and so the arc expression $x \wedge y$ of the CPN) is represented by a row in the $FW(t)$ matrix.*

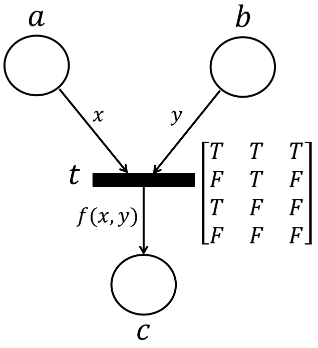

a
b
x
y
t
f(x,y)
c
$\begin{bmatrix} T & T & T \\ F & T & F \\ T & F & F \\ F & F & F \end{bmatrix}$

Figure 3.4: CBPN corresponding to Example. 2.1

CBPN marking:
Recall that a marking μ assigns to each place p a multi-set over p's colour set.

Definition 3.2. An initial marking of a CBPN is a safe marking μ_0 iff:

$$\forall p \in P: \ \mu_0(p) \neq \emptyset \rightarrow p \in Ic$$

Same as CPNs, a marked CBPN is a pair (N,μ) where N is a CBPN and μ is a marking with the following property:

$$\forall p \in P: \ |\mu(p)| \leqslant 1$$

Definition 3.3. A marked CBPN (N,μ) is said to be safe iff:

$$\forall p \in P, \ \forall \mu \in R(N,\mu_0): |\mu(p)| \leqslant 1$$

Definition 3.4. Given a marked CBPN (N,μ), a marking μ', with $\mu' \neq \mu$, is said to be a submarking of μ, we write $\mu \sqsubseteq \mu'$, iff

$$\mu'(p) = c \rightarrow \mu(p) = c, p \in P, c \in C(p)$$

3.2.2 Dynamic Behaviour of a CBPN

Until now we have only defined the static structure of a CBPN. The dynamic behaviour is determined by the transition's enabling and firing rules as given in what follows. It is worth noting that an input arc of a transition t is labelled with a typed variable, whereas the output one consists of a function that simply sets the appropriate token colour in a place $p \in t^\bullet$ using $FW(t)$. For a transition t to be enabled it must be possible to find a binding of the variables that appear in the surrounding arc expressions of t.

Binding:
Let b be a $|^\bullet t|$-vector where the v_p^{th} component, denoted $b(v_p)$, represents the value assigned to an input arc variable $E(p,t)$ that is present in the place p. We denote b as a binding if it corresponds to a row of $FWin(t)$.

When t fires with a given binding, using $FW(t)$, it removes from each input place the token colour to which the corresponding input arc variable is valued. Analogously, it adds to each output place the token colour to which the expression on the output arc evaluated. Indeed, A^+ denotes the transitive closure of the flow relation. Formally, the irreflexivity of A^+ means that a CBPN is acyclic, which help us defining a partial order, referred to as "≺", over transitions of a CBPN as follows:

$$\text{Let } t_1, t_2 \in T : t_1 \prec t_2 \Leftrightarrow t_1 A^+ t_2.$$

Definition 3.5. A transition $t \in T$ is *enabled* at a marking μ, denoted $\mu[t>$, iff:

$$E(p,t) < b > \leqslant \mu(p) \text{ and } \nexists t' \in T : t' \prec t \text{ s.t } \mu[t'>, \forall p \in {}^\bullet t$$

Definition 3.6. An enabled transition $t \in T$ may fire at a marking μ, with respect to a certain firing way, yielding a new marking μ', denoted $\mu[t > \mu'$, with:

$$\mu'(p) = \mu(p) - E(p,t) < b > + E(t,p) < b >$$

Definition 3.7. Two transitions are said to be *concurrent* iff each time they are both enabled, the firing of one does not disable the other, formally:

$$\exists \mu \in R(N, \mu_0) : \mu[t_1 > \text{ and } \mu[t_2 > \text{ and } t_1 \not\prec t_2 \text{ and } t_2 \not\prec t_1$$

Definition 3.8. A marked CBPN is *deterministic* iff:
$\forall \mu \in R(N,\mu_0), \forall t_1, t_2 \in T$

if $\mu[t_1 >$ and $\mu[t_2 >$ then t_1 and t_2 are *concurrent*.

Hence, given a marked CBPN (N,μ), we denote by a *step* the set of enabled and concurrent transitions in μ.

Definition 3.9. A step $s = \{t_1,...,t_n\}$ may fire in μ yielding a new marking μ' such that:

$$\mu' = \sum_{i=1}^{n} \mu_i, \mu[t_i > \mu_i$$

We call a final marking μ_f the marking where no transition is enabled.

3.3 Example

In order to touch on the main concepts of a CBPN model and make things clear, let us consider as an example the net depicted in Fig. 3.5.
Formally, it is given by $N = (\Sigma, P, T, A, C, FW)$ where:

- $\Sigma = \{a,b,d,n,h,l,r\}$
- $P = \{p_1,\cdots,p_{10},A,B,C,D\}$ with
  $Ic = \{p_1,\ldots,p_3\}$ and $Mn = \{p_7,\ldots,p_9\}$
- $T = \{t_1,\cdots,t_8\}$
- The colour sets attached to places are as follows:
  $C(p_1) = C(p_3) = C(p_8) = \{h,l\}$;
  $C(p_2) = C(p_9) = \{a,b\}$;
  $C(p_4) = C(p_6) = C(p_7) = \{n,d\}$; and
  $C(p_5) = \{r\}$.

Each transition has its FW-matrix that shows the different firing ways t respects. It is to be noted that one can determine the type (fork, join) of each transition by only inspecting the associated matrix. As samples, t_2 and t_3 are fork transitions, they are used to split certain input colours. By the way, t_2 and t_3 are dummy transitions, and hence, the places A,B,C and D are dummy too. Thus, the colour sets associated with these places according to the meant colours are the following, $C(A) = C(B) = C(p_2)$ and $C(C) = C(D) = \{n\}$.

On other hand t_5,t_7 and t_8 are all join transitions. One should notice the difference between these transitions. The transition t_7 consists of a conjunction of causes. While transition t_5 resembles the logical connective OR, its enabling requires the marking of at least one of its input places A or D; and we exclude the possibility of enabling the transition t_8 when both places p_5 and p_6 are marked, p_5 and p_6 are mutually exclusive.

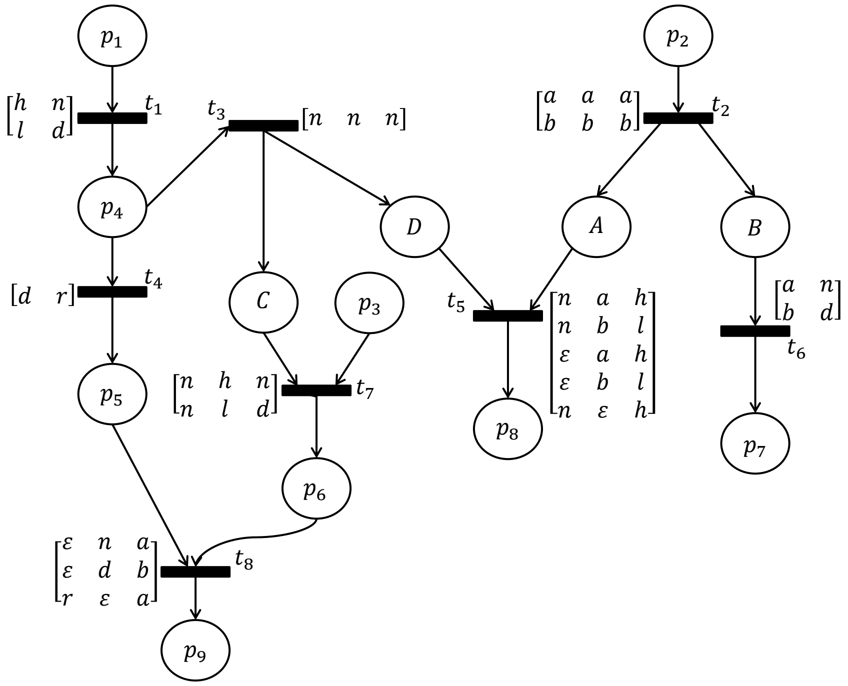

p_1
p_2
$\begin{bmatrix} h & n \\ l & d \end{bmatrix}$
t_1
t_3
$[n \quad n \quad n]$
$\begin{bmatrix} a & a & a \\ b & b & b \end{bmatrix}$
t_2
p_4
D
A
B
$[d \quad r]$
t_4
C
p_3
t_5
$\begin{bmatrix} n & a & h \\ n & b & l \\ \varepsilon & a & h \\ \varepsilon & b & l \\ n & \varepsilon & h \end{bmatrix}$
$\begin{bmatrix} a & n \\ b & d \end{bmatrix}$
t_6
p_5
$\begin{bmatrix} n & h & n \\ n & l & d \end{bmatrix}$
t_7
p_8
p_7
p_6
$\begin{bmatrix} \varepsilon & n & a \\ \varepsilon & d & b \\ r & \varepsilon & a \end{bmatrix}$
t_8
p_9

Figure 3.5: A CBPN example.

Now comes the net behaviour simulation. Consider an initial marking $\mu_0 = p_1(l) + p_2(a)$, the notation $p(c)$ means that the place p is marked with colour c. A step $s = \{t_1, t_2\}$ is enabled at μ_0. The firing of s with respect to second and first rows of $FW(t_1)$ and $FW(t_2)$ respectively leads to a new marking $\mu_1 = p_4(d) + A(a) + B(a)$. Fig. 3.6 shows the reachability graph corresponding to μ_0. Note that t_5 is enabled at μ_1 even though only place A is marked, t_5 is fired with respect to the third row of $FW(t_5)$ getting colour a from A and setting colour h in p_8. The same as t_8 when p_5 becomes marked. Finally, μ_3 is a final marking, where only places of Mn are marked.

$$\begin{tikzcd}
\mu_0 = p_1(l) + p_2(a) \arrow[d, "t_1, t_2"] \\
\mu_1 = p_4(d) + A(a) + B(a) \arrow[d, "t_4, t_5, t_6"] \\
\mu_2 = p_5(r) + p_8(h) + p_7(n) \arrow[d, "t_8"] \\
\mu_3 = p_7(n) + p_8(h) + p_9(a)
\end{tikzcd}$$

Figure 3.6: Reachability graph of CBPN of Fig. 3.5.

3.4 BPN-CBPN Translation

Since CBPNs represent the coloured version of BPNs, we propose in this section a simple procedure for translating a BPN $N' = (P', T'_N, T'_{OR}, F')$ into a CBPN model. As well as, we provide a proof of correctness of our algorithm.

3.4.1 Translation procedure

In such a procedure, we make use of the following definitions. Both functions d_p (for *place_domain*) where

$$d_p : P' \rightarrow P$$

and d_t (for *transition_domain*) where

$$d_t : (T'_N \cup T'_{OR}) \rightarrow T$$

are used to indicate the folding of a given node $x \in (P' \cup T'_N \cup T'_{OR})$. Whereas, the functions

$$In, Out : (T'_N \cup T'_{OR}) \to 2^P$$

have, to some extent, the same interpretations as $^\bullet t$ and $t^\bullet$ respectively. They consist of external relations (as most of the used functions are) defined between the transitions of the BPN model and the places of the resulting CBPN (they can be seen as a *place_domain* but this time for transitions).
In its turn, the function

$$clr : P' \to \Sigma$$

helps in defining the colour $c \in \Sigma$ corresponding to the place $p \in P'$. Finally, an update to the transition matrix can be realized over time by adding new firing ways corresponding to BPN transitions, in other words row-vectors of colours, through the *update* function.

Now, a BPN-CBPN mapping can be defined informally by the following rules.

Rule 1:
For each set of places $\{p_1, \ldots, p_n\} \subset P'$, we associate a place $p \in P$ such that

$$d_p(p_1) = \ldots = d_p(p_n) = p$$

as long as, we attach to p the colour set $\{c_1, \ldots, c_n\}$,

$$C(p) = \{c_1, \ldots, c_n\} \subseteq \Sigma : clr(p_i) = c_i, \forall i = 1..n$$

Rule 2:
For each set of transitions $\{t_1, \ldots, t_m\} \subset T'_N \cup T'_{OR}$, we associate a transition $t \in T$ such that

$$d_t(t_1) = \ldots = d_t(t_m) = t$$

Then, we build up the $FW(t)$ matrix. Each transition $t_i, (i = 1..m)$ corresponds to one of t's firing ways if $t_i \in T'_N$; while, in the simplest case, it is represented by at least three possible firing ways if it belongs to T'_{OR}.

Rule 3:
By folding places and transitions, the connections among them must take place, we mean by that the arcs of the net model. Let

$$t' \in \{t_1, \ldots, t_m\} \subset (T'_N \cup T'_{OR}) : d_t(t_i) = t, \forall i = 1..m, t \in T$$

- For each $p \in In(t')$ we add an arc (p,t) labelled with the expression v_p (here, v_p denotes a typed variable having the same type as p's colour set).
- For each $p \in Out(t')$ we add an arc (t,p) whose expression is

  $$f(v_{p_1}, \ldots, v_{p_n}, p)$$

  where $p_i \in In(t'), \forall i = 1..n$.

A formalization of such rules is given by Algorithm 1.

Algorithm description:

The proposed procedure performs the translation of a BPN model in, mainly, two steps:

- the first step (loop from line 2 to line 6) is all about places and colours, while
- the second one (loop from line 7 to line 28) is in charge of defining transitions and building connections between net components.

Each set of BPN places belonging to the same *place_domain* will be replaced by a single CBPN place, whereas each of these places becomes one of its colours. Analogously, gathering the BPN transitions sharing the same In and Out sets as a single CBPN transition, then constructing its matrix where each of these transitions presents one of its possible firing ways. By folding places and transitions, the arcs connecting them are labelled with expressions as a typed variable for a transition's input arc and a selective function for its output one.

Example 3.2. *As an example of a BPN model, let us consider the net showed in Fig 3.7 (table 5.3 shows the key for the used acronyms). The model is adapted from an example given in [42], which is used to represent a model in the domain of car*

Algorithm 1 Translation procedure

```
Require: BPN $N' = (P', T'_N, T'_{OR}, F')$
Ensure: CBPN $N = (\Sigma, P, T, A, C, FW)$

$\Sigma \leftarrow P \leftarrow T \leftarrow \emptyset$
for $\{p_1,\dots,p_n\} \subset P'$ such that $d_p(p_1) = \dots = d_p(p_n) = p$ do
    $P \leftarrow P \cup \{p\}$
    $C(p) \leftarrow \{clr(p_1),\dots,clr(p_n)\}$
    $\Sigma \leftarrow \Sigma \cup C(p)$
end for
for $\{t_1,\dots,t_m\} \subset (T'_N \cup T'_{OR})$ such that $d_t(t_i) = \dots = d_t(t_m) = t$ do
    $T \leftarrow T \cup \{t\}$
    for $t' \in \{t_1,\dots,t_m\}$ do
        if $t' \in T_N$ then
            ⊳ Let $^\bullet t' = \{p_1,\dots,p_n\}$, $t'^\bullet = \{p'_1,\dots,p'_k\}$
            $update(FW(t), [clr(p_1)\dots clr(p_n)\ clr(p'_1)\dots clr(p'_k)])$
        else
            ⊳ Let $^\bullet t' = \{p_1, p_2\}$, $t'^\bullet = \{p'\}$
            $update(FW(t), [clr(p_1)\ clr(p_2)\ clr(p')])$
            $update(FW(t), [clr(p_1)\ \varepsilon\ clr(p')])$
            $update(FW(t), [\varepsilon\ clr(p_2)\ clr(p')])$
        end if
        for $p_i \in In(t_1)$ do
            $A \leftarrow A \cup \{(p_i, t)\}$
            $E((p_i, t)) \leftarrow v_{p_i}$
        end for
        for $p_i \in Out(t_1)$ do
            $A \leftarrow A \cup \{(t, p_i)\}$
            $E((t, p_i)) \leftarrow f(v_{p_1},\dots,v_{p_n}, p_i)$
        end for
    end for
end for
```

engine faults. It looks too simple, but it is sufficient as an example to show the usefulness of the translation procedure.

The model consists of three behaving modes of a specific system part (with an outcome of 21 places and 11 transitions); where, for the sake of simplicity and clarity, each of these modes is given by a BPN. For instance, transition t_l models the fact that a high_oil_consumption *(modeled by place $oc(h)$) can be caused*

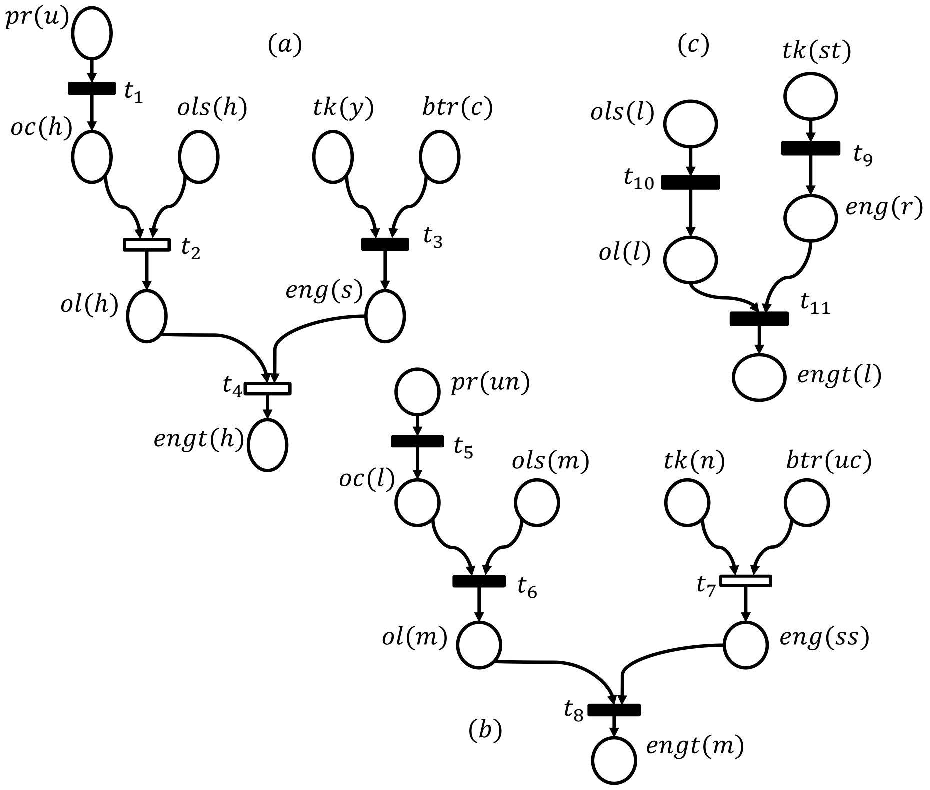


Figure 3.7: BPN examples representing a system's different behaving modes.

Entity	Acronym	Admissible-values
Battery	btr	Charged (c), uncharged (uc)
Engine	eng	Started (s), suspend (ss), rusted (r)
Oil-lack	ol	High (h), medium (m), low (l)
Oil-loss	ols	High (h), medium (m), low (l)
Turned-key	tk	Yes (y), no (n), stuck (st)
Piston-rings	pr	Used (u), unused (un)
Oil-consumption	oc	High (h), medium (m), low (l)
Engine-temperature	engt	High (h), medium (m), low (l)

Table 3.1: Acronyms used in Fig. 3.7

by using_piston_rings *(modeled by place* $pr(u)$*). The transition* t_2[1] *models the*

[1] Graphically, an OR-transition is represented by an empty thick bar

fact that a high_engine_temperature *(modeled by place $engt(h)$) can be caused by either a* high_oil_lack *(modeled by place $ol(h)$); or when the* engine_started *(modeled by place $eng(s)$).*

One should notice that the first two BPNs ((a) and (b)) describe almost the same processes, while the last one is a little bit different. In fact, such processes are chosen carefully to show how a variety of processes sharing at least the same system components can be all represented in, to some extent, a succinct way. Fig 3.8 presents the CBPN corresponding to the BPN depicted in Fig 3.7 by applying the above procedure. The net consists of 8 places and 6 transitions (much less than first BPNs).

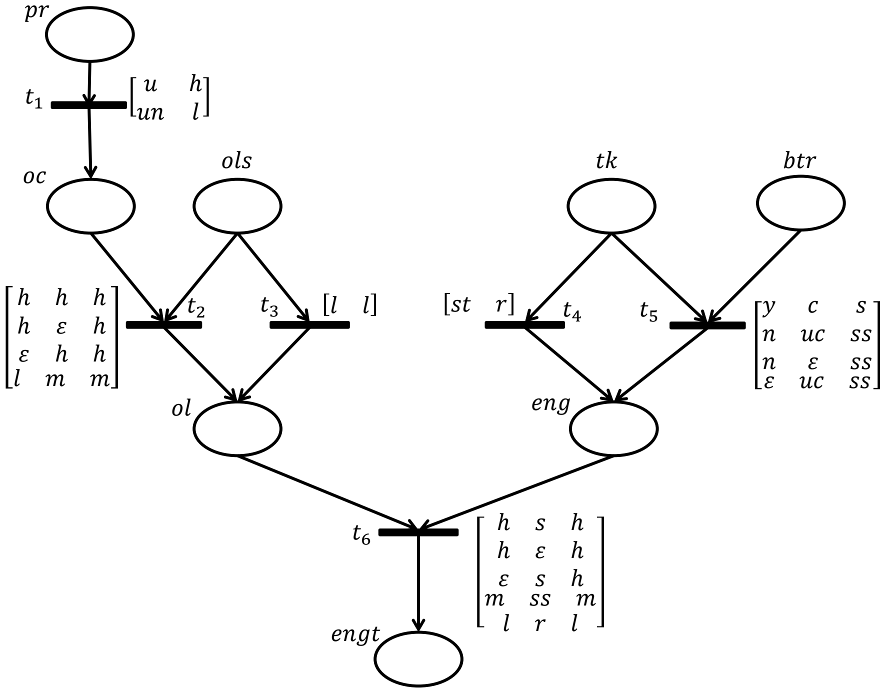

pr
t1
[u h; un l]
oc
ols
tk
btr
[h h h; h ε h; ε h h; l m m]
t2
t3
[l l]
[st r]
t4
t5
[y c s; n uc ss; n ε ss; ε uc ss]
ol
eng
t6
[h s h; h ε h; ε s h; m ss m; l r l]
engt

Figure 3.8: The CBPN corresponding to the BPNs of Fig. 3.7.

Places are folded and transitions too, for example, place pr is the place_domain of both places $pr(u)$ and $pr(un)$

$$pr = d_p(pr(u)) = d_p(pr(un)) \rightarrow C(pr) = \{u, un\}$$

Transition t_6 represents the folding of BPN transitions t_4, t_8 and t_{11}

$$t_6 = d_t(t_4) = d_t(t_8) = d_t(t_{11})$$

Notice that t_4 is an OR-transition, it fills up three rows of the FW matrix of the CBPN transition t_6 as it is interpreted into, the last two rows of $FW(t_6)$ correspond to t_8 and t_{11} respectively.

It is worth noting that because of the coloured Petri nets nature, the net size is more reduced and the model system becomes too simple. In fact, in most cases a system's behaving modes are described similarly, one can imagine the size that can be gained when using CPNs. Even in the worst cases, the places would be folded which serves a lot.

3.4.2 Proof of correctness

Given a CBPN $N = (\Sigma, P, T, A, C, FW)$ and a BPN $N' = (P', T'_N, T'_{OR}, F')$. It is worth noticing, here, that in order for N to be the corresponding CBPN of N', the features characterizing a BPN model have to be kept unchanged in the CBPN N. Thereby, we give in the following the formalization of all those features in terms of CBPNs to be checked in the net model N. Starting with the structural properties.

* Each BPN place can be connected at most to one input and one output transitions, then $\forall p \in P', \forall t \in {}^\bullet d_p(p) \cup d_p(p)^\bullet$,

$$\exists!(i,j) \in \mathbb{N}^2 : \; FW(t)_{ij} = clr(p)$$

The $\exists!$ symbol denotes the uniqueness quantification. $FW(t)_{ij}$ refers to the entry of the i^{th} row and the j^{th} column of the matrix $FW(t)$.

* Structurally, an Or-transition looks as a particular And-transition ($|{}^\bullet t| \geq 2 \wedge |t^\bullet| = 1$). Whereas its semantic is different, it can be interpreted into, at least, three possible firing ways (by making use of the inhibitor arcs). When translating a BPN into a CBPN model, each of these ways is described by a FW-row. Thus, in a CBPN model, the firing ways of a transition that correspond to an Or-transition are treated as one way. Moreover,

$$\forall t' \in T_N \cup T_{OR}, \exists t \in T : \; d_t(t') = t$$

Let $\forall n,m,l \in \mathbb{N}$: $FW_{in}(t)_{n,m}$ and $FW_{out}(t)_{n,l}$ be the input and output submatrices of t respectively. Then,

$$t' \in T_N \rightarrow (m = 1 \wedge l > 0) \vee (m > 0 \wedge l = 1)$$

while $m \geq 2$ and $l = 1$ for the case of $t' \in T_{OR}$.

By keeping such properties, the resulted net is acyclic and deterministic (as consequences of net structure).

Up to here, just the structural properties of a BPN are shown preserved in the corresponding CBPN. The step that follows consists of determining a correspondence between the BPN and CBPN behaviours.

Definition 3.10. Given a marked BPN (N', μ') and a corresponding marked CBPN (N, μ),

$$\mu \mathrel{\widehat{=}} \mu' \Leftrightarrow \forall p \in P' : \mu'(p) = 1 \rightarrow \mu(d_p(p)) = clr(p)$$

where $\widehat{=}$ is the correspondence symbol.

The correcteness of such a procedure can now be captured by the following proposition:

Proposition 3.1. *Given a marked BPN (N', μ'_0) and its corresponding CBPN (N, μ_0) where $\mu_0 \widehat{=} \mu'_0$, let $\mu' \in R(N', \mu'_0)$ and $\mu \in R(N, \mu_0)$ such that $\mu \widehat{=} \mu'$,*

$$\forall p \in P' : \ (N', \mu'_0) \vdash \mu'(p) \rightarrow (N, \mu_0) \vdash \mu(dp(p))$$

Proof. We proceed to prove this proposition by contradiction.

$\forall p \in P' : \ (N', \mu'_0) \vdash \mu'(p) \rightarrow (N, \mu_0) \vdash \mu(dp(p))$

$\forall p \in P'$, supposing that $(N', \mu'_0) \vdash \mu'(p)$, while $(N, \mu_0) \vdash \mu(dp(p))$ does not hold. Then,

$\exists p \in P' : \ (N', \mu'_0) \vdash \mu'(p) \wedge (N, \mu_0) \nvdash \mu(dp(p))$

$\exists p \in P' : \mu'(p) \neq 0 \wedge \mu(d_p(p)) \neq clr(p)$

$\neg \ [\forall p \in P' : \ \mu'(p) = 0 \ \vee \mu(d_p(p)) = clr(p)]$

$\neg \ [\forall p \in P' : \ \mu'(p) \neq 0 \rightarrow \mu(d_p(p)) = clr(p)]$

As a result, $\neg(\mu \widehat{=} \mu')$, which is a contradiction. ■

3.5 Conclusion

What has been presented in this chapter is a particular class of CPNs called Coloured Behavioural Petri Nets aimed at modelling the causal behaviour of the system under study. In fact, the main issue about them is attaching a matrix to each transition in order to determine explicitly its possible firing ways. In fact, CBPNs are introduced mainly for diagnostic reasoning, however they can not be restricted just for that purpose. They can provide a very useful and helpful tool when dealing with problems that require a backward analysis on reachability of CPNs for reasoning. Particularly for this, the use of matrices plays a major role. Instead of inverting the surrounding expressions when a transition fires backwardly, the process needs a simple manipulation of its matrix where the input block becomes output and vice-versa.

We will show in the next chapter how the diagnostic problem can be formalized in terms of reachability in CBPNs and can be implemented by exploiting the CW-analysis technique as a backward analysis on reachability graph performed in terms of transitions' matrices.

CHAPTER 4

CW-ANALYSIS FOR DIAGNOSTIC PROBLEM SOLVING

This chapter presents a CBPN-based approach for system diagnosis, where a model describes the whole system. First we define a specific backward analysis technique based on reachability of CBPNs, by which we show the usefulness of FW-matrices. We refer to this technique as the CW-analysis technique. Secondly it is shown how the diagnostic problem can be formalized in terms of reachability in CBPNs, and how the CW-analysis technique can be exploited to implement the diagnostic reasoning scheme.

4.1 Introduction

With the fact that various practical tasks in the field of AI, such as diagnostic problem solving, require a backward reasoning [45], the suitability of backward reachability analysis is very clear when the problem to deal with is given in terms of PNs ([1], [10], [30], [50]). Generally, it corresponds to a forward analysis of the reverse net model. For classical PNs, such net can be obtained from the original one by reversing the direction of the arcs. It needs also an inversion of their expressions for the case of CPNs. Whereas it can be done just by changing the blocks of the transitions' matrices, besides the arcs reversing, in case CBPNs are used.

4.2 CW-analysis

In this section, we define a particular analysis technique for CBPNs that we call CW-analysis. With no need to a net inversion, the CW-analysis consists of a backward reachability analysis performed by simple manipulation of the FW-matrices with the use of an *inhibited colour*.

The reason behind using *inhibited colours* is the following. Generally, the backward reachability analysis can lead to a wide range of markings, some of them are unreachable in the original net, whereas others have no sense with the case under study. From each of the obtained markings, a forward analysis needs to be accomplished to check whether this marking is exactly the required one or not. In order to perform such a process in a single phase, we introduce the concept of *inhibited colour*. We seek by that blocking the production of certain colours along the analysis process.

We should mention that we inspire the use of *inhibited colours* from the BW-analysis method proposed in [42] to denote the falsity of the associated condition represented by a given place in a BPN model.

4.2.1 Formal definition

We stand by an *inhibited colour*, which we refer to as c^w for $c \in \Sigma$, for a condition that is certainly unsatisfied in the case under examination. Thus, an additional marking's description can be used. Let $p \in P$ with $C(p) = \{c_i, c_j\}$ and $\mu(p) = c_i$, the marking of p can be given by $\mu(p) = c_j^w$. A remark is worthwhile on such descriptions. Notice that the first one indicates exactly the actual marking of p (by means of normal colours). Whereas by using inhibited colours, a spectrum of possible p's markings holds,

$$\mu(p) = c_j^w \rightarrow \mu(p) = c_i \text{ or } \mu(p) = \emptyset$$

In other words, we focus on a particular absent colour, therefore we don't care whatever the accurate p's marking is.

Now, let us stand by the subscript ($\_^B$) to the *backward analysis* process. Given a transition t, recall that the $FW(t)$ matrix can be decomposed into $FW_{in}(t)$ and $FW_{out}(t)$ sub-matrices. Thus, $FW^B(t)$ corresponds to $FW(t)$ when

$$FW_{in}^B(t) = FW_{out}(t) \text{ and } FW_{out}^B(t) = FW_{in}(t)$$

For an arc expression, $E^B(x, y)$ is a typed variable, v_y, if $E(x, y)$ is a selective function and vice versa, with $x, y \in P \cup T$.

By making use of the FW^B matrix and the E^B expressions, a transition t is backwardly enabled according to the following definition.

Definition 4.1. Given a marked CBPN (N_i, μ), a transition $t \in T_i$ is backwardly enabled at μ, (denoted $\mu[t >^B$), iff:

$$\forall p \in \ t^\bullet : E^B(t, p) < b > \leqslant \mu(p) \ \wedge \ \nexists t' \succ t : \mu[t' >^B$$

It should be clear that b refers to a binding defined over $FW^B(t)$, whereas " $\succ$ " denotes the inverse relationship of the partial order " $\prec$ " defined previously. The back-firing of t at the marking μ returns the net progress a step backwards, yielding a new marking μ' given by:

$$\mu'(p) = \mu(p) - E^B(t, p) < b > + E^B(p, t) < b >$$

Notice that the backward firing rule has no concern with the kind of colours whether they are normal or inhibited. However, when a transition fires, it produces the same kind of colours as it consumes.

Definition 4.2. Let (N_i, μ) be a marked CBPN, μ is said to be inconsistent iff:

$$\exists t \in T,\ \exists p, p' \in t^\bullet : \mu(p) \neq \mu(p')$$

Inconsistency is a relevant concept to backward reachability analysis that comes up when some places in output of a fork transition are marked with different colours, and particularly the situation of a place with distinguishable markings. Notice that inconsistent markings within inhibited colours are implicitly involved in Def. 4.2. Let $t \in T$ with $t^\bullet = \{p, p'\}$ and $\mu(p) = c_i$, the consistency of μ depends on the marking of p'. For the case where $\mu(p') = c_i^w$, μ is obviously inconsistent $\mu(p) \neq \mu(p')$, there is no normal colour in common

$$\mu(p') = c_i^w \rightarrow \mu(p') = c_j \text{ or } \mu(p') = \emptyset$$

while $\mu(p) = c_i$. Whereas, if

$$\mu(p') = c_j^w \rightarrow \mu(p') = c_i \text{ or } \mu(p') = \emptyset$$

then there is a normal colour c_i in common between $\mu(p)$ and $\mu(p')$, here μ is said to be consistent.

Forced transition:

In case some places are marked alike while others are empty, we go into another concept termed *forced transition*, which is already introduced in [42] for BPNs. Here, we suppose that all the unmarked places, the necessary ones for the back-firing of the meant transition, are marked with the same colour as the marked ones.

Definition 4.3. Given a marked CBPN (N_i, μ) and a fork transition t such that ${}^\bullet t = \{p\}$ and $t^\bullet = \{p_1, ..., p_m\}$, we say that t is forced at the marking μ iff:

- t is not backwardly enabled at μ.

- $\exists p_i(1 \leq i \leq m) | \mu(p_i) \neq \emptyset$.
- μ is not inconsistent.
- $\nexists t' \succ t$ where t' is backwardly enabled or forced at μ.

When the transition t becomes forced at a marking μ, then $\forall p, p' \in t^\bullet$ where $\mu(p) = \emptyset$ and $\mu(p') \neq \emptyset$, we consider $\mu(p) = \mu(p')$.

Within inhibited colours, a transition becomes forced at a marking μ if there exists at least one normal colour in common between the marked places. Then, the empty places are supposed to be marked with that colour. For various colours in common, a path in the reachability graph is built for each one.

Example 4.1. *Back to example 3.3. Let us consider the marking $\mu = p_8(h) + p_9(b^w)$. A possible reason behind using the inhibited colour b^w is that considering it as an undesirable state, and so it is aimed to check the initial situations (the initial markings from which colour b can be reached) in order to avoid it. As it could be that, such a colour is not present in the net model (to get this case we recommend deleting the second row of $FW(t_8)$, by which colour b can be produced in place p_9).*

By the way, one should differentiate between an admissible value and a modelled one. A place can carry a token with a specific value that is not even present in the corresponding CBPN, there is no marking neither a transitions sequence that can produce such a value.

By means of the CW-analysis, we can get all the possible markings by exploring all the possible alternatives. In case we face an inconsistent marking, the explored path is not correct, the examination must be stopped here. Continuing this process, it is easy to draw the graph shown in Figure 4.1. The root node is the marking μ, the arcs are labelled with steps, as a set of transitions that are backwardly fired; the negation symbol is used for transitions that are fired with inhibited colours and framed transitions represent forced ones.

As a step s denotes, in this case, the set of concurrent backwardly enabled transitions at a given marking, its back-firing way S_F is determined by each of these transitions' back-firing ways. Thus, for $s = \{t_1, \ldots, t_n\}$

$$S_F = \{(t_1, i), \ldots, (t_n, j)\}$$

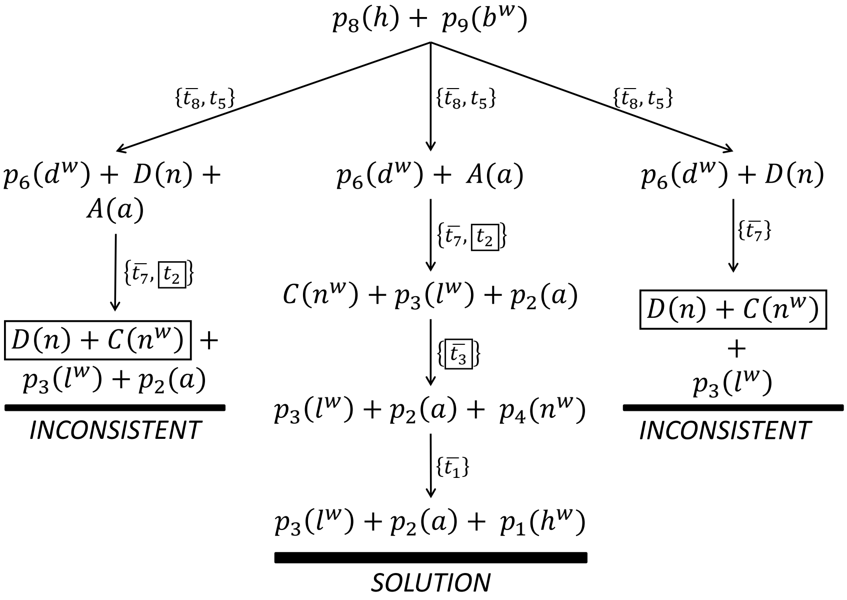


Figure 4.1: The CW-analysis graph of Example 3.3

where each transition is associated with its i^{th} firing way according to which it is backwardly enabled. In the case of multiple back-firing ways for some transitions (when a transition has multiple firing ways with the same output), the set of back-firing ways of s that is S_F can be obtained by combining them. Given a step s and a marking μ such that $\mu[s\rangle^B$. Algorithm 2 shows the main steps to follow to define recursively the set S_F corresponding to s.

4.2.2 Analysis algorithm

We can now provide an algorithm for the computation of initial markings set μ^{Ini}. Algorithm 3 encodes the main steps of the CW-analysis technique as discussed above. The process starts by checking the consistency of the given marking μ (line 1). If so, it looks for an enabled step at μ (line 4); otherwise, it discards that marking, and stops developing that branch of the graph (line 2).

Back to line 4, the function **BEnabledStep** (μ) returns the set of concurrent backwardly enabled transitions at μ. It could be empty, and so the marking μ is considered initial (line 6). On the other hand (line 8), the process makes a call for

Algorithm 2 BFiringWays

Require: A step s, a marking μ

Ensure: The set of back-firing ways of s

```
if $s = \emptyset$ then
    return $\{\emptyset\}$
else
    ▷ Choose $t \in s$
    $S_F \leftarrow$ BFiringWays $(s - \{t\}, \mu)$
    $T_F \leftarrow$ BFways $(t, \mu)$ // Back-firing ways of $t$ at $\mu$
    $S_{Fnew} \leftarrow \emptyset$
    for $t_f \in T_F$ do
        for $s_f \in S_F$ do
            $S_{Fnew} \leftarrow S_{Fnew} \cup \{\{t_f\} \cup s_f\}$
        end for
    end for
    return $S_{Fnew}$
end if
```

Algorithm 3 InitialMarkingsComputing

Require: A marking μ, the set μ^{Ini} (initially empty)

Ensure: The set μ^{Ini} of initial markings

```
if $\exists t \in T : |t^\bullet| > 1, \exists p, p' \in t^\bullet : \mu(p) \neq \mu(p')$ st $\mu(p) \neq \emptyset$ and $\mu(p') \neq \emptyset$ then
    $\mu$ is inconsistent
else
    $s \leftarrow$ BEnabledStep $(\mu)$
    if $s = \emptyset$ then
        $\mu^{Ini} \leftarrow \mu^{Ini} \cup \{\mu\}$
    else
        ▷ Let $s = \{t_1, \ldots, t_n\}$, $n \geq 1$
        $S_F \leftarrow$ BFiringWays $(s, \mu)$
        for $s_f \in S_F$ do
            ▷ Let $s_f = \{(t_1, i), \ldots, (t_n, j)\}$
            $\mu' \leftarrow$ BFire $(s_f, \mu)$
            InitialMarkingsComputing$(\mu', \mu^{Ini})$
        end for
    end if
end if
```

the **BFiringWays** (defined previously), given the found step (s) and the marking μ, to determine the set of back-firing ways of s (line 9). For each of these back-firing ways results a new marking μ' through the back-firing function **BFire** (line 12). For each obtained marking the process starts anew until no step is enabled. At the end of the computing process, the possible initial markings corresponding to μ are ranged in μ^{Ini}.

4.3 Formalizing Diagnosis with CBPNs

In this part of the thesis, we show how the definition of diagnostic problem introduced previously can be formalized in terms of CBPN models. CBPNs are introduced mainly to represent the causal behaviour of the system to be diagnosed. The system's states (that could be in when processing) are described in terms of places that are classified into initial-causes, internal states and manifestations (same classification as for causal models states). The transitions represent the different relationships, causal dependencies, between the system states. The main feature concerning CBPNs is the use of matrices to describe such dependencies, as a way to deal with the problem of complexity when analysing the net model backwardly. Hence, instead of inverting the net expressions and particularly those associated with arcs, the analysis process can be performed on the basis of such matrices just by simple manipulation of their columns.

Indeed, a diagnostic problem is pointed out when it appears a discrepancy between the intended behaviour, derived from the system model or given implicitly in the case of faulty models, and the real one as an observation OBS obtained from the system itself. In terms of CBPNs, OBS corresponds to a final marking μ^{OBS} where only manifestation places could be marked

$$\forall p \in P : \mu^{OBS}(p) \neq \emptyset \rightarrow p \in Mn$$

A CBPN diagnostic problem $CBPNDP$ corresponding to the logical DP is then given by the following definition.

Definition 4.4. A CBPN diagnostic problem is defined as

$$CBPNDP = (N, M^{init}, \langle M^{+}, M^{-} \rangle)$$

where:

- $M^{init} = \{(p,c)|p \in Ic, c \in C(p)\}$
- $M^{+} = \{(p,c)|p \in Mn, c \in C(p), \mu^{OBS}(p) = c\}$
- $M^{-} = \{(p,c)|p \in Mn, c \in C(p), \mu^{OBS}(p) \neq c\}$

N is the CBPN, corresponding to BM, describing the causal behaviour of the system to be diagnosed. M^{init} is a set of couples (p,c) in terms of which diagnoses would be given, it could be seen as the set of possible markings of initial-cause places. $\langle M^{+}, M^{-}\rangle$ represents the obtained observation; M^{+} and M^{-} are two sets of couples (p,c) corresponding respectively to Ψ^{+} and Ψ^{-}.

In principle, a solution to such a problem consists of a marking from which the observation marking can be reached. Since we are dealing with the diagnostic problem such marking has to be initial (often, only initial-cause places can be marked). In order to show how to characterize diagnostic solutions for such a $CBPNDP$, the following definitions are required.

Definition 4.5. Given a marked CBPN (N,μ) and a couple $(p,c), p \in P, c \in C(p)$:

$$(N,\mu) \vdash (p,c) \leftrightarrow \exists \mu' \in R(N,\mu) : \mu'(p) = c$$

where $\vdash$ is the derivation symbol.

Definition 4.6. Given a marked CBPN (N,μ) and a couple $(p,c), p \in P, c \in C(p)$:

$$(N,\mu) \nvdash (p,c) \leftrightarrow \forall \mu' \in R(N,\mu) : \mu'(p) \neq c$$

Both definitions describe the cases of deriving and non-deriving a particular marked place from a specified marked CBPN respectively. A generalization of such definitions for a set of marked places can be given by the following definition.

Definition 4.7. Given a marked CBPN (N,μ) and a set of couples, denoting particular marked places, $Q = \{(p,c)|p \in P, c \in C(p)\}$. Thus,

$$(N,\mu) \vdash Q \leftrightarrow \exists \mu' \in R(N,\mu) | \forall (p,c) \in Q : \mu'(p) = c$$

whereas,

$$(N,\mu) \nvdash Q \leftrightarrow \forall \mu' \in R(N,\mu) | \forall (p,c) \in Q : \mu'(p) \neq c$$

Up to here, the notion of a diagnosis can be captured as follows.

Definition 4.8. Given a diagnostic problem $CBPNDP = (N, M^{init}, \langle M^+, M^- \rangle)$. An initial marking μ^{ini} is a solution to CBPNDP iff:

$$(N, \mu^{ini}) \vdash M^+ \quad \text{and} \quad (N, \mu^{ini}) \nvdash M^-$$

4.4 Diagnostic problem solving within CBPNs

Now that we know about defining the diagnostic problem in terms of CBPNs, we next would like to know how to accomplish the reasoning task, obviously by exploiting the CW-analysis technique defined previously.

When a system does not work as expected, we get an observation OBS, actually a symptom, to be explained. As outlined in a previous chapter, a classification concerning such an observation needs to account for, that means defining which ones have to be entailed by a diagnosis and which ones have to be kept for consistency checking. In terms of CBPNs, such an observation consists of a marking μ^{OBS} where only manifestation places are marked. Moreover, it is classified into M^+ and M^- in order to perform the reasoning process by making use of the CW-analysis technique, starting from a marking μ such that

$$\forall p \in P : \mu(p) = \begin{cases} c & \text{if } (p,c) \in M^+ \\ c^w & \text{if } (p,c) \in M^- \\ \emptyset & \text{otherwise} \end{cases}$$

In fact, the CBPN models, and so the CW-analysis are defined mainly for diagnostic reasoning. Recall that a solution to $CBPNDP$ must deal with both constraints of Def 4.8. A traditional way to ensure that is to perform a backward analysis to get the set of candidate solutions and then to check their consistency by a forward one corresponding to each of them (a diagnosis must reach no element of M^-). By making use of the CW-analysis, such a process can be performed in a single phase. Of course, thanks go to the concept of *inhibited colour*, where it becomes possible to block certain colours from being produced.

Diagnostic solutions can be directly obtained, when performing the CW-analysis, as a set of initial markings ranged in

$$\mu^{ini} \subseteq 2^{M^{init}}$$

where $\forall \mu_i \in \mu^{ini}$,

$$\exists \mu' \in R(N, \mu_i) : \mu \sqsubseteq \mu'$$

Example 4.2. *To show how diagnoses are computed using the CW-analysis defined above, we return to the CBPN shown in Fig. 3.5. Let us consider the diagnostic problem $DP = (N, M^{init}, < M^+, M^- >)$ characterized by the following observation $\mu^{OBS} = p_8(h) + p_9(a)$. The first step consists of choosing which observed manifestations must be covered by a diagnosis. In fact, as discussed in [15], this implies the existence of a spectrum of definitions varying from a pure consistency-based to a pure abductive diagnosis for the same observation according to the classification of M^+ and M^-.*

For the current example, let $M^+ = \{(p_8, h)\}$ and $M^- = \{(p_9, b))\}$. The step that follows consists of using the CW-analysis method to solve DP. Fig.4.1. shows the backward reachability graph corresponding to the current example. Starting from a marking $\mu = p_8(h) + p_9(b^w)$, we seek finding diagnoses that cover M^+ consistently with M^-. It is worth noting that a framed transition represents the fact that it is forced, whereas it is over-lined if it is inhibited for certain firing ways that produce the meant inhibited colour. The framed places indicate the cause behind the marking inconsistency. For the case we have, three paths are starting from μ, within two of them the search stops since their terminal nodes are inconsistent markings ($C, D \in t_5^\bullet$ and $n \neq n^w$). These paths represent the possible alternatives to get the colour h in the place p_8, because each of them corresponds to a row of $FW^B(t_5)$. A diagnosis to DP is a marking $\mu' \in \mu^{ini}$ such that $\mu' = p_1(h) + p_2(a) + p_3(l)$.

A meaningful explanation is that, by imposing that N describes a faulty behaviour of a system, the problem resides in the component corresponding to p_2 when it is instantiated with the value corresponding to colour a. However, no relevance to components corresponding to p_1 and p_3 if they are instantiated with values corresponding to colours h and l respectively and simultaneously.

4.5 Conclusion

In this chapter, we have, first, defined a backward reachability analysis technique devoted specifically for CBPNs. The interesting thing about the CW-analysis technique is exploiting matrices attached to transitions when being performed as a way to reduce the complexity problem related to that task. Secondly, a formalization of a CBPN-based diagnosis approach for centralized systems has taken place where the system model is described in the whole in terms of CBPNs. Here, the diagnosis reasoning mechanism has been implemented by exploiting the CW-analysis technique.

With the fact that an increasing number of nowadays built systems are concurrent and often distributed, the classical diagnostic approach with a centralized system, having a model of the whole system to be diagnosed and receiving all observation signalizations, becomes quite inappropriate. Instead, the most suitable architecture when constructing such a system would be the distributed one. In the following chapter, a distributed diagnostic approach based on place-bordered CBPNs will be introduced. In such an approach, the diagnostic system itself will be defined as a set of diagnostic agents each of which is in charge of a specific part of the system.

CHAPTER 5

MODULAR CBPN-BASED DIAGNOSIS

Since the systems concerned in this thesis consist of a collection of interacting subsystems, the current chapter provides an extension of the CBPN-based approach defined previously to a distributed one. It presents a modular description of the system behaviour based on place-bordered CBPNs. It is followed by a formalization of the distributed CBPN-based approach in terms of a set of diagnostic agents each of which diagnoses a subsystem.

5.1 Introduction

It is often the case that a system cannot be diagnosed as a whole, the reason being the size or the scale of the system or practically the computationally complexity due to the state space explosion. Consider the system to be diagnosed as a collection of interacting subsystems $S_1,...,S_n$, in which a fault propagation is conceivable, $i.e$, when a fault occurs in a subsystem, it may propagate to its neighbours. For such systems:

- * Centralized diagnostic system is certainly inappropriate. There is only one diagnoser in charge of the entire system S, having its whole model, capturing all observations, then performing a global diagnosis.

- * Decentralized diagnostic system is barely accepted. Here, a local diagnoser is attached to each subsystem S_i of S, with a central coordination process to perform global diagnosis.

- * Distributed diagnostic system is the most suitable. No need for a central coordination process, but rather a global diagnosis would be accomplished through communications among local diagnosers.

Within the distributed view, the diagnostic system would be performed as multiple diagnostic agents, with one agent per subsystem, having its detailed local model, receiving the local observations and computing preliminary diagnoses. Moreover, it can exchange limited information with the adjacent agents for consistency checking, in order to recover the same results as a centralized system, which has a global view of the entire system.

In terms of CBPNs, a diagnostic problem is defined as

$$CBPNDP = \bigcup_{i=1}^{n} CBPNDP_i$$

where each $CBPNDP_i$ is defined over a subsystem $S_i, i = 1..n$. A full description of the distributed CBPN-based diagnostic approach is in the following.

5.2 System model

According to the multiagent diagnostic approach, the overall model of the system to be diagnosed is distributed over the agents. Thereby, it is defined as a set of n CBPN models with bordered places, where each model describes a subsystem S_i. The interactions between such subsystems are represented through tokens that may pass via the bordered places (also refer to as common places). Formally, the system model is given by

$$N_S = \{(N_i, P_i^{In}, P_i^{Out}) : i = 1, 2, ..., n\}$$

where

- $N_i = (\Sigma_i, P_i, T_i, A_i, C_i, FW_i)$
- $P_i^{In} = \{p \in P_i | (p^\bullet \in T_i) \wedge ({}^\bullet p \notin T_i)\}$
- $P_i^{Out} = \{p \in P_i | (p^\bullet \notin T_i) \wedge ({}^\bullet p \in T_i)\}$

N_i is a CBPN model describing the causal behaviour of the subsystem S_i. P_i^{In} and P_i^{Out} denote the sets of bordered places of N_i corresponding to In_i and Out_i respectively.

Definition 5.1. Given a CBPN model $N = (\Sigma, P, T, A, C, FW)$. Given a set of place-bordered CBPNs

$$N_S = \{(N_i, P_i^{In}, P_i^{Out}) | N_i = (\Sigma_i, P_i, T_i, A_i, C_i, FW_i), i = 1, 2, ..., n\}$$

N_S is the corresponding place-bordered CBPNs of N iff:

- $\Sigma = \bigcup_{i=1}^{n} \Sigma_i$
- $P = \bigcup_{i=1}^{n} P_i$ and $\forall i \Rightarrow \exists j : P_i \cap P_j \triangleq P_{ij} \neq \emptyset$, $(P_{ij} \subseteq P_i^{In} \cup P_i^{Out})$
- $T = \bigcup_{i=1}^{n} T_i$ and $\forall i \neq j \Rightarrow T_i \cap T_j = \emptyset$
- $A = \bigcup_{i=1}^{n} A_i$, $(A_i = (P_i \times T_i) \cup (T_i \times P_i))$

P_{ij} refers to the set of places in common between two CBPNs N_i and N_j, whether inputs or outputs. Each subsystem interacts with at least one another subsystem; whereas their transition sets are mutually disjoint. It is quite clear that the colour function C_i, and also that concerning the firing ways FW_i could be defined by restricting the corresponding global functions C and FW on the sets P_i and T_i respectively.

It is already known that a CBPN model is acyclic by definition, thus each N_i is acyclic. With the assumption that the interactions between the local CBPN models are acyclic, the whole net model, N, resulting from the conjunction of the local models N_i is acyclic too.

Example 5.1. *Let us consider, as a typical example, a system S composed of three interacting subsystems S_1, S_2 and S_3 (adapted from an example presented in [42]). The causal behaviour of each subsystem is described by a CBPN. Formally, the system model is given by*

$$N_s = \{(N_i, P_i^{In}, P_i^{Out}) : i \in \{1,2,3\}\}$$

with:

- $P_1^{In} = \{A, C\}$, $P_1^{Out} = \{B\}$,
- $P_2^{In} = \emptyset$, $P_2^{Out} = \{A\}$,
- $P_3^{In} = \{B\}$, *and* $P_3^{Out} = \{C\}$.

Table 5.1 shows the colour set corresponding to each place. Fig. 5.1. gives the graphical representation of the corresponding models.

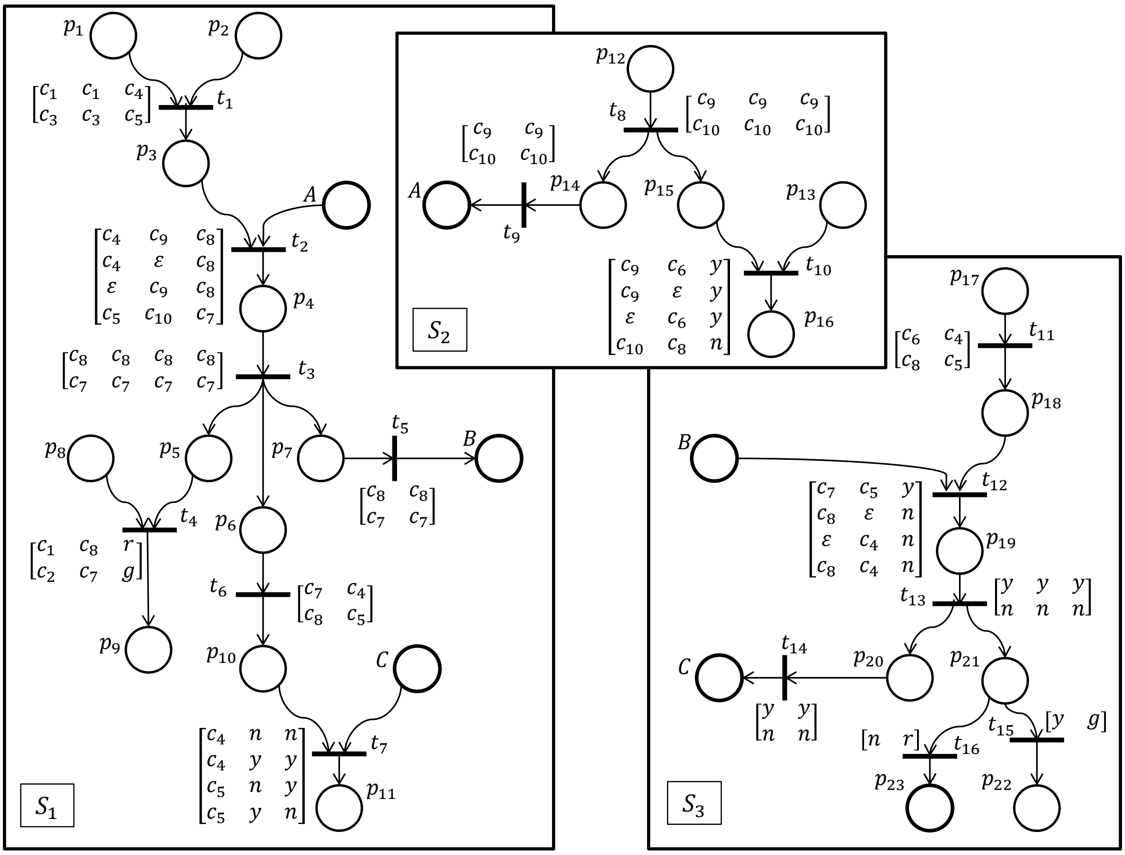
5.3 Local preliminary diagnosis

As mentioned previously, the diagnostic system is a multiagent system, where each agent A_i is in charge of a subsystem S_i. Thus, A_i must be provided by S_i's detailed description given as

$$(N_i, P_i^{In}, P_i^{Out})$$

$p \in P_i$	$C_i(p)$
p_1, p_2, p_8	$\{c_1, c_2, c_3\}$
p_3, p_{10}, p_{18}	$\{c_4, c_5\}$
$p_4, p_5, p_6, p_7, p_{13}, p_{17}, B$	$\{c_6, c_7, c_8\}$
$p_{12}, p_{14}, p_{15}, A$	$\{c_9, c_{10}\}$
p_9, p_{22}	$\{r, o, g\}$
$p_{11}, p_{16}, p_{19}, p_{20}, p_{21}, C$	$\{y, n\}$

Table 5.1: N_s places' colour set.



p_1
p_2
t_1
$\begin{bmatrix} c_1 & c_1 & c_4 \\ c_3 & c_3 & c_5 \end{bmatrix}$
p_3
A
t_2
$\begin{bmatrix} c_4 & c_9 & c_8 \\ c_4 & \varepsilon & c_8 \\ \varepsilon & c_9 & c_8 \\ c_5 & c_{10} & c_7 \end{bmatrix}$
p_4
t_3
$\begin{bmatrix} c_8 & c_8 & c_8 & c_8 \\ c_7 & c_7 & c_7 & c_7 \end{bmatrix}$
p_8
p_5
p_7
t_5
B
$\begin{bmatrix} c_8 & c_8 \\ c_7 & c_7 \end{bmatrix}$
t_4
p_6
$\begin{bmatrix} c_1 & c_8 & r \\ c_2 & c_7 & g \end{bmatrix}$
t_6
$\begin{bmatrix} c_7 & c_4 \\ c_8 & c_5 \end{bmatrix}$
p_9
p_{10}
C
$\begin{bmatrix} c_4 & n & n \\ c_4 & y & y \\ c_5 & n & y \\ c_5 & y & n \end{bmatrix}$
t_7
p_{11}
S_1
p_{12}
t_8
$\begin{bmatrix} c_9 & c_9 & c_9 \\ c_{10} & c_{10} & c_{10} \end{bmatrix}$
$\begin{bmatrix} c_9 & c_9 \\ c_{10} & c_{10} \end{bmatrix}$
A
t_9
p_{14}
p_{15}
p_{13}
$\begin{bmatrix} c_9 & c_6 & y \\ c_9 & \varepsilon & y \\ \varepsilon & c_6 & y \\ c_{10} & c_8 & n \end{bmatrix}$
t_{10}
p_{16}
S_2
p_{17}
t_{11}
$\begin{bmatrix} c_6 & c_4 \\ c_8 & c_5 \end{bmatrix}$
p_{18}
B
t_{12}
$\begin{bmatrix} c_7 & c_5 & y \\ c_8 & \varepsilon & n \\ \varepsilon & c_4 & n \\ c_8 & c_4 & n \end{bmatrix}$
p_{19}
t_{13}
$\begin{bmatrix} y & y & y \\ n & n & n \end{bmatrix}$
t_{14}
C
p_{20}
p_{21}
$\begin{bmatrix} y & y \\ n & n \end{bmatrix}$
$[n \quad r]$
t_{16}
t_{15}
$[y \quad g]$
p_{23}
p_{22}
S_3

Figure 5.1: A modular CBPN

it is the one who is responsible to receive any local observation Obs_i corresponding to S_i when the system S goes wrong. When that happens, A_i performs a local diagnosis by means of S_i's net model (N_i) in order to explain the local Obs_i.

Recall that, in terms of CBPNs, an observation consists in a final marking μ^{Obs_i} where

$$\forall p \in P_i : \mu^{Obs_i}(p) \neq \emptyset \rightarrow p \in Mn_i$$

Thus, a local diagnostic problem related to the subsystem S_i is defined as

$$CBPNDP_i = ((N_i, P_i^{In}, P_i^{Out}), \langle M_i^+, M_i^- \rangle)$$

here, $(N_i, P_i^{In}, P_i^{Out})$ denotes the place bordered CBPN describing S_i; whereas $\langle M_i^+, M_i^- \rangle$ is the local observation. In this case, a preliminary diagnosis to $CBPNDP_i$ is an initial marking μ_i^{ini} such that

$$(N_i, \mu_i^{ini}) \vdash M_i^+ \text{ and } (N_i, \mu_i^{ini}) \nvdash M_i^-$$

As outlined in the previous chapter, the diagnostic reasoning scheme can be implemented by making use of the CW-analysis technique. Each time agent A_i receives a local observation, as a μ^{Obs_i} marking, the diagnosis process is launched. It starts by classifying the received observation (locally) into M_i^+ and M_i^-, to determine which observed manifestations must be covered (entailed) by a diagnosis. Then, starting from a marking $\mu \sqsubseteq \mu^{Obs_i}$, the CW-analysis seeks to find the initial markings μ^{Ini_i} from which μ can be reached. The result of the CW-analysis comes out through a reachability graph whose root node is the marking μ whereas the terminal nodes are either initial markings ranged in μ^{Ini_i} or inconsistent ones. Practically, μ^{Ini_i} represents local diagnoses to $CBPNDP_i$.

$$\mu^{Ini_i} = \{\mu | \forall p \in P_i : \mu(p) \neq \emptyset \Rightarrow^\bullet p = \emptyset \\ \wedge (N_i, \mu) \vdash M_i^+ \wedge (N_i, \mu) \nvdash M_i^- \}$$

A remark is worthwhile here. In a subsystem's CBPN model, a source place describes either a local initial state of the corresponding causal model; or a bordered place used as input to such a model from a neighbouring one. By the first, we obtain the set of local diagnoses Δ_i; whereas the second ones are used particularly to refine such local diagnoses.

$$\Delta_i = \{\prod_{Ic_i}(\mu) | \mu \in \mu^{Ini_i}\}$$

where $\prod_{Ic_i}$ denotes the restriction on $Ic_i \subset P_i$.

Example 5.2. *Back to the previous example, the diagnostic system consists of three agents A_1,A_2 and A_3, where each is in charge of a subsystem S_1,S_2 and S_3 respectively. In the following, we show how an agent would explain locally the received observation. Let us consider the following system state.*

- * *Agent A_1 receives the observation $\mu^{Obs_1} = p_9(r) + p_{11}(y)$ from S_1,*
- * *Agent A_2 receives the observation $\mu^{Obs_2} = p_{16}(y)$ from S_2, and*
- * *Agent A_3 receives the observation $\mu^{Obs_3} = p_{22}(r)$ from S_3.*

Notice that $C(p_{22}) = \{r,g,o\}$, whereas the colour g is the only one present in the given net model. One should differenciate between the admissible-values of a particular state or a variable from its modelled ones. While place p_{22} can hold an r, g, or o token colour, the only modelled one is the g colour.

A local diagnostic problem is defined at the level of each agent as

$$CBPNDP_i = ((N_i, P_i^{In}, P_i^{Out}), < M_i^+, M_i^- >), i = 1,2,3$$

We consider the classification where both sets M_1^- and M_2^- are empty, while $M_3^- = \{(p_{22},g)\}$. Hence,

- ▷ $M_1^+ = \{(p_9,r),(p_{11},y)\}$,
- ▷ $M_2^+ = \{(p_{16},y)\}$, *and*
- ▷ $M_3^+ = \emptyset$.

Preliminary diagnoses can be computed, by each agent using the CW-analysis technique as shown in the previous chapter. At the end, each agent gets a set of initial markings ranged in μ^{Ini_i}.

Graph of Fig. 5.2 represents the CW-analysis leading to the computation of μ^{Ini_1} markings. As results, A_1 obtains:

$\mu_1^{Ini_1} = \{p_1(c_1), p_2(c_1), p_8(c_1), A(c_9), C(n)\}$,

$\mu_2^{Ini_1} = \{p_1(c_1), p_2(c_1), p_8(c_1), C(n)\}$, *and*

$\mu_3^{Ini_1} = \{p_8(c_1), A(c_9), C(n)\}$.

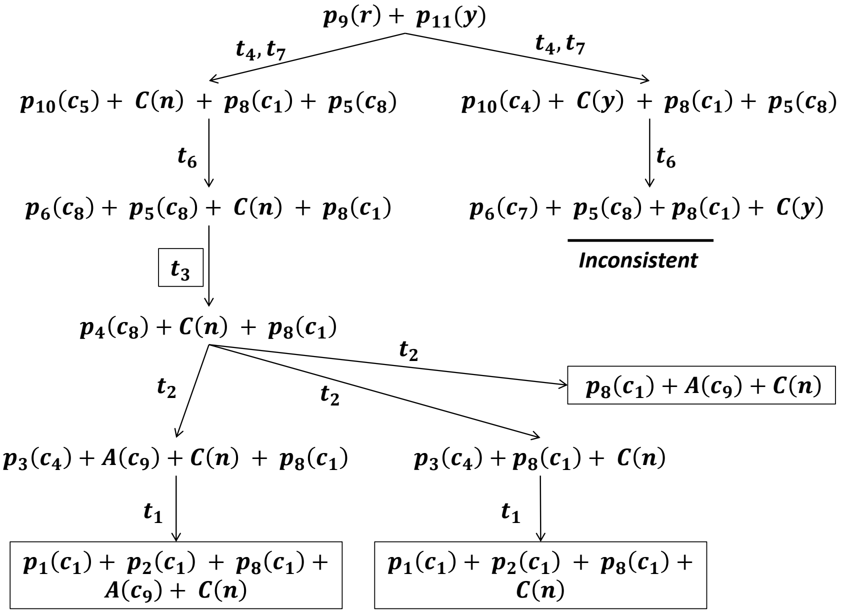

p9(r) + p11(y)
t4, t7
t4, t7
p10(c5) + C(n) + p8(c1) + p5(c8)
p10(c4) + C(y) + p8(c1) + p5(c8)
t6
t6
p6(c8) + p5(c8) + C(n) + p8(c1)
p6(c7) + p5(c8) + p8(c1) + C(y)
Inconsistent
t3
p4(c8) + C(n) + p8(c1)
t2
t2
t2
p8(c1) + A(c9) + C(n)
p3(c4) + A(c9) + C(n) + p8(c1)
p3(c4) + p8(c1) + C(n)
t1
t1
p1(c1) + p2(c1) + p8(c1) + A(c9) + C(n)
p1(c1) + p2(c1) + p8(c1) + C(n)

Figure 5.2: The CW-analysis graph of Agent A_1

Since diagnoses are defined by the smallest set of marked places, $\mu_1^{Ini_1}$ must be discarded

$$\mu_3^{Ini_1} \sqsubseteq \mu_1^{Ini_1}$$

By restricting the left markings on the places belonging to Ic_1, the local diagnoses of $CBPNDP_1$ are the following:

- $\Delta_1^1 = \{(p_1,c_1),(p_2,c_1),(p_8,c_1)\}$
- $\Delta_2^1 = \{(p_8,c_1)\}$

Both explanations indicate that $CBPN_3$ has a hand in the made observation by receiving the colour n in the place C; whereas the second one stands alone in being affected by $CBPN_2$ also, by receiving the colour c_9 in the place A.

Agents A_2 and A_3 construct the CW-analysis graphs of $CBPN_2$ and $CBPN_3$ respectively, they come to:

$$\begin{aligned} \mu^{Ini_2} &= \{p_{12}(c_9), p_{13}(c_6)\} \quad (A_2) \\ \mu^{Ini_3} &= \{p_{17}(c_8^w), B(c_7^w\} \quad\;\; (A_3) \end{aligned}$$

Thus, the local diagnoses obtained by both agents are:

$$\begin{array}{ll} \Delta^2 = \{(p_{12}, c_9), (p_{13}, c_6)\} & (A_2) \\ \Delta^3 = \{(p_{17}, c_8^w)\} & (A_3) \end{array}$$

The explanation gotten by A_3 means that in order to avoid having the colour g in the place p_{22}, one must avoid the situation where p_{17} is marked by the colour c_8, besides receiving a colour which differs from c_7 in the place B from $CBPN_1$.

5.4 Cooperation between agents

Summing up. When the system S falls down, the agents must make a diagnosis. Each agent A_i locally executes the diagnosis process once it receives local observation Obs_i. Agent A_i computes the local preliminary diagnoses for Obs_i by making use of the CW-analysis as explained before. However, the obtained explanations of the different agents may not be globally consistent when they are considered all together. This is because agents work in isolation, whereas the net models do not have disjoint sets of places (they can change the markings of the common places, and then affect each other).

In order to deal with such a problem, agents must communicate with each other to recover the results of a centralized agent that would have a global view of the whole system. By communication, agents exchange their local diagnoses for consistency checking by sending messages to each other. Each agent A_i sends to each of its neighbourhood A_j a message Msg for each of its local diagnoses. Such a message contains the markings of N_i's input places obtained during the reasoning process.

$$Msg_{i \to j} = \mu_{i \to j}^{Msg} = \{ \prod_{P_i^{In} \cap P_{ij}} (\mu) | \mu \in \mu^{Ini_i} \}$$

By the way, just after finding the local diagnoses, each agent exploits them to come out with the markings of its corresponding net output places. In other words, for each marking $\mu \in \mu^{Ini_i}$, agent A_i builds the corresponding μ's graph, obviously through a forward analysis, to predict the marking of P_i^{Out} places. We refer to such markings as μ^{Out_i}, then,

$$\mu^{Out_i} = \{ \prod_{P_i^{Out}} (\mu) | \mu \in R(N_i, \mu^{Ini_i}) \wedge p \in P_i^{Out} \Rightarrow \mu(p) \neq \emptyset \}$$

Note. *The graph construction must be terminated just when attaining the required marking.*

Upon reception of Msg (which is assumed to be correctly received by A_j), A_j has to check the consistency of this message with its local diagnoses. More accurately, A_j performs a comparison between each of the μ^{Out_j} markings and the received message. Let μ^{Msg} be the marking encoded in Msg; we say that μ^{Msg} (or Msg) conforms with A_j's local diagnosis, from which a marking $\mu \in \mu^{Out_j}$ has been computed, iff:

$$\forall p \in P_j^{Out} \cup P_{ji}, \mu^{Msg}(p) = \mu(p)$$

After checking all the local diagnoses, through μ^{Out_j} markings, A_j's behaviour depends on the case A_j faces.

- For the case where at least one of the μ^{Out_j} markings conforms to Msg, A_j responds to A_i message Msg affirmatively. Such a response indicates that the A_i local diagnosis, from which Msg is generated, is supported by A_j local diagnoses.

- If it is not the case, A_j sends a negative response to A_i; which can be interpreted as none of the A_j's local diagnoses can be in coincidence with that of A_i.

Each agent has to respond to each message it receives, with either a positive or negative response; as well as waiting responses for its sent messages if any. When A_i receives positive response for its sent message Msg, it is beyond dispute; the local diagnosis corresponding to Msg is supported by those of A_j. While on the contrary, when receiving a negative response to Msg, A_i realizes the conflict of its diagnosis (corresponding to Msg) with the ones of A_j. However, A_i may face the case where such a diagnosis is already used to validate consistency with diagnoses of another neighbourhood A_k (i.e., $k \neq j$). A_i must discard such a diagnosis anyway, as well as A_k must eliminate those ones which are in conformity with Msg.

It should be noticed that due to the safeness and acyclicity properties of the local net models, besides the acyclicity of the interactions between them, the consistency checking process terminates after some rounds of communication. At that point, the diagnostic agents achieve a stability condition in terms of their local diagnoses. Therefore, a global diagnosis of the whole system can be characterized by combining those local diagnoses, provided that no cycle of blames arises (i.e., agent A_i blames the cause of a problem on the subsystem managed by agent A_j, while agent A_j blames the cause of the problem on the subsystem managed by agent A_i). The recovering of global diagnoses can be captured by the following proposition. Actually, it is an extension of the one presented in [3] for distributed diagnosis within BPNs.

Proposition 5.1. *Given the overall diagnostic problem*

$$CBPNDP = (N, \langle M^{+}, M^{-} \rangle)$$

Given a local diagnostic problem

$$CBPNDP_i = ((N_i, P_i^{In}, P_i^{Out}), \langle M_i^{+}, M_i^{-} \rangle)$$

Let Δ, Δ_i be sets of diagnoses corresponding to $CBPNDP$, $CBPNDP_i$ respectively. Then,

$$CBPNDP = \bigcup_{i=1}^{n} CBPNDP_i \;\Rightarrow\; \prod_{N_i}(\Delta) = \Delta_i, \forall i = 1..n$$

Proof. The idea underlying the proof of this proposition is that both global and local diagnoses come out of applying the same analysis technique on the same net model (N corresponds to N_s, see Def. 5.1), and starting from the same made observation. ■

Example 5.3. *Continuing with the previous example, each agent A_i has got a set of local explanations Δ_i. For each diagnosis, and from the one hand, A_i sends a message Msg to each neighbour that has a concern (by participating in such a diagnosis with at least a place in common). On the other hand, A_i computes the markings of its output places to be used for consistency checking. Table 5.3 sums the obtained results.*

Sender/Receiver	Sent Msg	Receiver μ^{Out}	Response
$A_1 \dashrightarrow A_2$	(A, c_9)	(A, c_9)	ok
$A_1 \dashrightarrow A_3$	(C, n)	(C, y^w)	ok
$A_3 \dashrightarrow A_1$	(B, c_7^w)	(B, c_8)	ok

Table 5.2: Cooperation results obtained by agents A_1, A_2 and A_3

As a sample, the first row of the table indicates that agent A_1 sends a massage $Msg((A, c_9))$ to agent A_2 (e.i., A_1 needs to have the colour c_9 in the place A). Agent A_2, and from its local diagnosis, gets $\mu^{Out_2}(A) = c_9$, which coincides with the received message. Consequently, A_2 responds to the received request from A_1 by a positive response. By the same way one can read the second and the third rows, but only in these cases, the received Msg conforms with the local diagnosis implicitly. As an example, for the second row, $\mu^{Msg}(C) = n$ while $\mu^{Out_3}(C) = y^w$, place C must hold a colour which differs from y. Notice that $C_3(C) = \{y, n\}$ and $\mu^{Out_3}(C) = y^w \to (\mu^{Out_3}(C) = n$ or $\mu^{Out_3}(C) = \emptyset)$, so n is the colour in common between $\mu^{Msg}(C)$ and $\mu^{Out_3}(C)$, thus they are in conformity.

At the end, all agents get positive responses for their sent messages; which makes the obtained local diagnoses consistent with each other. It should be noted here that agent A_1 has two diagnoses Δ_1^1 and Δ_2^1 where $\Delta_2^1 \subset \Delta_1^1$, both diagnoses are consistent with those of other agents, thus Δ_1^1 must be discarded (it is not minimal).

Finally, the observed misbehaviour of the whole system is explained by the following diagnoses:

$$\begin{array}{ll} \Delta^1 = \{(p_8, c_1)\} & \textit{for } A_1 \\ \Delta^2 = \{(p_{12}, c_9), (p_{13}, c_6)\} & \textit{for } A_2 \\ \Delta^3 = \{(p_{17}, c_8^w)\} & \textit{for } A_3 \end{array}$$

5.5 Conclusion

This chapter has been dedicated to the introduction of a distributed CBPN-based diagnostic approach since most of nowadays systems are concurrent and distributed. The system model is defined as a collection of place-bordered CBPNs, while the diagnostic system consists of a set of diagnostic agents each of which is in charge of a specific part of the system. The diagnosis reasoning mechanism is implemented locally by exploiting the CW-analysis technique. The final step consists in checking global consistency of the obtained diagnoses by exchanging limited information about the marking of common places between neighbouring CBPN models.

Chapter 6

Conclusion

With the profound diffusion of technological systems in the real world, fault diagnosis has become a major requirement because of its importance in terms of system reliability, security, and efficiency. A diagnostic process is concerned with the automated generation of diagnoses that explain an incorrect behaviour of the system under consideration. Recently, and since most of the designed systems are concurrent and distributed, fault diagnosis has turned to be a very crucial and challenging task. In this thesis, we have focused on the causal model-based diagnosis of distributed systems by means of CPNs. The main contributions can be summarized as follows:

- We have introduced the CBPN models as a particular class of CPNs intended for the description of a system's causal behaviour. In fact, we have turned specifically to CPNs in order to tackle the problem of complexity in terms of net representation when using classical PNs. Besides, we have proposed associating a matrix with each transition in order to determine explicitly its different ways of firing, instead of being implicit in the surrounding expressions. In fact, the use of matrices simplifies particularly the net analysis when performed in a backward fashion.

- In the context of fault diagnosis, we have developed a model-based approach in terms of CBPNs. The approach adopts a centralized architecture, where the behaviour of the system to be diagnosed is described in the whole by a CBPN model. Therefore, the diagnostic reasoning scheme would be performed by exploiting a particular analysis technique called CW-analysis, that we have defined, as a backward reachability analysis method suited for CBPNs. Such a method makes use of transitions matrices instead of reversing the net expressions. Moreover, it uses the inhibited colour concept when processing to block certain colours, which helps in performing the diagnostic reasoning in a single step.

* Always in the same context, we have extended the proposed approach to implementing diagnosis of spatially distributed systems. Here, a system consists of a collection of interacting subsystems that cooperate among each other. In the distributed CBPN-based approach, the diagnostic system itself has been defined as a set of diagnostic agents each of which is in charge of a specific subsystem. Hence, the overall system model is distributed over the agents. It consists of a set of place-bordered CBPNs. Finally, diagnoses are locally generated, using the CW-analysis method, at the level of each subsystem, then checked for global consistency (in terms of communication among agents).

To the best of our knowledge, besides being introduced for diagnosis purposes, CBPNs can provide a very useful and helpful tool when dealing with problems requiring a backward analysis on reachability of CPNs for reasoning. The main issue about them is the use of firing ways matrices, and so instead of inverting the expressions surrounding a transition, the process needs a simple manipulation of its matrix (by changing the input and output blocks).

It is a fact that any new proposal gets limits. CPNs are good means of reducing the size of the net model. However, the reachability graph, since we are interested in, is almost the same that of classical PNs. The only distinguishing thing is the marking vector size (each component of the vector indicates the marking of a place). The places number is less in CPNs than in PNs.

Up to here, there are a couple of open lines for interesting future works.

- First, the proposed approach requires an evaluation on real systems (possibly, a local Ethernet network where each agent resides in a particular host of the network).
- Secondly, to study the possibility of using structural analysis, and mainly *invariants*, instead of reachability analysis, which suffer from the combinatorial explosion during the consistency checking of the generated initial markings.

BIBLIOGRAPHY

[1] C. ANGLANO AND L. PORTINALE, *Bw analysis: a backward reachability analysis for diagnostic problem solving suitable to parallel implementation*, in International Conference on Application and Theory of Petri Nets, Springer, 1994, pp. 39–58.

[2] P. BARONI, G. LAMPERTI, P. POGLIANO, AND M. ZANELLA, *Diagnosis of a class of distributed discrete-event systems*, IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30 (2000), pp. 731–752.

[3] H. BENNOUI, *Interacting behavioral petri nets analysis for distributed causal model-based diagnosis*, Autonomous agents and multi-agent systems, 28 (2014), pp. 155–181.

[4] K. R. BOEL AND G. JIROVEANU, *Distributed contextual diagnosis for very large systems*, IFAC Proceedings Volumes, 37 (2004), pp. 333–338.

[5] M. BOUALI, P. BARGER, AND W. SCHON, *Colored petri net inversion for backward reachability analysis*, IFAC Proceedings Volumes, 42 (2009), pp. 227–232.

[6] M. P. CABASINO, A. GIUA, C. N. HADJICOSTIS, AND C. SEATZU, *Fault model identification and synthesis in petri nets*, Discrete Event Dynamic Systems, 25 (2015), pp. 419–440.

[7] M. P. CABASINO, A. GIUA, A. PAOLI, AND C. SEATZU, *Decentralized diagnosis of discrete-event systems using labeled petri nets*, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 43 (2013), pp. 1477–1485.

[8] M. P. CABASINO, A. GIUA, M. POCCI, AND C. SEATZU, *Discrete event diagnosis using labeled petri nets. an application to manufacturing systems*, Control Engineering Practice, 19 (2011), pp. 989–1001.

[9] ——, *Discrete event diagnosis using labeled petri nets. an application to manufacturing systems*, Control Engineering Practice, 19 (2011), pp. 989–1001.

[10] J. CARDOSO, L. KUNZLE, AND R. VALETTE, *Petri net based reasoning for the diagnosis of dynamic discrete event systems*, in Proceedings of the 6th international fuzzy systems association world congress, July, 1995, pp. 333–336.

[11] S. M. CHO, H. S. HONG, AND S. D. CHA, *Safety analysis using coloured petri nets*, in Proceedings 1996 Asia-Pacific Software Engineering Conference, IEEE, 1996, pp. 176–183.

[12] X. CONG, M. P. FANTI, A. M. MANGINI, AND Z. LI, *Decentralized diagnosis by petri nets and integer linear programming*, IEEE Transactions on Systems, Man, and Cybernetics: Systems, (2017), pp. 1–12.

[13] L. CONSOLE, D. T. DUPRÉ, AND P. TORASSO, *On the relationship between abduction and deduction*, Journal of Logic and Computation, 1 (1991), pp. 661–690.

[14] L. CONSOLE AND P. TORASSO, *Hypothetical reasoning in causal models*, International Journal of Intelligent Systems, 5 (1990), pp. 83–124.

[15] ——, *A spectrum of logical definitions of model-based diagnosis*, Computational intelligence, 7 (1991), pp. 133–141.

[16] M. CORDIER, P. DAGUE, M. DUMAS, F. LEVY, J. MONTMAIN, M. STAROSWIECKI, AND L. TRAVE-MASSUYES, *Ai and automatic control approaches of model-based diagnosis: Links and underlying hypotheses*, in 4th IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes, vol. 1, 2000, pp. 274–279.

[17] M.-O. CORDIER, P. DAGUE, M. DUMAS, F. LÉVY, J. MONTMAIN, M. STAROSWIECKI, AND L. TRAVÉ-MASSUYES, *A comparative analysis of ai and control theory approaches to model-based diagnosis*, in ECAI, 2000, pp. 136–140.

[18] J. DE KLEER, A. K. MACKWORTH, AND R. REITER, *Characterizing diagnoses and systems*, Artificial intelligence, 56 (1992), pp. 197–222.

[19] R. DEBOUK, S. LAFORTUNE, AND D. TENEKETZIS, *Coordinated decentralized protocols for failure diagnosis of discrete event systems*, Discrete Event Dynamic Systems, 10 (2000), pp. 33–86.

[20] M. DIAZ, *Les réseaux de Petri: modèles fondamentaux*, Hermes, 2001.

[21] M. DOTOLI, M. P. FANTI, A. M. MANGINI, AND W. UKOVICH, *On-line fault detection in discrete event systems by petri nets and integer linear programming*, Automatica, 45 (2009), pp. 2665–2672.

[22] B. EL AYEB, P. MARQUIS, AND M. RUSINOWITCH, *Deductive/abductvie diagnosis: the da-principles*, in Proceedings of the 9th European Conference on Artificial Intelligence, 1990, pp. 47–52.

[23] ——, *Preferring diagnoses by abduction*, IEEE transactions on systems, man, and cybernetics, 23 (1993), pp. 792–808.

[24] E. FABRE AND A. BENVENISTE, *Partial order techniques for distributed discrete event systems: Why you cannot avoid using them*, Discrete Event Dynamic Systems, 17 (2007), pp. 355–403.

[25] E. FABRE, A. BENVENISTE, S. HAAR, AND C. JARD, *Distributed monitoring of concurrent and asynchronous systems*, Discrete Event Dynamic Systems, 15 (2005), pp. 33–84.

[26] S. GENC AND S. LAFORTUNE, *Distributed diagnosis of place-bordered petri nets*, IEEE Transactions on Automation science and Engineering, 4 (2007), pp. 206–219.

[27] A. GIUA AND M. SILVA, *Petri nets and automatic control: A historical perspective*, Annual Reviews in Control, 45 (2018), pp. 223–239.

[28] K. JENSEN, L. M. KRISTENSEN, AND L. WELLS, *Coloured petri nets and cpn tools for modelling and validation of concurrent systems*, International Journal on Software Tools for Technology Transfer, 9 (2007), pp. 213–254.

[29] G. JIROVEANU AND R. BOEL, *Petri net model-based distributed fault diagnosis for large interacting systems*, in Proceedings of the 16th International Workshop on Principles of Diagnosis (DX05), 2005, pp. 25–30.

[30] ——, *Petri net model-based distributed fault diagnosis for large interacting systems*, in Proceedings of the 16th International Workshop on Principles of Diagnosis (DX05), 2005, pp. 25–30.

[31] G. JIROVEANU AND R. K. BOEL, *A distributed approach for fault detection and diagnosis based on time petri nets*, Mathematics and computers in simulation, 70 (2006), pp. 287–313.

[32] Y. LI, *Diagnosis of large software systems based on colored petri nets*, PhD thesis, Université Paris Sud-Paris XI, 2010.

[33] C. MAHULEA, C. SEATZU, M. P. CABASINO, AND M. SILVA, *Fault diagnosis of discrete-event systems using continuous petri nets*, IEEE Transactions on Systems, Man, and Cybernetics–Part A: Systems and Humans, 42 (2012), pp. 970–984.

[34] ——, *Fault diagnosis of discrete-event systems using continuous petri nets-draft*, (2014).

[35] T. MURATA, *Petri nets: Properties, analysis and applications*, Proceedings of the IEEE, 77 (1989), pp. 541–580.

[36] J. OHAN DE KLEER AND B. C. WILLIAMS, *Diagnosis with behavioral modes*, Proceeding& of the IJ CAI, 1 (1989), pp. 1324–1330.

[37] Y. Pencolé, R. Pichard, and P. Fernbach, *Modular fault diagnosis in discrete-event systems with a cpn diagnoser*, IFAC-PapersOnLine, 48 (2015), pp. 470–475.

[38] D. Poole, *Representing knowledge for logic-based diagnosis.*, in FGCS, 1988, pp. 1282–1290.

[39] ——, *Normality and faults in logic-based diagnosis.*, in IJCAI, vol. 89, Citeseer, 1989, pp. 1304–1310.

[40] L. Portinale, *Verification of causal models using petri nets*, International journal of intelligent systems, 7 (1992), pp. 715–742.

[41] ——, *Petri net models for diagnostic knowledge representation and reasoning*, PhD Tesis, Dipartamento di Informatica–Universita'di Torino, (1993).

[42] ——, *Behavioral petri nets: a model for diagnostic knowledge representation and reasoning*, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 27 (1997), pp. 184–195.

[43] W. Qiu and R. Kumar, *A new protocol for distributed diagnosis*, in 2006 American Control Conference, IEEE, 2006, pp. 6–pp.

[44] R. Reiter, *A theory of diagnosis from first principles*, Artificial intelligence, 32 (1987), pp. 57–95.

[45] E. Rich and K. Knight, *Artificial intelligence*, McGraw-Hill, New, (1991).

[46] N. Roos, A. Ten Teije, and C. Witteveen, *A protocol for multi-agent diagnosis with spatially distributed knowledge*, in Proceedings of the second international joint conference on Autonomous agents and multiagent systems, ACM, 2003, pp. 655–661.

[47] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, *Diagnosability of discrete-event systems*, IEEE Transactions on automatic control, 40 (1995), pp. 1555–1575.

[48] M. SCHROEDER AND G. WAGNER, *Distributed diagnosis by vivid agents*, in Proceedings of the first international conference on Autonomous agents, 1997, pp. 268–275.

[49] C. SEATZU, *Fault diagnosis of discrete event systems using petri nets.*, in VECoS, 2014, pp. 12–15.

[50] V. SRINIVASAN AND M. A. JAFARI, *Fault detection/monitoring using time petri nets*, IEEE transactions on systems, man, and cybernetics, 23 (1993), pp. 1155–1162.

[51] P. STRUSS AND O. DRESSLER, *Integrating fault models into the general diagnostic engine*, in Proc. of the Inter. Joint Conf. on Artificial Intelligence (IJCAI'89), Detroit, MI, 1989, pp. 1318–1323.

[52] R. SU AND W. WONHAM, *A model of component consistency in distributed diagnosis*, in Discrete Event Systems 2004 (WODES'04): A Proceedings Volume from the 7th IFAC Workshop, Reims, France, 22-24 September 2004, Elsevier, 2005, p. 417.

[53] R. SU, W. WONHAM, J. KURIEN, AND X. KOUTSOUKOS, *Distributed diagnosis for qualitative systems*, in Sixth International Workshop on Discrete Event Systems, 2002. Proceedings., IEEE, 2002, pp. 169–174.

[54] G. ZHU, Z. LI, N. WU, AND A. AL-AHMARI, *Fault identification of discrete event systems modeled by petri nets with unobservable transitions*, IEEE Transactions on Systems, Man, and Cybernetics: Systems, (2017), pp. 1–13.