Università degli Studi di Cagliari

西南交通大学

PHD DEGREE at the University of Cagliari

Electronic and Computer Engineering

PHD DEGREE at Southwest Jiatong University

Traffic Information Engineering and Control

Cycle XXXIV

VERIFICATION AND APPLICATION OF DETECTABILITY BASED ON PETRI NETS

………

………

ING-INF/04 AUTOMATICA

………………………………………………………………………………

PhD Student:	Hao Lan
Supervisor UniCa	Prof. Carla Seatzu
Supervisor SWJU	Prof. Jin Guo

Final exam. Academic Year 2020 – 2021

Thesis defence: November 2021 Session

摘 要

在实际系统中，由于传感器的限制和环境的影响，系统的动态变化常常不能完全被掌握，获取的信息或测量的数据常常不完善，所以系统操作员并不总是对系统有完整的了解。但系统的状态信息却非常重要，操作员需要估计系统的状态才能做出决定，例如故障诊断，反馈控制和隐蔽性分析等系统操作和分析都需要确定系统的状态。由于其重要性，状态估计问题在离散事件系统中受到了研究者们很多的关注，这促进了系统状态估计方法的研究。其中可检测性在近年来备受关注，研究者在可检测性的框架下，以更系统的方式研究了离散事件系统的状态估计问题。可检测性描述了系统状态能否被确定的能力，具体而言，系统具有可检测性意味着，当系统运行一段时间后，操作员根据系统产生输出或信号，能够唯一的确定系统的当前状态和后续状态。

为了对实际系统进行建模和分析，首先要有强有力的离散事件系统建模工具来描述外界对系统的不同观测行为。其次，通过穷举所有状态的分析方法可能产生状态爆炸问题，对实际系统并不适用。则设计更为高效、可实现的系统可检测性分析方法尤为重要。由于可检测性对系统的要求很严格，其可能适用于部分系统，但要求所有系统达到可检测性要求并不合理。因此，本论文主要研究了基于Petri网模型的系统可检测性验证方法，并放宽了可检测性的要求，提出了C-可检测性概念，给出了C-可检测性的形式化定义和验证方法。最后将C-可检测性性质应用于铁路系统中，验证了其针对实际系统的有效性。主要的结果如下：

1. 将四种类型的可检测性从有限自动机扩展到标记Petri网，即在标记Petri网中正式定义了强可检测性，弱可检测性，周期性强可检测性和周期性弱可检测性。

2. 提出了一种基于基础可达图的方法（BRG-观测器法）来对标记Petri网系统的四种可检测性进行分析。基于基础可达图（basis reachability graph，BRG），该方法无需枚举与观察结果一致所有标识，只需要求解整数线性方程式即能表达所有的状态。并且BRG的状态数已经被其他研究者证明不大于可达图（reachability graph，RG）的状态数。运用基于BRG的分析方法，提高了分析效率，避免了可检测性的状态空间爆炸问题。

3. 在Petri网框架下，提出了三种新的结构来分析强可检测性和周期性强可检测性，并且通过检验这些结构中的强连通分量来验证可检测性。其中构造这三种结构以及计算强连通分量都是多项式复杂度。与目前的其他方法相比，这三种方法具有更低的算法复杂度。这三种方法不需要计算整个可达空间，也不需要列举与观测一致的所有状态，对于强可检测性或周期性强可检测性的验证更为高效。

4. 针对可检测性对于很多系统要求可能太过严格的问题，提出了C-可检测性性质，该性质只要求系统的关键状态能够被唯一确定。并且根据要求的严苛程度，将该性质划分为了强C-可检测性、弱C-可检测性、周期性强C-可检测性和周期性弱C-可检测性这四类。本论文对这四种C-可检测性给出了严格的形式化定义，并基于BRG提出了高效的验证方法。特别是当系统的关键状态由一组广义互斥约束来描述时，可以通过解决一组整数线性规划问题来验证系统的C-可检测性。

5. 最后，在标记Petri网的框架下，为铁路信号系统的状态估计问题提供一个通用的建模框架，将C-可检测性应用于铁路信号系统中，验证了其在实际系统的有效性。无线闭塞中心切换是铁路信号系统的一个重要功能，它影响铁路的运输效率，可靠性和安全性。本论文以中国列车控制系统中的RBC切换为例，首先使用标记Petri网对RBC切换过程进行建模。然后，运用所提出的方法来分析该切换过程，最终证明了RBC切换过程满足强C-可检测性。

关键词： 可检测性；Petri网；离散事件系统；状态估计；铁路信号系统

Abstract

In many real-world systems, due to limitations of sensors or constraints of the environment, the system dynamics is usually not perfectly known. However, the state information of the system is usually crucial for the purpose of decision making. The state of the system needs to be determined in many applications such as fault diagnosis, state-feedback control, opacity, etc. Due to its importance, the state estimation problem has received considerable attention in the discrete event system (DES) community. Recently, the state estimation problem has been studied systematically in the framework of detectability. The detectability properties characterize the possibility to determine the current and the subsequent states of a system after the observation of a finite number of events generated by the system.

To model and analyze practical systems, powerful DES models are needed to describe the different observation behaviors of the system. Secondly, due to the state explosion problem, analysis methods that rely on exhaustively enumerating all possible states are not applicable for practical systems. It is necessary to develop more efficient and achievable verification methods for detectability. Furthermore, since detectability could be too restrictive in real applications, it may be suitable for some applications but may be too strong in others. Thus, in this thesis, efficient detectability verification methods using Petri nets are investigated, then detectability is extended to a more general definition (C-detectability) that only requires that a given set of crucial states can be distinguished from other states. Formal definitions and efficient verification methods for C-detectability properties are proposed. Finally, C-detectability is applied to the railway signal system to verify the feasibility of this property. The main results of this research are listed as below:

1. Four types of detectability are extended from finite automata to labeled Petri nets. In particular, strong detectability, weak detectability, periodically strong detectability, and periodically weak detectability are formally defined in labeled Petri nets.

2. Based on the notion of basis reachability graph (BRG), a practically efficient approach (the BRG-observer method) to verify the four detectability properties in bounded labeled Petri nets is proposed. Using basis markings, there is no need to enumerate all the markings that are consistent with an observation, as they can be describe by solving an integer linear equation. It has been shown by other researchers that the size of the BRG is usually much smaller than the size of the reachability graph (RG). Thus, the method improves the analysis efficiency and avoids the state space explosion problem.

3. Three novel approaches for the verification of the strong detectability and periodically strong detectability are proposed, which use three different structures whose construction has a polynomial complexity. Moreover, rather than computing all cycles of the structure at hand, which is NP-hard, it is shown that strong detectability can be verified looking at the strongly connected components whose computation also has a polynomial complexity. As a result, they have lower computational complexity than other methods in the literature. Without computing the whole reachability space and without enumerating all the markings consistent with an observation, the three proposed approaches are more efficient for the verification of strong detectability and periodically strong detectability.

4. Detectability could be too restrictive in real applications since it requires that the current and the subsequent states always have to be determined without uncertainty. Thus, detectability is extended to C-detectability that only requires that a given set of crucial states can be distinguished from other states. Four types of C-detectability are defined in the framework of labeled Petri nets: strong C-detectability, weak C-detectability, periodically strong C-detectability, and periodically weak C-detectability. Moreover, efficient approaches are proposed to verify such properties in the case of bounded labeled Petri net systems based on the BRG. Furthermore, if the crucial states are described by a set of generalized mutual exclusion constraints, then C-detectability properties can be verified by solving a set of integer linear programming problems.

5. Finally, a general modeling framework of railway systems is presented for the states estimation using labeled Petri nets. Then, C-detectability is applied to railway signal systems to verify its feasibility in the real-world system. The radio block center (RBC) handover procedure in the railway signal system is an important function of RBC, which affects the transport efficiency, reliability and safety of railways. Taking the RBC handover procedure in the Chinese train control system level 3 (CTCS-3) as an example, the RBC handover procedure is modeled using labeled Petri nets. Then based on the proposed approaches, it is shown that that the RBC handover procedure satisfies strongly C-detectability.

Keywords: Detectability, Petri nets, discrete event systems, state estimation, railway signal systems

Sommario

In molti sistemi ferroviari, a causa delle limitazioni dei sensori o dei vincoli ambientali, la dinamica del sistema è solitamente non perfettamente nota. Tuttavia, la conoscenza dello stato del sistema è tipicamente cruciale allo scopo di prendere decisioni sul sistema stesso. Lo stato del sistema necessita di essere determinato in molte applicazioni quali la diagnosi di guasto, il controllo in retroazione, l'opacità, etc. Data la sua importanza, il problema della stima dello stato ha ricevuto considerevole attenzione nella comunità dei Sistemi ad Eventi Discreti. Recentemente è stato studiato con riferimento al problema della detectabilità. La detectabilità caratterizza la possibilità di determinare lo stato corrente e gli stati successivi di un sistema sulla base dell'osservazione di un numero finito di eventi generati dal sistema.

Nella modellazione e analisi dei sistemi reali, i modelli ad eventi discreti sono necessari per descrivere le diverse osservazioni prodotte dal sistema durante la sua evoluzione. Inoltre, a causa del problema di esplosione dello stato, i metodi di analisi attraverso enumerazione esaustiva di tutti gli stati possibili non sono applicabili a sistemi di dimensioni reali. è necessario pertanto sviluppare dei metodi piùefficaci per la verifica della detectabilità. Inoltre, poichéla detectabilità è una proprietà molto restrittiva, questa puòessere utile in alcune applicazioni ma puòrivelarsi troppo restrittiva in altre. Pertanto in questa tesi, ci si focalizza dapprima su metodi efficienti di verifica della detectabilità usando le Reti di Petri come modello di riferimento. Successivamente, si propone una definizione di detectabilità piùgenerale (C-detectabilità) che fa riferimento ad uno specifico sottoinsieme di stati, imponendo che solo lo stato di tali stati sia perfettamente ricostruito. Alcune proprietà di C-detectabilità sono dapprima formalizzate, quindi metodi efficienti per la loro verifica sono proposti. Infine, la C-detectabilità è applicata al sistema di segnaletica ferroviaria per verificare l'ammissibilità di tali proprietà.

I principali risultati di questa ricerca sono enumerati nei seguenti punti:

1. Le reti di Petri sono un formalismo grafico e matematico applicabile ai sistemi ad eventi discreti ed hanno un potere di modellazione superiore rispetto agli automi a stati finiti. In questa tesi, vengono riproposte con riferimento alle reti di Petri con etichetta quattro nozioni di detectabilità precedentemente formalizzate nell'ambito degli automi a stati finiti. In particolare: la detectabilità forte, la detectabilità debole, la detectabilità periodicamente forte e la detectabilità periodicamente debole.

2. Basandoci sulla nozione di grafo di base di raggiungibilità (BRG: basis reachability

graph), viene proposto un metodo efficace nella pratica (metodo BRG-observer) per la verifica delle suddette proprietà di detectabilità per reti di Petri con etichetta. Grazie alle marcature di base, non vi è necessità di enumerare tutte le marcature che sono consistenti con una osservazione ma è sufficiente risolvere un sistema di equazioni lineari. è stato dimostrato che il BRG ha solitamente dimensioni molto ridotte rispetto al grafo di raggiungibilità (RG: reachability graph). Perciòil metodo migliora l'efficacia dell'analisi ed evita problemi di esplosione dello spazio di stato.

3. Tre nuovi approcci per la verifica della forte detectabilità e della periodicamente forte detectabilità vengono proposte, basandosi su tre diverse strutture il cui calcolo ha complessità polinomiale. Inoltre, piuttosto che calcolare tutti i cicli della struttura di riferimento, che sarebbe NP-hard, si dimostra come la forte detectabilità possa essere verificata guardando le componenti fortemente connesse il cui calcolo ha anch'esso una complessità polinomiale. Come conseguenza, tale approccio ha una complessità computazionale inferiore rispetto ad altri metodi proposti nella letteratura. Senza calcolare l'intero spazio di raggiungibilità e senza enumerare tutte le marcature consistenti con una osservazione, i tre approcci proposti sono piùefficienti per la verifica della detectabilità forte e periodicamente forte.

4. La detectabilità è una proprietà molto restrittiva poichérichiede che gli stati corrente e seguenti siano sempre determinati senza incertezza. Pertanto, in questa tesi si generalizza la definizione di detectabilità introducendo la C-detectabilità che richiede soltanto che un dato insieme di stati cruciali possa essere distinto dagli altri stati. Vengono definiti quattro tipi di C-detectabilità nell'ambito delle reti di Petri con etichetta, ossia la C-detectabilità forte, debole, periodicamente forte e periodicamente debole. Inoltre, vengono proposti degli approcci efficienti per la verifica di tali proprietà nel caso di sistemi di reti di Petri limitati con etichetta basati sul BRG. Inoltre, se gli stati cruciali sono descritti come un insieme di vincoli di mutua esclusione generalizzati, le proprietà di C-detectabilità possono essere verificate risolvendo un insieme di problemi di programmazione lineare intera.

5. Infine, viene considerato un problema di stima di stati cruciali in ambito ferroviario usando le reti di Petri con etichetta come modello di riferimento. Viene quindi studiato un problema di verifica della C-detectabilità in sistemi di segnaletica ferroviaria. La procedura di consegna del centro di blocco radio (RBC: radio block center) è una funzione importante che ha un impatto significativo nell'efficienza dei trasporti, oltre che nella affidabilità e sicurezza ferroviarie. Con riferimento alla procedura di consegna RBC del sistema ferroviario cinese, e in particolare al livello 3 (CTCS-3: Chinese train control system - level 3), viene dapprima modellata la procedura di consegna RBC usando le reti di Petri con etichetta. Successiva-

mente, la C-detectabilità del modello rete di Petri della procedura di consegna è verificata mediante l’approccio proposto.

Keywords: Rilevabilità, reti di Petri, sistemi a eventi discreti, stima dello stato, sistemi di segnaletica ferroviaria

Table of Contents

Chapter 1: Introduction

1.1 Background and Motivation

In recent years, with the rapid development of science and technology, the size of all kinds of systems is larger and larger, and the logic of the systems is more and more complex. Moreover, in many applications, due to the limitations of sensors or the constraints of the environment, the system dynamics is usually not perfectly known. However, the state information of the system needs to be determined for many applications. Thus, state estimation plays an important role in system design and analysis, and it is one of the central problems in systems and control theory. Accurate state information of the system is always necessary for system supervision control [1, 2], fault diagnosis [3, 4] and safety analysis [5, 6]. When any emergency occurs, knowing whether the system has reached a critical state can help the operators to respond and deal with it in a timely and correct manner. Timely detection of the current state of the system can prevent the system from entering a more dangerous situation and causing greater loss. Furthermore, analyzing the state of system is helpful to determine whether there are potential risks in the system specification and development process, which can improve the design of the system and guarantee the safety of the system. Analysis of crucial states of the system is also helpful for fault localization and fault diagnosis. For example, the state estimation of a train is important, if at some point, two trains have to use the same railroad. We need to make sure that we can accurately estimate the state of each train (train's location) in order to avoid collision.

Detectability is a property used to investigate the state of the system [7]. The detectability properties characterize the possibility to determine the current and the subsequent states of a system after the observation of a finite number of events generated by the system. As an important property in the class of state estimation problems, detectability is closely related to many security/privacy properties, e.g., diagnosability, opacity, observability [8–11]. Although such properties are significantly different among them, they all characterize the ability of the system to derive information on the system behavior based on partial information about its evolution. Therefore, the analysis of some of such properties can be reduced to the analysis of other properties. As an example, the problem of establishing if certain faulty states have been reached, can be formulated in terms of a detectability problem [11–13]. Another example is provided by opacity, which describes the capability of a system to hide its states to an outside intruder, namely, the intruder should not be able to realize when certain states, which define the secret, have been reached [6]. Clearly, if a system is detectable, it is not opaque [9, 10, 14]. Meanwhile, attack detection and identification in cyber-physical systems can be viewed as a particular application of detectability analysis [15, 16]. Finally, detectability is a property which reveals to be fundamental in many other practical problems, such as state-feedback control [1, 2], fault prognosis [17, 18] and predictability [19, 20].

Due to its importance, the detectability problems have been extensively investigated in discrete event systems (DESs) [7, 21–24]. However, there are still several problems not addressed:

(1) Most of the literature on detectability is in the framework of finite automata, and there are only few works based on Petri nets, even if Petri nets have stronger modeling power than finite automaton. Moreover, the works using Petri nets are all based on the reachability graph (RG) of the Petri net. However, it is known that the state explosion issue is unavoidable to construct the RG of large-sized systems.

(2) Although some analysis structures with polynomial complexity have been proposed as a tool for the verification of detectability in the automata framework, they require the computation of all cycles of these structures, whose computation complexity is NP-hard. In other words, the complexity of the l verification method is still very high. Thus, it is necessary to search for more efficient verification algorithms.

(3) Detectability could be too restrictive in real applications since it requires that the current and the subsequent states always have to be determined without uncertainty. Imposing detectability could be too rigorous in many real applications, since it typically requires a huge number of sensors associated with transitions. To use detectability in these applications, a more general definition of detectability is needed.

(4) At present, all the works on detectability are focused on theoretical research, not applied to the real-word system. The railway signal system is a safety-critical system, and its current state is closely related with its safety. Thus, in this thesis, problems of detectability verification are investigated in the context of railway signal systems.

Therefore, to solve the above problems, we first study detectability of DESs using Petri nets where some events are unobservable. More precisely, we first formalize the definitions of the detectability properties in the Petri net framework and propose solutions to the detectability verification problem. Given a DES that is modeled by a Petri net, the detectability verification problem consists in determining whether the system satisfies certain detectability properties. Then, we extend the detectability to C-detectability that only requires that a given set of crucial states can be distinguished from other states. Clearly, detectability is a special case of C-detectability, where the set of crucial states is equivalent to the whole state space. The verification problem of C-detectability is investigated. Finally, the C-detectability is applied to railway signal systems to verify its feasibility.

1.2 Detectability Problem in DESs

Discrete-event systems (DESs) are dynamical systems with discrete state-spaces and event-driven dynamics [25]. DESs can clearly describe the relationship between the various parts of the system, and they are extensively used for modeling both logical systems that are inherently event-driven and symbolic abstractions of continuous/hybrid dynamical systems. In many situations, the system under consideration can be modeled as a discrete event system, such as railway systems [26–29], communication systems [30–32], and manufacturing systems [33–36]. In the last decades, a very rich literature on DESs has been produced, since several man-made systems can be efficiently modeled in this framework [7, 25, 37–39]. In particular, a great attention has been devoted to partially observed DESs. Indeed, not all events occurring in the system can be measured, or their measuring could be too costly or unreliable. This leads to a series of fundamental problems such as fault diagnosis [40], state-feedback control under partial state observation [1], opacity [6], etc. This explains why the state estimation problem under partial observation of the system evolution has been extensively investigated in the DES community [6, 7, 37, 39–41], and a huge number of problem formulations have been proposed.

State estimation is one of the most fundamental problems in DESs [7, 42]. State estimation is a method of estimating the state of a dynamical system based on available measurement data (the input and output of the system). If state estimation cannot determine in which state the system is, then it can help us to know the set of all possible states in which the system may be given current and past observations. In many problems, e.g., supervisory control, fault diagnosis and opacity analysis, the state information of the system is usually crucial for the purpose of decision making. However, in many real-world systems, due to the limitations of sensors or the constraints of the environment, the system dynamics is usually not perfectly known. Therefore, state estimation is an important issue in the analysis and design of DES, especially for problems that need to estimate the state of the system based on incomplete observations. In the context of DESs, due to the application of state estimation in many different problems, it has been extensively studied [1, 3, 5, 18, 37, 43]. The problem of state estimation dates back to the study of the property of observability; see, e.g., [37, 44, 45]. In this problem, it is assumed that the system's behavior is only partially-known and we want to infer the state of the system based on incomplete or imperfect information. State estimation of DES has also been investigated for different classes of system models including max-plus automata [46], timed Petri nets [43] and stochastic Petri nets [47]. The state estimation problem is also closely related to many practical problems, including state feedback control problem [1], fault diagnosis problem [3, 4], fault prognosis problem [18], state disambiguation problem [2, 48], information-flow security problem [5, 6], and opacity problem [9].

In the railway signaling system area, the state estimation related problem has also been extensively investigated based on the DES models, including fault diagnosis [49, 50], decision-making [51] and supervisory control [29, 52]. In [52], Giua and Seatzu propose a supervisory control method for railway networks based on Petri nets, and they design a a controller to ensure safeness and liveness of the railway networks. Based on Petri nets, decision-making strategies in fixed-block systems are proposed [49], and diagnosis of the fixed-block systems [51] and diagnosis of multi-track level crossings [50] are studied. In [53], the RBC handover procedure is modeled by timed automata, and the safety of the RBC handover procedure is validated. A binary decision diagram-based symbolic supervisor synthesis method is proposed to ensure time and space efficiency of the high-speed railway station when dealing with a practical supervisory control problem in [29]. Based on proper state transition maps and corresponding relation matrices, an approach of traffic state prediction and conflict detection is proposed in [54].

Recently, the state estimation of DES has been investigated in a more systematic manner in the context of detectability [7, 21–24, 55–58]. The detectability properties characterize the possibility to determine the current and the subsequent states of a system after the observation of a finite number of events generated by the system. Detectability has been studied earlier in DESs, typically denoted as observability [8, 44, 45]. The observability of the current state and initial state is discussed in [45], and whether the current state can be determined periodically is investigated in [44]. The notion of detectability was first proposed and studied in [7] in the deterministic finite automaton framework based on the assumption that the states and the events are partially observable. Shu et al. [7] defined four types of detectability: strong detectability, weak detectability, strong periodic detectability, and weak periodic detectability. The four types of detectability are verified using the notion of observer, whose complexity is exponential w.r.t. the number of states of the system. Polynomial algorithms based on the notion of detector have been proposed in [23] to check strong detectability and strong periodic detectability of a given automaton. Checking weak detectability and weak periodic detectability is proved to be PSPACE-complete [24] and PSPACE-hard for a very restricted class of automata [22]. Finally, Shu and Lin [13, 59] extended detectability to delayed detectability and developed a polynomial algorithm for its verification. Masopust [22] shows that even for very simple DESs that do not have trivial-cycles (the simplest deadlock free DESs), the verification of weak and weak periodic detectability is still intractable.

To meet different requirements, the notion of detectability has been studied more extensively. Initially formulated with reference to the current state, the notion of detectability has been then extended to study initial state estimation [61, 66] and trajectory detection [62]. In [61], a polynomial algorithm based on the notion of reversed verifier has been proposed to verify strong I-detectability. The verification algorithm for trajectory detectability requires polynomial-time using a twin-machine-like construction, while the algorithm for verifying periodic trajectory detectability has exponential complexity [62]. In [21, 42, 55, 67, 68], detectability has been investigated in a stochastic setting. For probabilistic finite-state automata, while checking strong I-detectability is proved to be PSPACE-complete [42], checking A-detectability and AA-detectability are proved to be PSPACE-hard [21] and polynomial time [67], respectively. The notion of detectability has also been extended to modular DESs [20, 69], networked DESs [70], and fuzzy DESs [71]. New types of detectability are proposed, including D-detectability [23], and K-detectability [63]. In [72–75], the enforcement of detectability is studied. We summarize in Table 1-1 a general overview of decidability and complexity results of detectability published up to date in the literature.

In this thesis, the reference formalism is Petri nets. Petri nets are a graphical and mathematical modeling tool with a higher modeling power than finite state automata. Furthermore, using structural analysis and algebraic techniques, a series of problems can be solved more efficiently using Petri nets rather than automata, such as supervisory control [76], fault diagnosis [77], opacity [6]. The observability of unlabeled Petri nets was formalized by Giua and Seatzu [8], including marking observability and strong marking observability. In [65], the authors extend strong detectability and weak detectability in DESs to labeled Petri nets. Strong detectability is proved to be decidable and checking the property is EXPSPACE-hard, while weak detectability is proved to be undecidable. Recently, Zhang and Giua [78] investigate eventual strong detectability and weak approximate detectability on labeled Petri nets. These approaches are all based on the RG of the Petri net. For bounded labeled Petri nets, since their RG is a finite automaton, detectability verification problems are clearly decidable. However, it is known that the state explosion issue is unavoidable to construct the RG of large-sized systems. Therefore, applying the automaton-based approaches to labeled Petri nets may not

Table 1-1 Decidability and complexity results for different detectability verification problems.

Detectability	System model	Decidability	Technique	Complexity	Order	Ref.
Strong detectability	Finite-state automata	Decidable	Detector	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^4)$	[23]
Strong periodic detectability			Detector	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^4)$	[23]
Weak detectability			Observer	PS-C.	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert})$	[24]
Weak periodic detectability			Observer	PS-C.	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert})$	[24]
Strong D-detectability			Detector	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^4)$	[23]
Strong periodic D-detectability			Observer	PS-C.	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert})$	[60]
Weak D-detectability			Observer	PS-C.	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert})$	[60]
Weak periodic D-detectability			Observer	PS-C.	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert})$	[60]
Strong I-detectability			Reversed verifier	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^4)$	[61]
Weak I-detectability			Reversed observer	-	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert})$	[61]
Trajectory detectability			Twin-Machine	Poly.	$\mathcal{O}(\lvert E\rvert^2\lvert X\rvert^5)$	[62]
Periodic trajectory detectability			Observer	-	$\mathcal{O}(\lvert E\rvert 2^{\lvert X\rvert}+ \lvert E\rvert^2\lvert X\rvert^5)$	[62]
Strong K-detectability			K-detector	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^{2K+2})$	[63]
(k1,k2)-detectability			Two-Way Verifier	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^6)$	[64]
N-(k1,k2)-detectability			Augmented automaton	Poly.	$\mathcal{O}(\lvert E\rvert\lvert X\rvert^6)$	[59]
Strong detectability	Unbounded Petri nets		Twin-plant	EXPS-H.	-	[65]
Weak detectability		Undecidable	-	-	-	[65]

E: the set of events of the automaton system; X: the set of states of the automaton system.
Poly.: Polynomial time; PS-C.:PSPACE-complete; EXPS-H.: EXPSPACE-hard.

work. In this thesis, we first extend the four detectability notions to labeled Petri nets and then based on the notion of basis markings, efficient approaches to verifying the four detectability properties are proposed.

Detectability requires that the current and the subsequent states always have to be determined without uncertainty. This requirement is useful in some applications but may be too strong in others, since it typically requires a huge number of sensors associated with transitions. As a result, other properties have been defined in the literature that consist in a relaxation of detectability. For instance, current-state opacity: a system is current-state opaque with respect to a given secret S (defined as a subset of states) if it is never possible to establish if the current state is actually in set S. Compared with detectabilty, current-state opacity only requires to determine whether the current state is in S or not, without precisely reconstructing the current state. To address such an issue, in this thesis we propose different notions of detectability. In particular, we formalize the notion of C-detectability, where “C” stands for “crucial”. C-detectability requires that if the set of markings consistent with a certain observation contains crucial states, then the crucial state has to be determined uniquely after a finite number of observations. In other words, we extend detectability to C-detectability that only requires that a given set of crucial states can be distinguished from the other states. Clearly, detectability is a special case of C-detectability, where the set of crucial states is equivalent to the whole state space.

1.3 Research Contents

In this thesis, we first extend the four detectability notions to labeled Petri nets, and then based on the notion of basis markings, efficient approaches to verifying the four detectability properties are proposed. Then, we extend detectability to C-detectability. In more detail, four types of C-detectability are defined. Based on the notions of basis marking and basis reachability graph (BRG) [77], efficient approaches to verify the above four C-detectability properties are proposed. Finally, we apply the C-detectability to the railway signal system to verify the correctness and effectiveness of the method. The specific content is divided into the following three parts.

1. Research on detectability verification method based on Petri net. In this part, we extend four types of detectability from finite automata to labeled Petri nets, which have larger modeling power than finite automata. Moreover, based on the notion of basis markings, approaches are developed to verify the four detectability properties in a bounded labeled Petri net system.

1) Strong detectability, weak detectability, strong periodic detectability, and weak periodic detectability are formally defined in labeled Petri nets.

2) Efficient approaches to verifying the above four detectability properties in bounded labeled Petri nets are proposed. By constructing the observer of the BRG rather than the RG, the four detectability properties can be verified.

3) Three efficient approaches are provided for the verification of strong detectability and strong periodic detectability using three different structures. The three approaches do not require the calculation of the entire reachability space or the construction of an observer. Moreover, the construction of the three structures has polynomial complexity.

4) A series of numerical examples are presented to compare the efficiency of the proposed methods.

2. Research on the C-detectability based on Petri nets. In this part, we extend detectability to C-detectability that only requires that a given set of crucial states can be distinguished from other states. We define four types of C-detectability in the framework of labeled Petri nets. Moreover, we propose efficient approaches to verify such properties in the case of bounded labeled Petri net systems. Based on the notions of basis marking and BRG, efficient approaches to verify the above four C-detectability properties are proposed.

1) Strong C-detectability, weak C-detectability, periodically strong C-detectability, and periodically weak C-detectability are formally defined in labeled Petri nets.

2) Efficient approaches to verify the above four C-detectability properties in bounded labeled Petri nets are proposed. By constructing the observer of the BRG, the four C-detectability properties can be checked. By constructing the detector of the BRG, strong C-detectability and periodically strong C-detectability can be checked more efficiently.

3) Rather than computing all the elementary cycles in the observer [7, 23], which is NP-hard, we show that C-detectability can be verified by computing strongly connected components [79], which is of polynomial complexity with respect to the size of the observer.

4) Two examples showing the efficiency of the proposed approaches are presented.

3. Application of C-detectability in railway signal system. In this part, we study the C-detectability of the RBC handover. Taking the RBC handover procedure in the Chinese train control system level 3 (CTCS-3) as an example, we first model the RBC handover procedure using labeled Petri nets. Then an efficient approach is used to check C-detectability of the labeled Petri net modeling the handover procedure.

1) According to the specification of the RBC handover procedure in CTCS-3, we build the sequence diagram of the RBC handover procedure.

2) Based on the sequence diagram, the RBC handover procedure is split into three main subsystems modeled by labeled Petri nets, then the whole system model is built by the composition of the basic subsystem models.

3) Using the notion of BRG and observer, the C-detectability properties of the RBC handover procedure are checked efficiently.

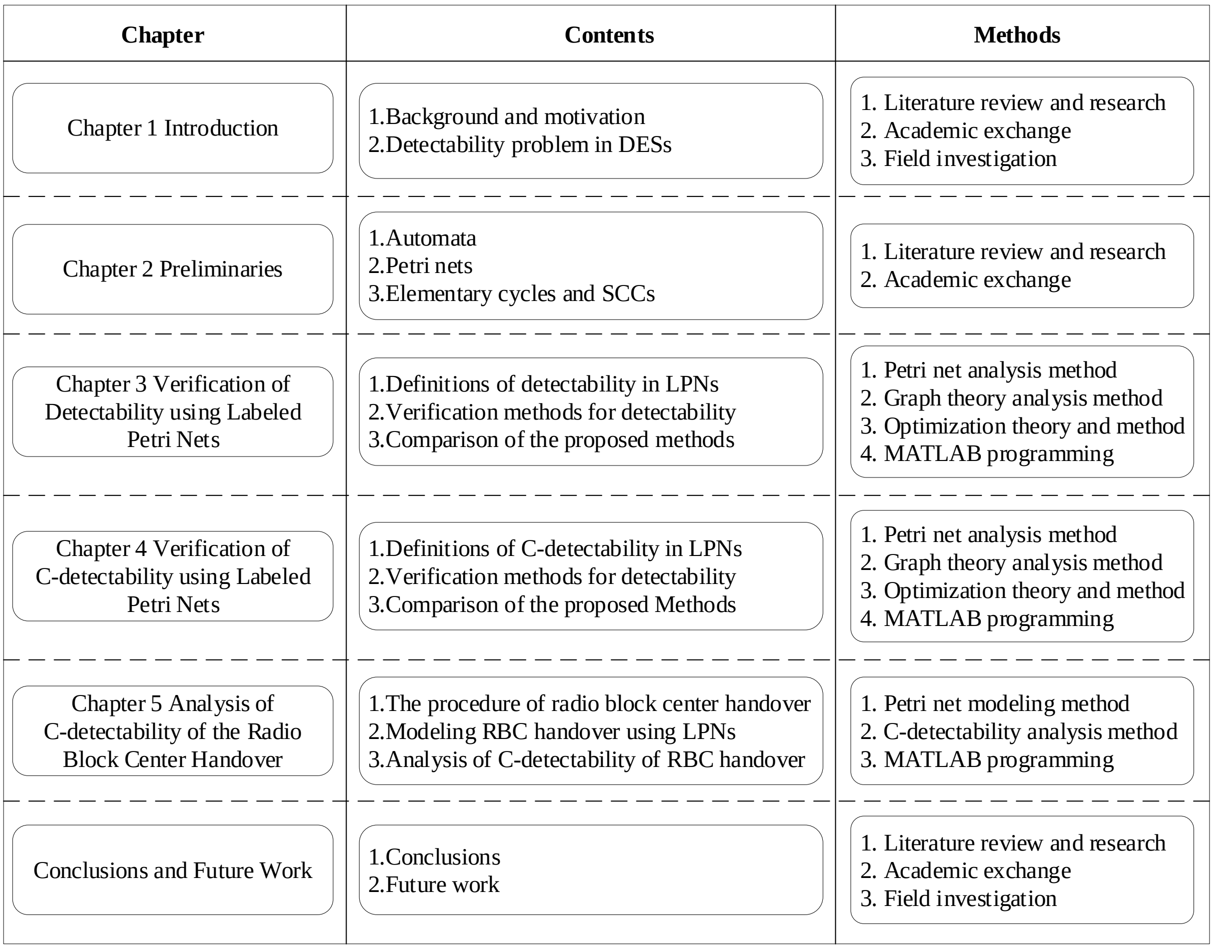
1.4 Organization and Contribution of the Thesis

The thesis focuses on detectability properties and C-detectability properties for systems that are modeled as labeled Petri nets. Moreover, the application of C-detectability is also provided. The organization and main contribution of the thesis are summarized as follows, which are also shown in Fig. 1-1.

Chapter 1: The background and the research motivation of the detectability are presented. The current works and results of detectability are reviewed, and the main research content and technical route of the thesis are explained. We give an overview of the relevant literature on detectability analysis, and position our contributions with respect to these works.

Chapter 2: This chapter presents some basics on automata, Petri nets, elementary cycles and strongly connected components.

Chapter 3: We formalize and analyze the four types of detectability properties for sys-



Chapter	Contents	Methods
Chapter 1 Introduction	1.Background and motivation 2.Detectability problem in DESs	1. Literature review and research 2. Academic exchange 3. Field investigation
Chapter 2 Preliminaries	1.Automata 2.Petri nets 3.Elementary cycles and SCCs	1. Literature review and research 2. Academic exchange
Chapter 3 Verification of Detectability using Labeled Petri Nets	1.Definitions of detectability in LPNs 2.Verification methods for detectability 3.Comparison of the proposed methods	1. Petri net analysis method 2. Graph theory analysis method 3. Optimization theory and method 4. MATLAB programming
Chapter 4 Verification of C-detectability using Labeled Petri Nets	1.Definitions of C-detectability in LPNs 2.Verification methods for detectability 3.Comparison of the proposed Methods	1. Petri net analysis method 2. Graph theory analysis method 3. Optimization theory and method 4. MATLAB programming
Chapter 5 Analysis of C-detectability of the Radio Block Center Handover	1.The procedure of radio block center handover 2.Modeling RBC handover using LPNs 3.Analysis of C-detectability of RBC handover	1. Petri net modeling method 2. C-detectability analysis method 3. MATLAB programming
Conclusions and Future Work	1.Conclusions 2.Future work	1. Literature review and research 2. Academic exchange 3. Field investigation

Fig. 1-1 The structure of the thesis.

tems that are modeled as labeled Petri nets with partial observation on their transitions. We provide four new approaches for the verification of such detectability properties using four different structures, and analyze their computational complexity.

Chapter 4: In order to focus more on the estimation of crucial states of the system, we propose four types of C-detectability in the framework of labeled Petri nets: strong C-detectability, weak C-detectability, periodically strong C-detectability, and periodically weak C-detectability. Then, the approaches are proposed to verify such properties for bounded labeled Petri net systems.

Chapter 5: We investigate the C-detectability of the RBC handover. The RBC handover procedure in the Chinese train control system level 3 is modeled by labeled Petri nets. Then, the efficient approaches proposed in Chapter 4 are used to check C-detectability of the labeled Petri net modeling the handover procedure.

Conclusion and Future work: We conclude the thesis and present potential directions for future work.

Chapter 2: Preliminaries

In this section we recall the formalisms used in this thesis and some results on state estimation in automata and Petri nets [25, 77, 80].

2.1 Automata

2.1.1 Automaton models

A nondeterministic finite (state) automaton (NFA) is a 5-tuple $A = (X, E_A, f, x_0, X_m)$, where

- $X = \{x_0, x_1, ..., x_n\}$ is the finite set of states,
- $E_A = \{a, b, ...\}$ is the finite set of events,
- $x_0 \in X$ is the initial state,
- $X_m \subseteq X$ is the set of marked states,
- $f : X \times E_\varepsilon \to 2^X$ is the transition relation.

$E_\varepsilon = E_A \cup \{\varepsilon\}$ and ε is the empty word. If $X_m = \emptyset$, the NFA is denoted by $A = (X, E_A, f, x_0)$. The transition relation f can be extended to $f : X \times E_\varepsilon^* \to 2^X$ in a standard manner. Given an event sequence $w \in E_\varepsilon^*$, if $f(x_0, w)$ is defined in A, $f(x_0, w) \neq \emptyset$ is the set of states reached in A from x_0 with w occurring. On the contrary, if $f(x_0, w)$ is not defined in A, we denote $f(x_0, w) = \emptyset$.

Given a subset of states $Y \subseteq X$, the language generated from Y is $\mathcal{L}(A, Y) = \{w \in E_\varepsilon^* | \exists x \in Y : f(x, w)!\}$. If $Y = \{x\}$ is a singleton, the generated language is simply denoted by $\mathcal{L}(A, x)$. The language generated from the initial states is denoted by $\mathcal{L}(A)$.

Example 2.1 Fig. 2-1 shows the graphical structure of a NFA $A = (X, E_A, f, x_0)$. $X = \{0, 1, 2, 3, 4\}$, $E_A = \{a, b\}$ and $x_0 = 0$. The transition relation is: $2 \in f(0, \varepsilon)$, $1, 3 \in f(0, a)$, $1 \in f(1, b)$, $4 \in f(2, a)$, $4 \in f(3, b)$ and $4 \in f(4, b)$. Let an event sequence be $w = abbb$, by Fig. 2-1, we have that $1, 4 \in f(0, w)$, thus $w \in \mathcal{L}(A)$. ◇

2.1.2 Automata operation

In this section, we introduce two tools used in the thesis: observer and detector, which are useful in the verification of the properties of interest.

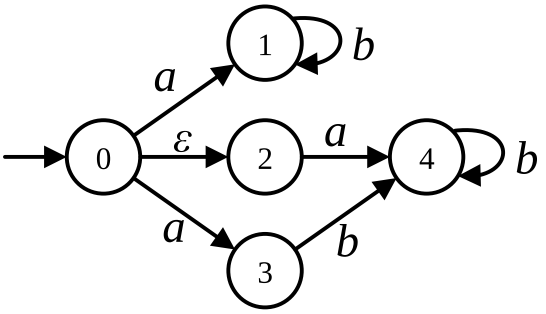


Fig. 2-1 The NFA in Example 2.1.

2.1.2.1 Observer

Given an NFA, its observer is a deterministic finite (state) automaton (DFA). Each state of the observer is a subset of states of X in which the NFA resides after a certain event sequence has occurred. Thus, the observer is also called the equivalent DFA of the given NFA.

Given an NFA $A = (X, E_A, f, x_0, X_m)$, the unobservable reach of each state $x \in X$ is

$$UR(x) = \{y \in X | \exists w \in \{\varepsilon\}^* : y \in f(x, w)\}$$

the set of states that can be reached from x by an empty word. This definition can be extended to a set of states $Y \subseteq X$ by

$$UR(Y) = \bigcup_{x \in Y} UR(x).$$

Let a NFA be $A = (X, E_A, f, x_0)$, its observer is denoted by $A_o = (\mathcal{X}, E_A, f_o, \hat{X}_0)$, where $\mathcal{X} \subseteq 2^X$ is a finite set of states. The initial state of A_o is $\hat{X}_0 = UR(x_0)$. The event set of the observer is E_A. The transition function $f_o : \mathcal{X} \times E \to \mathcal{X}$ is defined in Algorithm 1.

The observer can be constructed following the procedure in Algorithm 1, which works as follows. First, the initial node $\hat{X}_0 = UR(x_0)$ is added to a set of unchecked nodes $\mathcal{X}_{new}$ (Steps 1 to 2). Then, for all nodes $\hat{X}$ in $\mathcal{X}_{new}$, consider all the states x in $\hat{X}$. Compute the set of states $\hat{X}_t$ that can be reached from x by firing e, and then compute the unobservable reach $\hat{X}'$ of the set $\hat{X}_t$ (Steps 3 to 6). Next, add an edge from $\hat{X}$ to $\hat{X}'$ labeled e (Step 7). If $\hat{X}'$ does not exist in the observer, then add it to $\mathcal{X}$ and $\mathcal{X}_{new}$ (Steps 8 to 10). This procedure runs iteratively until there is no unchecked node in $\mathcal{X}_{new}$.

According to Algorithm 1, in the worst case, there are $2^n - 1$ states in the observer, where n is the number of states of A. Thus, the complexity of computing the observer is $\mathcal{O}(2^n)$.

Algorithm 1 Construction of the observer

```
Input: A NFA $A = (X, E_A, f, x_0)$.
Output: The corresponding observer $A_o = (\mathcal{X}, E_A, f_o, \hat{X}_0)$.
$\hat{X}_0 := UR(x_0)$,
$\mathcal{X} := \{\hat{X}_0\}$, $\mathcal{X}_{new} := \{\hat{X}_0\}$.
for all nodes $\hat{X} \in \mathcal{X}_{new}$, do
    for all $e \in E_A$, do
        $\hat{X}_t := \{x \in X | \exists x' \in \hat{X} : x \in f(x', e)\}$,
        $\hat{X}' := UR(\hat{X}_t)$,
        $f_o(\hat{X}, e) := \hat{X}'$,
        if $\hat{X}' \notin \mathcal{X}$, then
            $\mathcal{X} := \mathcal{X} \cup \{\hat{X}'\}$, $\mathcal{X}_{new} := \mathcal{X}_{new} \cup \{\hat{X}'\}$.
        end if
    end for
    $\mathcal{X}_{new} := \mathcal{X}_{new} \setminus \{\hat{X}\}$.
end for
```

Example 2.2 Consider the NFA A in Fig. 2-1, where $E_A = \{a, b\}$ and $x_0 = 0$. Since $2 \in f(0, \varepsilon)$, $UR(x_0) = \{0, 2\}$. Now, we use Algorithm 1 to build the observer of the NFA. First, by Step 1, $\hat{X}_0 = UR(x_0) = \{0, 2\}$. For $\hat{X}_0$, only event a is enabled and its execution leads to three different states 1, 3, 4, since $1, 3 \in f(0, a), 4 \in f(2, a)$. By Steps 5 to 7, node $\hat{X}_1$ can be reached from node $\hat{X}_0$, where $\hat{X}_1 = \{1, 3, 4\}$. Namely, $\hat{X}_1 = f_o(\hat{X}_0, a)$. Starting from $\hat{X}_1$, only event b may be executed. The execution of b leads to states 1 and 4. Thus, $\hat{X}_2 = \{1, 4\}$ and $\hat{X}_2 = f_o(\hat{X}_1, b)$. For $\hat{X}_2$, only event b is enabled and its execution also leads to states 1 and 4. Thus, $\hat{X}_2 = f_o(\hat{X}_2, b)$. Therefore, the obtained observer of the NFA A is A_o, which is shown in Fig. 2-2. Clearly, The observer A_o is a DFA. ◇

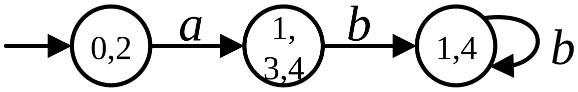


Fig. 2-2 The observer of the NFA in Fig. 2-1.

2.1.2.2 Detector

The detector of a given automaton is a NFA, whose size is polynomial with respect to the number of states of the considered automaton [23]. Given a NFA $A = (X, E_A, f, x_0)$, we denote $A_d = (Q, E_A, f_d, q_0)$ the detector of A, where $Q \subseteq 2^X$ is a finite set of states. The initial state of A_d is $q_0 = UR(x_0)$, and the other states of A_d are subsets of X with cardinality at most equal to 2. The event set of the detector is E_A. The transition function $f_d : Q \times E \to 2^Q$ is defined in Algorithm 2.

Algorithm 2 Construction of the detector

```
Input: A NFA $A = (X, E_A, f, x_0)$.
Output: The corresponding detector $A_d = (Q, E_A, f_d, q_0)$.
1:  $q_0 := UR(x_0)$,
2:  $Q := \{q_0\}$, $Q_{new} := \{q_0\}$.
3:  for all nodes $q \in Q_{new}$, do
4:      for all $e \in E_A$, do
5:          $q_e := \{x \in X | \exists x' \in q, x \in f(x', e)\}$,
6:          $q_t := UR(q_e)$,
7:          if $|q_t| = 1$, then
8:              $f_d(q, e) := \{q_t\}$,
9:              if $q_t \notin Q$, then
10:                 $Q := Q \cup \{q_t\}$, $Q_{new} := Q_{new} \cup \{q_t\}$.
11:             end if
12:         else
13:             $f_d(q, e) := \emptyset$,
14:             for all $q' \subseteq q_t$ with $|q'| = 2$, do
15:                 $f_d(q, e) := f_d(q, e) \cup \{q'\}$,
16:                 if $q' \notin Q$, then
17:                     $Q := Q \cup \{q'\}$, $Q_{new} := Q_{new} \cup \{q'\}$.
18:                 end if
19:             end for
20:         end if
21:     end for
22:     $Q_{new} := Q_{new} \setminus \{q\}$.
23: end for
```

The procedure to construct the detector of a given NFA is summarized in Algorithm 2, which works as follows. First, the initial node $q_0 = UR(x_0)$ is added to a set of unchecked nodes Q_{new} (Steps 1 to 2). Then, for all nodes q in Q_{new}, consider all the states x in q. Compute the set of states q_e that can be reached from x by firing e, and then compute the unobservable reach q_t of the set q_e (Steps 3 to 6). If the cardinality of q_t is equal to 1, then add an edge from q to q_t labeled e (Steps 7 to 11). Else, compute all the strict subsets $q' \subseteq q_t$ with $|q'| = 2$ as new nodes, then add an edge from q to q' labeled e (Steps 12 to 15). If q' does not exist in the detector, then add it to Q and Q_{new} (Steps 16 to 18). This procedure runs iteratively until there is no unchecked node in Q_{new}.

According to Algorithm 2, in the worst case, the detector has n states whose cardinality is one, and $\frac{n\times(n-1)}{2}$ states whose cardinality is two, where n is the number of states of A. Thus, the number of states of the detector is bounded by $\frac{n\times(n+1)}{2}$. Moreover, the number of transitions is bounded by $(\frac{n\times(n+1)}{2})^2 \times e$, where e is the number of events of A. Therefore, the complexity of constructing it is polynomial w.r.t. the size of the BRG, which is $\mathcal{O}(en^4)$.

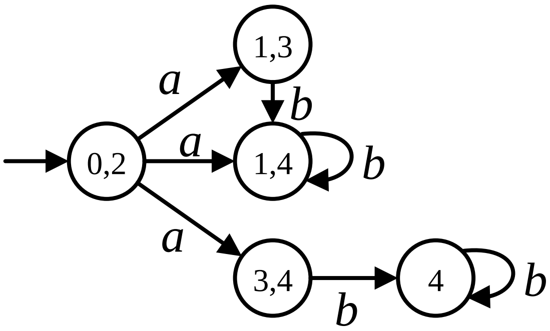


Fig. 2-3 The detector of the NFA in Fig. 2-1.

Example 2.3 Consider again the NFA A in Fig. 2-1, where $E_A = \{a, b\}$ and $x_0 = 0$. Now, we use Algorithm 2 to build the detector of the NFA. First, by Step 1, $q_0 = UR(x_0) = \{0, 2\}$. For q_0, only event a is enabled and its execution leads to three different states 1, 3, 4. By Steps 5 to 17, three different nodes can be reached from node q_0, each one containing two states. Namely, $q_1, q_2, q_3 \in f_d(q_0, a)$, where $q_1 = \{1, 3\}, q_2 = \{1, 4\}$ and $q_3 = \{3, 4\}$. Starting from q_1, only event b may be executed. The execution of b leads to states 1 and 4. Thus, $q_2 \in f_d(q_1, b)$. For q_2, the execution of b also leads to states 1 and 4, i.e., $q_2 \in f_d(q_2, b)$. For q_3, $4 \in f(3, b)$ and $4 \in f(4, b)$, thus $q_4 \in f_d(q_3, b)$ and $q_4 = \{4\}$. Finally, we can obtain the detector A_d of the NFA A, which is shown in Fig. 2-3. Clearly, The detector A_d is also a NFA without the empty word. $\diamond$

2.2 Petri nets

2.2.1 Petri net models

A Petri net is a structure $N = (P, T, Pre, Post)$, where

- P is a set of m places, graphically represented by circles;
- T is a set of n transitions, graphically represented by bars;
- $Pre : P \times T \to \mathbb{N}$ is the pre-incidence functions that specify the arcs directed from places to transitions.

- $Post : P \times T \to \mathbb{N}$ is the post-incidence functions that specify the arcs directed from transitions to places.

Note that in this thesis, we use $\mathbb{N}$ and $\mathbb{Z}$ to denote the sets of nonnegative integers and integers, respectively. The incidence matrix of N is denoted by $C = Post - Pre$. A Petri net is acyclic if there are no oriented cycles.

A marking is a vector $M : P \to \mathbb{N}$ that assigns to each place a non-negative integer number of tokens, graphically represented by black dots. The marking of place p is denoted by $M(p)$. A marking is also denoted by $M = \sum_{p \in P} M(p) \cdot p$. A Petri net system $\langle N, M_0 \rangle$ is a net N with initial marking M_0.

A transition t is enabled at marking M if $M \geq Pre(\cdot, t)$ and may fire yielding a new marking $M' = M + C(\cdot, t)$. We write $M[\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j1} \cdots t_{jk}$ is enabled at M, and $M[\sigma\rangle M'$ to denote that the firing of σ yields M'. The set of all enabled transition sequences in N from marking M is $L(N, M) = \{\sigma \in T^* | M[\sigma\rangle\}$. Given a transition sequence $\sigma \in T^*$, the function $\pi : T^* \to \mathbb{N}^n$ associates with σ the Parikh vector $y = \pi(\sigma) \in \mathbb{N}^n$, i.e., $y(t) = k$ if transition t appears k times in σ. Given a sequence of transitions $\sigma \in T^*$, its prefix, denoted by $\sigma' \preceq \sigma$, is a string such that $\exists \sigma'' \in T^* : \sigma'\sigma'' = \sigma$. The length of σ is denoted by $|\sigma|$.

A marking M is reachable in $\langle N, M_0 \rangle$ if there exists a transition sequence σ such that $M_0[\sigma\rangle M$. The set of all markings reachable from M_0 defines the reachability set of $\langle N, M_0 \rangle$, denoted by $R(N, M_0)$. A Petri net system is bounded if there exists a nonnegative integer $k \in \mathbb{N}$ such that for any place $p \in P$ and any reachable marking $M \in R(N, M_0)$, $M(p) \leq k$ holds. Given a bounded Petri net, its reachability set $R(N, M_0)$ can be graphically represented by the reachability graph (RG) that is a directed graph whose nodes are reachable markings and arcs are tagged by transitions in T. If $M[t\rangle M'$ and $M, M' \in R(N, M_0)$, then M and M' are two nodes in the RG and there is an arc from M to M' tagged with t.

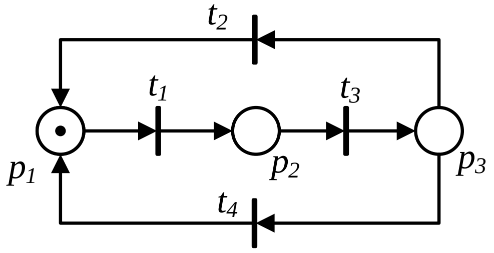


Fig. 2-4 A Petri net system.

Example 2.4 Consider the Petri net system in Fig. 2-4. Let the Petri net system be $\langle N, M_0 \rangle$ with $M_0 = p_1$ (or denoted as $M_0 = [1\ 0\ 0]^T$). In the net $N = (P, T, Pre, Post)$,

$P = \{p_1, p_2, p_3\}, T = \{t_1, t_2, t_3, t_4\}$,

$$Pre = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, Post = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

and the incidence matrix

$$C = \begin{bmatrix} -1 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 1 & -1 \end{bmatrix}.$$

At M_0, $M_0 \geq Pre(\cdot, t_1)$, thus, t_1 is enabled at M_0 and $M_1 = M_0 + C(\cdot, t_1) = [0\ 1\ 0]^T$. Let a transition sequence $\sigma = t_1 t_3 t_2 t_1$, which are enabled at M_0, then $y = \pi(\sigma) = [2\ 1\ 1\ 0]^T$. The maximal number of tokens in a place is 1 and thus the Petri net system is bounded. The RG of the Petri net system is shown in Fig. 2-5. ◇

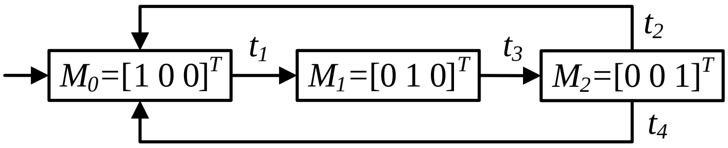


Fig. 2-5 The RG of the Petri net system in Fig. 2-4.

2.2.2 Labeled Petri net models

A labeled Petri net (LPN) system is a 4-tuple $G = (N, M_0, E, \ell)$, where

- $\langle N, M_0 \rangle$ is a Petri net system;
- E is the alphabet (a set of labels);
- $\ell : T \to E \cup \{\varepsilon\}$ is the labeling function.

The labeling function ℓ assigns to each transition $t \in T$ either a symbol from E or the empty word ε. Therefore, the set of transitions can be partitioned into two disjoint sets $T = T_o \dot{\cup} T_u$, where $T_o = \{t \in T | \ell(t) \in E\}$ is the set of observable transitions with $|T_o| = n_o$, and $T_u = T \setminus T_o = \{t \in T | \ell(t) = \varepsilon\}$ is the set of unobservable transitions with $|T_u| = n_u$. Given a marking $M \in R(N, M_0)$, we define

$$UR(M) = \{M' \in \mathbb{N}^m | M[\sigma_u\rangle M', \sigma_u \in T_u^*\}$$

its unobservable reach. Namely, the set of markings reachable from M through unobservable transition sequences. We denote as $L(N, M_0) = \{\sigma \in T^* | M_0[\sigma\rangle\}$ the set of transition sequences enabled at initial marking in $R(N, M_0)$. Finally we denote as

$$L^{\infty}(G) = \{\sigma \in T^* | \sigma \in L(N, M_0) \wedge |\sigma| \text{ is infinite}\}$$

the set of transition sequences of infinite length that are enabled at initial marking in $R(N, M_0)$. The labeling function can be extended to sequences $\ell : T^* \to E^*$ as

$$\ell(\sigma t) = \begin{cases} \ell(\sigma)\ell(t) & \text{if } t \in T_o, \\ \ell(\sigma) & \text{otherwise,} \end{cases}$$

where $\sigma \in T^*$ and $t \in T$. Given a set of markings $Y \subseteq R(N, M_0)$, the language generated by G from Y is

$$\mathcal{L}(G, Y) = \bigcup_{M \in Y} \{w \in E^* | \exists \sigma \in L(N, M) : w = \ell(\sigma)\}.$$

In particular, $\mathcal{L}(G, \{M_0\}) = \{w \in E^* | \exists \sigma \in L(N, M_0) : w = \ell(\sigma)\}$ is the language generated by G, which is also denoted by $\mathcal{L}(G)$. Let $w \in \mathcal{L}(G)$ be an observed word. We denote as

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m | \exists \sigma \in L(N, M_0) : M_0[\sigma\rangle M, \ell(\sigma) = w\} \tag{2-1}$$

the set of markings consistent with w. When $|\mathcal{C}(w)| \neq 1$, markings in $\mathcal{C}(w)$ are confusable since any of them could be the current marking given the observation w; otherwise, we say that the markings in $\mathcal{C}(w)$ are distinguishable.

Given an LPN system $G = (N, M_0, E, \ell)$ and the set of unobservable transitions T_u, the T_u-induced subnet $N' = (P, T', Pre', Post')$ of N is the net resulting by removing all transitions in $T \setminus T_u$ from N, where Pre' and $Post'$ are the restrictions of Pre, $Post$ to T_u, respectively. The incidence matrix of the T_u-induced subnet is denoted by $C_u = Post' - Pre'$.

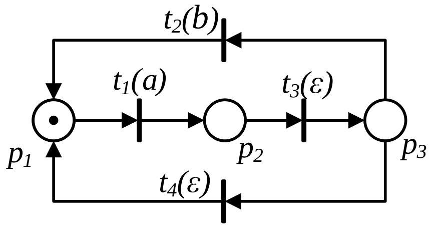


Fig. 2-6 An LPN system.

Example 2.5 Consider the LPN system $G = (N, M_0, E, \ell)$ in Fig. 2-6, where $E = \{a, b\}$, $\ell(t_1) = a$, $\ell(t_2) = b$, and $\ell(t_3) = \ell(t_4) = \varepsilon$. Thus, $T_o = \{t_1, t_2\}$ and $T_u = \{t_3, t_4\}$.

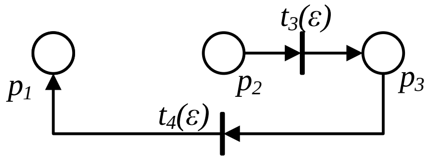


Fig. 2-7 The T_u-induced subnet of the LPN system in Fig. 2-6.

The RG of the LPN system is shown in Fig. 2-5. Since $M_1[t_3\rangle M_2$ and $M_1[t_3t_4\rangle M_0$, $UR(M_1) = \{M_0, M_1, M_2\}$. Given an observation $w = a$, $\mathcal{C}(a) = \{M_0, M_1, M_2\}$. Let a transition sequence be $\sigma = (t_1t_3t_2)^*$, clearly, σ is enabled at M_0, thus $\sigma \in L(N, M_0)$ and $\sigma \in L^\infty(G)$. Then the observation $w = \ell(\sigma) = (ab)^*$ and $w \in \mathcal{L}(G)$. The T_u-induced subnet $N' = (P, T', Pre', Post')$ of N is shown in Fig. 2-7, and the incidence of N' is

$$C_u = \begin{bmatrix} 0 & 1 \\ -1 & 0 \\ 1 & -1 \end{bmatrix}.$$

Clearly, the T_u-induced subnet is acyclic since there is no cycle in N'. ◇

2.2.3 Basis Markings

The basis reachability graph (BRG) of an LPN system summarizes in a compact form the information contained in its RG. Each node in the BRG represents not only the marking associated with it, but also its unobservable reach. In addition, only markings (called basis markings) reachable through observable transitions and the unobservable transition sequences whose firing is necessary to enable the observable transitions, are enumerated. As a consequence, the size of the BRG is usually much smaller than that of the RG, thus the BRG has been efficiently used to verify some properties [6]. Before providing the algorithm for its construction, we recall some results on state estimation using basis markings proposed in [6, 77].

Definition 2.1 Given a marking M and an observable transition $t \in T_o$, we denote as

$$\Sigma(M, t) = \{\sigma \in T_u^* | M[\sigma\rangle M', M' \geq Pre(\cdot, t)\}$$

the set of explanations of t at M and

$$Y(M, t) = \{y_u \in \mathbb{N}^{n_u} | \exists \sigma \in \Sigma(M, t) : y_u = \pi(\sigma)\}$$

the set of e-vectors. ◇

Thus $\Sigma(M,t)$ is the set of unobservable transition sequences whose firing at M enables t. Among all the explanations, to provide a compact representation of the reachability set we are interested in finding the minimal ones, i.e., the ones whose firing vector is minimal.

Definition 2.2 Given a marking M and an observable transition $t \in T_o$, we denote as

$$\Sigma_{min}(M,t) = \{\sigma \in \Sigma(M,t) | \nexists \sigma' \in \Sigma(M,t) : \pi(\sigma') \lneqq \pi(\sigma)\}$$

the set of minimal explanations of t at M and

$$Y_{min}(M,t) = \{y_u \in \mathbb{N}^{n_u} | \exists \sigma \in \Sigma_{min}(M,t) : y_u = \pi(\sigma)\}$$

the corresponding set of minimal e-vectors. ◇

Different approaches can be applied to computing $Y_{min}(M,t)$ [77, 81, 82]. In particular, when the T_u-induced subnet is acyclic the approach proposed by Cabasino et al. [77] only requires algebraic manipulations. Note that since a given place may have two or more unobservable input transitions, i.e., the T_u-induced subnet is not backward conflict free, the set of minimal explanations is not necessarily a singleton.

Definition 2.3 Given an LPN system $G = (N, M_0, E, \ell)$ whose T_u-induced subnet is acyclic, its basis marking set $\mathcal{M}_b$ is defined as follows:

- $M_0 \in \mathcal{M}_b$;
- If $M \in \mathcal{M}_b$, then $\forall t \in T_o, \forall y_u \in Y_{min}(M,t)$,

$$M' = M + C(\cdot,t) + C_u \cdot y_u \Rightarrow M' \in \mathcal{M}_b.$$

A marking $M_b \in \mathcal{M}_b$ is called a basis marking of G. ◇

The set of basis markings contains the initial marking and all other markings that are reachable from a basis marking by firing a transition sequence $\sigma_u t$, where $t \in T_o$ is an observable transition and σ_u is a minimal explanation of t at M. Note that since $y_u \in Y_{min}(M,t)$, t is enabled at some marking in the unobservable reach of M.

By Definition 2.3, basis markings and BRG can be recursively computed from the initial marking if the T_u-induced subnet is acyclic. Given an LPN system $G = (N, M_0, E, \ell)$, its BRG is an NFA, where each state is a basis marking, the set of events is the alphabet of the LPN system, and there is no transition labeled with the empty word. The procedure to construct the BRG of an LPN system is summarized in Algorithm 3, which works as follows.

Algorithm 3 Computation of BRG

Input: A bounded LPN system $G = (N, M_0, E, \ell)$

Output: The corresponding BRG $B = (\mathcal{M}_b, E, f, M_0)$.

```
1: $\mathcal{M}_b := \{M_0\}, \mathcal{M}_{new} := \{M_0\}$.
2: for all nodes $M \in \mathcal{M}_{new}$, do
3:     for all $t$ s.t. $Y_{min}(M, t) \neq \emptyset$ do
4:         for all $y \in Y_{min}(M, t)$ do
5:             $M' := M + C_u \cdot y + C(\cdot, t)$;
6:             $f(M, \ell(t)) := f(M, \ell(t)) \cup \{M'\}$;
7:             if $M' \notin \mathcal{M}_b$, then
8:                 $\mathcal{M}_b := \mathcal{M}_b \cup \{M'\}, \mathcal{M}_{new} := \mathcal{M}_{new} \cup \{M'\}$;
9:             end if
10:        end for
11:    end for
12:    $\mathcal{M}_{new} := \mathcal{M}_{new} \setminus \{M\}$.
13: end for
```

First, the initial node M_0 is added to a set of unchecked nodes $\mathcal{M}_{new}$ (Step 1). Then, for all markings M in $\mathcal{M}_{new}$, if at marking M there exists an observable transition t for which a minimal explanation exists, then we compute the markings reached firing t and its minimal explanations (Steps 2 to 4). Let M' be one of such markings. Add an edge from M to M' labeled $\ell(t)$ (Steps 5 to 6). If such a node does not exist in the BRG, then add it to $\mathcal{M}_b$ and $\mathcal{M}_{new}$ (Steps 7 to 9). This procedure runs iteratively until there is no unchecked node in $\mathcal{M}_{new}$. Clearly, $\mathcal{M}_b \subseteq R(N, M_0)$ and $\mathcal{L}(B) = \mathcal{L}(G)$.

We briefly analyze the complexity of Algorithm 3 in terms of number of basis markings enumerated through the procedure. The complexity of constructing a BRG highly depends on the structure of the net system. If all transitions are observable, then the set of basis markings is identical to the set of reachable markings, i.e., $\mathcal{M}_b = R(N, M_0)$. Although in the worst case constructing the BRG has the same complexity as constructing the RG, in practical cases the number of basis markings is much smaller than the number of reachable markings [6, 77, 83]. Therefore, the proposed BRG-based approaches usually have significant advantages over the RG-based approaches.

Note that to apply the BRG approach, two assumptions are made:

1) the LPN system is bounded, and

2) its T_u-induced subnet is acyclic.

Assumption 1) guarantees that the number of basis markings is finite. Assumption 2) allows us to iteratively compute the basis markings and the set of markings that are reachable from a basis marking using the state equation in Proposition 2.1.

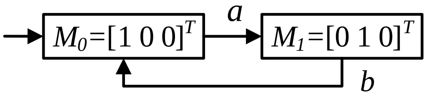


Fig. 2-8 The BRG of the LPN system in Fig. 2-6.

Example 2.6 Consider the LPN system in Fig. 2-6, where transitions t_3 and t_4 are unobservable, and transitions t_1 and t_2 are labeled by a and b, respectively. At the initial marking $M_0 = [1\ 0\ 0]^T$, the minimal explanations of t_1 is $\Sigma_{min}(M_0, t_1) = \{\varepsilon\}$, and thus $Y_{min}(M_0, t_1) = \{\vec{0}\}$. The corresponding basis marking is $M_0 + C(\cdot, t_1) = M_1 = [0\ 1\ 0]^T$. At M_1, the minimal explanation of t_2 is $\Sigma(M_1, t_2) = \{t_3\}$, and thus $Y_{min}(M_1, t_2) = \{[1\ 0]^T\}$. The basis marking obtained is $M_1 + C(\cdot, t_2) + C_u \cdot [1\ 0]^T = M_0$. By Algorithm 3, the set of basis markings of G is $\mathcal{M}_b = \{M_0, M_1\}$, and the obtained BRG is shown in Fig. 2-8. ◇

We denote

$$\mathcal{C}_b(w) = \{M_b \in \mathcal{M}_b | \exists w \in \mathcal{L}(B) : M_b \in f(M_0, w)\}$$

the set of basis markings consistent with a given observation $w \in \mathcal{L}(G)$.

Proposition 2.1 [77] Let $G = (N, M_0, E, \ell)$ be an LPN system whose T_u-induced subnet is acyclic, and $w \in \mathcal{L}(G)$ an observation generated by G. The following two statements hold:

1. A marking M is reachable iff there exists a basis marking $M_b \in \mathcal{M}_b$ such that

$$M = M_b + C_u \cdot y_u \tag{2-2}$$

has a nonnegative solution $y_u \in \mathbb{N}^{n_u}$.

2.

$$\mathcal{C}(w) = \bigcup_{M_b \in \mathcal{C}_b(w)} UR(M_b) \tag{2-3}$$

Statement 1 of Proposition 2.1 implies that any solution $y_u \in \mathbb{N}^{n_u}$ of Eq. (2-2) corresponds to the firing vector of a transition sequence σ enabled at M_b, i.e., $M_b[\sigma\rangle$ and $\pi(\sigma) = y_u$. Under the assumption that the T_u-induced subnet is acyclic, the unobservable reach $UR(M_b)$

of M_b can be re-written as

$$UR(M_b) = \{M \in \mathbb{N}^m | M = M_b + C_u \cdot y_u,\ y_u \in \mathbb{N}^{n_u}\}. \tag{2-4}$$

According to Statement 2 and Eq. (2-4), the set of markings consistent with an observation can be characterized using linear algebra rather than enumerating all the reachable markings.

Example 2.7 Consider again the LPN system in Fig. 2-6, whose RG is shown in Fig. 2-5 and BRG is shown in Fig. 2-8. $\mathcal{M}_b = \{M_0, M_1\}$. There exists $y_u = [1\ 0]^T$ such that $M_2 = [0\ 0\ 1]^T = M_1 + C_u \cdot y_u$. According to Fig. 2-7, the T_u-induced subnet is acyclic, thus M_2 is reachable from M_1. Since $\mathcal{C}_b(a) = \{M_1\}$ and $UR(M_1) = \{M_0, M_1, M_2\}$, $\mathcal{C}(a) = \{M_0, M_1, M_2\}$. ◇

2.3 Elementary cycles and strongly connected components

In this subsection, we recall the notions of elementary cycles and strongly connected components in a directed graph.

Definition 2.4 [Elementary cycles] An elementary cycle in a directed graph is a path $\gamma = v_1 e_1 v_2 \ldots v_k e_k v_1$, where v_i is a node and e_i is an edge with $i \in \{1, 2, \ldots, k\}$, no node appears twice, apart from the first and the last node that coincide. The corresponding observation of the elementary cycle is $w = e_1 e_2 \ldots e_k$. A node v_i contained in the elementary cycle γ is denoted by $v_i \in \gamma$. ◇

Finding all the elementary cycles in a directed graph is known to be an NP-hard problem. In this thesis, the algorithm in [84] is used to find all the elementary cycles. The algorithm has a time bound of $\mathcal{O}((n + e)(c + 1))$, where n, e and c are the number of nodes, edges and elementary cycles, respectively. Note that in [84] the author points out that the number of elementary cycles in a directed graph can grow faster with the number n of nodes than the exponential 2^n. Hereafter, elementary cycles are simply referred as cycles.

A directed graph $\mathcal{G}$ is strongly connected, if for each pair of its nodes n_i, n_j, there exist directed paths $n_i \to n_j$ and $n_j \to n_i$.

Definition 2.5 [Strongly connected components] In a directed graph $\mathcal{G}$, the subgraphs $\mathcal{G}_i$ of $\mathcal{G}$ are called strongly connected components (SCCs) of $\mathcal{G}$ if (i) each $\mathcal{G}_i$ is strongly connected $(1 \leq i \leq n)$; (ii) no $\mathcal{G}_i$ is a subgraph of a strongly connected subgraph of $\mathcal{G}$. ◇

Finding all the SCCs is proven to be of polynomial complexity w.r.t. the size of the graph [79]. In this thesis, only SCCs that contain at least one cycle (including self-loops) are considered. Note that if an SCC does not contain a cycle, then it contains only one node without self-loops. Clearly, finding all the SCCs that contain at least one cycle is also of polynomial complexity w.r.t. the size of the graph.

In this thesis, a node v_i is said to be reachable from a cycle (or an SCC) if there exists one node v_j in the cycle (or the SCC) from which v_i is reachable.

Chapter 3: Verification of Detectability using Labeled Petri Nets

Detectability describes the property of a system to uniquely determine, after a finite number of observations, the current and the subsequent states. In this chapter, we formalize and analyze four types of detectability: strong detectability, weak detectability, strong periodic detectability, and weak periodic detectability for systems that are modeled as labeled Petri nets (LPNs) with partial observation on their transitions. We provide four new approaches for the verification of such detectability properties using four different structures, and analyze their computational complexity. Without computing the whole reachability space and without enumerating all the markings consistent with an observation, the proposed approaches are more efficient.

3.1 Introduction

In recent years, detectability has drawn a lot of attention from researchers in the discrete event systems (DESs) community [22, 24, 42]. In this chapter, we present four new approaches for the analysis and testing of some detectability properties of LPNs. Strong detectability, weak detectability, strong periodic detectability, and weak periodic detectability are fromally defined in LPNs. The choice of LPNs as the reference formalism originates from the fact that they allow to effectively formalize state estimation problems in the presence of partial observation, simultaneously considering silent and indistinguishable events. The detectability properties characterize the possibility to determine the current and the subsequent states of a system after the observation of a finite number of events generated by the system. We focus on four detectability properties, and consider the situation where both the structure and the initial marking of the Petri net are known, while the system evolution is only partially observed.

In order to reduce the computational complexity of verifying detectability of a system modeled as a LPN, we propose four approaches: 1) BRG-observer method: by analyzing the observer of the BRG of the system. The observer is a deterministic finite-state automaton, whose size is exponential with respect to the number of states of the considered automaton [25]. 2) BRG-detector method: by analyzing the detector of the BRG of the system. The detector is a nondeterministic finite-state automaton, whose size is polynomial with respect to the number of states of the considered automaton [23]. 3) BRG-V method: by checking the verifier of the BRG of the system. The complexity of constructing the verifier is polynomial in the number of states of the given automaton [85, 86]. 4) VN-BRG method: by analyzing the BRG of the verifier net of the system. The verifier net is a Petri net, whose construction has polynomial complexity in terms of the size of the LPN system. It is noticed that all the four approaches are based on the BRG, a graph that allows to summarize in a compact form all the information contained in the RG. In more detail, thanks to the notion of basis markings [77], there is no need to enumerate all the reachable markings, which usually causes the state explosion issue. This leads to a relevant advantage in terms of computational complexity since the BRG is typically much smaller than the RG.

It is known that the complexity of finding all the cycles in a directed graph is NP-hard. Thus, in this chapter rather than computing all cycles of the structure following the approaches in [13, 23, 66], we show that strong detectability can be verified looking at the strongly connected components whose computation has a polynomial complexity. Finally, MATLAB codes are developed to implement the proposed approaches. Numerical results are presented to illustrate them and compare their efficiency.

The rest of the chapter is organized as follows. Strong detectability, weak detectability, strong periodic detectability and weak periodic detectability in LPNs are defined in Section 3.2. In Section 3.3, the approaches based on the BRG and observer are presented to verify the four detectability properties. In Section 3.4, based on the BRG and its detector, we propose an approach to verify strong detectability and strong periodic detectability. In Section 3.5, strong detectability is verified by analyzing the verifier of the BRG of the system. Using the verifier net and its BRG, an approach is proposed to verify strong detectability in Section 3.6. In Section 3.7, a parametric example that illustrates the efficiency of the proposed approaches is given. Conclusions are finally drawn in Section 3.8

3.2 Definitions of Detectability

In [23], four detectability properties have been defined: strong detectability, weak detectability, strong periodic detectability, and weak periodic detectability. In this section we extend these four detectability notions to LPNs.

3.2.1 Definitions

Detectability is a property related to the possibility that the system's current and subsequent states can be uniquely determined after a finite length of observation. In literature, it is assumed that

1) The LPN system G is deadlock free. This means that $\forall M \in R(N, M_0), \exists t \in T$ such that $M[t\rangle$, i.e., any reachable marking enables at least one transition;

2) The T_u-induced subnet is acyclic.

The two assumptions above guarantee that any transition sequence enabled in the system can continue infinitely long as well as its corresponding observation. Similar assumptions are commonly made when detectability is studied (e.g. [7, 24, 65]). Note that Assumption 2) is more restrictive than assuming that there are no strings of unobservable events of infinite length since the existence of a cycle of unobservable transitions in the Petri net structure does not imply that such a cycle is enabled. However, Assumption 2) is a structural assumption that can be verified in polynomial time and that leads to computational advantages in the verification of detectability (as shown in the following sections).

Now, we extend the definitions of detectability defined in [23] to LPNs in a formal way.

Definition 3.1 [**Strong detectability**] An LPN system $G = (N, M_0, E, \ell)$ is said to be strongly detectable if there exists a finite integer $K \in \mathbb{N}$ such that

$$\forall \sigma \in L^{\infty}(G), \forall \sigma' \preceq \sigma, |w| \geq K \Rightarrow |\mathcal{C}(w)| = 1,$$

where $w = \ell(\sigma')$. ◇

An LPN system is strongly detectable if the current and the subsequent states of the system can be determined after a finite number of events observed for all evolutions of the system.

Example 3.1 Consider the LPN system in Fig. 3-1(a). Its RG is shown in Fig. 3-1(b). The resulting observer is reported in Fig. 3-1(c). After a^* is observed, the current state of the system can be uniquely determined, being $\mathcal{C}(a^*) = \{M_2\}$. If $(ab)^*ab$ is observed, the estimation of the current marking is $\mathcal{C}((ab)^*ab) = \{M_1\}$, while if $(ab)^*a$ is observed, $\mathcal{C}((ab)^*a) = \{M_2\}$. Thus, the two states can also be uniquely determined. Therefore, by Definition 3.1, the LPN system is strongly detectable. ◇

Definition 3.2 [**Weak detectability**] An LPN system $G = (N, M_0, E, \ell)$ is said to be weakly detectable if there exists a finite integer $K \in \mathbb{N}$ such that

$$\exists \sigma \in L^{\infty}(G), \forall \sigma' \preceq \sigma, |w| \geq K \Rightarrow |\mathcal{C}(w)| = 1,$$

where $w = \ell(\sigma')$. ◇

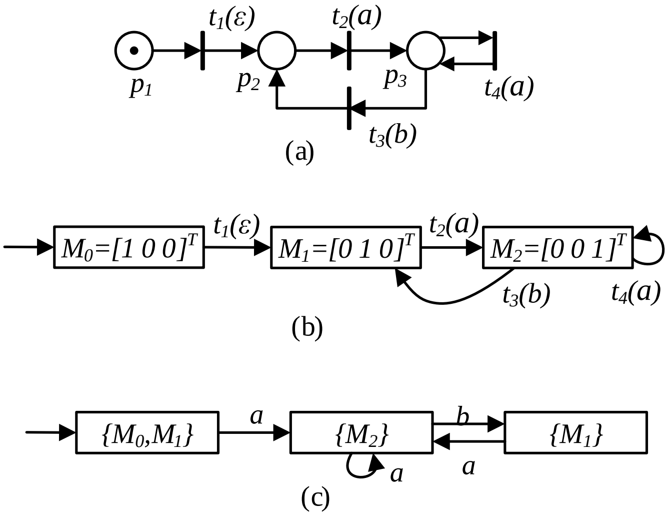


Fig. 3-1 An LPN system (a), its RG (b), and the observer of the RG (c).

An LPN system is weakly detectable if the current and the subsequent states of the system can be determined after a finite number of events observed for some evolutions of the system. According to the definitions of strong detectability and weak detectability, obviously if an LPN system is strongly detectable, it is weakly detectable as well.

Example 3.2 Consider again the LPN system in Fig. 3-1(a). Now we suppose that transition t_2 is a unobservable transition. Then the resulting observer is reported in Fig. 3-2. Clearly, the LPN system is not strongly detectable since after b^* is observed, the estimation contains markings M_1 and M_2. However, since after a^* is observed, the estimation only contains one marking M_2, by Definition 3.2, the LPN system is weakly detectable. ◇

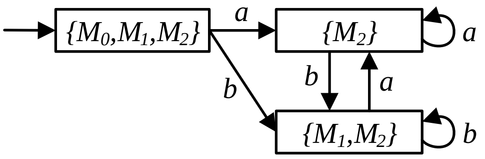


Fig. 3-2 The observer in Example 3.2

Definition 3.3 [**Strong periodic detectability**] An LPN system $G = (N, M_0, E, \ell)$ is said to be strongly periodically detectable if there exists a finite integer $K \in \mathbb{N}$ such that $\forall \sigma \in L^{\infty}(G), \forall \sigma' \preceq \sigma$,

$$\exists \sigma'' \in T^* : \sigma'\sigma'' \preceq \sigma \wedge |\ell(\sigma'')| \leq K \Rightarrow |\mathcal{C}(w)| = 1,$$

where $w = \ell(\sigma'\sigma'')$. ◇

An LPN system is strongly periodically detectable if the current and the subsequent states of the system can be periodically determined for all evolutions of the system. In other words, "periodically detectable" implies that as a string σ continues, eventually there is only one state consistent with the corresponding observation. We point out that for different evolutions the period may be different. Note that as the system is bounded one can find an upper bound for all periods.

Example 3.3 Consider the LPN system in Fig. 3-3(a). Its RG is shown in Fig. 3-3(b), and the observer of the RG is shown in Fig. 3-3(c). State $\{M_2\}$ of the observer contains only one marking. Thus, when the transition sequence $(t_1t_2t_4)^*$ fires and we observe $(aa)^*$, we know that the current state of the system is periodically $\{M_2\}$ (when the a is observed even times). When observing $(ab)^*a$ (the transition sequence $t_1(t_2t_3)^*t_2$ fires), and we realize that$\{M_2\}$ is the current state of the system. By Definition 3.3, the LPN system is strongly periodically detectable and the finite integer K in the definition can equal to 2. Note that the system is also weakly detectable, but not strongly C-detectable. ◇

Definition 3.4 [**Weak periodic detectability**] An LPN system $G = (N, M_0, E, \ell)$ is said to be weakly periodically detectable if there exists a finite integer $K \in \mathbb{N}$ such that $\exists \sigma \in L^\infty(G), \forall \sigma' \preceq \sigma$,

$$\exists \sigma'' \in T^* : \sigma'\sigma'' \preceq \sigma \wedge |\ell(\sigma'')| \leq K \Rightarrow |\mathcal{C}(w)| = 1,$$

where $w = \ell(\sigma'\sigma'')$. ◇

An LPN system is weakly periodically detectable if the current and the subsequent states of the system can be periodically determined for some evolutions of the system. By Definitions 3.1 to 3.4, if an LPN system is strongly periodically detectable, it is also weakly periodically detectable; if an LPN system is strongly/weakly detectable, it is periodically strongly/weakly detectable as well.

Example 3.4 Let us consider again the LPN system in Fig. 3-3(a). Now we suppose that transition t_4 is a unobservable transition. Then the resulting observer is reported in Fig. 3-4. When a^* is observed, the current state of the system contains three markings, being $\mathcal{C}(a^*) = \{M_0, M_1, M_2\}$. If $(ab)^*a$ is observed, the estimation of the current marking is also state $\{M_0, M_1, M_2\}$. As a result, by Definition 3.3, the LPN system is not strongly periodically detectable. However, when $(ab)^*ab$ is observed, the estimation of the current marking is $\mathcal{C}((ab)^*ab) = \{M_1\}$. Thus, the current state can be uniquely determined. Therefore, by Definition 3.4, the LPN system is weakly periodically detectable.

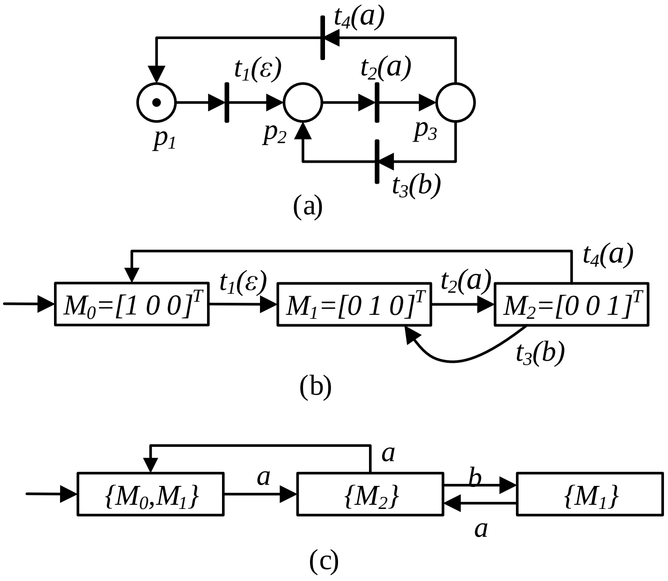


Fig. 3-3 An LPN system in Example 3.3 (a), its RG (b), and the observer of the RG (c).

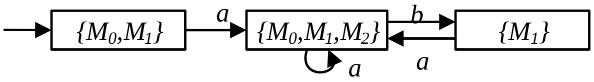


Fig. 3-4 The observer in Example 3.4.

Let us consider another LPN system in Fig. 3-5. Its RG is shown in Fig. 3-6(a), and the observer of the RG is shown in Fig. 3-6(b). When $a(bg)^*$ is observed (the transition sequence $t_1t_2(t_8t_9t_{10})^*$ fires), the current state of the system can be uniquely determined, which is equal to M_2. However, there always exist two arbitrarily long sequences (prefixes of the previous sequence) $t_1t_2(t_8t_9t_{10})^*t_8$ and $t_1t_2(t_8t_9t_{10})^*t_3$ (having the same observation $a(bg)^*b$) such that the current state cannot be determined, that is, if $a(bg)^*b$ is observed, the current state could be any state in $\{M_3, M_4, M_5, M_6, M_7\}$. Therefore, according to Definition 3.1, the LPN system is not strongly detectable.

On the other hand, when the transition sequence $t_1t_2(t_8t_9t_{10})^*$ fires and we observe $a(bg)^*$, we know that the current state of the system is periodically M_2 (after seeing g). When observing $ab(c)^*$ (the transition sequence $t_1t_2t_3(t_4)^*$ fires), and we realize that M_3 is the current state of the system. When observing $ab(d)^*$ (the transition sequence $t_1t_2t_5(t_7)^*$ fires), we realize that M_6 is the current state of the system. Therefore, according to Definitions 3.2, 3.3 and 3.4, the LPN system is weakly detectable, strongly periodically detectable and weakly periodically detectable. ◇

In the automaton framework, the (state) observer is constructed to verify detectability[7, 23]. To verify bounded LPN, first one needs to construct the RG and then follow the methods by constructing the observer of the RG. It is known that, the complexity of constructing the

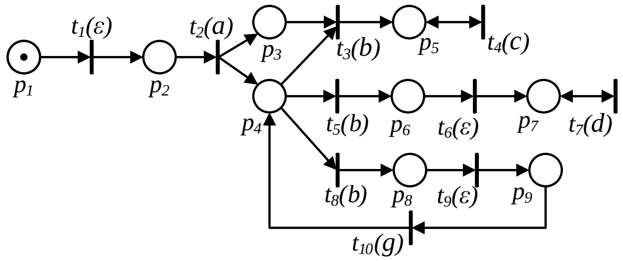
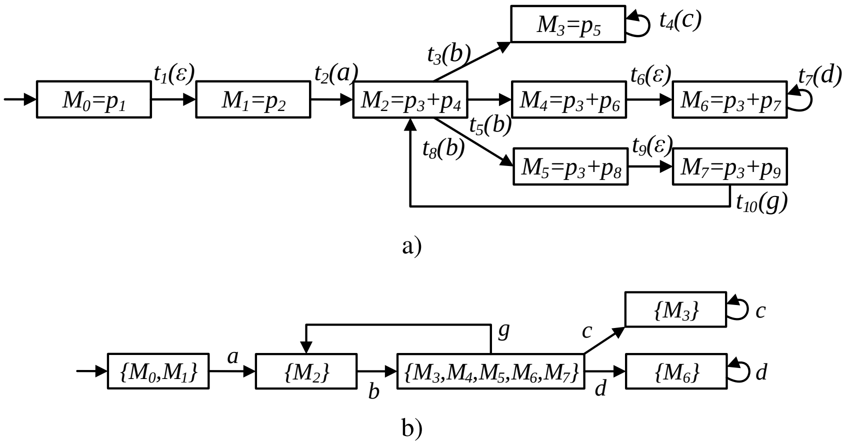


Fig. 3-5 An LPN system.



a)

b)

Fig. 3-6 The RG of the LPN system in Fig. 3-5 (a), the observer of the RG (b).

RG of the Petri net is exponential in the size of the net system (number of places, transitions, tokens in the initial marking). Moreover, in the worst case, the complexity of constructing the observer is exponential in the number of states of the system. Therefore, to verify detectability of large-sized systems the state explosion problem cannot be avoided. In this section, we present an approach to verifying detectability without enumerating all states of the system.

3.2.2 BRG for Detectability

In this chapter, we propose a modified BRG that characterizes if there is a confusable companion of a basis marking. To make sure the nodes of the BRG is finite, we assume that the LPN system is bounded.

Given a bounded LPN system G, for each basis marking $M_b \in \mathcal{M}_b$, a binary scalar is assigned by function $\Psi(M_b) : \mathcal{M}_b \to \{0, 1\}$ that is defined as follows:

$$\Psi(M_b) = \begin{cases} 1 & \text{if } M_b + C_u \cdot y_u \geq 0 \text{ has a positive integer solution;} \\ 0 & \text{otherwise.} \end{cases} \tag{3-1}$$

Lemma 3.1 Let G be an LPN whose T_u-induced subnet is acyclic, and $M_b \in \mathcal{M}_b$ a basis marking of G. If $\Psi(M_b) = 1$, there exists an observation w and a marking $M \in R(N, M_0)$ such that $M, M_b \in \mathcal{C}(w)$ and $M \neq M_b$.

Proof: By assumption $\Psi(M_b) = 1$, Eq. (3-1) has a positive integer solution. Since the T_u-induced subnet of G is acyclic, there is a marking M reachable from M_b by firing unobservable transitions $\sigma_u \in T_u^*$ whose corresponding firing vector is $y_u = \pi(\sigma_u)$. Let $\sigma \in T^*$ be a transition sequence such that $M_0[\sigma\rangle M_b$ and $\ell(\sigma) = w$. Clearly, $M_0[\sigma\sigma_u\rangle M$ and $\ell(\sigma\sigma_u) = w$. Therefore, $M_b, M \in \mathcal{C}(w)$. Moreover, as the T_u-induced subnet is acyclic and $y_u \neq \vec{0}$, $M \neq M_b$. □

In simple words, if $\Psi(M_b) = 1$, M_b has a confusable companion that is different from M_b. However, if $\Psi(M_b) = 0$ there may be also a marking confusable with M_b since there may exist another basis marking M_b' that is confusable with M_b. In this case, to determine if M_b has a confusable companion it is necessary to do further analysis.

In this chapter, we denote $B = (X, E, f, x_0)$ the BRG for detectability of an LPN system $G = (N, M_0, E, \ell)$, where $X \in \mathcal{M}_b \times \{0, 1\}$ is a finite set of states, and each state $x \in X$ of the BRG is a pair $(M_b, \Psi(M_b))$. We denote $x(1)$, $x(2)$ the first and the second element of x respectively. The initial state of the BRG is $x_0 = (M_0, \Psi(M_0))$. The event set of the BRG is the alphabet E. The transition relation is $f : X \times E \to 2^X$. As illustrated in [6, 77, 83], the BRG of an LPN is usually much smaller than its corresponding RG, and the reachability analysis transformed into determining if a linear equation has an positive integer solution.

Example 3.5 Let us consider again the LPN system in Fig. 3-5 whose T_u-induced subnet is acyclic. The LPN system has 8 reachable markings and only 6 of them are basis markings, namely, $\mathcal{M}_b = \{M_0, M_2, M_3, M_4, M_5, M_6\}$. When M_b in Eq. (3-1) equals M_0, the equation has one positive integer solution. Thus, $\Psi(M_0) = 1$. On the other hand, for M_2, Eq. (3-1) does not have a positive solution. Therefore, $\Psi(M_2) = 0$. Therefore, the BRG for detectability is the graph in Fig. 3-7. ◇

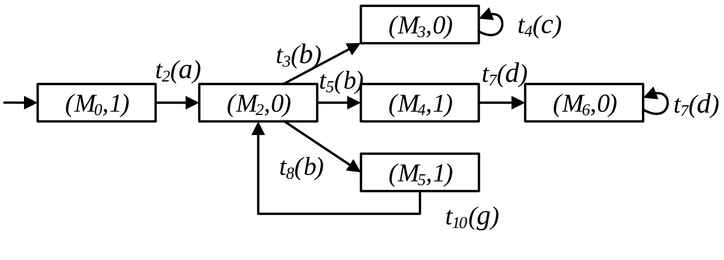


Fig. 3-7 The BRG of the LPN system in Fig. 3-5.

Proposition 3.1 An LPN system G does not perform any detectability defined herein if for all basis markings $M_b \in \mathcal{M}_b$ of G, $\Psi(M_b) = 1$.

Proof: Since $\forall M_b \in \mathcal{M}_b$, $\Psi(M_b) = 1$, by Lemma 3.1, all basis markings M_b of G have a confusable marking that is different from M_b. By Proposition 2.1, for all observations $w \in \mathcal{L}(G)$, $\mathcal{C}(w)$ is not a singleton, i.e., $|\mathcal{C}(w)| > 1$. Therefore, it is not possible for the system to have any detectability defined in Definitions 3.1, 3.2, 3.3 and 3.4. □

3.3 Verification of Detectability based on BRG and Observer

In this section, we introduce the observer of the BRG. Then we show how the observer of the BRG can be used to verify the four detectability properties. This approach is called BRG-observer method. In the following, we present necessary and sufficient conditions for strong detectability, weak detectability, strong periodic detectability, and weak periodic detectability, by analyzing the observer of the BRG of the original LPN system.

3.3.1 Observer of the BRG

Proposition 3.1 only provides necessary conditions for detectability as aforementioned $\Psi(M_b) = 0$ does not necessarily imply that there are no markings confusable with M_b. We construct the observer of the BRG to further investigate the sufficient and necessary conditions for detectability. The observer of a BRG $B = (X, E, f, x_0)$ is denoted as $B_o = (\mathcal{X}, E, f_o, \hat{X}_0)$, where $\mathcal{X} \subseteq 2^{\hat{X}}$ is the set of states, E is the set of events, f_o is the transition function and $\hat{X}_0 = \{x_0\}$ is the initial state. Each state of B_o corresponds to a set $\mathcal{C}_b(w)$, that is, let $f_o(\hat{X}_0, w) = \hat{X}$, then $\mathcal{C}_b(w) = \bigcup_{x \in \hat{X}} x(1)$. Therefore, the complexity of constructing B_o is $\mathcal{O}(2^{|\mathcal{M}_b|})$, which is smaller than the complexity of constructing the observer of the RG, which is equal to $\mathcal{O}(2^{|R(N,M_0)|})$. In the following, necessary and sufficient conditions for detectability are provided based on the inspection of the cycles in the observer.

3.3.2 Verification

Theorem 3.1 Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic, and $B_o = (\mathcal{X}, E, f_o, \hat{X}_0)$ the observer of its BRG. The LPN system G is strongly detectable if and only if for any cycle γ_j in B_o, $\forall \hat{X}_{ji} \in \gamma_j$, $\forall w \in E^*$ that $f_o(\hat{X}_{ji}, w)$ is defined, $f_o(\hat{X}_{ji}, w) = \{(M_b, 0)\}$, where $M_b \in \mathcal{M}_b$.

Proof: (If) Let $\sigma \in L^{\infty}(G)$ and $w = \ell(\sigma)$. Since the T_u-induced subnet is acyclic, w is also of infinite length. As B_o has finite nodes while w is an infinite string, there exists a cycle $\gamma_j = \hat{X}_{j1}e_{j1}\hat{X}_{j2}\ldots\hat{X}_{jk}e_{jk}\hat{X}_{j1}$ and $w_1, w_2 \in E^*$ such that $w = w_1(e_{j1}e_{j2}\ldots e_{jk})^*w_2$ and $|w_1|$ is finite. Namely, the path along w must contain a cycle in B_o because in a graph with a finite number of nodes and no unobservable cycles it is impossible to have a path with an infinite length. For all $\sigma' \in T^* : \ell(\sigma') = w_1$, as the T_u-induced subnet is acyclic and $|w_1|$ is finite, $|\sigma'|$ is also finite. Therefore, there exists an integer $K \geq |\sigma'|$ such that $\forall\sigma'' \preceq \sigma$ with $|\sigma''| \geq K$, $\ell(\sigma'') = w_1w'$, where $w' \preceq (e_{j1}e_{j2}\ldots e_{jk})^*w_2$, and states in $f_o(\hat{X}_0, w_1w')$ are reachable from γ_j. By assumption that $\forall w \in E^*$ that $f_o(\hat{X}_{ji}, w)$ is defined, $f_o(\hat{X}_{ji}, w) = \{(M_b, 0)\}$, thus $f_o(\hat{X}_0, w_1w') = \{(M_b, 0)\}$, and $\mathcal{C}_b(w_1w') = \{M_b\}$. Moreover, $\Psi(M_b) = 0$, i.e., Eq. (3-1) does not have a positive integer solution. By Proposition 2.1, $|\mathcal{C}(w_1w')| = |\mathcal{C}_b(w_1w')| = |\{M_b\}| = 1$. Since for all $\sigma \in L^\infty(G)$ the induction holds, by Definition 3.1, the LPN system is strongly detectable.

(Only if) Assume that there exists a cycle $\gamma_i = \hat{X}_{i1}e_{i1}\hat{X}_{i2}\ldots\hat{X}_{ik}e_{ik}\hat{X}_{i1}$, $w_0 \in E^*$, a state $\hat{X}_{ir}$ in γ_i (with $1 \leq r \leq k$ and $f_o(\hat{X}_0, w_0(e_{i1}\ldots e_{ik})^*e_{i1}\ldots e_{ir}) = \hat{X}_{ir}$), and a string $w' \in E^*$ such that $f_o(\hat{X}_{ir}, w')$ is defined, and either $|f_o(\hat{X}_{ir}, w')| > 1$ (Case 1) or $f_o(\hat{X}_{ir}, w') = \{(M_b, 1)\}$ (Case 2). For these two cases, we prove that the LPN system is not strongly detectable.

Suppose that the LPN system is strongly detectable. Since the LPN system is deadlock free, there exist another cycle $\gamma_j = \hat{X}_{j1}e_{j1}\hat{X}_{j2}\ldots\hat{X}_{jl}e_{jl}\hat{X}_{j1}$ and $\sigma \in L^\infty(G)$ such that $\ell(\sigma) = w = w_0(e_{i1}\ldots e_{ik})^*e_{i1}\ldots e_{ir}w'(e_{j1}\ldots e_{jl})^*$. Since the LPN system is strongly detectable, there exists an integer $K \in \mathbb{N}$ such that $\forall\sigma_1 \preceq \sigma$ with $|\sigma_1| \geq K$, $|\mathcal{C}(w_1)| = 1$ where $w_1 = \ell(\sigma_1)$. Clearly, we can always find an integer z such that $w_1 = w_0(e_{j1}\ldots e_{jk})^z e_{j1}\ldots e_{jr}w')$, $|w_1| \geq K$ and $w_1 \preceq w$. Let $\sigma_1 \preceq \sigma$ with $\ell(\sigma_1) = w_1$. Obviously, $|\sigma_1| \geq K$.

Case 1: $|f_o(\hat{X}_{ir}, w')| > 1$

By assumption, we have $f_o(\hat{X}_{ir}, w') = f_o(\hat{X}_0, w_1)$ and $|f_o(\hat{X}_0, w_1) = \mathcal{C}_b(w_1)| > 1$. By Proposition 2.1, $|\mathcal{C}(w_1)| > 1$ that leads to a contradiction.

Case 2: $f_o(\hat{X}_{ir}, w') = \{(M_b, 1)\}$

By assumption, we have $f_o(\hat{X}_{ir}, w') = f_o(\hat{X}_0, w_1) = \{(M_b, 1)\}$. Therefore, $\mathcal{C}_b(w) = \{M_b\}$ and $\Psi(M_b) = 1$. Since Eq. (3-1) has a positive integer solution and the T_u-induced subnet is acyclic, there exists a marking $M = M_b + C_u \cdot y_u$ and $M \neq M_b$. Thus, $M, M_b \in \mathcal{C}(w_1)$, i.e., $|\mathcal{C}(w_1)| > 1$ that leads to a contradiction. □

In words, an LPN system is strongly detectable if and only if in the observer of its BRG, all states reachable from a cycle have the form $\{(M_b, 0)\}$, i.e., there is only one element

$(M_b, \Psi(M_b))$ in $f_o(\hat{X}_{ji}, w)$ and $\Psi(M_b) = 0$.

Theorem 3.2 Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic, and $B_o = (\mathcal{X}, E, f_o, \hat{X}_0)$ the observer of its BRG. The LPN system G is weakly detectable if and only if there exists a cycle γ_j in B_o such that $\forall \hat{X}_{ji} \in \gamma_j, \hat{X}_{ji} = \{(M_b, 0)\}$, where $M_b \in \mathcal{M}_b$.

Proof: (If) Assume that $\exists \gamma_j = \hat{X}_{j1} e_{j1} \hat{X}_{j2} \ldots \hat{X}_{jk} e_{jk} \hat{X}_{j1} : \forall \hat{X}_{ji} \in \gamma_j, \hat{X}_{ji} = \{(M_b, 0)\}$. Clearly, there exist $\sigma \in L^{\infty}(G)$ and $w_1 \in E^*$ such that $\ell(\sigma) = w = w_1(e_{j1} \ldots e_{jk})^*$ and $|w_1|$ is finite. Since the T_u-induced subnet is acyclic, there exists an integer $K \in \mathbb{N}$ such that $\forall \sigma_1 \in L(N, M_0)$ with $\ell(\sigma_1) = w_1$, $|\sigma_1| \leq K$. For all $\sigma_1 \preceq \sigma$ with $|\sigma_1| \geq K$, $\ell(\sigma_1) = w_1 \preceq w$ and $\exists \hat{X}_{jr} \in \gamma_j$, $f_o(\hat{X}_0, w_1) = \hat{X}_{jr}$. By assumption, $\hat{X}_{jr} = \{(M_b, 0)\}$. Therefore, $f_o(\hat{X}_0, w_1) = \{(M_b, 0)\}$, $\mathcal{C}_b(w_1) = \{M_b\}$, and $\Psi(M_b) = 0$. Since Eq. (3-1) does not have a positive integer solution, by Proposition 2.1, $\mathcal{C}(w_1) = \mathcal{C}_b(w_1) = \{M_b\}$. Thus, the LPN system is weakly detectable.

(Only if) Assume that such a cycle in the theorem does not exist. Namely, $\forall \gamma_j$, $\forall \hat{X}_{ji} \in \gamma_j$, either $|\hat{X}_{ji}| > 1$ or $\hat{X}_{ji} = \{(M_b, 1)\}$. Suppose that the LPN system is weakly detectable, i.e., $\exists K \in \mathbb{N}$, $\exists \sigma \in L^{\infty}(G)$ such that $\forall \sigma_1 \preceq \sigma$ with $|\sigma_1| \geq K$, $|\mathcal{C}(\ell(\sigma_1))| = 1$. Since σ is of an infinite length and B_o has a finite number of nodes, the path along $\ell(\sigma) = w$ must contain a cycle $\gamma_j = \hat{X}_{j1} e_{j1} \hat{X}_{j2} \ldots \hat{X}_{jk} e_{jk} \hat{X}_{j1}$, i.e., there exist $w_1, w_2 \in E^*$ such that $w = w_1(e_{j1} \ldots e_{jk})^* w_2$ and $|w_1|$ is finite. Similarly to the "Only if" part of Theorem 3.1's proof, we can always find $\sigma_1 \preceq \sigma$ such that $|\sigma_1| \geq K$ but $|\mathcal{C}(w_1)| > 1$, where $w_1 = \ell(\sigma_1)$, leading to a contradiction. □

That is, the LPN system is weakly detectable if and only if there is at least one cycle γ_j in the observer such that all states $\hat{X}_{ji}$ in the cycle have the form $\hat{X}_{ji} = \{(M_b, 0)\}$.

Theorem 3.3 Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic, and $B_o = (\mathcal{X}, E, f_o, \hat{X}_0)$ the observer of its BRG. The LPN system G is strongly periodically detectable if and only if for any cycle γ_j in B_o, $\exists \hat{X}_{jr} \in \gamma_j : \hat{X}_{jr} = \{(M_b, 0)\}$, where $M_b \in \mathcal{M}_b$.

Proof: (If) Let $\sigma \in L^{\infty}(G)$ and $w = \ell(\sigma)$. Since the T_u-induced subnet is acyclic and B_o has a finite number of nodes, $|w|$ is infinite and w must pass a cycle γ_j in B_o. Assume that $\exists \hat{X}_{jr} \in \gamma_j$: $\hat{X}_{jr} = \{(M_b, 0)\}$. For all $\sigma_1 \preceq \sigma$, there exists $\sigma_2 \in T^*$ such that $f_o(\hat{X}_0, w_1 w_2) = \hat{X}_{jr}$ and $|w_1 w_2| < K + 1$, where $w_1 = \ell(\sigma_1)$, $w_2 = \ell(\sigma_2)$ and K is the number of nodes in B_o. In other words, from any state along w in B_o the state $\hat{X}_{jr}$ can be always reached within $K+1$ steps. Therefore, $\mathcal{C}_b(w_1w_2) = \{M_b\}$ and $\Psi(M_b) = 0$. Since Eq. (3-1) has no positive integer solution, by Proposition 2.1, $\mathcal{C}(w_1w_2) = \{M_b\}$. Therefore, the LPN system is strongly periodically detectable.

(Only if) Assume that the condition in the theorem does not hold. Namely, there exists a cycle $\gamma_j = \hat{X}_{j1}e_{j1}\hat{X}_{j2}\ldots\hat{X}_{jk}e_{jk}\hat{X}_{j1}$ such that $\forall\hat{X}_{ji} \in \gamma_j$, $|\hat{X}_{ji}| > 1$ or $\hat{X}_{ji} = \{(M_b, 1)\}$. Let $\sigma = L^\infty(G)$ such that $\ell(\sigma) = w = w_0(e_{j1}\ldots e_{jk})^*$, where $w_0 \in E^*$. Since for all $\hat{X}_{ji} \in \gamma_j$, $|\hat{X}_{ji}| > 1$ or $\hat{X}_{ji} = \{(M_b, 1)\}$, for all $\sigma_1 \preceq \sigma$ and $\sigma_2 \in T^*$ such that $\sigma_1\sigma_2 \preceq \sigma$, w_1w_2 enters the cycle, $|\mathcal{C}(w_1w_2)| > 1$. Therefore, such a K does not exist and the LPN system is not strongly periodically detectable. □

A sufficient and necessary condition for strong periodic detectability is that all cycles of the observer of its BRG have a state in the form $\{(M_b, 0)\}$.

Theorem 3.4 Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic, and $B_o = (\mathcal{X}, E, f_o, \hat{X}_0)$ the observer of its BRG. The LPN system G is weakly periodically detectable if and only if there exists a cycle γ_j in B_o such that $\exists\hat{X}_{jr} \in \gamma_j, \hat{X}_{jr} = \{(M_b, 0)\}$, where $M_b \in \mathcal{M}_b$.

Proof: (If) According to the proof of Theorem 3.3, when a cycle γ_j satisfies the condition, for any observation w that passes γ_j the current state of the system can be periodically determined. Therefore, if there exists such a cycle, we can always find a transition sequence σ satisfies the condition in Definition 3.4, and the LPN system is weakly periodically detectable.

(Only if) Assume that there are no such cycles. That is, for all cycles γ_j, and for all $\hat{X}_{ji} \in \gamma_j$, either $|\hat{X}_{ji}| > 1$ or $\hat{X}_{ji} = \{(M_b, 1)\}$. For any $\sigma \in L^\infty(G)$, there exists a cycle γ_j that $\ell(\sigma)$ passes. By the assumption and according to the proof of Theorem 3.3, for any σ there is no such a integer K. Therefore, the LPN system is no weakly periodically detectable. □

Example 3.6 Let us consider again the LPN system in Fig. 3-5 whose BRG is shown in Fig. 3-7. Now we use Theorems 3.1 to 3.4 to check detectability. The observer of its BRG for

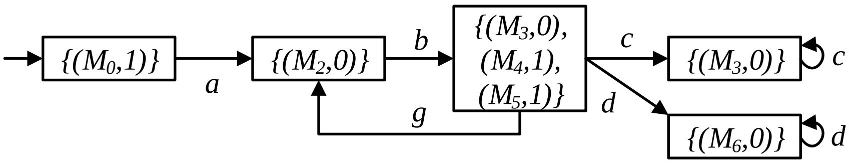


Fig. 3-8 The observer of the BRG in Fig. 3-7.

detectability is shown in Fig. 3-8. In Fig. 3-8, we can see that there is a cycle $\gamma_1 = \{(M_2, 0)\}$ $b\{(M_3, 0), (M_4, 1), (M_5, 1)\}g\{(M_2, 0)\}$ containing state $\{(M_3, 0), (M_4, 1), (M_5, 1)\}$ whose cardinality is 3. Thus, there exists a cycle that does not satisfy the condition that all states are in the form $\{(M_b, \Psi(M_b))\}$ with $\Psi(M_b) = 0$. Therefore, the LPN system is not strongly detectable. On the other hand, the state $\{(M_2, 0)\}$ in γ_1 satisfies the form $\{(M_b, 0)\}$. In other cycles $\gamma_2 = \{(M_3, 0)\}c\{(M_3, 0)\}$ and $\gamma_3 = \{(M_6, 0)\}c\{(M_6, 0)\}$, all their states are in the form $\{(M_b, 0)\}$, therefore, the LPN system is strongly periodically detectable, weakly detectable and weakly periodically detectable. ◇

3.4 Verification of Detectability based on BRG and Detector

In the previous section, we show that the above four detectability properties can be verified using the notions of BRG and observer. The BRG of an LPN system is usually much smaller than its corresponding RG. In this way, the state explosion problem is practically avoided. However, building the observer of the BRG has an exponential complexity. Thus, it is important to search for more efficient algorithms for checking detectability in LPNs. Motivated by the fact that in the automaton framework checking strong detectability and strong periodic detectability is polynomial time, in the following, we look for efficient methods to check them in Petri net systems, which do not require the use of the observer.

In this section, we introduce the detector of the BRG. Then we show how the detector of the BRG can be used to verify strong detectability and strong periodic detectability with lower complexity, compared with the method in BRG-observer method. This approach is called BRG-detector method. The notion of detector was first proposed in [23] for verification of detectability in the framework of automata. In the following, we present necessary and sufficient conditions for strong detectability and strong periodic detectability, by analyzing the detector of the BRG of the original LPN system.

3.4.1 Detector of the BRG

In [23], the detector is proposed to check, in polynomial time, whether an automaton system satisfies strong (periodic) detectability property. Now, we construct the detector of the BRG for the verification in the framework of Petri nets. Given a BRG $B = (X, E, f, x_0)$ built as explained in Section 3.2.2, we denote $B_d = (Q, E, f_d, q_0)$ the detector of the BRG $B = (X, E, f, x_0)$ for detectability, where $Q \subseteq 2^X$ is a finite set of states. The initial state of B_d is $q_0 = \{x_0\}$, and the other states of B_d are subsets of X with cardinality at most equal to 2. The event set of the detector is the alphabet E. The transition function $f_d : Q \times E \to 2^Q$

is defined in Algorithm 2.

According to Algorithm 2, the complexity of constructing it is polynomial w.r.t. the size of the BRG, which is $\mathcal{O}(|E||\mathcal{M}_b|^4)$.

Example 3.7 Consider again the LPN system in Fig. 3-5 whose BRG is shown in Fig. 3-7. The detector of the BRG is presented in Fig. 3-9. The initial state of the detector contains only one marking, i.e., the initial marking of the BRG. At the initial state of the BRG only event a is enabled and its execution leads to a single marking, namely $(M_2, 0)$. This node only containing such a pair is added to the detector and it can be reached from the initial marking firing a. Starting from $(M_2, 0)$ in the BRG, only event b may be executed. The execution of b at such a marking leads to three different markings in the BRG. Thus, three different nodes can be reached from node $\{(M_2, 0)\}$ in the detector, each one containing two pairs, which are the possible pairwise combinations obtained by the three pairs corresponding to the three different basis markings. $\diamond$

In simple words, the detector of the BRG is constructed by recombining in pairs the states in $\mathcal{C}_b(w)$ whenever $|\mathcal{C}_b(w)| > 2$. Namely, for any state $q \in f_d(q_0, w)$ in B_d, $\bigcup_{x\in q} x(1) \subseteq \mathcal{C}_b(w) \subseteq \mathcal{C}(w)$.

Proposition 3.2 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_d = (Q, E, f_d, q_0)$ the detector of its BRG. There exists an observation $w \in E^*$ such that $|\mathcal{C}(w)| \neq 1$, iff there exists a state $q \in Q$ such that $|q| = 2$ or $\exists x \in q$ such that $x(2) = 1$.

Proof: (If) Assume that there exists a state $q \in Q$ such that $|q| = 2$ or $\exists x \in q$ with $x(2) = 1$. If $x(2) = 1$, by Lemma 3.1, there exists an observation $w \in E^*$ such that $|\mathcal{C}(w)| \neq 1$. If $|q| = 2$, let $q = \{x_1, x_2\}$, $x_1 \neq x_2$. According to the construction of the detector, there exists an observation w such that $q \in f_d(q_0, w)$, $q = \{x_1, x_2\}$ and $x_1 \neq x_2$. Thus $x_1(1), x_2(1) \in \mathcal{C}(w)$. Therefore, $|\mathcal{C}(w)| \neq 1$.

(Only if) Assume that there exists an observation $w \in E^*$ such that $|\mathcal{C}(w)| \neq 1$, thus there exist two different markings $M_1, M_2 \in \mathcal{C}(w)$ with $M_1 \neq M_2$. According to the construction of the detector, if $M_1, M_2 \in \mathcal{C}_b(w)$, then there exists a state $q \in Q$ such that $|q| = 2$;

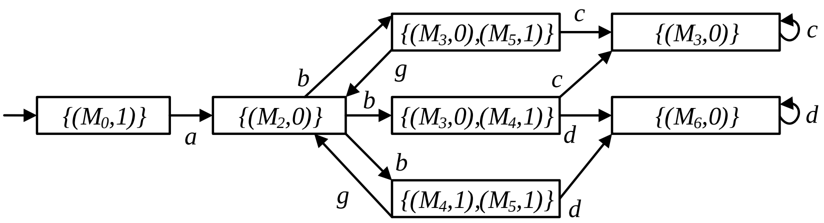


Fig. 3-9 The detector of the BRG in Fig. 3-7.

if either M_1 or M_2 not in $\mathcal{C}_b(w)$, by Proposition 2.1, there exists at least one state $q \in Q$ containing a state x of the BRG such that $x(2) = 1$. □

In words, in an LPN system, there exists an observation w such that $\mathcal{C}(w)$ contains more than one marking, iff there exists a state q in the detector such that $|q| = 2$ or $\exists x \in q$ that $x(2) = 1$.

3.4.2 Verification

Based on Proposition 3.2, a sufficient condition for strong detectability can be easily obtained.

Corollary 3.1 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_d = (Q, E, f_d, q_0)$ the detector of its BRG. The LPN system G is strongly detectable if $\forall q \in Q$, $q = \{(M_b, 0)\}$ where $M_b \in \mathcal{M}_b$.

By Corollary 3.1, if each state of the detector contains only one basis marking M_b and $\Psi(M_b) = 0$, then we can conclude that the system is strongly detectable. However, this condition is not necessary because detectability allows finite delays to ascertain the current state, namely, it may happen that G is strongly detectable but there are some states q from the beginning not satisfying the condition. In the following, necessary and sufficient conditions for detectability are provided based on the inspection of the cycles in the detector.

Theorem 3.5 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_d = (Q, E, f_d, q_0)$ the detector of its BRG. The LPN system G is strongly detectable iff for any $q \in Q$ reachable from a cycle in B_d, $q = \{(M_b, 0)\}$ where $M_b \in \mathcal{M}_b$.

Proof: (If) By contrapositive. Assume that system G is not strongly detectable. This implies that for all $K \in \mathbb{N}$, there exists $\sigma \in L^\infty(G)$ such that $\exists \sigma' \preceq \sigma$, with $w' = \ell(\sigma')$, $|w'| \geq K \Rightarrow |\mathcal{C}(w')| \neq 1$. Since σ has an infinite length, B_d has a finite number of nodes, and there is no cycle of unobservable transitions, the path along $\ell(\sigma) = w$ must contain a cycle $\gamma_j = q_{j1}e_{j1}q_{j2}\ldots q_{jk}e_{jk}q_{j1}$. Thus the observation of σ can be written as $w = w_0(e_{j1}\ldots e_{jk})^n w_2$, where $|w_0|$ is finite, $n \in \{1, 2, 3, \ldots\}$ and $w_0, w_2 \in E^*$. Let $K = |w_0|$. Then, there exists $w' = \ell(\sigma') = w_0 w''$ such that $|w'| \geq K$ and $w'' \preceq (e_{j1}\ldots e_{jk})^n w_2$. Under the initial assumption that $|\mathcal{C}(w')| \neq 1$, by Proposition 3.2, there exists a state $q \in f_d(q_0, w_0 w'')$ such that $|q| = 2$ or $\exists x \in q$ with $x(2) = 1$. Namely, there exists a state q reachable from a cycle in B_d such that $|q| = 2$ or $\exists x \in q$ with $x(2) = 1$.

(Only if) By contrapositive. Assume in the detector there exists a state q reachable from a cycle but $q \neq \{(M_b, 0)\}$. Namely, there exist $\gamma_j = q_{j1}e_{j1}q_{j2} \ldots q_{jk}e_{jk}q_{j1}$, $q_{jr} \in \gamma_j$ ($r \in \{1, 2, \ldots, k\}$), and $w' \in E^*$ such that $q \in f_d(q_{jr}, w')$ and $q \neq \{(M_b, 0)\}$. Since there are no cycles of unobservable transitions, there exist $\sigma \in L^\infty(G)$ and $w_1, w_2 \in E^*$ such that $\ell(\sigma) = w_1(e_{j1}e_{j2} \ldots e_{jk})^n w_2$, $n \in \{1, 2, 3, \ldots\}$ and $|w_1|$ is finite. Therefore, for any $K \in \mathbb{N}$, there exists $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_1(e_{j1}e_{j2} \ldots e_{jk})^m (e_{j1}e_{j2} \ldots e_{jr})w'$ and $|\ell(\sigma')| \geq K$, where $w' \preceq (e_{jr+1} \ldots e_{jk})(e_{j1}e_{j2} \ldots e_{jk})^k w_2$ and $m + k + 1 = n$. Let $w_0 = w_1(e_{j1}e_{j2} \ldots e_{jk})^m(e_{j1}e_{j2} \ldots e_{jr})$. Clearly, $q_{jr} \in f_d(q_0, w_0)$. With the initial assumption, $q \in f_d(q_{jr}, w') = f_d(q_0, w_0w')$. By Proposition 3.2, this implies that $|\mathcal{C}(w_0w')| \neq 1$. Therefore, the system is not strongly detectable. □

In words, an LPN system is strongly detectable iff in the detector of the BRG, all the states reachable from any cycle have the form $\{(M_b, 0)\}$, i.e., there is only one element $(M_b, \Psi(M_b))$ in such states and $\Psi(M_b) = 0$.

Remark 1: Although the complexity of the construction of the detector according to [23] is polynomial, it is known that the complexity of finding all the cycles in a directed graph is NP-hard. Thus, the complexity of verifying strong detectability based on detector in [23] is not actually polynomial. However, finding all the SCCs in a directed graph is of polynomial complexity w.r.t the size of the graph. Clearly, if a state of the detector is reachable from a cycle, it is also reachable from an SCC. Therefore, Theorem 3.5 can be rephrased as follows.

Corollary 3.2 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_d = (Q, E, f_d, q_0)$ the detector of its BRG. The LPN system G is strongly detectable iff for any $q \in Q$ reachable from an SCC in B_d, $q = \{(M_b, 0)\}$ where $M_b \in \mathcal{M}_b$.

Now, we present necessary and sufficient conditions for strong periodic detectability.

Theorem 3.6 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_d = (Q, E, f_d, q_0)$ the detector of its BRG. The LPN system G is strongly periodically detectable iff for any cycle γ_j in B_d, $\exists q \in \gamma_j$, $q = \{(M_b, 0)\}$, where $M_b \in \mathcal{M}_b$.

Proof: (If) By contrapositive. Assume that the LPN system G is not strongly periodically detectable. This implies that for all $K \in \mathbb{N}$, there exists a transition sequence $\sigma \in L^\infty(G)$ with a prefix $\sigma' \preceq \sigma$ such that $\forall \sigma'' \in T^*, \sigma'\sigma'' \preceq \sigma, |\ell(\sigma'')| \leq K \Rightarrow |\mathcal{C}(w')| \neq 1$ where $w' = \ell(\sigma'\sigma'')$. Since σ has an infinite length, B_d has a finite number of nodes, and there is no cycle of unobservable transitions, eventually the tail of the path along $\ell(\sigma) = w$ will be in a cycle $\gamma_j = q_{j1}e_{j1}q_{j2} \ldots q_{jk}e_{jk}q_{j1}$. Thus, w contains the corresponding observation of

γ_j, and there exist $w_0 \in E^*$ and $w_2 \preceq e_{j_1} \ldots e_{j_k}$ such that $w = w_0(e_{j1} \ldots e_{jk})^n w_2$, $|w_0|$ is finite and $n \in \{1, 2, 3, \ldots\}$. Let $\sigma' \preceq \sigma$ such that $|\ell(\sigma')| \geq |w_0|$. Then, for all $\sigma'' \in T^*$ such that $\sigma'\sigma'' \preceq \sigma$, $|\ell(\sigma'')| \leq K$, $q_{jr} \in \gamma_j$ and $q_{jr} \in f_d(q_0, w')$, where $w' = \ell(\sigma'\sigma'')$ and $r \in \{1, 2, \ldots, k\}$. Under the initial assumption that $|\mathcal{C}(w')| \neq 1$, by Proposition 3.2, $q_r \in f_d(q_0, w')$ such that $|q_r| = 2$ or $\exists x \in q_r$ with $x(2) = 1$. Namely, for all $q_r \in \gamma_j$, $q_r \neq \{(M_b, 0)\}$.

(Only if) By contrapositive. Assume that there exists a cycle $\gamma_j = q_{j1}e_{j1}q_{j2} \ldots q_{jk} e_{jk}q_{j1}$ in B_d and $\forall q_{jr} \in \gamma_j$, $q_r \neq \{(M_b, 0)\}$. Since there are no deadlocks nor cycles of unobservable transitions in the system, there exist $\sigma \in L^\infty(G)$ and $w_0 \in E^*$ such that $\ell(\sigma) = w_0(e_{j1} \ldots e_{jk})^*$ and $|w_0|$ is finite. Let $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_0$. Then for all $K \in \mathbb{N}$, $\forall \sigma'' \in T^*, \sigma'\sigma'' \preceq \sigma, \ell(\sigma'\sigma'') = w', |\ell(\sigma'')| \leq K$ such that $q_{jr} \in f_d(q_0, w')$ and $q_{jr} \in \gamma_j$. Under the initial assumption that $q_r \neq \{(M_b, 0)\}$, by Proposition 3.2, this implies that $|\mathcal{C}(w')| \neq 1$. Therefore, the system is not strongly periodically detectable. □

Therefore, an LPN system is strongly periodically detectable iff in the detector of the BRG, all the cycles contain a state having the form $\{(M_b, 0)\}$.

Remark 2: Note that even if each SCC contains at least one state having the form $\{(M_b, 0)\}$, not all cycles necessarily contain a state having the form $\{(M_b, 0)\}$. Therefore, the condition for strong periodic detectability cannot be reformulated in terms of SCCs. However, it is easy to find that we can check Theorem 3.6 by its contrapositive, namely, the system is not strongly periodically detectable iff there exists one cycle γ_j in B_d such that for all $q \in \gamma_j$, $q \neq \{(M_b, 0)\}$. Thus, we just need to find one cycle such that all its states do not have the form $\{(M_b, 0)\}$, which makes the approach polynomial complexity w.r.t. the size of the detector. More precisely, Theorem 3.6 can be checked by removing all the states having the form $\{(M_b, 0)\}$ in the detector, then finding whether there exists a cycle in the remaining parts.

Example 3.8 Consider again the LPN system in Fig. 3-5. Its BRG is shown in Fig. 3-7, and the detector of the BRG is shown in Fig. 3-9. Now we use Theorems 3.5 and 3.6 to check its strong detectability and strong periodic detectability. In Fig. 3-9, we can see that there is a cycle $\gamma_1 = \{(M_2, 0)\}b\{(M_3, 0), (M_5, 1)\}g\{(M_2, 0)\}$ containing state $\{(M_3, 0), (M_5, 1)\}$ whose cardinality is 2 and $\Psi(M_5) = 1$, thus, there exists a cycle that does not satisfy the condition that all states are in the form $q = \{(M_b, \Psi(M_b))\}$ with $\Psi(M_b) = 0$. Therefore, the LPN system is not strongly detectable. On the other hand, the state $\{(M_2, 0)\}$ in γ_1 satisfies the form $\{(M_b, 0)\}$. In another cycle $\gamma_2 = \{(M_3, 0)\}c\{(M_3, 0)\}$, the only state $\{(M_3, 0)\}$ is in the form $\{(M_b, 0)\}$, therefore, the LPN system is strongly periodically detectable.

Consider another LPN system in Fig. 3-10(a), where $M_0 = \{p_1\}$ and $M_1 = \{p_2\}$. The BRG and the detector of the LPN system are shown in Fig. 3-10(b) and 3-10(c), respectively. Clearly, there is a cycle $\gamma_1 = \{(M_0, 0), (M_1, 0)\}a\{(M_0, 0), (M_1, 0)\}$ such that all its states do not satisfy the form $\{(M_b, 0)\}$. Thus, the LPN system is not strongly periodically detectable, and of course not strongly detectable. $\diamond$

The above results show that, rather than enumerating all reachable markings and constructing the detector of the RG, strong detectability and strong periodic detectability can be verified through the detector of the BRG. The complexity of constructing B_d is $\mathcal{O}(|E||\mathcal{M}_b|^4)$, which is much smaller than the RG-based approaches. Furthermore, since the problem of finding all elementary cycles is NP-hard, we prove that strong detectability can be verified by just computing all the SCCs in the detector, which is polynomial complexity w.r.t. the size of the detector, and strong periodic detectability can be verified by just finding one special cycle, which is also polynomial complexity w.r.t. the size of the detector. Therefore, the complexity of the proposed approaches is further reduced.

3.5 Verification of Strong Detectability based on BRG and Verifier

In this section, we first introduce the verifier of the BRG. Then we show how it can be used as an effective tool for the verification of strong detectability. This approach is called BRG-V method. Verifier was first proposed in [85] for verification of diagnosability in the framework of automata. In the following, we present necessary and sufficient conditions for strong detectability, by analyzing the verifier of the BRG of the original LPN system.

3.5.1 Verifier of the BRG

In [85], verifier is proposed to analyze diagnosability in the framework of automata. In the following, without fault transitions, verifier is constructed to check strong detectability of an LPN system.

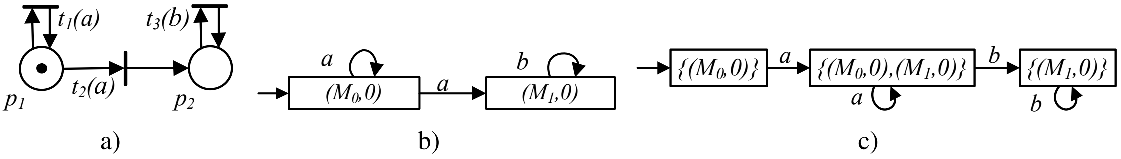


Fig. 3-10 An LPN system (a), the BRG (b) and the detector (c).

Given a BRG $B = (X, E, f, x_0)$ built as explained in Section 3.2.2, the verifier of B is obtained by synchronization of B with itself. We denote the verifier as $B_v = (Q_v, E, f_v, q_{v0})$, where $Q_v \subseteq X \times X$ is the set of states, $q_{v0} = (x_0, x_0)$ is the initial state, E is the alphabet, and $f_v : Q_v \times E \to 2^{Q_v}$ is the transition relation.

The procedure to construct the verifier of the BRG is summarized in Algorithm 4, which works as follows. First, the initial node $q_{v0} = (x_0, x_0)$ is added to a set of unchecked nodes Q_{new} (Steps 1 to 2). Then, for all nodes $q = (x', x)$ in Q_{new}, and for all events $e \in E$, if there exists a pair (x'_1, x_1) such that x'_1 can be reached from x' executing e and x_1 can be reached from x executing e, then make $q' = (x'_1, x_1)$ reachable from q executing event e (Steps 3 to 6). In more detail, we add an edge from q to q' labeled e. If q' does not exist in the verifier, then we add it to Q_v and Q_{new} (Steps 7 to 9). This procedure runs iteratively until there is no unchecked node in Q_{new}.

Algorithm 4 Construction of the verifier

```
Input: A BRG $B = (X, E, f, x_0)$.
Output: The corresponding verifier $B_v = (Q_v, E, f_v, q_{v0})$
 1: $q_{v0} := (x_0, x_0)$,
 2: $Q_v := \{q_{v0}\}$, $Q_{new} := \{q_{v0}\}$.
 3: for all nodes $q = (x', x) \in Q_{new}$, do
 4:    for all $e \in E$, do
 5:       for all pairs $q' = (x'_1, x_1)$ with $x'_1 \in f(x, e)$ and $x_1 \in f(x, e)$, do
 6:          $f_v(q, e) := f_v(q, e) \cup \{q'\}$,
 7:          if $q' \notin Q_v$, then
 8:             $Q_v := Q_v \cup \{q'\}$, $Q_{new} := Q_{new} \cup \{q'\}$.
 9:          end if
10:       end for
11:    end for
12:    $Q_{new} := Q_{new} \setminus \{q\}$.
13: end for
```

By Algorithm 4, in the worst case, there are $|\mathcal{M}_b|^2$ states and $|E||\mathcal{M}_b|^4$ transitions. Thus, the complexity of constructing the verifier is polynomial in the number of states of the BRG, which is $\mathcal{O}(|E||\mathcal{M}_b|^4)$.

Example 3.9 Consider the LPN system in Fig. 3-11 and its BRG in Fig. 3-12. The verifier of the BRG is presented in Fig. 3-13. ◇

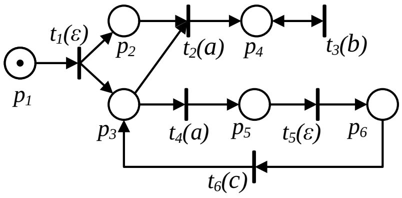


Fig. 3-11 The LPN system in Example 3.9.

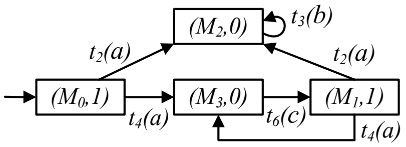


Fig. 3-12 BRG of the LPN system in Fig. 3-11.

Proposition 3.3 There exists an observation $w \in \mathcal{L}(G)$ such that $|\mathcal{C}(w)| \neq 1$, iff there exists a state $q_v = (x', x) \in Q_v$ such that $x'(1) \neq x(1)$ or $x'(2) = 1$ or $x(2) = 1$.

Proof: (If) Assume that there exists a state $q_v = (x', x) \in Q_v$ such that $x'(1) \neq x(1)$ or $x'(2) = 1$ or $x(2) = 1$. If $x'(1) \neq x(1)$, by Algorithm 4, there exists an observation w such that $q_v \in f_v(q_{v0}, w)$. Thus $x'(1), x(1) \in \mathcal{C}(w)$. Since $x'(1) \neq x(1)$, $|\mathcal{C}(w)| \neq 1$. If $x'(2) = 1$ or $x(2) = 1$, by Lemma 3.1, there exists an observation $w \in E^*$ such that $|\mathcal{C}(w)| \neq 1$.

(Only if) Assume that there exists an observation $w \in E^*$ such that $|\mathcal{C}(w)| \neq 1$. This implies that there exist two different markings $M_1, M_2 \in \mathcal{C}(w)$ with $M_1 \neq M_2$. By Algorithm 4, if $M_1, M_2 \in \mathcal{C}_b(w)$, then there must exist a state $q_v = (x', x) \in Q_v$ such that $x'(1) = M_1$ and $x(1) = M_2$, i.e., $x'(1) \neq x(1)$; if M_1, M_2 do not all belong to $\mathcal{C}_b(w)$, then by Eq. (3-1), there must exist a state $q_v = (x', x) \in Q_v$ such that $x'(2) = 1$ or $x(2) = 1$. □

In simple words, by inspecting the existence of a state $q_v = (x', x)$ such that $x'(1) \neq x(1)$ or $x'(2) = 1$ or $x(2) = 1$ in the verifier of the BRG, one can conclude whether there is an observation w such that $\mathcal{C}(w) \neq 1$. This result helps us to determine strong detectability of the LPN system.

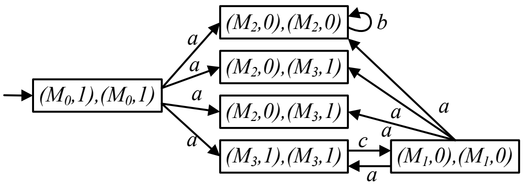


Fig. 3-13 Verifier of the BRG in Fig. 3-12.

3.5.2 Verification

Based on Proposition 3.3, a sufficient condition for strong detectability can be obtained.

Corollary 3.3 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_v = (Q_v, E, f_v, q_{v0})$ the verifier of its BRG. The LPN system G is strongly detectable if $\forall q_v = (x', x) \in Q_v$ satisfy that $x'(1) = x(1)$ and $x'(2) = x(2) = 0$.

The following necessary and sufficient condition for strong detectability is also derived from Proposition 3.3.

Theorem 3.7 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_v = (Q_v, E, f_v, q_{v0})$ the verifier of its BRG. The LPN system G is strongly detectable iff for any $q_v \in Q_v$ reachable from a cycle in B_v, $q_v = ((M_b, 0), (M_b, 0))$ where $M_b \in \mathcal{M}_b$.

Proof: (If) By contrapositive. Assume that system G is not strongly detectable. This implies that for all $K \in \mathbb{N}$, there exists $\sigma \in L^\infty(G)$ such that $\exists \sigma' \preceq \sigma$, with $w' = \ell(\sigma'), |w'| \geq K \Rightarrow |\mathcal{C}(w')| \neq 1$. Since σ has an infinite length, B_v has a finite number of nodes, and there is no cycle of unobservable transitions, the path along $\ell(\sigma) = w$ must contain a cycle $\gamma_j = q_{j1} e_{j1} q_{j2} \ldots q_{jk} e_{jk} q_{j1}$. Thus the observation of σ can be written as $w = w_0 (e_{j1} \ldots e_{jk})^n w_2$, where $|w_0|$ is finite, $n \in \{1, 2, 3, \ldots\}$ and $w_0, w_2 \in E^*$. Let $K = |w_0|$. Then, there exists $w' = \ell(\sigma') = w_0 w''$ such that $|w'| \geq K$ and $w'' \preceq (e_{j1} \ldots e_{jk})^n w_2$. Under the initial assumption that $|\mathcal{C}(w')| \neq 1$, by Proposition 3.3, there exists a state $q_v = (x', x) \in f_v(q_{v0}, w_0 w'')$ such that $x'(1) \neq x(1)$ or $x'(2) = 1$ or $x(2) = 1$. Namely, there exists a state $q_v = (x', x)$ reachable from a cycle in B_v such that $q_v \neq ((M_b, 0), (M_b, 0))$ where $M_b \in \mathcal{M}_b$.

(Only if) By contrapositive. Assume that in the verifier there exists a state $q_v = (x', x)$ reachable from a cycle and $q_v \neq ((M_b, 0), (M_b, 0))$, i.e., $x'(1) \neq x(1)$ or $x'(2) = 1$ or $x(2) = 1$. Namely, there exist $\gamma_j = q_{j1} e_{j1} q_{j2} \ldots q_{jk} e_{jk} q_{j1}$, $q_{jr} \in \gamma_j$ ($r \in \{1, 2, \ldots, k\}$), and $w' \in E^*$ such that $q_v \in f_v(q_{jr}, w')$. Since there are no cycles of unobservable transitions, there exist $\sigma \in L^\infty(G)$ and $w_1, w_2 \in E^*$ such that $\ell(\sigma) = w_1 (e_{j1} e_{j2} \ldots e_{jk})^n w_2$ and $|w_1|$ is finite. Therefore, for any $K \in \mathbb{N}$, there exists $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_1 (e_{j1} e_{j2} \ldots e_{jk})^m (e_{j1} e_{j2} \ldots e_{jr}) w'$ and $|\ell(\sigma')| \geq K$, where $w' \preceq (e_{jr+1} \ldots e_{jk})$ $(e_{j1} e_{j2} \ldots e_{jk})^k w_2$ and $m + k + 1 = n$. Let $w_0 = w_1 (e_{j1} e_{j2} \ldots e_{jk})^m (e_{j1} e_{j2} \ldots e_{jr})$. Clearly, $q_{jr} \in f_v(q_{v0}, w_0)$. With the initial assumption, $q_v \in f_v(q_{jr}, w') = f_v(q_{v0}, w_0 w')$. By Proposition 3.3, this implies that $|\mathcal{C}(w_0 w')| \neq 1$. Therefore, the system is not strongly detectable. □

Therefore, an LPN system is strongly detectable iff in the verifier of its BRG, all states reachable from a cycle have the form $((M_b, 0), (M_b, 0))$. Here, we can also take advantages from SCCs. Thus Theorem 3.7 can be rewritten as follows.

Corollary 3.4 Let G be an LPN system whose T_u-induced subnet is acyclic, and $B_v = (Q_v, E, f_v, q_{v0})$ the verifier of its BRG. The LPN system G is strongly detectable iff for any $q_v \in Q_v$ reachable from an SCC in B_v, $q_v = ((M_b, 0), (M_b, 0))$ where $M_b \in \mathcal{M}_b$.

Example 3.10 Consider again the LPN system in Fig. 3-11. Its BRG is shown in Fig. 3-12, and the verifier of the BRG is shown in Fig. 3-13. Now we use Theorem 3.7 to check strong detectability of the system. In the verifier, state $((M_3, 1), (M_3, 1))$ belongs to a cycle, so it is not true that all states are in the form $((M_b, 0), (M_b, 0))$. Therefore, the LPN system is not strongly detectable. ◇

Analogously to what has been done using the detector in Section 3.4, we try to check strong periodic detectability by inspection of the cycles in the verifier of the BRG. However, we finally find that the system may not be strongly periodically detectable even if in any cycle γ_j in B_v, $\exists q_v = (x', x) \in \gamma_j$, such that $q_v = ((M_b, 0), (M_b, 0))$. This is shown in the following example.

Example 3.11 Consider the LPN system in Fig. 3-10(a). The verifier of the BRG of the LPN system is shown in Fig. 3-14. There are two cycles $\gamma_1 = ((M_0, 0), (M_0, 0))a((M_0, 0), (M_0, 0))$ and $\gamma_2 = ((M_1, 0), (M_1, 0))a((M_1, 0), (M_1, 0))$. All the states in the cycles satisfy the form $((M_b, 0), (M_b, 0))$. However, as shown in Example 3.8, the system is not strongly periodically detectable. ◇

The above results show that strong detectability can be verified through the verifier of the BRG, by checking all the SCCs in the verifier. The complexity of constructing B_v is $\mathcal{O}(|E||\mathcal{M}_b|^4)$ and the complexity of computing all the SCCs in the verifier is polynomial w.r.t. the size of the verifier. Therefore, the complexity of the approach is also reduced.

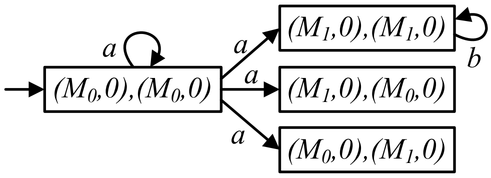


Fig. 3-14 Verifier of the BRG in Fig. 3-10(b).

3.6 Verification of Strong Detectability based on Verifier Net and BRG

In this section, we introduce the construction of the verifier net, which is still a Petri net, and discuss some of its properties. Then, we show how the BRG of the verifier net can be used to verify strong detectability. This approach is called VN-BRG method. Verifier net was first proposed in [87] for verification of diagnosability. The verifier net is a labeled Petri net that is built from the original LPN system. In this section, we present necessary and sufficient conditions for strong detectability by analyzing the BRG of the verifier net. This approach is related to several works on state estimation of Petri nets [65, 78, 87]. In particular, it is closely related to the work of Masopust and Yin [65] who used a twin-plant construction algorithm to verify strong detectability. Indeed, the twin-plant is a Petri net, while the proposed verifier net is a labeled Petri net. Furthermore, we construct the BRG of the verifier net, thus avoiding to enumerate all the markings.

3.6.1 Verifier Net

In [87], the verifier net (VN) is proposed to check diagnosability of an LPN system. In this section, by modifying the labeling function of the VN, we will make it useful for the analysis of strong detectability.

Let $G = (N, M_0, E, \ell)$ be an LPN system, where $N = (P, T, Pre, Post)$, $T = T_o \dot{\cup} T_u$, and $\ell : T \to E \cup \{\varepsilon\}$. Let $N' = (P', T', Pre', Post')$ be a copy of N where each place p_i in N is denoted as p'_i and each transition t_i in N is denoted as t'_i. We denote $G' = (N', M'_0, E, \ell')$ a copy of G, that is, the initial marking $M'_0 = M_0$, the set of labels in G' is the alphabet E, the labeling function of G' is equal to ℓ, i.e., $\forall t'_i \in T', \ell'(t'_i) = \ell(t_i)$.

The VN is a labeled Petri net system obtained by composing G with G' assuming that the synchronization is performed on the observable transition labels. We denote the VN $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$, where $\tilde{N} = (\tilde{P}, \tilde{T}, \tilde{Pre}, \tilde{Post})$ is a Petri net, $\tilde{M}_0 = \begin{bmatrix} M'_0 \\ M_0 \end{bmatrix}$ is the initial marking of V, E is the alphabet, $\tilde{\ell} : \tilde{T} \to E \cup \{\varepsilon\}$ is the labeling function of V. In net $\tilde{N}$, $\tilde{P} = P' \cup P$ is a set of places of V, and according to the labeling function $\tilde{\ell}$, let λ be the empty transition, the set of transitions can be partitioned into two disjoint sets $\tilde{T} = \tilde{T}_o \cup \tilde{T}_u$, where $\tilde{T}_o = \{(t', t) | t' \in T'_o, t \in T_o, \ell'(t') = \ell(t) \in E\}$ is the set of observable transitions, and $\tilde{T}_u = (T'_u \times \{\lambda\}) \cup (\{\lambda\} \times T_u)$ is the set of unobservable transitions, i.e., $\tilde{\ell}(\tilde{T}_o) \in E$ and

$\tilde{\ell}(\tilde{T}_u) = \varepsilon$. The function $\tilde{Pre} : \tilde{P} \times \tilde{T} \to \mathbb{N}$ and $\tilde{Post} : \tilde{P} \times \tilde{T} \to \mathbb{N}$ are defined as detailed in Algorithm 5. Note that in [87], N' is a subnet of N and the labeling function of the VN is also different from this structure.

Algorithm 5 Construction of the Verifier Net

```
Input: An LPN system $G = (N, M_0, E, \ell)$, where $N = (P, T, Pre, Post)$, $T = T_o \cup T_u$,
    and $\ell : T \to E \cup \{\varepsilon\}$.
Output: The corresponding VN $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$, where $\tilde{N} = (\tilde{P}, \tilde{T}, \tilde{Pre}, \tilde{Post})$, and
    $\tilde{\ell} : \tilde{T} \to E \cup \{\varepsilon\}$.
 1: $G' = (N', M'_0, E, \ell')$ be a copy of $G$.
 2: $\tilde{P} = P' \cup P$, $\tilde{M}_0 = \begin{bmatrix} M'_0 \\ M_0 \end{bmatrix}$.
 3: for all transitions $t_u \in T_u$, do
 4:     • add a transition $\tilde{t} = (\lambda, t_u) \in \tilde{T}$, $\tilde{\ell}(\tilde{t}) := \varepsilon$;
 5:     • for all $p' \in P'$, $\tilde{Pre}(p', \tilde{t}) := \tilde{Post}(p', \tilde{t}) := 0$;
 6:     • for all $p \in P$, $\tilde{Pre}(p, \tilde{t}) := Pre(p, t_u)$ and $\tilde{Post}(p, \tilde{t}) := Post(p, t_u)$;
 7: end for
 8: for all transitions $t'_u \in T'_u$, do
 9:     • add a transition $\tilde{t} = (t'_u, \lambda) \in \tilde{T}$, $\tilde{\ell}(\tilde{t}) := \varepsilon$;
10:     • for all $p' \in P'$, $\tilde{Pre}(p', \tilde{t}) := Pre'(p', t'_u)$ and $\tilde{Post}(p', \tilde{t}) := Post'(p', t'_u)$
11:     • for all $p \in P$, $\tilde{Pre}(p, \tilde{t}) := \tilde{Post}(p, \tilde{t}) := 0$;
12: end for
13: for all labels $e \in E$, do
14:     • for any pair $(t'_o, t_o)$ with $t'_o \in T'_o$ , $t_o \in T_o$, $\ell'(t'_o) := \ell(t_o) = e$;
15:     • add a transition $\tilde{t} = (t'_o, t_o) \in \tilde{T}$, $\tilde{\ell}(\tilde{t}) := e$;
16:     • for all $p' \in P'$, $\tilde{Pre}(p', \tilde{t}) := Pre'(p', t'_o)$ and $\tilde{Post}(p', \tilde{t}) := Post'(p', t'_o)$;
17:     • for all $p \in P$, $\tilde{Pre}(p, \tilde{t}) := Pre(p, t_o)$ and $\tilde{Post}(p, \tilde{t}) := Post(p, t_o)$.
18: end for
```

According to Algorithm 5, the initial marking $\tilde{M}_0$ of VN is the concatenation of the initial marking of G' and G (Step 2). All the unobservable transitions are indicated with a pair $\tilde{t} = (\lambda, t_u)$ (Step 3 to 7) or $\tilde{t} = (t'_u, \lambda)$ (Steps 8 to 12), where $t_u \in T_u$ in G, $t'_u \in T'_u$ in G', and $\tilde{\ell}(\tilde{t}) = \varepsilon$. All the observable transitions are indicated as $\tilde{t} = (t'_o, t_o)$, where $t'_o \in T'_o$ in G', $t_o \in T_o$ in G, and $\tilde{\ell}(\tilde{t}) = \ell(t'_o) = \ell(t_o)$ (Steps 13 to 18).

Since the VN is a labeled Petri net, the properties of Petri net in Section 2.2 are also suitable for the VN. Given a VN $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$, the incidence matrix of V is $\tilde{C} = \tilde{Post} - \tilde{Pre}$. Let $\tilde{N}' = (\tilde{P}', \tilde{T}', \tilde{Pre}', \tilde{Post}')$ be the $\tilde{T}_u$-induced subnet of $\tilde{N}$, where $\tilde{T}_u$ is the set of unobservable transitions. The incidence matrix of the $\tilde{T}_u$-induced subnet is denoted by $\tilde{C}_u = \tilde{P}ost' - \tilde{P}re'$.

By Algorithm 5, the number of places and tokens of a VN is twice that of the LPN system. In the worst case, the number of the transitions of a VN is n^2, where n is the number of the transitions of the LPN system. Thus, the complexity of constructing a VN is polynomial in the size of the original LPN system.

Example 3.12 Let us consider again the LPN system in Fig. 3-11, whose VN is presented in Fig. 3-15. The set of places of the VN is obtained by the union of the set of places P of the system G in Fig. 3-11 and the set of places P' of the system G', where G' is a copy of G. The initial marking is $\tilde{M}_0 = p_1' + p_1$, and there are four unobservable transitions $\tilde{T}_u = \{(t_1', \lambda), (\lambda, t_1), (t_5', \lambda), (\lambda, t_5)\}$, and six observable transitions $\tilde{T}_o = \{(t_2', t_2), (t_4', t_4)$, $(t_2', t_4), (t_4', t_2), (t_3', t_3), (t_6', t_6)\}$. ◇

Lemma 3.2 There exists a transition sequence $\tilde{\sigma} \in \tilde{T}^*$ in V, where $\tilde{\sigma} = (t_{j1}', t_{j1})$ $(t_{j2}', t_{j2}) \cdots (t_{jk}', t_{jk})$, iff there exists a transition sequence $\sigma' = t_{j1}' t_{j2}' \cdots t_{jk}' \in T'^*$ in G', and a transition sequence $\sigma = t_{j1} t_{j2} \cdots t_{jk} \in T^*$ in G, and $\ell'(\sigma') = \ell(\sigma) = \tilde{\ell}(\tilde{\sigma})$.

Proof: By Algorithm 5, the VN is constructed by all pairs of transition sequences that have the same observation. Thus, the result can be easily obtained. □

In other words, for any transition sequence $\tilde{\sigma} \in L(\tilde{N}, \tilde{M}_0)$ in V whose first and second components are σ' and σ, we can find σ' in G' and σ in G, that have the same observation $\ell'(\sigma') = \ell(\sigma)$. On the other hand, for any $\sigma' \in L(N', M_0')$ and $\sigma \in L(N, M_0)$, with $\ell'(\sigma') = \ell(\sigma)$, we can also find transition sequence $\tilde{\sigma}$ in V whose first and second components are σ' and σ.

Lemma 3.3 There exists a transition sequence $\tilde{\sigma} \in L(\tilde{N}, \tilde{M}_0)$ in V such that $\tilde{M}_0[\tilde{\sigma}\rangle\tilde{M} = \begin{bmatrix} M' \\ M \end{bmatrix}$ with $M' \neq M$, iff there exist two different markings $M_1, M_2 \in R(N, M_0)$ in G, where $M_0[\sigma_1\rangle M_1$, $M_0[\sigma_2\rangle M_2$, $\ell(\sigma_1) = \ell(\sigma_2) = \tilde{\ell}(\tilde{\sigma})$.

Proof: (If) Assume that $M_0[\sigma_1\rangle M_1$, $M_0[\sigma_2\rangle M_2$ such that $\ell(\sigma_1) = \ell(\sigma_2)$ and $M_1 \neq M_2$. Since G' is a copy of G, there exists $\sigma' \in L(N', M_0')$ such that $M_0'[\sigma'\rangle M' = M_2$ and $\ell'(\sigma') = \ell(\sigma_2) = \ell(\sigma_1)$. By Lemma 3.2 and Algorithm 5, there exist $\tilde{\sigma} \in L(\tilde{N}, \tilde{M}_0)$ such that $\tilde{M}_0[\tilde{\sigma}\rangle\tilde{M} = \begin{bmatrix} M' \\ M_1 \end{bmatrix}$ with $M' \neq M_1$.

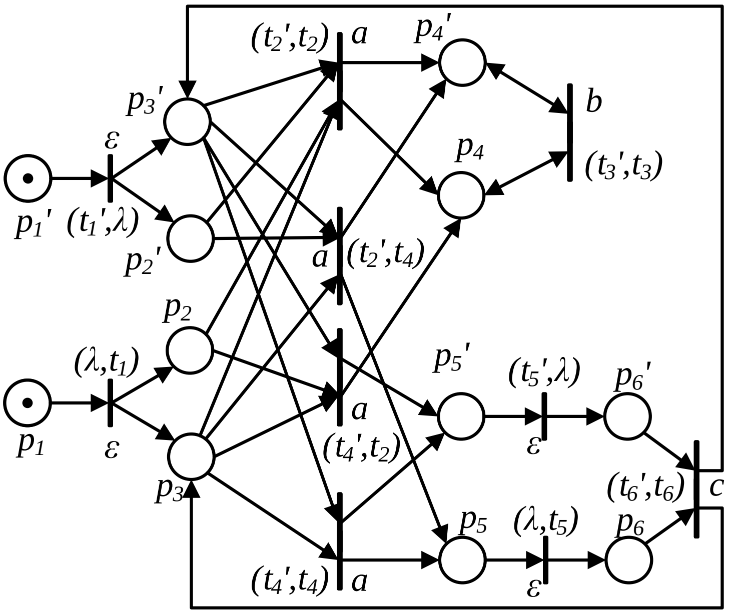


Fig. 3-15 The VN of the LPN system in Fig. 3-11.

(Only if) Assume that $\tilde{M}_0[\tilde{\sigma}\rangle\tilde{M} = \begin{bmatrix} M' \\ \\ M \end{bmatrix}$ with $M' \neq M$. By Lemma 3.2 and Algorithm 5, there exist $\sigma' \in L(N', M_0')$ and $\sigma \in L(N, M_0)$ such that $M_0'[\sigma'\rangle M'$, $M_0[\sigma\rangle M$ and $\ell'(\sigma') = \ell(\sigma)$. Since G' is a copy of G, there exists $\sigma_1 \in L(N, M_0)$ such that $M_0[\sigma_1\rangle M_1 = M'$, with $\ell(\sigma_1) = \ell'(\sigma')$. Thus, $\ell(\sigma_1) = \ell(\sigma)$ and $M_1 \neq M$. □

Therefore, in an LPN system, if there exists a reachable marking $\tilde{M} = \begin{bmatrix} M' \\ \\ M \end{bmatrix} \in R(\tilde{N}, \tilde{M}_0)$ in its VN with $M' \neq M$, then there must exist two different transition sequences whose observations are the same, while the markings reached by them are also different from each other in the LPN system.

Lemma 3.4 There exist two transition sequences $\tilde{\sigma}_1, \tilde{\sigma}_2 \in L(\tilde{N}, \tilde{M}_0)$ in V, with $\tilde{\ell}(\tilde{\sigma}_1) = \tilde{\ell}(\tilde{\sigma}_2)$, $\tilde{M}_0[\tilde{\sigma}_1\rangle\tilde{M}_1$, $\tilde{M}_0[\tilde{\sigma}_2\rangle\tilde{M}_2$, and $\tilde{M}_1 \neq \tilde{M}_2$, iff there exist two transition sequences σ_1 and σ_2 in G such that $M_0[\sigma_1\rangle M_1, M_0[\sigma_2\rangle M_2, M_1 \neq M_2$, and $\ell(\sigma_1) = \ell(\sigma_2) = \tilde{\ell}(\tilde{\sigma}_1)$.

Proof: (If) Assume that there exist two transition sequences σ_1 and σ_2 in G such that $M_0[\sigma_1\rangle M_1, M_0[\sigma_2\rangle M_2, M_1 \neq M_2$, and $\ell(\sigma_1) = \ell(\sigma_2) = \tilde{\ell}(\tilde{\sigma}_1)$. Since G' is a copy of G, there exist $\sigma_1', \sigma_2' \in L(N', M_0')$ such that $M_0'[\sigma_1'\rangle M_1' = M_1$ and $M_0'[\sigma_2'\rangle M_2' = M_2$. By Lemma

3.2 and Algorithm 5, there exist $\tilde{\sigma_1}, \tilde{\sigma_2} \in L(\tilde{N}, \tilde{M_0})$ such that $\tilde{M_0}[\tilde{\sigma_1}\rangle\tilde{M_1} = \begin{bmatrix} M_1' \\ M_1 \end{bmatrix}$ and $\tilde{M_0}[\tilde{\sigma_2}\rangle\tilde{M_2} = \begin{bmatrix} M_2' \\ M_2 \end{bmatrix}$. Clearly, $\tilde{M_1} \neq \tilde{M_2}$.

(Only if) Assume that $\tilde{M_0}[\tilde{\sigma}_1\rangle\tilde{M_1} = \begin{bmatrix} M_1' \\ M_1 \end{bmatrix}$, $\tilde{M_0}[\tilde{\sigma}_2\rangle\tilde{M_2} = \begin{bmatrix} M_2' \\ M_2 \end{bmatrix}$, with $\tilde{M_1} \neq \tilde{M_2}$. By Lemma 3.2 and Algorithm 5, there exist $\sigma_1', \sigma_2' \in L(N', M_0')$ and $\sigma_1, \sigma_2 \in L(N, M_0)$ such that $M_0'[\sigma_1'\rangle M_1'$, $M_0[\sigma_1\rangle M_1$, $M_0'[\sigma_2'\rangle M_2'$, $M_0[\sigma_2\rangle M_2$ and $\ell'(\sigma_1') = \ell(\sigma_1) = \ell'(\sigma_2) = \ell(\sigma_2)$. Since G' is a copy of G, there exist $\sigma_3, \sigma_4 \in L(N, M_0)$ such that $M_0[\sigma_3\rangle M_3 = M_1'$, $M_0[\sigma_4\rangle M_4 = M_2'$, with $\ell(\sigma_3) = \ell'(\sigma_1')$ and $\ell(\sigma_4) = \ell'(\sigma_2')$. Since $\tilde{M_1} \neq \tilde{M_2}$, M_1', M_1, M_2', M_2 can not all be equal. Namely, M_1, M_2, M_3, M_4 can not all be equal. Since $\ell(\sigma_1) = \ell(\sigma_2) = \ell(\sigma_3) = \ell(\sigma_4)$, the result holds. □

In other words, in an LPN system, if there exist two different markings with the same observation in its VN, then there must exist two different markings in the LPN system that can be reached when observing the same event sequence.

Proposition 3.4 The $\tilde{T_u}$-induced subnet of V is acyclic, iff the T_u-induced subnet of G is acyclic.

Proof: (If) Assume that the $\tilde{T_u}$-induced subnet of V is not acyclic. Clearly, there exists a cycle in the $\tilde{T_u}$-induced subnet, i.e., there exists a transition sequence $\tilde{\sigma_u} = (t_{j1}', t_{j1})(t_{j2}', t_{j2}) \cdots (t_{jk}', t_{jk}) \in \tilde{T_u}^*$, such that $\tilde{M}[\tilde{\sigma_u}\rangle\tilde{M}$. By Lemma 3.2, there must exist a transition sequence $\sigma = t_{j1}t_{j2}\cdots t_{jk}$ in G, $\ell(\sigma) = \tilde{\ell}(\tilde{\sigma}) = \varepsilon$. Let $\tilde{M} = \begin{bmatrix} M' \\ M \end{bmatrix}$, thus $M[\sigma\rangle M$. Therefore, the T_u-induced subnet of G is also not acyclic.

(Only if) Assume that the T_u-induced subnet of G is not acyclic. Clearly, there exists a cycle in the T_u-induced subnet, i.e., there exists a transition sequence $\sigma_u = t_{j1}t_{j2}\cdots t_{jk} \in T_u^*$, such that $M[\sigma_u\rangle M$. Since G' is a copy of G, there also exists a transition sequence $\sigma' = t_{j1}'t_{j2}'\cdots t_{jk}'$ in G' that $M'[\sigma'\rangle M'$, with $\ell'(\sigma') = \ell(\sigma_u) = \varepsilon$. By Lemma 3.2, there must exist a transition sequence $\tilde{\sigma} = (t_{j1}', t_{j1})(t_{j2}', t_{j2}) \cdots (t_{jk}', t_{jk})$ and a marking $\tilde{M} = \begin{bmatrix} M' \\ M \end{bmatrix}$, such that $\tilde{M}[\tilde{\sigma}\rangle\tilde{M}$ with $\tilde{\ell}(\tilde{\sigma}) = \ell'(\sigma') = \ell(\sigma_u) = \varepsilon$. Therefore, The $\tilde{T}_u$-induced subnet of V is not acyclic. □

3.6.2 BRG of the VN

In this subsection, we show how the BRG of the VN can be used to verify detectability, thus again avoiding the enumeration of all the states of the LPN system. Obviously, such an approach can be applied provided that the T_u-induced subnet of the LPN is acyclic.

To distinguish the BRG of the original system and the BRG of the VN, we denote $V_b = (\tilde{X}, E, \tilde{f}, \tilde{x}_0)$ the BRG of the VN $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$, where $\tilde{X} \subseteq \tilde{\mathcal{M}}_b \times \{0, 1\}$ is a finite set of states, and each state $\tilde{x} \in \tilde{X}$ of the BRG is a pair $(\tilde{M}_b, \Psi(\tilde{M}_b))$. We denote the i-th (with $i = 1, 2$) element of $\tilde{x}$ as $\tilde{x}(i)$. The initial node of the BRG is $\tilde{x}_0 = (\tilde{M}_0, \Psi(\tilde{M}_0))$.

According to [83, 88], in the worst case, the complexity of constructing a BRG is equal to that of the RG. Thus, in the worst case, the complexity of constructing the BRG is exponential in the VN's size.

Example 3.13 Consider again the LPN system in Fig. 3-11. Its VN in Fig. 3-15 is already introduced in Example 3.12. The VN has 13 reachable markings and 6 basis markings. We take $\tilde{M}_0$ and $\tilde{M}_1$ as examples to compute $\Psi(\tilde{M}_0)$ and $\Psi(\tilde{M}_1)$. For basis marking $\tilde{M}_0 = p_1' + p_1$, the Eq. (3-1) has 3 solutions. In this case, $\Psi(\tilde{M}_0) = 1$. For basis marking $\tilde{M}_1 = p_4' + p_4$, by Eq. (3-1), the equation does not have a positive integer solution. Therefore, $\Psi(\tilde{M}_1) = 0$. The BRG of the VN is presented in Fig. 3-16. ◇

Proposition 3.5 Let $G = (N, M_0, E, \ell)$ be an LPN system, and $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$ the VN of G. There exists an observation $w \in E^*$ of G with $|\mathcal{C}(w)| \neq 1$, iff there exists a state $\tilde{x} = (\tilde{M}_b, \Psi(\tilde{M}_b))$ of V_b, such that $\Psi(\tilde{M}_b) = 1$ or $\tilde{M}_b = \begin{bmatrix} M_b' \\ M_b \end{bmatrix}$ with $M_b' \neq M_b$.

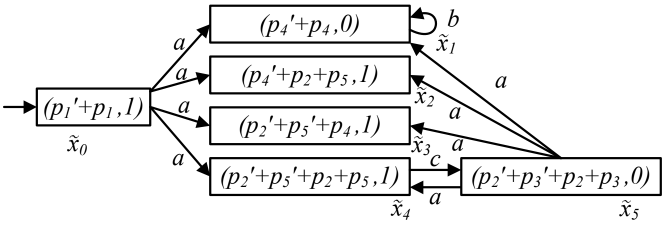


Fig. 3-16 The BRG of the VN in Fig. 3-15.

Proof: (If) Assume that there exists a state $\tilde{x} = (\tilde{M}_b, \Psi(\tilde{M}_b))$ of V, such that $\Psi(\tilde{M}_b) = 1$ or $\tilde{M}_b = \begin{bmatrix} M_b' \\ \\ M_b \end{bmatrix}$ with $M_b' \neq M_b$.

Case 1: $\tilde{M}_b = \begin{bmatrix} M_b' \\ \\ M_b \end{bmatrix}$ with $M_b' \neq M_b$. By Lemma 3.3, there must exist $M_1, M_2 \in R(N, M_0)$ in G, where $M_0[\sigma_1\rangle M_1 = M_b'$, $M_0[\sigma_2\rangle M_2 = M_b$, $\ell(\sigma_1) = \ell(\sigma_2)$. Let the observation of G be $w = \ell(\sigma_1) = \ell(\sigma_2)$, where $w \in E^*$. Therefore, $M_1, M_2 \in \mathcal{C}(w)$, thus $|\mathcal{C}(w)| \neq 1$.

Case 2: $\Psi(\tilde{M}_b) = 1$. This implies that Eq. (3-1) has a positive integer solution, Thus, there exists an unobservable transition $\tilde{t}_u$ that is enabled at marking $\tilde{M}$. Let $\tilde{M}_0[\tilde{\sigma}\rangle\tilde{M}_b[\tilde{t}_u\rangle\tilde{M}$ with $\tilde{\ell}(\tilde{\sigma}) = w$. Since the T_u-induced subnet of G is acyclic, by Proposition 3.4, the $\tilde{T}_u$-induced subnet of V is also acyclic. Thus, $\tilde{M} \neq \tilde{M}_b$ and $\tilde{\ell}(\tilde{\sigma}\tilde{t}_u) = \tilde{\ell}(\tilde{\sigma})$. By Lemma 3.4, there must exist two different markings $M_1, M_2 \in R(N, M_0)$ in G with $M_1 \neq M_2$, where $M_0[\sigma_1\rangle M_1$, $M_0[\sigma_2\rangle M_2$, $\ell(\sigma_1) = \ell(\sigma_2) = \tilde{\ell}(\tilde{\sigma}) = w$. Therefore, $M_1, M_2 \in \mathcal{C}(w)$, thus $|\mathcal{C}(w)| \neq 1$.

(Only if) Assume that there exists an observation $w \in E^*$ of G with $|\mathcal{C}(w)| \neq 1$, i.e., there exist two different markings $M_1, M_2 \in \mathcal{C}(w)$ in G with $M_1 \neq M_2$, where $M_0[\sigma_1\rangle M_1$, $M_0[\sigma_2\rangle M_2$, $\ell(\sigma_1) = \ell(\sigma_2) = w$. By Lemma 3.3, there must exist a transition sequence $\tilde{\sigma} \in L(\tilde{N}, \tilde{M}_0)$ with $\ell(\tilde{\sigma}) = w$, $\tilde{M}_0[\tilde{\sigma}\rangle\tilde{M} = \begin{bmatrix} M' \\ \\ M \end{bmatrix}$ such that $M' = M_1, M = M_2$. Since $\tilde{M} \in R(\tilde{N}, \tilde{M}_0)$, by construction of the BRG, if $\tilde{M} \in \tilde{\mathcal{M}}_b$, the result holds; if $\tilde{M} \notin \tilde{\mathcal{M}}_b$, there must exist a basis marking $\tilde{M}_b \in \tilde{\mathcal{M}}_b$ from which $\tilde{M}$ can be reached, namely, $\Psi(\tilde{M}_b) = 1$. □

Therefore, there exists an observation w to which it corresponds a set of consistent markings $\mathcal{C}(w)$ containing more than one marking, iff there exists a state $\tilde{x} = (\tilde{M}_b, \Psi(\tilde{M}_b))$ in the BRG of its VN, such that either $\Psi(\tilde{M}_b) = 1$ or $\tilde{M}_b = \begin{bmatrix} M_b' \\ \\ M_b \end{bmatrix}$ with $M_b' \neq M_b$.

3.6.3 Verification

Based on Proposition 3.5, a sufficient condition for strong detectability can be obtained.

Corollary 3.5 Let $G = (N, M_0, E, \ell)$ be an LPN system whose T_u-induced subnet is acyclic, $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$ the VN of G, and $V_b = (\tilde{X}, E, \tilde{f}, \tilde{x}_0)$ the BRG of V. The system is strongly detectable if for all states $\tilde{x} = (\tilde{M}_b, \Psi(\tilde{M}_b))$ of V_b, it holds that $\Psi(\tilde{M}_b) = 0$ and $\tilde{M}_b = \begin{bmatrix} M_b' \\ M_b \end{bmatrix}$ with $M_b' = M_b$.

In the following, necessary and sufficient conditions for detectability are provided based on the inspection of the cycles in the BRG of the VN.

Theorem 3.8 Let $G = (N, M_0, E, \ell)$ be an LPN system whose T_u-induced subnet is acyclic, $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$ the VN of G, and $V_b = (\tilde{X}, E, \tilde{f}, \tilde{x}_0)$ the BRG of V. The LPN system G is strongly detectable iff for any $\tilde{x} \in \tilde{X}$ reachable from any cycle in V_b, $\tilde{x} = \left(\begin{bmatrix} M_b' \\ M_b \end{bmatrix}, 0 \right)$ with $M_b' = M_b$.

Proof: (If) By contrapositive. Assume that system G is not strongly detectable. This implies that for all $K \in \mathbb{N}$, there exists $\sigma \in L^\infty(G)$ such that $\exists \sigma' \preceq \sigma$, with $w' = \ell(\sigma')$, $|w'| \geq K \Rightarrow |\mathcal{C}(w')| \neq 1$. By Lemma 3.2, there exists a transition sequence $\tilde{\sigma} \in L^\infty(V)$ and $\tilde{\sigma}' \preceq \tilde{\sigma}$, with $\tilde{\ell}(\tilde{\sigma}) = \ell(\sigma)$, $\tilde{\ell}(\tilde{\sigma}') = \ell(\sigma') = w'$. Since the T_u-induced subnet of G is acyclic, by Proposition 3.4, the $\tilde{T}_u$-induced subnet of V is acyclic. Since $\tilde{\sigma}$ has an infinite length, V_b has a finite number of nodes, and there is no cycle of unobservable transitions, the path along $\tilde{\ell}(\tilde{\sigma}) = w$ must contain a cycle $\gamma_j = \tilde{x}_{j1} e_{j1} \tilde{x}_{j2} \ldots \tilde{x}_{jk} e_{jk} \tilde{x}_{j1}$. Thus, the observation of $\tilde{\sigma}$ can be written as $w = w_0 (e_{j1} \ldots e_{jk})^n w_2$, where $|w_0|$ is finite, $n \in \{1, 2, 3, \ldots\}$ and $w_0, w_2 \in E^*$. Let $K = |w_0|$. Then, there exists $w' = \tilde{\ell}(\tilde{\sigma}') = w_0 w''$ such that $|w'| \geq K$ and $w'' \preceq (e_{j1} \ldots e_{jk})^n w_2$. Under the initial assumption that $|\mathcal{C}(w')| \neq 1$, by Proposition 3.5, there exists a state $\tilde{x} = (\tilde{M}_b, \Psi(\tilde{M}_b)) \in \tilde{f}(\tilde{x}_0, w_0 w'')$ such that $\Psi(\tilde{M}_b) = 1$ or $\tilde{M}_b = \begin{bmatrix} M_b' \\ M_b \end{bmatrix}$ with $M_b' \neq M_b$. Clearly, the state $\tilde{x}$ is reachable from a cycle in V_b.

(Only if) By contrapositive. Assume in the BRG of a VN, there exists a state $\tilde{x} = (\tilde{M}_b, \Psi(\tilde{M}_b))$ reachable from a cycle and $\Psi(\tilde{M}_b) = 1$ or $\tilde{M}_b = \begin{bmatrix} M_b' \\ M_b \end{bmatrix}$ with $M_b' \neq M_b$. Namely, there exist $\gamma_j = \tilde{x}_{j1} e_{j1} \tilde{x}_{j2} \ldots \tilde{x}_{jk} e_{jk} \tilde{x}_{j1}$, $\tilde{x}_{jr} \in \gamma_j$ ($r \in \{1, 2, \ldots, k\}$), and $w' \in E^*$ such that $\tilde{x} \in \tilde{f}(\tilde{x}_{jr}, w')$. Since the T_u-induced subnet of G is acyclic, by Proposition 3.4, the $\tilde{T}_u$-induced subnet of V is acyclic. Thus, there exist $\tilde{\sigma} \in L^\infty(V)$ and $w_1, w_2 \in E^*$

such that $\tilde{\ell}(\tilde{\sigma}) = w_1(e_{j1}e_{j2}\ldots e_{jk})^n w_2$ and $|w_1|$ is finite. Therefore, for any $K \in \mathbb{N}$, there exists $\tilde{\sigma}' \preceq \tilde{\sigma}$ such that $\tilde{\ell}(\tilde{\sigma}') = w_1(e_{j1}e_{j2}\ldots e_{jk})^m(e_{j1}e_{j2}\ldots e_{jr})w'$ and $|\tilde{\ell}(\tilde{\sigma}')| \geq K$, where $w' \preceq (e_{jr+1}\ldots e_{jk})(e_{j1}e_{j2}\ldots e_{jk})^k w_2$ and $m+k+1=n$. Let $w_0 = w_1(e_{j1}e_{j2}\ldots e_{jk})^m(e_{j1}$ $e_{j2}\ldots e_{jr})$. Clearly, $\tilde{x}_{jr} \in \tilde{f}(\tilde{x}_0, w_0)$. Thus, $\tilde{x} \in \tilde{f}(\tilde{x}_{jr}, w') = \tilde{f}(\tilde{x}_0, w_0w')$. Since $\tilde{\sigma} \in L^\infty(V)$ and $\tilde{\sigma}' \preceq \tilde{\sigma}$, by Lemma 3.2, there exist $\sigma \in L^\infty(G)$ and $\sigma' \preceq \sigma$, with $\ell(\sigma') = \tilde{\ell}(\tilde{\sigma}') = w_0w'$. Under the initial assumption, by Proposition 3.5, this implies that $|\mathcal{C}(w_0w')| \neq 1$. Therefore, the system is not strongly detectable. □

In words, an LPN system is strongly detectable iff in the BRG of its VN, all states reachable from a cycle have the form $\left(\begin{bmatrix} M_b' \\ M_b \end{bmatrix}, 0\right)$ with $M_b' = M_b$. Here, we can also take advantages on SCCs. Thus Theorem 3.8 can be rewritten as follows.

Corollary 3.6 Let $G = (N, M_0, E, \ell)$ be an LPN system whose T_u-induced subnet is acyclic, $V = (\tilde{N}, \tilde{M}_0, E, \tilde{\ell})$ the VN of G, and $V_b = (\tilde{X}, E, \tilde{f}, \tilde{x}_0)$ the BRG of V. The LPN system G is strongly detectable iff for any $\tilde{x} \in \tilde{X}$ reachable from any SCC in V_b, $\tilde{x} = \left(\begin{bmatrix} M_b' \\ M_b \end{bmatrix}, 0\right)$ with $M_b' = M_b$.

Example 3.14 Consider again the LPN system in Fig. 3-11. Its VN is shown in Fig. 3-15, and the BRG of the VN is shown in Fig. 3-16. Now we use Theorem 3.8 to check its strong detectability. In the BRG, we can see that $\tilde{x}_5(2) = 0$ and $\tilde{x}_4(2) = 1$, thus there exists a cycle that does not satisfy all states having the form $\left(\begin{bmatrix} M_b' \\ M_b \end{bmatrix}, 0\right)$ with $M_b' = M_b$. Therefore, the LPN system is not strongly detectable. ◇

Analogously to Section 3.5, the following example shows that the LPN system is not strongly periodically detectable even if for any cycle γ_j in V_b, $\exists \tilde{x} \in \tilde{X}$, $\tilde{x} = \left(\begin{bmatrix} M_b' \\ M_b \end{bmatrix}, 0\right)$ with $M_b' = M_b$.

Example 3.15 Consider the LPN system in Fig. 3-10(a). The VN of the LPN system and the BRG of the VN are shown in Fig. 3-17(a) and 3-17(b). Clearly, all the states in the cycles are in the form $\left(\begin{bmatrix} M_b' \\ M_b \end{bmatrix}, 0\right)$ with $M_b' = M_b$. However, the system is not strongly

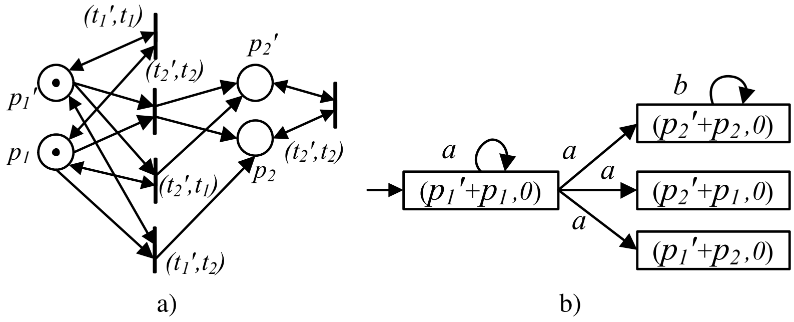


Fig. 3-17 The VN of the LPN system in Fig 3-10 (a), and the BRG of the VN (b).

periodically detectable. ◇

The above results show that strong detectability can be verified through the BRG of the VN, by checking all the SCCs in the BRG. The complexity of computing all the SCCs in the BRG is polynomial w.r.t. the size of the BRG.

3.7 Comparison of the proposed Methods

Since the complexity of constructing the BRG cannot be quantitatively measured in general, the efficiency of the four proposed methods cannot be compared directly. In this section, a series of numerical examples are presented, to compare the efficiency of the four proposed methods. To implement the approaches proposed in this work, we developed MATLAB codes [89] to compute the BRG of a bounded LPN system, its observer, its detector, its verifier, the BRG of the VN, and to determine the detectability properties of bounded LPN systems.

Let us consider the LPN system in Fig. 3-18 whose T_u-induced subnet is acyclic, and where $T_u = \{t_1, t_2, t_3\}$ and $T_o = \{t_4, t_5, \cdots, t_{12}\}$. The initial marking in place p_1 is a parameter $k \in \{1, 2, \cdots\}$.

The number of markings in the BRG of the LPN system, the observer, the verifier, the

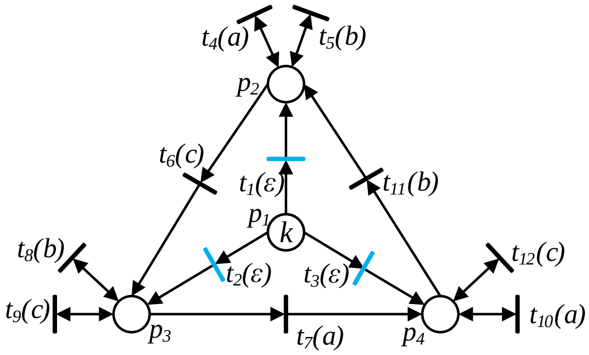


Fig. 3-18 The LPN system considered in Section 3.7.

detector, and the BRG of the VN for different values of k are reported in Table 3-1. Correspondingly, time (in seconds) to compute them, as well as the results relative to the two detectability properties for the different values of k, are summarized in Table 3-2. Computations are performed using MATLAB on a laptop with Intel i7-7700 CPU 3.6GHz processor and 8G DDR3 RAM.

- In Table 3-1, Column 2 illustrates the number of basis markings of the LPN system. Columns 3 to 5 show the number of states in the observer, the detector and the verifier, respectively. Column 6 illustrates the number of basis markings of the VN.

- In Table 3-2, the corresponding time (in seconds) is presented in Columns 2 to 5, which illustrate the time to compute observer, detector, verifier and the BRG of the VN, respectively. In Table 3-2 "o.t." means out of time, in the case where the tool did not halt within 10 hours.

- In Table 3-2, Columns 6 and 7 summarize the properties satisfied by the LPN system for the different values of k in Table 3-1. "SD" and "PSD" stand for strong detectability and strong periodic detectability, respectively. "Y" means that the LPN system satisfies the property, and "N" means that the LPN system does not satisfy the property.

The following conclusions can be drawn from the results in Tables 3-1 and 3-2.

- When k is larger than 4, the number of states of the observer is much larger than that of the verifier and the BRG of the VN, while the number of states of the verifier is much larger than that of the detector.

- The BRG of the VN of the LPN system and the verifier of the BRG of the LPN system always have the same number of states. However, the BRG-V method is more efficient than the VN-BRG method.

- When k is larger than 2, the time needed to compute the observer of the BRG is much longer and grows faster than that required to compute the verifier of the BRG.

- When k is larger than 6, the time needed to compute the observer of the BRG is longer and grows faster than that required to compute the BRG of the VN.

- Whatever the value of k, the time needed to compute the detector of the BRG is much shorter and grows slower than that required to compute the other three structures.

In summary, BRG-detector method, BRG-V method and VN-BRG method are practically more efficient for large-size Petri net systems than BRG-observer method. In particular, the BRG-detector method is the most efficient in the considered examples.

Table 3-1 Cardinality of sets for different values of k in Fig. 3-18.

k	$\|\mathcal{M}_b\|$	$\|\mathcal{X}\|$	$\|Q\|$	$\|Q_v\|$	$\|\tilde{X}\|$
1	4	7	7	10	10
2	10	28	37	82	82
3	20	163	172	362	362
4	35	844	562	1157	1157
5	56	4123	1486	3026	3026
6	84	22327	3404	6890	6890
7	120	135277	7022	14162	14162
8	165	o.t.	13367	26897	26897
9	220	o.t.	23872	47962	o.t.

$\mathcal{M}_b$: the set of basis markings of the LPN system;
$\mathcal{X}$: the set of states in the observer of the BRG;
Q: the set of states in the detector of the BRG;
Q_v: the set of states in the verifier of the BRG;
$\tilde{X}$: the set of basis markings of the VN.

Table 3-2 Time and results for different values of k in Fig. 3-18.

k	τ_o	τ_d	τ_v	τ_{bv}	SD	PSD
1	0.020s	0.018s	0.024s	0.051s	N	N
2	0.131s	0.098s	0.199s	0.553s	N	N
3	1.459s	0.605s	1.387s	5.409s	N	N
4	14.415s	3.535s	9.481s	53.850s	N	N
5	119.70s	20.64s	56.79s	301.64s	N	N
6	1317.06s	96.64s	285.23s	1607.43s	N	N
7	18907.73s	433.89s	1207.52s	7057.02s	N	N
8	o.t.	1530.11s	4374.29s	23692.88s	N	N
9	o.t.	4893.05s	15050.46s	o.t.	N	N

3.8 Conclusions

In the chapter, strong detectability, weak detectability, strong periodic detectability and weak periodic detectability have been defined in labeled Petri nets. Four new approaches to verify the detectability of a labeled Petri net system are developed. The first approach is based on a structure called observer, the second approach is based on a structure called detector, the third one is based on a structure called verifier, and the last one is based on a labeled Petri net called verifier net. All the four approaches use basis reachability graph techniques. Through solving an integer linear equation, the proposed approaches avoid exhaustively enumerating the reachability space. This leads to significant advantages in terms of computational complexity. After careful derivation, the first approach can be used to check the four detectability properties, the second approach can be used to check strong and strong periodic detectability, while the last two methods have the limitation of only allowing the verification of strong detectability. Finally, in all the considered testing examples, it is shown that the BRG-detector method is the most efficient among the four methods for large-size Petri net systems.

Chapter 4: Verification of C-detectability using Labeled Petri Nets

Detectability describes the property of a system to uniquely determine, after a finite number of observations, the current and the subsequent states. In this chapter, we extend detectability to C-detectability that only requires that a given set of crucial states can be distinguished from other states. We define four types of C-detectability in the framework of labeled Petri nets (LPNs): strong C-detectability, weak C-detectability, periodically strong C-detectability, and periodically weak C-detectability. Moreover, we propose efficient approaches to verify such properties in the case of bounded LPN systems. The proposed approaches use the notion of basis marking and thus do not require an exhaustive enumeration of the reachability space.

4.1 Introduction

Detectability describes the property of a system to uniquely determine, after a finite number of observations, the current and the subsequent states. It typically requires a large number of sensors associated with transitions to satisfy the detectability properties. Thus, imposing detectability could be too restrictive in real applications. To address such issues, in this chapter we propose different notions of detectability. In particular, we formalize the notion of C-detectability, where “C” stands for “crucial”. C-detectability requires that if the set of markings consistent with a certain observation contains crucial states, then the crucial state has to be determined uniquely after a finite number of observations. In other words, we extend detectability to C-detectability that only requires that a given set of crucial states can be distinguished from the other states. Clearly, detectability is a special case of C-detectability, where the set of crucial states is equivalent to the whole state space. Based on the notions of basis marking and basis reachability graph (BRG) [77], efficient approaches to verify the above four C-detectability properties are proposed. The contributions of the chapter can be summarized as follows.

- Strong C-detectability, weak C-detectability, periodically strong C-detectability, and periodically weak C-detectability are formally defined in LPNs.
- Efficient approaches to verify the above four C-detectability properties in bounded LPNs are proposed. Thanks to basis markings, there is no need to enumerate all the markings

that are consistent with an observation. This leads to significant advantages in terms of computational complexity since the BRG is usually much smaller than the RG, thus allowing to deal with problems that are otherwise infeasible. By constructing the observer of the BRG, the four C-detectability properties can be checked. By constructing the detector of the BRG, strong C-detectability and periodically strong C-detectability can be checked more efficiently.

- Rather than computing all the elementary cycles in the observer [7, 23], which is NP-hard, we show that C-detectability can be verified by computing strongly connected components [79], which is of polynomial complexity with respect to the size of the observer.

- When a system satisfies a certain C-detectability property, original methods are proposed to compute the smallest number of observed events after which the crucial states can be distinguished.

The rest of the chapter is organized as follows. Strong C-detectability, weak C-detectability, periodically strong C-detectability and periodically weak C-detectability in LPNs are defined in Section 4.2. In Section 4.3, the approaches based on BRG and observer are presented to verify the four C-detectability properties in bounded LPNs. In Section 4.4, the approaches based on BRG and detector are provided to verify strong C-detectability properties in bounded LPNs. A parametric example that illustrates the efficiency of the proposed approaches is given in Section 4.5. Finally, conclusions are presented in Section 4.6.

4.2 Definition of C-detectability

4.2.1 Definition

A Petri net system is detectable if its current state and the subsequent ones can be uniquely determined after a finite number of observations. This requirement may be too strong in some applications. In this chapter, we relax such a definition and introduce the property of C-detectability, where "C" stands for "crucial". In particular, we only care about a given set of states, called crucial states, and want to be sure that when the system reaches such states, they are uniquely identified.

The following two assumptions are made:

1) The LPN system G is deadlock free. This means that $\forall M \in R(N, M_0), \exists t \in T$ such that $M[t\rangle$, i.e., any reachable marking enables at least one transition;

2) The T_u-induced subnet is acyclic.

The two assumptions above guarantee that any transition sequence enabled in the system can continue infinitely long as well as its corresponding observation. Similar assumptions are commonly made when detectability is studied (e.g. [7, 24, 65]). Note that Assumption 2) is more restrictive than assuming that there are no strings of unobservable events of infinite length since the existence of a cycle of unobservable transitions in the Petri net structure does not imply that such a cycle is enabled. However, Assumption 2) is a structural assumption that can be verified in polynomial time and that leads to computational advantages in the verification of C-detectability (as shown in the following sections).

Let us now introduce the notion of crucial markings and the C-detectability properties considered in this chapter, namely, strong, weak, periodically strong, and periodically weak C-detectability.

Definition 4.1 Given an LPN system $G = (N, M_0, E, \ell)$ and the set of its reachable markings $R(N, M_0)$, the set of crucial markings is a subset of markings $\mathcal{M}_c \subseteq R(N, M_0)$. $\diamond$

C-detectability requires that any crucial marking $M \in \mathcal{M}_c$ is distinguishable from the other markings after a finite number of observations. In the following, we formalize four C-detectability properties, namely, strong C-detectability, weak C-detectability, periodically strong C-detectability and periodically weak C-detectability.

Definition 4.2 [**Strong C-detectability**] Let $G = (N, M_0, E, \ell)$ be an LPN system and $\mathcal{M}_c$ the set of crucial markings. System G is strongly C-detectable with respect to (w.r.t.) $\mathcal{M}_c$ if there exists a finite integer $K \in \mathbb{N}$ such that $\forall \sigma \in L^{\infty}(G)$, $\forall \sigma' \preceq \sigma$ with $|w'| \geq K$, the following condition holds:

$$\mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w')| = 1, \tag{4-1}$$

where $w' = \ell(\sigma')$. $\diamond$

In words, an LPN system is strongly C-detectable if we can uniquely determine all markings in $\mathcal{M}_c$ after a finite number of observations for all possible evolutions of the system. Meanwhile, if there is no crucial marking in $\mathcal{C}(w)$ it does not matter whether markings in $\mathcal{C}(w)$ are distinguishable from other markings or not.

Example 4.1 Consider the LPN system in Fig. 4-1(a). Let the set of crucial markings be $\mathcal{M}_c = \{M_0\} = \{[1\ 0\ 0]^T\}$. Its RG is shown in Fig. 4-1(b). The resulting observer is reported in Fig. 4-1(c). After a^* is observed, the current state of the system can be uniquely determined, being $\mathcal{C}(a^*) = \{M_0\}$. On the contrary, if b^* is observed, the estimation of the current marking is $\mathcal{C}(b^*) = \{M_1, M_2\}$, namely there are two consistent markings but none of them is a crucial marking. Therefore, by Definition 4.2, the LPN system is strongly C-detectable w.r.t. $\mathcal{M}_c$. $\diamond$

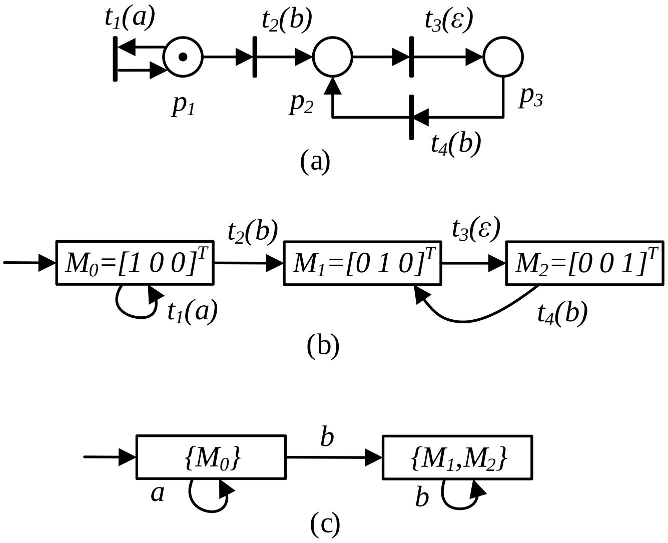


Fig. 4-1 An LPN system (a), its RG (b), and the observer of the RG (c).

Definition 4.3 [**Weak C-detectability**] Let $G = (N, M_0, E, \ell)$ be an LPN system and $\mathcal{M}_c$ the set of crucial markings. System G is weakly C-detectable w.r.t. $\mathcal{M}_c$ if there exist a finite integer $K \in \mathbb{N}$ and a transition sequence $\sigma \in L^\infty(G)$ such that $\forall \sigma' \preceq \sigma$ with $|w'| \geq K$, the condition in Eq. (4-1) holds. ◇

In simple words, weak C-detectability implies that markings in $\mathcal{M}_c$ can be distinguished after a finite number of observations, at least during one possible evolution of the system, but not necessarily during all of them, as in the case of strong C-detectability.

Example 4.2 Let us consider again the LPN system in Fig. 4-1(a). Let the set of crucial markings be $\mathcal{M}_c = \{M_0, M_1\} = \{[1\ 0\ 0]^T, [0\ 1\ 0]^T\}$. Clearly, the LPN system is not strongly C-detectable w.r.t. $\mathcal{M}_c$ since after b^* is observed, the estimation contains a crucial marking M_1 which cannot be distinguished from M_2. However, since after a^* is observed, the estimation only contains one marking M_0 in $\mathcal{M}_c$, by Definition 4.3, the LPN system is weakly C-detectable w.r.t. $\mathcal{M}_c$. ◇

Definition 4.4 [**Periodically strong C-detectability**] Let $G = (N, M_0, E, \ell)$ be an LPN system and $\mathcal{M}_c$ the set of crucial markings. System G is periodically strongly C-detectable w.r.t. $\mathcal{M}_c$ if there exists a finite integer $K \in \mathbb{N}$ such that $\forall \sigma \in L^\infty(G), \forall \sigma' \preceq \sigma$,

$$\exists \sigma'' \in T^* : \sigma'\sigma'' \preceq \sigma, |\ell(\sigma'')| \leq K,$$
$$\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w)| = 1, \tag{4-2}$$

where $w = \ell(\sigma'\sigma'')$. ◇

Therefore, an LPN system is periodically strongly C-detectable if we can periodically distinguish markings in $\mathcal{M}_c$ for all trajectories of the system. In other words, "periodically C-detectable" means that, as an arbitrary sequence in $L^\infty(G)$ continues, from time to time the set of markings consistent with the corresponding observation contains either a single marking or no marking in $\mathcal{M}_c$. We point out that for different evolutions of the system the period may be different. However, if the system is bounded one can find an upper bound for all the periods.

Example 4.3 Consider the LPN system in Fig. 4-2(a). Let the set of crucial markings be $\mathcal{M}_c = \{M_2\} = \{[0\ 0\ 1\ 0]^T\}$. Its RG is shown in Fig. 4-2(b), and the observer of the RG is shown in Fig. 4-2(c). State $\{M_0, M_1\}$ of the observer contains no crucial marking in the estimation, i.e., no crucial marking is confused with other markings. On the contrary, the other two states of the observer contain the crucial marking together with at least one additional marking. Let us now focus on state $\{M_2, M_3\}$. There exists only one sequence $\sigma \in L^\infty(G)$ with $\ell(\sigma) = b(ab)^*$ that leads to state $\{M_2, M_3\}$. However, if we consider $\sigma = t_3(t_4t_5t_1t_3)^*$, then for any $\sigma' \preceq \sigma$ (for instance $\sigma' = t_3t_4t_5t_1$) there exists $\sigma'' = t_3t_4t_5$ such that $\sigma'\sigma'' \preceq \sigma$, $|\ell(\sigma'')| \leq 2$ and $\mathcal{C}(\ell(\sigma'\sigma'')) = \{M_0, M_1\} \cap \mathcal{M}_c = \emptyset$. By Definition 4.4, the LPN system is periodically strongly C-detectable and the finite integer K in the definition is equal to 2. Note that the system is also weakly C-detectable, but not strongly C-detectable.

◇

Definition 4.5 [**Periodically weak C-detectability**] Let $G = (N, M_0, E, \ell)$ be an LPN system and $\mathcal{M}_c$ the set of crucial markings. System G is periodically weakly C-detectable w.r.t. $\mathcal{M}_c$ if there exist a finite integer $K \in \mathbb{N}$ and a transition sequence $\sigma \in L^\infty(G)$ such that $\forall \sigma' \preceq \sigma$, the condition in Eq. (4-2) holds. ◇

An LPN system is periodically weakly C-detectable if there exists at least one sequence enabled at the initial marking such that from time to time the set of markings consistent with the corresponding observation contains either a single marking or no marking in $\mathcal{M}_c$.

Example 4.4 Let us consider again the LPN system in Fig. 4-2(a). Let the set of crucial markings be $\mathcal{M}_c = \{M_0\} = \{[1\ 0\ 0\ 0]^T\}$. When a^* is observed, the crucial marking M_0 is confused with M_1, while if $(ab)^*$ is observed, state $\{M_2, M_3\}$ is reached, which does not contain any crucial marking. On one hand, there exist a finite integer $K = 2$ and sequence $\sigma = t_3(t_4t_5t_1t_3)^* \in L^\infty(G)$ such that for any $\sigma' \preceq \sigma$ (for instance $\sigma' = t_3t_4t_5$) there exists $\sigma'' = t_1t_3$ satisfying $\sigma'\sigma'' \preceq \sigma$, $|\ell(\sigma'')| \leq K$ and $\mathcal{C}(\ell(\sigma'\sigma'')) = \{M_2, M_3\} \cap \mathcal{M}_c = \emptyset$. On the other hand, there also exists sequence $\sigma = (t_1t_2)^* \in L^\infty(G)$ such that no finite integer K

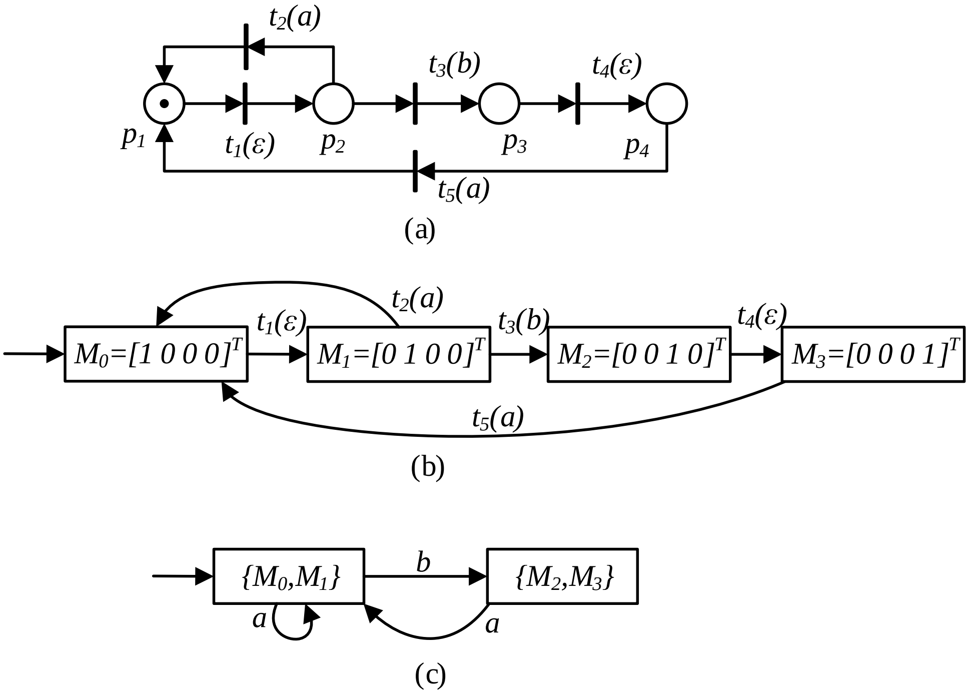
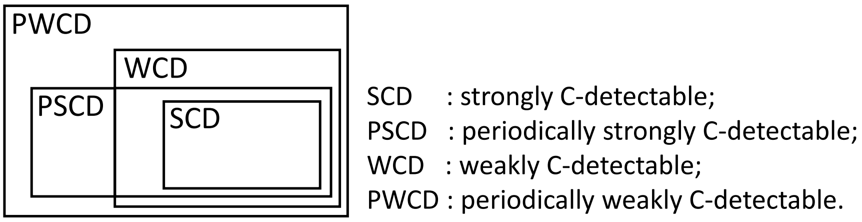


Fig. 4-2 The LPN system in Example 4.3 (a), its RG (b), and the observer of the RG (c).

can be found such that $\forall\sigma' \preceq \sigma$, the condition in Eq. (4-2) holds. As a result, by Definition 4.4, the LPN system is not periodically strongly C-detectable. However, by Definition 4.5, the LPN system is periodically weakly C-detectable. $\diamond$

We finally notice that, by Definitions 4.2 to 4.5, the relationship among the four detectability properties can be summarized by the Venn diagram in Fig. 4-3, where a property in a box implies the properties whose corresponding boxes contain it. For instance, if an LPN system is strongly C-detectable (SCD box), it is certainly also weakly C-detectable (WCD box), periodically strongly C-detectable (PSCD box), and periodically weakly C-detectable (PWCD box). However, if an LPN system is weakly C-detectable, it may not be periodically strongly C-detectable, or vice versa. For instance, in Example 4.2, the LPN system is weakly C-detectable, but not periodically strongly C-detectable. Now, assume that transition t_2 in Fig. 4-2(a) is removed. In such a case, the selfloop labeled a at state $\{M_0, M_1\}$ in the observer



PWCD
WCD
PSCD
SCD
SCD : strongly C-detectable;
PSCD : periodically strongly C-detectable;
WCD : weakly C-detectable;
PWCD : periodically weakly C-detectable.

Fig. 4-3 The relationship among the four detectability properties.

in Fig. 4-2(c) would no longer exist. If $M_c = \{M_2\}$, the LPN system is periodically strongly C-detectable, but not weakly C-detectable.

In the automaton framework, detectability analysis is performed using the notion of observer [7, 23]. Obviously, in the case of bounded LPN systems the same approach can be used first constructing the RG of the net system and then computing its observer (as Examples 4.1 to 4.4 illustrate). However, such an approach could be infeasible in the case of systems with a large state space. Indeed, the RG of a Petri net system is exponential in the size of the net (number of places, transitions, tokens in the initial marking) and the observer of the RG is exponential in the number of reachable markings.

In this chapter, we show how the above four detectability properties can be verified using the notion of basis marking, thus avoiding an exhaustive enumeration of all the markings in the RG.

4.2.2 BRG for C-detectability

In this chapter, using the notion of basis marking, we introduce the BRG for C-detectability. To guarantee that the BRG is finite, we assume that the LPN system is bounded.

For each basis marking $M_b \in \mathcal{M}_b$ two values are respectively assigned by functions $\alpha : \mathcal{M}_b \to \{0, 1\}$ and $\beta : \mathcal{M}_b \to \{0, 1\}$ that are defined by Eqs. (4-3) and (4-4), respectively:

$$\alpha(M_b) = \begin{cases} 1 & \text{if } \mathcal{M}_c \cap UR(M_b) \neq \emptyset; \\ 0 & \text{otherwise.} \end{cases} \tag{4-3}$$

$$\beta(M_b) = \begin{cases} 1 & \text{if } |UR(M_b)| > 1; \\ 0 & \text{if } |UR(M_b)| = 1. \end{cases} \tag{4-4}$$

Since $M_b \in UR(M_b)$, $|UR(M_b)| \geq 1$.

Lemma 4.1 Given a basis marking $M_b \in \mathcal{M}_b$, $|UR(M_b)| > 1$ iff the following equation

$$M_b + C_u \cdot y_u \geq \vec{0} \tag{4-5}$$

has a positive solution $y_u \in \mathbb{N}^{n_u}_{\geq 1}$.

Proof: (If) Suppose Eq. (4-5) has a positive integer solution $y_u \in \mathbb{N}^{n_u}_{\geq 1}$, i.e., there exists at least one of the elements in the vector y_u that is a positive integer. Thus, there exists an unobservable transition t that is enabled at marking M_b. Let $M_b[t\rangle M$. With the assumption that the T_u-induced subnet is acyclic, we have $M \neq M_b$. By definition of unobservable reach, $M_b, M \in UR(M_b)$. Thus $|UR(M_b)| > 1$.

(Only if) If $|UR(M_b)| > 1$, there exists a marking $M \in UR(M_b)$ such that $M \neq M_b$. Let $\sigma_u \in T_u^*$ such that $M_b[\sigma_u\rangle M$ and $y_u = \pi(\sigma_u)$. Therefore, y_u is a solution to Eq. (4-5). Since $M \neq M_b$, $y_u \in \mathbb{N}^{n_u}_{\geq 1}$. □

Lemma 4.1 shows that the value of $\beta(M_b)$ can be computed by simply checking whether Eq. (4-5) has a positive integer solution. We also point out that to compute $\alpha(M_b)$ there is no need to enumerate all markings in $UR(M_b)$ either, but we simply need to check whether there exists a marking $M \in \mathcal{M}_c$ such that $M = M_b + C_u \cdot y_u$ has a solution $y_u \in \mathbb{N}^{n_u}$.

In this chapter, we denote as $B = (X, E, f, x_0)$ the BRG for C-detectability of an LPN system $G = (N, M_0, E, \ell)$, where $X \subseteq \mathcal{M}_b \times \{0,1\} \times \{0,1\}$ is a finite set of states, and each state $x \in X$ of the BRG is a triple $(M_b, \alpha(M_b), \beta(M_b))$. We denote the i-th (with $i \in \{1,2,3\}$) element of x as $x(i)$. The initial node of the BRG is $x_0 = (M_0, \alpha(M_0), \beta(M_0))$. Note that $|X| = |\mathcal{M}_b|$ since for a given basis marking M_b and a given set of crucial markings $\mathcal{M}_c$ the values of $\alpha(M_b)$ and $\beta(M_b)$ are uniquely determined, i.e., there is only one triple $(M_b, \alpha(M_b), \beta(M_b))$ assigned to M_b. The event set of the BRG is the alphabet E.

Lemma 4.2 Let G be an LPN system, $\mathcal{M}_c$ the set of crucial markings, and $M_b \in \mathcal{M}_b$ a basis marking. If $\alpha(M_b) = 1$, there exists an observation $w \in \mathcal{L}(G)$ such that $M_b \in \mathcal{C}(w)$ and $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset$.

Proof: Assume that $\alpha(M_b) = 1$. By Eq. (4-3), $\alpha(M_b) = 1$ implies that there exists a marking $M \in \mathcal{M}_c \cap UR(M_b)$. Let $M' \in R(N, M_0)$, $\sigma \in T^*$ and $\sigma_u \in T_u^*$ such that $M'[\sigma\rangle M_b[\sigma_u\rangle M$ and $\ell(\sigma) = w$. Clearly, $\ell(\sigma\sigma_u) = w$. Therefore, $M_b, M \in \mathcal{C}(w)$ and $M \in \mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset$. □

In simple words, if $\alpha(M_b) = 1$, then there exists an observation $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w)$ contains crucial markings. However, even if $\alpha(M_b) = 0$ there may exist an observation w and another basis marking $M_b' \neq M_b$ such that $M_b', M_b \in \mathcal{C}(w)$ but $\alpha(M_b') = 1$. In this case, $\mathcal{C}(w) \cap \mathcal{M}_c$ is still not empty.

Lemma 4.3 Let G be an LPN system, $\mathcal{M}_c$ the set of crucial markings, and $M_b \in \mathcal{M}_b$ a basis marking. If $\beta(M_b) = 1$, there exists an observation $w \in \mathcal{L}(G)$ such that $M_b \in \mathcal{C}(w)$ and $|\mathcal{C}(w)| > 1$.

Proof: Assume that $\beta(M_b) = 1$, i.e., $|UR(M_b)| > 1$. Let $M' \in R(N, M_0)$ and $\sigma \in T^*$ such that $M'[\sigma\rangle M_b$ and $\ell(\sigma) = w$. Therefore, $M_b \in \mathcal{C}_b(w)$. By Eq. (2-3), $UR(M_b) \subseteq \mathcal{C}(w)$. Since $|UR(M_b)| > 1$, $|\mathcal{C}(w)| > 1$. □

In simple words, if $\beta(M_b) = 1$, then there exists an observation $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w)$ contains more than one marking. However, even if $\beta(M_b) = 0$ there may be another basis marking M_b' such that $M_b, M_b' \in \mathcal{C}(w)$ and $M_b' \notin UR(M_b)$. In this case, $|\mathcal{C}(w)|$ is still greater than 1.

Lemmas 4.2 and 4.3 show that constructing the BRG is not sufficient for C-detectability analysis. In the following, we construct the observer of the BRG to derive necessary and sufficient conditions for C-detectability.

4.3 Verification of C-detectability based on BRG and Observer

4.3.1 Observer of the BRG in C-detectability

We denote $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of the BRG $B = (X, E, f, x_0)$ for C-detectability, where $\mathcal{X} \subseteq 2^X$ is a finite set of nodes and $\mathcal{X}_m \subseteq \mathcal{X}$ is the set of marked states (a definition of them is provided later). The event set of the observer is the alphabet E. The transition function is $\delta : \mathcal{X} \times E \to \mathcal{X}$. The initial state is taken as $\hat{X}_0 = \{x_0\}$. Clearly, all markings in a state of B_o correspond to the markings in a set $\mathcal{C}_b(w)$, where w is the sequence of events in E^* leading from the initial state of the observer to the current state. Namely, if $\delta(\hat{X}_0, w) = \hat{X}$, then $\mathcal{C}_b(w) = \bigcup_{x \in \hat{X}} x(1)$. Therefore, the complexity of constructing B_o is $\mathcal{O}(2^{|\mathcal{M}_b|})$, which is smaller than the complexity of constructing the observer of the RG, which is equal to $\mathcal{O}(2^{|R(N,M_0)|})$.

Proposition 4.1 Let G be an LPN system, $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of its BRG, and $\mathcal{M}_c$ the set of crucial markings. There exists an observation $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w) \cap \mathcal{M}_c = \emptyset$, iff there exists a state $\hat{X} \in \mathcal{X}$ such that $\forall x \in \hat{X}$, $x(2) = 0$.

Proof: (If) Let $w \in \mathcal{L}(G)$ be an observation and $\delta(\hat{X}_0, w) = \hat{X}$. With the assumption that for all $x \in \hat{X}$, $x(2) = 0$, i.e., for all $M_b \in \mathcal{C}_b(w)$, $UR(M_b) \cap \mathcal{M}_c = \emptyset$, and by Eq. (2-3), $\mathcal{C}(w) \cap \mathcal{M}_c = \emptyset$.

(Only if) Assume that there exists $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w) \cap \mathcal{M}_c = \emptyset$. Let $\hat{X} = \delta(\hat{X}_0, w)$. By Eq. (2-3), $\bigcup_{M_b \in \mathcal{C}_b(w)} UR(M_b) \cap \mathcal{M}_c = \emptyset$. Therefore, for all $M_b \in \mathcal{C}_b(w)$, $UR(M_b) \cap \mathcal{M}_c = \emptyset$. By Eq. (4-3), for all $x \in \hat{X}$, $x(2) = 0$. □

In simple words, given a state $\hat{X} \in \mathcal{X}$, if all the triples $(M_b, \alpha(M_b), \beta(M_b))$ in $\hat{X}$ have $\alpha(M_b) = 0$, then there exists an observation $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w)$ does not contain crucial markings.

Proposition 4.2 Let G be an LPN system and $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of its BRG. There exists an observation $w \in \mathcal{L}(G)$ such that $|\mathcal{C}(w)| = 1$, iff there exists a state $\hat{X} \in \mathcal{X}$ such that $\hat{X} = \{(M_b, \alpha(M_b), 0)\}$, where M_b is a basis marking of G, and $\alpha(M_b) \in \{0, 1\}$.

Proof: (If) Assume there exists such $\hat{X} = \{(M_b, \alpha(M_b), 0)\}$, where $\alpha(M_b)$ may be either 0 or 1. Clearly, there exists an observation $w \in \mathcal{L}(G)$ such that $\delta(\hat{X}_0, w) = \hat{X}$ and $\mathcal{C}_b(w) = \{M_b\}$. Since $\beta(M_b) = 0$, i.e., $UR(M_b) = \{M_b\}$, by Eq. (2-3), $\mathcal{C}(w) = \mathcal{C}_b(w) = \{M_b\}$. Thus, $|\mathcal{C}(w)| = 1$.

(Only if) Assume there exists an observation $w \in \mathcal{L}(G)$ such that $|\mathcal{C}(w)| = 1$. By Eq. (2-3), $|\bigcup_{M_b \in \mathcal{C}_b(w)} UR(M_b)| = 1$, i.e., there is only one marking $M_b \in \mathcal{C}(w)$ and $UR(M_b) = \{M_b\}$. By Eq. (4-4), $\beta(M_b) = 0$. Then $\delta(\hat{X}_0, w) = \hat{X} = \{(M_b, \alpha(M_b), 0)\}$. □

By Proposition 4.2, given a state $\hat{X} \in \mathcal{X}$, if and only if $\hat{X}$ contains only one state $x = (M_b, \alpha(M_b), 0)$, then there exists an observation $w \in \mathcal{L}(G)$ whose corresponding $\mathcal{C}(w)$ contains only one marking M_b.

We now define the set of marked states as the set of states in B_o that contain only one or no crucial marking, namely:

$$\mathcal{X}_m = \{\hat{X} \in \mathcal{X} | \hat{X} = \{x\}, x(3) = 0\} \cup \{\hat{X} \in \mathcal{X} | \forall x \in \hat{X}, x(2) = 0\}.$$

Corollary 4.1 Let G be an LPN system, $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of its BRG, and $\mathcal{M}_c$ the set of crucial markings. Given an observation $w \in \mathcal{L}(G)$, $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w)| = 1$ holds iff $\delta(\hat{X}_0, w) \in \mathcal{X}_m$.

Proof: Follows from Propositions 4.1 and 4.2 and from the definition of the set $\mathcal{X}_m$ of marked states. □

The above proposition implies that, given an observation that leads to a marked state in the observer, its current marking can be distinguished from a crucial marking.

Example 4.5 Let us consider the LPN system in Fig. 4-4 whose T_u-induced subnet is acyclic and where $T_o = \{t_1, t_5\}$ and $T_u = \{t_2, t_3, t_4, t_6\}$. Let the set of crucial markings be $\mathcal{M}_c = \{M_0\} = \{[1\ 0\ 0\ 0\ 0\ 0]^T\}$. The LPN system has 6 reachable markings and only two

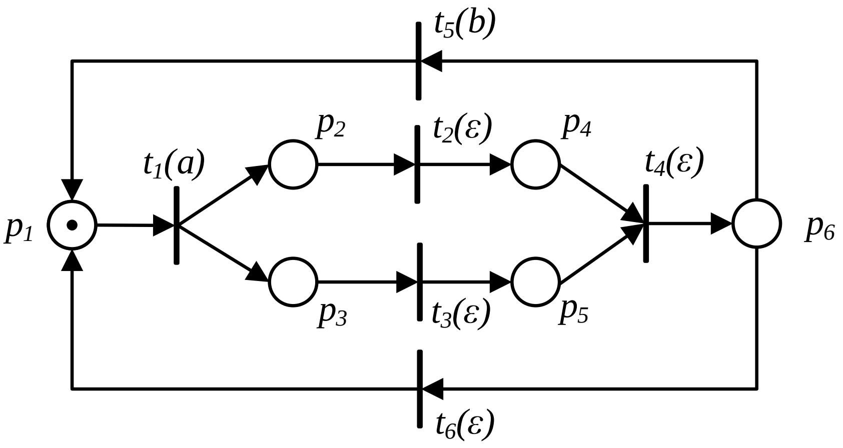


Fig. 4-4 The LPN system in Example 4.5.

of them are basis markings: $M_0 = [1\ 0\ 0\ 0\ 0\ 0]^T$ and $M_1 = [0\ 1\ 1\ 0\ 0\ 0]^T$. By Eq. (2-4), $UR(M_0) = \{M_0\}$, $\mathcal{M}_c \cap UR(M_0) \neq \emptyset$ and $|UR(M_0)| = 1$. Therefore, by Eqs. (4-3) and (4-4), respectively, $\alpha(M_0) = 1$ and $\beta(M_0) = 0$. Moreover, $UR(M_1) = R(N, M_0)$, thus $\mathcal{M}_c \cap UR(M_1) \neq \emptyset$ and $|UR(M_1)| > 1$, which imply $\alpha(M_1) = 1$ and $\beta(M_1) = 1$. Thus, the BRG for C-detectability is the graph in Fig. 4-5. The observer of the BRG for C-detectability is shown in Fig. 4-6, where $\mathcal{X}_m = \{\hat{X}_0\}$. ◇

Corollary 4.2 Let G be an LPN system and $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of its BRG. System G is strongly C-detectable if $\mathcal{X} = \mathcal{X}_m$.

Proof: Assume $\mathcal{X} = \mathcal{X}_m$. By Corollary 4.1, $\forall w \in \mathcal{L}(G), \mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w)| = 1$. Namely, for any evolution of the system, crucial markings can always be distinguished from other markings. Therefore, G is strongly C-detectable. □

In simple words, if all states of the observer are marked, we can conclude that the system is strongly C-detectable. However, the condition that all states are marked is not necessary. In the next section, sufficient and necessary conditions for C-detectability are provided based on the inspection of the cycles in the observer.

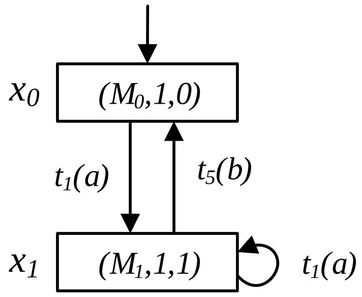


Fig. 4-5 BRG of the LPN system in Fig. 4-4.

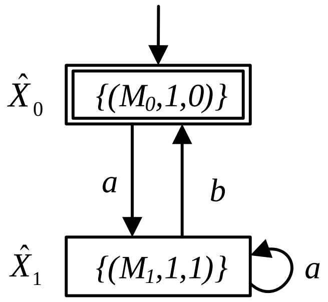


Fig. 4-6 Observer of the BRG in Fig. 4-5.

4.3.2 Verification of C-detectability

Since C-detectability considers the transition sequences of infinite length, we first study the properties of cycles in the observer. In the following, we write $\hat{X}_{ji} \in \gamma_j$ to denote that $\hat{X}_{ji}$ is a node belonging to cycle γ_j. The set of cycles in the observer is denoted by Γ.

Definition 4.6 [Unambiguous cycle] Given the set $\mathcal{M}_c$ of crucial markings, a cycle $\gamma \in \Gamma$ of the observer $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ is

- unambiguous w.r.t. $\mathcal{M}_c$ if $\forall \hat{X} \in \gamma$, $\hat{X} \in \mathcal{X}_m$;
- semi-unambiguous w.r.t. $\mathcal{M}_c$ if $\exists \hat{X} \in \gamma$, $\hat{X} \in \mathcal{X}_m$;
- ambiguous w.r.t. $\mathcal{M}_c$ if $\forall \hat{X} \in \gamma$, $\hat{X} \notin \mathcal{X}_m$.

◇

In words, if all states contained in a cycle are marked, then the cycle is said to be unambiguous since for all the observations corresponding to the nodes of the cycle, crucial markings either do not appear in the node (none of them is consistent with the observation), or the node only contains a single crucial marking (one of them is consistent with the observation, but it is not confused with other markings). Furthermore, if there exists at least one marked state in the cycle, then the cycle is said to be semi-unambiguous. Clearly, an unambiguous cycle is also semi-unambiguous, while the converse may not be true. Finally, the cycle is said to be ambiguous if the current marking is always confusable with other markings. We now prove that in an unambiguous cycle, any transition sequence consistent with the observation of the cycle satisfies the condition in Eq. (4-1).

Proposition 4.3 Let $G = (N, M_0, E, \ell)$ be an LPN system, and $\mathcal{M}_c$ the set of crucial markings. There exists an unambiguous cycle γ_j in the observer of its BRG iff there exist a finite integer $K \in \mathbb{N}$ and a transition sequence $\sigma \in L^{\infty}(G)$ such that $\forall \sigma' \preceq \sigma$ with $|w'| \geq K$, the condition in Eq. (4-1) holds, where $w' = \ell(\sigma')$.

Proof: (If) Assume that $\exists K \in \mathbb{N}$, $\exists \sigma \in L^{\infty}(G)$ such that $\forall \sigma' \preceq \sigma$ with $\ell(\sigma') = w'$, $|w'| \geq K$, $\mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w')| = 1$. Since σ has an infinite length, B_o has a finite number of nodes, and there is no cycle of unobservable transitions, eventually the tail of the path along $\ell(\sigma) = w$ will be in a cycle $\gamma_j = \hat{X}_{j1}e_{j1}\hat{X}_{j2} \ldots \hat{X}_{jk}e_{jk}\hat{X}_{j1} \in \Gamma$. Thus, w must contain the corresponding observation of γ_j, and there exist $w_0 \in E^*$ and $w_2 \preceq e_{j_1} \ldots e_{j_k}$ such that $w = w_0(e_{j1} \ldots e_{jk})^* w_2$ and $|w_0|$ is finite. Thus, for all $i \in \{1, 2, \ldots, k\}$ there exists $w' \preceq w$ such that $|w'| \geq K$ and $\delta(\hat{X}_0, w') = \hat{X}_{ji} \in \gamma_j$. Under the initial assumption and Corollary 4.1, $\hat{X}_{ji} \in \mathcal{X}_m$. Therefore, the cycle γ_j is unambiguous.

(Only if) Assume that there exists an unambiguous cycle $\gamma_j = \hat{X}_{j1}e_{j1}$ $\hat{X}_{j2} \ldots \hat{X}_{jk}e_{jk}\hat{X}_{j1} \in \Gamma$. Namely, $\forall i \in \{1, 2, \ldots, k\}$, $\hat{X}_{ji} \in \mathcal{X}_m$. Since there are no deadlocks nor cycles of unobservable transitions in the system, there exist $\sigma \in L^{\infty}(G)$ and $w_0 \in E^*$ such that $\ell(\sigma) = w_0(e_{j1} \ldots e_{jk})^*$ where $|w_0|$ is finite. Let $K = |w_0|$, $\sigma' \preceq \sigma$, $w' = \ell(\sigma')$ and $|\ell(\sigma')| \geq K$. Clearly, $\delta(\hat{X}_0, w') = \hat{X}_{ji} \in \gamma_j$ for some $i \in \{1, 2, \ldots, k\}$, i.e., eventually when $|\ell(\sigma)| \geq K$ the evolution of σ will lead $\ell(\sigma)$ to containing the observation of γ_j in the observer. Under the initial assumption and Corollary 4.1, $\mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w')| = 1$ holds. □

In other words, an unambiguous cycle $\gamma_j \in \Gamma$ in B_o, whose observation is $e_{j1} \ldots e_{jk}$, corresponds to a set of infinite length transition sequences σ such that $\ell(\sigma) = w = w_0(e_{j1} \ldots e_{jk})^* w_2$ with $w_0 \in E^*$ and $w_2 \preceq e_{j_1} \ldots e_{j_k}$. There also exists a finite integer K such that for all $w' \preceq w$ with $|w'| \geq K$, the current marking can be determined uniquely whether $\mathcal{C}(w')$ contains a crucial marking after w' has been observed.

Proposition 4.4 Let $G = (N, M_0, E, \ell)$ be an LPN system, and $\mathcal{M}_c$ the set of crucial markings. There exists a semi-unambiguous cycle γ_j in the observer of its BRG iff there exist a finite integer $K \in \mathbb{N}$ and a transition sequence $\sigma \in L^{\infty}(G)$ such that $\ell(\sigma)$ contains the observation of γ_j and $\forall \sigma' \preceq \sigma$, the condition in Eq. (4-2) holds.

Proof: (If) Assume that $\exists K \in \mathbb{N}$, $\exists \sigma \in L^{\infty}(G)$ such that $\forall \sigma' \preceq \sigma$, $\exists \sigma'' \in T^*, \ell(\sigma'\sigma'') = w' : \sigma'\sigma'' \preceq \sigma, |\ell(\sigma'')| \leq K, \mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w')| = 1$. Since σ has an infinite length, B_o has a finite number of nodes, and there is no cycle of unobservable transitions, eventually the tail of the path along $\ell(\sigma) = w$ will be in a cycle $\gamma_j = \hat{X}_{j1}e_{j1}\hat{X}_{j2} \ldots \hat{X}_{jk}$ $e_{jk}\hat{X}_{j1} \in \Gamma$. Thus, w contains the corresponding observation of γ_j, and there exist $w_0 \in E^*$ and $w_2 \preceq e_{j_1} \ldots e_{j_k}$ such that $w = w_0(e_{j1} \ldots e_{jk})^* w_2$ and $|w_0|$ is finite.

Now we prove that in γ_j there exists a marked state. Let $\sigma' \preceq \sigma$ such that $|\ell(\sigma')| \geq |w_0|$. Then, there exists $\sigma'' \in T^*$ such that $\sigma'\sigma'' \preceq \sigma$, $|\ell(\sigma'')| \leq K$, and $\delta(\hat{X}_0, w') = \hat{X}_{jr} \in \gamma_j$, where $w' = \ell(\sigma'\sigma'')$ and $r \in \{1, 2, \ldots, k\}$. Under the initial assumption and Corollary 4.1, $\hat{X}_{jr} \in \mathcal{X}_m$. Thus, the cycle γ_j is semi-unambiguous.

(Only if) Assume that there exists a semi-unambiguous cycle $\gamma_j = \hat{X}_{j1}e_{j1}\hat{X}_{j2}\ldots\hat{X}_{jk}$ $e_{jk}\hat{X}_{j1} \in \Gamma$. Namely, there exist $w \in E^*$ and $r \in \{1, 2, \ldots, k\}$ such that $\delta(\hat{X}_0, w) = \hat{X}_{jr} \in \mathcal{X}_m$. Since there are no deadlocks nor cycles of unobservable transitions in the system, there exist $\sigma \in L^\infty(G)$ and $w_0 \in E^*$ such that $\ell(\sigma) = w_0(e_{j1}\ldots e_{jk})^*$ and $|w_0|$ is finite. Let $\sigma' \preceq \sigma$ and $|w_0(e_{j1}\ldots e_{jk})| = K \in \mathbb{N}$. From Fig. 4-7, it is clear that there exists $\sigma'' \in T^*$ such that $\sigma'\sigma'' \preceq \sigma$, $|\ell(\sigma'')| \leq K$, and $\ell(\sigma'\sigma'') = w$. Under the initial assumption and Corollary 4.1, $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w)| = 1$ holds. □

In simple words, a semi-unambiguous cycle γ_j in B_o corresponds to a set of infinite length transition sequences σ whose observation contains $(e_{j1}\ldots e_{jk})^*$ and for any prefix of σ after at most K observable events, the current crucial marking can be uniquely determined. Since the observer is finite, the current crucial marking is periodically detectable. Summarizing, Proposition 4.4 (resp., Proposition 4.3) formalizes the relation between semi-unambiguous (resp., unambiguous) cycles and the estimation of crucial markings. Based on them, necessary and sufficient conditions for C-detectability are derived. In the following, a state $\hat{X}$ is said to be reachable from a cycle if there exists at least one state in the cycle from which $\hat{X}$ is reachable.

Theorem 4.1 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of its BRG. The LPN system G is strongly C-detectable w.r.t. $\mathcal{M}_c$ iff for any $\hat{X} \in \mathcal{X}$ reachable from a cycle in B_o, $\hat{X} \in \mathcal{X}_m$.

Proof: (If) Assume that all states reachable from a cycle in B_o are in $\mathcal{X}_m$. Let $\sigma \in L^\infty(G)$. Since the system is bounded and there are no cycles of unobservable transitions, the observation w of σ contains at least $w_1 \in E^*$ that corresponds to the observation of a cycle γ_j

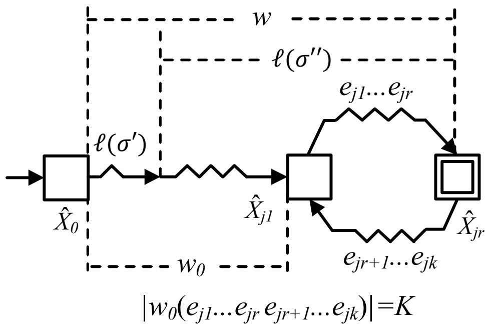


Fig. 4-7 Illustration of the proof (Only if part) of Proposition 4.4.

in B_o. Therefore, the observation of σ can be written as $w = w_0 w_1^* w_2$ where $|w_0|$ is finite, and $w_0, w_1, w_2 \in E^*$. Let $|w_0| = K$ and $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_0 w'$. Clearly, $w' \preceq w_1^* w_2$ and $|\ell(\sigma')| \geq K$. Let $\hat{X} = \delta(\hat{X}_0, w_0 w')$, i.e., $\hat{X}$ is reachable from γ_j. Under the initial assumption, $\hat{X} \in \mathcal{X}_m$. By Corollary 4.1, this means that condition $\mathcal{C}(w_0 w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w_0 w')| = 1$ holds. Therefore, the crucial marking consistent with the observation $w_0 w'$ can be certainly determined. Since the system is bounded and there are no cycles of unobservable transitions, for all $\sigma \in L^\infty(G)$ there exists an upper bound of K such that for all the prefixes σ' with $|\ell(\sigma')| \geq K$, $\ell(\sigma')$ leads to a cycle or to a state reachable from a cycle in B_o. Therefore, the system is strongly C-detectable.

(Only if) We prove this argument by justifying its contrapositive. Assume in the observer there exists a state reachable from a cycle but not in $\mathcal{X}_m$. Namely, there exist $\gamma_j = \hat{X}_{j1} e_{j1} \hat{X}_{j2} \ldots \hat{X}_{jk} e_{jk} \hat{X}_{j1} \in \Gamma$, $\hat{X}_{jr} \in \gamma_j$ ($r \in \{1, 2, \ldots, k\}$), and $w' \in E^*$ such that $\delta(\hat{X}_{jr}, w')$ is defined but $\delta(\hat{X}_{jr}, w') \notin \mathcal{X}_m$. Since there are no cycles of unobservable transitions, there exist $\sigma \in L^\infty(G)$ and $w_1, w_2 \in E^*$ such that $\ell(\sigma) = w_1 (e_{j1} e_{j2} \ldots e_{jk})^* w_2$ and $|w_1|$ is finite. Therefore, for any $K \in \mathbb{N}$, there exists $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_1 (e_{j1} e_{j2} \ldots e_{jk})^* (e_{j1} e_{j2} \ldots e_{jr}) w'$ and $|\ell(\sigma')| \geq K$, where $w' \preceq (e_{jr+1} \ldots e_{jk})$ $(e_{j1} e_{j2} \ldots e_{jk})^* w_2$. Let $w_0 = w_1 (e_{j1} e_{j2} \ldots e_{jk})^* (e_{j1} e_{j2} \ldots e_{jr})$. Clearly, $\delta(\hat{X}_0, w_0) = \hat{X}_{jr}$. With the initial assumption, $\delta(\hat{X}_0, w_0 w') = \delta(\hat{X}_{jr}, w') \notin \mathcal{X}_m$. By Corollary 4.1, this implies that $\mathcal{C}(w_0 w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w_0 w')| = 1$ does not hold. Therefore, the system is not strongly C-detectable. □

In words, an LPN system is strongly C-detectable iff any state reachable from a cycle in the observer is a marked state.

It is known that the complexity of finding all the cycles in a directed graph is NP-hard. However, finding all the strongly connected components (SCCs) is of polynomial complexity w.r.t. the size of the graph [79]. Meanwhile, Theorem 4.1 shows that C-detectability is closely related to the cycles in the observer B_o. Herein, only SCCs that contain at least one cycle (including self-loops) are considered. Note that if an SCC does not contain a cycle, then it contains only one node without self-loops. Thus, obviously, finding all the SCCs that contain at least one cycle is also of polynomial complexity w.r.t. the size of the graph. Clearly, if a state of the observer is reachable from a cycle, it is also reachable from a state in an SCC. Therefore, Theorem 4.1 can be rephrased as follows.

Corollary 4.3 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ the observer of its BRG. The LPN system G is strongly C-detectable w.r.t.

$\mathcal{M}_c$ iff for any state $\hat{X} \in \mathcal{X}$ reachable from a state in an SCC in B_o, $\hat{X} \in \mathcal{X}_m$.

Theorem 4.2 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and B_o the observer of its BRG. The LPN system G is weakly C-detectable w.r.t. $\mathcal{M}_c$ iff in B_o there exists a cycle γ_j that is unambiguous w.r.t. $\mathcal{M}_c$.

Proof: Follows from Proposition 4.3. □

Note that differently from strong C-detectability, the necessary and sufficient condition for weak C-detectability cannot be reformulated in terms of SCCs. Indeed, the existence of an unambiguous cycle does not imply that there exists an SCC whose nodes are all marked states. However, the converse is true. This allows us to derive the following sufficient condition for weak C-detectability.

Corollary 4.4 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and B_o the observer of its BRG. The LPN system G is weakly C-detectable w.r.t. $\mathcal{M}_c$ if there exists an SCC in B_o such that all its nodes are in $\mathcal{X}_m$.

Theorem 4.3 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and B_o the observer of its BRG. The LPN system G is periodically strongly C-detectable w.r.t. $\mathcal{M}_c$ iff all cycles in B_o are semi-unambiguous w.r.t. $\mathcal{M}_c$.

Proof: Follows from Proposition 4.4. □

We point out that even if each SCC contains at least one marked state, not all cycles are necessarily semi-unambiguous. Therefore, the condition for periodically strong C-detectability cannot be reformulated in terms of SCCs.

The following theorem provides a necessary and sufficient condition for periodically weak C-detectability.

Theorem 4.4 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and B_o the observer of its BRG. The LPN system G is periodically weakly C-detectable w.r.t. $\mathcal{M}_c$ iff there exists a cycle in B_o that is semi-unambiguous w.r.t. $\mathcal{M}_c$.

Proof: Follows from Proposition 4.4. □

Now, if B_o contains a semi-unambiguous cycle, then it also contains an SCC where there is at least one marked state, and the other way around. Thus, necessary and sufficient conditions for periodically weak C-detectability can be reformulated as the following corollary.

Corollary 4.5 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and B_o the observer of its BRG. The LPN system G is periodically weakly C-detectable w.r.t. $\mathcal{M}_c$ iff in B_o there exists an SCC such that at least one of its node belongs to $\mathcal{X}_m$.

The following result can be trivially derived from the previous ones.

Corollary 4.6 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and B_o the observer of its BRG. If all cycles in B_o are ambiguous, G does not satisfy any C-detectability property w.r.t. $\mathcal{M}_c$.

The above results show that, rather than enumerating all reachable markings and constructing the observer of the RG, all the four types of C-detectability can be verified through the observer of the BRG. In [23], a structure called detector is proposed to verify strong detectability and strong periodic detectability. Even though the size of the detector is polynomial w.r.t. the number of states of the system, it cannot be used to verify weak and weak periodic detectability. On the contrary, the observer of the BRG can be used to verify all the C-detectability properties. Furthermore, if the set of crucial markings is changed, only functions α and β should be updated.

By Theorems 4.1, 4.2, 4.3 and 4.4, efficient approaches are proposed to necessarily and sufficiently verify the four considered C-detectability properties of an LPN system by analyzing all cycles in the observer B_o of its BRG. The complexity of constructing B_o is $\mathcal{O}(2^{|\mathcal{M}_b|})$, which is much smaller than the RG-based approaches. Furthermore, since the problem of finding all cycles is NP-hard, we prove that strong C-detectability and periodically weak C-detectability can be verified by just computing all the SCCs in the observer, which is of polynomial complexity w.r.t. the size of the observer. Therefore, the complexity of the proposed approaches is further reduced.

In the following subsection, we show that, when the set of crucial markings is described by a set of linear constraints, the values of α and β functions can be determined by solving appropriate integer linear programming problems.

4.3.3 Crucial markings in terms of GMECs

It is well-known that generalized mutual exclusion constraints (GMECs) [90] describe convex sets of markings. This allows us to take advantage of integer linear programming in the solution to several problems. We now discuss how the analysis of the above C-decidability properties can be simplified if the set of crucial markings is described by a set of GMECs, namely,

$$\mathcal{M}_c = (W, K) = \bigcap_{i=1}^{r} \{M \in \mathbb{N}^m | w_i^T \cdot M \leq k_i\},$$

where $w_i \in \mathbb{Z}^m$ and $k_i \in \mathbb{Z}$ with $i = 1, 2, \cdots, r$. Such a set of GMECs can also be written as $\mathcal{M}_c = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$, where $W = [w_1, w_2, \cdots, w_r]^T$ and $K = [k_1, k_2, \cdots, k_r]^T$. In addition, the following constraint sets are also defined.

Definition 4.7 Let $M \in R(N, M_0)$ be a marking of an LPN system $G = (N, M_0, E, \ell)$, and $\mathcal{M}_c = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$ the set of crucial markings.

- The $\mathcal{Y}(M)$-constraint set is defined by

$$\mathcal{Y}(M) = \begin{cases} M' = M + C_u \cdot y_u \\ W \cdot M' \leq K \\ M' \in \mathbb{N}^m \\ y_u \in \mathbb{N}^{n_u} \end{cases} \tag{4-6}$$

- The $\mathcal{Z}(M)$-constraint set is defined by

$$\mathcal{Z}(M) = \begin{cases} M' = M + C_u \cdot y_u \\ M' \in \mathbb{N}^m \\ y_u \in \mathbb{N}_{\geq 1}^{n_u} \end{cases} \tag{4-7}$$

◇

In Eqs. (4-6) and (4-7), $M' = M + C_u \cdot y_u$ describes a marking M' reachable from M by firing only unobservable transitions. In Eq. (4-6), $W \cdot M' \leq K$ implies that $M' \in \mathcal{M}_c$. The following corollary shows that the values of $\alpha(M_b)$ and $\beta(M_b)$ associated with a given basis marking M_b can be computed looking at the feasibility of the two constraint sets $\mathcal{Y}(M)$ and $\mathcal{Z}(M)$, respectively.

Corollary 4.7 Given a basis marking $M_b \in \mathcal{M}_b$ of an LPN system G and $\mathcal{M}_c = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$ the set of crucial markings,

1. $\alpha(M_b) = 1$ iff the $\mathcal{Y}(M_b)$-constraint set is feasible;
2. $\beta(M_b) = 1$ iff the $\mathcal{Z}(M_b)$-constraint set is feasible.

Proof: We prove the two statements separately, providing a series of iff conditions.

(Statement 1)

$\alpha(M_b) = 1$

$\Leftrightarrow \mathcal{M}_c \cap UR(M_b) \neq \emptyset$ [by Eq. (4-3)]

$\Leftrightarrow \exists y_u \in \mathbb{N}^{n_u} : M_b + C_u \cdot y_u = M \in \mathbb{N}^m$ and $W \cdot M \leq K$ [by Eq. (2-4)]

$\Leftrightarrow$The $\mathcal{Y}(M_b)$-constraint set is feasible [by Eq. (4-6)].

(Statement 2)

$\beta(M_b) = 1$

$\Leftrightarrow |UR(M_b)| > 1$ [by Eq. (4-4)]

$\Leftrightarrow \exists y_u \in \mathbb{N}^{n_u}_{\geq 1} : \ M_b + C_u \cdot y_u \geq \vec{0}$ [by Lemma 4.1]

$\Leftrightarrow$The $\mathcal{Z}(M_b)$-constraint set is feasible [by Eq. (4-7)].

□

Based on Corollary 4.7, the construction of the BRG for C-detectability requires the solution to a certain number of integer linear programming problems (ILPPs). However, for some net structures (see [6]) the complexity of constructing the BRG can be reduced by relaxing ILPPs into linear programming problems (LPPs).

Example 4.6 Consider again the LPN system in Fig. 4-4. Let the set of crucial markings be $\mathcal{M}_c = \{M \in \mathbb{N}^6 | M(p_1) \geq 1\}$, i.e., $W = [-1\ 0\ 0\ 0\ 0\ 0]$ and $K = -1$. By solving Eq. (4-6), $\alpha(M_0) = 1$ and $\alpha(M_1) = 0$. By solving Eq. (4-7), $\beta(M_0) = 0$ and $\beta(M_1) = 1$. Therefore, the BRG for C-detectability is identical to the one in Fig. 4-5 and the observer is identical to the one in Fig. 4-6 and $\mathcal{X}_m = \{\hat{X}_0\}$.

There is no unambiguous cycle in the observer. Thus by Theorems 4.1 and 4.2, the LPN system is neither strongly detectable nor weakly detectable w.r.t. $\mathcal{M}_c$. On the other hand, there is a cycle $\gamma_1 = \hat{X}_0 a \hat{X}_1 b \hat{X}_0$ containing the marked state $\hat{X}_0$. By Definition 4.6, γ_1 is semi-unambiguous. Therefore, by Theorem 4.4 the LPN system is periodically weakly C-detectable w.r.t. $\mathcal{M}_c$. However, there also exists a cycle $\gamma_2 = \hat{X}_1 a \hat{X}_1$ that is not semi-unambiguous, thus by Theorem 4.3 the LPN system is not periodically strongly C-detectable.

◇

4.3.4 Computation of the smallest value of $\boldsymbol{K}$ in Definitions 4.2 to 4.5

In practical problems, in addition to establishing if a system satisfies a certain C-detectability property, it is important to compute the smallest number of observed events after which the states of interest are distinguished, or periodically distinguished. By Definitions 4.2 to 4.5，if a system satisfies a certain C-detectability property, K may take infinite values. In more detail, if a property holds for a certain K, then it holds for any $K' > K$. Thus, it is important to compute the smallest values of K in Definitions 4.2 to 4.5. The four values are called $\bar{K}_s$, $\bar{K}_{sp}$, $\bar{K}_w$ and $\bar{K}_{wp}$, respectively. In the following, given a LPN system G, and the observer $B_o = (\mathcal{X}, E, \delta, \hat{X}_0, \mathcal{X}_m)$ of its BRG, we show that the four values can be calculated by looking at the observer B_o.

• When system G satisfies strong C-detectability, $\bar{K}_s$ can be calculated as follows:

1. Compute the longest path L from $\hat{X}_0$ to the nodes in $\mathcal{X} \setminus \mathcal{X}_m$ in B_o;
2. Let $\bar{K}_s = |L|$, where $|L|$ denotes the number of nodes in L.

• When system G satisfies periodically strong C-detectability, $\bar{K}_{sp}$ can be calculated as follows:

1. Compute B_o' by removing all marked nodes and their connected transitions in B_o;
2. Compute the longest path L in B_o';
3. Let $\bar{K}_{sp} = |L|$.

• When system G satisfies weak C-detectability, $\bar{K}_w$ can be calculated as follows:

1. Compute the set Γ of elementary cycles in B_o only including nodes in $\mathcal{X}_m$;
2. For all cycles $\gamma_i \in \Gamma$, compute the set S_i of paths including no cycle from $\hat{X}_0$ to γ_i;
3. For all path $s_{i,j} \in S_i$, compute the longest path $L_{i,j}$ from $\hat{X}_0$ to non-marked notes in $s_{i,j}$;
4. Let $\bar{K}_w = \underset{i:\gamma_i\in\Gamma;j:s_{i,j}\in S_i}{min}(|L_{i,j}|)$.

• When system G satisfies periodically weak C-detectability, $\bar{K}_{wp}$ can be calculated as follows:

1. Compute the set Γ of elementary cycles in B_o such that there exists nodes belong to $\mathcal{X}_m$;
2. For all cycles $\gamma_i \in \Gamma$, compute the set S_i of paths including no cycle from $\hat{X}_0$ to γ_i;
3. For all path $s_{i,j} \in S_i$, connect $s_{i,j}$ with its correspond cycle γ_i to obtain $s_{i,j}'$;
4. Remove all marked nodes and their connected transitions in $s_{i,j}'$, and compute the longest path $L_{i,j}$ in the remaining part;
5. Let $\bar{K}_{wp} = \underset{i:\gamma_i\in\Gamma;j:s_{i,j}\in S_i}{min}(|L_{i,j}|)$.

4.4 Verification of C-detectability based on BRG and Detector

In this section, we show how the detector of the BRG can be used to verify strong C-detectability and strong periodic C-detectability.

4.4.1 Detector of the BRG in C-detectability

In [23], the detector is proposed to check, in polynomial time, whether an automaton system satisfies strong (periodic) detectability property. Now, we construct the detector of the BRG for the verification in the framework of Petri nets. We denote $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of the BRG $B = (X, E, f, x_0)$ for detectability, where $Q \subseteq 2^X$ is a finite set of states and $Q_m \subseteq Q$ is the set of marked states (a definition of them is provided later). The initial state of B_d is $q_0 = \{x_0\}$, and the other states of B_d are subsets of X with cardinality at most equal to 2. The event set of the detector is the alphabet E. The transition function $f_d : Q \times E \to 2^Q$ is defined in Algorithm 2. The complexity of constructing it is polynomial w.r.t. the size of the BRG, which is $\mathcal{O}(|E||\mathcal{M}_b|^4)$.

Proposition 4.5 Let G be an LPN system, $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG, and $\mathcal{M}_c$ the set of crucial markings. There exists an observation $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset$, iff there exists a state $q \in Q$ such that $\exists x \in q$, $x(2) = 1$.

Proof: (If) Let $w \in \mathcal{L}(G)$ be an observation and $q \in f_d(q_0, w)$. With the assumption that there exists $x \in q$, $x(2) = 1$, i.e., there exists $M_b \in \mathcal{C}_b(w)$, $UR(M_b) \cap \mathcal{M}_c \neq \emptyset$, and by Proposition 2.1, $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset$.

(Only if) Assume that there exists $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset$. By Proposition 2.1, $\bigcup_{M_b \in \mathcal{C}_b(w)} UR(M_b) \cap \mathcal{M}_c \neq \emptyset$. Therefore, there exists $M_b \in \mathcal{C}_b(w)$, $UR(M_b) \cap \mathcal{M}_c \neq \emptyset$. According to the construction of the detector, there exists a state $q \in f_d(q_0, w)$, such that $\exists x \in q$, $x(2) = 1$. □

In words, given a state $q \in Q$, if there exists a triple $(M_b, \alpha(M_b), \beta(M_b))$ in q have $\alpha(M_b) = 1$, then there exists an observation $w \in \mathcal{L}(G)$ such that $\mathcal{C}(w)$ contains crucial markings.

Proposition 4.6 Let G be an LPN system and $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG. There exists an observation $w \in \mathcal{L}(G)$ such that $|\mathcal{C}(w)| \neq 1$, iff there exists a state $q \in Q$ such that $|q| = 2$ or $\exists x \in q$ such that $x(3) = 1$.

Proof: (If) Assume that there exists a state $q \in Q$ such that $|q| = 2$ or $\exists x \in q$ with $x(3) = 1$. If $x(3) = 1$, by Lemma 4.3, there exists an observation $w \in E^*$ such that

$|\mathcal{C}(w)| \neq 1$. If $|q| = 2$, let $q = \{x_1, x_2\}$, $x_1 \neq x_2$. According to the construction of the detector, there exists an observation w such that $q \in f_d(q_0, w)$, $q = \{x_1, x_2\}$ and $x_1 \neq x_2$. Thus $x_1(1), x_2(1) \in \mathcal{C}(w)$. Therefore, $|\mathcal{C}(w)| \neq 1$.

(Only if) Assume that there exists an observation $w \in E^*$ such that $|\mathcal{C}(w)| \neq 1$, thus there exist two different markings $M_1, M_2 \in \mathcal{C}(w)$ with $M_1 \neq M_2$. According to the construction of the detector, if $M_1, M_2 \in \mathcal{C}_b(w)$, then there exists a state $q \in Q$ such that $|q| = 2$; if either M_1 or M_2 not in $\mathcal{C}_b(w)$, by Proposition 2.1, there exists at least one state $q \in Q$ containing a state x of the BRG such that $x(3) = 1$. □

By Proposition 4.6, in an LPN system, there exists an observation w such that $\mathcal{C}(w)$ contains more than one marking, iff there exists a state q in the detector such that $|q| = 2$ or $\exists x \in q$ that $x(3) = 1$.

We now define the set of marked states as the set of states in B_d that contain only one or no crucial marking, namely:

$$Q_m = \{q \in Q | q = \{x\}, x(3) = 0\} \cup \{q \in Q | \forall x \in q, x(2) = 0\}.$$

Proposition 4.7 Let G be an LPN system, $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG, and $\mathcal{M}_c$ the set of crucial markings. Given an observation $w \in \mathcal{L}(G)$, $\mathcal{C}(w) \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w)| \neq 1$ holds iff there exists a state $q \in f_d(q_0, w)$ such that $q \notin Q_m$.

Proof: Follows from Propositions 4.5 and 4.6. □

4.4.2 Verification of C-detectability

Based on Proposition 4.7, a sufficient condition for strong C-detectability can be easily obtained.

Corollary 4.8 Let G be an LPN system and $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG. System G is strongly C-detectable if $Q = Q_m$.

The following necessary and sufficient condition for strong C-detectability is also derived from Proposition 4.7.

Theorem 4.5 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG. The LPN system G is strongly C-detectable w.r.t. $\mathcal{M}_c$ iff for any $q \in Q$ reachable from a cycle in B_d, $q \in Q_m$.

Proof: (If) By contrapositive. Assume that system G is not strongly C-detectable. This implies that for all $K \in \mathbb{N}$, there exists $\sigma \in L^{\infty}(G)$ such that $\exists \sigma' \preceq \sigma$, with $w' = \ell(\sigma')$, $|w'| \geq K, \mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w')| \neq 1$. Since σ has an infinite length, B_d has a finite number of nodes, and there is no cycle of unobservable transitions, the path along $\ell(\sigma) = w$ must contain a cycle $\gamma_j = q_{j1}e_{j1}q_{j2}\ldots q_{jk}e_{jk}q_{j1}$. Thus the observation of σ can be written as $w = w_0(e_{j1}\ldots e_{jk})^n w_2$, where $|w_0|$ is finite, $n \in \{1, 2, 3, \ldots\}$ and $w_0, w_2 \in E^*$. Let $K = |w_0|$. Then, there exists $w' = \ell(\sigma') = w_0 w''$ such that $|w'| \geq K$ and $w'' \preceq (e_{j1}\ldots e_{jk})^n w_2$. Under the initial assumption that $\mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset$ and $|\mathcal{C}(w')| \neq 1$, by Proposition 4.7, there exists a state $q \in f_d(q_0, w_0 w'')$ such that $q \notin Q_m$. Namely, there exists a state q reachable from a cycle in B_d such that $q \notin Q_m$.

(Only if) By contrapositive. Assume in the detector there exists a state q reachable from a cycle but $q \notin Q_m$. Namely, there exist $\gamma_j = q_{j1}e_{j1}q_{j2}\ldots q_{jk}e_{jk}q_{j1}$, $q_{jr} \in \gamma_j$ ($r \in \{1, 2, \ldots, k\}$), and $w' \in E^*$ such that $q \in f_d(q_{jr}, w')$ and $q \notin Q_m$. Since there are no cycles of unobservable transitions, there exist $\sigma \in L^{\infty}(G)$ and $w_1, w_2 \in E^*$ such that $\ell(\sigma) = w_1(e_{j1}e_{j2}\ldots e_{jk})^n w_2$, $n \in \{1, 2, 3, \ldots\}$ and $|w_1|$ is finite. Therefore, for any $K \in \mathbb{N}$, there exists $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_1(e_{j1}e_{j2}\ldots e_{jk})^m(e_{j1}e_{j2}\ldots e_{jr})w'$ and $|\ell(\sigma')| \geq K$, where $w' \preceq (e_{jr+1}\ldots e_{jk})(e_{j1}e_{j2}\ldots e_{jk})^k w_2$ and $m + k + 1 = n$. Let $w_0 = w_1(e_{j1}e_{j2}\ldots e_{jk})^m(e_{j1}e_{j2}\ldots e_{jr})$. Clearly, $q_{jr} \in f_d(q_0, w_0)$. With the initial assumption, $q \in f_d(q_{jr}, w') = f_d(q_0, w_0 w')$ and $q \notin Q_m$. By Proposition 4.7, this implies that $\mathcal{C}(w_0 w') \cap \mathcal{M}_c \neq \emptyset$ and $|\mathcal{C}(w_0 w')| \neq 1$. Therefore, the system is not strongly C-detectable.

□

In words, an LPN system is strongly C-detectable iff any state reachable from a cycle in the detector is a marked state. Here, we can also take advantages from SCCs. Thus Theorem 4.5 can be rewritten as follows.

Corollary 4.9 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG. The LPN system G is strongly C-detectable w.r.t. $\mathcal{M}_c$ iff for any $q \in Q$ reachable from an SCC in B_d, $q \in Q_m$.

Now, we present necessary and sufficient conditions for periodically strong C-detectability.

Theorem 4.6 Let G be an LPN system, $\mathcal{M}_c$ a set of crucial markings, and $B_d = (Q, E, f_d, q_0, Q_m)$ the detector of its BRG. The LPN system G is periodically strongly C-detectable w.r.t. $\mathcal{M}_c$ iff for any cycle γ_j in B_d, $\exists q \in \gamma_j$, $q \in Q_m$.

Proof: (If) By contrapositive. Assume that the LPN system G is not periodically strongly C-detectable. This implies that for all $K \in \mathbb{N}$, there exists a transition sequence $\sigma \in L^{\infty}(G)$ with a prefix $\sigma' \preceq \sigma$ such that $\forall \sigma'' \in T^*, \sigma'\sigma'' \preceq \sigma, |\ell(\sigma'')| \leq K, \mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset \Rightarrow |\mathcal{C}(w')| \neq 1$ where $w' = \ell(\sigma'\sigma'')$. Since σ has an infinite length, B_d has a finite number of nodes, and there is no cycle of unobservable transitions, eventually the tail of the path along $\ell(\sigma) = w$ will be in a cycle $\gamma_j = q_{j1}e_{j1}q_{j2}\ldots q_{jk}e_{jk}q_{j1}$. Thus, w contains the corresponding observation of γ_j, and there exist $w_0 \in E^*$ and $w_2 \preceq e_{j_1}\ldots e_{j_k}$ such that $w = w_0(e_{j1}\ldots e_{jk})^n w_2$, $|w_0|$ is finite and $n \in \{1, 2, 3, \ldots\}$. Let $\sigma' \preceq \sigma$ such that $|\ell(\sigma')| \geq |w_0|$. Then, for all $\sigma'' \in T^*$ such that $\sigma'\sigma'' \preceq \sigma$, $|\ell(\sigma'')| \leq K$, $q_{jr} \in \gamma_j$ and $q_{jr} \in f_d(q_0, w')$, where $w' = \ell(\sigma'\sigma'')$ and $r \in \{1, 2, \ldots, k\}$. Under the initial assumption that $\mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset$ and $|\mathcal{C}(w')| \neq 1$, by Proposition 4.7, $q_r \in f_d(q_0, w')$ such that $q_r \notin Q_m$. Namely, for all $q_r \in \gamma_j$, $q_r \notin Q_m$.

(Only if) By contrapositive. Assume that there exists a cycle $\gamma_j = q_{j1}e_{j1}q_{j2}\ldots q_{jk}$ $e_{jk}q_{j1}$ in B_d and $\forall q_{jr} \in \gamma_j$, $q_r \notin Q_m$. Since there are no deadlocks nor cycles of unobservable transitions in the system, there exist $\sigma \in L^{\infty}(G)$ and $w_0 \in E^*$ such that $\ell(\sigma) = w_0(e_{j1}\ldots e_{jk})^*$ and $|w_0|$ is finite. Let $\sigma' \preceq \sigma$ such that $\ell(\sigma') = w_0$. Then for all $K \in \mathbb{N}$, $\forall \sigma'' \in T^*, \sigma'\sigma'' \preceq \sigma, \ell(\sigma'\sigma'') = w', |\ell(\sigma'')| \leq K$ such that $q_{jr} \in f_d(q_0, w')$ and $q_{jr} \in \gamma_j$. Under the initial assumption that $q_r \notin Q_m$, by Proposition 4.7, this implies that $\mathcal{C}(w') \cap \mathcal{M}_c \neq \emptyset$ and $|\mathcal{C}(w')| \neq 1$. Therefore, the system is not periodically strongly C-detectable. □

Therefore, a bounded LPN system is strongly periodically C-detectable iff in the detector of the BRG, all the cycles contain a state in Q_m.

Example 4.7 Consider the LPN system in Fig. 4-8, where $T_o = \{t_2, t_3, t_4, t_5, t_7, t_9\}$, $T_u = \{t_1, t_6, t_8\}$. There are 7 reachable markings in the LPN system, and only 5 of them are basis markings, where $M_0 = p_1$, $M_2 = p_3 + p_4$, $M_3 = p_5$, $M_4 = p_3 + p_6$, and $M_5 = p_3 + p_7$. Let the set of crucial markings be $\mathcal{M}_c = \{M \in \mathbb{N}^8 | M(p_5) \geq 1\} \cup \{M \in \mathbb{N}^8 | M(p_8) \geq 1\}$, i.e., $W = [0\ 0\ 0\ 0\ -1\ 0\ 0\ -1]$ and $K = -1$. Consider the basis marking M_3 and M_4. By solving Eq. (4-6), $\alpha(M_3) = 1$ and $\alpha(M_4) = 4$. By solving Eq. (4-7), $\beta(M_3) = 0$ and $\beta(M_4) = 1$. Therefore, the BRG for C-detectability is identical to the one in Fig. 4-9 and the detector is identical to the one in Fig. 4-10.

According to Fig. 4-10, there are 4 cycles in the detector. Namely, $\gamma_1 = \{(M_2, 0, 0)\}$ $b\{(M_3, 1, 0), (M_4, 1, 1)\}d\{(M_2, 0, 0)\}$, $\gamma_2 = \{(M_2, 0, 0)\}b\{(M_3, 1, 0), (M_5, 1, 1)\}$ $d\{(M_2, 0, 0)\}$, $\gamma_3 = \{(M_2, 0, 0)\}b\{(M_4, 1, 1), (M_5, 1, 1)\}d\{(M_2, 0, 0)\}$, and

$\gamma_4 = \{(M_3, 1, 0)\}c\{(M_3, 1, 0)\}$. There exist states in the cycles that are not marked state, e.g., $\{(M_3, 1, 0)$ and $(M_4, 1, 1)\}$. Thus, by Theorems 4.5, the LPN system is not strongly C-detectable w.r.t. $\mathcal{M}_c$. On the other hand, there exists at least one marked state in each cycle, e.g., $\{(M_2, 0, 0)\}$ and $\{(M_3, 1, 0)\}$. Thus, by Theorem 4.6, the LPN system is periodically strongly C-detectable w.r.t. $\mathcal{M}_c$. ◇

Therefore, rather than enumerating all reachable markings and constructing the detector of the RG, strong C-detectability and strong periodic C-detectability can be verified through the detector of the BRG.

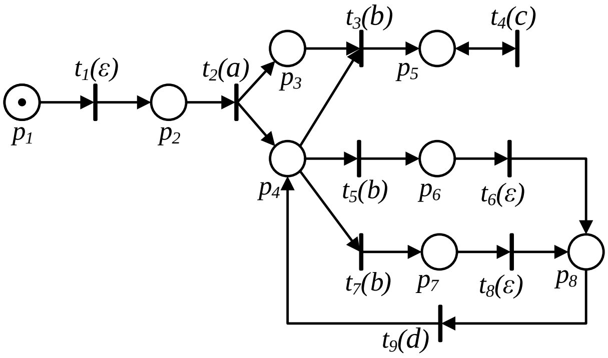


Fig. 4-8 The LPN system in Example 4.7.

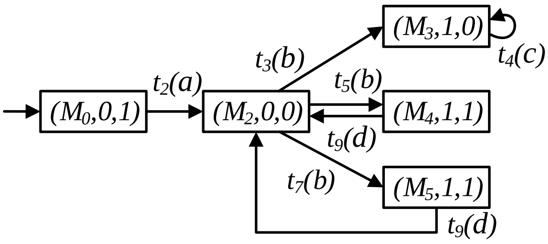


Fig. 4-9 The BRG of the LPN system in Fig. 4-8.

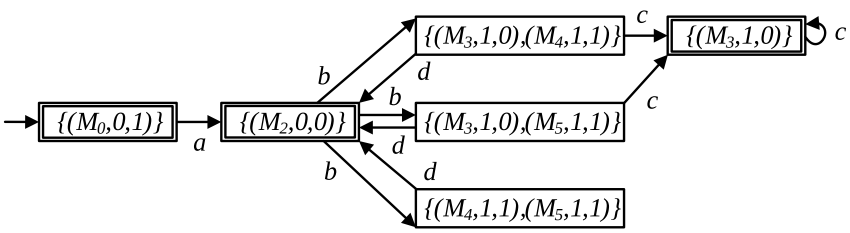

$\{(M_3,1,0),(M_4,1,1)\}$
c
$\{(M_3,1,0)\}$
c
b
d
b
c
$\{(M_0,0,1)\}$
$\{(M_2,0,0)\}$
$\{(M_3,1,0),(M_5,1,1)\}$
a
d
b
d
$\{(M_4,1,1),(M_5,1,1)\}$

Fig. 4-10 The detector of the BRG in Fig. 4-9.

4.5 Comparison of the proposed Methods

To compare the proposed approaches, a series of numerical examples are presented. To implement the approaches proposed in this work, we developed MATLAB codes [91] to compute the RG, the BRG, the observer and the detector to analyze the C-detectability properties of a bounded LPN system. Computations are performed using MATLAB on a laptop with Intel i7-7700 CPU 3.6GHz processor and 8G DDR3 RAM.

4.5.1 Comparison of the BRG-based method and the RG-based method

Now we first compare the BRG-based method with the RG-based method. Let us consider the LPN system in Fig. 4-11 whose T_u-induced subnet is acyclic, and where $T_o = \{t_1, t_7, t_8, t_9\}$ and $T_u = \{t_2, t_3, t_4, t_5, t_6\}$. The initial marking in place p_1 is a parameter $k \in \{2, 3, \cdots\}$. Let
$\mathcal{M}_c = \{M \in \mathbb{N}^{10} | W \cdot M \leq K\}, W = [\begin{array}{cccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{array}]$, and $K = -2$.

Time (in seconds) to compute the RG, the BRG and the observer for different values of k is reported in Table 4-1. Correspondingly, results relative to the four types of C-detectability for the different values of k are summarized in Table 4-2.

- In Table 4-1, Columns 2 and 3 illustrate the number of reachable markings $|R(N, M_0)|$ and the number of basis markings $|\mathcal{M}_b|$, respectively. Column 6 shows the number of states of the observer of the BRG $|\mathcal{X}|$. Note that the observers of the RG and the BRG always have the same number of states [6].

- In Table 4-1, the corresponding time (in seconds) is presented in Columns 4, 5, 7 and 8, where Columns 4 and 5 illustrate the time to compute $R(N, M_0)$ and $\mathcal{M}_b$, respectively. Columns 7 and 8 show the time to compute observers of RG and BRG, respectively. In Table 4-1 "o.t." means out of time, in the case where the tool did not halt within 10 hours.

- In Table 4-2, Columns 2 to 5 summarize the properties satisfied by the LPN system for the different values of k in Table 4-1."SCD", "WCD", "PSCD" and "PWCD" stand for strong C-detectability, weak C-detect-ability, periodically strong C-detectability, and periodically weak C-detectability, respectively. "Y" means that the LPN system satisfies the property, and

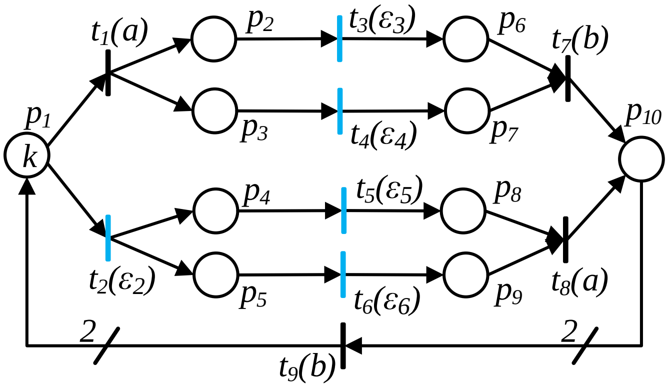


Fig. 4-11 The LPN system considered in Section 4.5.

"N" means that the LPN system does not satisfy the property.

Table 4-1 Cardinality of sets $R(N, M_0)$, $\mathcal{M}_b$, $|\mathcal{X}|$ and time to compute them (in seconds) for different values of k in Fig. 4-11.

k	$\|R(N, M_0)\|$	$\|\mathcal{M}_b\|$	T_r	T_b	$\|\mathcal{X}\|$	T_{r_o}	T_{b_o}
2	53	6	0.01s	1.52s	6	0.07s	1.54s
3	200	10	0.14s	2.97s	10	0.43s	2.99s
4	606	15	1.42s	5.48s	15	2.72s	5.54s
5	1572	21	10.89s	7.68s	21	15.40s	7.75s
6	3630	28	62.22s	10.93s	28	79.20s	11.03s
7	7656	36	328.05s	13.93s	36	389.13s	14.07s
8	15015	45	1205.80s	18.11s	45	1385.40s	18.30s
9	27742	55	4382.00s	27.07s	55	4915.20s	27.34s
10	48763	66	14478.00s	28.24s	66	16007.00s	28.59s
11	o.t.	78	o.t.	38.37s	78	o.t.	38.83s
15	o.t.	136	o.t.	62.04s	136	o.t.	63.10s
20	o.t.	231	o.t.	106.23s	231	o.t.	108.46s

Table 4-2 The analysis results of the four detectability properties for the different values of k.

k	SCD	WCD	PSCD	PWCD
2	N	N	Y	Y
3	N	N	Y	Y
4	N	N	N	Y
5	N	N	N	Y
6	N	N	N	Y
7	N	N	N	Y
8	N	N	N	Y
9	N	N	N	Y
10	N	N	N	Y
11	N	N	N	Y
15	N	N	N	Y
20	N	N	N	Y

The following conclusions can be drawn from the results in Tables 4-1 and 4-2.

- The number of reachable markings is much larger than that of basis markings.
- When k is larger than 4, the time needed to compute the observer of the RG is much longer and grows faster than that required to compute the observer of the BRG. This implies that using the RG-based approaches to analyze C-detectability becomes infeasible when the state space becomes larger and larger.
- Table 4-2 shows that in the considered examples C-detectability properties depend on the value of k.

In summary, the BRG-based method are practically efficient in particular for large-size Petri net systems.

4.5.2 Comparison of the observer-based method and the detector-based method

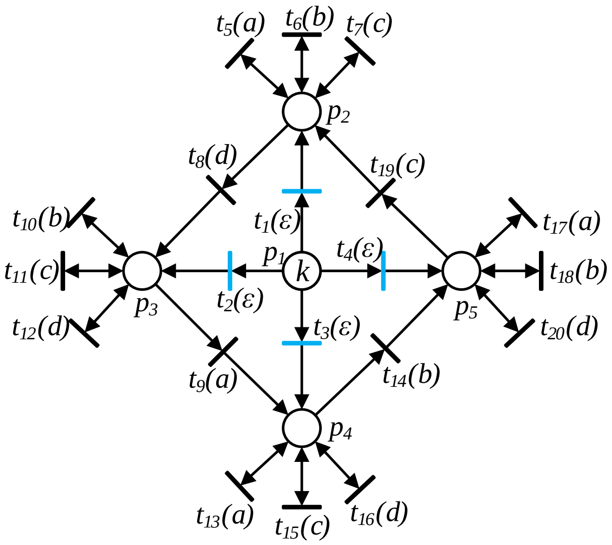


Fig. 4-12 The LPN system considered in Section 4.5.2.

Let us consider the LPN system in Fig. 4-12 whose T_u-induced subnet is acyclic, and where $T_u = \{t_1, t_2, t_3, t_4\}$, $T_o = \{t_5, t_6, \cdots, t_{20}\}$. The initial marking in place p_1 is a parameter $k \in \{1, 2, \cdots\}$. Let

$\mathcal{M}_c = \{M \in \mathbb{N}^{10} | W \cdot M \leq K\}$, $W = [\ 0 \quad 0 \quad 0 \quad 0 \quad -1\ ]$, and $K = -2$。

Table 4-3 reports the number of markings in the BRG of the LPN system, the observer, and the detector for different values of k. Correspondingly, time (in seconds) to compute them, as well as the results relative to the two C-detectability properties for the different values of k, are also summarized in Table 4-3.

- In Table 4-3, Column 2 illustrates the number of basis markings of the LPN system. Columns 3 and 4 show the number of states in the observer, the detector, respectively.
- In Table 4-3, the corresponding time (in seconds) is presented in Columns 5 and 6, which illustrate the time to compute observer and detector, respectively. In Table 4-3 "o.t."

Table 4-3 The results for different values of k in Fig. 4-12

k	$\lvert\mathcal{M}_b\rvert$	$\lvert\mathcal{X}\rvert$	$\lvert Q\rvert$	T_{b_o}	T_{b_d}	SCD	PSCD
1	5	15	11	0.53s	0.42s	Y	Y
2	15	91	92	2.89s	1.71s	N	N
3	35	771	562	37.98s	8.62s	N	N
4	70	8277	2347	835.65s	85.12s	N	N
5	126	85231	7751	20094.25s	956.31s	N	N
6	210	o.t.	21737	o.t.	8994.41s	N	N

means out of time, in the case where the tool did not halt within 10 hours.

- In Table 4-3, Columns 7 and 8 summarize the properties satisfied by the LPN system for the different values of k. “SCD” and “PSCD” stand for strong C-detectability and strong periodic C-detectability, respectively. “Y” means that the LPN system satisfies the property, and “N” means that the LPN system does not satisfy the property.

The following conclusions can be drawn from the results in Table 4-3.

- When k is larger than 2, the number of states of the detector is smaller than that of the observer.
- Whatever the value of k, the time needed to compute the detector of the BRG is much shorter and grows slower than that required to compute the the observer.
- Table 4-3 shows that in the considered examples C-detectability properties depend on the value of k.

In summary, BRG-detector method is practically more efficient for large-size Petri net systems than BRG-observer method.

4.6 Conclusions

In this chapter, four different C-detectability properties of labeled Petri net systems are proposed and approaches to verify them are provided. Such approaches are based on the notion of basis marking that prevents exhaustive enumeration of the state space. This leads to significant advantages in terms of computational complexity. In more detail, a basis reachability graph for C-detectability is defined. For Petri nets whose unobservable subnet is acyclic, the C-detectability properties can be decided by looking at the observer or detector of the basis reachability graph, which is usually much smaller than the reachability graph. The effectiveness of the presented approaches is demonstrated via two parametric examples.

Chapter 5: Analysis of C-detectability of the Radio Block Center Handover

The radio block center (RBC) is one of the most essential ground systems in a high-speed train control system both in Europe and in China. The RBC handover procedure is an important function of RBC, which affects the transport efficiency, reliability and safety of railways. Analysis of crucial states in the RBC handover procedure is helpful to determine whether there are potential risks in the procedure, and to locate the fault in time when a fault occurs. In this chapter, we study the C-detectability of the RBC handover. This property has been defined in discrete event systems and requires that the crucial states can be determined uniquely by observing the system output. Taking the RBC handover procedure in the Chinese train control system level 3 (CTCS-3) as an example, we first model the RBC handover procedure using labeled Petri nets (LPNs). Then, the approach proposed in Chapter 4 is used to check C-detectability of the LPN modeling the handover procedure.

5.1 Introduction

In the last decades, there has been a rapid improvement in railway systems in China. Chinese train control system level 3 (CTCS-3) is a typical safety-critical system that has bidirectional wireless information transmission between on-board subsystems and ground subsystems to monitor the movement of trains [92].

In CTCS-3, a radio block center (RBC) is one of the most essential ground systems, which elaborates messages to be sent to the train based on the information received from external ground subsystems and the information exchanged with the on-board systems. RBCs provide trains movement authority (MA) that allows them to move forward. An RBC area is a trackside area that is supervised by one RBC. At any time when a train runs in CTCS-3, it must be supervised by an RBC. However, due to the limitation of the control capacity of a single RBC, the railway is divided into many segments governed by different RBCs. The R-BC handover procedure enables the train to automatically pass from one RBC area to another RBC area without any action of the driver. Clearly, the RBC handover procedure affects the transport efficiency and the operation safety of CTCS-3. Thus, it is necessary to provide formal methods to analyze its properties. In fact, according to EN 50128 [93], formal methods are highly recommended to design and analyze safety-critical systems. In [94], three position computation models are proposed to improve the positioning accuracy for high-speed trains. In [95], based on a mathematical model and three mixed integer programming heuristic approaches, a planning procedure is proposed to satisfy the freight requirements in the railway network. Recently, the RBC handover procedure has been extensively invested using formal methods [53, 96–102]. In [53, 96, 103–105], the RBC handover procedure is modeled by timed tools. Using timed automata, the safety of the RBC handover procedure is validated in [53], and an integrated model-based test case generation method is proposed to guarantee the function correctness of the RBC handover procedure in [96]. In [106], the RBC handover procedure is modeled by Modeling, Simulation and Verification Language (MSVL), and the correctness of the specifications of the RBC handover procedure is verified. In [97, 107, 108], the RBC handover procedure is modeled by stochastic Petri nets, and the reliability, safety and rationality of RBC handover protocol are analyzed and verified based on the model. In [98, 109–113], colored Petri nets are used to model the RBC handover specification. The time spent and the success rate of the RBC handover are studied in [109] and the authors in [98] generate test cases and sequences based on the models, and use them to test the function of an RBC platform. These works have studied some properties of the RBC handover, however none of them is related to the state estimation problem of the RBC handover. Estimating crucial states in the RBC handover procedure is helpful to determine whether there are potential risks in the procedure. Especially, when any emergency occurs, knowing whether the system has reached a crucial state is helpful to respond to the emergency. Analysis of crucial states in the RBC handover procedure is also helpful for fault location and fault diagnosis. Thus, in this thesis, we focus our attention on C-detectability of the RBC handover procedure. C-detectability is an important property defined in state estimation problems, which requires that a given set of crucial states can be uniquely distinguished from other states, after a finite number of observations.

The reference formalism of this work is Petri nets, which are extensively used to model many classes of systems. Recently, Petri nets have been used to model and analyze railway systems [50, 51, 114, 115]. In [52] and [116], Petri nets are used to analyze and control railway networks. The intermodal freight transport terminals are modeled by timed Petri nets, and its performance is simulated and evaluated by the model in [114]. Based on LPNs, the decision-making strategies in fixed-block systems are proposed [51], and the diagnosis of the fixed-block systems [115] and the multi-track level crossing [50] are studied. However, these approaches require the construction of the reachability graph (RG) of the Petri net, and suffer the state explosion problem.

In this chapter, LPNs are used as the formal method to model the RBC handover procedure and study its C-detectability. Based on the notion of basis reachability graph (BRG) [77], the C-detectability properties of the RBC handover procedure are checked efficiently, since an exhaustive enumeration of all the markings in the RG is avoided. The contributions of the chapter can be summarized as follows.

- The RBC handover dynamics in high-speed railways are formalized in terms of LPNs.
- The C-detectability properties of the considered system are studied based on previous theoretical results by ourselves.
- Finally, MATLAB codes are developed to implement the verification approach, and to obtain the time costs for the considered application.

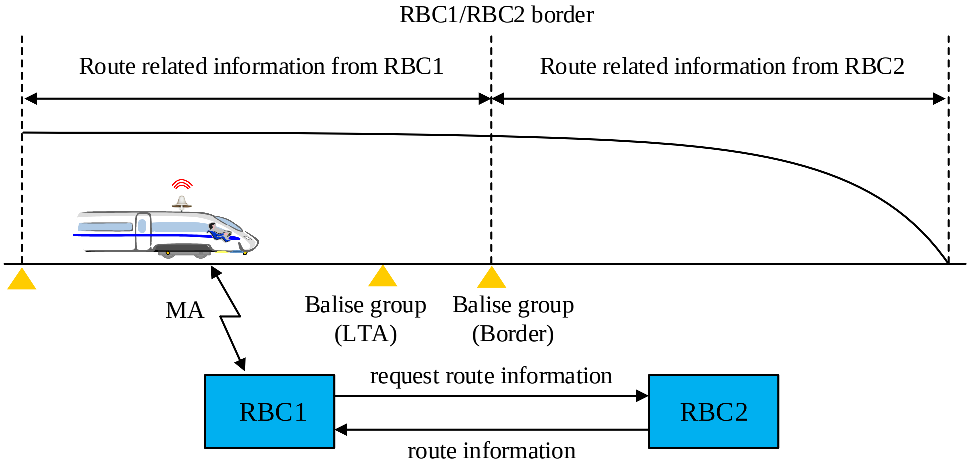
In the rest of the chapter, basics on the RBC handover procedure are provided in Section 5.2. In Section 5.3, the RBC handover procedure is modeled by LPNs. In Section 5.4, the C-detectability analysis of the RBC handover procedure is provided. Finally, conclusions are drawn in Section 5.5.

5.2 The Radio Block Center Handover

5.2.1 The Procedure of Radio Block Center Handover

In this section, we introduce the RBC handover procedure in CTCS-3 defined in [92].

As shown in Fig. 5-1, when a train passes from RBC1 area to RBC2 area, RBC2 will provide route related information to RBC1 so that trains are able to pass the border of the two RBC areas without slowing down and to obtain the MA without interruption. During the RBC handover procedure, there are two important balise groups that will send messages to the train



RBC1/RBC2 border
Route related information from RBC1
Route related information from RBC2
MA
Balise group
(LTA)
Balise group
(Border)
request route information
RBC1
RBC2
route information

Fig. 5-1 RBC handover.

when the train passes above them. One is called level transition announcement balise group (LTA), which is placed at the border of another RBC area (RBC handover pre-announcement point) to provide the position of the train. The other is placed at the handover point (the border of RBC1/RBC2) to execute the handover immediately.

There are two options in the procedure of RBC handover: 1) RBC handover with two normal mobile terminals, 2) RBC handover with one normal mobile terminal (MT). In this chapter, we focus on the second option. The operational logic of RBC handover with one normal MT is as follows:

1. When a train reaches the LTA, the train sends a position report to RBC1 via MT.

2. After RBC1 receives the position report from the train, it sends the handover command (message packet 131) to the train, meanwhile it sends handover notice and the route request information to RBC2.

3. When RBC2 receives the information from RBC1, it sends route related information to RBC1.

4. Based on the information received from RBC2, RBC1 generates MA and sends it to the train.

5. When the maximum safe front end of the train reaches the handover point and receives the massage from the border balise group, the train sends a position report to RBC1 via MT, and RBC1 forwards the position report to RBC2.

6. After receiving the position report from RBC1, RBC2 sends takeover information to RBC1.

7. When the minimum safe rear end of the train reaches the handover point, the train sends a position report to RBC1 via MT.

8. When the position report from the train is received by RBC1, RBC1 sends the disconnection command (message packet 42) to the train.

9. After receiving the disconnection order from RBC1, the train disconnects the communication with RBC1, and establishes a communication session with RBC2. After that the train only communicates with RBC2. Thus, the handover procedure is completed.

The above RBC handover procedure is summarized in the sequence diagram in Fig. 5-2. Note that in the chapter RBC1 always refers to the handing over RBC, while RBC2 always refers to the accepting RBC.

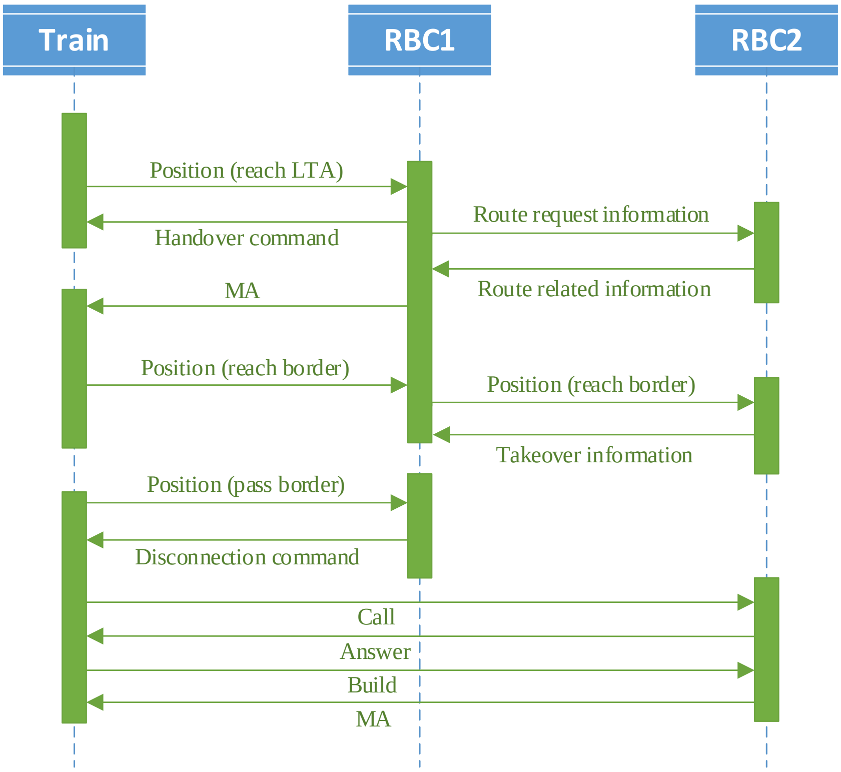


Fig. 5-2 The sequence diagram of RBC handover.

5.2.2 Modeling Mechanism

It is known that a model is a mathematical description and simplification of physical systems such that some of their behavior and properties can be analyzed via the model. In this thesis, the RBC handover procedure is modeled with a LPN, which provides not only a mathematical but also a graphical description of the system. In LPNs, states change with the occurrences of events, and the only outputs of the system are strings of signals corresponding to the events generated by the system. Note that, due to limited sensor ability or cost consideration, the occurrence of some events may not be detectable by sensors. Therefore, we observe the behavior of the system through a “mask” that projects event sequences σ to strings of signals w, called observations. This mechanism is illustrated in Fig. 5-3. Finally, the states of the system can be estimated based on the observations.

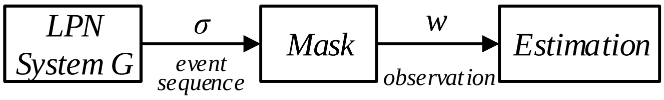


Fig. 5-3 Modeling mechanism.

5.3 Modeling RBC Handover using Labeled Petri Nets

In this section we show how to model the RBC handover procedure with a LPN. The RBC handover system is divided into three subsystems: the railway traffic, RBC1 and RBC2. The whole model is obtained through the composition of the models relative to the three subsystems.

5.3.1 Modeling the railway traffic

The railway traffic is modeled as the LPN system in Fig. 5-4. There are eleven places and seven transitions, whose physical meaning is summarised in Tables 5-1 and 5-2, respectively.

The LPN system describes the behavior of the train passing from RBC1 area to RBC2 area.

• Initially, a train approaches RBC2 area and when it reaches the LTA, the train sends its position report to RBC1, i.e., transition t_{r1} fires.

• If the train receives a handover command and an MA from RBC1, i.e., places p_{r8} and p_{r9} are marked, it will keep running and when its maximum safe front end reaches the handover point, the train will send its position to RBC1, i.e., transition t_{r2} fires.

• When the minimum safe rear end of the train reaches the handover point, the train sends its position report to RBC1, i.e., transition t_{r3} fires.

• After receiving the disconnection order from RBC1, i.e., place p_{r10} is marked, the train disconnects the communication with RBC1, i.e., transition t_{r4} fires.

• The train calls RBC2, i.e., transition t_{r5} fires.

• If the train builds a communication session with RBC2, i.e., place p_{r11} is marked, the train will operate under the supervision of RBC2, i.e., transition t_{r6} fires.

• Finally, the handover ends and the next train can approach RBC2 area from RBC1 area, i.e., transition t_{r7} fires.

Note that in the normal situation, all the above transitions are observable, since all the signals are recorded by the recorder of the train.

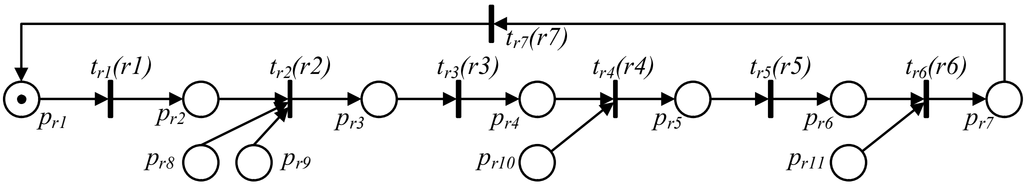


Fig. 5-4 The LPN system modeling a train passing the RBC border.

Table 5-1 Transitions in Fig. 5-4

T	$\ell(t)$	Physical meaning
t_{r1}	$r1$	a train reaches the LTA and sends its position report to RBC1
t_{r2}	$r2$	the maximum safe front of the train reaches the handover point and the train sends its position report to RBC1
t_{r3}	$r3$	the minimum safe rear end of the train reaches the handover point and the train sends its position report to RBC1
t_{r4}	$r4$	the train disconnects the communication with RBC1
t_{r5}	$r5$	the train calls RBC2
t_{r6}	$r6$	the train communicates with RBC2
t_{r7}	$r7$	the RBC handover ends

Table 5-2 Places in Fig. 5-4

P	Physical meaning
p_{r1}	a train is approaching RBC2 area
p_{r2}	the train has passed the LTA
p_{r3}	the maximum safe front end of the train has passed the handover point
p_{r4}	the minimum safe rear end of the train has passed the handover point
p_{r5}	the train has disconnected the communication with RBC1
p_{r6}	the train has called RBC2
p_{r7}	the train has established a communication session with RBC2
p_{r8}	the train has received a handover command from RBC1
p_{r9}	the train has received an MA from RBC1
p_{r10}	the train has received a disconnection command from RBC1
p_{r11}	the train has received the reply from RBC2

5.3.2 Modeling RBC1

The operation of RBC1 is modeled as the LPN system in Fig. 5-5. There are twelve places and six transitions, and their physical meaning is summarised in Tables 5-3 and 5-4.

The LPN system describes the behavior of RBC1 during the RBC handover procedure.

- Initially, RBC1 is free and when it receives the position report claiming that a train has reached the LTA, i.e., place p_{h8} is marked, RBC1 begins the handover procedure. This corresponds to the firing of transition t_{h1}.

- Then RBC1 sends the handover command to the train, i.e., transition t_{h2} fires, mean-

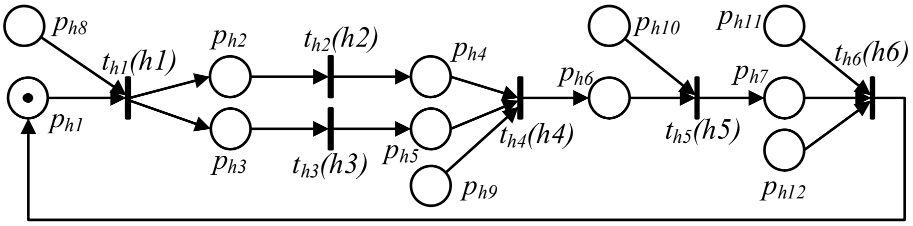


Fig. 5-5 The LPN system of RBC1.

while it sends handover notice and route request information to RBC2, i.e., transition t_{h3} fires.

- After receiving the reply from RBC2, i.e., place p_{h9} is marked, RBC1 generates an MA and sends it to the train, i.e., transition t_{h4} fires.

- If RBC1 receives the position report claiming that the maximum safe front end of the train has reached the handover point, i.e., place p_{h10} is marked, then RBC1 forwards the position report to RBC2, i.e., transition t_{h5} fires.

- If RBC1 receives the position report claiming that the minimum safe rear end of the train reaches the handover point, i.e., place p_{h11} is marked, then RBC1 sends the disconnection command to the train, i.e., transition t_{h6} fires.

5.3.3 Modeling RBC2

The operation of RBC2 is modeled as the LPN system in Fig. 5-6. There are seven places and four transitions, and their physical meaning is summarised in Tables 5-5 and 5-6.

The LPN system describes the behavior of RBC2 during the RBC handover procedure.

- Initially, RBC2 is free and when it receives the handover notice and the route request information from RBC1, i.e., place p_{a5} is marked, RBC2 begins the handover procedure, i.e., transition t_{a1} fires.

- Then, RBC2 sends route information to RBC1, i.e., transition t_{a2} fires.

- After receiving the position report claiming that the maximum safe front end of the train reaches the handover point, i.e., place p_{a6} is marked, RBC2 sends takeover information to RBC1, i.e., transition t_{a3} fires.

- Finally, when the communication session is established with the train, i.e., place p_{a7} is marked, the train operates under the supervision of RBC2, i.e., transition t_{a4} fires.

Table 5-3 Transitions in Fig. 5-5

T	$\ell(t)$	Physical meaning
t_{h1}	$h1$	RBC1 starts the handover procedure
t_{h2}	$h2$	RBC1 sends the handover command to the train
t_{h3}	$h3$	RBC1 sends the handover notice and the route request information to RBC2
t_{h4}	$h4$	RBC1 generates an MA and sends it to the train
t_{h5}	$h5$	RBC1 forwards the position report to RBC2: the maximum safe front end of the train reaches the handover point
t_{h6}	$h6$	RBC1 sends a disconnection command to the train

Table 5-4 Places in Fig. 5-5

P	Physical meaning
p_{h1}	RBC1 is free
p_{h2}	RBC1 has started the handover procedure
p_{h3}	RBC1 has started the handover procedure
p_{h4}	RBC1 has sent a handover command to the train
p_{h5}	RBC1 has sent handover notice and route request information to RBC2
p_{h6}	RBC1 has sent an MA to the train
p_{h7}	RBC1 has sent a position report to RBC2
p_{h8}	RBC1 has received the position report: the train reaches the LTA
p_{h9}	RBC1 has received route information from RBC2
p_{h10}	RBC1 has received the position report: the maximum safe front end of the train has passed the handover point
p_{h11}	RBC1 has received the position report: the minimum safe rear end of the train has passed the handover point
p_{h12}	RBC1 has received takeover information from RBC2

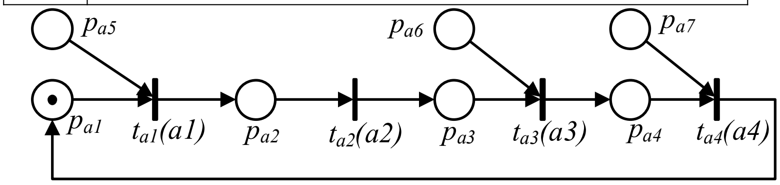


Fig. 5-6 The LPN system of RBC2.

5.3.4 Modeling the RBC handover

Given the models of the three subsystems, we may construct the global model of the RBC handover procedure with one normal mobile terminal.

According to the operational logic of the RBC handover in Section 5.2, we can obtain the mutual dependence of the transitions and the markings of the three subsystems, then the global model can be built. Let us focus on the first two sub-models. The following relationships exist between them.

- When a train reaches the LTA, it sends its position report to RBC1. Thus, transition t_{r1} fires and place p_{h8} is marked.
- When the train has received the handover command from RBC1 (transition t_{h2} fires

Table 5-5 Transitions in Fig. 5-6

T	$\ell(t)$	Physical meaning
t_{a1}	$a1$	RBC2 starts the handover procedure
t_{a2}	$a2$	RBC2 sends route information to RBC1
t_{a3}	$a3$	RBC2 sends takeover information to RBC1
t_{a4}	$a4$	RBC2 communicates with the train

Table 5-6 Places in Fig. 5-6

P	Physical meaning
p_{a1}	RBC2 is free
p_{a2}	RBC2 has started handover procedure
p_{a3}	RBC2 has sent route information to RBC1
p_{a4}	RBC2 has sent takeover information to RBC1
p_{a5}	RBC2 has received the position report: the train reaches the LTA
p_{a6}	RBC2 has received the position report: the maximum safe front end of the train has passed the handover point
p_{a7}	RBC2 has received the calling from the train

and place p_{r8} is marked), and an MA from RBC1 (transition t_{h4} fires and place p_{r9} is marked), the maximum safe front end of the train can reach the handover point, and sends a position report to RBC1 (transition t_{r2} fires and place p_{h10} is marked).

- If RBC1 receives the position report claiming that the minimum safe rear end of the train reaches the handover point (transition t_{r3} fires and place p_{h11} is marked), then RBC1 sends the disconnection command to the train (transition t_{h6} fires and place p_{r10} is marked).

Analogously, according to the communication and cooperation among the three subsystems, the whole system of the RBC handover procedure is modeled as the LPN system in Fig. 5-7.

Now we consider four events which may become unobservable in the RBC handover procedure. Note that in the normal situation, all the transitions in Fig. 5-7 are observable, since all the signals are received and recorded by the recorder. However, trains and RBCs operate outdoors, thus they are often affected by many complicated environment factors, such as thunder strikes, storms, and electromagnetic interference. Therefore, some signals may be lost or the recorder may not work well.

The four unobservable events can be divided into two types. The first type of unobservable events is caused by the two RBCs. The recorder may have failed so that it does not record two signals: one signal is that RBC1 sends the handover notice and the route request information to RBC2, modeled by transition $t_{h3}(h3)$; the other is the signal corresponding to RBC2 beginning the handover procedure, modeled by transition $t_{a1}(a1)$. In this application, we assume this failure is permanent. Thus, in the PN model with faulty events, transitions $t_{h3}(h3)$ and $t_{a1}(a1)$ are replaced by the unobservable transitions $t_{h3}(\varepsilon)$ and $t_{a1}(\varepsilon)$, respectively.

The other unobservable events in the faulty model are related to the train. In particular, there are two of such unobservable events. Indeed, affected by the environment, the train may not receive the position message from the border balise group (transition t_{r8} fires), and the disconnect command message from RBC1 (transition t_{r10} fires). In the first situation, even

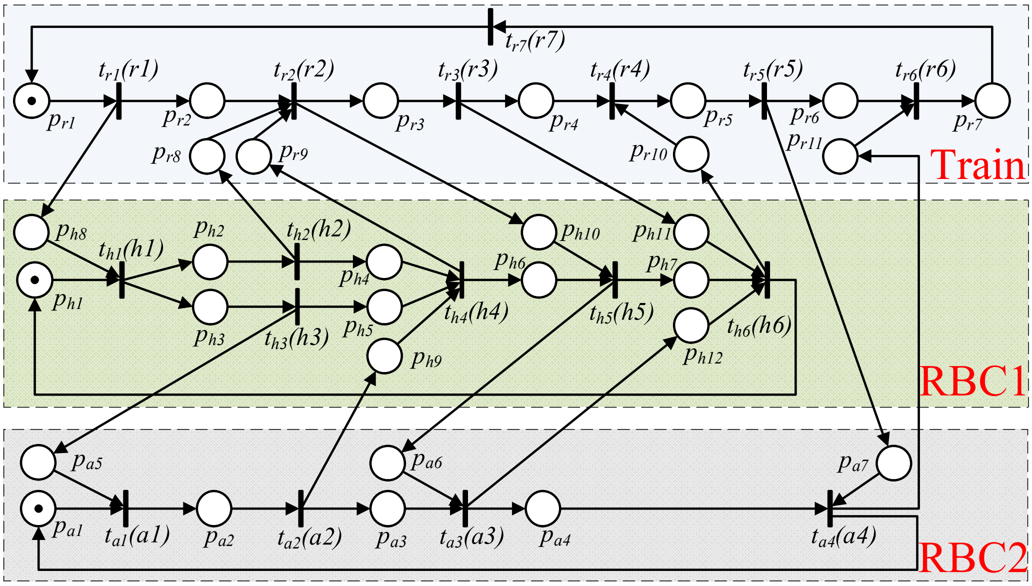


Fig. 5-7 The LPN system of RBC handover under normal behavior.

though the train loses the position message from the border balise group, according to the specification [92], the train can also calculate its position by its on-board equipment. Thus, after a while, when its calculation indicates that the maximum safe front of the train has reached the handover point, then the train will also send the position report to RBC1 (transition t_{r9} fires). In the second situation, according to the specification [92], if the train does not receive the information for a certain while, then it will disconnect with RBC1 (transition t_{r11} fires). After that, the train starts calling RBC2. The two situations occur intermittently, thus the system would follow both normal condition (transitions t_{r2} and t_{r4} fire) and the signal loss condition (transitions t_{r8} and t_{r10} fire).

In conclusion, the LPN system of RBC handover in the presence of faults is the one reported in Fig. 5-8, where the four unobservable events are denoted by blue transitions (t_{r8}, t_{r10}, t_{h3} and t_{a1}). Note that compared with the model in Fig. 5-7, there are two more arcs linked to place p_{r10} (in Fig. 5-8): the arc from transition t_{r4} to place p_{r10} ensures that p_{r10} is marked after the firing of t_{r4}; the other arc from p_{r10} to t_{r5} regards the marking of p_{r10} as one of the requirements for firing t_{r5}. The arc from p_{r10} to t_{r4} ensures that the marking of p_{r10} is necessary for the firing of t_{r4}, which depicts nominal operation. The arc from p_{r10} to t_{r5} ensures that the token in p_{r10} will be consumed at each cycle whenever an unobservable transition t_{r10} has fired. This ensures the boundedness of place p_{r10}. Thus, an arc is also added from t_{r4} to p_{r10} to ensure that the token from p_{r10} consumed during the firing of t_{r4} is got back into p_{r10} to make the firing of t_{r5} possible.

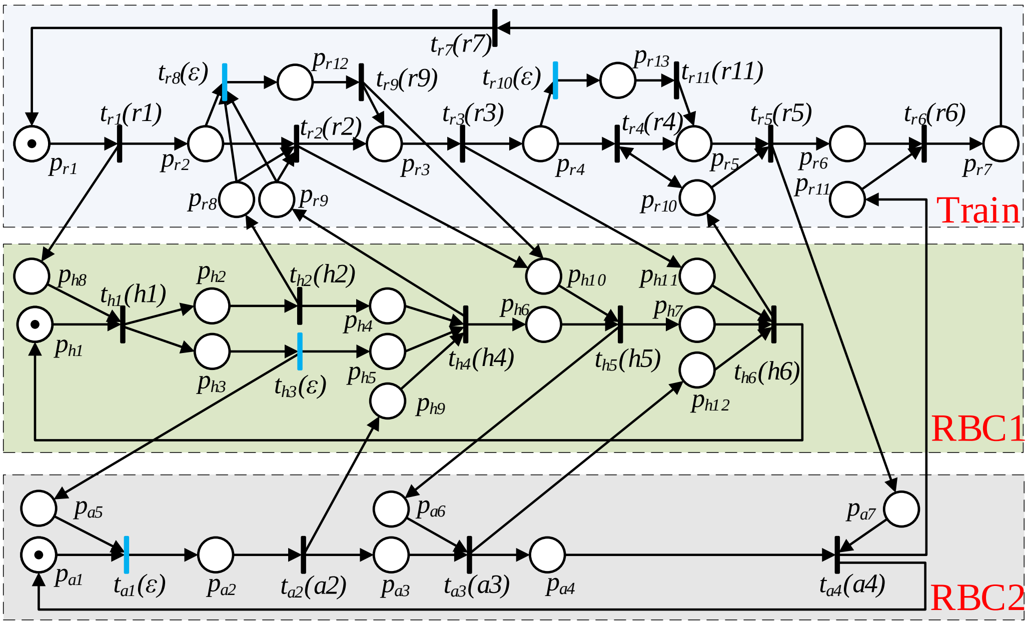


Fig. 5-8 The LPN system of RBC handover with faulty events.

5.4 Analysis of C-detectability of RBC Handover

In this section, we investigate the C-detectability properties of the RBC handover procedure modeled with the LPN system in Fig. 5-8, where $T_u = \{t_{r8}, t_{r10}, t_{h3}, t_{a1}\}$. Clearly, the LPN system is bounded and the T_u-induced subnet is acyclic. There are 30 reachable markings in the LPN system, and only 21 of them are basis markings. The set of basis markings of the LPN system in Fig. 5-8 is reported in Table 5-7.

In the RBC handover procedure, there are three crucial states that must be determined by the operator. The three crucial states represent the following three crucial times: the beginning of the RBC handover, the train reaching the two RBC borders, and the end of the RBC handover. The beginning of the RBC handover occurs when a train reaches the LTA and sends a position report to RBC1, which corresponds to marking M_1 in Table 5-7. The train reaches the two RBC borders when the maximum safe front end of the train passes the handover point, which corresponds to marking M_7 in Table 5-7. The RBC handover is completed when the train establishes a communication session with RBC2, which corresponds to marking M_{20} in Table 5-7. In other words, the set of the crucial markings is $\mathcal{M}_c = \{M_1, M_7, M_{20}\}$. As shown in Chapter 4, the set of the crucial markings can be also described by generalized mutual exclusion constraints (GMECs). Thus, the set of the crucial markings can be rewritten as $\mathcal{M}_c = \{M \in \mathbb{N}^{32} | 2M(p_{h8}) + M(p_{r3}) + M(p_{h6}) + 2M(p_{r7}) \geq 2\}$. Note that as shown in Table 5-7, $M_1(p_{h8}) = 1$, $M_{20}(p_{r7}) = 1$, and $M_7(p_{r3}) + M_7(p_{h6}) = 2$. Thus, $\mathcal{M}_c = \{M_1, M_7, M_{20}\}$.

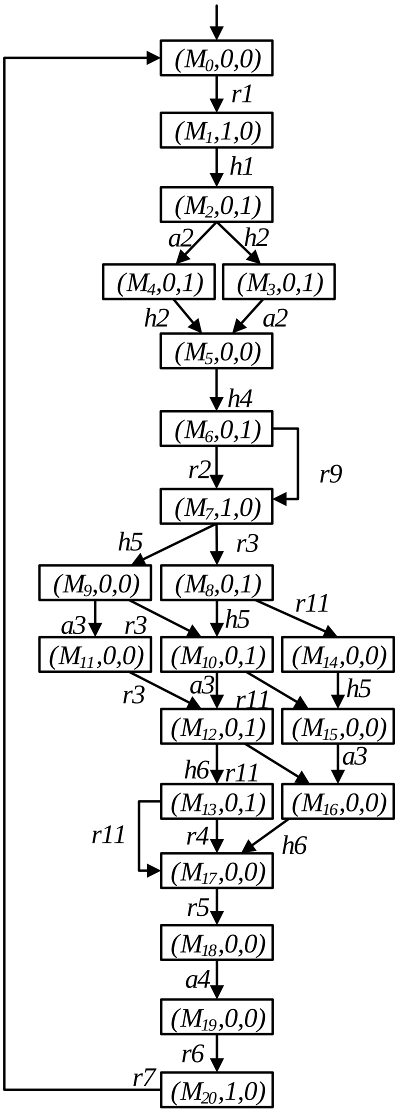


Fig. 5-9 The BRG of the LPN system in Fig. 5-8.

According to the Section 4.2.2, we may construct the BRG of the LPN system in Fig. 5-8 for C-detectability, which is reported in Fig. 5-9. Again we refer to Table 5-7 for the marking definition. Since none of the labels of the transitions in the LPN system is identical, all the transitions in BRG are distinguishable. Thus, each state in the observer contains only one state of the BRG. Thus, the observer of the BRG is omitted.

All the states of the observer are marked states, namely they belong to set $\mathcal{X}_m$. Therefore, by Theorems 4.1, 4.2, 4.3 and 4.4 in Section 4.3, the RBC handover system is strongly C-detectable, and consequently also periodically strongly C-detectable, weakly C-detectable and periodically weakly C-detectable. Namely, each crucial state of the RBC handover procedure can be uniquely determined after a finite number of observations for all possible evolutions of the system. Let us consider two event sequences: $r1h1a2h2h4r2$ and $r1h1h2a2h4r9r3$.

Table 5-7 Markings in Fig. 5-9

$Marking$	$Places$
M_0	$p_{r1} + p_{h1} + p_{a1}$
M_1	$p_{r2} + p_{h1} + p_{h8} + p_{a1}$
M_2	$p_{r2} + p_{h2} + p_{h3} + p_{a1}$
M_3	$p_{r2} + p_{r8} + p_{h4} + p_{h3} + p_{a1}$
M_4	$p_{r2} + p_{h2} + p_{h5} + p_{h9} + p_{a3}$
M_5	$p_{r2} + p_{r8} + p_{h4} + p_{h5} + p_{h9} + p_{a3}$
M_6	$p_{r2} + p_{r8} + p_{r9} + p_{h6} + p_{a3}$
M_7	$p_{r3} + p_{h6} + p_{h10} + p_{a3}$
M_8	$p_{r4} + p_{h6} + p_{h10} + p_{h11} + p_{a3}$
M_9	$p_{r3} + p_{h7} + p_{a3} + p_{a6}$
M_{10}	$p_{r4} + p_{h7} + p_{h11} + p_{a3} + p_{a6}$
M_{11}	$p_{r3} + p_{h7} + p_{h12} + p_{a4}$
M_{12}	$p_{r4} + p_{h7} + p_{h11} + p_{h12} + p_{a4}$
M_{13}	$p_{r4} + p_{r10} + p_{h1} + p_{a4}$
M_{14}	$p_{r5} + p_{h6} + p_{h10} + p_{h11} + p_{a3}$
M_{15}	$p_{r5} + p_{h7} + p_{h11} + p_{a3} + p_{a6}$
M_{16}	$p_{r5} + p_{h7} + p_{h11} + p_{h12} + p_{a4}$
M_{17}	$p_{r5} + p_{r10} + p_{h1} + p_{a4}$
M_{18}	$p_{r6} + p_{h1} + p_{a4} + p_{a7}$
M_{19}	$p_{r6} + p_{r11} + p_{h1} + p_{a1}$
M_{20}	$p_{r7} + p_{h1} + p_{a1}$

When $r1h1a2h2h4r2$ is observed, the maximum safe front end of the train reaches the handover point, the train will send its position to RBC1. By Fig. 5-9, the current state contains only one marking M_7 which is a crucial marking, i.e., the crucial marking M_7 can be uniquely determined. When $r1h1h2a2h4r9r3$ is observed, the minimum safe rear end of the train reaches the handover point, the train sends its position report to RBC1. By Fig. 5-9, the state of the BRG is $(M_8, 0, 1)$. Thus the current state can not be uniquely determined. However, the current state does not contain any crucial state, namely, this event sequence does not influence the determination of the crucial states. On the contrary, no matter what event sequence is observed, when the current state contains a crucial marking, the current state contains only one marking, therefore the RBC handover system is strongly C-detectable. Since all the states of the observer are marked states, according to Section 4.3.4, smallest value of K that satisfies Definition 4.2 is $K = 0$. Namely, from the very beginning of the system evolution, whenever the state of the system is crucial, it can be unambiguously determined.

Finally, based on Theorem 4.1 in this work, we developed MATLAB codes [91] to compute the BRG and the observer of the RBC handover LPN model, to analyze the C-detectability properties of the model, and to record the time costs of the procedures. The computations are performed using MATLAB on a laptop with Intel i7-7700 CPU 3.6GHz processor and 8G DDR3 RAM. Finally, we obtain the result that the RBC handover model is strongly C-detectable. It only takes 1.90s to build the BRG, and only 2.20s to complete the whole verification approach. Therefore, the proposed results are definitely applicable to the considered physical problem.

5.5 Conclusions

RBC handover is one of the most essential functions in CTCS-3. In this chapter, labeled Petri nets are used to model the RBC handover procedure based on only one normal mobile termination. The RBC handover procedure is split into three main subsystems modeled by labeled Petri nets, then the whole system model is built by the composition of the basic subsystem models. In this way, the RBC handover procedure is expressed in a more concise and understandable manner. Moreover, considering the crucial states, we construct the basis reachability graph and its observer to show that the RBC handover procedure satisfies strong C-detectability.

Chapter 6: Conclusions and Future Work

In this chapter, conclusions are drawn and the directions on future research in this topic are also discussed.

6.1 Conclusions

In the thesis, we investigated detectability problems in discrete event systems modeled with bounded labeled Petri net systems. The operator knows the structure of the system but partially observes the behavior of the system. Based on the knowledge of the system and its observation, the operator wants to know whether the states (or crucial states) of the system can be uniquely determined.

(1) Detectability:

The system is said to be detectable if the current and the subsequent states of the system can be uniquely determined after the observation of a finite number of events. We formalized the notion of strong detectability, weak detectability, strong periodic detectability and weak periodic detectability in labeled Petri nets. Four new approaches to verify the detectability properties of the system are developed. We show that based on the basis marking these four detectability properties can be efficiently verified in bounded LPNs. Through solving an integer linear equation, the proposed approaches avoid exhaustively enumerating the reachability space. The first approach is based on a structure called observer. We only need to construct one structure: the observer of the basis reachability graph for detectability, the four detectability properties can be verified at a time. The second approach is based on a structure called detector. This approach can be used for the verification of strong detectability and strong periodic detectability. The last two approaches are based on verifier and verifier net, respectively. Strong detectability can be checked by the two approaches. All the four approaches use basis reachability graph technique that prevents exhaustive enumeration of the state space. This leads to significant advantages in terms of computational complexity compared with previous approaches. Moreover, the last three structures are constructed in polynomial time. Finally, the effectiveness of the presented approaches is demonstrated via a parametric example.

(2) C-detectability:

The goal of detectability properies may be too strong in some applications. In this thesis, we relax such a definition and introduce the property of C-detectability, where “C” stands for "crucial". In particular, we only care about a given set of states, called crucial states, and want to be sure that when the system reaches such states, they are uniquely identified. The notion of strong C-detectability, weak C-detectability, periodically strong C-detectability and periodically weak C-detectability is defined in labeled Petri nets. We have clarified the relation among the four C-detectability properties. The approaches to verify the four different C-detectability properties are provided. Such approaches are based on the notion of basis marking that prevents exhaustive enumeration of the state space. This leads to significant advantages in terms of computational complexity. In more detail, the basis reachability graph for C-detectability is defined. For Petri nets whose unobservable subnet is acyclic, the C-detectability properties can be decided by looking at the observer or detector of the basis reachability graph, which is usually much smaller than the reachability graph. If the crucial states are described by a set of generalized mutual exclusion constraints (GMECs), then C-detectability properties can be verified by solving a set of integer linear programming problems (ILPPs). Finally, the effectiveness of the presented approaches is demonstrated via two parametric examples.

(3) C-detectability of RBC handover:

The RBC handover procedure enables trains to automatically pass from one RBC area to another RBC area without any action of the driver. It is one of the most essential functions in CTCS-3. In this thesis, labeled Petri nets are used to model the RBC handover procedure based on only one normal mobile termination. The RBC handover procedure is split into three main subsystems modeled by labeled Petri nets, then the whole system model is built by the composition of the basic subsystem models. In this way, the RBC handover procedure is expressed more concise and understandable. Moreover, considering the crucial states, we construct the basis reachability graph and its observer to show that the RBC handover procedure satisfies strongly C-detectability.

6.2 Future work

The work in the thesis points out several potential research directions.

For the detectability verification problem, we only considered the problem in logical Petri net models, i.e., labeled Petri nets, and there is no time factor or probability. Clearly, this is not the case in practice. Therefore, extending the notion of detectability timed/stochastic Petri nets and Petri nets with probability would be one direction of our future research. The problem would be how to extend the notion of detectability in the new Petri net models and how to efficiently verify the new detectability properties. For timed Petri nets, the operator may refine its estimation taking the time factor into account. Therefore, the problem would be more complicated. In Petri nets with probability, the firing of a transition has its probability. If we assume the operator also knows the firing probability of all transitions, then its estimation would be with confidence.

In this thesis, we do not tackle the enforcement problem of the detectability of labeled Petri net systems. Given a system that is not detectable, the detectability enforcement problem consists in turning the system into a detectable one. Approaches to detectability enforcement may rely on supervisory control, dynamically restraining the observability of events.

In this thesis, we do not consider the characteristics of the railway signal system model, that is, their network structure presents the characteristics of a specific workflow. Considering the characteristics, there may exist more efficient methods for the verification of the C-detectability properties in railway signal system. Moreover, we can also consider analyzing the various subsystems of the railway signal system first, and then carry out the formal methods on the entire system to realize state estimation and early fault diagnosis for the railway signal system.

Acknowledgements

First and foremost, my deepest and sincere gratitude goes to my supervisors Prof. Jin Guo and Prof. Carla Seatzu, for considering and accepting me as their student. In particular, Prof. Jin Guo gave me continuous support in my research, and provided a conducive and friendly research environment throughout my PhD. study. His critical comments, encouragement, advice, guidance and extensive research experience have much enabled me to grow and learn how to conduct research. Prof. Carla Seatzu dedicated a lot of time to guide me. I learned a lot from her kindness, patience, rigorous academic attitude and insights research style. Her guidance helped me in all the time of my research, writing papers, discussing research problems and writing this thesis.

I would like to greatly thank my assistant supervisor Dr. Yin Tong, for her continuous guidance, support, and encouragement throughout my PhD. study. Without her guidance, advice, and valuable inputs on my research ideas and writings, this work would not have been possible. Special thanks to Prof. Alessandro Giua, who put forward many constructive suggestions on my academic research, and broadened my academic horizons with his profound knowledge.

Thankfulness to the School of Information Science and Technology in Southwest Jiaotong University (SWJTU) for giving me financial support to study in both SWJTU and University of Cagliari (UniCa).

I want to thank the teachers in my lab consisting of Prof. Xiaomin Wang, Dr. Yadong Zhang, Dr. Liang Ma, Mr. Wudong Yang, Mr. Gang Xie and Dr. Xiao Han for their guidance and help in academic and research projects. Thanks to Ms. Ziyi Yang, who has given me meticulous care and help in my study and life since I entered the University. I would like to thank my lab mates, Dr. Yao Li, Dr. Kehong Li, Dr. Zicheng Wang, Dr. Hao Gao, Dr. Chang Rao, Ms. Shan Yan, Mr. Zhi Zha, Mr. Jian Wang, Mr. Shuo Wang, Ms. Qian Yu, Mr. Wengang Ma, Mr. Jingteng Fan and others for their friendship and insightful discussions.

I am very grateful to my parents, Yuangao Lan and Jiping Tan, for their unlimited support and love. I would also like to express my heartfelt gratitude to my lovely wife Yan Mao for her understanding, support, patience, and encouragement.

Last but not least, I want to thank whoever helped me in tackling the problems encountered at any stage of this dissertation.

References

[1] A. Giua, C. Seatzu, F. Basile. Observer-based State-feedback Control of Timed Petri Nets with Deadlock Recovery. IEEE Transactions on Automatic Control. 2004, 49(1):17–29

[2] W. Wang, S. Lafortune, F. Lin. An Algorithm for Calculating Indistinguishable States and Clusters in Finite-state Automata with Partially Observable Transitions. Systems & Control Letters. 2007, 56(9-10):656–661

[3] N. Ran, H. Su, A. Giua, et al. Codiagnosability Analysis of Bounded Petri Nets. IEEE Transactions on Automatic Control. 2017, 63(4):1192–1199

[4] J. Zaytoon, S. Lafortune. Overview of Fault Diagnosis Methods for Discrete Event Systems. Annual Reviews in Control. 2013, 37(2):308–320

[5] R. Jacob, J.-J. Lesage, J.-M. Faure. Overview of Discrete Event Systems Opacity: Models, Validation, and Quantification. Annual reviews in control. 2016, 41:135–146

[6] Y. Tong, Z. Li, C. Seatzu, et al. Verification of State-based Opacity Using Petri Nets. IEEE Transactions on Automatic Control. 2017, 62(6):2823–2837

[7] S. Shu, F. Lin, H. Ying. Detectability of Discrete Event Systems. IEEE Transactions on Automatic Control. 2007, 52(12):2356–2359

[8] A. Giua, C. Seatzu. Observability of Place/Transition Nets. IEEE Transactions on Automatic Control. 2002, 47(9):1424–1437

[9] R. Jacob, J.-J. Lesage, J.-M. Faure. Opacity of Discrete Event Systems: Models, Validation and Quantification. IFAC-PapersOnLine. 2015, 48(7):174–181

[10] F. Lin. Opacity of Discrete Event Systems and its Applications. Automatica. 2011, 47(3):496–503

[11] S. H. Zad, R. H. Kwong, W. M. Wonham. Fault Diagnosis in Discrete-event Systems: Framework and Model Reduction. IEEE Transactions on Automatic Control. 2003, 48(7):1199–1212

[12] F. Lin. Diagnosability of Discrete Event Systems and its Applications. Discrete Event Dynamic Systems. 1994, 4(2):197–212

[13] S. Shu, F. Lin. Delayed Detectability of Discrete Event Systems. IEEE Transactions on Automatic Control. 2013, 58(4):862–875

[14] A. Saboori, C. N. Hadjicostis. Verification of Initial-state Opacity in Security Applications of Discrete Event Systems. Information Sciences. 2013, 246:115–132

[15] L. K. Carvalho, Y.-C. Wu, R. Kwong, et al. Detection and Mitigation of Classes of Attacks in Supervisory Control Systems. Automatica. 2018, 97:121–133

[16] F. Pasqualetti, F. Dörfler, F. Bullo. Attack Detection and Identification in Cyber-physical Systems. IEEE transactions on automatic control. 2013, 58(11):2715–2729

[17] R. Ammour, E. Leclercq, E. Sanlaville, et al. Fault Prognosis of Timed Stochastic Discrete Event Systems with Bounded Estimation Error. Automatica. 2017, 82:35–41

[18] S. Takai. Robust Prognosability for a Set of Partially Observed Discrete Event Systems. Automatica. 2015, 51:123–130

[19] S. Genc, S. Lafortune. Predictability of Event Occurrences in Partially-observed Discrete-event Systems. Automatica. 2009, 45(2):301–311

[20] X. Yin, S. Lafortune. Verification Complexity of a Class of Observational Properties for Modular Discrete Events Systems. Automatica. 2017, 83:199–205

[21] C. Keroglou, C. N. Hadjicostis. Detectability in Stochastic Discrete Event Systems. Systems & Control Letters. 2015, 84:21–26

[22] T. Masopust. Complexity of Deciding Detectability in Discrete Event Systems. Automatica. 2018, 93:257–261

[23] S. Shu, F. Lin. Generalized Detectability for Discrete Event Systems. Systems & Control Letters. 2011, 60(5):310–317

[24] K. Zhang. The Problem of Determining the Weak (periodic) Detectability of Discrete Event Systems Is Pspace-complete. Automatica. 2017, 81:217–220

[25] C. G. Cassandras, S. Lafortune. Introduction to Discrete Event Systems. Springer Science & Business Media, 2009

[26] A. Chiappini, A. Cimatti, C. Porzia, et al. Formal Specification and Development of a Safety-critical Train Management System. Springer Berlin Heidelberg, 1999

[27] A. Zimmermann, G. Hommel. A Train Control System Case Study in Model-based Real Time System Design. Proceedings International Parallel and Distributed Processing Symposium. IEEE, 2003:1–8

[28] Y. Xie, T. Tang, T. Xu, et al. Research on Method of Modeling and Formal Verification of the CTCS-3 Train Control System Specification. Journal of the China Railway Society. 2011, 33(7):67–72

[29] T. Xu, H. Wang, T. Yuan, et al. Bdd-based Synthesis of Fail-safe Supervisory Controllers for Safety-critical Discrete Event Systems. IEEE Transactions on Intelligent Transportation Systems. 2016, 17(9):2385–2394

[30] Y. Cao, B. Cai, T. Tang, et al. Reliability Analysis of CTCS Based on Two GSM-R Double Layers Networks Structures. 2009 WRI International Conference on Communications and Mobile Computing. IEEE, 2009, 3:242–246

[31] L. Chen, T. Tang. Modeling of GSM-R Double-level Network and its Reliability Analysis Based on Stochastic Petri Net. Journal of the China Railway Society. 2012, 34(3):75–82

[32] R. Liang, F. Liu, L. Han, et al. Application with Petri Network in Fault Diagnosis of Railway Communication. Journal of Beijing University of Posts and Telecommunications. 2017, 40(S1):126–129

[33] Z. Li, M. Zhou. Elementary Siphons of Petri Nets and Their Application to Deadlock Prevention in Flexible Manufacturing Systems. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. 2004, 34(1):38–51

[34] M. P. Cabasino, M. Dotoli, C. Seatzu. Modelling Manufacturing Systems with Place/transition Nets and Timed Petri Nets. Formal Methods in Manufacturing, CR-C Press, 2018. 3–28

[35] N. Du, H. Hu. Review of Robust Control Policies for Automated Manufacturing Systems. Control Theory & Applications. 2018, 35(1):79–85

[36] L. V. Alves, P. N. Pena. Secure Recovery Procedure for Manufacturing Systems Using Synchronizing Automata and Supervisory Control Theory. IEEE Transactions on Automation Science and Engineering. 2020

[37] F. Lin, W. M. Wonham. On Observability of Discrete-event Systems. Information sciences. 1988, 44(3):173–198

[38] P. J. Ramadge, W. M. Wonham. The Control of Discrete Event Systems. Proceedings of the IEEE. 1989, 77(1):81–98

[39] Y. Wu, S. Lafortune. Comparative Analysis of Related Notions of Opacity in Centralized and Coordinated Architectures. Discrete Event Dynamic Systems. 2013, 23(3):307–339

[40] M. P. Cabasino, A. Giua, C. Seatzu. Fault Detection for Discrete Event Systems Using Petri Nets with Unobservable Transitions. Automatica. 2010, 46(9):1531–1539

[41] A. Giua, C. Seatzu, D. Corona. Marking Estimation of Petri Nets with Silent Transitions. IEEE Transactions on Automatic Control. 2007, 52(9):1695–1699

[42] X. Yin. Initial-state Detectability of Stochastic Discrete-event Systems with Probabilistic Sensor Failures. Automatica. 2017, 80:127–134

[43] Z. Ma, Z. Li, A. Giua. Marking Estimation in a Class of Time Labeled Petri Nets. IEEE Transactions on Automatic Control. 2019, 65(2):493–506

[44] C. M. Ozveren, A. S. Willsky. Observability of Discrete Event Dynamic Systems. IEEE Transactions on Automatic Control. 1990, 35(7):797–806

[45] P. J. Ramadge. Observability of Discrete Event Systems. 25th IEEE Conference on Decision and Control. 1986:1108–1112

[46] A. Lai, S. Lahaye, A. Giua. State Estimation of Max-plus Automata with Unobservable Events. Automatica. 2019, 105:36–42

[47] R. Ammour, E. Leclercq, E. Sanlaville, et al. State Estimation of Discrete Event Systems for Rul Prediction Issue. International Journal of Production Research. 2017, 55(23):7040–7057

[48] D. Sears, K. Rudie. On Computing Indistinguishable States of Nondeterministic Finite Automata with Partially Observable Transitions. 53rd IEEE Conference on Decision and Control. IEEE, 2014:6731–6736

[49] M. S. Durmus, S. Takai, M. T. Soylemez. Fault Diagnosis in Fixed-block Railway Signaling Systems: A Discrete Event Systems Approach. IEEJ Transactions on Electrical and Electronic Engineering. 2014, 9(5):523–531

[50] B. Liu, M. Ghazel, A. Toguyeni. Model-based Diagnosis of Multi-track Level Crossing Plants. IEEE Transactions on Intelligent Transportation Systems. 2016, 17(2):546–556

[51] M. S. Durmus, S. Takai, M. T. Soylemez. Decision-making Strategies in Fixed Block Railway Signaling Systems: A Discrete Event Systems Approach. IEEJ Transactions on Electrical and Electronic Engineering. 2015, 10(2):186–194

[52] A. Giua, C. Seatzu. Modeling and Supervisory Control of Railway Networks Using Petri Nets. IEEE Transactions on Automation Science and Engineering. 2008, 5(3):431–445

[53] J. Lv, T. Tang. Formal Modeling and Analysis of RBC Subsystem in CTCS Level 3 Using UPPAAL. World Congress on Computer Science & Information Engineering. 2009

[54] T. Zhu, J. M. M. S. de Pedro. Railway Traffic Conflict Detection via a State Transition Prediction Approach. IEEE Transactions on Intelligent Transportation Systems. 2016, 18(5):1268–1278

[55] S. Shu, F. Lin, H. Ying, et al. State Estimation and Detectability of Probabilistic Discrete Event Systems. Automatica. 2008, 44(12):3054–3060

[56] S. Shu, F. Lin. Detectability of Discrete Event Systems with Dynamic Event Observation. Systems & control letters. 2010, 59(1):9–17

[57] K. Zhang, A. Giua. Weak (approximate) Detectability of Labeled Petri Net Systems with Inhibitor Arcs. IFAC-PapersOnLine. 2018, 51(7):167–171

[58] K. Zhang, A. Giua. K-delayed Strong Detectability of Discrete-event Systems. IEEE 58th Conference on Decision and Control. IEEE, 2019:7647–7652

[59] L. Zhou, S. Shu, F. Lin. N-(k_1, k_2)-detectability of Discrete Event Systems under Nondeterministic Observations. IEEE Annual American Control Conference. 2018:294–299

[60] J. Balun, T. Masopust. On Verification of Strong Periodic D-detectability for Discrete Event Systems. IFAC-PapersOnLine. 2020, 53(4):263–268

[61] Z. Liu, X. Yin, S. Li. Improved Approaches for Verifying I-detectability of Discrete-event Systems. 12th IEEE Asian Control Conference. 2019:248–253

[62] X. Yin, Z. Li, W. Wang. Trajectory Detectability of Discrete-event Systems. Systems & Control Letters. 2018, 119:101–107

[63] C. N. Hadjicostis, C. Seatzu. K-detectability in Discrete Event Systems. 55th IEEE Conference on Decision and Control. 2016:420–425

[64] Y. Liu, Z. Liu, X. Yin, et al. An Improved Approach for Verifying Delayed Detectability of Discrete-event Systems. Automatica. 2020

[65] T. Masopust, X. Yin. Deciding Detectability for Labeled Petri Nets. Automatica. 2019, 104:238–241

[66] S. Shu, F. Lin. I-detectability of Discrete-event Systems. IEEE Transactions on Automation Science and Engineering. 2012, 10(1):187–196

[67] C. Keroglou, C. N. Hadjicostis. Verification of Detectability in Probabilistic Finite Automata. Automatica. 2017, 86:192–198

[68] P. Zhao, S. Shu, F. Lin, et al. Detectability Measure for State Estimation of Discrete Event Systems. IEEE Transactions on Automatic Control. 2018, 64(1):433–439

[69] T. Masopust, X. Yin. Complexity of Detectability, Opacity and A-diagnosability for Modular Discrete Event Systems. Automatica. 2019, 101:290–295

[70] Y. Sasi, F. Lin. Detectability of Networked Discrete Event Systems. Discrete Event Dynamic Systems. 2018, 28(3):449–470

[71] A. O. Mekki, F. Lin, H. Ying, et al. Fuzzy Detectabilities for Fuzzy Discrete Event Systems. IEEE International Conference on Fuzzy Systems. 2017:1–6

[72] S. Shu, Z. Huang, F. Lin. Online Sensor Activation for Detectability of Discrete Event Systems. IEEE Transactions on Automation Science and Engineering. 2013, 10(2):457–461

[73] S. Shu, F. Lin. Enforcing Detectability in Controlled Discrete Event Systems. IEEE Transactions on Automatic Control. 2013, 58(8):2125–2130

[74] X. Yin, S. Lafortune. A Uniform Approach for Synthesizing Property-enforcing Supervisors for Partially-observed Discrete-event Systems. IEEE Transactions on Automatic Control. 2016, 61(8):2140–2154

[75] X. Yin, S. Li. Supervisory Control for Delayed Detectability of Discrete Event Systems. IEEE 15th International Conference on Automation Science and Engineering (CASE). IEEE, 2019:480–485

[76] Z. Ma, Z. Li, A. Giua. Design of Optimal Petri Net Controllers for Disjunctive Generalized Mutual Exclusion Constraints. IEEE Transactions on Automatic Control. 2015, 60(7):1774–1785

[77] M. P. Cabasino, A. Giua, M. Pocci, et al. Discrete Event Diagnosis Using Labeled Petri Nets. An Application to Manufacturing Systems. Control Engineering Practice. 2011, 19(9):989–1001

[78] K. Zhang, A. Giua. On Detectability of Labeled Petri Nets and Finite Automata. Discrete Event Dynamic Systems. 2020:1–33

[79] R. Tarjan. Depth-first Search and Linear Graph Algorithms. SIAM Journal on Computing. 1972, 1(2):146–160

[80] T. Murata. Petri Nets: Properties, Analysis and Applications. Procedings of the IEEE. 1989, 77(4):541–580

[81] K. R. Boel, G. Jiroveanu. Distributed Contextual Diagnosis for Very Large Systems. IFAC Proceedings Volumes. 2004, 37(18):333–338

[82] G. Jiroveanu, R. K. Boel. Contextual Analysis of Petri Nets for Distributed Application-s. 16th International Symposium on Mathematical Theory of Networks and Systems. 2004, 135:136

[83] Z. Ma, Y. Tong, Z. Li, et al. Basis Marking Representation of Petri Net Reachability Spaces and its Application to the Reachability Problem. IEEE Transactions on Automatic Control. 2017, 62(3):1078–1093

[84] D. B. Johnson. Finding all the Elementary Circuits of a Directed Graph. SIAM Journal on Computing. 1975, 4(1):77–84

[85] T.-S. Yoo, S. Lafortune. Polynomial-time Verification of Diagnosability of Partially Observed Discrete-event Systems. IEEE Transactions on Automatic Control. 2002, 47(9):1491–1495

[86] S. Jiang, Z. Huang, V. Chandra, et al. A Polynomial Algorithm for Testing Diagnosability of Discrete-event Systems. IEEE Transactions on Automatic Control. 2001, 46(8):1318–1321

[87] M. P. Cabasino, A. Giua, S. Lafortune, et al. A New Approach for Diagnosability Analysis of Petri Nets Using Verifier Nets. IEEE Transactions on Automatic Control. 2012, 57(12):3104–3117

[88] Y. Tong, Z. Li, C. Seatzu, et al. Verification of Current-state Opacity Using Petri Nets. IEEE American Control Conference. 2015:1935–1940

[89] H. Lan, Y. Tong. Matlab Toolbox for Detectability Verification of Bounded Petri Nets. Available: https://www.researchgate.net/publication/350878750_MATLAB_toolbox_for_detectability_verification_of_bounded_Petri_nets, 2021

[90] A. Giua, F. DiCesare, M. Silva. Generalized Mutual Exclusion Contraints on Nets with Uncontrollable Transitions. IEEE International Conference on Systems, Man and Cybernetics. 1992, 2:974–979

[91] H. Lan, Y. Tong. Matlab Toolbox for C-detectability Verification of Bounded Petri Nets. Available: https://www.researchgate.net/publication/351904344_MATLAB_toolbox_for_C-detectability_verification_of_bounded_Petri_nets, 2021

[92] T. M. of Railways of The People's Republic of China. System Requirements Specification of the CTCS-3 Train Control System. China Railway Publishing House. 2008

[93] Railway Applications-communications, Signalling and Processing Systems-software for Railway Control and Protection Systems. EN 50128, BSI Standards Publication. 2011

[94] D. Chen, L. Wang, L. Li. Position Computation Models for High-speed Train Based on Support Vector Machine Approach. Applied Soft Computing. 2015, 30:758–766

[95] D. Anghinolfi, M. Paolucci, S. Sacone, et al. Freight Transportation in Railway Networks with Automated Terminals: A Mathematical Model and MIP Heuristic Approaches. European Journal of Operational Research. 2011, 214(3):588–594

[96] J. Lv, H. Wang, H. Liu, et al. A Model-based Test Case Generation Method for Function Testing of Train Control Systems. IEEE International Conference on Intelligent Rail Transportation (ICIRT). 2016

[97] D. Pan, Y. Zheng. Formal Modeling, Analysis and Verification of RBC Handover for CTCS-3 Train Control System. Application Research of Computers. 2013, 2

[98] W. Zheng, C. Liang, R. Wang, et al. Automated Test Approach Based on all Paths Covered Optimal Algorithm and Sequence Priority Selected Algorithm. IEEE Transactions on Intelligent Transportation Systems. 2014, 15(6):2551–2560

[99] Y. Chen, C. Ding. Research on TRSL-based RBC Level Transition Scene. Railway Standard Design. 2016:08

[100] X. Han. Safety Analysis of RBC Handover Based on UML and STPA. Master's thesis, Beijing Jiaotong University. 2016

[101] Y. Xia. Research on Safety Analysis Method for RBC Handover Based on NuSMV and STPA. Master's thesis, Beijing Jiaotong University. 2018

[102] X. Liu, L. Yuan, J. Lv, et al. Mutation Model-based Generation of Test Cases for CTCS-3 Train Control System. Railway Computer Application. 2015:54–57

[103] J. LV, X. Zhu, K. Li, et al. Model-based Test Case Automatic Generation of CTCS-3 Train Control System. Journal of Southwest Jiaotong University. 2015, 50(5):917–927

[104] Y. An, G. Li. Formal Modeling and Analysis of RBC Handover Based on Timed-UML Sequence Diagram. Railway Standard Design. 2016, 60(6):132–138

[105] S. Xu, M. Xiao. The Formal Modeling and Verification of RBC Handover Protocol for High-speed Train Based on Timed Raise. Railway Standard Design. 2015, 59(6):138–143

[106] K. Yang, Z. Duan, C. Tian. Modeling and Verification of RBC Handover Protocol. Electronic Notes in Theoretical Computer Science. 2014, 309:51–62

[107] R. Niu, Y. Cao, T. Tang. Formal Modeling and Analysis of RBC Handover Protocol for ETCS-2 Using Stochastic Petri Nets. Journal of the china railway society. 2009, 31(4):52–58

[108] Y. Chen, X. Wang, J. Dang, et al. Formal Modeling and Analyzing of CTCS Radio Communication Based on Stochastic Petri Nets. Journal of the China Railway Society. 2011, 33(8):63–68

[109] Y. Zhang, T. Tang. The Modeling and Formal Analysis of RBC Handover for CTCS-3 Train Control System Based on Colored Petri Nets. Journal of the China Railway Society. 2012, 34(7):49–55

[110] Y. Wang, J. Wu. Analysis to RBC Handover Procedure of CTCS-3 Train Control System. Railway Signalling Communication. 2010, (04):12–16

[111] Y. Zhang, T. Tang, Q. Huang, et al. The Test of Train Control System Based on Colored Petri Net. 2011 9th World Congress on Intelligent Control and Automation. IEEE, 2011:315–320

[112] D. Wu. Test Case Generation Based on Colored Petri Net and its Application in Train Control System. Ph.D. thesis, Beijing Jiaotong University. 2010

[113] W. Li. The Modeling and Verification of RBC Handover Based on Colored Petri Nets. Ph.D. thesis, Beijing Jiaotong University. 2009

[114] D. Giglio, N. Sacco. A Petri Net Model for Analysis, Optimisation, and Control of Railway Networks and Train Schedules. IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016:2442–2449

[115] M. S. Durmus, I. Ustoglu, R. Y. Tsarev, et al. Modular Fault Diagnosis in Fixed-block Railway Signaling Systems. IFAC-PapersOnLine. 2016, 49(3):459–464

[116] M. Dotoli, N. Epicoco, M. Falagario, et al. A Timed Petri Nets Model for Performance Evaluation of Intermodal Freight Transport Terminals. IEEE Transactions on Automation Science and Engineering. 2015, 13(2):842–857

List of Publications

I. Academic Publications

1 **Hao Lan**, Yin Tong, Jin Guo and Carla Seatzu. Verification of C-detectability using Petri nets, Information Sciences, 2020, 528: 294-310. (SCI: 000532827200018, JCR Q1)

2 **Hao Lan**, Yin Tong, Jin Guo and Alessandro Giua. Comments on "A new approach for the verification of infinite-step and K-step opacity using two-way observers" [Automatica, 2017(80)162-171], Automatica, 2020, 122: 109290. (SCI: 000598166000009, JCR Q1)

3 **Hao Lan**, Yin Tong and Carla Seatzu. Analysis of Strong and Strong Periodic Detectability Using Bounded Labeled Petri Nets, Nonlinear Analysis: Hybrid Systems, 2021, 42: 101087. (SCI: 000701711900018, JCR Q1)

4 **Hao Lan**, Yin Tong and Carla Seatzu. Verification of Infinite-step Opacity Using Labeled Petri Nets, IFAC-PapersOnLine, 2020, 53(2): 1729-1734. (EI: 20212410505443)

5 **Hao Lan**, Yin Tong, Jin Guo and et al. A Test Path Generation Method Based on SSM Models, 2018 IEEE International Conference on Software Quality, Reliability and Security Companion. 2018. (EI: 20183605769315)

6 Yin Tong and **Hao Lan**. Current-State Opacity Verification in Modular Discrete Event Systems, IEEE 58th Conference on Decision and Control. 2019. (EI: 20201408369122)

7 Yin Tong, **Hao Lan** and Jin Guo. Verification of Detectability in Labeled Petri Nets, 2019 American Control Conference, 2019. (EI: 20193807455479)

8 Yue Yao, Yin Tong and **Hao Lan**. Initial-State Estimation of Multi-Channel Networked Discrete Event Systems, IEEE Control Systems Letters, 2020, 4(4): 1024-1029. (EI: 20202708892206)

9 **Hao Lan**, Yin Tong and Carla Seatzu. Crucial States Estimation in Radio Block Center Handover Using Labeled Petri nets, IEEE Transactions on Automation Science and Engineering. (Conditionally Accept, SCI)

10 Yin Tong, **Hao Lan** and Carla Seatzu. Verification of K-step and Infinite-step Opacity Using Labeled Petri Nets, Automatica. (Provisionally accepted, SCI)

II. Participation in Academic Programs

1 National Natural Science Foundation of China, Decentralized opacity verification and enforcement in Discrete event systems, Grant：2017X007-D, 2019.01-2021.12.

2 Key Research Projects of China Railway Corporation, Research on Safety Function Test Technology of Autonomous Train Control System, Grant：61803317, 2017.02-2018.12.

3 Project RASSR05871 MOSIMA financed by Region Sardinia, FSC 2014-2020, annuity 2017, Subject area 3, Action Line 3.1.