

Title	ペトリネットの診断可能性についての研究
Author(s)	林, 欣
Citation	
Issue Date	2001-06
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/1545
Rights	
Description	Supervisor: 平石 邦彦, 情報科学研究科, 修士



修 士 論 文

ペトリネットの診断可能性についての研究

指導教官 平石邦彦 助教授

北陸先端科学技術大学院大学
情報科学研究科情報システム専攻

林 欣

平成 13 年 6 月 27 日

目 次

1	はじめに	1
1.1	研究の背景	1
1.2	研究の概要	2
2	準備	3
2.1	離散事象システム	3
2.2	ペトリネット	4
3	離散事象システムの診断可能性	7
3.1	システムのモデル	7
3.2	表記法	8
3.3	診断可能性	8
3.3.1	定義	9
3.3.2	診断器	9
3.3.3	診断可能性の必要十分条件	11
4	ペトリネットに対する診断可能性判定問題	15
4.1	準備	15
4.2	ペトリネットの診断可能性	16
4.3	診断可能性判定問題	16
4.4	一般ラベルペトリネットの診断可能性	17
5	自由ラベルペトリネットの診断可能性	20
5.1	仮定	20

5.2	構造的診断可能性	20
5.3	初期マーキング依存診断可能性	26
6	まとめ	29
A		30
A.1	診断器構成アルゴリズム	30
A.2	遅延の求め方	31
謝辞		39

第 1 章

はじめに

1.1 研究の背景

安全性，信頼性，さらに経済性の観点から，システムの正確かつ適時な故障診断に対する要求が高まっており，それにより故障診断に関する研究が進展してきた．これらの研究の多くは自動診断システム（automated diagnostic systems）に関するものであり，理論的な枠組や設計／実装の方針の相違から，様々な方式が提案されている．Ramadge と Wonham により提案された離散事象システムの制御理論に基づく方法もその一つである [1]．この枠組では，システムはオートマトンで表現され，そのふるまいは発生する事象列の集合（すなわち，事象集合上の言語）として表現される．事象には観測可能な事象（可観測事象）とそうでない事象（非観測事象）の 2 種類がある．このとき，観測された有限の事象の履歴から，過去にどのような種類の障害が発生したかを検出できるとき，システムは診断可能であるという．

従来の研究では，有限オートマトンで記述されるような一般の離散事象について診断可能性が議論されていた．一方で，並行的，非同期的，分散的な離散事象システムに対しては，ペトリネットのほうが簡潔かつ強力であり，広く用いられている．さらに，診断可能性に対しては，ペトリネットの特徴であるグラフ構造的性質を用いることで，より詳細な議論を行うことが可能であると考えられる．

1.2 研究の概要

離散事象システム (DES: Discrete Event Systems) において, 一部の事象の発生のみが観測可能 (部分観測可能) であるとする. このとき, 診断可能性 (diagnosability) とは, 発生した有限長の事象系列の観測により, どの観測不可能な事象グループが発生したかが決定可能かどうかをいう.

ペトリネットは離散事象システムのモデルとして広く用いられている. その特徴として, 並行的な事象の発生を許すようなシステムを比較的小さいサイズのモデルで表現できることが挙げられる. 並行システムでは, モデルのサイズの指数関数オーダーの状態空間を持つ, いわゆる状態空間爆発の問題があり, システム解析の大きな障害となっている.

本研究では, 有限オートマトンで行われたものと同様な議論をペトリネットに適用し, 診断可能であるための条件, および, 診断可能性を保つような制御方式について検討する. ここで, ペトリネットではグラフ構造的性質を用いることで, より詳細な議論が可能であると考えられる.

本稿は以下の様に構成されている. 2 章では, 本稿で用いる概念および用語の解説を行う. 3 章では, 離散事象システムに対する診断可能性について述べる. 4 章では, ペトリネットの診断可能性について定義し, 解決すべき 2 つの問題, 構造的診断可能性判定問題, および, マーキング依存診断可能性判定問題, を提示する. 5 章ではそれらの問題に対し, 診断可能であるための必要十分条件を示す. 6 章では, 本研究で得られた結果をまとめ, さらに今後の課題を示す.

第 2 章

準備

2.1 離散事象システム

事象が非同期的，離散的に生起することによって状態が変化するシステムは離散事象システム (discrete event systems) と呼ばれる．コンピュータネットワーク，FMS (Flexible Manufacturing Systems)，オペレーティングシステム，通信システム，データベースシステム，シーケンス制御などがその典型的な例である．

離散事象システムに対するモデリングや解析に関しては，排他制御や並行処理制御などの個々の問題に対しては多くの手法が提案されているが，統一的な方法論は少なかった．しかしながら，コンピュータ応用技術の発達にともない，大規模な離散事象システムが現れ，またその制御問題も複雑になってきた．そのため，離散事象システムに対するシステム理論的研究が近年急速に注目されるようになってきた．

離散事象システムのモデルとしては，待ち行列ネットワーク (queuing networks) のように事象の生起時刻に関しての情報も入った評価モデル (performance models) と，形式言語，オートマトン，ペトリネット (Petri nets) のように時刻に関しては考慮せずに事象の生起順のみを考える論理がある．評価モデルはスループットや応答時間のようなシステムの性能評価には適しているが，一般に理論的解析が困難である．したがって，排他制御や並行処理制御のように生起する事象の順番が重要な制御問題の場合は，論理モデルを用いた方が，理論的解析が容易となる．

2.2 ペトリネット

離散事象システムの解析や設計に必要なモデルを考える際に重要なこととして、その表現能力と解析能力が挙げられる。離散事象システムに特徴的な非同期・並行動作、有限資源共有に起因する競合、デッドロックなどの表現能力とともに、検証・性能評価などの解析やシミュレーションを可能にする数学モデルであること、階層的な設計過程に対応して、各階層で一貫して用いることのできるモデルであることが望ましい。ペトリネットは上記の要件を満たす離散事象システムモデルの一つとして、計算機科学を含む広い分野で、その有用性が認識されている [2]。

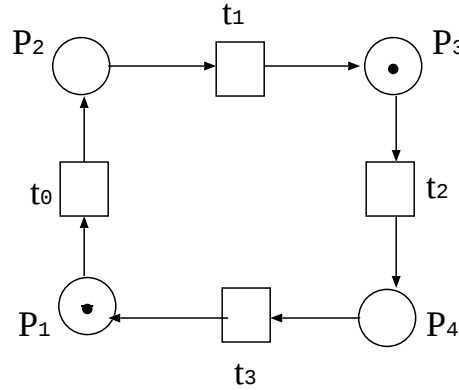


図 2.1: ペトリネット PN

ペトリネットは 4 項組 $PN = (P, T, A, M_0)$ である。ここで、 P はプレース (place) の有限集合、 T はトランジション (transition) の有限集合、 $A : (P \times T \cup T \times P) \rightarrow \mathbb{N}$ はプレースとトランジションの接続を表す写像、 $M_0 : P \rightarrow \mathbb{N}$ は初期マーキング (initial marking) である。初期マーキングを除いた $N = (P, T, A)$ をネット構造 (net structure) という。プレース / トランジションネットはプレースとトランジションという 2 種類の節点をもつ有向 2 部グラフとして見ることができ、通常、図 2.1 のように描く。

図では、プレースを丸 $\bigcirc$ 、トランジションを $\square$ または $|$ で表す。また、写像 A はアーク (arc) $\rightarrow$ により表す。 $A(x, y) = n \geq 1$ のとき n 本のアーク (または本数を枝の上にかいた一本のアーク) を節点 x から節点 y へ向けて描く。また、初期マーキングは各プレース p 内に $M_0(p)$ 個の $\bullet$ (これをトークン (token)) と呼ぶ) を描くことにより表す。トークンはシステムの状態を表す指標であり、システムの実行中に事項に示す規則に従ってネット中

を移動する．各プレースのトークン数 (local state) が変化することにより，システムの状態 (global state) が変化する．プレースにトークンが存在するとき，そのプレースはマークされている (marked) という．プレース p およびトランジション t について $A(p, t) \geq 1$ のとき， p は t の入力プレース， t は p の出力トランジションという． $A(p, t) \geq 1$ のとき， p は t の出力プレース， t は p の入力トランジションという．

各プレースに存在するトークンの個数を表す写像 $M : P \rightarrow \mathbb{N}$ をマーキング (marking) と呼ぶ．マーキングは各プレース中のトークンの分布，すなわちシステムの分散状態を表す．マーキングはオートマトンにおける状態に対応し，初期値 M_0 からトランジションの発火 (firing) により推移していく．トランジション t はマーキング M において次の条件を満たすときに発火可能 (enabled) であるという．

$$\forall p \in P : M(p) \geq A(p, t).$$

すなわち，トランジション t は各入力プレース p 上にその間のアークの重みである $A(p, t)$ 個以上のトークンが存在するとき発火可能になる．発火可能なトランジションは発火させることができる．トランジション t の発火により次のマーキング M' に変化する．

$$M'(p) = M(p) + A(t, p) - A(p, t) \quad (p \in P).$$

このトランジションの発火によるマーキングの変化を記法

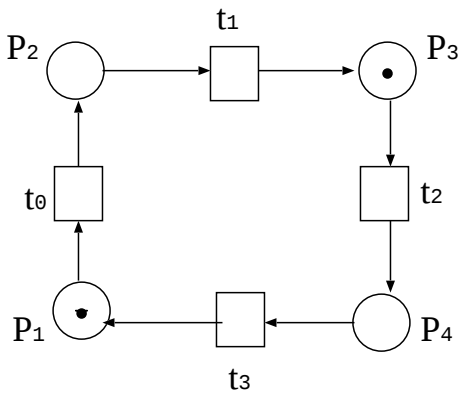
$$M \xrightarrow{t} M'$$

で表す．また，発火可能性のみを表すときは，

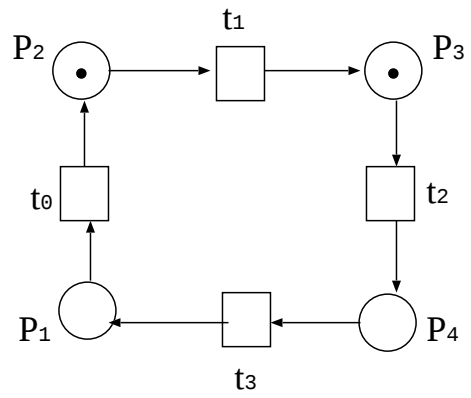
$$M \xrightarrow{t}$$

と書く．

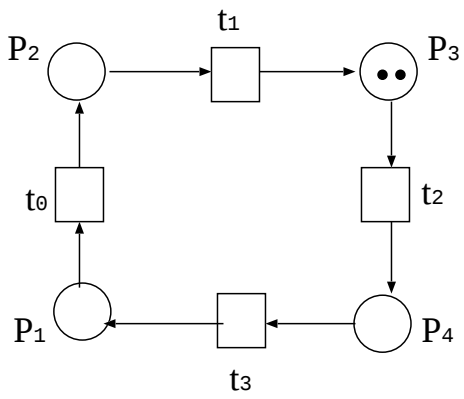
トランジションの発火の様子を図 2.2 に示す．トランジションの各入力プレースからアークの本数のトークンが失われ，出力プレースにはアークの本数のトークンが加えられる．



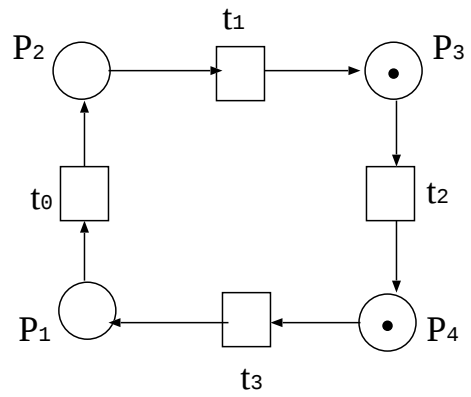
(a) 初期状態



(b) t_0 の発火



(c) t_1 の発火



(d) t_2 の発火

図 2.2: トランジションの発火

第 3 章

離散事象システムの診断可能性

3.1 システムのモデル

離散事象システムは決定性有限状態マシン (FSM: Finite State Machine)

$$G = (X, \Sigma, \delta, x_0)$$

としてモデル化される．ここで， X は状態の有限集合， Σ は事象の有限集合， δ は遷移関数， x_0 はシステムの初期状態である． δ は一般には部分関数である． G はシステムの正常および障害の両方のふるまいを表現する．システムのふるまいは G によって生成される prefix-closed 言語 $L(G)$ によって表現される．以降， G を固定して考えるので， $L(G)$ を単に L で表す．言語 L は正規である． Σ^* により，集合 Σ 上の，空文字列を含む，すべての有限長の文字列の集合を表す． $L \subseteq \Sigma^*$ である．

事象集合 Σ は $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ のように分割される．ここで， Σ_o は可観測事象の集合を， Σ_{uo} は非可観測事象集合を表す． $\Sigma_f \subseteq \Sigma$ は診断すべき障害事象の集合を表す．一般性を失わずに $\Sigma_f \subseteq \Sigma_{uo}$ を仮定する．観測可能な障害事象はその観測により診断できるからである．さらに，障害事象集合を以下のようにいくつかの集合に分割する．

$$\Sigma_f = \Sigma_{f_1} \dot{\cup} \cdots \dot{\cup} \Sigma_{f_m}.$$

Π_f でこの分割を表す．以下の議論では，同じ性質を持つ障害が発生したかどうかについてのみ注目する．言い換えると，同定するのは障害そのものではなく，障害のタイプである．今後，” 障害タイプ F_i が生起した” と書くとき，それは集合 Σ_{f_i} のある事象が生起したという意味となる．

G について以下を仮定する：

1. G によって生成される言語 L はライブである．

これは各 $x \in X$ において，少なくとも1つの事象が生起可能であることを意味する．
すなわち，システムはどの事象も生起可能ではない状態に到達することはない．

2. G には観測できない事象のサイクルが存在しない．すなわち， $\exists n_o \in N (\forall_{ust \in L}) s \in \Sigma_{uo}^* \Rightarrow \|s\| \leq n_o$ ．ここで， $\|s\|$ は文字列 s の長さを表す．

3.2 表記法

以下，論文中で使われる言語は prefix-closed であることを仮定する． $\bar{s}$ は集合 $s \subseteq \Sigma^*$ の prefix-closure を表す． $L(G, x)$ は G の状態 x から生起可能なすべての文字列の集合を表す． L/S で S の後に続く L の文字列の集合 (postlanguage) を表す．すなわち，

$$L/S = \{t \in \Sigma^* \mid st \in L\}$$

である．

$$\Psi(\Sigma_{fi}) = \{s \in L \mid s_f \in \Sigma_{fi}\}$$

を定義する．ここで， s_f は文字列 s の最後の事象である． $\Psi(\Sigma_{fi})$ は集合 Σ_{fi} に含まれる障害事象で終るような言語 L のすべての文字列の集合を表す． $\sigma \in \Sigma$ ， $s \in \Sigma^*$ に対して，表記法 $\sigma \in s$ により， σ が文字列 s 中の事象であるということを表す． $\Sigma_{fi} \in s$ により，ある $\sigma_f \in \Sigma_{fi}$ に対して $\sigma_f \in s$ であることを表す．つまり， $\bar{s} \cup \Psi(\Sigma_{fi}) \neq \emptyset$ のことである．

$P : \Sigma^* \rightarrow \Sigma_o^*$ は文字列中の非可観測事象を”消す”という通常の写像操作を表す．逆写像操作 P_L^{-1} は $P_L^{-1}(y) = \{s \in L \mid P(s) = y\}$ により定義される．

3.3 診断可能性

文献 [4, 5] に従い，離散事象システムの診断可能性について述べる．

3.3.1 定義

観測された事象の記録を用いて、有限の遅延で任意のタイプの障害の発生を検出することができるとき、言語 L は診断可能という。ここで有限の遅延とは、障害に続く有限個の事象の発生を意味する。形式的には以下のように診断可能性が定義できる。

定義 3.1 prefix-closed かつ live な言語 L は、もし以下の条件を満たすならば、写像 P および Σ_f についての分割 Π_f に関して診断可能という。

$$(\forall i \in \Pi_f)(\exists n_i \in N)(\forall s \in \Psi(\Sigma_{fi}))(\forall t \in L/s)[\|t\| \geq n_i \Rightarrow D].$$

ここで、観測可能条件 D は、つぎのように定義される。

$$\omega \in P_L^{-1}[P(st)] \Rightarrow \Sigma_{fi} \in \omega.$$

診断可能性の概念を図 3.1 を用いて説明する。 s はシステムによって生成されたタイプ F_i の障害事象で終る任意の文字列である、そして t は s の後に続く任意の十分に長い文字列である。診断可能性は文字列 st と同じ観測可能事象の系列を生成する言語 L に属するすべての文字列はタイプ F_i の障害事象を含むことを要求する。つまり、文字列 st に対して、 P 操作によって観測できる事象のみからなる文字列ができる、さらに、 P_L^{-1} の操作によって、 st と同じ観測結果をもたらす文字列（図 3.1 の中では w_1, w_2, w_3 ）ができる。このとき、文字列 w_1, w_2, w_3 すべてに F_i が含まれるならば、 F_i という障害が発生したとわかる。したがって、 s について遅延 $\|t\|$ でタイプ F_i の障害事象の検出ができる。

3.3.2 診断器

診断可能性は診断器を作ることによって判定できる。FSM G によって与えられた離散事象システムの診断器は $L(G_d) = P(L)$ を満たす決定性の FSM $G_d = (Q_d, \Sigma_o, \delta_d, q_0)$ であり、以下の性質をもつ。

1. すべての観測可能な事象の発生の後に、システムの現在の状態見積りを与える。ここで、状態見積もりとは、状態の集合である。

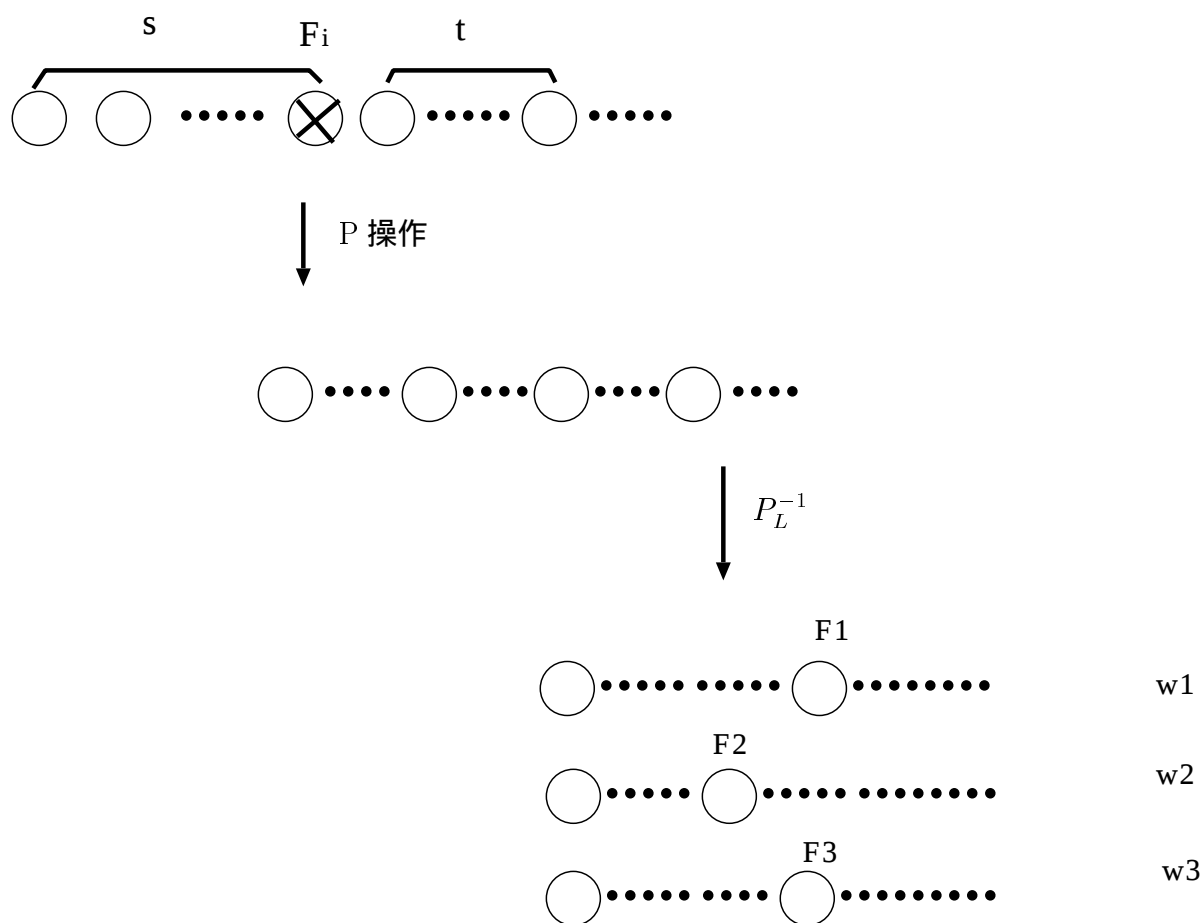


図 3.1:

2. 状態見積りに付随した障害ラベルの形で，過去に発生した障害の情報を与える．状態見積りもりの各状態に対し，障害事象が発生していなければ N を，発生していれば発生したタイプ F_i をラベルとして付ける．

診断器を用いて障害を診断するには，状態見積りに付随したラベルをチェックすればよい．診断器において，すべての状態見積りがラベル F_i を持つような状態 x に遷移すれば，タイプ F_i の障害がすでに起こったと結論できる．このような状態を F_i -certain 状態という．また，診断器の F_i -uncertain 状態とは，ラベル F_i を持つ状態見積りと，ラベル F_i を持たない状態見積りをそれぞれ少なくとも 1 つずつ含む状態である．

3.3.3 診断可能性の必要十分条件

診断可能性の必要十分条件は、診断器の条件として設定することができる。診断器中の F_i -indeterminate cycle の概念は診断可能性の必要十分条件を考える上で重要な要素である。 G_d の F_i -indeterminate cycle とは F_i -uncertain 状態のみから構成された cycle のことである。

定理 3.2 [4] 正規, prefix-closed, かつ, ライブな言語 L は以下の条件を満足するとき, かつそのときに限り, 診断可能である: すべての障害タイプ F_i に対して, F_i -indeterminate cycles が G_d に存在しない。

上の定理の条件は、任意の F_i -uncertain 状態から診断器上の有限個の状態遷移で F_i -certain 状態に到達することを意味する。さらに、つぎの結果が得られている。

系 3.3 [4] L は正規, prefix-closed, かつ, ライブな言語とする。 n_o は L に含まれる観測不可能事象からなる最も長い文字列の長さとする。 $\Sigma_{f_i} (i = 1, 2, \dots, m)$ は Σ 中の障害事象の集合を表す。もし, L は障害タイプ F_i について遅延 n_i で診断可能であれば, 診断器 G_d は, タイプ F_i の障害事象の発生が続くただか $n_i + n_o$ 個以内の事象の発生の後, タイプ F_i の障害事象の発生を検出できる。

なお, ここで述べた診断器は同じタイプの障害が複数回発生した場合に, その回数までは区別しない。しかしながら, 同様の考え方により, 回数を区別する診断器を構成することが可能である。

診断不可能な例を示す。

例 3.1 図 3.2 のシステム G に対応診断器 G_d は図 3.3 になる。 $\Sigma_f = \Sigma_{f_1} = \{\sigma_{f_1}\}$, そして, $\Sigma_{uo} = \Sigma_f \cup \{\sigma_{uo}\}$ とする。診断器は事象系列 $\beta\gamma\delta$ に対応する F_i -uncertain 状態の cycle をもつ。この cycle に対応して G の中で 2 つの cycle がある。1 つは診断器の cycle の中に F_i ラベルを持つ 3-5 状態を含む。もう 1 つは診断器の cycle の中に N というラベルを持つ状態 11-13 を含む。そして, 観測不能事象 σ_{uo} を経由して, 状態 14 に到達する。したがって, システム G は診断不可能である。

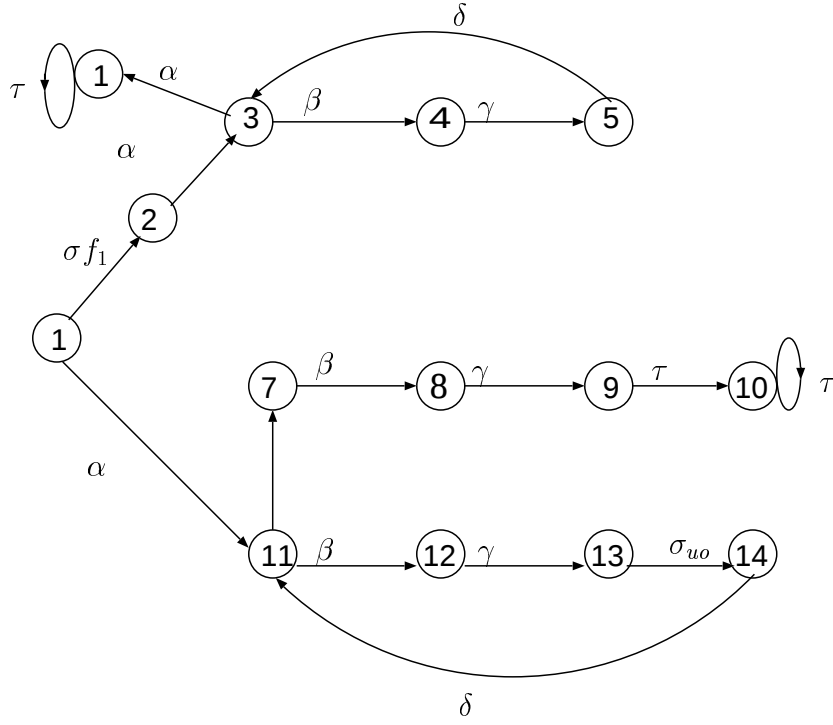


図 3.2: 診断不可能なシステム G .

例では, G_d の cycle は G の cycle に直接対応していた . しかしながら , 一般的には , G_d の Fi -indeterminate cycle が G に対して , 1 つあるいは 2 つ以上の cycle に対応することになるかもしれない .

つぎに , 診断可能な例を示す .

例 3.2 図 3.4 , 図 3.5 に診断可能な例を示す . 診断可能性の条件において , 観測可能事象に射影した状態空間の cycle で , 含まれる状態の障害事象グループのラベルが一意に決まらないもの (Fi -indeterminate cycle) が存在しないため , 診断可能である .

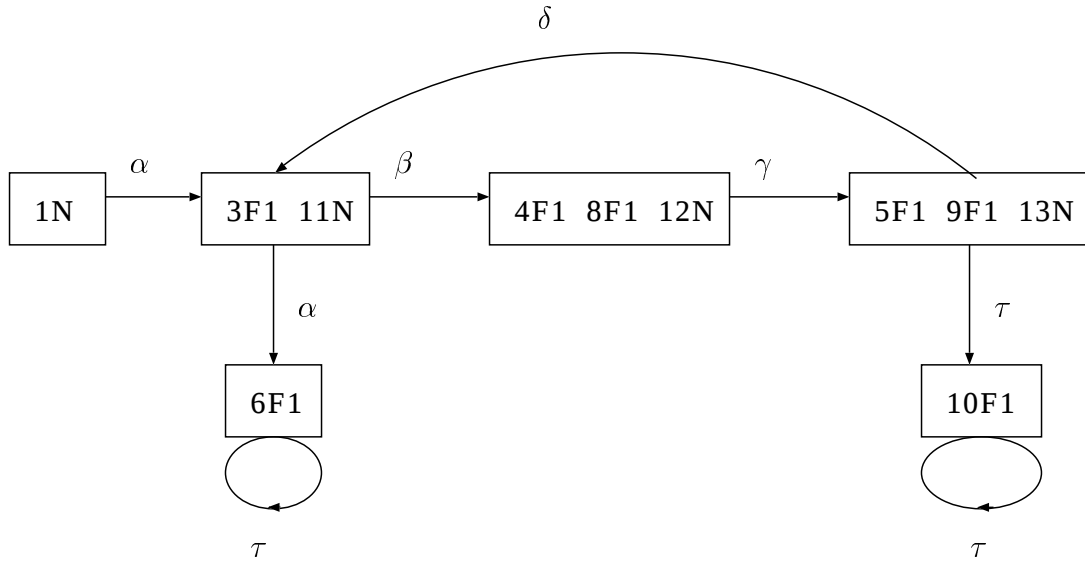


図 3.3: 診断器 G_d .

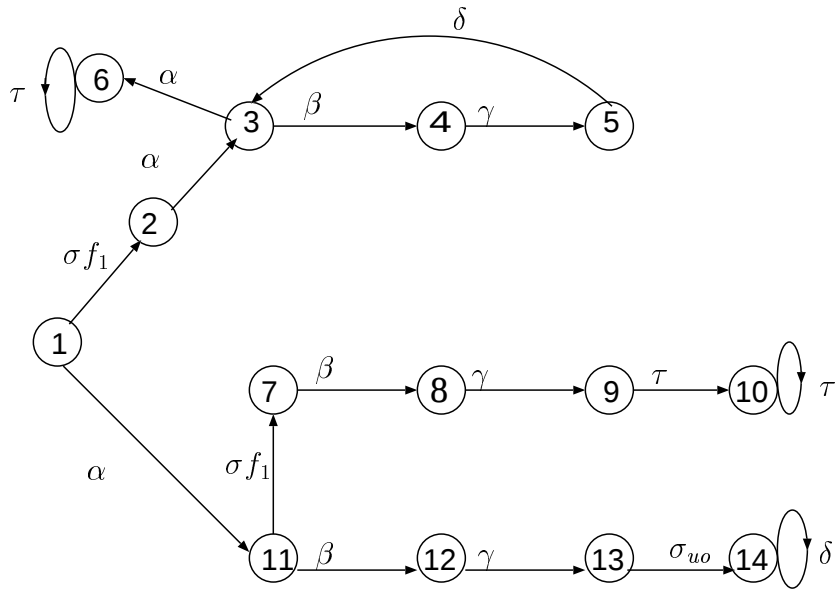


図 3.4: 診断可能なシステム G .

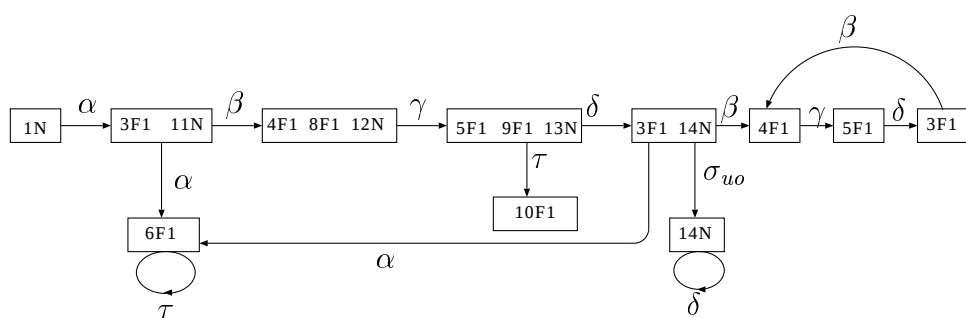


図 3.5: 診断器 Gd .

第 4 章

ペトリネットに対する診断可能性判定問題

従来研究の診断可能性の定義では、システムを表すオートマトンが与えられているとしているが、実際にはこのオートマトンのサイズが膨大になり、診断可能性を判定するためには多大の計算時間を必要とする。本研究では、この問題をペトリネットの構造的特徴を用いることで回避することを目的とする。

4.1 準備

Σ を空ラベル λ を含むラベルの集合、 $\ell : T \rightarrow \Sigma$ をラベル付け関数とする。 ℓ は $T^* \rightarrow \Sigma^*$ に拡張される。ラベル付け関数 ℓ が定義されたペトリネット (ペトリネット構造) を PN^ℓ (C^ℓ) で表す。 $L(PN)$ により、 PN において、初期マーキングから発火可能なトランジション系列の集合を表す。

以下を満たすときペトリネット PN はライブであるという。

$$\forall s \in L(PN) \exists t \in T : st \in L(PN).$$

ラベル付けペトリネットを、ラベル付け関数の性質により以下のように分類する。

1. 自由ラベルペトリネット：各トランジションには固有のラベルまたは λ がラベルつけられている。すなわち、

$$\forall t_i, t_j \in T : \ell(t_i) = \ell(t_j) \neq \lambda \Rightarrow t_i = t_j.$$

2. 一般ラベルペトリネット：上記の制約のない一般の場合．

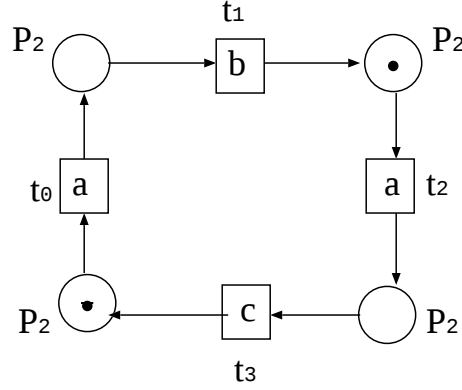


図 4.1: 一般ペトリネット

図 4.1 は 一般ラベルペトリネットの例である． λ のラベルがついたトランジションは観測不能，それ以外のトランジションは観測可能であるという．

4.2 ペトリネットの診断可能性

T 上の言語 L は以下を満たすときラベル付け関数 ℓ および障害トランジション $t_f \in T$ に関して診断可能であるという．

$$\exists n \in \mathbb{N}[(st_f s' \in L \wedge \|s'\| \geq n) \Rightarrow (\forall s'' \in L : \ell(st_f s') = \ell(s'') \Rightarrow t_f \in s'').$$

また， $L(PN)$ が ℓ および t_f に関して診断可能なとき， PN^ℓ は t_f に関して診断可能であるという．一般性を失うことなしに， $\ell(t_f) = \lambda$ を仮定する．

4.3 診断可能性判定問題

以下の 2 つの診断可能性判定問題を定義する．

1. 構造的診断可能性判定問題：ラベル付きペトリネット構造 C^ℓ および障害トランジション t_f が与えられる．このとき，以下が成り立つかどうかを判定する： (C^ℓ, M_0)

がライブであるような任意の初期マーキング M_0 に対して, (C^ℓ, M_0) が t_f に関して診断可能である.

2. 初期マーキング依存診断可能性判定問題: ライブなラベル付きペトリネット PN^ℓ および障害トランジション t_f が与えられる. このとき, PN^ℓ が t_f に関して診断可能であるかどうかを判定する.

4.4 一般ラベルペトリネットの診断可能性

一般ラベルペトリネットの診断可能性問題は, 自由ラベルペトリネットの診断可能性問題に帰着できる.

一般ラベルペトリネット PN^ℓ から以下のようにして自由ラベルペトリネット $\underline{PN}^{\ell'}$ を作る (図 4.2).

1. 複数のトランジションにつけられている空でないラベルからなる集合を Σ' とする. また, それらのラベルが付けられているトランジション集合を T' とする.
2. 各 $a \in \Sigma'$ に対し, 1つの入力プレース p_a^I と1つの出力プレース p_a^O をもつトランジション t_a を加える. また, $\ell'(t_a) = a$ とする.
3. $\ell(t_i) = a$ ならば, t_i を2つのトランジション t_i^I, t_i^O , および1つのプレース p_i で置き換える. このとき,
 - $\ell'(t_i^I) = \ell'(t_i^O) = \lambda$.
 - t_i^I の入力 t_i のそれに等しく, t_i^O の出力 t_i のそれに等しい.
 - t_i^I の出力 p_i および p_a^I , t_i^O の入力 p_i および p_a^O とする. これらのアークの重みはすべて1とする.

以下が成り立つ.

- 任意の $s \in L(PN)$ に対し, 含まれる各 $t_i \in T'$ を系列 $t_i^I t_{l(t_i)} t_i^O$ で置き換えた系列を $\underline{s}$ とする. このとき, $\underline{s} \in L(\underline{PN})$ である.
- 任意の $s \in L(\underline{PN})$ に対し, 各 $t_i \in T'$ について, s に含まれる t_i^I, t_i^O を消去し, さらに $t_{l(t_i)}$ を t_i で置き換えた系列を $\bar{s}$ とする. このとき, $\bar{s} \in L(PN)$ である.

- 言語

$$L'(\underline{PN}) = \{s \in L(\underline{PN}) \mid s = \overline{(\underline{s})}\}$$

を定義する．このとき，写像 $\underline{\cdot}$ は $L(\underline{PN})$ と $L'(\underline{PN})$ の間の 1 対 1 対応であり， $\overline{\cdot}$ は $\underline{\cdot}$ の逆写像である．

- 任意の $s \in L(\underline{PN})$ について， $l(s) = l(\underline{s})$ である．
- 任意の $s \in L(\underline{PN})$ について，

$$t_f \in s \Leftrightarrow t_f \in \underline{s}$$

が成り立つ．

以上より，言語 $L(\underline{PN})$ が ℓ に関して診断可能ならば，かつそのときに限り，言語 $L'(\underline{PN})$ が ℓ' に関して診断可能であることが示せる．

$L(\underline{PN}) - L'(\underline{PN})$ の系列については以下が成り立つ．任意の $s \in L(\underline{PN})$ について，

- $t_f \in s$ ならば， $\ell'(s) = \ell'(s')$ かつ $t_f \in s'$ であるような $s' \in L'(\underline{PN})$ が存在する．
- $t_f \notin s$ ならば， $\ell'(s) = \ell'(s')$ かつ $t_f \notin s'$ であるような $s' \in L'(\underline{PN})$ が存在する．

s' は各 $t_i \in T'$ について， t_i^I, t_i^O を対応する $t_{l(t_i)}$ の直前，直後に移動させることで得られる．このことから，言語 $L'(\underline{PN})$ についての診断可能性を議論すれば十分であることがわかる．

以上の議論からつぎの定理が得られる．

定理 4.1 一般ラベルペトリネット PN^ℓ が診断可能ならば，かつそのときに限り，自由ラベルペトリネット $\underline{PN}^\ell$ は診断可能である．

以下の章では，自由ラベルペトリネットの診断可能性についてのみ扱う．

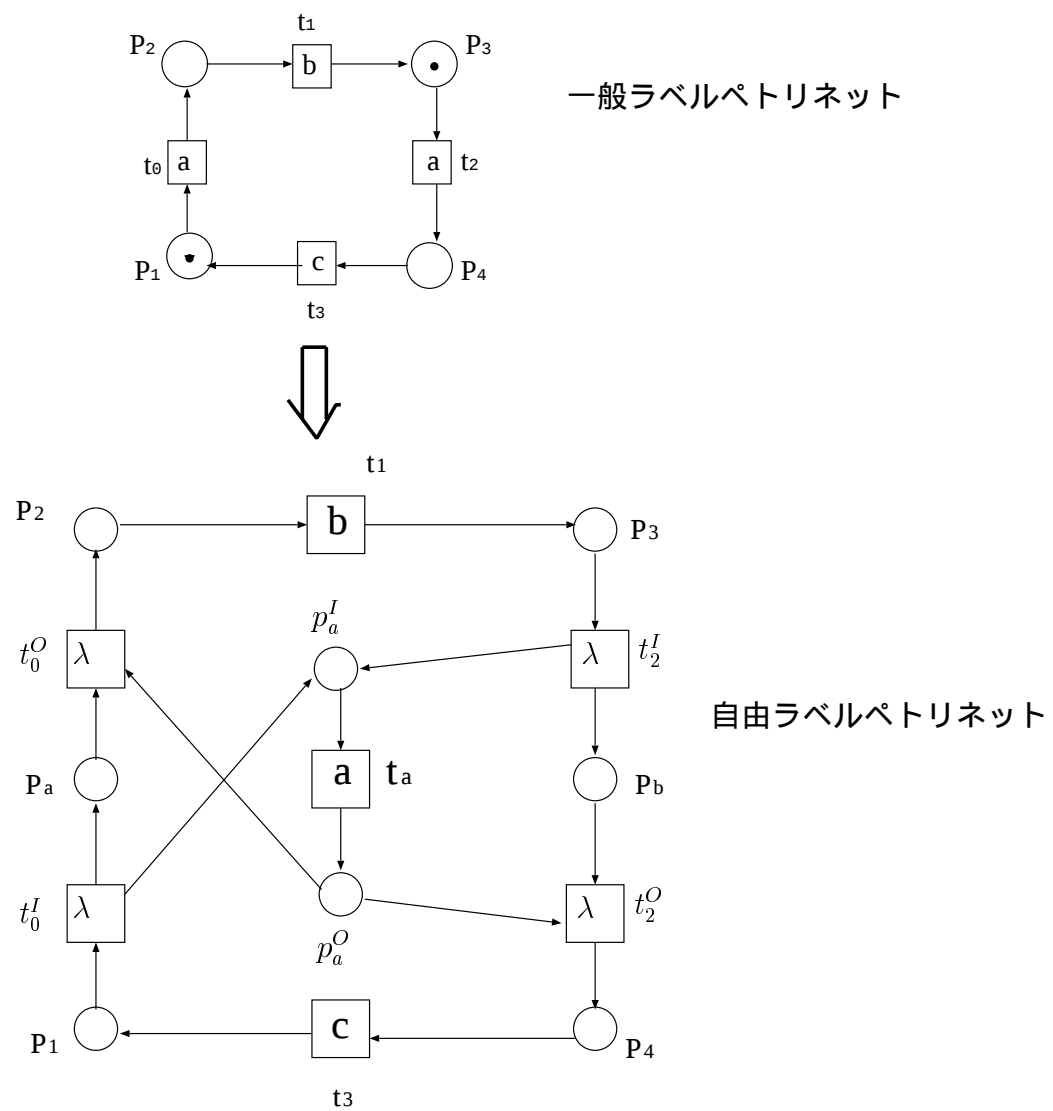


図 4.2: 一般ラベルペトリネットの自由ラベルペトリネットへの変換 .

第 5 章

自由ラベルペトリネットの診断可能性

本章では，自由ラベルペトリネットの診断可能性に対する必要十分条件を示す．

5.1 仮定

有限オートマトンで表現される離散事象システムと同様に，自由ラベル付きペトリネット PN^ℓ に以下の仮定を置く．

- A1. PN^ℓ はライブである．すなわち，デッドなマーキング（どのトランジションも発火可能でないマーキング）は初期マーキングから到達しない．
- A2. PN^ℓ において，初期マーキングから到達可能なマーキングから発火可能な，観測不能なトランジションのみからなる無限系列は存在しない．

5.2 構造的診断可能性

自由ラベルペトリネット (C^ℓ, M_0) が与えられる． t_f を障害トランジションとし，つぎのようなライブな初期マーキング M_0 が存在したと仮定する．

1. $M_0 \xrightarrow{t_f}$ ．
2. t_f を含まない発火系列 s が存在して，

(i) $M_0 \xrightarrow{s} M, M \geq M_0$.

(ii) $M_0 \xrightarrow{t_f s}$.

このとき, $l(t_f s^*) = l(s^*)$ なので, t_f が発火したことを判定できない .

いま ,

$$\Gamma = \{x \in \mathbb{N}^T \mid Ax \geq 0\}$$

とする . Γ のベクトルを T -増加ベクトルとよぶ . Γ のベクトルは , その回数の発火によりトークン数が減少しないような発火回数ベクトルである .

$\psi(s) : T \rightarrow \mathbb{N}$ により , 発火系列 s に各トランジションが何回出現するかを示す写像 (発火回数ベクトル) を表す . x を発火回数ベクトルとしたとき , $x(t_i) > 0$ であるようなトランジション集合を x のサポート集合といい T_x で表す . すなわち ,

$$T_x = \{t \in T \mid x(t_i) > 0\}.$$

補題 5.1 ペトリネットの任意の T -増加ベクトル x に対し , $M_0 \xrightarrow{s} M, M \geq M_0$ かつ $\psi(s) = x$ であるような初期マーキング M_0 および発火系列 s が存在する .

証明 十分多くのトークンを初期マーキングに与えれば , $x(t) > 0$ であるようなトランジション t を $x(t)$ 回だけ任意の順序で発火させることができる . ■

補題 5.2 (Lemma 4.1, [6]) 非負整数ベクトルの無限列は非減少な無限長の部分列を含む .

補題 5.3 t_f がすべての T -増加ベクトルのサポート集合に含まれるならば , ライブな任意の初期マーキングから t_f は必ず発火する .

証明 ペトリネットはライブなので , 初期マーキングから発火可能な無限列が存在する . また , それに対応したマーキングの無限列が存在する . 補題 5.2 より , それは非減少な無限長の部分列 $M_{[1]}, M_{[2]}, \dots$ を含む . $M_{[i]} \xrightarrow{s} M_{[i+1]}$ とすれば , $\psi(s)$ は T -増加ベクトルであり , s は t_f を含む . ■

定理 5.4 自由ラベルペトリネット構造が t_f について構造的診断可能であるための必要十分条件は，任意の T -増加ベクトル x についてつぎの (i), (ii) を満たすことである．

(i) $x(t_f) > 0$ ．

(ii) x のサポート集合に少なくとも 1 つは空でないラベルをもつトランジションが存在する．

証明 必要性は前の議論より従う．十分性を示す．どのようなライブな初期マーキングを与えても，(ii) よりいずれは，ある T -増加ベクトル以上の回数の発火が行われることになる．(i) よりその中には t_f が含まれる．ゆえに，構造的診断可能である． ■

t_f がすべての T -増加ベクトルのサポート集合に含まれるならば，何も観測しなくても， t_i がいずれ発火することは確定している．問題は， t_i が確実に発火したことが判定できるかどうか，すなわち，診断可能性の定義における自然数 n の値を求めることができるかどうかである．

初期マーキングが与えられれば， n の値の最小値は状態遷移グラフを探索することで求められる．アルゴリズムを付録に示す．以下では， T -増加ベクトルに対応する発火系列が出現するのに必要な発火回数の上界を求める問題について考察する．これにより，探索することなしに， n の値の上界の 1 つを求めることができる．

問題：トランジションの発火により生成されるマーキングの系列を考える．

$$m_0 \xrightarrow{t_1} m_1 \xrightarrow{t_2} \dots \xrightarrow{t_k} m_k$$

ただし，任意の $i < j$ について， $m_i \leq m_j$ ではないとする．このとき， k の上界を求めよ． ■

各トランジションからプレース p_i への出力アークの重みの最大値を w_i とする．

1 次元の場合： $m_0(p_1)$ 以下の非負整数の総数は $m_0(p_1)$ 個なので，

$$k \leq m_0(p_1).$$

2 次元の場合：

- $m_j(p_1) > m_0(p_1)$ ならば $m_j(p_2) < m_0(p_2)$ である .

$$m_{j_1}(p_1) > m_0(p_1), m_{j_2}(p_1) > m_0(p_1), m_{j_1}(p_2) = m_{j_2}(p_2) (j_1 < j_2)$$

ならば ,

$$m_{j_1}(p_1) > m_{j_2}(p_1)$$

でなければならない . このような j_i の列

$$j_1 < j_2 < \cdots < j_r$$

を考える . すなわち ,

$$m_{j_1}(p_1) > m_{j_2}(p_1) > \cdots > m_{j_r}(p_1) \quad (5.1)$$

$$m_{j_1}(p_2) = m_{j_2}(p_2) = \cdots = m_{j_r}(p_2)$$

となるような j_i の列である .

まず , $m_{j_1}(p_1)$ の値の上界を求める . マーキング系列 $m_0 m_1 \cdots m_k$ において , m_0 から始まり , 第 1 成分が増加する部分列 $m_0 m_{l_1} m_{l_2} \cdots m_{l_v}$ を考えると , 第 2 成分は単調減少する . すなわち ,

$$m_0(p_1) < m_{l_1}(p_1) < m_{l_2}(p_1) < \cdots < m_{l_v}(p_1),$$

$$m_0(p_2) > m_{l_1}(p_2) > m_{l_2}(p_2) > \cdots > m_{l_v}(p_2) \geq 0$$

である . したがって , $v \leq m_0(p_2)$ である . このことから ,

$$m_{j_1}(p_1) \leq m_{l_v}(p_1) \leq m_0(p_1) + w_1 \cdots v \leq m_0(p_1) + w_1 \cdot m_0(p_2)$$

が得られる .

r の上界を求める . (5.1) 式より ,

$$m_{j_1}(p_1) - (r + 1) \geq 0$$

であり ,

$$r \leq 1 + m_{j_1}(p_1) \leq 1 + m_0(p_1) + w_1 \cdot m_0(p_2)$$

が得られる .

このような列 $j_1 < j_2 < \cdots < j_r$ はたかだか $m_0(p_2)$ 個存在するので , $m_j(p_1) > m_0(p_1)$ かつ $m_j(p_2) < m_0(p_2)$ であるような j の個数の上界として ,

$$m_0(p_2) \cdot (1 + m_0(p_1) + w_1 \cdot m_0(p_2))$$

が得られる .

- $m_j(p_1) < m_0(p_1)$ かつ $m_j(p_2) > m_0(p_2)$ であるような j の個数の上界は同様にして

$$m_0(p_1) \cdot (1 + m_0(p_2) + w_2 \cdot m_0(p_1))$$

である .

- $m_j(p_1) \leq m_0(p_1)$ かつ $m_j(p_2) \leq m_0(p_2)$ であるような j の個数の上界は

$$(m_0(p_1) + 1) \cdot (m_0(p_2) + 1)$$

である .

- したがって , k の上界として

$$\begin{aligned} & m_0(p_2) \cdot (1 + m_0(p_1) + w_1 \cdot m_0(p_2)) \\ & + m_0(p_1) \cdot (1 + m_0(p_2) + w_2 \cdot m_0(p_1)) \\ & + (m_0(p_1) + 1) \cdot (m_0(p_2) + 1) \end{aligned}$$

が得られる .

n 次元の場合 : 同様な考え方により , k の上界はつぎの式で表される .

$$\sum_{i=1, n} U_{\bar{i}} \cdot (1 + m_0(p_i) + w_i \cdot U_{\bar{i}}) + \prod_{i=1, n} (m_0(p_i) + 1). \quad (5.2)$$

ここで , 第 i 次元以外への成分からなるベクトル列に対する k の上界を $U_{\bar{i}}$ である .

$m_j^{[\bar{i}]}$ により , m_j の第 i 次元以外の成分からなるベクトルを表す .

- $m_j(p_i) > m_0(p_i)$ であるような m_j からなる部分列

$$m_{j_1} m_{j_2} \cdots m_{j_q}$$

に対し，列

$$m_{j_1}^{[i]} m_{j_2}^{[i]} \cdots m_{j_q}^{[i]}$$

を考える．このとき， $q - 1 \leq U_i$ である．

$$m_{j_1}(p_i) > m_0(p_i), m_{j_2}(p_i) > m_0(p_i), m_{j_1}^{[i]} = m_{j_2}^{[i]} (j_1 < j_2)$$

のとき，

$$m_{j_1}(p_i) > m_{j_2}(p_i)$$

でなければならない．このような j_i の列

$$j_1 < j_2 < \cdots < j_r$$

を考える． $m_{j_1}(p_i)$ の上界はつぎのように与えられる．

$$m_{j_1}(p_i) \leq m_0(p_i) + w_i \cdot (q - 1) \leq m_0(p_i) + w_i \cdot U_i$$

したがって，

$$r \leq 1 + m_{j_1}(p_i) \leq 1 + m_0(p_i) + w_1 \cdot U_i$$

が得られる．このような列 $j_1 < j_2 < \cdots < j_r$ はたかだか U_i 個存在するので， $m_j(p_i) > m_0(p_i)$ であるような j の個数の上界として，

$$U_i \cdot (1 + m_0(p_i) + w_1 \cdot U_i)$$

が得られる．

- $m_j(p_i) \leq m_0(p_i)$ ($i = 1, \dots, n$) であるような j の個数の上界として

$$\prod_{i=1,n} (m_0(p_i) + 1)$$

が得られる．

このように求められた k の上界よりも多いトランジション数を観測すれば，それまでの発火系列の発火回数ベクトルはある T -増加ベクトルを含む．

5.3 初期マーキング依存診断可能性

非有界ペトリネットでは、状態遷移グラフが無限の大きさをもつので、有限オートマトンのように診断器を作る方法では診断可能性は判定できない。しかしながら、マーキングが非減少となるような発火系列は任意回発火できるという性質から、つぎの補題が得られる。

補題 5.5 PN^ℓ をラベル付ペトリネット、 M_0 を初期マーキングとする。以下のような発火系列 $s_1 s_2, s_3 s_4$ が存在するならば、 PN^ℓ は診断不可能である。

- (i) $M_0 \xrightarrow{s_1} M_1 \xrightarrow{s_2} M_2, M_1 \leq M_2$;
- (ii) $M_0 \xrightarrow{s_3} M_3 \xrightarrow{s_4} M_4, M_3 \leq M_4$;
- (iii) $l(s_1) = l(s_3), l(s_2) = l(s_4)$;
- (iv) $t_f \in s_1 s_2, t_f \notin s_3 s_4$.

証明 任意の自然数 k について、系列 $s_1(s_2)^k, s_3(s_4)^k$ は (i) M_0 から発火可能；(ii) 観測結果が等しい；(iii) 前者は t_f を含み後者は含まない。したがって、診断可能性の定義より PN^ℓ は診断可能ではない。 ■

補題 5.5 の条件を満たす系列は、有限オートマトンの場合の診断器 G_d 上の F_i -indeterminate cycle に対応する。このような系列は（もし存在するならば）初期マーキングからの幅優先探索により有限の手続きで発見できる。

例：図 5.1 において、 $s_1 = t_f, s_2 = t_2, s_3 = t_1, s_4 = t_2$ とすると補題の条件を満たす。従って、診断可能ではない。

補題 5.5 の条件は、 PN が診断不可能であるための必要条件にもなる。

補題 5.6 PN^ℓ をラベル付きペトリネット、 M_0 を初期マーキングとする。 PN^ℓ が診断不可能ならば、補題 5.5 の (i)–(iv) を満たす発火系列 $s_1 s_2, s_3 s_4$ が存在する。

証明 PN は診断不可能なので、診断可能性の定義式より、任意の自然数 n に対して以下のような発火系列 s, s', s'' が存在する。

$$st_f s' \in L(PN) \wedge \|s'\| \geq n \wedge l(st_f s') = l(s'') \wedge t_f \notin s''.$$

仮定 A2 より，観測不可能なトランジションのみからなる無限発火系列は存在しないので， n を大きくすれば，条件を満たす系列 s'' もそれに応じて長くなる．いま，

$$s' = s'_a s'_b, \quad s'' = s''_a s''_b, \quad l(st_f s'_a) = l(s''_a)$$

となるように系列 s', s'' を分割する．さらに， $l(s'_b) = l(s''_b)$ なので，

$$\begin{aligned} s'_b &= \alpha_1 \alpha_2 \cdots \alpha_m, \\ s''_b &= \beta_1 \beta_2 \cdots \beta_m, \\ l(\alpha_i) &= l(\beta_i) \quad (i = 1, \dots, m) \end{aligned}$$

と分割できる．このとき，以下のマーキングを定義する．

$$M'_0 = M_0 + A\psi(st_f s'_a); \quad M'_i = M_0 + A\psi(st_f s'_a \alpha_1 \cdots \alpha_i) \quad (i = 1, \dots, m),$$

$$M''_0 = M_0 + A\psi(s''_a); \quad M''_i = M_0 + A\psi(s''_a \beta_1 \cdots \beta_i) \quad (i = 1, \dots, m).$$

ベクトル $[M'_i, M''_i]$ の列を考えると，補題 5.2 より n を十分大きくとれば，この列は非減少な部分列を含む．すなわち，ある j, k ($j < k$) が存在して，

$$M'_j \leq M'_k, \quad M''_j \leq M''_k$$

である．

$$\begin{aligned} s_1 &= st_f s'_a \alpha_1 \cdots \alpha_j, \\ s_2 &= \alpha_{j+1} \cdots \alpha_k, \\ s_3 &= s''_a \beta_1 \cdots \beta_j, \\ s_4 &= \beta_{j+1} \cdots \beta_k \end{aligned}$$

とすれば，補題 5.5 の条件を満たす． ■

定理 5.7 PN^ℓ をラベル付ペトリネット， M_0 を初期マーキングとする． PN^ℓ が診断可能であるための必要十分条件は，補題 5.5 の条件を満たす系列が存在しないことである．

残された問題は，定理 5.7 の条件をチェックする有限のステップで停止する手続きが存在するかどうかである．前述のように，幅優先探索を用いれば，補題 5.5 の条件を満たす系列が存在する場合には必ず見つけることができるが，存在しない場合は探索が終了しない．よく知られているように，ペトリネットに関するいくつかの問題は決定不能である [7]．診断可能性の判定問題が決定可能かどうかについては今後の課題である．

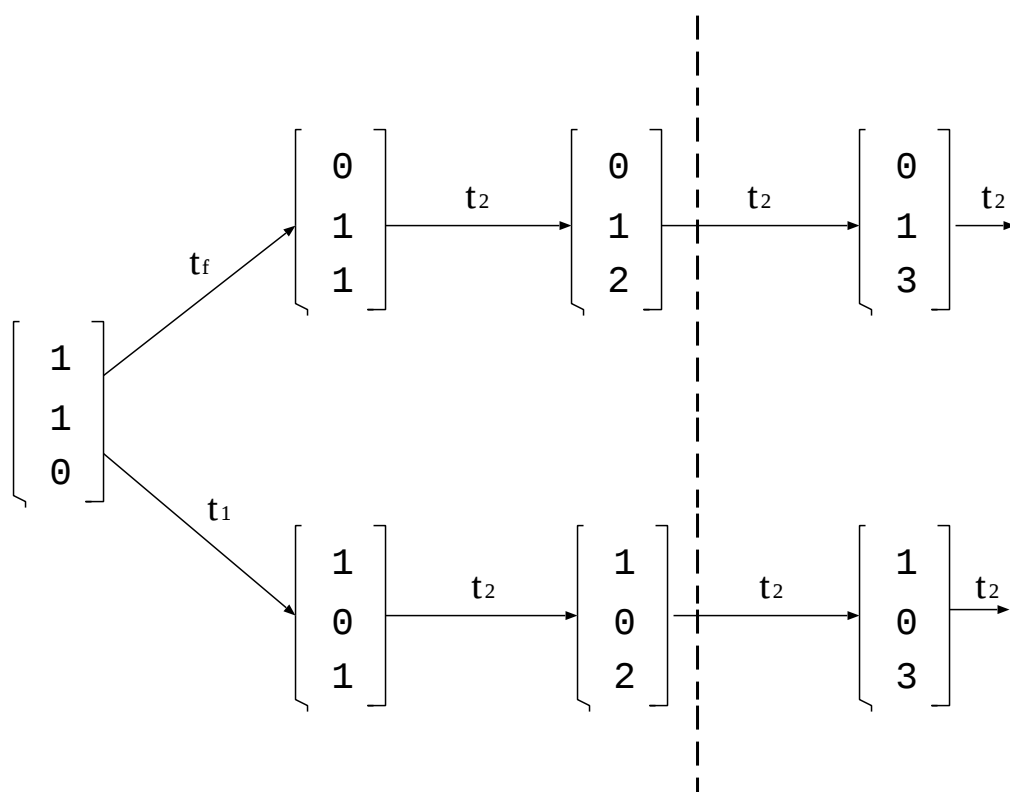
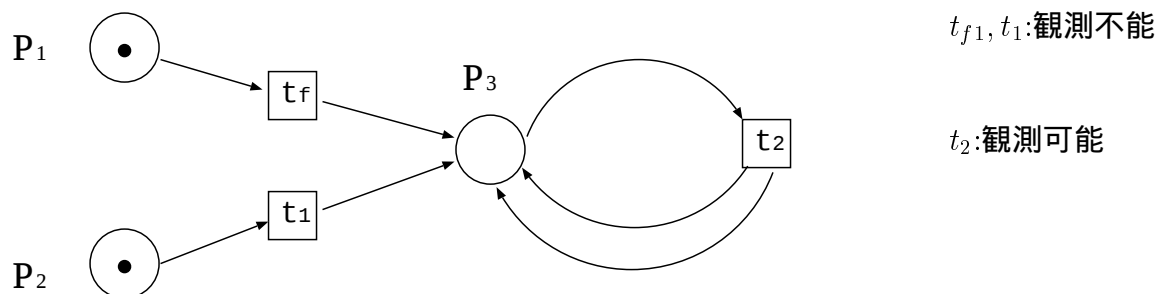


図 5.1: 非有界ペトリネットにおいて診断可能性を判定する例 .

第 6 章

まとめ

本稿では，オートマトンで記述した離散事象システム診断可能性についての議論をペトリネットに適用し，つぎの結果が得られた．

- 一般ラベルペトリネットの診断可能性問題は自由ラベルペトリネットの診断可能性問題に帰着できる．
- 任意のライブな初期マーキングに対して診断可能であるという構造的診断可能性，および，与えられた 1 つの初期マーキングに対して診断可能性であるというマーキング依存診断可能性の 2 つの問題を提示し，それらについて，診断可能であるための必要十分条件を示した．
- 診断可能である場合に，診断できるまでの遅延を計算するアルゴリズムを示した．

有界なペトリネットに対しては，診断可能性は決定可能である．非有界なペトリネットに対し，マーキング依存診断可能性を判定する問題が決定可能かどうかについては今後の課題として残された．

付 録 A

与えられた自由ラベルペトリネットに対する診断器の構成法を示し，さらに診断可能な場合に遅延 n を求めるアルゴリズムを示す．

A.1 診断器構成アルゴリズム

初期マーキング M_0 から以下のような幅優先探索を行う．

- 探索木の各ノードは，ラベル N または F が付いたマーキングの集合（状態見積もりという）である．ルートノードは $N_0 = \{N : M_0\}$ である．

- ノード

$$N_i = \{L_1^i : M_1^i, \dots, L_k^i : N_v^i\},$$

および，観測可能なトランジション t から，子ノード

$$N_j = \{L_1^j : M_1^j, \dots, L_r^j : M_w^j\}$$

を作る．ここで，

$$\exists s_k \in T^* : M_k^i \xrightarrow{s_k t} M_l^j \wedge \ell(s_k t) = t$$

$$L_l^j = \begin{cases} F & (L_k^i = F) \\ F & (L_k^i = N \wedge t_f \in s_k) \\ N & (L_k^i = N \wedge t_f \notin s_k) \end{cases}$$

である．

- certain 状態とは，ラベル F をもつマーキングのみからなる状態見積りのことである．また，uncertain 状態とは，ラベル F がついているマーキングと N がついているマーキングをそれぞれ少なくとも1つずつ含む状態見積りのことである．
- 新しいノード N_i が作られたとき，
 - certain 状態に入ったら，それ以上深くは探索しない．
 - ルートから N_i までのパス上のノードに同じ状態見積りをもつノードが存在すれば， F -indeterminate cycle ができるので，診断不可能と判定して探索は停止する．

最後に，同じ状態見積りを1つのノードとして表現することにより，診断器が構成できる．

A.2 遅延の求め方

1. 初期マーキング M_0 からの深さ優先探索により，つぎのようなマーキング M_i を求める．

$$\exists s \in T^* : M_0 \xrightarrow{stf} M_i \wedge t_f \notin s.$$

このような M_i が発見されるごとに，以下のようにして非負整数値 n_i を求める．

- 1-1 M_i から以下のような深さ優先探索を行う．

- 探索の1ステップは（観測可能／不能に関係なく）発火可能な1つのトランジションの発火である．
- 探索木の各ノードは，組
 (マーキング，対応する診断器の状態見積り)
 からなる．
- 診断器上で certain 状態に入れば，それより深くは探索せず，バックトラックを行う．

- 同じ値をもつノードが探索済みならば、それより深くは探索しない．発火可能なトランジションによる遷移先のノードがすべて探索済みの場合，バックトラックを行う．

1-2 上記の深さ優先探索において，バックトラックした順番の逆順により，ノード集合上のトポロジカルソートを得る．これにより，探索木のノードに 0 から k までの番号を振る．

1-3 $val(0) = 0$ とする． $l = 1, \dots, k$ の順で， $val(l)$ をつぎのように計算する：ノード l の 1 つ手前のノードを $l_1, \dots, l_r$ としたとき，

$$val(l) = \max\{val(l_1), \dots, val(l_r)\} + 1.$$

- $val(l)$ の値の最大値を n_i とする．

2. n_i の最大値を遅延値とする．

例として図 A.1 のペトリネットを考える．ここで，

- t_f ：障害トランジション．
- t_3 ：観測不能トランジション．
- t_1, t_2 ：観測可能トランジション．

である．

マーキング遷移図は図 A.2 である．これから作られる診断器 G_d は図 A.3 である．遅延値を求めるための計算過程を図 A.4, A.5 に示す．

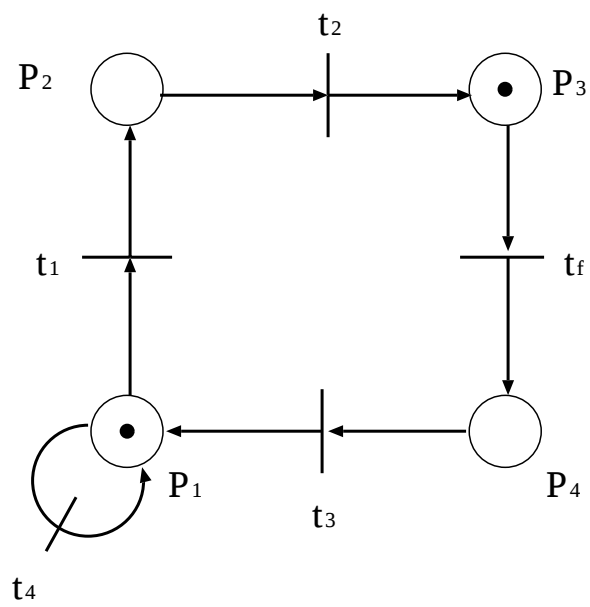


図 A.1: 診断可能ペトリネット

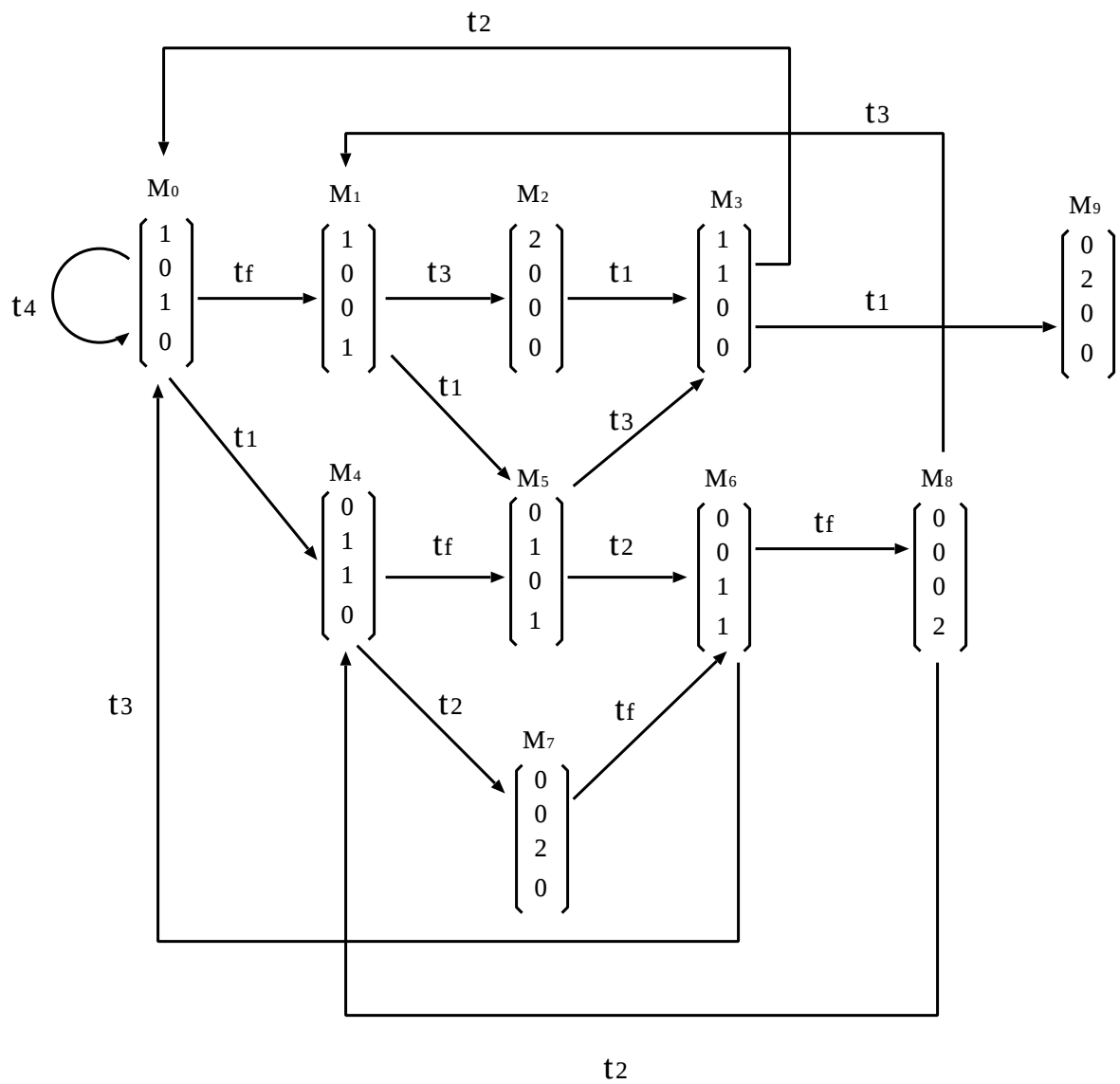
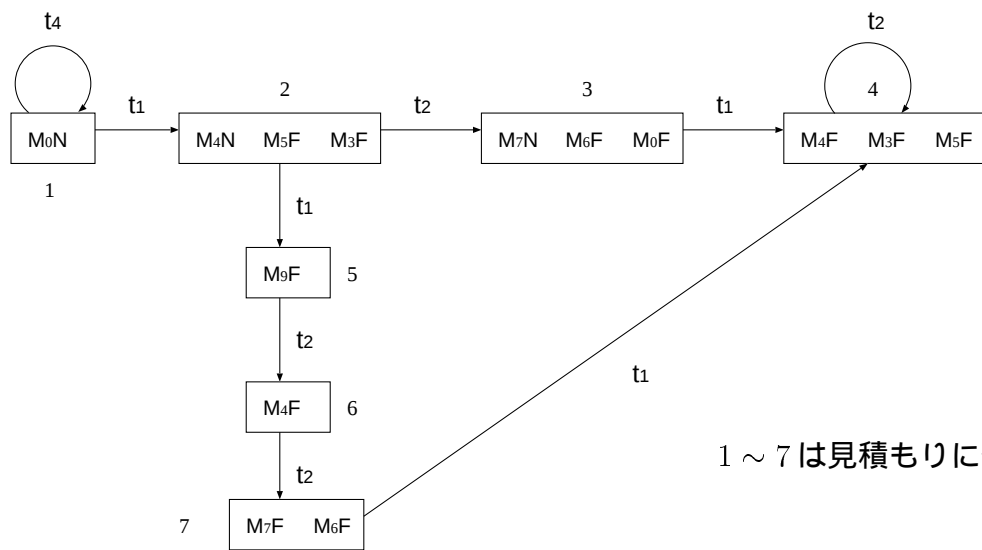
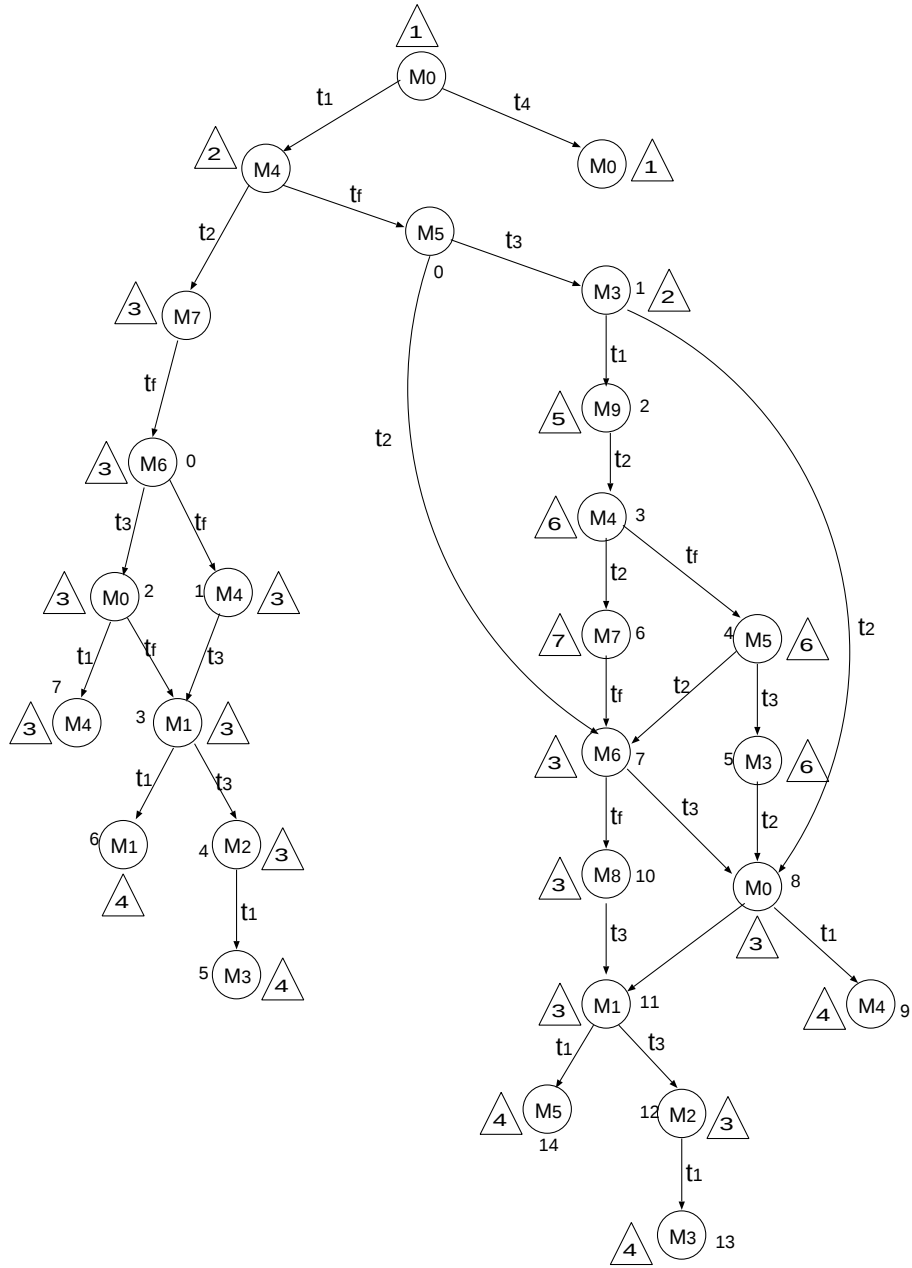


図 A.2: マーキング遷移図 .



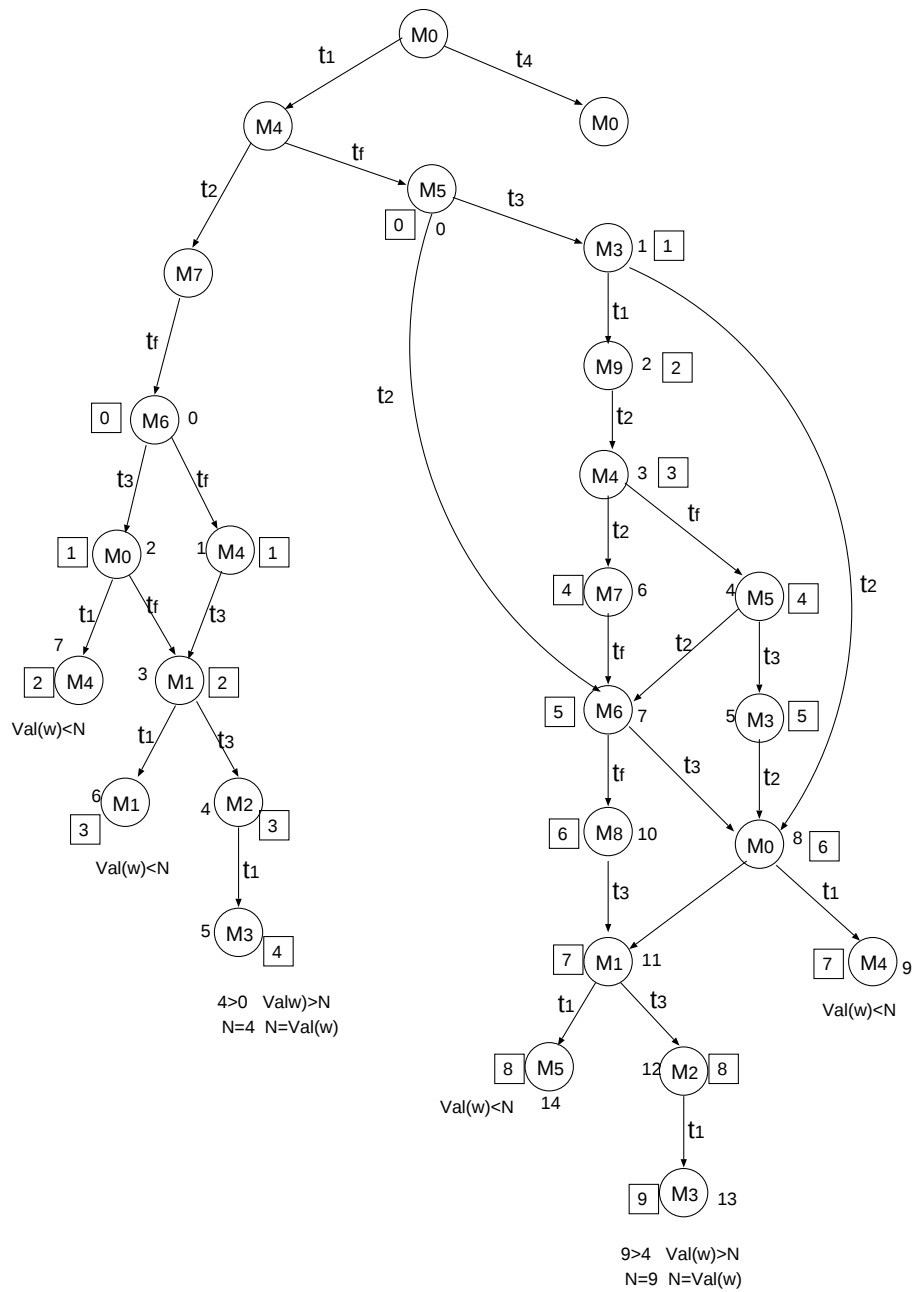
1 ~ 7 は見積もりに付けた番号である .

図 A.3: 診断器 G_d .



△₁ - △₄ は診断器上の見積もり番号である .
 1~13 はトポロジカルソートの番号である .

図 A.4: 遅延を求めるための探索 .



1 ~ 9 各マーキングに付いている値

1~13 はトポロジカルソートの番号である .

図 A.5: 遅延値を求めるための計算過程 .

参考文献

- [1] P.J. Ramadge and W. M. Whonham: The control of discrete event systems, in Proc. IEEE, Vol. 77, No. 1, pp.81–98 (1989).
- [2] 離散事象システム研究専門委員会編, ペトリネットとその応用, (社)計測自動制御学会, (1992).
- [3] 潮 俊光, 離散事象システムにおける制御問題とスーパーバイザ, システム/制御/情報, Vol.34, No.9, pp.531-538 (1990).
- [4] M.Sampath, S.Lafortune, and D. Teneketzis, Active Diagnosis of Discrete-Event Systems, IEEE Transactions on Automatic Control, Vol.43, No.7, pp.908-929 (1998).
- [5] F. Lin, Diagnosability of Discrete Event Systems and Its Applications, Discrete Event Dynamic Systems, Vol.4, pp.197-212(1994).
- [6] R. karp and R. Miller, Parallel Program Schemata, J. Computer and System Science, Vol.3, pp.147-195 (1969).
- [7] J.L.Peterson, Petri Net Theory and the Modeling of Systems, Prentice-Hall (1981).

謝辞

本研究を行うにあたり，日頃から温かくご指導いただしてくれた平石助教授に深く感謝致します．また，有益なご助言や御討論いただいた平石研究室の皆様に感謝致します．