

PPN . 095549749

UNIVERSITÉ Paul Verlaine - METZ S.C.D.	
N° Inv	2005007S
Cote	S/M 05/03
Loc	mag. 1 ^{er} étage

THÈSE

présentée à

L'Université Paul Verlaine METZ

Faculté des Sciences

UFR Mathématiques, Informatique, Mécanique

pour obtenir le titre de

DOCTEUR

**EXCLU DU
PRÊT**

Spécialité

SCIENCES DE L'INGÉNIER
(mention : AUTOMATIQUE)

par

Zied ACHOUR

Titre de la thèse :

**Contribution à la synthèse des contrôleurs des systèmes à
événements discrets partiellement observables**

Soutenue le 20 octobre 2005 devant le jury composé de :

Rapporteurs : Etienne CRAYE Professeur à l'Ecole Centrale de Lille
Robert VALETTE Directeur de Recherche CNRS au LAAS

Examinateurs : Gérard MOREL Professeur à l'Université Henri Poincaré de Nancy
Janan ZAYTOON Professeur à l'Université de Reims

Directeur de thèse : Nidhal REZG Professeur à l'Université Paul Verlaine de Metz

Co-directeur de thèse : Xiaolan XIE Professeur à l'Ecole Nationale Supérieur des Mines de Saint-Etienne

BIBLIOTHEQUE UNIVERSITAIRE DE METZ



031 536275 2



Avertissement

Cette thèse est le fruit d'un long travail approuvé par le jury de soutenance et disponible à l'ensemble de la communauté universitaire élargie.

Elle est soumise à la propriété intellectuelle de l'auteur au même titre que sa version papier. Ceci implique une obligation de citation, de référencement dans la rédaction de tous vos documents.

D'autre part, toutes contrefaçons, plagiats, reproductions illicites entraînent une poursuite pénale. Enfin, l'autorisation de diffusion a été accordée jusqu'à nouvel ordre.

➤ Contact SCD Metz : daniel.michel@scd.univ-metz.fr

CPI articles L 122. 4

CPI articles L 335.2- L 335.10

http://www.cfcopies.com/V2/leg/leg_droi.php

<http://www.culture.gouv.fr/culture/infos-pratiques/droits/protection.htm>

Ecrire au docteur : prénom.nom@.....fr

**EXCLU DU
PRÊT**

PPN 095545749

UNIVERSITE Paul Verlaine - METZ S.C.D.	
N° Inv.	2005 007 S
Cote	S/MR 05/03
Loc.	mag 1 ^{er} étage

THÈSE

présentée à

L'Université Paul Verlaine METZ

Faculté des Sciences

UFR Mathématiques, Informatique, Mécanique

pour obtenir le titre de

DOCTEUR



Spécialité

SCIENCES DE L'INGÉNIER
(mention : AUTOMATIQUE)

par

Zied ACHOUR

Titre de la thèse :

**Contribution à la synthèse des contrôleurs des systèmes à
événements discrets partiellement observables**

Soutenue le 20 octobre 2005 devant le jury composé de :

Rapporteurs : Etienne CRAYE Professeur à l'Ecole Centrale de Lille
Robert VALETTE Directeur de Recherche CNRS au LAAS

Examinateurs : Gérard MOREL Professeur à l'Université Henri Poincaré de Nancy
Janan ZAYTOON Professeur à l'Université de Reims

Directeur de thèse : Nidhal REZG Professeur à l'Université Paul Verlaine de Metz

Co-directeur de thèse : Xiaolan XIE Professeur à l'Ecole Nationale Supérieur des Mines de Saint-Etienne

A la mémoire de mon père
A ma mère
A mon frère et mes sœurs
A ma femme

Remerciements

Mes travaux de thèse ont été réalisés au sein de l'équipe AGIP du laboratoire LGIPM à Metz dont je tiens à remercier le directeur M. Gabriel ABBA, Professeur à École nationale d'ingénieurs de Metz.

Je tiens à exprimer mes remerciements les plus sincères à M. Nidhal REZG, Professeur à l'Université Paul Verlaine de Metz, qui m'a suivi et guidé tout au long de ce travail. Je tiens à lui exprimer ma gratitude et mes remerciements les plus sincères pour ses conseils et le temps qu'il a consacré à diriger cette thèse.

J'exprime aussi toute ma reconnaissance à mon co-directeur de thèse M. Xiaolan XIE actuellement Professeur à l'Ecole Nationale Supérieur des Mines de Saint-Etienne, pour la confiance qu'il m'a témoignée et pour son soutien tout le long de ces trois années de thèse.

Ma gratitude et mes remerciements vont ensuite aux membres du jury :

A M. Gérard MOREL, Professeur à l'Université Henri Poincaré de Nancy, d'avoir bien voulu examiner ce travail et pour l'honneur qu'il m'a fait de présider de ce jury.

A M. Etienne CRAYE, Professeur à l'Ecole Centrale de Lille et M. Robert VALETTE, Directeur de Recherche CNRS au LAAS, pour avoir accepté d'être rapporteurs de ce travail et pour leurs commentaires constructifs et leurs remarques pertinentes.

A M. Janan ZAYTOON, Professeur à l'Université de Reims, pour avoir accepté d'examiner ce travail, pour l'intérêt qu'il a porté au sujet.

Je remercie vivement tous les membres du laboratoire LGIPM et en particulier Sofiene, Codrut, Iyad, Smail et Mohammed, pour les encouragements et le soutien reçu durant ces trois années de thèse.

Je ne saurais assez remercier mes amis de toujours Slim, Karim, Chokri et Souhail.

Mes remerciements et ma gratitude vont à ma chère mère, mes deux sœurs et mon frère qui ont toujours eu confiance en moi, pour m'avoir encouragé et soutenu durant tous les moments difficiles.

Enfin, un remerciement très particulier à celle qui a tout quitté pour me rejoindre en France et qui m'a donné le courage pour surmonter les moments difficiles durant cette thèse, pour son amour, son soutien et sa confiance.

Table des matières

Introduction	1
1 Théorie de la commande par supervision : Principe et état de l'art.....	5
1.1 Les systèmes à événements discrets	6
1.2 Outils de modélisation.....	7
1.2.1 Langages formels et automates	7
1.2.1.1 Langages formels.....	7
1.2.1.2 Automates finis.....	8
1.2.2 Problème de synthèse des contrôleurs à base des langages formels	11
1.2.2.1 Problème de supervision.....	12
1.2.2.2 Observabilité, Contrôlabilité et existence de superviseurs.....	13
1.2.2.3 La synthèse du superviseur.....	15
1.2.3 Réseaux de Petri	15
1.2.3.1 Notions de base.....	15
1.2.3.2 Principe de fonctionnement et propriétés d'un RdP	17
1.2.4 Réseaux de Petri pour la supervision.....	19
1.2.4.1 Problème d'états interdits (PEI)	19
1.2.4.2 Problème de transitions d'états interdites (PTEI).....	20
1.2.4.3 Contrôllabilité et existence de contrôleurs	20
1.2.4.4 Approches de contrôle des SED totalement observables	22
1.2.4.5 Approches de contrôle des SED partiellement observables	26
1.2.5 Autre travaux sur l'observabilité	31
1.3 Conclusion.....	32
2 Commande optimale des graphes d'événements partiellement observables ..	33
2.1 Introduction	34
2.2 Commande par supervision des graphes d'événements partiellement observables	34
2.3 Observabilité.....	37

2.4	Politique de commande dans le cas général.....	40
2.5	Solutions analytiques pour des cas spécifiques	42
2.5.1	Propriétés structurelles des graphes d'événements.....	42
2.5.2	Contraintes CGEM avec une seule place critique.....	44
2.5.3	Contraintes CGEM avec plusieurs places critiques	46
2.5.3.1	Cas de places critiques indépendantes	46
2.5.3.2	Cas de places critiques dépendantes	46
2.6	Commande d'une cellule automatisée d'assemblage des tiges de piston ...	48
2.7	Conclusion	50
3	Commande optimale des réseaux de Petri partiellement observables.....	49
3.1	Introduction.....	52
3.2	Définitions et notations utilisées	52
3.3	Comportement admissible contrôlable	53
3.3.1	Observabilité du procédé	53
3.3.2	Le graphe d'atteignabilité observateur.....	53
3.3.3	Le graphe d'atteignabilité observateur raffiné	56
3.3.4	Le graphe d'atteignabilité observateur contrôlable.....	56
3.4	Synthèse de la commande	58
3.4.1	Préliminaires et relations.....	58
3.4.2	Place de contrôle pure	59
3.4.3	Place de contrôle impure.....	61
3.5	Exemple d'un système de production	63
3.6	Conclusion	66
4	Caractérisation de l'existence des contrôleurs réseaux de Petri	69
4.1	Introduction.....	70
4.2	Existence de contrôleurs RDP	70
4.2.1	Marquages de base	70
4.2.2	Condition pour l'existence du contrôleur RdP	71
4.2.3	Observabilité et existence du contrôleur RdP optimal.....	72
4.2.3.1	Cas des macro-états correspondant au même vecteur de tirs observable mais ayant un contrôle différent	72
4.2.3.2	Cas des équations de cycle n'admettant que zéro comme solution....	74

4.3	Synthèse de contrôleurs RdP partiels	78
4.3.1	Contrôleur partiel.....	78
4.3.2	Réseau contrôlé	80
4.3.3	Synthèse de contrôleurs RdP partiels	80
4.4	Conclusion.....	83
5	Commande optimale en Grafcet	85
5.1	Introduction	86
5.2	Synthèse de superviseur Grafcet	87
5.3	Méthodologie de synthèse de la commande par supervision	88
5.4	Synthèse de la commande avec la théorie des régions	92
5.4.1	Nouvelle interprétation de la théorie des régions	92
5.4.1.1	La condition d'atteignabilité	92
5.4.1.2	L'équation de cycle	93
5.4.1.3	La condition de séparation.....	94
5.4.2	Algorithme de synthèse	95
5.5	Application	96
5.6	Autres exemples traités.....	99
5.7	Conclusion.....	100
Conclusion	101	
Bibliographie.....	103	

Introduction

Les systèmes à événements discrets (SED) sont une abstraction utile pour décrire et modéliser de nombreux systèmes conçus par l'Homme tels que les systèmes informatiques, les réseaux de télécommunications, les réseaux de transport ou les systèmes de production (lignes d'assemblage, ateliers flexibles...). Ces systèmes obéissent à des règles opérationnelles, ou algorithmes, et dont les transformations ont lieu en réponse à l'occurrence d'événements asynchrones discrets dans le temps (arrivée d'un client, arrivée d'un ordre d'exécution ou achèvement d'une tâche).

Afin d'améliorer la qualité et de maîtriser la complexité sans cesse croissante de la conception et du développement de ces systèmes, il est indispensable d'élaborer des approches et des outils qui permettent d'abord d'expliciter précisément le comportement des systèmes, et ensuite de l'analyser. Ces approches doivent avoir une représentation formelle permettant l'analyse, la vérification et la validation.

Parmi l'ensemble des modèles existants tels que les réseaux de files d'attente, les automates temporisés, l'algèbre max-plus, les chaînes de markov, etc, les réseaux de Petri (RdP), qui sont l'outil choisi dans le travail présenté dans ce mémoire, possèdent un intérêt fondamental indéniable puisqu'ils permettent de modéliser et de maîtriser les comportements des systèmes parallèles et distribués, synchronisés et communicants. Par leur relation avec les machines à états, les réseaux de Petri constituent des représentations faciles à comprendre et donc à manipuler, à la fois pour la création des modèles et pour leur analyse. Ils peuvent être utilisés pour la vérification des propriétés telles que la vivacité et la bornitude.

Les réseaux de Petri contribuent aussi à la synthèse de la commande des systèmes. La synthèse de la commande des SED a pour objectif de contraindre le système à respecter un ensemble de comportements définis par un cahier des charges. Compte tenu de la complexité des systèmes considérés, il est indispensable de se munir d'outils et de méthodes formelles pour construire les contrôleurs. Le contrôleur, appelé aussi superviseur, qui est lui-même un SED sera par la suite couplé au système non contrôlé pour la synthèse de la commande permettant ainsi de restreindre son fonctionnement au comportement désiré par rapport à un objectif donné. Le problème de contrôle peut être exprimé par une succession de séquences d'événements ou un ensemble d'états

interdits. C'est dans ce contexte que la théorie de la supervision des systèmes à événements discrets a été introduite par les travaux de Ramadge et Wonham [RW89], elle repose sur la théorie des langages formels et les automates.

Dans la théorie de la supervision, le système complet est constitué de deux entités. La première est le procédé, c'est la partie qui doit être supervisée. Elle est considérée comme un SED qui génère spontanément des événements. La seconde est aussi un SED et représente le superviseur. Quand le comportement du procédé non supervisé (fonctionnement en boucle ouverte) est jugé non satisfaisant par rapport à ce qui est souhaité, le but de la théorie de la supervision est de modifier dans une certaine limite, le langage généré par le procédé par l'ajout d'un superviseur. Le comportement souhaité est obtenu en imposant que le langage généré par le procédé couplé au superviseur appartienne à un certain langage de spécification. Ainsi le superviseur va restreindre le comportement du procédé en observant les séquences d'événements.

Ramadge et Wonham et après eux de nombreux auteurs, ont étendu à la théorie des Automates et des Langages Formels la problématique de la commande, qui agit dans ce cas sur l'inhibition de certaines transitions d'état pour éviter les comportements non désirés en faisant en sorte que l'automate ne produise qu'un sous-langage admissible du langage qu'il peut produire en boucle ouverte. Toutefois, cet ensemble de comportements admissibles ne peut être quelconque, car l'occurrence de certains événements ne peut être empêchée par le superviseur. De tels événements sont alors dits incontrôlables. On parle alors de comportement maximum permis.

Mise à part l'existence d'événements incontrôlables, la limitation des capteurs, et/ou la commande distribuée des systèmes peut être une cause d'inobservabilité de certains événements. Le superviseur ne peut pas détecter l'occurrence d'un événement inobservable et donc l'évolution du procédé d'un état à un autre. Pour les SED partiellement observables, le superviseur ne peut pas distinguer entre deux séquences contenant des transitions inobservables et ayant les mêmes transitions observables. Par conséquent, la synthèse des contrôleurs devient une opération délicate.

Ainsi, les travaux de recherche, menés dans le cadre de cette thèse, traitent de la synthèse de la commande des SED partiellement observables et utilisant les réseaux de Petri comme formalisme de modélisation. Une première contribution de cette thèse se situe au niveau de l'extension de la synthèse de la commande basée sur des modèles réseaux de Petri et la théorie des régions en intégrant la contrainte d'observabilité des événements. La deuxième contribution intéressante concerne le développement d'une méthode formelle de synthèse de la commande à partir d'un Grafset de commande du procédé en s'appuyant sur une nouvelle interprétation de la théorie des régions.

Pour les modèles du procédé exprimés en réseaux de Petri, nous proposons deux approches de synthèse de la commande des SED en présence d'événements incontrôlables et/ou inobservables. Ces approches permettent de résoudre le problème des états interdits caractérisé par un ensemble de Contraintes Généralisées d'Exclusion Mutuelles (CGEM) en exploitant les propriétés structurelles des graphes d'événements. Pour le problème des transitions d'états interdites une extension de l'approche de synthèse de la commande développée à Metz par Ghafari et al. [GRX03a] aux SED partiellement observables est proposée.

L'exploitation des propriétés structurelles des graphes d'événements nous a permis de synthétiser une loi de commande pour le problème d'états interdits avec la contrainte

d'observabilité des événements. Pour cette approche, nous nous intéressons aux cas où les CGEM concernent une ou plusieurs places du modèle du procédé. Dans chaque cas, l'expression analytique de la loi de commande est exprimée par le pire cas de la CGEM en termes de marquage atteignable. La loi de commande est alors évaluée en ligne par le superviseur. Ces travaux sont développés dans le chapitre 2 de ce mémoire.

La deuxième approche traite du cas des problèmes des transitions d'états interdites. Elle repose sur la théorie des régions pour des modèles réseaux de Petri généralisés bornés. L'approche de synthèse développée intègre la notion de réversibilité avec les contraintes d'incontrôlabilité et d'inobservabilité des événements. L'approche proposée détermine un contrôleur RdP maximum permisif, quand il existe. Le contrôleur est un ensemble de places de contrôle qui peuvent être pures ou impures. La première étape, basée sur une théorie de Ramadge-Wonham, détermine le graphe de marquage observable. Dans la deuxième étape, nous utilisons la théorie des régions pour déterminer un ensemble de places de contrôle à ajouter au modèle RdP initial. Ces places de contrôle garantissent le comportement désiré. Par ailleurs, des conditions nécessaires pour l'existence du contrôleur RdP pour les SED partiellement observables sont établies. Ces travaux sont présentés dans les chapitres 3 et 4 de ce mémoire.

La deuxième contribution proposée par cette thèse concerne l'utilisation de la théorie des régions pour synthétiser un superviseur à partir des modèles de commande du procédé SED exprimés en GRAFCET. Les spécifications traitées sont du type état interdit et en intégrant l'aspect réversibilité du procédé. Pour ce faire, une nouvelle interprétation de la théorie des régions a été développée et permet de déterminer formellement un ensemble de variables de contrôle à intégrer aux modèles de commande du procédé exprimés en GRAFCET. L'évolution des variables de contrôle obéit à une loi de commande opérée par un Grafset de supervision. Ces travaux sont développés dans le chapitre 5 de ce mémoire.

Chapitre 1

Théorie de la commande par supervision : Principe et état de l'art

Dans ce chapitre, nous présentons les fondements de la théorie de la commande par supervision des Systèmes à Événements Discrets (SED) à travers les résultats de Ramadge et Wonham (R/W). Ces auteurs considèrent que le superviseur assure au SED un fonctionnement admissible issu des spécifications de commande en agissant sur les séquences d'événements générées. Les travaux de R/W se basent principalement sur les langages formels pour modéliser un SED à superviser et le superviseur. Ces premiers travaux ont constitué une base pour la majorité des résultats postérieurs dans ce domaine.

Nous nous intéressons dans ce chapitre aux approches qui utilisent les réseaux de Petri. Les réseaux de Petri ont été beaucoup utilisés pour résoudre des problèmes d'états interdits dans le cas des SED totalement observables. Nous présentons dans ce chapitre deux approches utilisant les réseaux de Petri pour le problème d'états interdits dans le cas des SED totalement observables, il s'agit de l'approche de Giua et al., et l'approche de Ghaffari et al. Dans le cas des SED partiellement observables, nous présentons les principaux résultats issus des travaux de Moody et al. ainsi que Giua et Seatzu. En conclusion, nous situons nos travaux par rapport aux approches existantes dans le cadre des SED partiellement observables.

1.1 Les systèmes à événements discrets

Les systèmes à événements discrets (SED) sont des systèmes dynamiques dont l'espace des états est discret et dont l'évolution est conforme à l'occurrence d'événements physiques à des intervalles de temps généralement irréguliers ou inconnus. Leurs trajectoires d'états sont constantes par morceaux.

Considérons l'exemple d'un système de production. L'évolution du niveau d'un stock est déterminée par l'occurrence des événements *arrivée d'une pièce dans le stock* et *départ d'une pièce du stock*. Ces événements sont étiquetés respectivement par les symboles *a* et *d*. Ce stock peut être modélisé par un SED. Une évolution possible de ce stock est présentée dans la figure 1.1.

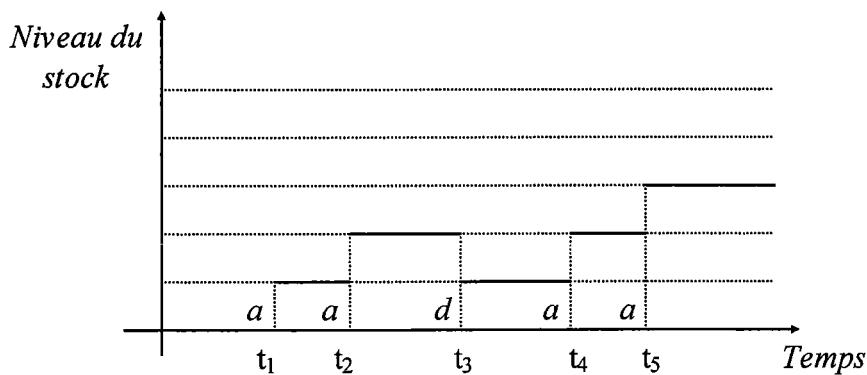


Figure 1.1. Chronogramme de l'évolution d'un stock

Dans l'état initial, le stock est supposé vide. A l'instant t_1 , l'événement *a* se produit et le niveau du stock augmente d'une pièce. L'occurrence de l'événement *d* à l'instant t_3 , fait diminuer le niveau du stock d'une pièce. On retrouve les SED dans plusieurs domaines d'applications tels que la production manufacturière, les réseaux de communication, l'informatique, etc. Différents aspects du comportement d'un système peuvent être considérés selon l'application envisagée. Par conséquent, différents outils de modélisation et d'analyse des SED ont été développés. Il existe trois niveaux d'abstractions pour la modélisation et l'analyse des SED : logiques, temporisés et stochastiques. Le choix du niveau d'abstraction approprié dépend des objectifs de l'analyse.

Dans certaines applications, on s'intéresse au comportement logique du système, pour assurer qu'un *ordre d'événements* précis se produit afin de satisfaire un ensemble de spécifications. Par exemple : premier arrivé premier servi pour un système de production. On peut aussi s'intéresser à chercher si un état (ou un ensemble d'états) est atteint ou non. Dans ce contexte, l'instant d'occurrence des événements est inutile, et il est suffisant de modéliser le comportement non temporisé du système en utilisant des outils de modélisation comme les automates ou les réseaux de Petri autonomes.

Dans d'autres applications, le temps est essentiel et doit être pris en compte explicitement par le modèle. Ces modèles sont appelés temporisés. Il s'agit des modèles où le temps est déterministe comme les réseaux de Petri temporels et les automates

temporisés, et les modèles stochastiques où le temps est aléatoire comme les chaînes de Markov et les réseaux de files d'attente.

Dans la suite, nous nous intéressons uniquement aux modèles logiques.

1.2 Outils de modélisation

1.2.1 Langages formels et automates

Un des moyens formels pour étudier le comportement logique des SED est basé sur la théorie des langages et des automates. Le point de départ est le fait que chaque SED est associé à un ensemble d'événements Σ fini. Cet ensemble Σ représente l'alphabet du langage. Un événement est représenté par un symbole, et toutes les séquences finies d'événements sont appelées mots (ou chaînes) sur l'alphabet Σ . La longueur d'un mot s est notée $|s|$, représente le nombre de symbole de s (par exemple, $|aabbb| = 4$).

L'ensemble de toutes les chaînes qui peuvent être formées sur les éléments de Σ , y comprise la chaîne vide ϵ , est noté Σ^* . Etant donné l'alphabet $\Sigma = \{a, b\}$, on obtient alors $\Sigma^* = \{\epsilon, a, b, aa, ab, ba, aaa, \dots\}$.

1.2.1.1 Langages formels

Définition 1.1 On appelle langage défini sur un alphabet Σ , tout sous-ensemble de Σ^* .

a. Préfixes d'une chaîne et préfixe-clôture d'un langage

La concaténation uv de deux chaînes u et v est une nouvelle chaîne qui définit la suite des symboles de u immédiatement suivis par les symboles de v . La chaîne u est dite préfixe de uv . La chaîne vide ϵ représente l'élément identité de la concaténation : $u\epsilon = \epsilon u = u$ pour toute chaîne u . La préfixe-clôture d'un langage L est le langage contenant tous les préfixes des chaînes de L . On notera par \bar{L} la préfixe-clôture du langage L .

$$\bar{L} = \{s_1 \in \Sigma^* \mid \exists s_2 \in \Sigma^*, s_1s_2 \in L\}$$

Par exemple, la préfixe-clôture du langage $L = \{aabbb\}$ est définie par $\bar{L} = \{\epsilon, a, aa, aab, aabb\}$. Par définition, nous pouvons remarquer que \bar{L} contient L .

Tout langage égal à sa préfixe-clôture, est qualifié de préfixe-clos, c'est-à-dire, L est préfixe-clos si $L = \bar{L}$. Par exemple, le langage $L = \{aabbb\}$ n'est pas préfixe-clos, mais le langage $\bar{L} = \{\epsilon, a, aa, aab, aabb\}$ est préfixe-clos.

b. Expressions régulières et langages réguliers

Une expression régulière sur un alphabet Σ est une expression dont les opérandes sont des symboles de Σ , et dont les opérateurs sont pris dans l'ensemble $\{+, ., ^*\}$. Par exemple l'expression $a + a.b^*$ est une expression régulière.

Un langage régulier est un langage qui peut être défini par une expression régulière. Par exemple, soit le langage L sur l'alphabet $\Sigma = \{a, b\}$ qui comprend toutes les chaînes telles que a et b apparaissent alternativement et telles que a apparaît en premier. Le langage $L = \{\epsilon, a, ab, aba, abab, ababa, \dots\}$. Ce langage est régulier puisqu'il peut être décrit par l'expression régulière : $(a.b)^* . (\epsilon + a)$.

L'expression régulière $\epsilon + a . (b.a)^* . (\epsilon + b)$ permet aussi de décrire le langage L . Ainsi, en général, plusieurs expressions régulières correspondent à un même langage régulier.

1.2.1.2 Automates finis

Un automate est une machine à états qui permet de décrire le fonctionnement entrées/sorties d'un SED. Le moyen le plus simple de présenter cette notion est de considérer le diagramme états-transitions.

Exemple 1.1. Considérons le diagramme états-transitions de la figure 1.2, où les nœuds représentent les états et les arcs associés à des symboles de l'alphabet représentent les transitions entre les états. L'ensemble des état $Q = \{q_0, q_1, q_2\}$. L'état initial q_0 est représenté par une flèche entrante. Les états finaux (ou marqués) sont représentés par des doubles cercles, ainsi : $Q_m = \{q_0, q_2\}$. L'ensemble des symboles associés aux arcs est l'ensemble des événements (alphabet) $\Sigma = \{a, b, g\}$. Les arcs dans ce diagramme modélisent une représentation graphique de la fonction de transition $f: Q \times \Sigma \rightarrow Q$:

$$\begin{array}{ll} f(q_0, a) = q_0 & f(q_0, g) = q_2 \\ f(q_1, a) = q_0 & f(q_1, b) = q_1 \\ f(q_2, b) = q_2 & f(q_2, a) = f(q_2, g) = q_1 \end{array}$$

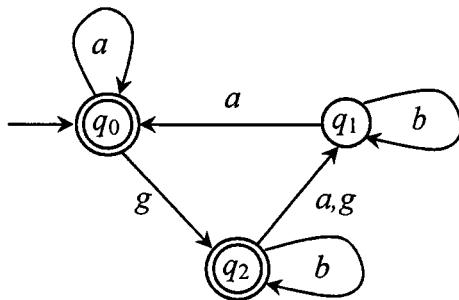


Figure 1.2. Diagramme états-transitions de l'exemple 1.1

La notation $f(q_0, g) = q_2$ signifie que l'occurrence de l'événement g à partir de l'état q_0 mène à l'état q_2 .

Remarques 1.1 :

Trois remarques peuvent être tirées à partir de l'exemple 1.1. :

- L'occurrence d'un événement ne change pas forcément d'état ; $f(q_0, a) = q_0$.

- A partir d'un état, on peut avoir deux événements différents dont l'occurrence mène à un même état ; $f(q_2, a) = f(q_2, g) = q_1$.
- La fonction f est une fonction partielle dans son domaine $Q \times \Sigma$ puisqu'on n'a pas besoin d'avoir une transition pour chaque événement de Σ à partir de chaque état ; les instances $f(q_0, b)$ est $f(q_1, g)$ ne sont pas définies.

Définition 1.2 Un automate fini A est un 5-uplet $A = (Q, \Sigma, f, q_0, Q_m)$ où :

- Q est l'ensemble fini des états.
- Σ est un ensemble fini de symboles d'entrée (ensemble des événements), appelé alphabet d'entrée.
- f est la fonction de transition d'états de $Q \times \Sigma$ vers Q qui associe un état d'arrivée à un état de départ et à un symbole d'entrée.
- $q_0 \in Q$ est l'état initial.
- $Q_m \subseteq Q$ est l'ensemble des états marqués.

L'automate A de la figure 1.2 est dit *déterministe* dans le sens où depuis tout état, il n'existe pas deux transitions de sortie qui soient associées à un même symbole et qui conduisent à deux états différents. En d'autres termes, connaissant l'état courant et le symbole d'entrée de l'automate, on peut déterminer sans équivoque le prochain état de l'automate. Les automates ne respectant pas cette propriété, sont appelés *automates non déterministes*.

Définition 1.3 Un état $q \in Q$ est dit accessible s'il existe une chaîne $s \in \Sigma^*$ telle que $q = f(q_0, s)$. Par extension, un automate A est dit accessible si tous ses états sont accessibles.

Définition 1.4 Un état $q \in Q$ est dit co-accessible s'il existe une chaîne $s \in \Sigma^*$ telle que $f(q_0, s) \in Q_m$. Par extension, un automate A est dit co-accessible si tous ses états sont co-accessibles.

On distingue deux classes importantes de langage selon que l'on implique les états marqués ou non.

a. Langage représenté par un automate fini

La relation entre les langages et les automates est facilement établie en analysant le diagramme états-transitions d'un automate. En partant de l'état initial et en considérant tous les chemins orientés du diagramme états-transitions, on obtient le *langage généré* de l'automate fini. Si l'on considère parmi tous ces chemins uniquement ceux finissant par des états marqués, on obtient le *langage marqué* de l'automate fini.

Définition 1.5 Le langage généré par $A = (Q, \Sigma, f, q_0, Q_m)$ est

$$L(A) = \{s \in \Sigma^* \mid f(q_0, s) \text{ est défini}\}$$

Le langage marqué par A est

$$L_m(A) = \{s \in \Sigma^* \mid f(q_0, s) \in Q_m\}$$

Le langage généré par un automate est toujours préfixe-clos $\bar{L}(A) = L(A)$.

Le langage $L_m(A) \subseteq L(A)$ puisque $Q_m \subseteq Q$

b. Equivalence d'automates

Il est clair qu'il existe plusieurs méthodes pour construire un automate qui génère ou marque un langage donné. Deux automates sont dits équivalents s'ils génèrent et marquent les mêmes langages (Figure 1.3).

Définition 1.6 Les deux automates A_1 et A_2 sont dits équivalents si $L(A_1) = L(A_2)$ et $L_m(A_1) = L_m(A_2)$.

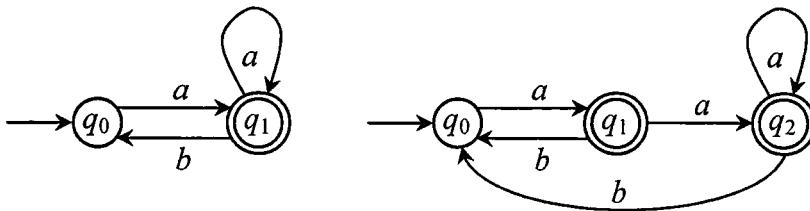


Figure 1.3. Deux automates équivalents

c. Opération sur les automates et les langages

Considérons deux langages L_1 et L_2 .

- *L'intersection* de L_1 et L_2 , noté $L_1 \cap L_2$, définie sur Σ , désigne le langage contenant toutes les chaînes qui appartiennent à la fois à L_1 et à L_2 . Formellement :

$$L_1 \cap L_2 = \{s \mid s \in L_1 \wedge s \in L_2\}$$

- *L'union* de L_1 et L_2 , noté $L_1 \cup L_2$, définie sur Σ , désigne le langage contenant toutes les chaînes qui sont soit contenues dans L_1 , soit contenues dans L_2 . Formellement :

$$L_1 \cup L_2 = \{s \mid s \in L_1 \vee s \in L_2\}$$

- *La concaténation* de L_1 et L_2 définie sur Σ , par :

$$L_1 L_2 = \{s \mid s = uv, u \in L_1 \wedge v \in L_2\}$$

d. Produit et composition d'automates

On définit deux mécanismes d'intégration d'automates : le produit synchrone, noté par \times , et la composition synchrone, noté par \parallel . Pour simplifier, nous présentons ces deux mécanismes pour l'intégration de deux automates A_1 et A_2 uniquement. $A_1 \times A_2$ et $A_1 \parallel A_2$ sont considérés comme deux systèmes résultants d'une interconnexion entre les composants des systèmes A_1 et A_2 comme cela est montré à la figure 1.4.

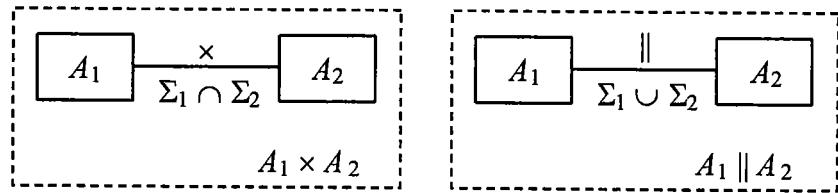


Figure 1.4. Interconnexion des automates A_1 et A_2

- Le *Produit synchrone* $A_1 \times A_2$ des deux automates $A_1 = (Q_1, \Sigma, f_1, q_{01}, Q_{m1})$ et $A_2 = (Q_2, \Sigma, f_2, q_{02}, Q_{m2})$ définis sur Σ est un automate dont l'espace d'état est $Q_1 \times Q_2$ et un événement est admis si il est admis dans A_1 et A_2 .

$$A_1 \times A_2 = (Q_1 \times Q_2, \Sigma, f, (q_{01}, q_{02}), Q_{m1} \times Q_{m2}) \text{ où}$$

$$f(q_1, q_2, e) = (f_1(q_1, e), f_2(q_2, e)) \text{ si } f_1(q_1, e)! \text{ et } f_2(q_2, e)!$$

$$f(q_1, q_2, e) = \text{non définie sinon}$$

- La *composition synchrone* $A_1 \parallel A_2$ des deux automates $A_1 = (Q_1, \Sigma, f_1, q_{01}, Q_{m1})$ et $A_2 = (Q_2, \Sigma, f_2, q_{02}, Q_{m2})$ est un automate dont l'espace d'état est $Q_1 \times Q_2$.

$$A_1 \parallel A_2 = (Q_1 \times Q_2, \Sigma \cup \Sigma_2, f, (q_{01}, q_{02}), Q_{m1} \times Q_{m2}) \text{ où}$$

$$f(q_1, q_2, e) = (f_1(q_1, e), f_2(q_2, e)) \text{ si } f_1(q_1, e)! \text{ et } f_2(q_2, e)!$$

$$f(q_1, q_2, e) = (f_1(q_1, e), q_2) \text{ si } f_1(q_1, e)! \text{ et } e \notin \Sigma_2$$

$$f(q_1, q_2, e) = (q_1, f_2(q_2, e)) \text{ si } e \notin \Sigma_1 \text{ et } f_2(q_2, e)!$$

$$f(q_1, q_2, e) = \text{non définie sinon}$$

La notation $f(q, e)!$ signifie que l'événement e est tirable à partir de l'état q .

1.2.2 Problème de synthèse des contrôleurs à base des langages formels

Le besoin de méthodes formelles et d'outils performants capables de traiter des problèmes de supervision a donné naissance à la théorie de la commande par supervision des SED au début des années 80 par P.J. Ramadge et W.M. Wonham [RW 89]. Des modèles logiques sont utilisés pour décrire le fonctionnement du procédé qui est considéré comme un SED évoluant de manière spontané en générant des événements. Dans la théorie de Ramadge et Wonham, le procédé est considéré comme évoluant en boucle fermée avec le superviseur (figure 1.5). Celui-ci a la tâche d'orienter l'évolution du système dans l'objectif de restreindre son fonctionnement au comportement désiré.

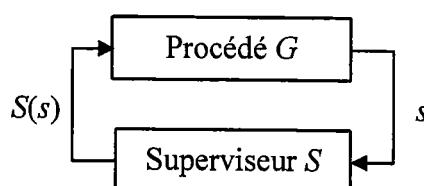


Figure 1.5. Schéma de supervision

Les entrées du superviseur sont les sorties du procédé, et vis versa. Le superviseur peut modifier le fonctionnement du procédé en autorisant ou en interdisant l'occurrence d'événements dits contrôlables Σ_c . Par contre, il ne peut en aucun cas inhiber l'occurrence d'événements dits incontrôlables Σ_{uc} . Ce type de contrôle est appelé contrôle par retour d'événement.

1.2.2.1 Problème de supervision

Considérons un SED modélisé par les deux langages L et L_m définis sur l'ensemble des événements Σ . L est l'ensemble des chaînes que le SED peut générer et $L_m \subseteq L$ est le langage marqué utilisé pour représenter les fins des opérations ou des tâches. L est toujours préfixe-clos, c'est-à-dire $L = \overline{L}$. Considérons l'automate $G = (Q, \Sigma, f, q_0, Q_m)$ tel que $L(G) = L$ et $L_m(G) = L_m$. L'objectif de la commande par supervision est de concevoir un superviseur S afin de le coupler en boucle fermée avec le procédé G pour assurer le comportement désiré. L'ensemble des événements Σ est subdivisé en deux sous-ensembles disjoints $\Sigma = \Sigma_c \cup \Sigma_{uc}$.

La fonction de transition de G peut être commandée par S dans le sens où les événements contrôlables de G peuvent être autorisés ou inhibés par S . Formellement, un superviseur S est une fonction $S : L(G) \rightarrow 2^\Sigma$.

Pour toute séquence $s \in L(G)$, $S(s) \cap \Gamma(f(q_0, s))$ est l'ensemble des événements autorisés par le superviseur S et que G peut exécuter à partir de son état courrant $f(q_0, s)$. En d'autres termes, G ne peut pas exécuter un événement appartenant à l'ensemble des événements possibles $\Gamma(f(q_0, s))$ à partir de son état courrant $f(q_0, s)$ si cet événement n'est pas aussi contenu dans $S(s)$.

Le système évoluant en boucle fermée constitué d'un procédé G et de son superviseur S est noté S/G . Le système contrôlé S/G est un SED dont on peut déterminer son langage généré ainsi que son langage marqué. Ces deux langages sont des sous ensemble de $L(G)$ et $L_m(G)$ contenant les séquences possible en présence de S . Formellement, ceci est défini comme suit.

Définition 1.7 *Langage généré et langage marqué par S/G .*

Le langage généré par S/G est défini comme suit :

- $\epsilon \in L(S/G)$ et
- $[(s \in L(S/G)) \text{ et } (s\sigma \in L(G)) \text{ et } (\sigma \in S(s))] \Leftrightarrow [s\sigma \in L(S/G)]$.

Le langage marqué par S/G est défini comme suit :

$$L_m(S/G) := L(S/G) \cap L_m(G)$$

Dans les modèles où les états marqués correspondent à des fins de tâches, ce langage revêt de l'importance dans la mesure où il caractérise les séquences intéressantes qui permettent d'accomplir des tâches tout en respectant les contraintes de supervision. On dira que le superviseur est non-bloquant pour G si toute séquence du système contrôlé peut toujours être complétée pour atteindre un état marqué, c'est-à-dire :

$$L_m(S/G) \subseteq \overline{L_m(S/G)} \subseteq L(S/G) \subseteq L(G)$$

Définition 1.8 Le SED S/G est non bloquant si

$$L(S/G) = \overline{L_m(S/G)}$$

1.2.2.2 Observabilité, Contrôlabilité et existence de superviseurs

Nous considérons dans cette section le cas où le superviseur ne peut pas voir ou observer tous les événements produits par le procédé G . Dans ce cas, l'ensemble des événements Σ est divisé en deux sous-ensembles disjoints

$$\Sigma = \Sigma_o \cup \Sigma_{uo}$$

où

- Σ_o est l'ensemble des événements observables,
- Σ_{uo} est l'ensemble des événements inobservables.

L'inobservabilité des événements est due à la limitation des capteurs dans un système, et/ou la commande distribuée de certains systèmes. La commande en boucle fermée des SED partiellement observable est représentée à la figure 1.6 et intercale la projection observable P entre le procédé G et le superviseur que nous noterons S_p .

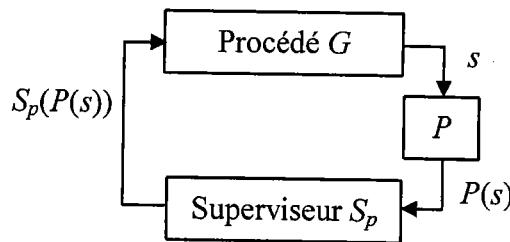


Figure 1.6. Structure de la commande par supervision des SED partiellement observable

La projection observable $P : \Sigma^* \rightarrow \Sigma_o^*$ est définie comme suit :

$$P(\varepsilon) = \varepsilon$$

$$P(e) = \begin{cases} e & \text{si } e \in \Sigma_o \\ \varepsilon & \text{si } e \notin \Sigma_o \end{cases}$$

$$P(se) = P(s) P(e) \quad \text{pour } s \in \Sigma^* \text{ et } e \in \Sigma$$

En présence d'événements inobservables et donc de la projection observable P , le superviseur ne peut pas distinguer entre deux séquences s_1 et s_2 ayant une même projection $P(s_1) = P(s_2)$. Le superviseur appliquera donc un même contrôle $S_p(P(s_1))$. Ceci implique que le contrôle ne peut changer qu'après l'occurrence d'un événement observable, c'est-à-dire quand $P(s_1)$ change.

La controllabilité des langages est une propriété importante dans le problème de synthèse des superviseurs. Elle a été introduite par Ramadge et Wonham pour caractériser l'existence de superviseur pour un problème donné [RW89].

Définition 1.9 Soit un langage $K \subseteq \Sigma^*$. K est contrôlable par rapport à $L(G)$ si

$$\bar{K}\Sigma_{uc} \cap L(G) \subseteq \bar{K}.$$

Autrement dit, si K est contrôlable, alors toute séquence possible dans le système composée d'un préfixe quelconque d'une séquence de K suivi d'un événement incontrôlable est aussi un préfixe d'une séquence de K .

La contrôlabilité et le non blocage des systèmes partiellement observables nécessitent des conditions supplémentaires. Intuitivement, l'observabilité implique :

S'il est impossible de différentier entre deux séquences, alors il est judicieux d'appliquer un même contrôle.

Définition 1.10 Soient K et $M = \bar{M}$ deux langages définis sur Σ . Soient Σ_c l'ensemble des événements contrôlable et Σ_o l'ensemble des événements observables avec P la projection observable $\Sigma^* \rightarrow \Sigma_o^*$. K est dit observable par rapport à M , P et Σ_c si pour toute séquence $s \in \bar{K}$ et pour tout événement $\sigma \in \Sigma_c$,

$$(s\sigma \notin \bar{K}) \text{ et } (s\sigma \in M) \Rightarrow P^{-1}[P(s)] \cap \bar{K} = \emptyset$$

Exemple 1.2. Soient $\Sigma = \{u, b\}$ et le langage $M = \{\overline{ub}, \overline{bu}\}$. Soient $\Sigma_{uo} = \{u\}$ et $\Sigma_{uc} = \{b\}$. Vérifions si le langage $K_1 = \{bu\}$ est observable par rapport à M , Σ_o et Σ_c .

Selon la définition 1.10 de l'observabilité, on doit commencer par examiner $s = \varepsilon \in \bar{K}_1$. Cet événement peut être étendu en dehors de \bar{K}_1 par l'événement contrôlable $\sigma = u$, et $u \in M$. D'un autre côté, il n'existe pas une autre séquence dans \bar{K}_1 commençant par une séquence ayant la même projection observable que ε et finissant par u . Ceci implique que pour ces s et σ , $P^{-1}[P(s)] \cap \bar{K}_1 = \emptyset$. Ensuite, on doit examiner $s = b$. Comme il n'existe pas d'événement contrôlable qui étend s dans M mais pas dans \bar{K}_1 , la condition d'observabilité est aussi vérifiée. De même, si on considère $s = bu$. On peut donc conclure que K_1 est observable.

Considérons maintenant le langage $K_2 = \{bu\}$ et $\Sigma_c = \{b\}$. Dans ce cas, si $s = \varepsilon$ et $\sigma = b \in \Sigma_c$, on a $s\sigma = b \in M \setminus \bar{K}_2$. Mais $s' = u \in P^{-1}[P(s)]$ puisque $u \in \Sigma_{uo}$, et $s'\sigma = ub \in \bar{K}_2$, ce qui est contradictoire avec la condition d'observabilité. En conclusion, avec ce choix de Σ_c , K_2 n'est pas observable. On note que si l'événement b est incontrôlable, alors K_2 sera observable mais pas contrôlable.

Théorème 1.1 : Soit un SED G , où $\Sigma_{uc} \subseteq \Sigma$ est l'ensemble des événements incontrôlables et $\Sigma_o \subseteq \Sigma$ est l'ensemble des événements observables. Soit P la projection observable de Σ^* vers Σ_o^* . Soit un langage $K \subseteq L_m(G)$, où $K \neq \emptyset$. Il existe un superviseur non-bloquant S_p pour G tel que :

$$L_m(S_p/G) = K \quad \text{et} \quad L(S_p/G) = \bar{K}$$

si et seulement si les trois conditions suivantes sont vérifiées :

1. K est contrôlable par rapport à $L(G)$ et Σ_{uc} .
2. K est observable par rapport à $L(G)$, P et Σ_c .
3. K est $L_m(G)$ -clos ($\bar{K} \cap L_m(G) = K$).

1.2.2.3 La synthèse du superviseur

Si le langage des spécifications L_{spec} d'un procédé est contrôlable, alors il est réalisable tout en respectant l'incontrôllabilité des événements de Σ_{uc} . Dans le cas contraire, une façon naturelle de faire respecter les spécifications serait de restreindre encore le comportement contrôlé à un sous-langage K de L_{spec} qui soit contrôlable. Cependant, dans le souci d'autoriser au procédé le maximum d'états possibles, il est intéressant de choisir K comme le plus grand sous-langage contrôlable de L_{spec} .

Soit $C(L)$ l'ensemble des sous-langages contrôlables d'un langage L . $C(L)$ est nécessairement non vide car le langage vide est contrôlable. D'autre part, $C(L)$ est clos par union, c'est à dire, l'union de deux éléments de $C(L)$ est un élément de $C(K)$. Donc, $C(K)$ admet un plus grand élément $SupC(L)$ et il est unique [RW87]. Donc, si L_{spec} n'est pas contrôlable, le langage $K = SupC(L_{spec})$ est la meilleure approximation qui permet de respecter les spécifications tout en restreignant le procédé le minimum possible. Le superviseur qui permet de réaliser un tel langage est dit optimal ou maximum permissif.

Cependant, dans le cas général, il n'existe pas d'algorithme efficace pour le calcul du plus grand sous-langage contrôlable d'un langage de spécification. Des difficultés peuvent apparaître aussi au niveau de la décidabilité de la propriété de contrôllabilité.

Dans le cas particulier où les langages du procédé et de spécification sont réguliers, et par conséquent admettent des représentations sous forme d'automates à états finis, toutes les propriétés requises pour l'existence du superviseur sont décidables par une simple exploration des espaces d'états des automates. De plus, il a été prouvé que le plus grand langage contrôlable est régulier [WR87]. Un algorithme pour le calcul de ce langage a été développé par Ramadge et Wonham. Cet algorithme est polynomial en la taille des automates du procédé et de spécification [GW00].

1.2.3 Réseaux de Petri

L'explosion combinatoire du nombre d'états rend difficile la mise en œuvre de la modélisation des SED de certaines tailles. Les réseaux de Petri (RdP) ont, par rapport aux automates, l'avantage d'être un modèle dont la représentation est compacte et beaucoup plus riche, s'adaptant parfaitement à la description de certains types de SED. Ces modèles ont été introduits et développés par C.A. Petri en 1960. Il y a une grande similitude entre les automates et les réseaux de Petri puisque ces derniers représentent également explicitement les fonctions de transition des SED. Les réseaux de Petri peuvent représenter une large classe de langages dont la classe des langages réguliers. Le fait que de nombreux outils et techniques d'analyse aient été développés pour l'étude des modèles RdP est une motivation supplémentaire pour la considération des ces modèles.

1.2.3.1 Notions de base

Un réseau de Petri comporte deux types de nœuds, les places et les transitions, et des arcs orientés qui les relient. La manière dont ces places et ces transitions sont reliées, définit le comportement d'un RdP. Une place est représentée par un cercle et une transition par un trait ou un rectangle. Le nombre de places et de transitions est fini et non nul.

Définition 1.11 Un Réseaux de Petri est un quadruplet $N = (P, T, A, w)$ où

P est l'ensemble fini de places ;

T est l'ensemble fini de transitions ;

$A \subseteq (P \times T) \cup (T \times P)$ est l'ensemble des arcs, des places vers les transitions et des transitions vers les places ;

$w : A \rightarrow \{1, 2, 3, \dots\}$ est la fonction poids sur les arcs.

(P, T, A, w) n'admet pas de places ou de transitions isolées.

Dans ce mémoire, nous faisons l'hypothèse que l'ensemble des transitions $T = T^c \cup T^u$ est formé de deux sous-ensembles ; T^c l'ensemble des *transitions contrôlables* et T^u l'ensemble des *transitions incontrôlables*. L'ensemble $T^u = T^f \cup T^{uo}$ et aussi constitué de *transitions libres* (T^f) et de *transitions inobservables* (T^{uo}). Les transitions contrôlables sont représentées par des rectangles, les transitions inobservables par des rectangles hachurés et les transitions libres par des barres.

Un arc est de la forme (p_i, t_j) ou (t_j, p_i) , et le poids relatif à un arc est un entier positif. Si les poids des arcs sont tous égaux à 1, alors le réseau de Petri est dit ordinaire. Si l'arc $(p, t) \in A$, alors on dit que p (respectivement t) est une place d'entrée de la transition t (respectivement transition de sortie de la place p). Si une place p est à la fois place d'entrée et de sortie d'une même transition t , alors elle est dite impure, sinon elle est pure. Un RdP pur est un RdP qui ne contient aucune place impure, sinon il est impur. Dans la suite, nous utiliserons les notations suivantes :

- $p\bullet$ (respectivement $\bullet p$) désigne l'ensemble des transitions de sortie (respectivement d'entrée) de la place p .
- $t\bullet$ (respectivement $\bullet t$) désigne l'ensemble des places de sortie (respectivement d'entrée) de la transition t .

La distribution des jetons dans les places détermine le marquage du réseau. Ce marquage M associe un nombre entier $M(p_i)$ (positif ou nul) à chaque place p_i du réseau. Ce marquage est modélisé par une fonction $M_i : P \rightarrow \mathbb{N}$, où $M_i(p)$ représente le nombre de jetons contenus dans la place p au $i^{\text{ème}}$ marquage et \mathbb{N} l'ensemble des entiers. Un marquage M est dit binaire si toutes les places du réseau contiennent au plus un jeton.

Le marquage M d'un RdP est défini par le vecteur des marquages de ses places : $M = (M(p_1), M(p_2), \dots, M(p_n))^t$. L'ensemble des marquages qu'il est possible d'atteindre à partir de M_0 par un ou plusieurs franchissements est noté \mathcal{M} .

Exemple 1.3. Considérons le réseau de Petri de la figure 1.7 dont l'ensemble des places $P = \{p_1, p_2, p_3, p_4, p_5\}$, l'ensemble des transitions $T = \{t_1, t_2, t_3, t_4\}$ avec le marquage courant $M = (0, 0, 1, 0, 1)$.

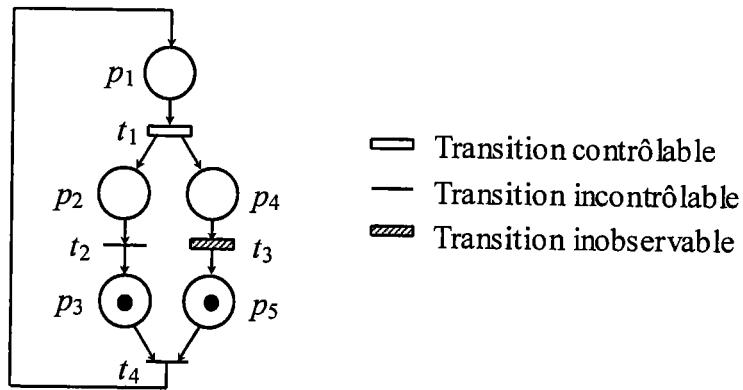


Figure 1.7. Modèle réseau de Petri de l'exemple 1.3

1.2.3.2 Principe de fonctionnement et propriétés d'un RdP

Une transition t est dite validée ou franchissable à partir d'un marquage M , on note $M[t]$, si toute place d'entrée p de t contient un nombre de jetons au moins égal au poids de l'arc qui relie p à t . Une transition validé t peut être franchie. Le marquage du réseau M est alors transformé en un marquage M' de la manière suivante :

$$M'(p) = \begin{cases} M(p) - w(p, t) & \text{si } p \in \bullet t \\ M(p) + w(t, p) & \text{si } p \in t \bullet \\ M(p) - w(p, t) + w(t, p) & \text{si } p \in \bullet t \cap t \bullet \\ M(p) & \text{sinon} \end{cases}$$

Dans le modèle RdP de la figure 1.7, les seules places marquées sont p_3 et p_5 par conséquent, la seule transition validée est la transition t_4 . Le marquage M suite au franchissement de t_4 devient $M' = (1, 0, 0, 0, 0)$.

a. Equation d'état (équation fondamentale)

Définissons d'abord la matrice d'incidence C d'un RdP. C est une matrice $m \times n$ où m , représente le nombre de place et n , le nombre de transition du réseau. Une composante (j, i) de la matrice est de la forme

$$C(p_i, t_j) = w(t_j, p_i) - w(p_i, t_j).$$

Cette matrice peut être aussi définie comme la différence de deux matrices C^+ , la matrice d'incidence avant et C^- la matrice d'incidence arrière, telles que :

$$\begin{aligned} C^+(p_i, t_j) &= w(t_j, p_i) \\ C^-(p_i, t_j) &= w(p_i, t_j). \end{aligned}$$

Définissons maintenant le vecteur d'occurrence $\vec{\sigma}$ de dimension m appelé aussi vecteur de comptage. La $j^{\text{ème}}$ composante de ce vecteur correspond au nombre d'occurrence de la transition t_j dans la séquence σ de transitions franchissables à partir du marquage initial M_0 . L'équation d'état est donnée par :

$$M = M_0 + C \cdot \vec{\sigma}.$$

b. Quelques propriétés

Ci-après sont présentées quelques propriétés des RdP qui seront utiles dans la suite.

RdP borné : Un RdP est k -borné si le nombre de jetons dans chaque place p et à n'importe quel marquage atteignable M ne dépasse pas k . Un RdP est dit borné s'il est k -borné pour un certain entier positif k .

Un RdP est sauf s'il est 1-borné.

RdP vivant : Un RdP est vivant si chacune de ses transitions est vivante, c'est à dire que, quel que soit le marquage M , il existe toujours un marquage atteignable à partir de M qui permet de franchir t .

Si aucune transition n'est franchissable à partir d'un état atteignable M , alors M est un état de blocage. Un RdP vivant est un RdP sans blocage, mais la réciproque n'est pas toujours vraie.

RdP réversible : Un RdP est réversible si, à partir de n'importe quel état atteignable M , il existe une séquence franchissable qui permet de revenir à M_0 .

RdP conservatif : Un RdP est conservatif s'il existe un vecteur de pondération des places X à composantes strictement positives tel que, pour tout marquage initial M_0 et tout marquage M atteignable à partir de M_0 ,

$$X^t \cdot M = X^t \cdot M_0.$$

RdP persistant : Un RdP est persistant pour un marquage M_0 si, pour tout couple de transitions franchissables, le franchissement d'une des deux transitions ne rend pas l'autre infranchissable. Cela signifie qu'en cas de conflit entre deux transitions, le choix qui est fait sur l'ordre des franchissements n'a aucune conséquence sur la possibilité de franchir ces transitions.

c. Les invariants

p-invariants : Un p-invariant d'un RdP est un vecteur X d'entiers non négatifs de dimension $\text{card}(P) = n$ et qui vérifie

$$X^t \cdot C = 0$$

où C est la matrice d'incidence du RdP.

En utilisant l'équation d'état des RdP, une propriété importante des p-invariants découle de leur définition, à savoir qu'un p-invariant X vérifie

$$X^t \cdot M = X^t \cdot M_0$$

et ce pour n'importe quel marquage atteignable M . Ce qui signifie que la somme des marquages des places pondérés par le vecteur X est constante, quelle que soit l'évolution du RdP.

t-invariants : Un t-invariant est un vecteur Y d'entiers positifs de dimension $\text{card}(T) = m$ qui vérifie

$$C \cdot Y^t = 0.$$

Soit σ une séquence franchissable à partir de M_0 telle que $\bar{\sigma}$ est un t-invariant. Alors, en franchissant σ , on revient au marquage initial. Cette propriété découle directement de la définition des t-invariants et de l'équation d'état.

1.2.4 Réseaux de Petri pour la supervision

Nous nous sommes intéressés dans la section 1.2.2, aux problèmes de supervision où les spécifications s'exprimant sous la forme d'un comportement désiré du procédé. Les actions de contrôle émises par le superviseur, à un instant donné, dépendent des séquences d'événements générés jusqu'alors par le procédé. Nous pouvons aussi définir un problème de supervision par un ensemble d'états admissibles pour le procédé, ou encore, par un ensemble d'états interdits. Il est alors possible de concevoir un superviseur qui interdit au système d'atteindre les états interdits en se basant sur la séquence d'événements générés.

La politique la plus communément utilisée pour traiter les problèmes d'états interdits est de type retour d'état. Le superviseur n'est pas censé mémoriser l'historique de l'évolution du système. L'action de contrôle, qui consiste toujours en une liste d'événements autorisés, est déterminée en observant uniquement l'état courant du système contrôlé.

1.2.4.1 Problème d'états interdits (PEI)

Formellement, un contrôle par retour d'état d'un RdP (N, M_0) est une fonction $C : \mathcal{M} \rightarrow \Gamma$ où Γ est l'ensemble des lois de contrôle défini par $\Gamma = \{\gamma \subseteq T \mid \gamma \supseteq T^u\}$. (voir figure 1.8)

Dans un réseau N_C muni du contrôle C , une transition t est autorisée à partir d'un état M ssi :

- $M[t]$,
- $t \in C(M)$.

D'après la définition de l'ensemble des lois de contrôle Γ , les transitions incontrôlables sont toujours autorisées par le contrôleur. On désignera par \mathcal{M}_C l'ensemble des états atteignables dans N_C et R_C le graphe d'atteignabilité correspondant.

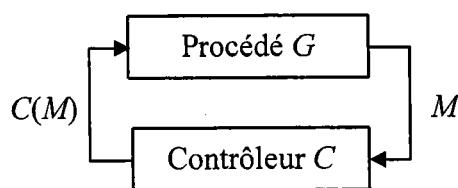


Figure 1.8. Principe du contrôle par retour d'état

L'objectif dans un problème d'états interdits est de synthétiser un contrôleur C qui garantit que les états atteignables du système à contrôler soient dans un ensemble d'états admissibles spécifié, ou encore que le système à contrôler ne visite jamais des états interdits bien déterminés.

Les états admissibles peuvent être les états qui satisfont un prédictat Q défini comme

$$Q : \mathcal{M} \rightarrow \{0, 1\}.$$

Les états admissibles sont alors identifiés aux éléments de l'ensemble

$$\mathcal{M}_Q = \{M \mid M \in \mathcal{M}, Q(M) = 1\}.$$

L'ensemble des états interdits est tout naturellement l'ensemble complémentaire de \mathcal{M}_Q .

On note par $(M \xrightarrow{\sigma} M')$ le chemin qui relie un nœud M à un nœud M' dans un graphe et correspondant à la séquence de franchissement σ .

1.2.4.2 Problème de transitions d'états interdites (PTEI)

Le Problème de transitions d'états interdites est un problème plus général que celui du problème d'états interdits.

Définition 1.12 *Un problème de transitions d'état interdites (ou PTEI) correspond à un comportement admissible R défini par :*

1. $M_0 \in R$;
2. $\forall M \in R, \exists \sigma \mid (M_0 \xrightarrow{\sigma} M) \in R$.

La première condition, qui traduit l'admissibilité du marquage initial, est évidemment nécessaire pour l'existence de contrôle. La deuxième condition impose l'atteignabilité de tout marquage admissible à partir de M_0 par un chemin dans R ou encore que tous les marquages intermédiaires soient admissibles. Notons que pour un problème de transitions d'état interdites, des transitions possibles entre états admissibles n'appartiennent pas nécessairement à R .

Une sous-classe importante de la classe des PTEI est la classe des problèmes d'états interdits PEI. Un comportement admissible par rapport à des spécifications de type états interdits peut être défini comme suit :

Définition 1.13 *Un problème d'états interdits (ou PEI) correspond à un comportement admissible qui satisfait les conditions 1. et 2. de la définition 1.12 et la condition supplémentaire suivante :*

3. $\forall (M \xrightarrow{t} M') \in R(N, M_0), M, M' \in R \Rightarrow (M \xrightarrow{t} M') \in R$.

Un problème d'états interdits est bien un problème de transitions d'états interdites, mais l'inverse est faux.

1.2.4.3 Contrôllabilité et existence de contrôleurs

Pour caractériser l'existence de solution pour un problème d'états interdits, Y. Li et W. M. Wonham ont exprimé la propriété de contrôllabilité dans le contexte du contrôle par retour d'état [LW93]. Leur étude portait sur *les systèmes à événements discrets vectoriels* (SEDV).

Un SEDV est un SED $G = (\Sigma, \mathcal{M}, \delta, X_0)$ dont l'état est décrit par des variables d'état entières x_1, x_2, \dots, x_n [LW93]. L'espace \mathcal{M} des états du système est l'ensemble des vecteurs entiers de dimension n .

La fonction de transition d'un SEDV $\delta: \mathcal{M} \times \Sigma \rightarrow \mathcal{M}$ est telle que:

$$\delta(M, e) = M + E_e$$

où E_e est appelé *le vecteur de déplacement* correspondant à l'événement e . $\delta(M, e)$ est défini si $M \geq F_e$, où $F_e \in \mathcal{M}$ est le vecteur de condition d'occurrence.

Les réseaux de Petri constituent un modèle équivalent aux SEDV [LW93][Pet81]. Les résultats prouvés pour les systèmes SEDV sont donc valables pour les réseaux de Petri.

Soit un réseau de Petri (N, M_0) et un prédictat de spécifications Q . Supposons que l'état initial satisfait Q , c-à-d $M_0 \in \mathcal{M}_Q$. Soit $R_Q(N, M_0)$ l'ensemble des marquages atteignables à partir de M_0 par l'intermédiaire de marquages satisfaisant Q . Il est alors défini comme suit.

Définition 1.14 $R_Q(N, M_0)$ est tel que:

1. $M_0 \in R_Q(N, M_0)$;
2. Si $M \in R_Q(N, M_0)$ et $M[t] M' \in \mathcal{M}_Q$, alors $M' \in R_Q(N, M_0)$;
3. Tout état de $R_Q(N, M_0)$ satisfait les conditions 1 ou 2.

Il découle de la définition 1.14 que pour tout état $M \in R_Q(N, M_0)$, il existe $M_1, M_2, \dots, M_p \in \mathcal{M}$ et $t_0, t_1, \dots, t_{p-1} \in \Sigma$ tels que

- $\forall i = 0, 1, \dots, p - 1, M_i [t_i] M_{i+1}$;
- $\forall i = 0, 1, \dots, p, M_i \in R_Q(N, M_0)$;
- $M_p = M$.

Autrement dit, pour tout état M satisfaisant Q , il existe toujours une séquence franchissable à partir de M_0 qui mène à M et telle que les marquages intermédiaires satisfont également Q .

La définition suivante introduit la notion de contrôlabilité d'une spécification d'états interdits Q [LW93].

Soit un réseau (N, M_0) et une spécification d'état interdits Q définie sur l'ensemble \mathcal{M} . \mathcal{M}_Q est contrôlable par rapport à (N, M_0) si

1. $\mathcal{M}_Q = R_Q(N, M_0)$ et
2. $\forall t \in T^u$, si $M \in \mathcal{M}_Q$ et $M[t] M'$ alors $M' \in \mathcal{M}_Q$.

Il est clair qu'on a toujours $R_Q(N, M_0) \subseteq \mathcal{M}_Q$. La condition 1 de cette définition impose donc que tous les états admissibles par rapport à Q soient atteignables par l'intermédiaire d'états admissibles. La seconde condition traduit naturellement l'admissibilité des états atteints de façon non contrôlable à partir d'états admissibles. La condition de contrôlabilité de l'ensemble des états admissibles est nécessaire et suffisante pour l'existence d'un contrôle par retour d'état comme il est énoncé dans le théorème 1.2 suivant [LW93].

Théorème 1.2 : Soit Q une spécification sur les états d'un RdP (N, M_0) telle que $M_0 \in \mathcal{M}_Q$. Il existe un contrôle par retour d'état C tel que $\mathcal{M}_C = \mathcal{M}_Q$ ssi \mathcal{M}_Q est contrôlable.

Un autre résultat important énoncé par Y. Li et W. M. Wonham concerne l'existence du plus grand sous-ensemble de marquages admissibles contrôlable d'un ensemble \mathcal{M}_Q [LW93].

Théorème 1.3 : Le plus grand élément de l'ensemble $S(\mathcal{M}_Q) = \{K \mid K \subseteq \mathcal{M}_Q \text{ et } K \text{ est contrôlable}\}$ existe toujours.

1.2.4.4 Approches de contrôle des SED totalement observables

Plusieurs approches ont été développées pour le contrôle des SED. Krogh [Kro87] ainsi que Ishikawa et Hiraishi [IH87] proposent une nouvelle approche de supervision basée sur l'utilisation des réseaux de Petri dans un but d'exploiter leur puissance de modélisation ainsi que leurs nombreux résultats mathématiques tels que la bornitude et la vivacité. D'autres approches basées sur les réseaux de Petri ont été proposées dans la littérature [GDS92] [LW94] [GDS93] [HK90] [GRX03a]. Dans la suite, nous présentons l'approche de Giua et celle de Ghaffari.

a. L'approche de Giua et al.

Les auteurs se sont intéressés principalement aux spécifications données par des inégalités linéaires sur les marquages qu'ils ont appelées des *Contraintes Généralisées d'Exclusion Mutuelle* (CGEM). Une contrainte de type CGEM est donnée par un couple (\vec{w}, k) , où \vec{w} est un vecteur d'entiers et k est une constante entière, et elle définit l'ensemble suivant d'états admissibles:

$$\mathcal{M}_{(\vec{w}, k)} = \{M \in \mathcal{M} \mid \vec{w}^T M \leq k\}. \quad [1.1]$$

L'ensemble des états admissibles correspondant à un ensemble de contraintes CGEM (W, \vec{k}) , avec $W = [\vec{w}_1 \dots \vec{w}_r]$ et $\vec{k} = (k_1 \dots k_r)$ est donné par

$$\mathcal{M}_{(W, \vec{k})} = \bigcap_{i=1}^r \mathcal{M}_{(\vec{w}_i, k_i)}.$$

Ce type de contraintes permet de traduire naturellement l'exclusion mutuelle dans l'utilisation de ressources communes partagées entre différents processus. Ce genre de situations est assez répandu dans les systèmes industriels. Dans [GDS92], les auteurs ont prouvé que dans le cas où toutes les transitions d'un réseau sont contrôlables, une contrainte (\vec{w}, k) de type CGEM peut toujours être satisfaite de façon optimale en ajoutant au réseau non contrôlé une place de contrôle ou *moniteur* définie comme suit [GDS92].

Définition 1.15 Soit un réseau de Petri (N, M_0) avec un ensemble de places P et une matrice d'incidence C et une CGEM (\vec{w}, k) . Un moniteur qui permet de respecter cette contrainte est une place S à ajouter à N telle que le réseau résultant (N^s, M_0^s) a comme

ensemble de places $P \cup \{S\}$ et une matrice d'incidence C^s définie par $C^s = \begin{pmatrix} C \\ -\vec{w}^T \cdot C \end{pmatrix}$.

La place S est pure. Elle est donc entièrement définie par C^s . Le marquage initial de (N^s, M_0^s) est donné par $M_0^s = \begin{pmatrix} M_0 \\ k - \vec{w}^T \cdot M_0 \end{pmatrix}$. Le marquage initial M_0 est supposé satisfaire la contrainte (\vec{w}, k) .

Donc, cette place supplémentaire a des arcs sortants vers (respectivement entrants depuis) toutes les transitions d'entrée (respectivement de sortie) de toute place p du réseau appartenant au support de \vec{w} et telle que $\vec{w}[p] > 0$. Ce sens est inversé pour les places avec des poids négatifs. Les poids des arcs dépendent des coefficients de \vec{w} et de la matrice d'incidence C . Un problème de CGEM est donc résolu en ajoutant autant de moniteurs que de contraintes CGEM. Il est toutefois possible d'identifier a priori les contraintes *redondantes* par rapport au réseau (c-à-d. toujours satisfaites) ou *équivalentes* entre elles (c-à-d. délimitant un même ensemble d'états admissibles) [GIU96].

Malheureusement, toute spécification d'états interdits ne peut pas se ramener à un ensemble de CGEM. En effet, l'ensemble d'états admissibles 1.1 correspondant à une contrainte de type CGEM est forcément convexe. Ce qui n'est pas nécessairement le cas pour un problème où les états interdits sont définies par une liste quelconque. Cependant, pour la classe des réseaux saufs et conservatifs, il existe toujours un ensemble de CGEM équivalent à une liste quelconque d'états interdits [GDS92].

Théorème 1.4 : Soit (N, M_0) un réseau sauf et conservatif. Alors, pour tout ensemble \mathcal{M}_F d'états interdits, il existe un ensemble de CGEM (W, \vec{k}) tel que $\mathcal{M} \setminus \mathcal{M}_F = \mathcal{M}_{(\vec{w}, k)}$.

En présence de transitions incontrôlables, les états admissibles constituent un sous-ensemble de l'ensemble défini par l'expression 1.1. En effet, des états qui ne sont pas interdits par les spécifications mais à partir desquels un état interdit peut être atteint par franchissement de transitions incontrôlables doivent être interdits également. Ainsi, l'ensemble des états admissibles correspondant à une contrainte de type CGEM est donné par:

$$\mathcal{M}_{(\vec{w}, k)}^c = \{M \in \mathcal{M} \mid (\forall \sigma \in (T^u)^*, M[\sigma]M') \vec{w}^T M' \leq k\}. \quad [1.2]$$

$\mathcal{M}_{(\vec{w}, k)}^c$ est un ensemble quelconque d'états admissibles. Il est donc possible qu'il n'existe pas un ensemble de contraintes (W, \vec{k}') de type CGEM tel que $\mathcal{M}_{(\vec{w}, k)}^c = \mathcal{M}_{(W, \vec{k}')}$. Par conséquent, il peut ne pas exister une solution avec des moniteurs pour un problème CGEM d'un réseau général avec des transitions incontrôlables. Cependant, grâce au théorème 1.4, un problème de CGEM d'un réseau sauf et conservatif peut toujours être résolu par des moniteurs même en présence de transitions incontrôlables [GDS92].

Les mêmes auteurs ont considéré les problèmes de CGEM, où \vec{w} est un vecteur d'entiers positifs, pour la classe des graphes d'événements [GDS93]. Pour cette classe de réseaux, ils ont défini les *places à contrôle sauf*. Une place p d'un graphe

d'événement est à contrôle sauf si, dans chaque chemin qui relie une transition contrôlable t à p et qui ne contient pas d'autres transitions contrôlables excepté t , le nombre de jetons ne peut pas dépasser 1. Pour cette classe de réseaux et de contraintes, Giua *et al.* ont montré que pour toute contrainte (\vec{w}, k) , il existe un ensemble de CGEM (W_c, \vec{k}_c) tel que $\mathcal{M}_{(W, \vec{k})} = \mathcal{M}_{(\vec{w}, k)}^c$.

Par conséquent, un contrôle maximum permisif qui satisfait (\vec{w}, k) peut être déterminé par un ensemble de moniteurs. Néanmoins, dans certains cas, le nombre de moniteurs peut être exponentiel en nombre de places dans le support de \vec{w} [GDS93]. Les auteurs ont également proposé une autre méthode pour déterminer un contrôleur RdP pour la même classe de réseaux et de contraintes et dont la taille augmente linéairement avec les places dans le support \vec{w} . Cette méthode se base sur la duplication des transitions contrôlables [GDS93].

b. L'approche de Ghaffari *et al.*

Dans cette approche, les auteurs se basent sur une modélisation du procédé par un RdP borné, ordinaire ou généralisé. Les spécifications sont de types PEI ou PTEI. Les auteurs déterminent formellement à l'aide de la théorie des régions un ensemble de places de contrôle à ajouter au modèle RdP du procédé. Cet ensemble de places de contrôle constitue le superviseur qui permet d'assurer le respect des spécifications.

L'approche opère en deux phases. Une première phase, basée sur le graphe de marquage, permet de déterminer l'ensemble des marquages admissibles. Puis, en utilisant la théorie des régions, des places de contrôle sont construites pour assurer le comportement désiré.

Soient (N, M_0) le modèle RdP du procédé contrôlé et R_c le graphe de marquage admissible respectant les spécifications. Pour déterminer l'ensemble des marquages admissibles les auteurs proposent l'algorithme 1.1. suivant :

Algorithme 1.1.

1. Déterminer de l'ensemble des marquages interdits.
2. Générer le graphe d'atteignabilité partiel $R_p(N, M_0)$.
3. Déterminer l'ensemble des marquages dangereux M_D .
4. Éliminer les nœuds appartenant à M_D du graphe $R_p(N, M_0)$.

Soit R le graphe ainsi obtenu.

5. Si R_c est co-atteignable, alors FIN. Sinon aller à 6.
6. Construire le plus grand sous-graphe co-atteignable $CA(R)$.
7. Calculer l'ensemble des marquages dangereux.
8. Éliminer de R_c les nœuds de M_B . Aller à 5.

FIN

Remarque 1.2 :

Un graphe d'atteignabilité partiel est un graphe d'atteignabilité où les successeurs des états interdits ne sont pas générés. On a noté par M_B l'ensemble de marquages bloquants.

La commande par supervision doit restreindre le comportement du système commandé à R_c en inhibant toute transition contrôlable qui mène à un marquage bloquant ou interdit. Le graphe d'atteignabilité obtenu correspond au comportement vivant maximal permisif du système commandé. Réciproquement, les contraintes d'états interdits et de vivacité sont satisfaites par tous les marquages de R_c , et aucun marquage ne mène de façon *incontrôlable* à l'extérieur de R_c . On en conclut que le graphe R_c obtenu constitue le comportement admissible vivant maximal.

Pour le problème de synthèse de la commande, basée sur les RdP, les modèles RdP du système à contrôler et le graphe R_c sont donnés. La théorie des régions est utilisée pour déterminer les places de contrôle à ajouter au modèle RdP initial du procédé à contrôler.

Considérons une place de contrôle p_c . Pour le RdP du système à superviser augmenté de p_c , chaque marquage du graphe R_c doit rester atteignable. Ceci implique que p_c doit vérifier *les conditions d'atteignabilité*:

$$M_c(p_c) = M_0(p_c) + C_c(p_c, \cdot) \vec{\Gamma}_M \geq 0 \quad \forall M \in R_c \quad [1.3]$$

où C_c , M_c et $\vec{\Gamma}_M$ sont respectivement la matrice d'incidence du réseau contrôlé, le marquage du réseau contrôlé et un chemin non-orienté de R reliant M_0 à M .

D'autres part, p_c doit satisfaire les équations de cycle correspondant aux cycles de R_c , donc l'application de la condition [1.3] le long d'un cycle non orienté quelconque δ conduit à la relation suivante:

$$\sum_{t \in T} C_c(p_c, t) \vec{\delta}[t] = 0, \quad \forall \delta \in \Delta. \quad [1.4]$$

où $\vec{\delta}[t]$ désigne la somme algébrique de toutes les occurrences de t ; dans δ et Δ l'ensemble des cycles de base du graphe R_c . $\vec{\delta}$ est le vecteur d'occurrences de δ . L'équation [1.4] est appelée *l'équation de cycle*.

Quand aux événements à séparer, pour obtenir δ à partir du graphe de marquage initial, seules les transitions menant d'un marquage admissible à un marquage non admissible doivent être inhibées. Par conséquent, chaque nouvelle place p_c doit interdire une transition contrôlable t qui mène d'un marquage admissible M à un état interdit M' . Cette interdiction se fait par l'ajout de la condition suivante appelée *condition de séparation* :

$$M'_c(p_c) = M_{c0}(p_c) + C_c(p_c, \cdot) \vec{\Gamma}_M + C_c(p_c, t) < 0. \quad [1.5]$$

Ainsi, pour chaque transition contrôlable qui mène à un état interdit, on résout le

système composé des équations de relations [1.3], [1.4] et [1.5] pour déterminer une nouvelle place de contrôle p_c .

Les auteurs ont aussi montré qu'un comportement souhaité R , sous-graphe du graphe d'atteignabilité d'un RdP borné (N, M_0) , peut être réalisé en ajoutant des places de contrôle pures à (N, M_0) ssi il existe une solution $(M_{c0}(p_c), C_c(p_c, .))$ pour le système linéaire incluant toutes les conditions [1.3], [1.4] et [1.5], pour chaque transition à inhiber.

Comme il n'est pas toujours possible de déterminer un contrôleur RdP avec uniquement des places de contrôle pures, les auteurs ont aussi développé une approche permettant de déterminer un contrôleur RdP avec des places de contrôle impures. Cette approche est aussi basée sur la théorie des régions.

1.2.4.5 Approches de contrôle des SED partiellement observables

a. L'approche de Moody et al.

Dans cette approche, les auteurs cherchent à construire un contrôleur RdP qui puisse répondre, en général de façon sous-optimale, à des spécifications sur les états de type CGEM pour des systèmes modélisés par des RdP avec des transitions incontrôlables et des transitions inobservables [MLA96] [MA99].

Le principe de la synthèse est relativement simple. Il s'agit d'ajouter des moniteurs (tels qu'ils sont définis par la définition 1.15) au modèle non contrôlé pour créer des invariants de place. Rappelons qu'un invariant de place x dans un réseau N est un vecteur d'entiers, solution de l'équation $x^T C = 0$. La somme pondérée des marquages des places dans le support de x est alors toujours constante. Ainsi, à chaque contrainte (\vec{w}, k) est ajoutée une variable d'écart m_s telle que

$$\vec{w}^T M + m_s = k. \quad [1.6]$$

Cette variable d'écart correspond à un moniteur s qui va garantir que le produit $\vec{w}^T M$ ne dépassera jamais k . Soit n_c le nombre de contraintes CGEM du problème, C_s la matrice d'incidence des places moniteurs et M_{s_0} le vecteur de leurs marquages initiaux. Alors C_s doit satisfaire

$$\begin{bmatrix} W^T & I \end{bmatrix} \begin{bmatrix} C \\ C_s \end{bmatrix} = 0, \quad [1.7]$$

où $W = [\vec{w}_1 \dots \vec{w}_{n_c}]$ est la matrice des contraintes CGEM.

La résolution de 1.7 permet de déterminer les attributs des arcs qui connectent les places moniteurs au réseau non contrôlé. Quand au vecteur marquage initial, il est solution de l'équation suivante :

$$W^T M_0 + M_{s_0} = \vec{k}. \quad [1.8]$$

L'ensemble des places moniteurs ainsi déterminé permet un contrôle maximum permisif.

En présence de transitions incontrôlables, un contrôleur *acceptable* ne doit pas tenter de les contrôler. Une condition suffisante pour avoir un contrôleur acceptable est la suivante:

$$\vec{w}^T C_s^u \leq 0$$

où C_s^u est la matrice constituée des colonnes de C_s correspondantes aux transitions incontrôlables. Autrement dit, il suffit qu'aucune des places du contrôleur n'ait d'arcs sortants vers les transitions incontrôlables du modèle non contrôlé [MA99].

En présence de transitions inobservables, un contrôleur *acceptable* ne doit pas tenter de l'observer. Une condition suffisante pour avoir un contrôleur acceptable est la suivante:

$$\vec{w}^T C_s^{uo} = 0$$

où C_s^{uo} est la matrice constituée des colonnes de C_s correspondantes aux transitions inobservables. Autrement dit, il suffit qu'aucune des places du contrôleur n'ait d'arcs entrants ou sortants vers les transitions inobservables du modèle non contrôlé [MA99].

Une contrainte (\vec{w}, k) qui peut être satisfaite par une place de contrôle qui ne contrôle pas les transitions incontrôlables et qui n'observe pas les transitions inobservables est dite *admissible*. Dans le cas contraire, la contrainte (\vec{w}, k) doit être transformée en une contrainte (\vec{w}', k') telle que:

- (\vec{w}', k') est admissible;
- (\vec{w}, k) couvre (\vec{w}', k') , i.e.

$$\vec{w}'^T M \leq k' \Rightarrow \vec{w}^T M \leq k. \quad [1.9]$$

Pour satisfaire la condition [1.9], les auteurs proposent la transformation des contraintes linéaires suivante:

$$\begin{aligned} \vec{w}' &= \vec{r}_1 + r_2 \vec{w} \\ k' &= r_2(k+1) - 1 \end{aligned} \quad [1.10]$$

où \vec{r}_1 est un vecteur de dimension $\text{card}(P)$ (le nombre des places du réseau non contrôlé) tel que $\vec{r}_1^T M \geq 0$ pour tout marquage atteignable M , et r_2 est un entier strictement positif. (\vec{w}', k') doit bien entendu satisfaire la condition d'admissibilité, c-à-d :

$$(\vec{r}_1 + r_2 \vec{w})^T C_s^u \leq 0$$

et de non-négativité du marquage initial, c-à-d :

$$\vec{r}_1^T M_0 + r_2 (\vec{w}^T M_0 - k - 1) \leq -1. \quad [1.11]$$

Soient (N, M_0) le réseau de Petri du procédé à contrôler et C sa matrice d'incidence. Ce réseau comporte un ensemble de transitions incontrôlables défini par C^u et un ensemble de transitions inobservables défini par C^{uo} . Considérons un ensemble de contraintes (W, \bar{k}) à respecter. Soient \vec{r}_1 et r_2 définis comme précédemment avec $\vec{r}_1 + r_2 \vec{w} \neq 0$ et soit :

$$[\vec{r}_1 \quad r_2] \begin{bmatrix} C_s^u & C_s^{uo} & -C_s^{uo} & M_0 \\ \vec{w}^T C_s^u & \vec{w}^T C_s^{uo} & -\vec{w}^T C_s^{uo} & \vec{w}^T M_0 - k - 1 \end{bmatrix} \leq [0 \ 0 \ 0 \ -1] \quad [1.12]$$

le contrôleur

$$\begin{aligned} C_c &= -(\vec{r}_1 + r_2 \vec{w}^T) C = -\vec{w}'^T C \\ M_{c0} &= r_2(k+1) - 1 - (\vec{r}_1 + r_2 \vec{w}^T) M_0 = k' - \vec{w}'^T M_0 \end{aligned}$$

existe et respecte les conditions de contrôlabilité et d'observabilité.

b. L'approche de Giua et Seatzu

L'approche de Giua et Seatzu [GS02] développe un algorithme pour l'estimation de l'état d'un réseau dont le marquage ne peut pas être directement observé à cause des trois hypothèses suivantes :

- La structure du réseau N est connue.
- Toutes les transitions sont observables.
- Le marquage initial est inconnu.

L'algorithme d'estimation des marquages d'un réseau de places/transitions est basé sur l'observation des événements en utilisant un graphe de recouvrement observateur et un vecteur d'erreur d'estimation relatif à chaque place du réseau. Les auteurs ont aussi montré que cette estimation générée par l'observateur, pouvait être utilisée pour la synthèse de contrôleurs. L'algorithme proposé par Giua et Seatzu interdit le franchissement des transitions menant en dehors du comportement admissible. Cet algorithme n'est pas nécessairement optimal dans le sens où une transition admissible dans le comportement désiré peut être inhibée.

L'ensemble $\mathcal{M}(w)$ représente l'ensemble des états consistants par rapport à une séquence de tirs w observée. Formellement, $\mathcal{M}(w) = \{M \mid \exists M', M' \xrightarrow{w} M\}$.

Dans la suite de cette partie, on note par M_w le marquage M tel que $M_0 \xrightarrow{w} M$ et par $\vec{0}_m$ ($\vec{1}_m$) un vecteur $m \times 1$ de zéro (de un) où m est le nombre de place du réseau.

Pour une évolution du réseau donnée $M_{w0} \xrightarrow{t_{\alpha 1}} M_{w1} \xrightarrow{t_{\alpha 2}} \dots$, l'algorithme 1.1 est utilisé pour déterminer le marquage estimé μ_{wi} relatif au marquage actuel M_{wi} . Cet algorithme est basé sur l'observation de la séquence de tirs $w_i = t_{\alpha 1} t_{\alpha 2} \dots t_{\alpha i}$.

Algorithme 1.2.

1. Soit le marquage estimé initial $\mu_{w0} = \vec{0}_m$ et $w = w_0$ (séquence vide).
2. Soit $i = 1$.
3. Attendre le franchissement de $t_{\alpha i}$
4. Mettre à jour le marquage estimé $\mu_{wi-1} = \mu'_{wi}$ avec

$$\mu'_{wi}(p) = \max\{\mu_{wi-1}(p), C(p, t_{\alpha i})\}.$$
5. Soit $\mu_{wi} = \mu'_{wi} + C(., t_{\alpha i})$.
6. Soit $i = i + 1$.
7. Aller en 3.

FIN

Les auteurs ont établi un certain nombre d'hypothèses et définitions :

- Le marquage estimé est borné : $\mu_w = M_w$
- On définit l'erreur de place : $e_p(M_w, \mu_w) \equiv M_w(p) - \mu_w(p)$ noté aussi e_p .
- On définit l'erreur d'estimation $e(M_w, \mu_w) \equiv \frac{1}{\epsilon} \cdot (M_w - \mu_w)$

Les deux fonctions d'erreur ainsi définies, ne sont pas croissantes :

$$e_p(M_{wt}, \mu_{wt}) = e_p(M_w, \mu'_{wt}) \leq e_p(M_w, \mu_w)$$

$$e(M_{wt}, \mu_{wt}) = e(M_w, \mu'_{wt}) \leq e(M_w, \mu_w)$$

L'ensemble des marquages consistants par rapport à la séquence de tirs observée w est alors :

$$\mathcal{M}(w) = \{M \mid \exists M', M' [w] M\} \equiv \{M \mid M \geq \mu_w\}$$

Le graphe de recouvrement observateur est ensuite défini et représente simultanément l'ensemble des marquages atteignables du réseau avec l'erreur d'estimation en utilisant l'algorithme 1.2. Le marquage initial est représenté par rectangle avec des angles arrondis. Les marquages dont le vecteur d'erreur d'estimation $= \vec{0}_m$ sont représentés par des rectangles foncés.

Exemple 1.4. Sur la figure 1.9, un réseau de Petri est représenté ainsi que son graphe de recouvrement observateur. Chaque nœud de ce graphe représente le marquage réel M_w et l'erreur d'estimation $e_p(M_w, \mu_w) \equiv M_w - \mu_w$.

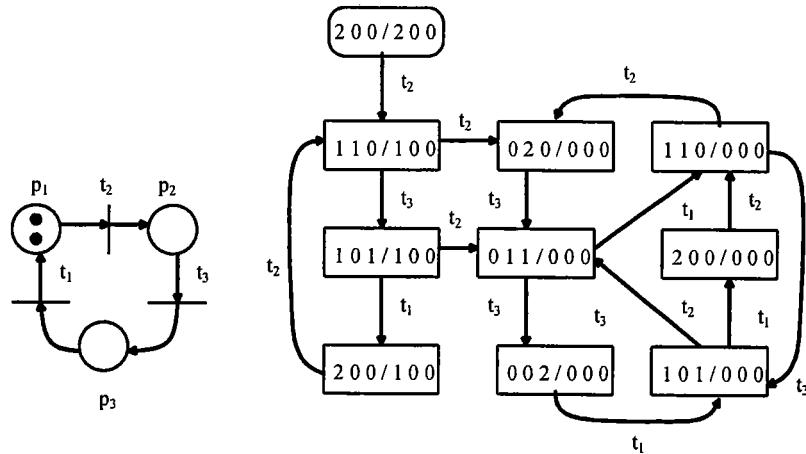


Figure 1.9. Exemple d'un RdP et de son graphe de recouvrement observateur

Dans une seconde partie, Giua et Seatzu introduisent la notion d'estimation de marquage avec macro-marquage. Dans ce cas, les auteurs supposent que le marquage $M-$ (dit marquage de départ) est connu. Après avoir évolué d'une manière inobservée, le réseau atteint un marquage M_0 (dit marquage initial) à partir duquel, le franchissement des transitions devient observable. Il est clair que $M_0 \in R(N, M-)$. L'ensemble des marquages consistants par rapport à la séquence de tirs observée w devient alors :

$$\mathcal{M}(w \mid M-) = \{M \mid \exists M_0 \in R(N, M-), M_0 [w] M\}.$$

Le macro-marquage est défini comme suit :

Définition 1.16 Considérons que l'ensemble des places P d'un réseau peut être écrit comme une union de $r+1$ sous-ensembles : $P = P_0 \cup P_1 \cup \dots \cup P_r$, tel que $P_0 \cap P_j = \emptyset$, $\forall j > 0$. Le nombre de jetons contenu dans P_j ($j > 0$) est connu et est égal à b_j . Cependant, le nombre de jetons dans P_0 est inconnu. Soit v_j le vecteur caractéristique relatif à chaque P_j , c-à-d, $v_j(p) = 1$ si $p \in P_j$ sinon $v_j(p) = 0$. Soit $V = [\vec{v}_1, \dots, \vec{v}_r]$ et $\vec{b} = [b_1, \dots, b_r]$. Le macro-marquage $\mathcal{V}(V, \vec{b}) = \{M \mid V^T \cdot M = \vec{b}\}$

Pour une évolution du réseau donnée $M_{w0} [t_{\alpha 1}] M_{w1} [t_{\alpha 2}] \dots$, l'algorithme 1.3 décrit ci-après est utilisé pour déterminer le marquage estimé μ_{wi} ainsi que la borne B_{wi} relatif au marquage actuel M_{wi} . Cet algorithme est basé sur l'observation de la séquence de tirs $w_i = t_{\alpha 1} t_{\alpha 2} \dots t_{\alpha i}$ et le macro-marquage initial $\mathcal{V}(V, \vec{b})$.

Algorithme 1.3

1. Soit le marquage estimé initial $\mu_{w0} = \vec{0}_m$ et $w = w_0$ (séquence vide).
2. Soit $B_{w0} = \vec{b}$.
3. Soit $i = 1$.
4. Attendre le franchissement de $t_{\alpha i}$.
5. Mettre à jour le marquage estimé $\mu'_{wi-1} = \mu'_{wi}$ avec

$$\mu'_{wi}(p) = \max\{\mu_{wi-1}(p), C(p, t_{\alpha i})\}.$$
6. Soit $\mu_{wi} = \mu'_{wi} + C(\cdot, t_{\alpha i})$.
7. Soit $B_{wi} = B_{wi-1} - V^T \cdot (\mu'_{wi} - \mu_{wi-1})$.
8. Soit $i = i + 1$.
9. Aller en 4.

FIN

L'ensemble des marquages consistants par rapport à la séquence de tirs observée w devient alors :

$$\mathcal{M}(w \mid V, \vec{b}) = \{M \mid V^T \cdot M = V^T \cdot \mu_w + B_w, M \geq \mu_w\}.$$

La politique de contrôle utilisée est définie ci-dessous :

Une transition t est inhibée après l'observation de la séquence de tirs w si et seulement si il existe un marquage admissible M consistant par rapport à w tel que le franchissement de t à partir de M mène à un état interdit.

L'ensemble des états admissibles est défini par des Contraintes Généralisées d'Exclusion Mutuelle (condition [1.1]).

Exemple 1.5. Considérons le réseau de Petri de la figure 1.9 avec un marquage initial $M_0 = [1, 1, 1]^T$ supposé inconnu. Soit l'ensemble des états interdits $F = \{M \mid M(p_1) > 2\}$. Le macro-marquage initial $M(p_1) + M(p_2) + M(p_3) = 3$. La figure 1.10 représente le graphe de recouvrement observateur du réseau. Chaque nœud du graphe est noté par $(M/e/B)$ où M est le marquage réel, e est l'erreur d'estimation et B la borne résultante.

Pour des raisons de simplification, l'évolution du graphe (figure 1.10) est arrêtée à chaque nœud où le vecteur d'erreur d'estimation = $\vec{0}_m$.

Les transitions en trait interrompu sont les transitions inhibées par le contrôleurs. En réalité, ces transitions ont été inhibées parce qu'il existe un marquage consistant par rapport à l'observation et à partir duquel, le franchissement de la transition mène à un état interdit. Nous pouvons rapidement voir que dans tous ces nœuds :

$$V^T \cdot \mu + B = V^T \cdot (M - e) + B = M(p_1) - e_{p1} + B = 3 > 2 \text{ ce qui viole la condition } M(p_1) \leq 2.$$

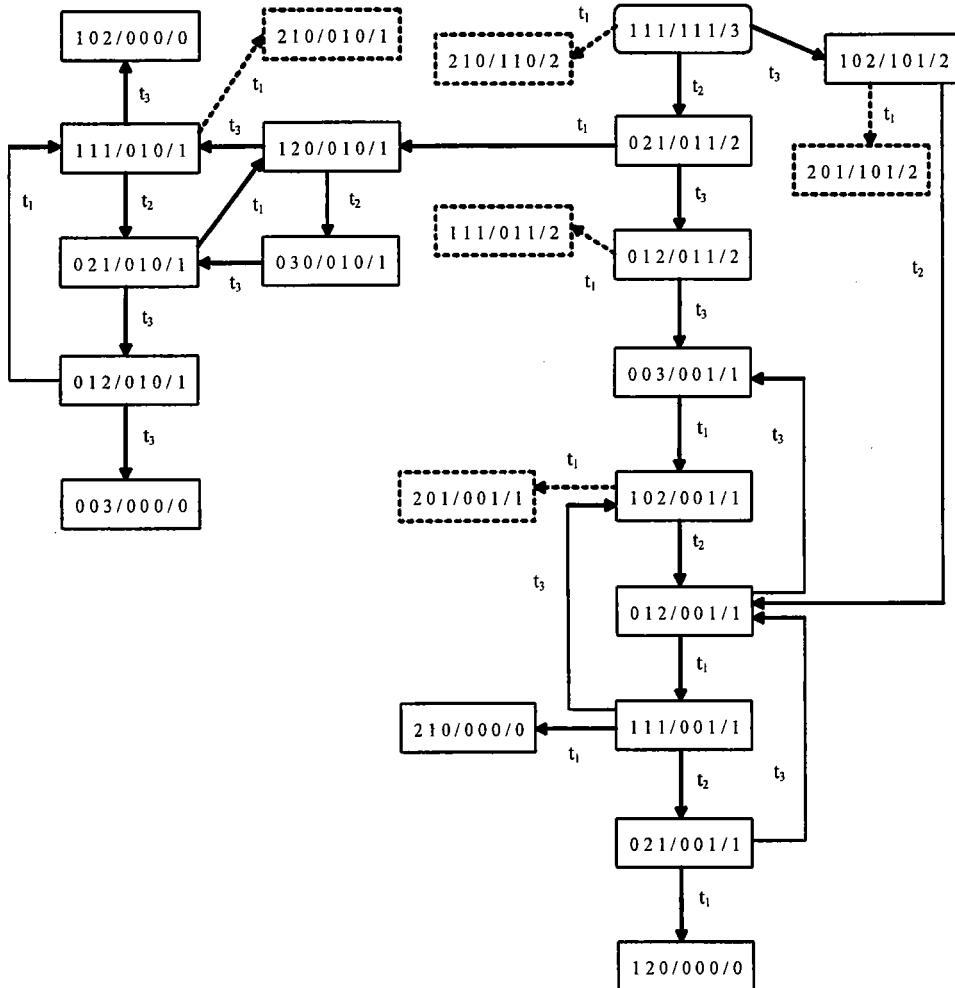


Figure 1.10. Graphe de recouvrement observateur du réseau contrôlé de l'exemple 1.5

1.2.5 Autre travaux sur l'observabilité

L'observabilité est une propriété fondamentale des systèmes à événements discrets. L'estimation des états d'un procédé et la commande par supervision des systèmes partiellement observables sont les deux grands thèmes d'observabilité les plus étudiés dans la littérature.

Pour les systèmes modélisés par des automates à états finis, Ramadge [Ram86] était le premier à montrer comment un observateur pouvait être déterminé pour les systèmes

partiellement observables. Caines et *al.* [CGW88] ont montré qu'il est possible d'utiliser la séquence observée pour déterminer l'ensemble des états équivalents (non distinguables). L'approche est basée sur la construction d'un arbre d'observation contenant l'ensemble des marquages non distinguables. Özveren et Willsky [ÖW90] ont proposé une approche pour la détermination de l'observateur qui permet de reconstruire un automate à états finis après l'observation d'une séquence finie d'événements. Özveren et Willsky ont aussi montré qu'un observateur peut avoir un nombre exponentiel d'états.

Li et Wonham [LW88], [LW93] ainsi que Takai et *al.* [TUK95] se sont intéressés au contrôle par retour d'état des systèmes partiellement observables. Les auteurs ont proposé des conditions nécessaires et suffisantes pour l'existence d'un contrôle par retour d'état optimal. Moody and Antsaklis [MA99] ont proposé une méthode de synthèse de la commande pour les modèles réseaux de Petri avec des transitions incontrôlables et des transitions inobservables. Leur approche consiste à modifier l'ensemble des marquages admissibles quand ce dernier ne respecte pas les conditions d'incontrôlabilité et d'inobservabilité.

1.3 Conclusion

Dans ce chapitre, nous avons présenté les fondements de la théorie de la commande par supervision des Systèmes à Événements Discrets (SED) à travers les résultats de Ramadge et Wonham (R/W). Nous nous sommes intéressés dans ce chapitre aux approches basées sur l'utilisation des réseaux de Petri pour les spécifications de type états interdits. Nous avons présenté dans un premier temps les approches traitant des systèmes à événements discrets totalement observables. Dans un deuxième temps, nous avons présenté les problèmes d'observabilité traités dans la littérature à travers l'approche de Moody et *al.* et celle de Giua et Seatzu. L'approche de Moody et *al.* traite de la synthèse de la commande des SED où les transitions du RdP du procédé sont partiellement observables. L'approche présentée par Giua et Seatzu cherche à estimer le marquage courant d'un RdP du procédé sachant que son marquage initial est inconnu et que toutes les transitions sont observables afin de lui appliquer le contrôle adéquat pour faire respecter les spécifications.

Chapitre 2

Commande optimale des graphes d'événements partiellement observables

L'exploitation des propriétés structurelles des graphes d'événements nous a permis de synthétiser une loi de commande que nous présentons dans ce chapitre pour le problème d'états interdits caractérisé par un ensemble de Contraintes Généralisées d'Exclusion Mutuelle (CGEM) avec la prise en compte de la contrainte d'observabilité des événements. Un graphe d'événements est un réseau de Petri dans lequel chaque place possède une seule transition d'entrée et une seule transition de sortie. Pour cette approche, nous nous intéressons aux cas où les CGEM concernent une ou plusieurs places critiques fortement indépendantes ou dépendantes. Dans chaque cas, l'expression analytique de la CGEM dans son pire cas, en termes de marquage atteignable, est donnée en fonction de la séquence de tirs observable du système. Ces contraintes sont alors évaluées en ligne par le superviseur. Nous prouvons aussi dans ce chapitre que pour toute séquence de transitions observables, il existe un unique marquage depuis lequel tout autre marquage possible du système, peut être atteignable d'une manière inobservable. Cette particularité importante, nous permet de concevoir une loi de commande efficace basée sur la séparation de l'observation et de la commande. Les résultats de cette partie ont fait l'objet des publications [ARX04a], [ARX04b] et [ARX04c].

2.1 Introduction

Dans ce chapitre, les travaux proposés par Ghaffari et al. [GRX03b] sur l'utilisation des graphes d'événements pour résoudre le problème d'état interdit sont étendus à la synthèse de commande des systèmes partiellement observables pour les spécifications de type CGEM.

La commande par supervision des réseaux de Petri partiellement contrôlables et partiellement observables a été étudiée dans [GS02], [MA99] et [Str00]. Moody et Antsaklis [MA99] et Stremersch [Str00] présentent des approches algébriques intéressantes mais ne garantissent pas toujours l'optimalité. L'approche que nous présentons dans ce chapitre concerne la commande par supervision des réseaux de Petri partiellement observables avec un marquage initial connu contrairement à celle présentée dans [GS02], où les auteurs considèrent le cas où le marquage initial est inconnu et toutes les transitions sont observables. En outre, comparé à [DX03] qui propose une analyse algébrique, notre approche fournit des résultats analytiques simples basés sur le concept de l'observateur. Notre approche est une extension de celle présentée par Ghaffari et al. [GRX03b]. Plus spécifiquement, nous avons :

- i) démontré que les problèmes de supervision en présence des événements inobservables peuvent être décomposés en deux sous-problèmes ; problème d'observabilité et problème de commande,
- ii) étendu les résultats analytiques de [GRX03b] aux graphes d'événements plus généraux avec des transitions inobservables pour des spécifications de types CGEM en utilisant de nouveaux résultats d'observabilité.

Ce chapitre est organisé comme suit. La section 2.2 introduit quelques définitions liées aux réseaux de Petri et présente le problème d'état interdit étudié. Des propriétés d'observabilité sont présentées dans la section 2.3. La section 2.4 propose la politique de commande optimale pour des spécifications de type CGEM dans le cas général. La section 2.5 présente la solution analytique pour des cas spécifiques de CGEM. Une illustration pratique de l'approche est donnée à la section 2.6.

2.2 Commande par supervision des graphes d'événements partiellement observables

Un graphe d'événements est un réseau de Petri ordinaire dans lequel chaque arc a un poids de un et chaque place a exactement une seule transition d'entrée et une seule transition de sortie [Mur89].

Un chemin orienté d'un graphe d'événements est un ordre alternatif de places et de transitions qui relient deux nœuds distincts (place ou transition). Le chemin est dit élémentaire si aucun nœud n'apparaît plus d'une fois dans la séquence. Un circuit est un chemin orienté partant d'une transition et revenant sur elle même. Il est élémentaire si aucun nœud n'apparaît plus d'une fois. Pour un chemin orienté quelconque $\pi = t_1 p_1 t_2 p_2 \dots p_n t_{n+1}$, on note par $M(\pi)$ la somme des marquages des places de π ; $M(\pi) = M(p_1) + \dots + M(p_n)$. La propriété suivante, due à Murata [Mur89], sera largement utilisée dans la suite du papier.

Propriété 2.1 : Le marquage de tout circuit ω est invariant ; $M(\omega) = M_0(\omega)$, $\forall M \in R(N, M_0)$. Le marquage d'un chemin orienté $\pi = t_1 p_1 \dots p_n t_{n+1}$ ne peut être modifié que par le franchissement de ses transitions d'extrémité, c'est à dire :

$$M(\pi) = M_0(\pi) + \bar{\sigma}(t_1) - \bar{\sigma}(t_{n+1}), \text{ où } M_0[\sigma]M.$$

Notre approche concerne la commande par supervision des graphes d'événement vivant (N, M_0) , c'est-à-dire chaque circuit élémentaire de (N, M_0) contient au moins un jeton. Cette condition est nécessaire et suffisante pour la vivacité d'un graphe d'événements [Mur89].

Rappelons que l'ensemble des transitions $T = T^c \cup T^u$ est formé de deux sous-ensembles ; T^c l'ensemble des *transitions contrôlables* et T^u l'ensemble des *transitions incontrôlables*. Le superviseur peut interdire le franchissement des transitions contrôlables mais pas celui des transitions incontrôlables. L'ensemble $T^u = T^f \cup T^{uo}$ est aussi constitué de *transitions libres* (T^f) et de *transitions inobservables* (T^{uo}). Il est possible qu'un procédé puisse avoir certains états atteignables à partir de transitions dont le franchissement ne peut pas être observé par le superviseur. Ces transitions sont dites inobservables. On notera que $T^{uo} \subseteq T^u$ et que $T^o = T^c \cup T^f$ est l'ensemble des transitions observables.

Le problème de la commande par supervision consiste à synthétiser un superviseur permettant d'assurer un comportement légal du procédé le plus permisif. L'ensemble des marquages admissibles est défini par un système d'inéquations linéaires $WM \leq K$ appelées contraintes généralisées d'exclusion mutuelles (CGEM), avec $W \in \mathbb{Z}^{n_c \times m}$, où Z représente l'ensemble des entiers, $K \in \mathbb{Z}^{n_c}$, m le nombre de place, n_c le nombre de contraintes et M le marquage courant du système. De plus, $W = [w_1, w_2, \dots, w_{n_c}]^T$ et $K = [k_1, \dots, k_{n_c}]^T$. Toute contrainte CGEM est représentée par un couplet (w_i, k_i) . Pour alléger l'écriture, il arrive que nous n'utilisons pas l'indice i et nous représentons la CGEM par (w, k) . Un état M satisfait une contrainte CGEM si $wM \leq k$, autrement, il viole la contrainte.

Définition 2.1 Soit $R^u(N, M_0)$ (resp. $R^{uo}(N, M_0)$) l'ensemble des marquages atteignables à partir du marquage M_0 en ne franchissant que des transitions incontrôlables (resp. inobservable).

Définition 2.2 Soit (N, M_0) un réseau de Petri. Un marquage est dit interdit si et seulement si il viole au moins une des contraintes CGEM. On peut traduire formellement l'ensemble des états interdits par

$$M_F = \{M \in R(N, M_0) / w_i M > k_i \text{ pour } i \in \{1, \dots, n_c\}\}.$$

Définition 2.3 Une place q est dite place critique s'il existe une contrainte (w_i, k_i) telle que $w_i[q] \neq 0$.

Le contrôleur doit respecter l'ensemble des CGEM. Formellement, la politique de commande d'un graphe d'événements totalement observable (GETO) se résume de la manière suivante :

Le franchissement d'une transition contrôlable t appartenant à un GETO à partir d'un marquage atteignable M est autorisé par la contrôle si et seulement si $G(w_i, M') \leq k_i$ pour toute spécification CGEM (w_i, k_i) où M' est le marquage atteint par le franchissement de t à partir de M et $G(w_i, M') = \text{MAX}\{w_i M^*, \forall M^* \in R^u(N, M')\}$.

Dans un graphe d'événement vivant N avec des transitions inobservables, le superviseur ne peut pas déterminer l'état réel du système. En effet, soient p_1 et p_2 deux places appartenant au graphe N tel que $p_1 \bullet = \bullet p_2 = \{t^{uo}\}$ où t^{uo} est une transition inobservable. Chaque fois qu'un jeton arrive dans la place p_1 , la transition t^{uo} devient franchissable. Comme cette dernière est inobservable, le superviseur ne peut pas déceler le moment de son franchissement. Dans ce cas, le jeton peut être soit dans la place p_1 ou la place p_2 . Ainsi le marquage réel du réseau est partiellement connu et l'analyse du pire cas des contraintes CGEM est alors difficile à faire.

D'une manière générale, étant donné une séquence de transitions observables σ^o , le franchissement d'une transition contrôlable t est interdit si

- il existe une séquence de transitions dont σ^o est sa séquence observable,
- t est franchissable après σ^o ,
- un marquage interdit est incontrôlablement atteignable suite au franchissement de σ^o .

Pour cette raison, nous proposons la structure de commande de la figure 2.1. Le rôle de l'observateur est de caractériser tous les marquages courants possibles en se basant sur la séquence des transitions observables. Le rôle du superviseur est de déterminer les transitions contrôlables à interdire après le franchissement de toute transition observable. Le module de commande est activé suite à l'occurrence d'une transition observable selon la politique suivante :

- Déterminer tous les marquages courants possible par l'observateur.
- Identifier les transitions contrôlables à interdire par le superviseur.

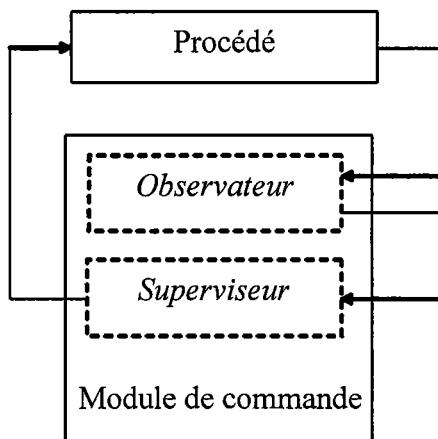


Figure 2.1. La structure de la commande par supervision

2.3 Observabilité

On note par:

- M : le marquage courant partiellement connu ;
- σ : la séquence de tirs partiellement connue comportant les transitions inobservables $M_0[\sigma]M$;
- σ^o : la séquence de transitions observables, $\sigma^o = P^o(\sigma)$, où P^o représente la fonction de projection observable et qui consiste à retirer de la séquence σ toutes les transitions inobservables.

Définition 2.4 Une séquence de transitions σ est dite conforme à σ^o si $M_0[\sigma] \in P^o(\sigma) = \sigma^o$. Soit $\Sigma(\sigma^o)$ l'ensemble de toutes les séquences conformes.

$$\Sigma(\sigma^o) = \left\{ \sigma \in T^* \mid M_0[\sigma] \in P^o(\sigma) = \sigma^o \right\}$$

Définition 2.5 Soit $\mathcal{M}(\sigma^o)$ l'ensemble de tous les marquages courants possibles atteignables à partir de M_0 par une séquence de transitions conforme à σ^o .

$$\mathcal{M}(\sigma^o) = \left\{ M \mid \exists \sigma \in \Sigma(\sigma^o), M_0[\sigma]M \right\}$$

Soient deux séquences σ_1 et σ_2 tel que $M_0[\sigma_1]M_1$ et $M_0[\sigma_2]M_2$. Les deux séquences sont conformes si elles sont conformes à une même séquence observable σ^o , c'est-à-dire $P^o(\sigma_1) = P^o(\sigma_2) = \sigma^o$ alors $\{\sigma_1, \sigma_2\} \subseteq \Sigma(\sigma^o)$. Les marquages M_1 et M_2 sont deux marquages courants possibles atteignables à partir de M_0 par les deux séquences de transitions conformes à σ^o et $\{M_1, M_2\} \subseteq \mathcal{M}(\sigma^o)$.

Considérons un vecteur \vec{X} tel que :

$$\vec{X}(t) = \begin{cases} \vec{\sigma}(t) & \forall t \in T^o \\ \left(\max_{t^o \in T^o} (\bar{\sigma}(t^o) - d(M_0, t, t^o)) \right)^+ & \forall t \in T^{uo} \end{cases}$$

où

$(y)^+ = \max\{0, y\}$ et $d(M_0, t, t^o)$ est la distance en termes de jetons entre t et t^o dans le marquage M_0 représentant le marquage du chemin minimal de tous les chemins joignant t à t^o dans N ne contenant aucune transition observable sauf t^o . Par convention, $d(M_0, t, t^o) = \infty$ si aucun chemin n'existe.

On notera que \vec{X} est déterminé uniquement par le vecteur de tirs de σ^o . Il est clair que \vec{X} est fonction de σ^o . Cependant, pour simplifier la notation, nous n'introduisons pas explicitement cette dépendance. Dans ce cas, \vec{X} joue un rôle très important dans la

caractérisation de la séquence de tirs partiellement connue. Il permet de déterminer le nombre minimal de fois qu'une transition inobservable est tirée.

Lemme 2.1 *Pour toute séquence de tirs $\sigma \in \Sigma(\sigma^o)$, $\vec{X} \leq \vec{\sigma}$.*

Preuve :

Si une transition t est observable, alors $\vec{X}(t) = \vec{\sigma}(t)$. Par contre, si t est inobservable alors pour toute transition observable $t^o \in T^o$, deux cas de figures se présentent :

(i) Il existe un chemin π dans N , constitué de transitions inobservables, joignant t à t^o . Selon la définition de distance, $d(M_0, t, t^o) = M_0(\pi)$. Depuis la propriété 1, $M(\pi) = M_0(\pi) + \vec{\sigma}(t) - \vec{\sigma}(t^o) \geq 0$ et donc $\vec{\sigma}(t) \geq \vec{\sigma}(t^o) - M_0(\pi) = \vec{\sigma}(t^o) - d(M_0, t, t^o)$.

(ii) Il n'existe pas de chemin entre t et t^o .

Dans ce cas, $d(M_0, t, t^o) = \infty$ et donc $\vec{\sigma}(t) \geq (\vec{\sigma}(t^o) - d(M_0, t, t^o))^+ = 0$. Comme résultat, $\vec{\sigma}(t) \geq (\vec{\sigma}(t^o) - d(M_0, t, t^o))^+$, $\forall t^o \in T^o$ et $\vec{\sigma}(t) \geq \vec{X}(t)$. \square

Lemme 2.2 *Il existe une séquence de tirs σ^* franchissable à partir du marquage initial M_0 tel que $\vec{\sigma}^* = \vec{X}$. Soit M^o le marquage résultant, c'est-à-dire $M^o = M_0 + C\vec{X}$.*

Preuve :

Pour prouver l'existence d'une séquence σ^* tel que $M_0[\sigma^*]M^o$ à partir de [Mur89], il est suffisant de montrer que $M^o(p) \geq 0$, $\forall p \in P$. quatre cas sont possible pour toute place p :

- 1^{er} cas : $\bullet p \in T^o$ et $p^\bullet \in T^o$. Par conséquent, $M^o(p) = M(p) \geq 0$.
- 2^{ème} cas : $\bullet p \in T^{uo}$ et $p^\bullet \in T^{uo}$. Par conséquent, $M^o(p) = M_0(p) + \vec{X}(\bullet p) - \vec{X}(p^\bullet)$. Si $\vec{X}(p^\bullet) = 0$, alors $M^o(p) \geq 0$. Sinon, il existe un chemin π de transitions inobservables joignant p^\bullet à au moins une transition observable $t^o \in T^o$ de sorte que $\vec{X}(p^\bullet) = \vec{X}(t^o) - M_0(\pi)$. Comme $\bullet p$ p π est aussi un chemin inobservable joignant $\bullet p$ à t^o , alors $\vec{X}(\bullet p) \geq \vec{X}(t^o) - (M_0(p) + M_0(\pi))$. En combinant ces deux résultats, nous aurons $\vec{X}(\bullet p) + M_0(p) - \vec{X}(p^\bullet) \geq 0$ et donc $M^o(p) \geq 0$.
- 3^{ème} cas : $\bullet p \in T^o$ et $p^\bullet \in T^{uo}$. Par conséquent, $M^o(p) = M_0(p) + \vec{X}(\bullet p) - \vec{X}(p^\bullet)$. Si $\vec{X}(p^\bullet) = 0$, alors $M^o(p) \geq 0$. Sinon, il existe un chemin π de transitions inobservables joignant p^\bullet à au moins une transition observable $t^o \in T^o$ de sorte que $\vec{X}(p^\bullet) = \vec{X}(t^o) - M_0(\pi)$. Comme $\bullet p$ et t^o sont tous les deux observables, Nous pouvons déduire de la propriété 1 que $M(\bullet p p \pi) = M_0(p) + M_0(\pi) + \vec{X}(\bullet p) - \vec{X}(t^o) \geq 0$.

Ce qui donne, $M^o(p) = M_0(p) + \vec{X}(\bullet p) - \vec{X}(p^\bullet) = M_0(p) + M_0(\pi) + \vec{X}(\bullet p) - \vec{X}(t^o) \geq 0$.

- 4^{ème} cas : $\bullet p \in T^{uo}$ et $p^\bullet \in T^o$. Dans ce cas et depuis la définition de \vec{X} , $\vec{X}(\bullet p) \geq \vec{X}(p^\bullet) - M_0(p)$ et donc $M^o(p) \geq 0$. \square

Le lemme 2.2 montre l'existence d'une séquence de tirs σ^* ayant \vec{X} comme vecteur de tirs, c'est-à-dire σ^* est conforme à σ^o . Cependant, nous ne pouvons pas toujours garantir la conformité de σ^* , chose pour laquelle, nous proposons le lemme 2.3 qui établit l'existence d'une séquence de tirs conforme dont \vec{X} est son vecteur de tirs.

Lemme 2.3 *Il existe une séquence de tirs $\sigma' \in \Sigma(\sigma^o)$ tel que $P^o(\sigma') = \sigma^o$ et $\vec{\sigma}' = \vec{X}$.*

Preuve :

Considérons une séquence de tirs inconnue σ et la séquence σ^* du lemme 2.2. A partir de la propriété 13 de [DX03], il existe une séquence σ' franchissable à partir de M_0 tel que $P^o(\sigma') = P^o(\sigma) = \sigma^o$ et $\vec{\sigma}' = \vec{\sigma}^* = \vec{X}$. \square

De plus, depuis le lemme 2.3, nous avons $\sigma' \in \Sigma(\sigma^o)$ et le marquage résultant $M^o \in \mathcal{M}(\sigma^o)$.

Théorème 2.1 *Pour tout marquage $M \in \mathcal{M}(\sigma^o) \setminus M_0[\sigma]M$, il existe une séquence $\sigma'' \in (T^{uo})^* \setminus M^o[\sigma'']M$, et $\vec{\sigma}' + \vec{\sigma}'' = \vec{\sigma}$ où σ' représente la séquence définie au lemme 2.3. Par conséquent, $\mathcal{M}(\sigma^o) = R^{uo}(G, M^o)$.*

Preuve :

De la manière où nous avons défini \vec{X} , et en utilisant le lemme 2.1, nous pouvons déduire que $\vec{\sigma} - \vec{X} \geq 0$. A partir du lemme 2.3, la séquence de tirs σ' est franchissable à partir de M_0 et mène au marquage M^o et $\vec{\sigma}' = \vec{X}$. Depuis [DX03], il existe une séquence σ'' tel que $M^o[\sigma'']$ et $\vec{\sigma}'' = \vec{\sigma} - \vec{X}$. Le marquage obtenu suite au franchissement de la séquence σ'' à partir de M^o est :

$$M^o + C(\vec{\sigma} - \vec{X}) = (M_0 + C\vec{X}) + C(\vec{\sigma} - \vec{X}) = M_0 + C\vec{\sigma} = M.$$

D'où nous déduisons que $M_0[\sigma'\sigma'']M$ et $\vec{\sigma}' + \vec{\sigma}'' = \vec{\sigma}$. \square

Le théorème 2.1, caractérise entièrement les deux ensembles suivants :

- L'ensemble de tous les marquages courants possibles.
- L'ensemble des séquences de tirs conformes possibles.

Le deuxième ensemble contient la séquence minimale σ' , définie par le lemme 2.3, minimale dans le sens de vecteur d'occurrence, qui peut être étendu en lui ajoutant la séquence de transitions inobservables σ'' pour avoir le vecteur d'occurrence de toutes les séquences de l'ensemble.

Le marquage correspondant à la séquence de tirs minimal σ' sera appelé *le marquage observateur* noté M^o , c'est-à-dire $M_0[\sigma']M^o$. D'après le théorème 2.1, tout marquage courant possible M peut être atteint à partir du marquage observateur M^o par le franchissement d'une séquence de transitions inobservables σ'' . La figure 2.2, illustre la relation entre le marquage observateur M^o et le marquage courant possible M .

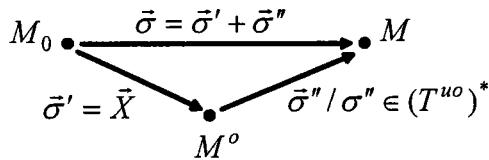


Figure 2.2. Relation M^o et M

Notons que pour caractériser l'ensemble de tous les marquages courants possibles, il n'est pas nécessaire de connaître la séquence σ^o de transitions observables. Il suffit pour cela de connaître le vecteur d'occurrence de σ^o . La politique optimale de contrôle, peut être basée sur le vecteur d'occurrence de σ^o au lieu du vecteur d'occurrence de σ . Notons aussi que bien que la séquence minimale σ' n'est pas unique, le vecteur d'occurrence minimal $\bar{\sigma}' = \bar{X}$ est unique. Il en résulte donc un marquage observateur M^o unique définissant le module observateur de la structure de la commande par supervision.

2.4 Politique de commande dans le cas général

En présence de transitions inobservables, le marquage d'état du système est partiellement connu. L'approche de contrôle par retour d'état présentée dans [GRX03b] ne peut pas être utilisée vu que le marquage courant M est inconnu. La politique de commande doit être basée sur la séquence σ^o de transitions observables.

Considérons une séquence σ^o de transitions observable, pour déterminer la politique de commande optimale nous nous intéressons à l'analyse du pire cas de chaque spécification CGEM (w, k) avant le franchissement de toute transition contrôlable t , c'est-à-dire $g(w, \sigma^o t) = \text{MAX}\{wM^*, \forall M^* \in R^u(N, M) \text{ et } \forall M' \in \mathcal{M}(\sigma^o t)\}$.

Nous pouvons déduire à partir du théorème 2.1, que l'observation et la supervision sont indépendantes. Le marquage observateur correspondant à $\sigma^o t$, noté $M^o(\sigma^o t)$, peut être utilisé pour l'analyse du pire cas de la manière suivante : $g(w, \sigma^o t) = G(w, M^o(\sigma^o t))$ avec $G(w, M) = \text{MAX}\{wM^*, \forall M^* \in R^u(N, M)\}$.

Avant de poursuivre, il faut noter qu'un problème de commande n'a pas de solution dans les deux cas suivants :

- Si les spécifications sont violées suite au franchissement d'une séquence de transitions incontrôlable depuis le marquage initial. C'est-à-dire, $g(w, \sigma) > k$ pour $\sigma \in (T^{uc})^*$;
- Si à l'état initial, les spécifications sont violées. C'est-à-dire, $g(w, \sigma) > k$ pour $\sigma = \epsilon$ et où ϵ représente la séquence vide.

Formellement, la politique de commande des graphes d'événement partiellement observable se résume de la manière suivante :

Pour une séquence σ^o de transitions observables, le franchissement d'une transition contrôlable t à partir d'un marquage M est autorisé par le contrôleur si et seulement si ;

- (i) *t est franchissable à partir d'au moins un marquage courrant possible M, c'est-à-dire $\exists M \in \mathcal{M}(\sigma^o) \mid M[t]$;*
- (ii) *$G(w, M^o(\sigma^o t)) \leq k$ pour toutes les spécifications CGEM (w, k).*

L'application de la politique de commande optimale nécessite tout d'abord la détermination des transitions contrôlables potentiellement franchissables. Pour cela, nous définissons un nouveau réseau (N^o, M_0) composé uniquement de transitions observables. Dans ce réseau, une place reliant deux transitions t et t' est rajoutée si et seulement si il existe un chemin entre ces deux transitions, c'est-à-dire, $d(M_0, t, t') \neq \infty$ dans le graphe d'événement initial (N, M_0) . Une transition contrôlable t vérifie bien la condition (i) de la Politique de commande, si et seulement si $\sigma^o t$ est franchissable dans (N^o, M_0) , ce qui est facilement vérifiable en ligne. L'application de cette approche nécessite également une mise à jour continue du marquage observateur M^o à chaque franchissement d'une transition observable.

L'algorithme de la politique commande optimale est donné ci-dessous :

Algorithme 2.1.

1. Construire le réseau d'observation (N^o, M_0)
2. $M^o = M_0$
3. Calculer $G(w, M^o)$ pour toute CGEM (w, k). Si $G(w, M^o) > k$ pour au moins une CGEM, alors pas de solution de commande et Fin algorithme.
4. Pour toute transition contrôlable t franchissable dans le réseau observation,
 - 4.1. Déterminer le marquage observateur $M^o(\sigma^o t)$
 - 4.2. Calculer $G(w, M^o(\sigma^o t))$ pour toute CGEM (w, k)
 - 4.3. Interdire t si $G(w, M^o(\sigma^o t)) > k$ pour toute CGEM (w, k)
5. Attendre le franchissement d'une transition observable t
6. Mettre à jour le marquage du réseau d'observation ainsi que le marquage observateur M^o
7. Aller à l'étape 4

En terme de complexité, notre politique de commande décrite dans l'algorithme 1 est polynomiale par rapport au nombre de transitions.

2.5 Solutions analytiques pour des cas spécifiques

La détermination de $G(w, M)$ pour l'analyse du pire cas, est basée sur le calcul de $y(q, \sigma^0)$ représentant le pire cas relatif à une place critique q . En d'autres termes, $y(q, \sigma^0)$ est le nombre maximal de jetons que peut contenir la place q en ne franchissant que des transitions incontrôlables après l'observation de la séquence σ^0 . Formellement,

$$y(q, \sigma^0) = \text{MAX}\{M^*(q), \forall M^* \in R^u(N, M) \text{ et } \forall M \in \mathcal{M}(\sigma^0)\}.$$

Nous pouvons déduire du théorème 2.1 que $y(q, \sigma^0) = Y(q, M^0)$ où $Y(q, M^0)$ représente le nombre maximal de jetons que peut contenir la place q en ne franchissant que des transitions incontrôlables à partir du marquage observateur M^0 . A partir de là, il est clair que notre politique de commande dépend de l'analyse du pire cas. Dans la suite de ce chapitre, nous utilisons les propriétés structurelles des graphes d'événements pour développer des solutions analytiques pour une analyse plus efficace du pire cas. Les résultats analytiques présentés dans cette partie, traitent la majorité des cas réels.

2.5.1 Propriétés structurelles des graphes d'événements

Les places critiques, les chemins d'influence et les zones d'influence caractérisent les propriétés structurelles d'un graphe d'événements [GRX03b]. Les chemins d'influence qui alimentent les places critiques en jetons d'une manière incontrôlable sont ainsi définis :

Définition 2.6 *Un chemin d'influence d'une place critique q , noté $\pi_i(q)$, est un chemin élémentaire qui relie t à q telle que t est la seule transition contrôlable et donc observable dans tout le chemin. L'ensemble de tous les chemins d'influence d'une place critique q est noté $\Pi(q)$.*

Soit le graphe d'événement représenté à la figure 2.3, où q_6 est une place critique. Cette place possède deux chemins d'influence représentés en foncé :

- $\pi_1(q_6) = t_1 q_1 t_3 q_7 t_4 q_6$,
- $\pi_2(q_6) = t_2 q_5 t_4 q_6$.

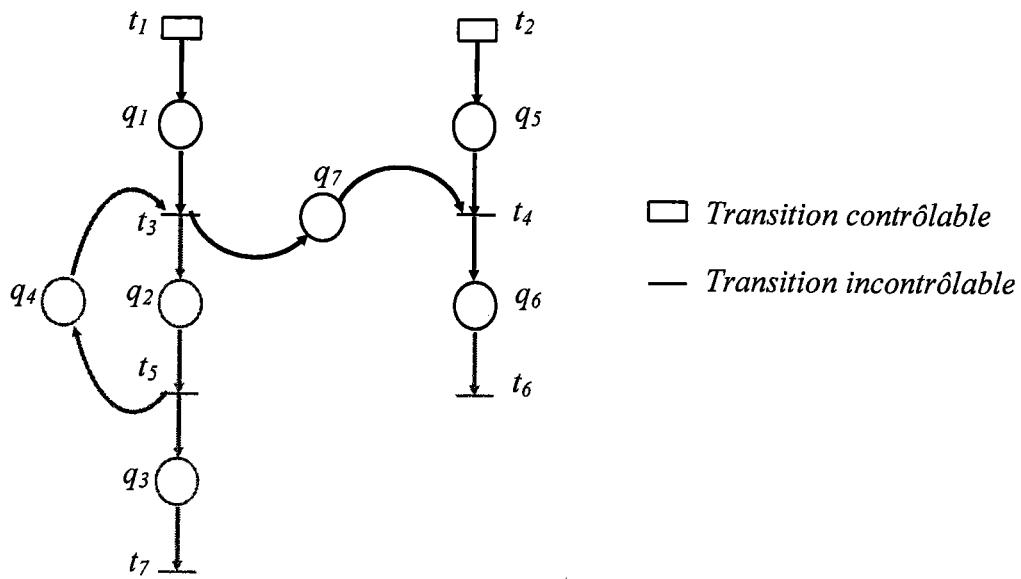


Figure 2.3. Chemins d'influence de la place critique q_6

Le marquage maximal que peut avoir une place q dépend du marquage du chemin $\pi(q)$ et plus précisément, du franchissement des transitions incontrôlables de ce chemin. Soit $\Omega(q)$ l'ensemble des circuits élémentaires de transitions incontrôlables contenant la place q . $\Pi(q)$ et $\Omega(q)$ définissent la zone d'influence de q .

Définition 2.7 Une zone d'influence $Z(q)$ d'une place critique q est le sous-réseau de N qui contient tous les sommets s , tel qu'il existe un chemin qui relie s à q et qui ne contient aucune transition contrôlable excepté éventuellement s .

Bien entendu la zone d'influence d'une place critique q inclut toutes les places dont le marquage peut être pris en compte dans l'évaluation du marquage du pire cas. La zone d'influence de q englobe $\Pi(q)$ et $\Omega(q)$.

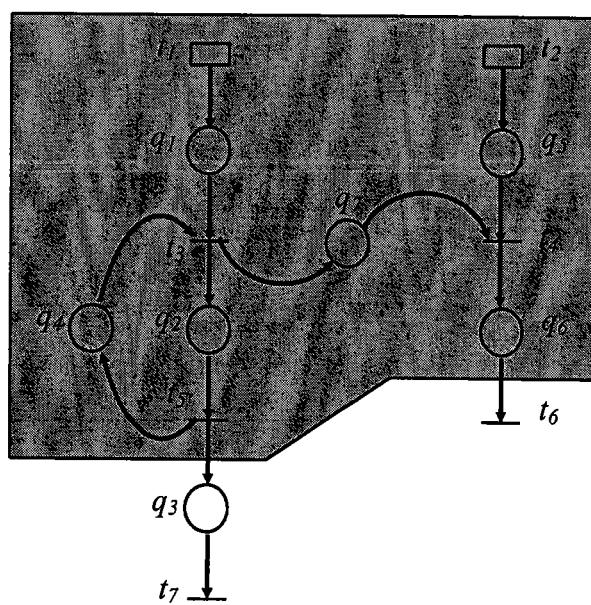


Figure 2.4. Zone d'influence de la place critique q_6

La zone d'influence $Z(q_6)$ de la place critique q_6 représenté à la figure 2.4 inclut les deux chemins critiques $\pi_1(q_6) = t_1 q_1 t_3 q_7 t_4 q_6$, et $\pi_2(q_6) = t_2 q_5 t_4 q_6$.

$$Z(q_6) = \{\pi_1(q_6), \pi_2(q_6)\}.$$

Soient q_1 et q_2 deux places critiques. Elles sont dites fortement indépendantes s'il n'existe pas de chemin contenant des transitions non contrôlables, qui relie q_1 à q_2 ou l'inverse, c'est-à-dire, $q_1 \notin Z(q_2)$ et $q_2 \notin Z(q_1)$. Elles sont faiblement indépendantes s'il n'existe aucun chemin d'influence ou circuit de transitions non contrôlables qui contient les deux places, c'est-à-dire, $q_1 \notin \Omega(q_2) \cup \Pi(q_2)$ et $q_2 \notin \Omega(q_1) \cup \Pi(q_1)$. Sinon elles sont dites dépendantes.

2.5.2 Contraintes CGEM avec une seule place critique

Pour respecter les spécifications de type états interdits représentées par des CGEM, le superviseur doit inhiber les transitions contrôlables si leur franchissement mène à des marquages dangereux. Dans les travaux de Ghaffari *et al.*, [GRX03b], les auteurs ont étudié le cas où le modèle du procédé G ne contient pas de transitions inobservables, le superviseur doit évaluer en ligne le pire cas $Y(q, M)$ représentant le nombre maximum de jetons accumulés dans q d'une façon incontrôlable à partir d'un marquage M . L'expression analytique de $Y(q, M)$ est donnée par le théorème 2.2.

Théorème 2.2 Pour toute place critique q et tout marquage atteignable M de (N, M_0) ,

$$Y(q, M) = \min \left\{ \min_{\pi \in \Pi(q)} M(\pi), SB(q) \right\}$$

où

$M(\pi) = M_0(\pi) + \sigma(t_\pi^c) - \sigma(q^\bullet)$, $M_0[\sigma]M$, t_π^c représente la seule transition contrôlable dans le chemin π ($t_\pi^c \rightarrow q$) et $SB(q) = \min M_0(\omega)$ représente la borne structurelle de $M(q)$ quand tous les circuits élémentaires ω sont considérés, y compris les circuits contenant des transitions contrôlables. On a $SB(q) = \max_{M \in R(N, M_0)} M(q)$.

Dans le cas où le modèle du procédé G contient des transitions inobservables, le superviseur ne peut pas déterminer l'état du système, puisque celui-ci est partiellement observable, d'où la nécessité de faire appel au marquage observateur pour calculer le pire cas.

Considérons le graphe de marquage (N, M_0) tel qu'il est représenté à la figure 2.5. Dans cet exemple, la GMEC (w, k) est associée à la place critique q et $w(q) \geq 0$. La transition $t = q^\bullet \in T^{uo}$, t_π^c représente la seule transition contrôlable dans le chemin $\pi(t_\pi^c \rightarrow q)$ et $t_{\delta_i}^o$ représente la première transition observable dans le chemin $\delta_i(q^\bullet \rightarrow t_{\delta_i}^o)$. δ_i est appelé chemin de sortie de la transition q^\bullet . Nous appelons un chemin de sortie d'une place critique q , un chemin élémentaire reliant q^\bullet à la première transition observable $t_{\delta_i}^o$. Il est clair que $t_{\delta_i}^o$ est la seule transition observable dans tout le chemin $\delta_i(q^\bullet \rightarrow t_{\delta_i}^o)$. L'évaluation du marquage de q au pire cas atteignable après l'observation

de la séquence σ^o , c'est-à-dire, à partir du marquage observateur M^o , revient à maximiser les jetons accumulés dans q par le franchissement de transitions incontrôlables à partir de M^o . Pour se faire, il faut déterminer le nombre de fois que q^\bullet est franchie. Comme cette transition est inobservable, nous utilisons son chemin de sortie pour calculer le nombre minimal de fois que celle-ci a été franchie.

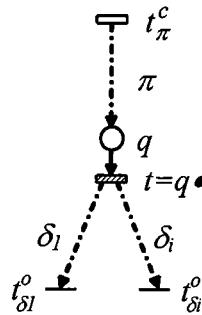


Figure 2.5. Exemple étudié

Dans ces conditions, nous nous proposons d'établir l'expression analytique du pire cas que peut avoir la place q en jetons de façon incontrôlable.

Théorème 2.3 Pour toute place critique q de (N, M_0) relativ à une contrainte (w, k) avec $w \geq 0$ et toute séquence de tirs observable σ^o , il existe deux séquences $\sigma \in (T)^*$ et $\sigma^* \in (T^*)^*$ tel que $P(\sigma) = \sigma^o$, $M_0[\sigma\sigma^*]M^*$ et $M^*(q) = Y(q, M^o)$, avec

$$Y(q, M^o) = \min \left\{ \min_{\pi \in \Pi(q)} M^o(\pi), SB(q) \right\}$$

où

$M^o(\pi) = M_0(\pi) + \bar{X}(t_\pi^c) - \bar{X}(q^\bullet)$, \bar{X} comme défini à la section 2.3, $SB(q)$ représente la borne structurelle de la place q , c'est-à-dire $SB(q) = \max_{M \in R(N, M_0)} M(q)$ et $\Pi(q)$ l'ensemble de tous les chemins d'influence de la place q .

Ceci implique que $g(w, \sigma^o) = G(w, M^o) = w(q) Y(q, M^o)$

Preuve : La preuve de ce théorème est directement obtenue depuis le théorème 2.2 ci-dessus et le théorème 2 de [GRX03b]. \square

$Y(q, M^o)$ est évalué en ligne à chaque franchissement d'une transition observable. Pour que la transition contrôlable t^c soit tirée, il faut que son franchissement ne viole pas la contrainte CGEM.

2.5.3 Contraintes CGEM avec plusieurs places critiques

2.5.3.1 Cas de places critiques indépendantes

Nous considérons dans cette partie les contraintes CGEM qui concernent des places critiques indépendantes. Le pire cas pour une contrainte avec des places critiques correspond à un marquage atteignable où chaque place contient un nombre de jetons égal au marquage maximal incontrôlablement atteignable.

Théorème 2.4 Soit $Cr(w) = \{q_1, q_2, \dots, q_r\}$ l'ensemble des places critiques relativement à une contrainte (w, k) avec $w \geq 0$. Si les places de $Cr(w)$ sont indépendantes, alors pour toute séquence de tirs observable σ^o , il existe deux séquences $\sigma \in (T)^*$ et $\sigma^* \in (T^u)^*$ tel que $P(\sigma) = \sigma^o$, $M_0[\sigma\sigma^*]M^*$ et $M^*(q_i) = Y(q_i, M^o)$ avec

$$Y(q, M^o) = \min \left\{ \min_{\pi \in \Pi(q)} M^o(\pi), SB(q) \right\}.$$

Ceci implique que $g(w, \sigma^o) = \sum_{q_i \in Cr(w)} w(q_i) Y(q_i, M^o)$.

Preuve : La preuve de ce théorème est directement obtenue depuis le théorème 2.2 ci-dessus et le théorème 2 de [GRX03b]. \square

Deux différentes situations de deux places critiques, q_1 et q_2 , indépendantes sont représentées à la figure 2.6.

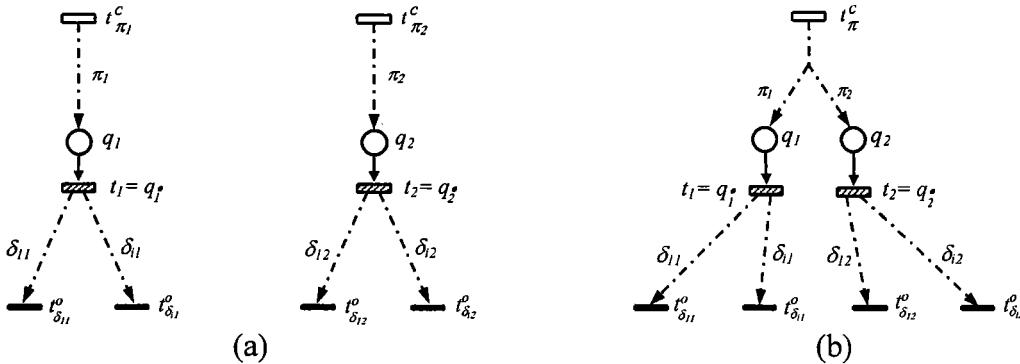


Figure 2.6. Différents cas de places critiques indépendantes

2.5.3.2 Cas de places critiques dépendantes

Dans cette partie, nous considérons uniquement le cas où les contraintes CGEM concernent des places critiques q_i dépendantes sur un même chemin L et ayant un même coefficient de pondération $w_i(q_i) = C$, pour une contrainte $C \geq 0$. Les places critiques considérées sont réparties sur un même chemin L contenant uniquement des transitions inobservables ou incontrôlables. Pour déterminer le pire cas, nous transformons une

telle CGEM en une équivalente avec une seule place critique q_L et un coefficient de pondération $w(q_L) = C$ (figure 2.7).

Définition 2.8 Un chemin critique est un chemin élémentaire $L = q_1 t_1 q_2 t_2 \dots q_n t_n$, tel que les transitions t_1, \dots, t_{n-1} sont des transitions inobservables ou incontrôlables sachant que $T'' \subseteq T'$ et les places q_1, \dots, q_n sont des places critiques correspondant à une contrainte (w, k) . Une place fictive q_L telle que $\bullet q_L = \bullet q_1, q_L \bullet = q_n \bullet$, $w_L(q_L) = \text{Max}(w_i(q_i))$ pour $i=1, \dots, n$ et $M_0(q_L) = M_0(q_1) + \dots + M_0(q_n)$, est une place équivalente à L .

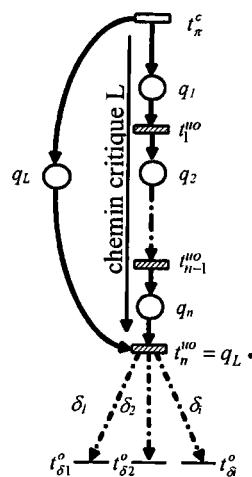


Figure 2.7. Cas de plusieurs places critiques dépendantes

Théorème 2.5 Soit $L = q_1 t_1 q_2 t_2 \dots t_{n-1} q_n$ un chemin critique d'un graphe (N, M_0) . Supposons qu'une place fictive q_L associée à L est ajoutée au réseau (N, M_0) . La place fictive q_L est une place redondante et pour tout marquage atteignable M , $M(q_L) = M(q_1) + \dots + M(q_n)$.

Preuve :

En ajoutant la place q_L , le réseau reste toujours un graphe d'événements. Par conséquent, d'après la propriété 1, pour tout marquage M atteignable dans le nouveau réseau tel que $M_0[\sigma]M$, $M(q_L) = M_0(q_L) + \bar{\sigma}(\bullet q_1) - \bar{\sigma}(q_n \bullet) = M(q_1) + \dots + M(q_n)$. Il est donc évident que q_L est une place redondante puisque $M(q_L) \geq M(q_n)$. \square

Notons que la place q_L telle qu'elle est définie par la définition 2.8 est une place redondante qui n'affecte en rien les marquages atteignables dans (N, M_0) . Par conséquent, l'analyse du pire cas pour la contrainte (w, k) dont les places critiques forment un chemin critique L peut être simplifiée en introduisant une place équivalente q_L , c'est-à-dire on remplace les termes d'une spécification CGEM $CM(q_1) + \dots + CM(q_n)$ relative à un chemin critique L par $CM(q_L)$.

En utilisant une place équivalente fictive q_L , l'analyse du pire cas atteignable d'une contrainte CGEM relative un chemin critique L peut être transformée en une analyse du pire cas atteignable de CGEM relative à une seul place critique q_L . Le théorème 2.3 peut

donc être utilisé pour l'évaluation du pire cas de contraintes CGEM relatives à plusieurs chemins critiques avec des places équivalentes indépendantes.

2.6 Commande d'une cellule automatisée d'assemblage des tiges de piston

La cellule automatisée d'assemblage des tiges de piston étudiée dans [MA99] est considérée comme un exemple d'illustration de l'approche proposée. Le modèle réseau de Petri du procédé est représenté à la figure 2.8. Le tableau 1 fournit la signification physique de chaque place. L'assemblage nécessite l'intervention de deux types de robots. Trois robots S-380 sont employés pour préparer et aligner les pièces à assembler, et trois robots M-1 permettant de fixer le chapeau sur la tige du piston. Nous considérons que les robots M-1 sont contrôlés par un autre superviseur indépendant. Dans ce cas, les transitions t_6 , t_7 , et t_8 sont considérées comme des transitions inobservables par notre superviseur.

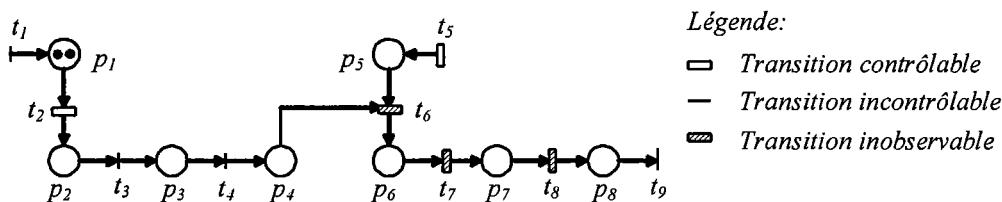


Figure 2.8. La cellule automatisée d'assemblage des tiges de piston

p_1	Le bloc moteur et le vilebrequin sont prêts à être traités.
p_2	Le robot S-380 aligne le vilebrequin.
p_3	Le robot S-380 met la tige du piston dans la zone de travail.
p_4	Le robot M-1 prépare le bloc moteur.
p_5	Le robot M-1 prend l'outil de maintien des pistons.
p_6	Le robot M-1 tire la tige du piston dans le bloc moteur, rend l'outil de maintien.
p_7	Le robot M-1 place un chapeau sur la tige du piston.
p_8	Le robot M-1 fixe le chapeau à la tige du piston.

Tableau 2.1. Description des places de la figure 2.8

Trois contraintes CGEM sont considérées :

- $M(p_5) + M(p_6) \leq 2$
- $M(p_2) + M(p_3) \leq 3$
- $M(p_5) + M(p_6) + M(p_7) + M(p_8) \leq 3$

Ces CGEM traduisent des contraintes de capacité sur le nombre disponible pour les outils de maintiens, les robots S-380 et les robots M-1.

La CGEM (a), $M(p_5) + M(p_6) \leq 2$, les places critiques p_5 et p_6 ont un même poids $w_5 = w_6 = 1$ et représentent un chemin critique L_1 . Une place équivalente q_{L1} de poids $w_{L1} = 1$ est ajoutée (figure 2.9).

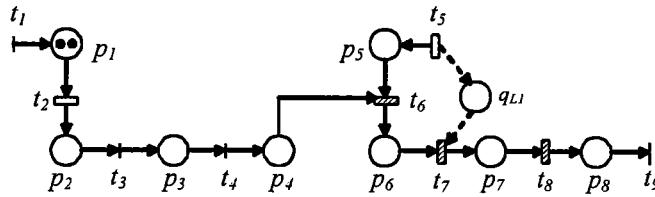


Figure 2.9. Place q_{L1} équivalente aux deux places critiques p_5 et p_6

Considérons la place équivalente q_{L1} et son chemin d'influence $t_5 q_{L1}$, pour déterminer le pire cas, nous utilisons le théorème 2.3.

$$g(q_{L1}, \sigma^o) = Y(q_{L1}, M^o) = M_0(\pi_1) + \vec{X}(t_5) - \vec{X}(t_7).$$

D'après la définition de \vec{X} , $g(q_{L1}, \sigma^o) = M_0(\pi_1) + \sigma(t_5) - (\sigma(t_9) - d(M_0, t_7, t_9))^+$. Comme $M_0(\pi_1) = 0$ et $d(M_0, t_7, t_9) = 0$ alors :

$$g(q_{L1}, \sigma^o) = \sigma(t_5) - \sigma(t_9). \quad [2.1]$$

La CGEM (b), $M(p_2) + M(p_3) \leq 3$, les places critiques p_2 et p_3 ont un même poids $w_2 = w_3 = 1$ et représentent un chemin critique L_2 . Une place équivalente q_{L2} de poids $w_{L2} = 1$ est ajoutée (figure 2.10).

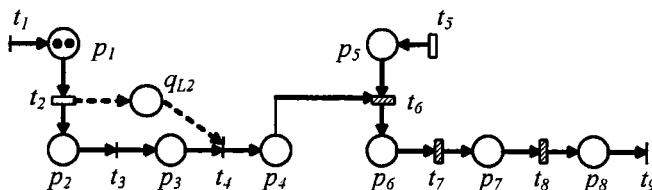


Figure 2.10. Place q_{L2} équivalente aux deux places critiques p_2 et p_3

Pour déterminer le pire cas, concernant la place q_{L2} et son chemin d'influence $t_2 q_{L2}$, en appliquant le théorème 2.3, $g(q_{L2}, \sigma^o) = Y(q_{L2}, M^o) = M_0(\pi_2) + \vec{X}(t_2) - \vec{X}(t_4)$, et de la même manière de résolution que pour la CGEM (a):

$$g(q_{L2}, \sigma^o) = \sigma(t_2) - \sigma(t_4). \quad [2.2]$$

La CGEM (c), $M(p_5) + M(p_6) + M(p_7) + M(p_8) \leq 3$, les places critiques p_5, p_6, p_7 et p_8 ont un même poids $w_5 = w_6 = w_7 = w_8 = 1$ et représentent un chemin critique L_3 . Une place équivalente q_{L3} de poids $w_{L3} = 1$ est ajoutée (figure 2.11).

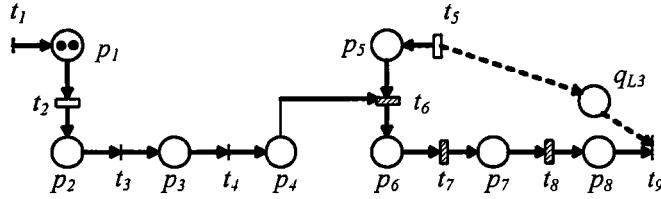


Figure 2.11. Place q_{L3} équivalente aux places critiques p_5 , p_6 , p_7 et p_8

Pour déterminer le pire cas, concernant la place q_{L3} et son chemin d'influence t_5q_{L3} , en appliquant le théorème 2.3, $g(q_{L3}, \sigma^o) = Y(q_{L3}, M^o) = M_0(\pi_3) + \bar{X}(t_5) - \bar{X}(t_9)$, et de la même manière de résolution que pour la CGEM (a):

$$g(q_{L3}, \sigma^o) = \sigma(t_5) - \sigma(t_9). \quad [2.3]$$

D'un point de vue contrôle, le superviseur évalue en ligne les prédictats [2.1]-[2.3]. Connaissant le marquage initial $M_0 = (2, 0, 0, 0, 0, 0, 0, 0)^t$ du graphe d'événement N , pour toute transition contrôlable et franchissable, le superviseur doit garantir le respect des contraintes suivantes :

$$\begin{aligned}\sigma(t_5) - \sigma(t_9) &\leq 2 \\ \sigma(t_2) - \sigma(t_4) &\leq 3\end{aligned}$$

2.7 Conclusion

Nous avons présenté dans ce chapitre une méthode simple et efficace de complexité polynomiale pour résoudre le problème d'états interdits des graphes d'événement en présence de transitions incontrôlable et ou inobservables. Les spécifications du contrôle sont données sous forme de contraintes linéaires de type CGEM. L'algorithme de la commande par supervision développé résume la politique de commande optimale qui permet de décider en ligne l'autorisation ou l'inhibition des transitions contrôlables afin que le système respecte le comportement admissible maximum permisif.

Avant d'autoriser le franchissement d'une transition contrôlable t à partir d'un marquage M , le superviseur détermine le marquage du pire cas pour une contrainte donnée. Ce marquage est atteint par une séquence de transitions incontrôlables et correspond à une valeur maximale de la contrainte. En présence de transitions inobservables, le superviseur ne peut pas connaître le marquage courant du système. Un module d'observation est alors proposé permettant de déterminer le marquage observateur M^o utilisé pour le calcul du pire cas. Ainsi, l'approche proposée dissocie l'observation de la commande. Le module de commande se charge d'inhiber la transition contrôlable t si cette dernière viole la contrainte. L'application de cette approche nécessite une mise à jour continue du marquage observateur M^o à chaque franchissement d'une transition observable. Cette tâche est réalisée par le module d'observation.

Chapitre 3

Commande optimale des réseaux de Petri partiellement observables

Dans ce chapitre, nous présentons une approche de synthèse des contrôleurs RdP pour le problème des transitions d'états interdites. Notre approche repose sur la théorie des régions pour des modèles RdP généralisés bornés. Elle intègre la notion de réversibilité avec les contraintes d'incontrôlabilité et d'inobservabilité des événements et détermine un contrôleur RdP maximum permisif, quand il existe. Le contrôleur est un ensemble de places de contrôle qui peuvent être pures ou impures. La première étape, basée sur la théorie de Ramadge-Wonham, détermine le graphe d'atteignabilité observable raffiné et contrôlé. Dans la deuxième étape, nous utilisons la théorie de régions pour déterminer un ensemble de places de contrôle à ajouter au modèle RdP initial. Ces places de contrôle garantissent le comportement désiré. Les résultats de cette partie font l'objet de la publication [ARX04d].

3.1 Introduction

Une méthode de synthèse de contrôleur RdP a été développée au sein de notre équipe et présentée dans [GRX03a]. La méthode est valable pour tout modèle RdP généralisé et borné. L'approche proposée construit dans un premier temps, le comportement admissible non bloquant maximum permis, puis s'appuie sur l'utilisation de la théorie des régions pour la synthèse de contrôleurs RdP. L'ensemble des transitions est subdivisé en deux sous-ensembles disjoints : T^c l'ensemble des transitions contrôlables et T^u celui des transitions incontrôlables.

Dans ce chapitre, proposons une approche de synthèse des contrôleurs RdP en intégrant la contrainte d'observabilité. Les travaux présentés dans [GRX03a] sont étendus à la synthèse des contrôleurs pour les systèmes modélisés par des réseaux de Petri partiellement observables. L'ensemble des transitions incontrôlable est donc subdivisé en deux sous-ensembles : T^o l'ensemble des transitions observables et T^{uo} celui des transitions inobservables. En présence de transitions inobservables, la synthèse des contrôleurs RdP devient une tâche plus difficile puisque l'état réel du système devient partiellement connu.

Ce chapitre est organisé comme suit. La section 2 présente des définitions et des notations utilisées dans ce chapitre. Le problème d'observabilité est traité dans la section 3. La section 4 présente l'approche de synthèse proposée. Une application de l'approche de synthèse sur un exemple de système de production est donnée dans la section 5.

3.2 Définitions et notations utilisées

Cette section présente des notations, des définitions ainsi que quelques propriétés qui seront utilisées dans la suite de ce chapitre.

L'ensemble des transitions considéré $T = T^c \cup T^u$ est subdivisé en transitions contrôlables (T^c) et transitions incontrôlables (T^u). L'ensemble $T^u = T^f \cup T^{uo}$ et lui aussi subdivisé en deux sous-ensembles, celui des transitions libre (T^f) et celui des transitions inobservable (T^{uo}). Il faut noter que $T^{uo} \subseteq T^u$ et que $T^o = T^c \cup T^f$ représente l'ensemble des transitions observables.

Dans la suite du chapitre, la notation $x[t] \rightarrow (x[t] \rightarrow x')$ signifie que la transition t est franchissable à partir de l'état x (et mène à l'état x'). Cette notation est étendue aux séquences de transitions c'est-à-dire $x[\sigma]$ et $x[\sigma] \rightarrow x'$.

La projection observable est aussi utilisée dans ce chapitre. Comme définition, nous considérons celle proposée dans la littérature par Cassandras et Lafourture [CL99], à savoir, la projection observable est une fonction $P : T^* \rightarrow (T^o)^*$ avec :

$$\begin{aligned} P(\varepsilon) &:= \varepsilon \\ P(t) &:= \begin{cases} t & \text{si } t \in T^o \\ \varepsilon & \text{si } t \in T^{uo} \end{cases} \\ P(\sigma t) &:= P(\sigma)P(t) \quad \text{pour } \sigma \in T^*, t \in T \end{aligned}$$

3.3 Comportement admissible contrôlable

Notre approche traite de la synthèse des contrôleurs RdP pour le problème de transitions d'état interdites. Le problème de type transitions d'état interdites est plus général que le problème classique d'états interdits. En effet, dans ce type de problème, des transitions d'états peuvent être interdites sans pour autant que les états qu'elles engendrent ne soient forcément des états interdits.

Le comportement admissible du système contrôlé est déterminé à partir de l'approche de Ramadge-Wonham (R/W) en prenant l'état initial comme unique état marqué pour garantir la réversibilité du procédé. Dans notre approche, le marquage initial est supposé connu.

3.3.1 Observabilité du procédé

La synthèse des contrôleurs pose un problème d'observabilité dans le cas des systèmes partiellement observables. Pour mettre en évidence ce problème, nous considérons l'exemple 3.1 décrit ci-dessous.

Exemple 3.1 : Soit le réseau de Petri de la figure 3.1. A partir du marquage initial $(1, 0, 0, 0)^t$ et après le franchissement de la transition t_1 , l'état réel du procédé devient inconnue. En effet t_2 et t_3 sont deux transitions inobservables. Le jeton peut être dans la place p_2 , ou dans p_3 ou dans p_4 .

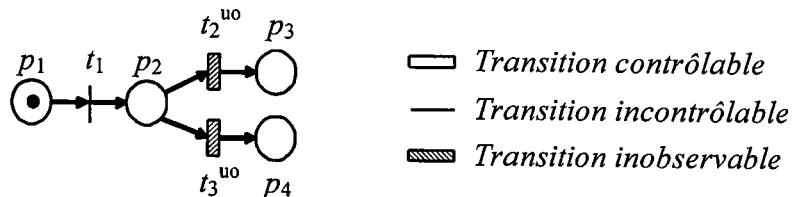


Figure 3.1. Modèle réseau de Petri avec des transitions inobservables

Les séquences $\sigma_1 = t_1$, $\sigma_2 = t_1 t_2$ et $\sigma_3 = t_1 t_3$ ont une même projection observable : $P(\sigma_1) = P(\sigma_2) = P(\sigma_3) = \sigma^o = t_1$. Selon la définition 2.5 du chapitre 2, l'ensemble de tous les marquages courants possibles atteignables à partir de M_0 par une séquence de transitions conforme par rapport à σ^o , $\mathcal{M}(\sigma^o = t_1) = \{M_1 = (0, 1, 0, 0)^t, M_2 = (0, 0, 1, 0)^t, M_3 = (0, 0, 0, 1)^t\}$. En d'autres termes, le marquage réel du réseau peut être M_1 , M_2 ou M_3 .

3.3.2 Le graphe d'atteignabilité observateur

Le graphe d'atteignabilité $RG(N, M_0)$ est utilisé pour modéliser le comportement d'un réseau de Petri (N, M_0) borné et pour la synthèse du contrôleur. En présence de transitions inobservables, le marquage des états du procédé devient partiellement connu et le graphe d'atteignabilité ne peut plus être utilisé directement pour la synthèse. Pour cette raison, nous nous sommes proposés de transformer le graphe d'atteignabilité en un graphe d'atteignabilité observateur, noté $RG^o(N, y_0)$, pour représenter toutes les

séquences possibles. L'algorithme 3.1 issu depuis des travaux de Cassandras et Lafortune [CL99] est utilisé pour déterminer le graphe d'atteignabilité observateur.

Chaque nœud du graphe d'atteignabilité $RG(N, M_0)$ représente un marquage d'état. Par contre, chaque nœud du graphe d'atteignabilité observateur $RG^O(N, y_0)$, représente un ensemble de marquages d'états possibles. Comme le modèle réseaux de Petri (N, M_0) est borné alors le graphe d'atteignabilité est fini est par conséquent, le graphe d'atteignabilité observateur est aussi fini. La construction du graphe d'atteignabilité observateur $RG^O(N, y_0)$ est basée sur l'hypothèse que le marquage initial est connu ainsi que les définitions suivantes.

Définition 3.1 Soit $R^{uo}(x)$ l'ensemble des états indistinguables par rapport à un marquage de réseau de Petri x . En d'autres termes, $R^{uo}(x)$ représente l'ensemble des états atteignables à partir de l'état x en franchissant seulement des transitions inobservables. Formellement, $R^{uo}(x) = \{x' \in RG(N, M_0) \mid \exists \sigma \in (T^{uo})^* \text{ tel que } x[\sigma] x'\}$. Pour un ensemble S , $R^{uo}(S) = \bigcup_{x \in S} R^{uo}(x)$.

Dans l'exemple précédent, il est clair qu'un état de l'observateur ne peut être modifié que suite au franchissement d'une transition observable. Chaque état de l'observateur représente un ensemble d'états du procédé. Dans la suite de ce mémoire, les états de l'observateur sont appelés macro-état et les états du procédé micro-état. Plus précisément, chaque macro-état y correspond à un ensemble de micro-états indistinguables. Par conséquent, le macro-état initial y_0 de l'observateur correspond à l'ensemble des micro-états $R^{uo}(x_0)$ qui sont des états atteignables à partir de l'état initial x_0 par le franchissement de transitions inobservables.

Définition 3.2 Une transition t est dite franchissable à partir d'un macro-état y si t est franchissable à partir d'au moins un micro-état x de y c'est-à-dire, $\exists x \in y \text{ et } t \in T \text{ tel que } x[t]$.

Définition 3.3 Le franchissement d'une transition observable t à partir d'un macro-état y mène à un macro-état y' défini comme suit :

$$y' = \bigcup_{\substack{x \in y \\ x[t]x'}} R^{uo}(x')$$

où y' représente l'ensemble des micro-états atteignables à partir du micro-état x de y en franchissant d'abord la transition observable t suivie de transitions inobservables.

Remarque 3.1

Deux macro-états y et y' sont considérés comme étant le même macro-état s'ils ont le même ensemble de micro-états.

La construction du graphe d'atteignabilité observateur $RG^O(N, y_0)$ de $RG(N, M_0)$ est résumée par l'algorithme suivant :

Algorithme 3.1 : La construction du graphe d'atteignabilité observateur

Soit à construire le graphe d'atteignabilité observateur $RG^O(N, y_0)$ du réseau de Petri (N, M_0) à partie du graphe d'atteignabilité $RG(N, M_0)$

1. Définir le macro-état initial $y_0 = R^{uo}(x_0)$
2. Pour tout macro-état y inexploré et pour toute transition observable t franchissable à partir de y , déterminer le macro-état y' obtenu en franchissant t à partir de y .
3. Si y' existe, ajouter un arc (y, y') étiqueté t , sinon, ajouter un nouveau macro-état y' dans le graphe d'atteignabilité observateur puis ajouter l'arc (y, y') étiqueté t .
4. Si il existe au moins un macro-état inexploré, aller à l'étape 2. Sinon, Fin.

Utilisons l'algorithme 3.1 pour déterminer le graphe d'atteignabilité observateur $RG^O(N, y_0)$ du modèle réseaux de Petri de l'exemple 3.1 (figure 3.1). Le graphe d'atteignabilité $RG(N, M_0)$ du réseau est donné à la figure 3.2.a. Le macro-état initial y_0 est $y_0 = R^{uo}(x_0) = \{x_0\}$. La transition t_1 est la seule transition observable franchissable à partir de y_0 et menant à un macro-état y_1 défini comme suit :

$$y_1 = \bigcup_{\substack{x \in y_0 \\ x \neq t_1}} R^{uo}(x) = R^{uo}(x_1) = \{x_1, x_2, x_3\}.$$

Comme aucune transition observable n'est franchissable à partir de $y_1 = \{x_1, x_2, x_3\}$ alors la construction est terminée. Le graphe d'atteignabilité observateur $RG^O(N, y_0)$ est donné à la figure 3.2.b.

Si le franchissement d'une transition observable t^o mène du macro-état y au macro-état y' alors on dit que y' est atteignable à partir de y et on note $y / [t^o] y'$.

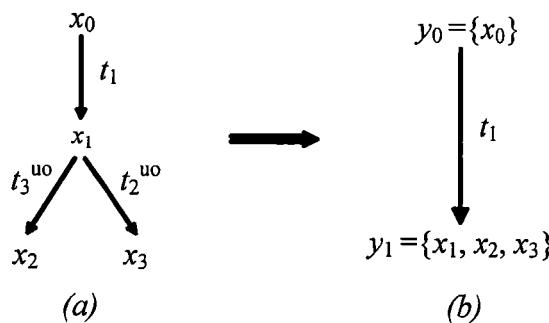


Figure 3.2. Graphe d'atteignabilité $RG(N, M_0)$ et graphe d'atteignabilité observateur $RG^O(N, y_0)$ de l'exemple 3.1

Remarque 3.2

Le franchissement d'une transition observable t^o à partir d'un macro-état y mène à un autre macro-état même si t^o est franchissable depuis plus qu'un micro-état de y . Ceci implique que la relation d'atteignabilité d'un graphe d'atteignabilité

observateur $RG^O(N, y_0)$ est une représentation globale des différentes relations de micro-état-transition dans le graphe d'atteignabilité $RG(N, M_0)$.

En résumé, le franchissement d'une transition inobservable t^{in} à partir d'un micro-état x_i mène à un micro-état x_j appartenant au même macro-état. D'un autre côté, le franchissement d'une transition observable t^o à partir d'un macro-état y mène à un autre macro-état y' .

3.3.3 Le graphe d'atteignabilité observateur raffiné

Cette section introduit le graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$ qui est un graphe d'état obtenu par raffinement du graphe d'atteignabilité observateur $RG^O(N, y_0)$. Ce raffinement consiste à introduire les transitions inobservables entre les micro-états dans l'objectif d'étudier par la réversibilité du procédé. Plus précisément, chaque macro-état y comporte tous les nœuds qui représentent ses micro-états ainsi que toutes les transitions inobservables qui les relient entre eux. Le graphe d'atteignabilité observateur raffiné est équivalent à la composition synchrone de $RG(N, M_0)$ et $RG^O(N, y_0)$. La figure 3.3 représente le graphe d'atteignabilité observateur raffiné de l'exemple 3.1.

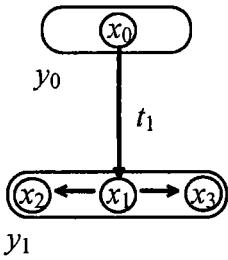


Figure 3.3. Graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$ de l'exemple 3.1

3.3.4 Le graphe d'atteignabilité observateur contrôlable

Cette section s'intéresse au comportement admissible contrôlable représenté par le graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, y_0)$. La détermination de $RG^{CO}(N, y_0)$ est basée sur les transitions d'états interdites, la condition de vivacité en tenant compte des transitions incontrôlables / inobservables.

Définition 3.4 Un macro-état est dit interdit si au moins un de ses micro-états est interdit. Soit Y_F l'ensemble des macro-états interdits.

Définition 3.5 Un macro-état est dit dangereux si il mène d'une manière incontrôlable à un macro-état interdit. Soit Y_D l'ensemble des macro-états dangereux.

Les ensembles Y_F et Y_D sont directement déterminés à partir du graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$.

Définition 3.6 Le Sous-Graphe Vivant (*SGV*) est un sous-graphe de $RG^{RO}(N, y_0)$ contenant tous les macro-états y_i dont tous les micro-états x_i peuvent menés au micro-état x_0 représentant le marquage initial.

Définition 3.7 Un macro-état est dit bloquant si au moins un de ses micro-état mène d'une manière incontrôlable en dehors du Sous-Graphe Vivant du graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$. Soit Y_B l'ensemble des macro-états bloquants.

En d'autres termes, un macro-état est dit bloquant si au moins un de ses micro-états est bloquant.

La détermination du comportement admissible maximum permisif consiste à déterminer et enlever de manière itérative tous les macro-états interdits, dangereux et bloquants jusqu'à la convergence vers un *SGV* qui ne contient ni des macro-états interdits, ni dangereux et ni bloquants. La construction du *SGV* représentant le comportement admissible maximum permisif et non bloquant est donnée par l'algorithme suivant :

Algorithme 3.2 : La construction du Sous-Graphe Vivant

Soit à construire le Sous-Graphe Vivant représentant le comportement admissible maximum permisif et non bloquant à partir du modèle RdP (N, M_0) du procédé à superviser ;

1. Générer le graphe d'atteignabilité $RG(N, M_0)$ du modèle RdP (N, M_0) du procédé à superviser.
2. Générer le graphe d'atteignabilité observateur $RG^O(N, y_0)$.
3. Construire le graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$.
4. Définir l'ensemble des macro-états interdits Y_F .
5. Identifier l'ensemble des macro-états dangereux Y_D en explorant $RG^{RO}(N, y_0)$.
6. Déterminer le graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, y_0)$ dérivé de $RG^{RO}(N, y_0)$ en supprimant Y_D .
7. Vérifier si $RG^{CO}(N, y_0)$ est un Sous-Graphe Vivant à fin de respecter la contrainte de vivacité.
 - 7.1. Si $RG^{CO}(N, y_0)$ est un SGV alors aller en 10.
 - 7.2. Si $RG^{CO}(N, y_0)$ n'est pas un SGV alors calculer le SGV.
8. Remplacer $RG^{RO}(N, y_0)$ par le SGV déterminer dans 7.2 et remplacer Y_F par l'ensemble des macro-états n'appartenant pas au SGV.
9. Aller à l'étape 5.
10. $RG^{CO}(N, y_0)$ est le comportement admissible.

L'algorithme 3.2 permet de déterminer le contrôleur maximum permisif, puisque uniquement les macro-états dangereux et les macro-états bloquants sont éliminés. Le *SGV* est noté $RG^{CO}(N, y_0)$ et représente le graphe d'atteignabilité observateur contrôlable. Le $RG^{CO}(N, y_0)$ est utilisé pour générer le contrôleur RdP, sous forme de places de contrôle à intégrer au modèle RdP du procédé. Soient Y_L l'ensemble des macro-états de $RG^{CO}(N, y_0)$ et Ω l'ensemble des macro-état-transitions menant en

dehors de $RG^{CO}(N, y_0)$. Formellement, l'ensemble des macro-état-transitions à interdire par le contrôleur est $\Omega = \{(y, t) \mid y[t > y' \wedge y \in Y_L \wedge y' \notin Y_L]\}$. Les éléments de Ω sont appelés des instances de séparation.

3.4 Synthèse de la commande

Les problèmes d'états interdits et les problèmes de transitions d'état interdites (Ghaffari, *et al.* 2003) pour les réseaux de Petri bornés (N, M_0) peuvent être résolus par l'ajout de places de contrôle p_c définie pas $M_0(p_c), C^+(p_c, .), C(p_c, .)$ où $M_0(p_c)$ est son marquage initial et $C^+(p_c, .)$ (respec. $C(p_c, .)$) est le poids des arcs à partir des transitions de N vers p_c (respec. à partir de p_c vers les transitions de N). La contrainte d'observabilité fait que la place de contrôle p_c ne peut être connectée qu'aux transitions observables.

3.4.1 Préliminaires et relations

L'approche de synthèse de la commande proposée dans ce chapitre, tient en compte des transitions d'états interdits, de la condition de vivacité ainsi que des transitions incontrôlables / inobservables. L'objectif est de déterminer le comportement admissible contrôlable à partir du graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$ et des spécifications qui sont exprimées par des transitions d'états interdites. Enfin, pour l'obtention du contrôleur RdP optimal, si il existe, nous utilisons la théorie des régions introduite par Badouel et Darouneau [BBD95] [BD99] [BBD97].

Considérons le modèle RdP (N, M_0) du procédé à superviser et son graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, y_0)$. Pour toute place p et pour toutes transitions observables t franchissable à partir d'un macro-état y de $RG^{CO}(N, y_0)$:

$$\begin{aligned} y'(p) &= y(p) + C(p, t), \\ \forall (y \xrightarrow{t} y') \in RG^{CO}(N, y_0) \end{aligned} \tag{3.1}$$

où y_0 est le macro-état initial, $C(p, .)$ le vecteur d'incidence de p et y' le macro-état atteint par l'arc t à partir de y .

Considérons maintenant un cycle non orienté γ du graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, y_0)$. En appliquant l'équation d'état [3.1] aux différents nœuds de γ , puis en les sommant, cela donnera *l'équation de cycle* suivante :

$$\sum_{t \in T} C(p, t) \cdot \bar{\gamma}[t] = 0, \quad \forall \gamma \in S \tag{3.2}$$

où $\bar{\gamma}[t]$ représente la somme algébrique de toutes les occurrences de t dans γ et S , l'ensemble des cycles non orientés de $RG^{CO}(N, y_0)$.

$$y(p) = y_0(p) + C(p, .) \bar{\Gamma}_y,$$

où $\vec{\Gamma}_y$ représente le vecteur algébrique de tirs de Γ_y . L'atteignabilité de tout macro-état y de $RG^{CO}(N, y_0)$ implique la condition d'atteignabilité suivante :

$$\begin{aligned} y_0(p) + C(p, \cdot) \vec{\Gamma}_y &\geq 0, \\ \forall y \in RG^{CO}(N, y_0) \end{aligned} \quad [3.3]$$

Lemme 3.1 Toute place de contrôle p_c du réseau contrôlé doit satisfaire les deux relations [3.2] et [3.3].

3.4.2 Place de contrôle pure

Dans le but d'obtenir exactement le comportement désiré, pour toute instance de séparation $(y \xrightarrow{t} y')$ de Ω , tel que y est un macro-état admissible de $RG^{CO}(N, y_0)$ et t , une transition contrôlable à interdire à partir de y . Le franchissement de t est interdit par l'ajout d'une place de contrôle p_c . Si p_c est une place de contrôle pure alors le franchissement de t est interdit à partir de y si et seulement si :

$$\begin{aligned} y_{c0}(p_c) + C_c(p_c, \cdot) \vec{\Gamma}_y + C_c(p_c, t) &< 0, \\ \forall (y \xrightarrow{t} y') \in \Omega \end{aligned} \quad [3.4]$$

La relation [3.4] est appelée *condition de séparation*.

Théorème 3.1 Le comportement désiré RG^{CO} peut être obtenu par l'ajout de places de contrôle pures au réseau RdP (N, M_0) initial si et seulement si il existe une solution $(y_{c0}(p_c), C_c(p_c, \cdot))$ qui satisfait les conditions [3.2], [3.3] et [3.4] pour toute instance de séparation de Ω .

Preuve :

(\Leftarrow) Considérons le réseau contrôlé $(N_c, M_{c0}) = (N, M_0) \cup \{p_c\}$. Puisque toutes ses places vérifient les conditions (2) et (3), toutes les transitions d'état de RG^{CO} sont franchissables. Donc $RG^{CO} \subseteq R(N_c, M_{c0})$. De plus, toute instance de séparation de l'ensemble Ω , n'appartenant pas RG^{CO} est empêchée par le marquage d'une place de contrôle. Par conséquent, $RG^{CO} = R(N_c, M_{c0})$.

(\Rightarrow) Supposons que le marquage d'atteignabilité du réseau contrôlé (N_c, M_{c0}) est exactement RG^{CO} . Chaque place du réseau (N_c, M_{c0}) vérifie alors nécessairement les conditions [3.2] et [3.3] et pour chaque instance (y, t) de Ω , t est forcément non validée par le marquage d'une certaine place p_c , ce qui satisfait la condition de séparation [3.4].

□

L'Algorithme 3.3 ci-dessous résume la méthodologie de synthèse à base de places pures pour un comportement maximum permisif et non bloquant.

Algorithme 3.3 : Synthèse des places de contrôle pures

Soit RG^{CO} le comportement désiré et Ω l'ensemble des instances de séparation.

1. Déterminer l'arbre de recouvrement de RG^{CO} et l'ensemble de ses cycles de bases.
2. Générer les équations de cycle de base [3.2] en utilisant la méthode de Gauss.
3. Générer la condition d'atteignabilité [3.3] pour chaque macro-état y de RG^{CO} .
4. Tant que $\Omega \neq \emptyset$, Faire :
 - 4.1. Générer la condition de séparation [3.4] pour chaque instance de séparation (y, t) de Ω .
 - 4.2. Résoudre le système linéaire composé des relations [3.2], [3.3] et [3.4].

Soit $(y_{c0}(p_c), C_c(p_c, .))$ la solution correspondante.

 - 4.3. Eliminer toutes les instances de Ω qui peuvent être résolues par $(y_{c0}(p_c), C_c(p_c, .))$.

FIN Tant que.
5. Eliminer les places de contrôle redondantes.

Les places de contrôle pures ne peuvent pas résoudre tous les problèmes de transitions d'état interdites. Dans certains cas, il n'est pas possible de déterminer un contrôleur RdP avec uniquement des places de contrôles pures. Le problème suivant en est un exemple.

Exemple 3.2 : Considérons le modèle réseau de Petri de la figure 3.4.a. Les transitions t_1^{uo} et t_3^{uo} sont inobservables. La spécification de commande est d'interdire le franchissement de t_2 si t_4 est franchi, c'est à dire, interdire le franchissement de t_2 si les places p_3 et p_4 sont vides. Le graphe d'atteignabilité observateur raffiné $RG^{RO}(N, y_0)$ est donné à la figure 3.4.b et le graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, y_0)$, sans tenir compte de la contrainte de vivacité, est obtenu en interdisant t_2 à partir de y_2 . Le problème de transition d'état interdite revient à considérer l'instance de séparation $(y_2 \xrightarrow{t_2} y_3)$. Supposons que le problème peut être résolu par une place de contrôle pure p_c .

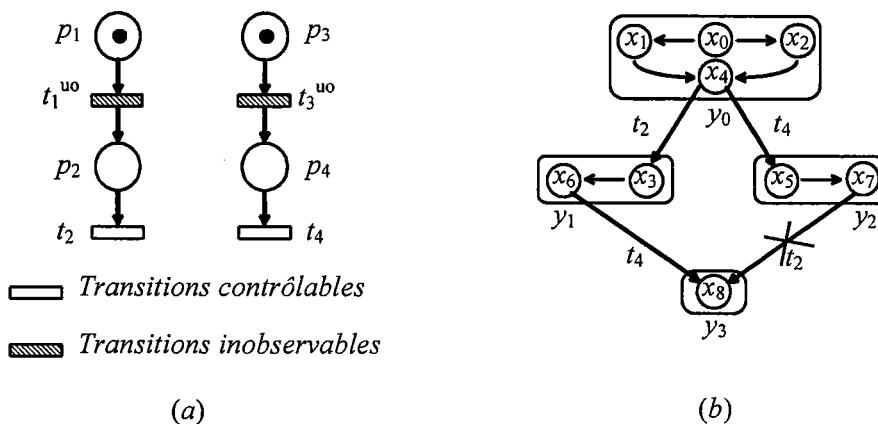


Figure 3.4. Problème de transition d'état interdite

Utilisons de la théorie des régions pour déterminer la place p_c . Le comportement désiré ne contient pas de cycle, p_c doit donc satisfaire le système suivant :

Les conditions d'atteignabilité de tout macro-état y de $RG^{CO}(N, y_0)$:

- (3.i) $y_{c0}(p_c) \geq 0$
- (3.ii) $y_1 : y_{c0}(p_c) + C_c(p_c, t_2) \geq 0$
- (3.iii) $y_2 : y_{c0}(p_c) + C_c(p_c, t_4) \geq 0$
- (3.iv) $y_3 : y_{c0}(p_c) + C_c(p_c, t_2) + C_c(p_c, t_4) \geq 0$

La condition de séparation :

$$(3.v) \quad (y_2 \xrightarrow{t_2} y_3) : y_{c0}(p_c) + C_c(p_c, t_4) + C_c(p_c, t_2) < 0$$

Le système linéaire (3.i)-(3.v) représente un ensemble de conditions contradictoires. Le problème de transition d'état interdit considéré n'admet pas une solution sous forme de place de contrôle pure. Cependant, il existe pour ce problème une solution sous forme de place de contrôle impure comme il est montré dans la section suivante.

3.4.3 Place de contrôle impure

Une place impure est une place pour laquelle il existe au moins une transition qui est en même temps transition d'entrée et transition de sortie. Pour une instance de séparation (y, t) de l'ensemble Ω , seules les places impures ayant une boucle contenant la transition t et cherchant à interdire le franchissement de t à partir de y sont considérées. Une place de contrôle impure p_c qui interdit l'instance de séparation (y, t) est caractérisée par son marquage initial $y_{c0}(p_c)$, son vecteur d'incidence $C_c(p_c, .)$ et $C_c^-(p_c, t)$ le poids de l'arc sortant vers t .

En considérant une place de contrôle impure p_c , les conditions (3) ne sont plus suffisantes pour garantir l'atteignabilité des macro-états du graphe $RG^{CO}(N, y_0)$. La place p_c doit satisfaire d'autres conditions supplémentaires. Ainsi, il en résulte

$$y_c(p_c) = y_{c0}(p_c) + C_c(p_c, .) \vec{\Gamma}_{y_i} \geq C_c^-(p_c, t), \quad [3.5]$$

$$\forall y_i[t] \text{ dans } RG^{CO}(N, y_0)$$

La condition de séparation de l'instance (y, t) par la place impure p_c devient :

$$y_{c0}(p_c) + C_c(p_c, .) \vec{\Gamma}_y < C_c^-(p_c, t) \quad [3.6]$$

Les conditions [3.2], [3.3], [3.5] et [3.6] sont nécessaires et suffisantes pour l'existence d'une place de contrôle impure interdisant (y, t) .

Théorème 3.2 Le comportement désiré RG^{CO} peut être obtenu par l'ajout de places de contrôle impures au réseau RdP (N, M_0) initial si et seulement si il existe une solution $(y_{c0}(p_c), C_c(p_c, \cdot), C_c^-(p_c, t))$ qui satisfait les conditions [3.2], [3.3], [3.5] et [3.6] pour toute instance de séparation de Ω .

La preuve de ce théorème est similaire à celle du théorème 3.1 pour l'existence de place de contrôle pures.

Exemple 3.3 : Considérons de nouveau le problème de transitions d'état interdites de la figure 3.4. Ce problème peut être résolu par l'ajout d'une place de contrôle impure p_c si et seulement si p_c satisfait les conditions (3.i), (3.ii), (3.iii), (3.iv) ainsi que les deux conditions suivantes :

$$(3.vi) \quad y_{c0}(p_c) \geq C_c^-(p_c, t_2)$$

$$(3.vii) \quad y_{c0}(p_c) + C_c(p_c, t_4) < C_c^-(p_c, t_2)$$

Une solution possible est tel que $y_{c0}(p_c) = 1$, $C_c(p_c, t_4) = -1$, $C_c(p_c, t_2) = 0$ et $C_c^-(p_c, t_2) = 1$. Le réseau contrôlé est donné à la figure 3.5.

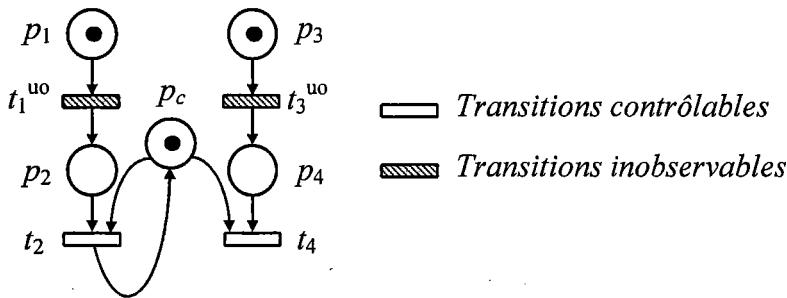


Figure 3.5. Solution pour le problème de transition d'état interdite de la figure 3.4.

La combinaison des conditions [3.5] et [3.6] relatives à l'instance de séparation (y, t) permet d'écrire la condition suivante :

$$\begin{aligned} C(p_c, \cdot) (\vec{\Gamma}_M - \vec{\Gamma}_{M^*}) &> 0, \\ \forall M[t] \text{ dans } RG^{CO}(N, M_0) \end{aligned} \quad [3.7]$$

Remarque 3.3

La condition [3.7] permet d'affirmer qu'il existe une place de contrôle impure résolvant une instance de séparation (y, t) si et seulement si le système linéaire constitué par les relations [3.2] et [3.7] admet une solution.

Pour déterminer une place de contrôle impure, nous commençons par déterminer son vecteur d'incidence en résolvant le système de conditions [3.2] et [3.7] puis son marquage initial et le vecteur de poids $C_c^-(p_c, t)$ tels que la place est une solution faisable des équations d'atteignabilité [3.3] et [3.5]. La démarche de détermination d'une place de contrôle impure est résumée par l'algorithme suivant :

Algorithme 3.4 : Synthèse des places de contrôle impures

Soit RG^{CO} le comportement désiré et Ω l'ensemble des instances de séparation.

1. Déterminer l'arbre de recouvrement de RG^{CO} et l'ensemble de ses cycles de base.
2. Générer les équations de cycle de base (2) en utilisant la méthode de Gauss.
3. Générer la condition d'atteignabilité (3) pour chaque macro-état y de RG^{CO} .
4. Tant que $\Omega \neq \emptyset$, Faire :
 - 4.1. Pour une instance $(y_i \xrightarrow{t} y_j)$ de Ω , générer la condition (7) pour chaque instance macro-état y de RG^{CO} .
 - 4.2. Résoudre le système linéaire composé des relations (2) et (7). Soit $C_c(p_c)$ la solution correspondante.
 - 4.3. Calculer $y_{c0}(p_c) = \max\{0, \max\{-C_c(p_c)\bar{\Gamma}_y, \forall y \in RG^{CO}\}\}$.
 - 4.4. Calculer $C_c^-(p_c, t) = \min\{y_{c0}(p_c) + C_c(p_c)\bar{\Gamma}_y, \forall y | (y \xrightarrow{t} y') \in RG^{CO}\}$.
 - 4.5. Eliminer toutes les instances de Ω qui peuvent être résolues par $(y_{c0}(p_c), C_c(p_c), C_c^-(p_c, t))$.
5. FIN Tant que.
5. Eliminer les places de contrôle redondantes.

3.5 Exemple d'un système de production

Considérons un système de production constitué de deux ressources R_1 et R_2 fabriquant deux types de produits A et B . Le modèle réseaux de Petri est donné à la figure 3.6.a. L'ensemble des transitions contrôlable est $T^c = \{t_1, t_4\}$. Le superviseur contrôle uniquement le déclenchement du processus de fabrication. Les opérations sur les deux produits, ne sont pas observable par le superviseur, il n'observe que l'arrivée et la sortie des pièces. L'ensemble des transitions inobservables est $T^{uo} = \{t_2, t_5\}$. Le graphe d'atteignabilité $RG(N, M_0)$ est donné à la figure 3.6.b.

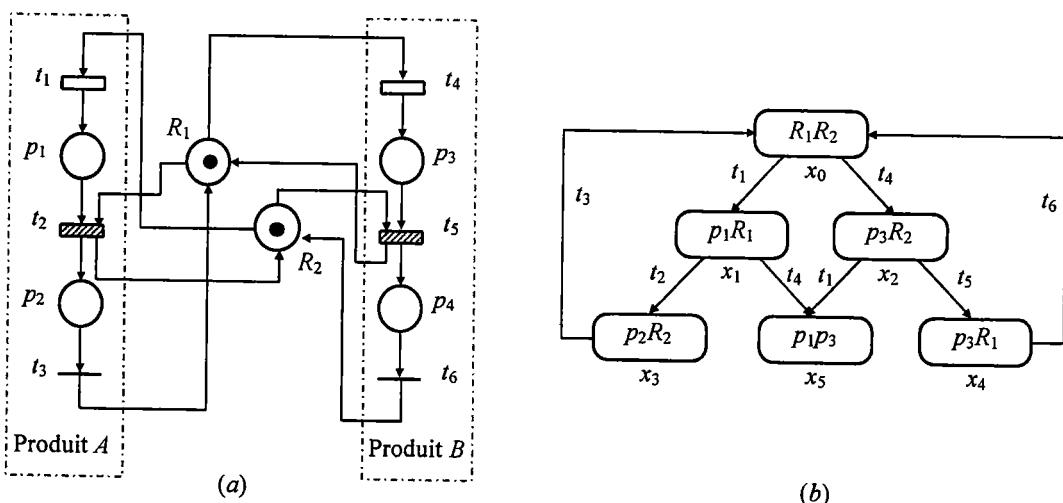


Figure 3.6. Système de production

(a) Modèle RDP (N, M_0)

(b) Graphe d'atteignabilité $RG(N, M_0)$

Pour déterminer le contrôleur RdP, nous allons appliquer notre approche de synthèse présentée dans ce chapitre. En présence de transitions inobservables, nous devons construire le graphe d'atteignabilité observateur $RG^O(N, y_0)$. Pour se faire, nous utilisons l'algorithme 3.1.

Soit le macro-état initial ; $y_0 = R^{uo}(x_0) = \{x_0\}$.

- A partir du macro-état $y_0 = \{x_0\}$ (voir figure 3.7) :
Deux transitions observables t_1 et t_4 sont franchissables :

- $x_0[t_1] x_1$ alors il existe un macro-état y_1 tel que $y_0[t_1] y_1$ avec $y_1 = R^{uo}(x_1) = \{x_1, x_3\}$.
- $x_0[t_4] x_2$ alors il existe un macro-état y_2 tel que $y_0[t_4] y_2$ avec $y_2 = R^{uo}(x_2) = \{x_2, x_4\}$.

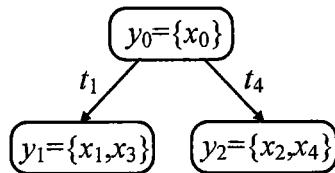


Figure 3.7. Macro-états atteignables à partir de y_0

- A partir du macro-état $y_1 = \{x_1, x_3\}$ (voir figure 3.8) :

Une transition observable t_4 est franchissable à partir de x_1 et une transition observable t_3 est franchissable à partir de x_3 :

- $x_1[t_4] x_5$ alors il existe un macro-état y_3 tel que $y_1[t_4] y_3$ avec $y_3 = R^{uo}(x_5) = \{x_5\}$.
- $x_3[t_3] x_0$ alors $y_1[t_3] y_0$.

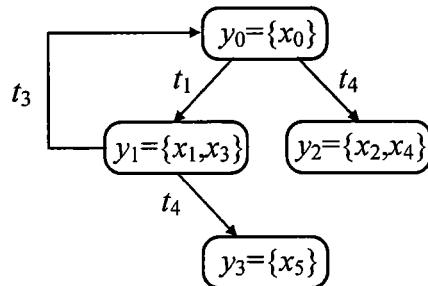


Figure 3.8. Macro-états atteignables à partir de y_1

- A partir du macro-état $y_2 = \{x_2, x_4\}$ (voir figure 3.9) :

Une transition observable t_1 est franchissable à partir de x_2 et une transition observable t_6 est franchissable à partir de x_4 :

- $x_2[t_1] x_5$ alors $y_2[t_1] y_3$.
- $x_4[t_6] x_0$ alors $y_2[t_6] y_0$.

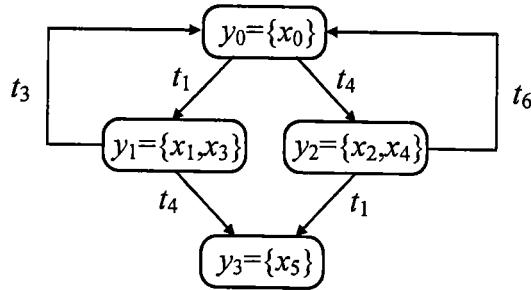


Figure 3.9. Macro-états atteignables à partir de y_2

- A partir du macro-état $y_3 = \{x_5\}$, aucune transition observable n'est franchissable. Le macro-état y_3 est un macro-état bloquant.

La construction du graphe d'atteignabilité observateur $RG^O(N, M_0)$ est terminé puisque tous les macro-états ont été explorés.

Construisons maintenant le graphe d'atteignabilité observateur raffiné $RG^{RO}(N, M_0)$ en intégrant les transitions inobservables entre les micro-états. $RG^{RO}(N, M_0)$ est donné à la figure 3.10.

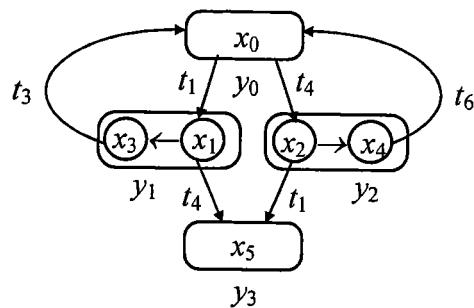


Figure 3.10. Graphe d'atteignabilité observateur raffiné $RG^{RO}(N, M_0)$

Pour obtenir le comportement maximum permisif non bloquant (figure 3.11), il faut éliminer de $RG^{RO}(N, M_0)$ le macro-état y_3 qui est un macro-état bloquant. L'ensemble des instances de séparation que nous devons considérer est $\Omega = \{(y_1, t_4), (y_2, t_1)\}$.

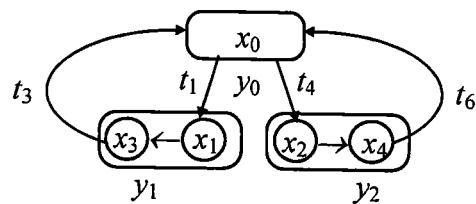


Figure 3.11. Graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, M_0)$

La synthèse des places de contrôle à intégrer au modèle RdP initial du procédé utilise l'algorithme 3.3 puisque la solution sous forme de places pures existe. Une seule condition de séparation est utilisée pour les deux instances $\{(y_1, t_4), (y_2, t_1)\}$:

$$(C_1): \quad y_{c0}(p_c) + C_c(p_c, t_1) + C_c(p_c, t_4) < 0$$

Le graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, M_0)$ contient deux cycles différents et donc deux équations de cycles qui sont les suivantes :

$$(C_2): \quad C_c(p_c, t_4) + C_c(p_c, t_6) = 0$$

$$(C_3): \quad C_c(p_c, t_1) + C_c(p_c, t_3) = 0$$

Le graphe d'atteignabilité observateur contrôlable $RG^{CO}(N, M_0)$ comporte trois macro-états admissibles, ce qui donne les trois conditions d'atteignabilité suivantes :

$$(C_4): \quad y_0 \rightarrow y_{c0}(p_c) \geq 0$$

$$(C_5): \quad y_1 \rightarrow y_{c0}(p_c) + C_c(p_c, t_1) \geq 0$$

$$(C_6): \quad y_2 \rightarrow y_{c0}(p_c) + C_c(p_c, t_4) \geq 0$$

Le système linéaire composé des conditions (C_1) - (C_6) admet une solution $C_c(p_c, .) = (-1, 0, 1, -1, 0, 1)$ avec $y_{c0}(p_c) = 1$ comme marquage initial de la place de contrôle p_c . Les transitions t_1 et t_4 sont ses deux transitions de sortie et t_3 et t_6 sont ses deux transitions d'entrée. Le réseau contrôlé est donné à la figure 3.12.

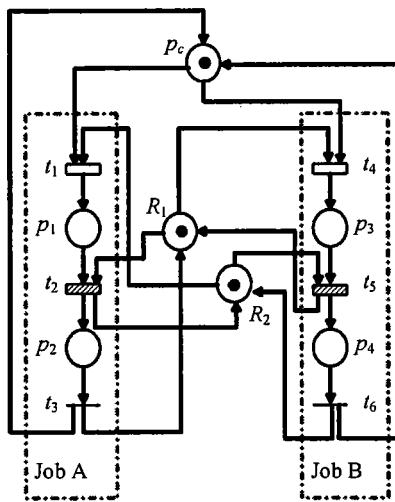


Figure 3.12. Réseaux contrôlé du système de production

3.6 Conclusion

Nous avons présenté dans ce chapitre une méthodologie optimale pour la synthèse des contrôleurs RdP pour résoudre les problèmes de type transitions d'états interdites en tenant compte de la contrainte de vivacité en présence de transitions inobservables. En effet, cette approche permet de déterminer un ensemble de places de contrôle à intégrer au modèle réseau de Petri initial du procédé à superviser.

Le graphe d'atteignabilité est utilisé pour modéliser le comportement d'un réseau de Petri et pour la synthèse de sa commande. En présence de transitions inobservables, l'état réel du système devient partiellement connu et le graphe d'atteignabilité ne peut plus être utilisé directement pour la synthèse de la commande. Un graphe observateur déduit du graphe d'atteignabilité, permet de connaître les différents états possibles suite au franchissement d'une transition observable. Pour la prise en compte de la contrainte de réversibilité, un graphe d'atteignabilité observateur raffiné est déduit.

A partir de ce le graphe et des spécifications d'états interdits ou de transitions d'état interdites, nous avons synthétisé un ensemble de places de contrôle à intégrer au modèle RdP du procédé partiellement observable à l'aide de la théorie des régions.

Chapitre 4

Caractérisation de l'existence des contrôleurs réseaux de Petri

Dans la première partie de ce chapitre, nous discutons de l'existence d'un contrôleur RdP pour des spécifications de type transitions d'états interdites. Les conditions nécessaires et suffisantes pour l'existence d'une place de contrôle pure ou impure résolvant une instance de séparation, dans le cas d'un modèle RdP totalement observable, sont d'abord présentées. Deux conditions supplémentaires, nécessaires mais non suffisantes pour l'existence d'un contrôleur RdP optimal, dues à la contrainte d'inobservabilité sont ensuite développées. Dans la deuxième partie de ce chapitre, nous proposons une approche pour résoudre le problème de transitions d'état interdites afin de contourner la non existence de contrôleur RdP pour certains problèmes. Si les deux conditions d'existence relatives à l'observabilité sont satisfaites, l'idée consiste à construire plusieurs places de contrôle quand une seule place ne permet pas de résoudre une instance de séparation. L'ensemble de ces places est appelé contrôleur RdP partiel. Les résultats de cette partie font l'objet d'une publication [ARX05].

4.1 Introduction

Nous avons présenté dans le chapitre précédent une approche basée sur la théorie des régions qui traite le problème des transitions d'états interdites et permettant la synthèse de contrôleurs réseaux de Petri. Néanmoins, un problème de transitions d'états interdites n'est pas toujours soluble par l'ajout d'un ensemble de places de contrôle qu'elles soient pures ou impures.

Dans ce chapitre, nous discutons d'abord de l'existence d'un contrôleur sous forme de places de réseaux de Petri pour des modèles totalement observables puis, nous évoquons l'influence de l'inobservabilité des événements sur l'existence de contrôleurs optimal.

4.2 Existence de contrôleurs RDP

Pour caractériser l'existence des contrôleurs RdP, nous devons introduire le concept de marquages de base.

4.2.1 Marquages de base

D'après des résultats connus de la théorie des graphes, les équations des cycles se ramènent en général aux équations des *cycles de base* [GM94]. Un cycle de base correspond à un arc n'appartenant pas à l'arbre de recouvrement du graphe appelé généralement co-arête. Etant donné que G est connexe, les cycles de base sont alors au nombre de $n_A - n_M + 1$, où n_A et n_M sont respectivement le nombre des arcs et des marquages du graphe. La détermination des cycles de base d'un graphe se fait en un temps polynomial. Le nombre n_C d'équations de cycle de base indépendantes est au plus égal au nombre des transitions $\text{card}(T)$.

Nous notons par *vecteurs d'incidence de base*, la base des solutions du système composé des équations indépendantes des cycles de base. Cette base a une dimension égale à $\text{card}(T) - n_C$.

Soit un modèle totalement observable RdP (N, M_0) et un comportement souhaité R . n_C est le nombre d'équations de cycles de base indépendantes (équation [3.2]) parmi les cycles de base de $R(N, M_0)$. Soit $B = (e_1, e_2, \dots, e_n)$ une base de l'espace des solutions des n_C équations. Rappelons que $\{e_1, e_2, \dots, e_n\}$ sont les vecteurs d'incidence de base. Donc, $n = \text{card}(T) - n_C$.

On a alors d'après les résultats de Ghaffari et al. [GRX03a], pour tout marquage M et toute place p , du modèle ou de contrôle, les résultats suivants.

Lemme 4.1 : Pour toute place p , du modèle ou de contrôle, il existe un vecteur $\mu(p)$ de réels tel que:

$$C(p, \cdot) \vec{\Gamma}_M = \mu(p)^T m$$

où $m = (e_1 \vec{\Gamma}_M, e_2 \vec{\Gamma}_M, \dots, e_n \vec{\Gamma}_M)$ est le marquage de base associé à M .

Lemme 4.2 : Pour toute place p , du modèle ou de contrôle, on a:

$$\forall M \in R, M(p) = M_0(p) + \mu(p)^T m.$$

Cette relation est immédiate en utilisant l'équation d'état des RdP et le lemme 4.1.

A l'aide des marquages de base, une caractérisation géométrique a été déterminée pour les comportements non réalisables par l'ajout de places de contrôle pures et/ou impures.

4.2.2 Condition pour l'existence du contrôleur RdP

Dans le cas d'un modèle RdP totalement observable, des conditions nécessaires et suffisantes pour l'existence du contrôleur RdP ont été présentées par Ghaffari et al. [GRX03]. Le théorème suivant fournit la condition nécessaire et suffisante pour l'existence d'une place de contrôle impure qui résout une instance de séparation d'événement donnée.

Théorème 4.1 Il existe une place de contrôle impure qui interdit une transition d'état $(M \xrightarrow{t} M')$ ssi le marquage de base m n'est pas une combinaison convexe des marquages de base correspondants aux marquages validant la transition t . Autrement dit, la relation suivante n'est pas vraie.

$$\exists \lambda \geq 0 \mid \sum_{k=1}^r \lambda_k = 1 \text{ et } m = \sum_{M_k \in R \setminus M_t[t]} \lambda_k m_k$$

où r est le nombre des marquages validant t .

En utilisant, le lemme 4.2 et le théorème 4.1, on a de façon immédiate la condition suffisante suivante pour l'existence de place de contrôle impure.

Corollaire 4.1 : Il existe une place de contrôle impure p_c qui interdit le franchissement de t à partir de M si M n'est pas une combinaison convexe des marquages admissibles validant t .

Pour l'existence d'une place de contrôle pure résolvant une instance de séparation d'événement donnée, le théorème suivant fournit la condition nécessaire et suffisante.

Théorème 4.2. Il existe une place de contrôle pure qui interdit une transition d'état $(M \xrightarrow{t} M')$ ssi le marquage de base m' (correspondant au marquage M') n'est pas une combinaison convexe de tous les marquages admissibles de R . Autrement dit, la relation suivante n'est pas vraie:

$$\exists \lambda \geq 0 \mid \sum_{k=1}^r \lambda_k = 1 \text{ et } m' = \sum_{M_k \in R} \lambda_k m_k$$

où r est le nombre de marquages dans R .

De même que pour les places de contrôle impures, en utilisant le lemme 4.2 et le théorème 4.2, on obtient une condition suffisante d'existence de place pure interdisant une transition d'état donnée.

Corollaire 4.2 : Il existe une place de contrôle pure p_c qui interdit une transition d'état $(M \xrightarrow{t} M')$ si M' n'est pas une combinaison convexe des marquages de R .

On note que la condition du corollaire 4.2 est seulement suffisante mais pas nécessaire pour l'existence de places de contrôle impures. Dans certains cas, la contrainte d'inobservabilité des événements fait qu'un contrôleur RdP optimal n'existe pas. Nous présenterons dans la suite de ce chapitre les deux conditions relatives à l'observabilité pour l'existence du contrôleur RdP.

4.2.3 Observabilité et existence du contrôleur RdP optimal

L'inobservabilité de certaines transitions conduit à un langage de transitions observables qui n'est pas un langage RdP, c'est-à-dire ne respectant pas les propriétés de base telles que les équations d'état. Nous présentons ici deux cas.

4.2.3.1 Cas des macro-états correspondant au même vecteur de tirs observable mais ayant un contrôle différent

Considérons le problème de contrôle de la figure 4.1.a. Il s'agit d'un problème de transition d'état interdite où dans le modèle RdP (N, M_0) on désire interdire le franchissement de la transition T quand les places p_3 et p_5 sont marquées. C'est-à-dire inhiber T à partir du macro-état y_3 et l'autoriser dans les autres macro-états du modèle. Le graphe d'atteignabilité observateur contrôlable représentant le comportement observable souhaité est montré à la figure 4.1.b.

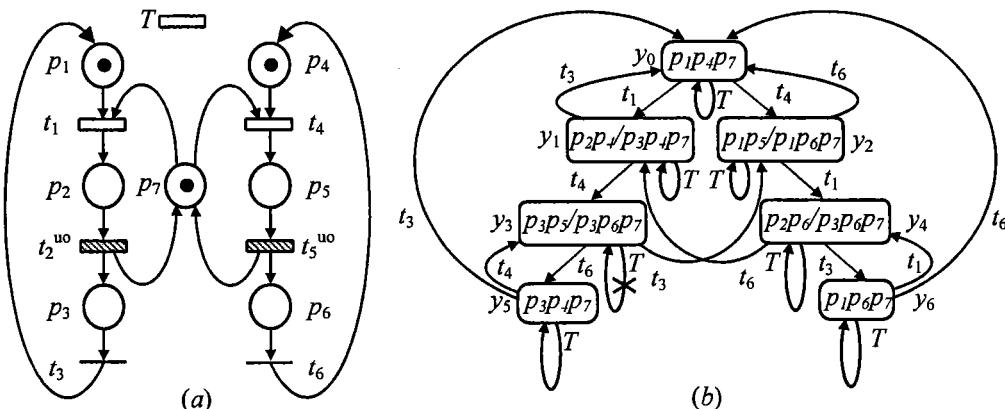


Figure 4.1. Exemple 1 de problème de transition d'état interdite

L'unique transition d'état à interdire pour réaliser le comportement souhaité est $(y_3 \xrightarrow{T} y_3)$.

La condition [3.5] du chapitre 3 relative à la possibilité de franchir T à partir du macro-état y_8 est :

$$(4.i) \quad (y_4 \xrightarrow{T} y_4) : y_{c0}(p_c) + C_c(p_c, t_4) + C_c(p_c, t_1) \geq C_c^-(p_c, T).$$

Cependant, la condition de séparation [3.6] du chapitre 3 relative à l'instance de séparation est :

$$(4.ii) \quad (y_3 \xrightarrow{T} y_3) : y_{c0}(p_c) + C_c(p_c, t_1) + C_c(p_c, t_4) < C_c^-(p_c, T)$$

Les deux conditions (4.i) et (4.ii) sont contradictoires. Par conséquent, il n'existe pas une place de contrôle pure ou impure qui résout ce problème de transitions d'état interdites. Le corollaire suivant rajoute une condition nécessaire pour l'existence du contrôleur RdP optimal.

Théorème 4.3. *Il existe une place de contrôle p_c qui interdit le franchissement d'une transition t à partir d'un macro-état y_1 tel que $y_0[\sigma_1] y_1$ si il n'y a pas un macro-état y_2 tel que $y_0[\sigma_2] y_2$ et $\bar{\sigma}_1^\circ = \bar{\sigma}_2^\circ$ à partir duquel t est franchissable.*

Preuve :

Considérons les macro-états y'_1 et y'_2 tels que $y_1[t] y'_1$ et $y_2[t] y'_2$. D'après le théorème 3.1 du chapitre 3, Le comportement désiré peut être obtenu par l'ajout de places pures de contrôle au réseau RdP (N, M_0) initial si et seulement si il existe une solution $(y_{c0}(p_c), C_c(p_c, .))$ qui satisfait les condition [3.2], [3.3] et [3.4] pour toute instance de séparation de Ω . Cependant, la condition d'atteignabilité [3.3] de $y'_2 \Rightarrow y_{c0}(p_c) + C_c(p_c, .) \bar{\sigma}_2^\circ + C_c(p_c, t) \geq 0$ et la condition de séparation [3.4] de l'instance $(y_1 \xrightarrow{t} y'_1) \Rightarrow y_{c0}(p_c) + C_c(p_c, .) \bar{\sigma}_1^\circ + C_c(p_c, t) < 0$. C'est deux conditions sont contradictoires si $\bar{\sigma}_1^\circ = \bar{\sigma}_2^\circ$. Il n'existe donc pas de places de contrôle pures pour résoudre ce problème.

De la même manière, à partir du théorème 3.2, Le comportement désiré peut être obtenu par l'ajout de places de contrôle impures au réseau RdP (N, M_0) initial si est seulement si il existe une solution $(y_{c0}(p_c), C_c(p_c, .), C_c^-(p_c, t))$ qui satisfait les condition [3.2], [3.3], [3.5] et [3.6] pour toute instance de séparation de Ω . La condition [3.5] $\Rightarrow y_{c0}(p_c) + C_c(p_c, .) \bar{\sigma}_2^\circ \geq C_c^-(p_c, t)$, et la condition [3.6] $\Rightarrow y_{c0}(p_c) + C_c(p_c, .) \bar{\sigma}_1^\circ < C_c^-(p_c, t)$. C'est deux conditions sont contradictoires si $\bar{\sigma}_1^\circ = \bar{\sigma}_2^\circ$. Il n'existe donc pas de places de contrôle impures pour résoudre le problème.

□

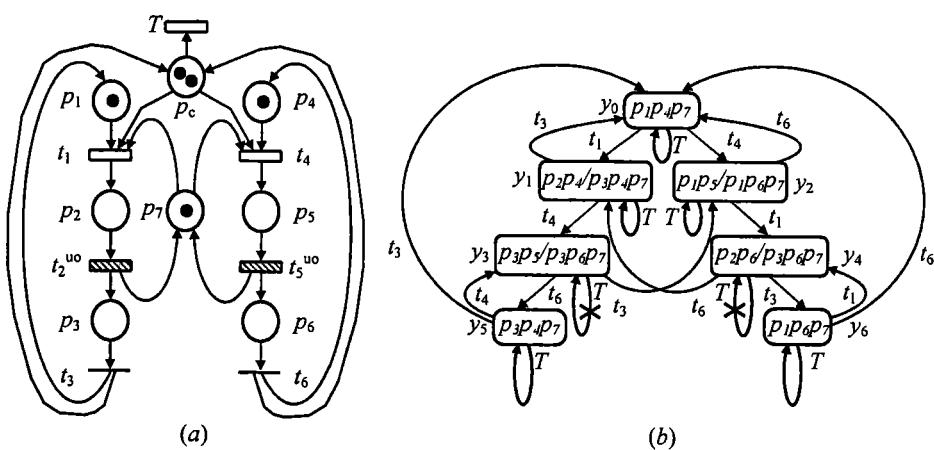


Figure 4.2. Réseau contrôlé du problème de contrôle de la figure 4.1.

Néanmoins un contrôleur plus restrictif pour ce problème de transition d'état interdite existe. La politique de commande à adapter, consiste à appliquer à y_4 le même contrôle que celui appliqué à y_3 , c'est à dire inhiber T à partir du macro-état y_4 . Le réseau contrôlé est donné dans la figure 4.2. Le contrôleur ainsi obtenu est optimal au sens des places de contrôles mais sous optimal par rapport aux solutions utilisant les langages formels et les automates, car le nombre d'états admissibles est plus réduit.

D'une manière générale, nous appliquons la même politique de commande aux macro-états atteignables à partir du macro-état initial par un même vecteur de tirs observable.

4.2.3.2 Cas des équations de cycle n'admettant que zéro comme solution

La non existence d'un contrôleur RdP optimal pour le problème de contrôle présenté ci-dessus est due à la contrainte d'inobservabilité de certains événements du procédé. À travers l'exemple suivant, nous présenterons un second cas de figure où la contrainte d'inobservabilité fait que les équations de cycle [3.2] n'admettent que zéro comme unique solution pour $C_c(p_c, \cdot)$. Par conséquent, aucune place de contrôle ne peut être trouvée.

Considérons le modèle RdP et son graphe d'atteignabilité observateur contrôlable donné par la figure 4.3. Le problème de contrôle consiste à interdire le franchissement de la transition T quand la place p_4 est marquée, c'est-à-dire inhiber T à partir de y_2 et l'autoriser dans les autres macro-états du modèle.

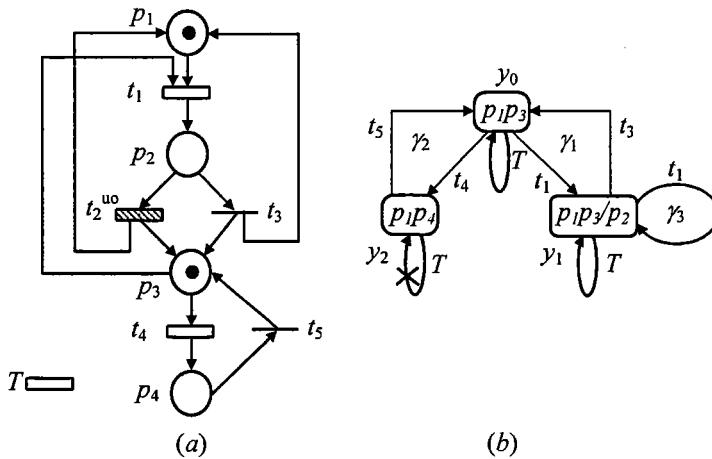


Figure 4.3. Exemple 2 de problème de transition d'état interdite

L'utilisation de la théorie des régions pour la détermination de places de contrôle afin de résoudre ce problème de transition d'état interdite nous donne :

- quatre équations de cycle :

$$(4.iii) \quad \gamma_1 : C_c(p_c, t_1) + C_c(p_c, t_3) = 0$$

$$(4.iv) \quad \gamma_2 : C_c(p_c, t_4) + C_c(p_c, t_5) = 0$$

$$(4.v) \quad \gamma_3 : C_c(p_c, t_1) = 0$$

$$(4.vi) \quad \gamma_4 : C_c(p_c, T) = 0$$

- cinq conditions d'atteignabilité [3.3] et [3.5] du chapitre 3 :

$$(4.vii) \quad y_0 : y_{c0}(p_c) \geq 0$$

$$(4.viii) \quad y_1 : y_{c0}(p_c) + C_c(p_c, t_1) \geq 0$$

$$(4.ix) \quad y_2 : y_{c0}(p_c) + C_c(p_c, t_4) \geq 0$$

$$(4.x) \quad (y_0 \xrightarrow{T} y_0) : y_{c0}(p_c) \geq C_c^-(p_c, T)$$

$$(4.xi) \quad (y_1 \xrightarrow{T} y_1) : y_{c0}(p_c) + C_c(p_c, t_1) \geq C_c^-(p_c, T)$$

- et une condition de séparation [3.6] du chapitre 3 :

$$(4.xii) \quad (y_2 \xrightarrow{T} y_2) : y_{c0}(p_c) + C_c(p_c, t_4) < C_c^-(p_c, T)$$

Le système constitué par les conditions (4.iii)- (4.xii) peut être résolu par l'ajout d'une seule place de contrôle impure p_c telle que $C_c(p_c, t_4) = -1$, $C_c(p_c, t_5) = 1$, $C_c(p_c, T) = 0$, $C_c^-(p_c, T) = 1$ et $y_{c0}(p_c) = 1$. Le modèle contrôlé est donné par la figure 4.4.

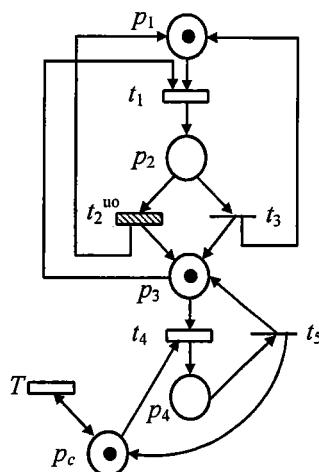


Figure 4.4. Une solution avec une place impure du problème de la figure 4.2

Considérons maintenant le même modèle RdP mais avec la spécification d'interdire le franchissement de la transition T quand la place p_2 est marquée, c'est-à-dire inhiber T à partir de y_1 et l'autoriser dans les autres macro-états du modèle. Le graphe d'atteignabilité observateur contrôlable est donné par la figure 4.5.

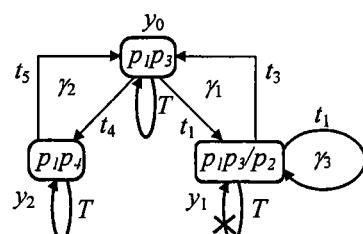


Figure 4.5. Exemple 3 de problème de transition d'état interdite

L'utilisation de la théorie des régions pour la détermination de places de contrôle afin de résoudre ce problème de transition d'état interdite nous donne :

- quatre équations de cycle :

$$(4.xiii) \quad \gamma_1 : C_c(p_c, t_1) + C_c(p_c, t_3) = 0$$

$$(4.xiv) \quad \gamma_2 : C_c(p_c, t_4) + C_c(p_c, t_5) = 0$$

$$(4.xv) \quad \gamma_3 : C_c(p_c, t_1) = 0$$

$$(4.xvi) \quad \gamma_4 : C_c(p_c, T) = 0$$

- cinq conditions d'atteignabilité [3.3] et [3.5] du chapitre 3 :

$$(4.xvii) \quad y_0 : y_{c0}(p_c) \geq 0$$

$$(4.xviii) \quad y_1 : y_{c0}(p_c) + C_c(p_c, t_1) \geq 0$$

$$(4.xix) \quad y_2 : y_{c0}(p_c) + C_c(p_c, t_4) \geq 0$$

$$(4.xx) \quad (y_0 \xrightarrow{T} y_0) : y_{c0}(p_c) \geq C_c^-(p_c, T)$$

$$(4.xxi) \quad (y_2 \xrightarrow{T} y_2) : y_{c0}(p_c) + C_c(p_c, t_4) \geq C_c^-(p_c, T)$$

- et une condition de séparation [3.6] du chapitre 3 :

$$(4.xxii) \quad (y_1 \xrightarrow{T} y_1) : y_{c0}(p_c) + C_c(p_c, t_1) < C_c^-(p_c, T)$$

Comme $C_c(p_c, t_1) = C_c(p_c, t_3) = 0$, les conditions (4.xx) et (4.xxii) sont contradictoires. Par conséquent, il n'existe pas une place de contrôle pure ou impure qui résout ce problème de transitions d'état interdites. Remarquons que si la transition t_2 était observable alors le problème de contrôle aurait une solution sous forme de place de contrôle pure telle que $C_c(p_c, t_1) = -1$, $C_c(p_c, t_2) = C_c(p_c, t_3) = 1$, $C_c(p_c, T) = -1$, et $M_{c0}(p_c) = 1$.

Considérons maintenant, le même problème de contrôle de l'exemple 3, mais en ajoutons une transition inobservable t_6 entre les places p_4 et p_3 (figure 4.6).

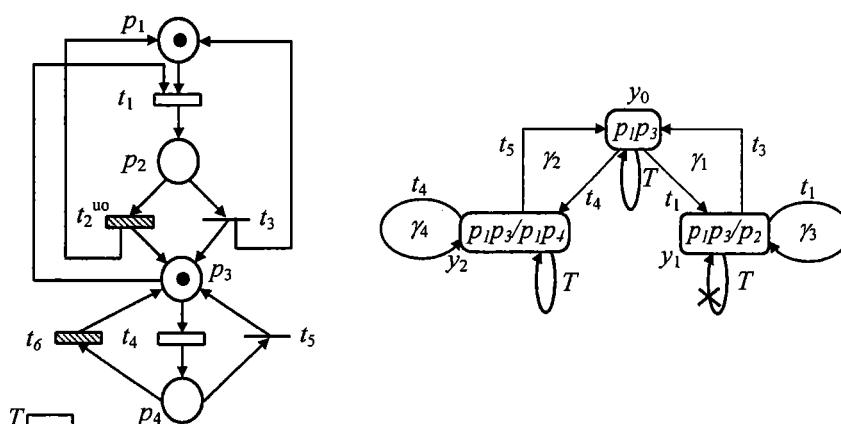


Figure 4.6. Exemple 4 de problème de transition d'état interdite

L'utilisation de la théorie des régions pour la détermination de places de contrôle afin de résoudre ce problème de transition d'état interdite nous donne cinq équations de cycle :

$$(4.xxiii) \quad \gamma_1 : C_c(p_c, t_1) + C_c(p_c, t_3) = 0$$

$$(4.xxiv) \quad \gamma_2 : C_c(p_c, t_4) + C_c(p_c, t_5) = 0$$

$$(4.xxv) \quad \gamma_3 : C_c(p_c, t_1) = 0$$

$$(4.xxvi) \quad \gamma_4 : C_c(p_c, t_4) = 0$$

$$(4.xxvii) \quad \gamma_5 : C_c(p_c, T) = 0$$

A partir de là, nous pouvons conclure qu'il n'existe pas de place de contrôle pure ou impure pour résoudre ce problème de transition d'état interdite puisque $C_c(p_c, .) = \vec{0}$. On note par $\vec{0}$, le vecteur $n_t \times 1$ dont tous les éléments sont égaux à zéro où n_t est le nombre de transition du réseau.

Par ailleurs, le théorème suivant apporte une condition nécessaire pour l'existence du contrôleur RdP optimal.

Théorème 4.4 *S'il existe une place de contrôle p_c interdisant le franchissement d'une transition t à partir d'un macro-état y , alors l'ensemble des équations de cycle [3.2] admettent une solution pour $C_c(p_c, .) \neq \vec{0}$.*

Preuve :

Il est clair que si l'ensemble des équations de cycle [3.2] n'admettent que zéro comme unique solution pour $C_c(p_c, .)$ alors la place de contrôle p_c existe sauf qu'elle ne contrôle aucune transition et du fait, elle ne peut pas interdire le franchissement d'une transition t à partir d'un macro-état y .

□

Pour l'existence d'une place de contrôle pure ou impure afin d'inhiber une instance de séparation ($y \xrightarrow{T} y'$) où $y_0 [\sigma_1] y'$, deux conditions sont nécessaires mais non suffisantes :

C_1 : Il n'existe pas un macro-état y'' tel que $y_0 [\sigma_2] y''$ et $\bar{\sigma}_1^o = \bar{\sigma}_2^o$ à partir duquel T est franchissable.

C_2 : L'ensemble des équations de cycle [3.2] admettent une solution pour $C_c(p_c, .) \neq \vec{0}$.

Nous proposons dans la suite de ce chapitre une extension de l'approche basée sur la théorie des régions pour résoudre le problème de type PTEI à l'aide de places de contrôle quand un contrôleur unique n'existe pas. Cette approche s'applique que si et seulement si les conditions C_1 et C_2 sont satisfaites. Elle consiste à déterminer un ensemble de contrôleurs RdP partiels, oeuvrant conjointement, pour garantir le respect de la spécification du type PTEI. La synthèse et la coordination des contrôleurs RdP partiels dans le cas des SED totalement observables sont proposées par Ghaffari et al. [GRX03]. Pour les sections suivantes, nous proposons une extension de cette approche au cas des SED partiellement observables.

4.3 Synthèse de contrôleurs RdP partiels

Considérons un problème de type PTEI caractérisé par un modèle RdP(N, M_0), un comportement observable souhaité RG^{CO} et un ensemble d'instance de séparation Ω . S'il n'existe pas de contrôleur RdP permettant de résoudre la spécification PTEI, alors, il existe forcément une instance de séparation d'événement $s = (y \xrightarrow{T} y') \in \Omega$ telle que le système linéaire composé des équations des cycles [3.2], des contraintes d'atteignabilité [3.3], et de la condition de séparation d'événement relative à s n'admet pas de solution. Désormais, nous noterons ce système par $S_{RG}(s)$.

L'idée principale qui sous-tend la méthode présentée ici consiste à déterminer, non plus une seule place de contrôle pour interdire s , mais un ensemble de places de contrôle que l'on appellera *contrôleur partiel*.

Dans ce qui suit nous définissons un contrôleur partiel ainsi que le modèle du système contrôlé par des contrôleurs partiels.

4.3.1 Contrôleur partiel

Comme l'instance s ne peut pas être interdite quand toutes les autres transitions de RG^{CO} sont autorisées, il est alors possible qu'en restreignant l'ensemble des macro-états admissibles de RG^{CO} à un sous-ensemble r , une solution puisse être déterminée. En effet, cela revient à relâcher quelques contraintes d'atteignabilité qui définissent la place de contrôle. Cette solution est une place p_r dont le marquage reste positif pour tout macro-état appartenant à r . Pour avoir l'ensemble du comportement admissible, on détermine une seconde place $p_{\bar{r}}$ dont le marquage reste positif pour tout macro-état appartenant à $\bar{r} = RG^{CO} \setminus r$ et qui interdit aussi s . Ainsi, un macro-état est autorisé si au moins une des deux places l'autorise. Les deux places constituent un contrôleur partiel noté $C_p(s) = \{ p_r, p_{\bar{r}} \}$ permettant l'atteignabilité des macro-états de RG^{CO} et interdit s . Un tel contrôleur est défini comme suit :

Définition 4.1 Soit $\{p_1, \dots, p_k\}$ l'ensemble des places d'un contrôleur partiel $C_p(s)$. Il existe au moins une instance $s = (y \xrightarrow{T} y') \in \Omega$ et un ensemble $\{RG_1^{CO}, \dots, RG_k^{CO}\}$, tels que :

1. $\forall i = 1 \dots k, RG_i^{CO} \subset RG^{CO}$;
2. $\bigcup_{i=1 \dots k} RG_i^{CO} = RG^{CO}$;
3. $\forall i = 1 \dots k, \forall y \in RG_i^{CO}(N, M_0), y(p_i) \geq 0$;
4. $\forall i = 1 \dots k, y'(p_i) < C^-(p_i, T)$;

Ainsi, la synthèse des contrôleurs partiels revient à subdiviser le comportement observable souhaité RG^{CO} en plusieurs sous-comportements RG_i^{CO} , pas nécessairement disjoints, et déterminer pour chaque sous comportement RG_i^{CO} une place de contrôle p_i qui permet de réaliser RG_i^{CO} tout en interdisant l'instance s .

La loi de commande devient alors :

Une transition T contrôlable est validée par un contrôleur partiel C_p si et seulement si il existe une place $p \in C_p$ telle que $y(p) + C(p, T) \geq 0$.

En d'autres termes, une transition contrôlable T est validée dans un réseau (N, M_0) muni d'un contrôleur partiel C_p ssi :

- pour toute place $p \in N \cap \bullet T$, $y(p) \geq C(p, T)$;
- il existe au moins une place $p_i \in C_p(s)$, telle que $y(p_i) + C(p_i, T) \geq 0$;

Donc, la règle conventionnelle de franchissement dans les réseaux de Petri est appliquée seulement vis à vis des places du réseau non contrôlé. Tandis que l'existence d'une seule place de chaque contrôleur partiel, qui a un marquage positif ou nul après le franchissement d'une transition validée par les places du réseau non contrôlé, suffit pour franchir la transition. Il est clair qu'une telle définition du contrôle implique que l'on tolère un marquage négatif des places de contrôle dans le modèle contrôlé.

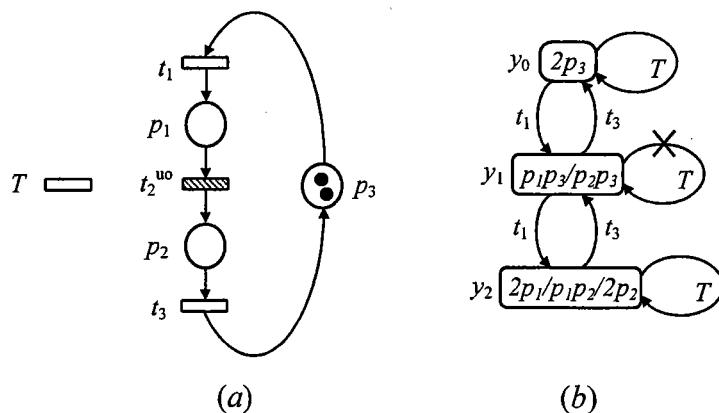


Figure 4.6. Exemple de PETI qui n'admet pas de solution avec une place de contrôle

Considérons le problème de contrôle de la figure 4.6.a. Il s'agit d'un PTEI, où on désire interdire le franchissement de la transition T quand $M(p_1)+M(p_2)=1$ et l'autoriser dans les autres états du modèle. Le comportement observable souhaité RG^{CO} est montré à la figure 4.6.b. Ce comportement n'est pas réalisable par l'ajout de places de contrôle impures. En effet, si une place de contrôle impure p_c existe alors, d'après le théorème 3.2, elle vérifie le système suivant :

- (4.i) $y_{c0}(p_c) \geq 0$
- (4.ii) $y_{c0}(p_c) + C_c(p_c, t_1) \geq 0$
- (4.iii) $y_{c0}(p_c) + C_c(p_c, T) \geq 0$
- (4.iv) $y_{c0}(p_c) + 2 \times C_c(p_c, t_1) \geq 0$
- (4.v) $y_{c0}(p_c) + 2 \times C_c(p_c, t_1) + C_c(p_c, T) \geq 0$
- (4.vi) $y_{c0}(p_c) \geq C_c^-(p_c, T)$
- (4.vii) $y_{c0}(p_c) + 2 \times C_c(p_c, t_1) \geq C_c^-(p_c, T)$
- (4.viii) $y_{c0}(p_c) + C_c(p_c, t_1) < C_c^-(p_c, T)$

Ce système n'admet pas de solution réalisable et donc il n'existe pas un contrôleur RdP unique pour résoudre ce problème de contrôle. Néanmoins, les deux conditions C_1 et C_2 sont satisfaites. Le réseau considéré admet donc un contrôleur constitué de contrôleur partiel que nous déterminerons dans la suite.

4.3.2 Réseau contrôlé

Considérons un modèle RdP (N, M_0) , un comportement observable souhaité RG^{CO} et un ensemble d'instance de séparation Ω composé de n instances. Considérons que parmi les n éléments de Ω il y a k instances pour lesquelles il n'existe pas de solution avec des places de contrôle. A partir de là, il faut déterminer k contrôleurs partiels $\{C_{p1}, \dots, C_{pk}\}$ associés à ces instances. Le modèle contrôlé est alors l'union de $(k+1)$ réseaux de Petri indépendants. k réseaux correspondant chacun au réseau contrôlé par un contrôleur partiel et un réseau qui correspond au réseau non contrôlé augmenté des places de contrôle résolvant les $(n - k)$ instances restantes de Ω .

Ces modèles s'exécutent de façon synchrone. Si une transition est franchie alors elle l'est dans tous les modèles en même temps. Le franchissement des transitions contrôlables validées dans le modèle sans contrôle se décide selon la logique suivante.

Une transition contrôlable, validée dans le modèle sans contrôle, est franchissable ssi elle est validée par tous les contrôleurs partiels.

Autrement, Le modèle contrôlé peut aussi être défini comme un seul RdP constitué du modèle initial (N, M_0) augmenté des k contrôleurs partiels et des places de contrôle résolvant les $(n - k)$ autres instances, où les places appartenant au même contrôleur sont différencierées par exemple par une couleur commune. Dans ce cas, pour franchir une transition contrôlable T , il faut qu'il existe au moins une place de chaque couleur qui retrouve un marquage positif ou nul en franchissant T .

4.3.3 Synthèse de contrôleurs RdP partiels

La différence entre un contrôleur RdP partiel avec des places pures et celui avec des places impures réside simplement dans les contraintes d'atteignabilité et de séparation à considérer dans le système $S_{RG}(s)$ pour séparer une transition d'état s . Nous développons dans ce qui suit la procédure de synthèse de contrôleurs partiels avec des places pures.

Rappelons que pour avoir une solution sous forme d'une place de contrôle pure p_c , $S_{RG}(s)$ doit contenir les équations indépendantes des cycles de base de RG^{CO} , les conditions d'atteignabilité des macro-états de RG^{CO} et la condition de séparation relative à $s = (y \xrightarrow{t} y')$. C'est à dire :

$$S_R(s) = \begin{cases} \sum_{t \in T} C_c(p_c, t) \cdot \vec{\gamma}[t] = 0, & \forall \gamma \in S \\ y_{c0}(p_c) + C_c(p_c, ..) \vec{\Gamma}_y \geq 0, & \forall y \in RG^{CO}(N, y_0) \\ y_{c0}(p_c) + C_c(p_c, ..) \vec{\Gamma}_y + C_c(p_c, t) < 0, & \forall (y \xrightarrow{t} y') \in \Omega \end{cases}$$

Si s ne peut pas être interdite par une place de contrôle pure alors il existe dans le système $S_{RG}(s)$ un sous-ensemble d'inégalités incompatibles avec la condition de séparation. La procédure de synthèse d'un contrôleur partiel est basée sur

l'identification de ce sous-ensemble de contraintes. Certaines de ces contraintes sont alors relâchées dans le but de déterminer un sous-système de $S_{RG}(s)$ qui admet une solution. Cette solution constitue alors une place de contrôle du contrôleur partiel associé à s . L'algorithme présenté ci-dessous, résume la procédure de synthèse de toutes les places de contrôle d'un contrôleur partiel.

Algorithme 4.1: Synthèse d'un contrôleur partiel $C_p(s)$ correspondant à une transition d'état interdite s .

Soit $i = 1 \dots n$ le compteur de places de contrôle dans le contrôleur $C_p(s)$. L désigne la liste des conditions d'atteignabilité appartenant à l'ensemble des contraintes incompatibles de $S_{RG}(s)$.

1. *Initialisation: $i = 1$, $RG_i^{CO} = RG^{CO}$ et $L_i = L = \emptyset$.*
2. *Résoudre $S_{RGi}(s)$. Si une solution existe aller à 6. Sinon aller à 3.*
3. *Identifier l'ensemble E des contraintes incompatibles de $S_{RGi}(s)$. Ajouter à L_i la liste des conditions d'atteignabilité appartenant à E .
Soit $S_{RGi}(s) = S_{RGi}(s) \setminus L_i$.*
4. *Résoudre $S_{RGi}(s)$. Si $S_{RGi}(s)$ n'a pas de solution aller à 3. Sinon aller à 5.*
5. *Pour toute condition $l_{ij} \in L_i$ faire:*
 - 5.1. $S_{RGi}(s) = S_{RGi}(s) \cup \{l_{ij}\}$.
 - 5.2. *Résoudre $S_{RGi}(s)$.
Si une solution existe alors $L_i = L_i \setminus \{l_{ij}\}$. Sinon $S_{RGi}(s) = S_{RGi}(s) \setminus \{l_{ij}\}$.*
6. *Soit p_i la solution de $S_{RGi}(s)$. Si $L_i = \emptyset$ alors aller à 8. Sinon aller à 7.*
7. *$S_{RGi}(s)$ est le système linéaire contenant les équations de cycle, la condition de séparation et les conditions d'atteignabilité de L_i .
Faire $i = i + 1$ puis aller à 2.*
8. $k = i$ et $C_p(s) = \{p_i, i = 1 \dots k\}$.

Les contraintes incompatibles dans un système linéaire $S_{RG}(s)$ sont identifiées à l'étape 3. Mais, toutes ces contraintes ne peuvent pas être relâchées. Seule la relaxation des conditions d'atteignabilité est autorisée. Il est d'abord clair que la condition de séparation relative à s doit être vérifiée par toute place de contrôle de $C_p(s)$. Il en est de même pour les équations de cycle des cycles de base de RG^{CO} . En effet, en absence de contraintes relatives aux équations de cycle, la solution du système linéaire est une place de contrôle pouvant avoir deux marquages différents correspondant au même marquage dans le réseau sans contrôle. Le comportement du système contrôlé risque dans ce cas d'être différent du comportement souhaité RG^{CO} . Il est aussi possible, dans le cas de la synthèse du contrôleur partiel, que le même macro-état soit en même temps autorisé et interdit par la place en question.

L'étape d'identification et de relaxation de conditions d'atteignabilité incompatibles se fait de façon itérative jusqu'à déterminer un sous-système de $S_{RG}(s)$ qui est réalisable.

Une fois un sous-système de $S_{RG}(s)$ réalisable est identifié, dans l'étape 5, on cherche à rajouter les conditions d'atteignabilité relâchées une à la fois et à tester à

chaque fois la faisabilité du système linéaire résultant. Ces conditions sont rajoutées dans un ordre aléatoire. Jusqu'à identifier le plus grand sous-système réalisable de $S_{RG}(s)$, notons-le $S_{RG1}(s)$, et un ensemble de conditions d'atteignabilité qui rendent irréalisable $S_{RG1}(s)$.

$S_{RG1}(s)$ contient au moins une condition d'atteignabilité, en plus des équations de cycle et de la condition de séparation.

Soit p_1 une solution de $S_{RG1}(s)$. Toutes les conditions d'atteignabilité qui ont été relâchées pour obtenir $S_{RG1}(s)$ sont maintenant considérées, avec les équations de cycle et la condition de séparation de s , dans un autre sous-système, $S_{RG2}(s)$ (étape 7). Si $S_{RG2}(s)$ est réalisable et p_2 est une solution de $S_{RG2}(s)$, alors la procédure s'arrête et le contrôleur partiel $C_p(s)$ est donné par $C_p(s) = \{p_1, p_2\}$. Sinon, la procédure décrite ci-dessus est réitérée avec $S_{RG}(s) = S_{RG2}(s)$.

L'algorithme 4.1 donne une solution en un nombre fini d'itérations, puisque le nombre de contraintes d'atteignabilité dans un système $S_{RG}(s)$ est nécessairement fini. Le nombre de places de contrôle générées est alors au pire égal au nombre de contraintes d'atteignabilité. Mais, en pratique, ce nombre est beaucoup plus petit.

Soit maintenant un problème PTEI quelconque à résoudre en interdisant les transitions d'état d'un ensemble Ω . L'algorithme suivant résume la synthèse de contrôleurs RdP pour toutes les instances s de Ω .

Algorithme 4.2: Synthèse de contrôleurs partiels pour un PTEI donné.

Soit RG^{CO} le comportement observable souhaité d'un réseau (N, M_0) et Ω l'ensemble des transitions d'état à interdire par éventuellement un ensemble de contrôleurs partiels C_p .

1. *Initialisation:* $C_p = \emptyset$.
2. *Pour tout* $s_i \in \Omega$ *faire:*
 - 2.1. *Pour tout contrôleur* $C_{p_j} \in C_p$, *vérifier si* C_{p_j} *résout* $S_R(s_i)$. *Si oui aller à 2. Sinon aller à 2.2.*
 - 2.2. *Résoudre* $S_R(s_i)$.
Si une solution P_i *existe, alors* $C_{p_i} = \{P_i\}$. *Ajouter* C_{p_i} *à* C_p .
Sinon aller à 2.3.
 - 2.3. *Construire le contrôleur partiel* C_{p_i} *en utilisant l'algorithme 4.1.*
3. *Éliminer les contrôleurs partiels redondants de* C_p .

Appliquons maintenant l'algorithme 4.2 pour résoudre l'exemple du problème de contrôle de la figure 4.6. Nous présentons dans la figure 4.7, une solution à ce problème sous forme d'un contrôleur avec deux places de contrôle p_{c1} et p_{c2} .

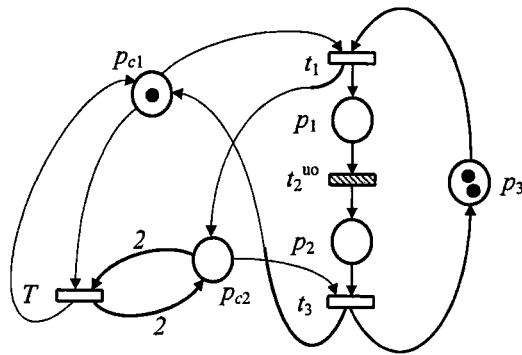


Figure 4.7. Solution du problème de la figure 4.6 avec un contrôleur partiel

La place p_{c1} satisfait les conditions (4.i), (4.ii), (4.iii), (4.vi) et (4.viii). Par contre, La place p_{c2} satisfait les conditions (4.i), (4.ii), (4.iv), (4.v), (4.vii) et (4.viii). Ainsi, les deux places interdisent la transition d'état s , mais chacune, considérée seule, permet de réaliser un sous-comportement de RG^{CO} , comme le montre la figure 4.8.

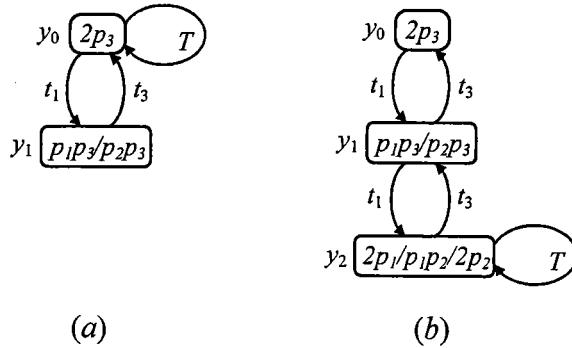


Figure 4.4. (a) Comportement du réseau contrôlé uniquement par p_{c1}
(b) Comportement du réseau contrôlé uniquement par p_{c2}

Dans cet exemple, le modèle contrôlé est constitué d'un seul RdP correspondant à l'unique contrôleur partiel de la solution.

4.4 Conclusion

Nous avons traité dans ce chapitre le problème d'existence d'un contrôleur RdP pour des spécifications de type transitions d'états interdites. Les conditions nécessaires et suffisantes pour l'existence d'une place de contrôle pure ou impure résolvant une instance de séparation d'événement donnée dans le cas d'un modèle RdP totalement observable sont d'abord abordées. Deux conditions supplémentaires, nécessaires mais non suffisantes pour l'existence d'un contrôleur RdP optimal et dues à la contrainte d'inobservabilité sont ensuite développées. Pour les modèles respectant ces deux contraintes, nous avons présenté une solution en terme de places de contrôle pour résoudre le problème de transitions d'état interdites. Pour une instance de séparation donnée, l'idée consiste à construire plusieurs places de contrôle quand une place unique n'existe pas. Chaque place permet au modèle d'atteindre un sous- ensemble de macro-

états admissibles. Dans ce cas, il s'agit de problème de synthèse pour les PTEI basé sur les contrôleurs partiels et agissant en un "OU" logique.

Chapitre 5

Commande optimale en Grafcet

Une approche originale de synthèse de la commande pour les systèmes à événements discrets est proposée dans ce chapitre. Cette approche a pour objectif principal de déterminer formellement un ensemble de variables de contrôle à ajouter aux modèles Grafcets de commande du procédé et de générer les Grafcets de supervision correspondant. La détermination de cet ensemble de variables de contrôle est basée sur l'utilisation d'une nouvelle interprétation de la théorie des régions. Les résultats de cette partie ont fait l'objet de la publication [AR04]

5.1 Introduction

Dans ce chapitre, nous présentons une méthode formelle optimale et directe pour la synthèse et l'implémentation des superviseurs en Grafcet. La notion d'optimalité est liée au nombre d'états atteignables par le système en boucle fermée, c'est-à-dire sous supervision. La notion directe est liée à son aspect implémentation sur les automates programmables industriels (API). En effet, l'approche proposée permet de déterminer un ensemble de variables de contrôle à intégrer aux modèles Grafcets de commande initiaux. Ainsi, le procédé supervisé, respecte les spécifications. Le calcul des variables de contrôle repose sur le modèle automate du procédé, déduit de son modèle Grafcet de commande et l'utilisation d'une nouvelle interprétation de la théorie des régions.

Sur le plan implémentation de la commande par supervision, on constate un manque de contributions, néanmoins, il existe un certain nombre d'approches intéressantes dans la synthèse de la commande par supervision dont l'implémentation se fait directement sur les équipements programmables. On peut citer l'approche de Brandin et al. [BWB91], Arinez et al., [ABSB93], Balemi et al., [BHGWF93], Charbonnier et al., [CAD99], Ndjeb Hagbebell [Ndj99] et Zaytoon et Carré-Ménétrier [ZC01]. L'approche proposée par Brandin et al. [BWB91] ainsi que celle de Arinez et al. [ABSB93] sont à base d'automate. L'automate synthétisé représentant le fonctionnement désiré est traduit manuellement en langage à contacts sur les Automates Programmables Industriels (API). Dans l'approche présentée par Balemi et al. [BHGWF93], l'automate du fonctionnement désiré est implanté dans un ordinateur connecté au procédé à travers une interface. La supervision est faite en temps réel en comparant l'état du procédé avec celui de l'automate du fonctionnement désiré. Suite à cette comparaison, la commande est générée pour inhiber ou autoriser l'occurrence d'un événement. Les travaux présentés par Ndjeb Hagbebell [Ndj99] ainsi que Zaytoon et Carré-Ménétrier [ZC01] sont très intéressants et permettent de générer un modèle de supervision directement en GRAFCET dont l'implémentation sur les API est facile.

Plusieurs travaux se sont intéressés à la traduction du Grafcet en automate équivalent. Roussel et al. [ROU94] ont mis en place un algorithme d'extraction de l'automate des situations stables (ASS) à partir d'un modèle Grafcet. Implanté dans l'outil AGGLAE, l'algorithme s'appuie sur l'algèbre de Boole formalisant la notion de fronts sur les variables. L'automate obtenu est un automate mono-état et déterministe, il correspond à une machine de Mealy binaire, uniforme et complètement spécifiée. Les actions du modèle Grafcet sont associées aux situations stables accessibles et les identificateurs des transitions sont remplacés par les conditions de franchissement. Dans leur démarche de synthèse et implantation d'une commande supervisée par Grafcet, Charbonnier et al. [CAD99] traduisent les Grafcets partiels de commande ainsi que les Grafcets de supervision en automate événementiel à états finis. Dans cette approche, une hypothèse est faite lors de la génération du modèle automate du procédé, il s'agit de la non simultanéité des événements externes non corrélés.

Dans l'approche de synthèse de la commande que nous proposons, nous supposons que le modèle automate du procédé est déjà déduit à partir de son modèle Grafcet de commande selon la méthode proposée par Charbonnier et al. [CAD99]. La synthèse est alors faite sur l'automate équivalent déduit en intégrant les spécifications de commande et de sûreté. Les spécifications de commande sont conjuguées avec le modèle du procédé en utilisant la composition synchrone des automates. Les spécifications de

sûreté considérées sont de type états interdits. Ces états interdits sont à éliminer de l'automate résultant.

Le superviseur recherché doit alors respecter les spécifications et préserver la réversibilité du procédé supervisé tout en étant le plus permissif possible. Pour ce faire, une nouvelle interprétation de la théorie des régions a été élaborée afin de déterminer un ensemble de variables de contrôle à ajouter aux modèles de commande initiaux en Grafcet sans avoir recours à une nouvelle étape de traduction et d'implémentation en langage de commande.

Dans ce qui suit, nous définissons le problème de la commande par supervision. La section 5.3 présente les différentes étapes constituant la méthodologie de synthèse développée. La section 5.4 développe la nouvelle interprétation de la théorie des régions pour synthétiser un superviseur en Grafcet. Une illustration pratique de l'approche ainsi qu'un jeu de données sur d'autres exemples sont présentés à la section 5.5.

5.2 Synthèse de superviseur Grafcet

Dans ce chapitre, nous nous sommes intéressés au développement d'une méthode formelle de synthèse des contrôleurs à partir d'un automate à états finis déduit d'un Grafcet de commande du procédé. La déduction de l'automate est faite selon l'approche introduite par charbonnier [CAD99]. Le type de spécifications considéré dans notre approche est le problème d'états interdits connu sous le nom de spécifications de sûreté. Les spécifications de sûreté sont exprimées sous forme d'un ensemble Q_I d'états à interdire. L'approche de synthèse permet de déterminer formellement un ensemble de variables de contrôle en se basant sur l'utilisation d'une nouvelle interprétation de la théorie des régions. Les variables de contrôle déterminées sont associées aux modèles Grafcets de commande du procédé de telle sorte que le système en boucle fermée (procédé + superviseur) respecte les spécifications de sûreté ainsi que la propriété de non blocage. La propriété de non blocage se traduit par la possibilité d'atteindre un certains nombre d'états marqués, ou finaux, à partir de n'importe quel état. Dans notre démarche, nous nous restreignons au cas où l'état initial est le seul état marqué. La propriété de non blocage est ainsi équivalente à celle de réversibilité du procédé (Vue au chapitre 2).

Nous supposons dans cette approche que l'ensemble des événements Σ est subdivisé en deux sous-ensembles disjoints et totalement observables : $\Sigma = \Sigma_c \cup \Sigma_u$, où Σ_c (resp. Σ_u) représente l'ensemble des événements contrôlables (resp. incontrôlables). Le superviseur ne peut agir, autoriser ou interdire, que sur les événements contrôlables. Par conséquent, pour respecter les spécifications, il est nécessaire d'empêcher l'atteignabilité d'un ensemble d'états interdits, comportant tous les états dangereux à partir desquels le système peut évoluer par une séquence d'événements incontrôlables vers des états interdits.

Définition 5.1 Soient $G (Q_G, \Sigma, \delta, q_0)$ un automate à états finis et Σ_u un ensemble d'événements incontrôlables. Un état atteignable q est dit dangereux si et seulement si, il existe une séquence d'événements incontrôlables partant de q et menant à un état interdit. Formellement, l'ensemble des états dangereux est représenté par :

$$Q_D = \{q \in Q_G \mid \exists q' \in Q_I \wedge \sigma \in \Sigma_u^*, q[\sigma] q'\}. Il est évident que Q_I \subseteq Q_D.$$

Dans cette approche, nous imposons la condition de la réversibilité. En d'autres termes, à partir de tout état de G , il existe une séquence ramenant à l'état initial. Ainsi le comportement du procédé respectant les spécifications d'états interdits et préservant la réversibilité peut être défini comme suit.

Définition 5.2 *L'ensemble Q_A des états admissibles est le plus grand ensemble d'états atteignables tel que : i) $Q_A \cap Q_D = \emptyset$. ii) Il est possible d'atteindre l'état initial depuis n'importe quel état admissible sans passer par un état interdit. iii) Le passage à un état non admissible depuis un état admissible se fait par l'occurrence d'un événement contrôlable.*

Il est clair que Q_A est défini de telle sorte que, à partir de n'importe quel état de Q_A , le système ne peut pas évoluer de façon non contrôlable vers l'extérieur de Q_A . Les variables de contrôle à intégrer aux modèles Grafcets de commande du procédé permettent au système de rester dans l'ensemble des états admissibles Q_A . Il faut noter que Q_A représente le plus grand ensemble d'états admissibles et par conséquent $G_c(Q_A, \Sigma, \delta, q_0)$ est le comportement le plus permis possible.

Définition 5.3 *Un superviseur est le plus permis possible si et seulement si, tout état admissible de Q_A est atteignable et tout état dangereux de Q_D ne l'est pas sous supervision. Un tel superviseur est dit optimal.*

Pour satisfaire par la suite la propriété de non blocage, l'automate G_c doit être une composante fortement connexe (CFC) comportant l'état initial q_0 . L'ensemble des états bloquant est donc défini comme suit :

Définition 5.4 *Un état q_B est dit bloquant si et seulement si, q_B est un état de la CFC est mène d'une manière incontrôlable en dehors des états de la CFC. L'ensemble des états bloquant est noté Q_B . Formellement :*

$$Q_B = \{q \in \text{CFC} \mid \exists q' \notin \text{CFC} \wedge \sigma \in \Sigma_u^*, q[\sigma] q'\}$$

5.3 Méthodologie de synthèse de la commande par supervision

En se basant sur les Grafcets de commande (procédé + commande locale) du procédé, on génère l'automate à états finis équivalent. A partir de l'automate équivalent et connaissant l'ensemble des états interdits Q_I issu des spécifications de sûreté, on cherche à déterminer les variables de contrôle qu'il faut ajouter aux modèles Grafcets initiaux pour restreindre l'automate équivalent à G_c dont l'ensemble des états est Q_A . Ces variables de contrôle constituent la loi de commande à imposer au système pour respecter les spécifications.

L'approche proposée opère en deux phases. Une première phase, consiste à générer l'automate équivalent déduit des modèles Grafcets de commande du procédé non contrôlé pour déterminer l'ensemble des états admissibles Q_A . Puis, en phase deux, et en utilisant une nouvelle interprétation de la théorie des régions présentée à la section 5.4.2, des variables de contrôle sont déterminées pour assurer le comportement désiré.

La première phase de la méthodologie de synthèse peut être résumée dans l'algorithme suivant. Cette phase consiste à traduire les Grafcets de commande en automate équivalent puis d'identifier les états interdits depuis les spécifications de sûreté et de vivacité. L'algorithme de synthèse proposé par Kumar [Kum91], étendu au comportement admissible maximum permisif non bloquant, est ensuite utilisé afin de générer l'automate du superviseur.

Algorithme 5.1 : Détermination du comportement admissible maximum permisif non bloquant.

1- Traduire les Grafcets de commande du procédé en automate équivalent G .

2- Identifier l'ensemble des états interdits Q_I de G .

3- Identifier l'ensemble des états dangereux Q_D de G .

A partir des états interdits, une exploration par chaînage arrière de l'automate G est faite pour identifier les états dangereux. L'ensemble Q_D est mis à jour au fur et à mesure. Si q_0 est lui-même un état dangereux, alors le problème de la supervision n'admet pas de solution.

4- Déduire l'automate contrôlé G_c , à partir de G en supprimant l'ensemble des états dangereux Q_D .

5- Vérifier si G_c est une composante fortement connexe (CFC).

5.1- Si G_c est une CFC alors aller à 8.

5.2- Si G_c n'est pas CFC alors calculer la CFC.

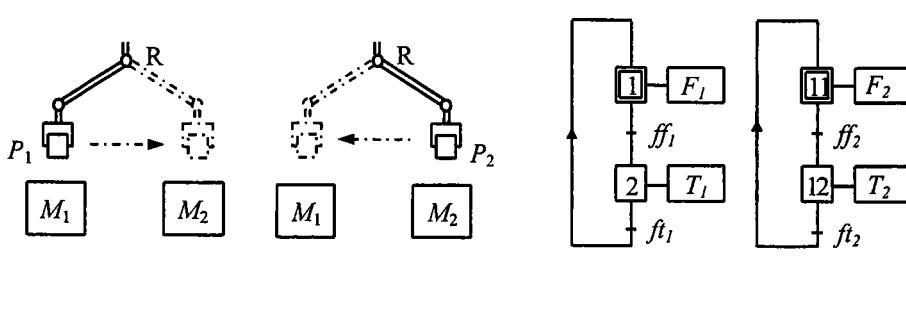
6- Remplacer G_c par la CFC calculée en 5.2 et remplacer Q_I par l'ensemble des états qui se trouvent en dehors de la CFC.

7- Aller à 3.

8- G_c est le comportement souhaité le plus permisif possible et non bloquant.

FIN

Exemple 5.1 Considérons un système de production composé de deux machines M_1 et M_2 ainsi qu'un robot R , fabriquant deux types de produit P_1 et P_2 . La fabrication de P_1 nécessite M_1 puis M_2 et celle de P_2 nécessite M_2 puis M_1 . Le robot R se charge des opérations de transfert de M_1 vers M_2 (figure 5.1.a) et de M_2 vers M_1 (figure 5.1.b). La demande de fabrication de P_1 et de P_2 arrive de façon aléatoire dans le système.



- (a) Cycle du produit P_1
 (b) Cycle du produit P_2
 (c) Grafcet de commande de la machine M_1
 (d) Grafcet de commande de la machine M_2

Figure 5.1. Système de production.

Spécification de commande :

SP_1 : Le traitement d'un produit P_k sur la machine M_j est lancé après son traitement sur la machine M_i avec $i \neq j$.

La traduction de la spécification SP_1 en automate est donnée par la figure 5.2 ci-dessous.

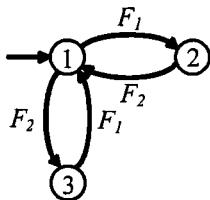


Figure 5.2. Traduction de la spécification en automate

Spécification de sûreté :

SP_2 : La machine M_i ne peut commencer le traitement d'un produit que lorsque la machine M_j se libère avec $i \neq j$.

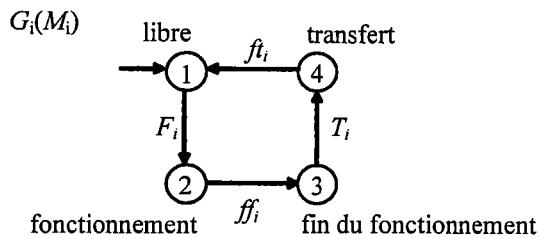
La spécification SP_2 permet d'éviter les situations de blocage dans le système et elle est motivée par le fait de supprimer les encours et gagner ainsi en espace. A SP_2 correspond un ensemble d'états interdits à déterminer.

Le lancement d'exécution de l'opération sur la machine M_i se fait suite à l'occurrence de l'événement F_i (événement contrôlable généré par l'automate programmable). L'événement incontrôlable ff_i indique que la machine M_i a fini la première phase d'usinage du produit P_i . Dans ce cas, l'API lance la phase de transfert (T_i). L'événement ft_i indique la fin de l'opération et par conséquent la réalisation du produit P_i . L'automate représentant le fonctionnement de la machine M_i est noté $G_i(M_i)$ (figure 5.3). L'approche de déduction de l'automate équivalent est similaire à celle proposée par [CAD99] avec l'hypothèse de la non simultanéité des événements externes. Le début du travail et le début du transfert correspondent à des sorties du système de commande. En revanche, la fin de l'opération et la fin du transfert qui sont des événements provenant des capteurs correspondent à des entrées du système de commande.

Comme le système de commande observe le procédé de manière asynchrone, alors nous considérons l'hypothèse de la non simultanéité des événements externes.

Il faut remarquer que les événements F_i et T_i sont des événements contrôlables et sont traduits dans le contexte Grafcet en actions tandis que ff_i et ft_i sont des événements incontrôlables dont on ne peut interdire l'occurrence. Dans le cadre d'une représentation par Grafcet, les événements contrôlables sont associés aux étapes car il est possible de les interdire. Pour les événements incontrôlables, ils sont associés aux transitions car ils sont le résultat d'une action et par conséquent impossible à inhiber. En autres termes, l'ensemble des événements contrôlables Σ_c est constitué des événements d'activation et

des événements de désactivation des ordres du Grafset. Les événements non contrôlables Σ_u sont associés aux variables d'entrée du Grafset.



$F_i \in \Sigma_c$: début d'exécution sur M_i $T_i \in \Sigma_c$: début du transfère à partir de M_i
 $f_{f_i} \in \Sigma_u$: fin d'exécution sur M_i $f_{t_i} \in \Sigma_u$: fin du transfère à partir de M_i

Figure 5.3. Modèle automate du fonctionnement de la machine M_i

L'automate résultant G du système intégrant la spécification de commande SP_I , est obtenu par la composition synchrone de $G_1(M_1)$, $G_2(M_2)$ et $G_3(SP_I)$ (Figure 5.4).

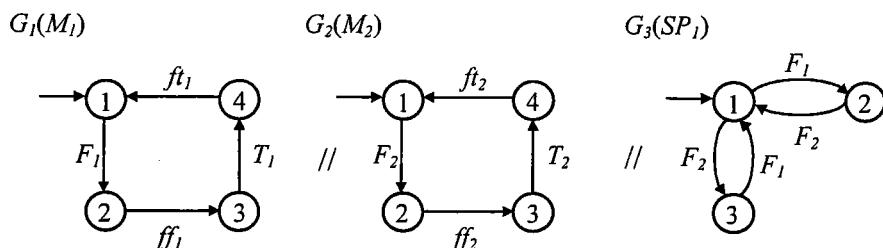


Figure 5.4. Composition synchrone des automates $G_1(M_1)$, $G_2(M_2)$ et $G_3(SP_I)$

$G = \bigcup_{i=1}^3 G_i$ comporte 48 états et 88 transitions d'états. G est donnée par la figure 5.5.

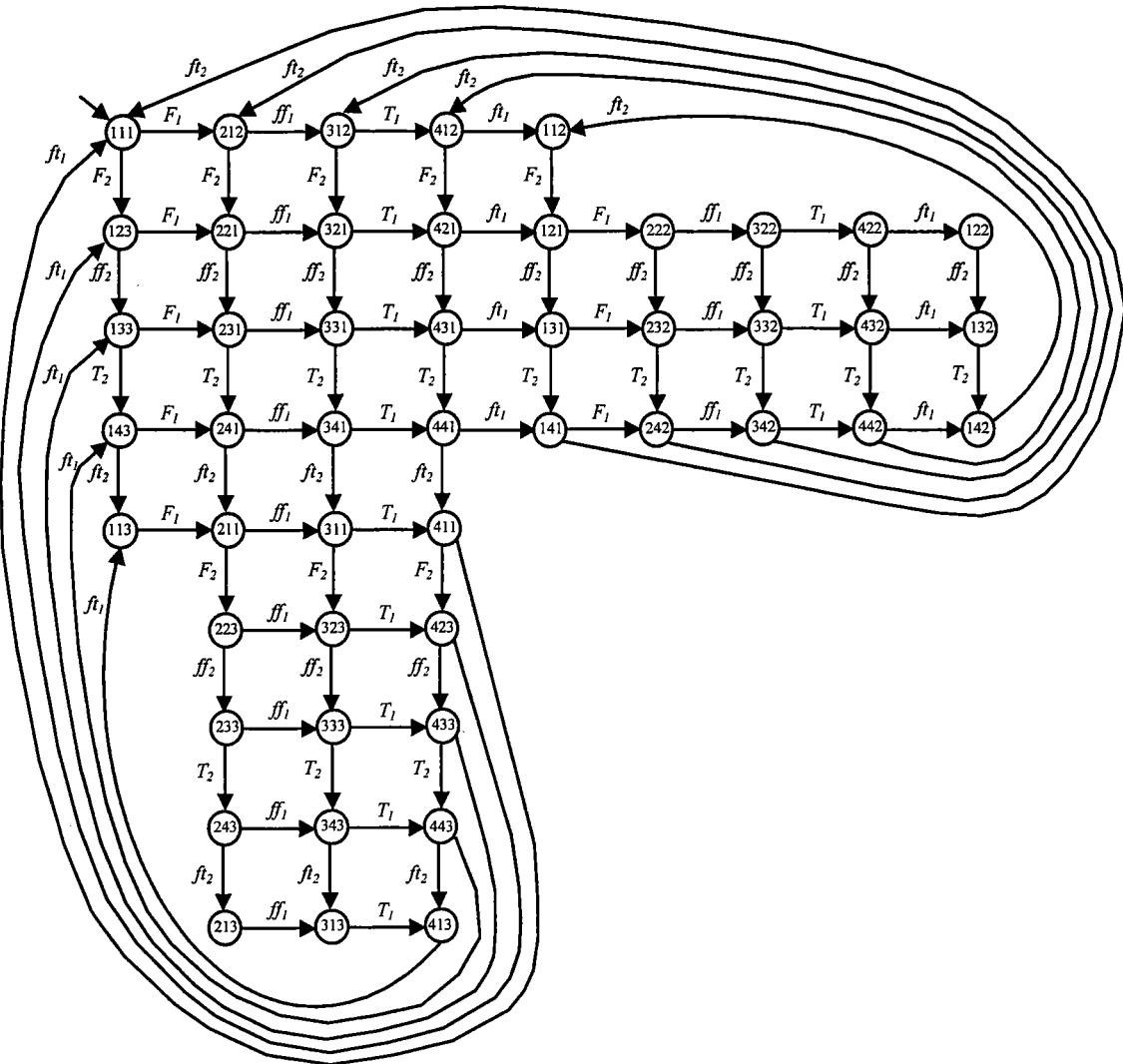


Figure 5.5. Modèle automatique $G = \sum_{i=1}^3 G_i$ de la figure 5.4

Pour faire respecter la spécification de sûreté SP_2 , on cherche à déterminer l'ensemble des états interdits. Dans cet exemple, l'ensemble Q_I est simple à déterminer puisqu'il s'agit de reconnaître les états de G pour lesquels les machines M_1 et M_2 sont toutes les deux engagées. En utilisant l'algorithme 5.1 de la méthode de synthèse, on détermine alors Q_A , le plus grand ensemble d'états admissibles, et par conséquent l'automate G_c préservant la réversibilité du procédé supervisé. L'ensemble des états interdits est donné par la figure 5.6.

L'application de l'algorithme 1 à l'exemple précédent en tenant compte de la spécification de sûreté SP_2 permet d'éliminer 33 états de G (voir figure 5.6).

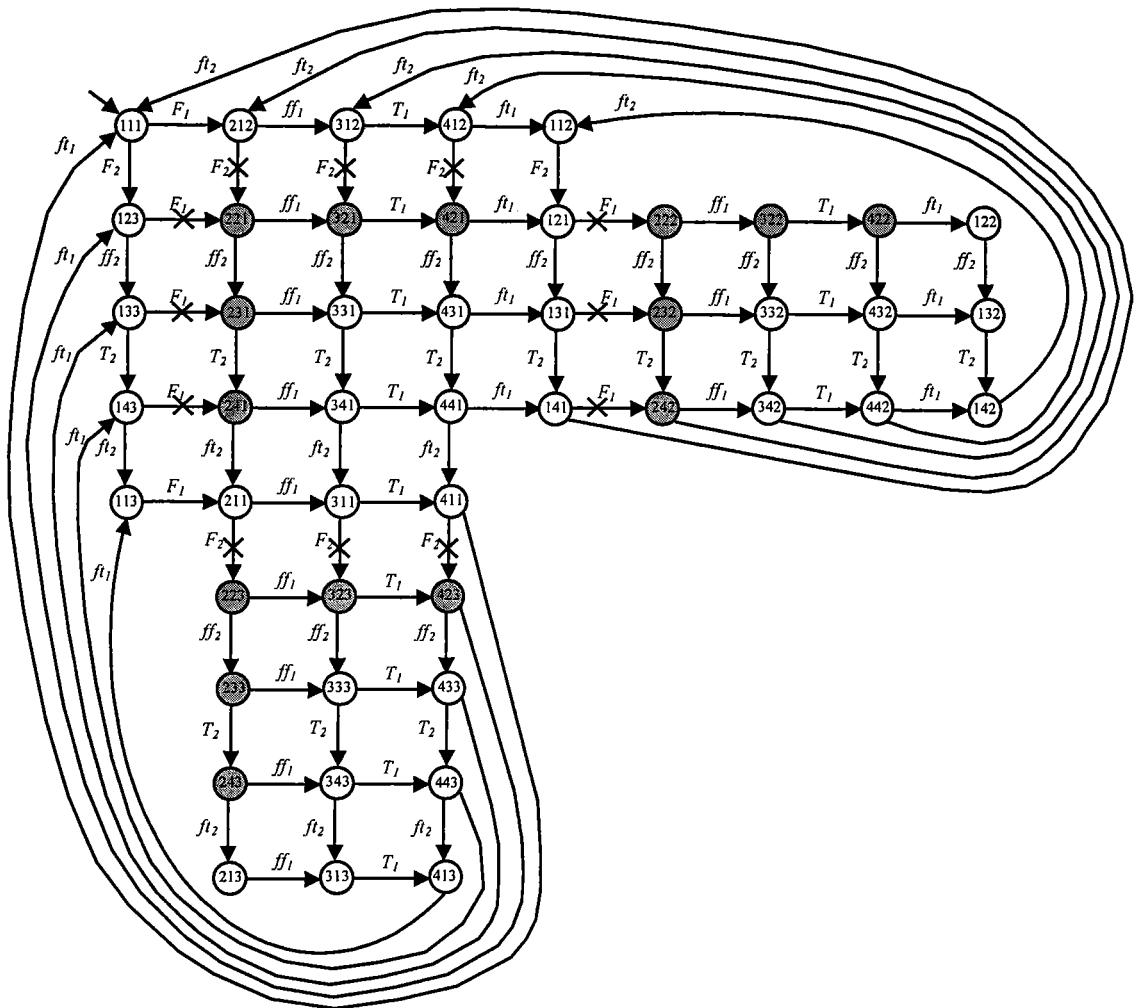


Figure 5.6. Etats interdits et instances à séparer

L'automate G_c est donné par la figure 5.7.

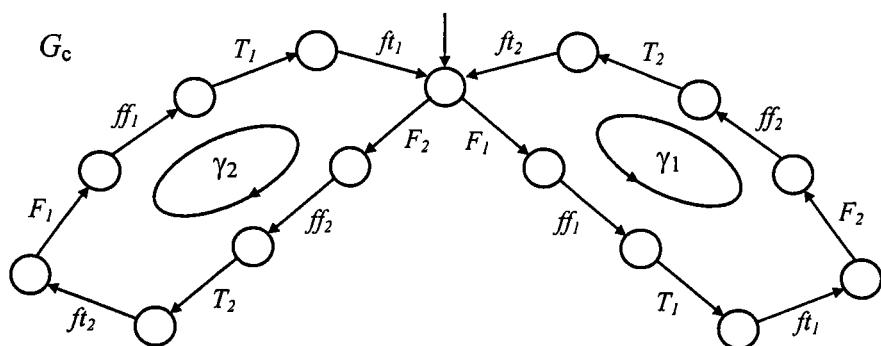


Figure 5.7. Modèle automate du fonctionnement désiré

5.4 Synthèse de la commande avec la théorie des régions

5.4.1 Nouvelle interprétation de la théorie des régions

L'objectif recherché par la méthode de synthèse présentée dans cette thèse est de synthétiser un superviseur en Grafset en utilisant une nouvelle interprétation de la théorie des régions. Cette nouvelle interprétation de la théorie des régions permet de déterminer un ensemble de variables de contrôle à ajouter aux modèles Grafsets de commande du procédé non supervisé de telle sorte que le fonctionnement en boucle fermée soit exactement l'automate G_c obtenu à partir de l'automate G sachant que G_c respecte les spécifications. Les variables de contrôles obtenues par la nouvelle interprétation de la théorie des régions permettent d'assurer le fonctionnement le plus permis possible. Ces variables de contrôle sont déterminées en fonction de l'ensemble des instances de séparation Ω avec :

$$\Omega = \{w_k = (q_i \xrightarrow{\alpha} q_j) / \alpha \in \Sigma_c \wedge q_i \in G_c \wedge q_j \in G - G_c\}.$$

Pour ce faire, on associe à chaque instance de séparation $w_k = (q_i \xrightarrow{\alpha} q_j) / w_k \in \Omega$, une variable de contrôle C_k . On définit par la suite une fonction de contrôle $U(C_k)$ comme suit :

$$U(C_k) / q_j = U(C_k) / q_i + C_k^\alpha$$

où

$U(C_k) / q_j$: la valeur de la fonction de contrôle à l'état q_j ,

$U(C_k) / q_i$: la valeur de la fonction de contrôle à l'état q_i ,

$C_k^\alpha \in \mathbb{Z}$: la variable d'incrémentation de $U(C_k)$ suite à l'occurrence de l'événement α .

En se basant sur les fondements de la théorie des régions, la nouvelle interprétation que nous proposons repose toujours sur la condition d'atteignabilité, l'équation de cycle et la condition de séparation. Dans la nouvelle interprétation de la théorie des régions, la loi de commande \tilde{U} est définie comme suit :

$$\tilde{U}(q_i \xrightarrow{\alpha(C_k)} q_j) = \begin{cases} 1 & \text{ssi } U(C_k) / q_j = U(C_k) / q_i + C_k^\alpha \geq 0 \quad (\alpha \text{ est autorisé}) \\ 0 & \text{ssi } U(C_k) / q_j = U(C_k) / q_i + C_k^\alpha < 0 \quad (\alpha \text{ est inhibé}) \end{cases}$$

5.4.1.1 La condition d'atteignabilité

La condition d'atteignabilité traduit le fait que tout état q_i de G_c est atteignable à partir de l'état initial q_0 . Par conséquent, le contrôle doit autoriser l'accès à cet état. Pour ce faire, la valeur de $U(C_k) / q_i$ doit être positive ou nulle. Ainsi la condition d'atteignabilité s'écrit sous la forme suivante :

$$U(C_k) / q_i = U(C_k) / q_0 + \sum_{\alpha_i \in s} C_k^{\alpha_i} \geq 0 \quad [5.1]$$

$U(C_k) / q_0$ représente la valeur initiale de la fonction de contrôle relative à l'état initial et s la séquence d'événements α_i menant de q_0 à q_i .

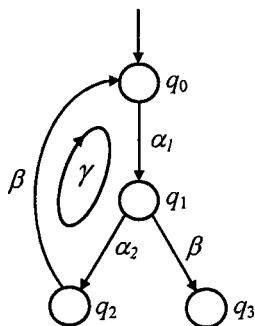


Figure 5.8. Automate A

Considérons l'automate A de la figure 5.8. Supposons dans cet exemple que tous les événements sont contrôlables ($\Sigma_c = \{\alpha_1, \alpha_2, \beta\}$) et que l'état q_3 est un état interdit ($Q_F = \{q_3\}$). Pour obtenir le comportement admissible, le contrôle doit interdire l'événement β à partir de l'état q_1 . $w_1 = (q_1 \xrightarrow{\beta} q_3)$ est donc la seule instance de séparation à considérer. Pour cela, une seule variable de contrôle notée C_1 est nécessaire et la valeur de la fonction de contrôle relative à l'état q_3 doit être négative. Les trois états (q_0 , q_1 et q_2) doivent être atteignables, par conséquent, les valeurs de la fonction de contrôle relatives à ces états doivent être positives ou nulles. Les trois conditions d'atteignabilité sont donc :

$$\begin{aligned} U(C_1)/q_0 &\geq 0 ; \\ U(C_1)/q_1 &= U(C_1)/q_0 + C_1^{\alpha_1} \geq 0 ; \\ U(C_1)/q_2 &= U(C_1)/q_0 + C_1^{\alpha_1} + C_1^{\alpha_2} \geq 0 . \end{aligned}$$

5.4.1.2 L'équation de cycle

D'autre part, la fonction de contrôle doit satisfaire les équations de cycle

$$\sum_{\alpha_i \in \gamma} C_k^{\alpha_i} = 0, \quad \forall \gamma \in S_c \quad [5.2]$$

où γ est un cycle appartenant à l'ensemble des cycles S_c de l'automate G_c . γ est composé d'une succession d'événements α_i .

Reprendons l'exemple de l'automate A (figure 5.8). La fonction de contrôle $U(C_1)/q_0$ doit retrouver sa valeur initiale suite au cycle γ , c'est-à-dire l'occurrence des événements α_1 , α_2 et β , d'où l'expression de l'équation de cycle :

$$\begin{aligned} U(C_1)/q_0 &= U(C_1)/q_0 + C_1^{\alpha_1} + C_1^{\alpha_2} + C_1^{\beta} \\ \Rightarrow C_1^{\alpha_1} + C_1^{\alpha_2} + C_1^{\beta} &= 0 \end{aligned}$$

5.4.1.3 La condition de séparation

Pour retrouver le fonctionnement le plus permis, il faut séparer l'ensemble des événements menant aux états dangereux. Soient s la séquence formée des α_i événements, permettant d'atteindre q_i à partir de q_0 et β un événement contrôlable menant de l'état q_i à l'état q_j non admissible.

$$U(C_k)/q_j = U(C_k)/q_i + C_k^\beta < 0$$

$$U(C_k)/q_j = U(C_k)/q_0 + \sum_{\alpha_i \in S} C_k^{\alpha_i} + C_k^\beta < 0 \quad [5.3]$$

avec $q_0, q_i \in G_c$ et $q_j \in G - G_c$.

Ceci définit donc l'instance de séparation $w_k = (q_i \xrightarrow{\beta} q_j)$. La condition de séparation est donnée par la relation [5.3].

Pour l'exemple de la figure 5.8, l'état q_3 est le seul état interdit. Comme β est un événement contrôlable alors l'instance de séparation est $w_1 = (q_1 \xrightarrow{\beta} q_3)$. Pour interdire l'atteignabilité de q_3 , la valeur de la fonction de contrôle $U(C_1)/q_3$ doit être négative. La condition de séparation est :

$$U(C_1)/q_3 = U(C_1)/q_0 + C_1^{\alpha_1} + C_1^\beta < 0$$

La résolution du système [5.1] - [5.3] permet de déterminer les variables de contrôle, si elles existent, correspondantes à chaque événement ainsi que la valeur initiale de la fonction de contrôle. Ce qui nous permet de construire les Grafcets de supervision. Une des solutions qui permet de résoudre le système d'équations est définie comme suit:

$$U(C_1)/q_0 = 0, C_1^{\alpha_1} = 0, C_1^{\alpha_2} = +1, C_1^\beta = -1.$$

L'automate représentant le comportement le plus permis G_c ainsi que l'évolution de la fonction de contrôle est représenté à la figure 5.9. La mise à jour de la fonction de contrôle est faite par les Grafcets de supervision lors de l'occurrence de l'un des événements α_1 , α_2 et β .

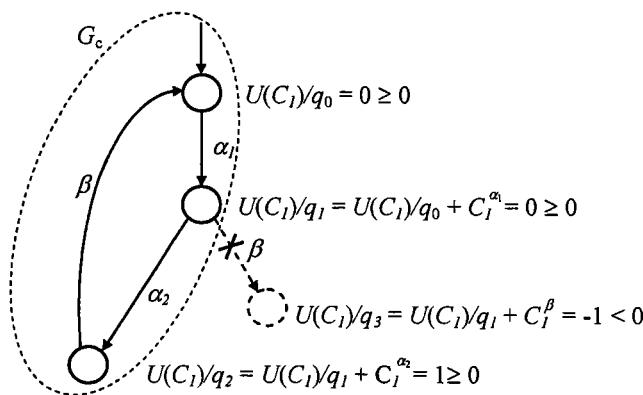


Figure 5.9. Evolution de la fonction de contrôle

Théorème 5.1 Un comportement souhaité G_c , sous graphe d'un automate G , déduit des Grafcets de commande, peut être réalisé en ajoutant des variables de contrôle aux Grafcets de commande ssi il existe une solution $U(C_k)$ pour le système linéaire incluant toutes les conditions [5.1] et [5.2] et une des conditions [5.3], pour chaque instance de Ω .

La preuve de ce théorème est faite par analogie par rapport à celle du théorème 3.1 (Chapitre 3) sur l'existence de places de contrôle pures.

5.4.2 Algorithme de synthèse

L'algorithme 5.2 suivant résume la méthode de synthèse des variables de contrôle qui permettent d'interdire à un automate G les transitions de l'ensemble Ω pour réaliser le comportement désiré modélisé par G_c tout en respectant la contrainte réversibilité. La réversibilité est traduite ici par un comportement non bloquant et la possibilité d'atteindre l'état initial à partir de tout état du système. L'automate G est déduit à partir des Grafcets de commande du procédé.

Algorithme 5.2 : Synthèse des variables de contrôle

- 1- Générer l'automate G à partir des grafcet de commande du procédé ;
 - 2- Déterminer Ω à partie de l'ensemble des états interdits Q_I ;
 - 3- Générer G_c ;
 - 4- Ecrire la condition d'atteignabilité pour tout état de G_c .
 - 5- Ecrire les équations de cycle.
 - 6- Tant que $\Omega \neq \emptyset$ faire:
 - 6.1- Ecrire la condition de séparation pour chaque élément de Ω ;
 - 6.2- Résoudre le système [5.1] - [5.3]. Soit $U(C_k)$ la solution correspondante ;
 - 6.3- Eliminer de Ω toutes les instances traitées par $U(C_k)$;
 - 7- Eliminer les variables de contrôle redondantes ;
 - 8- Déduire les Grafcets de supervision correspondant.
- FIN

La solution du système [5.1] – [5.3], si elle existe, permet d'avoir les variables de contrôle à ajouter aux Grafset de commande et construire ainsi le superviseur associé qui s'occupera de la mise à jour des fonctions de contrôle suite à l'occurrence des événements observés.

5.5 Application

Reprendons l'exemple introduit à la section 5.3 afin de déterminer le superviseur associé permettant de respecter la spécification de sûreté SP_2 . Nous rappelons qu'il y a 33 états non admissibles dans G et 12 instances de séparation représentées par l'ensemble Ω : (Voir figure 5.6).

$$\Omega = \left\{ \begin{array}{l} \left(q_{123} \xrightarrow{F_1} q_{221} \right), \left(q_{133} \xrightarrow{F_1} q_{231} \right), \left(q_{143} \xrightarrow{F_1} q_{241} \right), \left(q_{121} \xrightarrow{F_1} q_{222} \right) \\ \left(q_{131} \xrightarrow{F_1} q_{232} \right), \left(q_{141} \xrightarrow{F_1} q_{242} \right), \left(q_{212} \xrightarrow{F_2} q_{221} \right), \left(q_{312} \xrightarrow{F_2} q_{321} \right) \\ \left(q_{412} \xrightarrow{F_2} q_{421} \right), \left(q_{211} \xrightarrow{F_2} q_{223} \right), \left(q_{311} \xrightarrow{F_2} q_{323} \right), \left(q_{411} \xrightarrow{F_2} q_{423} \right) \end{array} \right\}$$

En appliquant l'algorithme 5.2, nous trouvons 12 conditions de séparation respectivement des états (221), (321), (421), (231), (241), (222), (232), (242), (223), (323) et (423). Pour cela nous utilisons 12 variables de contrôle C_k avec $k = 1 \rightarrow 12$.

$U_0(C_1) + C_1^{F_1} + C_1^{F_2} < 0 ;$	$w_1 = (q_{123} \xrightarrow{F_1} q_{221})$
$U_0(C_2) + C_2^{F_1} + C_2^{F_2} < 0 ;$	$w_1' = (q_{212} \xrightarrow{F_2} q_{221})$
$U_0(C_3) + C_3^{F_1} + C_3^{ff_1} + C_3^{F_2} < 0 ;$	$w_2 = (q_{312} \xrightarrow{F_2} q_{321})$
$U_0(C_4) + C_4^{F_1} + C_4^{ff_1} + C_4^{T_1} + C_4^{F_2} < 0 ;$	$w_3 = (q_{412} \xrightarrow{F_2} q_{421})$
$U_0(C_5) + C_5^{F_2} + C_5^{ff_2} C_5^{F_1} < 0 ;$	$w_4 = (q_{133} \xrightarrow{F_1} q_{231})$
$U_0(C_6) + C_6^{F_2} + C_6^{ff_2} + C_6^{T_2} + C_6^{F_1} < 0 ;$	$w_5 = (q_{143} \xrightarrow{F_1} q_{241})$
$U_0(C_7) + C_7^{F_1} + C_7^{ff_1} + C_7^{T_1} + C_7^{ft_1} + C_7^{F_2} + C_7^{F_1} < 0 ;$	$w_6 = (q_{121} \xrightarrow{F_1} q_{222})$
$U_0(C_8) + C_8^{F_1} + C_8^{ff_1} + C_8^{T_1} + C_8^{ft_1} + C_8^{F_2} + C_8^{ff_2} + C_8^{F_1} < 0 ;$	$w_7 = (q_{131} \xrightarrow{F_1} q_{232})$
$U_0(C_9) + C_9^{F_1} + C_9^{ff_1} + C_9^{T_1} + C_9^{ft_1} + C_9^{F_2} + C_9^{ff_2} + C_9^{T_2} + C_9^{F_1} < 0 ;$	$w_8 = (q_{141} \xrightarrow{F_1} q_{242})$
$U_0(C_{10}) + C_{10}^{F_2} + C_{10}^{ff_2} + C_{10}^{T_2} + C_{10}^{ft_2} + C_{10}^{F_1} + C_{10}^{F_2} < 0 ;$	$w_9 = (q_{211} \xrightarrow{F_2} q_{223})$
$U_0(C_{11}) + C_{11}^{F_2} + C_{11}^{ff_2} + C_{11}^{T_2} + C_{11}^{ft_2} + C_{11}^{F_1} + C_{11}^{ff_1} + C_{11}^{F_2} < 0 ;$	$w_{10} = (q_{311} \xrightarrow{F_2} q_{323})$
$U_0(C_{12}) + C_{12}^{F_2} + C_{12}^{ff_2} + C_{12}^{T_2} + C_{12}^{ft_2} + C_{12}^{F_1} + C_{12}^{ff_1} + C_{12}^{T_1} + C_{12}^{F_2} < 0 ;$	$w_{11} = (q_{411} \xrightarrow{F_2} q_{423})$

12 équations de cycle : ($k = 1 \rightarrow 12$).

$$C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} + C_k^{ft_1} + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} + C_k^{ft_2} = 0$$

168 conditions d'atteignabilité sont dégagées pour permettre l'atteignabilité des états de $Q_A = \{(111), (212), (312), (412), (112), (121), (131), (141), (123), (133), (143), (113), (211), (311), (411)\}$ constituant tous les états de G_c : ($k = 1 \rightarrow 12$).

$$\begin{aligned}
U_0(C_k) &\geq 0 \\
U_0(C_k) + C_k^{F_1} &\geq 0 \\
U_0(C_k) + C_k^{F_1} + C_k^{ff_1} &\geq 0 \\
U_0(C_k) + C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} &\geq 0 \\
U_0(C_k) + C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} + C_k^{ft_1} &\geq 0 \\
U_0(C_k) + C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} + C_k^{ft_1} + C_k^{F_2} &\geq 0 \\
U_0(C_k) + C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} + C_k^{ft_1} + C_k^{F_2} + C_k^{ff_2} &\geq 0 \\
U_0(C_k) + C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} + C_k^{ft_1} + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} &\geq 0 \\
U_0(C_k) + C_k^{F_2} &\geq 0 \\
U_0(C_k) + C_k^{F_2} + C_k^{ff_2} &\geq 0 \\
U_0(C_k) + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} &\geq 0 \\
U_0(C_k) + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} + C_k^{ft_2} &\geq 0 \\
U_0(C_k) + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} + C_k^{ft_2} + C_k^{F_1} &\geq 0 \\
U_0(C_k) + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} + C_k^{ft_2} + C_k^{F_1} + C_k^{ff_1} &\geq 0 \\
U_0(C_k) + C_k^{F_2} + C_k^{ff_2} + C_k^{T_2} + C_k^{ft_2} + C_k^{F_1} + C_k^{ff_1} + C_k^{T_1} &\geq 0
\end{aligned}$$

Une des solutions nécessite seulement les trois variables de contrôle C_a , C_b et C_c .

Première variable de contrôle :

$$U_0(C_a) = 1, C_a^{F_2} = -1, C_a^{ft_1} = +1, C_a^{F_1} = C_a^{ff_1} = C_a^{T_1} = C_a^{ff_2} = C_a^{T_2} = C_a^{ft_2} = 0.$$

Deuxième variable de contrôle :

$$U_0(C_b) = 1, C_b^{F_1} = -1, C_b^{ft_2} = +1, C_b^{ff_1} = C_b^{T_1} = C_b^{ft_1} = C_b^{F_2} = C_b^{ff_2} = C_b^{T_2} = 0.$$

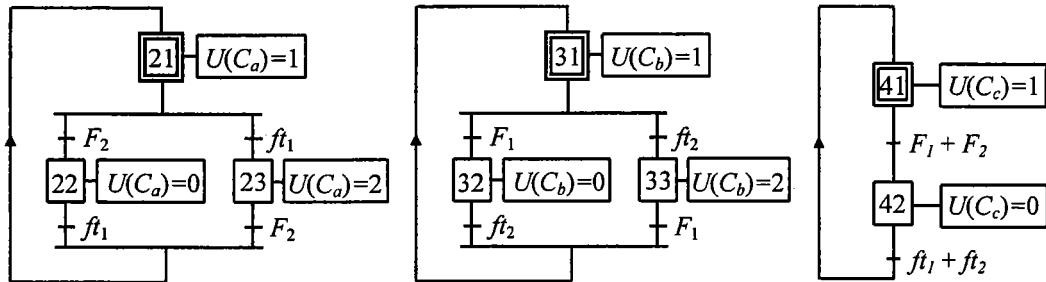
Troisième variable de contrôle :

$$U_0(C_c) = 1, C_c^{F_1} = C_c^{F_2} = -1, C_c^{ft_1} = C_c^{ft_2} = +1, C_c^{ff_1} = C_c^{T_1} = C_c^{ff_2} = C_c^{T_2} = 0.$$

Cette solution est à trois variables de contrôle uniquement car nous avons éliminé toutes celles qui sont redondantes. Les variables C_a et C_c contrôlent l'événement contrôlable F_2 . C_b et C_c contrôlent l'événement contrôlable F_1 .

Le superviseur formellement trouvé est représenté à la figure 5.10. Il contrôle le système dont le fonctionnement est toujours commandé par les Grafsets de commande de la figure 5.1c, et 5.1d. La supervision utilise trois variables de contrôle C_a , C_b et C_c .

L'évolution des trois fonctions de contrôle est représentée par les trois modèles Grafcet constituant le superviseur.



(a) Première fonction de contrôle $U(C_a)$
(b) Deuxième fonction de contrôle $U(C_b)$
(c) Troisième fonction de contrôle $U(C_c)$

Figure 5.10. Les Grafcets de supervision

La structure de commande-supervision proposée à la figure 5.11, intègre le procédé, constitué du procédé et de sa commande locale, ainsi que son superviseur.

Comme $C_b^{F_1} = -1$ et $C_c^{F_1} = -1$, alors l'occurrence de l'événement F_1 décrémente les fonctions $U(C_b)$ et $U(C_c)$ or les fonctions de contrôle doivent toujours être positives ou nulles pour ne pas aller au delà du comportement désiré. Ce qui explique la condition sur l'occurrence de F_1 (si $U(C_b) \geq 1$ et $U(C_c) \geq 1$) dans les Grafcets de commande. Le même raisonnement peut être fait pour l'événement F_2 (figure 5.11).

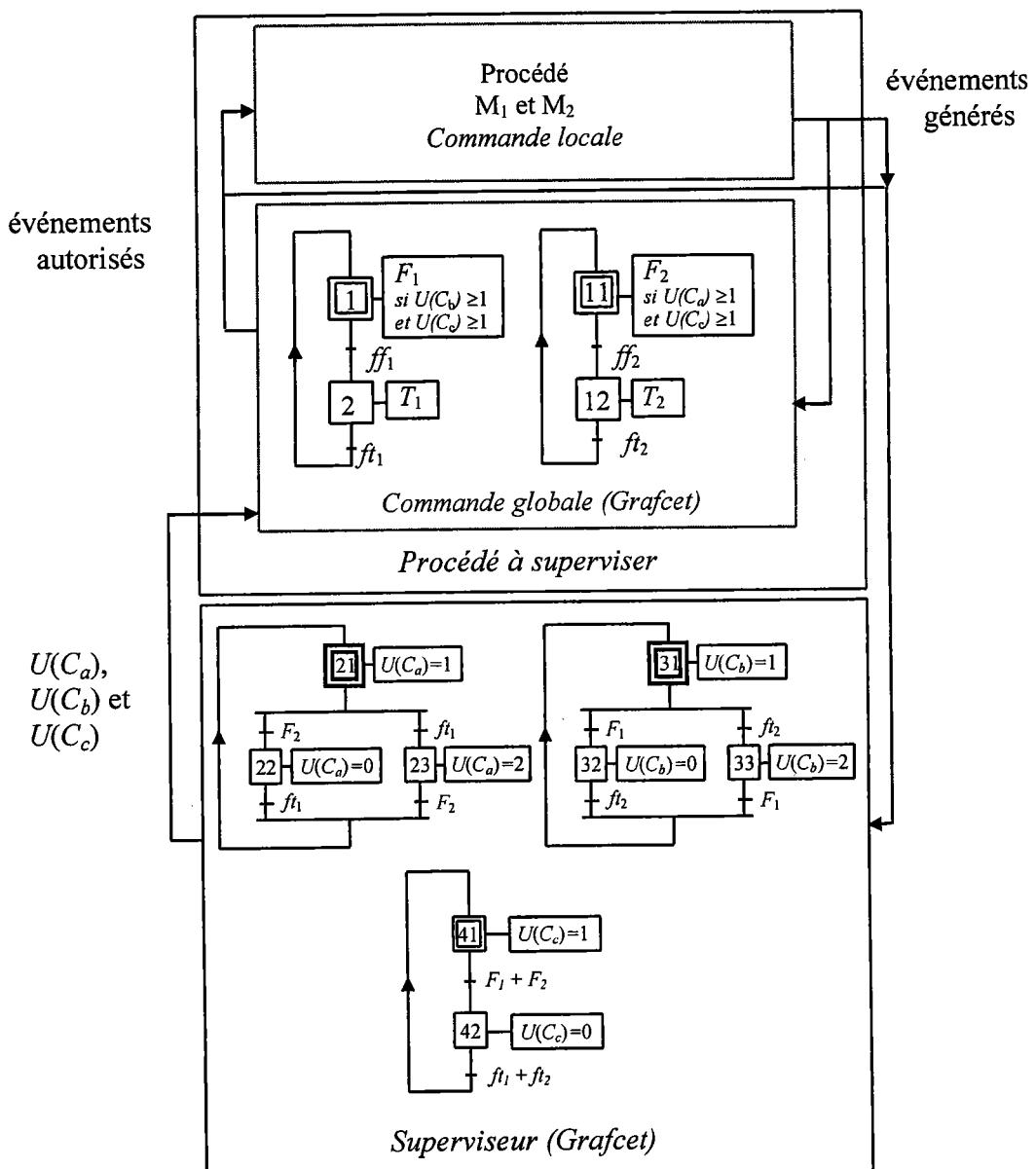


Figure 5.11. La structure de commande-supervision.

5.6 Autres exemples traités

Pour donner une idée sur l'efficacité de l'approche proposée et son coût en termes de temps d'exécution machine, un jeu de données pour des exemples plus complexes dont le nombre d'états de l'automate G et celui des instances de séparation sont importants a été réalisé. Les résultats sont présentés dans le tableau 1 suivant :

Nb états G	Nb états G_c	Nb Inst.	Sép.	Nb Var.	Cont.	Temps CPU
48	15	12		3		0.04
261	215	47		3		0.14
774	699	74		4		0.24
1684	1288	101		4		0.75
3547	3414	128		4		1.68
12477	12074	401		2		12.16

Tableau 5.1. Autres exemples traités.

5.7 Conclusion

Nous avons présenté dans ce chapitre une contribution pour le problème de la synthèse de la commande par supervision pour les modèles Grafcet. L'approche proposée permet de synthétiser un superviseur permettant de faire respecter les spécifications et garantissant la réversibilité du procédé contrôlé. Le superviseur calculé est sous forme d'un ensemble de variables de contrôle à ajouter aux modèles initiaux des Grafcets de commande du procédé. Pour les spécifications, il s'agit des spécifications de commande et de sûreté.

La détermination de ces variables de contrôle est basée sur une nouvelle interprétation de la théorie des régions ainsi que le modèle du procédé déduit de ses Grafcets de commande. L'implémentation de la loi de commande est simple, puisqu'il suffit d'intégrer les variables de contrôle aux modèles initiaux de commande sans trop de modifications. C'est une approche de synthèse optimale dans le sens de sa permissivité et directe au sens de son implémentation aux niveaux des équipements programmables.

Conclusion

Dans ce mémoire nous avons développé une approche de synthèse de la commande pour les SED partiellement observables. Trois contributions ont été développées, une première se situe au niveau de l'extension de l'approche structurelle initiée par les travaux de Ghaffari et al. pour les graphes d'événements partiellement observables. La deuxième contribution se situe au niveau de l'extension de la théorie des régions à la synthèse de la commande des SED partiellement observables. La troisième contribution concerne le développement d'une méthode formelle de synthèse de la commande à partir d'un Grafcet de commande du procédé en s'appuyant sur une nouvelle interprétation de la théorie des régions.

Pour les modèles du procédé utilisant les réseaux de Petri comme formalisme de modélisation, nous avons développé deux approches de synthèse de la commande. La première exploitation des propriétés structurelles des graphes d'événements pour la synthétiser une loi de commande résolvant les spécifications de type états interdits caractérisés par un ensemble de Contraintes Généralisées d'Exclusion Mutuelles (CGEM). Nous avons considéré l'hypothèse que certains événements du SED à contrôler peuvent être incontrôlables et/ou inobservables. Pour cette première approche, nous avons prouvé que pour toutes séquence de transitions observables, il existe un unique marquage depuis lequel tout autre marquage possible du système, peut être atteignable d'une manière inobservable. Cette particularité importante, nous permet de concevoir une loi de commande efficace basée sur la séparation de l'observation et de la commande. Cette loi de commande consiste à déterminer le pire cas suite à une autorisation de franchissement d'une transition contrôlable à évaluer en temps réel si ce pire cas viole les CGEM. La deuxième approche permet de déterminer un contrôleur RdP pour les SED modélisés en un RdP partiellement observable pour résoudre les problèmes du type transitions d'états interdites (PTEI). La synthèse du contrôleur agit en deux phases. En premier lieu, le comportement observable maximum permis et non bloquant est déterminé, et en second lieu, la théorie des régions est utilisée pour la détermination d'un contrôleur RdP quand il existe. Le contrôleur est un ensemble de places de contrôle pouvant être pures ou impures.

Le problème de synthèse d'un contrôleur RdP n'est pas toujours un problème solvable en termes de places RdP. Pour cela, nous avons prouvé dans ce mémoire les conditions nécessaires et suffisantes pour l'existence de places de contrôle pures ou impures résolvant une instance de séparation donnée. La preuve porte sur les cas des SED totalement observables et partiellement observables. Nous avons également prouvé que pour le cas des SED partiellement observables, il est nécessaire de satisfaire deux conditions supplémentaires, nécessaires mais non suffisantes pour l'existence d'un contrôleur RdP optimal et ceci est du à la contrainte d'inobservabilité des événements.

Pour contourner la non existence d'un contrôleur RdP, une solution est proposée et consiste à construire plusieurs places de contrôle pour inhiber une transition interdite quand une seul place de contrôle n'existe pas. Chacune de ces places permettra au modèle d'atteindre une partie du comportement admissible. L'ensemble de ces places est appelé contrôleur RdP partiel.

Pour les modèles du procédé utilisant le GRAFCET comme formalisme de modélisation, nous avons proposé une approche originale de synthèse de la commande. Cette approche a pour objectif principal de déterminer formellement un ensemble de variables de contrôle à intégrer aux modèles Grafcets de commande du procédé et de générer les Grafcets de supervision correspondants. La détermination de cet ensemble de variables de contrôle est basée sur l'utilisation d'une nouvelle interprétation de la théorie des régions.

Pour résumer, nous avons développé des approches pour la synthèse de la commande des SED partiellement observables pour résoudre des problèmes de type transitions d'états interdites. Une première approche exploite les propriétés structurelles des graphes d'événements pour synthétiser une loi de commande. La deuxième approche permet la synthèse des contrôleurs RdP sous forme de places de contrôles pures ou impures en utilisant la théorie des régions. Une extension de cette méthode a également été développée pour déterminer un contrôleur RdP même quand la méthode originale échoue. Nous avons aussi étendue l'utilisation de la théorie des régions pour l'adaptée aux modèles du procédé utilisant le GRAFCET comme formalisme de modélisation. Dans cette approche, nous déterminons des variables de contrôle à intégrer dans les Grafcet de commande et dont l'évolution est gérée par des Grafcet de supervision.

Il est intéressant d'introduire la contrainte temporelle et dans la modélisation du procédé et dans les spécifications. Comme perspective de cette thèse, il est possible d'étendre les approches proposées pour résoudre des contraintes temporelles.

Bibliographie

- [ABSB93] Arinez J.F., Benhabib B., Smith K.C., Brandin B.A., "Design of a PLC-based supervisory-control system for a manufacturing workcell", *Proceedings of the Canadian High Technology Show and Conference*, Toronto, 1993.
- [AR04] Achour Z., Rezg N., "Commande par supervision des systèmes à événements discrets basée sur l'utilisation du GRAFCET et la théorie des régions", *Journal européen des systèmes automatisés RS série JESA*, vol. 38, n° 1-2, pp 37-58, 2004.
- [ARX03] Achour Z., Rezg N., Xie X. "Commande des systèmes partiellement observables basée sur les graphes d'événements", *MSR'03 - Modélisation des Systèmes Réactifs*, Metz, France, October, 2003.
- [ARX04a] Achour Z., Rezg N., Xie X., "Supervisory Control of Partially Observable Marked Graphs", *IEEE Transaction on Automatic Control.*, vol. 49, n° 11, pp 2007-2011, Nov. 2004.
- [ARX04b] Achour Z., Rezg N., Xie X., "Supervisory Control of Marked Graphs with Partial Observations", *International Journal of Production Research*, vol. 42, n° 14, p. 2827-2838, 2004.
- [ARX04c] Achour Z., Rezg N., Xie X. "Supervisory Control of DES with Unobservable Events Based on Structural Approach", *IEEE International Conference on Networking, Sensing and Control*, Taipei, Taiwan, March 2004.
- [ARX04d] Achour Z., Rezg N., Xie X., "Supervisory Controller of Petri Nets Under Partial Observation" *WODES'04 - IFAC 7th Workshop on Discrete Event Systems*, 22-24, Reims, France, pp. 49-54, 2004.
- [ARX05] Achour Z., Rezg N., Xie X., "On the existence of Petri net Controller for Discrete Event Systems under Partial Observation", *16th IFAC WORLD CONGRESS*, Prague, July 4-8, 2005.
- [BBD95] Badouel E., Bernardinello L., Darondeau P., "Polynomial algorithms for the synthesis of bounded nets", *CAAP'95, Springer Verlag LNCS 915*, pp. 364-378, 1995.
- [BBD97] Badouel E., Bernardinello L., Darondeau P., "The synthesis problem for elementary nets systems is NP-complete", *Theoretical Computer Science*, vol. 186, pp. 107-134, 1997.
- [BD99] Badouel E., Darondeau P., "Theory of regions", *Lectures on Petri Nets I : Basic Models*, Springer Verlag, 1999.

- [BHGWF93] Balemi S., Hoffmann G.J., Gyugyi P., Wong-Toi H., Franklin G.F., "Supervisory control of a rapid thermal multiprocessor", *IEEE Transactions on Automatic Control*, vol. 38, pp.1040-1059, 1993.
- [BWB91] Brandlin B.A., Wonham W.M., Benhabib B., "Discrete event system supervisory control applied to the management of manufacturing workcells", *Computer-Aided Production Engineering*, pp. 527-536, Amsterdam:Elsevier 1991.
- [CAD99] Charbonnier F, H. Alla, R. David, "The Supervised Control of Discrete Event Dynamic Systems", *IEEE Transactions on Control Systems Technology*, vol. 7, n° 2, March 1999.
- [CGW88] Caines P. E., Greiner R., Wang S., "Dynamical logic observers for finite automata," in *Proc. 27th Conf. Decision and Control*, Austin, TX, pp. 226–233, Décembre 1988.
- [CL99] Cassandras C.G., Lafortune S., "Introduction to Discrete Event Systems", Kluwer Academic Publishers, 1999.
- [DX03] Darondeau Ph. and Xie X.L., "Linear Control of Live Marked Graphs," *Automatica*, vol. 39, n° 3, pp 429-440, March 2003.
- [GDS92] Giua A., DiCesare F., Silva M., "Generalized mutual exclusion constraints on nets with uncontrollable transitions", In *Proceedings of IEEE Conference on Systems, Man and Cybernetics-Chicago*, Illinois, USA, 1992.
- [GDS93] Giua A., DiCesare F., Silva M., "Petri net supervisors for generalized mutual exclusion constraints", *12th IFAC World Congress*, Sidney, Australia, pp. 267-270, 1993.
- [GM94] Gondran M., Minoux M., "Graphes et algorithmes", Paris, Eyrolles, 1994.
- [GRX03b] Ghaffari A., Rezg N. and Xie X., "Feedback control logic for forbidden state problem of marked graphs", *IEEE Trans. on Automatic Control*, vol. 48, n° 1, pp.18-29, 2003.
- [GRX03a] Ghaffari A., Rezg N., Xie X., "Design of Live and Maximally Permissive Petri Net Controller Using the Theory of Regions." *IEEE Transactions on Robotics and Automation*, vol. 19, pp.137-142, 2003.
- [GS02] Giua A., Seatzu C., "Obervability of place/transition nets", *IEEE Transactions on Automatic Control*, vol. 47, n° 9, pp. 1424-1437, Septembre 2002.
- [GW00] Gohari P., Wonham W.M., "On the complexity of supervisory control design in the RW framework", *IEEE Transactions on Systems Mans and Cybernetics-Part B: Cybernetics*, vol. 30, n° 5, Octobre 2000.
- [HK90] Holloway L., Krogh B., "Synthesis of feedback control logic for a class of controlled Petri nets", *IEEE Trans. Automatic Control*, vol. 35, n° 5, pp. 514-523, 1990.
- [IH87] Ishikawa A., Hiraishi K., "Analysis and control of discrete event systems represented by Petri nets", in *Discrete Event Systems : Models and*

- Applications*, Vol. 103 of Lecture Notes in Control and Information Sciences, Springer, Verlag, pp.115-134, 1987.
- [Kro87] Krogh B. H., “Controlled Petri nets and maximally permissive feedback logic”, *25th Annual Allerton Conference*, University of Illinois, Urbana, pp. 317-326, 1987.
- [Kum91] Kumar R., “*Supervisory Synthesis Techniques for Discrete event Dynamical Systems*”, Thesis for Ph. D. degree, Université du Texas, Août 1991.
- [LW88] Li Y., Wonham W. M., “Controllability and observability in the state-feedback control of discrete-event systems,” in *Proc. 27th Conf. Decision and Control*, Austin, TX, pp. 203–207, Décembre 1988.
- [LW93] Li Y., Wonham W. M., “Control of vector discrete-event systems—Part I: The base model,” *IEEE Transactions on Automatic Control*, vol. 38, pp. 1215–1227, Août 1993.
- [LW94] Li Y., Wonham W. M., “Control of vector discrete event systems II – Controller synthesis”, *IEEE Trans. On Automatic Control*, vol. 39, n° 3, pp. 512-531, 1994.
- [MA99] Moody J., Antsaklis P. J., “*Petri Net Supervisors for DES with Uncontrollable and Unobservable Transitions*”, Report 99-004 (ISIS), 1999.
- [MLA96] Moody J. O., Lemmon M., Antsaklis P. J., “Supervisory control of Petri nets with uncontrollable/unobservable transitions”, *35th IEEE CDC*, Kobe, Japan, 1996.
- [Mur89] Murata T., “Petri nets: properties, analysis and application”, *Proceeding of IEEE*, vol. 44, n° 4, pp. 541-579, 1989.
- [Ndj99] Ndjab Hagbebelle C., “*Synthèse de la commande des systèmes à événements discrets par GRAFCET*”, Thèse de Doctorat de l'Université de Reims Champagne Ardenne, 16 Septembre 1999.
- [ÖW90] Özveren C. M., Willsky A. S., “Observability of discrete event dynamic systems,” *IEEE Trans. On Automatic Control*, vol. 35, pp. 797–806, Juillet 1990.
- [Pet81] Peterson J.L., “*Petri net theory and the modeling of systems*”, Prentice-Hall, 1981.
- [Ram86] Ramadge P. J., “Observability of discrete-event systems,” in *Proc. 25th Conf. Decision and Control*, Athens, Greece, pp. 1108–1112, Décembre 1986.
- [Rou94] Roussel J.M., “*Analyse de Grafcets par génération logique de l'automate équivalent*”, Thèse de Doctorat de l'Ecole Normale Supérieure de Cachan, 16 Décembre 1994.
- [RW87] Ramadge P.J., Wonham W.M., “Supervisory control of a class of discrete event processes”, *SIAM J., Control and Optimization*, vol. 25, pp. 206-230, Janvier 1987.
- [RW89] Ramadge P.J., Wonham W.M., “The control of discrete event systems”, *IEEE Proceedings*, vol. 77, n° 1, pp. 81-98, Janvier 1989.

- [RXG00] Rezg N., Xie X., Ghaffari A., "Supervisory Control in Discrete Event Systems Using the Theory of Regions", *Discrete Event Systems Analysis and Control*, pp. 391-398, 2000.
- [Str00] Stremersch G., "Linear Algebraic Design of Supervisors for Partially Observed Petri Nets", *Proc. IFAC Conf. on Control Systems Design (CSD'2000)*, Bratislava, Slovak Republic, pp 281-286, 2000.
- [TUK95] Takai S., Ushio T., Kodama S., "Static-state feedback control of discrete-event systems under partial observation," *IEEE Transactions on Automatic Control*, vol. 40, pp. 1950–1955, Novembre 1995.
- [WR87] Wonham W.M., Ramadge P.J., "On the supremal controllable sublanguage of a given language", *SIAM J. Control and Optimization*, vol. 25, n° 3, pp. 637-659, 1987.
- [ZC01] Zaytoon J., Carré-Ménétrier V., "Synthesis of control implementation for discrete manufacturing systems." *International Journal of Production Research*, vol. 39, n° 2, pp. 329-345, 2001.

Contribution à la synthèse des contrôleurs des systèmes à événements discrets partiellement observables

Résumé

Dans ce travail, nous proposons des méthodes de synthèse des lois de commande pour les systèmes à événements discrets partiellement observables. Selon le modèle utilisé, nous avons apporté deux types de contributions. Une première contribution se situe au niveau de l'extension de la synthèse de la commande basée sur des modèles réseaux de Petri et la théorie des régions en intégrant la contrainte d'observabilité des événements. La deuxième contribution intéressante concerne le développement d'une méthode formelle de synthèse de la commande à partir d'un Grafset de commande du procédé en s'appuyant sur une nouvelle interprétation de la théorie des régions. Pour les modèles du procédé exprimés en réseaux de Petri, nous proposons deux approches de synthèse de la commande des SED en présence d'événements incontrôlables et/ou inobservables. Ces approches permettent de résoudre le problème des états interdits caractérisé par un ensemble de Contraintes Généralisées d'Exclusion Mutualées (CGEM) en exploitant les propriétés structurelles des graphes d'événements. L'exploitation des propriétés structurelles des graphes d'événements nous a permis de synthétiser une loi de commande pour le problème d'états interdits avec la contrainte d'observabilité des événements. Pour cette approche, nous nous intéressons aux cas où les CGEM concernent une ou plusieurs places du modèle du procédé. La deuxième approche traite du cas des problèmes des transitions d'états interdites (PTEI). L'approche de synthèse développée intègre la notion de réversibilité avec les contraintes d'incontrôlabilité et d'inobservabilité des événements. L'approche proposée détermine un contrôleur RdP maximum permis, quand il existe. Les conditions nécessaires pour l'existence du contrôleur RdP pour les SED partiellement observables sont établies. La deuxième contribution proposée par cette thèse concerne l'utilisation de la théorie des régions pour synthétiser un superviseur à partir des modèles de commande du procédé SED exprimés en GRAFCET. Les spécifications traitées sont du type état interdit et en intégrant l'aspect réversibilité du procédé. Pour ce faire, une nouvelle interprétation de la théorie des régions a été développée et permet de déterminer formellement un ensemble de variables de contrôle à intégrer aux modèles de commande du procédé exprimés en GRAFCET.

Mots-clés : Réseaux de Petri, Grafset, théorie des régions, synthèse de la commande, contrôleur, observabilité, système à événement discret.

Abstract

In this work, we present control synthesis approaches for discrete events systems with partial observation. According to the used model, we propose two types of contributions. A first contribution is an extension of the supervisory control based on the Petri net (PN) models and the theory regions by integrating the observation constraint of the events. The second interesting contribution relates to the development of a formal method of control synthesis starting from a Grafset control plant while being based on a new interpretation of the theory of regions. For the plant modelled with Petri nets, we propose two approaches of control synthesis. These approaches solve the forbidden stats problem characterized by a set of General Mutual Exclusion Constraints (GMEC) by exploiting the structural properties of the marked graphs. Structural properties are proposed to perform the worst-case analysis for each GMEC specification with any given initial marking when uncontrollable and/or unobservable transitions are allowed. Efficient solutions are proposed for the determination of the maximal uncontrollably reachable marking of any critical place. Second approach resolves the forbidden state-transition problems (FSTP). The developed synthesis approach integrates the concept of liveness with uncontrollable / unobservable transitions. The suggested approach determines the maximum permissive PN controller, when it exists. The necessary conditions for the existence of the PN controller for the partially observable DES are established. The second contribution of this work relates to the use of the theory of regions to synthesize a supervisor from a Grafset control plant model for forbidden state specifications and integrating the reversibility aspect of the plant. For this, a new interpretation of the theory of regions was developed to formally determine a set of control variables to integrate into the initial Grafset control model which constitutes the supervisor.

Keywords: Petri net, Grafset, theory of regions, control synthesis, Controller, Observability, Discrete Event System.