Modélisation et analyse du comportement des systèmes informatiques temporisés

Nicolas Halbwachs

THESE

présentée à

l' Université Scientifique et Médicale de Grenoble

et à

l' Institut National Polytechnique de Grenoble

pour obtenir le grade de

DOCTEUR ES SCIENCES MATHEMATIQUES

par

Nicolas HALBWACHS

MODELISATION ET ANALYSE DU COMPORTEMENT DES SYSTEMES INFORMATIQUES TEMPORISES.

Thèse soutenue le 8 juin 1984 devant la commission d'examen.

G. SAUCIER	Président
G. BERRY M. SINTZOFF	Rapporteurs
P. CASPI P. COUSOT J. SIFAKIS J.P. VERJUS	Examinateurs

UNIVERSITE SCIENTIFIQUE ET MEDICALE DE GRENOBLE

Année universitaire 1982-1983

Président de l'Université : M. TANCHE

MEMBRES DU CORPS ENSEIGNANT DE L'U.S.M.G.

(RANG A)

SAUF ENSEIGNANTS EN MEDECINE ET PHARMACIE

PROFESSEURS DE 1ère CLASSE

ARNAUD Paul	Chimie organique
ARVIEU Robert	Physique nucléaire I.S.N.
AUBERT Guy	Physique C.N.R.S.
AYANT Yves	Physique approfondie
BARBIER Marie-Jeanne	Electrochimie
BARBIER Jean-Claude	Physique expérimentale C.N.R.S. (labo de magnétisme)
BARJON Robert	Physique nucléaire I.S.N.
BARNOUD Fernand	Biosynthèse de la cellulose-Biologie
BARRA Jean-René	Statistiques - Mathématiques appliquées
BELORISKY Elie	Physique
BENZAKEN Claude (M.)	Mathématiques pures
BERNARD Alain	Mathématiques pures
BERTRANDIAS Françoise	Mathématiques pures
BERTRANDIAS Jean-Paul	Mathématiques pures
BILLET Jean	Géographie
BONNIER Jean-Marie	Chimie générale
BOUCHEZ Robert	Physique nucléaire I.S.N.
BRAVARD Yves	Géographie
CARLIER Georges	Biologie végétale
CAUQUIS Georges	Chimie organique
CHIBON Pierre	Biologie animale
COLIN DE VERDIERE Yves	Mathématiques pures
CRABBE Pierre (détaché)	C.E.R.M.O.
CYROT Michel	Physique du solide
DAUMAS Max	Géographie
DEBELMAS Jacques	Géologie générale
DEGRANGE Charles	Zoologie
DELOBEL Claude (M.)	M.I.A.G. Mathématiques appliquées
DEPORTES Charles	Chimie minérale
DESRE Pierre	Electrochimie
DOLIQUE Jean-Michel	Physique des plasmas
DUCROS Pierre	Cristallographie
FONTAINE Jean-Marc	Mathématiques pures
GAGNAIRE Didier	Chimie physique

.../...

GASTINEL Noël	Analyse numérique - Mathématiques appliquées
GERBER Robert	Mathématiques pures
GERMAIN Jean-Pierre	Mécanique
GIRAUD Pierre	Géologie
IDELMAN Simon	Physiologie animale
JANIN Bernard	Géographie
JOLY Jean-René	Mathématiques pures
JULLIEN Pierre	Mathématiques appliquées
KAHANE André (détaché DAFCO)	Physique
KAHANE Josette	Physique
KOSZUL Jean-Louis	Mathématiques pures
KRAKOWIAK Sacha	Mathématiques appliquées
KUPTA Yvon	Mathématiques pures
LACAZE Albert	Thermodynamique
LAJZEROWICZ Jeannine	Physique
LAJZEROWICZ Joseph	Physique
LAURENT Pierre	Mathématiques appliquées
DE LEIRIS Joël	Biologie
LLIBOUTRY Louis	Géophysique
LOISEAUX Jean-Marie	Sciences nucléaires I.S.N.
LOUP Jean	Géographie
MACHE Régis	Physiologie végétale
MAYNARD Roger	Physique du solide
MICHEL Robert	Minéralogie et pétrographie (géologie)
MOZIERES Philippe	Spectrométrie - Physique
OMONT Alain	Astrophysique
OZENDA Paul	Botanique (biologie végétale)
PAYAN Jean-Jacques (détaché)	Mathématiques pures
PEBAY PEYROULA Jean-Claude	Physique
PERRIAUX Jacques	Géologie
PERRIER Guy	Géophysique
PIERRARD Jean-Marie	Mécanique
RASSAT André	Chimie systématique
RENARD Michel	Thermodynamique
RICHARD Lucien	Biologie végétale
RINAUDO Marguerite	Chimie CERMAV
SENGEL Philippe	Biologie animale
SERGERAERT Francis	Mathématiques pures
SOUTIF Michel	Physique
VAILLANT François	Zoologie
VALENTIN Jacques	Physique nucléaire I.S.N.
VAN CUTSEN Bernard	Mathématiques appliquées
VAUQUOIS Bernard	Mathématiques appliquées
VIALON Pierre	Géologie

PROFESSEURS DE 2ème CLASSE

ADIBA Michel	Mathématiques pures
ARMAND Gilbert	Géographie

.../...

AURIAULT Jean-Louis	Mécanique
BEGUIN Claude (M.)	Chimie organique
BOEHLER Jean-Paul	Mécanique
BOITET Christian	Mathématiques appliquées
BORNAREL Jean	Physique
BRUN Gilbert	Biologie
CASTAING Bernard	Physique
CHARDON Michel	Géographie
COHENADDAD Jean-Pierre	Physique
DENEUVILLE Alain	Physique
DEPASSEL Roger	Mécanique des fluides
DOUCE Roland	Physiologie végétale
DUFRESNOY Alain	Mathématiques pures
GASPARD François	Physique
GAUTRON René	Chimie
GIDON Maurice	Géologie
GIGNOUX Claude (M.)	Sciences nucléaires I.S.N.
GUITTON Jacques	Chimie
HACQUES Gérard	Mathématiques appliquées
HERBIN Jacky	Géographie
HICTER Pierre	Chimie
JOSELEAU Jean-Paul	Biochimie
KERCKOVE Claude (M.)	Géologie
LE BRETON Alain	Mathématiques appliquées
LONGEQUEUE Nicole	Sciences nucléaires I.S.N.
LUCAS Robert	Physiques
LUNA Domingo	Mathématiques pures
MASCLE Georges	Géologie
NEMOZ Alain	Thermodynamique (CNRS - CRTBT)
OUDET Bruno	Mathématiques appliquées
PELMONT Jean	Biochimie
PERRIN Claude (M.)	Sciences nucléaires I.S.N.
PFISTER Jean-Claude (détaché)	Physique du solide
PIBOULE Michel	Géologie
PIERRE Jean-Louis	Chimie organique
RAYNAUD Hervé	Mathématiques appliquées
ROBERT Gilles	Mathématiques pures
ROBERT Jean-Bernard	Chimie physique
ROSSI André	Physiologie végétale
SAKAROVITCH Michel	Mathématiques appliquées
SARROT REYNAUD Jean	Géologie
SAXOD Raymond	Biologie animale
SOUTIF Jeanne	Physique
SCHOOL Pierre-Claude	Mathématiques appliquées
STUTZ Pierre	Mécanique
SUBRA Robert	Chimie
VIDAL Michel	Chimie organique
VIVIAN Robert	Géographie

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Année universitaire 1982-1983

Président de l'Université : D. BLOCH

Vice-Président : René CARRE
Hervé CHERADAME
Marcel IVANES

PROFESSEURS DES UNIVERSITES :

ANCEAU François	E.N.S.I.M.A.G.
BARRAUD Alain	E.N.S.I.E.G.
BAUDELET Bernard	E.N.S.I.E.G.
BESSON Jean	E.N.S.E.E.G.
BLIMAN Samuel	E.N.S.E.R.G.
BLOCH Daniel	E.N.S.I.E.G.
BOIS Philippe	E.N.S.H.G.
BONNETAIN Lucien	E.N.S.E.E.G.
BONNIER Etienne	E.N.S.E.E.G.
BOUVARD Maurice	E.N.S.H.G.
BRISSONNEAU Pierre	E.N.S.I.E.G.
BUYLE BODIN Maurice	E.N.S.E.R.G.
CAVAIGNAC Jean-François	E.N.S.I.E.G.
CHARTIER Germain	E.N.S.I.E.G.
CHENEVIER Pierre	E.N.S.E.R.G.
CHERADAME Hervé	U.E.R.M.C.P.P.
CHERUY Arlette	E.N.S.I.E.G.
CHIAVERINA Jean	U.E.R.M.C.P.P.
COHEN Joseph	E.N.S.E.R.G.
COUMES André	E.N.S.E.R.G.
DURAND Francis	E.N.S.E.E.G.
DURAND Jean-Louis	E.N.S.I.E.G.
FELICI Noël	E.N.S.I.E.G.
FOULARD Claude	E.N.S.I.E.G.
GENTIL Pierre	E.N.S.E.R.G.
GUERIN Bernard	E.N.S.E.R.G.
GUYOT Pierre	E.N.S.E.E.G.
IVANES Marcel	E.N.S.I.E.G.
JAUSSAUD Pierre	E.N.S.I.E.G.
JOUBERT Jean-Claude	E.N.S.I.E.G.
JOURDAIN Geneviève	E.N.S.I.E.G.
LACOUME Jean-Louis	E.N.S.I.E.G.
LATOMBE Jean-Claude	E.N.S.I.M.A.G.

.../...

LESSIEUR Marcel	E.N.S.H.G.
LESPINARD Georges	E.N.S.H.G.
LONGEQUEUE Jean-Pierre	E.N.S.I.E.G.
MAZARE Guy	E.N.S.I.M.A.G.
MOREAU René	E.N.S.H.G.
MORET Roger	E.N.S.I.E.G.
MOSSIERE Jacques	E.N.S.I.M.A.G.
PARIAUD Jean-Charles	E.N.S.E.E.G.
PAUTHENET René	E.N.S.I.E.G.
PERRET René	E.N.S.I.E.G.
PERRET Robert	E.N.S.I.E.G.
PIAU Jean-Michel	E.N.S.H.G.
POLOUJADOFF Michel	E.N.S.I.E.G.
POUPOT Christian	E.N.S.E.R.G.
RAMEAU Jean-Jacques	E.N.S.E.E.G.
RENAUD Maurice	U.E.R.M.C.P.P.
ROBERT André	U.E.R.M.C.P.P.
ROBERT François	E.N.S.I.M.A.G.
SABONNADIERE Jean-Claude	E.N.S.I.E.G.
SAUCIER Gabrielle	E.N.S.I.M.A.G.
SCHLENKER Claire	E.N.S.I.E.G.
SCHLENKER Michel	E.N.S.I.E.G.
SERMET Pierre	E.N.S.E.R.G.
SILVY Jacques	U.E.R.M.C.P.P.
SOHM Jean-Claude	E.N.S.E.E.G.
SOUQUET Jean-Louis	E.N.S.E.E.G.
VEILLON Gérard	E.N.S.I.M.A.G.
ZADWORNY François	E.N.S.E.R.G.

PROFESSEURS ASSOCIES

BASTIN Georges	E.N.S.H.G.
BERRIL John	E.N.S.H.G.
CARREAU Pierre	E.N.S.H.G.
GANDINI Alessandro	U.E.R.M.C.P.P.
HAYASHI Hirashi	E.N.S.I.E.G.

PROFESSEURS UNIVERSITE DES SCIENCES SOCIALES (Grenoble II)

BOLLIET Louis
Chatelin Françoise

PROFESSEURS E.N.S. Mines de Saint-Etienne

RIEU Jean
SOUSTELLE Michel

CHERCHEURS DU C.N.R.S.

FRUCHART Robert	Directeur de Recherche
VACHAUD Georges	Directeur de Recherche

.../...

ALLIBERT Michel	Maître de Recherche
ANSARA Ibrahim	Maître de Recherche
ARMAND Michel	Maître de Recherche
BINDER Gilbert	
CARRE René	Maître de Recherche
DAVID René	Maître de Recherche
DEPORTES Jacques	
DRIOLE Jean	Maître de Recherche
GIGNOUX Damien	
GIVORD Dominique	
GUELIN Pierre	
HOPFINGER Emil	Maître de Recherche
JOUD Jean-Charles	Maître de Recherche
KAMARINOS Georges	Maître de Recherche
KLEITZ Michel	Maître de Recherche
LANDAU Ioan-Dore	Maître de Recherche
LASJAUNIAS J.C.	
MERMET Jean	Maître de Recherche
MUNIER Jacques	Maître de Recherche
PIAU Monique	
PORTESEIL Jean-Louis	
THOLENCE Jean-Louis	
VERDILLON André	

CHERCHEURS du MINISTERE de la RECHERCHE et de la TECHNOLOGIRE (Directeurs et Maîtres de Recherches, ENS Mines de St. Etienne)

LESBATS Pierre	Directeur de Recherche
BISCONDI Michel	Maître de Recherche
KOBYLANSKI André	Maître de Recherche
LE COZE Jean	Maître de Recherche
LALAUZE René	Maître de Recherche
LANCELOT Francis	Maître de Recherche
THEVENOT François	Maître de Recherche
TRAN MINH Canh	Maître de Recherche

PERSONNALITES HABILITEES à DIRIGER des TRAVAUX de RECHERCHE (Décision du Conseil Scientifique)

ALLIBERT Colette	E.N.S.E.E.G.
BERNARD Claude	E.N.S.E.E.G.
BONNET Rolland	E.N.S.E.E.G.
CAILLET Marcel	E.N.S.E.E.G.
CHATILLON Catherine	E.N.S.E.E.G.
CHATILLON Christian	E.N.S.E.E.G.
COULON Michel	E.N.S.E.E.G.
DIARD Jean-Paul	E.N.S.E.E.G.
EUSTAPOPOULOS Nicolas	E.N.S.E.E.G.
FOSTER Panayotis	E.N.S.E.E.G.

.../...

GALERIE Alain	E.N.S.E.E.G.
HAMMOU Abdelkader	E.N.S.E.E.G.
MALMEJAC Yves	E.N.S.E.E.G. (CENG)
MARTIN GARIN Régina	E.N.S.E.E.G.
NGUYEN TRUONG Bernadette	E.N.S.E.E.G.
RAVAINE Denis	E.N.S.E.E.G.
SAINFORT	E.N.S.E.E.G. (CENG)
SARRAZIN Pierre	E.N.S.E.E.G.
SIMON Jean-Paul	E.N.S.E.E.G.
TOUZAIN Philippe	E.N.S.E.E.G.
URBAIN Georges	E.N.S.E.E.G. (Laboratoire des ultra-réfractaires ODEILLON)
GUILHOT Bernard	E.N.S. Mines Saint Etienne
THOMAS Gérard	E.N.S. Mines Saint Etienne
DRIVER Julien	E.N.S. Mines Saint Etienne
BARIBAUD Michel	E.N.S.E.R.G.
BOREL Joseph	E.N.S.E.R.G.
CHOVET Alain	E.N.S.E.R.G.
CHEHIKIAN Alain	E.N.S.E.R.G.
DOLMAZON Jean-Marc	E.N.S.E.R.G.
HERAULT Jeanny	E.N.S.E.R.G.
MONLLOR Christian	E.N.S.E.R.G.
BORNARD Guy	E.N.S.I.E.G.
DESCHIZEAU Pierre	E.N.S.I.E.G.
GLANGEAUD François	E.N.S.I.E.G.
KOFMAN Walter	E.N.S.I.E.G.
LEJEUNE Gérard	E.N.S.I.E.G.
MAZUER Jean	E.N.S.I.E.G.
PERARD Jacques	E.N.S.I.E.G.
REINISCH Raymond	E.N.S.I.E.G.
ALEMANY Antoine	E.N.S.H.G.
BOIS Daniel	E.N.S.H.G.
DARVE Félix	E.N.S.H.G.
MICHEL Jean-Marie	E.N.S.H.G.
OBLED Charles	E.N.S.H.G.
ROWE Alain	E.N.S.H.G.
VAUCLIN Michel	E.N.S.H.G.
WACK Bernard	E.N.S.H.G.
BERT Didier	E.N.S.I.M.A.G.
CALMET Jacques	E.N.S.I.M.A.G.
COURTIN Jacques	E.N.S.I.M.A.G.
COURTOIS Bernard	E.N.S.I.M.A.G.
DELLA DORA Jean	E.N.S.I.M.A.G.
FONLUPT Jean	E.N.S.I.M.A.G.
SIFAKIS Joseph	E.N.S.I.M.A.G.
CHARUEL Robert	U.E.R.M.C.P.P.
CADET Jean	C.E.N.G.
COEURE Philippe	C.E.N.G. (LETI)

.../...

DELHAYE Jean-Marc	C.E.N.G. (STT)
DUPUY Michel	C.E.N.G. (LETI)
JOUVE Hubert	C.E.N.G. (LETI)
NICOLAU Yvan	C.E.N.G. (LETI)
NIFENECKER Hervé	C.E.N.G.
PERROUD Paul	C.E.N.G.
PEUZIN Jean-Claude	C.E.N.G. (LETI)
TAIEB Maurice	C.E.N.G.
VINCENDON Marc	C.E.N.G.

LABORATOIRES EXTERIEURS

DEMOULIN Eric	C.N.E.T.
DEVINE	C.N.E.T. (R.A.B.)
GERBER Roland	C.N.E.T.
MERCKEL Gérard	C.N.E.T.
PAULEAU Yves	C.N.E.T.
GAUBERT C.	I.N.S.A. Lyon

REMERCIEMENTS

Si cet ouvrage constitue ma thèse, c'est parce que Paul Caspi a soutenu la sienne depuis quelques années. En effet, ce travail est le résultat d'une collaboration permanente entre nous, et il me serait bien difficile de préciser ce qui en revient à chacun. Lui adresser ici mes remerciements serait un euphémisme.

Patrick Cousot m'a formé à la recherche au cours de la préparation de ma thèse de troisième cycle. J'espère en avoir acquis un peu de son exigeance et de sa rigueur scientifique.

Je remercie vivement

Madame Gabrièle Saucier, qui m'a accueilli dans son équipe de recherche, et m'y a fourni d'excellentes conditions de travail;

Messieurs Gérard Berry, Michel Sintzoff, Joseph Sifakis et Jean-Pierre Verjus qui, aprés avoir relu et annoté le manuscrit, ont accepté de participer au jury de cette thèse.

Je remercie également

mes collègues de l'équipe "Conception et Sécurité de Systèmes", et en particulier Paul Amblard, Jean-Louis Bergerand, Mohammed Moalla, Daniel et Eric Pilaud;

le Laboratoire d'analyse numérique, qui, en me laissant l'usage de son équipement de traitement de textes, m'a permis de réaliser ce document, ainsi que le service de reprographie de l'IMAG, qui en a assuré le tirage.

Je remercie enfin ma petite famille, qui a supporté avec patience un thésard anxieux, distrait, et souvent acariâtre.

PLAN DE L'OUVRAGE

DEUXIEME PARTIE :
OUTILS D'ANALYSE DES SYSTEMES TEMPORISES

CHAPITRE 1 : INTRODUCTION

Afin de situer les motivations de ce travail, et les idées qui le sous-tendent, il nous faut commencer, au risque d'énoncer quelques lieux communs, par un ensemble de considérations concernant l'importance et les qualités souhaitables d'un formalisme de description du comportement des systèmes informatiques, dans une démarche rigoureuse de conception ou de vérification de ces systèmes.

1.1. VERIFICATION, CONCEPTION CERTIFIEE ET FORMALISATION

Tout processus de vérification formelle d'un système informatique a pour but de démontrer la "conformité" entre le comportement du système réalisé et son comportement souhaité. Afin d'assurer un caractère rigoureux à cette démonstration, trois éléments sont nécéssaires:

- La description formelle du comportement souhaité, ou spécification initiale du système, construite à partir d'une "intention" informelle.

- La description formelle du comportement réalisé. En ce qui concerne les réalisations logicielles, cette description se déduit de la sémantique du langage de programmation utilisé; dans le cas des réalisations matérielles, le comportement des composants peut être approché à divers niveaux d'abstraction (architectural, logique, électrique).

- Une relation de conformité, équivalence ou préordre (simulation), sur l'ensemble des comportements.

Ces trois éléments sont aussi des préalables nécéssaires de toute démarche de conception certifiée. Une telle démarche, motivée par la difficulté constatée de prouver à postériori une réalisation, consiste, en général à construire progressivement la réalisation, par transformations successives et certifiées des spécifications.

Le premier fondement d'une démarche rigoureuse de conception ou de validation de systèmes informatiques est donc la formalisation de la notion de comportement. Or, le choix d'un formalisme particulier n'influence pas seulement la commodité, mais aussi la rigueur de la démarche. En effet, la correction d'une réalisation ne peut être établie que relativement à la validité des trois éléments cités précédemment, à savoir:

- à la conformité entre la spécification formelle et l'intention initiale. Cette intention étant, par définition, informelle, cette conformité ne peut évidemment pas être établie formellement. C'est pourquoi une qualité fondamentale que l'on peut exiger d'un formalisme de spécification est de permettre une traduction aussi naturelle que possible de l'intention initiale, afin de minimiser les risques de distorsions, au cours de la formalisation.

- à la conformité entre le comportement du système réalisé et sa description. Concernant les réalisations logicielles, cette conformité ne dépend que de la correction du compilateur utilisé, relativement à la sémantique du langage et de la machine. Dans le domaine des réalisations matérielles, ceci impose que le formalisme permette une description précise du fonctionnement des composants (portes, bascules, connexions, voire même des transistors ...).

- à la "validité" de la relation de conformité entre comportements. En ce qui concerne les systèmes déterministes, cette conformité est facile à appréhender, en termes d'égalité de fonctions. Il est beaucoup plus problématique de définir une notion d'équivalence pour des systèmes indéterministes ou parallèles, équivalence assez fine pour préserver les propriétés essentielles - notamment les propriétés de vivacité - sans pour autant distinguer des comportements intuitivement indiscernables.

1.2. SYSTEMES TEMPORISES

Il est une classe de systèmes dont le comportement se formalise aisément: Ce sont les systèmes que l'on peut considérer comme des transformateurs d'états. L'exécution d'un tel système ne dépend que de son état initial, et son résultat, si l'exécution se termine, est l'état final atteint. Le système réalise ainsi une relation (une fonction, s'il est déterministe) sur un ensemble d'états, relation qui le définit complètement, du point de vue de sa correction : La succession effective des états intermédiaires parcourus, et des actions effectuées au cours de son exécution, n'intervient que dans l'évaluation de critères secondaires, concernant ses performances, son aptitude à la modification, ses paramètres de sureté de fonctionnement etc... De nombreux modèles ont été proposés pour cette classe de systèmes, qui ont conduit aux méthodes classiques de spécification [Liskov & Zilles] et de preuve de programmes [Floyd], [Hoare 69], ainsi que d'expression de la sémantique des langages [Hoare & Lauer], [Sethi].

Il reste que cette formalisation en termes de relation sur un ensemble d'états n'est pas directement applicable à toute une classe de systèmes informatiques, que nous désignerons ici sous le terme, volontairement vague, de "systèmes temporisés" : Il s'agit des systèmes qui reçoivent leurs entrées et délivrent leurs sorties tout au long de leur exécution, laquelle n'est pas nécéssairement finie. Un processus dans un système parallèle, un système interactif ou temps réel, sont des exemples de tels systèmes, dont le résultat ne peut être défini par un état final, mais plutôt par une séquence de sorties en correspondance avec une séquence d'entrées.

Plusieurs raisons motivent l'usage du terme de "systèmes temporisés" dans ce contexte:

- D'une part, la correction du résultat dépend, en général, non seulement de la suite des valeurs émises en réponse à une séquence d'entrées, mais également des "instants" où ces valeurs sont émises, ces instants étant identifiés soit relativement aux instants de réception des entrées (temps logique, ou ordinal), soit relativement à une échelle de temps physique ("temps réel"). Par exemple:

  . Dans un système d'interrogation interactif, il n'est pas indifférent que la réponse du système à une requête soit délivrée avant ou après la requête suivante de l'usager.

  . Dans un système temps réel, on pourra imposer un temps de réponse entre une entrée et une sortie, comme, par exemple entre l'apparition d'une situation dangereuse et l'émission d'une alarme.

- D'autre part, il s'agit de systèmes dont le comportement peut dépendre, même du point de vue de la correction, de paramètres temporels. Ainsi, le séquencement des actions dans un système parallèle dépend-t-il évidemment de la vitesse d'exécution des divers processus qui le composent.

C'est d'ailleurs dans le contexte de la programmation parallèle que la modélisation du comportement des systèmes temporisés a été particulièrement étudiée. Or, les outils logiciels de la programmation parallèle sont essentiellement des mécanismes de synchronisation et de communication, dont le rôle est, précisément, de rendre le comportement externe d'un système indépendant des temps d'exécution des processus qui le composent, ceci afin que la correction d'un programme soit indépendante de paramètres inconnus, voire variables, tenant aux performances du matériel, ou à la charge du système hôte. Cette indépendance vis à vis du temps d'exécution présente des avantages évidents, concernant la portabilité des systèmes, et la facilité à les concevoir, les prouver et les modifier. Par suite, une caractéristique commune à la plupart des modèles du parallélisme est de ne prendre en compte aucune notion métrique de temps: Deux systèmes présentant la même succession d'entrées et de sorties sont formalisés de manière équivalente. Cette approche n'est donc pas applicable aux systèmes dont la correction dépend du temps d'exécution, c'est à dire, principalement, à deux types de systèmes:

- Les systèmes temps réel, dans la mesure où, d'une part, leurs spécifications comprennent des contraintes temporelles (temps de réponse, fréquences d'échantillonage etc...) et où, d'autre part, la nécéssité de satisfaire à ces contraintes conduit souvent le concepteur à faire l'économie de mécanismes de synchronisation pénalisant les performances, en tenant compte explicitement des temps d'exécution.

- Les systèmes matériels, pour lesquels les problèmes de portabilité ne se posent pas, et dont la réalisation est très souvent optimisée par la prise en compte des délais de réponse (temps de franchissement d'une porte, de stabilisation d'une bascule ...), délais qui sont connus assez précisément.

On distingue ainsi deux classes de systèmes temporisés, selon la notion de temps à laquelle ils font appel:

- Dans les systèmes asynchrones, le temps n'intervient que pour définir une relation d'ordre partiel entre les évènements internes ou externes, survenant au cours de l'exécution du système (temps ordinal). C'est pourquoi ces systèmes sont généralement modélisés comme des systèmes séquentiels indéterministes, dont l'ensemble des comportements est l'ensemble des suites d'évènements totalement ordonnés de manière compatible avec l'ordre partiel (entrelacement d'actions atomiques).

- On entre dans le domaine des systèmes synchrones dés que l'occurrence simultanée de deux évènements revêt une signification particulière. Dans ce contexte, le temps n'est plus seulement ordinal, mais aussi métrique, puisque, dés lors que l'on peut forcer l'occurrence simultanée de deux évènements, on peut synchroniser ("piloter", selon le vocabulaire de [Austry & Boudol]) l'exécution d'un système par une horloge.

1.3. LES APPROCHES DE LA FORMALISATION DU COMPORTEMENT DES SYSTEMES

On peut distinguer, principalement, deux approches de la formalisation du comportement des systèmes informatiques, que nous appellerons respectivement formalisations algorithmique et comportementale.

1.3.1. La formalisation algorithmique

Elle consiste à modéliser le système par une relation de succession sur un ensemble d'états. L'état du système, à un instant donné, résume toute l'information sur son comportement passé, nécéssaire à l'élaboration de son comportement futur, c'est à dire de son état suivant (ou des divers états suivants, dans le cas d'un système indéterministe). La relation de succession est exprimée au moyen d'un ensemble de relations élémentaires, qui font partie du modèle. La plupart des modèles du parallélisme, synchrone ou asynchrone, participent de cette approche. Par exemple, l'ensemble des états d'un réseau de Pétri [Peterson] est l'ensemble de ses marquages, la seule relation élémentaire entre les marquages étant définie par l'opération de mise à feu d'une transition. De même, on peut assimiler l'ensemble des agents de SCCS [Milner 82] à un ensemble d'états, entre lesquels les actions définissent des relations élémentaires.

La formalisation algorithmique présente des avantages indéniables:

- Elle se prête bien à la preuve formelle, en particulier au moyen de raisonnements inductifs (On étudie la fermeture transitive de la relation de succession, qui est un plus petit point fixe).

- Elle se prête bien à la description de la sémantique des langages, ainsi qu'à celle des composants matériels au niveau architectural.

- Dans une démarche de conception progressive, une description de type algorithmique conduit de manière naturelle, voire même automatisable, à une réalisation.

Les critiques que l'on peut faire à cette approche concernent essentiellement son usage à l'étape de la spécification initiale. En effet, les formalismes algorithmiques conduisent à définir une machine abstraite, ayant le comportement souhaité, plutôt que ce comportement lui-même. La définition d'une telle machine nécessite généralement un travail d'analyse conséquent, au cours duquel peuvent s'introduire des erreurs. Or ces erreurs de spécification sont les plus graves et les plus couteuses: En effet, nous avons déjà noté qu'elles n'étaient pas décelables au cours de la preuve formelle. Elles ont donc de fortes chances de persister dans le système jusqu'à sa phase de réception ou d'exploitation, et donc, de venir remettre en cause la conception dans son ensemble. Un autre inconvénient, qui découle des remarques précédentes, est le risque de sur-spécification, c'est à dire le risque d'effectuer, dés la spécification initiale, un certain nombre de choix de réalisation, fermant ainsi la porte à des solutions acceptables, et eventuellement plus avantageuses. En effet, le spécificateur est souvent conduit, par commodité, à introduire dans sa description certains états internes de la machine abstraite. Or la définition des états internes et de leur succession relève clairement de la tâche de conception. Un dernier problème soulevé par l'approche algorithmique résulte encore de l'introduction des états internes dés la spécification, et concerne la définition de la relation de conformité. En effet, cette relation doit, évidemment, faire abstraction des états internes, en ne portant que sur le comportement externe des systèmes. De là résultent les difficiles problèmes de définition d'une "bonne" équivalence observationnelle [Milner 80], [Milner 82], [André & Boeri], [Darondeau & Kott], [Hennessy & de Nicola] entre machines à états.

Sans nier les qualités de la formalisation algorithmique aux niveaux inférieurs de la conception, nous lui préférerons, en ce qui concerne l'étape des spécifications initiales, un mode comportemental de description.

1.3.2. La formalisation comportementale

Elle consiste à considérer le système comme une "boite noire", recevant ses entrées de son environnement, et lui restituant ses sorties. Dans cette approche, on cherchera donc à décrire ce que le système fait, ou doit faire, sans dire comment il le fait. C'est le mode de spécification habituellement appliqué aux programmes séquentiels, lorsqu'on spécifie un tél programme par un couple de prédicats [Floyd], [Hoare 69], ou par une fonction [Scott], [Tennent]. Si l'on veut appliquer cette approche aux systèmes temporisés, il convient d'éviter d'avoir à définir les états d'un système, c'est à dire, comme nous l'avons remarqué plus haut, le résumé de l'histoire passée du système, nécéssaire à tout instant à l'élaboration de son avenir. Un formalisme comportemental doit donc permettre la manipulation de toute l'histoire d'un système. Ces considérations ont conduit certains auteurs [Abrial 82], [Hoare 81], [Kahn & McQueen], à assimiler un système temporisé à un transformateur d'histoires, adaptant ainsi aux systèmes temporisés la modélisation des systèmes séquentiels comme transformateurs d'états. Dans cette optique, l'histoire d'une variable est la séquence de ses valeurs au cours du temps (Cette notion d'histoire est à rapprocher de la notion de variable en LUCID [Ashcroft & Wadge]). Un système réalise alors une relation entre l'histoire de ses entrées et celle de ses sorties, relation qui définit complètement son comportement externe.

1.4. PLAN DE LA THESE

Le fondement de ce travail est un modèle comportemental applicable à tous les systèmes temporisés, et permettant donc la prise en compte d'une notion métrique de temps. Ce modèle est issu de préoccupations concernant la spécification des systèmes temps réel, préoccupations qui se sont progressivement élargies, d'une part vers une classe plus générale de systèmes, incluant les systèmes asynchrones, et d'autre part vers les problèmes de conception, d'analyse et de preuve de ces systèmes. Nous avons ainsi suivi un chemin inverse du courant qui se fait jour, ces dernières années, où des travaux dédiés au parallélisme évoluent vers le domaine des systèmes synchrones et temps réel.

Dans une première partie, nous présenterons notre formalisme, tel que nous le concevons comme outil de spécification. Dans cette optique, nous chercherons donc surtout à permettre une formalisation naturelle d'une intention informelle, plutôt qu'à définir un modèle complètement axiomatisé. Notre formalisme, présenté au chapitre 2, est fondé sur les notions d'évènement et de variable, appréhendées en termes de suites d'instants et de valeurs. Quoique quelques outils soient proposés pour définir des relations entre suites, il est sous-entendu que la spécification et la preuve d'un système peuvent faire appel à toute la richesse du langage mathématique. A titre d'illustration, cette approche est appliquée, au chapitre 3, à la conception certifiée d'un arbitre de bus distribué, depuis ses spécifications initiales jusqu'à sa réalisation matérielle.

Dans une deuxième partie, nous étudierons des méthodes d'analyse de descriptions de systèmes logiques, au niveau algorithmique, méthodes utilisables, par exemple, pour l'évaluation des performances ou pour le choix de l'architecture d'implantation. Pour cela, nous construirons un calcul formel sur les évènements. Dans ce calcul (chapitre 4), l'ensemble des évènements est plongé dans l'anneau des séries formelles à une variable, muni d'une relation d'ordre, ce qui permet d'appliquer les transformations algébriques usuelles sur ces séries, à l'analyse d'une description en évènements. Nous montrerons au chapitre 5 que ce calcul permet d'exprimer le fonctionnement de nombreux systèmes logiques, en particulier les systèmes modélisables au moyen de diverses extensions des réseau de Pétri. Nous donnerons aussi des exemples de description et d'analyse de problèmes à l'aide du calcul, en particulier dans le domaine de l'ordonnancement.

La principale difficulté du calcul formel en évènements concerne le traitement des inéquations, qui sera abordé au chapitre 6. Enfin, le chapitre 7 traite des résultats approchés, concernant le fonctionnement asymptotique des systèmes, que l'on peut obtenir en appliquant aux évènements les résultats classiques concernant les informations que fournissent les transformées de Laplace, au voisinage de zéro, sur le comportement de leurs originaux à l'infini.

PREMIERE PARTIE

SPECIFICATION ET PREUVE DE SYSTEMES TEMPORISES

CHAPITRE 2 :

UN FORMALISME DE DESCRIPTION DU COMPORTEMENT DES SYSTEMES TEMPORISES

Notre premier travail concerne la formalisation, en termes mathématiques, de l'évolution au cours du temps des divers éléments - évènements, variables - composant les entrées-sorties d'un système. A partir de cette formalisation, le spécificateur pourra tirer pleinement profit de toute la richesse du langage mathématique pour décrire la relation que doit réaliser son système. Les avantages du langage mathématique dans le domaine de la spécification ont été reconnus [Abrial 78], [Caplain], concernant sa puissance d'expression, sa rigueur - tant au niveau de la précision qu'il autorise que du consensus qui s'est établi quant à sa sémantique -, et l'arsenal de résultats dont on dispose pour y effectuer des déductions formelles. Cette étape de conceptualisation sera guidée par le domaine d'application visé, à savoir les systèmes informatiques temporisés, dont les caractéristiques sont le caractère discret des évolutions et le rôle particulier assigné à la dimension temporelle. Nous tenterons, tout au long de l'exposé, de justifier les options prises, notamment à la lumière de l'expérience que nous avons tirée de l'examen de plusieurs cahiers des charges réels, relevant du domaine des systèmes temps réel [Caspi & Halbwachs 79].

2.1. CONCEPTS DE BASE

2.1.1. Temps

Nous nous réfèrerons toujours à un repère de temps universel, qui sera celui d'un observateur extérieur au système. Il est clair que le problème, étudié dans [Lamport], de la mesure relative du temps par plusieurs horloges locales, dans un système distribué, ne se pose pas, au niveau de la description.

Nous noterons $\mathbb{T}$ l'ensemble des instants. Dans la plupart des cas, on peut considérer cet ensemble comme discret, et l'assimiler à l'ensemble $\mathbb{Z}$ des entiers relatifs. Cependant, cette discrétisation du temps risque de conduire à des simplifications abusives, notamment dans le contexte des systèmes distribués; c'est pourquoi nous présenterons le modèle en supposant le temps continu ($\mathbb{T} = \mathbb{R}$), et nous n'introduirons l'hypothèse de temps discret que lorsqu'elle sera nécessaire pour établir certains résultats spécifiques.

Les éléments de $\mathbb{T}$ seront appelés instants ou dates, lorsqu'on considèrera la structure affine de $\mathbb{T}$, et délais ou durées lorsqu'on considérera sa structure vectorielle. On notera $\overline{\mathbb{T}}$ l'ensemble $\mathbb{T} \cup \{ -\infty , +\infty \}$.

2.1.2. Evènements

Les objets primitifs que nous formaliserons sont les évènements et les variables. Intuitivement, la notion d'évènement recouvre tout ce que l'on a coutume d'appeler un changement d'état du système ou de son environnement (même s'il est paradoxal de définir en termes d'états un objet primitif d'un modèle qui veut précisément faire abstraction de la notion d'état !). Ainsi, l'affectation d'une valeur à une variable, le basculement d'une condition, l'exécution d'un rendez-vous, l'arrivée d'un signal d'horloge, sont des exemples d'évènements. Un tel évènement peut survenir plusieurs fois au cours de la vie d'un système, mais, puisque nous nous intéressons aux systèmes discrets, nous supposerons qu'il ne peut survenir qu'un nombre fini de fois au cours d'une période

finie. A un niveau d'abstraction adéquat, nous pouvons décider qu'une occurrence d'un évènement n'a pas de durée: Elle sera considérée comme une coupure dans le temps, qui sépare les périodes antérieures et postérieures à cette occurrence. Après ces préliminaires informels, nous pouvons formaliser la notion d'évènement.

Fidèles à notre projet de manipuler des histoires, nous caractériserons un évènement e par la suite croissante de ses dates d'occurrences, appréhendée au moyen de sa fonction "date", notée τe (ou $\tau(e)$). Cette fonction applique $\overline{\mathbb{N}}$ dans $\overline{\mathbb{T}}$, et sa valeur en n est la date de la n-ième occurrence de e. Elle est supposée vérifier les propriétés suivantes:

[$\tau 1$] $\quad \tau e$ est croissante, au sens large

[$\tau 2$] $\quad \tau e(0) = -\infty$

[$\tau 3$] $\quad \tau e(1) > -\infty$

[$\tau 4$] $\quad \tau e(+\infty) = \lim_{n \to \infty} \tau e(n) = +\infty$

Commentaires:

La propriété [$\tau 1$] exprime que les occurrences sont numérotées par ordre chronologique large. Ceci n'exclut donc pas qu'un même évènement puisse avoir plusieurs occurrences simultanées. Cette éventualité, à première vue surprenante, peut être justifiée par l'exemple suivant: Soit une ressource r partagée par plusieurs processus séquentiels $p_1 \ldots p_n$, et supposons que l'on veuille décrire les demandes d'accés à la ressource par les processus. On peut se placer du point de vue des processus, et décrire les évènements d_i (i=1..n) survenant, respectivement, chaque fois que le processus p_i demande la ressource. On peut aussi décrire ce système du point de vue de la ressource, en définissant l'évènement d correspondant à la demande de la ressource par l'un quelconque des processus. Cet évènement peut alors avoir plusieurs occurrences simultanées.

Les propriétés [$\tau 2$] et [$\tau 3$] ne sont que des conventions consistant d'une part à rajouter à tout évènement une occurrence de numéro zéro, survenue "au début des temps", qui sera

commode, par exemple, pour désigner la prise de valeur initiale d'une variable, et d'autre part à identifier univoquement la numérotation des dates d'occurrence.

Enfin, la propriété [τ4] exprime l'hypothèse citée plus haut, qui contraint un évènement à ne survenir qu'un nombre fini de fois au cours d'une période finie.

2.1.3. Variables

L'évolution d'une variable (au sens informatique) au cours de la vie d'un système sera modélisée par la suite de ses valeurs, et par un évènement qui survient chaque fois que la variable prend une nouvelle valeur dans cette suite. Une variable X est donc caractérisée par un triplet (Dx, νx, x), où:

- Dx est le domaine des valeurs de X;
- νx est une application de $\mathbb{N}$ dans Dx, dont la valeur en n est la n-ième valeur prise par X au cours de son évolution.
- x est un évènement tel que X prend la valeur νx(n) à l'instant τx(n).

Commentaires:

- Remarquons que deux valeurs successives dans la suite des valeurs d'une variable X peuvent être égales. Une occurrence de l'évènement x ne correspond donc pas nécéssairement à un changement effectif de valeur.
- νx(0) est la valeur initiale de X.
- Nous aurions pu décrire l'évolution d'une variable par une fonction de $\mathbb{T}$ dans Dx, donnant la valeur de la variable à chaque instant. Nous n'avons pas choisi cette formalisation, en raison des ambiguïtés que nous avons relevées dans des spécifications de systèmes discrets, dont le rédacteur, accoutumé aux réalisations analogiques, décrivait les variables comme si celles-ci variaient de manière continue. Par exemple, dans de telles spécifications, on peut trouver la description d'une sortie s, élaborée en fonction des entrées a et b, sous la forme d'une équation s = f(a,b). Or l'interprétation naturelle

de cette équation - qui est qu'à tout instant t, on doit avoir s(t) = f(a(t),b(t)) - est manifestement irréalisable stricto sensu, puisqu'elle suppose que la fonction f puisse être évaluée en un temps nul. De plus, si l'on tolère un délai de réponse, cette spécification devient ambigüe : Il n'est pas clair si la sortie s doit être réévaluée à chaque changement de l'une ou l'autre des entrées a et b, ou seulement lorsque les deux entrées ont changé, ou encore à une fréquence indépendante des fréquences d'échantillonage de a et b. Ces raisons motivent notre parti pris de mettre l'accent sur le caractère discret de l'évolution d'une variable. Nous verrons plus loin que notre formalisation permet quand même d'exprimer la valeur d'une variable à chaque instant, mais nous avons voulu que cette expression ne soit pas primitive.

2.1.4. Exemples d'application à la formalisation de contraintes temporelles

Nous avons ainsi défini les seuls objets primitifs de notre modèle, ainsi que les seuls axiomes qui lui sont propres. Nous pourrions en rester là, en affirmant que le comportement temporel de n'importe quel système peut être décrit mathématiquement à l'aide de ces objets. Nous donnons maintenant quelques exemples de spécifications, issu du domaine des systèmes temps réel.

2.1.4.1. Evènements périodiques: Dans le domaine du contrôle de processus ou du traitement du signal, on a souvent affaire à des évènements périodiques. La stricte périodicité d'un évènement e, de période Δ, peut être exprimée dans notre modèle, par la contrainte suivante:

$$\forall n \in \mathbb{N}^* , \tau e(n+1) = \tau e(n) + \Delta$$

Cependant, il n'existe pas d'évènement strictement périodique. Généralement, le terme d'évènement périodique apparaissant dans un cahier des charges, doit être interprété d'une manière plus souple, comme, par exemple:

- en termes de période maximum: L'intervalle de temps séparant deux occurrences successives de e doit être inférieur à Δ:

$$\forall n \in \mathbb{N}^* , \tau e(n+1) \leqslant \tau e(n) + \Delta$$

- en termes de période moyenne: e doit survenir une fois et une seule dans tout intervalle de durée Δ, à compter d'un instant initial t_0:

$$\forall n \in \mathbb{N}^* , t_0 + (n-1)\Delta \leqslant \tau e(n) < t_0 + n\Delta$$

2.1.4.2. Temps de réponse: Lorsqu'une variable de sortie Y est élaborée en fonction d'une variable d'entrée X (Y=f(X)), il est courant que les spécifications du système imposent un temps de réponse, δ, entre l'acquisition d'une valeur de X et l'émission de la valeur correspondante de Y. Cependant, nous avons rencontré, dans des cahiers des charges réels, ce type de contrainte appliqué à des situations où l'échantillonage de X et l'émission de Y étaient périodiques (par exemple, au sens de la période maximum définie ci-dessus), avec des périodes différentes. Dans ce cas, la contrainte de temps de réponse peut être interprétée, au moins, de trois manières différentes:

- Soit les périodes effectives de X et de Y doivent être égales, et il y a correspondance bi-univoque entre leurs valeurs:

$$\forall n \in \mathbb{N}^* , \nu y(n) = f(\nu x(n)) \text{ et } \tau x(n) \leqslant \tau y(n) \leqslant \tau x(n) + \delta$$

- Soit Y peut être calculée à une fréquence inférieure à celle de X, mais chaque valeur de Y est élaborée à partir d'une valeur de X datant au plus de δ :

$$\forall n \in \mathbb{N}^* , \exists m \in \mathbb{N}^* \text{ tel que}$$
$$\nu y(n) = f(\nu x(m)) \text{ et } \tau x(m) \leqslant \tau y(n) \leqslant \tau x(m) + \delta$$

- Soit Y doit être calculée à une fréquence au moins égale à celle de X, et chaque acquisition d'une nouvelle valeur de X provoque l'élaboration de Y dans un délai inférieur à δ (Cette situation se présente lorsque X n'est pas le seul paramètre de la fonction f) :

$$\forall m \in \mathbb{N}^* \ , \ \exists n \in \mathbb{N}^* \text{ tel que}$$
$$\nu y(n) = f(\nu x(m)) \text{ et } \tau x(m) \leqslant \tau y(n) \leqslant \tau x(m) + \delta$$

Ces exemples, très simples, illustrent l'utilité du formalisme pour lever certaines ambiguïtés inhérentes à l'usage de la langue naturelle. Par contre, ils mettent aussi en évidence le caractère rudimentaire de nos notations et la lourdeur qui en résulte, en particulier du fait que nous n'avons pas encore les moyens de manipuler les suites globalement, ce qui nous impose de décrire les contraintes portant sur chacun de leurs termes, à grand renfort de quantificateurs. C'est pourquoi, sans vouloir interdire la notation séparée des termes d'une suite, ni restreindre l'usage du langage mathématique dans toute sa généralité, nous allons définir maintenant certains outils qui seront d'un usage courant pour la description des comportements.

2.2. OUTILS DE DESCRIPTION ET PREMIERS RESULTATS

2.2.1. Compteurs

Quoique la donnée de τe définisse complètement les dates d'occurrence de l'évènement e, il est apparu utile de considérer un évènement d'un autre point de vue, qui est celui de ses compteurs d'occurrences: Si e est un évènement, on lui associe deux applications, μe et $\mu^+ e$, de $\overline{\mathbb{T}}$ dans $\overline{\mathbb{N}}$, définies comme suit:

$$\mu e = \lambda t.\text{Card} \{ n \in \mathbb{N}^* \mid \tau e(n) < t \}$$

$$\mu^+ e = \lambda t.\text{Card} \{ n \in \mathbb{N}^* \mid \tau e(n) \leqslant t \}$$

$\mu e(t)$ (resp. $\mu^+ e(t)$) est donc le nombre d'occurrences de e - abstraction faite de l'occurrence d'indice zéro - survenues strictement (resp. au sens large) avant t. D'après leurs définitions et les propriétés de τe, ces fonctions vérifient les propriétés suivantes:

[μ1] μe et $\mu^+ e$ sont croissantes;

[μ2] Leurs restrictions à $\mathbb{T}$ sont à valeurs dans $\mathbb{N}$ (d'après [τ4]);

[μ3] $\mu e(-\infty) = -1$;

[μ4] $\mu^+ e(-\infty) = 0$;

[μ5] Si $\mathbb{T} = \mathbb{R}$, μe (resp. $\mu^+ e$) est continue à gauche (resp., à droite);

[μ6] $\mu e \leqslant \mu^+ e$;

Commentaires:

Dans l'énoncé de [μ6], comme dans toute la thèse, l'ordre $\leqslant$ sur les fonctions est l'ordre partiel point par point ($f \leqslant g \iff \forall x,\ f(x) \leqslant g(x)$).

La propriété μ3, qui n'est guère intuitive, sera justifiée algébriquement au §2.3.1.

La donnée de μe ou de $\mu^+ e$ définit complètement les dates d'occurrences de e, puisque la fonction τe s'en déduit:

$$\tau e = \lambda n.\sup \{ t \in \mathbb{T} \mid \mu e(t) < n \} = \lambda n.\inf \{ t \in \mathbb{T} \mid \mu^+ e(t) \geqslant n \}$$

en admettant que $\sup(\emptyset) = -\infty$.

L'utilité des compteurs d'occurrences a déjà été démontrée, en particulier pour la description et la programmation de la synchronisation entre processus [Robert & Verjus], [Reed & Kanodia]. Notons que nous pourrons écrire des invariants plus généraux que ceux de [Robert & Verjus], dans la mesure où nous pourrons exprimer des invariants non seulement instantanés - par exemple $\mu e \leqslant \mu f$ - mais aussi présentant une "épaisseur temporelle" - par exemple $\mu e \leqslant \mu f \circ (I + \Delta)$, où I dénote l'identité et Δ dénote la fonction constante $\lambda t.\Delta$, de $\mathbb{T}$ dans $\mathbb{T}$. C'est principalement cette possibilité d'exprimer des contraintes "temporellement épaisses" qui nous permettra de nous affranchir de la notion d'état.

D'autres fonctions utiles se déduisent des fonctions déjà obtenues, par composition fonctionnelle.

2.2.2. Trajectoires d'une variable

On définit deux fonctions donnant la valeur d'une variable X à chaque instant:

$$\tilde{\nu}x = \nu x \circ \mu x \quad \text{et} \quad \tilde{\nu}^{+}x = \nu x \circ \mu^{+} x$$

Commentaires:

> Cette définition de la valeur instantanée d'une variable par deux fonctions peut surprendre. Elle évite, en fait, de répondre à la question oiseuse "quelle est la valeur d'une variable à l'instant où celle-ci change de valeur", tout en permettant de dénoter ses valeurs juste avant ($\tilde{\nu}x$) et juste après ($\tilde{\nu}^{+}x$) son changement.

2.2.3. Dernière occurrence

Les fonctions θe et $\theta^{+}e$ donnent, à chaque instant t, la date de la dernière occurrence de l'évènement e précédant strictement (resp. au sens large) t:

$$\theta e = \tau e \circ \mu e \quad \text{et} \quad \theta^{+}e = \tau e \circ \mu^{+} e$$

On a:

[θ1] $\quad \theta e < \theta^{+}e$ (d'après [τ1] et [μ6]) ;

[θ2] $\quad \theta^{+}e < I$, ou I est l'identité de $\mathbb{T}$ dans $\mathbb{T}$ (d'après la définition de $\mu^{+}e$) ;

Les fonctions $\mu e \circ \tau e$ et $\mu^{+} e \circ \tau e$, pour lesquelles nous n'introduirons pas de notations particulières, ont des propriétés analogues:

[μ7] $\quad \mu e \circ \tau e < I - 1$

[μ8] $\quad I < \mu^{+} e \circ \tau e$

où I dénote maintenant l'identité de $\mathbb{N}$ dans $\mathbb{N}$ et 1 est la fonction constante $\lambda x.1$ de $\mathbb{N}$ dans $\mathbb{N}$. Plus généralement, nous ne nommerons pas différemment l'identité de $\mathbb{N}$ dans $\mathbb{N}$ et l'identité de $\mathbb{T}$ dans $\mathbb{T}$, le contexte permettant toujours de lever l'ambiguïté. De la même façon, un élément n de $\mathbb{N}$ pourra aussi désigner, selon le contexte, les fonctions constantes $\lambda x.n$, de $\mathbb{N}$ ou $\mathbb{T}$ dans $\mathbb{N}$, et un élément t de $\mathbb{T}$ pourra désigner les fonctions constantes $\lambda x.t$ de $\mathbb{N}$ ou $\mathbb{T}$ dans $\mathbb{T}$.

2.2.4. Exemple d'application à la description et l'analyse d'un système asynchrone

Cet exemple illustre l'utilisation des fonctions de dernière occurrence pour dénoter des relations temporelles non triviales entre variables. Il concerne un multi-calculateur tolérant les pannes, proposé par la société SFENA [Billoir] et destiné à assumer des tâches de pilotage automatique d'avion.

On considère six calculateurs C_i (i=1...6) organisés en anneau, de telle sorte que chaque calculateur puisse diffuser ses résultats vers ses trois successeurs dans l'anneau. Une quantité v, variant continument au cours du temps, est échantillonnée périodiquement par trois capteurs redondants, K_1, K_2, K_3, chaque capteur K_i étant connecté au calculateur C_i (cf. figure 1).

Périodiquement, chaque capteur K_i échantillonne une valeur de v et l'envoie à son calculateur C_i. Soit X_i (i=1...3) la variable correspondante. Les calculateurs connectés à un capteur diffusent les valeurs reçues de leurs capteurs, les autres calculateurs diffusent la valeur moyenne des valeurs qu'ils reçoivent. Soit Y_i (i=1...6) le résultat émis par le calculateur C_i. En l'absence de panne, nous pouvons décrire les variables du système comme suit:

$$\forall i=1...3,\ \tilde{v}x_i = v \circ \Theta x_i$$

$$\tilde{v}y_i = \tilde{v}x_i \circ \Theta y_i$$

$$\forall i=4...6,\ \tilde{v}y_i = \frac{1}{3}\left[\tilde{v}y_{i-1} + \tilde{v}y_{i-2} + \tilde{v}y_{i-3}\right] \circ \Theta y_i$$

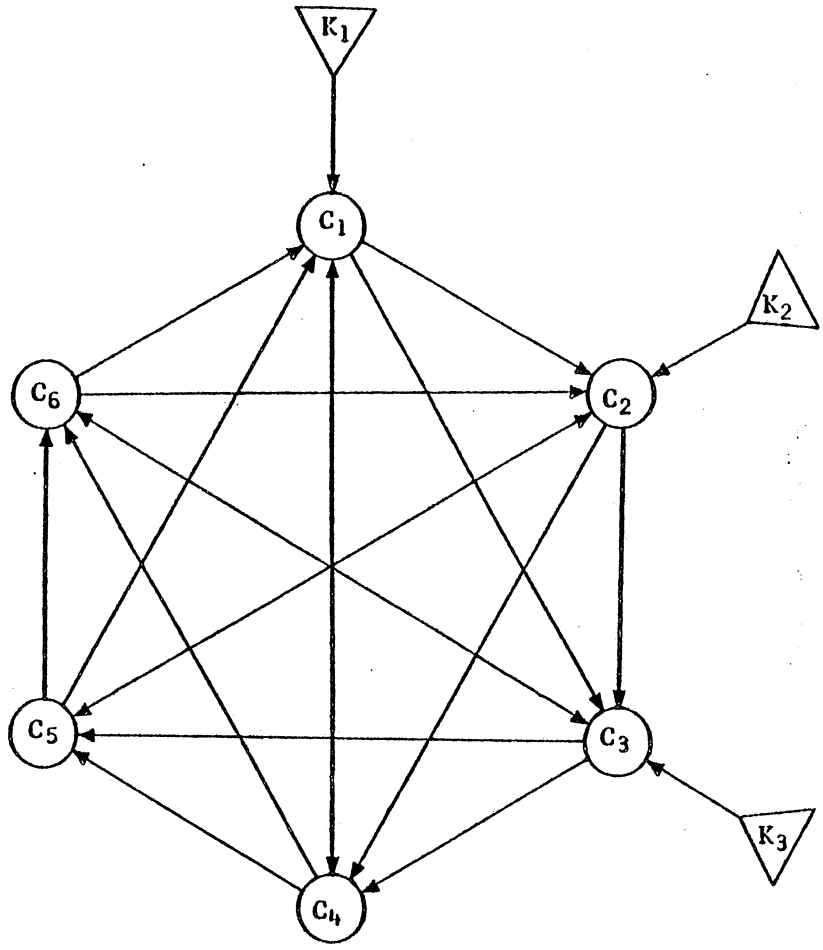


Figure 1

Calculateur en anneau

On en déduit l'expression suivante de $\tilde{v}y_6$:

$$\tilde{v}y_6 = \frac{1}{3} v \circ \theta x_3 \circ \theta y_3 \circ \theta y_6 + \frac{1}{9} \Sigma_{i=1}^{3} v \circ \theta x_i \circ \theta y_i \circ \theta y_4 \circ \theta y_6$$
$$+ \frac{1}{9} \Sigma_{i=2}^{3} v \circ \theta x_i \circ \theta y_i \circ \theta y_5 \circ \theta y_6$$
$$+ \frac{1}{27} \Sigma_{i=1}^{3} v \circ \theta x_i \circ \theta y_i \circ \theta y_4 \circ \theta y_5 \circ \theta y_6$$

Dans cette expression, un terme comme

$$v \circ \theta x_2 \circ \theta y_2 \circ \theta y_4 \circ \theta y_5 \circ \theta y_6(t)$$

signifie " la valeur de v à l'instant de la dernière prise de valeur de

X_2, précédant la dernière prise de valeur de Y_2, précédant ..., précédant la dernière prise de valeur de Y_6, précédant t".

Supposons maintenant que les échantillonnages et les émissions soient périodiques, et que - quoique les périodes puissent être légèrement différentes, puisque chaque calculateur possède sa propre horloge - on connaisse une borne supérieure Δ de ces périodes. Alors, toutes les fonctions θ considérées satisfont:

$$I - \Delta \leqslant \theta < I$$

Sous ces hypothèses, on peut évaluer, à l'aide de l'expression de $\tilde{\nu}y_6$, une borne supérieure de l'erreur $|v(t) - \tilde{\nu}y_6(t)|$, borne qui peut servir à régler le seuil de détection des pannes. Pour cela, on remplace $v(t)$ par αt, où α est une borne supérieure de la dérivée de v, et, à l'aide de l'inéquation sur les fonctions θ, on obtient:

$$\forall t \ , \quad |v(t) - \tilde{\nu}_6(t)| \leqslant \frac{34}{9} \ \alpha \ . \ \Delta$$

Il est clair que ce résultat pourrait être obtenu autrement; cependant, notons qu'il est obtenu ici de manière systèmatique, ceci étant du au fait que l'on a pu formaliser très précisément le fonctionnement, relativement complexe, de ce système asynchrone.

2.2.5. Evènements à occurrences simples

Contrairement aux fonctions τe, μe et $\mu^+ e$, les fonctions Θe et $\Theta^+ e$ ne caractérisent pas complètement la séquence des dates d'occurrence de l'évènement e, sauf si cette séquence est strictement croissante: Dans ce cas, e sera dit à occurrences simples.

Les quatre propriétés suivantes sont équivalentes et caractérisent les évènements à occurrences simples:

[OS1] $\quad \forall n, \ \tau e(n) \in \mathbb{T} \Rightarrow \tau e(n+1) > \tau e(n)$

[OS2] $\quad \mu^+ e \leqslant \mu e + 1$ sur $\mathbb{T}$

$$\left.\begin{array}{ll} [OS3] & \mu^{+}e \circ \tau e = I \\ [OS4] & \mu e \circ \tau e = I - 1 \end{array}\right\} \text{ sur } \{n \mid \tau e(n) \in \mathbb{T}\}$$

2.2.6. Relations d'ordre sur les évènements

Deux relations d'ordre sur les évènements seront d'un usage courant:

2.2.6.1. Relation de précédence : Si e et f sont deux évènements, on notera $e \leqslant f$ si et seulement si $\mu e \leqslant \mu f$. On a aussi:

$$e \leqslant f \iff \mu^{+}e \leqslant \mu^{+}f \iff \tau e \geqslant \tau f$$

Cette relation munit l'ensemble des évènements d'une structure de treillis, et les opérateurs de bornes inférieure (inf) et supérieure (sup) s'en déduisent directement. De plus, c'est un inf-demi-treillis complet, dont le plus petit élément est l'évènement sans occurrence, noté 0 ($\mu 0 = 0$, $\tau 0 = +\infty$).

Cette relation d'ordre peut s'interpréter en termes de causalité, au sens que si $e \leqslant f$, la n-ième occurrence de e ne peut se produire que postérieurement à la n-ième occurrence de f.

On notera $<$ non pas l'ordre strict induit par $\leqslant$, mais l'ordre strict point par point:

$$e < f \iff \forall n \in \mathbb{N}^{*},\ \tau f(n) \in \mathbb{T} \implies \tau e(n) > \tau f(n)$$
$$\iff \mu^{+}e \leqslant \mu f \text{ sur } \mathbb{T}$$

2.2.6.2. Relation de sous-suite : Si e et f sont deux évènements, on notera $e \sqsubseteq f$ si et seulement si τe est une sous-suite de τf, c'est à dire s'il existe une application r, de $\mathbb{N}$ dans $\mathbb{N}$, strictement croissante, telle que $\tau e = \tau f \circ r$.

La relation $\sqsubseteq$ n'est qu'un préordre sur l'ensemble des suites, mais

c'est un ordre sur les suites croissantes, qui caractérisent les évènements. On a

[SS1] $e \sqsubseteq f \Rightarrow e \lessdot f$

L'ensemble des évènements muni de la relation $\sqsubseteq$ est encore un treillis et un inf-demi-treillis complet, dont les opérateurs de bornes inférieure et supérieure sont notés $\sqcap$ et $\sqcup$.

2.2.7. Opérations sur les évènements

Nous définissons maintenant deux opérations très utiles pour construire des évènements, la somme et la translation.

2.2.7.1. Somme : La somme de deux évènements e et f correspond à la fusion des suites τe et τf. Elle se définit sur les compteurs comme suit:

$$g = e + f \iff \mu g = \mu e + \mu f$$

La somme préserve les relations $\lessdot$ et $\sqsubseteq$. L'évènement 0 est son élément neutre. On a aussi:

[θ3] $g = e + f \Rightarrow \theta g = \sup(\theta e, \theta f)$

et si g est à occurrences simples, l'implication inverse est aussi vraie.

D'autre part, une condition nécéssaire et suffisante pour que e soit une sous-suite de f est qu'il existe un évènement e' tel que $f = e + e'$. Cet évènement e' pourra être noté $e - f$. Les propriétés suivantes en découlent:

[SS2] $e \sqsubseteq f \iff \mu f - \mu e$ est croissante

[SS3] $e \sqsubseteq f \iff \mu^{+} f - \mu^{+} e$ est croissante

[SS4] $e \sqsubseteq f \iff \mu^{+}f - \mu f \geq \mu^{+}e - \mu e$

2.2.7.2. Translation : Soit Δ un délai ($\Delta \in \mathbb{T}$), et e un évènement. On définit l'évènement translaté de e selon Δ, noté $R^{\Delta}e$, par l'une ou l'autre des identités suivantes:

$$\tau(R^{\Delta}e) = \tau e + \Delta$$

$$\mu(R^{\Delta}e) = \mu e \circ (I-\Delta)$$

(Δ est une fonction constante, de $\mathbb{N}$ dans $\mathbb{T}$ dans la première identité, de $\mathbb{T}$ dans $\mathbb{T}$ dans la seconde).

La notation exponentielle est justifiée par les propriétés suivantes:

[R1] $R^{\Delta}R^{\Delta'} = R^{\Delta+\Delta'}$

[R2] R^{0} est l'identité sur les évènements

On a aussi :

[R3] $R^{\Delta}(e+f) = R^{\Delta}e + R^{\Delta}f$

De plus, l'opérateur R^{Δ} préserve les ordres $\leq$ et $\sqsubseteq$. Par rapport à $\leq$, il est extensif si $\Delta<0$ et contractant si $\Delta>0$.

2.2.7.3. Exemple: Spécification d'évènements périodiques: Nous disposons maintenant des outils pour spécifier directement en termes de suites, les divers types de périodicité abordés au §2.1.4.1. Si $t \in \mathbb{T}$, on notera $\underline{t}$ l'évènement tel que $\tau\underline{t}(1) = t$ et $\tau\underline{t}(n) = +\infty$ pour $n > 1$. Alors :

- L'évènement e est strictement périodique, de période Δ, si et seulement si:

$$e = R^{\Delta}e + \underline{\tau e(1)}$$

- L'évènement e est de période maximum Δ, si et seulement si:

$$e \geq R^{\Delta}e + \underline{\tau e(1)}$$

- L'évènement e est de période moyenne Δ, si et seulement si il existe un évènement f strictement périodique, de période Δ, tel que:

$$f \geq e > R^{\Delta}f$$

2.2.8. Conditions et filtrage

2.2.8.1. Conditions : Une condition est une variable à valeurs dans { vrai , faux }. Toute propriété portant sur des fonctions du temps pourra être interprétée comme une condition: Par exemple, on notera $(\mu e > \mu f)$ la condition C telle que $\tilde{\nu}c(t)$ = vrai si et seulement si $\mu e(t) > \mu f(t)$.

Outre ses composantes usuelles $(\nu c, c)$, on associe à une condition C deux évènements $c\uparrow$ et $c\downarrow$, représentant respectivement le passage de C de la valeur faux à la valeur vrai, et inversement. L'idée qui inspire cette définition est de ne retenir, dans la suite des prises de valeurs de C, que celles qui correspondent à un changement de valeur effectif (cf. §2.1.3., premier commentaire). On a :

[C1] $\quad \tilde{\nu}c \circ \tau c\uparrow \circ (I+1) =$ faux et $\tilde{\nu}c \circ \tau c\downarrow \circ (I+1) =$ vrai

[C2] $\quad \tilde{\nu}^{+}c \circ \tau c\uparrow \circ (I+1) =$ vrai et $\tilde{\nu}^{+}c \circ \tau c\downarrow \circ (I+1) =$ faux

[C3] $\quad \tilde{\nu}c = \tilde{\nu}^{+}c \circ \Theta(c\uparrow + c\downarrow)$

On appliquera aux conditions les opérateurs booléens usuels: Négation, notée $\neg$, conjonction, notée $\wedge$, et disjonction, notée $\vee$.

2.2.8.2. Filtrage : Nous utiliserons principalement les conditions pour filtrer les évènements: Si e est un évènement et C est une condition, on définit les évènements e| c et e| c^+, filtrages de e par C, comme suit:

$$e \mid c = \bigsqcap \{ f \sqsubseteq e \mid \tilde{\nu} c \circ \tau f = \text{vrai} \}$$

$$e \mid c^+ = \bigsqcap \{ f \sqsubseteq e \mid \tilde{\nu}^+ c \circ \tau f = \text{vrai} \}$$

Intuitivement e | c (resp. e | c^+) est l'évènement qui survient chaque fois que e survient lorsque $\tilde{\nu} c$ (resp. $\tilde{\nu}^+ c$) est vraie.

Une condition nécéssaire et suffisante pour que l'évènement e résulte d'un filtrage de l'évènement f, est que:

[Φ1] $$(\mu^+ f - \mu f) \circ \tau e = (\mu^+ e - \mu e) \circ \tau e$$

En effet, cette équation exprime qu'aux instants où e survient, il survient autant d'occurrences de e que de f.

Si C1 et C2 sont deux conditions exclusives, c'est à dire telles que $\tilde{\nu} c_1 \wedge \tilde{\nu} c_2 = \text{faux}$, alors $e \mid c_1 + e \mid c_2 = e \mid (c_1 \vee c_2)$. Il en résulte que:

[Φ2] $$e \mid c + e \mid \neg c = e$$

Les propriétés de l'opérateur de filtrage, en relation avec les autres opérateurs du modèle, sont complexes. Certaines d'entre-elles peuvent être mises en évidence en utilisant les "fonctions de sous-suite" qui, à toute occurrence du résultat du filtrage associent une occurrence simultanée de l'évènement filtré. Nous y reviendrons au §2.3.1.

2.2.8.3. Exemple: Spécifications d'une bascule D sur fronts. Une bascule D sur fronts reçoit une entrée D, qui est une condition, et un évènement h - généralement un front d'horloge - et élabore une condition Q, que l'on peut décrire, de manière comportementale, comme suit:

- La sortie Q prend ses valeurs chaque fois que h survient: $q = h$
- La suite des valeurs de Q est celle des valeurs courantes de D aux instants où h se produit: $\nu q = \tilde{\nu} d \circ \tau h$

Par composition à droite avec $\mu q = \mu h$, on obtient l'équation homogène:

$$\tilde{\nu} q = \tilde{\nu} d \circ \Theta h$$

qui exprime que la valeur courante de Q à l'instant t est la valeur qu'avait D à l'instant de la dernière occurrence de h précédant t.

D'un point de vue plus algorithmique, on peut décrire les évènements $q\uparrow$ et $q\downarrow$. Ainsi $q\uparrow$ survient chaque fois que h survient à un instant où D est vrai et Q est faux:

$$q\uparrow = h \mid (D \wedge \neg Q)$$

et, de même,

$$q\downarrow = h \mid (\neg D \wedge Q)$$

Dans l'une et l'autre de ces spécifications, la bascule est supposée se stabiliser instantanément. On pourait prendre en compte, dans une certaine mesure, le délai de stabilisation de la bascule, de la manière suivante:

$$\tilde{\nu} q = \tilde{\nu} d \circ \Theta h \circ r \quad \text{avec} \quad I - \varepsilon \leqslant r \leqslant I$$

$$R^{\varepsilon}(h \mid (D \wedge \neg Q)) \leqslant q\uparrow \leqslant h \mid (D \wedge \neg Q)$$
$$R^{\varepsilon}(h \mid (\neg D \wedge Q)) \leqslant q\downarrow \leqslant h \mid (\neg D \wedge Q)$$

où ε est une majoration du délai de stabilisation.

Notons cependant que ces nouvelles spécifications sont encore idéalisées: Il serait plus difficile d'admettre les oscillations transitoires de la bascule entre deux états stables, c'est à dire de spécifier que la sortie Q est éventuellement indéterminée pendant un délai ε après toute occurrence de h.

2.3. OUTILS DE DEDUCTION COMPLEMENTAIRES

Nous avons terminé l'exposition de notre formalisme, au cours de laquelle nous avons dégagé certaines propriétés parmi les plus évidentes et les plus utilisées. Afin de faciliter l'usage de ce formalisme pour effectuer des preuves, nous allons enrichir nos outils de déduction, notamment en ce qui concerne les sous-suites et les évènements filtrés, ainsi que pour faciliter les raisonnements inductifs. Tout d'abord, nous allons montrer que nos fonctions "date" et "compteurs" constituent des représentations de Gallois, ce qui nous permettra de justifier leur choix, et de généraliser un grand nombre de leurs propriétés.

2.3.1. Pseudo-inverses de fonctions sur des ensembles ordonnés

2.3.1.1. Définitions : Soient $(\mathbb{D},<)$ et $(\mathbb{D}',<)$ deux ensembles ordonnés, et f et g deux fonctions croissantes, respectivement de $\mathbb{D}$ dans $\mathbb{D}'$ et de $\mathbb{D}'$ dans $\mathbb{D}$. Alors:

- g est une pseudo-inverse à droite de f
- f est une pseudo-inverse à gauche de g

si et seulement si

$$f \circ g < I \text{ et } g \circ f > I$$

Remarque: Le couple (f,g) constitue alors une représentation de Gallois [Sanchis]. Cette notion de représentation a été souvent utilisée [Cousot], [Scott 76] pour construire des fermetures supérieures dans des treillis complets.

2.3.1.2. Proposition : Si f admet une pseudo-inverse à droite (resp. à gauche), celle-ci est unique, et on la notera f^{-1} (resp. ^{-1}f).

Démonstration: Soient g et g' deux pseudo-inverses à droite de f.

On a:

$$I < g' \circ f, \text{ donc } g < g' \circ f \circ g .$$

Or $f \circ g < I$, et g' est croissante. Donc

$$g' \circ f \circ g < g' \text{ et } g < g'$$

On montrerait de même $g' \leq g$. La démonstration pour la pseudo-inverse à gauche est analogue.

2.3.1.3. Théorème : Sous réserve que ${}^{-1}f$, f^{-1}, ${}^{-1}g$ et g^{-1} existent, on a:

$\alpha)$ $f^{-1} \circ f \circ f^{-1} = f^{-1}$ et $f \circ f^{-1} \circ f = f$

$\beta)$ $f \geq g \iff f^{-1} \leq g^{-1}$

$\gamma)$ $(f \circ g)^{-1}$ et ${}^{-1}(f \circ g)$ existent, et

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1} \quad , \quad {}^{-1}(f \circ g) = {}^{-1}g \circ {}^{-1}f$$

Démonstration: $\alpha)$ Puisque $f^{-1} \circ f \geq I$, $f^{-1} \circ f \circ f^{-1} \geq f^{-1}$. D'autre part, $f \circ f^{-1} \leq I$, et la croissance de f^{-1} entrainent $f^{-1} \geq f^{-1} \circ f \circ f^{-1}$.

$\beta)$ $f \geq g$ entraine $f \circ f^{-1} \geq g \circ f^{-1}$. Donc $I \geq g \circ f^{-1}$, qui entraine, d'après la croissance de g^{-1}, $g^{-1} \geq g^{-1} \circ g \circ f^{-1}$ et puisque $g^{-1} \circ g \geq I$, $g^{-1} \geq f^{-1}$. L'implication inverse se montre de manière analogue.

$\gamma)$ Il faut montrer $g^{-1} \circ f^{-1} \circ f \circ g \geq I$ et $f \circ g \circ g^{-1} \circ f \leq I$, ce qui résulte directement des propriétés de f^{-1} et g^{-1}.

2.3.1.4. Proposition : Si ${}^{-1}f$ et f^{-1} existent, les propriétés suivantes sont équivalentes:

$\alpha)$ $f^{-1} \circ f = I$

$\beta)$ ${}^{-1}f \circ f = I$

$\gamma)$ ${}^{-1}f \geq f^{-1}$

$\delta)$ f est strictement croissante

Démonstration: . $f \circ f^{-1} \geq I$ entraine $f^{-1} \circ f \circ {}^{-1}f \geq f^{-1}$. Donc, $f^{-1} \circ f = I$ entraine ${}^{-1}f \geq f^{-1}$ et (α) entraine (γ). De même (β) entraine (γ).

. On a toujours $f^{-1} \circ f \geq I \geq {}^{-1}f \circ f$. Or $\gamma)$ implique ${}^{-1}f \circ f \geq f^{-1} \circ f$. Donc (γ) entraine (α) et (γ) entraine (β).

.. Si $x > x'$ et si $f^{-1} \circ f = I$, on a $f^{-1} \circ f(x) > f^{-1} \circ f(x')$. f étant croissante, $f(x) \geq f(x')$. Si l'on avait $f(x) = f(x')$, on ne pourait avoir $f^{-1} \circ f(x) > f^{-1} \circ f(x')$. Donc $f(x) > f(x')$ et (α) entraine (δ).

. Enfin, supposons que f soit strictement croissante et qu'il existe x tel que $f^{-1} \circ f(x) > x$. Alors on aurait $f \circ f^{-1} \circ f(x) > f(x)$, ce qui est impossible puisque $f \circ f^{-1} \circ f = f$. Donc $f^{-1} \circ f = I$ et (δ) entraine (α).

2.3.1.5 Définition : Soient ($\mathbb{D}$, $\leqslant$, inf, sup, $\perp$, $\top$) et ($\mathbb{D}'$, $\leqslant$, inf, sup, $\perp'$, $\top'$) deux treillis complets. Une fonction f, totale de $\mathbb{D}$ dans $\mathbb{D}$, sera dite :

- indéfiniment sup-distributive, si et seulement si, pour toute partie X de $\mathbb{D}$, $\sup \{ f(x) \mid x \in X \} = f(\sup \{ x \mid x \in X \})$
- indéfiniment inf-distributive, si et seulement si, pour toute partie X de $\mathbb{D}$, $\inf \{ f(x) \mid x \in X \} = f(\inf \{ x \mid x \in X \})$

Il est évident que l'une ou l'autre de ces propriétés entraine la croissance de f.

2.3.1.6. Théorème : Soit f une fonction totale d'un treillis complet $\mathbb{D}$ dans un treillis complet $\mathbb{D}'$. Alors une condition nécessaire et suffisante pour que f admette une pseudo-inverse à droite, est que f soit indéfiniment sup-distributive. Dans ce cas la pseudo-inverse est

$$f^{-1} = \lambda y.\ \sup \{ x \in \mathbb{D} \mid f(x) \leqslant y \}$$

Démonstration: Supposons que f admette une pseudo-inverse à droite f^{-1} . Soit X une partie de $\mathbb{D}$, supX sa borne supérieure. On a

$$x \in X \Rightarrow x \leqslant \sup X \Rightarrow f(x) \leqslant f(\sup X)$$

Donc

$$\sup \{ f(x) \mid x \in X \} \leqslant f(\sup X)$$

D'autre part

$$x \in X \Rightarrow f(x) \leqslant \sup \{ f(x) \mid x \in X \}$$
$$\Rightarrow x \leqslant f^{-1} \circ f(x) \leqslant f^{-1}(\sup \{ f(x) \mid x \in X \})$$

Donc

$$\sup X \leqslant f^{-1} (\sup \{ f(x) \mid x \in X \})$$

Soit

$$f(\sup X) \leqslant f \circ f^{-1} (\sup \{ f(x) \mid x \in X \}) \leqslant \sup \{ f(x) \mid x \in X \}$$

Donc $f(\sup X) = \sup \{ f(x) \mid x \in X \}$ et f est indéfiniment sup-distributive.

Inversement, supposons que f soit indéfiniment sup-distributive, et posons $g = \lambda y.\ \sup \{ x \in \mathbb{D} \mid f(x) \leq y \}$. Alors:

$$g(f(x)) = \sup \{x' \in \mathbb{D} \mid f(x') \leq f(x) \} \geq x$$

puisque x est l'un des x'. D'autre part

$$f(g(y)) = f(\sup \{x \in \mathbb{D} \mid f(x) \leq y \})$$
$$= \sup \{f(x) \in \mathbb{D} \mid f(x) \leq y \} \leq y$$

Donc $g = f^{-1}$

On montrerait de même le théorème dual:

2.3.1.7. Théorème : Soit f un fonction totale d'un treillis complet $\mathbb{D}$ dans un treillis complet $\mathbb{D}'$. Alors une condition nécessaire et suffisante pour que f admette une pseudo-inverse à gauche est que f soit indéfiniment inf-distributive. Dans ce cas la pseudo-inverse est

$$^{-1}f = \lambda y.\ \inf \{x \in \mathbb{D} \mid f(x) \geq y \}$$

2.3.1.8. Proposition : Si une fonction f, totale d'un treillis complet $\mathbb{D}$ dans un treillis complet $\mathbb{D}'$, admet une pseudo-inverse à gauche ^{-1}f et une pseudo-inverse à droite f^{-1} , alors

$$f(\bot) = \bot' \quad \text{et} \quad f(\top) = \top'$$
$$f^{-1}(y) = \top \iff y = \top'$$
$$^{-1}f(y) = \bot \iff y = \bot'$$

Démonstration: f, ^{-1}f et f^{-1} étant totales, on a:

$$f(\bot) = \inf \{ y \in \mathbb{D}' \mid f^{-1}(y) \geq \bot \} = \inf \{ y \in \mathbb{D}' \} = \bot'$$
$$f(\top) = \sup \{ y \in \mathbb{D}' \mid {}^{-1}f(y) \leq \top \} = \sup \{ y \in \mathbb{D}' \} = \top'$$
$$f^{-1}(\top') = \sup \{ x \in \mathbb{D} \mid f(x) \leq \top' \} = \sup \{ x \in \mathbb{D} \} = \top$$
$$^{-1}f(\bot') = \inf \{ x \in \mathbb{D} \mid f(x) \geq \bot' \} = \inf \{ x \in \mathbb{D} \} = \bot$$

D'autre part

$$f^{-1}(y) = \top \implies y \geqslant f \circ f^{-1}(y) = f(\top) = \top' \implies y = \top'$$
$$^{-1}f(y) = \bot \implies y \leqslant f \circ {}^{-1}f(y) = f(\bot) = \bot' \implies y = \bot'$$

Nous pouvons revenir maintenant à nos fonctions "date" et "compteurs" .

2.3.1.9. Proposition : Pour tout évènement e ,

$$(\tau e)^{-1} = \mu^{+} e \quad \text{et} \quad {}^{-1}(\tau e) = \mu e + 1$$

Démonstration : Cette affirmation est presque entièrement impliquée par les propriétés [μ7], [μ8] et [Θ2] . La seule inéquation à montrer est

[μ9] $\qquad \tau e \circ (\mu e + 1) \geqslant I$

qui est une conséquence de la définition de μe .

Commentaires :

Les résultats précédants justifient le choix de deux fonctions compteurs, l'une continue à gauche et l'autre continue à droite (puisque, pour les fonctions de $\mathbb{N}$ dans $\mathbb{R}$, les continuités à gauche et à droite coïncident avec l'indéfinie sup- et inf- distributivité). D'autre part

. La proposition 2.3.1.8 justifie [τ2], [τ4] et [μ2]. Elle justifie également [μ3], puisqu'elle impose $(\mu e + 1)(-\infty) = 0$, soit $\mu e(-\infty) = -1$.

Notons que les hypothèses équivalentes [τ3] et[μ4] ne sont pas justifiables algébriquement, et ne relèvent que de l'intuition.

. Le théorème 2.3.1.3.β justifie le choix de l'ordre sur les compteurs.

. La proposition 2.3.1.4 justifie [OS1], [OS2], [OS3] et [OS4]

. Enfin, le théorème 2.3.1,3 nous permet d'effectuer directement des déductions non triviales, comme par exemple:

$$\tau e \circ \mu^{+} f \geq \tau g \circ \mu^{+} h \Rightarrow \tau h \circ (\mu g + 1) \geq \tau f \circ (\mu e + 1)$$

Dans ce type de déductions par "pseudo-inversion", on pourra utiliser le fait que $(\mu e)^{-1} = \tau e \circ (I+1)$.

2.3.2. Fonctions de sous-suite

Par définition de la relation de sous-suite, si $e \sqsubseteq f$ il existe une application r, strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$, telle que $\tau e = \tau f \circ r$. Une telle application sera appelée fonction de sous-suite associée au couple (e,f).

Il est clair que, si $e \sqsubseteq f$, les occurrences de f simultanées avec la n-ième occurrence de e sont les occurrences d'indice m telles que

$$\mu f \circ \tau e(n) + 1 \leq m \leq \mu^{+} f \circ \tau e(n)$$

Il en résulte que l'ensemble des fonctions de sous-suite associées au couple (e,f) est l'ensemble des fonctions r, strictement croissantes, telles que:

$$s_{min}(e,f) \leq r \leq s_{max}(e,f)$$

où

$$s_{min}(e,f) = \mu f \circ \tau e + 1 \quad \text{et} \quad s_{max}(e,f) = \mu^{+} f \circ \tau e$$

Une conséquence de ce résultat est que, si f est à occurrences simples, le couple (e,f) n'admet qu'une fonction de sous-suite, puisque:

[OS2] $\qquad s_{min}(e,f) = s_{max}(e,f)$

Quoiqu'on ait $\tau e = \tau f \circ s_{min}(e,f) = \tau f \circ s_{max}(e,f)$, notons que $s_{min}(e,f)$ et $s_{max}(e,f)$ ne sont en général pas des fonctions de sous suite associées à (e,f), puisqu'elles ne sont pas nécéssairement strictement croissantes.

2.3.2.1. Proposition : Si $e \subseteq f$, les fonctions

$$r_{min}(e,f) = (\mu f - \mu e) \circ \tau e + I$$

et

$$r_{max}(e,f) = (\mu^{+} f - \mu^{+} e) \circ \tau e + I$$

sont des fonctions de sous-suite associées à (e,f). De plus, l'ensemble des fonctions de sous-suite associées à (e,f) est l'ensemble des fonctions strictement croissantes comprises entre $r_{min}(e,f)$ et $r_{max}(e,f)$.

Démonstration:

Ces fonctions sont strictement croissantes, puisque I est strictement croissante et que d'après [SS2] et [SS3], $\mu f - \mu e$ et $\mu^{+} f - \mu^{+} e$ sont croissantes. D'autre part:

$$[\mu 6] \Rightarrow s_{min}(e,f) \leq r_{min}(e,f)$$

$$[\mu 7] \Rightarrow r_{max}(e,f) \leq s_{max}(e,f)$$

$$[SS4] \Rightarrow r_{min}(e,f) \leq r_{max}(e,f)$$

D'autre part, il est facile de voir que $r_{min}(e,f)$ et $r_{max}(e,f)$ sont respectivement la plus petite et la plus grande fonction strictement croissante comprise entre $s_{min}(e,f)$ et $s_{max}(e,f)$.

Cette proposition entraine qu'une condition nécéssaire et suffisante pour que e résulte d'un filtrage de f est que le couple (e,f) n'admette qu'une fonction de sous-suite, que nous noterons simplement r(e,f). En effet d'après [Φ1]:

$$\exists c \text{ telle que } e = f \mid c \iff r_{min}(e,f) = r_{max}(e,f)$$

2.3.2.2. Lemme: Si $e = f \mid c$ et si $g \subseteq e$, alors toute fonction de sous-suite associée à (g,f) est supérieure à r(e,f).

Démonstration:

On va montrer $r_{min}(g,f) \geq r(e,f)$. On a:

$$r_{min}(g,f) = (\mu f - \mu g) \circ \tau g + I = (\mu f - \mu g) \circ \tau e \circ r' + I$$

où r' est une fonction de sous-suite associée à (g,e). Or r' est extensive et $\mu f - \mu g$ est croissante. Donc:

$$r_{min}(g,f) \geq (\mu f - \mu g) \circ \tau e + I$$

Enfin $\mu g \leq \mu e \Rightarrow r_{min}(g,f) \geq (\mu f - \mu e) \circ \tau e + I = r(e,f)$

2.3.2.3. Proposition : Si $e_1 = f_1 \mid c$ et $e_2 = f_2 \mid c$, et si $\tilde{\nu}c \circ \tau f_1 = \tilde{\nu}c \circ \tau f_2$, alors $r(e_1,f_1) = r(e_2,f_2)$.

Démonstration :

Soit x l'évènement tel que $\tau x = \tau f_1 \circ r(e_2,f_2)$. On a $x \sqsubseteq f_1$. D'autre part:

$$\begin{aligned} \tilde{\nu}c \circ \tau x &= \tilde{\nu}c \circ \tau f_1 \circ r(e_2,f_2) \\ &= \tilde{\nu}c \circ \tau f_2 \circ r(e_2,f_2) \\ &= \tilde{\nu}c \circ \tau e_2 \\ &= \text{vrai} \end{aligned}$$

Donc $x \sqsubseteq e_1$, d'après la définition du filtrage, et d'après le lemme précédent, $r(e_2,f_2) \leq r(e_1,f_1)$. On montrerait de même l'inégalité opposée.

Cette proposition peut être utilisée pour "projeter" sur e_1 et e_2 une propriété liant f_1 et f_2. Par exemple, de l'égalité des fonctions de sous-suites $r(e_1,f_1)$ et $r(e_2,f_2)$, on pourra conclure:

$$f_1 \leq f_2 \Rightarrow \tau f_1 \circ r(e_1,f_1) \geq \tau f_2 \circ r(e_2,f_2) \Rightarrow e_1 \leq e_2$$

De même cette proposition entraine que :

$$\tilde{\nu}c = \tilde{\nu}c \circ (I + \Delta) \Rightarrow R^{\Delta}(e \mid c) = (R^{\Delta} e) \mid c$$

2.3.3. Causalité et induction

Nous situerons la problématique de ce paragraphe par un exemple:

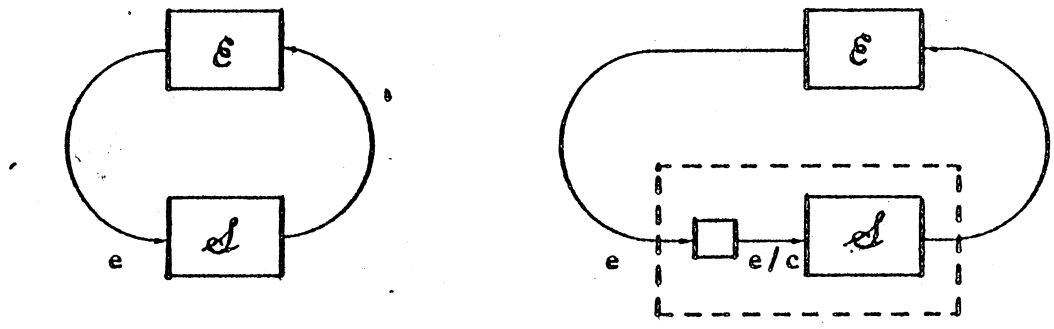
Soit un système S, dans un environnement E (cf. figure 2.a). S reçoit de E un évènement d'entrée e, et restitue à E ses sorties. On veut prouver la propriété P_1 suivante:

P_1: "Chaque fois que S reçoit e, une certaine condition C est vraie "

Soit maintenant le système S' (cf. figure 2.b) construit à partir de E en intercalant sur l'entrée e un dispositif de filtrage par C, et supposons que l'on sache prouver la propriété P_2:

P_2: "Chaque fois que S' reçoit e, la condition C est vraie"

Peut-on en conclure que le filtrage est inutile, et que, par conséquent, la propriété P_1 est démontrée ? En termes plus généraux, peut-on remplacer un sous-système S' par un autre, S, alors que S et S' ne sont équivalents que sous des hypothèses concernant le reste du système (ici l'environnement E), hypothèses qui peuvent porter sur les sorties du sous-système (les sorties de S' peuvent influencer l'élaboration de e



-a- -b-

Figure 2
Système bouclé

par E) ? La réponse à cette question n'est pas aussi évidente qu'il y parait, pour les raisons suivantes:

- Elle nécessite une démonstration par induction, qui pourrait être, informellement, la suivante dans l'exemple considéré : P_2 entraine que lors de la première occurrence de e, C est vérifiée. Si, lors des n premières occurrences de e, C est vérifiée, alors les sorties élaborées par S et S' en réponse à ces n premières occurrences sont les mêmes, et la n+1-ième occurrence de e, élaborée par E en réponse à ces sorties sera la même. Donc, d'après P_2, C sera vérifiée lors de cette n+1-ième occurrence.

- Cette démonstration fait appel à un principe de causalité temporelle : Les mêmes causes produisent les mêmes effets, ou, plus spécifiquement, le comportement d'un système à un instant donné, ne dépend que de son passé. Or notre formalisme permet d'écrire des spécifications qui violent ce principe. Par exemple, on peut trés bien spécifier un système qui émet ses sorties avant de recevoir les entrées servant à les élaborer.

- De plus, dans le contexte général du temps continu où nous nous sommes placés, il faut prendre des précautions pour assurer la validité des démonstrations par récurrence. En effet, un raisonnement hâtif sur les entiers peut conduire à des paradoxes analogues à celui d'"Achille et la tortue" : Ayant prouvé une propriété sur une suite d'intervalles $[-\infty,t_n]$, où (t_n) est une suite strictement croissante d'instants, on en déduit que la propriété est vraie pour tout instant. Or si la suite (t_n) est convergente, la démonstration n'est valide que jusqu'à sa limite. Pour éviter ce type d'inconsistances, nous aurons besoin d'une hypothèse plus forte que la simple causalité, que nous appellerons "surcausalité", et qui impose qu'il existe un délai ε ($\varepsilon > 0$) tel que le comportement d'un système à l'instant t ne dépende que de son histoire passée jusqu'à l'instant $t - \varepsilon$.

Notre approche consistant à manipuler globalement les histoires, plutôt que les états instantanés, se prête mal aux raisonnements inductifs. C'est pourquoi nous allons démontrer ,une fois pour toutes - par induction - un théorème d'intéret général, dont l'application permet, dans de nombreux cas, d'éviter les démonstrations par récurrence. Pour cela, il nous faut d'abord formaliser nos hypothèses de causalité. Notons que l'intéret du concept de causalité dépasse le cadre de ce théorème d'induction, dans la mesure où, si notre formalisme permet d'écrire des spécifications non causales - laissant ainsi au spécificateur un degré de liberté profitable au caractère naturel du processus de spécification -, le spécificateur devra, par la suite, s'assurer que ses spécifications admettent une réalisation causale, et même sur-causale, puisque aucune machine concrète ne peut réagir instantanément à des stimuli externes.

2.3.3.1. Définitions : Soit $\mathbb{F}$ un ensemble de fonctions totales de $\mathbb{T}$ dans un ensemble D. Si $\theta \in \mathbb{F}$, on notera $\theta[t]$ la restriction de θ à $[-\infty,t]$.

- Une fonction G, de $\mathbb{F}$ dans $\mathbb{F}$, une relation binaire R sur $\mathbb{F}$, seront dites causales, si et seulement si, $\forall t \in \mathbb{T}$, $\forall \theta \in \mathbb{F}$,

$$\theta[t] = \theta'[t] \Rightarrow G(\theta)[t] = G(\theta')[t]$$
$$\Rightarrow \{ \theta''[t] \mid \theta R \theta'' \} = \{ \theta''[t] \mid \theta' R \theta'' \}$$

- Une fonction G, de $\mathbb{F}$ dans $\mathbb{F}$, une relation binaire R sur $\mathbb{F}$, seront dites sur-causales, si et seulement si $\exists \varepsilon > 0$ tel que $\forall t \in \mathbb{T}$,

$$\theta[t] = \theta'[t] \Rightarrow G(\theta)[t+\varepsilon] = G(\theta')[t+\varepsilon]$$
$$\Rightarrow \{ \theta''[t+\varepsilon] \mid \theta R \theta'' \} = \{ \theta''[t+\varepsilon] \mid \theta' R \theta'' \}$$

2.3.3.2. Propriétés : - α) Si G est une fonction causale, et si R est une relation sur-causale, la relation $G.R = \{ (\theta,\theta') \mid G(\theta) R \theta' \}$ est sur-causale.

- β) Si R est une relation sur-causale totale ($Dom(R) = \mathbb{F}$), et si $\theta[t] \in \{\theta'[t] \mid \theta R \theta' \}$, il existe $\bar{\theta}$ dans $\mathbb{F}$ tel que $\theta R \bar{\theta}$ et $\bar{\theta}[t] = \theta[t]$.

Démonstration:

La propriété α) est une conséquence directe des définitions 2.3.2.1. La propriété β) nécéssite une démonstration par récurrence:

Soit $P(t,\theta)$ la propriété $\theta[t] \in \{ \theta'[t] \mid \theta R \theta' \}$. On a $P(t,\theta) \Rightarrow \exists \theta_1$ tel que $\theta R \theta_1$ et $\theta_1[t] = \theta[t]$. D'après la sur-causalité de R, ceci implique

$$\{ \theta''[t+\varepsilon] \mid \theta R \theta'' \} = \{ \theta''[t+\varepsilon] \mid \theta_1 R \theta'' \}$$

Or $\theta_1[t+\varepsilon]$ appartient au premier de ces ensembles, et donc également au second. On a donc $P(t+\varepsilon,\theta_1)$. On peut ainsi construire une suite $\theta_0 = \theta, \theta_1, \ldots, \theta_n, \ldots$ telle que $\forall i \in \mathbb{N}$,

$$\theta_i[t+i\varepsilon] = \theta_{i+1}[t+i\varepsilon] \text{ et } P(t+i\varepsilon, \theta_i)$$

La suite $(t+i\varepsilon)$ tendant vers l'infini avec i, la suite des fonctions partielles $\theta_i[t+i\varepsilon]$ admet une borne supérieure (au sens des domaines) $\bar{\theta}$, qui est une fonction totale vérifiant $\theta R \bar{\theta}$ et $\bar{\theta}[t] = \theta[t]$.

2.3.3.3. Théorème de sur-causalité : Soient G une fonction causale totale, et R une relation sur-causale totale, telles que :

1) $\exists t_0 \in \mathbb{T}$ tel que $\forall \theta \in \mathbb{F}$, $\theta[t_0] = G(\theta)[t_0]$

2) $G(\theta) R \theta \Rightarrow \theta = G(\theta)$

Alors $\theta R \theta \Rightarrow \theta = G(\theta)$

Démonstration:

Soit θ tel que $\theta R \theta$. On a $\theta[t_0] = G(\theta)[t_0]$, d'après (1). Supposons $\theta[t] = G(\theta)[t]$ et montrons $\theta[t+\varepsilon] = G(\theta)[t+\varepsilon]$: Puisque R est sur-causale, on a $\{ \theta'[t+\varepsilon] \mid \theta R \theta' \} = \{ \theta'[t+\varepsilon] \mid G(\theta) R \theta' \}$. Or $\theta[t+\varepsilon]$ appartient à cet ensemble puisque $\theta R \theta$. D'après 2.3.3.2, la relation G.R est sur-causale et il existe $\bar{\theta}$ tel que $G(\bar{\theta}) R \bar{\theta}$ et $\bar{\theta}[t+\varepsilon] = \theta[t+\varepsilon]$. D'après (2), $\bar{\theta} = G(\bar{\theta})$, et donc $\theta[t+\varepsilon] = G(\theta)[t+\varepsilon]$ de par la causalité de G.

2.3.2.4. Corollaire : Sous les hypothèses du théorème précédent, on a :

$$\theta R \theta \iff G(\theta) R \theta$$

Application : Ce corollaire permet de répondre à la question que nous posions à propos de l'exemple introductif du §2.3.3 . En effet soit R_1 la relation réalisée par le système S, et liant son évènement d'entrée e à ses sorties, et soit R_2 la relation réalisée par l'environnement E, et liant ces sorties à l'évènement e envoyé vers S. L'ensemble des évènements que S peut recevoir en entrée est donc l'ensemble des solutions de $e\ R_1.R_2\ e$. Supposons que la relation $R = R_1.R_2$ soit sur-causale, ce qui revient à dire que l'une ou l'autre des "machines" S et E possède un temps de réaction non nul. Soit G la fonction de filtrage $\lambda e.e\,|c$, qui est causale. Alors, la propriété P_2 équivaut à:

$$G(e)\ R\ e \implies e = G(e)$$

ce qui nous place sous les hypothèses du théorème 2.3.3.3, dont le corollaire fournit:

$$e\ R\ e \iff e = G(e)$$

c'est à dire la propriété P_1 que l'on voulait déduire.

CHAPITRE 3
ETUDE DE CAS : CONCEPTION CERTIFIEE D'UN ARBITRE DE BUS DISTRIBUE

Pour illustrer et expérimenter l'usage du formalisme présenté au chapitre précédent, nous allons l'appliquer à la conception certifiée d'un système matériel, qui est un arbitre asynchrone et distribué. Cet exemple est intéressant à plus d'un titre:

- Les spécifications intuitives de ce système sont comportementales. C'est le type même de système qu'il est difficile et peu naturel de décrire en termes de succession d'états. Nous éssaierons de mettre en évidence le caractère quasi-littéral du processus de formalisation de l'intention initiale.

- Cependant, nous verrons que l'interprétation littérale de cette intention informelle conduit à des spécifications irréalisables. Cet exemple nous permettra donc d'illustrer le processus de spécification, en ce qu'il oblige à préciser et corriger un cahier des charges incomplet ou ambigu, et ceci avant que la conception proprement dite du système ait commencé.

- Nous donnerons deux solutions algorithmiques de l'arbitre, dont nous prouverons formellement la correction, expérimentant ainsi, de manière conséquente, les outils de déduction dégagés au chapitre précédent. La première solution pourait être prouvée par des procédés classiques, dans la mesure où les délais de réaction des opérateurs utilisés

n'influencent pas sa correction, mais seulement son temps de réponse global. En revanche, dans la deuxième solution, nous montrerons notamment, qu'une unité accédant au bus doit le conserver pendant un intervalle de temps minimum, afin de laisser à l'arbitre le temps de revenir à un état de repos entre deux arbitrages.

- Nous donnerons les schémas architecturaux correspondant à ces deux solutions. A partir de descriptions formelles du comportement des composants (analogues à la description de la bascule D, donnée dans l'exemple 2.2.8.3), on pourrait prouver la conformité entre ces schémas et les descriptions algorithmiques. Par soucis de concision, ces preuves ne seront pas données ici.

3.1. SPECIFICATIONS DE L'ARBITRE

Un bus relie n unités U_1, ..., U_n, auxquelles on veut associer un dispositif d'arbitrage assurant, d'une part, l'exclusivité d'accès au bus, et d'autre part le respect d'un règle de priorité. Ce dispositif est distribué, au sens que chaque unité possède un élément d'arbitrage, l'allocation du bus resultant de la coopération de ces n éléments, sans que ceux-ci ne disposent d'aucune ressource centralisée (horloge ou mémoire communes, moniteurs, ...) pour se synchroniser.

Pour accéder au bus, une unité envoie une requête à son arbitre associé, et n'accède au bus qu'après en avoir reçu l'autorisation. Chaque arbitre connait l'état des requêtes de son unité propre et l'état d'occupation du bus. Les arbitres peuvent communiquer entre eux, pour élaborer les signaux d'autorisation qui doivent assurer les propriétés suivantes au système :

- L'exclusivité : A chaque instant, une unité au plus est autorisée à émettre sur le bus.

- La réactivité : Une unité n'est autorisée à émettre que si elle en a fait la demande.

- Le respect de la priorité : En cas de demandes concurrentes de plusieurs unités, c'est l'unité de plus faible indice qui est exaucée.

- La promptitude : Le bus ne peut rester à la fois libre et demandé.

Nous allons formaliser, en termes d'événements, cette spécification informelle. Afin de minimiser les risques d'erreur, cette formalisation sera progressive: Dans un premier temps, nous décrirons le comportement idéal du système, sans tenir compte des contraintes de faisabilité. La prise en compte de ces contraintes, et en particulier du caractère distribué de l'arbitrage, nous conduira par la suite à affaiblir cette première spécification.

3.1.1. Première spécification

On définit les événements suivants :

r_i (i = 1...n) : émission d'une requête par l'unité U_i

a_i (i = 1...n) : émission d'une autorisation vers l'unité U_i

ℓ_i (i = 1...n) : libération du bus par l'unité U_i.

La seule hypothèse concernant l'environnement du système d'arbitrage, est la "discipline" des unités: Une unité n'accède au bus qu'aprés en avoir reçu l'autorisation, et ne le libère qu'aprés y avoir accédé, soit encore, en désignant par $accés_i$ l'événement d'accés au bus par l'unité i :

$$\forall i=1..n,\ a_i > accés_i > \ell_i$$

Pour simplifier, nous n'introduirons pas, cependant, les événements $accés_i$, et nous nous contenterons de formaliser l'hypothèse de discipline des unités comme suit:

$$\forall i = 1...n,\ \ell_i < a_i \qquad \text{(DIS)}$$

Sous cette hypothèse, et compte tenu de la simplification précédente, une unité U_i sera supposée posséder le bus à l'instant t si et

seulement si son nombre d'autorisations $\mu a_i(t)$ est strictement supérieur à son nombre de libérations $\mu \ell_i(t)$.

Nous pouvons alors formaliser les contraintes de l'arbitre :

. Exclusivité : le nombre d'unités possédant le bus à l'instant t est $\Sigma\mu a_i(t) - \Sigma\mu \ell_i(t)$ (sauf indications contraires, les sommations s'entendent de 1 à n). En termes d'évènements, nous écrivons :

$$\Sigma a_i \leq \Sigma \ell_i + 1 \qquad \text{(EX)}$$

. Réactivité : $\forall i = 1...n, \quad a_i \leq r_i$ (RE)

. Priorité : Il faut écrire que lorsque l'unité U_i reçoit une autorisation, aucune unité d'indice inférieur à i ne demande le bus. Or, une unité U_j demande le bus à l'instant t si et seulement si son nombre de requêtes $\mu r_j(t)$ est strictement supérieur à son nombre d'autorisations $\mu a_j(t)$. On écrit donc :

$$1 \leq j < i \leq n \Rightarrow \mu r_j \circ \tau a_i \leq \mu a_j \circ \tau a_i \qquad \text{(PR)}$$

. Promptitude : Le bus est libre lorsque $\Sigma\mu \ell_i(t) > \Sigma\mu a_i(t)$. Il est demandé lorsque $\Sigma\mu r_i(t) > \Sigma\mu a_i(t) + 1$. D'après les contraintes d'exclusivité et de réactivité, il s'ensuit qu'à l'instant t,

- le bus est occupé si et seulement si $\Sigma\mu \ell_i(t) + 1 = \Sigma\mu a_i(t)$;
- le bus n'est pas demandé si et seulement si $\Sigma\mu r_i(t) = \Sigma\mu a_i(t)$.

La contrainte de promptitude, qui impose qu'à chaque instant, l'une ou l'autre de ces conditions doit être vraie, s'écrit donc :

$$\forall t, \ \inf(\Sigma\mu \ell_i(t) - \Sigma\mu a_i(t) + 1 \ , \ \Sigma\mu r_i(t) - \Sigma\mu a_i(t)) = 0$$

soit finalement

$$\Sigma a_i = \inf(\Sigma \ell_i + 1 \ , \ \Sigma r_i) \qquad \text{(PP)}$$

Les quatre règles EX, RE, PR et PP spécifient complètement les sorties (a_i) élaborées par l'arbitre en fonction de ses entrées (ℓ_i) et (r_i) . Cependant, une première analyse de ces spécifications révèle

qu'elles ne sont pas strictement réalisables. En effet :

- La contrainte de promptitude impose que l'arbitre réagisse instanément aux événements imprévisibles (ℓ_i) et (r_i).
- Telle qu'elle est formulée, la loi de priorité suppose que chaque élément d'arbitrage possède une image exacte de l'état instantané des requêtes de toutes les unités plus prioritaires, ce qui n'est pas réalisable dans un système distribué. Il nous faut donc assouplir les règles (PR) et (PP).

3.1.2. Spécification réalisable

Nous affaiblirons d'abord la contrainte de promptitude en une contrainte de temps de réponse. Soit $d = \inf(\Sigma r_i , \Sigma \ell_i + 1)$. Nous avons vu que c'est l'événement "demande d'arbitrage" qui survient chaque fois que :

- soit une requête survient alors que le bus est libre
- soit le bus est libéré alors qu'il est demandé.

La contrainte de promptitude ($\Sigma a_i = d$) est remplacée par la contrainte

$$\Sigma a_i > R^{\delta} d \qquad \text{(TR)}$$

qui impose, sous les hypothèses d'exclusivité et de réactivité, que toute demande d'arbitrage soit suivie, dans un délai inférieur à δ, de l'émission d'une autorisation - le délai de réponse δ étant un paramètre de l'arbitre.

Plusieurs solutions sont possibles pour affaiblir la règle de priorité. On choisit (arbitrairement) la suivante : L'accès au bus ne peut être donné à l'unité U_i que si aucune unité plus prioritaire que U_i ne demandait l'accès lors de la demande d'arbitrage ayant provoqué cette autorisation. Nous ecrivons :

$$1 \leq j < i \leq n \Rightarrow \mu a_j \circ \Theta d \circ \tau a_i = \mu r_j \circ \Theta d \circ \tau a_i \qquad \text{(PR')}$$

On peut donc récapituler les spécifications de l'arbitre comme suit :

- sous l'hypothèse de discipline :

$$\forall i = 1...n, \quad \ell_i < a_i \qquad \text{(DIS)}$$

- réaliser les événements a_i tels que :

$$\Sigma a_i < \Sigma \ell_i + 1 \qquad \text{(EX)}$$

$$\forall i = 1...n, \; a_i < r_i \qquad \text{(RE)}$$

$$\Sigma a_i > R^{\delta} d \qquad \text{(TR)}$$

avec $d = \inf(\Sigma r_i \; , \; \Sigma \ell_i + 1)$

$$1 < j < i < n \implies \mu a_j \circ \Theta d \circ \tau a_i = \mu r_j \circ \Theta d \circ \tau a_i \qquad \text{(PR')}$$

3.2. PREMIERE SOLUTION : JETON CIRCULANT

3.2.1. Algorithme

Un algorithme classique consiste, à chaque demande d'arbitrage, à émettre un "jeton" qui circule d'un arbitre à l'autre par ordre de priorités décroissantes, jusqu'à être capté par un arbitre dont l'unité demande le bus, laquelle reçoit l'autorisation d'accès. Soit j_i l'événement "réception du jeton par l'arbitre i". Soit ε une majoration du temps de propagation d'un signal entre deux arbitres. Lorsque l'arbitre associé à U_i reçoit un jeton,

- si l'unité U_i demande le bus, il émet l'autorisation;
- dans le cas contraire, il transmet le jeton vers l'arbitre de U_{i+1}.

Cet algorithme peut être formalisé comme suit :

$$\forall i = 1...n, \quad a_i = j_i \mid \mu r_i > \mu a_i + 1 \qquad (1)$$

$$d_i = j_i \mid \mu r_i < \mu a_i \qquad (2)$$

$$d_{i-1} > j_i > R^{\varepsilon} d_{i-1} \qquad (3)$$

$$d_0 = d = \inf(\Sigma r_i , \Sigma \ell_i + 1) \qquad (4)$$

Il nous faudra prendre quelques hypothèses supplémentaires pour pouvoir prouver cet algorithme. La première concerne le temps de réponse, qui ne peut, évidemment, être prouvé qu'à l'aide d'une hypothèse sur ε :

$$n\varepsilon < \delta \qquad (5)$$

La preuve de l'algorithme sera effectuée en supposant, d'autre part, que toute transmission inter arbitres prend un temps strictement positif, c'est à dire que

$$\forall i=1...n, \; j_i < d_{i-1} \qquad (3')$$

C'est une hypothèse réaliste, et nécessaire, au moins en ce qui concerne j_1 : En effet, si la demande d'arbitrage est provoquée par une requête de U_1, à l'instant précis de cette demande, cette requête n'est pas prise en compte par l'arbitre de U_1, en raison de la continuité à gauche des conditions. Donc si l'arbitre reçoit le jeton à cet instant, il le laissera passer, ce qui peut entrainer un blocage du système. Cette circonstance constitue un aléa temporel, au moins théoriquement possible, que nous n'avons détecté qu'au cours de la preuve.

3.2.2 Preuve de l'algorithme du jeton

3.2.2.1. Exclusivité et réactivité :

D'après (1) et (2), on a

$$a_i + d_i = j_i \;, \; i=1...n$$

et

$$j_i < d_{i-1} = j_{i-1} - a_{i-1}$$

soit

$$j_i + a_{i-1} < j_{i-1}$$

Par sommation, on obtient : $\Sigma a_i \leqslant j_1$

Et puisque, d'après (3) et (4), $j_1 \leqslant d_0 \leqslant \Sigma \ell_i + 1$,

$$\Sigma a_i \leqslant \Sigma \ell_i + 1$$

ce qui prouve l'exclusivité.

D'autre part, d'après (3'), (4) et (DIS), on tire

$$\Sigma \mu^+ a_i \leqslant \mu^+ j_1 \leqslant \mu d_0 \leqslant \Sigma \mu \ell_i + 1 \leqslant \Sigma \mu a_i + 1$$

d'où résulte l'occurrence simple des a_i :

$$\mu^+ a_i \leqslant \mu a_i + 1 \qquad \text{(OS)}$$

Alors:

(1) et (OS) $\qquad \mu r_i \circ \tau a_i \geqslant \mu a_i \circ \tau a_i + 1 = \mu^+ a_i \circ \tau a_i = I$

Par composition à droite avec μa_i , il vient

$$\mu r_i \circ \Theta a_i \geqslant \mu a_i$$

Or $\Theta a_i \leqslant I$, donc $\mu r_i \geqslant \mu r_i \circ \Theta a_i$, et enfin

$$\mu r_i \geqslant \mu a_i \qquad \text{(RE)}$$

3.2.2.2. Priorité :

La preuve du respect de la priorité est plus difficile. Elle nécessite l'établissement préalable de deux lemmes.

Lemme 1: L'unité U_k n'est jamais demandeuse au dernier d_0 précédant d_k

$$\mu a_k \circ \Theta d_0 \circ \tau d_k = \mu r_k \circ \Theta d_0 \circ \tau d_k \qquad \text{(L1)}$$

Démonstration: On a $\mu a_k \leqslant \mu r_k$, d'après la réactivité, et $\mu a_k \circ \tau d_k = \mu r_k \circ \tau d_k$, d'après (2).

Donc (croissance de μr_k et rétractivité de Θd_0):

$$\mu a_k \circ \tau d_k \geqslant \mu r_k \circ \Theta d_0 \circ d_k$$

Il reste à montrer $\mu a_k \circ \Theta d_0 \circ \tau d_k = \mu a_k \circ \tau d_k$ pour obtenir le lemme. On va montrer un résultat plus fort:

$$\forall i,k,\ \mu a_k \circ \Theta d_0 \circ \tau j_i = \mu a_k \circ \tau j_i \qquad (i)$$

(d_i étant une sous suite de j_i, cette relation sera encore vraie en remplaçant τj_i par τd_i, et en égalant i et k, on en déduit la relation cherchée).

On a $\mu^+ d_0 - 1 \leqslant \Sigma \mu a_k \leqslant \mu d_0$. Par composition avec τd_0 et d'après l'occurrence simple de d_0, il vient:

$$\Sigma \mu a_k \circ \tau d_0 = I - 1$$

D'où $\Sigma \mu a_k \circ \Theta d_0 \circ \tau j_i = \mu d_0 \circ \tau j_i - 1 \qquad (ii)$

D'autre part

$$\mu a_k + \mu^+ d_k \leqslant \mu^+ a_k + \mu^+ d_k \leqslant \mu d_{k-1}$$

Soit

$$\mu a_k \circ \tau j_i + \mu^+ d_k \circ \tau j_i \leqslant \mu^+ a_k \circ \tau j_i + \mu^+ d_k \circ \tau j_i \leqslant \mu d_{k-1} \circ \tau j_i \qquad (iii)$$

Or $\quad k \neq i \Rightarrow \mu d_k \circ \tau j_i = \mu^+ d_k \circ \tau j_i$

et $\quad \mu^+ a_i \circ \tau j_i + \mu^+ d_i \circ \tau j_i = \mu a_i \circ \tau j_i + \mu d_i \circ \tau j_i + 1$

En sommant les inéquations (iii) de k=1 à n, il vient donc:

$$\Sigma \mu a_k \circ \tau j_i + \Sigma \mu^+ d_k \circ \tau j_i \leqslant \Sigma \mu^+ a_k \circ \tau j_i + \Sigma \mu^+ d_k \circ \tau j_i \leqslant \Sigma \mu d_{k-1} \circ \tau j_i$$

Soit

$$\sum_{k \neq i} \mu a_k \circ \tau j_i + \mu^+ a_i \circ \tau j + \mu^+ d_i \circ \tau j_i + \mu^+ d_n \circ \tau j_i \leqslant \mu d_0 \circ \tau j_i + \mu d_i\ \tau j_i$$

$$= \mu a_i \circ \tau j_i + \mu d_i \circ \tau j_i + 1$$

Donc $\quad \Sigma \mu a_k \circ \tau j_i + 1 \leqslant \mu d_0 \circ \tau j_i$

Enfin, puisque $\Theta d_0 \circ \tau d_i < \tau d_i$, et d'après (ii), il vient:

$$\mu d_0 \circ \tau j_i - 1 = \Sigma \mu a_k \circ \Theta d_0 \circ \tau j_i \leqslant \Sigma \mu a_k \circ \tau j_i \leqslant \mu d_0 \circ \tau j_i - 1$$

Les membres extrêmes étant egaux, on en déduit

$$\Sigma\ \mu a_k \circ \Theta d_0 \circ \tau j_i = \mu a_k \circ \tau j_i$$

et comme $\mu a_k \circ \Theta d_0 \circ \tau j_i \leq \mu a_k \circ \tau j_i$, ceci implique (i) et termine la preuve du lemme 1.

Lemme 2 si $k < i$, il se produit une occurrence de d_k entre le dernier d_0 précédant j_i et j_i:

$$k < i \implies \Theta d_0 \circ \tau j_i = \Theta d_0 \circ \Theta d_k \circ \tau j_i$$

Démonstration: Il suffit de montrer que $\Theta d_0 \circ \tau j_i < \Theta d_k \circ \tau j_i$. Le lemme s'en déduira d'après la rétractivité de Θd_0.

On a:

$$\mu^+ j_i + \sum_{\ell=1}^{i-1} \mu a_\ell \leq \mu d_k + \sum_{\ell=1}^{k} \mu a_\ell \leq \mu d_0 \leq \mu j_i + \sum_{\ell=1}^{k} \mu a_\ell + 1$$

En composant avec τj_i, il vient:

$$I + 1 + \sum_{\ell=1}^{i-1} \mu a_\ell \circ \tau j_i \leq \mu d_k \circ \tau j_i + \sum_{\ell=1}^{k} \mu a_\ell \circ \tau j_i \leq \mu d_0 \circ \tau j_i \leq I+1+ \sum_{\ell=1}^{k} \mu a_\ell \circ \tau j_i$$

$$\leq I + 1 + \sum_{\ell=1}^{i-1} \mu a_\ell \circ \tau j_i$$

Les membres extrêmes étant égaux, il vient:

$$\mu d_k \circ \tau j_i + \sum_{\ell=1}^{k} \mu a_\ell \circ \tau j_i = \mu d_0 \circ \tau j_i \qquad \text{(iv)}$$

Posons $A_k = \sum_{\ell=1}^{k} a_\ell$ et $e_k = A_k + d_k$

On a $\mu^+ e_k < \mu d_0$, soit $\tau d_0 < \tau e_k$

En composant par τd_0 le premier membre de (iv), et par τe_k son second membre, on obtient $\Theta e_k \circ \tau j_i > \Theta d_0 \circ \tau j_i$.

Or $\Theta e_k = \sup(\Theta d_k, \Theta A_k)$. Donc:

$$\Theta d_0 \circ \tau j_i < \sup(\Theta d_k \circ \tau j_i\ ,\ \Theta A_k \circ \tau j_i) \qquad \text{(v)}$$

Enfin, on déduit de la relation (i), établie précédemment, la relation

$$\forall \ell, \quad \Theta a_\ell \circ \tau j_i = \Theta a_\ell \circ \Theta d_0 \circ \tau j_i$$

Or

$$\Theta a_\ell \circ \Theta d_0 \circ \tau j_i < \Theta d_0 \circ \tau j_i$$

Donc

$$\Theta A_k \circ \tau j_i = \sup_{\ell=1..k} (\Theta a_\ell \circ \tau j_i) < \Theta d_0 \circ \tau j_i \qquad \text{(vi)}$$

De (v) et (vi), on tire $\Theta d_0 \circ \tau j_i < \Theta d_k \circ \tau j_i$ C.Q.F.D.

Nous sommes maintenant en mesure de prouver le respect de la priorité. En effet, d'après le lemme 1, $\forall k$, $\mu a_k \circ \Theta d_0 \circ \tau d_k = \mu r_k \circ \Theta d_0 \circ \tau d_k$. Donc, $\forall k$, $\mu a_k \circ \Theta d_0 \circ \tau j_i = \mu r_k \circ \Theta d_k \circ \tau j_i$, et d'après le lemme 2,

$$k < i \implies \mu a_k \circ \Theta d_0 \circ \tau j_i = \mu r_k \circ \Theta d_0 \circ \tau j_i \qquad \text{(vii)}$$

Comme $a_i \subseteq j_i$, $k < i \implies \mu a_k \circ \Theta d_0 \circ \tau a_i = \mu r_k \circ \Theta d_0 \circ \tau a_i$ (PR')

3.2.2.3. Temps de réponse

Par sommation des relations $a_i + d_i \geq R^{\varepsilon} d_{i-1}$, il vient:

$$\Sigma a_i + d_n \geq R^{n\varepsilon} d_0 \qquad \text{(viii)}$$

Puisque $n\varepsilon < \delta$, il suffit de monter que $d_n = 0$, c'est à dire que, chaque fois que l'unité U_n reçoit un jeton, elle demande le bus:

$$\mu r_n \circ \tau j_n > \mu a_n \circ \tau j_n + 1$$

Cette relation est facile à obtenir, en vertu des résultats précédents:

Par définition de d_0, lorsque d_0 se produit, une unité au moins demande le bus:

$$\Sigma\mu r_i \circ \tau d_0 > \Sigma\mu a_i \circ \tau d_0 + 1$$

Donc, $\Sigma\mu r_i \circ \Theta d_0 \circ \tau j_n > \Sigma\mu a_i \circ \Theta d_0 \circ \tau j_n + 1$

Or, d'après (vii), $\sum_{i<n} \mu r_i \circ \Theta d_0 \circ \tau j_n = \sum_{i<n} \mu a_i \circ \Theta d_0 \circ \tau j_n$

Donc $\mu r_n \circ \Theta d_0 \circ \tau j_n = \mu a_n \circ \Theta d_0 \circ \tau j_n + 1$.

Enfin, d'après (i), $\mu a_n \circ \Theta d_0 \circ \tau j_n = \mu a_n \circ \tau j_n$

et comme $\mu r_n \circ \Theta d_0 \circ \tau j_n < \mu r_n \circ \tau j_n$, ceci achève la preuve

3.2.3. Schéma de cablage

En ce qui concerne la réalisation matérielle, on construit d'abord un montage réalisant (à un délai de réponse près) le filtrage d'un événement par une condition (figure 3). La bascule D échantillone la valeur de la condition C sur les fronts montants de l'entrée E. Après un délai Δ, suffisant à la stabilisation de la bascule, et sous réserve que deux fronts successifs de E soit séparés par un délai supérieur à Δ, les fronts montants des sorties F et G réalisent respectivement le filtrage de E↑ par C et par $\neg$C.

Les éléments d'arbitrage sont réalisés à l'aide de tels opérateurs. Le schéma complet est représenté par la figure 4. Le fonctionnement des unités est supposé être le suivant :

- L'émission d'une requête consiste à mettre à 1 la sortie R;
- Sur réception d'une autorisation (valeur 1 sur l'entrée A), la sortie R est remise à zéro et la sortie O est mise à 1;
- La libération du bus entraine l'annulation de O.

Sous ces hypothèses, et à partir d'une description du comportement des opérateurs (portes, bascules, fils, retards) on peut montrer la conformité de cette réalisation aux spécifications de l'arbitre.

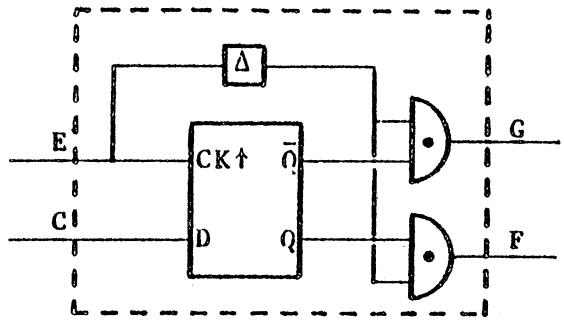


Figure 3
Circuit de filtrage

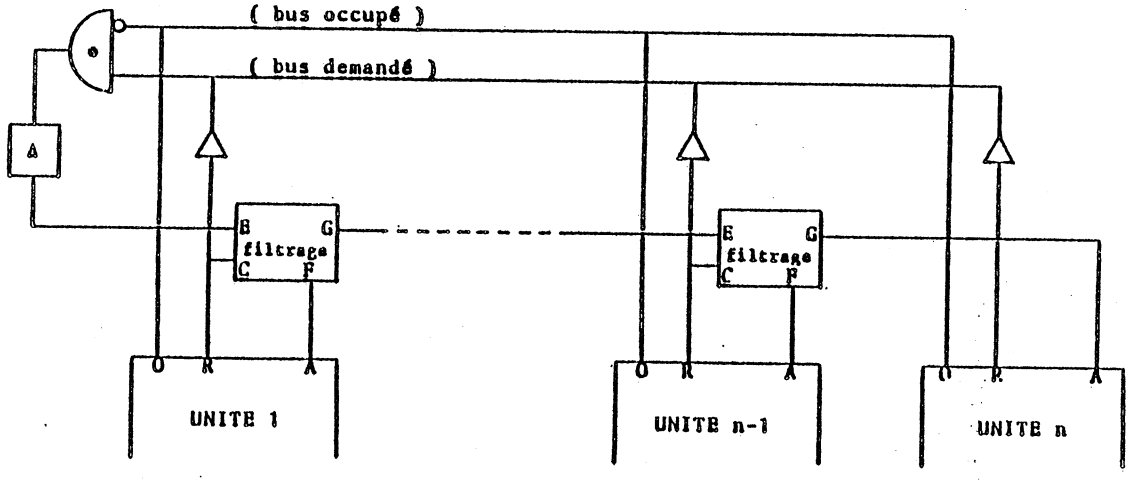


Figure 4
Arbitre par jeton circulant

3.3. DEUXIEME SOLUTION : CONDITION STABILISEE

Une autre solution, moins classique, consiste à transmettre le long de la chaine des arbitres, non pas l'événement "demande d'arbitrage" filtré de proche en proche, mais seulement la condition intervenant dans le filtrage. Apparemment très proche de la première, cette solution s'en révèle en fait très différente, tant du point de vue de la réalisation à laquelle elle mène, qu'en ce qui concerne sa preuve : Dans la preuve de

l'algorithme du jeton, les difficultés résident dans la démonstration du respect de la priorité et du temps de réponse. Ici le seul point délicat concernera l'exclusivité, les autres propriétés s'en déduisant sans difficulté.

3.3.1. Algorithme

Très informellement, chaque arbitre reçoit maintenant, directement, la demande d'arbitrage, et affiche, sur réception, son verdict personnel. Après un delai suffisant, le i-ème arbitre est assuré que tous les arbitres plus prioritaires ont pris leurs décisions, et est donc en mesure de prendre la sienne.

- Soit $d = \inf(\Sigma r_i , \Sigma \ell_i+1)$ l'événement "demande d'arbitrage" et soit d_i (i=1...n) l'image qu'en reçoit l'arbitre i. Cette réception est supposée strictement postérieure à l'émission, et soit ε_1 une majoration du temps de transmission :

$$d > d_i \geq R^{\varepsilon_1} d \quad , \quad i=1...n$$

- Soit C_i l'état des requêtes de U_i échantillonné sur réception de d_i :

$$C_i = (\mu r_i \circ \Theta d_i \geq \mu a_i \circ \Theta d_i + 1)$$

- Après un delai $\varepsilon_2 > \varepsilon_1$, compté à partir de la réception de d_i, l'arbitre i est assuré que tous les autres arbitres ont reçu la demande d_j, et ont donc affiché leur état C_j. Il peut donc prendre sa décision :

$$a_i = b_i \mid A_i$$
$$\text{avec } b_i = R^{\varepsilon_2} d_i \quad \text{et} \quad A_i = C_i \wedge \bigwedge_{j<i} \neg C_j$$

- On s'aperçoit, en essayant de prouver cette solution, qu'elle n'est correcte que si l'on suppose qu'une unité qui accède au bus le conserve pendant un delai minimum, ε_3, avec $\varepsilon_3 > \varepsilon_1$, c'est à dire sous l'hypothèse :

$$\ell_i \geq R^{\varepsilon_3} a_i \quad , \quad \varepsilon_3 > \varepsilon_1$$

- Le temps de réponse de l'arbitre est alors $\varepsilon_1 + \varepsilon_2$, et pour satisfaire la contrainte TR, on doit donc prendre $\varepsilon_1+\varepsilon_2 < \delta$.

3.3.2. Preuve de l'exclusivité

La preuve de cette solution soulève des difficultés d'un autre ordre que celle de l'algorithme du jeton, pour la raison suivante : Dans l'algorithme du jeton, il est clair qu'entre deux arbitrages, l'ensemble des arbitres revient à un état de repos. Il suffit donc de prouver l'invariance des propriétés requises sur un intervalle de temps séparant deux état de repos. Par contre, ici, le bon fonctionnement de l'arbitre dans l'avenir, dépend, à priori, de tout son passé. Dans ce cas, la démonstration nécessite clairement un raisonnement par induction. C'est pourquoi nous utiliserons le théorème de sur-causalité (§2.3.2.3). Pour cela, nous procèderons en trois étapes :

- Nous montrerons d'abord que si tous les arbitres prenaient leurs décisions de manière synchrone (c'est à dire si tous les b_i étaient simultanés), l'exclusivité serait assurée.

- Nous considérerons ensuite un système d'arbitrage connaissant les décisions synchrones et les décisions asynchrones, et élaborant la borne inférieure de ces décisions. Nous montrerons que cette borne inférieure satisfait encore à l'exclusivité.

- Enfin, nous montrerons que la borne inférieure élaborée est toujours la décision asynchrone, et, par application du théorème de sur-causalité nous en déduirons que l'élaboration de cette borne inférieure, et donc la connaissance de la décision synchrone (irréalisable) sont inutiles.

a) Soit $b_0 = R^{\varepsilon 2} d_0$ et $a'_i = b_0 \mid A_i$ (décisions synchrones).

On a $\Sigma a'_i = \Sigma b_0 \mid A_i$. Or les A_i sont exclusives, donc:

$$\Sigma\, b_0 \mid A_i = b_0 \mid \bigvee_{i=1}^{n} A_i$$

On en déduit:

$$\Sigma\, a'_i \lessdot b_0 \lessdot d_0 \lessdot \Sigma\, \ell_i + 1$$

b) Soit maintenant $a_i = \inf(a'_i, a''_i)$, où les a''_i sont les décisions asynchrones:

$$a''_i = b_i \,|A_i \text{ avec } b_i = R^{\varepsilon 2}\, d_i$$

On a alors:

$$\Sigma\, a_i \lessdot \Sigma\, a'_i \lessdot b_0 \lessdot d_0 \lessdot \Sigma\, \ell_i + 1$$

d'où l'exclusivité des a_i.

c) Il reste à montrer $a''_i \lessdot a'_i$, d'où l'on pourra conclure, d'après le théorème de sur-causalité, que $a_i = a''_i$ et donc l'exclusivité de l'arbitre asynchrone.

- Montrons d'abord l'entrelacement des d_j et des b_i, c'est à dire que la n-ième occurrence de b_i succède strictement à la n-ième occurrence de d_j et précède sa n+1-ième occurrence. Ce qu'on peut écrire:

$$\mu d_j \circ \tau b_i = I \qquad \text{(i)}$$

Pour cela, remarquons tout d'abord que deux occurrences successives de d_j sont séparées par un intervalle d'au moins $\varepsilon_2 - \varepsilon_1 + \varepsilon_3$. En effet:

$$d_j \lessdot d_0 \lessdot 1 + \Sigma\, \ell_i \lessdot 1 + R^{\varepsilon 3} \Sigma\, a_i \lessdot 1 + R^{\varepsilon 3} \Sigma\, a'_i$$

$$\lessdot 1 + R^{\varepsilon 3} b_0 = 1 + R^{\varepsilon 2 + \varepsilon 3} d_0 \lessdot 1 + R^{\varepsilon 2 + \varepsilon 3 - \varepsilon 1} d_j \qquad \text{(ii)}$$

Ceci entraine que:

- d_j est à occurrences simples
- $d_0 \lessdot 1 + R^{\varepsilon 2 + \varepsilon 3} d_0$

Donc, puisque $\varepsilon_3 > \varepsilon_1$ et $\varepsilon_2 > \varepsilon_1$,

$$d_j \leqslant d_0 \leqslant 1+R^{\varepsilon_2+\varepsilon_3}d_0 \leqslant 1+R^{\varepsilon_1+\varepsilon_2}d_0 \leqslant 1+b_i \leqslant 1+R^{\varepsilon_2}d_0 < 1+R^{\varepsilon_1}d_0 \leqslant 1+d_j$$

soit

$$d_j \leqslant 1 + b_i < 1 + d_j$$

et

$$\tau d_j \circ (I+1) \geqslant \tau b_i > \tau d_j$$

En composant par μd_j, et comme d_j est à occurrences simples, il vient:

$$\mu d_j \circ \tau d_j \circ (I+1) = \mu^+ d_j \circ \tau d_j = I \geqslant \mu d_j \circ \tau b_i > \mu d_j \circ \tau d_j = I-1$$

soit

$$\mu d_j \circ \tau b_i = I \qquad (i)$$

- Par composition avec τd_j, il vient:

$$\forall i,j \in [0 \ldots n],\ \Theta d_j \circ \tau b_i = \tau d_j$$

soit,

$$\forall i,j \in [0 \ldots n],\ \Theta d_j \circ \tau b_i = \Theta d_j \circ \tau b_0$$

et donc, d'après la définition des conditions C_j et A_j,

$$\tilde{\nu} A_j \circ \tau b_i = \tilde{\nu} A_j \circ \tau b_0 \qquad (iii)$$

On peut donc appliquer la proposition 1.2.6, et déduire:

$$b_i \leqslant b_0 \Rightarrow \quad a_i'' = b_i | A_i \leqslant b_0 | A_i = a_i'$$

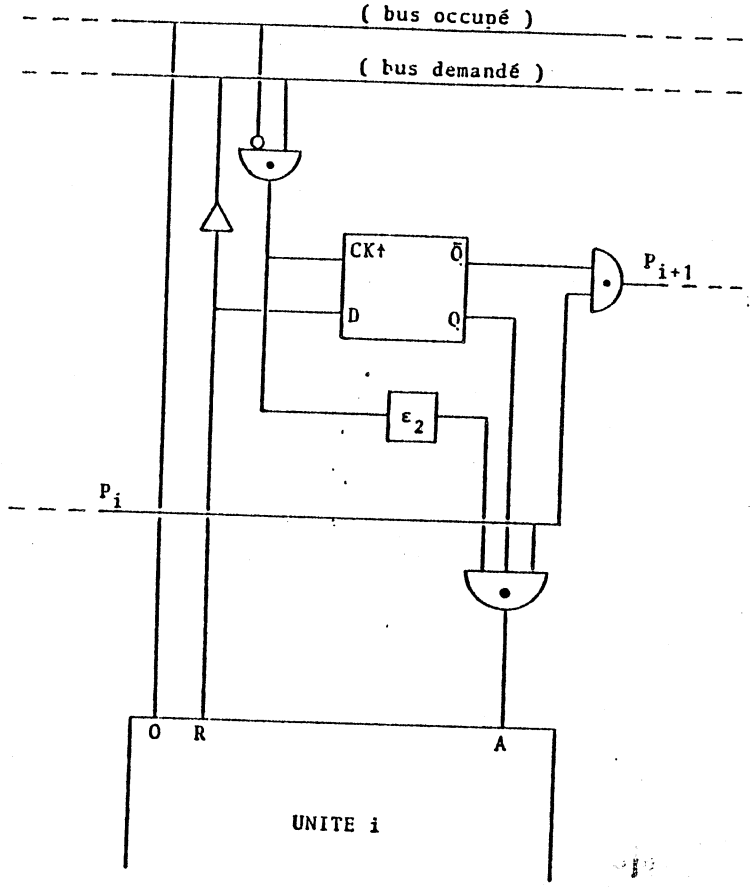


Figure 5
Arbitre par condition stabilisée

3.3.3. Schéma de cablage

La figure 5 présente un schéma de cablage de l'arbitre par condition stabilisée. L'arbitre i reçoit en P_i la condition

$$\bigwedge_{j<i} \neg C_j \circ \Theta d_j$$

élaborée par ses prédécesseurs (cette entrée est fixée à 1 pour le

premier arbitre). Il y rajoute son propre terme $\neg C_i$ - échantillonné au moyen d'une bascule, sur reception d'une demande d'arbitrage - et émet le résultat vers l'entrée P_{i+1} de son successeur. Par ailleurs, chaque demande d'arbitrage est retardée d'un délai ε_2, avant de provoquer, si l'entrée P_i est vraie et si une requête a été échantillonnée, l'émission d'une autorisation.

Ce schéma met en lumière le temps de réponse de cette solution, notablement plus court que celui de la précédente, dans la mesure où une demande d'arbitrage ne traverse ici qu'une bascule.

3.4. CONCLUSION

Nous avons illustré l'usage de notre formalisme à la conception et à la preuve d'un système distribué. Nous espérons avoir montré que l'approche comportementale permet une spécification naturelle (on écrit simplement ce que le système doit faire, sans indiquer comment il le fait), même si, sous la forme brute que nous avons présentée, le formalisme peut paraître rebutant (un certain "sucre syntaxique" est assurément nécéssaire pour rendre les descriptions plus lisibles). Une autre caractéristique de ce mode de description est d'être applicable depuis les spécifications initiales jusqu'à un niveau très proche de la réalisation, y compris matérielle (en fait, jusqu'au niveau logique, le formalisme étant, à l'évidence, peu adapté à la description du comportement transitoire des composants entre deux états stables). Le formalisme a d'ailleurs été largement utilisé par [Amblard] à la description et à la preuve du matériel.

En ce qui concerne la validation, la preuve de certaines propriétés, apparemment évidentes, est d'une difficulté surprenante. Il est clair que cette difficulté provient du niveau de détail de la preuve, mais une conclusion que nous tirons de cette expérience est que ce niveau de détail est nécessaire à la rigueur de la démonstration, dans la mesure où d'autres propriétés de l'arbitre, non moins évidentes en apparence, se sont révélées fausses au cours de la preuve.

En conclusion, l'argument principal que nous avons avancé en faveur du formalisme présenté dans cette première partie, est de minimiser les risques d'erreur au cours du processus de formalisation initiale des spécifications, de par le caractère "naturel" de ce processus. Ce caractère naturel est évidemment subjectif et non quantifiable, aussi donnons-nous ici, au travers d'un exemple trés simple, des éléments de comparaison avec d'autres formalismes.

L'exemple est la spécification d'un canal parfait : le canal reçoit sequentiellement des messages à une extrémité, et les délivre séquentiellement à l'autre extrémité, sans perte de message et en préservant leur ordre.

Donnons les spécifications de ce canal dans deux formalismes trés différents.

Le premier est une logique temporelle [Koymans & De Roever], utilisant, entre autres, les opérateurs temporels suivants:

- l'opérateur "toujours" : $\Box P$ est vrai si et seulement si le prédicat P est toujours vrai, dans le futur, à partir de l'instant considéré;
- l'opérateur "inévitablement" : $\Diamond P$ est vrai ssi le prédicat P est vrai au moins une fois dans le futur, à partir de l'instant considéré;
- l'opérateur "suivant" : $\circ P$ est vrai ssi le prédicat P est vrai à l'instant suivant l'instant considéré (le temps étant discret);
- l'opérateur "avant" : $\blacklozenge P$ est vrai ssi P a été vrai au moins une fois avant l'instant considéré.

Le canal parfait peut être spécifié dans cette logique de la manière suivante: On suppose que chaque message est univoquement identifié, et on modélise la réception et la délivrance d'un message m au moyen des prédicats accept(m) et deliver(m). La spécification du canal tient alors en six axiomes:

. Les axiomes (1) et (2) expriment la séquentialité de la reception et de la délivrance des messages:

1) accept(m) & accept(m') => m = m'

2) deliver(m) & deliver(m') => m = m'

. L'axiome (3) exprime que tout message reçu sera ultérieurement délivré:

3) accept(m) => ◇ deliver(m)

. Les axiomes (4) et (5) imposent respectivement que le canal ne duplique ni ne génère de message:

4) deliver(m) => o□ ¬deliver(m)

5) deliver(m) => ♦accept(m)

. Enfin, l'axiome (6) impose le respect de l'ordre des messages:

6) accept(m) & o◇accept(m') =>

□(deliver(m) => ¬♦deliver(m'))

Le deuxième modèle est celui de [Chen & Yeh]. On y décrit des entités appelées évènements, auxquelles peuvent être associées des valeurs. Ainsi, dans le cas du canal parfait, décrira-t-on deux ensembles d'évènements R et D, correspondant aux réceptions et aux délivrances de messages, évènements auxquels seront associées les teneurs des messages. Deux relations sont définies sur les évènements:

Une relation de préordre, qui exprime la succession dans le temps:

e → f ssi e précède f

Une relation d'ordre strict, qui exprime la causalité:

e ≫ f ssi e est une cause de f

La spécification du canal parfait dans ce modèle est la suivante:

- Le canal ne perd ni n'engendre de message:

∀r ∈ R, ∃d ∈ D tel que r ≫ d

∀d ∈ D, ∃r ∈ R tel que r ≫ d

- Le canal ne duplique pas de message:

∀r ∈ R, ∀d, d' ∈ D, (r ≫ d & r ≫ d') => (d = d')

- La propriété suivante exprime à la fois la préservation de l'ordre et la séquentialité:

$$\forall r, r' \in R, \forall d, d' \in D, (r \gg d \;\&\; r' \gg d') \Longrightarrow$$
$$[(r \nrightarrow r' \;\&\; d \nrightarrow d') \vee (r = r' \;\&\; d = d') \vee (r' \nrightarrow r \;\&\; d' \nrightarrow d)]$$

- Enfin on exprime la relation évènements/messages:

$$\forall r \in R, \forall d \in D, r \gg d \Longrightarrow r.msg = d.msg$$

Ces deux modèles ne constituent évidemment qu'un échantillon, parmi les formalismes de spécification comportementale des systèmes parallèles et temps réèl. Nous les avons choisis surtout parce que les articles cités traitent tous deux le même exemple. Dans notre formalisme, le canal peut être décrit comme suit:

Soient R et D les variables représentant respectivement les messages reçus et délivrés par le canal. Alors l'équation suivante exprime à la fois que le canal

- ne duplique pas de message
- ne génère pas de message
- respecte l'ordre des messages.

$$1)\ \nu d = \nu r$$

Il faut encore exprimer:

2) que la délivrance d'un message succède à sa reception: $d \lessdot r$

3) l'occurrence simple des évènements r et d (séquentialité), par l'une des propriétés caractéristiques données au §2.2.5.

4) que tout message reçu est délivré au bout d'un temps fini:

$$\mu d(+\infty) = \mu r(+\infty)$$

Remarque:

Cette dernière équation illustre l'expression des propriétés d'inévitabilité, dans notre modèle, à l'aide de relations entre compteurs à l'infini. Ce procédé permet aussi d'exprimer différents types d'équité. L'exploitation de ce type de contraintes dans les preuves reste cependant à étudier.

Par cet exemple, notre propos est surtout d'illustrer la simplicité de l'équation (1), traduisant trois contraintes intuitivement très simples - la suite des messages délivrés est la même que la suite des messages reçus - mais nettement plus complexes à exprimer dans les deux autres modèles.

DEUXIEME PARTIE

OUTILS D'ANALYSE DES SYSTEMES TEMPORISES

CHAPITRE 4

CALCUL FORMEL EN EVENEMENTS

Dans la première partie de cette thèse, notre objectif principal n'a pas été d'obtenir des méthodes de déduction systématiques - à l'inverse d'autre modèles plus algorithmiques et mieux axiomatisés (Réseaux de Pétri [Giraut & Reisig], logique temporelle [Queille], [Bochmann], [Hailpern & Owicki], [Schwartz, Melliar-Schmit & Vogt], [Moszkowski], algèbres de processus [Milner 80], [Milner 82], [Austri & Boudol], [Cardelli], modèles axiomatiques [Shostak] ou dénotationnels [Gordon] - mais plutôt d'assurer la correction des spécifications. Pour cela, nous nous sommes contenté d'introduire deux concepts - les évènements et les variables - ainsi qu'un ensemble de notations qui nous paraissent fournir un cadre adéquat pour formaliser le contenu d'un cahier des charges, à la fois naturellement, précisément, et sans introduire de fausses contraintes. Nous n'avons abordé les problèmes d'analyse et de preuve que ne manière relativement naïve, en affirmant simplement qu'une fois le comportement d'un système formalisé en termes mathématiques, tout l'arsenal des mathématiques pouvait lui être appliqué à des fins d'analyse . Il reste que les démonstrations que nous avons données pour illustrer cette approche paraissent difficiles à systématiser. C'est pourquoi nous allons explorer maintenant un modèle, fondé sur les mêmes concepts, mais plus restreint quant à sa puissance d'expression, à partir duquel nous tenterons de dégager des méthodes systématiques d'analyse. En particulier, nous nous restreindrons dorénavant au domaine des systèmes logiques, c'est à dire que les objets que nous décrirons seront des évènements et des conditions.

Le calcul que nous allons construire est fondé sur une formalisation un peu différente de la notion d'évènements : L'idée qui préside à cette nouvelle formalisation consiste à considérer le compteur d'un évènement du point de vue de sa transformée de Laplace. Nous allons, en fait, définir les évènements comme cas particuliers d'objets plus généraux, que nous appellerons "pseudo-évènements".

4.1. L'ANNEAU ORDONNE DES PSEUDO-EVENEMENTS

4.1.1 Définitions :

Un pseudo-évènement x sur $\mathbb{T}$ est une série formelle de la forme:

$$x = \sum_{n=1}^{\sharp x} \bar{x}_n R^{x_n}$$

où

- $(\bar{x}_n)$ est une suite d'entiers relatifs non nuls ;
- (x_n) est une suite strictement croissante d'éléments de $\mathbb{T}$;
- ces deux suites ont la même longueur, $\sharp x$, qui peut être finie ou infinie, mais si $\sharp x = +\infty$, alors x_n tend vers l'infini avec n.

On notera A($\mathbb{T}$), ou simplement A, l'ensemble des pseudo-évènements sur $\mathbb{T}$. L'ensemble A est muni des opérateurs de somme et de produit usuels sur les séries formelles, qui le munissent d'une structure d'anneau unitaire, dont les éléments neutres sont:

- pour l'addition, le pseudo-évènement 0, tel que $\sharp 0 = 0$;
- pour la multiplication, le pseudo-évènement $1 = R^0$.

Cet anneau est intègre et de caractéristique zéro:

- $xy = 0 \;\&\; x \neq 0 \;\Rightarrow\; y = 0$
- $\forall n \in \mathbb{N}^*, \forall x \neq 0 , \quad nx = \sum_{i=1}^{n} x \neq 0$

Il contient donc un sous-ensemble [$\mathbb{Z}$], isomorphe à $\mathbb{Z}$. Nous ne noterons pas différemment les pseudo-évènements de [$\mathbb{Z}$] et les entiers:

$$\forall n \in \mathbb{Z} \ , \ nR^0 = n$$

Un évènement est un pseudo-évènement dont les coefficients $\bar{x}_n$ sont positifs (Par convention, 0 est un évènement). Dans le cas d'un évènement, le coefficient $\bar{x}_n$ est le nombre d'occurrences de x survenant à l'instant x_n . On notera E($\mathbb{T}$), où simplement E, le sous-ensemble de A($\mathbb{T}$) constitué par les évènements.

Il est clair que, pour tout $x \in A(\mathbb{T})$, il existe un couple (e,f) d'évènements tel que $x = e - f$. Cependant ce couple n'est pas unique: En fait A est le groupe des différences de E, c'est à dire le quotient de E×E par la relation d'équivalence:

$$(e_1, f_1) \equiv (e_2, f_2) \quad \text{s.s.i.} \quad e_1 + f_2 = f_1 + e_2$$

4.1.2. Compteurs et ordre

A tout pseudo-évènement x peut être associée, de manière bi-univoque, une "fonction compteur" μx, de $\mathbb{T}$ dans $\mathbb{Z}$, définie comme suit:

$$\mu x = \lambda t. \sum_{x_n < t} \bar{x}_n$$

On définit sur A la relation d'ordre suivante :

$$x \leqslant y \iff \mu x \leqslant \mu y$$

(A,$\leqslant$) est un treillis, dont les opérateurs de bornes inférieure (inf) et supérieure (sup) sont les opérateurs correspondants sur les compteurs.

4.1.3. Commentaires :

- La fonction compteur μx d'un pseudo-évènement x n'est croissante que si x est un évènement, auquel cas la définition ci-dessus coïncide avec la définition 2.2.1. La relation d'ordre sur A coïncide donc, sur E, avec la relation de précédence définie au §2.2.6.1.

L'évènement strictement périodique survenant aux instants 0, Δ, 2Δ, ..., $n\Delta$, ... sera noté dorènavant $\Sigma_{n>0}R^{n\Delta}$. Nous avons vu au §2.2.7.3 que cet évènement est l'unique solution de l'équation

$$e = R^{\Delta}e + 1 \qquad (1)$$

où 1 ($=R^0$) est l'évènement dont l'unique occurrence, à date finie, survient à l'instant zéro. Cet exemple appelle quelques remarques:

- La notation des évènements sous forme de séries fait abstraction d'une part, de l'occurrence d'indice zéro survenant à $-\infty$, et d'autre part, de toutes les occurrences survenant à $+\infty$: N'apparaissent dans la série, sous forme d'exposants, que les dates d'occurrences appartenant à $\mathbb{T}$.

- L'expression $R^{\Delta}e$, que nous considérions jusqu'ici comme dénotant le résultat de l'application de l'opérateur de translation R^{Δ} à l'évènement e, peut être vue maintenant comme le produit de e par l'évènement R^{Δ} - série à un seul terme - qui est l'évènement dont l'unique occurrence survient à l'instant Δ .

- Dans l'anneau A, on peut déduire de l'équation (1), l'équation formellement équivalente

$$e(1-R^{\Delta}) = 1 \qquad (2)$$

Nous allons franchir, au §4.2, l'étape suivante de la résolution formelle de l'équation (1), consistant à "diviser" par le pseudo-évènement $1-R^{\Delta}$, les deux membres de l'équation (2).

4.2. INVERSION ET DIVISION EUCLIDIENNE

4.2.1. Pseudo-évènements inversibles

4.2.1.1. Proposition : Une condition nécéssaire et suffisante pour q'un pseudo-évènement $x \in A(\mathbb{T})$ admette un inverse, est que $\bar{x}_1 = \pm 1$.

Démonstration:

Soit x un pseudo-évènement tel que $\bar{x}_1 = \pm 1$. On peut écrire

$$x = \bar{x}_1 R^{x_1} (1 - y)$$

avec $$y = -\bar{x}_1 \sum_{n=2}^{\#x} \bar{x}_n R^{x_n - x_1}$$

Notons y^k le produit itéré k fois de y par lui-même, et soit

$$x' = \bar{x}_1 R^{-x_1} \sum_{k>0} y^k$$

Alors $xx' = \bar{x}_1^2 R^0 (\sum_{k>0} y^k - \sum_{k>1} y^k) = 1$, et x' est donc l'inverse de x.

Inversement supposons que x ait un inverse x'. Alors $xx'=1$, et le premier terme de la série xx' est $\bar{x}_1 \bar{x}'_1 R^{x_1 + x'_1}$. On doit donc avoir $\bar{x}_1 \bar{x}'_1 = 1$, ce qui, dans $\mathbb{Z}$, entraine $\bar{x}_1 = \pm 1$.

4.2.1.2. Corollaires :

- Soit e une évènement tel que $e_1 > 0$. Alors l'inverse de 1-e est un évènement puisque

$$\frac{1}{1 - e} = \sum_{k>0} e^k$$

- Une condition nécéssaire et suffisante pour que l'inverse d'un évènement e soit un évènement est que $e = R^{\Delta}$. Il est clair que $1/R^{\Delta} = R^{-\Delta}$. Donc $\{ R^{\Delta} \mid \Delta \in \mathbb{T} \}$ est l'ensemble des unités du demi-anneau $(E(\mathbb{T}), +, \times)$.

4.2.1.3. Commentaires :

- Notre structure est sensiblement plus riche que l'anneau A(ℕ) des séries formelles généralement considéré en mathématiques et qui a trouvé des applications en théorie des langages [Berstel]. Ces séries, généralisation des polynômes, sont à exposants entiers naturels. Il en résulte que les seules séries inversibles, dans cette algèbre sont les séries telles que $\bar{x}_1 = \pm 1$ et $x_1 = 0$. C'est pourquoi l'opérateur de "quasi inversion" a été introduit [Berstel], qui associe à toute série x telle que $x_1 > 0$, sa quasi-inverse:

$$1/(1-x) = \sum_{k>0} x^k .$$

- A(ℤ) est l'algèbre $\mathbb{Z}[[R]][R^{-1}]$ des séries formelles de Laurent, de la forme $\Sigma_{n>n_0} a_n R^n$ ($a_n \in \mathbb{Z}$), dans laquelle les résultats d'inversibilité précédants sont classiques, ainsi que les développements qui suivent, concernant la division Euclidienne [Samuel].

- Ces résultats sur l'inversibilité nous permettent, dés à présent, d'achever la résolution de l'équation $e = R^{\Delta}e + 1$, puisque, de $e(1-R^{\Delta}) = 1$, on déduit, d'après l'inversibilité de $1 - R^{\Delta}$ pour $\Delta > 0$,

$$e = \frac{1}{1 - R^{\Delta}} = \sum_{n>0} R^{n\Delta}$$

ce qui est bien l'expression de l'évènement strictement périodique survenant à 0, Δ, 2Δ, ..., nΔ, ...

4.2.2. Division Euclidienne

4.2.2.1. Norme d'anneau : L'application u, de A dans ℕ, définie par

$$u(x) = \begin{cases} 0 \ , \text{ si } x = 0 \\ |\bar{x}_1| , \text{ si } x \neq 0 \end{cases}$$

est une norme d'anneau de A, c'est à dire que:

- $u(x) = 0$ si et seulement si $x = 0$;
- $u(xy) = u(x)u(y)$;
- $u(x) = 1$ si et seulement si x est inversible .

4.2.2.2. Théorème : Si $\mathbb{T} = \mathbb{R}$ ou $\mathbb{Z}$, l'anneau $A(\mathbb{T})$ est Euclidien, c'est à dire que, pour tout x, y dans $A(\mathbb{T})$ $(y \neq 0)$, il existe q et r dans $A(\mathbb{T})$ tels que:

$$x = yq + r \quad \text{et} \quad u(r) < u(y)$$

Démonstration : Nous allons donner l'algorithme de la division Euclidienne, qui est très proche de la division des polynômes selon les puissances croissantes de la variable.

L'algorithme construit deux suites $(q(k))$ et $(r(k))$ de pseudo-évènements comme suit:

Etape 0 : Soient $\underline{r}(0) = x$ et $q(0) = 0$;
Etape k+1 : Si $|\underline{r}(k)_1| \geq \bar{y}_1$, soit $\alpha_k = \underline{r}(k)_1/\bar{y}_1$. Si $\alpha_k \in \mathbb{Z}$, posons:

$$p(k) = \alpha_k R^{r(k)_1 - y_1}$$
$$q(k+1) = q(k) + p(k)$$
$$r(k+1) = r(k) - p(k)y$$

Alors, à chaque étape k ainsi atteignable, on a évidemment:

$$x = y\, q(k) + r(k)$$

Trois situations peuvent se présenter dans le déroulement de cet algorithme:

- Soit on s'arrête à une étape k, parce que $|\underline{r}(k_1)| < \bar{y}_1$. Dans ce cas, le résultat est atteint, puisque $u(r(k)) < u(y)$.
- Soit on s'arrête à une étape k, parce que $\alpha_k \notin \mathbb{Z}$. Alors, soit α le plus petit entier plus grand que α_k si $\alpha_k > 0$, le plus grand entier plus petit que α_k si $\alpha_k < 0$. Posons

$$p = \alpha\, R^{r(k)_1 - y_1} \qquad q = q(k) + p \qquad r = r(k) - py$$

Alors, par définition de α, on a $u(r) < u(y)$ et $x = yq + r$.

- Soit l'algorithme ne s'arrête pas. Alors la suite $(r(k)_1)$ tend vers $+\infty$ avec k, donc la suite $(r(k))$ tend vers 0 (au sens de la convergence simple des fonctions compteurs) et la suite $(q(k))$ tend vers une limite q telle que $x = yq$.

4.3. EXEMPLE D'APPLICATION

Nous disposons dés à présent des éléments algébriques pour appliquer notre calcul à l'analyse d'un système très simple:

Le système reçoit deux séquences de requêtes, strictement périodiques. La première séquence débute à l'instant 0, avec une période de 2 unités de temps, la deuxième débute à l'instant 1, avec une période 4. Le système est composé de n processeurs identiques, sur lesquels le traitement d'une requête de la première séquence requiert 7 unités de temps, alors qu'une requête de la deuxième séquence nécessite un traitement de 5 unités de temps. Les requêtes sont traitées à mesure de leur arrivée, avec la seule contrainte qu'un processeur ne peut rester inactif alors qu'il existe des requêtes non prises en compte.

On se pose le problème de trouver le nombre minimum de processeurs assurant que toute requête soit prise en compte dés son arrivée.

Modélisons ce problème en termes d'évènements. Soient

- a_i (i=1,2) l'évènement associé à l'arrivée des requêtes de la i-ième séquence ;
- e_i (i=1,2) l'évènement associé à la prise en compte des requêtes de la i-ième séquence par l'un des processeurs ;
- f_i (i=1,2) l'évènement associé à la fin de traitement des requtes de la i-ième séquence .

D'après 4.2.1.3, les évènements a_i s'écrivent:

$$a_1 = \frac{1}{1 - R^2} \qquad a_2 = \frac{R}{1 - R^4} \qquad (1)$$

Les temps de traitements spécifiés donnent:

$$f_1 = R^7 e_1 \qquad f_2 = R^5 e_2 \qquad (2)$$

Chaque requête doit être prise en compte dés son arrivée:

$$e_1 = a_1 \qquad e_2 = a_2 \qquad (3)$$

Ecrivons maintenant que le nombre de processeurs actifs à chaque instant est inférieur à n . Ce nombre, à l'instant t_0 est

$$\mu e_1(t) + \mu e_2(t) - \mu f_1(t) - \mu f_2(t)$$

c'est à dire qu'il est toujours égal au compteur du pseudo-évènement $e_1 + e_2 - f_1 - f_2$. On écrit:

$$e_1 + e_2 - f_1 - f_2 \leq n \qquad (4)$$

La résolution des équations (2) et (3), à l'aide des équations (1), et le remplacement dans (4) par les expressions trouvées, donnent:

$$\frac{1}{1 - R^2} + \frac{R}{1 - R^4} - \frac{R^7}{1 - R^2} - \frac{R^6}{1 - R^4} \leq n$$

Soit x le pseudo-évènement constituant le membre gauche de cette inégalité. Il nous faut chercher la valeur maximum de sa fonction compteur μx . En réduisant les fractions au même dénominateur, on obtient:

$$x = \frac{1 + R^2}{1 - R^4} + \frac{R}{1 - R^4} - \frac{R^7(1 + R^2)}{1 - R^4} - \frac{R^6}{1 - R^4}$$

$$= \frac{1 + R + R^2 - R^6 - R^7 - R^9}{1 - R^4}$$

Effectuons les premières étapes de la division Euclidienne :

$$x = 1 + \frac{R + R^2 + R^4 - R^6 - R^7 - R^9}{1 - R^4}$$

$$= 1 + R + \frac{R^2 + R^4 + R^5 - R^6 - R^7 - R^9}{1 - R^4}$$

$$= 1 + R + R^2 + \frac{R^4 + R^5 - R^7 - R^9}{1 - R^4}$$

$$= 1 + R + R^2 + R^4 + \frac{R^5 - R^7 + R^8 - R^9}{1 - R^4}$$

$$= 1 + R + R^2 + R^4 + R^5 + \frac{-R^7 + R^8}{1 - R^4}$$

On a donc écrit x sous la forme e + y, où $e = 1 + R + R^2 + R^4 + R^5$ est un évènement à 5 occurrences, et $y = (-R^7 + R^8)/(1 - R^4)$ est un pseudo évènement négatif, puisque c'est le pseudo-évènement $-R^7 + R^8$ répété à la période 4 (cf. figure 6.a). On obtient donc $x < 5$, et 5 processeurs suffisent. On a de plus construit la "fonction de charge", μx, du système, et la figure 6.b montre qu'après une phase d'initialisation, le système a un fonctionnement périodique, tel qu'il existe un processeur inactif une unité de temps sur quatre.

4.4. INEGALITES DE PSEUDO-EVENEMENTS

Notre calcul est ainsi assez puissant pour résoudre toute équation linéaire . Cependant, la description des systèmes à l'aide de ce calcul fait un large usage des inéquations, qui permettent l'expression de phénomènes asynchrones. Nous allons donc maintenant explorer les propriétés des opérateurs algébriques par rapport à la relation d'ordre sur les pseudo-évènements.

4.4.1. Inégalités et somme

Proposition: La somme préserve l'ordre dans A, c'est à dire que:

$$\forall a,b,c \in A,\ a > b \Rightarrow a + c > b + c$$

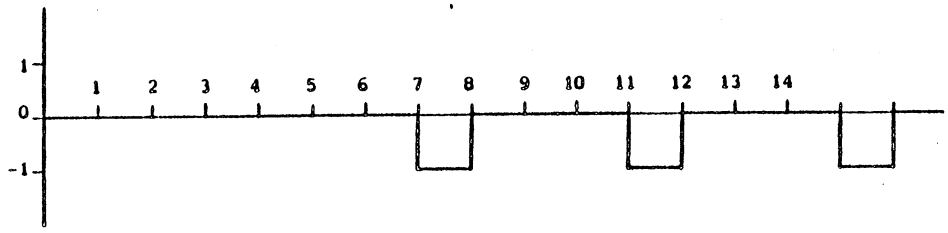


Figure 6.a
Fonction compteur de $y = (-R^7 + R^8) / (1 - R^4)$

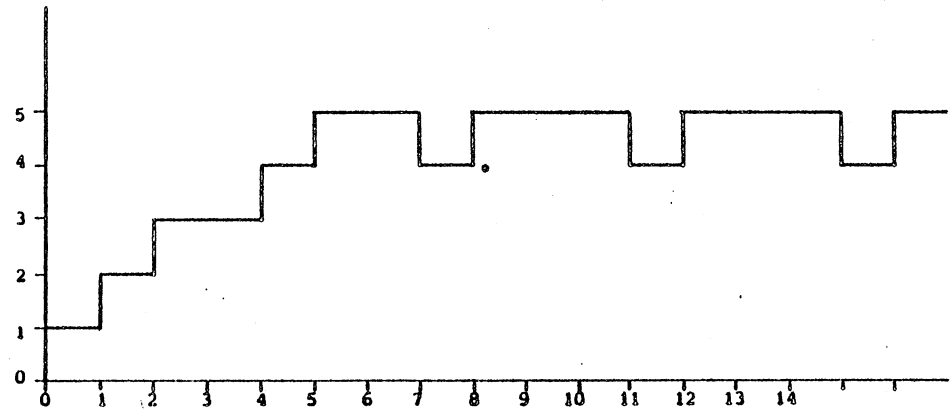


Figure 6.b
Fonction de charge du système

4.4.2. Inégalités et produit

La plupart des études concernant les anneaux ordonnés (par exemple [Zimmermann]) prennent comme hypothèse la monotonie du produit positif (la preuve en est qu'en mathématique, on appelle souvent opérateur positif un opérateur qui préserve l'ordre), c'est à dire que:

$$a \geq b \;\&\; c \geq 0 \;\Rightarrow\; a.c \geq b.c$$

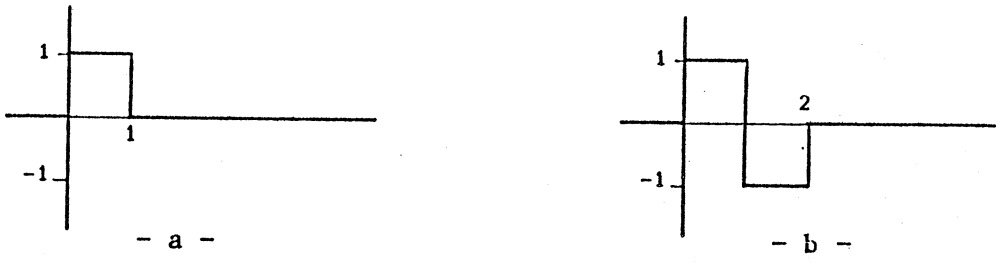


Figure 7
Compteurs de $1 - R$ et de $(1 - R)^2 = 1 - 2R + R^2$

Cette hypothèse n'est pas vérifiée dans A : Par exemple 1-R est positif (figure 7.a), mais son carré $(1 - R)^2 = 1 - 2R + R^2$ n'est pas comparable à 0 (figure 7.b) .

Dans l'étude d'un anneau ou d'un corps ordonné F, dans lequel le produit positif ne préserve pas l'ordre, trois ensembles, et leurs duaux, sont intéressants à caractériser:

$$Mon(F) = \{ a \in F \mid \forall x \geq 0 , ax \geq 0 \}$$

$$F^+ = \{ a \in F \mid a \geq 0 \}$$

$$\tilde{F}^+ = \{ a \in F \mid \exists x > 0 \text{ tel que } ax \geq 0 \}$$

Par exemple, si l'on ordonne le corps $\mathbb{C}$ des complexes comme suit :

$$a + ib \leq a' + ib' \iff a \leq a' \ \& \ b \leq b'$$

on a :

$$Mon(\mathbb{C}) = \mathbb{R}^+$$
$$\mathbb{C}^+ = \{ a + ib \mid a \in \mathbb{R}^+, b \in \mathbb{R}^+ \}$$
$$\tilde{\mathbb{C}}^+ = \{ a + ib \mid a \in \mathbb{R}^+ \}$$

Lorsque $0 \leq 1$ et que la somme préserve l'ordre dans F, on a :

. $Mon(F) \subset F^+ \subset \tilde{F}^+$

. Mon(F) est stable par somme et produit

. F^+ est stable par somme

. F^+ et $\tilde{F}^+$ sont stables par produit par un élément de Mon(F)

4.4.2.1. Proposition : $Mon(A) = E$

Démonstration : $E \subset Mon(A)$ résulte du fait que la somme et l'opérateur de délai R^Δ préservent l'ordre dans A. Réciproquement, montrons que si $x \in A - E$, il existe $\varepsilon > 0$ tel que $x(1-R^\varepsilon)$ n'est pas positif. Puisque $1 - R^\varepsilon$ est positif, cela impliquera que le produit par x ne préserve pas l'ordre. Si $x \in A - E$, il existe $n \in \mathbb{N}^*$ tel que $\underline{x}_n < 0$. Choisissons alors ε tel que $0 < \varepsilon < x_{n+1} - x_n$ (ou tel que $\varepsilon > 0$, si $n = \#x$). Alors $\mu x(x_n + \varepsilon) = \mu x(x_n) + \underline{x}_n$ et si $y = x(1 - R^\varepsilon)$, $\mu y(x_n + \varepsilon) = \mu x(x_n + \varepsilon) - \mu x(x_n) = \underline{x}_n < 0$. Donc $x(1 - R^\varepsilon)$ n'est pas positif .

4.4.2.2. Exemple : Considérons les deux inégalités suivantes, portant sur un évènement x :

$$(1) \quad x(1 - R^\Delta) \leq 1$$

$$(2) \quad x \leq \frac{1}{1 - R^\Delta}$$

La première signifie que deux occurrences successives de x sont séparées par un délai supérieur à Δ (cf. §2.2.7.3) . Si $\Delta > 0$, $1/(1 - R^\Delta)$ est un évènement (cf. §4.2.1.2) et l'on peut en multiplier les deux membres de l'inéquation (1), qui implique donc (2). Par contre l'implication inverse est fausse, parceque $1 - R^\Delta$ n'est pas un évènement. La figure 8 montre le compteur d'un évènement satisfaisant (2) mais non pas (1).

4.4.2.3. Proposition: $\tilde{A}^+ = \{0\} \cup \{ x \in A \mid \underline{x}_1 > 0 \}$

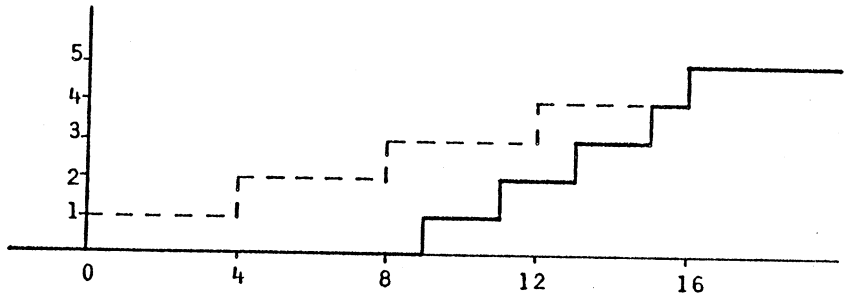


Figure 8

$x \leq 1/(1-R^4)$ mais $x(1-R^4) < 1$

Démonstration : Si $x \in \tilde{A}^+$, il existe $y > 0$ tel que $xy > 0$. Soit $z = xy$. Si $z=0$ alors $x=0$ d'après l'integrité de A . Sinon $\bar{z}_1 = \bar{x}_1 \bar{y}_1$, avec $\bar{z}_1 > 0$ et $\bar{y}_1 > 0$, donc $\bar{x}_1 > 0$. Inversement, si $\bar{x}_1 > 0$ alors il existe un délai Δ et deux évènements e et f tels que $x = R^{\Delta}(e - f)$, avec $e_1 = 0$ et $f_1 > 0$. Donc $1/(1 - f)$ est strictement positif (c'est, en fait, un évènement non nul, d'après 4.2.1.2) et $x/(1 - f) = R^{\Delta}(e - 1)/(1 - f) + R^{\Delta}$ est positif (c'est un évènement). Donc $x \in \tilde{A}^+$.

On a démontré en fait un résultat plus fort, qui est :

$$\bar{x}_1 > 0 \iff \exists e \in E \text{ tel que } ex \in E$$

En résumé, le fait que le produit positif ne préserve pas l'ordre constitue un lourd handicap pour traiter les inéquations. Néammoins, nous avons montré que le produit par un évènement préserve l'ordre, et que tout pseudo-évènement peut être transformé, par produit par un évènement, soit en évènement, soit en l'opposé d'un évènement. Ces résultats sont précieux, mais il ne faut pas perdre de vue que le produit d'une inéquation par un évènement peut affaiblir considérablement la contrainte initiale, comme l'a montré l'exemple 4.4.2.2.

4.5. TEMPS DISCRET

Dans ce paragraphe, nous allons explorer les propriétés particulières de $A(\mathbb{Z})$. La plus importante concerne la caractérisation des évènements à l'aide de leurs dérivées discrètes.

4.5.1. Dérivée discrète

Si $a \in A(\mathbb{Z})$, nous appellerons dérivée discrète de a, le pseudo-évènement $a(1-R)$. Cette appellation est motivée par la proposition suivante - évidente, mais très utile - qui correspond à la propriété caractéristique des fonctions réelles dérivables croissantes, qui est que leur dérivée est positive.

Proposition : Un pseudo-évènement $a \in A(\mathbb{Z})$ est un évènement si et seulement si sa dérivée $a(1-R)$ est positive.

Démonstration : $a \in E(\mathbb{Z})$ si et seulement si, pour tout $n \in \mathbb{Z}$, $\mu a(n) \geq \mu a(n-1)$. Puisque $\mu(a(1-R)) = \lambda n.\mu a(n) - \mu a(n-1)$, le résultat s'ensuit.

Il y a donc symétrie complète entre les problèmes liés à l'ordre dans $A(\mathbb{Z})$ et les problèmes de caractérisation des évènements, puisque :

$$A^+(\mathbb{Z}) = \{ e(1-R) \mid e \in E(\mathbb{Z}) \}$$

et

$$E(\mathbb{Z}) = \{ a/(1-R) \mid a \in A^+(\mathbb{Z}) \}$$

4.5.2. Conditions et filtrage

La proposition 4.5.1. nous permet d'exprimer algébriquement un ensemble d'opérateurs, de relations et de propriétés que nous avions définis au chapitre 2. On se limitera parfois, dans ce paragraphe, au sous ensemble $A(\mathbb{N})$ de $A(\mathbb{Z})$.

4.5.2.1. Relation de sous-suite : Si $e,f \in E(\mathbb{Z})$, alors

$$e \sqsubseteq f \iff e(1-R) \lessdot f(1-R)$$

Démonstration: D'après 2.2.7.1, $e \sqsubseteq f \iff f-e \in E$. Donc $e \sqsubseteq f \iff (f-e)(1-R) \gtrdot 0$.

4.5.2.2. Evènements à occurrences simples : $e \in E(\mathbb{N})$ est à occurrences simples si et seulement si $e(1-R) \lessdot 1$.

Démonstration : $e \in E(\mathbb{N})$ est à occurrences simples si et seulement si $e \sqsubseteq 1/(1-R)$.

4.5.2.3. Conditions : On appellera condition un pseudo-évènement $c \in A(\mathbb{N})$ tel que $0 \lessdot c \lessdot 1$ (Notons que le compteur d'une telle condition est toujours nul aux instants négatifs) .

Les opérateurs booléens s'expriment dans l'algèbre :

$$c \wedge c' = \inf(c,c')$$
$$c \vee c' = \sup(c,c')$$
$$\neg c = 1 - c$$

Notons que si $\Delta > 0$, $R^{\Delta} \neg c = \neg R^{\Delta} c + \inf(c,1-R^{\Delta}) - \inf(1-c,1-R^{\Delta})$.

Si c est une condition, il existe $c\uparrow$ et $c\downarrow \in E(\mathbb{N})$ tels que

- $c = c\uparrow - c\downarrow$
- $c\uparrow \gtrdot c\downarrow \gtrdot c\uparrow - 1$
- $\inf(c\uparrow(1-R) , c\downarrow(1-R)) = 0$

(La dernière équation exprime que $c\uparrow$ et $c\downarrow$ n'ont pas d'occurrences simultanées) .

4.5.2.4. Filtrage : Si c est une condition et si $e \in E(\mathbb{N})$ est à occurrences simples, alors :

$$e \mid c = \frac{\inf_{\cdot}\ (\ e(1-R)\ ,\ Rc\ )}{1 - R}$$

$$e \mid c^{+} = \frac{\inf\ (\ e(1-R)\ ,\ c\ )}{1 - R}$$

CHAPITRE 5

PUISSANCE D'EXPRESSION ET APPLICATIONS DU CALCUL

Afin d'illustrer la puissance d'expression de notre calcul formel, nous allons montrer maintenant comment les descriptions exprimées au moyen de divers modèles classiques peuvent être systématiquement traduites dans le calcul. En plus de son caractère illustratif, cette traduction présente un intéret pratique pour la formalisation initiale des problèmes. En effet, contrairement au formalisme de spécification présenté dans la première partie, le calcul formel ne prétend pas être un outil naturel de description, et l'exemple présenté au §4.3 montre que la formalisation algébrique est loin d'être évidente. C'est pourquoi il est intéressant de pouvoir la déduire d'une description dans un autre formalisme, plus intuitif, qui peut être le formalisme de spécification présenté au chapitre 2, ou un formalisme plus algorithmique comme, par exemple, un modèle dérivé des réseaux de Pétri.

Nous étudierons successivement une hiérarchie de modèles "asynchrones", c'est à dire sans notion quantitative de temps - qui sont les automates rationnels, les réseaux de Pétri ordinaires et avec test à zéro - et un modèle synchrone, les réseaux de Pétri temporisés.

Nous illustrerons également, à la fin de ce chapitre, l'usage du calcul à la formalisation et à l'analyse de quelques problèmes.

5.1. SUITES DE SYMBOLES

Soit $Q = \{ q_1 , \dots , q_k \}$ un ensemble fini. L'ensemble Q^ω des suites infinies d'éléments de Q est l'ensemble des applications de $\mathbb{N}$ dans Q . L'ensemble Q^* des suites finies d'éléments de Q est l'ensemble des fonction σ de $\mathbb{N}$ dans Q, dont le domaine de définition est un intervalle $[0, |\sigma|[$ de $\mathbb{N}$, avec $|\sigma| \in \mathbb{N}$. L'ensemble des suites d'éléments de Q est l'ensemble $Q^\infty = Q^* \cup Q^\omega$.

Nous décrirons les suites en termes d'évènements, en associant à toute suite σ et à tout élément q de Q un évènement qui est la suite des rangs de l'élément q dans σ .

Proposition : Soient

$$\Xi^\omega(Q) = \{ (\hat{q}_i)_{i=1..k} \in E(\mathbb{N})^k \mid \Sigma_{i=1}^{k} \hat{q}_i = \frac{1}{1-R} \}$$

$$\Xi^\infty(Q) = \{ (\hat{q}_i)_{i=1..k} \in E(\mathbb{N})^k \mid \Sigma_{i=1}^{k} \hat{q}_i (1-R)^2 \leq 1-R \}$$

Alors Q^ω et $\Xi^\omega(Q)$ d'une part, et Q^∞ et $\Xi^\infty(Q)$ d'autre part, sont en bijection par l'application $\xi = \lambda\sigma. (\hat{q}_i(\sigma))_{i=1..k}$ telle que

$$\forall i=1\dots k,\ \hat{q}_i(\sigma) = \Sigma_{n>0}\ Q_n^{(i)}\ R^n$$

où $Q_n^{(i)}$ = si $\sigma(n)$ est défini et $\sigma(n) = q_i$ alors 1 sinon 0

Démonstration : Il est clair que ξ est injective . La "condition de suite" $\Sigma\ \hat{q}_i(1-R)^2 \leq 1-R$ exprime que l'évènement $\Sigma\ \hat{q}_i$ est à occurrences simples et que la suite de ses dates d'occurrences est un intervalle $[0, |\sigma|[$ ($|\sigma| \in \bar{\mathbb{N}}$) de $\mathbb{N}$. En effet, ceci revient à dire qu'il existe un évènement f ("fin de suite") tel que $\Sigma\ \hat{q}_i + f/(1-R) = 1/(1-R)$. Ecrivons que f est un évènement, on obtient la condition de suite :

$$f(1-R) = (1-R) - \Sigma\ \hat{q}_i(1-R)^2 \geq 0$$

Il s'ensuit que $\xi(Q^{\infty}) = \Xi^{\infty}(Q)$ et, en posant $f = 0$, que $\xi(Q^{\omega}) = \Xi^{\omega}(Q)$.

Cette caractérisation des suites de symboles en termes de k-uples d'évènements va nous permettre de décrire les systèmes asynchrones, en considérant ceux-ci comme définissant leur propre horloge : La suite des occurrences d'évènements survenant au cours d'un fonctionnement d'un tel système constitue la base de temps par rapport à laquelle ce fonctionnement est décrit. On dira, abusivement, qu'un évènement survient à l'"instant" n, si l'une de ses occurrences est la n-ième dans cette suite des occurrences de tous les évènements du système. En conséquence, les évènements considérés apprtiennent à $E(\mathbb{N})$, et nous pourrons tirer pleinement parti des résultats du §4.5 .

5.2. AUTOMATES RATIONNELS

5.2.1. Définition :

Un automate rationnel M est un quadruplet (V,Q,v,q_0), où

- V est un vocabulaire fini
- Q est un ensemble fini d'états
- v est une fonction de $Q \times Q$ dans V
- $q_0 \in Q$ est l'état initial

Un comportement d'un tel automate est une suite c de V^{∞}, telle qu'il existe une suite σ de $(Q \times Q)^{\infty}$ telle que

1) $|\sigma| = |c|$ $(\in \overline{\mathbb{N}})$
2) $\sigma(0) = (q_0, q)$ pour un certain $q \in Q$
3) $\forall n < |\sigma|$, $\sigma(n) \in Def(v)$
4) $\forall n < |\sigma|$, $v(\sigma(n)) = c(n)$
5) si $|\sigma| = n \in \mathbb{N}$, alors $\sigma(n) = (q_n , q_{n+1})$ et $\forall q \in Q$, $(q_{n+1} , q) \notin Def(v)$

5.2.2. Langage des arcs

Avant de décrire l'ensemble L(M) des suites c satisfaisant la définition précédente, nous décrirons l'ensemble S(M) des suites σ satisfaisant les hypothèses (2), (3) et (5) .

Pour cela, on associe à tout couple d'états (q_i, q_j) appartenant à Def(v), un évènement e_{ij} de E(IN). Ces évènements sont en nombre fini. Pour tout état $q \in Q$, notons $q^{\cdot}$ (resp. $^{\cdot}q$) l'ensemble des états q' tels que (q,q') (resp. (q',q)) appartient à Def(v).

Alors, en remarquant - très informellement - que l'automate M quitte l'état q à l'"instant" n si et seulement si il l'a atteint à l'"instant" n-1 et $q^{\cdot} \neq \emptyset$, on peut écrire :

$\forall q_i$ tel que $q_i^{\cdot} \neq \emptyset$,

(S1) $$\sum_{q_j \in q_i^{\cdot}} e_{ij} = R \sum_{q_k \in {}^{\cdot}q_i} e_{ki} + \delta_{i0}$$

où δ_{i0} = si i=0 alors 1 sinon 0

On obtient ainsi un système d'équations linéaires qui caractérise l'ensemble $\xi(S(M)) = \{ \xi(\sigma) \mid \sigma \in S(v,q_0) \}$.

5.2.3. Langage Rationnel

Nous sommes alors en mesure de caractériser le langage L(M) reconnu par l'automate M, c'est à dire l'ensemble des suites c satisfaisant la définition 5.1.2.1 . Associons à tout symbole $a \in V$ un évènement $e_a \in E(IN)$. Alors :

$$(e_a \mid a \in V) \in \xi(L(M)) \iff \exists\, (e_{ij})_{i,j} \in \xi(S(M)) \text{ tel que}$$

(S2) $$\forall a \in V \ , \quad e_a = \sum_{v(q_i,q_j) = a} e_{ij}$$

On sait donc caractériser $\xi(L(M))$ comme projection sur $\{ e_a \mid a \in V \}$ du domaine défini par (S1) et (S2), c'est à dire par un système de Card(Q)+Card(V) équations linéaires à Card(Def(v))+Card(V) variables. Cette projection peut être effectuée, à l'aide de la proposition 4.5.1 , jusqu'à concurrence de l'élimination de Card(Q)+Card(V) variables. Donc si Card(Q)+Card(V) $\geq$ Card(Def(v)), $\xi(L(M))$ peut être caractérisé par un système d'inéquations sans variables auxiliaires.

Exemple

Considérons l'automate M, dont le graphe est représenté par la figure 9 . Le langage des arcs est caractérisé par le système d'équations suivant :

$$e_{01} + e_{03} = R\, e_{40} + 1$$

$$e_{12} = R\, e_{01}$$

$$e_{34} = R\, e_{03}$$

$$e_{40} = R\, e_{34}$$

Le langage reconnu est caractérisé en adjoignant à ce système les équations suivantes :

$$e_a = e_{01} + e_{03}$$

$$e_b = e_{12} + e_{40}$$

$$e_c = e_{34}$$

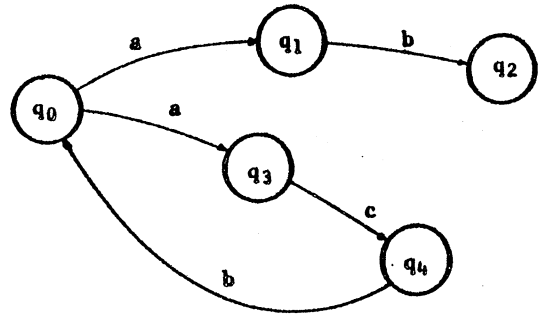


Figure 9: Automate M

Eliminons les variables auxiliaires e_{ij} : On a

$$e_{34} = e_c \quad , \quad e_{40} = R\, e_c \quad , \quad e_{03} = R^{-1} e_c$$

$$e_{01} = R^2 e_c - R^{-1} e_c + 1 \quad , \quad e_{12} = R^3 e_c - e_c + R$$

et

$$e_a = R^2 e_c - R^{-1} e_c + 1 + R^{-1} e_c$$

$$e_b = R^3 e_c - e_c + R + R\, e_c$$

On écrit que e_{12} est un évènement ($e_c \in E$ et $e_{12} \in E$ impliquent e_a, e_b et $e_{ij} \in E$, $\forall i,j$) :

$$R(1 - R) \geq e_c(1 - R^3)(1 - R)$$

Donc $\xi(L(M)) = \{ (e_a, e_b, e_c) \in E(\mathbb{N})^3$ tels que

$$e_c(1 - R^3)(1 - R) \leq R(1 - R)$$

$$e_a = R^2 e_c + 1$$

$$e_b = R - e_c(1 - R - R^3) \}$$

5.2.4. Comportements potentiels

Ce paragraphe constitue une approche du problème de l'équivalence observationnelle entre automates.

Dans l'introduction de son ouvrage sur CCS [Milner 80], R. Milner remarque que l'équivalence classique entre automates - deux automates sont équivalents s'ils reconnaissent le même langage - n'est pas assez fine pour prendre en compte certaines propriétés, notamment les propriétés de vivacité des systèmes d'automates communiquants . A titre d'exemple, il donne les automates M et M' représentés, respectivement, par les figures 9 et 10, qui reconnaissent tous deux le langage $(acb)^*ab$. Cependant, l'automate M' peut toujours accepter le symbole c après avoir accepté a, ce qui n'est pas le cas de l'automate M . Il s'ensuit que, dans la philosophie de CCS, l'automate M peut être bloqué dans un certain environnement, alors que M' ne l'est pas. Ceci nous amène à essayer

de décrire plus finement le comportement d'un automate, en exprimant, à chaque étape, l'ensemble des symboles acceptables (et non plus, simplement, acceptés) par l'automate. Pour cela on caractérise un ensemble P(M) de vecteurs $(f_a \mid a \in V)$ d'évènements, chacun de ces vecteurs étant interprété de la manière suivante :

$(f_a \mid a \in V)$ est un fonctionnement potentiel de l'automate s'il existe une suite σ, satisfaisant aux conditions (2), (3) et (5) de la définition 5.1.2.1 , telle que f_a a une occurrence à l'instant n si et seulement si le symbole a est acceptable à partir du n-ième état atteint par l'automate dans σ .

La caractérisation de P(M) s'obtient encore à partir de S(M) :

$$(f_a)_{a \in V} \in P(M) \iff$$

$$\exists (e_{ij})_{i,j} \in S(M) \text{ tel que } \forall a \in V \ , \ f_a = \sum_{q_i \in {}^{\circ}a} e_{ij}$$

$$\text{où } {}^{\circ}a = \{ q_i \in Q \mid \exists\, q_j \in Q \text{ tel que } v(q_i, q_j) = a \}$$

Reprenons l'exemple des automates M et M' des figures 9 et 10 . Pour M on obtient :

$$f_a = e_a \ , \ f_b = e_b \ , \ f_c = e_c \ , \text{ soit } P(M) = L(M)$$

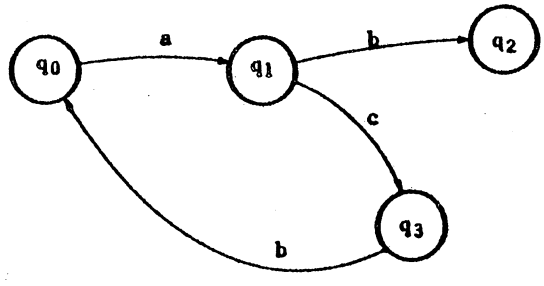


Figure 10 : Automate M'

P(M') est caractérisé par le système :

$$\left.\begin{aligned} e_{01} &= Re_{30} + 1 \\ e_{12} + e_{13} &= Re_{01} \\ e_{30} &= Re_{13} \end{aligned}\right\} \quad S(M')$$

$$f_a = e_{01}$$

$$f_b = e_{12} + e_{13} + e_{30}$$

$$f_c = e_{12} + e_{13}$$

Soit, après projection :

$(f_a, f_b, f_c) \in P(M')$ si et seulement si

$$f_a(1 - R) \geq 1 - R \geq f_a(1 - R)(1 - R^3)$$
$$Rf_b = f_a(1 + R^2) - 1$$
$$f_c = Rf_a$$

La différence entre P(M) et P(M') est évidente. Par exemple, dans P(M') on a $f_c(1-R) \geq R(1-R)$, contrainte à laquelle P(M) n'est pas soumis.

5.3. RESEAUX DE PETRI ET EXTENSIONS

Nous allons considérer maintenant un ensemble de modèles dérivés des réseaux de Pétri (RdP). En ce qui concerne les réseaux non temporisés, le principal résultat est l'expression du comportement des réseaux avec test à zéro (RdPZ), établissant, d'après [Agerwala], que notre calcul a la puissance de la Machine de Turing . Diverses extensions temporisées des réseaux de Pétri ont été proposées [Ramchandani], [Moalla, Pulou & Sifakis], [Chretienne], [Merlin], qui présentent entre elles des différences sensibles. Nous étudierons deux interprétations d'un même formalisme :

- Une interprétation asynchrone (RPT· [Chretienne]), dont nous proposerons une extension, les réseaux temporisés à contraintes (RPTC), dont la puissance d'expression est exactement la classe des systèmes caractérisables au moyen de systèmes finis d'inéquations linéaires en évènements .

- Une interprétation synchrone (RPTS [Moalla, Pulou & Sifakis]), qui consiste à n'admettre que les fonctionnements à vitesse maximale de l'interprétation asynchrone .

Nous n'étudierons pas ces modèles dans l'ordre, logique, où nous venons de les citer, mais dans un ordre susceptible de faciliter l'exposé des règles de traduction vers le calcul en évènements.

On peut voir le comportement d'un réseau de Pétri de deux points de vue : Celui des séquences de tirs et celui des séquences de marquages. Cependant, le premier point de vûe est plus riche que le second, puisque la séquence des marquages atteints se déduit de la séquence des transitions mises à feu. C'est pourquoi nous décrirons les séquences de mises à feu :

Soit $\sigma \in T^{\infty}$ une telle séquence (T étant l'ensemble des transitions du réseau). Nous la décrirons en associant à chaque transition x de T, un évènement $\hat{x}$ qui survient chaque fois que x est mise à feu dans σ . Dans le cas des modéles temporisés, la date de la n-ième occurrence de $\hat{x}$ sera effectivement une date, alors que, dans un contexte non temporisé, ce sera le rang de la n-ième apparition de la transition x dans la séquence σ .

La définition, classique [Peterson], des réseaux de Pétri, en termes de places, de transitions et de marques, est supposée connue. Nous nous bornerons à fixer quelques notations et à rappeler la définition matricielle des RdP.

Soient $P = \{ p_1, p_2, \ldots, p_m \}$ et $T = \{ x_1, x_2, \ldots, x_n \}$ les ensembles des places et des transitions d'un graphe de Pétri (graphe biparti). Un tel graphe pourra être caractérisé :

- soit par ses fonctions d'incidence : On notera
  - $\dot{p_i}$ (resp. $\dot{p_i}$) l'ensemble des transitions de sortie (resp. d'entrée) de la place p_i .
  - $\dot{x_j}$ (resp. $\dot{x_j}$) l'ensemble des places vidées (resp. remplies) par la transition x_j .

- soit par ses matrices d'incidences C^+ et C^- , matrices m×n dont les éléments appartiennent à l'ensemble {0,1} (à $\mathbb{N}$ dans le cas des réseaux généralisés), et telles que :

$$C^+_{ij} = \text{si } p_i \in \dot{x_j} \text{ alors 1 sinon 0}$$

$$C^-_{ij} = \text{si } x_j \in \dot{p_i} \text{ alors 1 sinon 0}$$

(Dans le cas des réseaux généralisés C^+_{ij} - resp. C^-_{ij} - est le poids de l'arc (p_i,x_j) - resp. (x_i,p_j))

L'ensemble des marquages du réseau est l'ensemble $\mathbb{N}^m$. Pour tout entier $j \in \{1..n\}$, la relation $\overset{j}{\rightarrow}$ (appelée "mise à feu de la j-ième transition") est définie sur $\mathbb{N}^m$ comme suit:

$$M_1 \overset{j}{\rightarrow} M_2 \iff M_1 - C^- I_j \geq 0 \text{ et } M_2 = M_1 + (C^+ - C^-)\, I_j$$

où les vecteurs sont ordonnés composante par composante, et où I_j est le j-ième vecteur de base de $\mathbb{R}^n$. Soit $\rightarrow$ l'union de ces n relations. Un comportement du réseau à partir du marquage M_0 est alors un chemin d'origine M_0 dans le graphe de la relation $\rightarrow$.

Un vecteur X de $\mathbb{N}^n$ est un vecteur de tir du réseau si et seulement si il existe un comportement fini

$$M_0 \overset{j_1}{\rightarrow} M_1 \overset{j_2}{\rightarrow} \cdots \overset{j_s}{\rightarrow} M_s$$

tel que :

$$\forall j = 1...n, \quad X_j = \text{Card} \{ k = 1..s \mid j_k = j \}$$

On montre aisément que, si X est un vecteur de tir, alors

$$M_s = M_0 + (C^+ - C^-) X \geq 0$$

On trouvera dans [Caspi & Halbwachs 84] une démonstration du résultat suivant, dont nous aurons besoin par la suite, et qui donne une condition nécéssaire et suffisante pour que l'implication inverse soit vraie:

Si (C^+, C^-) définit un (multi-)graphe biparti G sans circuit, alors, pout tout M_0 dans $\mathbb{N}^m$, tout vecteur X de $\mathbb{N}^n$ tel que

$$M_0 + (C^+ - C^-) X \geq 0$$

est un vecteur de tir du réseau de Pétri (G,M_0) . .

5.3.1. Réseaux de Pétri temporisés asynchrones

Nous commencerons par étudier l'interprétation asynchrone des réseaux de Pétri temporisés (RPT [Chretienne]) . Nous en déduirons une caractérisation de leur comportement à vitesse maximale, qui constitue l'interprétation synchrone (RPTS) de [Moalla, Pulou & Sifakis], et dont les réseaux ordinaires peuvent être vus comme un cas particulier.

5.3.1.1. Définition : Un réseau de Pétri temporisé est un réseau de Pétri à chaque place p_i duquel est affecté un délai $\Delta_i \in \mathbb{R}^+$. On suppose de plus que cette affectation est faite de telle sorte que le graphe obtenu en éliminant du graphe initial toutes les places de délai non nul, est sans circuit (absence de boucle de durée nulle).

La temporisation d'un réseau de Pétri consiste à associer à chaque mise à feu d'une transition une date, de telle sorte que si une marque, versée dans une place p_i par la mise à feu d'une transition de date t, participe à la mise à feu d'une nouvelle transition de date t', alors $t' > t+\Delta_i$. Plus précisément :

i) Si une marque atteint une place p_i à l'instant t, elle devient indisponible jusqu'à l'instant $t+\Delta_i$. Initialement toutes les marques sont disponibles.

ii) Une transition n'est validée que si toutes ses places d'entrées contiennent au moins une marque disponible.

D'un point de vue matriciel, un comportement du RPT est une fonction $\tilde{M}$ de $\mathbb{R}^+$ (ensemble des instants) dans $\mathbb{N}^m$ (ensemble des marquages), inductivement définie comme suit :

. $\tilde{M}(0) = M_0$

. L'ensemble des points de discontinuité de $\tilde{M}$ est un ensemble discret $T = \{t_1, t_2, \ldots, t_k, \ldots\}$.

. Si l'on note $\tilde{C}^+$ La matrice obtenue à partir de C^+ en annulant toutes les lignes d'indice i tel que $\Delta_i > 0$, alors, pour tout k tel que $0 < k < \text{Card}(T)$, il existe un vecteur de tir X(k) du réseau de Pétri (non temporisé) $((\tilde{C}^+, C^-), \tilde{M}(t_k))$, tel que pour tout t dans $\mathbb{R}^{*+}$, pour tout i = 1...m :

$$\tilde{M}(t)_i = (M_0)_i + \Big[C^+ \sum_{t_k \leq t-\Delta_i} X(k) - C^- \sum_{t_k < t} X(k) \Big]_i$$

$t_k < t$

$\tilde{M}$ est appelé marquage disponible. Le marquage total M est défini par:

$$M(t) = M_0 + (C^+ - C^-) \sum_{t_k < t} X(k)$$

5.3.1.2. Système d'inéquations linéaires associé à un RPT : Nous allons montrer comment l'ensemble des comportements d'un réseau de Pétri temporisé peut être caractérisé par un système d'inéquations linéaires en

évènements. Pour cela, nous associons à chaque transition x_i du réseau, un évènement $\hat{x}_i$ qui survient chaque fois que la transition x_i est mise à feu : Un comportement du RPT sera donc modélisé par un vecteur d'évènements $\hat{X} \in E^n$.

Théorème : Une condition nécessaire et suffisante pour que $\hat{X} \in E^n$ soit un comportement du RPT (C^+, C^-, M_0, Δ) est que:

$$M_0 + [R^{\Delta}]C^+\hat{X} \geq C^-\hat{X} \qquad (1)$$

où $[R^{\Delta}]$ est la matrice diagonale m×m, telle que $[R^{\Delta}]_{ii} = R^{\Delta_i}$ (i=1...m).

Démonstration: D'après la définition matricielle du comportement des RPT, une suite $(t_k, X(k))$ d'instants et de vecteurs de $\mathbb{N}^n$ définit un comportement du RPT (C^+,C^-,M_0,Δ) si et seulement si, pour tout k, X(k) est un vecteur de tir du réseau de Pétri $(C^+,C^-,M(t_k))$, où:

$$\tilde{M}(t_k)_i = (M_0)_i + \Big[C^+ \sum_{\substack{t_\ell < t_k - \Delta_i \\ t_\ell < t_k}} X(\ell) - C^- \sum_{t_\ell < t_k} X(\ell) \Big]_i$$

Or, puisque le graphe $(\tilde{C}^+,\tilde{C}^-)$ est sans circuit, ceci est équivalent à:

$$\tilde{M}(t_k) + (\tilde{C}^+ - \tilde{C}^-)X(k) \geq 0$$

En reportant dans cette inéquation l'expression de $\tilde{M}(t_k)$ on obtient:

$$(M_0)_i + \Big[C^+ \sum_{t_\ell < t_k - \Delta_i} X(\ell) - C^- \sum_{t_\ell < t_k} X(\ell)\Big]_i \geq 0 \ , \ i = 1..m \quad (2)$$

Soit maintenant le vecteur $\hat{X} = \Sigma_k X(k) R^{t_k}$. La fonction compteur (vectorielle) de $\hat{X}$ s'écrit :

$$\mu^{+}_{\hat{X}}(t) = \sum_{t_k < t} X(k)$$

Donc l'inéquation (2) s'écrit :

$$(M_0)_i + [C^{+}\mu^{+}_{\hat{X}}(t_k - \Delta_i) - C^{-}\mu^{+}_{\hat{X}}(t_k)]_i \geq 0 \quad (i=1\ldots m)$$

Soit :

$$(M_0)_i + [C^{+}R^{\Delta_i}\hat{X} - C^{-}\hat{X}]_i \geq 0 \quad (i=1\ldots m)$$

ou, sous une forme plus condensée:

$$M_0 + [R^{\Delta}]C^{+}\hat{X} \geq C^{-}\hat{X} \qquad (2)$$

Cette inéquation exprime simplement que le nombre de marques retirées d'une place p_i jusqu'à l'instant t est inférieur au nombre de marques initialement contenues dans p_i augmenté du nombre de marques versées dans p_i jusqu'à l'instant $t-\Delta_i$. Dans le cas d'un réseau non généralisé, on obtient le système d'inéquations linéaires suivant :

$$\forall p_i \in P \ , \quad \sum_{x_j \in p_i^{\cdot}} \hat{x}_j \leq (M_0)_i + \sum_{x_j \in {}^{\cdot}p_i} R^{\Delta_i}\hat{x}_j$$

On peut remarquer que l'inéquation matricielle (1) constitue un système d'inéquations linéaires d'un type particulier, puisque les termes constants et les termes retardés y sont astreints à n'apparaitre que dans le plus grand membre. Nous proposons maintenant une extension du modèle RPT correspondant à des systèmes d'inéquations plus généraux .

5.3.2. Réseaux temporisés à contraintes

Les RPT considérés jusqu'ici sont asynchrones: On peut les considérer comme décrivant des contraintes de type causal, qui autorisent un système à évoluer. En ce sens, l'ensemble des comportements d'un RPT n'est jamais vide, puisque le comportement $\hat{X} = 0$ est toujours admissible, rien n'obligeant le réseau à évoluer. Il est clair que l'on augmen-

te les capacités de modélisation des RPT si on les enrichit d'un formalisme de description de contraintes d'obligation.

Pour cela, on peut introduire des contraintes de temps de réponse: Certaines combinaisons linéaires d'évènements du système fournissent des dates limites pour d'autres combinaisons linéaires d'évènements. Ces contraintes peuvent s'écrire:

$$C'^{+}\hat{X} > [R^{\Delta'}]C'^{-}\hat{X}$$

où C'^{+} et C'^{-} sont deux matrices d'incidence $m' \times n$ d'entiers naturels, et Δ' est un m'-vecteur de réels positifs. Remarquons cependant que $\hat{X} = 0$ est encore une solution du système d'inéquations, puisque les nouvelles contraintes ne s'exercent éventuellement qu'après la première mise à feu de certaines transitions.

Pour contraindre le système à commencer ses évolutions, il faut imposer des dates limites aux occurrences initiales de certaines combinaisons linéaires d'évènements. La forme générale d'un système de contraintes d'obligation sera donc:

$$C'^{+}\hat{X} > [R^{\Delta'}](C'^{-}\hat{X} + M'_0)$$

où M'_0 est un m'-vecteur d'entiers naturels.

5.3.2.1. Définition : Un réseau de Pétri temporisé à contraintes (RPTC) est un couple $\{(C^{+},C^{-},M_0,\Delta), (C'^{+},C'^{-},M'_0,\Delta')\}$ de RPT à n transitions. Un vecteur $\hat{X}$ de E^n est un fonctionnement du RPTC si et seulement si:

- $\hat{X}$ est un fonctionnement du RPT (C^{+},C^{-},M_0,Δ)
- $\hat{X}$ vérifie $C'^{+}\hat{X} > [R^{\Delta'}](C'^{-}\hat{X} + M'_0)$

Le réseau $(C'^{+},C'^{-},M'_0,\Delta')$ sera appelé "anti-réseau".

Exemple : Δ_i représente le temps minimum de séjour d'une marque dans la place p_i . On peut maintenant spécifier de plus un temps maximum $\Delta_i' > \Delta_i$. Ces contraintes s'écrivent :

$$C^- \hat{X} > [R^{\Delta'}] C^+ \hat{X}$$

et correspondent à l'anti-réseau $(C^-, C^+, 0, \Delta')$.

5.3.2.2. Généralité des réseaux temporisés à contraintes : La classe des systèmes discrets temporisés modélisables au moyen de RPTC semble assez vaste. On peut essayer de situer cette classe par rapport à celle, plus générale, des systèmes décrits par des ensembles d'inéquations linéaires en évènements, c'est à dire dont l'ensemble des comportements est caractérisé par $M\hat{X} \leq B$, M et B étant respectivement une matrice m×n, et un n-vecteur de pseudo-évènements.

Notons d'abord qu'un pseudo évènement ayant, en général, une infinité de termes, un système dont la définition comporte des coefficients dans A peut donc dépendre d'une infinité de paramètres. Il est naturel de se restreindre aux systèmes dépendant d'un nombre fini de paramètres.

Définitions : Un pseudo-évènement a est fini ssi $\sharp a \in \mathbb{N}$. Un pseudo-évènement est rationnel, s'il est le quotient de deux pseudo-évènements finis. C'est une généralisation évidente de la notion de série $\mathbb{Z}$-rationnelle à une variable [Berstel].

Il est clair que l'ensemble des pseudo-évènements rationnels est un sous anneau de A.

Théorème : Pour tous M, B, respectivement matrice m×n et n-vecteur de pseudo évènements rationnels, l'ensemble des solutions dans E^n du système $M\hat{X} \leq B$ est la projection du système d'inéquations d'un RPTC.

Démonstration: Montrons d'abord que tout système à coefficients rationnels est la projection d'un système à coefficients finis: Soient a et b des pseudo-évènements finis, dénomina-

teurs communs des éléments de M et B et posons :

$$M = \frac{M'}{a} \quad , \quad B = \frac{B'}{b} \quad ,$$

M', B' étant formés de pseudo-évènements finis

Introduisons les nouveaux vecteurs d'évènements $\hat{X}_1$, $\hat{X}_2$, $\hat{X}_3$, $\hat{X}_4$, avec:

$$\hat{X} = a(\hat{X}_1 - \hat{X}_2) \quad , \quad B' = b(\hat{X}_3 - \hat{X}_4)$$

Le système $M\hat{X} \leqslant B$ est alors la projection sur $\hat{X}$ du système, à coefficients finis, suivant:

$$M'(\hat{X}_1 - \hat{X}_2) \leqslant \hat{X}_3 - \hat{X}_4$$

$$\hat{X} = a(\hat{X}_1 - \hat{X}_2)$$

$$b(\hat{X}_3 - \hat{X}_4) = B'$$

Montrons maintenant que tout système $M\hat{X} \leqslant B$, à coefficients finis est la projection d'un système de la forme:

$$M_0 + [R^{\Delta}]C^{+}\hat{Y} \geqslant C^{-}\hat{Y}$$

$$C'^{+}\hat{Y} \geqslant [R^{\Delta'}](C'^{-}\hat{Y} + M'_0)$$

M et B peuvent s'écrire $M = \sum_{i=1}^{k} M_i R^{t_i}$, $B = \sum_{i=1}^{k} B_i R^{t_i}$, où les M_i, B_i sont respectivement des matrices $m \times n$ et des m-vecteurs d'entiers. Introduisons les vecteurs d'évènements $\hat{X}_i$, $\hat{X}'_i$, $\hat{X}''_i$ i=1...k, avec

$$R^{t_i}\hat{X} = \hat{X}_i \quad , \quad \hat{X}'_i = R^{t_i}\hat{X}''_i \quad , \quad \hat{X}''_i = 1$$

On obtient alors:

. Une inéquation homogène et sans retard, qui peut être

indifféremment un système de réseau ou d'antiréseau:

$$\Sigma_{i=1}^{k} M_i \hat{X}_i \leq \Sigma_{i=1}^{k} B_i \hat{X}_i$$

. Un système de réseau:

$$\left.\begin{array}{l} \hat{X}_i \leq R^{t}{}_i \hat{X} \\ \hat{X}'_i \leq R^{t}{}_i \hat{X}''_i \\ \hat{X}''_i \leq 1 \end{array}\right\} \quad i = 1 \ldots k$$

. Un système d'antiréseau:

$$\left.\begin{array}{l} R^{t}{}_i \hat{X} \leq \hat{X}_i \\ R^{t}{}_i \hat{X}''_i \leq \hat{X}'_i \\ 1 \leq \hat{X}''_i \end{array}\right\} \quad i = 1 \ldots k$$

5.3.3. Réseaux de Pétri temporisés synchrones

Les réseaux de Pétri à contraintes, que nous venons de présenter, permettent de modéliser une classe de systèmes synchrones. Une autre façon d'étendre le modèle RPT pour prendre en compte les aspects synchrones, consiste à imposer qu'un RPT fonctionne à vitesse maximale [Ranchandani], [Moalla, Pulou & Sifakis] . Pour cela, on ajoute aux contraintes (i) et (ii) de la définition 5.3.1.1 la contrainte supplémentaire :

(iii) Une transition ne peut rester validée pendant un intervalle de temps strictement positif : Dés qu'elle est validée, elle doit être instantanément soit mise à feu, soit invalidée par la mise à feu d'une transition concurrente .

Pour simplifier, nous ne considérerons dorénavant que des réseaux non généralisés (tout arc du graphe est de poids 1) . Dans ce contexte, nous avons vu (§ 5.3.2.2) qu'une c.n.s. pour qu'un vecteur $(\hat{x}_i, i=1..n)$ d'évènements représente un fonctionnement asynchrone du RPT, à partir du marquage initial M_0 , est que:

$$\forall i=1...m \ , \quad \sum_{x_j \in p_i^{\cdot}} \hat{x}_j \leq (M_0)_i + \sum_{x_j \in {}^{\cdot}p_i} R^{\Delta_i} \hat{x}_j$$

Soit encore :

$$\forall j=1...n \ , \ \forall i=1...m \text{ tel que } p_i \in {}^{\cdot}x_j \ , \ .$$

$$\hat{x}_j \leq (M_0)_i + \sum_{x_\ell \in {}^{\cdot}p_i} R^{\Delta_i} \hat{x}_\ell - \sum_{\substack{x_\ell \in p_i^{\cdot} \\ \ell \neq i}} \hat{x}_\ell$$

Pour décrire le fonctionnement du réseau, interprété à vitesse maximale, il suffit de rendre les évènements $\hat{x}_j$ maximaux sous les contraintes précédentes. On obtient donc le système d'équations non linéaires suivant :

$$\forall j=1..n \ , \ \hat{x}_j = \inf_{p_i \in {}^{\cdot}x_j} \left((M_0)_i + \sum_{x_\ell \in {}^{\cdot}p_i} R^{\Delta_i} \hat{x}_\ell - \sum_{\substack{x_\ell \in p_i^{\cdot} \\ \ell \neq j}} \hat{x}_\ell \right)$$

Exemple : Revenons à l'exemple 4.3 . Le système étudié peut être modélisé par le réseau de Pétri temporisé synchrone de la figure 11 . En appliquant la régle de traduction précédente, on obtient immédiatement le système d'équations suivant :

$$\hat{a}_1 = R^2 \hat{a}_1 + 1 \qquad \hat{a}_2 = R\hat{a}_3 \qquad \hat{a}_3 = R\hat{a}_2 + 1$$

$$\hat{e}_1 = \inf (\hat{a}_1 \ , \ n + \hat{f}_1 + \hat{f}_2 - \hat{e}_2) \qquad \hat{f}_1 = R^7 \hat{e}_1$$

$$\hat{e}_2 = \inf (\hat{a}_2 \ , \ n + \hat{f}_1 + \hat{f}_2 - \hat{e}_1) \qquad \hat{f}_2 = R^5 \hat{e}_2$$

Enfin, la contrainte de prise en compte immédiate impose que les places p_1 et p_2 soient toujours vides, ce qui s'écrit :

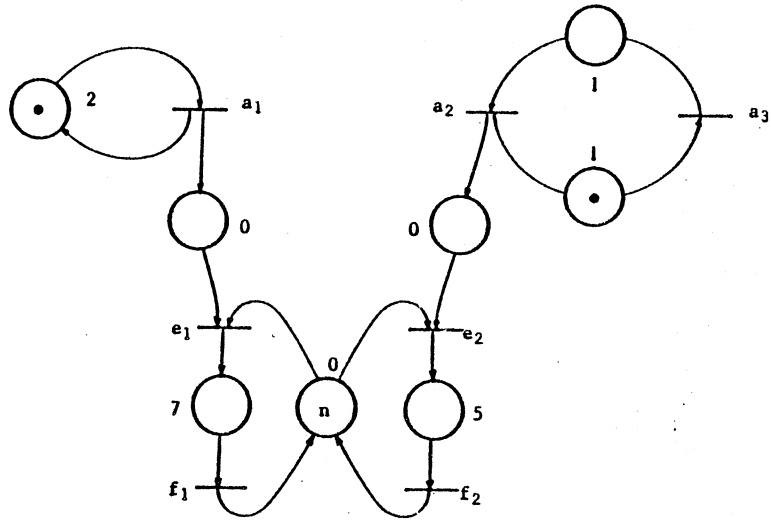
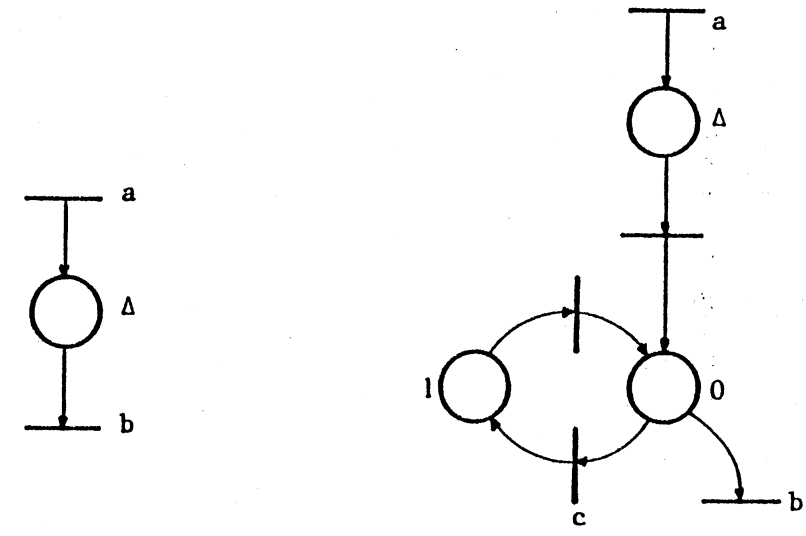


Figure 11
Réseau temporisé de l'exemple 4.3



$b \leq R^{\Delta}a$ <⟹> $c(1-R) = R^{\Delta}a-b$

Figure 12
Passage d'un RPT à un RPTS

$$\hat{e}_1 = \hat{a}_1 \quad , \quad \hat{e}_2 = \hat{a}_2$$

On a ainsi construit, de manière systématique, les contraintes du problème à partir du réseau de Pétri modélisant le système .

Remarque : En temps discret, à partir d'un RPT (asynchrone), on peut déduire, par le calcul, un réseau synchrone équivalent : En effet, le système d'inéquations du RPT

$$M_0 + [R^{\Delta}]C^{+}\hat{X} > C^{-}\hat{X}$$

est alors équivalent, d'après 4.5.1, à la propriété

$$(M_0 + [R^{\Delta}]C^{+}\hat{X} - C^{-}\hat{X}) \ / \ (1 - R) \in E^{m}$$

Soit $\hat{Y}$ ce vecteur d'évènements. Le système d'équations

$$\hat{Y} \ (1 - R) = M_0 + [R^{\Delta}]C^{+}\hat{X} - C^{-}\hat{X}$$

est alors un système de réseau synchrone. Intuitivement, ce réseau synchrone est obtenu à partir du RPT en rajoutant des transitions d'attente (cf. Figure 12). Ce procédé classique de désynchronisation est analogue à celui qui permet l'expression de l'asynchronisme en SCCS [Milner 83].

5.3.4. Réseaux de Pétri ordinaires.

La modélisation en évènements de l'ensemble des séquences de mises à feu d'un réseau de Pétri ordinaire se déduit de la caractérisation des comportements à vitesse maximale d'un réseau temporisé. En effet un réseau ordinaire peut être vu comme un réseau temporisé, dont toutes les places sont temporisées à 1, et dans lequel on interdit le tir simultané de plusieurs transitions par adjonction d'une place fictive p_{m+1}, telle que:

- Toute transition vide et remplit p_{m+1} ;
- p_{m+1} est temporisée à 1 et contient initialement une marque .

Par cet artifice, on obtient immédiatement la caractérisation de l'ensemble des séquences de tirs maximales d'un réseau de Pétri ordinaire, sous forme d'un système d'équations non linéaires :

$\forall x \in T$,

$$\hat{x} = \inf \left(1 + \sum_{y \in T} R\hat{y} - \sum_{\substack{y \in T \\ y \neq x}} \hat{y} \;,\; \inf_{p \in {}^\bullet x} \left(M_0(p) + \sum_{y \in {}^\bullet p} R\hat{y} - \sum_{\substack{y \in p^\bullet \\ y \neq x}} \hat{y} \right) \right)$$

On peut en déduire un système d'inéquations linéaires caractérisant l'ensemble des séquences de tir - non forcément maximales - du réseau :

$$\forall p \in P \;,\; \sum_{x \in p^\bullet} \hat{x} \leq M_0(p) + \sum_{x \in {}^\bullet p} R\hat{x}$$

auquel il convient alors d'adjoindre la condition de suite :

$$\sum_{x \in T} \hat{x} \, (1 - R)^2 \leq 1 - R$$

5.3.5. Test à zéro

Nous allons étudier, brièvement, le cas des réseaux avec test à zéro, dans le but d'établir, d'après [Agerwala], que notre calcul a la puissance de la machine de Turing .

Un réseau de Pétri avec test à zéro est un réseau de Pétri à chaque transition x duquel on associe un ensemble de places $\overset{\circ}{x}$. Les règles de fonctionnement sont les mêmes que celles des réseaux ordinaires, avec la contrainte supplémentaire qu'une transition x n'est validée par un marquage M que si aucune place appartenant à $\overset{\circ}{x}$ n'est marquée par M .

Si le vecteur d'évènements $(\hat{x} \mid x \in T)$ représente un fonctionnement du réseau, la condition "le marquage de la place p est nul" s'écrit :

$$\sup\ (\ 0\ ,\ 1 - M_0(p) - \sum_{y \in {}^\bullet p} \hat{y} + \sum_{y \in p^\bullet} \hat{y}\ )$$

et les contraintes supplémentaires liées au test à zéro, s'écrivent donc, d'après 4.5.2.4 :

$$\forall x \in T\ ,\ \forall p \in \overset{\circ}{x}\ ,$$

$$\hat{x}(1 - R) \leq \sup\ (\ 0\ ,\ 1 - M_0(p) - \sum_{y \in {}^\bullet p} R\hat{y} + \sum_{y \in p^\bullet} R\hat{y}\ )$$

5.4. DEUX EXEMPLES D'APPLICATION

Pour achever d'illustrer la puissance d'expression et l'usage du calcul pour l'analyse des systèmes temporisés, nous terminerons ce chapitre par quelques exemples concrets.

5.4.1. Ressource exclusive à usage permanent

On considère un système formé de deux processus p_1 et p_2 , partageant une ressource exclusive. Chaque processus p_i a un fonctionnement cyclique, consistant 1°) à demander la ressource, 2°) l'ayant acquise, à l'utiliser pendant un délai δ_i , 3°) à relâcher la ressource et travailler sans elle pendant un délai Δ_i , après lequel il revient demander la ressource (δ_i , $\Delta_i \in \mathbb{N}^*$) .

Ce système peut être représenté par le réseau de Pétri temporisé synchrone de la figure 13 .

On se pose alors le problème de trouver une condition nécéssaire et suffisante sur les délais δ_i , Δ_i (i=1,2), de telle sorte que la ressource soit utilisée en permanence .

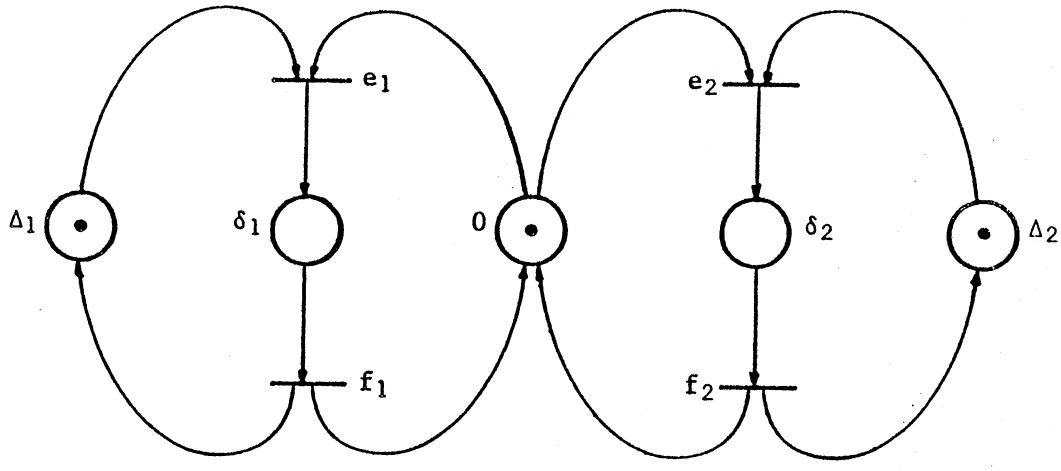


Figure 13
RPTS de la ressource exclusive

A partir du réseau, on peut formaliser l'ensemble des comportements du système comme suit :

$$e_1 = \inf (R^{\Delta_1} f_1 + 1 \ , \ f_1 + f_2 + 1 - e_2) \qquad f_1 = R^{\delta_1} e_1$$

$$e_2 = \inf (R^{\Delta_2} f_2 + 1 \ , \ f_1 + f_2 + 1 - e_1) \qquad f_2 = R^{\delta_2} e_2$$

et la contrainte d'utilisation permanente de la ressource s'écrit :

$$e_1 + e_2 = f_1 + f_2 + 1$$

Le problème se formalise donc de la manière suivante : Trouver une condition nécéssaire et suffisante sur les délais δ_i , Δ_i (i=1,2) pour que le système S ci-dessous admette une solution dans $E(\mathbb{N})^2$:

$$S = \begin{cases} e_i(1 - R^{\Delta_i+\delta_i}) < 1 \quad (i=1,2) \\ e_1(1 - R^{\delta_1}) + e_2(1 - R^{\delta_2}) = 1 \end{cases}$$

Alors, d'après l'équation contenue dans S, puisque 1 est un évènement, $e_1(1 - R^{\delta_1}) + e_2(1 - R^{\delta_2})$ doit être un évènement. Donc :

$$S \Rightarrow R^{\delta_1}(1 - R)e_1 + R^{\delta_2}(1 - R)e_2 \leq e_1(1 - R) + e_2(1 - R)$$

Or, puisque δ_i , $\Delta_i \in \mathbb{N}^*$, on a :

$$R^{\delta_i}e_i \leq Re_i \leq e_i \leq 1 + R^{\Delta_i+\delta_i}e_i \leq 1 + R.R^{\delta_i}e_i$$

Donc

$$0 \leq \inf(R^{\delta_i}(1 - R)e_i , e_i(1 - R))$$

$$\leq \inf(1 - e_i(1 - R) , e_i(1 - R)) \leq 0$$

D'où $\inf(R^{\delta_i}(1 - R)e_i , e_i(1 - R)) = 0$

On en déduit que

$$R^{\delta_i}(1 - R)e_i \leq e_j(1 - R) , \quad i = 1,2 , \ j = 2-i$$

> En effet, on se trouve dans la situation suivante :
>
> $a, b, c, d \in A(\mathbb{N})$
>
> $a + b \leq c + d$
>
> $\inf(a,c) = \inf(b,d) = 0$
>
> De $\inf(a,c) = 0$ on tire $b = \inf(a+b,c+b) \leq \inf(c+d,c+b)$.
> Donc $b \leq c + \inf(b,d) = c$. D'où $b \leq c$ et, par symétrie, $a \leq d$.

Alors $e_1 - R^{\delta_2}e_2$ et $e_2 - R^{\delta_1}e_1$ sont des évènements, et leur somme vaut 1. Donc l'un vaut 1 et l'autre est nul, et l'une des deux situations suivantes doit avoir lieu :

1) $e_2 = 1 + R^{\delta_1}e_1$ et $e_1 = R^{\delta_2}e_2$

2) $e_1 = 1 + R^{\delta_2}e_2$ et $e_2 = R^{\delta_1}e_1$

On a S <=> S_1 ou S_2 , avec, pour i=1,2 et j=2-i ,

$$S_i = \{ e_j = \frac{1}{1 - R^{\delta_1+\delta_2}} \ , \ e_i = \frac{R^{\delta_j}}{1 - R^{\delta_1+\delta_2}} \ ,$$

$$\frac{R^{\delta_j}(1 - R^{\delta_i+\Delta_i})}{1 - R^{\delta_1+\delta_2}} < 1 \ , \ \frac{1 - R^{\delta_j+\Delta_j}}{1 - R^{\delta_1+\delta_2}} < 1 \ \}$$

Donc S admet une solution si et seulement si

$$\frac{1 - R^{\delta_1+\Delta_1}}{1 - R^{\delta_1+\delta_2}} < 1 \quad \text{et} \quad \frac{1 - R^{\delta_2+\Delta_2}}{1 - R^{\delta_1+\delta_2}} < 1$$

ou, de manière équivalente, si et seulement si

$$\delta_1 + \delta_2 \geq \delta_1 + \Delta_1 \quad \text{et} \quad \delta_1 + \delta_2 \geq \delta_2 + \Delta_2$$

D'où la condition nécéssaire et suffisante finale :

$$\delta_2 \geq \Delta_1 \quad \text{et} \quad \delta_1 \geq \Delta_2$$

5.4.2. Tâche interruptible

On veut décrire une tâche, de durée $\Delta \in \mathbb{N}$, qui peut être interrompue à chaque instant entier. La tache est supposée non réentrante.

La modélisation de cette tâche en réseau de Pétri nécéssite un réseau synchrone assez complexe, et dont la structure dépend de Δ : Dans le réseau de la figure 14, la transition a représente le début de la tâche. Quand une marque atteint la place J_i, la tâche peut être soit interrompue, par la mise à feu de c_i - elle reste alors dans l'état interrompu I_i jusqu'à sa réactivation par la mise à feu de d_i - soit continuée pendant une unité de temps (place W_i) avant de devenir à nouveau interruptible . La transition b ($=b_\Delta$) représente la fin de la tâche.

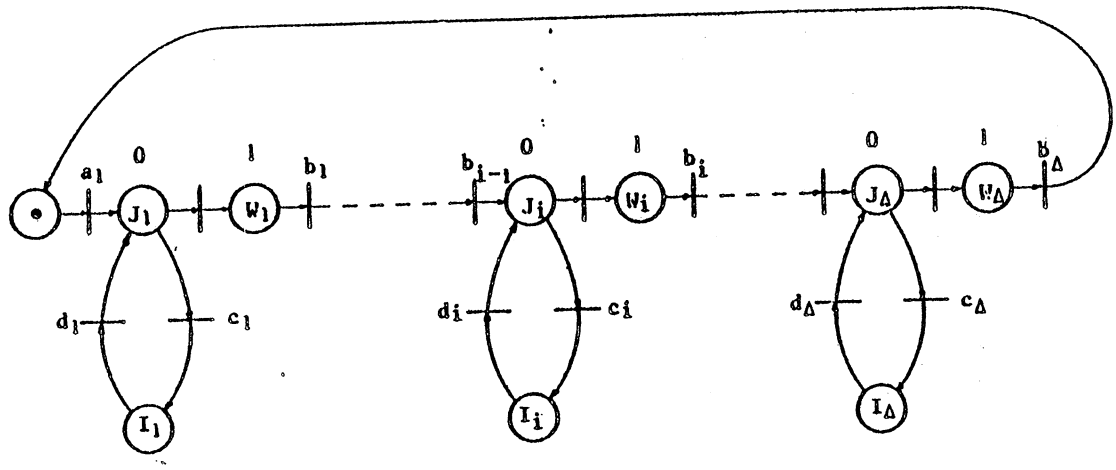


Figure 14

RPTS d'une tâche interruptible

Nous allons voir que notre calcul permet une formalisation concise de ce problème, et une démonstration formelle de l'équivalence entre cette formalisation et le réseau de Pétri.

Proposition : Soient $\hat{a}$, $\hat{b}$, $\hat{c}$, $\hat{d}$ les quatre évènements représentant respectivement le début, la fin, l'interruption et la réactivation de la tâche. Alors étant donnés $\hat{a}$, $\hat{c}$ et $\hat{d}$,l'évènement $\hat{b}$ est complètement déterminé par la relation suivante :

$$0 \leq \frac{\hat{a} + \hat{d} - \hat{c} - \hat{b}}{1 - R} - \Delta\hat{b} \leq \Delta$$

Démonstration : Notons $\hat{a} = \hat{b}_0$, $\hat{b} = \hat{b}_\Delta$, $\hat{c} = \sum_{i=1}^{\Delta} \hat{c}_i$, $\hat{d} = \sum_{i=1}^{\Delta} \hat{d}_i$, et $\hat{x} = (\hat{a} + \hat{d} - \hat{c} - \hat{b}) / (1 - R) - \Delta\hat{b}$.

D'après le réseau, on a :

$$\forall i = 1...\Delta \ , \ \hat{b}_i = R\hat{b}_{i-1} - R\hat{c}_i + R\hat{d}_i$$

d'où

$$\forall i = 1...\Delta \ , \ \hat{b}_i = R^i\hat{a} + \sum_{j=1}^{i} R^{i-j+1} (\hat{d}_j - \hat{c}_j)$$

et

$$\hat{b} = R^\Delta\hat{a} + \sum_{j=1}^{\Delta} R^{\Delta-j+1} (\hat{d}_j - \hat{c}_j)$$

Puisque la tâche n'est pas réentrante, on a $\hat{a} \leq \hat{b} + 1$, et donc :

$$\hat{a}(1 - R^\Delta) \leq 1 + \sum_{j=1}^{\Delta} R^{\Delta-j+1}(\hat{d}_j - \hat{c}_j) \qquad (1)$$

D'autre part :

$$\hat{x} = \hat{a}\left(\frac{1 - R^{\Delta}}{1 - R} - \Delta R^{\Delta} \right) + \sum_{j=1}^{\Delta} (\hat{d}_j - \hat{c}_j)\left(\frac{1 - R^{\Delta-j+1}}{1 - R} - \Delta R^{\Delta-j+1} \right)$$

Puisque $\frac{1 - R^{\Delta}}{1 - R} \leqslant \Delta$ et que $\hat{a}$ est un évènement, on obtient :

$$\hat{x} \leqslant \Delta(1 - R^{\Delta})\hat{a} + \sum_{j=1}^{\Delta} (\hat{d}_j - \hat{c}_j)\left(\frac{1 - R^{\Delta-j+1}}{1 - R} - \Delta R^{\Delta-j+1} \right)$$

Soit, en exploitant l'inéquation (1) :

$$\hat{x} \leqslant \Delta + \sum_{j=1}^{\Delta} (\hat{d}_j - \hat{c}_j) \frac{1 - R^{\Delta-j+1}}{1 - R}$$

Pour tout $j = 1 \ldots \Delta$, $(\hat{d}_j - \hat{c}_j)$ est négatif, et $\frac{1 - R^{\Delta-j+1}}{1 - R}$ est un évènement. Donc $\sum_{j=1}^{\Delta} (\hat{d}_j - \hat{c}_j) \frac{1 - R^{\Delta-j+1}}{1 - R}$ est négatif et $\hat{x} \leqslant \Delta$.

Pour montrer que $\hat{x}$ est positif, on utilise l'identité suivante :

$$1 \leqslant k \leqslant \Delta \Rightarrow \frac{1 - R^{k}}{1 - R} \Delta R^{k} = \sum_{n=1}^{k} (R^{n-1} - R^{k}) - (\Delta - k)R^{k}$$

Il vient:

$$\hat{x} = \hat{a} \sum_{n=1}^{\Delta} (R^{n-1} - R^{\Delta}) + \sum_{j=1}^{\Delta} (\hat{d}_j - \hat{c}_j)\left[\sum_{n=1}^{\Delta-j+1} (R^{n-1} - R^{\Delta-j+1}) - (j - 1)R^{\Delta-j+1} \right]$$

$$= \sum_{n=1}^{\Delta} \left[(R^{n-1} - R^{\Delta})\hat{a} + \sum_{j=1}^{\Delta-n+1} (R^{n-1} - R^{\Delta-j+1})(\hat{d}_j - \hat{c}_j) \right]$$

$$- \sum_{j=1}^{\Delta} (j - 1)R^{\Delta-j+1}(\hat{d}_j - \hat{c}_j)$$

$\hat{d}_j - \hat{c}_j$ etant négatif, il en est de même de $\sum_{j=1}^{\Delta} (j - 1)R^{\Delta-j+1}(\hat{d}_j - \hat{c}_j)$

Donc

$$\hat{x} \geq \sum_{i=1}^{\Delta} (1 - R^{\Delta-i+1})[\, R^{i-1}\hat{a} + \sum_{j=1}^{i} R^{i-j}(\hat{d}_j - \hat{c}_j)\,]$$

$$= \sum_{i=1}^{\Delta} (1 - R^{\Delta-i+1})(R^{-1}\hat{b}_i)$$

Comme les $\hat{b}_i$ sont des évènements, on en déduit :

$$\sum_{i=1}^{\Delta} (1 - R^{\Delta-i+1})(R^{-1}b_i) \geq 0$$

et donc $\hat{x} \geq 0$.

On a ainsi prouvé $0 \leq \hat{x} \leq \Delta$. Il nous reste à montrer que cette relation caractérise $\hat{b}$ en fonction de $\hat{a}$, $\hat{c}$ et $\hat{d}$. Pour cela nous allons montrer que chaque fois que $\hat{b}$ peut se produire, alors il doit se produire. Nous utiliserons la notation suivante : Si $\hat{y}$ et $\hat{z}$ sont deux pseudo-évènements, $[\hat{y}>\hat{z}]$ dénote la condition qui vaut vrai à l'instant t si et seulement si $\mu\hat{y}(t) > \mu\hat{z}(t)$.

Posons $\hat{y} = (\hat{a} + \hat{d} - \hat{c}) / (1 - R)$ et $\hat{z} = \hat{b}(\Delta + 1/(1 - R))$. On a $\hat{y} - \Delta \leq \hat{z} \leq \hat{y}$, et $\hat{z} = \Delta\hat{b}(1 - R) + R\hat{z} + \hat{b}$. Donc, la condition "$\hat{b}$ peut se produire" est équivalente à:

$$[\hat{y} > \Delta + 1 + R\hat{z}]$$

et la condition "$\hat{b}$ doit se produire" est équivalente à:

$$[\hat{y} - \Delta > R\hat{z}]$$

et ces deux conditions sont trivialement équivalentes.

Cette démonstration est certes longue et pénible; cependant on a ainsi prouvé, de manière complètement formelle, un résultat non trivial, qui peut être fort utile pour traiter les systèmes à interruptions.

5.5. APPLICATION AUX PROBLEMES D'ORDONNANCEMENT

5.5.1. Ordonnancement et "programmes linéaires" en évènements

Les problèmes d'ordonnancement se posent dans des disciplines variées, et particulièrement, en informatique, dans la phase d'implantation d'un système temporisé : Il s'agit de définir l'activation temporelle d'un ensemble de tâches, soumises à des contraintes de synchronisation (relations de succession, d'exclusion, ...), et nécéssitant des ressources (processeurs, mémoires, ...), et ceci en tenant compte explicitement des ressources dont on dispose effectivement pour l'implantation. Généralement, cet ordonnancement doit chercher à optimiser certains critères, comme le nombre de ressources, le temps d'achèvement de l'ensemble des tâches, le temps moyen ou maximum de réponse de chaque tâche à des requêtes externes etc... Une part de la bibliographie, très abondante, consacrée à ces problèmes, pourra être trouvée dans [Bourdon], qui montre également que, pour une classe importante de prblèmes d'ordonnancement, l'ensemble des contraintes intervenant dans le problème est modélisable au moyen d'un réseau de Pétri temporisé, et donc par un système d'inéquations linéaires en évènements. Nous nous bornerons à en donner un exemple, qui illustre bien la variété des contraintes auxquelles peut être soumis un problème d'ordonnancement.

Soient quatre tâches a, b, c, d à réaliser sur deux processeurs p_1 et p_2 , sachant que:

- Les tâches b et c ne peuvent être activées qu'après achèvement de la tâche a.
- Les tâches c et d ne peuvent être exécutées simultanément.
- La tâche d ne peut être effectuée que par le processeur p_1 .
- Si l'on note δ_{xi} le temps d'exécution de la tâche x sur le processeur p_i (i=1,2), on a:

$\delta_{a1} = 2$, $\delta_{a2} = 3$, $\delta_{b1} = 1$, $\delta_{b2} = 2$, $\delta_{c1} = 3$, $\delta_{c2} = 3$, $\delta_{d1} = 2$

La figure 15 représente un ordonnancement compatible avec ces contraintes, dont le temps d'achèvement est 6.

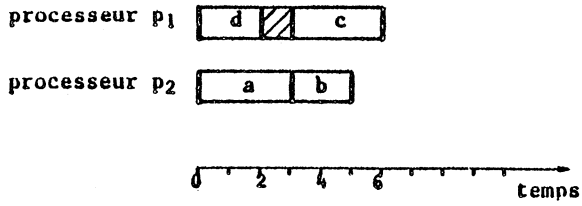
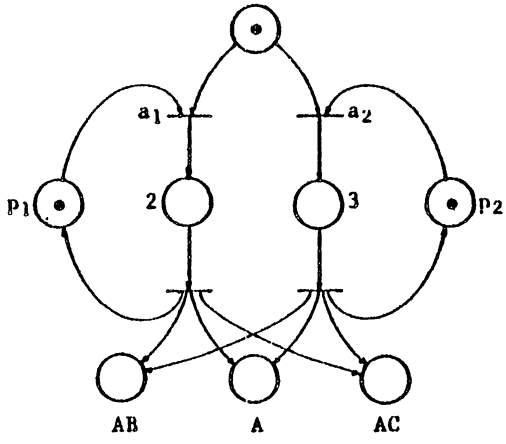
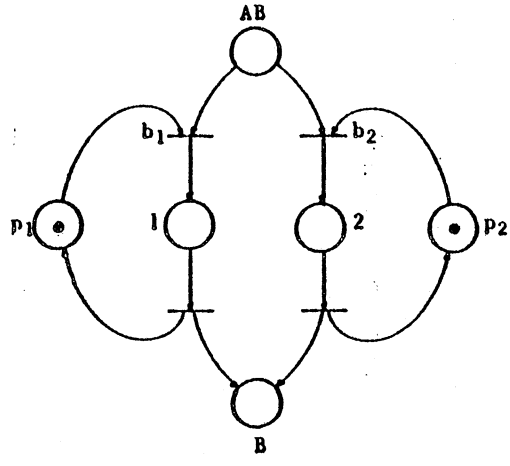


Figure 15

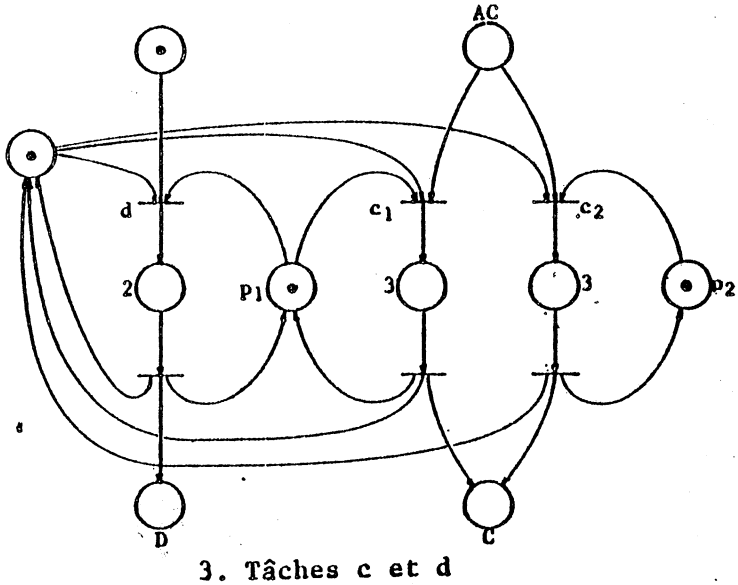
Ordonnancement compatible avec les contraintes de l'exemple 5.5.1



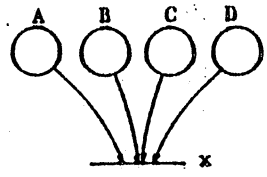
1. Tâche a



2. Tâche b



3. Tâches c et d



4. Transition d'achèvement

Figure 16

RPT du problème d'ordonnancement de l'exemple 5.5.1

Les contraintes de ce problème peuvent être modélisées sur un réseau de Pétri temporisé, que nous avons représenté, en raison de sa complexité, en trois sous-réseaux partageant des places (figure 16 (1), (2), (3)).

Supposons alors que le critère à minimiser soit le temps d'achèvement total. On peut adjoindre au réseau une nouvelle transition, qui n'est validée que lorsque les quatre tâches ont été exécutées (figure 16 (4)). Le problème se formalise donc en évènements comme un problème de maximisation de l'évènement associé à cette transition finale, sous les contraintes déduites du réseau, soit sous la forme suivante :

Maximiser l'évènement $\hat{x}$ tel que :

$$\left.\begin{array}{l} \hat{x} \leqslant R^2\hat{a}_1 + R^3\hat{a}_2 \\ \hat{x} \leqslant R\hat{b}_1 + R^2\hat{b}_2 \\ \hat{x} \leqslant R^3\hat{c}_1 + R^3\hat{c}_2 \\ \hat{x} \leqslant R^2\hat{d} \end{array}\right\} \text{dates d'achèvement}$$

$$\left.\begin{array}{l} \hat{a}_1 + \hat{a}_2 \leqslant 1 \\ \hat{b}_1 + \hat{b}_2 \leqslant R^2\hat{a}_1 + R^3\hat{a}_2 \\ \hat{c}_1 + \hat{c}_2 \leqslant R^2\hat{a}_1 + R^3\hat{a}_2 \\ \hat{d} \leqslant 1 \end{array}\right\} \text{dates d'activation}$$

$$\left.\begin{array}{l} \hat{a}_1(1 - R^2) + \hat{b}_1(1 - R) + \hat{c}_1(1 - R^3) + \hat{d}(1 - R^2) \leqslant 1 \\ \hat{a}_2(1 - R^3) + \hat{b}_2(1 - R^2) + \hat{c}_2(1 - R^3) \leqslant 1 \end{array}\right\} \text{processeurs}$$

$$\hat{d}(1 - R^2) + \hat{c}_1(1 - R^3) + \hat{c}_2(1 - R^3) \leqslant 1 \qquad \text{exclusivité de c et d}$$

Un très grand nombre de problèmes d'ordonnancement se ramènent ainsi à maximiser (ou minimiser) un évènement en tenant compte d'un système d'inéquations linéaires en évènements. Par analogie avec les problèmes d'optimisation linéaires dans $\mathbb{R}^n$, nous appellerons un tel problème "programme linéaire" dans $A(\mathbb{T})$. Au chapitre suivant, nous aborderons les problèmes auxquels nous nous sommes heurtés en tentant de résoudre ce type de programmes. Nous nous contenterons ici d'illustrer les résultats approchés que l'on peut obtenir, sur un problème simple.

5.5.2. Approximation de la solution d'un problème de "bin packing"

Dans ce paragraphe, nous présentons une méthode de résolution approchée d'une classe de problèmes d'ordonnancement simples, dont les caractéristiques sont les suivantes :

. Les tâches sont indépendantes : Elles ne sont soumises à aucune contrainte de succession ou d'exclusion.

. Les seules ressources sont les processeurs, qui sont tous identiques. Plus précisément, le problème se présente de manière suivante : On dispose de m processeurs de mêmes performances, sur lesquels on veut exécuter un ensemble de tâches indépendantes, partitionné en k classes $C_1, \ldots, C_k$ telles que :

- La classe C_i comprend n_i tâches .
- L'exécution d'une tâche appartenant à la classe C_i requiert le travail d'un processeur pendant Δ_i unités de temps ($\Delta_i \in \mathbb{N}^*$).
- Les classes sont indicées selon l'ordre croissant des temps d'exécution ($\Delta_1 < \Delta_2 < \ldots < \Delta_k$) .

. Le problème consiste à trouver une affectation temporelle des tâches aux processeurs, minimisant le temps global d'achèvement.

Les contraintes du problème se formalisent comme suit: Soit $\hat{a}_i$ l'évènement qui survient chaque fois qu'une tâche de la classe C_i est activée. On doit avoir :

$$\hat{a}_i \leq n_i \qquad i = 1 \ldots k \tag{1}$$

$$\sum_{i=1}^{k} \hat{a}_i (1 - R^{\Delta_i}) \leq m \tag{2}$$

Plutôt que de chercher à maximiser l'évènement d'achèvement, on montre que, du fait que les processeurs sont identiques, on peut choisir de maximiser l'intégrale discrète de la "fonction de charge" du système:

$$\sum_{i=1}^{k} a_i (1 - R^{\Delta_i})$$

pseudo-évènement dont le compteur est égal, à chaque instant, au nombre

de processeurs actifs. Donc soit $\hat{z}$ le pseudo-évènement à maximiser :

$$\hat{z} = \sum_{i=1}^{k} a_i \frac{1 - R^{\Delta_i}}{1 - R}$$

On peut faire une dernière remarque, évidente : Si toutes les tâches pouvaient être découpées en fractions de durée 1, l'ordonnancement optimal consisterait à faire travailler tous les processeurs tant qu'il existe au moins m fractions à exécuter, soit pendant q unités de temps, puis à exécuter les r fractions restantes, en une unité de temps, q et r étant respectivement le quotient et le reste de la division entière du temps de calcul total $\Sigma_{i=1}^{k} n_i\Delta_i$ par le nombre de processeurs m . La fonction de charge correspondant à cet ordonnancement optimal (et généralement irréalisable si l'on ne peut pas fractionner les tâches) est $m(1 - R^q) + rR^q(1 - R)$. On a donc certainement :

$$\hat{z} \leq m \frac{1 - R^q}{1 - R} + rR^q \qquad (3)$$

D'autre part, puisque les Δ_i sont indicés par ordre croissant, on a (en posant $\Delta_0=0$) :

$$1 - R^{\Delta_i} = \sum_{j=1}^{i} R^{\Delta_{j-1}} - R^{\Delta_j}$$

Donc

$$\hat{z} = \sum_{i=1}^{k} \hat{a}_i \sum_{j=1}^{i} \frac{R^{\Delta_{j-1}} - R^{\Delta_j}}{1 - R} = \sum_{j=1}^{k} \frac{R^{\Delta_{j-1}} - R^{\Delta_j}}{1 - R} \sum_{i=j}^{k} \hat{a}_i$$

Posons $\hat{x}_j = \sum_{i=j}^{k} \hat{a}_i$

On a, d'après (1) ,

$$\hat{x}_j = \sum_{i=j}^{k} \hat{a}_i = \hat{a}_j + \sum_{i=j+1}^{k} \hat{a}_i \leq n_j + \sum_{i=j+1}^{k} \hat{a}_i = n_j + \hat{x}_{j+1}$$

et comme $j < i \Rightarrow \Delta_j < \Delta_i \Rightarrow 1 - R^{\Delta_j} \leq 1 - R^{\Delta_i}$ et que les a_i sont des évènements,

$$\hat{x}_j(1 - R^{\Delta_j}) = \sum_{i=j}^{k} \hat{a}_i(1 - R^{\Delta_j}) \leq \sum_{i=j}^{k} \hat{a}_i(1 - R^{\Delta_i}) \leq m$$

Donc, $\hat{x}_j \leq m + R^{\Delta_j}\hat{x}_j$

Les $\hat{x}_j$ satisfont donc le système d'inéquations :

$$\hat{x}_j \leq \inf(n_j + \hat{x}_{j+1} , m + R^{\Delta_j}\hat{x}_j)$$
en posant $\hat{x}_{k+1} = 0$

Le vecteur X, dont les composantes sont les $\hat{x}_j$, est donc un pré-point fixe de la fonction vectorielle F, croissante de $E(\mathbb{Z})^k$ dans lui-même, telle que :

$$F(X)_j = \inf(n_j + X_{j+1} , m + R^{\Delta_j}X_j)$$

Nous montrerons au § 6.2.2 que cette fonction admet un plus grand point-fixe

$$\bar{X} = \inf_{n>0} F^n(N) ,$$

où N est le vecteur d'évènements dont la i-ième composante est n_i.

Donc $X \leq \bar{X}$ et $\hat{z} \leq \sum_{j=1}^{k} \frac{R^{\Delta_{j-1}} - R^{\Delta_j}}{1 - R} \bar{X}_j$ (4)

Enfin la contrainte (2) s'écrit $\hat{z}(1 - R) \leq m$, soit

$$\hat{z} \leq m + R\hat{z} \qquad (5)$$

On obtient donc, à partir de (3), (4) et (5), la contrainte approchée suivante, sur la fonction objectif :

$$\hat{z} \leq \inf(m \frac{1 - R^q}{1 - R} + rR^q , \sum_{j=1}^{k} \frac{R^{\Delta_{j-1}} - R^{\Delta_j}}{1 - R} \bar{X}_j , m + R\hat{z})$$

On peut ainsi construire une majoration de la valeur de la fonction objectif à l'optimum, en calculant itérativement le plus grand point fixe $\bar{z}$ de la fonction monotone

$$G = \lambda\hat{z}. \inf(m\frac{1 - R^q}{1 - R} + rR^q , \sum_{j=1}^{k} \frac{R^{\Delta_{j-1}} - R^{\Delta_j}}{1 - R} \bar{X}_j , m + R\hat{z})$$

L'expérience montre que cette majoration est très souvent égale à l'optimum, comme dans l'exemple suivant .

Exemple numérique :

$k = 3$, $m = 3$, $\Delta_1 = 2$, $\Delta_2 = 3$, $\Delta_3 = 4$, $n_1 = 1$, $n_2 = 3$, $n_3 = 1$

Calculons les $\bar{X}_j$:

$\bar{X}_3 = \inf(n_3 , m + R^{\Delta_3}\bar{X}_3) = \inf(1 , 3 + R^4\bar{X}_3) = 1$

$\bar{X}_2 = \inf(n_2 + \bar{X}_3 , m + R^{\Delta_2}\bar{X}_2) = \inf(4 , 3 + R^3\bar{X}_2)$

On trouve successivement $\bar{X}_2^0 = 4$, $\bar{X}_2^1 = 3 + R^3$, $\bar{X}_2^2 = 3 + R^3$.

Donc $\bar{X}_2 = 3 + R^3$

$\bar{X}_1 = \inf(n_1 + \bar{X}_2 , m + R^{\Delta_1}\bar{X}_1) = \inf(4 + R^3 , 3 + R^2\bar{X}_1)$

On trouve successivement $\bar{X}_1^0 = 4 + R^3$, $\bar{X}_1^1 = 3 + R^2 + R^3$, $\bar{X}_1^2 = 3 + R^2 + R^3$, soit $\bar{X}_1 = 3 + R^2 + R^3$

On peut maintenant calculer $\bar{z}$, plus grande solution de l'équation de point fixe suivante (On a $q = 5$ et $r = 0$) :

$$\bar{z} = \inf\left(3 + R\bar{z} \ , \ 3.\frac{1 - R^5}{1 - R} \ , \ \frac{1 + R^2}{1 - R}(3 + R^2 + R^3) + \frac{R^2 - R^3}{1 - R}(3 + R^3) + \frac{R^3 - R^4}{1 - R} \right)$$

$$= \inf(3 + 3R + 3R^2 + 3R^3 + 2R^4 + R^5 \ , \ 3 + R\bar{z})$$

$$= \inf\left(\frac{3 - R^4 - R^5 - R^6}{1 - R} \ , \ 3 + R\bar{z} \right)$$

On trouve successivement :

$\bar{z}^0 = (3 - R^4 - R^5 - R^6) / (1 - R)$

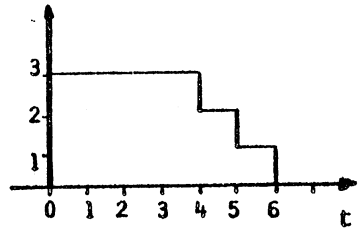
$\bar{z}^1 = \inf(\bar{z}^0 , 3 + R\bar{z}^0) = \bar{z}^0$

Soit $\bar{z} = (3 - R^4 - R^5 - R^6) / (1 - R)$

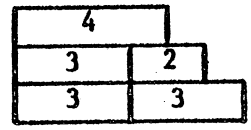
La fonction de charge correspondante est

$$\bar{z}(1 - R) = 3 - R^4 - R^5 - R^6$$

et son compteur est représenté par la figure 17.a . D'autre part la figure 17.b montre qu'il existe un ordonnancement avec cette fonction de charge, et donc que la borne $\bar{z}$ correspond exactement à l'optimum .



- a -



- b -

Figure 17

Solution du problème de "bin packing"

CHAPITRE 6

SYSTEMES D'INEQUATIONS LINEAIRES EN PSEUDO-EVENEMENTS

Nous avons regroupé dans ce chapitre les résultats des recherches que nous avons consacrées au problème de la résolution des programmes linéaires en pseudo-évènements. Quoique, sur le fond, ces recherches soient restées infructueuses, cet exposé est interessant de deux points de vue : On en dégagera d'une part certains résultats partiels, qui sont utilisables pour manipuler les systèmes d'inéquations linéaires, et d'autre part une compréhension plus profonde de la structure de l'ensemble des solutions d'un tel système.

On introduit les notations d'intervalles suivantes : Si a et b sont deux pseudo-évènements, on définit les ensembles :

$$[\![a) = \{ x \mid x \geq a \}$$

$$(b]\!] = \{ x \mid x \leq b \}$$

$$[\![a , b]\!] = [\![a) \cap (b]\!]$$

6.1. THEOREME DE L'OPTIMUM LOCAL

Nous allons démontrer un théorème analogue au "théorème fondamental de la programmation convexe" dans $\mathbb{R}^n$.

6.1.1. Programmes linéaires

Un demi-espace de $A(\mathbb{T})^n$ est l'ensemble des solutions, dans $A(\mathbb{T})^n$, d'une inéquations linéaire $\Sigma_{i=1}^{n} a_i x_i \leq b$, où les a_i et b appartiennent a $A(\mathbb{T})$, et les a_i ne sont pas tous nuls. Un polyèdre de $A(\mathbb{T})^n$ est l'intersection d'un nombre fini de demi-espaces.

On appelle programme linéaire dans $A(\mathbb{T})^n$ le problème suivant : Etant donné un polyèdre P de $A(\mathbb{T})^n$ et une application linéaire z, de $A(\mathbb{T})^n$ dans $A(\mathbb{T})$, trouver X dans P tel que la valeur de z en X soit maximale, c'est à dire tel que:

$$\forall Y \in A(\mathbb{T})^n,\ z(Y) \geq z(X) \text{ et } z(Y) \neq z(X) \Rightarrow Y \notin P$$

Un tel point X sera appelé optimum global du programme (P,z) .

Dans toute la suite on ne considérera que des programmes linéaires dans $A(\mathbb{Z})^n$. Soit $S = \{\Sigma_{i=1}^{n} a_{ij} X_i \leq b_i \mid j = 1...m\}$ un système d'inéquations à coefficients dans $A(\mathbb{Z})$, et P le polyèdre de ses solutions dans $A(\mathbb{Z})^n$. On notera $\tilde{P}$ le polyèdre des solutions de S dans $A(\mathbb{R})^n$.

6.1.2. Topologie de $A(\mathbb{R})$

6.1.2.1. Définition : $A(\mathbb{R})$ est muni de la topologie de la convergence simple presque partout sur les compteurs, c'est à dire qu'une suite $x_0, x_1, \ldots, x_k$ converge vers x dans $A(\mathbb{R})$ si et seulement si, pour presque tout $t \in \mathbb{R}$, la suite $\mu x_k(t)$ converge vers $\mu x(t)$. Soit Ω cette topologie. $A(\mathbb{R})^n$ sera muni de la topologie produit Ω^n .

6.1.2.2. Proposition : Soit $\Delta \in \mathbb{R}$, et Φ la topologie usuelle de $\mathbb{R}$. Les applications:

. $\lambda x.\ R^{\Delta}x$, de ($A(\mathbb{R})$, Ω) dans lui-même ,

. $\lambda x.\ x + y$, de ($A(\mathbb{R})^2$, Ω^2) dans ($A(\mathbb{R})$, Ω) ,

. $\lambda \delta.\ R^{\delta}$, de ($\mathbb{R}$, Φ) dans ($A(\mathbb{R})$, Ω) ,

sont continues

Par suite, toute application linéaire de $A(\mathbb{R})^n$ dans $A(\mathbb{R})$ est continue, au sens de Ω .

6.1.2.3. Corollaire : Tout polyèdre de $A(\mathbb{R})^n$ est fermé .

Démonstration : Soit $b \in A(\mathbb{R})$, et $(x_k \mid k \in \mathbb{N})$ une suite d'éléments de $(b\ ]]$. Si cette suite converge, sa limite appartient évidemment à $(b\ ]]$, donc $(b\ ]]$ est fermé. Un demi-espace $\{ X \mid zX \leq b \}$ est l'image inverse, par l'application linéaire, donc continue, z, du fermé $(b\ ]]$. Donc tout demi-espace est fermé, ainsi que l'intersection d'un nombre quelconque de demi-espaces.

6.1.2.4. Définition : Soit (P,z) un programme linéaire dans $A(\mathbb{Z})^n$. Un point X de P constitue un optimum local du programme, s'il existe un voisinage ω de X dans $A(\mathbb{R})^n$, tel que :

$$Y \in \omega \text{ et } z(Y) \geq z(X) \text{ et } z(Y) \neq z(X) \Rightarrow Y \notin \tilde{P}$$

6.1.3. Convexité

6.1.3.1. Segments : Soient $x,y \in A(\mathbb{Z})$. On appelle segment d'extrémités x et y l'ensemble

$$[x\ ,\ y] = \{ f_{xy}(\delta) \mid \delta \in [0,1] \}$$

$$\text{où } f_{xy} = \lambda\delta.\ \frac{x(1 - R^{\delta}) + y(R^{\delta} - R)}{1 - R}$$

On notera $]x , y[$ l'ensemble $[x , y] - \{x , y\}$.

6.1.3.2. Proposition : Pour tout couple (x,y) de $A(\mathbb{Z})^2$, si $x \leqslant y$ alors $[x , y] \subset [[x , y]]$.

Démonstration : On montre facilement que, pour tout $\delta \in]0,1[$, et pour tout $t \in \mathbb{R}$, si $u = f_{xy}(\delta)$ et $t' = t - \lfloor t \rfloor$, alors

$$0 < t' \leqslant \delta \Rightarrow \mu u(t') = \mu x(t)$$

et

$$\delta < t' < 1 \text{ ou } t' = 0 \Rightarrow \mu u(t') = \mu y(t)$$

Donc $\forall\delta \in]0,1[$ et $\forall t \in \mathbb{R}$, $\mu x(t) \leqslant \mu u(t) \leqslant \mu y(t)$. D'autre part $f_{xy}(0) = y$ et $f_{xy}(1) = x$.

6.1.3.3. Définition : On appelle fermeture convexe d'une partie B de A(ℤ) l'ensemble

$$K(B) = \bigcup_{x,y \in B} [x , y]$$

Les notions de segments et de fermeture convexe sont étendues à $A(\mathbb{Z})^n$, en posant $(F_{XY}(\delta))_i = f_{X_iY_i}(\delta)$.

6.1.3.4. Proposition : Si P est un polyèdre de $A(\mathbb{Z})^n$, alors $K(P) = \tilde{P}$.

Démonstration : Soient $H = \{ X \in A(\mathbb{Z})^n \mid zX \leqslant b \}$ un demi-espace de $A(\mathbb{Z})^n$, X et Y deux points de H, $\delta \in [0,1]$ et $U = F_{XY}(\delta)$. Alors $\sup(zX , zY) \leqslant b$, et d'aprés la linéarité de F_{XY}, $zU \in [zX , zY]$. Donc, d'aprés la proposition 6.1.3.2, $zU \in [[\inf(zX,zY),\sup(zX,zY)]]$. Par suite $zU \leqslant b$ et U appartient à $\tilde{H}$. Donc $K(H) = \tilde{H}$ et il en est de même de tout polyèdre .

6.1.3.5. Théorème : Tout optimum local d'un programme linéaire (P,z) dans $A(\mathbb{Z})^n$ est un optimum global .

Démonstration : Soit X un optimum local du programme (P,z) et supposons qu'il existe Y dans P tel que $zY \geqslant zX$ et $zY \neq zX$. Alors le segment $]X , Y[$ est inclus dans $\tilde{P}$ (d'aprés 6.1.3.4) et coupe tout voisinage de X : En effet, ce segment est l'image de l'intervalle $]0,1[$ par l'application continue F_{XY}, il est donc connexe. Or z croit strictement avec δ le long du segment $]X , Y[$. Il en résulte que tout voisinage de X contient un point $X' \in \tilde{P}$ tel que $zX' \geqslant zX$ et $zX' \neq zX$, ce qui contredit l'hypothèse que X est un optimum local.

6.2. SYSTEMES D'INEQUATIONS SATURABLES

6.2.1. Position du problème

Soit P un polyèdre de $A(\mathbb{Z})^n$, défini par le système d'inéquations linéaires $MX \leqslant B$ (M matrice $A(\mathbb{Z})^n \to A(\mathbb{Z})^m$, $B \in A(\mathbb{Z})^m$).

Une inéquation $\Sigma_{i=1}^{n} a_i X_i \leqslant b$ sera dite saturable dans P s'il existe X dans P tel que $\Sigma_{i=1}^{n} a_i X_i = b$.

Une inéquation peut n'être pas saturable pour la raison que A n'est qu'un anneau (c'est le cas par exemple, de $2x \leqslant 1$), mais nous n'explorerons pas ce cas, qui se présente rarement - dans la pratique, les pseudo-évènements sont généralement inversibles - et qui pose un problème algébrique classique (cf. la programmation en nombres entiers). Par contre, le cas d'une inéquation non saturable du fait de la nature partielle de la relation d'ordre, est très fréquent et mérite d'être étudié : Il est clair qu'un système d'inéquations linéaires peut n'être composé que d'inéquations non saturables, puisque

$$x \leqslant a \;\&\; x \leqslant b \iff x \leqslant \inf(a , b)$$

et que , si a et b ne sont pas comparables, inf(a , b) n'est égal ni à a ni à b.

Le problème que l'on est naturellement amené à se poser est le suivant :

1) Etant donné un système fini d'inéquations linéaires S, peut-on trouver un système S', équivalent à S, et dont toutes les inéquations soient saturables ?

2) Dans l'affirmative, le système S' comporte-t-il toujours un nombre fini d'inéquations ?

La solution à ce problème serait intéressante à plus d'un titre :

- D'une part, le système minimal S', cernant de plus prés les solutions de S, nous donnerait plus d'informations sur celles-ci.
- D'autre part, la connaissance de S' est nécessaire pour trouver les solutions extrémales - "sommets" du polyèdre des solutions de S - dont l'importance est capitale pour traiter des problèmes d'optimisation, comme les programmes linéaires .

Disons, dés à présent, que nous n'avons pas résolu la question (1) dans sa généralité, et que la réponse à la question (2) semble devoir être négative.

6.2.2. L'approche du point fixe

Rappelons que :

- Une fonction f, totale d'un treillis L dans un treillis L' est dite continue au sens des treillis, si et seulement si pour toute partie dirigée X de L admettant une borne supérieure $\overline{x}$ (resp. une borne inférieure $\underline{x}$), l'ensemble $\{ f(x) \mid x \in X \}$ admet une borne supérieure $\overline{y}$ (resp. une borne inférieure $\underline{y}$) telle que $\overline{y} = f(\overline{x})$ (resp. $\underline{y} = f(\underline{x})$) .

- Un élément x de L est un point-fixe (resp. un pré-point-fixe) de la fonction f de L dans L, si et seulement si $x = f(x)$ (resp. $x \leq f(x)$) .

6.2.2.1. Proposition : Pout tout a,b dans A($\mathbb{Z}$), $[\![a , b]\!]$ (resp. $[\![a)$, $(b]\!]$) est un treillis complet (resp. un inf-demi-treillis complet, un sup-demi-treillis complet) c'est à dire que toute partie de $[\![a , b]\!]$

(resp. de [[a), de (b]]) admet une borne inférieure et une borne supérieure dans [[a , b]] (resp. une borne inférieure dans [[a), une borne supérieure dans (b]]).

Notons que cette propriété n'est pas vérifiée dans A($\mathbb{R}$). Par exemple, la suite

$$x^{(n)} = R^{\frac{2n-2}{2n-1}} - R^{\frac{2n-1}{2n}} \quad , n \in \mathbb{N}^*$$

est incluse dans [[0 , 1]] , mais n'a pas de borne supérieure dans A($\mathbb{R}$)

6.2.2.2. Proposition : Si f et g sont des fonctions de A($\mathbb{Z}$) dans lui-même, continues au sens des treillis, si $\Delta \in \mathbb{Z}$, alors les fonctions $\lambda x.\ R^{\Delta}x$, $\lambda x.\ f(x) + g(x)$, $\lambda x.\ \min(f(x) , g(x))$, $\lambda x.\ \max(f(x) , g(x))$, sont continues au sens des treillis.

6.2.2.3. Application : Soient $e^{(1)}$, $e^{(2)}$, ..., $e^{(m)}$ des évènements appartenant à E($\mathbb{N}^*$) , et soit P l'ensemble des solutions dans A($\mathbb{Z}$) du système d'inéquations :

$$x(1 - e^{(i)}) < b^{(i)} \quad , i = 1...m$$

Alors P est l'ensemble des pré-points-fixes de la fonction

$$f_P = \lambda x. \inf_{i=1..m} (b^{(i)} + e^{(i)}x)$$

qui est continue au sens des treillis, en vertu de la proposition 6.6.2.2 . D'autre part, d'aprés 4.2.1.2 et 4.4.2.1, on a :

$$x(1 - e^{(i)}) < b^{(i)} \Rightarrow \quad x < \frac{b^{(i)}}{1 - e^{(i)}}$$

Donc P est inclus dans (β]] , où

$$\beta = \inf_{i=1..m} \left(\frac{b^{(i)}}{1 - e^{(i)}} \right)$$

Puisque $(\beta\ ]]$ est un sup-demi-treillis complet, si P est non vide il admet une borne supérieure $\bar{\beta}$, qui, en vertu du théorème de Tarski, est le plus grand point fixe de f_P . De plus, la séquence $(f_P^k(\beta) \mid k \in \mathbb{N})$ est contenue dans le treillis complet $[[\ \bar{\beta}\ ,\ \beta\ ]]$, et converge vers $\bar{\beta}$, d'après le théorème de Kleene, et en vertu de la continuité de f_P .

P n'est généralement pas égal à $(\bar{\beta}\ ]]$, mais par ce procédé, on peut, sous réserve de savoir calculer la limite $\bar{\beta}$, ajouter au système d'inéquations une nouvelle contrainte, impliquée par le système initial, et saturable puisque $\bar{\beta}$ appartient à P .

6.2.2.4. Exemple : Considérons le système d'inéquations suivant :

$$\frac{x}{1 - R} \leqslant \frac{1}{1 - R^3} \quad , \quad x \leqslant 1 - \frac{R^4}{1 + R}$$

Aucune des deux inéquations n'est saturable . Mais en posant $y = x / (1-R)$, le système se ramène à $y \leqslant f(y)$, avec :

$$f(y) = \inf\left(\frac{1}{1 - R^3} \quad , \quad 1 - \frac{R^4}{1 + R} + Ry \right)$$

Avec les notations du §6.2.2.3 , on a :

$$\beta = \inf\ \left(\frac{1}{1 - R^3} \quad , \quad \frac{1}{1 - R} - \frac{R^4}{1 - R^2} \right) \quad = \quad \frac{1}{1 - R^3}$$

Calculons alors le plus grand point fixe de f inférieur à β :

$$\beta_0 = f^0(\beta) = \beta = \frac{1}{1 - R^3}$$

$$\beta_1 = f(\beta) = \inf\ \left(\frac{1}{1 - R^3} \quad , \quad 1 - \frac{R^4}{1 + R} + \frac{R}{1 - R^3} \right)$$

$$= 1 + \frac{R^3 + R^7}{1 - R^6} \quad \text{(cf. figure 18)}$$

$$\beta_2 = f^2(\beta) = f(\beta_1)$$

$$= \inf\ \left(\frac{1}{1 - R^3} \quad , \quad 1 - \frac{R^4}{1 + R} + R + \frac{R^4 + R^8}{1 - R^6} \right) = \beta_1$$

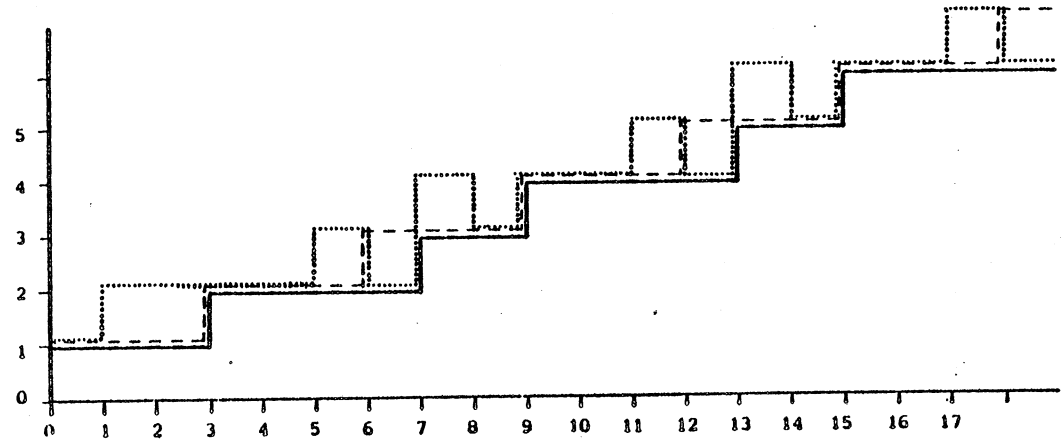


Figure 18

$$\beta_1 = \inf\left(\frac{1}{1 - R^3} , 1 - \frac{R^4}{1 + R} + \frac{R}{1 - R^3} \right)$$

La séquence a convergé vers $\bar{\beta} = 1 + (R^3 + R^7) / (1 - R^6)$ et la première inéquation du système initial peut être remplacée par l'inéquation saturable :

$$\frac{x}{1 - R} \leq 1 + \frac{R^3 + R^7}{1 - R^6}$$

L'application des théorèmes de points fixes nous permet donc, dans certains cas, heureusement assez fréquents dans la pratique, d'adjoindre à un système d'inéquations à une variable, une contrainte saturable. La même approche permet de démontrer le résultat, négatif, suivant :

6.2.2.5. Proposition : La projection de l'ensemble des solutions d'un système fini d'inéquations selon une de ses variables peut ne pas être caractérisable par un système fini d'inéquations.

Exemple : Soit $P = \{ (x,y,z) \mid x \leq z \leq y \ \& \ z(1-R) \geq 0 \}$ et soit P' la projection de P selon la troisième variable :

$$P' = \{ (x,y) \mid \exists z \text{ tel que } x \leq z \leq y \ \& \ z(1-R) \geq 0 \}$$

Pour effectuer la projection, cherchons la plus petite valeur $\underline{z}$ de z, telle que $(x,y,z) \in P$, x et y étant fixés . On a

$$z \geq \sup(x , Rz)$$

$\underline{z}$ est donc le plus petit point fixe de la fonction $\lambda z.\sup(x,Rz)$ plus grand que x . Evaluons itérativement ce plus petit point fixe. On obtient :

$$z_0 = x$$
$$z_1 = \sup(x , Rx)$$
$$- - - - - - - - - -$$
$$z_n = \sup_{0 \leq i \leq n} (R^i x)$$

Soit finalement, $\underline{z} = \sup_{i \in \mathbb{N}} (R^i x)$. La projection P' ne peut donc être caractérisée que par le système infini :

$$\forall i \in \mathbb{N},\ y \geq R^i x$$

Il s'agit donc de l'exemple, paradoxal, d'un polyèdre dont une projection n'est pas un polyèdre.

6.2.3. L'approche arithmétique

Considérons un système d'inéquations homogènes dans $A(\mathbb{Z})$:

$$P = \{ x \mid a^{(i)} x \geq 0 \ , \ i = 1...m \}$$

Alors

$$x \in P \iff \exists e^{(1)}, \ldots, e^{(m)} \in E(\mathbb{Z}), \text{ tels que } \frac{a^{(i)} x}{1 - R} = e^{(i)}$$

Soit encore, en supposant les $a^{(i)}$ inversibles,

$$x \in P \iff \exists\, e^{(i)} \in E(\mathbb{Z}),\ i = 1...m, \text{ tels que } x = e^{(i)} \frac{1 - R}{a^{(i)}}$$

P est donc l'ensemble des multiples communs, par des évènements, d'un ensemble $\{ \alpha^{(i)} = (1-R) / a^{(i)} , \ i = 1...m \}$. Si l'on dénote par $I(\alpha)$ l'ensemble

$$I(\alpha) = \{ e \in E(\mathbb{Z}) \mid e \frac{\alpha_1}{\alpha_i} \in E(\mathbb{Z}), \forall i = 2..m \}$$

on a alors $P = \{ e\alpha_1 \mid e \in I(\alpha) \}$. Or $I(\alpha)$ est un idéal de $E(\mathbb{Z})$:

. $e,f \in I(\alpha) \Rightarrow e + f \in I(\alpha)$

. $e \in I(\alpha), f \in E(\mathbb{Z}) \Rightarrow ef \in I(\alpha)$

On est donc amené à étudier les idéaux du demi-anneau $E(\mathbb{Z})$. En particulier, les questions importantes sont les suivantes:

. Tout idéal de $E(\mathbb{Z})$ est-il principal ? C'est à dire, pour tout idéal I de $E(\mathbb{Z})$, existe-t-il un générateur $g(I) \in E(\mathbb{Z})$ tel que $I = \{ e.g(I) \mid e \in E(\mathbb{Z}) \}$? Si tel était le cas, tout système homogène à une variable se ramènerait à une inéquation

$$\frac{x(1 - R)}{\alpha_1 g(I(\alpha))} \geq 0$$

Le contre-exemple 6.2.3.1 répond négativement à cette question.

. Tout idéal de $E(\mathbb{Z})$ est-il de type fini, c'est à dire est-il la somme d'un nombre fini d'idéaux principaux ? Si tel était le cas, il existerait $g_1, g_2, \ldots, g_k$ dans $E(\mathbb{Z})$, tels que

$$I(\alpha) = \{ \sum_{i=1}^{k} e_i g_i \mid e_i \in E(\mathbb{Z}), \ i = 1...k \}$$

et on aurait donc

$$x \in P \iff x = \sum_{i=1}^{k} x_i \quad \text{avec} \quad \frac{x_i(1 - R)}{g_i \alpha_1} \geq 0$$

Le contre-exemple 6.2.3.2, du à Ch. Reutenauer, répond négativement à cette question, ce qui clôt, malheureusement, le problème de trouver un système saturable fini équivalent à un système d'inéquations donné .

6.2.3.1. Proposition : L'intersection de deux idéaux principaux de $E(\mathbb{Z})$ n'est pas nécessairement un idéal principal.

Contre-exemple : Considérons les idéaux principaux suivants :

$$I_1 = (1 + R).E = \{ (1 + R)e \mid e \in E \}$$
$$I_2 = (1 + R + R^2).E = \{ (1 + R + R^2)e \mid e \in E \}$$

Alors

$x \in I_1 \cap I_2$

$\iff \exists e,f \in E$ tels que $x = e(1 + R) = f(1 + R + R^2)$

$\iff \exists f \in E$ tel que

$$f \frac{1 + R + R^2}{1 + R} \in E \quad \text{et} \quad x = f(1 + R + R^2)$$

$$\iff \exists f \in E \text{ tel que } f \frac{1 - R^3}{1 - R^2} \in E \quad \text{et} \quad x = f(1 + R + R^2)$$

$\iff \exists g \in A$ tel que $g(1 - R^3) \in E$ et $g(1 - R^2) \in E$ et $x = g(1 - R^2)(1 + R + R^2)$

$I_1 \cap I_2$ est donc engendré par les séries $g = \sum_{i=0}^{\infty} G_i R^i$ telles que :

. $\forall i \geq 3$, $G_i \geq G_{i-3}$

. $\forall i \geq 2$, $G_i \geq G_{i-2}$

On montre qu'un système générateur minimal de cet ensemble est composé de deux éléments $g' = 1 + R^2/(1-R)$ et $g'' = 1/(1-R)$ qui sont les générateurs des solutions de l'équation aux différences :

$$G_i = \max (G_{i-2} , G_{i-3}) \quad , \quad i \geq 3$$

En d'autres termes, $1 + R$ et $1 + R + R^2$ ont deux multiples communs indécomposables dans E, qui sont :

$$x' = (1 + R^3)(1 + R + R^2) \quad \text{et} \quad x'' = (1 + R)(1 + R + R^2)$$

et $(1 + R).E \cap (1 + R + R^2).E = x'.E + x''.E$

Cette situation, où l'intersection de deux idéaux principaux n'est pas un idéal principal, mais est un idéal de type fini est cependant encore un cas favorable, comme le montre la proposition suivante .

6.2.3.2. Proposition [Reutenauer] : L'intersection de deux idéaux principaux de $E(\mathbb{Z})$ n'est pas nécéssairement un idéal de type fini.

Contre-exemple : Considérons l'ensemble MC des multiples communs, par un évènement, de $x' = 1 + R$ et $x'' = 1/(1-R^2)$.

Si $x = \sum_{n\geq 0} X_n R^n \in MC$, alors:

(1) $\forall n \geq 2$, $X_n \geq X_{n-2}$

(2) $\forall n \geq 0$, $\sum_{0\leq i\leq n} (-1)^i X_{n-i} \geq 0$

Pour tout $k \in \mathbb{N}$ posons

$$y(k) = (1 + R^{2^{k+3}}) / (1 - R) + R^{2^{k+1}}$$

$$= \sum_{n=0}^{2^k} R^n + 2R^{2^{k+1}} + R^{2^{k+2}} + \sum_{n\geq 2^{k+3}} 2R^n$$

Alors, $y(k) \in MC$ puisque

$$\frac{y(k)}{1+R} = \frac{1 - R^{2^{k+2}}}{1 - R^2} + \frac{R^{2^{k+1}} + R^{2^{k+3}}}{1 - R^2} \in E$$

$$y(k)(1 - R^2) = 1 + R + R^{2^{k+1}} + R^{2^{k+4}} \in E$$

Supposons alors que MC admette un ensemble fini $G = \{g^{(1)} \ldots g^{(\ell)}\}$ de générateurs. Sans perte de généralité, on peut supposer que les éléments de G sont de la forme :

$$g^{(i)} = \sum_{n\geq 0} G_n^{(i)} R^n \quad \text{avec } G_0^{(i)} > 0$$

Alors puisque, G est fini, il existe $y = y(k) \notin G$. On a

$$y = \sum_{i=1}^{\ell} e^{(i)} g^{(i)}$$

et l'un des $e^{(i)}$ a un terme constant non nul. Donc,

$$y = g^{(i)} + z \text{ avec } z \neq 0 \text{ et } z \in MC$$

Donc $g^{(i)} \trianglelefteq y$, et $G_0^{(i)} = G_1^{(i)} = 1$. Par suite, tous les $G_n^{(i)}$ sont plus grands que 1 . D'autre part $g^{(i)} \trianglelefteq y$ entraine $G_{2k+1}^{(i)} = 1$ ou 2 . Montrons que si $G_{2k+1}^{(i)} = 2$ alors $g^{(i)} = y$ et que si $G_{2k+1}^{(i)} = 1$ alors $z \in MC$:

. Si $G_{2k+1}^{(i)} = 2$, comme $g^{(i)}$ satisfait (1), on a $G_{2k+1+2p}^{(i)} = 2$ pour tout p . Soit n le plus petit indice, plus grand que 2k+3, tel que $G_n^{(i)} = 1$. Un tel indice existe, puisque $g^{(i)} \neq y$, et de plus n est pair. Mais alors

$$\sum_{j=0}^{n} (-1)^j G_{n-j}^{(i)} = -1$$ et $g^{(i)}$ ne satisfait pas (2) .

. Si $G_{2k+1}^{(i)} = 1$, alors $z = R^{2k+1} + \sum_{n \geq 2k+3} Z_n R^n$, et z ne satisfait pas (2) .

L'hypothèse de l'existence d'un ensemble fini de générateurs de MC aboutit donc à une contradiction .

CHAPITRE 7

TRANSFORMEE DISCRETE ET ANALYSE ASYMPTOTIQUE

Les difficultés rencontrées dans la manipulation formelle des systèmes d'inéquations linéaires en pseudo-évènements, nous conduisent à étudier des méthodes d'analyse approchée. Dans ce chapitre nous explorerons la voie consistant à étudier le fonctionnement en moyenne des systèmes (nombre total d'occurrences, période moyenne d'un évènement ...) ce qui nous permettra de définir des méthodes systématiques d'analyse approchée supérieurement, ne fournissant que des conditions nécessaires. Pour cela, nous tirerons parti des résultats classiques concernant les informations que fournissent les transformées de Laplace, au voisinage de zéro, sur le comportement de leurs originaux à l'infini.

7.1. TRANSFORMEE DISCRETE

Nous avons déja mentionné l'analogie entre notre définition des pseudo évènements en termes de séries formelles, et les techniques utilisant une transformée discrète, classiquement mises en oeuvre pour la résolution des équations aux différences finies [Jury],[Karr]. Cependant, ces techniques n'ont jamais été étendues, à notre connaissance, au traitement d'inéquations.

7.7.1. Définition : A tout pseudo évènement $a = \sum_{n=1}^{\#a} \bar{a}_n R^{a_n}$, on associe la fonction ϕ_a, de $\mathbb{R}^+$ dans $\mathbb{R}$, définie par:

$$\phi_a(r) = \sum_{n=1}^{\#a} \bar{a}_n r^{a_n}$$

ϕ_a est généralement une fonction partielle, dont le domaine de définition est un intervalle $[0, r_a[$, où r_a est le rayon de convergence de la série.

7.1.2. Théorème : Si a est un pseudo évènement positif, alors ϕ_a est positive sur l'intervalle $[0, \min(1, r_a)[$. La réciproque est fausse.

Démonstration: Si ϕ_a converge sur $[0 , r_a[$, il en est de même de $\phi_a(e^{-x}) / x$ sur $]\max(0,x_a) , +\infty]$, avec $r_a = e^{-x_a}$. Mais $\phi_a(e^{-x}) / x$ n'est autre que la transformée de Laplace L_a de la fonction compteur μa pour l'abscisse réelle x:

$$L_a = \lambda p. \int_{-\infty}^{+\infty} \mu_a(t)\, e^{-pt} dt$$

qui existe donc sur $\{ p \mid Re(p) > \max(0,x_a) \}$. Si μa est positive, $L_a(x)$ est aussi positive pout tout x réel de ce domaine. Il en est de même de $\phi_a(e^{-x})$ pour tout x positif de ce domaine, et donc de $\phi_a(r)$ sur $[0 , \min(1,r_a)[$.

7.1.3. Application : Revenons à l'exemple du §5.4.1. Nous voulons trouver une condition nécessaire pour que le système S ci-dessous admette une solution dans $E(\mathbb{R})^2$ (on peut admettre maintenant des délais non entiers, tous les résultats de ce chapitre étant applicables au temps continu) :

$$S = \begin{cases} e_i(1 - R^{\Delta_i + \delta_i}) < 1 \quad (i=1,2) \\ e_1(1 - R^{\delta_1}) + e_2(1 - R^{\delta_2}) = 1 \end{cases}$$

Par élimination de e_2, on obtient :

$$S \Rightarrow \begin{cases} e_1(1 - R^{\Delta_1+\delta_1}) \leq 1 \\ \dfrac{R^{\delta_2}(1 - R^{\Delta_2})}{1 - R^{\delta_2}} \leq e_1 \dfrac{(1 - R^{\delta_1})(1 - R^{\Delta_2+\delta_2})}{1 - R^{\delta_2}} \end{cases}$$

Soit encore, en multipliant les inéquations précédentes par des évènements adéquats :

$$S \Rightarrow$$

$$\frac{R^{\delta_2}(1 - R^{\Delta_2})}{(1 - R^{\delta_2})(1 - R^{\delta_1})(1 - R^{\Delta_2+\delta_2})} \leq \frac{e_1}{1 - R^{\delta_2}} \leq \frac{1}{(1 - R^{\delta_2})(1 - R^{\Delta_1+\delta_1})}$$

Donc, une condition nécéssaire pour que S admette une solution est que

$$\frac{R^{\delta_2}(1 - R^{\Delta_2})}{(1 - R^{\delta_2})(1 - R^{\delta_1})(1 - R^{\Delta_2+\delta_2})} \leq \frac{1}{(1 - R^{\delta_2})(1 - R^{\Delta_1+\delta_1})}$$

Cette condition, relativement complexe, serait difficile à interpréter pour choisir effectivement les délais. Cependant, le passage en transformée discrète fournit :

$$S \Rightarrow \forall r \in [0 , \min(1 , \bar{r})[,$$

$$\frac{r^{\delta_2}(1 - r^{\Delta_2})}{(1 - r^{\delta_2})(1 - r^{\delta_1})(1 - r^{\Delta_2+\delta_2})} \leq \frac{1}{(1 - r^{\delta_2})(1 - r^{\Delta_1+\delta_1})}$$

où $\bar{r}$ est le minimum des rayons de convergence des séries constituant les deux membres de l'inéquation. Or, on remarque que ces rayons de convergence sont tous deux égaux à 1, puisque les numérateurs sont finis, et les termes de la forme $1 / (1 - r^{\alpha})$, $\alpha \in \mathbb{R}^{*+}$, ont pour rayon de convergence 1. De plus, les termes en $1-r^{\alpha}$ sont positifs sur le domaine $[0,1[$, et les simplifications algébriques usuelles des inéquations sont alors possibles. Donc :

$$S \Rightarrow \forall r \in [0,1[,$$

$$\frac{r^{\delta_2}(1 - r^{\Delta_2})}{1 - r^{\delta_1}} \leq \frac{1 - r^{\Delta_2+\delta_2}}{1 - r^{\Delta_1+\delta_1}}$$

En particulier, cette inégalité doit être vérifiée au voisinage de $r = 1$. Or, dans ce voisinage, on a:

$$\frac{r^{\delta_2}(1 - r^{\Delta_2})}{1 - r^{\delta_1}} \sim \frac{\Delta_2}{\delta_1} \quad \text{et} \quad \frac{1 - r^{\Delta_2+\delta_2}}{1 - r^{\Delta_1+\delta_1}} \sim \frac{\Delta_2 + \delta_2}{\Delta_1 + \delta_1}$$

Donc:

$$S \Rightarrow \frac{\Delta_2}{\delta_1} \leq \frac{\Delta_2 + \delta_2}{\Delta_1 + \delta_1} \Leftrightarrow \Delta_1.\Delta_2 \leq \delta_1.\delta_2$$

On a ainsi trouvé, de manière systématique, une condition nécessaire pour que S admette un solution. Cette condition n'est pas suffisante puisque la condition nécessaire et suffisante prouvée au §5.4.1 était $\Delta_2 < \delta_1$ et $\Delta_1 < \delta_2$.

Comme nous allons le voir, la condition nécessaire obtenue est exactement celle que l'on obtiendrait en appliquant la méthode proposée par J. Sifakis pour étudier le fonctionnement permanent des réseaux de Pétri temporisés [Sifakis]. Nous allons maintenant étudier les relations qui existent entre cette méthode et la notre.

7.2. ANALYSE DU COMPORTEMENT PERMANENT DES RESEAUX DE PETRI TEMPORISES

Nous rappelons dans ce paragraphe, les principaux éléments de la méthode de Sifakis. On ne considèrera que des réseaux temporisés, asynchrones et généralisés, selon leur définition matricielle (cf.§5.3.1) .

7.2.1. Semi-flots dans un graphe biparti [Memmi]

7.2.1.1. Définitions : Soit $G = (C^+, C^-)$ un n,m-multigraphe biparti, et $C = C^+ - C^-$.

. On appelle p-semi-flot (resp. p-sous-semi-flot) de G, tout vecteur Y de $\mathbb{N}^m$ tel que $Y^T C = 0$ (resp. $Y^T C \leq 0$).

. On appelle t-semi-flot (resp. t-sous semi-flot) de G, tout vecteur X de $\mathbb{N}^n$ tel que $CX = 0$ (resp. $CX \leq 0$).

7.2.1.2. Propriété : Chacun des ensembles définis ci-dessus possède une base finie, c'est à dire un sous-ensemble fini (Z_i) tel que tout élément Z de l'ensemble s'écrive:

$$Z = \Sigma \alpha_i . Z_i \quad , \alpha_i \in \mathbb{N}$$

7.2.2. La méthode de Sifakis

Le problème étudié dans [Sifakis] est la recherche de conditions nécessaires pour qu'un RPT admette un fonctionnement avec M(t) périodique. Soit un tel fonctionnement périodique, de période α. On a:

$$M(t+\alpha) = M(t) + (C^+ - C^-) \sum_{t \leq t_k < t+\alpha} X(k) = M(t)$$

Appelons intensité le n-vecteur $J = \frac{1}{\alpha} \sum_{t \leq t_k < t+\alpha} X(k)$.

Une première condition nécessaire est donc l'existence d'un vecteur intensité J de $(\mathbb{R}^+)^n$, vérifiant $(C^+ - C^-)J = 0$.

Une deuxième condition, plus difficile à dériver, est que, pour tout Y de la base des p-semiflots de $C = C^+ - C^-$, on doit avoir:

$$Y^T [\Delta] C^+ J \leq Y^T M_0$$

où $[\Delta]$ est la matrice diagonale m×m définie par $[\Delta]_{ii} = \Delta_i$, (i=1...m) .

Ces conditions sont utilisées pour étudier les performances des systèmes modélisables par RPT.

7.2.3. Exemple d'application

Appliquons cette méthode à l'exemple des §§5.4.1 et 7.1.3 : Cet exemple correspond au RPT de la figure 19 . Cherchons les conditions pour que ce réseau ait un fonctionnement permanent d'intensités $(j_{e_1}, j_{f_1}, j_{e_2}, j_{f_2})$. La condition CJ = 0 donne :

$$j_{e_1} = j_{f_1} \quad , \quad j_{e_2} = j_{f_2} \quad , \quad j_{e_1} + j_{e_2} = j_{f_1} + j_{f_2}$$

La base des p-semi flots est composée de trois vecteurs :

$$(1\,1\,0\,0\,0)\,,\ (0\,0\,0\,1\,1)\,,\ (0\,1\,1\,1\,0)$$

donnant les conditions

$$\delta_1 j_{e_1} + \Delta_1 j_{f_1} \leq 1$$

$$\delta_2 j_{e_2} + \Delta_2 j_{f_2} \leq 1$$

$$\delta_1 j_{e_1} + \Delta_2 j_{e_2} \leq 1$$

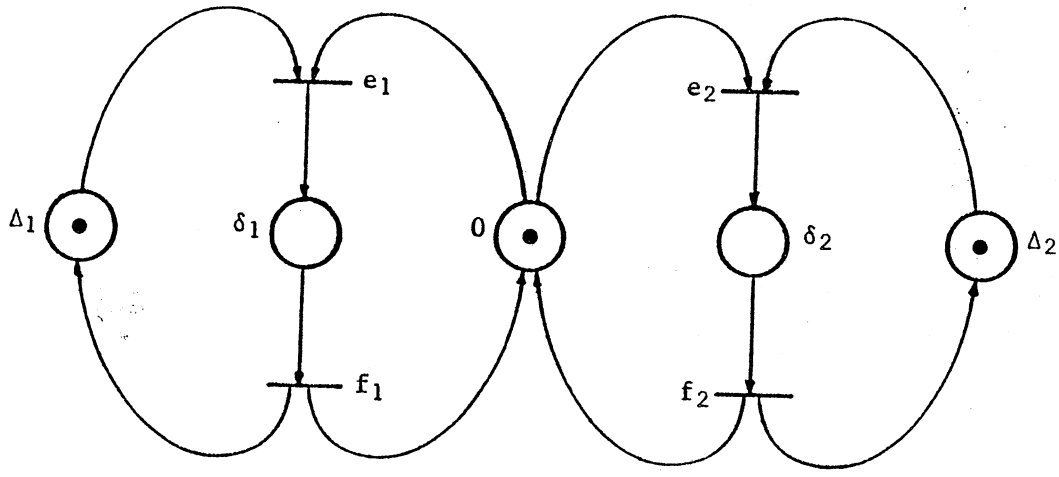


Figure 19
RPTS de la ressource exclusive

soit encore

$$(\delta_1 + \Delta_1) j_{e_1} \leq 1$$

$$(\delta_2 + \Delta_2) j_{e_2} \leq 1$$

$$\delta_1 j_{e_1} + \delta_2 j_{e_2} \leq 1$$

Cherchons un fonctionnement à utilisation maximum de la ressource :

$$\delta_1 j_{e_1} + \delta_2 j_{e_2} = 1$$

L'élimination de j_{e_2} donne :

$$(\delta_1 + \Delta_1) j_{e_1} \leq 1$$

$$\frac{(\delta_2 + \Delta_2)}{\delta_2} \leq 1 + \frac{\delta_1(\delta_2 + \Delta_2)}{\delta_2} j_{e_1}$$

ou :

$$(\delta_1 + \Delta_1)\ j_{e_1} \leq 1 \quad \text{et} \quad \Delta_2 \leq \delta_1(\delta_2 + \Delta_2)\ j_{e_1}$$

Soit la condition nécessaire :

$$\Delta_2(\delta_1 + \Delta_1) \leq \delta_1(\delta_2 + \Delta_2)$$

ou encore $\Delta_1\Delta_2 \leq \delta_1\delta_2$.

L'analogie avec notre solution (§7.1.3) est frappante, et motive les développements qui suivent.

7.3. INTENSITES ET TRANSFORMEE DISCRETE

Nous allons montrer que notre modélisation des RPT en termes d'évènements permet de retrouver et de généraliser la méthode de Sifakis. Au préalable, il nous faut énoncer quelques résultats complémentaires concernant les transformées discrètes.

7.3.1. Définition : Un pseudo évènement a est d'ordre γ ($\gamma \in \mathbb{R}^{*+}$) si et seulement si il existe un réèl non nul $J_a^{(\gamma)}$, tel que $\mu a(t)$ soit équivalent, à l'infini, à $J_a^{(\gamma)} / \Gamma(\gamma+1)$, où Γ est la factorielle généralisée. $J_a^{(\gamma)}$ est alors l'intensité d'ordre γ de a. On appellera simplement intensité, l'intensité d'ordre 1.

Un pseudo-évènement a est d'ordre 0 si et seulement si il existe un réèl $J_a^{(0)}$ tel que

$$\lim_{t\to\infty} \frac{1}{t} \int_0^t \mu a(\tau)\, d\tau = J_a^{(0)}$$

L'intensité d'ordre 0 peut être vue comme une valeur moyenne.

L'étude des intensités peut se mener à partir des transformées discrètes. Il est connu, en effet, que le comportement d'une transformée de Laplace au voisinage de l'origine fournit des informations sur le comportement de son original à l'infini.

7.3.2 Théorème : Si a est un pseudo-évènement d'ordre γ ($\gamma \geq 0$), alors

$$\lim_{r\to 1} (1-r)^{\gamma} \phi_a(r) = J_a^{(\gamma)}$$

Ce théorème dérive directement des théorèmes Abéliens en transformée de Laplace [Widder].
Remarquons que la réciproque est vraie:

- pour $\gamma > 0$, si a est un évènement (théorème de Karamata)
- pour $\gamma = 0$, si μa est bornée (théorème de Wiener)

7.4. Analyse en intensité des réseaux de Pétri temporisés

7.4.1. Définition : Un RPT admet un fonctionnement d'intensité $J^{(\gamma)} \in \mathbb{R}^{+n}$, $\gamma \in \mathbb{R}^{+}$, si et seulement si il existe un fonctionnement $\hat{X} \in E^n$ du réseau, tel que, pour tout i=1...n, $\hat{X}_i$ admette l'intensité d'ordre γ, $J_i^{(\gamma)}$.

7.4.2. Théorème : Si le RPT (C^+, C^-, M_0, Δ) admet un fonctionnement d'intensité $J^{(\gamma)}$ alors:

a) $C^+ J^{(\gamma)} \geq C^- J^{(\gamma)}$

b) Si de plus $\gamma=1$, alors pour tout Y de la base des p-sous-semi-flots de $C = C^+ - C^-$, on a:

$$Y^T[\Delta]C^+J^{(1)} \leq Y^T M_0$$

où $[\Delta]$ est la matrice diagonale m×m telle que $[\Delta]_{ii} = \Delta_i$.

Démonstration: a) Soit $\hat{X}$ un fonctionnement du RPT. D'après 5.3.1.2, on a:

$$M_0 + [R^{\Delta}]C^+\hat{X} \geq C^-\hat{X} \qquad (1)$$

Donc, d'aprés 7.1.2, pour tout $r \in [0,1[$,

$$M_0 + ([r^{\Delta}]C^+ - C^-)\,\phi_{\hat{X}}(r) \geq 0$$

où $\phi_{\hat{X}}(r)$ est le vecteur des transformées, et $[r^{\Delta}]$ est la matrice diagonale m×m telle que $[r^{\Delta}]_{ii} = r^{\Delta_i}$. Donc, pour tout $r \in [0,1[$,

$$(1-r)^{\gamma}M_0 + ([r^{\Delta}]C^+ - C^-)(1-r)^{\gamma}\phi_{\hat{X}}(r) \geq 0$$

et, par passage à la limite, $(C^+ - C^-)J^{(\gamma)} \geq 0$

b) Soit Y un p-sous-semi-flot de C. Alors $Y^T C^+ \leq Y^T C^-$ et $Y^T C^+\hat{X} \leq Y^T C^-\hat{X}$, puisque $\hat{X}$ est un vecteur d'évènements. D'autre part, comme $Y \geq 0$, le produit scalaire par Y conserve l'ordre, et de (1) on déduit:

$$Y^T M_0 + Y^T[R^{\Delta}]C^+\hat{X} - Y^T C^-\hat{X} \geq 0$$

En majorant $Y^T C^-\hat{X}$ par $Y^T C^+\hat{X}$, ceci entraine:

$$Y^T M_0 + Y^T([R^{\Delta}] - I)C^+\hat{X} \geq 0$$

où I est la matrice unité m×m. On peut encore écrire:

$$Y^T M_0 + Y^T([R^{\Delta}] - I)\frac{1}{1-R}C^+\hat{X}(1-R) \geq 0$$

Cette relation est encore vraie en transformée discrète sur $[0,1[$, et, par passage à la limite, puisque:

$$\lim_{r\to 1}\frac{I - [r^{\Delta}]}{1-r} = [\Delta]$$

il vient:

$$Y^T M_0 - Y^T[\Delta]C^+J^{(1)} \geq 0$$

7.4.3. Remarques : a) On peut trouver par cette méthode une autre condition nécessaire:

$$Y^T[\Delta]C^-J^{(1)} \leq Y^T M_0 \qquad (2)$$

En effet, l'équation du réseau peut s'écrire, de manière équivalente:

$$[R^{-\Delta}]M_0 + C^+\hat{X} \geq [R^{-\Delta}]C^-\hat{X}$$

D'où:

$$Y^T[R^{-\Delta}]M_0 + Y^TC^+\hat{X} \geq Y^T[R^{-\Delta}]C^-\hat{X}$$

$Y^T C^+ \hat{X}$ est majoré par $Y^T C^- \hat{X}$, et le passage à la limite en transformée discrète donne le résultat annoncé. Cependant, cette nouvelle condition est redondante puisque $Y^T[\Delta] \geq 0$ et $C^+J^{(1)} \geq C^-J^{(1)}$ entrainent $Y^T[\Delta]C^+J^{(1)} \geq Y^T[\Delta]C^-J^{(1)}$, et donc $Y^T[\Delta]C^+J^{(1)} \leq Y^T M_0$ entraine (2).

b) En ce qui concerne la comparaison entre notre méthode et celle de Sifakis, remarquons tout d'abord que celui-ci ne

s'interesse qu'aux fonctionnements bornés de réseaux consistants. La condition de borné implique l'égalité des flux ($C^+ J = C^- J$) et d'autre part, dans le cas des réseaux consistants - c'est à dire tels que l'équation précédente admette une solution J dont toutes les composantes sont strictement positives - on peut montrer que les ensembles des p-sous-semi-flots et des p-semi-flots sont égaux. Seuls les p-semi-flots sont donc considérés. Notre méthode s'applique aussi bien aux réseaux non consistants, et dans ce cas, la prise en compte des p-sous-semi-flots peut fournir des conditions supplémentaires, comme le montre l'exemple suivant:

Considérons le graphe (C^+, C^-) (cf.figure 20), défini par:

$$C^+ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \qquad C^- = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

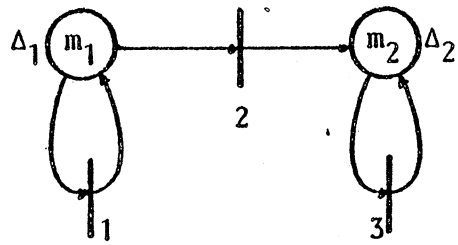


Figure 20
RPT non consistant

Un p-sous-semi-flot (y_1,y_2) de (C^+,C^-) vérifie $y_1 > y_2 > 0$. La base des p-sous-semi-flots est donc $\{(1,0) , (1,1)\}$. Les p-semi-flots (z_1,z_2) vérifient $z_1 = z_2 > 0$, et la base des semi-flots est donc $\{(1,1)\}$. Si un vecteur d'intensités (u,v,w) existe, il vérifie $u > 0$, $v = 0$, $w > 0$. Soient (Δ_1,Δ_2) les délais et (m_1,m_2) le marquage initial. On obtient:

. Sur la base des p-semi-flots, la condition suivante:

$$\Delta_1 u + \Delta_2 w \leqslant m_1 + m_2$$

. Sur la base des p-sous-semi-flots, les deux conditions, nécessaires et indépendantes:

$$\Delta_1 u \leqslant m_1$$

$$\Delta_1 u + \Delta_2 w \leqslant m_1 + m_2$$

7.5. ANALYSE EN INTENSITE DES RESEAUX TEMPORISES A CONTRAINTES

Les méthodes asymptotiques développées précédemment pour les RPT se généralisent directement aux RPTC:

7.5.1. Théorème : Soit le RPTC $\{(C^+, C^-, M_0, \Delta)\ ,\ (C'^+, C'^-, M'_0, \Delta')\}$. Posons:

$$C''^+ = \begin{bmatrix} C^+ \\ C'^+ \end{bmatrix} \quad C''^- = \begin{bmatrix} C^- \\ C'^- \end{bmatrix} \quad \Delta'' = \begin{bmatrix} \Delta \\ -\Delta' \end{bmatrix} \quad M''_0 = \begin{bmatrix} M_0 \\ -M'_0 \end{bmatrix}$$

Si le RPTC admet une intensité $J^{(\gamma)}$ d'ordre γ, alors:

$$C''^+ J^{(\gamma)} \geqslant C''^- J^{(\gamma)}$$

Si, de plus $\gamma=1$, alors, pour tout Y" de la base des p-sous-semi-flots de (C''^+, C''^-) on a:

$$Y''^T M''_0 \geqslant Y''^T [\Delta''] C''^+ J^{(1)}$$

et

$$Y''^T M''_0 \geqslant Y''^T [\Delta''] C''^- J^{(1)}$$

7.5.2. Remarques : a) On ne peut plus démontrer, comme dans la remarque §7.4.3.a , que la deuxième condition est redondante, du fait que, si $Y"$ est positif, en général $Y"^{T}[\Delta"]$ ne l'est pas.

b) Il y a, à priori, trois types d'éléments dans la base des p-sous-semi-flots de $(C"^{+},C"^{-})$, qui sont:

. les vecteurs $\binom{Y}{0}$, où Y est un p-sous-semi-flot de (C^{+},C^{-}) ;

les vecteurs $\binom{0}{Y'}$, où Y' est un p-sous-semi-flot de (C'^{+},C'^{-}) ;

. les vecteurs $\binom{Y}{Y'}$, où Y et Y' ne sont pas des p-sous-semi-flots de leurs graphes respectifs.

Les deux premiers types conduisent à des analyses séparées du réseau et de l'anti-réseau, fournissant respectivement des bornes supérieures et inférieures des intensités. Les vecteurs du troisième type permettent parfois de trouver de nouvelles conditions, qui ne sont ni des bornes supérieures, ni des bornes inférieures.

7.5.3 Exemple d'application

L'exemple suivant vise à montrer le type de résultats que l'on peut attendre d'une analyse en intensité des RPTC . Il montre aussi les précautions qu'il faut prendre lorsqu'on modélise un système en RPTC.

Considérons le réseau de la figure 21 . Le RPT dessiné en traits pleins peut être vu comme un système à un producteur et deux consommateurs, communiquant par un tampon de taille N_0. La durée de production est δ_p, celle de consommation est δ_{c_i} pour le consommateur i (i=1..2).

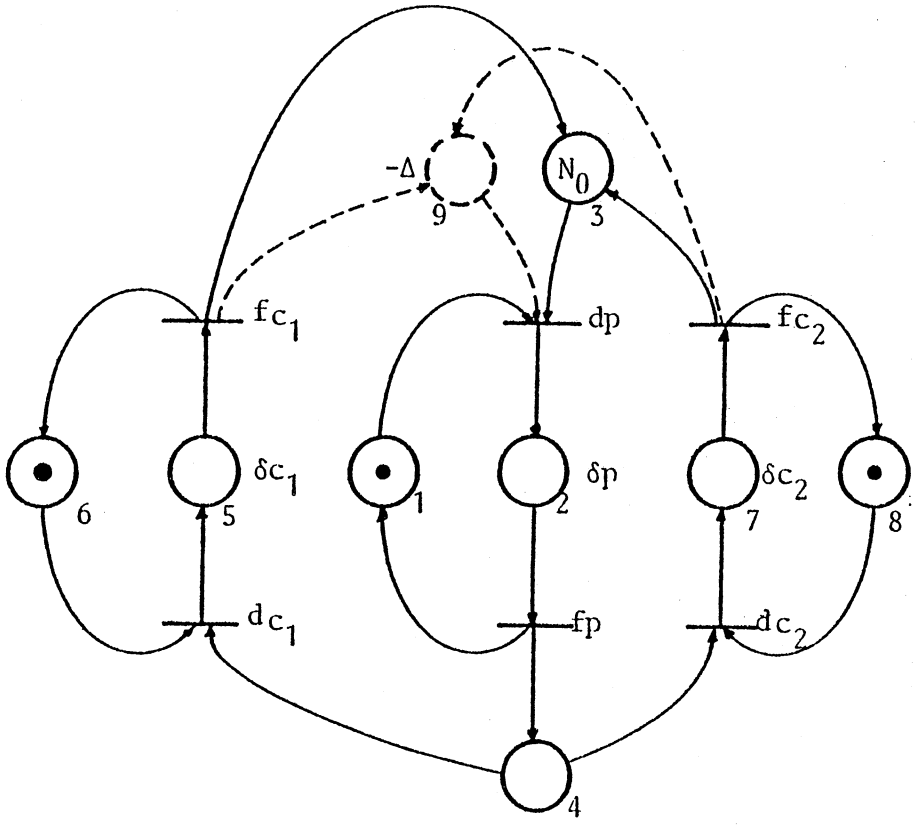


Figure 21
RPTC d'un système producteur-consommateurs

On a représenté en pointillés, sous forme d'anti-réseau, la contrainte d'obligation: Tout début de production doit être suivi d'une fin de consommation dans un intervalle de temps Δ.

L'analyse en intensité donne les résultats suivants:

La condition CJ > 0 donne:

$$j_{dp} = j_{fp} = j_p$$

$$j_{dc_i} = j_{fc_i} = j_{c_i}, \quad i=1,2$$

$$j_p = j_{c_1} + j_{c_2}$$

La base des p-sous-semi-flots comprend 5 éléments:

$$
\begin{array}{ccccccccc}
(1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0) \\
(0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0) \\
(0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0) \\
(0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0) \\
(0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1)
\end{array}
$$

Les quatre premiers éléments appartiennent au RPT proprement dit, le cinquième étant du type mixte réseau/anti-réseau. Ces p-sous-semi-flots sont en fait des semi-flots, le réseau étant consistant. Il s'ensuit que les deux types de conditions du théorème 7.5.1 sont équivalents. On trouve alors:

$$\delta_p \cdot j_p \leq 1$$

$$\delta_{c_i} \cdot j_{c_i} \leq 1 \ , \quad i=1,2$$

$$\delta_p \cdot j_p + \delta_{c_1} \cdot j_{c_1} + \delta_{c_2} \cdot j_{c_2} \leq N_0$$

$$\delta_p \cdot j_p + \delta_{c_1} \cdot j_{c_1} + \delta_{c_2} \cdot j_{c_2} - \Delta \cdot j_p \leq 0$$

Les quatre premières conditions sont celles de la méthode de Sifakis. Seule la dernière fait intervenir le temps de réponse Δ et est propre à la méthode généralisée. L'usage que l'on peut faire de ces conditions peut-être, par exemple, connaissant les délais, de déterminer un domaine polyédral du plan j_{c_1}, j_{c_2}, en dehors duquel (puisqu'il s'agit de conditions nécessaires) il n'y a certainement pas de fonctionnement en intensité possible:

La dernière condition peut s'écrire:

$$(\Delta - \delta_p - \delta_{c_1}) j_{c_1} + (\Delta - \delta_p - \delta_{c_2}) j_{c_2} \geq 0$$

Les j_{c_i} (i=1,2) étant, par essence, positifs, cette condition est irréalisable dés que

$$\Delta < \delta_p + \delta_{c_i} \ , \ i=1,2$$

Cette conclusion est logique: En effet les temps $\delta_p + \delta_{c_i}$ représentent les temps de traitement minimaux que subit un objet entre son début de

production et la fin de sa consommation par l'un ou l'autre des consommateurs. Si ces durées sont toutes deux supérieures à Δ, le temps de réponse exigé ne pourra certainement pas être tenu. En revanche, cette condition n'exclut pas, à priori, que ce temps de réponse puisse être tenu alors qu'une de ces durées est supérieure à Δ, si l'autre est inférieure à Δ, et ceci même si l'intensité du plus lent consommateur n'est pas nulle. Cette constatation qui n'est guère intuitive doit-elle faire conclure à la faiblesse des conditions nécessaires trouvées? Il semble qu'il n'en est rien. En effet, si les conditions trouvées ne sont pas suffisantes, on pourra néanmoins se convaincre qu'il peut exister des fonctionnements respectant le temps de réponse et correspondant à la situation évoquée ci-dessus. Cela tient au fait que le temps de réponse spécifié ne porte pas sur la durée de vie de chaque objet entre sa production et sa consommation: Le temps de réponse sera respecté si toute production d'un objet est suivie, moins de Δ aprés, par la consommation d'un objet (éventuellement autre, et produit antérieurement). Si l'intention du modèle était de spécifier une durée de vie maximale des objets entre leur production et leur consommation, le modèle aurait du être conçu différemment! En ce sens, cet exemple montre aussi les précautions à prendre lorsqu'on utilise les RPTC, notamment dans le cas des systèmes pipe-line.

7.6. MISE EN OEUVRE DE LA METHODE

Cette méthode peut être entièrement automatisée. Le seul problème délicat concerne la détermination automatique de la base des p-sous-semi-flots. Actuellement les recherches ont surtout porté sur l'étude des semi-flots [Martinez]. En fait, ce problème, comme celui, plus général des sous-semi-flots, est un cas particulier du problème de la détermination des vecteurs générateurs d'un cône de $\mathbb{R}^m$ défini par un système d'inéquations linéaires, qui est étudié et dont on pourra trouver des solutions dans [Halbwachs]. Notons enfin que le LAAS a développé un logiciel d'acquisition et d'analyse des réseaux de Pétri, OGIVE [Ayache], qui contient déja la détermination des semi-flots, et qui pourrait facilement intégrer la méthode proposée ici.

7.7. ANALYSE EN INTENSITE ET PROJECTION

Au §7.1.3, nous avons illustré une méthode par projections approchées, permettant d'obtenir des conditions nécessaires pour qu'un système admette des solutions. Il est clair que cette méthode est applicable à l'analyse en intensités de tous ordres, alors que la méthode du §7.4 ne permet d'étudier que les intensités d'ordre 1. Nous nous bornerons à illustrer cette constatation par un exemple de RPTC admettant une intensité d'ordre 2.

Considérons le système d'inéquations en évènements:

$$S = \begin{cases} x + y \leq 1 + 2Rx \\ R^2 x \leq y \end{cases}$$

En éliminant y, on obtient:

$$(1 - R)^2 x \leq 1$$

D'où l'on peut conclure que, si (x,y) vérifie S, alors:

a) x ne peut admettre d'intensité d'ordre strictement supérieur à 2.

b) si x admet une intensité d'ordre 2, $J_x^{(2)}$, alors $J_x^{(2)} \leq 1$.

On peut remarquer, de plus, qu'il existe une telle solution avec $J_x^{(2)}=1$, puisque $\{ x= 1/(1 - R)^2 , y= R^2/(1 - R)^2 \}$ est solution de S.

L'analyse en intensité a l'avantage d'être automatisable, mais nous avons montré, par contre, qu'elle s'applique à un type de problèmes moins vaste que la méthode de projection. Il semble que la comparaison des deux méthodes puisse être approfondie, en particulier dans deux directions:

. Il existe certainement une classe de systèmes pour lesquels l'existence d'un fonctionnement entraine l'existence d'une intensité d'ordre 1.

Pour cette classe, l'analyse en intensité fournirait des conditions nécessaires d'existence de solutions. Une clé du problème de la caractérisation de cette classe de systèmes semble être l'étude des systèmes à coefficients rationnels. Il apparait également que la solution de ce problème serait plus facile si l'on se restreignait à un modèle discret du temps.

. Une deuxième question, non abordée ici, concerne la richesse des résultats respectifs obtenus, sur le même problème, au moyen de l'analyse en intensités, et de la méthode de projection. Sur tous les exemples que nous avons traités, ces deux méthodes donnent les mêmes résultats, sans qu'il nous ait été possible de conclure à leur équivalence.

TABLE DES PRINCIPALES DEFINITIONS

PRINCIPALES NOTATIONS

$\circ$: composition fonctionnelle.

$\neg, \wedge, \vee$: négation, conjonction, disjonction booléennes.

$\leqslant$: relation d'ordre sur un ensemble. Sur un ensemble de fonctions, il s'agit de l'ordre point par point. Sur l'ensemble des (pseudo-)évènements, il s'agit de l'ordre sur leurs compteurs.

$<$: relation d'ordre strict. Sur un ensemble de fonctions, il s'agit de l'ordre strict point par point.

$+$: somme. La somme de deux (pseudo-)évènements correspond à celle de leurs compteurs.

$\subseteq$: relation de sous-suite entre evénements.

$|$: opérateur de filtrage d'un évènement par une condition. Utilisé aussi, dans les notations d'ensembles, comme abréviation de "tel que".

$\top, \bot$: éléments maximum et minimum d'un treillis complet.

$\#x$: nombre de termes du pseudo-évènement x.

0 : (pseudo-)évènement nul.

1 : dans la première partie, dénote la fonction $\lambda x.1$, de $\mathbb{N}$ ou $\mathbb{T}$ dans $\mathbb{N}$; dans la deuxième partie, dénote le pseudo-évènement unité.

$\sqcap, \sqcup$: opérateurs de bornes inférieure et supérieure de la relation de sous-suite.

A, A($\mathbb{T}$) : ensemble des pseudo-évènements (sur l'ensemble d'instants $\mathbb{T}$).

$[[a), (b]], [[a,b]]$: notation des intervalles de A.

$[a,b],]a,b[$: notation des segments de A.

C^+, C^- : matrices d'incidence avant et arrière d'un réseau de Pétri.

$\tilde{C}^-$, $\tilde{C}^+$: matrices d'incidence avant et arriére d'un réseau de Pétri temporisé réduit à ses places de durée nulle.

$C\uparrow$, $C\downarrow$: évènements fronts montant et descendant de la condition C.

$Def(f)$: domaine de définition de la fonction f .

D_x : domaine des valeurs de la variable x .

Δ_i : (chapitres 5 & 7) délai associé à la place p_i.

E, $E(\mathbb{T})$: ensemble des évènements (sur l'ensemble d'instants $\mathbb{T}$).

^{-1}f, f^{-1} : pseudo-inverses, à gauche et à droite, de la fonction f.

ϕa : transformée discrète du pseudo-évènement a.

I : identité sur $\mathbb{N}$ ou $\mathbb{T}$.

$J_a^{(\gamma)}$: intensité d'ordre γ du pseudo-évènement a.

λ : généralement réservé à la notation lambda des fonctions ($f=\lambda x.f(x)$).

μe, $\mu\tilde{e}^+$: fonctions compteur d'un (pseudo-)évènement.

M_0 : marquage initial d'un réseau de Pétri.

$M(t)$: marquage d'un réseau temporisé à l'instant t.

$\tilde{M}(t)$: marquage disponible d'un réseau temporisé à l'instant t.

$\overline{\mathbb{N}}$: $\mathbb{N} \cup \{+\infty\}$, $\mathbb{N}^*$: $\mathbb{N} - \{0\}$.

νx : suite des valeurs de la variable x.

$\tilde{\nu}x$, $\tilde{\nu}\tilde{x}^+$: fonctions trajectoire de la variable x.

$\tilde{P}$: prolongement à $A(\mathbb{R})^n$ du polyèdre P de $A(\mathbb{Z})^n$

$p^\bullet$, $^\bullet p$: ensemble des transitions vidant et remplissant la place p.

$\mathbb{R}^+$: ensemble des réels positifs . $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty,+\infty\}$.

R^Δ : opérateur de délai sur les évènements, ou, dans la deuxième partie, évènement dont l'unique occurrence survient à l'instant Δ.

$\mathbb{T}$: ensemble des instants . $\overline{\mathbb{T}} = \mathbb{T} \cup \{-\infty,+\infty\}$.

τe ou $\tau(e)$: fonction date de l'évènement e .

Θe, $\Theta\tilde{e}^+$: fonctions dernière occurrence de l'évènement e .

$\hat{x}$: évènement associé à la mise à feu de la transition x.

x : si X est une variable, dénote l'évènement "prise de valeur" de X.

$\bar{x}_n$: n-ième coefficient de la série formelle définissant le pseudo-évènement x.

x_n : n-ième exposant de la série formelle définissant le pseudo-évènement x.

$x^\bullet$, $^\bullet x$: ensemble des places remplies et vidées par la transition x.

Y^T: transposé du vecteur Y.

$\overline{\mathbb{Z}}$: $\mathbb{Z} \cup \{-\infty,+\infty\}$.

REFERENCES

[Abrial 78]

J.R. Abrial : "Z: A specification language". Proc. Int. Conf. on Mathematical Studies of Information Processing, Kioto, aout 78.

[Abrial 82]

J.R. Abrial : "Specification and construction of machines". A paraitre.

[Agerwala]

T. Agerwala : "A complete model for representing the coordination of asynchronous processes", R.R.n°32, John Hopkins Univ., Baltimore, juillet 74.

[Amblard]

P.Amblard : Problèmes temporels dans les circuits intégrés: Un point de vue architectural. Thèse de 3e Cycle, INPG, Grenoble, A paraître.

[André & Boeri]

C. André, F. Boeri : "The behaviour equivalence and its application in Petri nets analysis". Journée AFCET "Schémas de contrôle des systèmes informatiques", Paris, septembre 79.

[Ashcroft & Wadge]

E.A. Ashcroft, W.W. Wadge : "LUCID: A non procedural language with iteration". CACM, vol.20, n°7, juillet 77.

[Austry & Boudol]

D. Austry, G. Boudol : "Algèbre de processus et synchronisation". A paraitre.

[Ayache, Azéma & Diaz]

J. Ayache, P. Azéma, M. Diaz : "Towards fault tolerant real time systems by using Petri nets". 2nd Workshop on Application and Theory of Petri Nets, Bad Honnef, septembre 81.

[Berstel]

J. Berstel (ed.) : "Séries formelles en variables non commutatives et applications". 5e Ecole de Printemps d'Informatique Théorique, LITP, Paris, mai 78.

[Billoir]

T. Billoir : Communication au IEEE Workshop on the Validation of Fault Tolerant Computers and Systems, Luray, septembre 80.

[Bochmann]

G.V. Bochmann : "Hardware specification with temporal logic: An example". IEEE trans. on Computers, vol.C-31, n°3, mars 82.

[Bourdon]

M. Bourdon : "Une approche unifiée des problèmes d'ordonnancement statique discret". rapport de D.E.A., I.N.P.G, Grenoble, juin 82.

[Caplain]

M. Caplain : "Langage de spécification". Thèse d'état, Université de Grenoble, 1978.

[Cardelli]

L. Cardelli : "An algebraic approach to hardware description and verification". Thèse, Edimburgh Univ., avril 82.

[Caspi, Halbwachs & Moalla]

P. Caspi, N. Halbwachs, M. Moalla : "Approche comportementale pour la spécification des systèmes temps réel". Journée AFCET "Spécifications", Toulouse, septembre 80 .

[Caspi & Halbwachs 79]

P. Caspi, N. Halbwachs : Rapport final du contrat ADR/Crouzet n°511.79.2.1, I.N.P.G., décembre 79.

[Caspi & Halbwachs 82a]

P. Caspi, N. Halbwachs : "Algebra of events: A model for parallel and real time systems". Proc. Int. Conf. on Parallel Processing, Bellaire, aout 82.

[Caspi & Halbwachs 82b]

P. Caspi, N. Halbwachs : " An approach to real time systems modeling". Proc. Int. Conf. on Distributed Computing Systems, Miami; octobre 82.

[Caspi & Halbwachs 83]

P. Caspi, N. Halbwachs : "Conception certifiée de systèmes distribués: Un exemple". Rapport final de l'A.T.P.-P.C.S., octobre 83.

[Caspi & Halbwachs 84]

P.Caspi, N. Halbwachs : "Analyse approchée du comportement asymptotique de systèmes temporisés". A paraitre dans T.S.I.

[Chen & Yeh]

B.-T. Chen, R.T. Yeh : "Formal specification and verification of distributed systems". Proc. Int. Conf. on Distibuted Computing Systems, Miami, octobre 82.

[Chretienne]

Ph. Chretienne : "Some results on the control of timed Petri nets". 2nd Workshop on Applications and theory of Petri nets, Bad Honnef, septembre 81 .

[Cousot]

P. Cousot : "Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis complet, analyse sémantique des programmes". Thèse d'état, Grenoble, mars 78.

[Darondeau & Kott]

Ph. Darondeau, L. Kott : "On the observational semantics of fair parallelism". R.R. IRISA, Rennes, 1983.

[Floyd]

R.W.Floyd : "Assigning meaning to programs". Proc. Symp. in Applied Math., vol.19, A.M.S, Providence, 1967.

[Girault & Reisig]

C. Girault & W. Reisig (eds.) : "Application and theory of Petri nets". Informatik Fachberichte, Springer Verlag, 1982.

[Gordon]

M.J.C. Gordon : "Register transfer systems and their behaviours". Proc. 5th. Int. Symp. on Computer Hardware Description Languages, 1981.

[Halbwachs]

N. Halbwachs : "Détermination automatique de relations linéaires vérifiées par les variables d'un programme". Thèse de 3e cycle, Univ. de Grenoble, mars 79.

[Hailpern & Owicki]

B.T. Hailpern, S.S. Owicki : "Verifying network protocols using temporal logic". Technical Report n°192, Stanford Comp. Syst. Lab., juin 80.

[Hennessy & De Nicola]

M.C.B. Hennessy, R. De Nicola : " Testing equivalence for processes ". CSR-123-82, Comp. Science Dept., Edimburgh Univ., aout 82.

[Hoare 69]

C.A.R. Hoare :" An axiomatic approach to computer programming". CACM, vol.12, n°10, octobre 69.

[Hoare 82]

C.A.R. Hoare : "Specifications, programs and implementations". Technical Monograph PRG-29, Comp. Lab., Oxford Univ., juin 82.

[Hoare & Lauer]

C.A.R. Hoare, P.E.Lauer : "Consistent and complementary formal theories of the semantics of programming languages". Acta Informatica, 3, 1974.

[Jury]

E.I. Jury : "Theory and applications of the z-transform method". J.Wiley ed., 1964.

[Kahn & McQueen]

G. Kahn, D.B. Mac Queen : "Coroutines and networks of parallel processes". Proc. IFIP Congress, 1977.

[Karr]

M. Karr : "Summation in finite terms". JACM, vol.28, n°2, avril 81.

[Koymans & De Roever]

R. Koymans, W.P. De Roever : "Examples of a real time temporal logic specification". Workshop on the Analysis of Concurrent Systems, Cambridge, septembre 83.

[Lamport]

L. Lamport : "Time, clocks, and the ordering of events in a distributed system". CACM, vol.21, n°7, juillet 78.

[Martinez & Silva]

J. Martinez, J. Silva : "A simple and fast algorithm to obtain all invariants of a generalized Petri net". 2nd Workshop on Application and Theory of Petri nets, Bad Honnef, septembre 81.

[Memmi]

G. Memmi : "Fuites et semi-flots dans les réseaux de Petri". Thèse de Docteur-Ingénieur, Univ. Paris VI, décembre 78.

[Merlin]

P. Merlin : "A study in the recoverability of computer systems". Thèse, Univ. of California, 1974.

[Milner 80]

R. Milner : "A calculus of communicating systems". LNCS 92, 1980.

[Milner 83]

R. Milner : "Calculi for synchrony and asynchrony". TCS vol.25, n°3, juillet 83.

[Moalla, Pulou & Sifakis]

M. Moalla, J. Pulou, J. Sifakis : "Réseaux de Pétri synchronisés". RAIRO Automatique, Vol.12, n°2, 1978.

[Moszkowski]

B. Moszkowski : "A temporal logic for multi-level reasoning about hardware". Proc. 6th Int. Symp. on Computer Hardware Description Languages, Pittsburgh, mai 83.

[Peterson]

J.L. Peterson : "Petri nets". ACM Computing Surveys, Vol.9, n°3, septembre 77.

[Queille & Sifakis]

J.P. Queille, J. Sifakis : "Specification and verification of concurrent systems in CESAR", LNCS vol.137, avril 82.

[Ramchandani]

C. Ramchandani : "Analysis of asynchronous concurrent systems by timed Petri nets". Thèse, M.I.T., septembre 73.

[Reed & Kanodia]

D.P. Reed, R.K. Kanodia : "Synchronization with eventcounts and sequencers". CACM, vol.22, n°2, février 79.

[Reutenauer]

Ch. Reutenauer : Communication privée.

[Robert & Verjus]

P. Robert, J.P. Verjus : "Towards autonomous description of synchronization modules". Proc. IFIP Congress, Toronto, 1977.

[Samuel]

P. Samuel : "About Euclidean rings". Journal of Algebra, n°19, 1971.

[Sanchis]

L.E. Sanchis : "Data types as lattices, retractions, closures and projections". RAIRO Informatique Théorique, vol.11, n°4, 1977.

[Schwartz,Melliar-Smith & Vogt]

R.L. Schwartz, P.M. Melliar-Smith, F.H. Vogt : "An interval logic for higher level temporal reasoning". Tech. Report, SRI International, février 83.

[Scott 70]

D. Scott : "Outline of a mathematical theory of computation". Proc. 4th Annual Princeton Conf. on Information Science and Systems, 1970.

[Scott 76]

D. Scott : "Data types as lattices". SIAM Journal on Computing, 1976.

[Sethi]

R. Sethi :"Semantics of computer programs : Overview of language definition methods". Tech. Report, Bell Labs., septembre 77.

[Shostak]

R.E. Shostak : "Formal verification of circuit design". Proc. 6th Symp. on Computer Hardware Description Languages, 1981.

[Sifakis]

J. Sifakis : "Use of Petri nets for performance evaluation". Measuring, Modelling and Evaluating Computer systems, North Holland Pub. Co., 1977.

[Tennent]

R.D. Tennent : "The denotational semantics of programming languages". CACM, vol.19, n°8, aout 76.

[Widder]

D.V. Widder : "The Laplace transform", Princeton Univ. Press, 1946.

[Zimmermann]

U. Zimmermann : "Linear and combinatorial optimization in ordered algebraic structures". Annals of Discrete Math., n°10, North Holland Pub. Co., 1981.

dernière page de la thèse

AUTORISATION DE SOUTENANCE

VU les dispositions de l'article 5 de l'arrêté du 16 Avril 1974

VU les rapports de Madame G. SAUCIER

Monsieur G. BERRY

Monsieur M. SINTZOFF

M. HALBWACHS Nicolas est autorisé à présenter une thèse en soutenance pour l'obtention du grade de DOCTEUR D'ETAT ES SCIENCES

Fait à GRENOBLE, le 28 mai 1984

Le Président de l'U.S.M.G.

Le Président de l'I.N.P.G.

D. BLOCH
Président
de l'Institut National Polytechnique
de Grenoble

P.O. le Vice-Président,