Structure et comportement itératif de certains modèles discrets

El Houssine Snoussi

THESE

présentée à

Université Scientifique et Médicale de Grenoble

Institut National Polytechnique de Grenoble

pour obtenir le grade de
DOCTEUR DE 3ème cycle
Mathématiques Appliquées
option «analyse numérique»

par

SNOUSSI El Houssine

STRUCTURE ET COMPORTEMENT ITERATIF DE CERTAINS MODELES DISCRETS.

Thèse soutenue le 11 juin 1980 devant la commission d'examen

N. GASTINEL	Président
C. BENZAKEN	
J.M. LABORDE	Examinateurs
C. MOSER	
F. ROBERT	

UNIVERSITE SCIENTIFIQUE ET MEDICALE DE GRENOBLE

Monsieur Gabriel CAU : Président
Monsieur Joseph KLEIN : Vice-Président

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

PROFESSEURS TITULAIRES

MM.	AMBLARD Pierre	Clinique de dermatologie
	ARNAUD Paul	Chimie
	ARVIEU Robert	I.S.N.
	AUBERT Guy	Physique
	AYANT Yves	Physique approfondie
Mme	BARBIER Marie-Jeanne	Electrochimie
MM.	BARBIER Jean-Claude	Physique expérimentale
	BARBIER Reynold	Géologie appliquée
	BARJON Robert	Physique nucléaire
	BARNOUD Fernand	Biosynthèse de la cellulose
	BARRA Jean-René	Statistiques
	BARRIE Joseph	Clinique chirurgicale A
	BEAUDOING André	Clinique de pédiatrie et puériculture
	BELORIZKY Elie	Physique
	BARNARD Alain	Mathématiques pures
Mme	BERTRANDIAS Françoise	Mathématiques pures
MM.	BERTRANDIAS Jean-Paul	Mathématiques pures
	BEZES Henri	Clinique chirurgicale et traumatologie
	BLAMBERT Maurice	Mathématiques pures
	BOLLIET Louis	Informatique (I.U.T. B)
	BONNET Jean-Louis	Clinique ophtalmologie
	BONNET-EYMARD Joseph	Clinique hépato-gastro-entérologie
Mme	BONNIER Marie-Jeanne	Chimie générale
MM.	BOUCHERLE André	Chimie et toxicologie
	BOUCHEZ Robert	Physique nucléaire
	BOUSSARD Jean-Claude	Mathématiques appliquées
	BOUTET DE MONVEL Louis	Mathématiques pures
	BRAVARD Yves	Géographie
	CABANEL Guy	Clinique rhumatologique et hydrologique
	CALAS François	Anatomie
	CARLIER Georges	Biologie végétale
	CARRAZ Gilbert	Biologie animale et pharmacodynamie

.../...

MM.	CAU Gabriel	Médecine légale et toxicologie
	CAUQUIS Georges	Chimie organique
	CHABAUTY Claude	Mathématiques pures
	CHARACHON Robert	Clinique ot-rhino-laryngologique
	CHATEAU Robert	Clinique de neurologie
	CHIBON Pierre	Biologie animale
	COEUR André	Pharmacie chimique et chimie analytique
	COUDERC Pierre	Anatomie pathologique
	DEBELMAS Jacques	Géologie générale
	DEGRANGE Charles	Zoologie
	DELORMAS Pierre	Pneumophtisiologie
	DEPORTES Charles	Chimie minérale
	DESRE Pierre	Métallurgie
	DODU Jacques	Mécanique appliquée (I.U.T. I)
	DOLIQUE Jean-Michel	Physique des plasmas
	DREYFUS Bernard	Thermodynamique
	DUCROS Pierre	Cristallographie
	FONTAINE Jean-Marc	Mathématiques pures
	GAGNAIRE Didier	Chimie physique
	GALVANI Octave	Mathématiques pures
	GASTINEL Noël	Analyse numérique
	GAVEND Michel	Pharmacologie
	GEINDRE Michel	Electroradiologie
	GERBER Robert	Mathématiques pures
	GERMAIN Jean-Pierre	Mécanique
	GIRAUD Pierre	Géologie
	JANIN Bernard	Géographie
	KAHANE André	Physique générale
	KLEIN Joseph	Mathématiques pures
	KOSZUL Jean-Louis	Mathématiques pures
	KRAVTCHENKO Julien	Mécanique
	LACAZE Albert	Thermodynamique
	LACHARME Jean	Biologie végétale
Mme	LAJZEROWICZ Janine	Physique
MM.	LAJZEROWICZ Joseph	Physique
	LATREILLE René	Chirurgie générale
	LATURAZE Jean	Biochimie pharmaceutique
	LAURENT Pierre	Mathématiques appliquées
	LEDRU Jean	Clinique médicale B
	LE ROY Philippe	Mécanique (.I.U.T. I)

.../...

MM.	LLIBOUTRY Louis	Géophysique
	LOISEAUX Jean-Marie	Sciences nucléaires
	LONGEQUEUE Jean-Pierre	Physique nucléaire
	LOUP Jean	Géographie
Mlle	LUTZ Elisabeth	Mathématiques pures
MM.	MALINAS Yves	Clinique obstétricale
	MARTIN-NOEL Pierre	Clinique cardiologique
	MAYNARD Roger	Physique du solide
	MAZARE Yves	Clinique Médicale A
	MICHEL Robert	Minéralogie et pétrographie
	MICOUD Max	Clinique maladies infectieuses
	MOURIQUAND Claude	Histologie
	MOUSSA André	Chimie nucléaire
	NEGRE Robert	Mécanique
	NOZIERES Philippe	Spectrométrie physique
	OZENDA Paul	Botanique
	PAYAN Jean-Jacques	Mathématiques pures
	PEBAY-PEYROULA Jean-Claude	Physique
	PERRET Jean	Séméiologie médicale (neurologie)
	RASSAT André	Chimie systématique
	RENARD Michel	Thermodynamique
	REVOL Michel	Urologie
	RINALDI Renaud	Physique
	DE ROUGEMONT Jacques	Neuro-Chirurgie
	SARRAZIN Roger	Clinique chirurgicale B
	SEIGNEURIN Raymond	Microbiologie et hygiène
	SENGEL Philippe	Zoologie
	SIBILLE Robert	Construction mécanique (I.U.T. I)
	SOUTIF Michel	Physique générale
	TANCHE Maurice	Physiologie
	VAILLANT François	Zoologie
	VALENTIN Jacques	Physique nucléaire
Mme	VERAIN Alice	Pharmacie galénique
MM.	VERAIN André	Physique biophysique
	VEYRET Paul	Géographie
	VIGNAIS Pierre	Biochimie médicale

.../...

PROFESSEURS ASSOCIES

MM.	CRABBE Pierre	CERMO
	SUNIER Jules	Physique

PROFESSEURS SANS CHAIRE

Mlle	AGNIUS-DELORS Claudine	Physique pharmaceutique
	ALARY Josette	Chimie analytique
MM.	AMBROISE-THOMAS Pierre	Parasitologie
	ARMAND Gilbert	Géographie
	BENZAKEN Claude	Mathématiques appliquées
	BIAREZ Jean-Pierre	Mécanique
	BILLET Jean	Géographie
	BOUCHET Yves	Anatomie
	BRUGEL Lucien	Energétique (I.U.T. I)
	BUISSON René	Physique (I.U.T. I)
	BUTEL Jean	Orthopédie
	COHEN-ADDAD Jean-Pierre	Spectrométrie physique
	COLOMB Maurice	Biochimie médicale
	CONTE René	Physique (I.U.T. I)
	DELOBEL Claude	M.I.A.G.
	DEPASSEL Roger	Mécanique des fluides
	GAUTRON René	Chimie
	GIDON Paul	Géologie et minéralogie
	GLENAT René	Chimie organique
	GROULADE Joseph	Biochimie médicale
	HACQUES Gérard	Calcul numérique
	HOLLARD Daniel	Hématologie
	HUGONOT Robert	Hygiène et médecine préventive
	IDELMAN Simon	Physiologie animale
	JOLY Jean-René	Mathématiques pures
	JULLIEN Pierre	Mathématiques appliquées
Mme	KAHANE Josette	Physique
MM.	KRAKOWIACK Sacha	Mathématiques appliquées
	KUHN Gérard	Physique (I.U.T. I)
	LUU DUC Cuong	Chimie organique - pharmacie
	MICHOULIER Jean	Physique (I.U.T. I)
Mme	MINIER Colette	Physique (I.U.T. I)

.../...

MM.	PELMONT Jean	Biochimie
	PERRIAUX Jean-Jacques	Géologie et minéralogie
	PFISTER Jean-Claude	Physique du solide
Mlle	PIERY Yvette	Physiologie animale
MM.	RAYNAUD Hervé	M.I.A.G.
	REBECQ Jacques	Biologie (CUS)
	REYMOND Jean-Charles	Chirurgie générale
	RICHARD Lucien	Biologie végétale
Mme	RINAUDO Marguerite	Chimie macromoléculaire
MM.	SARROT-REYNAULD Jean	Géologie
	SIROT Louis	Chirurgie générale
Mme	SOUTIF Jeanne	Physique générale
MM.	STIEGLITZ Paul	Anesthésiologie
	VIALON Pierre	Géologie
	VAN CUTSEM Bernard	Mathématiques appliquées

MAITRES DE CONFERENCES ET MAITRES DE CONFERENCES AGREGES

MM.	ARMAND Yves	Chimie (I.U.T. I)
	BACHELOT Yvan	Endocrinologie
	BARGE Michel	Neuro-chirurgie
	BEGUIN Claude	Chimie organique
Mme	BERIEL Hélène	Pharmacodynamie
MM.	BOST Michel	Pédiatrie
	BOUCHARLAT Jacques	Psychiatrie adultes
Mme	BOUCHE Liane	Mathématiques (CUS)
MM.	BRODEAU François	Mathématiques (I.U.T. B) (Personne étrangère habilitée à être directeur de thèse)
	BERNARD Pierre	Gynécologie
	CHAMBAZ Edmond	Biochimie médicale
	CHAMPETIER Jean	Anatomie et organogénèse
	CHARDON Michel	Géographie
	CHERADAME Hervé	Chimie papetière
	CHIAVERINA Jean	Biologie appliquée (EFP)
	COLIN DE VERDIERE Yves	Mathématiques pures
	CONTAMIN Charles	Chirurgie thoracique et cardio-vasculaire
	CORDONNER Daniel	Néphrologie
	COULOMB Max	Radiologie
	CROUZET Guy	Radiologie

.../...

MM.	CYROT Michel	Physique du solide
	DENIS Bernard	Cardiologie
	DOUCE Roland	Physiologie végétale
	DUSSAUD René	Mathématiques (CUS)
Mme	ETERRADOSSI Jacqueline	Physiologie
MM.	FAURE Jacques	Médecine légale
	FAURE Gilbert	Urologie
	GAUTIER Robert	Chirurgie générale
	GIDON Maurice	Géologie
	GROS Yves	Physique (I.U.T. I)
	GUIGNIER Michel	Thérapeutique
	GUITTON Jacques	Chimie
	HICTER Pierre	Chimie
	JALBERT Pierre	Histologie
	JUNIEN-LAVILLAVROY Claude	O.R.L.
	KOLODIE Lucien	Hématologie
	LE NOC Pierre	Bactériologie-virologie
	MACHE Régis	Physiologie végétale
	MAGNIN Robert	Hygiène et médecine préventive
	MALLION Jean-Michel	Médecine du travail
	MARECHAL Jean	Mécanique (I.U.T. I)
	MARTIN-BOUYER Michel	Chimie (CUS)
	MASSOT Christian	Médecine interne
	NEMOZ Alain	Thermodynamique
	NOUGARET Marcel	Automatique (I.U.T. I)
	PARAMELLE Bernard	Pneumologie
	PECCOUD François	Analyse (I.U.T. B) (Personnalité étrangère habilitée à être directeur de thèse)
	PEFFEN René	Métallurgie (I.U.T. I)
	PERRIER Guy	Géophysique-glaciologie
	PHELIP Xavier	Rhumatologie
	RACHALL Michel	Médecine interne
	RACINET Claude	Gynécologie et obstétrique
	RAMBAUD Pierre	Pédiatrie
	RAPHAEL Bernard	Stomatologie
Mme	RENAUDET Jacqueline	Bactériologie (pharmacie)
MM.	ROBERT Jean-Bernard	Chimie-physique
	ROMIER Guy	Mathématiques (I.U.T. B) (Personnalité étrangère habilitée à être directeur de thèse)
	SAKAROVITCH Michel	Mathématiques appliquées

.../...

MM.	SCHAERER René	Cancérologie
Mme	SEIGLE-MURANDI Françoise	Crytogamie
MM.	STOEBNER Pierre	Anatomie pathologie
	STUTZ Pierre	Mécanique
	VROUSOS Constantin	Radiologie

MAITRES DE CONFERENCES ASSOCIES

MM.	DEVINE Roderick	Spectro Physique
	KANEKO Akira	Mathématiques pures
	JOHNSON Thomas	Mathématiques appliquées
	RAY Tuhina	Physique

MAITRE DE CONFERENCES DELEGUE

M.	ROCHAT Jacques	Hygiène et hydrologie (pharmacie)

Fait à Saint Martin d'Hères, novembre 1977

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Année universitaire 1979-1980

Président : M. Philippe TRAYNARD

Vice-Présidents : M. Georges LESPINARD
M. René PAUTHENET

PROFESSEURS DES UNIVERSITES

MM.	ANCEAU François	Informatique fondamentale et appliquée
	BENOIT Jean	Radioélectricité
	BESSON Jean	Chimie Minérale
	BLIMAN Samuel	Electronique
	BLOCH Daniel	Physique du Solide - Cristallographie
	BOIS Philippe	Mécanique
	BONNETAIN Lucien	Génie Chimique
	BONNIER Etienne	Métallurgie
	BOUVARD Maurice	Génie Mécanique
	BRISSONNEAU Pierre	Physique des Matériaux
	BUYLE-BODIN Maurice	Electronique
	CHARTIER Germain	Electronique
	CHERADAME Hervé	Chimie Physique Macromoléculaires
Mme	CHERUY Arlette	Automatique
MM.	CHIAVERINA Jean	Biologie, Biochimie, Agronomie
	COHEN Joseph	Electronique
	COUMES André	Electronique
	DURAND Francis	Métallurgie
	DURAND Jean-Louis	Physique Nucléaire et Corpusculaire
	FELICI Noël	Electrotechnique
	FOULARD Claude	Automatique
	GUYOT Pierre	Métallurgie Physique
	IVANES Marcel	Electrotechnique
	JOUBERT Jean-Claude	Physique du Solide - Cristallographie
	LACOUME Jean-Louis	Géographie - Traitement du Signal
	LANCIA Roland	Electronique - Automatique
	LESIEUR Marcel	Mécanique
	LESPINARD Georges	Mécanique
	LONGEQUEUE Jean-Pierre	Physique Nucléaire Corpusculaire
	MOREAU René	Mécanique
	MORET Roger	Physique Nucléaire Corpusculaire
	PARIAUD Jean-Charles	Chimie - Physique
	PAUTHENET René	Physique du Solide - Cristallographie
	PERRET René	Automatique

.../...

MM.	PERRET Robert	Electrotechnique
	PIAU Jean-Michel	Mécanique
	PIERRARD Jean-Marie	Mécanique
	POLOUJADOFF Michel	Electrotechnique
	POUPOT Christian	Electronique - Automatique
	RAMEAU Jean-Jacques	Chimie
	ROBERT André	Chimie Appliquée et des matériaux
	ROBERT François	Analyse numérique
	SABONNADIERE Jean-Claude	Electrotechnique
Mme	SAUCIER Gabrielle	Informatique fondamentale et appliquée
M.	SOHM Jean-Claude	Chimie - Physique
Mme	SCHLENKER Claire	Physique du Solide - Cristallographie
MM.	TRAYNARD Philippe	Chimie - Physique
	VEILLON Gérard	Informatique fondamentale et appliquée
	ZADWORNY François	Electronique

CHERCHEURS DU C.N.R.S. (Directeur et Maître de Recherche)

M.	FRUCHART Robert	Directeur de Recherche
MM.	ANSARA Ibrahïm	Maître de Recherche
	BRONOEL Guy	Maître de Recherche
	CARRE René	Maître de Recherche
	DAVID René	Maître de Recherche
	DRIOLE Jean	Maître de Recherche
	KAMARINOS Georges	Maître de Recherche
	KLEITZ Michel	Maître de Recherche
	LANDAU Ioan-Doré	Maître de Recherche
	MERMET Jean	Maître de Recherche
	MUNIER Jacques	Maître de Recherche

Personnalités habilitées à diriger des travaux de recherche (décision du Conseil Scientifique)

E.N.S.E.E.G.

MM.	ALLIBERT Michel	
	BERNARD Claude	
	CAILLET Marcel	
Mme	CHATILLON Catherine	
MM.	COULON Michel	
	HAMMOU Abdelkader	
	JOUD Jean-Charles	
	RAVAINE Denis	
	SAINFORT	C.E.N.G.

.../...

MM. SARRAZIN Pierre
SOUQUET Jean-Louis
TOUZAIN Philippe
URBAIN Georges — Laboratoire des Ultra-Réfractaires ODEILLO

E.N.S.M.E.E.

MM. BISCONDI Michel
BOOS Jean-Yves
GUILHOT Bernard
KOBILANSKI André
LALAUZE René
LANCELOT Françis
LE COZE Jean
LESBATS Pierre
SOUSTELLE Michel
THEVENOT François
THOMAS Gérard
TRAN MINH Canh
DRIVER Julian
RIEU Jean

E.N.S.E.R.G.

MM. BOREL Joseph
CHEHIKIAN Alain
VIKTOROVITCH Pierre

E.N.S.I.E.G.

MM. BORNARD Guy
DESCHIZEAUX Pierre
GLANGEAUD François
JAUSSAUD Pierre
Mme JOURDAIN Geneviève
MM. LEJEUNE Gérard
PERARD Jacques

E.N.S.H.G.

M. DELHAYE Jean-Marc

E.N.S.I.M.A.G.

MM. COURTIN Jacques
LATOMBE Jean-Claude
LUCAS Michel
VERDILLON André

Je tiens à exprimer ma profonde gratitude à

Monsieur Noël GASTINEL pour l'honneur qu'il me fait en présidant le jury de cette thèse ,

Monsieur François ROBERT pour sa bienveillance , sa disponibilité et ses encouragements au cours de l'élaboration de ce travail ,

Messieurs Claude BENZAKEN , Jean-Marie LABORDE et Claude MOSER qui ont bien voulu faire partie de ce jury .

Je suis particulièrement sensible à l'enthousiasme et l'esprit de collaboration qui animent le groupe de travail " Comportement d'Itération" et je tiens à exprimer à tous ses membres ma sincère sympathie .

Je remercie également Mademoiselle Geneviève BICAIS qui a effectué avec compétence et amabilité la frappe de cette thèse, ainsi que tous les membres du service de reprographie pour l'excellente qualité de leur travail et surtout pour leur accueil toujours chaleureux .

SNOUSSI El Houssine

TABLE DES MATIERES

INTRODUCTION

Le but de notre travail était au départ , l'étude du comportement des itérations sur des fonctions booléennes , c'est-à-dire des fonctions de $\{0,1\}^n$ dans lui même . Il est clair qu'à priori , de telles itérations peuvent être complétement décrites par énumération de toutes les possibilités qui sont en nombre fini , mais dans la pratique , un tel procédé est exclu. On est donc amené à donner des informations -au moins locales- sur le graphe d'itération de telles fonctions à partir de leur expression analytique , ce qui nécessite le choix d'une structure algébrique sur l'ensemble $\{0,1\}^n$.

Dans [32,33,34] , F.Robert a développé une notion de rayon spectral booléen et de distance vectorielle booléenne permettant d'établir des conditions suffisantes de convergence et ceci en utilisant la structure algébrique sur $\{0,1\}^n$ induite par l'algèbre de Boole usuelle sur $\{0,1\}$ .Dans le même contexte différentes classes de fonctions booléennes ont été étudiées dans [15] et [16].

Une autre approche du problème consiste à considérer $\{0,1\}^n$ comme espace vectoriel sur le corps Z_2 des entiers modulo deux , et le problème devient un cas particulier de celui , plus général , de l'étude du comportement des itérations sur des fonctions de Z_p^n dans Z_p^n où p est un nombre premier . C'est ce point de vue que nous présentons dans le premier chapitre dans lequel nous avons établi quelques propriétés du graphe d'itération de certaines classes de fonctions .

Une fonction F de Z_p^n dans Z_p^n est définie par n fonctions f_i (i=1,2,...,n) de Z_p^n dans Z_p et la manipulation de telles fonctions peut se faire à partir de diverses représentations ; dans le second chapitre nous avons étudié le lien existant entre les différentes expressions de telles fonctions grâce à des représentations matricielles de structure tensorielle simple . Ceci nous a permis d'élaborer un algorithme de minimisation de l'expansion canonique de Reed-Muller généralisée [20].

Le troisième chapitre est consacré à l'étude de la factorisation d'une permutation des sommets de l'hypercube en un produit de permutations élémentaire Sur cette question nous apportons une solution dans le cas des permutations affines et nous abordons partiellement le cas général .

En annexe nous reprenons le texte d'un rapport de recherche -fait en collaboration avec E.Goles [37] - dans lequel nous avons étudié quelques aspects du comportement dynamique du processus d'expression génétique , en adaptant un formalisme booléen qui permet de généraliser les travaux efféctués dans ce domaine par R.Thomas [44] .

PREMIER CHAPITRE

ITERATIONS SUR DES FONCTIONS DE Z_p^n dans Z_p^n

I - PRELIMINAIRES

Pour $n \geq 1$, $\{0,1\}^n$ désigne l'ensemble des n-uplets $x = (x_1, x_2, \ldots, x_n)$ où $x_i \in \{0,1\}$. Une fonction booléenne F dans $\{0,1\}^n$ est une application de $\{0,1\}^n$ dans lui-même qui à $x \in \{0,1\}^n$ fait correspondre l'élément $F(x) = (f_1(x), f_2(x), \ldots, f_n(x))$.

On associe à F le graphe orienté G(F) dont l'ensemble des sommets est en bijection avec $\{0,1\}^n$ et l'ensemble des arcs est $\{(x,y) / y = F(x)\}$. G(F) est appelé graphe d'itération de F.

Nous nous intéressons à l'étude du comportement de l'itération

$$x^{r+1} = F(x^r) \qquad r = 0,1,2,\ldots$$

à partir d'un $x^0 \in \{0,1\}^n$.

Cette itération peut être complètement décrite si on est en mesure de construire G(F) ce qui n'est envisageable que si n est petit car le nombre de sommets de G(F) est 2^n.

La seule possibilité d'étudier cette itération serait de la décrire -au moins localement- à partir d'une expression analytique de la fonction F.

Dans [34] F. Robert a mis en évidence une notion de constraction booléenne et de rayon spectral booléen permettant d'étudier la convergence d'une telle itération et de transposer des résultats d'analyse numérique au contexte booléen. [32, 33].

Différentes classes de fonctions booléennes ont été par ailleurs étudiées dans [15,16]

Dans ces travaux, les opérations considérées dans l'expression analytique de F sont celles de l'Algèbre de Boole usuelle :

$B = (\{0,1\}, \vee, ., -)$ caractérisées par

$$a \vee b = 0 \iff a = b = 0$$
$$a \,.\, b = 1 \iff a = b = 1$$
$$\bar{a} = 0 \iff a = 1$$

On peut également exprimer une fonction booléenne à l'aide des opérations de $Z_2 = (\{0,1\}, +, ., -)$ caractérisées par

$$a + b = 0 \iff a = b$$
$$a \,.\, b = 1 \iff a = b = 1$$
$$\bar{a} = a + 1$$

Notons que la loi "." est la même dans Z_2 et B et les lois $\vee$ et $+$ sont liées par les relations

$$a + b = \bar{a}b \vee a\bar{b}$$

et $\forall a \in \{0,1\}$ et $\forall b \in \{0,1\}$

$$a \vee b = a+b+ab$$

Ces deux relations permettent donc de passer d'une expression dans B d'une fonction booléenne à son expression dans Z_2 et réciproquement.

Exemple 1 : n = 4

x	F(x)
0000	1110
0001	0010
0010	1001
0011	0101
0100	0010
0101	1110
0110	0101
0111	1001
1000	0100
1001	1000
1010	0011
1011	1111
1100	1000
1101	0100
1110	1111
1111	0011

Donc F s'écrit :

$$f_1(x) = \bar{x}_1 x_2 x_4 \vee x_1 \bar{x}_2 x_4 \vee x_1 x_2 \bar{x}_4 \vee \bar{x}_1 \bar{x}_2 \bar{x}_4$$

$$f_2(x) = \bar{x}_2 x_3 x_4 \vee x_2 \bar{x}_3 x_4 \vee x_2 x_3 \bar{x}_4 \vee \bar{x}_2 \bar{x}_3 \bar{x}_4$$

$$f_3(x) = x_1 \bar{x}_3 \vee x_3 \bar{x}_1$$

$$f_4(x) = x_3$$

et dans Z_2, F s'écrit :

$$f_1(x) = x_1 + x_2 + x_4 + 1$$

$$f_2(x) = x_2 + x_3 + x_4 + 1$$

$$f_3(x) = x_1 + x_3$$

$$f_4(x) = x_3$$

Pour une fonction booléenne F on notera :

$$F : B^n \to B^n \quad \text{ou} \quad F : Z_2 \to Z_2$$

pour exprimer que les opérations choisies dans l'écriture de F sont celles de B ou celles de Z_2.

L'exemple 1 illustre bien le fait que les opérations choisies peuvent, dans certains cas, faciliter l'étude du graphe d'itération de F, puisque dans cet exemple, F est affine dans Z_2.

Il apparait donc qu'il est intéressant de trouver des critères simples permettant de reconnaître si une fonction F de B^n dans lui-même est affine en tant qu'application de Z_2^n dans lui-même.

Notations :

Pour $x \in \{0,1\}^n$ et $\alpha \in \{0,1\}^n$ on note

$$x^\alpha = (x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n})$$

où

$$x_i^{\alpha_i} = \begin{cases} x_i & \text{si } \alpha_i = 1 \\ \bar{x}_i & \text{sinon} \end{cases}$$

Si J est une partie de $\{1,2,\ldots,n\}$ on définit P_J par

$$P_J(x) = \prod_{j \in J} x_j \qquad \forall x \in \{0,1\}^n$$

Pour $x \in \{0,1\}^n$ on définit la parité de x sur J par

$$w_J(x) = \sum_{i \in J} x_i \qquad \text{(somme dans } Z_2\text{)}$$

Propriétés

1- $\overline{a+b} = \bar{a} + b = a + \bar{b} = a + b + 1$

2- $\overline{a \vee b} = \bar{a}\bar{b} \vee ab$

3- $w_J(x) = \bigvee_{w_j(\alpha)=1} P_J(x^\alpha)$ où la somme est étendue à tous les α tels que

$w_J(\alpha) = 1$ et $J \subset \{1,2,\ldots,n\}$

4- $\overline{w_J(x)} = \bigvee_{w_J(\alpha)=0} P_J(x^\alpha)$

Démonstration :

Les propriétés 1 et 2 sont immédiates à partir des définitions de + et v . Les propriétés 3 et 4 se vérifient facilement par récurrence sur le nombre d'élément de J.

Proposition :

Soit $f : B^n \to B$, alors f est affine comme application de Z_2^n dans Z_2 ssi $\exists J \subset \{1,2,\ldots,n\}$ tel que

(1) $f(x) = \bigvee_{\alpha} P_J(x^{\alpha})$ où la somme booléenne est étendue à tous les α ayant même parité sur J.

Démonstration

f affine dans Z_2 <=> $\exists J \subset \{1,2,\ldots,n\}$ et $\varepsilon \in \{0,1\}$ tels que

$$f(x) = \sum_{i \in J} x_i + \varepsilon$$

qui s'écrit

$$f(x) = w_J(x)+\varepsilon = \bigvee_{w_J(\alpha)=\bar{\varepsilon}} P_J(x^{\alpha}) \text{ d'après les propriétés 3 et 4.}$$

On peut immédiatement déduire de cette proposition qu'une fonction $F : B^n \to B^n$ est affine en tant qu'application de Z_2^n dans Z_2^n si et seulement si chaque composante f_i de F est du type (1).

Dans l'exemple 1, toutes les composantes f_i de F dans l'écriture booléenne sont du type (1) donc $F : Z_2^n \longrightarrow Z_2^n$ s'écrit

$$F(x) = Ax+b$$

où A est la matrice d'incidence de F ($a_{ij} = 1$ ssi f_i dépend de x_j) et b est construit directement à partir de "la parité du nombre de barre" dans les monômes de chaque f_i ; plus précisément, si $f_i = \bigvee_{\alpha} P_J(x^{\alpha})$ alors $b_i = \overline{w_J(\alpha)}$.

Dans cet exemple :

$$A = \begin{bmatrix} 1101 \\ 0111 \\ 1010 \\ 0010 \end{bmatrix} \qquad \text{et } b = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

(Remarquons que A ne dépend pas des opérations choisies pour exprimer F).

Dans cette première partie, nous allons étudier de manière plus générale certaines classes de fonctions de Z_p^n dans Z_p^n où p est un nombre premier quelconque.

II - PROPRIETES DU GRAPHE D'ITERATION D'UNE FONCTION AFFINE

Soit p un nombre premier ≥ 2, l'ensemble Z_p des entiers modulo p est un corps et pour $n \geq 1$, Z_p^n désigne l'espace vectoriel de dimension n sur Z_p et on note $\mathcal{M}_n(Z_p)$ l'ensemble des matrices carrées d'ordre n à éléments dans Z_p.

L'étude du graphe d'itération d'une application linéaire

$$F : Z_p^n \to Z_p^n$$

$$x \to F(x) = Ax$$

a été très développée [13] [38]. Elle repose essentiellement sur la recherche d'une matrice A^* semblable à A (matrice compagnon ou forme normale), qui admet par conséquent la même structure de graphe. Mais dans la pratique, le calcul de A^* reste onéreux, car les algorithmes proposés reposent sur la détermination des diviseurs élémentaires de A.

Dans ce chapitre nous nous proposons de donner quelques propriétés du graphe d'itération G(F) d'une application affine :

$$F : Z_p^n \to Z_p^n$$

$$x \to F(x) = Ax+b \text{ où } A \in \mathcal{M}_n(Z_p) \text{ et } b \in Z_p^n$$

1- Structure des arbres

Définitions :

a) Soient x et y appartenant à Z_p^n tels que :

- $\exists\, r \geq 1 : F^r(x) = y$
- $\forall r' < r \quad F^{r'}(x) \neq y$
- $\forall s \geq 1 \quad F^s(y) \neq x$

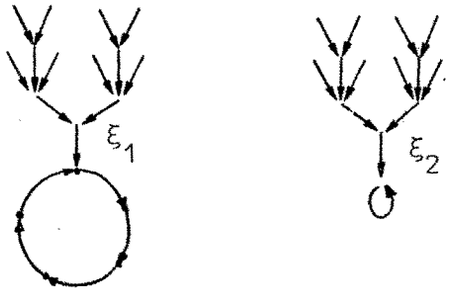
alors x est appelé r-antécédant de y.

b) Soit ξ appartenant à un cycle de G(F), le sous-graphe de G(F) contenant ξ et tous ses r-antécédants pour $r \geq 1$ est appelé arbre de racine ξ. Le plus petit entier ℓ tel que ξ n'admette aucun r-antécédant pour $r > \ell$ est appelé longueur de l'arbre.

c) Soient G_1 et G_2 deux arbres de G(F) de racine respectivement ξ_1 et ξ_2, nous dirons que G_1 et G_2 sont isomorphes s'il existe une bijection ϕ de G_1 dans G_2 telle que :

$$\forall x \in G_1 , \quad F(\phi(x)) = \phi(F(x))$$

Exemple :



Dans ce graphe ξ_1 et ξ_2 ont des arbres isomorphes de longueur 4.

Proposition 1.1

Si F est une application affine de Z_p^n dans Z_p^n, il existe $s \geq 1$ tel que

$$\forall x \in Z_p^n \quad \text{card } F^{-1}(x) \in \{0, p^s\}.$$

Démonstration :

Il est clair que $F^{-1}(b)$ est un sous-groupe de Z_p^n donc son ordre divise p^n c'est-à-dire :

$$\exists s \geq 1 \text{ tel que card } F^{-1}(b) = p^s$$

Soit $x \in Z_p^n$ tel que $F^{-1}(x) \neq \emptyset$ et soit $x^1 \in F^{-1}(x)$. On vérifie alors que :

$$F^{-1}(x) = F^{-1}(b)+x^1$$

donc card $F^{-1}(x)$ = card $F^{-1}(b) = p^s$.

Proposition 1.2

Les éléments de tous les cycles ont des arbres isomorphes.

Démonstration :

Soient ξ_1 et ξ_2 deux points appartenant à des cycles de longueur respectivement k_1 et k_2 notés $C_{k_1}(\xi_1)$ et $C_{k_2}(\xi_1)$

$\forall r \geq 1$, $\exists \nu_i \geq 0$ $\quad i = 1,2$ tels que ν_i+r est un multiple de k_1

Si $C^r(\xi_i)$ désigne l'ensemble des r-antécédants de ξ_i, posons :

$$\phi_r : C^r(\xi_1) \to C^r(\xi_2)$$

$$x \to \phi_r(x) = x+(p-1)F^{\nu_1}(\xi_1)+F^{\nu_2}(\xi_2)$$

et montrons que $\forall r \geq 1$, ϕ_r est une bijection.
(Notons d'abord que si $C^1(\xi_1)$ est vide alors $C^1(\xi_2)$ l'est aussi d'après la proposition 1.1).

* Vérifions que si $x \in C^r(\xi_1)$ alors $\phi_r(x) \in C^r(\xi_2)$

- $F^r(\phi_r(x)) = A^r x+(p-1)A^r F^{\nu_1}(\xi_1)+A^r F^{\nu_2}(\xi_2)+A_r b$

où $A_r b = (I+A+\ldots+A^{r-1})b$

$$F^r(\phi_r(x)) = F^r(x)+(p-1)A_r b+(p-1)[F^{r+\nu_1}(\xi_1)+(p-1)A_r b] + F^{\nu_2+r}(\xi_2)$$

$$= \xi_1+(p-1)F^{k_1}(\xi_1)+F^{k_2}(\xi_2)$$

$$= \xi_1+(p-1)\xi_1+\xi_2$$

$$= \xi_2$$

- Supposons qu'il existe $m < r$ tel que $F^m(\phi_r(x)) = \xi_2$ on aura
$F^m(\phi_r(x)) = F^m(x)+(p-1)F^{m+\nu_1}(\xi_1)+F^{m+\nu_2}(\xi_2) = \xi_2$

Si $k = p.p.c.m.(k_1,k_2)$ on obtient :

$$F^q(\xi_2) = F^{m+q}(x)+(p-1)F^{m+\nu_1+q}(\xi_1)+F^{m+\nu_2+q}(\xi_2)$$

$$\xi_2 = F^{m+q}(x)+(p-1)F^{m+\nu_1}(\xi_1)+F^{m+\nu_2}(\xi_2)$$

d'où :

$$F^{m+q}(x) = F^m(x) \qquad \forall x \quad C^r(\xi_1)$$

et alors :

$F^m(x) \in C_{k_1}(\xi_1)$ ce qui est impossible quand $m < r$

* Vérifions que $\forall r \geq 1, \phi_r$ est une bijection :

$$\phi_r(x) = \phi_r(y) \iff x+(p-1)F^{\nu_1}(\xi_1)+F^{\nu_2}(\xi_2) = y+(p-1)F^{\nu_1}(\xi_1)+F^{\nu_2}(\xi_2)$$

$$\iff x=y.$$

Ainsi $\forall r \geq 1$, ϕ_r est une bijection, d'où le résultat.

L'ensemble $\mathcal{M}_n(Z_p)$ étant fini, il existe deux entiers r et q tels que :

$$A^{r+q} = A^r \qquad (1)$$

Si r et q sont les plus petits entiers tels que (1) alors r est la longueur des arbres du graphe d'itération de F. En général, q peut prendre toutes

les valeurs entre 1 et p^n (en fait on montrera par la suite que $q \leq p^n-1$) par contre r reste petit par rapport à p^n. Nous nous proposons maintenant de trouver la meilleure borne supérieure (atteinte) de r.

Lemme :

Soit $M \in \mathcal{M}_n(Z_p)$ nilpotente, si m est le plus petit entier tel que $A^m = 0$ alors $m \leq n$.

Démonstration :

Supposons que $m > n$ et écrivons $m = n+k$, $k \geq 1$,le polynôme caractéristique de A est de la forme :

$$\det(A-\lambda I) = \lambda^s P_{n-s}(\lambda) \text{ où } s \geq 1 \text{ et } P_{n-s}(\lambda)$$

est un polynôme en λ de degré n-s tel que $P_{n-s}(0) \neq 0$.
Posons :

$$P_{n-s}(\lambda) = a_0+a_1\lambda+\ldots+a_{n-s}\lambda^{n-s}$$

Par le théorème de Caylay-Hamilton on obtient :

$$a_0+a_1A+\ldots+a_{n-s}A^{n-s} = 0.$$

En multipliant cette égalité par A^{m-s-1} on trouve :

$$a_0A^{m-s-1} = 0$$

Or m est le plus petit entier tel que $A^m = 0$ donc nécessairement $a_0 = 0$ ce qui contredit le fait que $P_{n-s}(0) = a_0 \neq 0$.

Proposition 1.3

Pour toute application affine F de $\{0,1\}^n$, la longueur des arbres de F est inférieure à n.

Démonstration :

Si $G(x) = Ax+b$

et $G'(x) = S^{-1}ASx+S^{-1}b$ où $S \in \mathcal{M}_n(Z_p)$ non singulière

alors, il est clair que G et G' ont la même structure de graphe. (en effet $G'(x) = y \Leftrightarrow G(Sx) = Sy$).

D'autre part, on sait que toute matrice à élément dans Z_p est semblable à une matrice du type :

$$\begin{bmatrix} A_1 & 0 \\ 0 & A_o \end{bmatrix}$$

où A_1 et A_o sont des matrices carrées à éléments dans Z_p telles que A_1 est non singulière et A_o nilpotente [38]

On peut donc supposer que l'application affine F est de la forme $F(x) = Ax+b$ où A est du type précédent.

Soient q et r les plus petits entiers tel que $A_1^q = I$ et $A_o^r = 0$.
Il vient :

$$A^{r+q} = \begin{bmatrix} A^{r+q} & 0 \\ 1 & \\ & \\ 0 & A_o^{r+q} \end{bmatrix} = \begin{bmatrix} A_1^r & 0 \\ & \\ 0 & 0 \end{bmatrix} = A^r$$

Or r est la longueur des arbres du graphe de F et d'après le lemme précédent $r \leq n$, ce qui démontre la proposition.

Remarquons que pour les applications affines $F(x) = Ax+b$ où A et b sont à éléments dans $\{0,1\}$, les itérations successives conduites sur F dans Z_2 aboutissent à des cycles éventuellement très grands (entre 1 et 2^n-1) et des arbres relativement courts (entre 0 et n) par contre les itérations conduites dans B^n sur une application affine $G(x) = Ax \vee b$ aboutissent à des cycles très courts par rapport à 2^n (entre 1 et $2^{n/2}$) et des arbres relativement longs (entre 1 et n^2). [15]

2 - Structure des cycles

Soient $A \in \mathcal{M}_n(Z_p)$ et r et q les plus petits entiers tels que

$$A^{r+q} = A^r$$

Proposition 2.1

Pour toute fonction affine $F(x) = Ax+b$ on a

$$\forall x \in Z_p^n \quad F^{r+pq}(x) = F^r(x)$$

Démonstration

$\forall x \in Z_p^n$ on a :

$$F^{r+pq}(x) = A^{r+pq}x+(I+A+\ldots+A^{r+pq-1})b$$

. $A^{r+q} = A^r \Rightarrow \forall k \in \mathbb{N}$, $A^{r+kq} = A^r$

en particulier $A^{r+pq} = A^r$

. Calculons $\sum_{k=0}^{r+pq-1} A^k$

$$\sum_{k=0}^{r+pq-1} A^k = \sum_{k=0}^{r-1} A^k + A^r \sum_{k=0}^{q-1} A^k + A^{r+q} \sum_{k=0}^{q-1} A^k + \ldots + A^{r+(p-1)q} \sum_{k=0}^{q-1} A^k$$

$$= \sum_{k=0}^{r-1} A^k + (A^r+A^{r+q}+\ldots+A^{r+(p-1)q}) \sum_{k=0}^{q-1} A^k$$

Or

$$A^r+A^{r+q}+\ldots+A^{r+(p-1)q} = pA^r = 0$$

d'où :

$$\sum_{k=0}^{r+pq-1} A^k = \sum_{k=0}^{r-1} A^k$$

donc $F^{r+pq}(x) = A^r x+(I+A+\ldots+A^{r-1})b = F^r(x)$

D'où le résultat.

Ainsi, les cycles d'une application affine ($F(x) = Ax+b$, $b \neq 0$) sont de longueur des diviseurs de pq, alors que dans le cas linéaire $F(x) = Ax$ les cycles sont de longueur des diviseurs de q. En outre, quand $b \neq 0$, on a la proposition suivante :

Proposition 2.2

Si F admet un point fixe, alors F n'admet que des cycles de longueur des diviseurs de q.

Démonstration :

Supposons exister $\xi \in Z_p^n$ tel que $F(\xi) = \xi$ et soient r et q les plus petits entiers tel que $A^{r+q} = A^r$

$$\forall x \in Z_p^n \quad F^{r+q}(x) = A^r x + (I+A+\ldots+A^{r+q-1})b$$

puisque $b = (I-A)\xi$ on a :

$$(I+A+\ldots+A^{r+q-1})b = (I+A+\ldots+A^{r-1})b + A^r(I+A+\ldots+A^{q-1})(I-A)$$

$$= (I+A+\ldots+A^{r-1})b + A^r(I-A^q)\xi$$

$$= (I+A+\ldots+A^{r-1})b$$

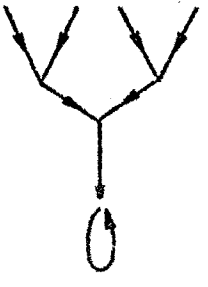
d'où

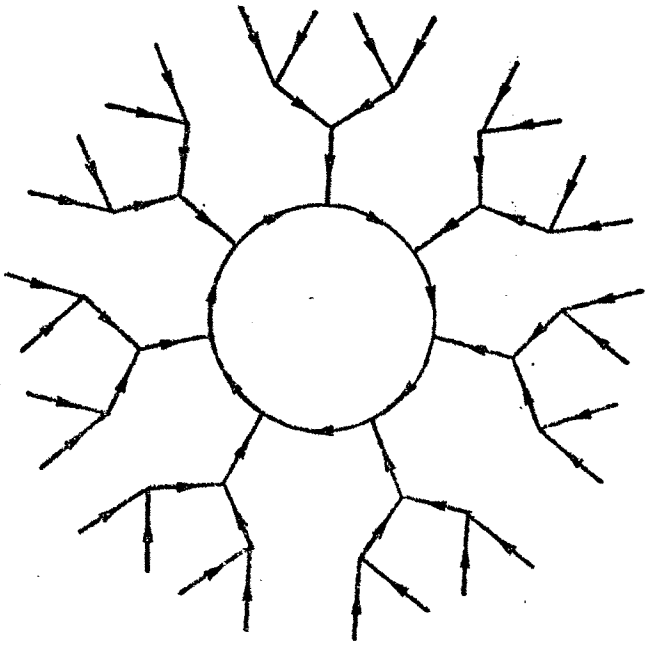
$$F^{r+q}(x) = F^r(x).$$

Nous donnons une série d'exemples illustrant les différentes propriétés établies dans ce chapitre.

Exemple 1 :

$$A = \begin{bmatrix} 001100 \\ 000011 \\ 101100 \\ 001000 \\ 010000 \\ 010000 \end{bmatrix} \qquad b = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$





Le graphe d'itération de $F(x) = Ax+b$ illustre les différentes propriétés établies dans ce chapitre :

- $\forall x \in Z_2^6$ card $F^{-1}(x) \in \{0,2\}$ (prop. 1.1)

- les éléments de tous les cycles ont des arbres isomorphes (prop. 1.2)

- la longueur des arbres est inférieure à 6 (prop. 1.3).

Exemple 2 : p = 2, n = 7

$$A = \begin{bmatrix} 1000100 \\ 0110000 \\ 1100000 \\ 0010000 \\ 0110000 \\ 0001100 \\ 0110110 \end{bmatrix}$$

Le graphe d'itération de F(x) = Ax est un arbre de longueur 7 (c'est un exemple où la borne de la proposition 1.3 est atteinte) (voir fig. 1).

Exemple 3 : n = 4, p = 2

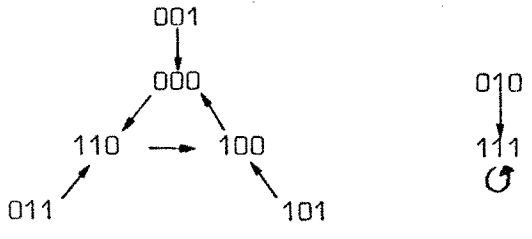
$$F(x) = \begin{bmatrix} 1110 \\ 0101 \\ 1111 \\ 1000 \end{bmatrix} x + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Le graphe d'itération de F est constitué d'un unique point fixe et d'un unique cycle de longueur 15 = 2^4-1 (voir fig. 2). Ainsi dans le cas général on ne peut espérer donner une borne des cycles meilleure que p^n-1.

Remarque

Si le graphe d'itération d'une fonction F de Z_p^n dans lui-même vérifie toutes les propriétés établies dans ce chapitre, la fonction F n'est pas nécessairement affine.

Par exemple : p = 2 , n = 3



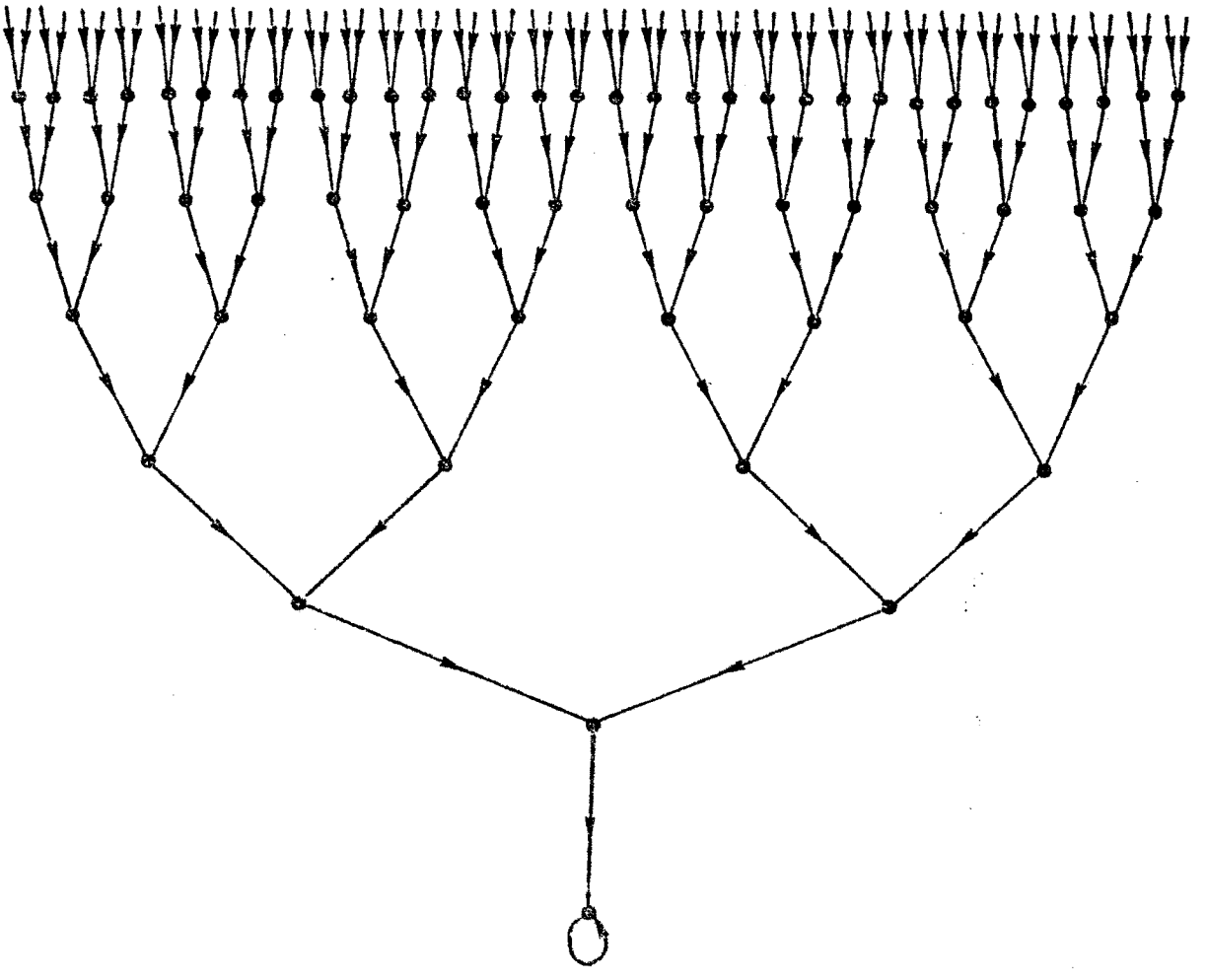


Figure 1 - Graphe d'itération - Exemple 2

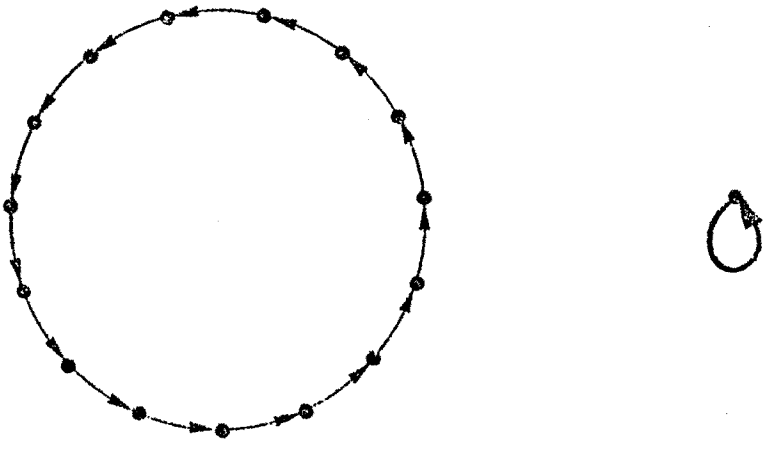


Figure 2 - Graphe d'itérations - Exemple 3

III - ANALYSE D'UN CAS PARTICULIER DE MATRICES

Dans ce chapitre nous nous intéressons aux matrices $A \in \mathcal{M}_n(Z_p)$ ayant par ligne (ou par colonne), exactement deux éléments non nuls et égaux à un.

Ce type de matrice correspond (quand p = 2) à la modélisation discrète de l'étude du comportement dynamique du processus d'expression génétique dans le cas où l'expression de chaque gène est un "ou-exclusif" de l'état d'excitation d'exactement deux gènes (fig.1). [43] [44] [45] [48]

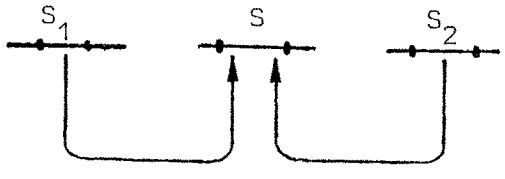


Fig. 1 état(S) = état(S_1) + état(S_2) (+ : ou-exclusif)

Les expériences citées dans [19] révèlent dans la dynamique de tels réseaux, une "grande" probabilité de rencontre des oscillateurs (cycles).

Dans le paragraphe suivant, nous allons déterminer le nombre d'états du réseau qui mènent en un pas, à l'état stationnaire où aucun gène ne s'exprime et par là confirmer la présence éventuelle de grands cycles.

1. Formulation et résultats

Soit $A \in \mathcal{M}_n(Z_p)$ (p premier impair) dont chaque ligne ne comporte que deux éléments non nuls et égaux à un.

Considérons la fonction :

$$F : Z_p^n \to Z_p^n$$

$$x \to F(x) = Ax+b \quad \text{où } b \in Z_p^n$$

Le problème est de déterminer :

$$\text{Card } \{x \in Z_p^n \ / \ F(x) = 0\}.$$

On a vu précédemment que si $\{x \in Z_p^n \ / \ F(x) = 0\}$ est non vide, alors

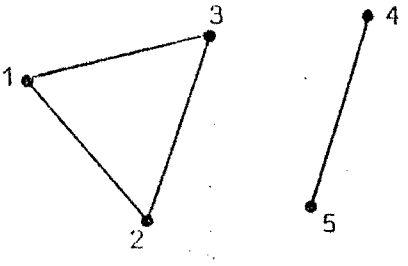
$$\text{card}\{x \in Z_p^n \ / \ F(x) = 0\} = \text{card}\{x/F(x)=b\} = \text{card}\{x/Ax=0\}$$

Notons G le graphe dont A est la matrice d'incidence arêtes-sommets, c'est-à-dire le graphe ayant n sommets, numérotés de 1 à n, tel que 2 sommets i et j sont reliés par une arête si et seulement si il existe dans A une ligne ayant ses deux uns en position i et j.
Pour $\xi \in Z_p^n$, notons G_ξ le sous-graphe de G dont les sommets correspondent aux positions non nulles de ξ ($G_0 = \emptyset$).

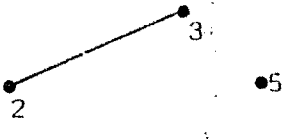
Exemple : n = 5 , p = 3

$$A = \begin{bmatrix} 10100 \\ 01100 \\ 00011 \\ 11000 \\ 10100 \end{bmatrix}$$

G :



si $\xi = \begin{bmatrix} 0 \\ 2 \\ 1 \\ 0 \\ 2 \end{bmatrix}$ G_ξ :



Proposition 1.1

Avec les notations précédentes et quand p > 2, on a :
$A\xi = 0 \Rightarrow G_\xi$ est une union de composantes connexes de G qui ne contiennent pas de cycle impair.

Démonstration :

Supposons que $A\xi = 0$, et soit i tel que $\xi_i \neq 0$ (si $\xi = 0$ la proposition est triviale). Notons C(i) la composante connexe de G contenant le sommet i montrons qu'alors $\forall j \in C(i) \quad \xi_j \neq 0$.

Soit $i = i_1, i_2, \ldots, i_r = j$ une chaîne dans C(i) joignant i et j puisque $A\xi = 0$ on a :

$$\xi_{i_1} + \xi_{i_2} = 0$$

$$\xi_{i_2} + \xi_{i_3} = 0$$

$$\vdots$$

$$\xi_{i_{r-1}} + \xi_{i_r} = 0$$

ainsi $\xi_{i_r} = (-1)^{r-1} \xi_{i_1}$ et donc $\forall j \in C(i) \quad \xi_j \neq 0$; ce qui prouve que G_ξ est une union de composantes connexes de G.

Supposons que G_ξ contienne une composante connexe ayant un cycle $j = j_1, j_2, \ldots, j_k = j$ alors, le même raisonnement que dans le cas d'une chaîne donnerait : $\xi_j = (-1)^{k-1} \xi_j$ => k est nécessairement impair (car $p \neq 2$), c'est-à-dire que le cycle est de longueur pair , d'où le résultat.

Il est clair, par ailleurs, que si un $\xi \in Z_p^n$ est tel que
- G_ξ est une union de composantes connexes de G sans cycle impair et
- i et j voisins => $\xi_i = -\xi_j$

alors $A\xi = 0$.

Corollaire :

Si k est le nombre de composantes connexes sans cycle impair dans G alors :

$$\text{card}\{x \in Z_p^n \ / \ Ax = 0\} = p^k$$

Démonstration :

Ecrivons $\quad G = I \cup (C_1 \cup C_2 \cup \ldots \cup C_k)$

où I est l'union des composantes connexes de G avec un cycle impair, et les C_i, $1 \leq i \leq k$, les k composantes connexes de G sans cycle impair.

D'après la proposition 1.1 et la remarque précédente Ax = 0 si et seulement si :

- $x_i = 0 \quad \forall i \in I$
- pour tout j, $x_{j_1} = -x_{j_2}$ pour tout couple de sommets voisins j_1 et j_2 de C_j

Le nombre possible de tel x est donc p^k.

Conséquences

Avec les notations précédentes on a :

A inversible dans $\mathcal{M}_n(Z_p)$ $(p \neq 2)$ si et seulement si toutes les composantes connexes de G contiennent un cycle impair.

Le plus grand cycle de F(x) = Ax+b est de longueur p^{n-k}

Remarques

Le cas p = 2 se traite de manière analogue sans que la notion de cycle impair intervienne puisque dans Z_2^n on a x = -x, et dans ce cas on a :

$\text{card}\{x \in Z_2^n \ / \ Ax = 0\} = p^{\nu}$ où ν est le nombre de composantes connexes de G.

Ainsi, pour cette classe de matrice, nous pouvons obtenir certaines propriétés du graphe d'itération ayant p^n sommets au vu du graphe G ayant n sommets, néanmoins la description complète du graphe d'itération reste difficile dans le cas général.

2. Exemple [25]

Soit A $\mathcal{M}_n(Z_2)$ la matrice définie par :

$$A = \begin{bmatrix} 1100 \ldots 0 \\ 0110 \ldots 0 \\ \vdots \quad\quad \vdots \\ 000 \ldots 11 \\ 100 \ldots 01 \end{bmatrix}$$

Quelles sont les plus petits entiers r et q vérifiant

$$A^{r+q} = A^r$$

Le polynôme caractéristique de A est

$$P_A(X) = (1+X)^n+1$$

En remarquant que pour toute valeur propre de A rang $(A-\lambda I) = n-1$ on déduit que le polynôme minimal de A est égal à son polynôme caractéristique, et on peut énoncer les résultats suivants concernant la valeur de r.

THEOREME 1

1) si n est de la forme $n = 2^\ell$ alors A est nilpotente
2) si n est de la forme $n = 2m+1$ alors $r = 1$
3) si n est de la forme $n = 2^\ell(2m+1)$ alors $r = 2^\ell$.

Démonstration :

1) $n = 2^\ell$

$P_A(A) = 0 \Rightarrow (I+A)^{2^\ell}+1 = 0$

or dans un corps fini de caractéristique 2 on a $\forall \ell \in \mathbb{N}$ $(1+X)^{2^\ell} = 1+X^{2^\ell}$

d'où $I+A^{2^\ell}+I = 0 \Rightarrow A^{2^\ell} = 0 \Rightarrow$ A est nilpotente

2) $n = 2m+1$

$P_A(X) = (1+X)^n+1 = \sum_{j=1}^{n} C_n^j X^j$ (où C_n^j sont les coefficients du binôme calculés modulo 2)

$P_A(X) = X \sum_{j=1}^{n} C_n^j X^{j-1}$ $\quad C_n^1 = n$ étant impair $\quad n = 1 \bmod(2)$

$P_A(X) = X\,\Psi(X)$ où $\Psi(X)$ est tel que $\Psi(0) \neq 0$

d'où $r = 1$.

3) $n = 2^{\ell}(2m+1)$

$$P_A(X) = 1+X)^{2^{\ell}(2m+1)}+1 = (1+X^{2^{\ell}})^{2m+1}+1 = \sum_{j=1}^{2m+1} C^{j}_{2m+1} X^{2^{\ell}j}$$

$$P_A(X) = X^{2^{\ell}} \sum_{j=1}^{2m+1} C^{j}_{2m+1} X^{2^{\ell}(j-1)}$$

or $C^{1}_{2m+1} = 1 \bmod (2)$ d'où

$$P_A(X) = X^{2^{\ell}}\phi(x) \text{ où } \phi(0) \neq 0$$

et $r = 2^{\ell}$.

Ce théorème donne la valeur de r en fonction seulement de la donnée de n, par contre la connaissance de q reste incomplète. En notant q(N) la valeur de q quand $A \in \mathcal{M}_N(Z_2)$ on a :

THEOREME 2

* Si n est un entier impair alors :

i) q(n) divise $2^{f}-1$ où f est le plus petit entier tel que $2^{f}-1$ soit un multiple de n.

ii) $q(n) \geq n$

* Si n est de la forme $2^{\ell}(2m+1)$ alors

i) $q(n) = 2^{\ell}q(2m+1)$ si $m \neq 0$

ii) $q(n) = 1$ si $m = 0$

Démonstration :

Supposons que n est impair.

Posons $J = I + A$

$$J = \begin{bmatrix} 010 \ldots 0 \\ 0010 \ldots 0 \\ \vdots \\ 00 \ldots .10 \\ 10 \ldots .00 \end{bmatrix}$$

Il est facile de voir que $J^{n} = I$ et $J^{k} \neq I \quad \forall k < n$.

i) Soit f le plus petit entier tel que 2^f-1 soit un multiple de n.
f existe, car n étant impair, il est premier avec 2 et dans le groupe cyclique $Z_n-\{0\}$ des entiers non nuls modulo n, 2 est générateur, c'est à-dire : $\exists k$ tel que $2^k = 1 \pmod n$
d'où :

$$A^{2^f} = (I+J)^{2^f} = I+J^{2^f} = I+J = A$$

or quand n est impair, d'après le théorème 1, r = 1 donc q(n) divise 2^f-1.

ii) Quand n est impair on a $A^{q(n)+1} = A$ c'est-à-dire que le polynôme $p(X) = X(X^{q(n)}+1)$ annule A => $P_A(X)$ divise p(X)
=> $n \leq q(n)+1$ et on ne peut avoir l'égalité car sinon on aurait :

$(1+X)^n+1 = X(X^{q(n)}+1)$ ce qui est impossible puisque cette égalité n'est pas vérifiée pour X=1.

donc $q(n) \geq n$.

Supposons maintenant que $n = 2^\ell(2m+1)$.

i) $m \neq 0$
D'après les théorème 1, quand $n = 2^\ell(2m+1)$ $m \neq 0$ alors $r = 2^\ell$ donc le polynôme minimal s'écrit sous la forme

$$P_A(X) = (1+X)^{2^\ell(2m+1)}+1 = X^{2^\ell}\Psi(X) \text{ avec } \Psi(0) \neq 0$$

or q(n) est défini comme étant le plus petit entier tel que $\Psi(X)$ divise $X^{q(n)}-1$:

$$(1+X)^{2^\ell(2m+1)}+1 = X^{2^\ell}\ \frac{X^{q(n)}-1}{Q(x)}\ , Q(0) \neq 0\ ,$$

d'autre part :

$$(1+X)^{2^\ell(2m+1)}+1 = (1+X^{2^\ell})^{2m+1}+1 = X^{2^\ell}\ \frac{X^{2^\ell q(2m+1)}-1}{R(X)}$$

car en dimension 2m+1 le polynôme minimal est de la forme

$$(1+X)^{2m+1}+1 = Y\,\frac{Y^{q(2m+1)}-1}{R(X)} \text{ où } R(X) \neq 0$$

donc $q(2^{\ell}(2m+1)) = 2^{\ell}q(2m+1)$

ii) Si $m = 0$, $n = 2^{\ell}$ et dans ce cas on a vu que A est nilpotente, d'où $q(n) = 1$.

En conclusion, pour compléter l'étude de la structure du graphe d'une telle matrice A, il faudrait déterminer la valeur q(n) quand n est impair. Nous sommes en mesure d'établir que $q(n) = 2^{f}-1$ si et seulement si q(n) est un multiple de n et il apparaît (sans qu'on ait pu le démontrer !) qu'en fait q(n) est toujours un multiple de n.

IV - CARACTERISATION DES PERMUTATIONS CYCLIQUES AFFINES

Soit K un corps fini de caractéristique un nombre premier $p \geq 2$
K est alors d'ordre $q = p^f$ avec $f \geq 1$.
Pour $n \geq 1$, soit

$$F : K^n \to K^n$$

$$x \to F(x) = Ax+b$$

où $A \in \mathcal{M}_n(K)$ et $b \in K^n-\{0\}$

F est une permutation affine que nous dirons cyclique si le graphe d'itération de F est constitué d'un unique cycle de longueur p^{nf}, c'est-à-dire

$$\forall x \in K^n \quad \{F^r(x), r = 0,1,\ldots,p^{nf}-1\} = K^n$$

Dans ce chapitre nous nous proposons de caractériser de telles permutations. Dans un premier temps, nous avions étudié le cas où $K = Z_2$, puis dans une note de R.V.MOODY et I.G. ROSENBERG [24], le problème a été résolu dans le cas $K = Z_p$ (p, premier quelconque). Une étude plus détaillée utilisant des arguments différents de ceux utilisés dans [24] nous a permis de donner une réponse au cas plus général où K est un corps fini quelconque.

1- Quelques résultats sur les matrices régulières

Soit K un corps fini de caractéristique $p \geq 2$ et de cardinal p^f, $f \geq 1$. Pour $n \geq 2$, on a la caractérisation suivante :

THEOREME 1

Il existe une matrice $A \in \mathcal{M}_n(K)$ telle que $A^{p^{nf-1}} = I$ si et seulement si (n = 2 et f = 1) ou (n = 3, p = 2 et f = 1).

Démonstration :

Soit $A \in \mathcal{M}_n(K)$ / $A^{p^{nf-1}} = I$

alors

$$(I-A)^{p^{nf-1}} = 0$$

donc (I-A) est un endomorphisme nilpotent de l'espace vectoriel K^n, d'où

$$(I-A)^n = 0$$ (démonstration strictement analogue à celle du lemme page 15).

* Supposons que $n \leq p^{nf-2}$

dans ce cas $(I-A)^{p^{nf-2}} = 0 \Rightarrow A^{p^{nf-2}} = I$ ce qui contredit l'hypothèse

* Supposons que $n > p^{nf-2}$

sachant que $p^{nf-2} \geq nf-1$ on a

$$n > p^{nf-2} > nf-2 \Rightarrow n(f-1) < 2$$

et nécessairement f = 1 (car $n \geq 2$), et dans ce cas on a

$$n > p^{n-2} > n-2 \Rightarrow p^{n-2} = n-1$$

et ceci n'est possible que si (n=2) ou (n=3 et p=2).

. Inversement :

* si n = 2 et f = 1 la matrice

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \mathcal{M}_2(Z_p) \quad \forall p \geq 2 \text{ (premier)}$$

et telle que

$$A^p = I$$

* si n = 3, f = 1 et p = 2

la matrice

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \in \mathcal{M}_n(Z_2)$$

et tel que

$$A^4 = I$$

le théorème est ainsi prouvé

2- Caractérisation des permutations affines cycliques

THEOREME 2

Il existe une permutation affine cyclique si et seulement si (n=1 et f=1) ou (n = p = 2 et f = 1).

Démonstration

. Supposons n = 1 et f = 1 alors la permutation F(x) = x+b b ≠ 0 est cyclique

. Supposons n = p = 2 et f = 1 alors la permutation

$$F(x) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} x + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ est cyclique}$$

Soit maintenant F une permutation affine et cyclique

$$F(x) = Ax+b \quad b \neq 0 \text{ et supposons que } n > 1$$

$$\forall k \in \mathbb{N} \; ; \; F^k(x) = A^k x + (I+A+\ldots+A^{k-1})b$$

on pose :

$$A_k = I+A+\ldots+A^{k-1}$$

Par hypothèse on a :

- A non singulier
- $q^n = p^{nf}$ est le plus petit entier k tel que $F^k(0) = 0$

$$\forall x \in K^n, \; F^{q^n}(x) = A^{q^n} x + A_{q^n} b = x$$

En particulier $A^{q^n} b = 0$, ainsi $\forall x \in K^n : A^{q^n} x = x \Rightarrow A^{q^n} = I$.

Soit r le plus petit entier tel que $A^r = I$ $(r < q^n)$, alors r est nécessairement un diviseur de q^n et est donc de la forme $p^\nu = r$.

$$F^{pr}(0) = (I+A+\ldots+A^{pr-1})b$$

$$= (I+A+\ldots+A^{r-1})b+A^r(I+A+\ldots+A^{r-1})b+\ldots+A^{(p-1)r}(I+A+\ldots+A^{r-1})b$$

$$= (I+A^r+\ldots+A^{(p-1)r})A_r b$$

$$= \underbrace{(I+I+\ldots+I)}_{p \text{ fois}} A_r b$$

$$F^{p^{\nu+1}}(0) = 0$$

donc $p^{\nu+1}$ est un multiple de q^n c'est-à-dire $\exists k \in \mathbb{N}$ tel que

$$p^{\nu+1} = kp^{nf} \Rightarrow 1 = kp^{nf-\nu-1} \quad (\text{car } \nu < nf)$$

$$\Rightarrow k = 1 \text{ et } nf = \nu+1 \ (p \geq 2)$$

d'où

$$r = p^{nf-1}$$

ainsi

$$A^{p^{nf-1}} = I \quad \text{et} \quad \forall r < p^{nf-1} \quad A^r \neq I$$

Etude de la structure du graphe de A

1°) Posons $\xi = A^{p^{nf-1}} b$, montrons que $\forall \alpha \leq p-1$ $\alpha\xi$ est un point fixe de A.

$$A(\alpha\xi) = \alpha A\xi = \alpha[A+A^2b+\ldots+A^{p^{nf-1}-1}+A^{p^{nf-1}}]b \quad \text{or } A^{p^{nf-1}} = I$$

$$\Rightarrow A(\alpha\xi) = \alpha(I+A+\ldots+A^{p^{nf-1}})b = \alpha\xi$$

Vérifions que ces p points fixes sont différents.
Si $\alpha\xi = \alpha'\xi$ alors ξ est nul, et dans ce cas

$$f^{p^{nf-1}}(0) = A_{p^{nf-1}}b = \xi = 0$$

ce qui n'est possible que si p = 1.

Donc $\{0, \xi, 2\xi, \ldots, (p-1)\xi\}$ est un sous-ensemble des points fixes de A.

2°) Vérifions que $\forall\alpha$, $1 \leq \alpha \leq p-1$, αb appartient à un cycle, noté $C(\alpha b)$ de longueur p^{nf-1}.
Il est clair que

$$\alpha b \in C(\alpha b) \iff b \in C(b)$$

$$(\text{puisque } A^r(\alpha b) = (\alpha b) \iff A^r b = b)$$

Soit r le plus petit entier tel que $A^r b = b$, r est nécessairement de la forme $r = p^\nu$ avec $\nu \leq nf-1$ (car tous les cycles de A sont de longueur des diviseurs de p^{nf-1}) ; et dans ce cas on a :

$$F^{p^{\nu+1}}(0) = (I+A+\ldots+A^{p^{\nu+1}-1})b$$

$$= (I+A+\ldots+A^{p^\nu-1})b+A^{p^\nu}(I+A+\ldots+A^{p^\nu-1})b+\ldots+$$

$$A^{(p-1)p^\nu}(I+A+\ldots+A^{p^\nu-1})b$$

$$= 0$$

et on a vu que dans ce cas $p^\nu = p^{nf-1}$.

Montrons que si $\alpha \neq \alpha'$ alors $C(\alpha b) \neq C(\alpha' b)$.
Supposons que $\alpha b \in C(\alpha' b)$ alors

$$\exists r < p^{nf-1} \quad \text{tel que } A^r(\alpha b) = \alpha' b$$

Or ξ est défini par :

$$\xi = \sum_{k=0}^{p^{nf-1}-1} A^k b$$

d'où

$$\alpha\xi = \alpha A^r \xi = \sum_{k=0}^{p^{nf-1}-1} A^k A^r (\alpha b)$$

$$= \sum_{k=0}^{p^{nf-1}-1} A^k (\alpha' b)$$

$$= \alpha' \xi$$

donc $\alpha\xi = \alpha'\xi$ et $\xi \neq 0$ prouvent que $\alpha = \alpha'$.

Ainsi, C(b), C(2b),...,C((p-1)b) sont des cycles différents de A, de longueur p^{nf-1}.

(Notons que ces cycles ne peuvent être réduits à des points fixes car $p^{nf-1} \neq 1$ puisqu'on a supposé que $n > 1$ et $p \geq 2$).

3°) Supposons que A admette un autre cycle de longueur p^{nf-1} autre que les C(αb) précédents, alors on aurait p points fixes et p cycles de longueur p^{nf-1} sur un nombre total de p^{nf} points, ce qui est impossible.

4°) Montrons enfin, que $b+\xi \in C(b)$.

Soit r le plus petit entier tel que $A^r(b+\xi) = b+\xi$ alors r est le plus petit entier tel que $A^r b = b$ c'est-à-dire $r = p^{nf-1}$.

Donc $b+\xi$ est sur un cycle de longueur p^{nf-1} qui est nécessairement (d'après §.3) l'un des C(αb).

Ainsi :

$$\exists r < p^{nf-1} \quad \text{tel que} \quad A^r(b+\xi) = \alpha b$$

d'où

$$\forall k \in \mathbb{N} \qquad A^{r+k}(b+\xi) = \alpha A^k b$$

et

$$\sum_{k=0}^{p^{nf-1}-1} \alpha A^k b = \sum_{k=0}^{p^{nf-1}-1} A^{r+k}(b+\xi)$$

$$\Rightarrow \alpha\xi = A^r\xi = \xi \Rightarrow \alpha = 1 \quad (\text{car } \xi \neq 0).$$

5°) Soit $r < p^{nf-1}$, le plus petit entier tel que

$$A^r b = b+\xi$$

ce qui donne :

$$\forall k \geq 0, \quad A^{kr} b = b+k\xi$$

ainsi, le plus petit k tel que $A^{kr}b = b$ est $k = p$ donc $pr = p^{nf-1} \Rightarrow r = p^{nf-2}$
D'autre part, $\xi \neq 0$, a été défini par :

$$\xi = \sum_{k=0}^{pr-1} A^k b$$

$$= (I+A+..+A^{r-1})b+A^r(I+A+..+A^{r-1})b+...+A^{(p-1)r}(I+A+..+A^{r-1})b$$

$$= (I+A+..+A^{r-1})[b+A^r b+A^{2r}b+..+A^{(p-1)r}b]$$

$$= [I+A+..+A^{r-1}][b+(b+\xi)+(b+2\xi)+..+b+(p-1)\xi]$$

$$= (1+2+..+(p-1))(I+A+..+A^{r-1})\xi$$

$$= (1+2+..+(p-1))r\xi$$

or ξ est non nul donc $1+2+...+(p-1) = 1$
et $r = p^{nf-2} = 1$
d'où

$$p = 2, \ n = 2 \text{ et } f = 1.$$

En résumé, nous avons montré que si F est une permutation cyclique et $n > 1$ alors $n = p = 2$ et $f = 1$. Pour terminer la démonstration il suffit de vérifier que quand $n = 1$ alors $f = 1$.

Soit $F(x) = ax+b$ $\quad (a \neq 0,\ b \neq 0)$ une permutation cyclique, on a :

$$\forall x \in K, \quad F^{p^f}(x) = x = a^{p^f}x+(1+a+\ldots+a^{p^f-1})b$$

en particulier pour $x = 0$, on a :

$$0 = (1+a+\ldots+a^{p^f-1})b$$

d'où

$a = 1$ et

$\forall x \in K \quad F^p(x) = x+pb = x$

donc

$f = 1$.

Ce qui achève la démonstration du théorème.

V - ITERATIONS SUR DES FONCTIONS SYMETRIQUES

Définitions :

Sur Z_p^n, on définit la relation d'équivalence $\mathcal{R}$ par :

$$x \mathcal{R} y \iff \exists \sigma \in \mathcal{P}_n \text{ tel que } \sigma(x) = y$$

où $\mathcal{P}_n$ désigne l'ensemble des permutations de $\{1,2,\ldots,n\}$.

Notons I_n^p le nombre de classes d'équivalence modulo $\mathcal{R}$ c'est-à-dire le nombre de vecteurs de Z_p^n non équivalents. Dans [6] on montre que

$$I_n^p = \frac{p(p+1)\ldots(p+n-1)}{n!} = C_{n+p-1}^{p-1}$$

par exemple $I_{10}^5 = 1001$ (très petit comparativement à $p^n \approx 10^7$).

Soit $F : Z_p^n \to Z_p^n$

F est dite symétrique $\iff \forall x \in Z_p^n, \forall \sigma \in \mathcal{P}_n \quad F(x) = F(\sigma(x))$.

Pour $\xi \in Z_p^n$, la fonction symétrique élémentaire ϕ_ξ associé à ξ est définie par :

$$\phi_\xi : Z_p^n \to Z_2$$

avec

$$\phi_\xi(x) = 1 \iff x \mathcal{R} \xi$$

$$\phi_\xi(x) = 0 \text{ sinon}$$

Il est clair que $\xi \mathcal{R} \xi' \iff \phi_\xi = \phi_{\xi'}$

Avec ces notations on a immédiatement :

Proposition :

$F : Z_p^n \to Z_p^n$ est symétrique si et seulement si

$$\exists A \in \mathcal{M}_{n \times I_n^p}(Z_p) \text{ telle que}$$

$$\forall x \in Z_p^n \qquad F(x) = A\Phi(x)$$

où $\Phi(x)$ désigne le vecteur des I_n^p fonctions symétriques élémentaires.

Exemple 2

Soit $F : Z_3^2 \to Z_3^2$

$$x \to F(x) = (f_1(x), f_2(x))$$

définie par sa table :

x →	F(x)
00	02
01	10
02	00
10	10
11	02
12	21
20	00
21	21
22	01

F ainsi définie est symétrique, et dans Z_3^2 les fonctions symétriques élémentaires sont : ϕ_{00}, ϕ_{01}, ϕ_{02}, ϕ_{11}, ϕ_{12}, ϕ_{22} définies par :

	ϕ_{00}	ϕ_{01}	ϕ_{02}	ϕ_{11}	ϕ_{12}	ϕ_{22}
00	1	0	0	0	0	0
01	0	1	0	0	0	0
02	0	0	1	0	0	0
10	0	1	0	0	0	0
11	0	0	0	1	0	0
12	0	0	0	0	1	0
20	0	0	1	0	0	0
21	0	0	0	0	1	0
22	0	0	0	0	0	1

La matrice A ayant deux lignes et $I_2^3 = 6$ colonnes se construit en mettant en colonne et dans l'ordre F(0,0), F(0,1), F(0,2), F(1,1), F(1,2) et F(2,2) et on a :

$$F(x) = A\,\Phi(x)$$

Notons que la proposition précédente nous donne une expression canonique de toute fonction symétrique de Z_p^n dans lui-même.

2 - Graphe d'une fonction symétrique

Proposition

Pour toute fonction F de Z_p^n dans lui-même, donnée par $F(x) = A\Phi(x)$ on a :

$$F(Z_p^n) = \{a_{.1}, a_{.2}, \ldots, a_{.I_n^p}\}$$

où $a_{.i}$ est la ième colonne de A.

Démonstration

Posons $\Phi(x) = (\phi_{\xi_1}, \phi_{\xi_2}, \ldots, \phi_{\xi_{I_n^p}})$

$$\forall x \in Z_p^n \quad \exists! i \;/\; x \mathscr{R} \xi_i$$

ainsi

$$\forall x \in Z_p^n\,,\ \phi_{\xi_k}(x) = 0 \quad \text{si } k \neq i \text{ et } \phi_{\xi_i}(x) = 1$$

donc

F(x) est une colonne de A.

Inversement, soit $a_{.i}$ une colonne de A, et soit $b \in Z_p^n$ tel que $b \mathscr{R} \xi_i$ alors

$F(b) = A\Phi(b) = a_{.i}$ car $\Phi(b)$ est partout nul sauf en position i.

Ainsi

$$F(Z_p^n) = \{a_{.0}, a_{.1}, \ldots, a_{.I_n^p}\}$$

De cette proposition on peut déduire immédiatement que les cycles d'une fonction symétrique sont au plus de longueur I_n^p . En plus on a une méthode simple pour construire le graphe d'itération d'une telle fonction à partir de la matrice A, ce qui réduit le problème de taille p^n à un problème de taille

I_n^p qui est très petit par rapport à p^n.

Exemple :

Reprenons la fonction de l'exemple 2.

F est définie par la matrice

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 2 & 0 \\ 2 & 0 & 0 & 2 & 1 & 1 \end{bmatrix}$$

Notons $E(k) = \{x \in Z_p^n / x \mathcal{R}_k\}$

dans cet exemple on a :

$E(0) = \{(00)\}$

$E(1) = \{(01), (10)\}$

$E(2) = \{(02), (20)\}$

$E(3) = \{(11)\}$

$E(4) = \{(12), (21)\}$

$E(5) = \{(22)\}$

et on a $\forall k \quad F(E_k) = a_{.k}$

$E(0) \rightarrow (02)$

$E(1) \rightarrow (10)$

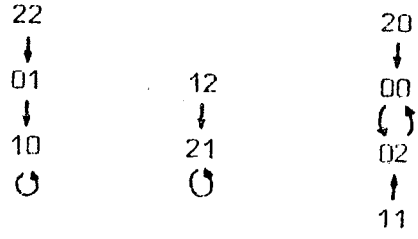
$E(2) \rightarrow (00)$

$E(3) \rightarrow (02)$

$E(4) \rightarrow (21)$

$E(5) = (01)$

d'où le graphe d'itération de F



Remarque

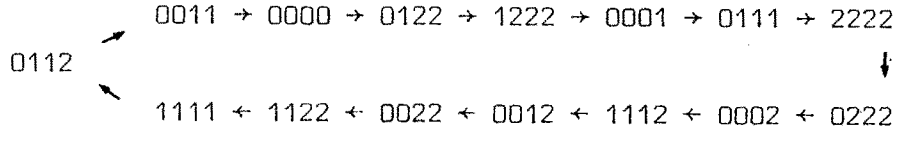
Pour tout couple d'entier (n,p) avec p premier, on peut construire une fonction symétrique F de Z_p^n dans lui-même qui admet un cycle de longueur I_n^p. Pour cela il suffit de construire F de telle manière que les colonnes de sa matrice A soient une permutation cyclique des I_n^p représentants des classes d'équivalence modulo $\mathscr{R}$; par exemple :

$$n = 4 \text{ et } p = 3, \quad I_n^p = 15$$

Construisons F de sorte que :

$$A = \begin{matrix} 0\,0\,1\,0\,0\,1\,2\,0\,1\,0\,0\,0\,1\,0\,0 \\ 1\,1\,1\,0\,0\,1\,2\,0\,2\,0\,1\,0\,1\,0\,2 \\ 2\,1\,1\,0\,2\,2\,2\,1\,2\,0\,1\,1\,1\,0\,2 \\ 2\,1\,2\,0\,2\,2\,2\,1\,2\,2\,2\,2\,1\,1\,2 \end{matrix}$$

Le graphe d'itération de F contient l'unique cycle de longueur 15 :



VI - QUELQUES PROPRIETES DES FONCTIONS LOCALES EN DIMENSION DEUX

Le travail que nous présentons dans ce chapitre constitue une généralisation en dimension deux d'une étude faite par HARARO et NOGUCHI dans [17] concernant les fonctions locales en dimension un. Ce genre de fonctions constitue, en particulier, une modélisation mathématique d'un réseau homogène de neurones [1]

Nous donnons des propriétés du comportement dynamique d'un réseau fini de cellules en dimension 2, uniformément connectées, c'est-à-dire que l'état de chaque cellule à l'instant t+1 dépend, par une même fonction de transition, de l'état, à l'instant t, des cellules d'un voisinage donné. De plus nous choisissons comme structure cellulaire la structure torique c'est-à-dire la périodicité aux bords.

1. Définitions

Pour pouvoir traiter le problème dans un cas très général et pour plus de clarté, nous utiliserons les notations et la terminologie des automates cellulaires.

Une fonction locale F (ou automate cellulaire fini) est caractérisée par la donnée d'un quadruplet $\{Q, Z_{n_1} \times Z_{n_2}, t, v\}$ où

a) Q est un ensemble fini non vide de cardinal q appelé ensemble des états

b) $Z_{n_1} \times Z_{n_2} = \{(i,j) / i \in Z_{n_1} \text{ et } j \in Z_{n_2}\}$ où Z_{n_1} est l'ensemble des entiers modulo n_1. $Z_{n_1} \times Z_{n_2}$ est appelé structure cellulaire.

c) v est la fonction de voisinage définie par

$k \geq 1$, $v : Z_{n_1} \times Z_{n_2} \to (Z_{n_1} \times Z_{n_2})^k$

et

$$v(i,j) = [(i+v_1, j+v'_1), (i+v_2, j+v'_2), \ldots, (i+v_k, j+v'_k)]$$

où les $v_i \in Z_{n_1}$ et les $v'_i \in Z_{n_2}$. L'entier k est appelé taille du voisinage.

d) $t : Q^k \to Q$ est appelé fonction de transition.

Nous appelons configuration toute application

$$c : Z_{n_1} \times Z_{n_2} \to Q$$

et notons $\mathscr{C}$ l'ensemble de toutes les configurations.

Avec ces notations une fonction locale F est définie par :

$$F : \mathscr{C} \to \mathscr{C}$$

$$c \to F(c)$$

avec

$$\forall (i,j) \in Z_{n_1} \times Z_{n_2},\ (F(c))(i,j) = t[c(i+v_1, j+v'_1), \ldots, c(i+v_k, j+v'_k)]$$

Exemple

$$Q = Z_2 \quad n_1 = n_2 = 3 \quad k = 2$$

$$V : Z_3 \times Z_3 \to (Z_3 \times Z_3)^2$$

$$(i,j) \to v(i,j) = [(i+2, j+2), (i+1, j)]$$

$$t : Z_2^2 \to Z_2$$

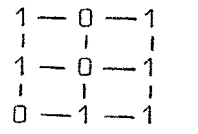
$$x = (x_1, x_2) \to t(x) = x_1 x_2 + 1$$

Ainsi F est définie par

$$F(c))(i,j) = t[c(i+2, j+2), c(i+1, j)]$$

$$= c(i+2, j+2).c(i+1, j)+1$$

par exemple soit c_o la configuration donnée par :



On adoptera comme indexation de l'espace cellulaire $Z_3 \times Z_3$ la numération usuelle

$$\begin{array}{ccccc} (0,0) & - & (0,1) & - & (0,2) \\ | & & | & & | \\ (1,0) & - & (1,1) & - & (1,2) \\ | & & | & & | \\ (2,0) & - & (2,1) & - & (2,2) \end{array}$$

Le calcul de $F(c_0)$ (i,j) pour $(i,j) \in Z_3 \times Z_3$ donne

$$\begin{array}{ccccc} 0 & - & 1 & - & 0 \\ | & & | & & | \\ 1 & - & 0 & - & 1 \\ | & & | & & | \\ 0 & - & 1 & - & 1 \end{array}$$

On définit la composition de deux fonctions locales F_1 et F_2 par

$$(F_1 \circ F_2(c))\ (i,j) = [F_1(F_2(c)](i,j)$$

On vérifie aisément que cette loi est associative.

2 - Etude de la transformation représentative de F.

Définissons les fonctions de "décodage" Ψ_1 et Ψ_2 par

$$\Psi_1 : \mathscr{C} \to Z_{p^{n_1}}^{n_2} \qquad \text{(rappelons que } q = \text{card } Q\text{)}$$

$$\Psi_2 : \mathscr{C} \to Z_{q^{n_2}}^{n_1}$$

avec

$$\Psi_1(c)(i) = c(0,i)+qc(1,i)+\ldots+q^{n_1-1}c(n_1-1,i) \quad \forall i \in Z_{n_2}$$

et

$$\Psi_2(c)(i) = c(i,0)+qc(i,1)+\ldots+q^{n_2-1}c(i,n_2-1) \quad \forall i \in Z_{n_1}$$

Notons que Ψ_1 et Ψ_2 sont bijectives.

Exemple : $n_1 = 3$, $n_2 = 5$, $Q = \{0,1\}$

$$c = \begin{matrix} 10101 \\ 01101 \\ 01100 \end{matrix}$$

$$\Psi_1(c) = \begin{bmatrix} 4 \\ 3 \\ 7 \\ 0 \\ 6 \end{bmatrix} \qquad \Psi_2(c) = \begin{bmatrix} 21 \\ 13 \\ 12 \end{bmatrix}$$

Soient F_{σ_1} et F_{σ_2} les deux opérateurs sur $\mathscr{C}$ définis par

$$F_{\sigma_1}(c)(i,j) = c(i-1,j)$$

et $$F_{\sigma_2}(c)(i,j) = c(i,j-1)$$

F_{σ_1} et F_{σ_2} sont deux fonctions locales caractérisées respectivement par les quadruplets

$$\{Q,\ Z_{n_1} \times Z_{n_2},\ t,\ \sigma_1\}$$

et

$$\{Q,\ Z_{n_1} \times Z_{n_2},\ t,\ \sigma_2\}$$

avec

$$\sigma_1(i,j) = (i-1,j)$$

$$\sigma_2(i,j) = (i,j-1) \qquad \forall (i,j) \in Z_{n_1} \times Z_{n_2}$$

et t est l'identité sur Q.

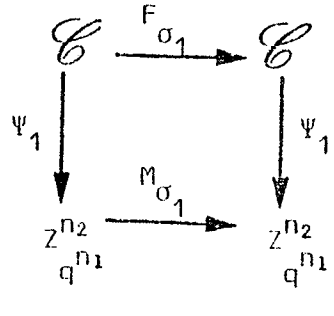
Soient enfin M_{σ_1} et M_{σ_2} appelés transformations représentatives de F_{σ_1} et F_{σ_2} les applications définies par :

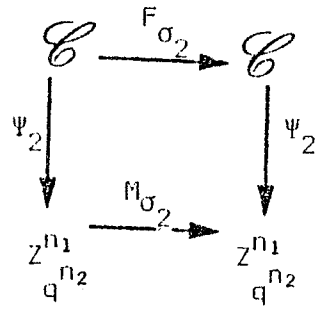
$$M_{\sigma_1}(\Psi_1(c)) = \Psi_1(F_{\sigma_1}(c))$$

et $$\forall c \in \mathscr{C}$$

$$M_{\sigma_2}(\Psi_2(c)) = \Psi_2(F_{\sigma_2}(c))$$

c'est-à-dire qu'on a le diagramme suivant :





Lemme 1

Si M_{σ_j} est la transformation représentative de F_{σ_j}, $j = 1,2$ alors :

$$\forall i \in Z_{n_j},\ M_{\sigma_j}(r)(i) = q.r(i) \bmod(q^{n_j}-1) \quad \text{si } r(i) \neq q^{n_j}-1$$

et

$$M_{\sigma_j}(r)(i) = r(i) \quad \text{si } r(i) = q^{n_j}-1$$

Démonstration :

$$\forall r \in Z_{q^{n_1}}^{n_2} \quad \exists c \in \mathscr{C} \quad \text{tel que } \Psi_1(c) = r$$

or

$$M_{\sigma_1}(\Psi_1(c)) = \Psi_1(F_{\sigma_1}(c))$$

$\forall i \in Z_{n_2}$ on a :

$$M_{\sigma_1}(\Psi_1(c)(i) = \Psi_1(F_{\sigma_1}(c)(i)$$

$$= F_{\sigma_1}(c)(0,i)+qF_{\sigma_1}(c)(1,i)+\ldots+q^{n_1-1}F_{\sigma_1}(c)(n_1-1,i)$$

$$= c(n_1-1,i)+qc(0,i)+\ldots+q^{n_1-1}c(n_1-2,i) \qquad (1)$$

$$= q[c(0,i)+qc(1,i)+\ldots+q^{n_1-2}c(n_1-2,i)]+c(n_1-1,i) \qquad (2)$$

si $r(i) = q^{n_1}-1$ alors $\Psi_1(c)(i) = q^{n_1}-1$ donc $c(j,i) = q-1$, $\forall j \in Z_{n_1}$ d'où

$$M_{\sigma_1}(\Psi_1(c))(i) = (q-1)(1+q+\ldots+q^{n_1-1}) = q^{n_1}-1 \quad \text{(d'après (1))}$$

si $r(i) \neq q^n - 1$ alors d'après (2) on a :

$$M_{\sigma_1}(r)(i) = q[c(0,i)+qc(1,i)+\ldots+q^{n_1-2}c(n_1-2,i)+q^{n_1-1}c(n_1-1,i)] \pmod{q^{n_1}-1}$$

$$= q\Psi_1(c)(i) \pmod{q^{n_1}-1}$$

d'où $$M_{\sigma_1}(r)(i) = qr(i) \pmod{q^{n_1}-1}$$

Pour M_{σ_2}, le même raisonnement conduirait à

$$M_{\sigma_2}(r)(i) = qr(i) \pmod{q^{n_2}-1} \quad \text{si } r(i) \neq q^{n_2}-1$$

et

$$M_{\sigma_2}(r)(i) = r(i) \quad \text{si } r(i) = q^{n_2}-1$$

Proposition 1

Pour $j = 1,2$; la longueur de tout cycle de M_{σ_j} est n_j ou bien un de ces diviseurs. Inversement, si ℓ est un diviseur de n_j alors il existe au moins un cycle de M_{σ_j} de longueur ℓ .

Démonstration :

D'après le lemme 1, on a :

$$M_{\sigma_j}^{n_j} = I_j \quad \text{pour } j = 1,2$$

et I_j est l'identité sur $Z_{q^{n_j}}^{n_j}$, ce qui prouve la première partie de la proposition.

Inversement, soit ℓ un diviseur de n_1 et soit $c \in \mathscr{C}$ telle que

$$c(i-\ell,j) = c(i,j) \qquad \forall (i,j) \in Z_{n_1} \times Z_{n_2}$$

(une telle configuration existe). Si ℓ est le plus petit entier vérifiant cette propriété alors ℓ est le plus petit entier tel que

$$F_{\sigma_1}^{\ell}(c) = c$$

et on a

$$M_{\sigma_1}^{\ell}(\Psi_1(c)) = \Psi_1(F_{\sigma_1}^{\ell}(c)) = \Psi_1(c)$$

donc $\Psi_1(c)$ appartient à un cycle de M_{σ_1} de longueur ℓ . Un raisonnement analogue pour M_{σ_2} prouverait la proposition 1.

Il est naturel de se demander sous quelles conditions une application de $\mathscr{C}$ dans lui-même est-elle une fonction locale.

THEOREME 1

Une application F de $\mathscr{C}$ dans $\mathscr{C}$, où $\mathscr{C} = \{c : Z_{n_1} \times Z_{n_2} \to Q\}$ est une fonction locale si et seulement si F commute avec F_{σ_1} et F_{σ_2}.

Démonstration :

Soit F une fonction locale caractérisée par le quadruplet

$$\{Q, Z_{n_1} \times Z_{n_2}, t, v\}$$

$$((F_{\sigma_1} \circ F)(c))(i,j) = (F_{\sigma_1}(F(c)))(i,j) = (F(c))(i-1,j)$$

$$((F \circ F_{\sigma_1})(c))(i,j) = (F(F_{\sigma_1}(c))(i,j)$$

$$= t(F_{\sigma_1}(c)(i+v_1, j+v_1'), \ldots, F_{\sigma_1}(c)(i+v_k, j+v_k'))$$

$$= t(c(i-1+v_1, j+v_1'), \ldots, c(i-1+v_k, j+v_k'))$$

$$= F(c)(i-1,j)$$

d'où $F_{\sigma_1} \circ F = F \circ F_{\sigma_1}$

(même raisonnement donnerait $F_{\sigma_2} \circ F = F \circ F_{\sigma_2}$)

Inversement supposons que $F_{\sigma_1} \circ F = F \circ F_{\sigma_1}$ et $F_{\sigma_2} \circ F = F \circ F_{\sigma_2}$

Pour tout couple $(i,j) \in Z_{n_1} \times Z_{n_2}$ définissons t_{ij} par :

$$t_{ij}(c(i,j),\ c(i+1,j),\ldots,c(i+n-1,j+n-1)) = F(c)(i,j)$$

ce qui exprime bien qu'en toute position (i,j) d'une configuration c, F agit en général, en fonction de toutes les c(p,q) pour $(p,q) \in Z_{n_1} \times Z_{n_2}$; exprimons que $F_{\sigma_1} \circ F = F \circ F_{\sigma_1}$

$\forall c \in \mathscr{C}$, $\forall (i,j) \in Z_{n_1} \times Z_{n_2}$

$$((F_{\sigma_1} \circ F)(c))(i,j) = (F_{\sigma_1}(F(c))(i,j) = F(c)(i-1,j)$$

$$= t_{i-1,j}(c(i-1,j),c(i,j),\ldots,c(i+n-2,j+n-1))$$

$$((F \circ F_{\sigma_1})(c))(i,j) = (F(F_{\sigma_1}(c))(i,j)$$

$$= t_{ij}((F_{\sigma_1}(c))(i,j)$$

$$= [(F_{\sigma_1}(c))(i\ \ ,j),..,(F_{\sigma_1}(c))(i+n-1,j+n-1)]$$

$$= t_{ij}(c(i-1,j),c(i,j),\ldots,c(i+n-2,j+n-1))$$

d'où

$$t_{ij} = t_{i-1,j} \qquad \forall (i,j) \in Z_{n_1} \times Z_{n_2}$$

De même en exprimant que $F_{\sigma_2} \circ F = F \circ F_{\sigma_2}$ on obtient

$$t_{ij} = t_{i,j-1} \qquad \forall (i,j) \in Z_{n_1} \times Z_{n_2}$$

ce qui prouve que tous les t_{ij} sont les mêmes donc F est une fonction locale et le théorème est démontré.

Corollaire :

L'ensemble des fonctions locales de $\mathscr{C}$ dans $\mathscr{C}$ est un semi-groupe.

Démonstration :

Soient F et F' deux fonctions locales, en utilisant la caractérisation du théorème 1, on a :

pour i =1,2 : $(F \circ F') \circ F_{\sigma_i} = F \circ (F' \circ F_{\sigma_i}) = F \circ (F_{\sigma_i} \circ F') = F_{\sigma_i} \circ F' \circ F'$

$= F_{\sigma_i} \circ (F \circ F')$

Nature des cycles d'une fonction locale

Nous nous intéressons à présent au comportement des itérations conduites sur des fonctions locales. Pour ce faire, nous utilisons la caractérisation donnée par le théorème 1.

Soient $\mathscr{R}_1$ et $\mathscr{R}_2$ les relations sur $\mathscr{C}$ définies de la manière suivante :

$$c \mathscr{R}_i c' \iff \exists \ell \ / \ F^{\ell}_{\sigma_i}(c) = c' \qquad i = 1,2$$

Il est clair que $\mathscr{R}_1$ et $\mathscr{R}_2$ sont des relations d'équivalence sur $\mathscr{C}$.

Définition

Une configuration $c \in \mathscr{C}$ est dite d-périodique par rapport à la première variable (respectivement la 2ème variable) si d est le plus petit entier tel que :

$$\forall (i,j) \in Z_{n_1} \times Z_{n_2} : c(i+d,j) = c(i,j)$$

(resp. $(c(i,j+d) = c(i,j)$)

Soit F une fonction locale, il est immédiat que :

Si $c \in \mathscr{C}$ est d-périodique par rapport à la première (resp. deuxième) variable, alors F(c) est d'-périodique par rapport à la première (resp. deuxième) variable où d' est un diviseur de d et ceci pour toute fonction locale F.

Cette remarque nous amène à dénombrer les différentes classes d'équivalences module $\mathscr{R}_1$ et $\mathscr{R}_2$.

Proposition :

a) si $c \in \mathscr{C}$ est une configuration d-périodique par rapport à la 1ère variable (resp. 2ème variable) alors la classe d'équivalence modulo $\mathscr{R}_1$ (resp $\mathscr{R}_2$) contenant c a d éléments.

b) toutes les configurations d'une même classe d'équivalence ont la même période respectivement par rapport à la 1ère et à la 2ème variable.

Démonstration :

b) Soit $c \in \mathscr{C}$, d-périodique par rapport à la 1ère variable et c' tel que $c' \mathscr{R}_1 c$ alors

$$\exists \ell \ / \ F^{\ell}_{\sigma_1}(c) = c'$$

d'où

$$c'(i+d,j) = (F^{\ell}_{\sigma_1}(c))(i+d,j) = c(i+d-\ell,j) = c(i-\ell,j)$$

$$= (F^{\ell}_{\sigma_1}(c))(i,j) = c'(i,j)$$

=> c' est d'-périodique par rapport à la 1ère variable avec d'/d d'autre part

$$c(i+d'-\ell,j) = (F^{\ell}_{\sigma_1}(c))(i+d',j) \qquad \text{(par définition de } F_{\sigma_1})$$

$$= c'(i+d',j) \qquad \text{(car } F^{\ell}_{\sigma_1}(c) = c')$$

$$= c'(i,j)$$

$$= (F^{\ell}_{\sigma_1}(c))(i,j)$$

$$= c(i-\ell,j)$$

or c est par hypothèse d-périodique par rapport à la première variable d'où d divise d' donc d' = d.

(Raisonnement analogue pour la périodicité par rapport à la 2ème variable).

a) La classe d'équivalence modulo $\mathscr{R}_1$ (resp. modulo $\mathscr{R}_2$) contenant c est de la forme

$$(c, F_{\sigma_i}(c), F^2_{\sigma_i}(c), \ldots, F^{d-1}_{\sigma_i}(c)) \qquad i = 1 \text{ (resp. } i = 2).$$

Lemme

Soit $U_i(d)$: i = 1,2, le nombre de classes d'équivalences modulo $\mathscr{R}_i$ constituées de configurations d-périodiques par rapport à la ième variable. Alors $U_i(d)$ est donné par

$$U_i(d) = \frac{1}{d} \sum_{d'/d} \mu(d') q^{n_{\bar{i}}\, d/d'} \qquad \bar{i} \in \{1,2\}-\{i\}$$

où q est le nombre d'éléments de Q et μ est la fonction de Möbius définie comme suit :

si $n = p_1^{r_1}.\, p_2^{r_2} \ldots p_\nu^{r_\nu}$ est la décomposition en nombre premier de n alors

* $\mu(1) = 1$
* $\mu(n) = 0$ s'il existe j tel que $r_j > 1$
* $\mu(n) = (-1)^r$ si $r_1 = r_2 = \ldots = r_\nu = 1$

Démonstration :

D'après la proposition précédente, chaque classe d'équivalence modulo $\mathscr{R}_i$ (i = 1,2) de configurations d'-périodiques contient d' éléments donc :

$$\sum_{d'/n_i} d' U_i(d') = q^{n_1 . n_2}$$

Soient $f(x) = (q^{n_{\bar{i}}})^x$ où $\bar{i} \in \{1,2\}-\{i\}$

et $g(x) = x.U_i(x)$

On a : $$q^{n_1 n_2} = f(n_i) = \sum_{d'/n_i} d' U_i(d') = \sum_{d'/n_i} g(d')$$

En utilisant la formule d'inversion de Möbius [6] on a :

$$g(n_i) = \sum_{d'/n_i} \mu(d')\, f\left(\frac{n_i}{d'}\right)$$

$$= \sum_{d'/n_i} \mu(d')(q^{\frac{n_i}{}})^{n_i/d'}$$

$$= \sum_{d'/n_i} \mu(d') q^{n_1 n_2/d'}$$

$$= n_i . U_i(n_i)$$

donc

$$U_i(n_i) = \frac{1}{n_i} \sum_{d'/n_i} \mu(d') q^{n_1 n_2/d'} .$$

$U_1(n_1)$ par exemple, est le nombre de classes d'équivalence modulo $\mathscr{R}_1$ dont les éléments sont de période exactement n_1 par rapport à la première variable et ceci sur des configurations

$$c : Z_{n_1} \times Z_{n_2} \to Q$$

Si on considère maintenant des configurations

$$c : Z_d \times Z_{n_2} \to Q \quad \text{où } d \in \mathbb{N}^*$$

alors un raisonnement analogue à ce qui précède donne

$$U_1(d) = \frac{1}{d} \sum_{d'/d} \mu(d')\, q^{n_2 d/d'}$$

ce qui prouve le lemme.

THEOREME

Supposons qu'on ait $n_1 \geq n_2$, alors la longueur du plus grand cycle réalisable par une fonction locale est au plus $q^{n_1 n_2} - q^{n_1} - q^{n_2} + q$ si $n_2 > 1$ et $q^{n_1} - q$ si $n_2 = 1$.
Quand $n_2 = 1$ cette borne est atteinte si et seulement si n_1 est premier.

Démonstration :

Nous avons vu que si $c \in \mathcal{C}$ est d'-périodique par rapport à l'une des variables alors pour toute fonction locale F, F(c) est d'-périodique par rapport à la même variable (avec d'/d). Ainsi, un cycle de F ne contient que des configurations de mêmes périodes respectivement par rapport à la 1ère et à la 2ème variable.

Les configurations 1-périodiques par rapport soit à la première, soit à la 2ème variable sont au nombre de $q^{n_1}+q^{n_2}-q$. En effet, si $n_2 > 1$, le nombre de configurations 1-périodiques par rapport à la ième variable(i=1,2) est $U_i(1) = q^{n_{\bar{i}}}$ ($\bar{i} = \{1,2\}-\{i\}$), et le nombre de configurations 1-périodiques simultanément par rapport à la 1ère et à la 2ème variable est q, ce sont toutes les configurations telles que $c(i,j) = c(0,0)$ $\forall (i,j) \in Z_{n_1} \times Z_{n_2}$ et c(0,0) prenant les q valeurs de Q.

Donc le maximum de configurations que l'on peut mettre (éventuellement !) dans un cycle d'une fonction locale, serait $q^{n_1 n_2}-(q^{n_1}+q^{n_2}-q)$. Nous n'avons pas pu exhiber une fonction locale qui admettrait un cycle d'une telle longueur.

Supposons maintenant que $n_2 = 1$, il est clair que dans ce cas il n'y a pas de configuration périodique par rapport à la 2ème variable donc le plus grand cycle qu'on pourrait obtenir serait de longueur au plus $q^{n_1}-q$. Si n_1 n'est pas premier, on ne peut obtenir par une fonction locale, un cycle contenant $q^{n_1}-q$ éléments puisque parmi ceux-ci il y a toutes les configurations d-périodiques, pour tout d diviseur de n_1. Inversement, supposons que n_1 est premier alors F_{σ_1} contient $U_1(n_1)$ cycles de longueur n_1 :

$$C_o = (c_{00}, c_{01}, \ldots, c_{0(n_1-1)})$$

$$C_1 = (c_{10}, c_{11}, \ldots, c_{1(n_1-1)})$$

$$\vdots$$

$$C_{r-1} = (c_{(r-1)0}, c_{(r-1)1}, \ldots, c_{(r-1)(n_1-1)})$$

où $$r = U_1(n_1) = \frac{1}{n_1}(q^{n_1}-q)$$

et F_{σ_1} contient $U_1(1) = q$ point fixes :

$$s_o, s_1, \ldots, s_{q-1}$$

Construisons F de la manière suivante :

$$F(c_{ij}) = c_{(i+1)j} \qquad \text{si } i \neq r-1$$

$$F(c_{(r-1)j}) = c_{0(j+1)} \qquad \text{si } j \neq n_1-1$$

$$F(c_{(r-1)(n-1)}) = c_{00}$$

$$F(s_i) = s_i \qquad \forall i \in \{0,1,\ldots,q-1\}$$

F est ainsi définie sur tout $\mathscr{C}$. Il est clair que F admet un cycle de longueur $q^n - q$ (par construction), il suffit de vérifier que F est bien une fonction locale. D'après le théorème 1 nous devons montrer que F commute avec F_{σ_1} :

$$\forall c \in \mathscr{C} \qquad (F \circ F_{\sigma_1})(c) = F(F_{\sigma_1}(c))$$

* si $c = s_i$ $(i \in \{0,1,\ldots,q-1\})$

$$(F \circ F_{\sigma_1})(s_i) = F(s_i) = s_i = F_{\sigma_1}(s_i) = F_{\sigma_1}(F(s_i)) = (F_{\sigma_1} \circ F)(s_i)$$

* si $c = c_{ij}$, $i \neq r-1$

$$(F_{\sigma_1} \circ F)(c_{ij}) = F_{\sigma_1}(F(c_{ij})) = F_{\sigma_1}(c_{(i+1)j})$$

$$= \begin{cases} c_{(i+1)(j+1)} & \text{si } j \neq n-1 \\ c_{(i+1)0} & \text{si } j = n-1 \end{cases}$$

et

$$(F \circ F_{\sigma_1})(c_{ij}) = F(F_{\sigma_1}(c_{ij}))$$

$$= \begin{cases} F(c_{i(j+1)}) & \text{si } j \neq n-1 \\ F(c_{io}) & \text{si } j = n-1 \end{cases}$$

$$= \begin{cases} c_{(i+1)(j+1)} & \text{si } j \neq n-1 \\ c_{(i+1)0} & \text{si } j = n-1 \end{cases}$$

donc $(F_{\sigma_1} \circ F)(c_{ij}) = (F \circ F_{\sigma_1})(c_{ij})$

* si $c = c_{(r-1)j}$ et $j \neq n_1-1$

$$(F_{\sigma_1} \circ F)(c_{(r-1)j}) = F_{\sigma_1}(F(c_{(r-1)j})) = F_{\sigma_1}(c_{o(j+1)})$$

$$= \begin{cases} c_{o(j+2)} & \text{si } j+1 \neq n_1-1 \\ c_{oo} & \text{si } j+1 = n_1-1 \end{cases}$$

$$= \begin{cases} F(c_{(r-1)(j+1)}) & \text{si } j+1 \neq n_1-1 \\ F(c_{(r-1)(n_1-1)}) & \text{si } j+1 = n_1-1 \end{cases}$$

$$= \begin{cases} F(F_{\sigma_1}(c_{(r-1)j})) & \text{si } j+1 \neq n_1-1 \\ F(F_{\sigma_1}(c_{(r-1)(n_1-2)})) & \text{si } j+1 = n_1-1 \end{cases}$$

$$= (F \circ F_{\sigma_1})(c_{(r-1)j})$$

* si $c = c_{oo}$

$$(F \circ F_{\sigma_1})(c_{oo}) = F(c_{o1}) = c_{11} = F_{\sigma_1}(c_{10}) = F_{\sigma_1}(F(c_{oo}))$$

$$= (F_{\sigma} \circ F)(c_{oo})$$

Ce qui prouve le théorème.

Différentes propriétés des fonctions locales en dimension deux ont été établies, grâce à la caractérisation donnée dans le théorème 1 et aux relations qu'elles ont avec les opérateurs F_{σ_1} et F_{σ_2} dont le comportement itératif est parfaitement connu.

DEUXIEME CHAPITRE

REPRESENTATION MATRICIELLE ET ALGORITHME DE MINIMISATION DE FONCTIONS DE Z_p^n DANS Z_p

§ 1 - Forme canonique et représentation matricielle

§ 2 - Forme canonique de polarité $\alpha \in Z_p^n$

§ 3 - Algorithme de minimisation

INTRODUCTION

Au cours de ces dernières années, plusieurs travaux ont été consacrés à l'étude des fonctions de Z_p^n dans Z_p (Galois Switching Functions) [29] [4] vu leur importance dans divers domaines : circuits logiques : [7], [8] [12], [31], complexité de calcul [2], [10],[31] ...

Dans cette partie, nous allons étudier quelques propriétés de telles fonctions en établissant une représentation matricielle simple utilisant les propriétés du produit tensoriel. Ceci nous permettra d'élaborer un algorithme de minimisation de l'expression d'une fonction f de Z_p^n dans Z_p et de prouver, incidemment, que la solution proposée par Swamy [39] dans le cas p = 2 est incorrecte.

Rappel:

Soient $A \in \mathcal{M}_{n\times m}(K)$ et $B \in \mathcal{M}_{r\times s}(K)$, deux matrices à éléments dans un corps K. Le produit tensoriel de A par B est défini par :

$$A \otimes B = \begin{vmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & & & \\ a_{n_1}B & a_{n_2}B & \cdots & a_{nm}B \end{vmatrix}$$

$A \otimes B \in \mathcal{M}_{nr \times ms}(K)$.

Nous noterons $A^{\otimes n} = A \otimes A \otimes \ldots \otimes A$, n fois.

Propriétés :

$$(A \otimes B)\cdot(x \otimes y) = Ax \otimes Ay,$$
$$(A \otimes B)\cdot(C \otimes D) = AC \otimes BD$$
$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1} \qquad \text{si A et B sont inversibles.}$$

I - FORME CANONIQUE ET REPRESENTATION MATRICIELLE

Pour $n \geq 1$, notons $\mathscr{E}_n$ l'ensemble des fonctions

$f : Z_p^n \to Z_p$ où p est un nombre premier.

PROPOSITION 1 : [20]

Toute fonction f de $\mathscr{E}_n$ s'écrit de manière unique sous la forme :

$$f(x_{n-1},x_{n-2},\ldots,x_o) = \sum_{i=0}^{p^n-1} a_i m_i(x) \qquad (1)$$

où $a_i \in Z_p$ et $m_i(x) = \prod_{j=0}^{n-1} x_j^{i_j}$, i_j est le jième bit dans l'écriture de i en base p : $i = (i_{n-1},\ldots,i_o)$.

Exemple : n = 2, p = 3

$$f(x_1,x_o) = a_o+a_1x_o+a_2x_o^2+a_3x_1+a_4x_1x_o+a_5x_1x_o^2+a_6x_1^2+a_7x_1^2x_o+a_8x_1^2x_o^2$$

Pour avoir $m_5(x)$ par exemple, on écrit 5 en base 3

$5 = 1 \times 3+2$ et $m_5(x_1,x_o) = x_1^1x_o^2$

REPRESENTATION MATRICIELLE :

Soit $f \in \mathscr{E}_n$ représentée par :

$$f(x) = \sum_{j=0}^{p^n-1} a_j m_j(x)$$

Posons :

$$a^* = (a_0, a_1,\ldots, a_{p^n-1})^t$$

et

$$f^* = (f(0,\ldots,0), f(0,\ldots,0,1) ,\ldots, f((p-1),\ldots, (p-1)))^t.$$

Enfin soit $M_1 \in \mathcal{M}_{p\times p}(\mathbb{Z}_p)$ construite de la manière suivante :

$$M_1 = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{p-1} \\ \vdots & & & & \\ 1 & i & i^2 & \cdots & i^{p-1} \\ \vdots & & & & \\ 1 & (p-1) & & \cdots & (p-1)^{p-1} \end{vmatrix}$$

$$M_1 = (m_{ij}^{(1)})_{ij} \quad i,j = 0,1,\ldots,p-1 \qquad m_{ij}^{(1)} = i^j \bmod(p).$$

Enonçons alors le résultat de base de cette étude :

Théorème 1 :

Pour tout $n \in \mathbb{N}$ et pour tout $f \in \mathcal{E}_n$ on a la représentation :

$$f^* = M_n\, a^*$$

où $M_n = M_1^{\otimes n}$ ($M_0 = 1$) est indépendante de f.

La démonstration est basée sur les 2 lemmes suivants :

Lemme 1 :

Toute fonction $f \in \mathcal{E}_n$ peut s'écrire sous la forme

$$(1) : f(x_{n-1},\ldots,x_0) = \sum_{i=0}^{p-1} (p-1) \prod_{\substack{j=0 \\ j\neq p-i}}^{p-1} (x_{n-1}+j)\, f(i,x_{n-2},\ldots,x_0)$$

Démonstration :

Posons $\alpha_i = (p-1) \prod_{\substack{j=0 \\ j\neq p-i}}^{p-1} (x_{n-1}+j)$

Pour montrer l'égalité (1), il suffit de prouver que :

$$\alpha_i = 1 \quad \text{si} \quad i = x_{n-1}$$
$$= 0 \quad \text{sinon.}$$

Si $i \neq x_{n-1}$, il est clair que :

$$\prod_{\substack{j=0 \\ j\neq(p-i)}}^{p-1} (x_{n-1}+j) = 0$$

Si $i = x_{n-1}$, $\alpha_i = (p-1) \prod_{k\in\mathbb{Z}_p} k$

$$= (p-1)\cdot(p-1)!$$

En remarquant que les éléments de $\mathbb{Z}_p^*$ sont les racines du polynôme $X^{p-1}-1$ alors $(p-1)!$ est le produit des racines ; d'où $(p-1)! = p-1 \ \mathrm{mod}(p)$.
Ainsi $\alpha_i = (p-1)\cdot(p-1) = 1 \quad \mathrm{mod}(p)$.

Lemme 2 :

Soit $f \in \mathscr{E}_n$ de représentation canonique

$$f(x) = \sum_{j=0}^{p^n-1} a_j \, m_j(x),$$

Posons :

$$g_i(x_{n-2},\ldots,x_0) = f(i, x_{n-2},\ldots,x_0) \quad i \in \mathbb{Z}_p$$

alors $\forall i \in \mathbb{Z}_p$:

$$g_i(x_{n-2},\ldots,x_0) = \sum_{j=0}^{p^{n-1}-1} a_j^{(i)} m_j(x_{n-2},\ldots,x_0)$$

avec

$$a_j^{(i)} = \sum_{r=0}^{p-1} i^r \, a_{rp^{n-1}+j}$$

Démonstration :

Soit $j = \sum_{\ell=0}^{n-1} \alpha_\ell \, p^\ell$, $a_j^{(i)}$ est le coefficient du monôme $\prod_{k=0}^{n-2} x_k^{\alpha_k}$. Or, dans l'écriture canonique de f, ce monôme provient de $x_{n-1}^{\beta} \prod_{k=0}^{n-2} x_k^{\alpha_k}$, $\beta = 0,1,\ldots,p-1$, en y remplaçant x_{n-1} par i. D'où :

$$a_j^{(i)} = a_j + i a_{j+p^{n-1}} + i^2 a_{j+2p^{n-1}} + \ldots + i^{p-1} a_{j+(p-1)p^{n-1}}$$

i.e $a_j^{(i)} = \sum_{r=0}^{p-1} i^r \, a_{rp^{n-1}+j}$

Démonstration du théorème 1 :

Par récurrence sur n.

Il est clair que pour n = 0, f étant l'application constante,

$$f^* = a^* = a_0$$

Pour n = 1, $f(x) = \sum_{j=0}^{p-1} a_j x^j = \sum_{j=0}^{p-1} m_{xj}^{(1)} a_j \quad \forall x \in \mathbb{Z}_p^n$

ce qui s'écrit : $f^* = M_1 a^*$.

Supposons le théorème vrai pour toute fonction de $\mathscr{E}_{n-1}$ et soit $f \in \mathscr{E}_n$. D'après le lemme 1, on a :

$$f(x_{n-1},\ldots,x_0) = \sum_{i=0}^{p-1} \alpha_i \, g_i(x_{n-2},\ldots,x_0)$$

où $$\alpha_i = (p-1) \prod_{\substack{j=0 \\ j\neq p-i}}^{p-1} (x_{n-1}+j)$$

et $$g_i(x_{n-2},\ldots,x_0) = f(i,x_{n-2},\ldots,x_0).$$

D'après le lemme 2 :

$$g_i(x_{n-2},\ldots,x_0) = \sum_{j=0}^{p^{n-1}-1} a_j^{(i)} \, m_j \, (x_{n-2},\ldots,x_0)$$

avec $$a_j^{(i)} = \sum_{r=0}^{p-1} i^r \, a_{rp^{n-1}+j}$$

Posons $b^r = (a_{rp^{n-1}}, a_{rp^{n-1}+1}, \ldots, a_{rp^{n-1}+p-1})^t$.

D'après l'hypothèse de récurrence, on a :

$$g_i(x_{n-2},\ldots,x_0) = \left[M_{n-1} \, a^{(i)*}\right]_k. \quad \text{où} \quad k = \sum_{j=0}^{n-2} x_j \, p^j$$

$$= \sum_{r=0}^{p-1} \left[i^r \, M_{n-1} \, b^r\right]_k.$$

$$= \sum_{r=0}^{p-1} \left[m_{ir}^{(1)} \, M_{n-1} \, b^r\right]_k.$$

donc $g_i(x_{n-2},\ldots,x_0)$ est la $k^{\text{ième}}$ ligne de la matrice :

$$M_{n-1}b^0 + m_{i_1}^{(1)} \, M_{n-1}b^1 + \ldots + m_{i(p-1)}^{(1)} \, M_{n-1}b^{p-1},$$

en remarquant que :

$(b^0, b^1, \ldots, b^{p-1}) = a^*$, on en déduit que $g_i(x_{n-2},\ldots,x_0)$ est la $k^{\text{ième}}$ ligne de $(M_1 \otimes M_{n-1})a^*$ ainsi $f^* = M_n a^*$.

CALCUL DE L'INVERSE DE M_1 :

Dans de nombreux problèmes, nous sommes amenés à déterminer les coefficients $\{a_j\}$ à partir de la donnée des p^n valeurs de f. Les propriétés du corps fini $\mathbb{Z}_p$, nous permet de calculer explicitement l'inverse de la matrice M_1.

Soit g une racine primitive modulo (p), c'est-à-dire un générateur du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, et soit M la matrice :

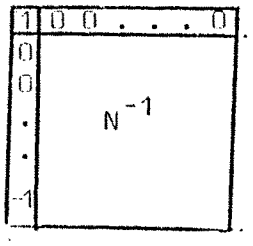
$$M = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 1 \\ 1 & g & g^2 & \ldots & g^{p-1} \\ \vdots & & & & \\ 1 & g^i & g^{2i} & \ldots & g^{(p-1)i} \\ \vdots & & & & \\ 1 & g^{(p-2)} & g^{2(p-2)} & \ldots & g^{(p-1)(p-2)} \end{vmatrix}$$

Le calcul de l'inverse de M nous permettra de calculer l'inverse de la matrice M_1. Remarquons d'abord que M est inversible. En effet, si $(e_1,\ldots,e_p)$ désigne la base canonique de $\mathbb{Z}_p^p$, considérons le sous-espace V engendré par $(e_2,\ldots,e_p)$, il est clair que V est stable par l'endomorphisme ϕ associé à M ; or, la matrice de ϕ/V par rapport à $(e_2,\ldots,e_p)$ est une matrice de "Van der Monde" qui est inversible. Par ailleurs, on a :

$$e_1 = \phi(e_1) - \phi(e_p)$$

ainsi $\phi^{-1}(e_1) = e_1 - e_p = (1 \quad 0 \quad 0 \quad \ldots \quad 0 \quad -1)^t$.

M est donc bien inversible et est de la forme :



ou N est une matrice de "Van der Monde".

CALCUL DE N^{-1} :

Rappelons qu'étant données k points distincts $\alpha_1,\ldots,\alpha_k$ d'un corps commutatif K et $b_1,\ldots,b_k$, k points de K, il existe un et un seul polynôme $P \in K(X)$ de degré $< k$ tel que la fonction polynômiale associée vérifie :

$$\forall i \in \{1,\ldots,k\} \qquad P(\alpha_i) = b_i.$$

Ce polynôme est donné par la formule de Lagrange :

$$P(X) = \sum_{i=1}^{k} b_i \prod_{\substack{j=1 \\ j\neq 1}}^{k} \frac{X-\alpha_j}{\alpha_i-\alpha_j}$$

si on pose $Q(X) = \prod_{i=1}^{k} (X-\alpha_j)$ on a :

$$Q'(X) = \sum_{i=1}^{k} \prod_{\substack{j=1 \\ j\neq i}}^{k} (X-\alpha_j) \qquad \text{et}$$

$$P(X) = \sum_{i=1}^{k} \frac{b_i}{Q'(\alpha_i)} \prod_{\substack{j=1 \\ j\neq i}}^{k} (X-\alpha_j) \qquad (*)$$

Désignons par $S_1^{(i)}$, $S_2^{(i)}$,..., $S_{k-1}^{(i)}$ les (k-1) fonctions symétriques élémentaires en α_1, α_2,..., α_{i-1}, α_{i+1},..., α_k, il résulte alors de (*) que la matrice :

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots\ldots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots\ldots & \alpha_2^{k-1} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ 1 & \alpha_k & \alpha_k^2 & \ldots\ldots & \alpha_k^{k-1} \end{vmatrix}$$

a pour matrice inverse la matrice :

$$\text{Diag}(1/Q'(\alpha_1),\ldots,1/Q'(\alpha_k)) \cdot \begin{vmatrix} (-1)^{k-1}S_{k-1}^{(1)} & (-1)^{k-2}S_{k-2}^{(1)} & \ldots\ldots & -S_1^{(1)} & 1 \\ (-1)^{k-1}S_{k-1}^{(2)} & (-1)^{k-2}S_{k-2}^{(2)} & \ldots\ldots & -S_1^{(2)} & 1 \\ \vdots & & & & \\ (-1)^{k-1}S_{k-1}^{(k)} & (-1)^{k-2}S_{k-2}^{(k)} & \ldots\ldots & -S_1^{(k)} & 1 \end{vmatrix}$$

Remarquons que si on pose $k = p-1$ et $\alpha_i = g^i$, cette matrice nous donne l'inverse de la matrice ${}^tN$.

Calcul de $S_i^{(j)}$ en fonction de g, i et j.

On a :

$$Q(X) = \prod_{i=1}^{p-1} (X-g^i) = X^{p-1}-1$$

car les g^i sont toutes les racines (p-1)ièmes de 1 dans $\mathbb{Z}/p\mathbb{Z}$.

On a donc : $\forall i \in \{1,\ldots,p-1\}$

$$Q'(g^i) = (p-1)\, g^{i(p-2)} = -g^{-i} \qquad (1)$$

Par ailleurs, considérons les polynômes :

$$P_i(X) = Q(X)(X-g^i)^{-1} \qquad i = 1,\ldots,p-1$$

$$= \sum_{j=0}^{p-3} (-1)^{p-2-j} S_{p-2-j}^{(i)} X^j + X^{p-2}$$

$\forall j \in \{0,1,\ldots,p-3\}$ on a :

$$S_{p-2-j}^{(i)} = (-1)^{j+1} \frac{1}{j!} \frac{d^j}{dX^j} [P_i(X)]_{X=0}$$

or $$\frac{d^j}{dX^j}[Q(X)(X-g^i)^{-1}] = \sum_{\ell=0}^{j} \binom{j}{\ell} Q^{(j-\ell)}(X) \frac{d^\ell}{dX^\ell}[(X-g^i)^{-1}]$$

d'où $$S_{p-2-j}^{(i)} = (-1)^{j+1}\, g^{-i(j+1)} \qquad (2)$$

puisque $$Q^{(k)}(X) = (p-1) \ldots (p-1-k)\, X^{p-1-k}$$

$$S^{(k)}(0) = 0 \quad \text{si } k \neq 0 \quad \text{et } Q(0) = -1$$

et $$\frac{d^j}{dX^j}[(X-g^i)^{-1}]_{X=0} = -j!\, g^{-i(j+1)}$$

Les identités (1) et (2) montrent que l'inverse de la matrice ${}^tN$ est la matrice :

$$- \text{Diag}(g, g^2, \ldots, 1) \begin{vmatrix} g^{-1} & g^{-2} & \ldots & g^{-(p-2)} & 1 \\ g^{-2} & g^{-4} & \ldots & g^{-2(p-2)} & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 1 & 1 & & 1 & 1 \end{vmatrix}$$

L'inverse de la matrice M est donc :

$$- \begin{vmatrix} -1 & 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & g^{-1} & g^{-2} & \ldots & g^{-(p-3)} & g^{(p-2)} \\ 0 & 1 & g^{-2} & g^{-4} & \ldots & g^{-2(p-3)} & g^{-2(p-2)} \\ \cdot & & & & & & \\ \cdot & & & & & & \\ \cdot & & & & & & \\ 0 & 1 & g^{-i} & g^{-2i} & \ldots & g^{-i(p-3)} & g^{-i(p-2)} \\ \cdot & \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot & \cdot \\ 1 & 1 & 1 & 1 & & 1 & 1 \end{vmatrix}$$

Remarquons que l'inverse de la matrice M_1 s'obtient de la manière suivante :

Si $M_1 =$ $\begin{array}{|c|c|} \hline 1 & 0\ 0\ \ldots\ 0 \\ \hline 1 & \\ \cdot & \\ \cdot & N \\ \cdot & \\ 1 & \\ \hline \end{array}$ alors $M_1^{-1} = -$ $\begin{array}{|c|c|} \hline -1 & 0\ 0\ \ldots\ 0 \\ \hline 0 & \\ 0 & \\ \vdots & R \\ 0 & \\ 1 & \\ \hline \end{array}$

où $R = (r_{ij})_{ij} = 1,2,\ldots,p-1$ avec $r_{ij} = n_{ji}^{p-2}$ $(= 1/n_{ji})$.

CALCUL DE M_n^{-1} :

$$M_n = M_1^{\otimes n} \qquad M_n^{-1} = (M_1^{-1})^{\otimes n}$$

donc la connaissance de M_1^{-1} détermine l'inverse de M_n, $\forall n$.

II - FORME CANONIQUE DE POLARITE $\alpha \in Z_p^n$ ET REPRESENTATION MATRICIELLE

D'après la proposition 1, $f \in \mathscr{E}_n$ s'écrit

$$f(x) = \sum_{i=0}^{p^n-1} a_i \, m_i(x)$$

Soit $\alpha = (\alpha_{n-1},\ldots,\alpha_o) \in Z_p^n$, en remplaçant $x = (x_{n-1},\ldots,x_1,x_o)$ par $x+\alpha = (x_{n-1}+\alpha_{n-1},\ldots,x_1+\alpha_1, x_o+\alpha_o)$ dans l'expression de f et en corrigeant les coefficients a_i on obtient la

PROPOSITION 2

Pour $\alpha \in Z_p^n$, toute fonction $f \in \mathscr{E}_n$ s'écrit de manière unique

$$f(x) = \sum_{i=0}^{p^n-1} a_i(\alpha) m_i(x+\alpha) \qquad (2)$$

où $a_i(\alpha) \in Z_p$ et $m_i(x+\alpha) = \prod_{j=0}^{n-1} (x_j+\alpha_j)^{i_j}$, i_j étant le jième bit dans l'écriture de i en base p.

Une fonction $f \in \mathscr{E}_n$, admet p^n expressions différentes selon le choix de α . L'expression de f sous la forme (2) est appelée forme canonique de polarité α (pour $\alpha = 0$ on retrouve l'expression (1))

Exemple : p = 2, n = 3 et f donnée par sa table

$x_2x_1x_o$	f(x)
0 0 0	1
0 0 1	0
0 1 0	0
0 1 1	0
1 0 0	1
1 0 1	1
1 1 0	0
1 1 1	1

polarité (000) : $f(x_2x_1x_o) = 1+x_o+x_1+x_ox_1+x_ox_2$

$a^*(000) = (1,1,1,1,0,1,0,0)^t$

polarité (001) : $f(x_2x_1x_o) = (1+x_o)+x_2+(1+x_o)x_1+(1+x_o)x_2$

$a^*(001) = (0,1,0,1,1,1,0,0)^t$

polarité (010) : $f(x_2x_1x_o) = (1+x_1)+x_o(1+x_1)+x_ox_2$

$a^*(010) = (0,0,1,1,0,1,0,0)$

polarité (011) $f(x_2x_1x_0) = (1+x_0)(1+x_1)+(1+x_0)x_2+x_2$

$a^*(011) = (0,0,0,1,1,1,0,0)$

etc...

Représentation matricielle

Soit $\alpha = (\alpha_{n-1},\ldots,\alpha_0) \in Z_p^n$

Posons $N_n(\alpha) = N_1(\alpha_{n-1}) \otimes N_{n-1}(\alpha_{n-2},\ldots,\alpha_0,\alpha_1)$ avec pour $k \in Z_p$

$$N_1(k) = (n_{ij}^{(1)}(k))_{ij} \qquad i,j = 0,1,\ldots,p-1$$

et

$$n_{ij}^{(1)}(k) = C_j^i k^{j-i} \mod(p) \text{ si } j \geq i$$

$$= 0 \text{ sinon}$$

Avec ces notations on a le :

THEOREME 2

Soit $\alpha \in Z_p^n$, si on écrit f sous la forme

$$f(x) = \sum_{i=0}^{p^n-1} a_i(\alpha)\, m_i(x+\alpha)$$

alors on a la relation

$$a^*(0) = N_n(\alpha)a^*(\alpha)$$

La démonstration se fait par récurrence sur n et elle est strictement analogue à celle du théorème 1.

Exemple : p = 2 et n = 2 $\quad \alpha = (\alpha_1, \alpha_0) \in Z_2^2$

$$f(x_1,x_0) = a_0(\alpha)+a_1(\alpha)(x_0+\alpha_0)+a_2(\alpha)(x_1+\alpha_1)+a_3(\alpha)(x_1+\alpha_i)(x_0+\alpha_0)$$

$$= a_0(\alpha)+\alpha_0 a_1(\alpha)+\alpha_1 a_2(\alpha)+\alpha_0\alpha_1 a_3(\alpha) +$$

$$[a_1(\alpha)+\alpha_1 a_3(\alpha)]x_0 +$$

$$[a_2(\alpha)+\alpha_0 a_3(\alpha)]x_1 +$$

$$a_3(\alpha)x_0x_1$$

d'où

$$\begin{bmatrix} a_0(0) \\ a_1(0) \\ a_2(0) \\ a_3(0) \end{bmatrix} = \begin{bmatrix} 1 & \alpha_0 & \alpha_1 & \alpha_0\alpha_1 \\ 0 & 1 & 0 & \alpha_1 \\ 0 & 0 & 1 & \alpha_0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} a_0(\alpha) \\ a_1(\alpha) \\ a_2(\alpha) \\ a_3(\alpha) \end{bmatrix}$$

qui s'écrit :

$$a^*(0) = \begin{bmatrix} 1 & \alpha_1 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & \alpha_0 \\ 0 & 1 \end{bmatrix} . a^*(\alpha)$$

COROLLAIRE

Si f s'écrit :

$$f(x) = \sum_{i=0}^{p^n-1} a_i(\alpha)m_i(x+\alpha)$$

alors

$$f = M_n N_n(\alpha)\ a^*(\alpha)$$

Démonstration :

D'après le théorème 1 on a :

$$f^* = M_n a^*(0)$$

et d'après le théorème 2

$$a^*(0) = N_n(\alpha)a^*(\alpha)$$

d'où

$$f^* = M_n N_n(\alpha)a^*(\alpha).$$

PROPOSITION 3:

Pour tout $\alpha \in Z_p^n$ on a la relation

$$M_n N_n(\alpha) = P_n(\alpha)M_n$$

où

$$P_n(\alpha) = P_1(\alpha_{n-1}) \otimes \ldots \otimes P_1(\alpha_o)$$

avec $\forall k \in Z_p$, l'élément à la place (i,j) dans $P_1(k)$ est donné par

$$[P_1(k)](i,j) = 1 \iff j = k+i \pmod p$$

Démonstration

$$M_n N_n(\alpha) = (M_1 \otimes M_1 \otimes \ldots \otimes M_1)(N_1(\alpha_{n-1}) \otimes N_1(\alpha_{n-2}) \otimes \ldots \otimes N_1(\alpha_o))$$

$$= M_1N_1(\alpha_{n-1}) \otimes \ldots \otimes M_1N_1(\alpha_o)$$

et

$$P_n(\alpha)M_n = P_1(\alpha_{n-1})M_1 \otimes \ldots \otimes P_1(\alpha_o)M_1$$

Il suffit donc de montrer que

$$\forall k \in Z_p : M_1N_1(k) = P_1(k)M_1$$

$\forall (i,j) \in Z_p \times Z_p$ on a

$$[M_1N_1(k)](i,j) = \sum_{r=0}^{p-1} M_1(i,r)[N_1(k)](r,j)$$

$$= \sum_{r=0}^{j} i^r C_j^r k^{j-r}$$

en effet $M_1(i,r) = i^r$ et $N_1(k)(r,j) = \begin{cases} C_j^r k^{j-r} & \text{si } j \geq r \\ 0 & \text{sinon} \end{cases}$

donc $[M_1N_1(k)](i,j) = (i+k)^j$.

D'autre part :

$$[P_1(k)M_1](i,j) = \sum_{r=0}^{p-1} P_1(k)(i,r)M_1(r,j)$$

$$= M_1(k+i,j)$$

$$= (k+i)^j$$

d'où l'égalité.

Remarque -

La matrice $P_1(k)$ pour $k \in Z_p$, est une matrice de permutation circulante, c'est-à-dire qu'elle possède un seul 1 par ligne et $[P_1(k)](i,j) = [P_1(k)](i-1,j-1)$, de plus la première ligne est définie par

$$[P_1(k)](0,j) = 1 \iff j = k$$

III - ALGORITHME DE MINIMISATION

Le problème de minimisation de l'expression d'une fonction $f \in \mathcal{E}_n$ se formule de la manière suivante :
parmi les p^n formes canoniques de polarité $\alpha \in Z_p^n$:

$$f(x) = \sum_{i=0}^{p^n-1} a_i(\alpha)\, m_i(x+\alpha)$$

quelle est celle qui minimise le nombre de composantes non nulles de $a^*(\alpha)$?

Ce problème a été largement traité particulièrement dans le cas $p = 2$, tout d'abord par Ramamoorthy en 1965 [30] puis résolu par Mukhopadhyay et Schmitz [26] ; leur algorithme repose sur la recherche d'une clique maximale d'un graphe construit à partir de l'expression de 2^n "fonctions de polarité" calculées à partir de f (du point de vue pratique cet algorithme n'est applicable que pour de petites valeurs de n). Une autre approche du problème a été proposée par Swamy dans [39] , et nous verrons sur un exemple que sa solution est fausse.

Récemment, Pradhan [29] a attiré l'attention sur le fait que l'utilisation de fonctions f de Z_p^n dans Z_p est, dans différents domaines pratiques, beaucoup plus performantes que les fonctions booléennes classiques. Ainsi le problème de minimisation de fonction $f \in \mathcal{E}_n$ prend toute son importance [11] [12] [21] [23] [26] [36]

L'algorithme que nous proposons, pour p premier quelconque, repose sur le théorème suivant :

THEOREME 3

Si la forme canonique de polarité $\alpha \in Z_p^n$ d'une fonction $f \in \mathcal{E}_n$ est :

$$f(x) = \sum_{i=1}^{p^n-1} a_i(\alpha) m_i(x+\alpha)$$

alors

$$a^*(\alpha) = M_n^{-1} Q_n(\alpha) f^*$$

où $Q_n(\alpha)$ est définie par

$$Q_n(\alpha) = Q_1(\alpha_{n-1}) \otimes \ldots \otimes Q_1(\alpha_o)$$

et pour $k \in Z_p$

$$[Q_1(k)](i,j) = 1 \iff i = j+k \pmod p$$

Démonstration

D'après le corollaire du théorème 2 on a :

$$f^* = M_n N_n(\alpha) a^*(\alpha)$$

et d'après la proposition3on obtient

$$f^* = P_n(\alpha) M_n\, a^*(\alpha)$$

Le calcul de M_n^{-1} a été fait, reste à montrer que $P_n(\alpha)$ a pour inverse $Q_n(\alpha)$, pour cela il suffit de vérifier que
$\forall k \in Z_p$: $[P_1(k)Q_1(k)](i,j) = 1 \iff i = j$

En effet :

$$[P_1(k)Q_1(k)](i,j) = \sum_{r=0}^{p-1} [P_1(k)](i,r).[Q_1(k)](r,j)$$

$$= [Q_1(k)](i+k,j)$$

car $P_1(k)(i,r) = 1 \iff r = i+k \mod (p)$

or, par définition, $[Q_1(k)](i+k,j) = 1 \iff i+k = j+k \pmod p$

$\iff i = j \pmod p$

Ainsi, $[P_1(k)Q_1(k)](i,j) = 1 \iff i = j$

$P_n^{-1}(\alpha)$ s'obtient en écrivant :

$$P_n^{-1}(\alpha) = P_1^{-1}(\alpha_{n-1}) \otimes \dots \otimes P_1^{-1}(\alpha_0) = Q_n(\alpha)$$

d'où

$$a^*(\alpha) = M_n^{-1} Q_n(\alpha) f^*$$

Exemple : $n = 2$ $p = 3$ et f de Z_3^2 dans Z_3 donnée par sa table :

$x_1 x_0$	$f(x)$
0 0	1
0 1	0
0 2	0
1 0	2
1 1	2
1 2	1
2 0	2
2 1	1
2 2	0

Supposons que l'on veuille exprimer f en fonction de (x_0+2) et (x_1+1) c'est à-dire sous sa forme canonique de polarité $\alpha = (1,2)$.

$$Q_2(1,2) = Q_1(1) \otimes Q_1(2)$$

avec

$$Q_1(1) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{et } Q_1(2) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$Q_2(1,2)f^* = \left[\begin{array}{c|c|c} O & O & \begin{matrix}0&1&0\\0&0&1\\1&0&0\end{matrix} \\ \hline \begin{matrix}0&1&0\\0&0&1\\1&0&0\end{matrix} & O & O \\ \hline O & \begin{matrix}0&1&0\\0&0&1\\1&0&0\end{matrix} & O \end{array}\right] \begin{bmatrix}1\\0\\0\\2\\2\\1\\2\\1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\2\\0\\0\\1\\2\\1\\2\end{bmatrix}$$

et

$$M_2^{-1}Q_2(1,2)f^* = \left[\begin{array}{c|c|c} \begin{matrix}1&0&0\\0&2&1\\2&2&2\end{matrix} & O & O \\ \hline O & \begin{matrix}2&0&0\\0&1&2\\1&1&1\end{matrix} & \begin{matrix}1&0&0\\0&2&1\\2&2&2\end{matrix} \\ \hline \begin{matrix}2&0&0\\0&1&2\\1&1&1\end{matrix} & \begin{matrix}2&0&0\\0&1&2\\1&1&1\end{matrix} & \begin{matrix}2&0&0\\0&1&2\\1&1&1\end{matrix} \end{array}\right] \begin{bmatrix}1\\0\\2\\0\\0\\1\\2\\1\\2\end{bmatrix} = \begin{bmatrix}1\\2\\0\\2\\0\\2\\0\\2\\0\end{bmatrix}$$

et donc :

$$f(x_1,x_0) = 1+2(x_0+2)+2(x_1+1)+(x_1+1)(x_0+2)^2+2(x_1+1)^2(x_0+2)$$

Cas particulier p = 2

Dans ce cas, les matrices utilisées précédemment possèdent les propriétés suivantes :

$M_n = M_n^{-1}$, et M_n est la matrice de parité de Pascal

$$P_n(\alpha) = P_n^{-1}(\alpha) = Q_n(\alpha) \quad \forall \alpha \in Z_2^n$$

En effet :

$$M_1 = \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix} \text{ donc } M_1^{-1} = M_1 \text{ et } M_n^{-1} = M_n$$

et

$$P_1(k) = \begin{bmatrix}\bar{k} & k\\ k & \bar{k}\end{bmatrix} \quad \forall k \in Z_2, \text{ donc } P_1^{-1}(k) = P_1(k) = Q_1(k)$$

$$P_n^{-1}(\alpha) = P_n(\alpha) = Q_n(\alpha) \quad \forall \alpha \in Z_2^n$$

Ainsi, si la forme canonique de polarité $\alpha \in Z_2^n$ s'écrit

$$f(x) = \sum_{i=0}^{2^n-1} a_i(\alpha)\, m_i(x+\alpha)$$

alors

$$f^* = P_n(\alpha) M_n a^*(\alpha)$$

et

$$a^*(\alpha) = M_n P_n(\alpha)\, f^* \qquad (1)$$

Cette dernière formule montre que la solution proposée par Swamy [39] pour le calcul de $a^*(\alpha)$ est incorrecte dès que $n \geq 3$.
En effet, sa solution est la suivante :

$$a^*(\alpha) = M_n f^*_\alpha$$

où f^*_α est le vecteur de 2^n composantes obtenu à partir de f^* par la permutation circulaire mettant $f(\alpha_{n-1},\ldots,\alpha_o)$ en tête.

Exemples :

$n = 2 \quad \alpha = (1,0)$

$$a^*(1,0) = M_2 \cdot \begin{vmatrix} f(1,0) \\ f(1,1) \\ f(0,0) \\ f(0,1) \end{vmatrix} \qquad \text{(solution de Swany)}$$

et $$a^*(1,0) = M_2 \cdot \begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix} \cdot \begin{vmatrix} f(0,0) \\ f(0,1) \\ f(1,0) \\ f(1,1) \end{vmatrix} \qquad \text{(d'après (1))}$$

donc, pour $n = 2$, les 2 solutions coïncident.

$n = 3, \quad \alpha = (0,0,1)$

$$a^*(0,0,1) = M_3 \cdot \begin{vmatrix} f(0,0,1) \\ f(0,1,0) \\ f(0,1,1) \\ f(1,0,0) \\ f(1,0,1) \\ f(1,1,0) \\ f(1,1,1) \\ f(0,0,0) \end{vmatrix} \qquad \text{(solution de Swamy)}$$

or d'après (1) on a :

$$a^*(0,0,1) = M_3 \cdot \begin{vmatrix} 0\ 1\ 0\ 0 & & \\ 1\ 0\ 0\ 0 & O & \\ 0\ 0\ 0\ 1 & & \\ 0\ 0\ 1\ 0 & & \\ & 0\ 1\ 0\ 0 & \\ O & 1\ 0\ 0\ 0 & \\ & 0\ 0\ 0\ 1 & \\ & 0\ 0\ 1\ 0 & \end{vmatrix} \cdot f^*$$

$$= M_3 \begin{vmatrix} f(0,0,1) \\ f(0,0,0) \\ f(0,1,1) \\ f(0,1,0) \\ f(1,0,1) \\ f(1,0,0) \\ f(1,1,1) \\ f(1,1,0) \end{vmatrix}$$

ce qui est bien entendu, différent de la solution de Swamy.

Algorithme

Il est clair que le théorème 3, nous donne une méthode matricielle de calcul des $a^*(\alpha)$, $\alpha \in Z_p^n$, et donc du vecteur $a^*(\alpha)$ qui réalise le minimum. Nous avons expérimenté cet algorithme dans le cas p = 2 en utilisant la structure tensorielle des matrices utilisées comme le montre l'exemple suivant :

Soit $f : Z_2^3 \to Z_2$ dont l'expression de polarité zéro est :

$$f(x_2,x_1,x_o) = a_o + a_1x_o + a_2x_1 + a_3x_ox_1 + a_4x_2 + a_5x_ox_2 + a_6x_1x_2 + a_7x_ox_1x_2$$

La matrice carrée A d'ordre 2^3 dont les colonnes sont les $a^*(\alpha)$ pour $\alpha \in Z_2^3$ se construit de manière itérative à partir de $a^*(0)$.

Posons :

$$A_1^0 = \begin{bmatrix} a_0 & a_0+a_1 \\ a_1 & a_1 \end{bmatrix} \qquad A_2^0 = \begin{bmatrix} a_2 & a_2+a_3 \\ a_3 & a_3 \end{bmatrix}$$

$$A_3^0 = \begin{bmatrix} a_4 & a_4+a_5 \\ a_5 & a_5 \end{bmatrix} \qquad A_4^0 = \begin{bmatrix} a_6 & a_6+a_7 \\ a_7 & a_7 \end{bmatrix}$$

$$A_1^1 = \begin{bmatrix} A_1^0 & A_1^0+A_2^0 \\ A_2^0 & A_2^0 \end{bmatrix} \qquad A_2^1 = \begin{bmatrix} A_3^0 & A_3^0+A_4^0 \\ A_4^0 & A_4^0 \end{bmatrix}$$

$$A_1^2 = \begin{bmatrix} A_1^1 & A_1^1+A_2^1 \\ A_2^1 & A_2^1 \end{bmatrix}$$

Il est facile de voir que $A_1^2 = A$.

Exemple :

$$f(x_2,x_1,x_0) = x_0+x_0x_1 + x_2x_1 + x_0x_2x_1$$

$$A_1^0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad A_2^0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$A_3^0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad A_4^0 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$A_1^1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad A_2^0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Les colonnes de A sont par construction, les différentes valeurs de $a^*(\alpha)$ pour $\alpha \in Z_2^3$ et le minimum est obtenu pour
$\alpha \in \{(0,0,0), (0,1,1), (1,0,0), (1,0,1), (1,1,1)\}$

Ainsi la forme canonique de f de polarité $\alpha = (101)$ s'écrit

$$f(x_2x_1x_0) = 1+\bar{x}_0+x_1+\bar{x}_0x_1\bar{x}_2$$

Le programme (Fortran) exécuté sur Multics donne les temps moyens suivants (en secondes)

n =	2	3	4	5	6	7	8
t =	0,15	0,16	0,18	0,27	0,63	1,95	7,15

Le programme que nous reproduisonsdonne,à partir d'un vecteur a^* les vecteurs α et $a^*(\alpha)$ réalisant le minimum, ainsi que le nombre de composantes non nulles de $a^*(\alpha)$

```
C  "EXPRESSION CANONIQUE MINIMALE D'UNE FONCTION BOULEENNE "
      common a(256,256)
      integer a
  100 format(//," dimension ?" )
  101 format(/," entrez le vecteur a1:" )
  200 format(i2)
  201 format(" l1=" ,i4)
  300 format("  ",32i1)
  400  format (32i1)
    1 write(6,100)
      read(5,200)n
      if(n.eq.0) goto 9999
      jj=2**n
      write(6,101)
      read(5,400)(a(i,1),i=1,jj)
      s1=0
      s=0
      do 2 i=1,jj
    2 s=s+a(i,1)
      l1=1
      do 4 m=1,n
      m1=2**(m-1)+1
      m2=2**m
      do 3 l=m1,m2
      j1=2**(n-m)
      do 6 j=1,j1
      i1=1+(j-1)*m2
      i2=i1+m1-2
      do 5 i=i1,i2
      l1=l-(m1-1)
      l2=i+m1-1
      a(i,1)=a(i,l1)+a(l2,l1)
      a(i,1)=mod2(a(i,1))
      a(l2,1)=a(l2,l1)
    5 continue
    6 continue
      s1=0
      do 7 i=1,jj
      s1=s1+a(i,1)
    7 continue
      if(s1.lt.s) goto 10
      goto 3
   10 s=s1
      l1=l
    3   continue
    4 continue
      write(6,300)(a(i,l1),i=1,jj)
      write(6,201)l1
      goto 1
 9999 close(6)
      stop
      end
```

TROISIEME CHAPITRE

FACTORISATION DES PERMUTATIONS DE L'HYPERCUBE

§ 1 - Présentation et interprétation du problème

§ 2 - Cas des permutations affines

§ 3 - Une approche du cas général

§ 4 - Etude des permutations du cube C_3

§ 5 - Etude des permutations de l'hypercube C_4

I - Présentation et interprétation du problème

Pour $n \in \mathbb{N}$, notons C_n l'hypercube de dimension n. La position d'un sommet x de C_n est définie par la donnée d'un n-uplet $(x_1, x_2, \ldots, x_n)$ de $\{0,1\}^n$. On appellera naturellement sommet voisin de x chacuns des (n+1) sommets ne différant de x que par une composante au plus (par commodité, on considère que tout sommet est son propre voisin) et une permutation sur C_n est dite élémentaire si elle transforme chaque sommet x de C_n en l'un de ses voisins.

Toute permutation P de C_n est décomposable en un produit de permutations élémentaires, car on peut recouvrir (au sens des sommets) l'hypercube C_n par un arbre, et toute permutation sur les sommets d'un arbre est factorisable en un produit de transpositions qui correspondent à des échanges de sommets voisins sur C_n.

Le problème auquel on s'est intéressé au sein du groupe de travail "Comportement d'itérations" [9] est celui de déterminer la quantité

$$\phi(n) = \max \{\ell(P),\ P \in \mathscr{P}_n\}$$

où $\mathscr{P}_n$ est l'ensemble de $(2^n)!$ permutations de C_n et $\ell(P)$ désigne la longueur minimale de la factorisation de P en produit de permutations élémentaires.

Ce problème s'inscrit dans le cadre général de la décomposition minimale d'une permutation en un produit de permutations compatibles avec un graphe donné [40], et c'est un problème qui intervient également en théorie des codes [3][46].

Interprétation matricielle :

Une permutation P des 2^n sommets de C_n peut être représentée par une matrice M de permutation d'ordre 2^n. Ainsi, si

$$P = P_1 \cdot P_2 \cdots P_r$$

est une décomposition de P en produit de permutations élémentaires P_i, alors :

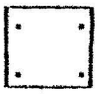
$$M = M_1 \cdot M_2 \cdots M_r$$

où M est la matrice de permutation représentant P est les M_i, $i = 1,\ldots,r$ sont les matrices de permutation représentant les permutations élémentaires P_i de C_n. Ainsi $\phi(n)$ peut être également défini par :

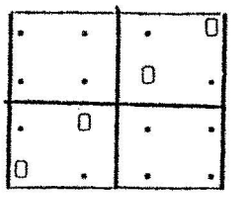
$$\phi(n) = \max\{r(M) \ / \ M \in \mathscr{R}_n\}$$

où $\mathscr{R}_n$ est l'ensemble des matrices de permutation d'ordre 2^n et r(M) désigne la longueur minimale de la décomposition de la matrice M en produit de matrices de permutations représentant des permutations élémentaires de C_n et dont la forme M_n est définie de manière récurrente par :

$M_1 =$



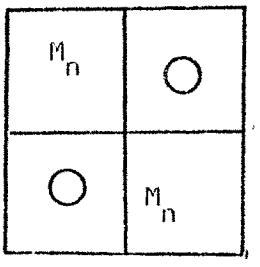
$M_2 =$



(les éléments égaux à 1 doivent être placés en une position indiquée par un point).

et plus généralement :

M_{n+1} =



Exemple 1

Soit P la permutation du cube C_3 donnée par :

x	P_x
000	111
001	101
010	001
011	100
100	010
101	000
110	110
111	011

P est factorisable en 3 permutations élémentaires de la manière suivante :

x	P_1x	P_2P_1x	$P_3P_2P_1x = Px$
000	010	011	111
001	101	101	101
010	000	001	001
011	111	110	100
100	110	010	010
110	100	100	110
111	011	111	011

Matriciellement cette décomposition peut s'écrire :

$$\begin{vmatrix} 00000100 \\ 00100000 \\ 00001000 \\ 00000001 \\ 00010000 \\ 01000000 \\ 00000010 \\ 10000000 \end{vmatrix} = \left|\begin{array}{cc} 1000 & 0000 \\ 0100 & 0000 \\ 0010 & 0000 \\ 0000 & 0001 \end{array}\right| \cdot \left|\begin{array}{cc} 0000 & 0010 \\ 0000 & 0100 \\ 0000 & 1000 \\ 0001 & 0000 \end{array}\right| \cdot \left|\begin{array}{cc} 0100 & 0000 \\ 1000 & 0000 \\ 0001 & 0000 \\ 0000 & 0001 \end{array}\right| \cdot \left|\begin{array}{cc} 0010 & 0000 \\ 0000 & 0100 \\ 1000 & 0000 \\ 0000 & 0001 \end{array}\right|$$

$$M = M_3 \cdot M_2 \cdot M_1$$

Interprétation algébrique

L'hypercube $C_n = \{0,1\}^n$ peut être considéré comme espace vectoriel de dimension n sur le corps Z_2. Soit $e^1, e^2, \ldots, e^n$ sa base canonique ($e^i_j = 0$ si $j \neq i$ et $e^i_i = 1$). Dans toute la suite $\{0,1\}^n$ sera muni des opérations "+" et "." induites par celles du corps Z_2.

Dans ce contexte, deux vecteurs différents x et y de $\{0,1\}^n$ sont voisins si :

$$\exists i \in \{1,2,\ldots,n\} \ / \ x+y = e^i.$$

Remarque -

Si une permutation P de C_n transforme un élément $a \in \{0,1\}^n$ en $\bar{a} = a+1$, alors, pour réaliser P(a) à l'aide de permutations élémentaires, il est nécessaire de procéder au moins n fois donc $\ell(P) \geq n$, ce qui nous donne la minoration :

$$\forall n \in \mathbb{N}, \quad \phi(n) \geq n.$$

I - CAS DES PERMUTATIONS AFFINES DE L'HYPERCUBE

DEFINITION

Soit $F : \{0,1\}^n \to \{0,1\}^n$

$$x \to F(x) = Ax + b \ , \ b \in \{0,1\}^n \ , \ A \in \mathcal{M}_n(Z_2)$$

F est une permutation affine de l'hypercube si A est inversible (les opérations considérées sont toujours celles du corps Z_2)

Il y a exactement $\prod_{i=0}^{n} (2^n - 2^i).2^n$ permutations affines de C_n [28]

Théorème 1

Toute permutation affine de l'hypercube se décompose en un produit d'au plus n permutations affines et élémentaires de l'hypercube.

La démonstration repose sur le lemme suivant :

Lemme 1

Si F est une permutation affine de l'hypercube, alors il existe F_1 permutation affine et élémentaire de l'hypercube telle que

$$\forall x \quad \{0,1\}^n \quad [(F_1 \circ F)(x)]_1 = x_1$$

Démonstration

Soit $F(x) = Ax + b$ $\quad A \in \mathcal{M}_n(Z_2)$ inversible et $b \in Z_2^n$

Soit $\alpha_{1.}^t$ la première ligne de A^{-1} .

Appelons K_1 la matrice identité dans laquelle on remplace la première ligne par $\alpha_{1.}^t$ et K_2 la matrice K_1 dans laquelle on remplace la $i_o^{ème}$ ligne par $(\alpha_{1.}^t + e_1 + e_{io})^t$ où io est le plus petit indice tel que $\alpha_{1io} = 1$.

Posons enfin

$$F_1(x) = \alpha_{11}[K_1x + (\alpha_{1.}^t b)e_1] + \bar{\alpha}_{11}[K_2x + (\overline{\alpha_1^t b})\, e_{io} + (\alpha_{1.}^t b)e_1]$$

Vérifions que F_1 est bien la fonction cherchée.

$$* \quad F_1(x) = \begin{cases} K_1x + (\alpha_{1.}^t b)e_1 & \text{si } \alpha_{11} = 1 \\ K_2x + (\overline{\alpha_{1.}^t b})e_{i_o} + (\alpha_{1.}^t b)e_1 & \text{si } \alpha_{11} = 0 \end{cases}$$

si $\alpha_{i1} = 1$ $\quad \det K_1 = \alpha_{11} = 1 \to K_1$ est inversible

si $\alpha_{11} = 0$ $\quad \det K_2 = \alpha_{1i_o} = 1 \to K_2$ est inversible

donc F_1 est bien une permutation affine de l'hypercube.

* F_1 est élémentaire

en effet

$\forall x \in \{0,1\}^n$

$$F_1(x) + x = \alpha_{11} [K_1 x + (\alpha_{1.}^t b)e_1] + \bar{\alpha}_{11} [K_2 x + \overline{(\alpha_{1.}^t b)} e_{i_o} + (\alpha_{1.}^t b)e_1] + x$$

$\forall k \neq 1$, io on a

$$(F_1(x)+x)_k = \alpha_{11} [x_k] + \bar{\alpha}_{11} [x_k] + x_k = 0$$

$$(F_1(x) + x)_1 = \alpha_{11} [\alpha_{1.}^t x + \alpha_{1.}^t b] + \bar{\alpha}_{11} [\alpha_{1.}^t x + \alpha_{1.}^t b] + x_1$$

$$= \alpha_{1.}^t x + \alpha_{1.}^t b + x_1$$

$$(F_1(x) + x)_{io} = \alpha_{11} [x_{io}] + \bar{\alpha}_{11} [\alpha_{1.}^t x + x_1 + x_{io} + \overline{(\alpha_{1.}^t b)}] + x_{io}$$

$$= \bar{\alpha}_{11} [\alpha_{1.}^t x + x_1 + \overline{\alpha_{1.}^t b}]$$

$$= \bar{\alpha}_{11} \overline{(\alpha_{1.}^t x + \alpha_{1.}^t b + x_1)}$$

Ainsi $\forall x \in \{0,1\}^n$ $(F_1(x) + x)_1 \cdot (F_1(x) + x)_{io} = 0$ de telle sorte que la première et la $i_o^{ème}$ composante de F_1 ne peuvent changer simultanèment donc F_1 est élémentaire.

* Reste à montrer que $\forall x \in \{0,1\}^n$ $[(F_1 \text{ o } F)x]_1 = x_1$

$$[F_1(F(x)]_1 = \alpha_{11}[\alpha_{1.}^t Ax + \alpha_{1.}^t b + \alpha_{1.}^t b] + \bar{\alpha}_{11}[\alpha_{1.}^t Ax + \alpha_{1.}^t b + \alpha_{1.}^t b]$$

$$= \alpha_{1.}^t Ax$$

$$= x_1$$

Ce qui achève la démonstration du lemme.

Démonstration du théorème :

D'après le lemme 1 on a

$F = F_1^{-1} \text{o } F_1'$

où F_1 est une permutation élémentaire affine de l'hypercube et F'_1 est une permutation affine de l'hypercube telle que

$$(F'_1(x))_1 = x_1$$

Nous allons montrer que

$\forall k$, $1 \leq k \leq n-1$, il existe $F_1, F_2, \ldots, F_k$ des permutations élémentaires affines de l'hypercube telles que

$F_k \circ \ldots \circ F_2 \circ F_1 \circ F = F'_k$ permutation affine de l'hypercube et

$[F'_k(x)]_i = x_i \qquad i = 1,2,\ldots,k$

Recurrence sur k :

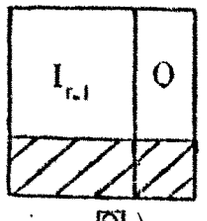
k = 1 est montré dans le lemme précédent.

Supposons avoir trouvé $F_1, F_2, \ldots, F_{r-1}$ des permutations élémentaires affines de l'hypercube telles que :

$F_{r-1} \circ F_{r-2} \circ \ldots \circ F_1 \circ F = F'_{r-1}$ soit une permutation affine de l'hypercube et $(F'_{r-1}(x))_i = x_i \qquad i = 1,2,\ldots,r-1$

Posons $F'_{r-1}(x) = A^{(r-1)}x + b^{(r-1)}$

$A^{(r-1)} \in \mathcal{M}_n(Z_2)$ inversible de la forme

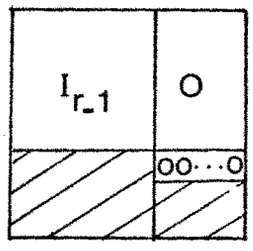
$A^{(r-1)} =$ 

$I_{r-1} \in \mathcal{M}_{(r-1)}(Z_2)$

et $b^{r-1)} =$ 

Soit $\alpha^t_{r.}$ la $r^{ième}$ ligne de $(A^{(r-1)})^{-1}$

Appelons $K_1^{(r)}$ la matrice identité dans laquelle on remplace la $r^{ième}$ ligne par $\alpha_{r.}^t$ et $K_2^{(r)}$ la matrice $K_1^{(r)}$ dans laquelle on remplace la $i_o^{ème}$ ligne par $(\alpha_{r.}^t + e_r + e_{io})^t$ où io est le plus petit indice $\geq r$ tel que $\alpha_{rio} = 1$. io existe bien sinon $[A^{(r-1)}]^{-1}$ serait de la forme :



et serait par conséquent singulière.

Posons $F_r(x) = \alpha_{rr}[K_1^{(r)}x + (\alpha_{r.}^t b^{r-1})e_r] + \bar{\alpha}_{rr}[K_2^{(r)}x + (\overline{\alpha_{r.}^t b^{r-1}})e_{io} + (\alpha_{r.}^t b^{r-1}$

Une démonstration identique au lemme précédent permet d'affirmer que F_r est une permutation affine et élémentaire de l'hypercube, il suffit de vérifier que

$$[F_r \circ F'_{r-1}(x)]_i = x_i \quad \text{pour } i = 1,2,\ldots,r$$

$$[F_r \circ F'_{r-1}(x)]_i = \alpha_{rr}[F'_{r-1}(x)]_i + \bar{\alpha}_{rr}[F'_{r-1}(x)]_i \qquad \text{si } i \leq r-1$$

$$= \alpha_{rr} x_i + \bar{\alpha}_{rr} x_i \quad \text{par hypothèse de recurrence.}$$

$$= x_i$$

et $[F_r \circ F'_{r-1}(x)]_r = \alpha_r^t F'_{r-1}(x) + \alpha_r^t b^{(r-1)}$

$$= \alpha_{r.}^t (A^{(r-1)}x + b^{(r-1)}) + \alpha_{r.}^t b^{(r-1)}$$

$$= \alpha_{r.}^t A^{(r-1)} x$$

$$= x_r$$

Il est clair d'après ce qui précède, qu'au plus à l'étape (n-1), on a

$F_{n-1} \circ F_{n-2} \circ \ldots \circ F_1 \circ F = F'_{n-1}$ avec F'_{n-1} élémentaire

puisque $(F'_{n-1}(x))_i = x_i \qquad i = 1,2,\ldots,n-1$

ainsi $F = F_1^{-1} \circ F_2^{-1} \circ \ldots \circ F_{n-1}^{-1} \circ F'_{n-1}$

d'où le résultat.

Remarque : La décomposition donnée dans le théorème est optimale dans le sens suivant :

Si $t(F)$ est le plus petit entier qui réalise la décomposition de F en un produit de permutations affines et élémentaires de l'hypercube, alors

$$\max_F t(F) = n$$

En effet la permutation affine $F(x) = \bar{x}$, change les n composantes de x, et comme toute permutation élémentaire n'en change qu'une seule, on a $t(F) \geq n$, or d'après ce qui précède $t(F) \leq n$ d'où l'égalité.

Exemple :

$$F(x) = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} x + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = A_0 x + b_0$$

Avec les notations utilisées dans la démonstration du théorème précédent, nous obtenons le programme suivant :

. la première ligne de A^{-1} est $\alpha^{(0)}_{1.} = 01110$ ainsi $\beta^{(0)}_{2.} = (10110)$

$$\text{d'où } F_1 \circ F(x) = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{vmatrix} x + \begin{vmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{vmatrix} = A_1 x + b_1$$

. la deuxième ligne de A_1^{-1} est $\alpha^{(1)}_{2.} = 10101$ ainsi $\beta^{(1)}_{3.} = (11001)$

$$\text{d'où } F_2 \circ F_1 \circ F(x) = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{vmatrix} x + \begin{vmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix} = A_2 x + b_2$$

. la troisième ligne de A_2^{-1} est $\alpha^{(2)}_{3.} = (01101)$

$$\text{d'où } F_3 \circ F_2 \circ F_1 \circ F(x) = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{vmatrix} x + \begin{vmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{vmatrix} = A_3 x + b_3$$

. la quatrième ligne de A_3^{-1} est $\alpha_{4.}^{(3)} = (01101)$ ainsi $\beta_{4.}^{(3)} = (01110)$

d'où $F_4 \circ F_3 \circ F_2 \circ F_1 \circ F(x) = x$

Une conséquence : calcul de $\phi(2)$

Soit $h : \{0,1\}^n \to \{0,1\}$

Nous dirons que h est équilibrée si et seulement si

$$|\{x \in \{0,1\}^n : h(x) = 0\}| = 2^{n-1}$$

Si $h^* \in \{0,1\}^{2^n}$ est le vecteur des valeurs de f(x) quand x parcourt $\{0,1\}^n$ et si a^* désigne le vecteurs des coefficients de f dans la forme de Reed-Muller alors

$$a^* = M_n h^*$$

où M_n est la matrice de parité de Pascal, (cf.chapitre 2).

Ainsi si h est équilibrée alors le degré total de h est inférieur ou égal à n-1.

Donc pour n=2 toute fonction équilibrée de $\{0,1\}^2 \to \{0,1\}$ est affine d'où le

Corollaire :

Toute permutation de C_2 est décomposable en un produit d'au plus deux permutations élémentaires d'où $\phi(2) = 2$.

Nous disposons d'un programme (Fortran) qui permet de factoriser une pemutation affine de C_n en produit d'au plus n permutations élémentaires. Ce programme nous donne, à chaque étape m de son exécution, la permutation affine $F_m \circ F_{m-1} \circ \ldots \circ F_1 \circ F$ puis la permutation élémentaire F_{m+1} $(m = 0,1,2,\ldots,n-1)$.

Exemple 1:

$$A = \begin{matrix} 11001 \\ 01001 \\ 00010 \\ 01010 \\ 11110 \end{matrix} \qquad \text{et} \quad b=0$$

M = 0

11001	01010101101010101010101001010101
01001	01010101101010100101010110101010
A= 00010	00110011001100110011001100110011
01010	00110011111001100001100111001100
11110	00111100110000111100001100111100

Permutation elementaire posant x1

11000	0	
01000	0	
A1= 00100	b1= 0	F1(x)=A1x+b1
00010	0	
00001	0	

M = 1 : Image de $(0,1)^5$ par F1oF

10000	00000000000000001111111111111111
01001	01010101101010100101010110101010
00010	00110011001100110011001100110011
01010	00110011111001100001100111001100
11110	00111100110000111100001100111100

Permutation elementaire posant x2

10000	0	
00110	0	
A2= 01010	b2= 1	F2(x)=A2x+b2
00010	0	
00001	0	

M = 2 Image de $(0,1)^5$ par F2oF1oF

10000	00000000000000001111111111111111
01000	00000000111111111000000011111111
00011	10011001100110011001100110011001
01010	00110011111001100001100111001100
11110	00111100110000111100001100111100

Permutation elementaire posant x3

10000	0	
01000	0	
A3= 10011	b3= 0	F3(x)=A3x+b3
10101	1	
00001	0	

M = 3 — Image de $\langle 0,1 \rangle^5$ par F3oF2oF1oF

```
10000   00000000000000000111111111111111
01000   00000000111111111000000011111111
00100   00001111000011110000111100001111
01101   01011010101001010101101010100101
11110   00111110011000011110000110011110 0
```

Permutation elementaire posant x4

```
      10000    0
      01000    0
A4=   00100 b4=0        F4(x)=A4x+b4
      11101    0
      11110    1
```

M = 4 — Image de $\langle 0,1 \rangle^5$ par F4oF3oF2oF1oF

```
10000   00000000000000000111111111111111
01000   00000000111111111000000011111111
00100   00001111000011110000111100001111
00010   00110011001100110011001100110011
10001   10101010101010100101010101010101
```

Permutation elementaire posant x5

```
      10000    0
      01000    0
A5=   00100 b5=0        F5(x)=A5x+b5
      00010    0
      10001    0
```

M = 5 — Image de $\langle 0,1 \rangle^5$ par F5oF4oF3oF2oF1oF

```
10000   00000000000000000111111111111111
01000   00000000111111111000000011111111
00100   00001111000011110000111100001111
00010   00110011001100110011001100110011
00001   01010101010101010101010101010101
```

Exemple 2 :

```
          011001
          110010
          000011
     A=   110011      et  b=0
          100011
          000111
```

M = 0

```
          011001     0101010111010101010101010310101010101010101110101010101010101001010101
          110010     0011001100110011111001100110011001100110011001100001100110011001100011
          000011     0110011001100110011001100110011001100110011001100110011001100110011001100110
A=        110011     0110011001100110101001100110011001100110011001100110011001011001100110011001100110
          100011     0110011001100110011001100110011010011001100110011001100110011001100110011001
          000111     0110100101110100101110100101110100101110100101110100101110100101110100101101001
```

Permutation elementaire posant x1

```
          001010     0
          010000     0
          100010     1
A1=       000100  b1=0          F1(x)=A1x+b1
          000010     0
          000001     0
```

M = 1 Image de (0,1) par F1oF

```
          100000     0000000000000000000000000000000001111111111111111111111111111111111111
          110010     0011001100110011111001100110011001100110011001100001100110011001100011
          111010     1100110000110011001100111111001100001100111110011001100110000110011
          110011     0110011001100110101001100110011001100110011001100110011001011001100110
          100011     0110011001100110011001100110011010011001100110011001100110011001100110
          000111     0110100101110100101110100101110100101110100101110100101110100101110100101101001
```

Permutation elementaire posant x2

```
          100000     0
          000110     0
          001000     0
A2=       010010  b2=1          F2(x)=A2x+b2
          000010     0
          000001     0
```

M = 2 Image de (0,1) par F2oF1oF

```
          100000     0000000000000000000000000000000001111111111111111111111111111111111111
          010000     0000000000000000011111111111111111000000000000000001111111111111111
          111010     1100110000110011001100111110011000011001111100110011001100001100011
          010001     1010101010101010100101010101010101101010101010101010010101010101010101
          100011     0110011001100110011001100110011010011001100110011001100110011001100110
          000111     0110100101110100101110100101110100101110100101110100101110100101110100101101001
```

Permutation elementaire posant x3

```
          100000     0
          010000     0
          001110     1
A3=       000100  b3=0          F3(x)=A3x+b3
          000010     0
          000001     0
```

M = 3 Image de $\{0,1\}^6$ par F3oF2oF1oF

```
100000  0000000000000000000000000000000011111111111111111111111111111111
010000  0000000000000000111111111111111100000000000000001111111111111111
001000  0000000011111111000000001111111100000000111111110000000011111111
010001  1010101010101010101010101010101101010101010101010101010101010101
100011  0110011001100110011001100110011010011001100110011001100110011001
000111  0110100101101001011010010110100101101001011010010110100101101001
```

Permutation elementaire posant x4

```
100000   0
010000   0
001000   0
A4= 100011  b4= 0        F4(x)=A4x+b4
100101   1
000001   0
```

M = 4 Image de $\{0,1\}^6$ par F4oF3oF2oF1oF

```
100000  0000000000000000000000000000000011111111111111111111111111111111
010000  0000000000000000111111111111111100000000000000001111111111111111
001000  0000000011111111000000001111111100000000111111110000000011111111
000100  0000111100001111000011110000111100001111000011110000111100001111
110110  0011110000111100110000111100001111000011110000110011110000111100
000111  0110100101101001011010010110100101101001011010010110100101101001
```

Permutation elementaire posant x5

```
100000   0
010000   0
001000   0
A5= 000100  b5= 0        F5(x)=A5x+b5
110110   0
000001   0
```

M = 5 Image de $\{0,1\}^6$ par F5oF4oF3oF2oF1oF

```
100000  0000000000000000000000000000000011111111111111111111111111111111
010000  0000000000000000111111111111111100000000000000001111111111111111
001000  0000000011111111000000001111111100000000111111110000000011111111
000100  0000111100001111000011110000111100001111000011110000111100001111
000010  0011001100110011001100110011001100110011001100110011001100110011
000111  0110100101101001011010010110100101101001011010010110100101101001
```

Permutation elementaire posant x6

```
100000   0
010000   0
001000   0
A6= 000100  b6= 0        F6(x)=A6x+b6
000010   0
000111   0
```

M = 6 Image de $\{0,1\}^6$ par F6oF5oF4oF3oF2oF1oF

```
100000  0000000000000000000000000000000011111111111111111111111111111111
010000  0000000000000000111111111111111100000000000000001111111111111111
001000  0000000011111111000000001111111100000000111111110000000011111111
000100  0000111100001111000011110000111100001111000011110000111100001111
000010  0011001100110011001100110011001100110011001100110011001100110011
000001  0101010101010101010101010101010101010101010101010101010101010101
```

II - UNE APPROCHE DU CAS GENERAL

L'algorithme proposé dans la démonstration du théorème précédent repose sur le fait que pour toute permuation affine F de C_n on a :

$\forall k \in \{1,2,\ldots,n\}$, $\exists E$ (permutation élémentaire): $[E \circ F(x)]_k = x_k$

Cette propriété reste-t-elle vraie si F n'est pas affine ?
La réponse est négative en général :

Exemple : $F : \{0,1\}^3 \to \{0,1\}^3$

$$f_1(x) = x_2 + x_3 + x_2x_3 + x_1x_2$$

$$f_2(x) = x_1 + x_2x_3 \qquad \text{(opérations dans } Z_2\text{)}$$

$$f_3(x) = x_1 + x_2 + x_2x_3$$

On vérifie dans cet exemple, que pour toute permuation élémentaire E :

$[E \circ F(x)]_1 \neq x_1$; par contre il existe E telle que $[E \circ F(x)]_2 = x_2$

La proposition suivante montre que dans cet exemple $\ell(F) \leq 3$

Proposition 1

Soit F une permutation de C_n

a) S'il existe une permutation élémentaire E et un entier k tels que

$[E \circ F(x)]_k = x_k$ alors $\ell(F) \leq 1 + \phi(n-1)$

b) S'il existe une permutation élémentaire E, un couple d'entiers (i,j) et un $\alpha \in \{0,1\}$ tels que

$[E \circ F(x)]_i = x_j + \alpha$, $(j,\alpha) \neq (i,0)$

alors $\ell(F) \leq 2 + \phi(n-1)$.

Démonstration

a) Démonstration immédiate

b) Posons

$$(E \circ F)(x) = (g_1(x),\ldots,g_{i-1}(x), x_j + \alpha, g_{i+1}(x),\ldots,g_j(x),\ldots,g_n(x))$$

et soit $E' : \{0,1\}^n \to \{0,1\}^n$ définie par

$$E'_k(x) = x_k \quad \text{pour } k \neq i \text{ et } j$$

$$E'_i(x) = x_j + \bar{\alpha}$$

$$E'_j(x) = x_i + \alpha$$

E' est une permutation élémentaire telle que

$$[E' \circ E \circ F(x)]_j = x_j$$

et d'après a)

$$\ell(E \circ F) \leq 1 + \phi(n-1)$$

d'où $\ell(F) \leq 2 + \phi(n-1)$

Quant une permutation vérifie les hypothèses de a) on dira brièvement qu'on peut poser x_i en f_i . De même si elle vérifie b) on dira qu'on peut poser $x_j + \alpha$ en f_i.

REMARQUE :

On pourrait penser que :

$\forall F \in \mathcal{P}_n$, $\exists E$ permutation élémentaire et $1 \leq i \leq n$ tels que :

$$[E \circ F(x)]_i = x_i \quad \text{ou} \quad [E \circ F(x)]_i = \bar{x}_i$$

ce qui n'est pas vrai en général.

EXEMPLE n = 4

x	F(x)
0 0 0 0	1 0 1 0
0 0 0 1	1 1 0 0
0 0 1 0	0 0 0 0
0 0 1 1	1 0 0 0
0 1 0 0	0 0 0 1
0 1 0 1	1 0 0 1
0 1 1 0	0 0 1 0
0 1 1 1	0 1 0 1
1 0 0 0	1 0 1 1
1 0 0 1	1 1 1 1
1 0 1 0	1 1 1 0
1 0 1 1	0 1 1 0
1 1 0 0	0 0 1 1
1 1 0 1	1 1 0 1
1 1 1 0	0 1 1 1
1 1 1 1	0 1 0 0

Il vient :

$$f_1(x) = 1+x_2+x_3+x_3x_4+x_2x_4+x_2x_3+x_1x_3+x_1x_2x_3$$

$$f_2(x) = x_4+x_3x_4+x_2x_4+x_1x_3+x_1x_2x_3$$

$$f_3(x) = 1+x_2+x_3+x_4+x_3x_4+x_2x_4+x_1x_4+x_1x_3+x_1x_2+x_1x_3x_4$$

$$f_4(x) = x_1+x_2+x_2x_3+x_1x_3+x_1x_2+x_2x_3x_4$$

Dans cet exemple on constate qu'il n'est pas possible de poser x_i , ni $\bar{x}_i$ en f_i pour $i=1,2,3,4$. Néanmoins F est factorisable en un produit de quatre permutations élémentaires :

$$\forall\, x \qquad F(x) = F_4\, F_3\, F_2\, F_1(x)$$

avec

x	$F_1(x)$	$F_2(x)$	$F_3(x)$	$F_4(x)$
0 0 0 0	0 1 0 0	0 1 0 0	1 0 0 0	1 0 0 0
0 0 0 1	0 0 0 0	0 1 0 1	1 0 0 1	0 1 0 1
0 0 1 0	0 1 1 0	0 0 1 0	0 0 0 0	0 1 1 0
0 0 1 1	0 0 1 0	0 0 1 1	0 0 0 1	0 0 1 0
0 1 0 0	0 1 0 1	0 0 0 0	1 1 0 0	0 0 0 0
0 1 0 1	0 0 0 1	0 0 0 1	1 1 0 1	0 1 0 0
0 1 1 0	0 1 1 1	0 1 1 0	0 1 0 0	1 1 1 0
0 1 1 1	0 0 1 1	0 1 1 1	0 0 1 1	0 1 1 1
1 0 0 0	1 1 0 0	1 0 0 1	1 0 1 0	1 0 1 0
1 0 0 1	1 1 0 1	1 0 1 1	1 0 1 1	0 0 0 1
1 0 1 0	1 0 1 0	1 1 1 0	0 0 1 0	1 0 1 1
1 0 1 1	1 0 1 1	1 0 1 0	1 1 1 1	0 0 1 1
1 1 0 0	1 0 0 0	1 0 0 0	1 1 1 0	1 1 0 0
1 1 0 1	1 0 0 1	1 1 0 0	0 1 0 1	1 0 0 1
1 1 1 0	1 1 1 0	1 1 1 1	0 1 1 0	1 1 1 1
1 1 1 1	1 1 1 1	1 1 0 1	0 1 1 1	1 1 0 1

Représentation d'une permutation par sa table

Une permutation $F = (f_1, f_2, \ldots, f_n)$ de C_n peut être représentée par une matrice T, $2^n \times n$, dont la $j^{ième}$ colonne correspond aux valeurs de f_j.

Si g est une application de $\{0,1\}^n$ dans $\{0,1\}$, dire qu'on peut poser g en f_j , $j \in \{1,2,\ldots,n\}$, revient à dire qu'on peut transformer la matrice T en une matrice T' de manière à ce que :

1) la $j^{ième}$ colonne de T' soit le vecteur des valeurs de g.

2) deux lignes de T et T' de même rang ne diffèrent que par une composante au plus (cad sont voisines).

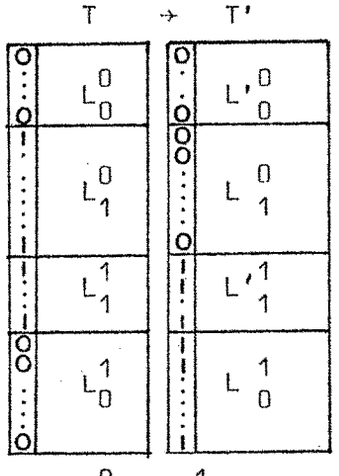
Nous allons voir sous quelles conditions cette transformation est possible .

Pour plus de clarté, nous nous interesserons seulement au cas $j = 1$ et $g(x) = x_1 \quad \forall x \in \{0,1\}^n$.

Pour p et q appartenant à $\{0,1\}$, posons :

$$L_p^q = \{x \in \{0,1\}^{n-1} \ / \ \exists y \in \{0,1\}^{n-1} : F(q,y) = (p,x)\}$$

Supposons que l'on veuille poser x_1 en f_1 , ceci se traduit (à une permutation près) par la transformation matricielle suivante :



On voit donc que L_1^0 et L_0^1 restent invariants, les conditions cherchées sont alors celles qui garantissent l'existence de L'^p_p , $p \in \{0,1\}$.

Soit $G(L_p^p , C_{n-1} , \Gamma_p)$ le graphe bipartie construit de la manière suivante :

Chaque élément $x \in L_p^p$ est relié à tous ses voisins dans C_{n-1} qui n'appartiennent pas à $L_{\bar{p}}^p$.

On notera $\Gamma_p(x) = V_{n-1}(x) - L_{\bar{p}}^{p}$ où $V_{n-1}(x)$ désigne l'ensemble des voisins immédiats de x dans C_{n-1} (en convenant que x est voisin de lui-même).

On est donc ramené à chercher les conditions qui garantissent l'existence de représentants distincts dans $\Gamma(x)$ pour chaque élément $x \in L_p^p$ (c'est-à-dire un couplage saturant les éléments de L_p^p.) Pour cela, nous disposons du théorème suivant :

Théorème de Hall [3]

Il existe un couplage saturant les sommets de L_p^p si et seulement si

$$\forall A \subset L_p^p \ : \ |\Gamma_p(A)| \geq |A| \ .$$

Nous allons, dans cette partie, établir une condition suffisante permettant d'appliquer le théorème de Hall.

DEFINITION

Si g et h sont deux fonctions équilibrées de $\{0,1\}^n$ dans $\{0,1\}$, nous notons

$$\delta(g,h) = \frac{1}{2} \left| \{x : g(x) \neq h(x)\} \right|$$

Cette quantité est entière car :

$$\left|\{x : g(x) \neq h(x)\}\right| = 2 \left|\{x : g(x) = 0 \text{ et } h(x) = 1\}\right|$$

Théorème 2

Soit $F : \{0,1\}^n \to \{0,1\}^n$ une permutation de C_n

et $g : \{0,1\}^n \to \{0,1\}$ équilibrée

s'il existe i tel que $\delta(f_i , g) < n$ alors

il existe une permutation élémentaire E telle que

$$[E \circ F(x)]_i = g(x) \qquad \forall x \in \{0,1\}^n$$

La démonstration repose sur le lemme suivant :

Lemme 2

Si $G(X,V_n)$ est le graphe de l'hypercube de dimension n alors

$$\forall A \subset X \ , \ A \neq \emptyset \qquad |V_n(A)| \geq \min \ \{2^n \ , \ |A| \ + n \ \}$$

Démonstration du lemme :

Nous raisonnons par recurrence sur n.

Le cas n = 1 est évident.

Supposons le résultat acquis pour n - 1 et montrons qu'il l'est alors pour n.

Posons $G_i = (X_i \ , \ V_{n-1}) \qquad i = 0,1$

les restrictions de $G = (X,V_n)$ aux sommets

$$X_i = \{x \in X \ ; \ x_1 = i \ \}$$

Pour $A \subset X$, posons

$$A_i = A \cap X_i \qquad i = 0,1$$

Nous avons alors

$$A = A_0 \cup A_1 \quad \text{d'où}$$

$$V_n(A) = V_n(A_0) \cup V_n(A_1)$$

de plus

$$|V_n(A_i)| = |V_{n-1}(A_i)| + |A_i|$$

par hypothèse de recurrence

$$|V_{n-1}(A_i)| \geq \min \{2^{n-1} \ , \ |A_i| + n - 1 \ \}$$

Nous distinguons alors les cas suivants :

1) $\exists i \in \{0,1\}$ tel que $|A_i| = 2^{n-1}$

alors $|V_{n-1}(A_i)| = |A_i| = 2^{n-1}$

d'où $|V_n(A)| = 2^n$

2) $\forall i \in \{0,1\}\ |A_1| < 2^{n-1}$

* $0 = |A_0| < |A_1| \leq 2^{n-1} - (n-1)$

  $|V_n(A)| = |V_n(A_1)| = |V_{n-1}(A_1)| + |A_1|$

  or $|V_{n-1}(A_1)| \geq |A_1| + n - 1$ et $|A| = |A_1| \geq 1$

  d'où $|V_n(A)| \geq |A| + n$

* $0 = |A_0|$ et $|A_1| > 2^{n-1} - (n-1)$

  $|V_n(A)| = |V_{n-1}(A_1)| + |A_1|$

  or $|V_{n-1}(A_1)| = 2^{n-1}$ et $|A| = |A_1|$

  d'où $|V_n(A)| \geq n + |A|$ pour $n \geq 2$

* $0 < |A_0| \leq 2^{n-1} - (n-1)$

  $|V_n(A)| \geq |V_{n-1}(A_0)| + |V_{n-1}(A_1)|$

  or $|V_{n-1}(A_0)| \geq |A_0| + n-1$ et $|V_{n-1}(A_1)| \geq |A_1| + 1$

  d'où $|V_n(A)| \geq |A_0| + n - 1 + |A_1| + 1$

  $|V_n(A)| \geq |A| + n$

* $2^{n-1}-(n-1) < |A_0|$, $|A_1| < 2^{n-1}$

$|V_{n-1}(A_0)| \geq 2^{n-1}$ et $|V_{n-1}(A_1)| \geq 2^{n-1}$

d'où

$|V_n(A)| \geq 2^n$

Démonstration du théorème

Il nous suffit de montrer que l'hypothèse du théorème de Hall est vérifiée pour les graphes $G(L_p^p , C_{n-1} , \Gamma_p)$ $p = 0,1$

(Nous démontrons ainsi le théorème dans le cas particulier i = 1 et $g(x) = x_1$)

$\forall A \subset L_p^p$ on a

$\Gamma_p(A) = V_{n-1}(A) - L_{\bar{p}}^p$

comme $|L_{\bar{p}}^p| < n$ nous avons

$|\Gamma_p(A)| \geq |V_{n-1}(A)| - n + 1$

$\geq \min \{2^{n-1} , |A| + n - 1\} - n + 1$

Nous distinguons 2 cas :

* $2^{n-1} \geq |A| + n - 1$

On a alors

$|\Gamma_p(A)| \geq |A| + n - 1 - n + 1 = |A|$

* $2^{n-1} < |A| + n - 1$

et on a

$|\Gamma_p(A)| = 2^{n-1} - |L_{\bar{p}}^p| = |L_p^p| \geq |A|$

donc, dans tous les cas, $\forall A \subset L_p^p$, $|\Gamma_p(A)| \geq |A|$

et le théorème de Hall s'applique.

III - ETUDE DES PERMUTATIONS DU CUBE C_3

PROPOSITION 2 (*)

Toute permutation de C_3 est décomposable en un produit d'au plus 3 permutations élémentaires, c'est-à-dire $\phi(3) = 3$.

Démonstration

pour i = 1,2,3 notons g_i la fonction définie par

$g_i(x) = x_i \quad \forall x \in \{0,1\}^3$

Soit alors F une bijection de $\{0,1\}^3$

* S'il existe i , $1 \leq i \leq 3$, tel que $\delta(f_i,g_i) \in \{0,1,2\}$

On est alors dans les conditions du théorème 2 donc il existe une permutation élémentaire E telle que

$$[E \circ F(x)]_i = x_i$$

et d'après la proposition 1 on a

$$\ell(F) \leq 1 + \phi(2)$$

or $\phi(2) = 2$ d'où $\ell(F) \leq 3$

* S'il existe i, $1 \leq i \leq 3$, tel que $\delta(f_i,g_i) = 4$ alors $f_i(x) = \bar{x}_i \quad \forall x \in \{0,1\}^3$

Soit E la permutation élémentaire définie par

$$E_k(x) = x_k \quad \text{pour } k \neq i$$

$$E_i(x) = \bar{x}_i$$

Il est clair que $[E \circ F(x)]_i = x_i$

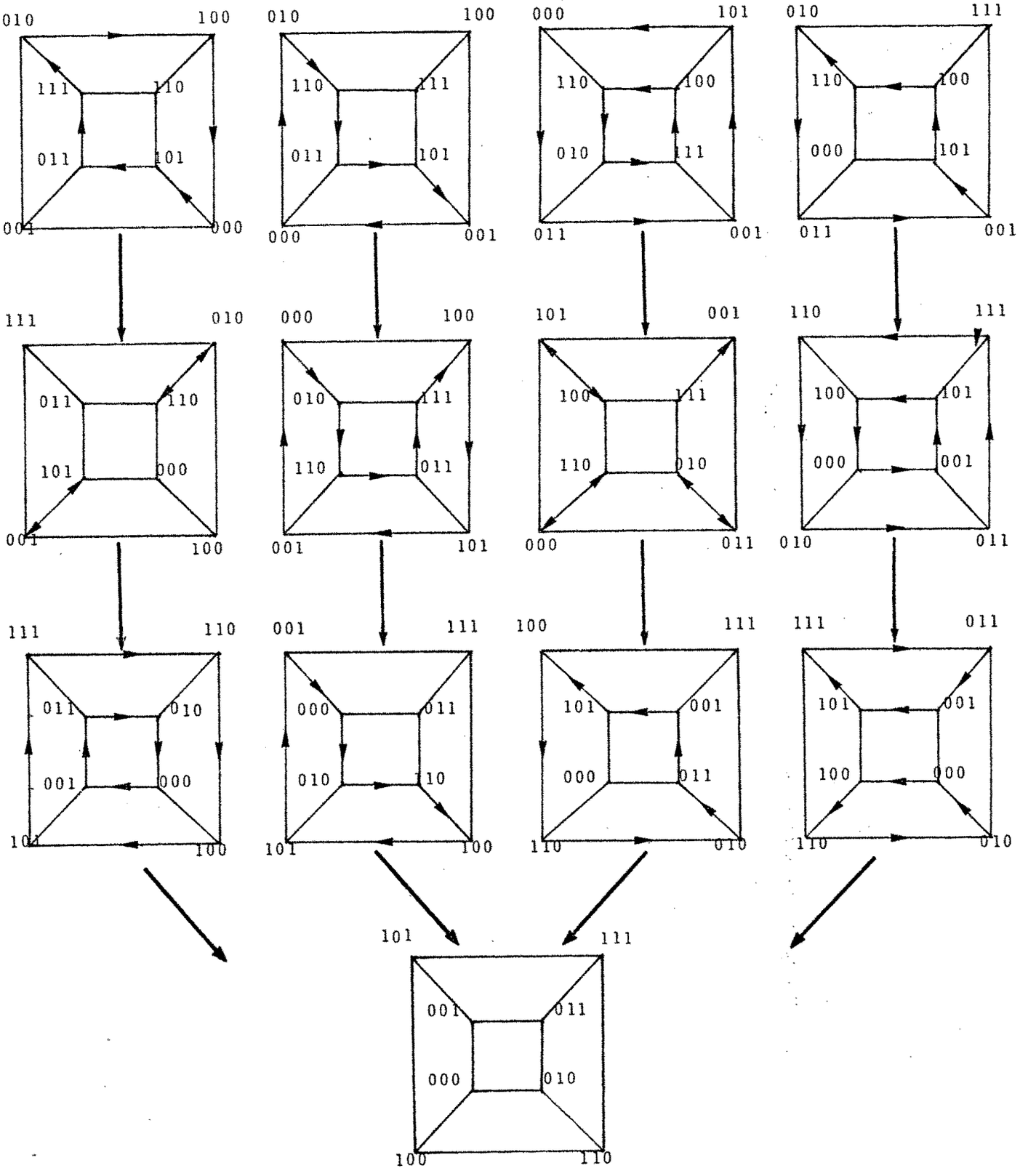
et d'après la proposition 1 on a

$$\ell(F) \leq 3$$

* Si $\forall i \quad 1 \leq i \leq 3$, $\delta(f_i,g_i) = 3$ alors les hypothèses du théorème de Hall ne sont mises en défaut que dans les 4 situations suivantes (aux symétries près) que nous allons traiter séparément :

---

* Ce resultat a été initialement prouvé par M.Tchuenté .


010 100 111 110 011 101 001 000
010 100 110 111 011 101 000 001
000 101 110 100 010 111 011 001
010 111 110 100 000 101 011 001
111 010 011 110 101 000 001 100
000 100 010 111 110 011 001 101
101 001 100 111 110 010 000 011
110 111 100 101 000 001 010 011
111 110 011 010 001 000 101 100
001 111 000 011 010 110 101 100
100 111 101 001 000 011 110 010
111 011 101 001 100 000 110 010
101 111 001 011 000 010 100 110

IV - ETUDE DES PERMUTATIONS DE C_4

Soit F une bijection de $\{0,1\}^4$ dans lui-même, nous allons prouver que $\phi(4) \leq 5$, mais sans pouvoir exhiber un exemple où $\ell(F) = 5$.

Lemme 3

Dans le cube C_3, les hypothèses du théorème de Hall ne sont mises en défaut que dans les deux situations suivantes :

i) $\exists\, \alpha \in L_p^p$, $p = 0,1$ tel que $\Gamma_p(\alpha) = \emptyset$

et dans ce cas on a nécessairement $V_3(\alpha) = L_{\bar{p}}^p$

ii) $|\Gamma_p(L_p^p)| < 4$

et dans ce cas on a nécessairement

L_p^p est de la forme : $\{abc, \bar{a}bc, a\bar{b}c, ab\bar{c}\}$

et $L_{\bar{p}}^p \subset V_3(L_p^p)$

Demonstration

Vérifions d'abord que le théorème de Hall ne peut être mis en défaut pour des parties A de L_p^p de cardinal 2 ou 3.

Si $|A| = 2$ alors $|V_3(A)| \geq 6$

or $|\Gamma_p(A)| \geq |V_3(A)| - |L_{\bar{p}}^p|$

d'où $|\Gamma_p(A)| \geq 2$

Si $|A| = 3$ alors $|V_3(A)| \geq 7$

d'où $|\Gamma_p(A)| \geq 3$

Montrons maintenant qu'on est nécessairement dans les situations i) et ii)

i) soit $\alpha \in L_p^p$ tel que $|\Gamma_p(\alpha)| = 0$

on a $\Gamma_p(\alpha) = V_3(\alpha) - L_{\bar{p}}^p \rightarrow V_3(\alpha) = L_{\bar{p}}^p$

ii) Supposons que $|\Gamma_p(L_p^p)| < 4$

$$\Gamma_p(L_p^p) = V_3(L_p^p) - L_{\bar{p}}^p \text{ et } |V_3(L_p^p)| \geq 7$$

le seul cas qui donne $|\Gamma_p(L_p^p)| < 4$ correspondrait à $|V_3(L_p^p)| = 7$

et cette situation ne peut se produire que si L_p^p est de la forme

$\{abc, \bar{a}bc, a\bar{b}c, ab\bar{c}\}$

de l'égalité $|\Gamma_p(L_p^p)| = |V_3(L_p^p)| - |V_3(L_p^p) \cap L_{\bar{p}}^p|$

on déduit $|V_3(L_p^p) \cap L_{\bar{p}}^p| = 7 - 3 = 4$

d'où $L_{\bar{p}}^p \subset V_3(L_p^p)$

PROPOSITION 3

i) Si F est une permutation de C_4 alors

il existe une permutation élémentaire E et un indice i

$1 \leqslant i \leqslant 4$ tels que

$$[E \circ F(x)]_i = x_1 \quad \text{ou} \quad [E \circ F(x)]_i = \overline{x_1}$$

ii) $\phi(4) \leq 5$

Démonstration

i) Si on suppose qu'on n'a pas l'assertion i), alors, nécessairement

$$\forall i \in \{1,2,3,4\} \quad \delta(f_i, g) = 4$$

où g est définie par $g(x) = x_1$

car sinon on utilise le théorème 2.

Par ailleurs, dire que l'on ne peut pas poser x_1 en f_1 revient à dire que le théorème de Hall est mis en défaut pour $G(L_p^p, C_3, \Gamma_p)$, et d'après le lemme 3 on est nécessairement dans l'une des situations suivantes :

a) $\exists \alpha \in L_p^p \ / \ \Gamma_p(\alpha) = \emptyset$

ou b) $|\Gamma_p(L_p^p)| < 4$

Notons T_p la restriction de la table de F à $x_1 = p$

Dans le cas a) on a nécessairement (à une permutation près des lignes)

$T_p =$

p	α_1	α_2	α_3
p	.	.	.
p	.	.	.
p	.	.	.
$\bar{p}$	α_1	α_2	α_3
$\bar{p}$	$\bar{\alpha}_1$	α_2	α_3
$\bar{p}$	α_1	$\bar{\alpha}_2$	α_3
$\bar{p}$	α_1	α_2	$\bar{\alpha}_3$

Il est facile de voir qu'on ne peut compléter ce tableau de manière à avoir quatre zéros et quatre uns par colonne .

Dans le cas b) on a (d'après le lemme 3)

$T_p =$

p	a	b	c
p	$\bar{a}$	b	c
p	a	$\bar{b}$	c
p	a	b	$\bar{c}$
$\bar{p}$	$L^p_{\bar{p}}$		
$\bar{p}$			
$\bar{p}$			
$\bar{p}$			

et $L^p_{\bar{p}} \subset V_3(L^p_p)$

Pour que dans T_p, chaque colonne contienne 4 zéros et 4 uns alors nécessairement $\bar{a}\ \bar{b}\ \bar{c} \in L^p_{\bar{p}}$ ce qui contredit le fait que $L^p_{\bar{p}} \subset V_3(L^p_p)$.

ii) S'obtient en appliquant la proposition 1.

ANNEXE

ETUDE DU GRAPHE DES CHEMINS POUR DES RESEAUX DE CONTROLE LOGIQUE .

Cette annexe reprend le texte d'un rapport de recherche réalisé en commun avec E.GOLES .

ETUDE DU GRAPHE DES CHEMINS POUR DES RESEAUX DE CONTROLE LOGIQUE

E. GOLES CHACC et M.H. SNOUSSI
Laboratoire de Mathématiques Appliquées
BP 53 X
38041 GRENOBLE FRANCE

Résumé : De récents travaux de R. THOMAS modélisent des phénomènes de contrôle génétique par une représentation booléenne. Ils posent le problème de l'étude du graphe des chemins construit à partir de fonctions booléennes compatibles avec un réseau de contrôle logique. P. VAN HAM et I. LASTERS ont établi des méthodes de réduction permettant de ramener le problème à l'étude de fonctions booléennes du type suivant :

$$F : \{0,1\}^n \to \{0,1\}^n$$

$$f_1(x) = g\ (x_2, \ldots, x_n)$$

$$f_i(x) = x_1, \quad 2 \leq i \leq n$$

Ils ont étudié les fonctions g du type "and" et "or" pour le cas où n=3. Nous généralisons ce travail au cas où n est quelconque et où g est du type "and", "or", "or-exclusif" ou fonction à seuil.

Abstract : Recents research of R. THOMAS modelize genetic control phenomena by means of boolean representation. They pose the problem of studyng the graph constructed from boolean functions which are derived from a logical control network. P. VAN HAM and I. LASTERS established methods reducing the problem to the study of boolean functions of the following type :

$$F : \{0,1\}^n \to \{0,1\}^n$$

$$f_1(x) = g\ (x_2, \ldots, x_n)$$

$$f_i(x) = x_1, \quad 2 \leq i \leq n$$

They present results for functions g of "and" and "or" type in case n = 3. We generalize this work with any n and g of type "and", "or", "exclusive-or" and "threshold".

GRAPHE DES CHEMINS POUR DES RESEAUX DE CONTROLE LOGIQUE

INTRODUCTION :

De récents travaux [1,2] ont modélisé les situations complexes de contrôle génétique à l'aide d'une représentation booléenne. Cette formulation ramène le problème de l'étude du comportement d'un gène, à la construction d'un graphe compatible avec une fonction booléenne.

$$F : \{0,1\}^n \to \{0,1\}^n$$

P. VANHAM et I. LASTERS [3] ont introduit des techniques de réduction permettant de se limiter à l'analyse des séquences temporelles d'états décrites par un système d'équations logiques du type suivant :

$$F : \{0,1\}^n \to \{0,1\}^n$$

$$x = (x_1, \ldots, x_n) \to F(x) = (f_1(x), \ldots, f_n(x))$$

avec $f_1(x)$ ne dépendant pas de x_1 et $f_i(x) = x_1$, $2 \leq i \leq n$

Dans ce travail, nous généralisons les résultats de VAN HAM et LASTERS, établis pour $n = 3$ et f_1 du type "et" et "ou", au cas où n est quelconque et f_1 du type "et", "ou", "ou-exlusif" ou fonction à seuil.

I - DEFINITIONS :

1 - graphe des chemins :

Pour une fonction $F : \{0,1\}^n \to \{0,1\}^n$, on définit le graphe des chemins G_F comme étant le graphe orienté des 2^n états possibles, et un successeur d'un sommet ρ est un sommet ρ' tel que :

$$\text{si } F(\rho) = \rho \text{ alors } \rho' = \rho$$

sinon, ρ' vérifie :

$d(\rho,\rho') = 1$ et $d(F(\rho), \rho') = d(F(\rho),\rho) - 1$

avec $d(x,y) = \sum_{i=1}^{n} |x_i - y_i|$

2 - état stable :

Un sommet ρ de G_F est un état stable si $F(\rho) = \rho$

3 - cycle instable:

C'est un circuit élémentaire de G_F qui contient au moins un sommet ayant un successeur hors du circuit.

4 - jardin d'Eden :

C'est un sommet n'ayant pas d'antécédent.

5 - ensemble attractif d'un état stable :

Soit ρ un état stable de G_F, on définit l'ensemble attractif de ρ, noté A_ρ, par

$\rho \in A_\rho$ et

si un sommet appartient à A_ρ alors tous ses successeurs appartiennent à A_ρ

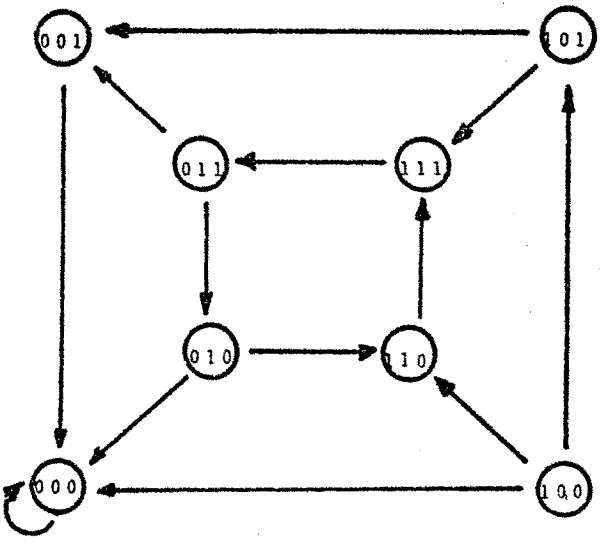
Exemple :

$f_1(x_1,x_2,x_3) = x_2\bar{x}_3$

$f_2(x_1,x_2,x_3) = x_1$

$f_3(x_1,x_2,x_3) = x_1$

x_1	x_2	x_3	f_1	f_2	f_3
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	1	0	0
0	1	1	0	0	0
1	0	0	0	1	1
1	0	1	0	1	1
1	1	0	1	1	1
1	1	1	0	1	1



* l'état (000) est un état stable
* l'ensemble attractif de (000) est {(000),(001)}
* {(011),(010), (110), (111)} est un cycle instable
* (100) est un jardin d'Eden.

Notation :

soient $x = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ et $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \{0,1\}^n$

on pose $x^{\alpha} = (x_1^{\alpha_1}, \ldots x_n^{\alpha_n})$

avec $x_i^{\alpha_i} = \begin{cases} x_i & \text{si } \alpha_i = 1 \\ \bar{x}_i & \text{si } \alpha_i = 0 \end{cases}$

II - ETUDE DES FONCTIONS DE "TYPE PRODUIT" :

Une fonction de type produit est définie de la manière suivante :

$$F_\P : \{0,1\}^n \to \{0,1\}^n$$

$$(x_1,x_2,\ldots,x_n) \to (f_1(x), x_1,\ldots,x_1)$$

avec $f_1(x) = x_2^{\alpha_2}\ldots x_n^{\alpha_n}$.

$\alpha = (\alpha_2,\ldots,\alpha_n) \in \{0,1\}^{n-1}$ étant fixé, une telle fonction possède les propriétés élémentaires suivantes :

a - $F_\P\ (1,\alpha_2,\ldots,\alpha_n) = (1,1,\ldots,1)$

b - $F_\P\ (0,\alpha_2,\ldots,\alpha_n) = (1,0,\ldots,0)$

c - $F_\P\ (1,x_2,\ldots,x_n) = (0,1,\ldots,1)$ si $(x_2,\ldots,x_n) \neq \alpha$

d - $F_\P\ (0,x_2,\ldots,x_n) = (0,0,\ldots,0)$ si $(x_2,\ldots,x_n) \neq \alpha$

e - si $\alpha = (1,1,\ldots,1) \in \{0,1\}^{n-1}$, alors $(0,0,\ldots,0)$ et $(1,1,\ldots,1)$ sont les uniques points fixes de $F_\P$

f - si $\alpha = (0,0,\ldots,0) \in \{0,1\}^{n-1}$, alors $F_\P$ n'a pas de point fixe

g - si $\alpha \neq (1,1,\ldots,1)$ et $\alpha \neq (0,0,\ldots,0)$, alors $(0,0,\ldots,0)$ est l'unique point fixe de $F_\P$

Pour la construction du graphe des chemins $G_\P$, nous utiliserons la notation condensée suivante :

$$X_k^\varepsilon = \{x \in \{0,1\}^n \ ; \ x_1 = \varepsilon, \sum_{i=2}^{n} x_i = k \text{ et } (x_2,\ldots,x_n) \neq (\alpha_2,\ldots,\alpha_n)\}$$

Théorème :

Le graphe des chemins $G_\P$, associé à $F_\P$, possède les propriétés suivantes :

1) Si $\alpha \neq (0,0,\ldots,0)$ et $\alpha \neq (1,1,\ldots,1)$

* l'état $(0,0,\ldots,0)$ est l'unique état stable et son domaine d'attraction est l'ensemble $\bigcup_{i=1}^{p} X_i^0$ où $p = \sum_{i=2}^{n} \alpha_i$

* $G_\P$ possède des cycles instables de longueur $2k$ pour $k = 2,3,\ldots,(n-p)$

*$(1,0,\ldots,0)$ est un jardin d'Eden

2) si $\alpha = (0,0,\ldots,0)$

* $G_{\P}$ n'a pas d'état stable

* $G_{\P}$ possède des cycles instables de longueur $2k$, $k = 2,3,\ldots,n$

3) si $\alpha = (1,1,\ldots,1)$

* $(0,0,\ldots,0)$ et $(1,1,\ldots,1)$ sont les uniques états stables de $G_{\P}$
* le domaine d'attraction de $(0,0,\ldots,0)$ est $\bigcup_{i=1}^{n-2} X_i^0$
* le domaine d'attraction de $(1,1,\ldots,1)$ est vide
* $G_{\P}$ n'admet pas de cycles
* $(0,1,1,\ldots,1)$ et $(1,0,\ldots,0)$ sont des jardins d'Eden

Démonstration :

Tous les résultats énoncés se déduisent directement de la construction du graphe $G_{\P}$

1er cas : $\alpha \neq (0,0,\ldots,0)$ et $\alpha \neq (1,1,\ldots,1)$, posons $p = \sum_{i=2}^{n} \alpha_i$

* soit $x \in X_k^0$, $k \neq 0$, alors $F_{\P}(x) = (0,0,\ldots,0)$

  Un suivant ξ de x est tel que $\xi_1 = 0$ et une composante de x non nulle et une seule prend la valeur 0, donc $\xi \in X_{k-1}^0$

  Dans le cas où $k = 0$ i.e $x = (0,0,\ldots,0)$ alors x est un état stable

* soit maintenant $x \in X_k^1$ alors $F_{\P}(x) = (0,1,\ldots,1)$

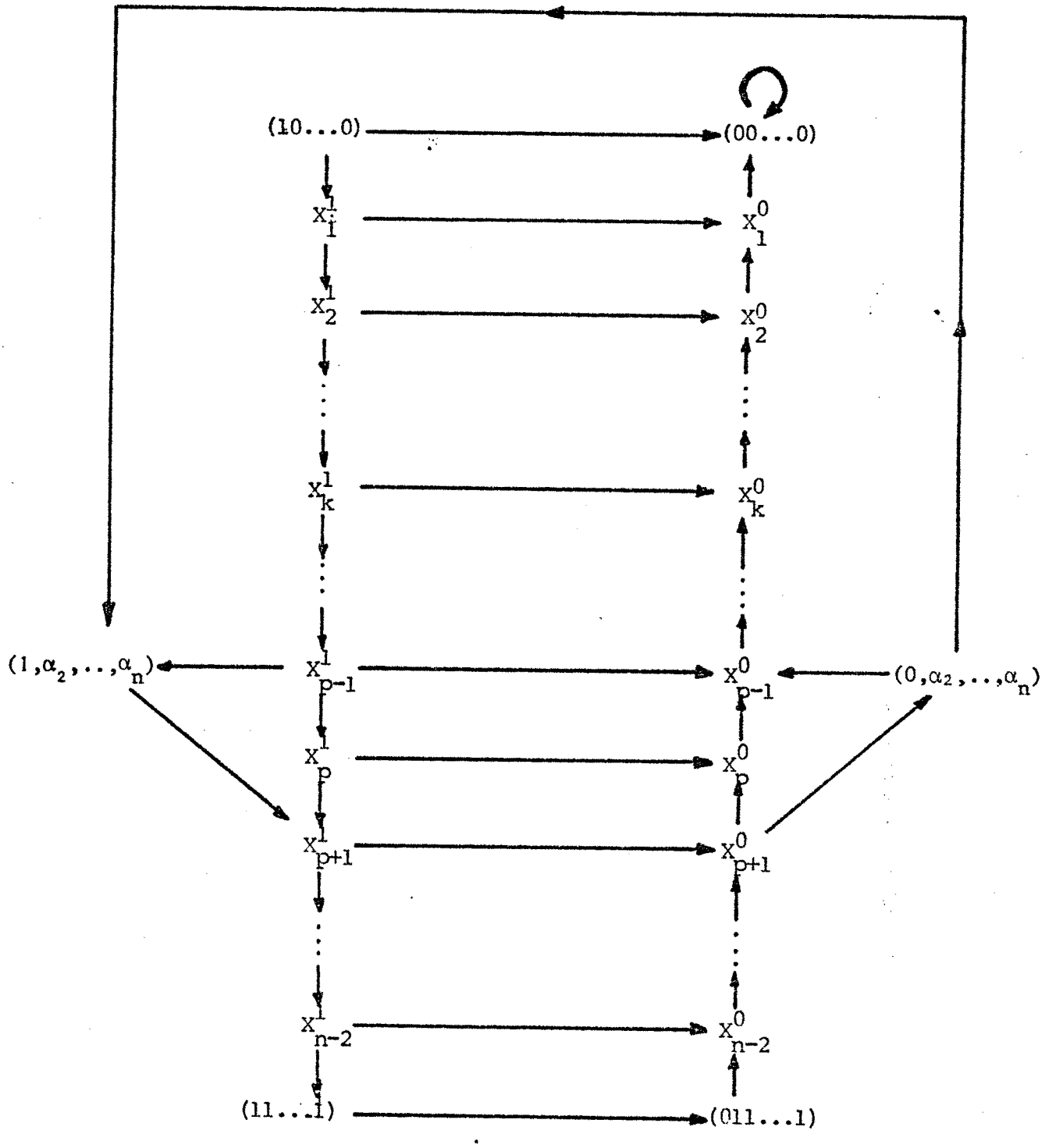
  si $k \neq n-1$, x possède, dans $G_{\P}$, deux types de successeur l'un appartenant à X_k^0 l'autre à X_{k+1}^1

  si $k = n-1$, i.e $x = (1,1,\ldots,1)$, x possède un seul successeur $(0,1,\ldots,1)$

* si $x = (0,\alpha_2,\ldots,\alpha_n)$ alors $F_{\P}(x) = (1,0,\ldots,0)$ et x possède deux successeurs, $(1,\alpha_2,\ldots,\alpha_n)$, ou bien un élément de X_{p-1}^0

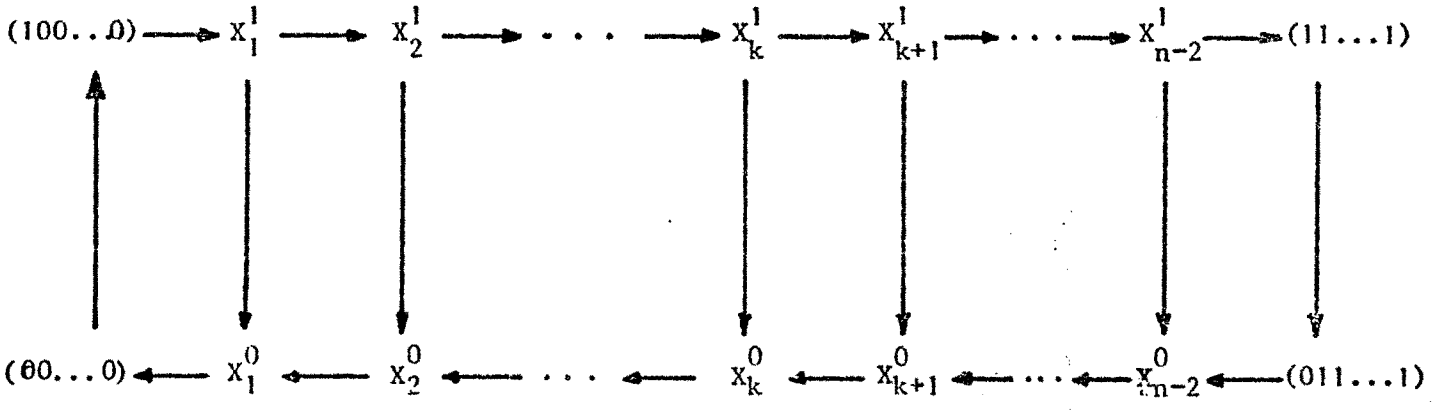
* si $x = (1,\alpha_2,\ldots,\alpha_n)$ alors $F_{\P}(x) = (1,1,\ldots,1)$
  et un successeur ξ de x est tel que une composante nulle (et une seule) de α prenne la valeur 1, c'est-à-dire que $\xi \in X_{p+1}^1$; d'où le graphe des chemins :

1er cas : $\alpha \neq (0,\ldots,0)$ et $\alpha \neq (1,\ldots,1)$



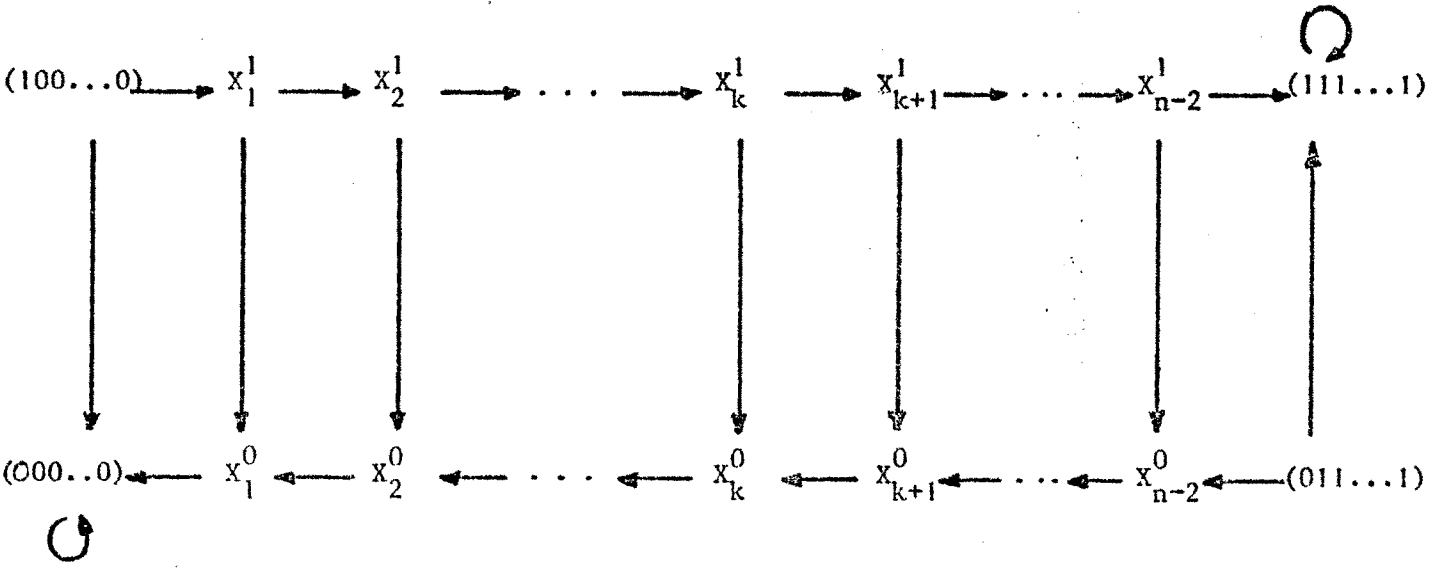
2e cas : $\alpha = (0,0,\ldots,0)$

On obtient le graphe suivant :



3e cas : $\alpha = (1,1,\ldots,1)$

On obtient le graphe suivant :



III - ETUDE DES FONCTIONS DE "TYPE SOMME" :

Soit $F_\Sigma : \{0,1\}^n \to \{0,1\}^n$

$$(x_1, x_2, \ldots, x_n) \to (f_1(x), x_1, \ldots, x_1)$$

où $f_1(x) = \sum_{i=2}^{n} x_i^{\alpha_i}$ (Σ : somme booléenne).

La construction de G_Σ, associé à F_Σ, se déduit de $G_\P$ associé à $F_\P$, d'après la proposition suivante :

Proposition :

Les graphes $G_\P$ et G_Σ se déduisent l'un de l'autre par l'isomorphisme :

$$x \to \bar{x} .$$

Démonstration :

Il suffit de montrer que si x est un successeur de y sur $G_\P$ alors $\bar{x}$ est un successeur de $\bar{y}$ sur G_Σ et réciproquement.

Posons :

$\Gamma_x^\P$ l'ensemble des successeurs de x dans $G_\P$

et Γ_x^Σ l'ensemble des successeurs de x dans G_Σ

Notons d'abord que y est un état stable pour $G_\P$ si et seulement si $\bar{y}$ est un état stable pour G_Σ. Il suffit de remarquer que :

$$\forall x \in \{0,1\}^n : F_\Sigma \bar{x} = \overline{F_\P x} .$$

Soit x un état non stable de $G_\P$ (et de G_Σ)

alors $y \in \Gamma_x^\P \iff d(x,y) = 1$ et $d(F_\P x, y) = d(F_\P x, x) - 1$

$\iff d(\bar{x},\bar{y}) = 1$ et $d(\overline{F_\P x}, \bar{y}) = d(\overline{F_\P x}, \bar{x}) - 1$

$\iff d(\bar{x},\bar{y}) = 1$ et $d(F_\Sigma \bar{x}, \bar{y}) = d(F_\Sigma \bar{x}, \bar{x}) - 1$

$\iff \bar{y} \in \Gamma_{\bar{x}}^\Sigma$.

Le théorème 1 nous permet alors d'affirmer les propriétés suivantes du graphe G_Σ :

1) Si $\alpha \neq (0,0,\ldots,0)$ et $\alpha \neq (1,1,\ldots,1)$

* l'état $(1,1,\ldots,1)$ est l'unique état stable et son domaine d'attraction est l'ensemble $\bigcup_{i=2}^{p+1} X_{n-i}^{1}$ où $p = \sum_{j=2}^{n} \alpha_j$

* G_Σ possède des cycles instables de longueur $2k$, $k = 2,3,\ldots,(n-p)$

* $(0,1,1,\ldots,1)$ est un jardin d'Eden

2) Si $\alpha = (0,0,\ldots,0)$

* G_Σ n'a pas d'état stable

* G_Σ possède des cycles instables de longueur $2k$ $k = 2,3,\ldots,n$

3) Si $\alpha = (1,1,\ldots,1)$

* $(0,0,\ldots,0)$ et $(1,1,\ldots,1)$ sont les uniques états stables de G_Σ

* le domaine d'attraction de $(0,0,\ldots,0)$ est vide et celui de $(1,1,\ldots,1)$ est l'ensemble $\bigcup_{i=1}^{n-2} X_i^1$

* G_Σ n'a pas de cycle

* $(0,1,1,\ldots,1)$ et $(1,0,\ldots,0)$ sont des jardins d'Eden.

IV - ETUDE DES FONCTIONS DE "TYPE OU-EXCLUSIF" :

Soit

$$F_{\oplus} : \{0,1\}^n \to \{0,1\}^n$$

$$(x_1,\ldots,x_n) \to (f_1(x), x_1, x_1, \ldots, x_1)$$

avec $f_1(x) = \bigoplus_{i=2}^{n} x_i^{\alpha_i}$

$\alpha = (\alpha_2,\ldots,\alpha_n) \in \{0,1\}^{n-1}$

$\oplus$: somme dans le corps $Z/2Z$

Une telle fonction peut s'écrire sous la forme :

$$F_{\oplus}(x) = A\,x \oplus b$$

avec

$$A = \begin{bmatrix} 0 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \\ \vdots & & & & \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}$$ matrice (nxn) à éléments dans $Z/_{2Z}$

$$b = \begin{bmatrix} \varepsilon \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \{0,1\}^n$$

et $\varepsilon = \begin{cases} 1 & \text{si} \quad |\bar{\alpha}| = \sum_{i=2}^{n} \bar{\alpha}_i \text{ est impair} \\ 0 & \text{sinon} \end{cases}$

Remarque : Il est clair que l'analyse du graphe des chemins $G_{\oplus}$ dépend de la parité de $|\bar{\alpha}|$ et de n. -

La fonction $F_\oplus$ ainsi définie possède les propriétés élémentaires suivantes :

* Si $|\bar{\alpha}|$ est pair et n pair alors (0,0,...,0) et (1,1,...,1) sont les uniques états stables de $G_\oplus$,
* Si $|\bar{\alpha}|$ pair et n impair alors (0,0,...,0) est l'unique état stable de $G_\oplus$,
* Si $|\bar{\alpha}|$ impair et n impair alors (1,1,...,1) est l'unique état stable de $G_\oplus$,
* Si $|\bar{\alpha}|$ impair et n pair alors $G_\oplus$ n'a pas d'état stable.

Construction des graphes des chemins.

Nous considérons, comme précedemment, les ensembles :

$$X_k^\epsilon = \{ x \in \{0,1\}^n \ ; \ x_1 = \epsilon \text{ et } \sum_{i=2}^{n} x_i = k \}$$

La construction des graphes repose sur le principe suivant :
supposons que $|\bar{\alpha}|$ est pair et n est pair et soit $x \in X_k^0$ par exemple .

On a alors : $F_\oplus(x) = (f_1(x) , 0,0,...,0)$

$$\text{avec } f_1(x) = \begin{cases} 1 \text{ si k est impair} \\ 0 \text{ sinon} \end{cases}$$

Donc si k est pair, un successeur ξ de x s'obtient en changeant une composante non nulle de x (et une seule) par 0 ; i.e $\xi \in X_{k-1}^0$

Si k est impair, $F_\oplus(x) = (1,0,...,0)$, et x admet deux types de successeurs ξ et ζ : ξ s'obtient en changeant seulement $x_1 = 0$ par $x_1 = 1$ i.e $\xi \in X_k^1$

et ζ s'obtient en changeant une composante non nulle de x par 0 i.e $\zeta \in X_{k-1}^0$

Un raisonnement analogue permet de construire le graphe des chemins et établir le théorème suivant :

Théorème :

Le graphe des chemins $G_\oplus$, associé à la fonction $F_\oplus$ possède les propriétés suivantes :

1) si $|\bar{\alpha}|$ est pair et n pair

* $(0,0,\ldots,0)$ et $(1,1,\ldots 1)$ sont les uniques états stables de $G_{\oplus}$ et leur domaine d'attraction est vide,

* $(0,1,1,\ldots,1)$ et $(1,0,0,\ldots,0)$ sont des jardins d'Eden,

* $G_{\oplus}$ possède des cycles instables de longueur $2k$, $k = 2,4,6,\ldots,n-2$,

2) si $|\bar{\alpha}|$ est pair et n impair

* $(0,0,\ldots,0)$ est l'unique état stable de $G_{\oplus}$, et son domaine d'attraction est vide,

* $(1,0,\ldots,0)$ est un jardin d'Eden,

* $G_{\oplus}$ admet des cycles instables de longueur $2k$, $k = 2,4,6,\ldots,n-1$

3) si $|\bar{\alpha}|$ est impair et n impair

* $(1,1,\ldots,1)$ est l'unique état stable de $G_{\oplus}$, et son domaine d'attraction est vide,

* $(0,1,1,\ldots,1)$ est un jardin d'Eden,

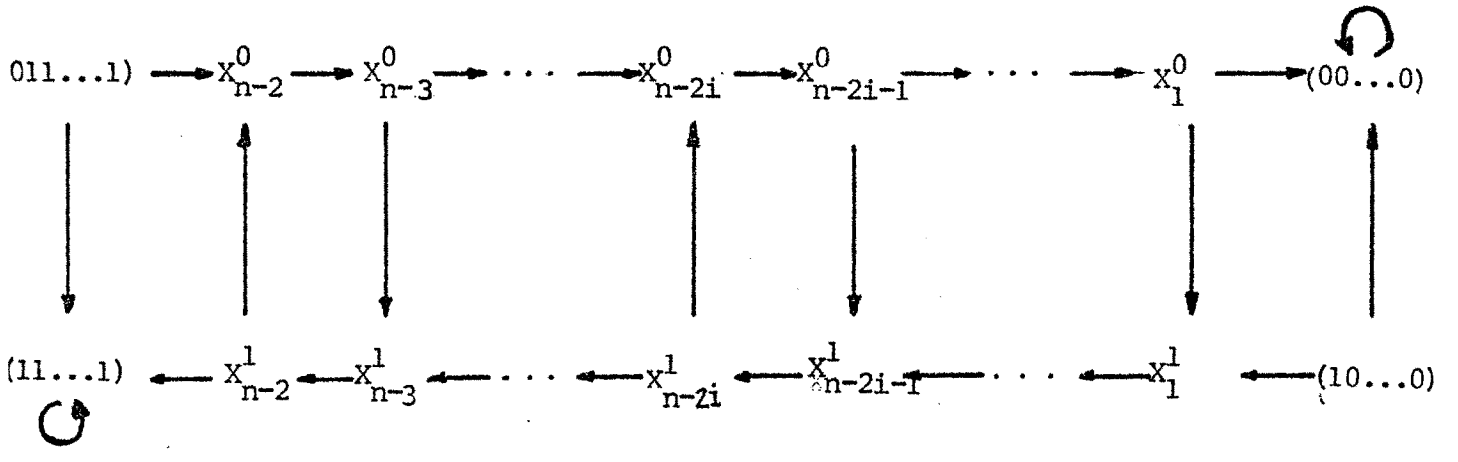
* $G_{\oplus}$ admet des cycles instables de longueur $2k$, $k = 2,4,6,\ldots,n-1$

4) si $|\bar{\alpha}|$ est impair et n pair

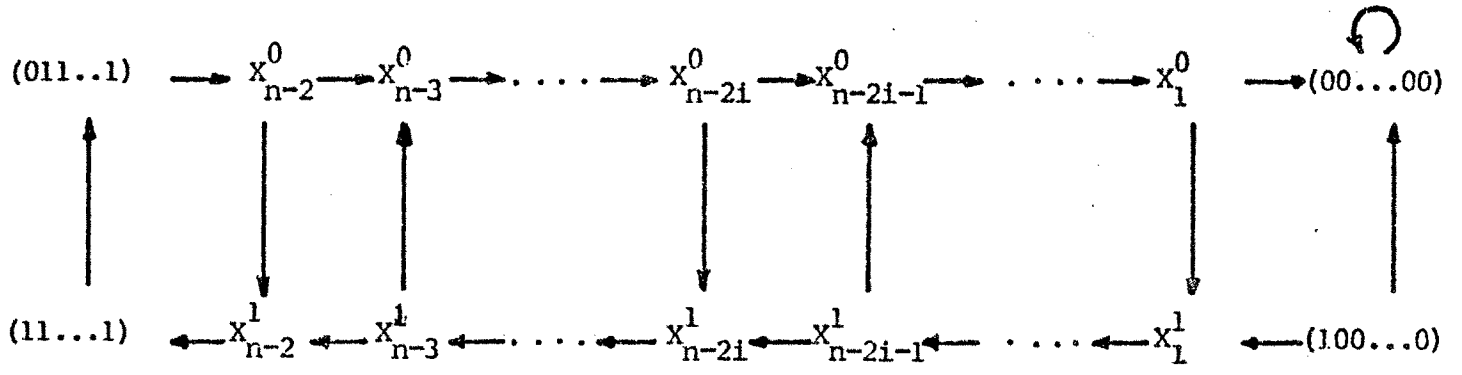
* il n'y a pas d'état stable ni de jardin d'Eden,

* $G_{\oplus}$ admet des cycles instables de longueur $2k$, $k = 2,4,\ldots,n$.

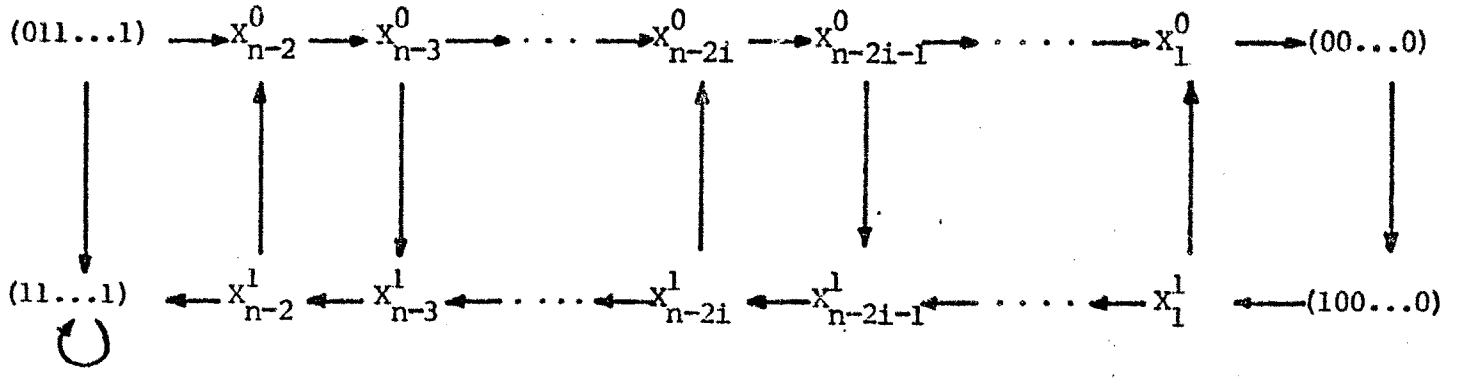
Graphe des chemins pour $|\bar{\alpha}|$ pair et n pair :



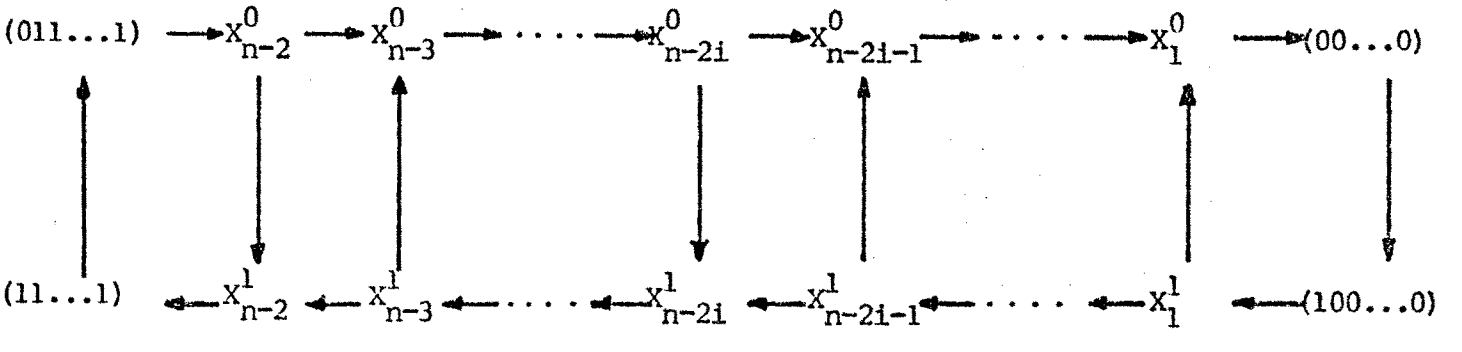
Graphe des chemins pour $|\bar{\alpha}|$ pair et n impair :



Graphe des chemins pour $|\bar{\alpha}|$ impair et n impair :



Graphe des chemins pour $|\bar{\alpha}|$ impair et n pair :



V - ETUDE DES FONCTIONS DE TYPE "SYMETRIQUES ELEMENTAIRES"

Soit $k \in \{0,1,\ldots,n-1\}$, considérons la fonction

$$F_k : \{0,1\}^n \to \{0,1\}^n$$

$$(x_1,\ldots,x_n) \to (f_1(x) , x_1,\ldots,x_1)$$

avec $f_1(x) = \begin{cases} 1 & \text{si } \sum_{i=2}^{n} x_i = k \\ 0 & \text{sinon} \end{cases}$

La fonction F_k ainsi définie vérifie les propriétés élémentaires suivantes :

* $F_k\ (1,x_2,\ldots,x_n) = (1,1,\ldots,1)$ si $\sum_{i=2}^{n} x_i = k$

* $F_k\ (0,x_2,\ldots,x_n) = (1,0,\ldots,0)$ si $\sum_{i=2}^{n} x_i = k$

* $F_k\ (1,x_2,\ldots,x_n) = (0,1,\ldots,1)$ si $\sum_{i=2}^{n} x_i \neq k$

* $F_k(0, x_2,\ldots,x_n) = (0,0,\ldots,0)$ si $\sum_{i=2}^{n} x_i \neq k$

* F_0 n'a pas d'état stable

* F_{n-1} admet $(0,0,\ldots,0)$ et $(1,1,\ldots,1)$ comme uniques états stables

* Si $k \in \{1,\ldots,n-2\}$, F_k admet $(0,0,\ldots,0)$ comme unique état stable.

Pour la construction du graphe des chemins G_k, associé à F_k, nous utilisons la notation :

$$X_k^{\varepsilon} = \{x \in \{0,1\}^n \ , \ x_1 = \varepsilon \text{ et } \sum_{i=2}^{n} x_i = k\} \ , \varepsilon \in \{0,1\}$$

L'analyse du graphe G_k permet d'établir le théorème suivant :

Théorème :

Le graphe des chemins G_k , associé à la fonction F_k , possède les propriétés suivantes :

1) Si $k = 0$

* G_k n'a pas d'état stable,

* G_k admet des cycles instables de longueur $2k$, $k = 2,3,\ldots,n$.

2) Si $k = n-1$

* G_k admet $(0,0,\ldots,0)$ et $(1,1,\ldots,1)$ comme uniques états stables

* le domaine d'attraction de $(0,0,\ldots,0)$ est l'ensemble $\bigcup_{i=1}^{n-2} X_i^0$ et celui de $(1,1,\ldots,1)$ est vide

* G_k n'admet aucun cycle

3) Si $k \in \{1,\ldots,n-2\}$

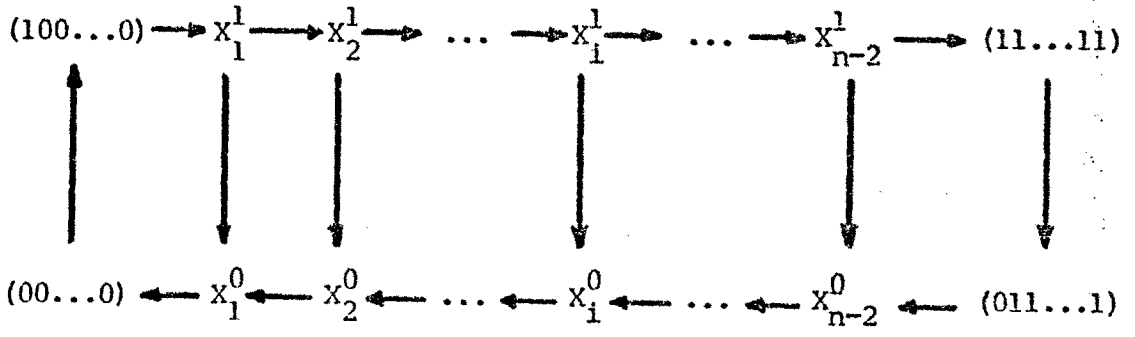
* $(0,0,\ldots,0)$ est l'unique état stable de G_k et son domaine d'attraction est $\bigcup_{i=1}^{k-1} X_i^0$

* G_k admet des cycles instables de longueur $2k'$, $k' = 2,3,\ldots,n-k$.

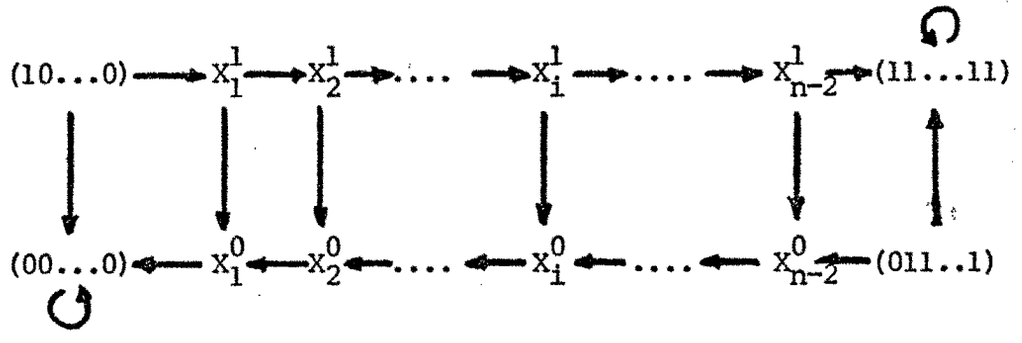
* l'état $(1,0,\ldots,0)$ est un jardin d'Eden

La démonstration est immédiate à partir de la construction des graphes G_k

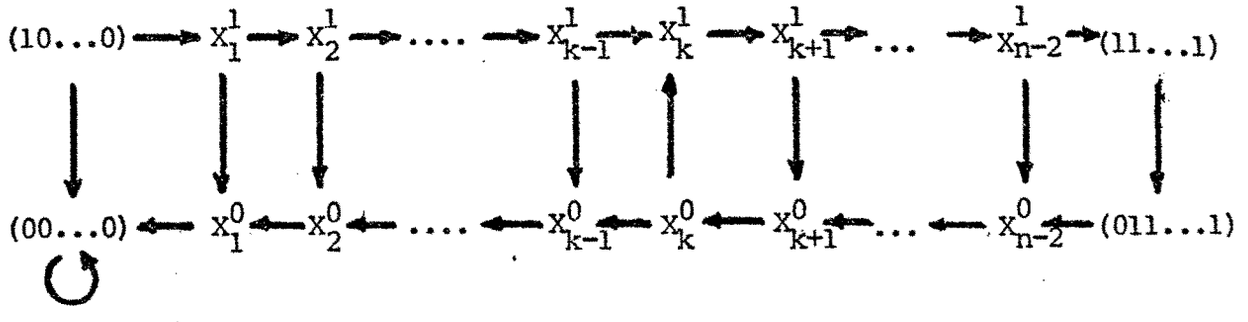
Graphe des chemins pour $k = 0$



Graphe des chemins pour k = n-1



Graphe des chemins pour k $\epsilon\{1,2,\ldots,n-2\}$



VI - ETUDE DES FONCTIONS DE "TYPE SEUIL"

Considérons la fonction F_s définie par :

$$F_s : \{0,1\}^n \to \{0,1\}^n$$

$$(x_1,\ldots,x_n) \mapsto (f_1(x), x_1,\ldots,x_1)$$

avec $f_1(x) = \begin{cases} 1 & \text{si } \sum_{i=2}^{n} x_i \geq k \quad , k\epsilon\{1,\ldots,n-1\} \\ 0 & \text{sinon} \end{cases}$

La fonction F_s ainsi définie possède les propriétés élémentaires suivantes :

* $F_s(1,x_2,\ldots,x_n) = \begin{cases} (11\ldots1) \text{ si } \sum_{i=2}^{n} x_i \geq k \\ (01\ldots1) \text{ sinon} \end{cases}$

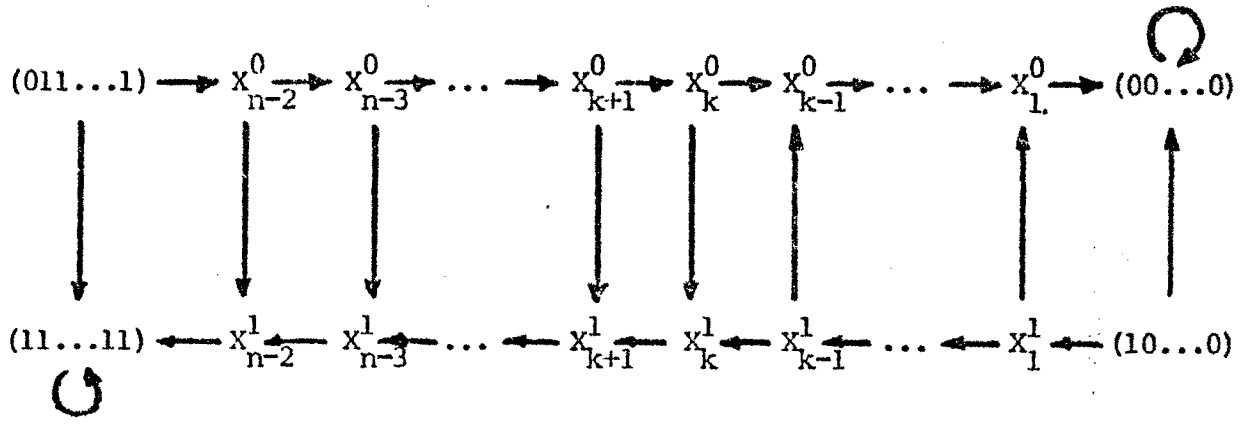
* $F_s(0,x_2,\ldots,x_n) = \begin{cases} (100..0) \text{ si } \sum_{i=2}^{n} x_i \geq k \\ (00\ldots0) \text{ sinon} \end{cases}$

* (00...0) et (11...1) sont les uniques états stables.

Posons

$$X_p^{\epsilon} = \{x \in \{0,1\}^n \ , \ x_1 = \epsilon \text{ et } \sum_{i=2}^{n} x_i = p\}, \ \epsilon \in \{0,1\}$$

Construction du graphe des chemins G_s , associé à F_s :



Théorème :

Le graphe des chemins G_s associé à F_s possède les propriétés suivantes :

* G_s admet (0,0,...,0) et (1,1,...,1) comme uniques états stables
* Le domaine d'attraction de (000...0) est $\bigcup_{i=1}^{k-1} X_i^0$
  et celui de (1,1,...,1) est $\bigcup_{i=k}^{n-2} X_i^1$
* G_s n'admet pas de cycle
* (011...1) et (100...0) sont des jardins d'Eden

TABLEAU RECAPITULATIF

TYPE DE FONCTION		ETATS STABLES	DOMAINE D'ATTRACTION	JARDINS D'EDEN	LONGUEUR DES CYCLES INSTABLES
$F_{\P}$	$\alpha \neq \vec{0}, \vec{1}$	$\vec{0}$	$\bigcup_{i=1}^{p} X_i^0$, $\lvert\alpha\rvert = p$	(100...0)	4,6,8,...2(n-p)
	$\alpha = \vec{0}$	$\emptyset$	$\emptyset$	$\emptyset$	4,6,8,...,2n
	$\alpha = \vec{1}$	$\vec{0}$ $\vec{1}$	$\bigcup_{i=1}^{n-2} X_i^0$ $\emptyset$	(011...1) (100...0)	
F_{Σ}	$\alpha \neq \vec{0}, \vec{1}$	$\vec{1}$	$\bigcup_{i=2}^{p+1} X_{n-i}^1$, $\lvert\alpha\rvert = p$	(011...1)	4,6,8,...,2(n-p)
	$\alpha = \vec{0}$	$\emptyset$	$\emptyset$	$\emptyset$	4,6,8,...,2n
	$\alpha = \vec{1}$	$\vec{0}$ $\vec{1}$	$\emptyset$ $\bigcup_{i=1}^{n-2} X_i^1$	(011...1) (100...0)	
F_s		$\vec{0}$ $\vec{1}$	$\bigcup_{i=1}^{k-1} X_i^0$ $\bigcup_{i=k}^{n-2} X_i^1$	(011...1) (100...0)	
F_k	$k = 0$	$\emptyset$	$\emptyset$	$\emptyset$	4,6,8,...,2n
	$k = n-1$	$\vec{0}$ $\vec{1}$	$\bigcup_{i=1}^{n-2} X_i^0$ $\emptyset$	(10...0) (01...1)	
	$k \in \{1,...,n-2\}$	$\vec{0}$	$\bigcup_{i=1}^{k-1} X_i^0$	(100...0)	4,6,8,...,2(n-k)
F_{Θ}	$\lvert\bar{\alpha}\rvert$ pair n pair	$\vec{0}$ $\vec{1}$	$\emptyset$	(01...1) (10...0)	4,8,12,...,2n-4
	$\lvert\bar{\alpha}\rvert$ pair n impair	$\vec{C}$	$\emptyset$	(1000...0)	4,8,12,...,2n-2
	$\lvert\bar{\alpha}\rvert$ impair n impair	$\vec{1}$	$\emptyset$	(011...1)	4,8,12,...,2n-2
	$\lvert\bar{\alpha}\rvert$ impair n pair	$\emptyset$	$\emptyset$	$\emptyset$	4,8,12,...,2n

BIBLIOGRAPHIE

(1) THOMAS R. "Boolean formalization of genetic control circuits"
J. Theor. Biol. (1973) 42, 563

(2) THOMAS R. "Logical Analysis of systems comprising feedback loops"
J. Theor. Biol. (1978) 73, 631-656

(3) P. VAN HAM and I. LASTERS "Reduction Methods for logical control networks"
J. Theor. Biol. (1978) 72, 269-281

BIBLIOGRAPHIE

[1] S. AMARI
Homogeneous Nets of Neuron-Like elements
Bid. Cybernet., vol. 17, (1975)

[2] T.C. BARTEE and D.I. SCHNEIDER
Computation with finite fields
Inform. Contr ., vol. 6, pp. 79-98 (June 1963)

[3] V.E. BENES
Mathematical Theory of Connecting Networks and Telephone Trafic
Academic Press New-York and London (1965)

[4] B. BENJAUTHRIT and I.S. REED
Galois Switching functions and their applications.
IEEE Trans. Comput., vol. C.25, pp. 79-86 (Jan. 1976)

[5] C. BERGE
Graphes et hypergraphes
Paris Dunod (1970)

[6] C. BERGE
Principes de combinatoire
Dunod Paris, 1968)

[7] B. CHRISTENSEN
Galois Switching Circuits
in 1974 Int. Symp. on Multivalued Logic, Mai 29-31, 1974,
Morgantown, W.V.

[8] J.P. DESCHAMPS and A. THAYSE
Applications of Discrete Functions. Part I.
Philips Res. Repts 28, 497-529 (1973)

[9] A. EBERHARD, F. ROBERT, E.H. SNOUSSI et M. TCHUENTE
Factorisation de permutations sur le cube
R.R. n° 194, IMAG (Grenoble) Février 1980

[10] G. EPSTEIN, G. FRIEDER and D. RINE
A Survey of the Development of Multiple Valued Logic as Related to Computer Science
in 1974 International Symp. Multiple-Valued Logic, May 29-31, 1974, pp. 303-314

[11] S. EYEN, I. KOHAVI and A. PAZ
On minimal Modulo 2 Sums of Products for Switching Functions
IEEE Trans. Comput. Vol. C-16, pp. 671-674 (october 1967)

[12] L.T. FISHER
Unateness Properties of AND-EXLUSIVE-OR Logic Circuits
IEEE Trans. Comput. vol. 23, pp. 93-97 (Feb. 1974)

[13] A. GILL
Linear Sequential Circuits, Analysis, Synthesis and Applications
Mc Graw Hill, Series in Systemes Science (1966)

[14] L. GLASS and J.S. PASTERNACK
Prediction of Limit Cycles in Mathematical Models of Biological Oscillations
Bull. Math. Biol. Vol. 40, pp. 28-44 (1978)

[15] E. GOLES
Etude du comportement des itérations sur les fonctions booléennes linéaires et de type produit.
R.R. n° 157 IMAG (février 1979)

[16] E. GOLES et J. OLIVOS
Periodic Behaviour of Generalized Threshold Functions
(Communication) Discret Math. 30 (1980), pp. 187-189

[17] M. HARAO and S. NOGUCHI
On some Dynamical Properties of Finite Cellular Automaton
IEEE Trans. Comput. Vol. C-27, n° 1, pp. 12-22 (January 1973)

[18] J.B. KAN and G.I. DAVIDA
Structured Design of Substitution Permutation Encryption Networks
IEEE Trans. Compt. Vol. C-28, n° 10, pp. 747-753 (october 1979)

[19] S. KAUFMANN
Behaviour of Randomly Constructed genetic Nets Binary elements Net:
University of Cincinnati.

[20] K.L. KODANDAPANI and R.V. SETULAR
Reed-Muller Canonical forms in Multivalued Logic
IEEE Trans. Comput. Vol. C-24, pp. 628-638 (June 1975)

[21] S.C. LEE and E.T. LEE
On Multivalued Symetric Functions
IEEE Trans. Comput. Vol. 16, pp. 312-317,(march 1972)

[22] S. LIN and G. MARKOWSKY
On a Class of One-Step Majority-Logic Decodable Cyclic Codes
IBM J.RES. Develop. Vol. 24, n° 1, (January 1980)

[23] S.B. MARINKOVIC and Z. TOSCI
Algorithme for Minimal Polarized Polynomial form Determination
IEEE Trans. Comput. vol. C-23, pp. 1313-1315, (December 1974)

[24] R.V. MOODY and I.G. ROSENBERG
Cycle Structure of Affine Transformation of Vector Spaces Over GF(p).
Preprint CRM-863 Montreal (March 1979).

[25] C. MOSER
Communication personnelle

[26] A. MUKHOPADHAYAY and G. SCHMITZ
Minimization of EXLUSIVE-OR and Logical Equivalence Switching Circuits.
IEE E Trans. Comput. Vol. C-19, pp. 132-140 (Feb. 1970)

[27] A. M. PATEL
Error Recovery Scheme for the IBM 3850 Mass Storage System.
IBM J. RES. DEVELOP. Vol. 24, n° 1 (Jan. 1980)

[28] W.H. PAYNE and K.L. Mc MILLEN
Orderly Enumeration of Nonsingular Binary Matrices Applied to Text Encryption.
Comm. ACM, vol. 21, n° 4, pp. 259-263 (April 1978)

[29] D. PRADHAN
A Theory of Galois Switching Functions
IEEE Trans. Comput. Vol. C-27, n0 3, pp. 239-248 (March 1978)

[30] C.V. RAMAMOORTHY
Procedure for Minimization of EXCLUSIVE-OR and LOGICAL-EQUIVALENCE Switching Circuits.
In 1965 IEEE Symp. Switching Theory and Logic Design (Ann. Arbor, Mich., oct. 6-8) pp. 143-149

[31] S.M. REDDY
Easily Testable Realizations for Logic Functions
IEEE Trans. Comput. Vol. C-21, pp. 1183-1188 (nov. 1972)

[32] F. ROBERT
Comparaison des modes operatoires d'un automate cellulaire fini.
R.R. n° 31, IMAG (février 1976) (soumis à Discrete Appl. Math.)

[33] F. ROBERT
Théorèmes de Perron-Frobenius et Stein-Rosenberg Booleens.
Linear Algebra and its App. (19), pp. 237-250 (1978).

[34] F. ROBERT
Itérations sur des ensembles finis et automates cellulaires contractants.
A paraître dans Linear Algebra and its Appl.

[35] E.H. SNOUSSI
Factorisation des permutations de l'hypercube en permutations élémentaires.
Séminaire d'Analyse Numérique, Grenoble, février 1980

[36] E.H. SNOUSSI
Représentation matricielle de polynômes sur Z_p/Z et forme canonique minimale d'une fonction booléenne.
Séminaire d'Analyse Numérique Grenoble, n° 316 avril 1979.

[37] E.H. SNOUSSI et E. GOLES
Etude du graphe des chemins pour des réseaux de controle logique.
R.R. n° 162 IMAG (Grenoble) Avril 1979.

[38] H.S. STONE
Discrete Mathematical Structures and their Applications
SRA Computer Science Series (1973)

[39. S. SWAMY
On generalized Reed-Muller Expansions
IEEE Trans. Comput. Vol. C-21, pp. 1008-1009 (sept. 1972)

[40] M. TCHUENTE
Parallel Calculation of a Linear Mapping on a Computer Network
Linear Algebra and its Appl. 28 : 223-247 (1979)

[41] M. TCHUENTE
Parallel Realization of Permutations over trees.
R.R. n° 202 IMAG (Grenoble) mars 1979

[42] M. TCHUENTE
Sur la complexité du calcul des permutations sur un graphe en étoile
R.R. n° 201 IMAG (Grenoble) avril (1980)

[43] R. THOMAS
Boolean Formalization of Genetic Control Circuits
J. Theor. Biol. pp. 542-563 (1973)

[44] R. THOMAS
Logical Analysis of Systems Comprising Feedback Loops
J. Theor. Biol. pp. 631-656 (1978)

[45] P. VAN HAM and I. LASTERS
Reduction Methods for Logical Control Networks
J. THeor. Biol. pp. 269-281 (1978)

[46] J. WOLFMANN
Un problème d'extremum dans les espaces vectoriels binaires
Colloque Franco-Canadien de Combinatoire, Montréal, Juin 1979

[47] H. YAMADA and S. AMOROSO
Structural and Behavioral Equivalence of Tessellation Automata
Inform. Contr. vol. 18, pp. 1-31 (1971)

[48] E.GOLES et E.H. SNOUSSI
Etude dynamique de certains modéles de control génétique
in Biométrie génétique , Ed.Legay J.M. and Tomassone R.(à paraîtr

Dernière page d'une thèse

VU

Grenoble, le 21 Mai 1980

Le Président de la thèse

Vu, et permis d'imprimer,

Grenoble, le 2 - JUIN 1980

Le Président de l'Université
Scientifique et Médicale

UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE