Contribution des structures algébriques ordonnées à la théorie des réseaux

Claude Benzaken

N° d'ordre

THESES

présentées à

LA FACULTE DES SCIENCES DE L'UNIVERSITE DE GRENOBLE

pour obtenir

LE GRADE DE DOCTEUR ES SCIENCES MATHEMATIQUES

par

Claude Benzaken

1ère thèse :

Contribution des structures algébriques ordonnées à la théorie des réseaux

2ème thèse :

ALGEBRE DE JORDAN ET DOMAINE DE POSITIVITE

Thèses soutenues le 4 mars 1968, devant la Commission d'examen :

Monsieur KUNTZMANN	Président
Monsieur FORTET	Invité
Monsieur KOSZUL	Examinateur
Monsieur VAUQUOIS	Examinateur

N° d'ordre

THESES

présentées à

LA FACULTE DES SCIENCES DE L'UNIVERSITE DE GRENOBLE

pour obtenir

LE GRADE DE DOCTEUR ES SCIENCES MATHEMATIQUES

par

Claude Benzaken

1ère thèse :

Contribution des structures algébriques ordonnées à la théorie des réseaux

2ème thèse :

ALGEBRE DE JORDAN ET DOMAINE DE POSITIVITE

Thèses soutenues le 4 mars 1968, devant la Commission d'examen :

Monsieur KUNTZMANN	Président
Monsieur FORTET	Invité
Monsieur KOSZUL	Examinateur
Monsieur VAUQUOIS	Examinateur

ACULTE DES SCIENCES — UNIVERSITE DE GRENOBLE

L I S T E D E S P R O F E S S E U R S

-:-:-:-:-

DOYEN HONORAIRE :

M. MORET

DOYEN :

M. BONNIER

PROFESSEURS TITULAIRES

MM.	NEEL Louis	Chaire de Physique Expérimentale
	HEILMANN René	Chaire de Chimie
	KRAVTCHENKO Julien	Chaire de Mécanique Rationnelle
	CHABAUTY Claude	Chaire de Calcul différentiel et Intégra
	BENOIT Jean	Chaire de Radioélectricité
	CHENE Marcel	Chaire de Chimie Papetière
	FELICI Noël	Chaire d'Electrostatique
	KUNTZMANN Jean	Chaire de Mathématiques Appliquées
	BARBIER Reynold	Chaire de Géologie Appliquée
	SANTON Lucien	Chaire de Mécanique des Fluides
	OZENDA Paul	Chaire de Botanique
	FALLOT Maurice	Chaire de Physique Industrielle
	KOSZUL Jean-Louis	Chaire de Mathématiques
	GALVANI O.	Mathématiques
	MOUSSA André	Chaire de Chimie Nucléaire
	TRAYNARD Philippe	Chaire de Chimie Générale
	SOUTIF Michel	Chaire de Physique Générale
	CRAYA Antoine	Chaire d'Hydrodynamique
	REULOS R.	Théorie des Champs
	BESSON Jean	Chaire de Chimie
	AYANT Yves	Physique Approfondie

GALLISSOT	Mathématiques
Mlle LUTZ Elisabeth	Mathématiques
BLAMBERT Maurice	Chaire de Mathématiques
BOUCHEZ Robert	Physique Nucléaire
LLIBOUTRY Louis	Géophysique
MICHEL Robert	Chaire de Minéralogie et Pétrographie
BONNIER Etienne	Chaire d'Electrochimie et d'Electrométallurgie
DESSAUX Georges	Chaire de Physiologie Animale
PILLET E.	Chaire de Physique Industrielle et Electrotechnique
YOCCOZ Jean	Chaire de Physique Nucléaire Théorique
DEBELMAS Jacques	Chaire de Géologie Générale
GERBER R.	Mathématiques
PAUTHENET R.	Electrotechnique
VAUQUOIS B.	Chaire de calcul électronique
BARJON R.	Physique Nucléaire
BARBIER Jean-Claude	Chaire de Physique
SILBER R.	Mécanique des fluides
BUYLE-BODIN Maurice	Chaire d'Electronique
DREFUYS B.	Thermodynamique
KLEIN J.	Mathématiques
VAILLANT F.	Zoologie et Hydrobiologie
ARNAUD Paul	Chaire de Chimie
SENGEL P.	Chaire de Zoologie
BARNOUD F.	Chaire de Biosynthèse de la cellulose
BRISSONNEAU P.	Physique
GAGNAIRE	Chaire de Chimie Physique
Mme KOFLER L.	Botanique
DEGRANGE Charles	Zoologie
PEBAY-PEROULA J.C.	Physique
RASSAT A.	Chaire de Chimie Systématique
DUCROS P.	Chaire de Cristallographie Physique
DODU Jacques	Chaire de Mécanique Appliquée I.U.T.
ANGLES D'AURIAC P.	Mécanique des Fluides
LACAZE A.	Thermodynamique

PROFESSEURS SANS CHAIRE

MM.	GIDON P.	Géologie et Minéralogie
	GIRAUD P.	Géologie
	PERRET R.	Servomécanisme
Mme	BARBIER M.J.	Electrochimie
Mme	SOUTIF J.	Physique
	COHEN J.	Electrotechnique
	DEPASSEL R.	Mécanique des Fluides
	GASTINEL N.	Mathématiques Appliquées
	GLENAT R.	Chimie
	BARRA J.	Mathématiques Appliquées
	COUMES A.	Electronique
	PERRIAUX J.	Géologie et Minéralogie
	ROBERT A.	Chimie Papetière
	BIAREZ J.P.	Mécanique Physique
	BONNET G.	Electronique
	CAUQUIS G.	Chimie Générale
	BONNETAIN L.	Chimie Minérale
	DEPOMMIER P.	Etude Nucléaire et Chimie Atomique
	HACQUES Gérard	Calcul Numérique
	POLOUJADOFF M.	Electrotechnique

PROFESSEURS ASSOCIES

MM.	NAPP-ZINN	Botanique
	RODRIGUES Alexandre	Mathématiques Pures
	STANDING Kenneth	Physique Nucléaire

MAITRES DE CONFERENCES

MM.	LANCIA Roland	Physique Atomique
Mme	KAHANE J.	Physique
	DEPORTES C.	Chimie
Mme	BOUCHE L.	Mathématiques
	SARROT-REYNAUD	Géologie Propédeutique
Mme	BONNIER M.J.	Chimie
	KAHANE A.	Physique Générale
	DOLIQUE J.M.	Electronique

BRIERE G.	Physique M.P.C.
DESRE G.	Chimie S.P.C.N.
LAJZROWICZ J.	Physique M.P.C.
VALENTIN P.	Physique M.P.C.
BERTRANDIAS J.P.	Mathématiques Appliquées - TMP
LAURENT P.J.	Mathématiques Appliquées - TMP
CAUBET J.P.	Mathématiques Pures
PAYAN J.J.	Mathématiques
Mme BERTRANDIAS F.	Mathématiques Pures M.P.C.
LONGEQUEUE J.P.	Physique
NIVAT M.	Mathématiques Appliquées
SOHM J.C.	Electrochmie
ZADWORNY F.	Electronique
DURAND F.	Chimie Physique
CARLER G.	Biologie Végétale
AUBERT G.	Physique M.P.C.
DELPUECH J.J.	Chimie Organique
PFISTER J.C.	Physique C.P.E.M.
CHIBON P.	Biologie Animale
IDELMAN S.	Physiologie Animale
BOUVARD Maurice	Hydrologie
RICHARD Lucien	Botanique
PELMONT Jean	Physiologie Animale
BLOGH D.	Electrotechnique I.P.
BOUSSARD J.Claude	Mathématiques Appliquées I.P.
MOREAU René	Hydraulique I.P.
BRUGEL L.	Energétique I.U.T.
SIBILLE R.	Construction Mécanique I.U.T.
ARMAND Yves	Chimie I.U.T.
BOLLIET Louis	Infromatique I.U.T.
KUHN Gérard	Energétique I.U.T.
GERMAIN Jean-Pierre	Construction Mécanique I.U.T.
CONTE René	Thermodynamique
JOLY Jean-René	Mathématiques Pures
PIERY Yvette	Biologie Animale

MAITRE DE CONFERENCES ASSOCIES

SAWCZUK A.	Mécanique des Fluides
CHEEKE J.	Thermodynamique
YAMADA O.	Physique du Solide
NATR Lubomir	B.M.P.V.
NAYLOR Arch	Physique Industrielle
SILBER Léo	Radioélectricité
NOZAKI Akihiro	Mathématiques Appliquées
RUTLEDGE Joseph	Mathématiques Appliquées
DONOHO Paul	Physique Générale
EGGER Kurt	B.M.P.V.

Je voudrais exprimer toute ma reconnaissance à Monsieur le Professeur KUNTZMANN pour les précieuses indications qu'il n'a cessé de me donner dans la poursuite de ce travail. Il est à l'origine de cette thèse qui s'appuie sur certains de ses travaux personnels.

Je ne manquerai pas d'adresser à Monsieur FORTET, Professeur à la SORBONNE, le témoignage de ma respectueuse gratitude, pour l'intérêt qu'il a porté à ce travail et les encouragements qu'il m'a prodigués après mes premières notes aux Comptes-Rendus.

Que Monsieur le Professeur KOSZUL trouve ici, l'expression de ma profonde reconnaissance pour m'avoir permis, en me donnant le sujet d'une deuxième thèse, d'élargir mes connaissances.

Je remercie très vivement Monsieur le Professeur VAUQUOIS d'avoir accepté de participer au Jury.

Je m'en voudrais enfin d'oublier Madame COGNE pour le soin constant qu'elle a apporté dans la mise en page de cette thèse.

A ma femme

I N T R O D U C T I O N

L'objet de cette thèse est d'apporter une contribution à l'étude des problèmes combinatoires qui interviennent en théorie des réseaux. (Réseaux abstraits ou graphes ou plus précisément réseaux logiques binaires).

Un réseau binaire combinatoire, peut être schématisé par une boite (figure 1) ayant un certain nombre n d'entrées et une sortie, les entrées et les sorties n'ayant que deux valeurs possibles 0 et 1 (on note 2 l'ensemble {0,1}), la sortie étant une fonction des n entrées. En quelque sorte un tel réseau est une application $f : 2^n \to 2$.

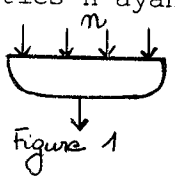


Figure 1

Un des problèmes fondamentaux, pour la construction de réseaux binaires (voir Roth et Wagner [24]) est le suivant : nous supposons possèder (avec autant d'exemplaires qu'on veut) divers réseaux standards réalisant diverses applications $f_i : 2^{n_i} \to 2$ ($n_i \in N$, $i = 1, 2...p$). Peut on dans ces conditions réaliser un réseau $f : 2^n \to 2$, par utilisation "combinatoire" des réseaux standards ?

Dans la plupart des cas, cette utilisation "combinatoire" peut être définie ainsi :

Par des "soudures" sur les entrées, on peut astreindre ces entrées à n'être plus indépendantes (mais égales). Une telle opération s'appelle <u>réduction</u>.

On peut enfin utiliser la sortie d'un réseau standard comme entrée d'un réseau suivant. C'est ce que nous appelons une <u>composition</u>.

Comme les applications $f : 2^n \to 2$ peuvent être définies par un élément (unique) d'une algèbre de Boole libre à n générateurs, comme à priori les nombres n, bien que finis, ne sont pas forcément bornés, on est amené à envisager au minimum, une algèbre de Boole libre Ω ayant pour base un ensemble infini dénombrable et traduire sur Ω les compositions (de deux éléments de Ω) et les réductions (d'un élément de Ω).

La notion de famille s'en déduit : une famille est une partie $\mathcal{F}$ de Ω stable (ou fermée) par rapport aux réductions et compositions. Cette notion répond parfaitement à la question de l'existence d'une synthèse possible d'un réseau f à partir de réseaux standards $f_1, f_2, \ldots, f_p$.

Toutes les familles ont été déterminées (voir Kuntzmann [15]). J'ai pu contribuer à cette détermination (note [1] et partie de [2]), en établissant l'existence de huit zones de filtration. Ces résultats constituent le premier chapitre. Parmi ces filtrations, la plus simple est :

$$M = MS_2 \supset MS_3 \supset MS_4 \supset \ldots \supset MS_i \supset MS_{i+1} \ldots\ldots \supset MS_\infty$$

(les inclusions sont strictes et entre deux familles consécutives, il n'y a aucune famille intermédiaire).

La famille M n'est autre que l'ensemble des applications booléennes croissantes ou encore le treillis distributif libre de même base que Ω.

Ce résultat semblait a première vue original au moment de la présentation des notes [1] et [2]. Ce n'est qu'en 1966 après des recherches bibliographiques poussées, que nous avons pu mettre la main sur un article de Post [21] publié en 1941 et réédité en 1965 ; cet article long de 118 pages, assez difficile à lire, pose le problème des familles, en termes de logique, et les détermine toutes (sans démontrer toutefois et sauf cas particulier qu'il n'en oublie aucune).

Bien entendu, concernant les filtrations, la définition que nous avons donnée des familles MS_i est tout à fait différente de celle de Post. Il en résulte d'ailleurs que les démonstrations diffèrent également. Nous enrichissons enfin, de nouvelles propriétés, ces familles MS_i. Par exemple : si $f > g$ et si $g \in MS_i$ alors $f \in MS_i$, par exemple enfin : la fonction $(n \geqslant 4)$ $s_n^2 : 2^n \to 2$ (définie par $s_n^2 = 1 \Leftrightarrow$ deux au moins des n variables ont pour valeur 1) engendre toute la famille MS_n. Cette génération est explicite.

A cette filtration particulière, correspond la notion d'indice d'une fonction croissante f : c'est l'entier n tel que $f \in MS_n$, $f \notin MS_{n+1}$.

Le chapitre 2 définit un moyen systématique de calculer l'indice d'une fonction croissante. La seule opération utilisée est une opération de dualisation (développement d'un produit de sommes). Nous obtenons comme conséquence, l'équivalence des définitions proposées par Post et moi-même pour la famille MS_i. D'autres critères de détermination de l'indice (de type récursif) sont définis.

Un des aspects originaux est le suivant : à tout graphe on peut associer une fonction booléenne $f \in M$. L'indice de f n'est autre que le nombre chromatique du graphe.

Il y a des fonctions croissantes f qui ne correspondent à aucun graphe. Nous sommes conduits a interpréter une fonction booléenne croissante comme un "polygraphe" ou encore l'ensemble des simplexes maximaux d'un complexe simplicial fini. Nous interprétons les opérations de réduction et composition sur ces polygraphes. Le théorème de génération de $f \in MS_n$ par s_n^2 nous permet d'en déduire : tout graphe n - chromatique est engendrable par réduction et composition, à partir du graphe complet d'ordre n - (on peut passer par des intermédiaires qui ne soient pas des graphes). Nous donnons dans la fin de ce chapitre un énoncé équivalent en termes de famille à la conjecture des quatre couleurs.

Le chapitre 3 reprend un travail de Zykov [29] portant sur les graphes et l'étend aux polygraphes c'est-à-dire aux fonctions booléennes croissantes. On définit ainsi somme et couplage de fonctions croissantes (notés par + et ×) et comme cas particuliers sommes et couplages directs de telles fonctions. Ces opérations (dans le cas direct) présentent l'intérêt suivant : si f a pour indice p et g pour indice q, f + g a pour indice sup (p,q) et f × g pour indice p + q.

Un théorème de structure est donné : toute fonction $f \in M$ ($\notin MS_\infty$) est décomposable par couplages et sommes directs, à l'aide de fonctions irréductibles. Le résultat est unique à l'ordre près des facteurs. Ce théorème étend non trivialement, le résultat de Zykov. Il a fallu en effet, pour lever les difficultés, faire appel à la notion (non involutive) de transposée et co-transposée d'une fonction, alors que pour le cas des graphes, seule la notion (involutive) de graphe complémentaire est utilisée.

Le reste du chapitre étend, très simplement, les résultats de Zykov concernant certains polynômes combinatoires (à coefficient entiers) associés à toute fonction croissante f et où les opérations de somme directe et couplage direct, se traduisent très simplement sur l'algèbre de ces polynômes.

Le chapitre 4 étudie les propriétés extrêmales des fonctions croissantes, en liaison avec l'indice.

On donne les limites possibles (et effectivement atteintes dans certains cas) de l'indice de f + g (ou f•g) quand on connait les indices de f et g. On étend aisément les résultats de Zykov [29].

Plus intéressante et originale est l'étude suivante : l'application qui à $f \in M$ fait correspondre son indice, étant une application croissante, quelles sont les fonctions extrêmales dans l'image réciproque de cette application ?

On montre que les éléments maximaux ne sont que relatifs ; on les détermine tous et on en déduit une génération, par produit, de tout élément f à partir des éléments maximaux de même indice et même support que f.

On montre que les éléments minimaux sont absolus (dès que l'indice ≥ 3). On donne un moyen d'en construire par couplage direct et par composition disjointe. On essaye de les caractériser récursivement. La réponse n'est que partielle.

Le chapitre 5 est consacré à des algorithmes. Il apparaît, dans tout le cours des chapitres précédents, que l'opération de dualisation d'une fonction booléenne est l'opération capitale (détermination de l'indice ou nombre chromatique, détermination des nombres de stabilité etc...). Cette opération par ailleurs, déborde largement du cadre de cette thèse (applications en logique, simplification des fonctions booléennes, théorie générale des équations booléennes, voir par exemple : S.Rudeanu [26]). Il nous a apparu intéressant d'y consacrer une petite analyse, permettant de conduire le calcul de duale, dans des conditions de performances, satisfaisantes.

Deux propositions ont été établies, simplifiant beaucoup un tel calcul ; on trouvera peut être une certaine analogie avec le travail de Pyne et Mac Cluskey [22] bien que ce dernier soit plus limité (dualisation des seules fonctions croissantes) et découle d'une technique de tableau, plus combinatoire qu'algébrique.

Des programmes ont été bâtis à partir de ces algorithmes ; ils ont donné confirmation, des performances attendues. Ils constituent une partie importante, de la bibliothèque des procédures de logique, dans le service de Mathématiques Appliquées de Grenoble.

Ce chapitre se termine enfin par d'autres algorithmes (décomposition, recherche d'équivalence sur des ensembles finis).

Le chapitre 6, change un peu d'objectif. Nous nous intéressons, aux problèmes des cheminements par arcs, sur un réseau donné. La littérature est abondante sur ce sujet. A l'inverse de techniques combinatoires, nous nous sommes efforcés de dégager le plus clairement possible, la structure algébrique qui se cache derrière ces problèmes. Cette structure que nous avons appelée "pseudo-treillis" est en fait connue sous le nom "gerbiers à éléments quasi-entiers" ; elle est étudiée par Dubreil-Jacotin, Croisot, Lesieur [10], mais vers des buts tout à fait différents, de ceux des cheminements. Le théorème clé concernant les applications aux cheminements, est le théorème généralisé de Lunc [17] (Lunc ne le démontre que dans le cas des algèbres de Boole). Ce théorème permet de définir une limite stationnaire (finie) pour toute suite $A + A^2 + .. + A^k$ construite à partir d'une matrice A. Ainsi le problème des plus courtes distances d'un sommet à un autre sur un réseau (routier par exemple) se ramène à un calcul systématique ne faisant appel à aucune technique combinatoire. Le théorème de Lunc, dans le cas des pseudo-treillis libres, donne nominativement les chemins d'un réseau. Aussi, nous nous sommes efforcés d'étudier les propriétés des pseudo-treillis libres. Les résultats qui semblent originaux sont les suivants : les pseudo-treillis libres sont réticulés (relativement à leur ordre). Lorsqu'ils ont une base finie, les idéaux sont principaux. Etant donné que tout homomorphisme de pseudo-treillis définit un idéal de ce pseudo-treillis et que réciproquement on peut construire les images homomorphes extrêmes (la plus fine et la plus grossière) correspondant à un idéal donné, la connaissance de tous les idéaux d'un pseudo-treillis libre de base finie est relativement précieuse. A titre d'exemple, nous définissons ainsi, les pseudo-treillis libres de carré nuls, commutatifs engendrés par un ensemble fini. Ils jouent, relativement à la détermination des chemins nominatifs d'un réseau, un rôle important par les simplifications qu'ils amènent concernant les calculs.

Le chapitre 7, enfin examine les problèmes de cheminements par sommets, dans un réseau. La structure de gerbier de carré nul, bien que pauvre sous l'angle algébrique, est une de celles que l'on peut retenir.

Le problème des cheminements par sommets ayant fait, par ailleurs l'objet de nombreux travaux (thèse de B.ROY [25]) nous n'avons pas trop insisté sur ce sujet. Toutefois nous présentons un algorithme pratique, de détermination des chemins simples d'un réseau.

Par contre nous avons étudié les réseaux avec couple d'entrée-sortie, dans la perspective des chemins simples joignant ces deux sommets. Nous sommes conduits alors à une équivalence entre réseaux et à la notion de réseau restreint qui est minimum dans sa classe d'équivalence. On montre que la détermination des réseaux maximaux d'une classe d'équivalence, se ramène encore au calcul de la duale d'une fonction booléenne. Nous citons une application d'un tel calcul : suppression du maximum de diodes d'un réseau de contacts, sans perturber la fonction de transfert.

Nous avons enfin profité, de ces notions, pour définir d'une manière plus synthétique les réseaux série-parallèles.

Les réseaux série-parallèles conduisent très naturellement à la notion de treillis série-parallèle. Un seul travail (à ma connaissance) a été entrepris sur de tels treillis (Elgott et Wright [12]).

Nous sommes partis d'une définition tout à fait différente de celle de ces auteurs, reposant seulement sur une condition simple de chaînes et il nous a semblé intéressant de définir ces treillis dans le cadre infini (complet).

Ces treillis ont une grande richesse de propriétés (la plupart du temps caractéristiques, bien qu'assez éloignées à première vue). C'est ainsi que les théorèmes que nous avons proposés, ne figurent pas dans la liste pourtant longue de ceux établis par Elgott et Wright.

CHAPITRE I

FAMILLES STABLES DE FONCTIONS BOOLEENNES CROISSANTES ET FAMILLES QUI EN DERIVENT. INDICE D'UNE FONCTION CROISSANTE.

1) Familles de fonctions booléennes.

On considère un ensemble fini dénombrable (naturellement ordonné) $U = \{a_1, a_2, \ldots, a_n, \ldots\}$ et dont les éléments sont appelés 'variables booléennes'.

Dans tout ce qui suivra on appellera Ω l'algèbre de Boole libre engendrée par U ; 0 et 1 désigneront les bornes universelles. Les opérations de borne supérieure, inférieure et de complément dans Ω seront respectivement notées $+$, . (signe parfois omis) et $'$.

Les éléments de Ω ne pourront être définis que par l'intermédiaire de formules dont les plus importantes sont les polynômes booléens.

Nous rappellerons qu'un monôme booléen μ est un produit d'un nombre fini de variables de U (certaines pouvant être complémentées) chaque variable du monôme figurant une fois parmi les facteurs sinon soit le monôme est nul (une variable et son complément), soit le monôme se simplifie.

Exemple : $a_1 a_2 a'_3$, $a_2 a_3 a_4 a_6$, a_1 sont des monômes.

Le nombre des lettres d'un monôme sera le degré de ce monôme.

Le monôme de degré 0 sera assimilé à l'élément 1 de Ω.

Un polynôme booléen est une somme d'un nombre fini q de monômes. Si q = 0 le polynôme sera assimilé à l'élément 0 de Ω.

Un polynôme booléen utilise, au total un nombre fini de variables de U. L'ensemble fini X de variables utilisées sera le support du polynôme. Un polynôme de support X sera désigné par p(X).

Les règles de l'algèbre de Boole permettent de définir, de manière peut être non unique, à partir de polynômes p(X), q(Y) un polynôme somme p(X) + q(Y), un polynôme produit p(X) . q(Y) et un polynôme complément $(p(X))'$.

En fait, les règles de l'algèbre de Boole permettent de définir une équivalence dans l'ensemble des polynômes (régulière par rapport aux sommes produits et compléments précédents) et Ω apparait comme l'ensemble quotient de l'ensemble des polynômes booléens par rapport à cette équivalence.

Si p(X) est un polynôme booléen et si μ est un monôme quelconque, on dit que μ est compatible avec p(X) si $\mu.p(X) \equiv \mu$.

Un monôme premier de p(X) est un monôme μ compatible avec p(X) et tel que tout monôme μ_1 déduit de μ en supprimant une lettre n'est plus compatible. Les monômes premiers de p(X) sont en nombre fini ; le polynôme formé de leur somme est la base complète de p(X).

La base complète présente l'intérêt suivant : c'est un polynôme équivalent à p(X) d'une part ; d'autre part deux polynômes sont équivalents si et seulement si ils ont même base complète.

On peut donc canoniquement représenter chaque $f \in \Omega$ par une et une seule base complète qu'on notera f(X) . X est l'ensemble support de f. Si X est vide alors f = 0 ou f = 1.

Mais on pourra représenter f par tout autre polynôme équivalent. Or à tout polynôme p(X) correspond naturellement une certaine application : les n variables X sont ordonnées par l'ordre induit de U. Soit $x_1, x_2 \ldots x_n$ ces variables dans l'ordre. On considère l'application $p : 2^n \to 2$ définie de la manière suivante :

Considérons un point $X_o = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ de 2^n ($\alpha_i = 0$ ou 1). Substituons dans le polynôme p(X) à chaque variable x_i la valeur α_i (et à x'_i la valeur complément) ; on obtient le résultat $p(X_o)$ en appliquant les règles de calcul booléen sur l'expression polynômiale.

Réciproquement à toute application $p : 2^n \to 2$ et à toute partie X de n variables de U on peut faire correspondre un polynôme p(X) dont l'application associée est p.

Pour ces raisons et par abus de langage tout élément de Ω s'appellera une <u>fonction booléenne</u> d'un nombre fini de variables.

Nous noterons enfin que si deux polynômes $p_1(X)$ et $p_2(Y)$ sont associés à un même élément p de Ω les applications p_1 et p_2 sont les mêmes si $X = Y$; si par contre $X \neq Y$ elles peuvent différer : mais alors l'une au moins des applications ne dépend pas de certaines variables.

1.1. <u>Réduction et composition dans Ω</u>.

On considère dans Ω les <u>deux opérations élémentaires</u> suivantes :

<u>Réduction d'une fonction</u>.

Soit <u>π une application de U dans U</u>. On désignera par x_π l'image correspondante à $x \in U$.

Si f appartient à Ω et si $X = \{x_1, x_2, \ldots x_n\}$ est l'ensemble support de f, on désigne par f_π et on l'appelle réduite de f par π l'élément de Ω obtenu à partir du polynôme f(X) en remplaçant chaque variable x_i par $(x_i)_\pi$ et x'_i par $(x_i)'_\pi$.

Nous noterons $\pi(X)$ l'image dans U de X.
Le support de f_π est une partie $T \subseteq \pi(X)$.
Nous noterons X_π l'ensemble ordonné (avec répétitions éventuelles)
$x_{1_\pi}, x_{2_\pi}, \ldots x_{n_\pi}$.

Nous avons alors :

$$f_\pi(T) = f(X_\pi)$$

La réduction π induit sur le support X de f une partition en p-classes : $X_1, X_2 \ldots, X_p$ $(p \leqslant n)$ chaque classe de variables ayant été confondue à une seule variable de U.

On dit alors que f_π est une réduite de f à <u>au plus p variables</u> car $|T| \leqslant p$.

<u>Composition de deux fonctions</u>.

Soient f et g deux fonctions. Considérons une variable x de U . Par définition la composée de f et g par rapport à x est la fonction notée $f \overset{x}{\circ} g$ obtenue en remplaçant dans f, x par g et x' par g' .

Bien entendu pour que cette composition ne soit pas triviale, on peut supposer que x appartient au support de f. Dans ce cas si f(x, X) est la fonction (précisée de son support) et si g(Y) est la fonction g, alors on notera :

$$f \overset{x}{\circ} g = f(g(Y), X)$$

La composition est dite disjointe si $X \cap Y = \phi$.

Propriétés et remarques.

1) Toute réduction est un homomorphisme dans Ω.

Cela veut dire que :

$$(f+g)_\pi = f_\pi + g_\pi \qquad (f.g)_\pi = f_\pi . g_\pi$$

$$(f')_\pi = (f_\pi)'$$

2) Le produit de deux réductions est une réduction. Toute réduction π dont la restriction sur le support X de f est l'identité est telle que $f_\pi = f$. En particulier ε étant l'application identique de U dans U $f_\varepsilon = f$ $(\forall f)$.

3) pour g fixé dans Ω et x fixé dans U , l'application $f \to f \overset{x}{\circ} g$ est un homomorphisme dans Ω.

Soit :

$$(f+h) \overset{x}{\circ} g = f \overset{x}{\circ} g + h \overset{x}{\circ} g$$
$$(f.h) \overset{x}{\circ} g = (f \overset{x}{\circ} g).(h \overset{x}{\circ} g)$$
$$(f') \overset{x}{\circ} g = (f \overset{x}{\circ} g)'$$

Notons que cette propriété n'a pas lieu quand f et x sont fixés et quand on fait varier g.

4) Si x n'appartient pas au support de f

$$f \overset{x}{\circ} g = f$$

5) Le produit de compositions doit nécessiter des parenthèses car on n'a pas en général

$$(f \overset{x}{\circ} g) \overset{y}{\circ} h = f \overset{x}{\circ} (g \overset{y}{\circ} h)$$

Exemple :

$$x\ y \overset{x}{\circ} \left(y\ t \overset{y}{\circ} (a+b)\right) = x\ y \overset{x}{\circ} (a\ t + b\ t) = a\ t\ y + b\ t\ y$$

$$(x\ y \overset{x}{\circ} y\ t) \overset{y}{\circ} (a+b) = y\ t \overset{y}{\circ} (a+b) = a\ t + b\ t$$

6) Toute composition non disjointe revient à faire une composition disjointe suivie d'une réduction.

En effet g(Y) et f(x, X) désignant les fonctions, considérons un ensemble Y_1 de variables telles que $|Y_1| = |Y|$ et $Y_1 \cap X = \phi$. Soit g_1 la fonction dans laquelle on a changé Y en Y_1 ; alors $f \overset{x}{\circ} g_1$ est une composée disjointe. Toute réduction π (il en existe) laissant invariant X et bijective de Y_1 sur Y est telle que :

$$(f \overset{x}{\circ} g_1)_{\pi} = f \overset{x}{\circ} g$$

1.2. Famille de fonctions booléennes.

Définition :

On désigne sous le nom de famille de fonctions booléennes toute partie $\mathcal{F} \subseteq \Omega$ fermée (ou stable) par rapport aux opérations élémentaires. Par convention l'ensemble vide ϕ sera considéré comme famille.

En d'autres termes :

$$\begin{cases} f \in \mathcal{F} \Rightarrow f_{\pi} \in \mathcal{F} \quad \text{pour toute réduction } \pi \\ f, g \in \mathcal{F} \Rightarrow f \overset{x}{\circ} g \in \mathcal{F} \quad \text{pour toute variable } x \text{ de } U \end{cases}$$

Puisque l'on considère simultanément les 2 opérations élémentaires. On peut supposer (remarque précédente 6) que les compositions envisagées sont disjointes.

Proposition : Soient $\mathcal{F}_\lambda$ $(\lambda \in \Lambda)$ un ensemble quelconque de familles indiciées par Λ . Alors $\bigcap_{\lambda\in\Lambda} \mathcal{F}_\lambda$ est une famille.

Ce résultat est évident. Comme Ω est lui-même une famille cela prouve que l'ensemble des familles ordonné par inclusion est un treillis complet.

Famille engendrée par une partie S.

C'est la famille intersection de toutes les familles $\mathcal{F}_\lambda$ contenant S. On la désigne par $\mathcal{F}(S)$.

Borne supérieure de deux familles $\mathcal{F}_1$, $\mathcal{F}_2$.

C'est la famille $\mathcal{F}(\mathcal{F}_1 \cup \mathcal{F}_2)$. On la désigne par $\mathcal{F}_1 \vee \mathcal{F}_2$.

Remarque :

Par définition même d'une famille, les variables du support d'un élément f de Ω n'ont pas d'importance en soi, puisque en rebaptisant ces variables par une réduction π partiellement injective sur ces variables on doit réobtenir un élément de la même famille que f.

On peut donc définir Ω à une équivalence près. On obtient la notion de fonction abstraite : c'est un élément f de Ω défini à un support près.
Dans ce cas réduire une fonction f revient simplement à se donner une partition du support X de f.

1.3. Famille maximale dans une autre.

Définition :

On dit que $\mathcal{F}$ est une famille maximale dans la famille $\mathcal{G}$ (ou $\mathcal{F}$ est une famille maximale de $\mathcal{G}$) si elle est couverte par $\mathcal{G}$ (au sens du treillis).

En d'autres termes cela signifie que :

$\mathcal{F} \subset \mathcal{G}$ et que pour toute autre famille $\mathcal{H}$,
$\mathcal{F} \subseteq \mathcal{H} \subseteq \mathcal{G}$ entraîne que $\mathcal{H} = \mathcal{F}$ ou $\mathcal{H} = \mathcal{G}$

Proposition : Une condition nécessaire et suffisante pour que les familles $\mathcal{F}_i$ ($i = 1, 2, \ldots p$) ne vérifiant aucune relation d'inclusion deux à deux et strictement contenues dans $\mathcal{F}$, soient les seules familles maximales de $\mathcal{F}$ et telles que toute sous famille stricte de $\mathcal{F}$ soit incluse dans l'une d'elle au moins, est que $\mathcal{F}$ soit engendrée par toute partie $S \subseteq \Omega$ constituée de p fonctions f_i (non forcément distinctes) mais satisfaisant à $f_i \in \mathcal{F}$, $f_i \notin \mathcal{F}_i$.

Condition nécessaire.

Soit S une partie vérifiant les conditions de la proposition, et $\mathcal{G}$ la famille engendrée par S.
Alors $\mathcal{G} \subseteq \mathcal{F}$. Mais :

$$\mathcal{G} \subset \mathcal{F} \Rightarrow \exists_i \ \mathcal{G} \subseteq \mathcal{F}_i$$

Cela est absurde car $f_i \in \mathcal{G}$ et $f_i \notin \mathcal{F}_i$.

Condition suffisante.

Chaque $\mathcal{F}_i$ est maximale sinon on peut trouver une famille $\mathcal{G}$ vérifiant :
$\mathcal{F}_i \subset \mathcal{G} \subset \mathcal{F}$.

Mais alors $\mathcal{G} \neq \mathcal{F}_j$ pour tout j = 1, 2..p. On pourrait former un ensemble S répondant aux conditions de la proposition et vérifiant en outre $S \subseteq \mathcal{G}$; S ne pourrait alors engendrer $\mathcal{F}$.

Toute autre sous-famille stricte $\mathcal{G}$ de $\mathcal{F}$ est incluse dans l'une au moins des p familles $\mathcal{F}_i$ sinon on pourrait de la même manière former un ensemble $S \subseteq \mathcal{G}$ répondant aux conditions de la proposition et n'engendrant pas $\mathcal{F}$.

Cela implique enfin, que les familles $\mathcal{F}_i$ sont les seules familles maximales de $\mathcal{F}$.

Cette proposition est la base pratique de la détermination complète et exhaustive du treillis des familles.

Toutefois une importante simplification va apparaître mise en lumière par les résultats suivants.

1.4. Dualité - Symétrie du treillis des familles.

Duale d'une fonction.

Soit $f \in \Omega$ représenté par le polynôme $f(x_1, x_2, .., x_n)$
On appelle duale de f la fonction $f^* \in \Omega$ représentée par le polynôme :

$$\left(f(x'_1, x'_2, \ldots, x'_n)\right)' \quad .$$

Rappelons les propriétés classiques [15] :

- $f \leqslant g \Longrightarrow f^* \geqslant g^*$
- $(f+g)^* = f^*.g^*$ et $(f.g)^* = f^*+g^*$
- $f^{**} = f$

La dualité nous conduit à la définition suivante (que l'on utilisera par la suite).

Définition :

Une fonction $f \in \Omega$ est dite respectivement surimpaire, impaire, sous impaire si

$$f \geq f^* \qquad (\text{resp } f = f^*) \quad (\text{resp. } f \leq f^*) \ .$$

Si f est surimpaire (sous impaire) sa duale est sous impaire (surimpaire).

Les opérations élémentaires ont vis à vis de la dualité la propriété suivante :

Lemme : f et g étant deux fonctions de supports disjoints nous avons :

(a) $(f_\pi)^* = (f^*)_\pi$ pour toute réduction π.

(b) $(f \overset{x}{\circ} g)^* = f^* \overset{x}{\circ} g^*$ pour toute variable x de f.

En effet :

(a) si f est représenté par $f(x_1, x_2, \ldots x_n)$ alors f_π est représenté par $f(x_{1_\pi}, x_{2_\pi}, \ldots, x_{n_\pi})$ et $(f_\pi)^*$ par le polynôme

$\left(f(x'_{1_\pi}, x'_{2_\pi}, \ldots, x'_{n_\pi})\right)' = f^*(x_{1_\pi}, x_{2_\pi}, \ldots, x_{n_\pi})$ donc (a) est démontré.

(b) Soit $\varphi(X, Y) = f\left(g(Y), X\right)$ un polynôme représentant $f \overset{x}{\circ} g$.

On a $\varphi^*(X, Y) = \left(\varphi(X', Y')\right)' = \left(f\left(g(Y'), X'\right)\right)'$ mais $g(Y') = \left(g^*(Y)\right)'$

donc $\varphi^*(X, Y) = f^*\left(g^*(Y), X\right)$.

Nous pouvons alors déduire :

Proposition : Si $\mathcal{F}$ est une famille alors l'ensemble $\mathcal{F}^*$ constitué de toutes les duales de $f \in \mathcal{F}$ est une famille. Si $\mathcal{F} \subset \mathcal{G}$ alors $\mathcal{F}^* \subset \mathcal{G}^*$ et si $\mathcal{F}$ est maximale dans $\mathcal{G}$, $\mathcal{F}^*$ l'est dans $\mathcal{G}^*$.

Cette proposition prouve que le treillis présente une symétrie dans la mesure où il existe des familles $\mathcal{F} \neq \mathcal{F}^*$ (non autoduales). Ce treillis a été complètement exhibé [21] [15]. Il contient (comme particularité essentielle) huit chaînes infinies dénombrables satisfaisant à la condition de chaîne croissante finie. Nous allons étudier le sous treillis $[\phi, M]$ qui est le plus petit pour lequel existe cette particularité.

2) Familles de fonctions croissantes strictes.

L'algèbre de Boole libre Ω contient (strictement) le treillis distributif libre M engendré par U (sans bornes 0 et 1). Dans ce cas à tout f appartenant à M on peut associer sa base complète ou polynôme irréductible :

$$\mu_1 + \mu_2 + .. + \mu_q$$

avec $q \geq 1$; chaque monôme étant de degré au moins 1 est un produit de variables non complémentées. En outre si $i \neq j$, μ_i n'est pas un multiple de μ_j.

Le support d'un élément de M n'est donc jamais vide.

La fonction booléenne $f : 2^n \to 2$ associée à la base complète f(X) est croissante stricte (*) dans le sens que :

(*) En fait le terme "croissante stricte" doit être pris dans le sens "croissante non constante".

$$\begin{cases} X_1, X_2 \in 2^n : X_1 \leq X_2 \Longrightarrow f(X_1) \leq f(X_2) \\ \text{Désignant par } \bar{0} \text{ et } \bar{1} \text{ les bornes de } 2^n, \text{ alors } f(\bar{0}) = 0 \quad \text{et} \quad f(\bar{1}) = 1 \end{cases}.$$

Réciproquement toute fonction f(X) strictement croissante peut être représentée par un polynôme sur X n'utilisant jamais de variables en complèment [15].

De la sorte, l'ensemble M s'identifiera à l'ensemble des fonctions croissantes strictes.

Théorème : L'ensemble M est une famille autoduale.

C'est évidemment une famille. La duale d'une fonction revient à échanger les opérations + et . dans les polynômes et à développer. Si la fonction est croissante stricte sa duale l'est.

Nous allons définir une certaine classe de fonctions qui vont jouer un rôle important dans la suite.

Définition :

On désigne par s_n^2 $(n \geq 2)$ une fonction croissante stricte dont le support contient n variables $x_1, x_2, \ldots x_n$ et définie par le polynôme : $\sum_{i \neq j} x_i x_j$

Cette fonction contient C_n^2 monômes distincts. Par exemple :

$$s_2^2 = x\,y$$

$$s_3^2 = x\,y + y\,z + z\,x$$

Le calcul montre que :

s_2^2 est sous impaire, non impaire.

s_3^2 est impaire ; s_n^2 est surimpaire non impaire pour $n \geqslant 4$.

2.1. Sur l'existence d'une double chaîne infinie de familles de fonctions croissantes strictes.

Définition I :

On appelle fonction atomique une fonction croissante stricte dont le polynôme irréductible contient au moins un monôme du premier degré. L'ensemble des fonctions atomiques est noté $M\,\Sigma$.

Par exemple les fonctions x, $x + y$, $x + y\,z$ sont des fonctions atomiques.

Théorème I :

L'ensemble $M\,\Sigma$ est une famille (non autoduale).
En outre si $f \in M\,\Sigma$ et si $g \geqslant f$ alors $g \in M\,\Sigma$.

Le caractère de famille de $M\,\Sigma$ est évident car réduction ou composition conservent toujours un monôme du 1^{er} degré dans les polynômes associés.

Cette famille n'est pas autoduale car $x\,y$ est la duale de $x + y$ (atomique) et n'est pas atomique.

Enfin le fait pour une fonction f d'être atomique est équivalent à dire que la fonction booléenne f(X) (croissante) prend la valeur 1 pour un atome du treillis 2^n. D'où il résulte que si $g \geq f$ et si f est atomique alors g est atomique.

On notera $M\Pi$ la famille duale de $M\Sigma$ qui peut être caractérisée comme l'ensemble des fonctions pour lesquelles une variable figure dans tous les monômes du polynôme associé.

Définition 2 :

Etant donné un entier $i \geq 2$ on désigne par MS_i l'ensemble des fonctions croissantes strictes f telles que toute réduite de f à i-1 variables au plus soit atomique.

Remarques :

Il est évident que $MS_2 = M$ car toute réduite à 1 variable de $f \in M$ ne comporte qu'une variable et est atomique.

Il est évident également que $MS_i \supseteq M\Sigma$ pour tout i , car toute réduite d'une fonction atomique est atomique quelque soit le nombre de variables de la réduite.

Théorème 2 :

Les ensembles MS_i sont des familles et nous avons

(a) $MS_i \supset MS_{i+1}$

(b) $MS_i \supset M\Sigma$ (c) en outre $M\Sigma = \bigcap_{i \geq 2} MS_i$ (d) pour $i \geq 3$ la famille MS_i n'est pas autoduale.

Il est tout à fait évident (d'après la définition) que MS_i est stable par rapport aux réductions.

Examinons la composition (cas disjoint).

Soit $\varphi(Y, Z) = f\big(Y, g(Z)\big)$ la composée de $f(Y, y)$ et de $g(Z)$ appartenant toutes les deux à MS_i.

Considérons une réduction π telle que $\varphi(Y, Z)$ se réduise à une fonction d'au plus $i-1$ variables.

Donc y_π $(y \in Y)$ et z_π $(z \in Z)$ ne parcourent que $i-1$ au plus variables distinctes. $\varphi(Y, Z)$ se réduit à :

$$\varphi(Y_\pi, Z_\pi) = f\big(Y_\pi, g(Z_\pi)\big)$$

Mais $g(Z_\pi)$ est alors atomique et il existe une variable z_π telle que $g(Z_\pi) \geqslant z_\pi$. En vertu de la croissance des fonctions on a :

$$\varphi(Y_\pi, Z_\pi) \geqslant f(Y_\pi, z_\pi)$$

Mais au deuxième membre les arguments Y_π et z_π n'ont que $i-1$ au plus valeurs distinctes. Donc ce deuxième membre est atomique et $\varphi(Y_\pi, Z_\pi)$ l'est également.

On constate aisément que toute fonction s_i^2 appartient à MS_i et non à MS_{i+1}. La relation d'inclusion évidente $MS_i \supseteq MS_{i+1}$ est donc stricte ce qui démontre (a).

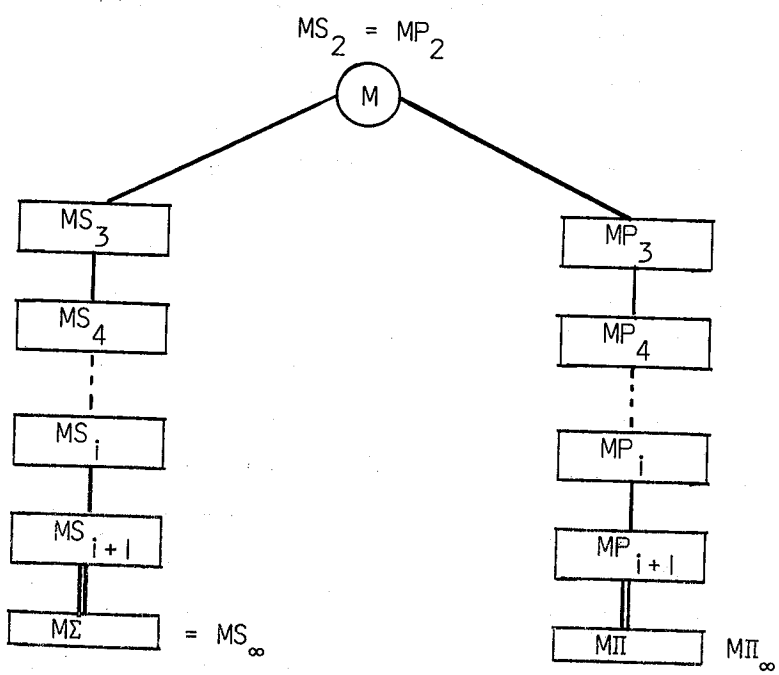
On démontre du même coup (b), cette fonction s_i^2 n'étant pas atomique.

Il en résulte que $M\Sigma \subseteq \bigcap_{i\geqslant 2} MS_i$; en fait on a une égalité car une fonction f appartenant à $\bigcap_{i\geqslant 2} MS_i$ vérifie la propriété que toute réduite f_π est atomique ; en particulier $f_\varepsilon = f$ est atomique. Donc (c) est démontré.

Enfin $x + y \in MS_i$ $(i \geqslant 3)$ alors que sa duale $x\,y \notin MS_i$ ($x\,y$ est sa propre réduite à 2 (< 3) variables). Ce qui démontre (d).

Il résulte donc l'existence d'une double chaîne infinie de familles. Nous reviendrons plus tard sur la recherche de leurs sous-familles maximales. Nous désignerons par MP_i la famille duale de MS_i ; bien entendu $MP_2 = MS_2 = M$. Nous noterons également de manière équivalente $M\Sigma$ ou MS_∞.

Le treillis comporte donc les inclusions suivantes :



Nous terminerons enfin par la propriété :

Proposition : si f appartient à la famille MS_i alors toute fonction $g \geqslant f$ appartient à MS_i.

En effet soit X le support de g et Y le support de f et supposons $f(Y) \leqslant g(X)$.

S'il y a des variables dans Y qui n'appartiennent pas à X , on considérera une réduction laissant les variables X inchangées et amenant les autres variables de Y sur une variable arbitraire x de X. Alors g(X) est inchangé et f(Y) se réduit à une fonction $f_{i_1}(X_{i_1})$ avec $X_{i_1} \subseteq X$. Cette fonction f_{i_1} appartient à MS_i et vérifie :

$$f_{i_1}(X_{i_1}) \leqslant g(X)$$

Cela étant toute réduction π réduisant g à au plus $i-1$ variables réduira f_{i_1} à au plus $i-1$ variables et donc : $f_{i_1\pi} \leqslant g_\pi$

Comme $f_{i_1\pi} \in M\Sigma$ c'est que $g_\pi \in M\Sigma$.

2.2. Indice d'une fonction croissante.

Puisque $MS_2 = M$, toute fonction croissante f appartiendra donc soit à $M\Sigma$, soit à MS_i mais pas à MS_{i+1}. Cela nous conduit à :

Définition 1 :

On appelle indice d'une fonction croissante stricte f l'entier noté $\nu(f)$ égal

1) à $+\infty$ si $f \in M\Sigma$

2) à i (fini) si $f \in MS_i$, $\notin MS_{i+1}$.

MS_i apparait alors comme l'ensemble des fonctions d'indice $\geqslant i$.
Nous avons relevé déjà l'importance de la fonction s_i^2 (défini à un support près de i variables).

Nous avons :

Proposition I :

Toute fonction f non atomique peut se réduire à une fonction s_r^2. Le plus petit entier r pour lequel cela est possible est l'indice de f.

Soit $\mu_1 + \mu_2 + \ldots + \mu_q$ le polynôme irréductible de f. Tous les monômes μ_i sont de degré $\geqslant 2$.

S'il y a un monôme (mettons μ_1) de degré supérieur à 2 on partage les lettres de μ_1 en deux paquets non vides disjoints S_1 et S_2 et on réduit les lettres S_1 à t_1 et les lettres S_2 à t_2. Ce monôme se réduit alors à un monôme du second degré et la fonction f se réduit à une fonction non atomique (sans quoi μ_1 serait le multiple d'un autre monôme). En continuant ainsi, on parvient à une fonction homogène de degré deux de ℓ variables.

S'il y a C_ℓ^2 monômes distincts, alors cette réduite est s_ℓ^2 ; sinon il manque, par exemple, un monôme $t_1 t_2$.

La réduction $t_1 = t_2$ n'introduit aucun monôme du 1^{er} degré et réduit d'une unité les variables de f.

Comme $C_2^2 = 1$ et que les réduites conservent au moins un monôme, on arrivera bien, pour conclure, à réduire f à une certaine fonction s_r^2.

Soit alors r le plus petit entier pour lequel cela est possible.

Alors $f \in MS_r$ sinon f admettrait une réduite à r-1 variables au plus, non atomique ; cette dernière fonction pourrait être réduite alors à s^2_q (avec $q \leqslant r-1$).
Donc r ne serait pas le plus petit entier.
Enfin f n'appartient pas à MS_{r+1} puisqu'elle se réduit à s^2_r ($\notin MS_{r+1}$). Donc r est bien l'indice de f.

Conséquence 1 :

Une réduction ne peut diminuer l'indice d'une fonction. En d'autres termes :

$$\forall_\pi \qquad \nu(f) \leqslant \nu(f_\pi)$$

La manière dont on a démontré cette précédente proposition nous conduit à la définition suivante.

Définition 2 :

On appelle nombres caractéristiques de f les entiers $n_1, n_2, \ldots n_s$ tels que f est réductible à $s^2_{n_i}$.

Remarque :

Il ne faut pas croire que l'ensemble des nombres caractéristiques de f($\notin M\Sigma$) soit réduit à un seul élément.

Par exemple $x_1 y_1 + x_2 y_2 + x_3 y_3$ admet les nombres caractéristiques 2 et 3.

La réduction $x_1, x_2, x_3 \to x$ et $y_1, y_2, y_3 \to y$ réduit la fonction à $x\,y$. La réduction

$x_1, x_2 \to x$, $y_2, y_3 \to y$, $y_1, x_3 \to z$ la réduit à

$s_3^2(x, y, z) = x\,z + x\,y + y\,z$.

Nous pouvons caractériser la famille MS_3 par la proposition suivante :

Proposition 2 :

La famille MS_3 n'est autre que l'ensemble des fonctions croissantes strictes, surimpaires.

Si $\nu(f) \geqslant 3$ montrons que f est surimpaire soit $f \geqslant f^*$. Si cela n'était pas, entre les fonctions booléennes $f(X)$ et $f^*(X)$ il existerait une valeur $X_o \in 2^n$ ($|X| = n$) pour X telle que $f(X_o) = 0$, $f^*(X_o) = 1$ ou encore $f(X'_o) = 0$. Il est évident que $X_o \neq \bar{0}$ et $\bar{1}$. Donc X_o permet de partitionner les variables X en deux classes. La classe U contient les variables ayant pris la valeur 1 en X_o et la classe V contient les autres variables.

Si l'on réduit les variables U à u et V à v la fonction f se réduit à une fonction $g(u, v)$ vérifiant :

$g(0, 0) = 0 = g(0, 1) = g(1, 0)$ alors que $g(1, 1) = 1$.

Donc $g = u\,v$. Par suite $\nu(f) = 2$ ce qui est absurde.

Inversement si f est surimpaire alors $f \geqslant f^*$; mais alors pour toute réduction π $f_\pi \geqslant (f^*)_\pi = (f_\pi)^*$. Donc f_π est surimpaire ; donc on ne peut réduire f à $x.y$ qui n'est pas surimpaire.

Donc $\nu(f) \geqslant 3$.

Conséquence 2 :

La famille intersection de MS_3 et MP_3 est l'ensemble des fonctions croissantes impaires. On la désigne par MI.

En effet $f \in MS_3 \Rightarrow f \geq f^*$; comme $f \in MP_3$ alors $f \leq f^*$; donc $f = f^*$.

Nous rappelerons les propositions [15].

Proposition 3 :

La famille MI n'est constituée que de fonctions d'indice 3 et est engendrée par la fonction s_3^2 (appelée majorité à 3 variables).

Remarque :

Une fonction d'indice 3 n'est pas forcément impaire.

Exemple : $f = a\,b + b\,c + c\,d + x\,y$ n'est pas impaire.
Son indice est trois $(x \to a \quad y \to b)$

Proposition 4 :

Toute fonction croissante stricte surimpaire est somme de fonctions croissantes strictes impaires.

2.3. Détermination exhaustive et complète de toutes les familles de fonctions croissantes strictes.

Les sous-familles de MΣ (resp MΠ) et de MI ont été déterminées.

On trouve la démonstration des résultats suivants en [15] dont certains sont d'ailleurs évidents :

- MΣ admet comme seule famille maximale la famille Σ (non autoduale) constituée des fonctions dont tous les monômes du polynôme irréductible sont du premier degré.

La famille duale de Σ est notée Π et consiste des fonctions dont le polynôme irréductible ne comporte qu'un monôme. La fonction $x + y\,z$ est un générateur de MΣ.

- La famille Σ (comme Π) admet pour seule famille maximale la famille notée E des fonctions croissantes d'une seule variable c'est-à-dire des fonctions x $(x \in U)$.

- La famille MI admet pour seule famille maximale la famille E (rappelons qu'elle est engendrée par la fonction s_3^2).

- E n'admet pour seule famille maximale que la famille vide ϕ.

Il ne reste donc qu'à chercher les familles maximales de MS_i $(i = 2, 3....)$.

Théorème I :

Pour $i \geq 4$, s_i^2 engendre la famille MS_i.

En effet comme $i \geq 4$ s_i^2 peut se réduire à :

$$s_i^2 (x, x, \ldots, x, y, z) = x + y\,z$$

et engendre donc toute fonction atomique : $x + \sum_k m_k$ où les m_k désignent des monômes.

Si f est engendrée par s_i^2 il en résulte que

$f + m_1 + m_2 + .. + m_q = (x + \Sigma m_k) \overset{\times}{o} f$ est engendrée par s_i^2. Donc si $g \geqslant f$, g est engendré par s_i^2. En particulier s_i^2 engendre s_j^2 $(j \geqslant i)$.

Soit alors p l'indice de $f(X) \in MS_i$. Donc $p \geqslant 1$. On peut réduire f(X) à s_p^2 en partageant les variables X en p classes $X_1, X_2, .., X_p$ et en confondant les variables de chaque classe respectivement à $t_1, t_2, .. t_p$. Si π est une telle réduction on a alors :

$$f(X_\pi) = s_p^2 (t_1, t_2, .. t_p) = s_p^2(T)$$

Considérons alors pour $k = 1, 2.. p$ les monômes m_k produits des variables de la classe X_k.

Nous avons :

1) $m_k \cdot m_\ell \leqslant f$ si $k \neq \ell$.

En effet si $m_k = m_\ell = 1$ c'est que les variables de X_k et de X_ℓ ont la valeur 1 et donc T a pris une valeur de hauteur deux dans 2^p et par suite $s_p^2(T)$ comme f ont la valeur 1.

2) Chaque fonction $\varphi_k = m_k + f$ est strictement plus grande que f puisque en annulant toutes les variables sauf celles de la classe X_k on a $\varphi_k = 1$ mais f prend la même valeur que $s_p^2(T)$ pour le k-ème atome de 2^p donc $s_p^2(T) = 0 = f$.

Par suite nous avons :

$$s_p^2(\varphi_1, \varphi_2, \ldots, \varphi_p) = \sum_{k \neq \ell} \varphi_k \varphi_\ell = \sum_{k \neq \ell} (f + m_k)(f + m_\ell) =$$

$$= \sum_{k \neq \ell} (f + m_k . m_\ell) = \sum_{k \neq \ell} f = f$$

Ces fonctions $\varphi_1, \varphi_2, \ldots \varphi_p$ sont strictement plus grandes que f ; elles appartiennent donc à MS_i.

Ayant un support au plus X elles appartiennent au treillis distributif libre engendré par X (qui est fini).

Si on recommence le processus sur elles, on sera amené donc au bout d'un nombre fini d'étapes à engendrer des fonctions atomiques et cela est possible.

Théorème 2 :

Les seules familles maximales de MS_i sont :

(a) MS_3 et MP_3 si $i = 2$

(b) MS_4 et MI si $i = 3$

(c) MS_{i+1} si $i > 3$

Nous utiliserons la proposition (1.3)

(a) Considérons deux fonctions f , g telles que :

- $f \in MS_2$, $f \notin MS_3$
- $g \in MS_2$, $g \notin MP_3$ ou encore : $g^* \in MS_2$, $g^* \notin MS_3$

Alors f et g^* sont d'indices deux et engendrent x y.

Donc f et g engendrent $x.y$ et $x + y$; ces deux dernières engendrent trivialement $MS_2 = M$.

(b) Soient f, g telles que :

$$\begin{cases} f \in MS_3 \text{ et } f \notin MS_4 \\ g \in MS_3 \text{ et } g \notin MI \text{ soit encore } g \notin MP_3 \text{ ou } g^* \notin MS_3. \end{cases}$$

f est d'indice 3 et engendre s_3^2 qui engendre MI ; g^* est d'indice deux, engendre $x\ y$; donc g engendre $x + y$. Avec f et g on engendre toute somme de fonctions impaires dont tout MS_3.

(c) Si f est telle que $f \in MS_i$, $f \notin MS_{i+1}$ $(i \geqslant 4)$ alors f est d'indice i et engendre s_i^2 qui engendre MS_i.

3) Les familles déduites des familles croissantes. Autres chaînes infinies.

Nous allons voir rapidement, la répercussion de l'existence des chaînes infinies de familles croissantes strictes sur l'ensemble des familles. A cause de la dualité, nous n'examinerons qu'un point de vue afin d'alléger l'exposé.

3.1. Enveloppe inférieure croissante d'une fonction.

Nous considérerons des fonctions croissantes au sens large.
Une fonction croissante (au sens large) est une fonction qui est soit croissante stricte, soit 0, soit 1.

L'application $f : 2^n \to 2$ associée à une fonction croissante f vérifie alors :

$$X_1 \geqslant X_2 \Longrightarrow f(X_1) \geqslant f(X_2) .$$

Soit f une fonction donnée, de support X ; considérons toutes les fonctions g croissantes telles que : $g \leqslant f$.

Il en existe car $0 \leqslant f$. Si le support Y de g n'est pas contenu dans f en rendant les variables de Y étrangères à X égales à 1 on obtient encore une fonction g_1 croissante telle que $g \leqslant g_1 \leqslant f$. Ces fonctions g_1 ayant un support contenu dans X sont en nombre fini ; leur somme a un sens et désigne une fonction notée $\underset{\vee}{f}$ croissante avec les propriétés suivantes :

$$\begin{cases} \underset{\vee}{f} \leqslant f \\ \text{pour toute fonction croissante } g \leqslant f \text{ alors } g \leqslant \underset{\vee}{f}. \end{cases}$$

Cela nous conduit à :

Définition :

L'enveloppe inférieure croissante d'une fonction f est la plus grande fonction croissante notée $\underset{\vee}{f}$ telle que $\underset{\vee}{f} \leqslant f$.

Propriété 1 :

si $f \leqslant g$ alors $\underset{\vee}{f} \leqslant \underset{\vee}{g}$.

En effet : $\underset{\vee}{f} \leqslant f \leqslant g$.

Propriété 2 :

Pour toute fonction f et toute réduction π :

$$\underset{\vee}{f}_{\pi} \leqslant \underset{\vee}{f_{\pi}}.$$

En effet de $\underset{\vee}{f} \leqslant f$ on déduit $\underset{\vee}{f}_{\pi} \leqslant f_{\pi}$ et donc $\underset{\vee}{f}_{\pi}$ (qui est croissante) est inférieure ou égale à $\underset{\vee}{f_{\pi}}$.

Propriété 3 :

Quelles que soient les fonctions f, g et la variable x alors

$$\underset{\vee}{f} \overset{x}{\circ} \underset{\vee}{g} \leqslant \underset{\vee}{(f \overset{x}{\circ} g)} .$$

En effet $\underset{\vee}{f} \leqslant f$ donc $\underset{\vee}{f} \overset{x}{\circ} g \leqslant f \overset{x}{\circ} g$; or $\underset{\vee}{g} \leqslant g$ et $\underset{\vee}{f}$ est une fonction croissante donc $\underset{\vee}{f} \overset{x}{\circ} \underset{\vee}{g} \leqslant \underset{\vee}{f} \overset{x}{\circ} g \leqslant f \overset{x}{\circ} g$. Comme $\underset{\vee}{f} \overset{x}{\circ} \underset{\vee}{g}$ est croissante cela prouve la propriété.

Proposition :

Soient une fonction booléenne f et x une de ses variables. Supposons que f soit représentée par le polynôme

$f = x.h + x'.k + r$ (h, k, r polynômes ne contenant pas x comme variables).

Alors $f_1 = f \overset{x}{\circ} (x + k)$ a même enveloppe inférieure croissante que f.

La substitution donne :

$f_1 = x.h + h.k + r$; mais :

$h.k = (x + x').h.k = x\,h\,k + x'\,h\,k \leqslant f$

donc $f_1 \leqslant f$;

Par suite $\underset{\vee}{f_1} \leqslant \underset{\vee}{f}$

Mais $\underset{\vee}{f_1} \geqslant \underset{\vee}{f} \overset{x}{\circ} \underset{\vee}{(x + k)} \geqslant \underset{\vee}{f} \overset{x}{\circ} x = \underset{\vee}{f}$;

Donc $\underset{\vee}{f} = \underset{\vee}{f_1}$.

Il faut noter que cette proposition, permet à partir d'une expression polynomiale d'une fonction de déterminer son enveloppe inférieure croissante et par une très légère modification de justifier l'algorithme de détermination des composants premiers d'une fonction par consensus, défini par ailleurs dans [28].

3.2. Chaînes infinies de familles déduites des familles de fonctions croissantes strictes.

Définition :

Etant donné l'entier $i \geqslant 2$ on définit

- MS_i | comme la réunion de la famille MS_i et de la fonction |.
- αS_i comme l'ensemble des fonctions f vérifiant :

$$\begin{cases} f \in MS_i \\ f(x, x, x, \ldots x) = x \qquad (\alpha) \end{cases}$$

- S_i comme l'ensemble des fonctions f telles que

$$f^{\downarrow} \in MS_i \quad |$$

Théorème | :

Les ensembles précédents sont des familles.

Cela résulte aisément des propriétés |, 2, 3 précédentes (3.|).

Remarque :

Nous pouvons étendre la définition à $i = \infty$, l'ensemble MS_∞ ayant un sens.

Propriétés des familles limites αS_∞ et S_∞

On démontre [15] que :

(1) $x + y' z$ engendre αS_∞

(2) $x + y'$ engendre S_∞

(3) toute fonction αS_2 non croissante peut engendrer $x + y' z$

(4) toute fonction S_2 non croissante peut engendrer soit $x + y' z$ soit $x + y'$ selon qu'elle appartient à αS_2 ou non.

Théorème 2 :

Nous avons entre les familles $\overleftarrow{MS_i\ |}$, αS_i, S_i les propriétés suivantes :

(a) $MS_i\ | \supset MS_{i+1}\ |$ $\qquad$ $MS_\infty\ | = \bigcap_i MS_i\ |$

$\alpha S_i \supset \alpha S_{i+1}$ $\qquad$ $\alpha S_\infty = \bigcap_i \alpha S_i$

$S_i \supset S_{i+1}$ $\qquad$ $S_\infty = \bigcap_i S_i$

(b) Les seules sous-familles maximales

de $MS_i\ |$ sont MS_i et $MS_{i+1}\ |$

de αS_i sont αS_{i+1} et MS_i

de S_i sont $MS_i\ |$, αS_i, S_{i+1}

En effet dans tous les cas on constate que : $s_i^2 \in MS_i\ |$ (resp αS_i, S_i) sans appartenir à $MS_{i+1}\ |$ (resp αS_{i+1}, S_{i+1}). Les inclusions larges évidentes sont donc strictes.

Les familles limites sont bien l'intersection des familles correspondantes à tous les niveaux i ainsi qu'il résulte pratiquement de la définition. Le point (a) est démontré.

- Les familles maximales de MS_i I sont MS_i et MS_{i+1} I. Il est évident d'abord que $MS_i \subset MS_i$ I.

Soient f et g appartenant à MS_i I et telles que

$f \notin MS_i$ (alors f = I)

$g \notin MS_{i+1}$ I alors g est $\in MS_i$ et d'indice i.

g engendre donc MS_i ; f étant égal à I nous engendrons donc MS_i I.

- De même $\alpha S_i \supset MS_i$ car $x + y' z \in \alpha S_i$ et n'est pas croissante.

Soient donc f, g appartenant à αS_i et telles que : $f \notin \alpha S_{i+1}$ et $g \notin MS_i$.

Alors g appartenant à αS_2 et étant non croissante engendre $x + y' z$ (propriété 3 précédente) et donc αS_∞.

D'après le choix de f, $\underset{\vee}{f}$ est d'indice i.

En nous appuyant sur la proposition 3.I précédente on peut engendrer $\underset{\vee}{f}$ avec les fonctions αS_∞.

En effet la substitution $x \to x + k$ si $f = x\,h + x'k + r$ revient à remplacer x par une fonction αS_∞ : en effet $\underset{\vee}{x + k} \geqslant x \in MS_\infty$.

Par ailleurs $x + k\,(x, x, \ldots x)$ peut être x ou alors I (si $k\,(x, x \ldots x) = x'$ ou I) ; la deuxième éventualité est à rejeter sinon

$$f\,(x, x \ldots x) = x\,h\,(x \ldots x) + x'\,k\,(x \ldots x) + r\,(x \ldots x)$$

serait égale soit à I soit à x' et cela est exclu.

Donc on peut engendrer $\underset{\vee}{f}$ c'est-à-dire MS_i. On dispose donc de $MS_i \cup \alpha S_\infty$.

Soit alors $\varphi = \underset{\vee}{\varphi} + m_1 + m_2 + .. + m_q$ une fonction quelconque de αS_i ; la fonction $x + m_1 + m_2 + .. + m_q$ est manifestement αS_∞ ; $\underset{\vee}{\varphi}$ appartient à MS_i ; par composition on obtient donc φ.

- Examinons enfin les sous-familles maximales de S_i.

Nous avons $S_i \supset \alpha S_i$ (l'inclusion est stricte car $x + y' \in S_i$ et $x + y' \notin \alpha S_i$) ; pour les mêmes raisons d'ailleurs $S_i \neq MS_i\ 1$.

Nous avons trois familles incluses strictement dans S_i : S_{i+1}, αS_i, $MS_i\ 1$. Considérons alors trois fonctions f, g, h de S_i telles que $f \notin S_{i+1}$, $g \notin \alpha S_i$, $h \notin MS_i\ 1$.

A partir de h (non croissante) appartenant à S_2 on peut obtenir (propriété 4 précédente) soit $x + y'\ z$ soit $x + y'$.

A partir de g de la même manière on obtient soit 1 soit $x + y'$.

Dans le cas le plus défavorable nous pouvons donc disposer au moins de $x + y'$ qui engendre S_∞ (contenant 1).

Utilisant toujours la proposition (3.1) précédente par substitution de fonctions du type $x + k$ (appartenant à S_∞) on peut donc avec f obtenir $\underset{\vee}{f}$ qui est manifestement d'indice i. Nous génerons donc $MS_i\ 1 \cup S_\infty$.

Soit alors $\varphi = \underset{\vee}{\varphi} + m_1 + m_2 + .. + m_q$ une fonction appartenant à S_i ; dans la fonction $x + \Sigma m_k$ (qui est une fonction S_∞), si l'on substitue à x la fonction $\underset{\vee}{\varphi}$ ($\in MS_i\ 1$) on obtient bien φ.

Le théorème est donc démontré.

CHAPITRE II

SUR LA DETERMINATION DE L'INDICE D'UNE FONCTION CROISSANTE STRICTE. APPLICATIONS A LA THEORIE DES NOMBRES CHROMATIQUES.

La notion d'indice d'une fonction croissante stricte a été introduite à partir de la chaîne infinie de familles emboitées MS_i. La définition de l'indice est donc une définition purement existentielle et assez peu constructive. Même le résultat de la proposition (Ch. I - 2.2) liant l'indice d'une fonction aux réduites du type s_p^2 de cette fonction est lui aussi assez peu constructif.

Nous allons définir un moyen systématique de calculer l'indice d'une fonction, au moyen des seules opérations booléennes.

1) Critère fondamental de détermination de l'indice.

1.1 Points caractéristiques, classes permises et saturées d'une fonction croissante stricte.

Soit f une fonction de Ω de support $A = \{a_1, a_2, \ldots, a_n\}$ croissante stricte à laquelle nous associons l'application $f : 2^n \to 2$.

Nous rappelons que l'algèbre de Boole 2^n est isomorphe à l'ensemble 2^A des parties de A. Cet isomorphisme est défini par :

- à $S \in 2^A$ on fait correspondre $X_S \in 2^n$, vecteur booléen dont les composantes sont 1 pour les seules variables de S.

- L'isomorphisme réciproque est celui qui fait correspondre à $X \in 2^n$ la partie S_X de A des variables ayant la valeur 1 sur X.

Définition 1 :

f étant une fonction croissante stricte de Ω on appelle point caractéristique de première espèce (resp. deuxième espèce) tout point X de 2^n minimal (resp. maximal) relativement à l'ordre de 2^n et tel que l'application associée $f : 2^n \to 2$ vérifie $f(X) = 1$ (resp. $f(X) = 0$).

En d'autres termes :

- X est caractéristique de première espèce si $f(X) = 1$ et si $Z < X$ entraîne $f(Z) = 0$.

- X est caractéristique de deuxième espèce si $f(X) = 0$ et si $Z > X$ entraîne $f(Z) = 1$.

Proposition 1 :

Soit $\mu_1 + \mu_2 + \ldots + \mu_q = f(a_1, a_2, \ldots a_n)$ le polynôme irréductible de la fonction croissante f. Les points caractéristiques de première espèce de f sont les points X_{μ_i} (obtenus par l'isomorphisme, chaque monôme μ_i étant assimilé à la à la partie des variables qu'il utilise). Les points de deuxième espèce de f sont les compléments respectifs des points de première espèce de f^*.

La première partie est évidente. Il est trivial que $f(X_{\mu_i}) = 1$. Par ailleurs si $Z < X_{\mu_i}$ cela entraîne par isomorphisme que $S_Z \subset \mu_i$; $f(Z) = 0$ sinon le monôme S_Z est compatible avec f et c'est un diviseur strict de μ_i et le monôme μ_i ne serait pas irréductible. Réciproquement si X est de première espèce, S_X est un monôme compatible avec f et tout diviseur de S_X ne l'est pas (sinon X n'est pas de première espèce).

La deuxième partie de cette proposition est évidente ; en effet Y de deuxième espèce pour f entraîne que :

$f^*(Y') = \big(f(Y)\big)' = 1$ car $f(Y) = 0$.

Si $Z < Y'$ cela entraîne que $Z' > Y$ donc $f(Z') = 1$ donc $\big(f(Z')\big)' = 0$ donc $f^*(Z) = 0$.

La proposition indique donc qu'à partir de la forme polynômiale de f, la détermination des points de 1ère espèce de f est triviale ; celle des points de 2^e espèce nécessite un calcul de duale.

Exemple : $f(a, b, c) = a\,b + a\,c$

Les points de 1ère espèce sont : (1, 1, 0) et (1, 0, 1).

$f^*(a, b, c) = (a + b)(a + c) = a + b\,c$

dont les points de 1ère espèce sont (1, 0, 0) et (0, 1, 1).

Donc (0, 1, 1) et (1, 0, 0) compléments respectifs sont les seuls points de 2^e espèce de f.

Considérons une réduction π et une fonction croissante stricte f de support A. Nous savons que cette réduction induit une partition de A en classes A_i. Ces classes A_i seront dites associées à π.

Soit une partie S de A. On dira qu'une réduction π est associée à S si S est classe associée à π et si toute autre classe associée à π n'a qu'un élément. On pourra toujours en construire une : en particulier si on choisit $x \notin A$ alors la réduction π définie par : $y_\pi = x$ si $y \in S$ et ($y_\pi = y$ si $y \notin S$, répond à la définition.

Définition 2 :

Etant donné une fonction croissante stricte non atomique et de support A on appelle :

1) Classe permise de f toute partie S de A telle que pour toute réduction π associée à S, alors f_π est non atomique.

2) Classe saturée de f toute classe permise maximale par inclusion.

Bien entendu puisque f est non atomique, toute classe réduite à un seul élément est permise.

Proposition 2 :

Les classes permises S de f correspondent bijectivement par isomorphisme aux points $X_S \in 2^n$ pour lesquels $f(X_S) = 0$. Il en résulte que les classes saturées de f correspondent bijectivement aux points caractéristiques de deuxième espèce de f.

Si S est permise, $f(X_S) = 0$; sinon en considérant une réduction π associée à S on constate que f_π prend la valeur 1 sur un atome, donc est atomique. Cela est donc absurde puisque S est permise.

Réciproquement si $f(X) = 0$, alors la classe S_X est permise sinon une réduction π associée à S_X est telle que f_π est atomique ; or cela est impossible sinon f prendrait la valeur pour un atome ou serait telle que $f(X) = 1$ ce qui est contradictoire.

L'isomorphisme $S \to X_S$ conservant l'ordre, il en résulte que les classes saturées correspondent bien aux points caractéristiques de deuxième espèce de f.

Il en résulte que l'on peut déterminer les classes saturées de f par le processus suivant :

On part de $f(A) = \pi_1 + \pi_2 + \ldots + \pi_q$ (irréductible)

On calcule $f^*(A) = \mu_1 + \mu_2 + \ldots + \mu_r$ (irréductible)

On en déduit que $\complement_A \mu_1, \complement_A \mu_2, \ldots, \complement_A \mu_r$ sont les classes saturées de f.

Dans l'exemple précédent $f = a\,b + a\,c$ on a $f^* = a + b\,c$ et $\{b, c\} = \complement a$ et $\{a\} = \complement b\,c$ sont les classes saturées de f.

1.2. Le critère fondamental de recouvrement.

Définition :

A étant le support de f, un recouvrement de A est un ensemble $A_1, A_2, \ldots, A_q$ où $A_i \neq \phi$, $A_i \subseteq A$ et $\bigcup_{i=1}^{q} A_i = A$. L'ordre du recouvrement est q.

Critère fondamental.

L'indice d'une fonction croissante f(A) n'appartenant pas à MΣ est le plus petit ordre des recouvrements de A par des classes saturées de f.

Soit en effet p l'indice de f. Il existe une réduction π induisant une partition $\{A_1, A_2, \ldots, A_p\}$ de A et telle que $f_\pi = s_p^2$. Chaque classe A_i est manifestement permise donc incluse dans une classe saturée S_i. L'ensemble $\{S_1, S_2, \ldots S_p\}$ est un recouvrement de A d'ordre p.

Réciproquement soit un recouvrement $\{S_1, S_2, \ldots S_p\}$ d'ordre minimum p par des classes saturées S_i. On peut supposer que ce recouvrement est irrédondant en ce sens que : $\forall i = 1, 2, \ldots p$, $S_i \not\subset \bigcup_{j \neq i} S_j$ (sinon p n'est pas minimum).

Considérons la partition de A : $\{A_1, A_2, \ldots, A_p\}$ définie par :

$$A_1 = S_1 \quad \text{et par récurrence} \quad A_i = S_i - \bigcup_{k<i} A_k.$$

Il s'agit d'une partition : en effet (1) $A_i \neq \phi$ sinon $S_i \subset S_1 \cup S_2 \ldots \cup S_{i-1}$ (2) $A_i \cap A_j = \phi$ trivialement et (3) $A_1 \cup A_2 \cup \ldots \cup A_p = A$ sinon $S_1 \cup S_2 \ldots \cup S_p \neq A$.

Considérons alors p variables t_i et une réduction π telle que :

$$x \notin A \rightarrow x_\pi = x$$

$$x \in A_i \rightarrow x_\pi = t_i$$

Montrons alors que $f_\pi = s_p^2$. Soit $e_1, e_2, \ldots, e_p$ les atomes de 2^p correspondants à $t_1, t_2, \ldots, t_p$.
Démontrer que $f_\pi = s_p^2$ est équivalent à démontrer que $f_\pi(e_i) = 0$ et $f_\pi(e_i + e_j) = 1 \quad (i \neq j)$.

Or $f_\pi(e_i) = f(X_{A_i}) = 0$ car A_i est permise (contenue dans S_i) et $f_\pi(e_i + e_j) = f(X_{A_i \cup A_j})$. Le résultat est 1 sinon $A_i \cup A_j$ est classe permise donc contenue dans une classe saturée S et alors l'ensemble

$$\{S_1, S_2, \ldots, S_{i-1}, S_{i+1}, \ldots, S_{j-1}, S_{j+1}, \ldots, S_p, S\}$$

est un recouvrement d'ordre p - 1 de A.
C'est un recouvrement car ou bien a $\in$ A appartient à A_k ($k \neq i$ et $k \neq j$) donc à S_k ou bien a appartient à l'une des classes A_i, A_j donc à S. Le résultat est donc absurde et cela suffit à prouver que $f_\pi = s_p^2$.

Compte tenu alors des résultats de la proposition (I 2.2) p est bien l'indice de f.

Corollaire 1 :

L'indice de f est le plus petit entier p tel que $\bar{1} = X_1 + X_2 + \ldots + X_p$ avec $f(X_i) = 0$.
Cela résulte de l'isomorphisme entre 2^n et 2^A.

Corollaire 2 (Critère de Post) :

Désignons par C_p ($p \geq 1$) la condition pour une fonction f d'être telle que tout ensemble de p monômes du polynôme f a au moins une lettre commune ; alors

f est d'indice p si et seulement si sa duale f^* satisfait le condition C_{p-1} et non la condition C_p.

En effet à partir de tout recouvrement d'ordre p de A par des classes saturées on déduit puisque $A = S_1 \cup S_2 \cup \ldots \cup S_p$ que $\phi = \complement_A A = \complement S_1 \cap \complement S_2 \ldots \cap \complement S_p$; or les $\complement S_i$ peuvent être assimilés à des monômes irréductibles de la duale f^*.
Donc f^* ne satisfait pas la condition C_p. Réciproquement si f^* ne satisfait la condition C_p alors il existe un recouvrement d'ordre p de A par des classes saturées. Cela suffit à démontrer ce critère.

C'est à partir de ce critère que Post a défini les familles MS_p.

Remarque :

- Si A est le support de f et si $B \supset A$, les monômes μ_i de la duale f^* ne contiennent que des lettres de A. Appelons classe saturée généralisée de f par rapport à B toute partie complémentaire par rapport à B des lettres de μ_i. Une telle classe généralisée contient donc toutes les lettres de B étrangères à A et le critère de recouvrement de B est encore valable.

- Lorsque f = 0, alors $f^* = 1$ et peut être considéré comme n'ayant qu'un monôme (vide de lettres). Alors la seule classe saturée généralisée de f par rapport à un ensemble B (non vide) est B elle même. Le critère fondamental donne comme indice 1. Nous serons donc amenés à considérer (et cela se vérifiera par la suite dans d'autres critères) que 0 est d'indice 1.

- Enfin si la fonction f est atomique on constate alors que les monômes de f^* comportent tous une même lettre x et les parties complémentaires de ces monômes seront encore appelées classes saturées de f. Aucune de ces classes ne contient bien sûr x.

Nous terminerons ce paragraphe, en signalant une propriété des nombres caractéristiques.

Proposition :

Si f a pour indice p et si S est une classe permise de f, alors pour toute réduction π associée à S, f_π est d'indice p ou p + 1.

L'indice de f_π est au moins p.

Considérons une réduction π' de f à s_p^2 induisant la partition $(S_1, S_2, \ldots, S_p)$ du support de f. A partir du recouvrement disjoint $(S, S_1-S, S_2-S, \ldots, S_p-S)$ on peut extraire une partition permise du support de f d'ordre au moins p et au plus p + 1 (certaine classe S_i-S peut être vide). Soit π une réduction associée à S : $\pi(S) = s$; alors $(s, S_1-S, \ldots, S_p-S)$ est une partition permise de f_π d'ordre au plus p + 1. La proposition s'en déduit.

Conséquence :

Si p est l'indice de f et si q (> p) en est un nombre caractéristique, alors tout entier r tel que $p \leqslant r < q$ est nombre caractéristique de f.

Nous pouvons réduire f à s_q^2 (cette dernière ayant l'indice q) par une réduction π induisant la partition $(S_1, S_2, \ldots, S_k, \ldots S_q)$. Désignons par $\pi_1, \pi_2, \ldots, \pi_q$ des réductions associées respectivement aux classes $S_1, \ldots S_q$. On voit que $\pi = \pi_1 \pi_2 \ldots \pi_q$. Désignant par $f_1 = f_{\pi_1}$ et par $f_k = (f_{k-1})\,\pi_k$, on a la suite de réduites de f suivante :

$$f \xrightarrow{\pi_1} f_1 \xrightarrow{\pi_2} f_2 \quad \ldots \quad \xrightarrow{\pi_k} f_k \longrightarrow \quad \ldots \quad \xrightarrow{\pi_q} s_q^2$$

L'indice a chaque étape augmente au plus d'une unité et part de la valeur p pour atteindre la valeur q - A un certain stade f_k sera d'indice r et pourra être réduite (de même que f) à s_r^2.

1.3. Algorithme du calcul de l'indice.

Le critère fondamental fournit un moyen assez simple de déterminer l'indice d'une fonction booléenne croissante $\notin M\Sigma$, lorsqu'elle est donnée sous forme d'un polynôme booléen irréductible.

On calcule la duale (par développement d'une somme) sous forme irréductible et on aboutit (par passage au complémentaire) aux classes saturées : $S_1, S_2, \ldots, S_N$. A chaque classe saturée est associée une variable de marquage $s_1, s_2, \ldots s_N$, booléenne de telle sorte qu'entre l'ensemble de toutes les parties de $\{S_1, S_2, \ldots S_N\}$ et l'algèbre de Boole 2^N, il y ait isomorphisme. La fonction booléenne $(s_1, s_2 \ldots, s_n)$ définie par :

$\varphi = 1 \iff$ la partie correspondante de $\{S_1, \ldots S_N\}$ est un recouvrement de A (ensemble des variables de f) est une fonction booléenne manifestement croissante. Il est tout à fait évident que le plus petit degré des monômes de φ est l'indice de f. Cette fonction φ se détermine simplement. On considère toutes les variables de A. A chacune d'elle on associe les classes saturées la contenant et on forme la somme des lettres de marquage correspondantes. Le produit de toutes ces sommes donnera φ.

Exemple :

Soit $f(x, y, z, t) = x\,y\,z + x\,y\,t + z\,t$.

Le calcul donne :

$$f^* = (x + y + z)\,(x + y + t)\,(z + t) = x\,z + x\,t + y\,z + y\,t + z\,t$$

Les classes saturées correspondantes sont :

$x\,z \rightarrow \{y, t\}$	notée par la variable	s_1
$x\,t \rightarrow \{y, z\}$	" "	s_2
$y\,z \rightarrow \{x, t\}$	" "	s_3
$y\,t \rightarrow \{x, z\}$	" "	s_4
$z\,t \rightarrow \{x, y\}$	" "	s_5

Pour couvrir : x il faut $s_3 + s_4 + s_5$
y il faut $s_1 + s_2 + s_5$
z il faut $s_2 + s_4$
t il faut $s_1 + s_3$

Le calcul de $(s_3 + s_4 + s_5)(s_1 + s_2 + s_5)(s_2 + s_4)(s_1 + s_3)$ donne
$s_1 s_4 + s_2 s_3 + s_1 s_2 s_5 + s_3 s_4 s_5$.
Il y a 4 recouvrements irrédondants de {x, y, z, t} dont deux d'ordre deux.
L'indice f est deux.

Nous noterons finalement que le calcul de l'indice revient à répéter la procédure fondamentale de développer un produit de sommes c'est-à-dire un calcul de duale.

1.4. Indice des fonctions symétriques.

On connait toutes les fonctions croissantes strictes symétriques de n variables. Ce sont les fonctions s_n^p ($1 \leqslant p \leqslant n$) dont le polynôme est constitué de la somme de tous les monômes de degré p (en nombre de C_n^p).

Donc ses points de 1ère espèce sont tous les points de hauteur p dans l'algèbre de Boole 2^n. (La hauteur d'un point $X \in 2^n$ est le nombre de 1 de X). Il en résulte que tout point Y de hauteur p - 1 est tel que $s_n^p(Y) = 0$, et en outre $Z > Y \quad s_n^p(Z) = 1$. Donc les points Y sont de deuxième espèce et ce sont les seuls car tout autre point est comparable à un point de hauteur p - 1. Il en résulte que les classes saturées de $s_n^p (p > 1)$ sont constituées de toutes (et seulement toutes) les classes à p - 1 éléments.

Nous pouvons alors montrer :

Proposition 1 :

La fonction symétrique s_n^p ($p > 1$) a pour nombre caractéristique q si et

seulement si on peut trouver une décomposition de n en la somme $\sum_{i=1}^{q} n_i$, les n_i vérifiant : (a) $1 \leqslant n_i \leqslant p-1$ (b) $n_i + n_j \geqslant p$ $(i \neq j)$.

La démonstration résulte du fait que les q classes $A_1, A_2, \ldots, A_q$ associées à une réduite s_q^2 de s_n^p vérifient : (a) A_i non vide et permise (b) $A_i \cup A_j$ $(i \neq j)$ est non permise. Réciproquement.

Nous pouvons alors déterminer tous les nombres caractéristiques de s_n^p.

Notations :

x et y étant deux entiers positifs x ⁄. y désignera le quotient de x par y.

Proposition 2 :

Les nombres caractéristiques de la fonction symétrique s_n^p sont les entiers compris entre $(n + p - 2)$ ⁄. $(p - 1)$ et n ⁄. p' si $p = 2p'$ ou $(n + 1)$ ⁄. p' si $p = 2p' - 1$.

Supposons en effet que nous ayons q entiers $n_1, n_2, \ldots n_q$ vérifiant les conditions (a) et (b). Supposons que $n_q = h$ est l'un des plus petits et posons $k = \inf (n_1, n_2, \ldots n_{q-1})$ $(k \geqslant h)$.

La condition (b) s'exprime par $h + k \geqslant p$.
Comme chaque $n_i \leqslant p - 1$ on a $n \leqslant q(p - 1)$. Le plus petit entier q vérifiant cette dernière inégalité sera tel que : $q(p - 1) = n + r_1$ avec $0 \leqslant r_1 \leqslant p - 2$; ce qui en posant $r_1 = p - 2 - r$ (avec $0 \leqslant r \leqslant p - 2$) donne
$n + p - 2 = q(p - 1) + r$.

Par ailleurs $n \geqslant k(q - 1) + h$ avec $h + k \geqslant p$.
Donc $k\,q \leqslant n + k - h \leqslant n + 2k - p$ et donc $q \leqslant (n + 2k - p)/k$.

Le second membre est une fonction décroissante de k or puisque $k + k \geqslant p$ il est évident que la plus petite valeur de k sera p' si $p = 2p'$ ou $p = 2p' - 1$.

Si $p = 2p'$ alors $q \leqslant (n + 2p' - 2p') / p' = n/p'$

Si $p = 2p' - 1$ alors $q \leqslant (n + 2p' - 2p' + 1) / p' = (n + 1) / p'$

Cela suffit à montrer les bornes possibles de q.

Les bornes sont atteintes. Désignons les par ν et μ. Nous avons $n = (p - 1)(\nu - 1) + r$ avec $1 \leqslant r \leqslant p - 1$. Considérons $\nu - 1$ classes à $p - 1$ éléments chacune et la $\nu^{ème}$ classe à r éléments. On vérifie les conditions de la proposition 1.

Si $p = 2p'$ alors $n = \mu p' + t$ $(0 < t < p')$. Considérons $\mu - 1$ classes à p' éléments et la $\mu^{ème}$ classe à $p' + t$ ($< p - 1$) éléments. On vérifie les conditions de la proposition 1.

De la même manière si $p = 2p' - 1$ nous avons $n + 1 = p'\mu + r$ avec $0 < r < p' - 1$ donc $n = p'\mu + r - 1$. On considère alors $\mu - 1$ classes à p' éléments, et une $\mu^{ème}$ à $p' + r - 1$ éléments.

Nous avons vu enfin (conséquence 1.3) que tout entier q tel que $\nu < q < \mu$ était nombre caractéristique de s_n^p. Nous allons l'établir directement.

Désignons dans tous les cas par p' la valeur correspondante à $p = 2p'$ ou $p = 2p' - 1$; on voit que les solutions extrêmes correspondent :

- la plus petite à $(\nu - 1)$ classes de $p - 1$ éléments, plus une classe à θ éléments $(1 \leqslant \theta \leqslant p - 1)$.

- la plus grande à $(\mu - 1)$ classes à p' éléments plus une classe à ρ éléments $(1 \leqslant \rho \leqslant p - 1)$.

Considérons alors $q - 1$ classes à p' éléments, plus une classe à ρ éléments. Les variables restantes peuvent être réparties parmi les $q - 1$ classes sans que celles-ci excèdent le nombre $p - 1$. En effet $q - 1 \geqslant \nu$ et par conséquent $(q - 1)(p - 1) \geqslant n$ ce qui prouve que c'est possible. Le partage que l'on obtient ainsi à q classes et vérifie les conditions de la proposition 1.

Exemple :

La fonction s^8_{36} a pour nombres caractéristiques les entiers compris entre $(36 + 6) \div 7 = 6$ et $36 \div 4 = 9$. Son indice est donc 6. On peut réduire s^8_{36} à S^2_8. Partons de 8 classes à 4 éléments, et rajoutons un élément au 4 premières. On répartit ainsi les 36 variables conformément à la proposition précédente.

Corollaire :

L'indice de s^p_n est l'entier $(n + p - 2) \div (p - 1)$.

2) Critère récursif. Applications.

Nous allons définir un critère récursif que nous utiliserons par la suite.

2.1. Critère récursif.

Définition :

S étant une partie de A, ensemble support d'une fonction croissante stricte f, on appelle reste de f par rapport à S, la fonction booléenne obtenue en annulant les variables S dans f(A).

Si S = A le résultat est évidemment nul.

Dans tous les cas le support du reste est contenu dans A - S, cette inclusion pouvant être stricte. Le support du reste peut être même vide même si A - S ne l'est pas.

Exemple : $f = a\,b + a\,c + e\,d$

le reste par rapport à {b, c, d} est 0

Lemme I :

Si l'indice du reste de la fonction croissante stricte f de support A, par rapport à une classe saturée S, est p alors p + 1 est un nombre caractéristique de f.

Posons $A = \{S, B\}$ l'ensemble des variables de f où $B = \{a, b, \ldots, \ell\}$. Désignons également par σ le monôme produit des variables S. Dire que S est classe saturée c'est dire que tout monôme construit à partir de lettres S n'est pas compatible avec f. Par contre les monômes σa, $\sigma b, \ldots \sigma\ell$ le sont. Il en résulte que :

$$f(A) = \sigma(a + b + \ldots + \ell) + \Sigma\, \sigma_i\, \beta_i + r$$

est une expression polynômiale (peut être non irréductible) de f, et où l'expression $\Sigma\, \sigma_i\, \beta_i$ représente une somme de monômes ayant à la fois des lettres dans S et B, r étant reste de f par rapport à S. Réduisons alors les variables S en une seule $s(\notin B)$. On obtient :

$$f_\pi(s, B) = s(a + b + \ldots + \ell) + r$$

(Chaque terme $\sigma_i\, \beta_i$ donne $s\, \beta_i \leqslant s(a + b + \ldots + \ell)$)

Il est évident alors, puisque r peut se réduire à $s_p^2(a_1, a_2, \ldots, a_p)$ que f_π peut se réduire à :

$$s(a_1 + a_2 + \ldots + a_p) + s_p^2(a_1, a_2 \ldots, a_p) = s_{p+1}^2(s, a_1 \ldots a_p)$$

Remarques :

Si f est atomique et contient donc le monôme du premier degré x, nous avons vu (remarques I.2) que la classe saturée S (conventionnelle) ne contient pas x et donc le reste de f par rapport à S est d'indice ∞. Le lemme reste donc valable dans ce cas.

- De même si le reste de f par rapport à S est nul, la réduction des variables S donne $f_\pi = s(a + b + \ldots + \ell)$ et f peut se réduire à s.a (a donc pour indice 2). Le lemme reste donc valable avec la convention déjà introduite que la fonction 0 pouvait être considérée comme d'indice 1.

Lemme 2 :

Soit f une fonction croissante stricte, d'indice fini p, de support A. Pour toute réduction π de f à s_p^2, induisant la partition $\{A_1, A_2, .., A_p\}$ de A on peut substituer p réductions π_i (i = 1, 2..p) ayant pour partitions associées $\{A_1^i, A_2^i, \ldots, A_p^i\}$ telles que :

(a) A_i^i est une classe saturée contenant A_i

(b) $A_j^i = A_j - A_i^i \cap A_j$ $(i \neq j)$

(c) $f_{\pi_i} = s_p^2$

Nous montrerons que chaque ensemble $\{A_1^i, A_2^i, \ldots, A_p^i\}$ est une partition de A.

Il est évident que $\bigcup_{j=1}^{p} A_j^i = A$.

Par ailleurs $A_j^i \neq \phi$ (cela est vrai si j = i). Si pour $j \neq i$, $A_j^i = \phi$ alors $A_i^i \cap A_j = A_j$ et par conséquent $A_i \cup A_j \subseteq A_i^i$ par suite $f(X_{A_i \cup A_j}) = 0$ et f_π serait différente de s_p^2.

Enfin $A_j^i \cap A_{j'}^i = \phi$ (si $j \neq j'$) ceci par construction.

Nous pouvons donc trouver une réduction π_i ayant cette partition associée. Montrons que $f_{\pi_i} = s_p^2$.

Or $f(X_{A_j^i}) = 0$ car $A_j^i \subseteq A_j$ et $f(X_{A_j}) = 0$.

Donc f_{π_i} n'est pas atomique et comporte p variables au plus. Comme p est l'indice de f cela entraîne que f_{π_i} est la fonction s_p^2.

Critère récursif.

Soit f une fonction croissante stricte et soit $\{S_1, S_2, \ldots, S_q\}$ l'ensemble des classes saturées contenant une variable arbitrairement choisie x du support A de f. Désignant par f_i le reste de f par rapport à S_i et par p_i son indice, alors l'indice p de f est égal à $\inf(p_i) + 1$.

Le lemme 1 nous dit que les nombres $p_i + 1$ sont des nombres caractéristiques de f. Donc l'indice p de f vérifie $p \leqslant \inf(p_i) + 1$.

Considérons une réduite f_π de f à s_p^2 de partition associée $\{A_1, A_2, \ldots, A_p\}$. Supposons que la variable x appartienne à la classe A_1. On peut substituer (lemme 2) une réduction π' avec $f_{\pi'} = s_p^2$ et telle que la partition associée $\{A'_1, A'_2, \ldots, A'_p\}$ contienne $A'_1 \supseteq A_1$ comme classe saturée. Confondant alors dans un premier temps les variables A'_1 à x, $s_p^2 = f_\pi$, est la réduite de $x(a + b + \ldots + \ell) + r$. Mais r est alors le reste de f par rapport à A'_1 (classe saturée contenant x). Son indice est donc un des nombres p_i. Il est évident alors que $x(a + b + \ldots + \ell) + r$ a pour indice $p_i + 1$; donc $p = p_i + 1 \geqslant \inf(p_i) + 1$.

Cela suffit à la démonstration.

Conséquence :

Si p est l'indice ($\neq 1$) de f croissante stricte, les restes de f par rapport aux classes permises ne peuvent avoir que les indices p ou p - 1 et l'un des restes au moins a pour indice p - 1.

En effet chaque reste $\varphi \leqslant f$; donc $\nu(\varphi) \leqslant p$; par ailleurs chaque reste est supérieur ou égal à un reste par rapport à une classe saturée et donc $\nu(\varphi) \geqslant p - 1$ (par suite du critère) ; enfin un reste au moins a pour indice p - 1 (par rapport à une classe saturée) ainsi qu'il résulte également de ce critère.

2.2. Indice d'une composition disjointe. Autre application.

Proposition 1 :

Si p et q sont les indices respectifs de f(u, X) et g(Y). Si la composée f[g(Y), X] est disjointe, son indice est soit p si $p \leqslant q$ soit le même que celui du reste de f par rapport à u si $q < p$.

La première partie est évidente car si $p \leqslant q$ les fonctions f et g appartiennent à MS_p de même que leur composée. Or Y est classe permise de $f \overset{u}{\circ} g$. La réduction des variables Y à u donne une réduite d'indice p.

La deuxième partie résulte d'abord du fait que $f(g(Y), X) \geqslant f(0, X)$ et donc l'indice de $f \overset{u}{\circ} g$ est au moins égal à celui du reste de f par rapport à u. Il est en fait égal. En effet posons $f = u\,h + k$; alors $f \overset{u}{\circ} g = g.h + k$ les supports de g, d'une part et de h et k étant disjoints ; soit r (p ou p - 1) l'indice du reste k.

On peut réduire k à $s^2_r(x_1, x_2, \ldots, x_r)$ et g à $s^2_q(y_1, y_2, \ldots y_q)$; $f \overset{u}{\circ} g$ se réduit alors à $s^2_q(y_1, y_2, \ldots y_q)\ \tilde{h} + s^2_r(x_1\ x_2 \ldots x_r)$. Comme $q < p$ donc $q \leqslant r$, on peut réduire respectivement y_1 à x_1, y_2 à $x_2, \ldots$, y_q à x_q.

On obtient :

$$s^2_q(x_1, x_2 \ldots x_q)\ \tilde{\tilde{h}} + s^2_r(x_1\ x_2 \ldots x_r)$$
$$= s^2_r(x_1, x_2, \ldots, x_r)$$

Nous allons démontrer une proposition qui nous sera utile par la suite.

Proposition 2 :

Supposons que deux fonctions f et g d'indices respectifs p + 1 et p aient une variable u commune à leur support et même reste k par rapport à cette variable.

Alors il existe une réduction π telle que :

(a) $\underline{f}_\pi = s^2_{p+1}(u, x_1, x_2, \ldots, x_p)$

(b) $\underline{g}_\pi \leqslant u\,(x_1 + x_2 + \ldots + x_{p-1}) + s^2_p(x_1, x_2, \ldots x_p)$

Nous poserons $f = u\,h + k$ et $g = u\,h_1 + k$.

Le reste k est d'indice p + 1 ou p. Il est d'indice p car $k \leqslant g$.

Considérons une réduction π_1 telle que $g_{\pi_1} = s_p^2(x_1, x_2, .. x_p)$. Cette réduction a induit une partition en p classes, sur le support {u, X} de g. Supposons que u appartienne à la p-ème classe de sorte que cette partition peut être écrite $\{X_1, X_2, \ldots, X_{p-1}, u\, X_p\}$.

L'ensemble $X_p \neq \phi$ sinon $\{X_1, X_2, .., X_{p-1}\}$ est une partition d'ordre $p - 1$ du support de k, formée de classes permises généralisées pour k et l'indice de k ne serait pas p. Donc à la partition $\{X_1, X_2 \ldots, X_p\}$, on peut associer une réduction π telle que $k_\pi = s_p^2(x_1, x_2, \ldots, x_p)$ et $u_\pi = u \neq x_1$. Alors $f = u\,h + k$ se réduit forcément selon π à $s_{p+1}^2(u, x_1, x_2, \ldots x_p)$ car h ne peut se réduire à 1 et f est d'indice $p + 1$; cependant $g = u.h_1 + k$ se réduit au plus à :

$$u(x_1 + x_2 + .. + x_{p-1}) + s_p^2(x_1, x_2, .. x_p)$$

(On peut continuer en effet à réduire u à x_p).

3) Application de la notion d'indice aux nombres chromatiques.

3.1. Nombre chromatique d'un graphe. Indice de la fonction booléenne associée.

La notion de nombre chromatique d'un graphe peut être introduite seulement pour les graphes symétriques. Nous rappellerons donc :

Définition 1 :

Un graphe symétrique (ou complexe linéaire [29]) est un ensemble fini A muni d'une relation binaire γ symétrique et jamais reflexive.

De manière équivalente on peut dire qu'un graphe est la donnée d'un couple (A, K) où A est un ensemble fini dont les éléments sont appelés les sommets et K est une partie de 2^A constituée de parties de A à deux éléments. Les éléments de K s'appellent les arêtes.

On représente topologiquement un graphe dans R^3 en associant aux éléments de A des points (distincts) et en joignant par un arc de Jordan deux points dès qu'ils sont dans la relation γ. Ces points seront dits adjacents. On admettra que cette réalisation est toujours possible de manière que deux arcs distincts n'aient aucun point en commun en dehors de leurs extrémités.

Un graphe est dit planaire, si une telle réalisation topologique peut se faire dans R^2.

Définition 2 :

Le nombre chromatique d'un graphe (A, K) est le plus petit entier naturel p, tel qu'on puisse affecter à chaque sommet un entier $i \in \{1, 2, \ldots, p\}$ de telle sorte que deux sommets adjacents quelconques aient des affectations (de manière plus imagée des colorations) distinctes.

Définition 3 :

Un ensemble intérieurement stable [7] d'un graphe (A, K) est une partie $S \subseteq A$ telle que deux éléments distincts quelconques de S ne sont jamais adjacents.

La notion d'ensemble intérieurement stable maximal (par inclusion) s'en déduit naturellement.

Proposition 1 :

Le nombre chromatique d'un graphe (A, K) est le plus petit des ordres des recouvrements de A par des ensembles intérieurement stables de (A, K).

Les ensembles stables peuvent être pris maximaux.

Cette proposition est tout à fait évidente si l'on constate que pour une coloration permise d'un graphe au moyen de p couleurs, l'ensemble S_i des sommets ayant la couleur i est un ensemble intérieurement stable de (A, K).

Cette proposition n'est autre (aux termes près) que celle du critère fondamental. Nous allons le voir plus précisément.

Fonction booléenne croissante associée à un graphe symétrique.

Soit un graphe (A, K). Associons à chaque sommet une variable booléenne indépendante. Nous assimilerons ainsi les n sommets A à l'ensemble de ces variables booléennes.

Soit $\gamma(A)$ la fonction booléenne complètement spécifiée par :

$\gamma(X) = 1 \iff S_X$ (L'ensemble des sommets de valeur 1 dans X) contient au moins une paire de sommets adjacents.

Il est tout à fait évident que $\gamma(A)$ est une fonction booléenne croissante (stricte si le graphe a des arêtes).

Proposition :

Les points caractéristiques de première espèce de la fonction booléenne $\gamma(A)$ associée au graphe (A, K) sont les points de hauteur deux correspondants aux paires de sommets adjacents. Les points caractéristiques de deuxième espèce correspondent aux ensembles de sommets intérieurement stables maximaux du graphe (A, K). Il en résulte que l'indice de $\gamma(A)$ n'est autre que le nombre chromatique du graphe.

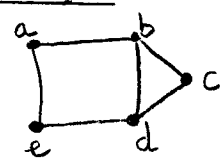
Considérons tous les somments X_i de hauteur deux associés aux paires de sommets adjacents. Il est évident que $\gamma(X_i) = 1$ et $Y < X_i \Longrightarrow \gamma(Y) = 0$ (Y est au plus de hauteur 1). Donc les points X_i sont de $1^{ère}$ espèce. Par ailleurs si $\gamma(X) = 1$, c'est que l'ensemble S_X contient au moins une paire de sommets adjacents, donc $X \geq X_i$ pour un i au moins. Donc les points X_i sont tous les points caractéristiques de première espèce.

Si $\gamma(Y) = 0$, de la même manière, c'est que S_Y est intérieurement stable ; si en outre $X > Y \Rightarrow \gamma(X) = 1$ c'est que S_Y est intérieurement stable maximal. Il en résulte (avec la propriété précédente et le critère fondamental) que l'indice de $\gamma(A)$ n'est autre que le nombre chromatique du graphe.

Nous retrouvons grâce à cette proposition, un moyen de déterminer tous les ensembles intérieurement stables d'un graphe. Ce résultat est très voisin de celui démontré dans [18] mais beaucoup plus synthétique.

Exemple :

Fig 1



Considérons le graphe de la figure 1.
La fonction croissante associée est

$\gamma(a, b, c, d, e) = ab + bc + cd + de + ea + bd$

Cherchons les ensembles intérieurement stables maximaux. Nous calculerons la duale :

$\gamma^*(a, b, c, d, e) = (a + b)(b + c)(c + d)(d + e)(e + a)(b + d)$

Nous obtenons après développement :

$\gamma^* = bce + bde + abd + acd$

Donc les ensembles intérieurement stables maximaux sont :

$\{a, d\} \leftarrow bce$, $\{a, c\} \leftarrow bde$, $\{c, e\} \leftarrow abd$, $\{b, e\} \leftarrow acd$

3.2. Notion de polygraphe.

Les fonctions booléennes croissantes associées ainsi aux divers graphes restent très particulières (homogènes, du second degré) et ne recouvrent pas toutes les fonctions croissantes. La théorie des familles, par contre, restreinte aux fonctions croissantes conduit naturellement à la notion d'indice applicable à toute fonction croissante. Cela suggère, l'extension de la notion de graphe à celle de polygraphe.

Définition :

On appelle polygraphe, la donnée d'un couple (A, K) (plus commodément désigné par K(A)) tel que

A est un ensemble fini de sommets, $K = \{K_1, K_2, .., K_q\}$ est un ensemble de parties de A.

Les éléments de K s'appelleront simplexes (ou encore noeuds, ou encore n - triangles si $|K_i| = n$; on peut en effet trouver un espace R^q avec q suffisamment grand pour plonger ce polygraphe comme un complexe simplicial).

Le polygraphe est dit nul si K est vide.

Le polygraphe est dit simple si $i \neq j \Longrightarrow K_i \not\subset K_j$.

On simplifie un polygraphe en ne gardant dans K que les simplexes minimaux. On obtient un polygraphe simple.

Si un simplexe de K est vide, le polygraphe est dit unité.

Si un simplexe de K comporte un seul sommet le polygraphe sera dit atomique.

Si tous les simplexes de K ont exactement deux éléments, on a un graphe symétrique.

On associe à un polygraphe, la fonction croissante ayant A comme ensemble de variables et pour monômes les produits des variables de chaque simplexe K_i. Cette fonction sera notée K(A) comme le polygraphe.

Le polygraphe est simple si les monômes sont premiers. Les polygraphes simples peuvent donc être assimilés aux fonctions croissantes.

On peut associer un réseau (pour avoir une représentation concrète d'un polygraphe).

On représente les sommets par des points, les simplexes par des ronds. On joint par arc un simplexe à tous les sommets qu'il contient

Exemple : $K(A) = abc + bcd + ad$

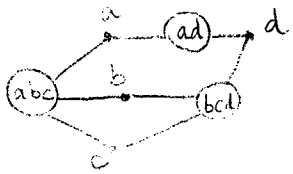
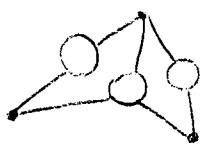


Fig2

Cette représentation donne le graphe associé lorsque le polygraphe est un graphe. (Les ronds sont alors des arêtes).

Simplifier un polygraphe c'est sur la représentation par réseau associé, supprimer les simplexes S tel qu'il existe un autre simplexe ayant tous ses sommets dans ceux de S.

Exemple :



se simplifie en :

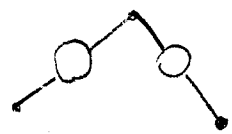


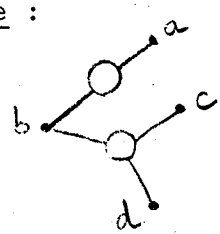
Fig. 3

Nous ne considérerons par la suite que des polygraphes simples.

Ordre entre polygraphes.

Un polygraphe K(A) est inférieur ou égal à un polygraphe L(A) si à tout simplexe K_i de K on peut trouver un simplexe L_j avec $K_i \supseteq L_j$.

Exemple :



est inférieur à

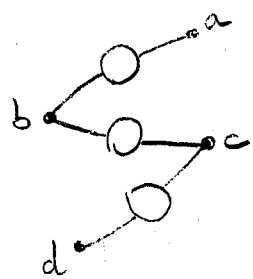


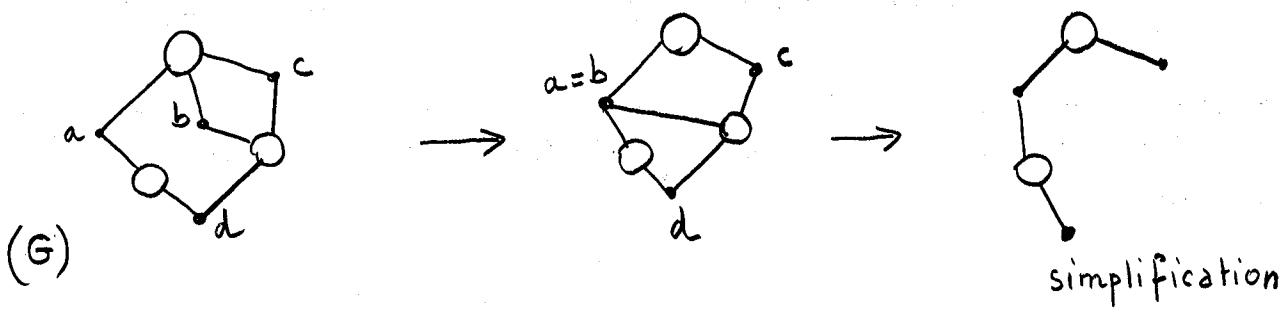
Fig. 4

Réduction et composition de polygraphes.

La réduction et la composition (disjointe) entre fonctions booléennes, peut désormais s'interpréter en termes de polygraphe.

La réduction consiste à confondre des sommets et simplifier ensuite, le polygraphe.

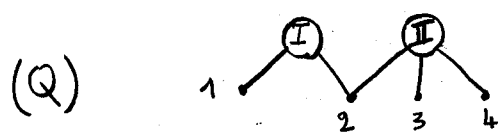
Exemple :



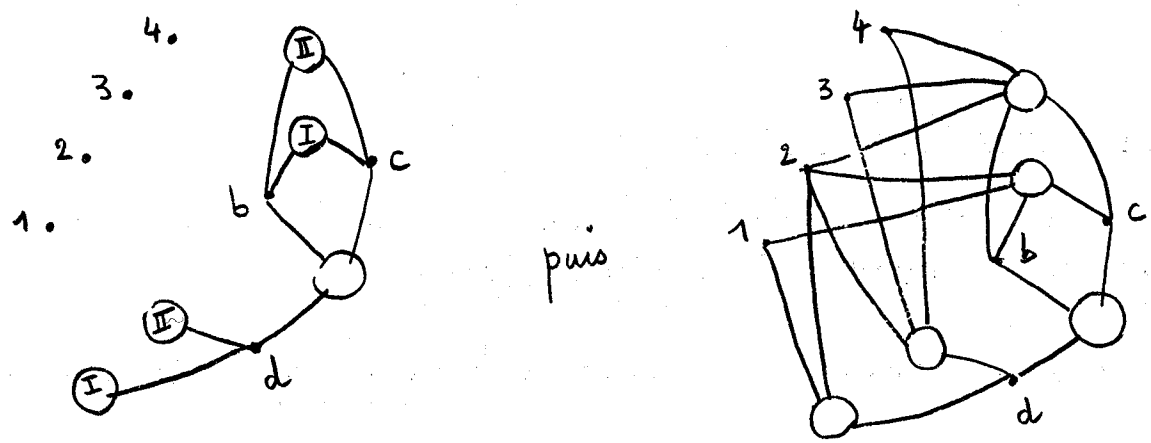
La composition disjointe peut aussi s'interpréter (de manière légèrement plus compliquée). Soit a un sommet du polygraphe G et K, L,.., M les simplexes contenant a. On substitue à a un polygraphe Q ayant p simplexes Q_1, Q_2,.. Q_p et n sommets. On supprime de G le sommet a et ses liaisons et on rajoute les n nouveaux sommets ; on prend pour chaque simplexe K, L,.. M, p répliques et on joint la i-ème réplique K_i respectivement aux sommets qui étaient contenus dans Q_i.

Exemple :

Prenons le polygraphe G précédent et soit Q le polygraphe :



Nous avons pour construire G $\overset{a}{\circ}$ Q les étapes :



Le nombre chromatique d'un polygraphe K(A) sera par définition l'indice de la fonction K(A). Il peut s'interpréter comme le plus petit entier p tel que l'on puisse colorier les sommets avec p couleurs de manière que les couleurs affectées aux sommets de chaque simplexe soient au moins en nombre de deux.

3.3. Applications de la théorie des familles à la théorie des graphes. Génération des graphes p-chromatiques. Conjecture des quatre couleurs.

On sent, obscurément, un lien entre les graphes p-chromatiques et les graphes complets d'ordre p (qui sont p-chromatiques). Pourtant ce lien n'a jamais été mis en évidence de manière claire. Toute tentative à ce sujet a été caduque. Un graphe p-chromatique n'a aucune raison de contenir un sous-graphe complet d'ordre p. On démontre même [24] que pour tout couple d'entiers p, q tels que $p \geqslant q > 1$, on peut construire un graphe p-chromatique tel que tout sous-graphe complet est au plus d'ordre q. On comprend dès lors la difficulté de ce lien possible. La théorie des familles le met clairement en lumière. Tout graphe p-chromatique (pour $p \geqslant 4$) est engendrable par compositions et réductions, à partir du seul graphe complet d'ordre p.

Il est peut être enfin intéressant d'envisager, grâce à la théorie des familles et compte tenu de la propriété précédente, une conjecture équivalente à celle des 4 couleurs. En effet, d'après cette théorie, nous savons qu'à partir d'un graphe complet d'ordre p, il n'est pas possible d'engendrer des polygraphes (en particulier graphes) de nombre chromatique < p.

Définition :

On appelle polygraphe droit, tout polygraphe réductible à un polygraphe inférieur ou égal à un graphe planaire et polygraphe gauche tout polygraphe qui n'est pas droit.

Un graphe planaire, par définition est droit (il est son propre réduit inférieur ou égal à lui-même). Un graphe peut être non planaire et droit (si son nombre chromatique est $\leqslant 4$).

Proposition :

Sont équivalentes à la conjecture des quatre couleurs les deux propositions suivantes :

(a) le graphe complet d'ordre 5 ne peut engendrer de polygraphes droits

(b) L'ensemble des polygraphes gauches est une famille :

Soit C la conjecture des 4 couleurs. C $\Rightarrow$ (a) car un polygraphe engendré par S_5^2 a pour nombre chromatique au moins 5 et ne peut se réduire à un polygraphe inférieur ou égal à un graphe planaire 4 -chromatique d'après (C).
(a) $\Rightarrow$ (C) car un graphe planaire (étant droit par définition) ne serait pas engendré par s_5^2. Son nombre chromatique serait donc au plus 4.

Désignons par $\mathcal{G}$ l'ensemble des polygraphes gauches, nous avons par définition $\mathcal{G} \subseteq MS_5$ (un polygraphe gauche a forcément un nombre chromatique supérieur ou égal à cinq).

Si (a) est vérifié c'est que $MS_5 \subseteq \mathcal{G}$. Donc $MS_5 = \mathcal{G}$ et (b) est vérifié. Réciproquement si $\mathcal{G}$ est une famille, comme le graphe complet d'ordre 5 appartient à $\mathcal{G}$ et non celui d'ordre quatre c'est que $\mathcal{G} = MS_5$ et donc le graphe complet d'ordre 5 ne peut engendrer des polygraphes droits.

Suite à ce résultat on ne doit toutefois pas avoir trop d'illusions concernant la conjecture des quatre couleurs, car la difficulté réside dans la caractérisation plus poussée des graphes planaires.

Toutefois, il est tout à fait évident que $\mathcal{G}$ est stable vis à vis des réductions et qu'en outre si $f \in \mathcal{G}$ et si $g \geq f$ alors $g \in \mathcal{G}$.

CHAPITRE III

PROPRIETES ALGEBRIQUES DES FONCTIONS CROISSANTES, EN RELATION AVEC L'INDICE. APPLICATIONS A CERTAINS POLYNOMES COMBINATOIRES.

On considère l'ensemble MOI des fonctions croissantes, c'est-à-dire le treillis distributif libre, engendré par l'ensemble dénombrable $U = \{a_1, a_2, \ldots, a_n \ldots\}$, auquel on a rajouté les bornes universelles 0 et 1.

Notations :

A étant une partie finie de U ($A = \{a_1, a_2, \ldots, a_n\}$) on notera A^+ et $A^\cdot$ respectivement les éléments $a_1 + a_2 + \ldots + a_n$ et $a_1 a_2 \ldots a_n$ de MOI. Si A est vide, A^+ sera identifié à 0 et $A^\cdot$ à 1.

Nous noterons également $A^{(2)}$ l'élément $s_n^2 (a_1, a_2 \ldots, a_n)$ étant entendu que si $n = 0$ ou 1, $A^{(2)} = 0$.

1) Fonctions croissantes précisées. Couplage et somme. Transposition et co-transposition.

1.1. Fonctions précisées. Somme et couplage.

Définition :

On appelle fonction croissante précisée la donnée d'un couple (f, A), noté f<A> tel que (1) f ∈ MOI (2) A est une partie finie non vide de U, contenant le support de f.

La fonction précisée f<A> est dite exacte si support f = A

Remarques :

(a) La notion de fonction croissante précisée est utile lorsqu'on considère le polygraphe associé (certains sommets peuvent n'appartenir à aucun simplexe).

(b) Elle est également utile, sur un plan plus algébrique. A étant une partie non vide, finie de U, le treillis distributif libre engendré par A noté $\mathcal{L}$(A) peut très bien comporter des éléments dont le support est strictement inclus dans A. Pour de tels éléments f, il est commode d'avoir l'élément précisé f<A>.

(c) Se donner une fonction précisée, c'est se donner f<A> où f représente une fonction croissante. L'ensemble A étant connu, nous adopterons la notation f<A> = f.

Exemple : f<a, b, c> = a + b

(d) On peut définir un ordre entre fonctions précisées

f<A> $\leqslant$ g<B> si f $\leqslant$ g et A $\subseteq$ B

(e) Si $\mathcal{F}$ est une famille quelconque de fonctions croissantes, une fonction précisée f<A> est dite appartenir à $\mathcal{F}$ si f ∈ $\mathcal{F}$

(f) Désignant par $\mathcal{P}$ l'ensemble des fonctions croissantes précisées, l'ensemble MOI est le quotient de $\mathcal{P}$ par l'équivalence :

f<A> ≡ g<B> si f = g

Nous allons définir, la somme et le couplage de deux fonctions croissantes précisées.

Auparavant et afin d'alléger les notations, les parties finies non vides de variables seront notées par des majuscules et les éléments quelconques de ces parties par des minuscules correspondantes. Par exemple A, B désignant des parties finies non vides de U, la notation $\sum a.b$ désignera $\sum_{\substack{a\in A \\ b\in B}} ab$

Somme de fonctions croissantes précisées.

Etant données les fonctions croissantes précisées f<A> et g<B> on appelle somme la fonction précisée
h<C> = f<A> + g<B> telle que $h = f + g$ et $C = A \cup B$

Couplage de fonctions croissantes précisées.

On définit le couplage de f<A> et g<B> comme la fonction précisée
h<C> = f<A> × g<B> telle que $C = A \cup B$ et $h = f + g + \sum_{a\neq b} ab$

Exemple : f<a, b, c> = abc g<a, b, d> = bd
f<a, b, c> + g<a, b, d> = abc + bd
f<a, b, c> × g<a, b, d> = abc + bd + ab + ad + ba + bd + ca + cb + cd
= bd + ab + ad + ac + bc + cd

Proposition :

L'ensemble des fonctions croissantes précisées est un gerbier commutatif vis à vis des opérations de somme et couplage.

Les opérations sont internes, partout définies. La somme est manifestement commutative, associative, idempotente.

Le couplage est évidemment commutatif.

Il est associatif car :

$$f\langle A\rangle \times \left(g\langle B\rangle \times h\langle C\rangle\right) = f\langle A\rangle \times \left(g + h + \sum_{b\neq c} bc\right) \langle B \cup C\rangle$$

Désignons par $D = B \cup C$. On a alors :

$$f\langle A\rangle \times \left(g\langle B\rangle \times h\langle C\rangle\right) = f + g + h + \sum_{b\neq c} bc + \sum_{a\neq d} ad$$

$$= f + g + h + \sum_{b\neq c} bc + \sum_{a\neq b} ab + \sum_{a\neq c} ac$$ (grâce à l'idempotence en algèbre de Boole)

On voit la parfaite symétrie dans le résultat entre $f\langle A\rangle$, $g\langle B\rangle$ et $h\langle C\rangle$.

Il ne reste que la distributivité du couplage par rapport à la somme. Or :

$$f\langle A\rangle \times \left(g\langle B\rangle + h\langle C\rangle\right) = f + g + h + \sum_{a\neq b} ab + \sum_{a\neq c} ac =$$

$$= \left(f + g + \sum_{a\neq b} ab\right) + \left(f + h + \sum_{a\neq c} ac\right) = f\langle A\rangle \times g\langle B\rangle + f\langle A\rangle \times g\langle C\rangle$$

Remarque :

En démontrant l'associativité du couplage, on a pu constater que :
$f\langle A\rangle \times g\langle B\rangle \times h\langle C\rangle = f\langle A\rangle \times g\langle B\rangle + f\langle A\rangle \times h\langle C\rangle + g\langle B\rangle \times h\langle C\rangle$
Nous allons le généraliser.

Propriété de concentration.

Considérons n fonctions ($n \geqslant 3$) précisées $\varphi_1, \varphi_2, \ldots, \varphi_n$ et désignons par $\sigma_n^q(\varphi_1, \varphi_2, \ldots, \varphi_n)$ la somme de tous les couplages de q fonctions précisées distinctes prises parmi les n, ($q \leqslant n$).
Nous avons :

$$\sigma_n^2(\varphi_1, \ldots \varphi_n) = \sigma_n^3(\varphi_1, \ldots, \varphi_n) = \ldots = \sigma_n^n(\varphi_1, \varphi_2, \ldots \varphi_n)$$

Cette propriété se démontre par récurrence. Elle est vrai pour $n = 3$ (remarque précédente). Supposons la vraie pour $n - 1$.

Nous avons :

$$\sigma_n^q(\varphi_1, \varphi_2 \ldots, \varphi_n) = \varphi_1 \times \sigma_{n-1}^{q-1}(\varphi_2, \varphi_3, \ldots \varphi_n) + \sigma_{n-1}^q(\varphi_2, \ldots, \varphi_n)$$

Soit encore :

$$\sigma_n^q(\varphi_1, \ldots, \varphi_n) = \varphi_1 \times \sigma_{n-1}^2(\varphi_2 \ldots \varphi_n) + \sigma_{n-1}^3(\varphi_2, \ldots, \varphi_n) =$$

$$= \sigma_n^3(\varphi_1, \varphi_2, \ldots, \varphi_n)$$

Or :

$$\sigma_n^2(\varphi_1, \varphi_2, \ldots, \varphi_n) = \sigma_3^2(\varphi_1, \varphi_2, \varphi_3) + \sigma_3^2(\varphi_1, \varphi_2, \varphi_4) + \ldots\ldots\ldots$$

$$\ldots\ldots + \sigma_3^2(\varphi_{n-2}, \varphi_{n-1}, \varphi_n) \qquad (C_n^3 \text{ termes})$$

Cela donne encore :

$$\sigma_n^2(\varphi_1, \ldots, \varphi_n) = \varphi_1 \times \varphi_2 \times \varphi_3 + \varphi_1 \times \varphi_2 \times \varphi_4 + \ldots\ldots = \sigma_n^3(\varphi_1, \varphi_2, \ldots \varphi_n)$$

La propriété est démontrée.

1.2. Transposition et co-transposition des fonctions précisées.

Soit f une fonction croissante et f^* sa duale. Pour toute fonction précisée f<A>, la fonction précisée f^*<A> sera appelée la duale de f<A>.

Définition 1 :

Soit f<A> une fonction croissante précisée telle que le polynôme irréductible $f = \mu_1 + \mu_2 + \ldots + \mu_q$. Désignons par $A^\cdot/\mu_i$ le monôme produit des lettres appartenant à A et non à μ_i. On appelle f^s<A> la fonction précisée telle que $f^s = A^\cdot/\mu_1 + A^\cdot/\mu_2 + \ldots + A^\cdot/\mu_q$.

Remarque :

Lorsque $f = 0$ $f^S = 0$; lorsque $f = 1$ alors $f^S = A^*$

Propriétés :

① L'expression polynômiale de f^S est irréductible

② $f^{SS}\langle A\rangle = f\langle A\rangle$

Définition 2 :

On appelle transposée (resp. co-transposée) de $f\langle A\rangle$ la fonction $f^{*S}\langle A\rangle$ (resp. $f^{S*}\langle A\rangle$). On la note $f^T\langle A\rangle$ (resp. $f^{\perp}\langle A\rangle$).

Par la définition, il résulte que :

$f^{T\perp}\langle A\rangle = f^{\perp T}\langle A\rangle = f\langle A\rangle$

Remarque :

Les monômes de $f^T\langle A\rangle$ donnent les classes saturées généralisées de f par rapport à A. (Cf Remarques II 1.2).

Proposition :

Une condition nécessaire et suffisante pour que $f^T\langle A\rangle$ soit exacte est que $f \notin M\Sigma 1$.

C.N. Si f appartient à $M\Sigma 1$, cela peut vouloir dire que $f = 1$. Donc $f^T\langle A\rangle = f^{*S}\langle A\rangle = 0$ et donc : support $f^T \neq A$. Cela peut vouloir dire enfin que $f\langle A\rangle = a + \varphi$. Mais alors $f^T\langle A\rangle = (a.\varphi^*)^S$; aucun monôme de f^T ne contiendra a et $f^T\langle A\rangle$ ne serait pas exacte.

C.S. Supposons que $f\langle A\rangle \notin M\Sigma 1$.
Posons B = support f^T et $C = \complement_A B$.

Nous avons $f^{T}\langle A\rangle = g$

Si $g = 0$ alors $f^{*S}\langle A\rangle = 0$ donc $f^{*}\langle A\rangle = 0$ et $f\langle A\rangle = 1$; cela est absurde.

Si $g \neq 0$ et si $C \neq \phi$ alors $f^{S}\langle A\rangle = C^{\cdot}.g^{S}$; d'où $f\langle A\rangle = f^{\overline{\perp}}\langle A\rangle = f^{TS*}\langle A\rangle = C^{+} + (g^{S})^{*}$. Alors f appartiendrait à MΣ. Donc $C = \phi$ et $f^{T}\langle A\rangle$ est exacte.

Par dualité on démontrerait :

Une condition nécessaire et suffisante pour que $f^{\perp}\langle A\rangle$ soit exacte est que $f \in M\Pi O$.

2) Sommes et couplages directs. Théorème de Structure.

2.1. Somme et couplage directs. Indices associés.

La somme (ou le couplage) de $f\langle A\rangle$ et $g\langle B\rangle$ est dite directe si $A \cap B = \phi$.

Nous avons alors pour le couplage direct :

$$f\langle A\rangle \times g\langle B\rangle = f + g + A^{+}.B^{+}$$

Nous noterons que si f et g n'appartiennent pas à MΣ1 et sont définies par les polynômes irréductibles respectifs $\alpha_1 + \alpha_2 + .. + \alpha_q$, et $\beta_1 + \beta_2 + .. + \beta_r$ alors $f\langle A\rangle + g\langle B\rangle = \alpha_1 + \alpha_2 + .. + \alpha_q + \beta_1 + ... + \beta_r$

et $f\langle A\rangle \times g\langle B\rangle = \alpha_1 + .. + \alpha_q + \beta_1 + .. + \beta_r + A^{+}.B^{+}$
sont tels que les polynômes du second membre sont irréductibles ; α_i n'est pas multiple de β_j et vice versa. Aucun monôme α_i (comme β_i) n'est multiple d'un monôme a.b. Aucun monôme a.b n'est multiple d'un monôme α_i ou β_i (sinon α_i ou β_i est du 1er degré ou égal à 1).

Le résultat enfin n'appartient pas à MΣI.

Remarque :

Si f et g n'appartiennent pas à MΣI, le couplage direct f<A> × g<B> est une fonction précisée exacte.

La somme directe et le couplage direct de fonctions croissantes précisées, ont une importance vis à vis de l'indice, mise en lumière par le résultat suivant :

Proposition :

Si f<A> et g<B> sont des fonctions croissantes précisées d'indice p et q et si $A \cap B = \phi$ le couplage (direct) (resp. la somme directe) de ces fonctions a pour indice p + q (resp. sup (p, q)).

Nous écarterons le cas évident où l'une de ces fonctions est atomique. Le cas f = I ou g = I n'est pas prévu (l'indice de la fonction I n'est pas défini). Donc f<A> × g<B> est exacte. Toute classe saturée de ce couplage est une partie soit de A soit de B (exclusivement). On ne peut en effet confondre une variable $a \in A$ et $b \in B$ (ab se réduisant au Ier degré). Donc une telle classe saturée est une classe saturée généralisée de f<A> ou g<B> exclusivement. Réciproquement.

Donc tout recouvrement de $A \cup B$ par des classes saturées sous tend un recouvrement de A et B par des classes saturées généralisées de f<A> (resp g<B>) dont l'ordre est la somme des ordres correspondants. Par suite p + q est l'indice du couplage direct.

Quant à la somme directe, il est évident (chapitre I) que l'indice r de f<A> + g<B> est plus grand que p et q. Donc $r \geqslant \sup(p, q)$.
On peut trouver alors une réduction π amenant respectivement les supports de f et g sur

$X = \{x_1, x_2, .. x_p\}$ et $Y = \{y_1, y_2, .. y_q\}$ avec $X \cap Y = \phi$

et en outre $f_\pi = s^2_p (x_1 .. x_p)$, $g_\pi = s^2_q (y_1, .. y_q)$.

Supposons $p \geqslant q$ et réduisons y_i à x_i pour $i = 1, 2, .. q$. On obtient $s_p^2 (x_1, x_2 \ldots, x_p)$ réduite de $f\langle A\rangle + g\langle B\rangle$. Donc $r = \sup (p, q)$.

Remarque :

On peut définir l'ensemble $\tilde{\mathcal{P}}$ des fonctions précisées à un support près, les couplages et sommes étant toujours directs (au besoin on changerait le nom des supports). Les opérations de couplage et somme (directs) sont internes sur $\tilde{\mathcal{P}}$ et font de $\tilde{\mathcal{P}}$ un gerbier. L'ensemble N des entiers naturels 1, 2... est aussi un gerbier relativement aux opérations sup, et somme ordinaire. Le passage d'une fonction précisée (abstraite) $f \in \tilde{\mathcal{P}}$ à son indice est un homomorphisme de gerbier.

Suite à cette proposition il est intéressant de décomposer toute fonction précisée au moyen de sommes et couplages directs. Nous allons démontrer un théorème donnant la structure (unique) d'une fonction précisée.

2.2. Fonctions précisées irréductibles. Théorème de Structure.

Dans tout ce paragraphe les fonctions précisées sont supposées ne pas appartenir à $M\Sigma 1$. Dans le cas d'une seule variable, elle ne peut être que $0\langle a\rangle = 0$.

Définition :

Une fonction précisée croissante $f\langle A\rangle$ est dite connexe, simple si elle n'est d'aucune manière une somme directe (resp. couplage direct) de deux fonctions précisées.

Elle est dite irréductible si elle est à la fois simple et connexe.

Remarques :

Une fonction précisée connexe est exacte sauf la fonction nulle. En effet si $f\langle A\rangle$ est telle que $B = \text{support } f \subset A$ alors en désignant par C le complémentaire de B, on a $f\langle A\rangle = f\langle B\rangle + 0\langle C\rangle$.

Lemme I :

Une condition nécessaire et suffisante pour que $f\langle A\rangle$ soit simple et que $f^{T}\langle A\rangle$ soit connexe.

C.N. $f\langle A\rangle$ n'appartient pas à MΣI donc (prop I.2) $f^{T}\langle A\rangle$ est exacte. Si elle était non connexe alors $f^{T}\langle A\rangle = g\langle B\rangle + h\langle C\rangle$ avec $B \cup C = A \quad B \cap C = \phi$, les fonctions $g\langle B\rangle$ et $h\langle C\rangle$ étant exactes donc non nulles.
Par suite $f^{TS}\langle A\rangle = C^{\cdot}.g^{S}\langle B\rangle + B^{\cdot}.h^{S}\langle C\rangle$
(g^{S} et $h^{S} \neq 0$). Donc :

$$f\langle A\rangle = f^{TS*}\langle A\rangle = (C^{+} + g^{\perp}\langle B\rangle)\ (B^{+} + h^{\perp}\langle C\rangle).$$

Les fonctions $g^{\perp}$ et $h^{\perp}$ étant différentes de I on a
$g^{\perp}\ B^{+} = g^{\perp}$ et $h^{\perp}.C^{+} = h^{\perp}$ donc :

$$f\langle A\rangle = C^{+}.B^{+} + h^{\perp}\langle C\rangle + g^{\perp}\langle B\rangle = h^{\perp}\langle C\rangle \times g^{\perp}\langle B\rangle .$$

$f\langle A\rangle$ ne serait pas simple.

C.S. Supposons $f^{T}\langle A\rangle$ connexe. Si $f\langle A\rangle$ n'était pas simple
$f\langle A\rangle = g\langle B\rangle \times h\langle C\rangle \iff$ (g et h $\notin$ MΣI sinon f $\in$ MΣI). Donc

$$f\langle A\rangle = g + h + B^{+}.C^{+}$$

D'où :
$f^{*}\langle A\rangle = g^{*}.h^{*}.(B^{\cdot} + C^{\cdot})$. Les fonctions g^{*}, h^{*} n'étant pas nulles il vient :

$f^{*}\langle A\rangle = g^{*}.C^{\cdot} + h^{*}.B^{\cdot}$; g^{*} et h^{*} étant de support B et C disjoints, et étant définies par des polynômes irréductibles, le polynôme résultant est irréductible. Donc

$f^{T}\langle A\rangle = f^{*S}\langle A\rangle = g^{T}\langle B\rangle + h^{T}\langle C\rangle$. Cela est absurde.

Lemme 2 :

La fonction précisée f<A> ne peut être à la fois non simple et non connexe.

En effet $f<A> = g<B> + h<C>$ $\quad (B \cap C = \phi)$

et $f<A> = \ell<D> \times k<E> = \ell<D> + k<E> + D^{+}.E^{+}$ sont deux éventualités contradictoires. $(D \cap E = \phi)$

Une lettre b de B et une lettre c de C n'appartiennent pas à un même monôme de f. Ces lettres font partie donc d'une des deux classes D, E (par exemple D).

Comme $E \neq \phi$ on choisit une lettre e de E. Les monômes eb et ec font partie de f. Donc $e \in B$ et $e \in C$. Cela contredit $B \cap C = \phi$

Lemme 3 : Soit $f<A> \notin M\Sigma I$.

Si f<A> est non connexe, elle est somme directe (unique à l'ordre près) de fonctions précisées connexes $\notin M\Sigma I$.

Si f<A> est non simple, elle est couplage direct (unique à l'ordre près) de fonctions simples précisées $\notin M\Sigma I$.

On démontre seulement la première partie de ce lemme la deuxième s'en déduira par application du lemme I.

La démonstration est classique. On utilise la relation d'équivalence $\equiv$ sur A définie par :

$(a_1 \neq a_2)$, $a_1, a_2 \in A$: $a_1 \equiv a_2$ s'il existe une suite de monômes irréductibles $\mu_1, \mu_2 \ldots, \mu_q$ de f tels que : $a_1 \in \mu_1$, $a_2 \in \mu_q$, $\mu_i \cap \mu_{i+1} \neq \phi$.

Si f<A> est connexe alors $\forall a_1, a_2 : a_1 \equiv a_2$. La relation d'équivalence sur A définit un partage de A en classes $A_1, A_2, .., A_r$. La fonction f<A> est alors somme de fonctions précisées $f_1<A_1> + f_2<A_2> + ... + f_r<A_r>$; chacune étant connexe, est somme des monômes contenant les lettres de A_i.

Le résultat est unique évidemment.

Chaque fonction f_i n'appartient pas à MΣ! puisque f n'y appartient pas.

Théorème de structure.

Toute fonction croissante précisée f<A> (n'appartenant pas à MΣ!) peut se décomposer au moyen de couplages et sommes directs, à partir de fonctions précisées irréductibles. Le résultat est unique à l'ordre près des termes et des facteurs.

En effet si f<A> est irréductible c'est terminé. Sinon f<A> est exclusivement soit non simple, soit non connexe et se décompose donc en somme directe unique de termes (ou couplage direct unique de facteurs). Les nouvelles fonctions précisées obtenus ont strictement moins de variables et n'appartiennent pas à MΣ!. On reprend sur elles les opérations et on aboutit ainsi à des fonctions irréductibles.

Exemple :

f<x, y, z, t, u> = xy + yz + zt + tx + ux + uy + uz + ut

f est connexe. Le calcul donne :

f^*<x, y, z, t, u> = xzu + ytu + xyzt .

Soit encore :

f^T<x, y, z, t, u> = yt + xz + u

On a trois composantes connexes ; donc

$$f\langle x, y, z, t, u\rangle = xz^{\perp}\langle x, z\rangle \times yt^{\perp}\langle y, t\rangle \times u^{\perp}\langle u\rangle$$

$$= 0\langle x, z\rangle \times 0\langle y, t\rangle \times 0\langle u\rangle$$

On obtient finalement :

$$f\langle x, y, z, t, u\rangle = (0\langle x\rangle + 0\langle z\rangle) \times (0\langle y\rangle + 0\langle t\rangle) \times 0\langle u\rangle$$

3) Application au calcul de certains polynômes combinatoires associés à une fonction croissante précisée.

Nous supposerons que les fonctions précisées n'appartiennent pas à $M\Sigma|$.

3.1. Polynôme permis et définitif attaché à une fonction croissante précisée.

Soit $f\langle A\rangle$ une fonction croissante précisée. Pour toute réduction π, il correspond une partition de A dont l'ordre sera par définition le nombre de classes. Cette partition sera dite permise si $f_\pi \notin M\Sigma$. Elle sera dite définitive si $f_\pi = s_p^2$ et si son ordre est p.

Définition du polynôme permis. $f\langle A\rangle$ étant une fonction précisée croissante, on appelle polynôme permis de $f\langle A\rangle$, le polynôme en la variable formelle t, à coefficients entiers $\geqslant 0$ que l'on écrit

$$P_{f\langle A\rangle} = \sum_{i=0}^{n} d_i\, t^i$$ où d_i représente le nombre de toutes les partitions permises distinctes de $f\langle A\rangle$ et d'ordre i. ($n = |A|$).

Définition du polynôme définitif. Dans les mêmes conditions on définit le polynôme formel $\Delta_{f<A>} = \sum \delta_i t^i$ où δ_i représente le nombre de partitions définitives distinctes et d'ordre i, de f<A>.

Remarques :

Nous noterons évidemment que :

(1) $\delta_i \leqslant d_i$ pour tout i.

(2) si p est l'indice de f<A>alors

$\delta_i = d_i = 0$ si $i < p$ et $\delta_p = d_p$. Cela résulte des propriétés démontrées dans le chapitre I. En particulier $\delta_o = d_o = 0$.

(3) Dans la pratique, on utilisera ces polynômes surtout pour des fonctions précisées exactes.

La connaissance du polynôme permis d'une fonction donne à la fois l'indice de la fonction et le nombre de toutes les manières possibles de réduire cette fonction sans tomber dans MΣ.

La connaissance du polynôme définitif d'une fonction donne les nombres caractéristiques de cette fonction (donc son indice) et le nombre de toutes les manières possibles de la réduire à une fonction s_p^2.

3.2. Calcul des polynômes permis et définitifs.

Nous commencerons par le polynôme permis qui est plus simple.

Nous noterons que si $f<A> = A^{(2)}$ et si $|A| = n$ alors $P = t^n$. Il n'y a qu'une partition permise ; c'est la partition triviale.

Si $f<A> \neq A^{(2)}$ c'est qu'il manque un monôme ab ($a, b \in A$).

Les partitions permises se classent alors en deux catégories disjointes :

(1) celles dans lesquelles a et b appartiennent à une même classe

(2) celles dans lesquelles a et b appartiennent à des classes disjointes.

Posons $A = \{a, b, C\}$.

Soit $f_1\langle a, C\rangle$ la fonction précisée déduite de f en remplaçant b par a. Cette fonction n'est pas atomique. Il y a une bijection évidente entre les partitions permises de $f\langle A\rangle$ de la catégorie (1) et l'ensemble de toutes les partitions permises de $f_1\langle a, C\rangle$.

Considérons de la même manière la fonction précisée $f_2\langle A\rangle = f + ab$. Il y a encore une bijection évidente entre les partitions permises de $f\langle A\rangle$ de la catégorie (2) et toutes les partitions permises de $f_2\langle A\rangle$.

On en conclue :

$$P_{f\langle A\rangle} = P_{f_1\langle a, C\rangle} + P_{f_2\langle A\rangle}$$

La fonction précisée $f_1\langle a, C\rangle$ a moins de variables. La fonction $f_2\langle A\rangle$ a autant de variables mais augmente et tend à se rapprocher de $A^{(2)}$.

En reprenant le processus, on arrivera, au bout d'un nombre fini d'étapes à déterminer $P_{f\langle A\rangle}$.

Remarque :

Si $f\langle A\rangle$ est exacte, il peut se faire que $f_1\langle a, C\rangle$ comme $f_2\langle A\rangle$ ne le soient plus. Cela justifie le fait qu'on ait défini les polynômes permis pour des fonctions précisées.

Exemple de calcul :

$f\langle a, b, c\rangle = abc$

$f_1\langle a, c\rangle = ac \rightarrow P_{f_1\langle a, c\rangle} = t^2$

$f_2\langle a, b, c\rangle = abc + ab = ab$

Il manque ac

$f_{21}\langle a, b\rangle = ab \rightarrow P_{f_{21}\langle a, b\rangle} = t^2$

$f_{22}\langle a, b, c\rangle = ab + ac$

Il manque enfin bc

$f_{221}\langle a, b\rangle = ab \rightarrow P_{f_{221}\langle a, b\rangle} = t^2$

$f_{222}\langle a, b, c\rangle = ab + ac + bc \rightarrow P_{f_{222}\langle a, b, c\rangle} = t^3$

D'où $P_{f\langle a, b, c\rangle} = 3t^2 + t^3$

Il y a 1 partition permise d'ordre 3. C'est la partition {a, b, c}. Il y a trois partitions permises d'ordre deux qui sont {ab, c}, {a, bc}, {b, ac}

Autre exemple : cas limite des fonctions nulles.

Nous avons $P_{o\langle a\rangle} = t$

Soit $O\langle a, b\rangle = O$.

$P_{o\langle a, b\rangle} = P_{o\langle a\rangle} + P_{ab\langle a, b\rangle} = t + t^2$

Il est évident que pour la fonction O de n variables, d_i représente le nombre de partitions distinctes d'un ensemble de n éléments en i classes.

Calcul du polynôme définitif.

Le calcul est plus compliqué. Nous utiliserons le résultat précédent en faisant la remarque suivante : deux types de modifications interviennent sur chaque fonction précisée. La première est une réduction élémentaire du type b := a. La deuxième n'en est pas une : elle consiste à rajouter un monôme du type ab pour éliminer les partitions où a et b sont dans une même classe. Nous pouvons alors adapter le processus précédent à condition de garder une fonction précisée témoin φ qui, initialement, sera la même que f<A> et à laquelle on fera subir seulement les réductions et non pas les augmentations de monômes. On sera amené à considérer alors des couples (φ, ψ) de fonctions précisées et à faire subir sur ψ les traitements de l'algorithme précédent et sur φ les seuls traitements correspondants aux réductions.

Il est évident alors que si l'on aboutit à un couple $(B^{(2)}, B^{(2)})$ alors on rajoutera t^p au polynôme (si $p = |B|$) ; si l'on aboutit à un couple $(\varphi, B^{(2)})$ avec $\varphi \neq B^{(2)}$ (donc $\varphi < B^{(2)}$), le processus s'arrêtera pour ce couple, sans rien rajouter au polynôme.

Exemple :

f<a, b, c, d> = abc + abd + cd

Posons φ cette première fonction précisée et soit (φ, φ) le premier couple. Il manque ab dans φ.

On aboutit alors aux deux couples :

$$\begin{cases} b := a & (ac + ad + cd,\ ac + ad + cd) \rightarrow \boxed{t^3} \\ & (\varphi,\ ab + cd) \end{cases}$$

Dans ce deuxième couple, il manque ac. On obtient alors deux couples :

$$\begin{cases} c := a & (ab + ad,\ ab + ad) = (\varphi_1, \varphi_1) \\ & (\varphi,\ ab + cd + ac) \end{cases}$$

Le premier $(\varphi_|, \varphi_|)$ où manque bd donne :

$\left\{\begin{array}{ll} d := b & (ab, ab) \rightarrow \boxed{t^2} \\ & (ab + ad, ab + ad + bd). \text{ Le processus s'arrête.} \end{array}\right.$

Le couple $(\varphi, ab + cd + ac)$ où manque ad donne :

$\left\{\begin{array}{ll} d := a & (ab + ac, ab + ac) \text{ qui donnera comme pour le couple } (\varphi_|, \varphi_|) \\ & \text{le seul monôme } \boxed{t^2} \\ & (\varphi, ab + ac + ad + cd) \end{array}\right.$

Dans ce dernier couple il manque bc. On obtient donc

$\left\{\begin{array}{ll} c := b & (ab + bd, ab + ad + bd). \text{ Le processus se bloque.} \\ & (\varphi, ab + ac + ad + bc + cd) \end{array}\right.$

Le dernier couple où manque bd donne enfin

$\left\{\begin{array}{ll} d := b & (bc + ab, ab + ac + bc). \text{ Le processus se bloque} \\ & (\varphi, ab + ac + ad + bc + bd + cd). \text{ Le processus se bloque.} \end{array}\right.$

Donc

$$\Delta_{f<a, b, c, d>} = t^3 + 2t^2$$

3.3. Application du couplage direct et de la somme directe au calcul des polynômes permis et définitifs.

Le calcul du polynôme permis est assez laborieux. Nous allons voir les simplifications qu'il en résulte lorsque la fonction est un couplage ou une somme directe.

Pour le polynôme définitif, seuls les couplages directs donnent des simplifications.

Proposition 1 :

Si le couplage f<A> × g<B> est direct alors entre les polynômes permis nous avons la relation

$$P_{f\times g} = P_f \cdot P_g \qquad \text{(produit des polynômes)}$$

Appelons $\mathcal{P}$ l'ensemble des partitions permises de f<A> × g<B> et $\mathcal{P}_1$, $\mathcal{P}_2$ ceux correspondants de f<A>, g<B>. A toute partition $\pi \in \mathcal{P}$, nous pouvons associer un couple $(\pi_1, \pi_2) \in \mathcal{P}_1 \times \mathcal{P}_2$. En effet toute classe de π est exclusivement contenue soit dans A soit dans B.π_1 est donc constituée de toutes les classes de π contenues dans A et π_2 des autres classes. Cette application : $\mathcal{P} \to \mathcal{P}_1 \times \mathcal{P}_2$ est manifestement bijective.

Par ailleurs si $\pi \to (\pi_1, \pi_2)$ nous avons
ordre (π) = ordre (π_1) + ordre (π_2).

Si on dénombre d_m partitions $\pi \in \mathcal{P}$ d'ordre m, si $d_i^{(1)}$, $d_j^{(2)}$ représentent respectivement le nombre des partitions π_1(resp π_2) $\in \mathcal{P}_1$ (resp.$\in \mathcal{P}_2$) et d'ordre i (resp. j) nous avons alors

$$d_m = \sum_{i=1}^{m-1} d_i^{(1)}\, d_{m-i}^{(2)} = \sum_{i=0}^{m} d_i^{(1)}\, d_{m-i}^{(2)}$$

(car $d_0^{(1)} = d_0^{(2)} = 0$).

Cela suffit à prouver la proposition.

Proposition 2 :

Dans les mêmes conditions, nous avons pour les polynômes définitifs :

$$\Delta_{f\times g} = \Delta_f \cdot \Delta_g$$

La démonstration de ce résultat est tout à fait analogue. Il suffit de restreindre l'application précédente : $\mathcal{P} \to \mathcal{P}_1 \times \mathcal{P}_2$ aux seules réductions $\mathcal{P}'$, définitives et constater que l'image (π_1, π_2) d'une réduction définitive π de $f\langle A\rangle \times g\langle B\rangle$ est constituée d'une réduction π_1 (resp. π_2) définitive de $f\langle A\rangle$ (resp. $g\langle B\rangle$).

Proposition 3 :

Si $f\langle A\rangle + g\langle B\rangle$ est une somme directe alors entre les polynômes permis

$P_f = \sum d_i^{(1)} t^i$, $P_g = \sum d_j^{(2)} t^j$ et $P_{f+g} = \sum d_m t^m$ existe la relation suivante :

$$d_m = \sum_{i=1}^{n} \sum_{j=1}^{p} d_i^{(1)} d_j^{(2)} \frac{i!\ j!}{(m-i)!(m-j)!(i+j-m)!}$$

(n et p désignant respectivement les nombres $|A|$ et $|B|$) et sous les conventions suivantes :

$$0! = 1 \quad \text{et} \quad \frac{1}{(-q)!} = 0 \quad \text{si} \quad q > 0.$$

Pour démontrer cette proposition, nous utiliserons l'algorithme (récursif) qui permet de construire le polynôme permis.

Simplement, la fonction $f\langle A\rangle + g\langle B\rangle$ se traitera par composante connexe. On cherchera les monômes ab qui manquent avec $a, b \in A$.

Nous aboutissons ainsi à :

$$P_{f+g} = P_{f_1+g} + P_{f_2+g}$$

puis $P_{f_1+g} = P_{f_{11}+g} + P_{f_{12}+g} + \ldots\ldots$ etc .....

Jusqu'à ce qu'on aboutisse au calcul de $P_{s_i^2+g}$.

Nous aurons donc :

$$P_{f+g} = \sum_{i=1}^{n} d_i^{(1)} \cdot P_{s_i^2+g}$$

$s_i^2 + g$ étant toujours une somme directe.

Pareillement $P_{s_i^2+g} = \sum_{j=1}^{p} d_j^{(2)} \cdot P_{s_i^2+s_j^2}$

$s_i^2 + s_j^2$ étant une somme directe.

Donc $P_{f+g} = \sum_{i=1}^{n} \sum_{j=1}^{p} d_i^{(1)} \cdot d_j^{(2)} \cdot P_{s_i^2+s_j^2}$

Il reste à calculer :

$$P_{s_i^2+s_j^2} = \sum_{m=1}^{n+p} d_m^{(ij)}\, t^m$$

Evidemment $d_m^{(ij)} = d_m^{(ji)}$. Supposons alors $j \leqslant i$. Si $m < i$ ou si $m > i+j$, $d_m^{(ij)} = 0$. Supposons $i \leqslant m \leqslant i+j$. Les i variables de s_i^2 appartiennent à des classes disjointes dans toute partition permise des $i+j$ variables de $s_i^2 + s_j^2$. Calculons alors le nombre des telles partitions d'ordre m. Considérons m classes $T_1\ T_2 \ldots T_m$ (provisoirement vides). Rangeons les i variables de s_i^2 dans les i premières $T_1, T_2 \ldots T_i$. Il est évident qu'elles appartiennent à des classes disjointes. Les $m-i$ autres classes contiendront chacune une et une seule variable de s_j^2. Nous avons donc C_j^{m-j} manières possibles de remplir ces classes $T_{i+1}, \ldots, T_m$. Il reste $j - (m-i) = j+i - m$ variables de s_j^2 à ranger dans les classes $T_1, T_2, \ldots, T_i$. Cela pourra se faire de A_i^{i+j-m} manières distinctes. On obtient, ce faisant toutes les partitions permises d'ordre m, sans répétition.
Donc

$$d_m^{(ij)} = C_j^{m-i} \cdot A_i^{i+j-m} = \frac{j!}{(m-i)!(i+j-m)!} \cdot \frac{i!}{(m-j)!}$$

Nous en déduisons :

$$d_m = \sum_{i=1}^{n} \sum_{j=1}^{p} d_i^{(1)} \, d_j^{(2)} \, d_m^{(ij)}$$

Exemple :

Nous avons vu que

$f\langle a, b, c, d, e\rangle = ab + bc + cd + ad + ea + eb + ec + ed$ se décomposait en :

$(O\langle a\rangle + O\langle b\rangle) \times (O\langle c\rangle + O\langle d\rangle) \times O\langle e\rangle$

On a $P_{O\langle a\rangle} = t = P_{O\langle b\rangle}$

On en déduit $P_{O\langle a\rangle + O\langle b\rangle} = t + t^2$

D'où

$P_f = (t + t^2)(t + t^2)\, t = t^3 + 2t^4 + t^5$

Remarque :

La dernière proposition n'a pas d'équivalent simple concernant les polynômes définitifs.

CHAPITRE IV

PROPRIETES EXTREMALES RELATIVES AUX FONCTIONS CROISSANTES ET LEUR INDICE.

Nous savons que l'application de l'ensemble partiellement ordonné M des fonctions booléennes croissantes strictes dans l'ensemble ordonné N des entiers naturels, définie par l'indice est une application respectant l'ordre. Il est donc intéressant de définir, les limites possibles des indices du produit et de la somme de fonctions booléennes quand on connait les indices de ces fonctions booléennes. Il est intéressant également de rechercher dans M les éléments extrémaux (maximaux et minimaux) dans l'image réciproque de cette application.

1) Majoration et minoration de l'indice d'un produit et d'une somme de fonctions booléennes.

1.1. Produit de fonctions booléennes.

Les résultats sont extrêmement simples et résumés par la proposition suivante :

Proposition :

f et g étant des fonctions booléennes croissantes respectivement d'indice p et q, l'indice r de f.g est compris entre deux et inf (p, q) les bornes pouvant être atteintes.

Le résultat est tout à fait évident quant aux bornes. Les bornes sont atteintes. Si les supports de f et g sont disjoints, mettons X et Y, la réduction $X \to x$ et $Y \to y$ donne pour fg le résultat xy d'indice deux.

Supposons à présent $q \geqslant p$ et soient $f = s_p^2(x_1, x_2 \ldots x_p)$ et $g = s_q^2(x_1, \ldots, x_p, \ldots x_q)$. On constate que $g \geqslant f$ donc $gf = f$ est d'indice $p = \inf(p, q)$. Nous avons donc $2 \leqslant \nu(f.g) \leqslant \inf(p, g)$.

On peut se poser le problème : existe t-il deux fonctions f et g telles que $\nu(f) = p$, $\nu(g) = q$ et telles que pour r choisi dans l'intervalle $[2, \inf(p, q)]$, fg soit d'indice r. Nous y répondrons un peu plus loin.

1.2. Somme de fonctions booléennes.

Les résultats prolongent ceux de [29] relatifs aux graphes.

Proposition I :

Si f et g sont d'indices respectifs p et q alors l'indice r de f+g est compris entre sup(p, q) et p.q, les bornes pouvant être atteintes.

Nous montrerons d'abord que ce sont bien des bornes. La borne inférieure est tout à fait évidente;qu'elle soit atteinte, cela est aussi évident : il suffit de considérer une somme directe.

Montrons que p.q est bien une borne supérieure. Nous désignerons par Z la réunion des supports de f et g.

Nous considérerons les fonctions précisées f<Z> et g<Z> ; la fonction f étant d'indice p on peut trouver une réduction de f à s_p^2 induisant une partition π_1 de Z en p classes (permises généralisées pour f). De la même manière on peut trouver une réduction de g à s_q^2 induisant une partition π_2 de Z en q classes (permises généralisées). La partition $\pi_1 \wedge \pi_2$ est formée de classes permises généralisées pour f<Z> + g<Z> et comporte au plus p.q classes. On peut lui associer une réduction permise d'ordre au plus p.q. Donc $\nu(f+g) \leqslant p.q$.

Montrons que la borne peut être atteinte. Considérons p.q variables notées x_{ij} ($i = 1, \ldots p$ et $j = 1, \ldots, q$) et posons les ensembles suivants de variables :

$$X_{i.} = \{x_{ij} \; ; \; j = 1, 2, \ldots, q\} \qquad (p \text{ ensembles})$$

$$X_{.j} = \{x_{ij} \; ; \; i = 1, 2, \ldots, p\} \qquad (q \text{ ensembles})$$

Les $X_{i.}$ (pour $i = 1, \ldots p$) constituent une partition des p.q variables X en p classes. De même les $X_{.j}$ constituent une partition de X en q classes.

Les fonctions $f\langle X\rangle = 0\langle X_{1.}\rangle \times 0\langle X_{2.}\rangle \ldots . \times 0\langle X_{p.}\rangle$ et $g\langle X\rangle = 0\langle X_{.1}\rangle \times 0\langle X_{.2}\rangle \ldots . \times 0\langle X_{.q}\rangle$ sont exactes et respectivement d'indice p et q.

Or la somme $f\langle X\rangle + g\langle X\rangle$ n'est autre que $s^2_{p.q}\langle X\rangle$ et d'indice p.q . La proposition est donc démontrée. Nous allons donner d'ailleurs une précision supplémentaire.

Proposition 2 :

Soit f une fonction quelconque d'indice p.q . Alors on peut trouver une fonction g d'indice p et une fonction h d'indice q, telles que f = g + h

Soit X le support de f.

Par hypothèse il existe une partition permise de X en p.q classes notées X_{ij} ($i = 1, \ldots p$) ($j = 1, 2 \ldots q$) telle que si on confond chaque classe à une variable x_{ij} la fonction f se réduise à $s^2_{p.q}(\ldots, x_{ij}, \ldots)$. Or cette dernière fonction peut se mettre sous la forme d'une somme $g'(\ldots, x_{ij}, \ldots) + h'(x\ldots, x_{ij}, \ldots)$ de fonctions respectivement d'indices p et q (cf. proposition précédente). Remplaçons chaque variable x_{ij} par la somme X^+_{ij} des variables de la classe X_{ij}.

On a (cf proposition 2 (2.1))

$f \leqslant s^{2}_{p\cdot q}(\ldots, X^{+}_{ij}, \ldots) = g + h$ en désignant par g et h le résultat de cette substitution sur les fonctions $g^{|}$ et $h^{|}$. Il est évident que l'indice de g (resp. h) est p (resp. q).

Donc $f \cdot (g + h) = f = \varphi + \psi$ où $\varphi = f \cdot g$ et $\psi = f \cdot h$. Soient p_1 et q_1 les indices de φ et ψ. Nous avons $p_1 \leqslant p$ et $q_1 \leqslant q$, mais $p\cdot q$ qui est l'indice de f, vérifie en vertu de la proposition 1 : $p\cdot q \leqslant p_1\cdot q_1$.

Donc obligatoirement $p = p_1$ et $q = q_1$.
La proposition est démontrée.

Corollaire 1 :

Toute fonction d'indice $p_1\cdot p_2\cdot \ldots \cdot p_n$ peut se mettre sous la forme d'une somme de n fonctions respectivement d'indices $p_1, p_2, \ldots, p_n$.

La proposition montre également le rôle important joué par des fonctions d'indice premier.

Corollaire 2 :

Pour qu'une fonction booléenne appartienne à la famille $mS_{p\cdot q}$, il faut qu'elle soit la somme d'une fonction mS_p et d'une fonction mS_q.

2) Fonctions maximales locales d'indice p.

L'application de M dans N définie par $\nu(f)$ est une application croissante.

Dès lors, on peut se poser la question naturelle suivante :

Existe t-il des éléments extrémaux (maximaux, minimaux) ayant un indice donné p ($p \geqslant 2$) ?

On peut poser la question de deux manières :

- localement quand on se fixe une partie finie X, de variables et qu'on considère l'ensemble (fini) des fonctions croissantes de support contenu dans X ; alors si l'ensemble des fonctions d'indice p n'est pas vide, il existera sûrement des éléments extrémaux. De telles fonctions seront dites localement extrêmales d'indice p, relativement à X.

- globalement enfin : une fonction f d'indice p sera dite globalement extrêmale si, quelque soit la partie finie X de variables, contenant son support, elle est localement extrêmale d'indice p, relativement à X.

Il en résulte que toute fonction extrêmale globale, d'indice p est localement extrêmale relativement à son support.

Une grande différence intervient entre fonctions maximales et minimales, ce qui justifie cette étude séparée. Cette différence résulte de la proposition suivante.

Proposition I :

Il n'existe pas de fonctions maximales globales d'indice p ($p \geqslant 2$).

En effet si une telle fonction f existait, alors en choisissant deux variables a, b en dehors de son support on voit que :

$f + ab > f$ et $\nu(f+ab) = \sup(p, 2) = p = \nu(f)$ cela est contradictoire.

Nous ne pouvons donc qu'essayer de caractériser les fonctions maximales locales.

Définition 1 :

Soit X un ensemble fini d'au moins p variables et $\pi = (X_1, X_2, \ldots, X_p)$ une partition de X en p classes. Nous désignons par $S_\pi(X)$ la fonction d'indice p définie par :

$$S_\pi(X) = 0\langle X_1 \rangle \times 0\langle X_2 \rangle \times \ldots \times 0\langle X_p \rangle = s_p^2(X_1^+, X_2^+, \ldots, X_p^+)$$

Proposition 2 :

Les seules fonctions maximales locales, d'indice p, relativement à un ensemble X d'au moins p variables, sont les fonctions $S_\pi(X)$.

Montrons d'abord que si f est maximale locale, d'indice p, relativement à X, alors le support de f est X. En effet soit B le complémentaire du support de f par rapport à X. Si $|B| \geqslant 2$ alors $f + B^\bullet > f$ et a même indice que f ; f n'est pas maximale. Si $|B| = 1$ alors $B = \{b\}$, la fonction $f + bx$ (x appartenant au support de f) est strictement plus grande que f et a même indice que f.

La fonction f étant d'indice p, peut se réduire à s_p^2, cette réduction induisant une partition π de X en p classes : $X_1, X_2, .., X_p$. Alors $f(X) \leqslant S_\pi(X)$ car tout monôme de f contient au moins deux variables appartenant à des classes différentes. S_π ayant pour indice p, les fonctions maximales, d'indice p, relativement à X ne peuvent être donc que les seules fonctions $S_\pi(X)$.

Montrons que $S_\pi(X)$ est localement maximale d'indice p. Soit $g(X) > S_\pi(X)$. Alors il existe un monôme premier de g qui n'est pas compatible avec S_π. Ce monôme μ est donc formé de lettres n'appartenant qu'à une seule classe de π mettons X_1. Par suite $g \geqslant S_\pi(X) + \mu = \mu\langle X_1 \rangle \times 0\langle X_2 \rangle \times \ldots \times 0\langle X_p \rangle$. La fonction figurant à droite est d'indice :

$$\underbrace{2 + 1 + \ldots + 1}_{p \text{ termes}} = p + 1 \text{ ; donc g est au moins d'indice } p + 1.$$

Ce résultat acquis, on peut essayer d'engendrer une fonction f d'indice p, par le produit des fonctions maximales locales d'indice p, de même support que f.

Proposition 3 :

Pour tout ensemble $\mathcal{S}$ de partitions permises du support d'une fonction f, tel que toute classe saturée de f appartiennent à au moins une partition de $\mathcal{S}$, nous avons : $f(X) = \prod_{\pi \in \mathcal{S}} S_\pi(X)$.

Tout d'abord, il est vrai que $f(X) \leq \prod_{\pi \in \mathcal{S}} S_\pi(X)$.

Montrons l'inégalité inverse. En posant $|X| = n$ et en considérant les applications de 2^n dans 2 définies par ces fonctions, il suffit de démontrer que pour tout point X_o caractéristique de deuxième espèce de f, alors $\prod S_\pi(X_o) = 0$.

Or l'ensemble S_{X_o} (II 1.1) est classe saturée de f et appartient à une partition $\pi' \in \mathcal{S}$. Donc $S_{\pi'}(X_o) = 0$ ainsi que $\prod_{\pi \in \mathcal{S}} S_\pi(X_o)$.

Exemple :

f = abc + abd + cd a pour classes saturées bd, ac, bc, ad, ab. L'ensemble $\mathcal{S}$ des partitions suivantes : {ab, c, d} {ac, bd} {ad, bc} répond aux conditions de la proposition.

Donc $f = s_3^2(a+b, c, d)\ s_2^2(a+c, b+d)\ s_2^2(a+d, b+c)$ ainsi qu'on peut le vérifier par calcul.

3) Fonctions minimales d'indice p.

Les fonctions minimales d'indice p, peuvent être définies à deux points de vue, comme précédemment : localement ou globalement (sous réserve d'existence).

Nous allons étudier les cas simples des indices 2, 3.

Indice 2 :

X étant un ensemble d'au moins deux variables, la seule et unique fonction localement minimale d'indice deux, relativement à X est le produit X°. En conséquence : il n'existe aucune fonction globalement minimale d'indice deux puisque si $Z \supset X$ alors $Z^{\circ} < X^{\circ}$ et l'indice reste deux.

Indice 3 :

Toute fonction d'indice 3 étant forcément surimpaire est supérieure ou égale à une fonction impaire (d'indice 3).

Les fonctions minimales d'indice 3 ne peuvent être que des fonctions impaires.

Toute fonction impaire est en fait globalement minimale d'indice 3.

En effet si f est impaire et si $g < f$ alors $g^{*} > f$ et donc $g^{*} > g$ et g est sous impaire, non impaire donc d'indice deux.

Nous allons voir plus généralement que pour $p \geqslant 3$ les fonctions localement minimales, sont globalement minimales.

3.1. Sur l'existence des fonctions minimales globales d'indice ($p \geqslant 3$).

Lemme :

Si les deux fonctions croissantes strictes f et g vérifient $f < g$ et si g comporte plus d'un monôme irréductible, alors on peut trouver une réduction, laissant g invariante et réduisant f à f_1 avec $f_1 < g$ et support de $f_1 \subseteq$ support de g.

Cela est déjà évident si support de $f \subseteq$ support de g. Supposons qu'il n'est est pas ainsi et soit Z l'ensemble des variables du support de f, étrangères au support de g. En réduisant ces variables Z à une seule z (étrangère à g) on obtient pour f la fonction $z\psi + \varphi$ vérifiant :

$$z\psi + \varphi \leqslant g$$

L'inégalité est stricte, sinon $\varphi = g$ or $\varphi \leqslant f$ (φ est l'ensemble des monômes de f ne contenant aucune variable dans Z) ; cela est donc absurde. Nous avons donc : $\varphi < g$ et par suite il existe un monôme μ de g non compatible avec φ. Ce monôme μ ne contient pas, d'après les hypothèses, toutes les variables du support de g. Soit donc y une variable n'appartenant pas à μ et dans le support de g. Réduisons alors la variable z à y. La fonction $z\psi + \varphi$ se réduit à $f_1 = yh + k \leqslant g$. L'inégalité est stricte car μ compatible avec g, ne l'est pas avec f_1 (sinon il l'aurait été avec φ). La fonction f_1 vérifie les conclusions du lemme.

Exemple :

Nous avons :

$ztuw + uv < uv + uw$. Réduisons t à z :

$zuw + uv < uv + uw$. uw n'est pas compatible avec $\varphi = uv$. Soit v (la seule variable) étrangère à uw. La réduction de z à v donne : $uvw + uv = uv < uv + uw$.

Théorème :

Si f est localement minimale d'indice p ($\geqslant 3$) relativement à son support, elle est globalement minimale.

En effet en vertu du lemme précédent si $g < f$ alors g peut se réduire à $g_1 < f$ et g_1 a son support contenu dans celui de f ; g_1 a donc pour indice p-1 au plus, de même que g.

Définitions et convention :

Nous dirons que la fonction précisée f<X> est minimale d'indice p lorsque :

(1) $p \geqslant 2$ f est localement minimale d'indice p et f<X> est exacte. Bien entendu si $p \geqslant 3$ f est alors minimale.

(2) $p = 1 \quad f = 0 \quad$ et $\quad |X| = 1$

Avant d'étudier plus en détail les fonctions minimales d'indice p, nous citerons cette propriété évidente.

Propriété des fonctions minimales d'indice p.

Si f est (localement) minimale d'indice p ($p \geq 2$) alors le reste de f par rapport à toute variable de son support est d'indice p-1.

Cela tient au fait que ce reste est d'indice p ou p-1 et que son support est contenu dans celui de f.

3.2. Construction de certaines fonctions minimales d'indice p par couplage direct, composition disjointe. Fonctions symétriques.

Théorème 1 :

Désignant par p et q les indices de f et g, une condition nécessaire et suffisante pour que le couplage direct $f\langle X\rangle \times g\langle Y\rangle$ donne une fonction minimale d'indice p+q est que les fonctions précisées $f\langle X\rangle$ et $g\langle Y\rangle$ soient respectivement minimales d'indice p et q.

C.N. Etant donné le rôle symétrique de f et g, on raisonnera sur $f\langle X\rangle$.

Si $p = 1$ alors $f = 0$. Montrons que $|X| = 1$. Si cela n'est pas alors $(x \in X)\ (0\langle x\rangle \times g\langle Y\rangle) < (0\langle X\rangle \times g\langle Y\rangle)$ et l'indice ne change pas.

Si $p \neq 1$ $f\langle X\rangle$ est exacte. Sinon on peut trouver $X_1 \subset X$ et $f\langle X_1\rangle \times g\langle Y\rangle = f + g + X_1^+ \cdot Y^+ < (f\langle X\rangle \times g\langle Y\rangle)$ les indices des deux membres étant les mêmes.

f est localement minimale par rapport à son support X ; sinon on peut trouver f_1 d'indice p avec $f_1 < f$ et support de $f_1 \subseteq X$ et $f_1\langle X\rangle \times g\langle Y\rangle = f_1 + g + X^+Y^+$ est strictement plus petite que $f\langle X\rangle \times g\langle Y\rangle$ tout en ayant même indice.

C.S. Prenons d'abord le cas $p \geqslant 2$, $q \geqslant 2$ et supposons que $f\langle X\rangle$ et $g\langle Y\rangle$ vérifient les conditions (suffisantes) du théorème, soit :

$$\psi < f + g + X^+Y^+$$

On peut supposer que le support de ψ est contenu dans $X \cup Y$ (lemme précédent 3.1). Nous pouvons alors écrire $\psi = f_1 + \psi_1 + g_1$ où f_1 (g_1) désigne la somme des monômes en X (resp. en Y) et où ψ_1 désigne la somme des monômes ayant à la fois des lettres dans X et Y.

On en déduit : $f_1 \leqslant f$, $g_1 \leqslant g$, $\psi_1 \leqslant X^+ \cdot Y^+$ l'une des inégalités étant stricte. Si c'est l'une des deux premières (par exemple $f_1 < f$) alors on a :

$$\psi < f_1 + X^+Y^+ + g$$

Donc $\psi < f_1\langle X\rangle \times g\langle Y\rangle$

Mais l'indice de f_1 est p-1 au plus ; donc l'indice de $f_1\langle X\rangle \times g\langle Y\rangle$ est p+q-1 au plus comme celui de ψ.

Si maintenant, seule la troisième inégalité est stricte : $\psi_1 < X^+Y^+$, alors il existe : xy $(x \in X, y \in Y)$ monôme non compatible avec ψ_1 et donc en désignant par X_1 (resp Y_1) les variables de X (resp Y) autres que x (resp y) on a :

$$\psi_1 \leqslant X_1^+ \cdot Y_1^+ + x\, Y_1^+ + y\, X_1^+$$

Décomposons f (respectivement g) par rapport à la variable x (resp. y) : $f = x f_1 + f_0$ et $g = y g_1 + g_0$, nous avons alors :
$\psi = f + g + \psi_1 \leqslant x f_1 + f_0 + y g_1 + g_0 + X_1^+ Y_1^+ + x Y_1^+ + y X_1^+$. Réduisons y à x, ψ se réduit à $\tilde{\psi}$ et

$$\tilde{\psi} \leqslant x f_1 + f_0 + x g_1 + g_0 + x(X_1^+ + Y_1^+) + X_1^+ Y_1^+$$

Or $x f_1 + x g_1 \leqslant x(X_1^+ + Y_1^+)$ car les fonctions f_1 et g_1 sont différentes de 1. On obtient

$$\tilde{\psi} \leqslant f_0 + g_0 + X_1^+ \cdot Y_1^+ + x(X_1^+ + Y_1^+)$$

et donc $\tilde{\psi} \leqslant f_0\langle X_1\rangle \times g_0\langle Y_1\rangle \times 0\langle x\rangle$

Or f_0, g_0 ont pour indices p-1 et q-1 (restes de fonctions minimales). L'indice du second membre est donc p-1 + q-1 + 1 = p+q-1. Donc ψ est au plus d'indice p+q-1.

Le cas p = q = 1 est évident. $0\langle x\rangle \times 0\langle y\rangle = xy$ est minimale (locale) d'indice deux.

Si p = 1, $q \geqslant 2$ alors $f\langle X\rangle \times g\langle Y\rangle = 0\langle x\rangle \times g\langle Y\rangle = x Y^+ + g$; si $\psi < x Y^+ + g$ (on peut supposer encore que son support est contenu dans {x, Y}) ; alors $\psi = xh + g_1$; si $g_1 < g$ le même raisonnement s'applique, g_1 est d'indice q-1 au plus et ψ d'indice q au plus alors que $x Y^+ + g$ est d'indice q+1. Si $g_1 = g$ c'est donc que

$$\psi \leqslant x Y_1^+ + g = x Y_1^+ + y g_1 + g_0$$

ψ peut se réduire à $\tilde{\psi} \leqslant x Y_1^+ + g_0$ et g_0 étant d'indice q-1 au plus $\tilde{\psi}$ est d'indice q au plus.

Conséquence :

Pour tout entier p > 2 et tout ensemble X d'au moins p variables, on peut construire des fonctions minimales d'indice p, de support X.

Si $|X| \geqslant p$ considérons p-2 variables $x_1, x_2, .., x_{p-2}$ et soit Z ($|Z| \geqslant 2$) les autres variables de X alors

$$0\langle x_1\rangle \times 0\langle x_2\rangle \times .. \times 0\langle x_{p-2}\rangle \times Z^{\bullet}\langle Z\rangle$$

est minimale d'indice p conformément au théorème et a pour support X.

Théorème 2 :

Une condition nécessaire et suffisante pour qu'une composée disjointe $f \overset{u}{\circ} g$ non triviale (les supports de g et f contiennent plus d'une variable) soit minimale d'indice p+1 ($p \geqslant 2$) est que f et g soient minimales d'indice p+1.

Nous désignerons par {u, X} le support de f et par Y celui de g.
Nous poserons $f = uh + k$ et $\varphi = f \overset{u}{\circ} g$. Nous avons :

$$\varphi = gh + k.$$

Condition nécessaire :

D'après la proposition 1 (chapitre II 2.2) nous savons que :

$$\nu(\varphi) = p + 1 = \begin{cases} \nu(f) & \text{si} \quad \nu(g) \geqslant \nu(f) \\ \nu(k) & \text{si} \quad \nu(g) < \nu(f) \end{cases}$$

Or k est reste de φ par rapport à Y (classe permise) et a donc pour indice p (φ est minimale d'indice p+1). La deuxième éventualité est donc à rejeter ; seule la première reste qui implique $\nu(f) = p + 1 \leqslant \nu(g)$.

g est d'indice p+1 sinon en prenant un reste convenable g_1 de g ($g_1 < g$) d'indice p+1 on a $f \overset{u}{\circ} g_1 < f \overset{u}{\circ} g$ les indices des deux membres étant p+1.

Les fonctions f et g sont minimales d'indice p+1, sinon on pourrait trouver deux fonctions f_1 et g_1 d'indice p+1 dont les supports sont respectivement contenus dans ceux de f et g et telles que l'une au moins des inégalités $f_1 \leqslant f$ et $g_1 \leqslant g$ soit stricte. Cela implique que

$f_1 \overset{u}{\circ} g_1 < f \overset{u}{\circ} g$ les indices étant inchangés.

Condition suffisante

Soit $\psi < g \cdot h + k$

g est une somme de monômes en Y et h une somme de monômes en X, k une somme de monômes en X.

Nous pouvons poser alors :

$\psi = \psi_1 + k_1$ où ψ_1 désigne la somme des monômes ayant à la fois des variables dans X et Y et k_1 celle des monômes n'ayant que X pour variables.

Bien entendu $\psi_1 \leqslant g \cdot h$ et $k_1 \leqslant k$ l'une des inégalités étant strictes.

Premier cas :

$k_1 < k$; alors $\psi \leqslant g \cdot h + k_1$; si on confond les variables Y en u, $gh + k_1$ se réduit à $uh + k_1 < uh + k$ donc $uh + k_1$ est d'indice p au plus, comme ψ.

Deuxième cas :

$k_1 = k$, $\psi_1 < g \cdot h$

Nous posons $g = \gamma_1 + \gamma_2 + \ldots + \gamma_q$ et $h = \eta_1 + \eta_2 + \ldots + \eta_r$ (sommes de monômes irréductibles).

Dire que $\psi_1 < g \cdot h$ c'est dire qu'un des monômes de $g \cdot h$ n'est pas compatible avec ψ_1. Nous supposerons que c'est le monôme $\gamma_1 \eta_1$.

Désignons par Y_1 les lettres Y ne figurant pas dans γ_1 et de même X_1 les lettres X ne figurant pas dans η_1.

Posons $g_1 = \gamma_1 \cdot Y_1^+ + \gamma_2 + \ldots + \gamma_q$

et $h_1 = \eta_1 \cdot X_1^+ + \eta_2 + \ldots + \eta_r$

Nous avons :

$g_1 < g$ et $h_1 < h$.

Par ailleurs on vérifie aisément que :

$\psi_1 \leqslant g\, h_1 + g_1\, h$ donc :

$\psi \leqslant g\, h_1 + g_1\, h + k < gh + k$

g_1 strictement plus petit que g est d'indice p et a même reste que g par rapport à une des variables de γ_1.

Donc (chapitre II prop.2 (2.2)) on peut réduire les variables Y à p+1 variables de manière que

$$\begin{cases} g_1 \to g_{1_\pi} < y(y_1 + y_2 \ldots + y_{p-1}) + s_p^2(y_1, \ldots, y_p) \\ g \to g_\pi = s_{p+1}^2(y_1, y_2, \ldots, y_p, y) \end{cases}$$

ψ se réduit à ψ_π et on a :

$\psi_\pi \leqslant s_{p+1}^2(y_1, \ldots, y_p, y)\, h_1 + s_p^2(y_1, \ldots, y_{p-1}, y_p + y)\, h + k$

De la même manière puisque $h_1 < h$ on a $u\, h_1 + k < uh + k$

Le premier membre $u\,h_1 + k$ est donc d'indice p et $uh + k$ d'indice p+1. Ces deux fonctions ont même reste par rapport à u.

On peut donc par une réduction, portant sur les seules variables X (en p classes) et toujours d'après la proposition 2 (chapitre II 2.2) réduire $uh + k$ à $u(x_1+x_2+..+x_p) + s_p^2(x_1,\ldots,x_p)$ cependant que $u\,h_1 + k$ se réduit au plus à :

$u(x_1+\ldots+x_{p-1}) + s_p^2(x_1\ldots x_p)$. Cela implique qu'on peut trouver une réduction telle que k se réduit à $s_p^2(x_1,\ldots, x_p)\,h$ à $x_1 + x_2 +..+ x_p$ et h_1 au plus à $x_1 +..+ x_{p-1}$.

Appelons cette deuxième réduction π'. Nous obtenons

$$\psi_{\pi\,\pi'} \leq s_{p+1}^2(y_1,\ldots, y_p, y)(x_1+..+x_{p-1}) + s_p^2(y_1,\ldots, y_{p-1}, y_p+y)(x_1+\ldots+x_p) + s_p^2(x_1,\ldots, x_p)$$

Réduisons alors

$$y_1 \to x_1,\ldots, y_{p-1} \to x_{p-1}$$

$$y_p \to x_p$$

$$y \to x_p$$

On obtient au second membre de l'inégalité précédente :

$$\left[x_p + s_{p-1}^2\,(x_1\ldots x_{p-1})\right]\,(x_1+\ldots+x_{p-1}) +$$

$$s_p^2(x_1,\ldots, x_p)\,(x_1+..+x_p) + s_p^2(x_1\ldots x_p)$$

$$= s_p^2(x_1, x_2\ldots, x_p)$$

ψ est donc au plus d'indice p.

Théorème 3 :

La fonction symétrique s_n^{q+1} $(q \geq 1)$ est minimale si et seulement si $n \equiv 1$ (modulo q).

Nous savons que l'indice p de s_n^{q+1} vérifie :

$$n = q(p-1) + r$$

avec r pouvant prendre les valeurs 1, 2,...., q. Cela nous donne q valeurs consécutives de n dont la plus petite est $(p-1)\,q+1$ et qui correspond à la plus petite fonction symétrique d'indice p, homogène de degré q+1.

Cette fonction est minimale.

Soit $f(X) < s_{(p-1)q+1}^{q+1}(X)$

Tous les monômes de f(X) sont de degré $\geq q+1$ et il manque au moins un monôme de degré q+1. Soit Z les lettres de ce monôme (en nombre q+1), et Y les autres lettres. Nous avons donc en posant $k = |Y|$:

$$f(X) \leq s_{q+1}^{q}(Z)\, S_k^{1}(Y) + s_{q+1}^{q-1}(Z)\, s_k^{2}(Y) + \ldots\ldots + s_k^{q+1}(Y)$$

Réduisons les lettres Z en une seule. Il vient

$$f(z, Y) \leq z \cdot Y^{+} + s_k^{q+1}(Y)$$

Or $\quad k = |X| - |Z| = (p-1)q+1 - q-1 = (p-2)\,q$

donc $s_k^{q+1}(Y)$ est d'indice p-2. Le second membre est d'indice p-1 et f est au plus d'indice p-1.

3.3. Essai de caractérisation récursive des fonctions minimales.

Les fonctions minimales d'indice 3 (c'est-à-dire impaires) peuvent être caractérisées de la manière suivante [15].

Pour toute variable x du support de f alors :

$$f(x, X) = xh(X) + k(X)$$

k(X) est sous impaire non impaire c'est-à-dire appartient à une certaine classe de fonctions d'indice 2 et en outre :

$$k(X) + h(X) = k^{*}(X).$$

Réciproquement k(X) étant sous impaire, non impaire $f(x, X) = xk^{*}(X) + k(X)$ est impaire.

Nous allons, essayer de généraliser ceci, aux cas des fonctions d'indice p (> 3).

Le reste k(X) par rapport à x d'une fonction minimale d'indice p, étant d'indice p-1 il est naturel de se poser les questions suivantes :

- A partir d'une fonction k(X) d'indice p-1 quelle est la plus petite fonction d'indice p, f(u, X) telle que f(0, X) = k(X). Nous y répondrons.

- Comment choisir (ou caractériser) ces fonctions k(X) pour que f(u, X) soit minimale ? La réponse sera partielle.

Associée d'une fonction.

Soit f une fonction d'indice $p \geqslant 2$. En désignant par $\mathcal{R}(f)$ l'ensemble des classes permises de f, telle que le reste de f par rapport à elles soit d'indice p-1, on désigne par associée de f et on la note f^{o} la fonction

$$f^{o} = \sum_{S \in \mathcal{R}(f)} S.$$

Remarques :

1) Si on prend un ensemble X contenant le support de f et si l'on prend les classes permises généralisées telles que le reste de f par rapport à elles soit d'indice p-1, on constate aisément qu'on obtient encore f^o par le même procédé ; en effet si $\eta\mu$ est une telle classe (μ ensemble de variables en dehors du support de f) on voit que η répond à la question et donc $\eta\mu + \eta \quad \eta$

2) Si f est minimale d'indice p et si son support est X alors

$f^o = X^+$ (le reste par rapport à chaque variable est d'indice p-1).

La réciproque est fausse

Exemple :

$f = ab + bc + cd + de + ea$ (indice 3)

On obtient $f^o = a + b + c + d + e$; f n'est pas 3-minimale $f > s_5^3(a, b, c, d, e)$ (d'indice 3).

Proposition 1 :

Si l'indice de f est $\geqslant 2$ alors nous avons $f + f^o \geqslant f^*$, l'égalité n'ayant lieu que si et seulement si f est sous impaire, non impaire.

- Si f est surimpaire, cela est vrai car $f \geqslant f^*$.
  Si f n'est pas surimpaire, elle est d'indice deux.
  Soit X_1 tel que $f^*(X_1) = 1$ c'est-à-dire $f(X'_1) = 0$.
  Si $f(X_1) = 1$ l'inégalité est satisfaite.
  Si $f(X_1) = 0$ comme $f(X'_1) = 0$ on peut réduire f(X) au produit en confondant les variables 1 de X_1 en x_1, les autres étant confondues en x_2. Mais alors $S_{X_1} \in \mathcal{R}$ et donc $f^o(X_1) = 1$.

- L'égalité ne peut avoir lieu que si f(X) est sous impaire $\left(\text{car } f^*(X) = f(X) + f^\circ(X) \Rightarrow f^*(X) \geqslant f(X)\right)$; f(X) ne peut être impaire sinon $f^\circ(X) = X^+$ (non impaire). Montrons qu'effectivement si f(X) est sous impaire non impaire, l'égalité vaut. Démontrons pour cela que $f^\circ(X) \leqslant f^*(X)$. Soit α un monôme premier de $f^\circ(X)$ donc $\{\alpha, \mathcal{C}\alpha\}$ est une réduction de f(X) au produit.
Par suite $f(X_\alpha) = 0 = f(X'_\alpha)$

Donc $f^*(X_\alpha) = 1$ et α est un monôme compatible avec f^*.

Proposition 2 :

Si f et g ont même indice p et si $f \leqslant g$ alors $f^\circ \geqslant g^\circ$.

En effet une classe $S \in \mathcal{R}(g)$ est d'une part permise pour f ; le reste de f par rapport à S est inférieur au reste de g par rapport à S (d'indice p-1) et est donc d'indice p-1 (ce reste en effet ne peut prendre que les valeurs p ou p-1).

Autres propriétés vis à vis du couplage et somme directe.

(1) Si f est le couplage direct $g\langle Y\rangle \times h\langle Z\rangle$ alors $f^\circ = g^\circ + h^\circ$ (somme directe) sous la convention que $0^\circ\langle X\rangle = X^\bullet$

En effet une classe permise S de f est soit permise pour g, soit pour h et réciproquement. Si le reste de f par rapport à S diminue d'une unité c'est que selon le cas le reste de g ou h par rapport à S a diminué aussi d'une unité.

(2) Si f est somme directe $g\langle Y\rangle + h\langle Z\rangle$, g et h ayant les indices p et q $(p \geqslant q)$ alors $f^\circ = g^\circ$ si $p > q$ et $f^\circ = g^\circ \cdot h^\circ$ si $p = q$.

En effet supposons $p > q$. Si $S \in \mathcal{R}(f)$, S n'est pas une partie de Z (sinon le reste par rapport à S a pour indice p). Si $S = \eta\zeta$ ($\eta \subseteq Y$ $\zeta \subseteq Z$) η est classe de $\mathcal{R}(g)$. Donc $f^{o}(X)$ ne peut être que inférieure ou égale à $g^{o}(Y)$. Il y a égalité car toute classe de $\mathcal{R}(g)$ appartient à $\mathcal{R}(f)$ comme on peut aisément le vérifier.

- Supposons $p = q$. Toute classe permise $S \in \mathcal{R}(f)$ contient à la fois des lettres de Y et Z et donc se décompose en $\eta\zeta$: $\eta \in \mathcal{R}(g)$, $\zeta \in \mathcal{R}(h)$ donc $f^{o}(X) \leqslant g^{o}(Y)\, h^{o}(Z)$.

Réciproquement, à une classe η quelconque de $\mathcal{R}(g)$ et une classe quelconque ζ de $\mathcal{R}(h)$ correspond une classe $\eta\zeta \in \mathcal{R}(f)$. D'où l'égalité.

Théorème I :

Soit f(X) une fonction d'indice p et $f^{o}(X)$ son associée. Alors $g(x, X) = x\, f^{o}(X) + f(X)$ est la plus petite fonction d'indice p+1 ayant pour reste f par rapport à x.

g(x, X) est en effet d'indice p ou p+1. Cela ne peut être p sinon par une partition $(x\, X_1, X_2, \ldots, X_p)$ on réduirait g à s_p^2.

Si $X_1 = \phi$ cela est impossible (f est d'indice p)

Si $X_1 \neq \phi$, $(X_1, X_2, \ldots, X_p)$ est une réduction définitive d'ordre p de f(X). Mais alors $X_1, X_2, \ldots, X_p \in \mathcal{R}(f)$ donc selon cette réduction $f^{o}(X)$ devient $x_1 + x_2 + \ldots + x_p$ et cela est absurde car on ne peut plus réduire x à x_1.

Soit maintenant une fonction $\psi(x, X) = xh(X) + f(X)$. Montrons que si $h(X) \not\geqslant f^{o}(X)$ alors ψ est d'indice p. Il existe, en effet, dans ce cas un monôme $S_1^{\bullet}$ de f^{o} non compatible avec h (et aussi avec f). Donc on peut réduire f à s_p^2 en utilisant cette classe S_1 et les autres classes $S_2, \ldots, S_p$ et en les confondant respectivement à $x_1, x_2, \ldots, x_p$. Le monôme x_1 ne peut apparaître alors dans la réduite de h (sinon $S_1^{\bullet}$ serait compatible avec h). Donc $h_\pi \leqslant x_2 + \ldots + x_p$ et $\psi_\pi < x(x_2 + \ldots + x_p) + s_p^2(x_1, x_2, \ldots, x_p)$.

ψ_π est manifestement d'indice p.

Conséquence :

Nous sommes en mesure de démontrer la propriété énoncée au début de ce chapitre (I.1) et que nous rappelons : Soient donnés trois entiers p, q, r vérifiant $2 < r < \inf(p, q)$. On peut trouver une fonction f d'indice r, qui soit le produit d'une fonction g d'indice p et d'une fonction k d'indice q.

Nous supposerons $p \leqslant q$. Considérons une fonction φ minimale d'indice r ayant un support X de q variables (il en existe d'après la conséquence 3.2). Soit $\psi\langle Z\rangle$ une fonction précisée d'indice p-r et telles que $Z \cap X = \phi$; alors $g = \varphi\langle X\rangle \times \psi\langle Z\rangle$ est d'indice p ;

$$g = \varphi + X^+Z^+ + \psi$$

Soit $h = s_q^2(X)$ d'indice q ; alors

$$f = gh = (\varphi + X^+Z^+ + \psi)\, s_q^2(X) = \varphi + s_q^2(X)\, Z^+$$

(En effet les monômes de φ contiennent seulement des lettres de X et donc, ψ n'étant pas atomique $\varphi \leqslant s_q^2(X)$; par ailleurs $\psi \leqslant Z^+$ et donc $\psi\, s_q^2(X) \leqslant Z^+\, s_q^2(X)$). f est manifestement d'indice r (on peut réduire Z à z et f se réduit à $\varphi + s_q^2(X)\, z$ qui est d'indice r d'après le théorème).

Théorème 2 :

La seule fonction minimale ayant le reste k (d'indice $p \geqslant 2$) par rapport à une de ses variables x, ne peut être que $xk^o + k$. Cette fonction est en fait minimale si et seulement si, k est régulière dans le sens suivant : il n'existe aucune fonction g de même indice que k vérifiant à la fois (1) $g < k$ (2) $g^o \leqslant k + k^o$.

La première partie résulte naturellement du théorème précédent car $xk^{\circ} + k$ est la plus petite fonction d'indice $p + 1$ ayant le reste k d'indice p.

Montrons que si $xk^{\circ} + k$ est minimale (d'indice $p + 1$) alors k est régulière. Autrement on pourrait trouver g d'indice p avec $g < k$ et $g^{\circ} \leqslant k + k^{\circ}$. Alors la fonction $xg^{\circ} + g$ est d'indice $p + 1$ et strictement plus petite que $xk^{\circ} + k$. On aboutirait à une contradiction.

Réciproquement si k est régulière (d'indice p), $xk^{\circ} + k$ est minimale d'indice $p + 1$. Supposons en effet que $f < xk^{\circ} + k$ avec f d'indice $p + 1$. Désignons par g le reste de f par rapport à x. Nous avons $g \leqslant k$ (f dépend donc de x car g est d'indice au plus p). En fait g est d'indice au moins p donc d'indice p. Si $g = k$ alors nécessairement (théorème 1) $f \geqslant xg^{\circ} + g = xk^{\circ} + k$; cela est contradictoire. Donc $g < k$. Comme

$$xg^{\circ} + g \leqslant f < xk^{\circ} + k$$

On en déduit que :

$$g^{\circ} \leqslant k^{\circ} + k$$

Le résultat est contradictoire (k ne serait pas régulière).

Il ne reste donc, qu'à caractériser les fonctions régulières d'indice p. Le résultat sera partiel.

Définitions :

Une variable du support de k est dite inutile si elle n'appartient pas au support de $k + k^{\circ}$. Un monôme μ de k est dit aberrant, si le reste de k par rapport à l'ensemble des variables de μ, a même indice que k.

Proposition 3 :

Si une fonction k est régulière, alors elle ne contient ni monôme aberrant ni variable inutile.

Supposons en effet que k régulière contienne un monôme μ aberrant. Posons $k = \mu + h$; le reste de h par rapport à μ a même indice que k. Désignons par Y les variables de k autres que μ et considérons :

$$g = \mu Y^{+} + h.$$

Nous avons $g < k$ et g a même indice que k. Soit $m \in g^{o}$; on peut réduire g à s_p^2 (p étant l'indice de k, g, h) en utilisant une partition associée $(m, S_2, \ldots, S_p)$. Les lettres de μ ne peuvent appartenir à une seule classe qu'à la condition que μ se confonde à cette classe. En effet μ est classe saturée de g. Dans ces conditions le reste de g par rapport à μ serait d'indice $p - 1$ (cela est absurde). Donc cette réduction sur k est permise et d'ordre p. Donc le reste de k par rapport à m est d'indice $p - 1$ et $m \in k^{o}$. Donc $g^{o} \leqslant k^{o}$; comme $g^{o} \geqslant k^{o}$, alors $g^{o} = k^{o}$. Donc $g^{o} \leqslant k + k^{o}$. Par suite k ne serait pas régulière.

Démontrons de même que k n'a pas de variable inutile. Si, en effet, x était inutile, le reste g de k par rapport à x aurait le même indice p que k. En posant $k = xh + g$ on déduit alors $g < k$. Soit μ un monôme de g^{o}. Donc on peut réduire g à s_p^2 en utilisant une partition du support de g, du type : $(\mu, S_2, \ldots, S_p)$ (x ne figurant pas dans cette partition). Cette réduction donne pour k : $k_\pi = xh_\pi + s_p^2$. Si $k_\pi = s_{p+1}^2$ cela prouve que $x\mu$ n'est pas classe permise de k donc $x\mu \leqslant k$ et $x\mu \leqslant k + k^{o}$. Comme $k + k^{o}$ ne dépend pas de x, alors $\mu \leqslant k + k^{o}$.

Si à présent $k_\pi \neq s_{p+1}^2$ on peut alors soit réduire $x\mu$ à une seule variable (et donc $x\mu \leqslant k^{o}$ donc $x\mu \leqslant k + k^{o}$ donc $\mu \leqslant k + k^{o}$) ou bien réduire x et une des classes S_i mais alors $\mu \in k^{o}$.

Dans tous les cas $g^{o} \leqslant k + k^{o}$ et k n'est pas régulière.

Réciproque partielle :

Si une fonction k ne contient aucun monôme aberrant, il n'existe alors aucune fonction g de même indice que k telle que $g < k$ et $g + g^{o} < k + k^{o}$.

En effet procédons par absurde. Il existe alors un monôme μ de $k + k^{o}$ non compatible avec $g + g^{o}$; comme $k^{o} \leq g^{o}$ (proposition 2), ce monôme μ appartient forcément à k ; μ n'est pas compatible non plus avec g : donc μ est classe permise de g et le reste de g par rapport à μ a même indice que g ; comme enfin $g < k$ le reste de k par rapport à μ a donc même indice que k. En conséquence μ est aberrant pour k.

Remarques :

1) La condition de non existence de monômes aberrants ou de variable inutile n'est pas suffisante pour que k soit régulière.

Exemple :

$k = ab + bc + cd + de + ea$ est d'indice 3, et n'a pas de monômes aberrants. Elle n'est pas impaire donc non minimale. Or :
$k^{o} = a + b + c + d + e$. Donc aucune variable n'est inutile. Toute fonction minimale g d'indice 3 inférieure à k, telle que $g^{o} = a + b + c + d + e$ vérifie alors : $g^{o} \leq k^{o} + k$. Donc k n'est pas régulière.

2) Lorsque k, n'admettant aucun monôme aberrant, n'est pas régulière, c'est qu'il existe g ayant même indice que k et telle que

$$g < k \qquad g + g^{o} = k + k^{o}$$

3) Notons toutefois que dans le cas d'indice deux la condition de non existence de monômes aberrants est nécessaire et suffisante pour que k soit régulière.

En effet si k d'indice deux n'est pas régulière, c'est qu'elle est non sous impaire. Il existe alors [15] deux monômes μ_1 et μ_2 de k n'ayant aucune lettre en commun. Chacun est aberrant.

C H A P I T R E V

SUR QUELQUES ALGORITHMES PRATIQUES : DUALISATION, DECOMPOSITION.

Le calcul de la duale d'une fonction booléenne, c'est à dire le développement d'un produit de sommes est une transformation fondamentale en algèbre de Boole.

Comme applications, nous pouvons citer :

- En logique, le passage d'une forme normale disjonctive à une forme normale conjonctive et inversement, est un calcul de duale (ce problème se rencontre par exemple dans la démonstration automatique).

- Dans la synthèse minimale deux couches d'une fonction booléenne donnée, on est amené (circuits et ou).

1) à rechercher les composants premiers de f. Cela peut se faire en prenant deux fois la duale de f [16] ;

2) à rechercher des bases irrédondantes (ou premières) de f. On recherche les couvertures ponctuelles par développement d'un produit de sommes [15].

- Enfin comme nous venons de le voir dans les chapitres précédents, le calcul de l'indice d'une fonction croissante (ou du nombre chromatique d'un graphe en particulier) est un calcul de duale.

La procédure de dualisation est donc tellement importante, qu'il est nécessaire de disposer de méthodes les plus performantes possibles.

Nous allons étudier, ce problème, sur le plan pratique, en essayant de diminuer le plus possible, le nombre d'opérations booléennes à effectuer.

Nous examinerons ensuite le problème des décompositions, c'est-à-dire celui de la recherche d'une partition en classes d'un certain ensemble, à partir d'une certaine relation de "voisinage".

1) Principe de la méthode algébrique de dualisation. Définition d'un coût théorique.

1.1. Codage du problème en machine.

Il est difficile de juger de l'efficacité d'une méthode sans faire quelques expériences sur calculatrices. En général et dans l'état actuel, les éléments de mémoire d'une calculatrice peuvent être assimilés à des vecteurs booléens ayant un nombre fixe de positions binaires (appelé capacité du mot machine) et les instructions élémentaires de ces calculatrices permettent de former, l'union, l'intersection et le complément booléen de ces mémoires.

On convient alors d'associer à chaque variable booléenne d'une fonction une position binaire d'un rang bien défini (d'une ou plusieurs mémoires selon le nombre de ces variables : problème analogue à la multiple précision) étant entendu que le complément d'une variable est considéré comme une variable distincte ; chaque monôme d'une fonction booléenne sera considéré comme l'ensemble de ses variables et sera codé par une mémoire (ou plusieurs selon les cas) dont les 1 caractériseront la présence de la lettre dans le monôme.

Supposons par exemple, que les mots machines possèdent 36 positions binaires ; en simple précision, nous pourrons traiter les fonctions croissantes jusqu'à 36 variables et les fonctions quelconques, jusqu'à 18 variables ; dans ce dernier cas nous conviendrons que les rangs d'une variable donnée et de son complément différent de 18 positions binaires.

Les monômes d'une fonction donnée seront rangés dans p mémoires consécutives, si p est leur nombre ; (quand p = 0 la fonction sera considérée comme nulle). Le monôme vide sera assimilé à 1 et codé par une mémoire nulle.

Le produit de deux monômes consiste à unir les mémoires correspondantes. Dans le cas de fonctions quelconques (non forcément croissantes) il faut s'assurer que le résultat n'est pas nul c'est-à-dire qu'une variable et son complément ne figurent pas dans le produit ; ce résultat occupant une certaine mémoire A, est décalé vers la droite de 18 positions dans une autre mémoire T ; si l'intersection de T et A n'est pas nulle, le résultat est nul.

On peut également, sans peine, reconnaître que deux monômes ont une variable en commun : l'intersection des mémoires correspondantes doit être non nulle.

Le produit de deux monômes ne présente donc aucune difficulté sur le plan programmation et particulièrement dans le cas de fonctions croissantes, où le temps d'exécution d'un tel produit est inférieur à celui d'une addition arithmétique.

La comparaison totale de deux monômes μ et ν est le calcul de la valeur logique : $\mu \leqslant \nu$ ou $\nu \leqslant \mu$; on forme pour cela le produit $\mu.\nu$ et on teste : $\mu\nu = \mu$ ou $\mu\nu = \nu$.

On appellera comparaison partielle entre μ et ν le calcul de la valeur logique : $\mu \leqslant \nu$ (il arrivera, en effet que par des considérations théoriques, le cas $\mu > \nu$ soit écarté). Elle est légèrement moins coûteuse qu'une comparaison totale.

1.2. Principe de la méthode de dualisation. Critère théorique. Algorithme de référence.

Soit $f = m_1 + m_2 + \ldots + m_q$ une expression polynômiale. Supposons que $g_i = \mu_1 + \mu_2 + \ldots + \mu_k$ soit la duale de $m_1 + m_2 + \ldots + m_i$, écrite sous forme irréductible. Le procédé envisagé consiste à calculer $g_{i+1} = g_i \cdot (m_{i+1}^*)$ sous forme irréductible. La procédure est terminée au calcul de g_q.

Le calcul de la duale d'une fonction écrite sous forme d'une somme de monômes, consiste donc à répéter le calcul plus restreint suivant :

Soit g une fonction booléenne, somme de k monômes irréductibles, soit $m = a_1 a_2 \ldots a_p$ un monôme de p lettres (certaines peuvent correspondre à des compléments de variables), déterminer le polynôme irréductible de la fonction

$$h = g \cdot (m^*) = g \cdot (a_1 + a_2 + \ldots + a_p)$$

avec $g = \mu_1 + \mu_2 + \ldots + \mu_k$

A ce stade, on est tenté de développer et de former les kp produits. Il restera l'élimination des multiples qu'on fera par des séries de comparaisons mutuelles de monômes. Ce qui alourdit donc la méthode, c'est le nombre total de ces comparaisons. On pourrait en avoir C_{kp}^2 (au maximum) (cas de fonctions où les supports de m et de g sont disjoints).

Par exemple pour k = 10 et p = 5 on peut avoir $C_{50}^2 = 1225$ comparaisons (inutiles dans le cas disjoint car aucune élimination n'intervient).

Nous choisirons donc, à titre de critère théorique le nombre de comparaisons en moyenne pour une étape du calcul de duale.

Nous allons et pour partir d'une référence, définir un algorithme où aucune analyse simplificatrice n'intervient.

Algorithme 0 (référence)

Les k monômes de g sont rangés dans k mémoires consécutives, le monôme $m = a_1 a_2 .. a_p$ dans une mémoire.

(1) Former le tableau m^* ayant p mémoires consécutives contenant $a_1, a_2, \ldots, a_p$.

(2) Former $\mu_1 a_1$. Si le résultat est nul continuer avec $\mu_1 a_2$ etc... puis éventuellement $\mu_2 a_1$, .. etc. Ranger le premier monôme non nul ainsi formé dans le tableau h. S'il n'y en a pas le processus s'arrête et h = 0.

(3) Supposons avoir formé dans h, tous les monômes $\mu_i a_\ell$ irréductibles entre eux et non nuls avec : $i < k$, $\ell \leq p$. On formera alors $\rho = \mu_i a_{\ell+1}$ (si $\ell < p$) ou $\mu_{i+1} a_1$ (si $\ell = p$).

Si ce monôme ρ est nul, on retourne à (3) avec ℓ (ou i) augmenté.

Si ρ est non nul on le compare aux monômes de h.

S'il advient que ρ est un multiple d'un monôme h on l'élimine et on repasse à la phase (3).

Si ρ est un diviseur d'un monôme μ de h, μ est éliminé de h et on continue ainsi à supprimer de h tous les multiples de ρ ; ρ est ensuite rangé dans h. On retourne à la phase (3).

(4) Le procédé s'arrête lorsque $i = k$, $\ell = p$.

Evaluation du coût théorique.

Sur les kp produits formés nous désignerons par :

n le nombre des produits non nuls

r le nombre des monômes du résultat.

Les r monômes ont été comparés deux à deux ce qui fait r(r-1)/2 comparaisons (totales).

Les monômes éliminés sont en nombre de n-r.

Bien entendu, il est difficile d'évaluer rigoureusement le nombre de comparaisons qu'il a fallu pour les éliminer. Si l'on voit les choses simplement et si l'on suppose que l'on a formé d'abord les r monômes définitifs, il faudra comparer chacun des n-r autres monômes à ces r monômes, l'élimination ayant lieu en moyenne après r/2 comparaisons.

Nous pouvons donc donner une évaluation approximative du coût.

Coût du produit d'une somme de k monômes par une somme de p lettres, ayant n monômes produits non nuls et r monômes au résultat final.

$$\text{coût} = r(r-1)/2 + (n-r)r/2 = (n-1)r/2$$

Exemple :

$$\begin{cases} g = ab + bd + bf + ace + cd + ad & (k = 6) \\ m = aef & (p = 3) \end{cases}$$

Le nombre des produits est donc : $n = kp = 18$.
On obtient :

$$h = ab + bf + ace + ad + bde + cde + cdf \qquad (r = 7)$$

Le coût théorique est donc

$17 \times 7/2 \neq 60$ comparaisons.

En fait, appliquons l'algorithme. On obtient dans l'ordre, les monômes suivants (certains sont barrés par suite d'élimination) ; ces monômes sont suivis du nombre de comparaisons qu'ils ont nécessitées :

ab (0), ~~abe~~ (1), ~~abf~~ (1), ~~abd~~ (1), bde (1), ~~bdf~~ (2)
~~abf~~ (1), ~~bdf~~ (3), bf (4), ace (3), ~~ace~~ (4), ~~acef~~ (4)
~~acd~~ (4), cde (5), cdf (6), ad (7), ~~ade~~ (7), adf (7)

Le coût réel est :

1 + 1 + 1 + 1 + 2 + 1 + 3 + 4 + 3 + 4 + 4 + 4 + 5 + 6 + 7 + 7 + 7 = 61.

Soit : 61 comparaisons réelles.

2) Procédures améliorées.

2.1. Première amélioration. Algorithme 1.

L'amélioration que nous proposons, repose sur la proposition suivante :

Proposition :

g étant une somme k de monômes irréductibles et $m = a_1 a_2 \ldots a_p$ un monôme quelconque, si l'on range les monômes de g en deux classes α, β, la première consistant de tous les monômes de g ayant au moins une lettre en commun avec m et la seconde tous les autres monômes de g, on obtient alors les monômes irréductibles de la fonction $h = g \cdot (a_1 + a_2 + \ldots + a_p)$ en prenant tous les monômes de la classe α, et tous les produits des monômes de β par les lettres a_ℓ et qui ne soient multiples d'aucun monôme α.

Désignons par $\alpha_1, \alpha_2, \ldots \alpha_q$ les monômes de la classe α et $\beta_{q+1}, \beta_{q+2}, \ldots, \beta_k$ les autres (de classe β).

Nous devons développer :

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_q + \beta_{q+1} + \ldots + \beta_k)(a_1 + a_2 + \ldots + a_p)$$

Nous constatons aisément que :

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_q)(a_1 + a_2 + \ldots + a_p) = \alpha_1 + \alpha_2 + \ldots + \alpha_q$$

et que les monômes α_i ne peuvent se réduire entre eux (hypothèse d'irréductibilité dans g).

Il reste à considérer les produits de :

$$(\beta_{q+1} + \ldots + \beta_k)(a_1 + a_2 + \ldots + a_p).$$

Ces produits sont irréductibles entre eux :
en effet, soient $\beta_j\, a_\ell$ et $\beta_i\, a_r$ deux produits distincts ; donc ou bien $r \neq \ell$ ou bien $r = \ell$ mais $i \neq j$.

Dans le premier cas ($r \neq \ell$) $\beta_j\, a_\ell$ ne peut être un multiple de $\beta_i\, a_r$ que si a_r fait partie de β_j mais alors β_j serait mal classé.

Dans le deuxième cas ($r = \ell$, $i \neq j$) dire que $\beta_i\, a_\ell$ est un multiple de $\beta_j\, a_\ell$ revient à dire (puisque $a_\ell \notin \beta_i, \beta_j$) que β_i est multiple de β_j (ce qui est contraire à l'hypothèse d'irréductibilité de g).

En conséquence les monômes $\beta_j\, a_\ell$ ne peuvent être que comparés aux monômes α_i.

On ne peut avoir α_i multiple de $\beta_j\, a_\ell$ sinon α_i est multiple de β_j. Donc ou bien $\beta_j\, a_\ell$ est un multiple d'un monôme α et est donc éliminé, ou bien il ne l'est pas et fait donc partie du résultat h.

Nous en déduisons l'algorithme :

Algorithme 1. (première amélioration)

k monômes de g occupent k mémoires consécutives
le monôme $m = a_1 a_2 \ldots a_p$ occupe une mémoire.

Première phase.

On parcourt les k monômes de g. Si l'intersection d'un tel monôme avec m est vide, ce monôme est rangé dans un tableau auxilliaire T. Si elle n'est pas vide ce monôme est rangé dans h.

On calcule dans cette phase le nombre q des monômes rangés en h. Il reste k-q monômes dans T.

Deuxième phase.

Constituer à partir de m les p monômes de m^*.

Troisième phase.

Former les produits d'un monôme de T successivement par a_i ($i = 1, 2..p$). Ne conserver que ceux différents de 0 et les comparer partiellement aux seuls q premiers monômes de h pour éventuellement les ranger en h ou les éliminer.

Cherchons à évaluer, l'amélioration obtenue.

Dans la première phase de classement, nous avons à faire pratiquement k comparaisons.

Désignons par n' le nombre des produits non nuls de T par m^*.

Désignons toujours par r le nombre total des monômes définitifs.

Les q premiers monômes de h n'ont exigé aucune comparaison.

Les r-q monômes supplémentaires définitifs ont exigé (r-q) q comparaisons partielles. Les n'-r+q produits éliminés, ont été éliminés après au plus q comparaisons partielles donc en moyenne q/2. Le coût est donc :

$$k + (r-q)\ q + (n'-r+q)\ q/2 = k + (n'+r-q)\ q/2$$

Coût dans l'algorithme I.	
n'	produits non nuls formés $\quad n' \leq (k-q)\ p$
q	monômes invariants (par premier classement)
r	monômes définitifs
k	monômes de g
coût = $k + (n'+r-q)\ q/2$	

Exemple :

Reprenons l'exemple précédent

$$\begin{cases} g = ab + bd + bf + ace + cd + ad & (k = 6) \\ m = aef & (p = 3) \end{cases}$$

La première phase donne (6 comparaisons)

$$\begin{cases} \alpha = ab + bf + ace + ad & (q = 4) \\ \beta = bd + cd & (k-q = 2) \end{cases}$$

On formera $n' = (k-q)\ p = 6$ produits.

Nous savons que $r = 7$

Le coût théorique est alors $6 + (6+7-4)\ 2 = 24$

En fait le calcul réel montre que :

bda	est	éliminé	au bout	de 1	comparaison
bde	est	conservé	"	" 4	"
bdf	est	éliminé	"	" 2	"
cda	est	éliminé	"	" 4	"
cde	est	conservé	"	" 4	"
cdf	est	conservé	"	" 4	"

Cela donne $6 + 19 = 25$ comparaisons réelles

L'amélioration obtenue est importante. On constate que dans le cas où g et m ont des supports disjoints le nombre des comparaisons est seulement égal à k (phase de classement). Il faut signaler en outre que les comparaisons effectuées ne sont que partielles.

2.2. Deuxième amélioration. Algorithme 2.

Nous allons encore améliorer le résultat précédent par la proposition suivante.

Proposition :

Reprenant les notations de la proposition 2.1 si l'on scinde à nouveau la classe α en $p+1$ sous classes repérées chacune par l'entier ℓ ($1 \leq \ell \leq p+1$) : la classe ℓ ($\ell \leq p$) contient les monômes α n'ayant que la lettre a_ℓ en commun avec m, et la classe $p+1$ constituée des monômes α ayant plus d'une lettre en commun avec m, alors le produit $\beta_j a_\ell$ ne peut être éliminé que par des monômes de la classe (ℓ).

En effet si $\beta_j\ a_\ell$ est multiple d'un monôme μ de α, comme $\beta_j\ a_\ell$ n'a que la lettre a_ℓ en commun avec m, c'est que μ qui a des lettres communes avec m ne peut avoir que la lettre a_ℓ commune avec m.

Nous pouvons alors construire un nouvel algorithme.

Algorithme 2.

(k monômes dans g, un monôme m à p lettres). Nous supposerons (théoriquement) que la capacité mémoire est suffisamment grande.

Nous disposons donc d'un tableau h et de p+1 tableaux auxilliaires $T_1, T_2, \ldots, T_p$ et T.

Première phase : classement.

On examine l'un après l'autre chacun des monômes μ_i de g.

- si $\mu_i \cap m = 0$ μ_i est rangé dans T
- si $\mu_i \cap m\ (\neq 0)$ est de degré supérieur ou égal à deux μ_i est rangé dans h.
- si $\mu_i \cap m\ (\neq 0)$ est de degré un, on détermine le rang ℓ $(1 \leqslant \ell \leqslant p)$ de la variable commune et on range μ_i à la fois dans T_ℓ et h.

Deuxième phase.

Construction du tableau m^* à p monômes.

Troisième phase.

On multiplie successivement chaque monôme β de T par les monômes a_ℓ $(1 \leqslant \ell \leqslant p)$.

On conserve les produits βa_ℓ non nuls.

On compare βa_ℓ aux seuls monômes de T_ℓ pour éventuellement le ranger dans h ou l'éliminer.

Essayons d'évaluer l'amélioration (s'il en est).

- La première phase est légèrement plus compliquée que dans l'algorithme précédent.

Le traitement de chacun des k monômes (en vue du classement) exige de manière sensiblement équivalente, deux comparaisons en moyenne. Donc au total 2k comparaisons.

- La troisième phase amène des améliorations. En effet les q monômes (invariants de g) vont occuper p+1 classes. En simplifiant à l'extrême chaque classe occupera en moyenne q/(p+1) monômes. Donc le coût d'élimination ou de conservation des produits βa_ℓ sera divisé par p+1 en moyenne.
D'où :

Coût théorique de l'algorithme 2
(mêmes notations que dans l'algorithme 1)
Coût = 2 k + (n'+r-q) q/2 (p+1)

Reprenons l'exemple précédent :

$$\begin{cases} g = ab + bd + bf + ace + cd + ad \\ m = aef \end{cases}$$

Le classement donne 12 (2 × 6) comparaisons.

$$\begin{cases} \beta = bd + cd \end{cases} \qquad \begin{cases} \alpha_a = ab + ad \\ \alpha_e = \phi \end{cases} \qquad \begin{cases} \alpha_f = bf \\ \alpha_{p+1} = ace \end{cases}$$

Le coût théorique est alors :

$$2 \times 6 + (6+7-4) \cdot 2/4 \not= 12 + 5 = \underline{17} \text{ comparaisons}$$

En fait le calcul donne :

bda	éliminé	après	|	comparaison
bde	conservé	"	0	"
bdf	éliminé	"	1	"
cda	éliminé	"	2	"
cde	conservé	"	0	"
cdf	conservé	"	1	comparaison

Soit : 12 + 5 = 17 comparaisons réelles.

2.3. Algorithmes pratiques. Comparaison.

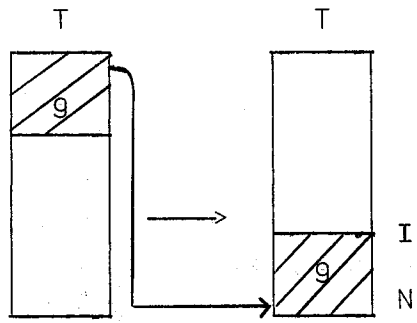
Nous avons négligé jusqu'à présent, la gestion des mémoires et les problèmes de capacité. Dans la pratique il faut en tenir compte. Nous allons donner un bref aperçu des programmes que nous avons écrits surtout en ce qui concerne la gestion des mémoires.

Dans tous les algorithmes nous avons en commun :
le mot m, un tableau m^* a au plus n mémoires (n désignant le nombre des variables) et un tableau T assez grand et partiellement rempli en tête des k monômes de g. On calcule h dans T.

Algorithme 0

On déplace les k mémoires (en tête) de T vers la queue du tableau T.

On peut le symboliser comme suit :

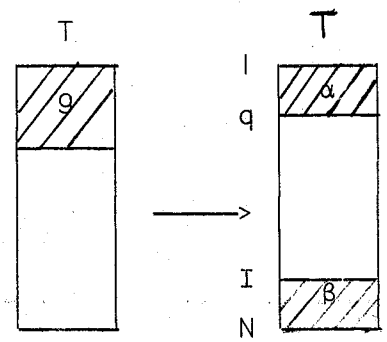


On balaye de I à N les dernières mémoires de T et on en forme les produits par les monômes de m^* . On les range en tête de T conformément à l'algorithme 0. On libère progressivement la queue du tableau T.

Les cas d'empiétements (dépassement de capacité) sont renvoyés à une référence laisée à l'initiative de l'utilisateur (message, utilisation de mémoires auxilliaires : bandes, disques etc...).

Algorithme I

Nous partons toujours dans les mêmes conditions. Mais on classe en deux parties les monômes (en tête) de T en conservant en tête de T les monômes invariants et en queue les monômes β à multiplier.



On balaye de I à N les monômes β en les multipliant par ceux de m^* et on les range éventuellement à la suite de α, après comparaison aux seuls q premiers monômes de T.

Les cas d'empiétements peuvent aussi se produire et sont pareillement déroutés.

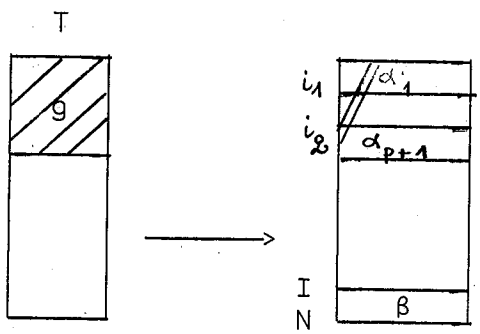
Algorithme 2

Les difficultés sont ici plus grandes, le classement étant plus compliqué.

Version A :

Elle dispose d'autant de mémoires que dans l'algorithme 1.

Simplement la zone α est à chaque étape modifiée de manière à mettre en zones contigues les p+1 classes. Bien entendu ces classes sont repérées par des indices (frontières)



La méthode de classement est alors très lourde surtout pour la programmation.

Version B :

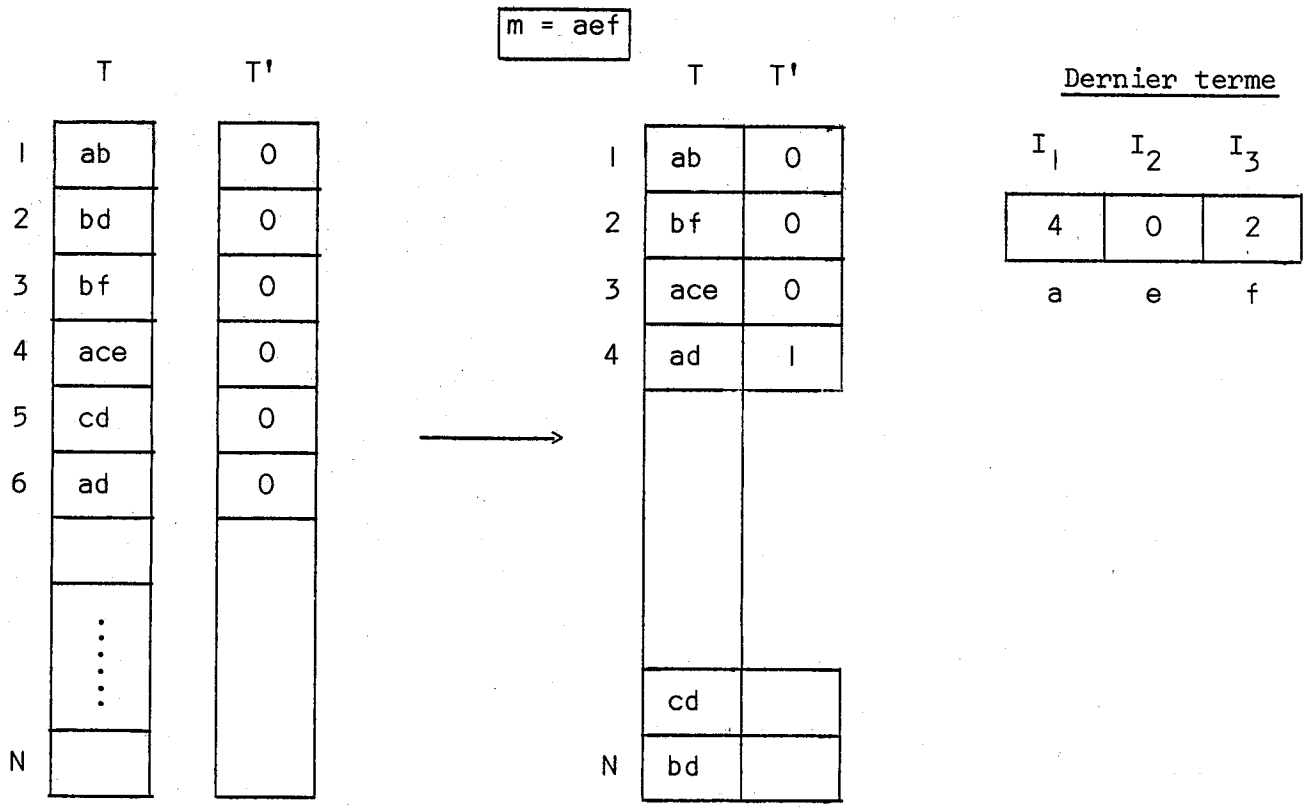
Le tableau T est dédoublé en T'. On fait appel à une technique de listes. On marque dans le tableau T' les références permettant de récupérer les monômes α d'une classe donnée.

Exemple :

En prenant l'exemple traité :

g = ab + bd + bf + ace + cd + ad

On obtient :



Nous avons en face de chacun des monômes α l'adresse du dernier monôme de la même classe. (Le cas d'adresse nulle signifie qu'il n'y en a plus). Les références I_1, I_2, I_3 donnent l'adresse des derniers termes respectivement de la classe a, e, f.

Le produit d'un monôme β par a_ℓ est alors comparé (en remontant les références) très simplement. Des déroutements sont évidemment envisagés.

On peut prévoir que cette deuxième version sera plus rapide au dépens d'un encombrement double de mémoires.

Voici pour terminer quelques résultats (comparatifs en temps de calcul) des divers algorithmes testés sur des fonctions booléennes (calculées par hasard).

Nombre variables	Nombre monômes	Nombre monômes de la duale	Temps algorithmes			
			0	1	2A	2B
5	8	11	1	0	0	0
6	16	12	10	2	1	1
7	26	18	42	3	2	2
8	53	30	260	14	9	6
9	76	95	Dep^T	86	35	22
10	100	300	Dep^T	Dep^T	187	95

Les prévisions théoriques se trouvent confirmées dans ces exemples.

Nous avons également essayé de comparer le calcul des composants premiers de f par double duale à une autre méthode (consensus par balayage sur les variables [28]). Voici quelques résultats en temps.

Nombre variables	Nombre monômes de f	Nombre de composants premiers	Temps	
			Consensus	Double Duale
7	34	27	11	4
8	37	62	37	26
8	58	122	173	31

Il faut signaler que la méthode double duale donne aussi les composants premiers de f^*.

3) Algorithmes annexes.

Nous venons de développer des algorithmes purement algébriques du calcul de la duale d'une fonction booléenne.

Nous allons examiner quelques problèmes annexes : dualisation partielle, problème particulier des graphes, problème de partitions.

3.1. Dualisation partielle.

Le problème dont il s'agit ici est le suivant : on désire calculer les monômes de plus bas degré de la duale d'une certaine fonction, sachant qu'il existe déjà des monômes de degré q.

Les méthodes développées précédemment (algorithme 1 surtout) s'adaptent très bien à ce problème.

Il suffit à chaque stade du calcul de $g.m^*$ de ne considérer que les monômes de g de degré au plus q-1. Les monômes invariants α de g sont bien entendu conservés. Les monômes à multiplier ne sont rangés dans β qu'à la condition que leur degré soit au plus q-2.

Vers la fin, le calcul risque d'être très simplifié en particulier si les monômes de g sont tous de degré q-1 (les multiplications et comparaisons ne sont plus à faire).

Donnons à titre d'exemple, une application concernant le problème de recouvrement minimum (recherche de bases premières, de nombre chromatique...)

On désire chercher les recouvrements minima de l'ensemble $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ par les parties suivantes :

a = {0, 3, 5, 7, 8} b = {0, 1, 2, 3, 4, 6}
c = {1, 2, 5, 6, 9} d = {0, 2, 4, 6, 7}
e = {1, 7, 8, 9} f = {2, 5, 7, 8, 9}
g = {1, 3, 4, 5, 8}

L'ensemble a, b, c est un tel recouvrement d'ordre trois. Cherchons s'il est possible de l'améliorer.

On établit la fonction de recouvrement dont les monômes sont associés aux différentes classes recouvrant successivement chaque sommet :

φ = abd + bceg + cdf + abg + bdg + acfg + bcd + adef + aefg + cef

Il faut calculer les monômes de φ^* (s'ils existent) de degré au plus deux. La somme des trois premiers monômes donne (à partir de l'algorithme 2) la duale suivante :

ac + cd + de + dg + bc + bd + bf + (aef) + (agf)

Les deux derniers monômes sont à éliminer. On rajoute abg. Les monômes ayant une lettre commune au moins avec abg sont alors :

ac + dg + bd + bf.

Ceux qui ont une lettre commune au moins avec bdg sont :

dg + bd + bf

Ceux qui restent après examen de acfg sont :

dg + bf

Après examen de bcd, il reste :

dg + bf. Après examen de adef il reste :

bf qui reste encore après examen de aefg et cef.

Il existe donc un (et un seul) recouvrement d'ordre deux.

Remarque :

Nous avons supposé qu'on connaissait déjà un monôme de la duale. On peut, en fait, en déterminer un simplement au départ (par exemple par ordre lexicographique).

3.2. Problèmes relatifs aux graphes. Fonctions croissantes homogènes de degré deux.

Dans le cas des graphes, la recherche des ensembles intérieurement stables, consiste à dualiser une fonction homogène croissante de degré deux. On peut peut-être simplifier encore le problème. Considérons en effet un ordre arbitraire sur les variables : pour chaque variable a_i on considère tous les monômes $a_i\ a_j$ $(j > i)$.

On peut avoir la duale de $\sum_{j>i} a_i\ a_j$ qui n'est autre que $(a_i + \prod_{j>i} a_j)$.

On est donc ramené, si n est le nombre de variables (ou de sommets) à calculer n-1 au plus produits de fonction du type : $a_i + \mu_i \quad i = 1, 2, .. n-1$ où μ_i est un monôme.

Cela conduit donc au problème restreint suivant : calculer, a étant une variable et m = bc ... ℓ un monôme ne contenant pas a, le produit :

h = g . (a+m) où g est une somme de monômes irréductibles.

Nous considèrerons un procédé tout à fait analogue à celui qui précède.

Nous classerons les monômes de g en 4 parties

- Dans la partie I nous mettrons les monômes multiples de a et m.
- Dans la partie II les monômes multiples de a et non de m.
- Dans la partie III les monômes multiples de m et non de a.
- Dans la dernière partie IV les autres monômes que nous noterons μ_i.

Il est évident que les monômes du type I ou II ou III sont des monômes irréductibles de h. Ils ne peuvent d'une part être éliminés entre eux, et ne peuvent être éliminés comme multiples de μ_i a ou μ_i bc .. ℓ (sinon ils seraient multiples de μ_i).

Considérons alors les monômes nouveaux provenant d'un produit μ_i a ou μ_i bc .. ℓ.

Nous pouvons voir que deux monômes μ_i a et μ_j bc ... ℓ sont non comparables entre eux. En effet dire que μ_i a est un multiple de μ_j bc ... ℓ c'est dire que μ_i est un multiple de bc ... ℓ (absurde). Dire que μ_j bc .. ℓ est un multiple de μ_i a c'est dire que μ_j est un multiple de a (absurde).

De la même manière μ_i a et μ_j a sont non comparables sinon μ_i et μ_j le seraient.

Par contre μ_i bc .. ℓ et μ_j bc ... ℓ peuvent être comparables entre eux.

Montrons que si μ_i a est éliminé, il ne peut l'être que par un monôme de type II. En effet il ne peut être éliminé par un monôme nouveau ; il ne peut être non plus éliminé par un monôme de type I ou III sinon c'est que $\mu_i \in$ III.

Un monôme, maintenant, du type μ_i bc .. dℓ ne peut être éliminé que par un monôme de type III ou par un autre monôme nouveau du type μ_j bcdℓ.

Nous considérerons finalement cinq classes : I, II, III, III', IV. Nous rangerons les monômes de g dans les classes I, II, III, IV. Nous multiplierons ensuite chaque monôme de la classe IV d'abord par a. Nous comparerons le produit aux seuls monômes de type II pour éventuellement le retenir. Nous multiplierons ensuite ce monôme par bc .. ℓ . Le résultat sera comparé aux monômes du type III. Si cette comparaison ne l'élimine pas, on continuera de le comparer aux monômes de III' pour éventuellement le retenir en III' ou éliminer des monômes de III'.

Nous ne faisons qu'ébaucher l'algorithme, et nous donnerons un exemple complet à la main.

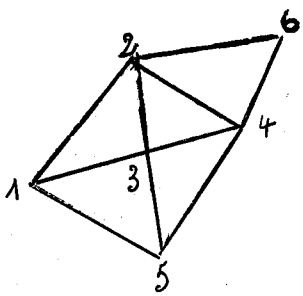


Fig. 1.

Soit par exemple le graphe de la figure 1 dont la fonction booléenne associée est :

$$f = a_1(a_2+a_3+a_5) + a_2(a_3+a_4+a_6) + a_3(a_4+a_5) + a_4(a_5+a_6).$$

La duale consiste donc à calculer :

$$(a_1+a_2\ a_3\ a_5).(a_2+a_3\ a_4\ a_6)\ (a_3+a_4\ a_5).(a_4+a_5\ a_6)$$

$g_1 = a_1 + a_2\ a_3\ a_5$ à multiplier par $a_2 + a_3\ a_4\ a_6$

I	a_2 II	$a_3\ a_4\ a_6$ III	III'	IV
	$a_2\ a_3\ a_5$			a_1
nouveaux	$a_1\ a_2$		$a_1\ a_3\ a_4\ a_6$	

D'où

$g_2 = a_2\ a_3\ a_5 + a_1\ a_2 + a_1\ a_3\ a_4\ a_6$ (à multiplier par $a_3 + a_4\ a_5$).

I	a_3 II	$a_4\ a_5$ III	III'	IV
	$a_2\ a_3\ a_5$ $a_1\ a_3\ a_4\ a_6$			$a_1\ a_2$
produits nouveaux	$a_1\ a_2\ a_3$		$a_1\ a_2\ a_4\ a_5$	

d'où

$g_3 = a_2\ a_3\ a_5 + a_1\ a_3\ a_4\ a_6 + a_1\ a_2\ a_3 + a_1\ a_2\ a_4\ a_5$ (à multiplier par $a_4 + a_5\ a_6$).

I	a_4 II	$a_5\ a_6$ III	III'	IV
	$a_1\ a_3\ a_4\ a_6$ $a_1\ a_2\ a_4\ a_5$			$a_2\ a_3\ a_5$ $a_1\ a_2\ a_3$
nouveaux	$a_2\ a_3\ a_4\ a_5$ $a_1\ a_2\ a_3\ a_4$		$a_2\ a_3\ a_5\ a_6$ $a_1\ a_2\ a_3\ a_5\ a_6$	

Au total nous obtenons

$$g = f^{+} = a_1 a_3 a_4 a_6 + a_1 a_2 a_4 a_5 + a_2 a_3 a_4 a_5 + a_1 a_2 a_3 a_4 + a_2 a_3 a_5 a_6$$

3.3. Recherche de partitions.

Nous avons établi un théorème de structure des fonctions booléennes croissantes (chapitre III). Dans des conditions analogues, on a un théorème de structure des fonctions croissantes par somme et produits direct [15]. Enfin plus généralement le problème de détermination des parties connexes d'un ensemble fini (avec relation de voisinage) ou celui de la détermination de la borne supérieure (au sens du treillis), d'un certain nombre de partitions se ramène à ceci :

On considère un ensemble A et une certaine famille α de parties $A_1, A_2, \ldots, A_q$. Déterminer la partition de A définie par l'équivalence :

$(a \neq b)$ $a \equiv b$ s'il existe une suite $A_{i_1}, A_{i_2}, \ldots A_{i_p}$ de parties dans α telles que

$$a \in A_{i_1} \quad , \quad b \in A_{i_p} \quad , \quad A_{i_k} \cap A_{i_{k+1}} \neq \phi .$$

Nous adopterons le procédé récursif suivant : désignons par α_k la famille partielle : $A_1, \ldots A_k$ $(k < q)$ et supposons avoir déterminé les classes de la partition associée à α_k : soient $S_1, S_2, \ldots, S_m$ ces classes (nous gardons seulement les classes à plus d'un élément). On "rajoute" la partie $S = A_{k+1}$. On balaye $S_1, S_2, \ldots S_m$.

Soit S_i la première classe telle que $S \cap S_i \neq \phi$. On forme l'union de S à S_i et on continue à balayer $S_{i+1}, \ldots, S_m$ celles ayant une intersection non vide avec S sont unies à la classe S_i puis supprimées.

Si toute classe S_i a une intersection vide avec S alors S est rajoutée à la suite de S_m. On obtient alors la partition associée à α_{k+1}.

Le processus s'arrête à k = q.

Exemple :

Soit l'ensemble {a, b, c, d, e, f, g, h, k} et les paquets de voisinage :

abc, ef, bch, ah, eg, bk

On forme

$$abc \xrightarrow{ef} \begin{cases} abc \\ ef \end{cases} \xrightarrow{bch} \begin{cases} abch \\ ef \end{cases} \xrightarrow{ah} \begin{cases} abch \\ ef \end{cases} \xrightarrow{eg} \begin{cases} abch \\ efg \end{cases}$$

$$\xrightarrow{bk} \begin{cases} abchk \\ efg \end{cases}$$

Dans la réunion de ces classes, il manque d.

Donc la partition est :

{abchk, d, efg}

CHAPITRE VI

SUR UNE STRUCTURE ALGEBRIQUE DES CHEMINEMENTS. PSEUDO-TREILLIS.

Nous nous intéresserons dans ce chapitre aux chemins simples et accessoirement aux circuits simples d'un réseau. On entend par chemin simple ou respectivement circuit simple toute suite d'articulations $a_1\ a_2\ a_3\ \ldots\ a_p$ telle que

1^{er}) il existe un couple de connexions au moins de a_k à a_{k+1} $(k=1,\ldots,\ p-1)$

2^{e}) les articulations sont toutes distinctes ($a_k \neq a_{k'}$ si $k \neq k'$) dans le cas de chemins simples. Seules les articulations a_1 et a_p sont les mêmes s'il s'agit d'un circuit simple.

Le chemin simple est dit d'origine a_1 et d'extrémité a_p.

Les chemins simples interviennent dans de nombreux problèmes :

- analyse ou synthèse de réseaux de contacts, orientés ou non.
- analyse ou synthèse de réseaux de Kirchoff.
- distance sur un réseau routier (éventuellement orienté : problème des villes).
- problème de flots dans un graphe.
- automates d'états finis.
- problèmes stochastiques des systèmes ayant un nombre fini d'états.

Il existe une nombreuse littérature à propos de ces problèmes. Les solutions proposées sont la plupart du temps combinatoires et cachent un caractère algébrique systématique.

Par ailleurs les structures algébriques que l'on a proposées la plupart du temps, ont consisté à se ramener à des théories classiques comme celles des groupes. Malheureusement cela n'est intéressant que dans le cas des réseaux symétriques (c'est-à-dire considérés comme non orientés) de sorte que la théorie perd de sa valeur lorsque la notion d'orientation intervient.

Nous allons utiliser une structure non aussi classique que celle des groupes (bien qu'elle ait été étudiée dans un tout autre sens [10]) mais qui rend bien compte des problèmes où la notion de chemin simple (ou circuit simples) intervient.

1) Pseudo-treillis. Description. Exemples.

1.1. Définitions. Remarques.

Pseudo-treillis.

Un pseudo-treillis (distributif) est un ensemble E muni de deux opérations internes partout définies ; la première notée + (et désignée par somme), la seconde notée par un point • (et désignée par produit) vérifient les règles suivantes :

I. E est un + demi-treillis (associativité, commutativité et idempotence de +).

II. E est un monoïde pour • (associativité du produit). En outre le produit est distributif à droite et à gauche par rapport à la somme.

III. La règle d'absorption suivante est vérifiée :

$$\forall a \quad \forall b \qquad a + (a \cdot b) = a + (b \cdot a) = a .$$

Un tel pseudo-treillis sera noté (E, +, •).

On rencontre de telles structures sous le nom de gerbiers dont les éléments sont quasi-entiers (gerbiers quasi-entiers [10]). Nous avons donné le nom de pseudo-treillis en raison de propriétés assez voisines avec celles des treillis distributifs.

Eléments neutres.

On peut avoir des éléments neutres pour ces opérations. On notera 0 s'il existe l'élément neutre de la somme et 1 celui du produit.

On vérifie à cause de III que $0 \cdot a = a \cdot 0 = 0$ pour tout a. On peut donc supposer que $0 \neq 1$ sinon E n'a qu'un élément.

On vérifie également que $1 + a = 1$ pour tout a.

Adjonction d'éléments neutres.

S'il manque un ou les deux éléments neutres on pourra toujours en adjoindre en posant :

$$\left.\begin{aligned} 0+a &= a \\ 0\cdot a &= 0 \end{aligned}\right\} \text{ pour tout a et } \left\{\begin{aligned} 0+0 &= 0 \\ 0\cdot 0 &= 0 \end{aligned}\right.$$

et de la même manière

$$\left.\begin{aligned} 1+a &= 1 \\ 1\cdot a &= a\cdot 1 = a \end{aligned}\right\} \text{ pour tout a et } \left\{\begin{aligned} 1+1 &= 1 \\ 1\cdot 1 &= 1 \end{aligned}\right.$$

On désignera, E étant un pseudo-treillis, par E^{01} le pseudo-treillis soit égal à E si E admet les deux éléments neutres, soit à E auquel on a adjoint 0 si E n'admet que le seul élément neutre 1, soit à E auquel on a adjoint 1 si E n'admet que le seul élément neutre 0, soit à E aux quels on a adjoint les deux éléments neutres si E n'en a pas.

Ordre dans un pseudo-treillis.

L'ensemble E est ordonné par l'opération + du demi treillis et on posera :

$$a \leqslant b \iff a + b = b$$

Cet ordre est isotone par rapport à la somme et au produit. C'est-à-dire :

$a \leqslant b \implies a+c \leqslant b+c$ et $a \cdot c \leqslant b \cdot c$ et $c \cdot a \leqslant c \cdot b$

En outre la loi d'absorption équivaut à affirmer que :

$a \cdot b \leqslant a$ et $b \cdot a \leqslant a$

1.2. Exemples de pseudo-treillis.

Bien entendu les treillis distributifs, les algèbres de Boole sont des pseudo-treillis (commutatifs, idempotents).

Nous citerons d'autres exemples intéressants :

Exemple 1 : Pseudo-treillis $(R^+, \inf, +)$.

L'ensemble des réels positifs est un pseudo-treillis pour les opérations inf et +. La règle I est évidente. La règle II l'est également pour l'associativité.
Nous avons en outre $a + \inf(b, c) = \inf(a+b, a+c)$. Enfin la règle III se vérifie car $\inf(a, a+b) = a$.

Les éléments neutres sont $+\infty$ pour inf et 0 pour +. L'ordre associé est total : c'est l'ordre dual de l'ordre ordinaire.

Exemple 2 : Pseudo-treillis $([0,1], \sup, \cdot)$.

L'ensemble des réels du segment $[0,1]$ forme un pseudo-treillis, comme on peut le vérifier, pour les opérations sup et $\cdot$ (produit ordinaire).

Cet exemple est intéressant, sous l'angle des probabilités. Il y a des éléments neutres 0 pour sup et 1 pour le produit.

L'ordre associé est total : c'est l'ordre habituel des réels.

Exemple 3 : Pseudo-treillis $(N^+, pgcd, \cdot)$.

L'ensemble des entiers naturels (positifs) est un pseudo-treillis vis à vis des opérations pgcd et produit ordinaire. La vérification de la distributivité est immédiate : $a \cdot pgcd(c, d) = pgcd(ac, ad)$

La règle d'absorption se vérifie également :

$pgcd(a, a \cdot b) = a$

Il n'y a pas d'élément neutre pour le pgcd. 1 est élément neutre du produit. L'ordre associé, est partiel : $a \leqslant b$ équivaut à : b divise a. Cet ordre est cependant réticulé.

1.3. Pseudo-treillis décomposable.

Cette notion qui nous sera utile par la suite ne fait intervenir des hypothèses que sur l'opération + du demi treillis.

Définition :

Le pseudo-treillis E est dit décomposable si pour tout triplet d'éléments x, y, z vérifiant $x \leqslant y + z$ alors il existe η et ζ avec :
$x = \eta + \zeta$ et $\eta \leqslant y$, $\zeta \leqslant z$

Rappelons qu'une partie P d'un ensemble ordonné est fermée si contenant x elle contient tout élément y tel que $y \leqslant x$.

Proposition :

Si P et Q sont deux parties fermées d'un pseudo-treillis E décomposable alors P + Q est fermée.

Soit $t \in P + Q$; donc $t = x + y$ avec $x \in P$ et $y \in Q$. Soit z tel que $z \leqslant t$. Donc $z \leqslant x + y$ et $z = \xi + \eta$ avec $\xi \leqslant x$ et $\eta \leqslant y$ en vertu de la décomposabilité de E. Comme P et Q sont fermées $\xi \in P$ et $\eta \in Q$. Donc $z \in P + Q$.

2) Matrices sur un pseudo-treillis. Généralisation du théorème de Lunc.

2.1. Matrices sur un pseudo-treillis E. Opérations usuelles.

Soit E un pseudo-treillis. Nous considèrerons l'ensemble $\mathfrak{M}_{n,p}$ des matrices à n lignes et p colonnes dont les éléments sont dans E^{01}.

On peut définir la somme de deux matrices A, B $\in \mathfrak{M}_{n,p}$. C'est la matrice c dont les éléments c_{ij} valent :

$$c_{ij} = a_{ij} + b_{ij}$$

Cette somme est associative, commutative, idempotente. La matrice $0 \in \mathfrak{M}_{n,p}$ dont tous les éléments sont nuls est élément neutre de la somme.

Cette opération étant une opération de demi treillis, l'ensemble $\mathfrak{M}_{n,p}$ est ordonné par :

$$A \leqslant B \iff A + B = B$$

On peut définir le produit d'une matrice A de $\mathfrak{M}_{np}$ par une matrice B de $\mathfrak{M}_{pq}$. C'est la matrice C de $\mathfrak{M}_{n,q}$ notée C = A B et dont les éléments valent :

$$c_{ij} = a_{i,1} \cdot b_{1,j} + a_{i,2} \cdot b_{2,j} + \ldots + a_{in}\, b_{nj} = \sum_{k=1}^{n} a_{ik}\, b_{kj}$$

(les sommes utilisées sont celles du pseudo-treillis).

Le produit est associatif et distributif par rapport à la somme (chaque fois qu'il est défini). Il est en outre compatible avec l'ordre.

$$A \leqslant B \Longrightarrow A \cdot C \leqslant B \cdot C \quad \text{et} \quad D \cdot A < D \cdot B$$

$$(A, B \in \mathfrak{M}_{n,p}\ ,\ C \in \mathfrak{M}_{p,q}\ ,\ D \in \mathfrak{M}_{r,n})$$

Cette dernière propriété tient à l'isotonie de l'ordre de E par rapport aux opérations + et • dans E.

Lorsqu'on se place sur $\mathcal{M}_{n,n}$, le produit matriciel devient loi interne partout définie. Notons que la règle d'absorption n'est pas vérifiée comme le montre l'exemple :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Il y a dans $\mathcal{M}_{n,n}$ une <u>matrice unité I</u> celle dont tous les éléments diagonaux sont 1 les autres étant nuls.

Une matrice A est dite <u>surunitaire</u> si $A \geqslant I$ ou, en d'autres termes si tous les éléments diagonaux de A sont 1.

On désignera par A^k (k entier > 0) le produit de k facteurs A. On vérifie (par récurrence par exemple) que :

$$(A+I)^k = I + A + A^2 + \ldots + A^k$$

Si A est surunitaire, cela donne :

$$A^k = A + A^2 + \ldots + A^k$$

2.2. <u>Généralisation du théorème de Lunc</u> [17] [23].

Le théorème, suivant, a été démontré par Lunc dans le cas où E est une algèbre de Boole. Il est valable sur un pseudo-treillis.

Théorème :

A étant une matrice carrée d'ordre n sur un pseudo-treillis E^{01}, la suite des matrices

$$S_k = A + A^2 + \ldots + A^k$$

devient stationnaire à partir du rang au plus n - 1 si A est surunitaire, au plus n autrement.

Nous constatons que $S_k = A + A^2 + \ldots + A^k$ peut s'écrire encore $S_k = A(I+A+\ldots+A^{k-1}) = A\cdot(I+A)^{k-1}$.

Désignons par A_1 la matrice I + A ; elle est surunitaire. Comme $A_1^{k-1} = A_1 + A_1^2 + \ldots + A_1^{k-1}$, il suffit de démontrer le théorème dans le cas où A est surunitaire.

Pour cela il suffira de démontrer que les termes non diagonaux $a_{ij}^{(k)}$ de A^k vont devenir stationnaires à partir du rang n - 1 au plus (les termes diagonaux $a_{ii}^{(k)}$ valent 1 quelque soit k).

Mais nous allons, encore simplifier : si l'on peut démontrer que pour toute matrice surunitaire d'ordre n les éléments non diagonaux de la dernière ligne $a_{nj}^{(k)}$ de A^k deviennent stationnaires à partir du rang au plus n - 1, le théorème sera prouvé.

En effet considérons la matrice (de permutation) T_{ni} déduite de la matrice unité I en permutant les lignes n et i. On vérifie 1) que $T_{ni}\ T_{ni} = I$ 2) que la matrice $B = T_{ni}\ A\ T_{ni}$ se déduit de A en permutant les lignes i, n et les colonnes i, n : elle reste donc surunitaire 3) $B^k = T_{ni}\ A^k\ T_{ni}$ grâce à la remarque 1.

Donc $\begin{cases} b_{nj}^{(k)} = a_{ij}^{(k)} & \text{si} \quad j \neq i \quad \text{et} \quad j \neq n \\ b_{nn}^{(k)} = a_{ii}^{(k)} = 1 \\ b_{ni}^{(k)} = a_{in}^{(k)} \end{cases}$

On peut donc considérer tout élément non diagonal $a_{ij}^{(k)}$ comme un élément de la n-ème ligne d'une matrice B^k où B (surunitaire) se déduit de A par permutation combinée de lignes et colonnes.

Soit alors A matrice surunitaire d'ordre n. Démontrons, par récurrence, que la dernière ligne de A^k stationne au rang au plus n - 1.

Cela est vrai si n = 2

$$A = \begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix} \qquad A^2 = \begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix}$$

Donc $A^2 = A$ d'où $A^p = A \quad (\forall\, p > 0)$

Supposons le théorème vrai à l'ordre n - 1 et découpons par blocs les matrices A et A^k selon :

$$A = \begin{pmatrix} B_1 & C_1 \\ L_1 & 1 \end{pmatrix} \qquad A^k = \begin{pmatrix} B_k & C_k \\ L_k & 1 \end{pmatrix}$$

avec $B_1, B_k \in \mathfrak{M}_{n-1,\, n-1}$ et surunitaires

$C_1, C_k \in \mathfrak{M}_{n-1,\, 1}$

$L_1, L_k \in \mathfrak{M}_{1,\, n-1}$

Le calcul, par blocs, de $A^{k+1} = A^k \cdot A$ donne :

$$(1) \quad L_{k+1} = L_k B_1 + L_1$$

or B_1 est surunitaire $B_1 \geqslant I$ donc $L_k B_1 \geqslant L_k I = L_k$. Par suite

$$L_{k+1} \geqslant L_k \geqslant L_{k-1} \geqslant \ldots \geqslant L_2 \geqslant L_1$$

Dans la relation (1) L_1 est redondant d'où :

$$L_{k+1} = L_k B_1$$

Et l'on tire :

$$L_{k+1} = L_1 B_1^k$$

B_1 étant une matrice surunitaire, d'ordre $n - 1$, B_1^k stationne d'après la récurrence à partir du rang au plus $n - 2$; donc L_k stationne à partir du ran au plus $n - 1$. Le théorème est démontré.

Remarques :

Dans la pratique on accélère la convergence en considérant les suites suivantes :

- si A est surunitaire, on considère la récurrence :

$S'_p = (S'_{p-1})^2$ avec $S'_1 = A$

La limite stationnaire est atteinte dès que $2^{p-1} \geqslant n-1$

- si A n'est pas surunitaire, on considère la récurrence :

$S'_p = S'_{p-1} + (S'_{p-1})^2$ et là encore la limite stationnaire est atteinte dès que $2^{p-1} \geqslant n$.

Nous terminerons, ce paragraphe, en donnant l'interprétation des termes de la limite stationnaire S_∞ associés à la matrice A d'ordre n.

Définitions :

A étant une matrice carrée d'ordre n, les indices étant des entiers choisis dans l'intervalle $[1, n]$ on désigne par :

- sous-terme de permutant de A entre les indices i et j toute quantité $a_{ii_1} \circ a_{i_1 i_2} \circ \ldots \circ a_{i_p j}$ associée à une suite quelconque $i\ i_1\ i_2 \ldots i_p\ j$ d'indices. La longueur de ce sous-terme sera par définition p + 1 (nombre d'indices de la suite diminué d'une unité).

- terme de permutant de A entre i et j tout sous-terme de permutant entre ces mêmes indices lorsque la suite $i\ i_1\ i_2 \ldots i_p\ j$ présente la particularité :

$$(E) \quad \begin{cases} i_k \neq i_{k'} \quad \text{si} \quad k \neq k' \quad \text{et} \quad i_k \neq i,\ i_k \neq j \quad \text{pour tout} \\ k = 1, \ldots . p \end{cases}$$

permutant de A entre i et j, la somme de tous les termes de permutants de A entre i et j. Cette quantité notée P_{ij} a un sens, le nombre des termes de permutants, entre i et j, étant manifestement fini.

Proposition 1 :

Si s est un sous-terme de permutant de A entre i et j alors $P_{ij} + s = P_{ij}$.

En effet s a été construit à partir d'une suite d'indices schématisée i I j. Si cette suite présente la particularité (E) alors s est un terme de permutant qu'on a déjà sommé dans P_{ij}. Si cette suite ne présente pas la particularité (E) on peut extraire une suite i J j présentant cette particularité et telle que deux indices consécutifs dans cette nouvelle suite soient consécutifs au moins une fois dans la suite initiale. Le terme t de permutant associé à cette suite i J j vérifie alors :

$$s \leqslant t \leqslant P_{ij} \qquad \text{donc} \qquad P_{ij} + s = P_{ij}$$

Proposition 2 :

Le terme $a_{ij}^{(k)}$ de la matrice A^k est la somme de tous les sous-termes de permutants de A de longueur k entre i et j.

Désignons par $p_{ij}^{(k)}$ la somme de ces sous-termes ; cela a un sens car leur nombre est fini. Nous avons :

$$p_{ij}^{(1)} = a_{ij}^{(1)} = a_{ij}$$

Si $p_{ij}^{(k-1)} = a_{ij}^{(k-1)}$ alors soit un sous-terme de permutant de longueur k, entre i et j, associé à la suite d'indices i I j. Si ℓ est le dernier indice de I on a ($I = L\ell$) $t_{iIj} = t_{iL\ell} \cdot a_{\ell j}$

On en déduit :

$$p_{ij}^{(k)} = \sum_{\substack{I \\ |I|=k-1}} t_{iIj} = \sum_{\ell=1}^{n} \left(\sum_{\substack{L \\ |L|=k-2}} t_{iL\ell} \right) \cdot a_{\ell j}$$

D'où

$$p_{ij}^{(k)} = \sum_{\ell=1}^{n} p_{i\ell}^{(k-1)} \cdot a_{\ell j} = \sum_{\ell=1}^{n} a_{i\ell}^{(k-1)} \cdot a_{\ell j} = a_{ij}^{(k)}$$

Conséquences 1 :

Les éléments de la matrice stationnaire S_∞ associée à A ne sont autres que les divers permutants de A.

En effet la limite stationnaire associée à A n'est autre que :

$A + A^2 + \ldots + A^p$ (avec $p = n - 1$ si A est surunitaire et $p = n$ sinon)

Le terme (i, j) de cette suite stationnaire est la somme de tous les sous-termes de permutants entre i et j et de longueurs 1, 2, ...p. Il est par ailleurs évident que les termes de permutants de A entre i et j sont au plus de longueur p. Cela suffit à démontrer la propriété.

2)

Entre les permutants de A nous avons l'inégalité :

$$P_{ij} \circ P_{k\ell} \leqslant P_{i\ell}$$

Cela tient simplement au fait que

$$S_\infty + S_\infty^2 = S_\infty$$

Applications :

Dans un réseau à n articulations (chaque articulation étant désignée par un indice variant de 1 à n) où un problème de chemins simples intervient, certains renseignements peuvent être attachés à chaque chemin simple, par l'intermédiaire d'un pseudo-treillis où l'opération produit est associée aux divers éléments d'un chemin simple, et l'opération somme aux divers chemins simples de mêmes extrémités. On peut alors renseigner le réseau au moyen d'une matrice A d'ordre n, sur le pseudo-treillis et donnant les renseignements élémentaires sur les chemins de longueur 1. La limite stationnaire donnera les renseignements relatifs aux chemins simples joignant tout couple (i, j) d'articulations.

A titre d'exemple, considérons le problème des plus courtes distances sur un réseau (routier par exemple) d'un croisement à un autre.

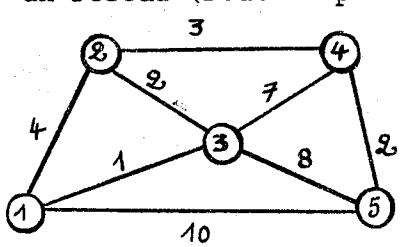


Figure 1.

On se placera dans le pseudo-treillis $(R^+, \inf, +)$ [exemples 1.2]

La matrice des distances, sans croisements intermédiaires, définissant le réseau (Figure 1) n'est autre que :

$$A = \begin{array}{c|ccccc} 1 & 0 & 4 & 1 & \infty & 10 \\ 2 & 4 & 0 & 2 & 3 & \infty \\ 3 & 1 & 2 & 0 & 7 & 8 \\ 4 & \infty & 3 & 7 & 0 & 2 \\ 5 & 10 & \infty & 8 & 2 & 0 \end{array}$$

Elle est surunitaire, d'ordre 5. La stationnarité est atteinte à l'ordre 4. On calcule A^2, puis A^4 dans le pseudo-treillis. On obtient :

$$A^4 = \begin{vmatrix} 0 & 3 & 1 & 6 & 8 \\ 3 & 0 & 2 & 3 & 5 \\ 1 & 2 & 0 & 5 & 7 \\ 6 & 3 & 5 & 0 & 2 \\ 8 & 5 & 7 & 2 & 0 \end{vmatrix}$$

Le terme (i, j) de cette matrice donne la plus courte distance du croisement i, au croisement j.

La méthode est extrêmement simple. Elle résulte du caractère systématique de la structure algébrique sous-jacente.

Bien entendu, dans cet exemple il est intéressant d'avoir la distance minimum, mais également un où les chemins réalisant cette distance.

Le moyen de retrouver ces chemins est intéressant car il se généralise pour d'autres problèmes.

Soient s_{ij} les termes de la limite stationnaire et a_{ij} les termes de la matrice initiale.

On forme les quantités $s_{ij} - s_{ik}$ $(k \neq j)$ qu'on compare à a_{kj}. Chaque fois qu'il y a égalité (et seulement dans ces cas) on peut affirmer qu'il existe un chemin de distance minimum s_{ij} partant de i à j et dont l'avant dernier sommet est k.

Exemple :

$$s_{15} = 8 \qquad s_{14} = 6 \qquad s_{13} = 1 \qquad s_{12} = 3 \qquad s_{11} = 0$$

Seule la différence $s_{15} - s_{14} = a_{45}$.

On prend le calcul sur s_{14}. Seule la différence $s_{14} - s_{13} = a_{34}$ etc...

On obtient le chemin (unique dans l'exemple) 1, 3, 2, 4, 5.

2.3. Méthode des réductions et des concentrations.

Si l'on veut mettre en oeuvre, le calcul de la limite stationnaire S_∞ d'une matrice A et particulièrement en machine, on est obligé de procéder par récurrence :

$$S_{k+1} = S_k + S_k^2$$

utiliser en conséquence, deux tableaux l'un servant à stocker S_k, l'autre servant à calculer S_{k+1}, faire enfin des transferts de tableaux.

On peut éviter cela et utiliser, un seul tableau. On utilisera deux procédés : concentration et réduction.

La méthode de concentration est une méthode de récurrence algorithmique utilisant un seul tableau T comme mémoire de manoeuvre et dont les éléments de mémoire sont notés T_{ij}.

On initialise le tableau T aux valeurs de la matrice A et on pose $k = 1$.

On passe du tour k au tour k + 1 comme suit.

En balayant d'abord sur l'indice i de ligne puis sur l'indice j de colonne, on modifie chaque composante T_{ij} selon :

$$T_{ij} := T_{ij} + \sum_{\ell=1}^{n} T_{i\ell} \cdot T_{\ell j}$$

On s'arrête dès que $2^{k-1} \geq n$ (cas d'une matrice quelconque).

Les composantes du tableau final ne sont autres que les termes de S_∞.

Pour le démontrer appelons β_{ij}^{k} les composantes du tableau après le tour k. Appelons a_{ij}^{k} les termes de S_k ; nous avons les relations de récurrence :

$$a_{ij}^{(k+1)} = a_{ij}^{(k)} + \sum_{\ell=1}^{n} a_{i\ell}^{(k)} \cdot a_{\ell j}^{(k)}$$

et successivement :

$$i < j \qquad \beta_{ij}^{(k+1)} = \beta_{ij}^{(k)} + \sum_{\ell=1}^{i-1} \beta_{i\ell}^{(k+1)} \cdot \beta_{\ell j}^{(k+1)} + \sum_{\ell=i}^{j-1} \beta_{i\ell}^{(k+1)} \cdot \beta_{\ell j}^{(k)} + \sum_{\ell=j}^{n} \beta_{i\ell}^{(k)} \cdot \beta_{\ell j}^{(k}$$

$$i = j \qquad \beta_{ii}^{(k+1)} = \beta_{ii}^{(k)} + \sum_{\ell=1}^{i-1} \beta_{i\ell}^{(k+1)} \cdot \beta_{\ell i}^{(k+1)} + \sum_{\ell=i}^{n} \beta_{i\ell}^{(k)} \cdot \beta_{\ell i}^{(k)}$$

$$j < i \qquad \beta_{ij}^{(k+1)} = \beta_{ij}^{(k)} + \sum_{\ell=1}^{j-1} \beta_{i\ell}^{(k+1)} \cdot \beta_{\ell j}^{(k+1)} + \sum_{\ell=j}^{i-1} \beta_{i\ell}^{(k)} \cdot \beta_{\ell j}^{(k+1)} + \sum_{\ell=i}^{n} \beta_{i\ell}^{(k)} \cdot \beta_{\ell j}^{(k}$$

Les valeurs initiales $a_{ij}^{(1)}$ et $\beta_{ij}^{(1)}$ étant égales, on constate aisément à partir de ces relations que :

$$a_{ij}^{(k)} \leqslant \beta_{ij}^{(k)} \qquad \forall\, i,\ j,\ k$$

et qu'en outre $\beta_{ij}^{(k)} \leqslant a_{ij}^{\infty}$ (terme général de S_∞).

Cela suffit à montrer que l'algorithme converge vers la solution S_∞. On peut même gagner des tours.

Voyons le, sur l'exemple précédent (matrice des distances) du réseau de la figure 1. On obtient après 1 tour d'algorithme (les modifications des éléments de A sont marquées à droite d'une flèche)

$$A^{(2)} = \begin{vmatrix} 0 & 4 \to 3 & 1 & \infty \to 6 & 10 \to 8 \\ 4 \to 3 & 0 & 2 & 3 & \infty \to 5 \\ 1 & 2 & 0 & 7 \to 5 & 8 \to 7 \\ \infty \to 6 & 3 & 7 \to 5 & 0 & 2 \\ 10 \to 8 & \infty \to 5 & 8 \to 7 & 2 & 0 \end{vmatrix} = A^4$$

On a atteint la limite stationnaire au bout d'un tour alors qu'il faut aller jusqu'à A^4 (deux tours) par la méthode normale.

La méthode des réductions est plus théorique. Elle est analogue à celle décrite dans [25] à propos des matrices booléennes et qui s'étend au cas des pseudo-treillis.

L'application qui à une matrice $A \in \mathfrak{M}_{nn}$ fait correspondre la limite stationnaire $A + A^2 + \ldots$ sera notée μ. Cette application est une fermeture dans l'ensemble ordonné $\mathfrak{M}_{nn}$ en ce sens que :

$$\begin{cases} A \leqslant B \Longrightarrow \mu(A) \leqslant \mu(B) \\ A \leqslant \mu(A) \\ \mu\big(\mu(A)\big) = \mu(A) \end{cases}$$

Pour chaque indice $k = 1, 2, \ldots n$ nous introduisons une application appelée <u>réduction par rapport à k</u> et notée $\mu_k : \mathfrak{M}_{n,n} \to \mathfrak{M}_{h,n}$, définie par :

$$A = (a_{ij}) \qquad \mu_k(A) = (b_{ij})$$

$$\text{avec} \quad b_{ij} = a_{ij} + a_{ik} \cdot a_{kj}$$

On constate que $b_{ij} = a_{ij}$ si $k = i$ ou $k = j$ donc μ_k ne modifie pas les termes de la ligne k et de la colonne k.

On obtient les résultats analogues à ceux de [25]

- Chaque application μ_i est idempotente et le produit de deux applications μ_i et μ_j commute. A savoir :

$$\mu_i \circ \mu_i = \mu_i \qquad \text{et} \qquad \mu_i \circ \mu_j = \mu_j \circ \mu_i$$

$$- \ \mu \circ \mu_i = \mu_i \circ \mu \quad \text{pour tout } i$$

$$- \ \mu = \mu_1 \circ \mu_2 \circ \ldots \circ \mu_n$$

Cette autre description de la limite stationnaire au moyen des réductions par rapport aux divers indices présente l'intérêt également de ne travailler que sur un seul tableau.

Un autre intérêt est le suivant. Il se peut que l'on ne s'intéresse qu'à un seul terme de la limite stationnaire par exemple a^{∞}_{12}.

Comme chaque application μ_k n'apporte de modifications au terme (i, j) que par l'intermédiaire de deux éléments dont l'un est situé sur la ligne i et l'autre sur la colonne j, on constate que si l'on applique successivement les

réductions μ_n, μ_{n-1},... μ_3 respectivement sur les matrices principales (emboitées) A_{n-1}, A_{n-2},.., A_2 d'ordres respectifs n - 1, n - 2,.., 2 (cf figure 2), on obtient bien en position (1, 2) de A_2 le terme a^{∞}_{12}.

A =

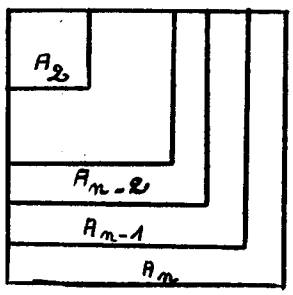


Figure 2 -

3) Pseudo-treillis associés à certains monoïdes. Cas des pseudo-treillis libres. Principales propriétés.

3.1. Pseudo-treillis associés à un monoïde factoriel.

Définition :

On appelle monoïde à ordre factoriel (ou plus simplement monoïde factoriel) un monoïde muni d'une relation d'ordre vérifiant :

(a) l'isotonie : $a \leqslant b \Longrightarrow ac \leqslant bc$ et $ca \leqslant cb$

(b) l'absorption : $a \cdot b \leqslant a$ et $b \cdot a \leqslant a$

Remarques 1 :

Si le monoïde possède une unité 1 la condition (b) peut être remplacée par : $b \leqslant 1$ $(\forall b)$ puisqu'alors par isotonie : $ab \leqslant a$ et $ba \leqslant a$.
On constate alors que 1 est élément maximum. La réciproque est fausse (voir exemple plus loin).

2 :

Si le monoïde possède un zéro : $0x = x0 = 0 \quad \forall x$ alors 0 est l'élément minimum de M (car $0 \cdot x \leqslant x$ donc $0 \leqslant x \quad \forall x$). Réciproquement si M possède un élément minimum noté 0 alors comme $0x \leqslant 0$ on en déduit que $0x = 0 \; \forall x$ (de même $x0 = 0$). Donc 0 est un élément zéro de M.

Exemples :

L'ensemble des réels R^+ vis à vis de l'addition est un monoïde factoriel pour l'ordre dual de l'ordre ordinaire : $a + b \geqslant a$. Notons également que l'ensemble des réels positifs supérieurs à $a(>0)$ en est un sous(monoïde ayant un élément maximum à (ordre dual) pourtant non élément unité $(a+a \neq a)$.

- La relation d'ordre sur les entiers positifs définie par :
$a \leqslant b \overset{def}{=} [b \text{ divise } a]$ est un ordre factoriel pour le monoïde multiplicatif N^+.

Proposition I :

L'ensemble $\mathcal{F}$ des parties finies non vides, d'un monoïde factoriel multiplicatif M est un gerbier vis à vis des opérations d'union (notée +) et de produit noté $\cdot$ (extension aux parties). La relation de préordre sur $\mathcal{F}$ définie par : $f \lhd g$ si à tout $f_i \in f$ il existe $g_j \in g$ avec $f_i \leq g_j$ induit une relation de congruence sur le gerbier $\mathcal{F}$ dont le quotient noté $\mathcal{G}(M)$ est un pseudo-treillis (noté pseudo-treillis associé au monoïde factoriel M).

$\mathcal{F}$ est manifestement un gerbier (associativité du produit $\cdot$) (associativité et idempotence de +) (distributivité de $\cdot$ par rapport à +).

La relation $f \lhd g$ est manifestement un préordre sur $\mathcal{F}$, compatible avec les opérations de $\mathcal{F}$.

L'équivalence associée $f \equiv g$ si $f \lhd g$ et si $g \lhd f$ est donc compatible avec les opérations de $\mathcal{F}$. C'est donc une congruence.

L'ensemble quotient $\mathcal{E}(M)$ est donc un gerbier. C'est en fait un pseudo-treillis. Soit en effet deux éléments a, b de $\mathcal{E}(M)$ et soit α, β deux représentants respectifs dans $\mathcal{F}$. Nous avons :

$\alpha + \alpha\beta \lhd \alpha$ à cause de l'absorption dans le monoïde M. Par ailleurs $\alpha \lhd \alpha + \alpha\beta$ trivialement ; donc $\alpha + \alpha\beta \equiv \alpha$. En passant aux classes, il vient : $a + ab = a$. De manière analogue $a + ba = a$.

Remarques complémentaires :

(1) Le pseudo-treillis $\mathcal{E}(M)$ peut posséder des éléments neutres

- pour l'addition. Soit 0 cet élément neutre. 0 est une classe de $\mathcal{F}$. Soit h un élément (de $\mathcal{F}$) de cette classe et soit m un élément de h. Nous avons classe $\{m\} \leqslant$ classe $(h) = 0$; donc classe $\{m\} = 0$ comme $m \in M$, alors $\forall x \in M$: classe $\{m\} \leqslant$ classe $\{x\}$ donc $m \leqslant x$. Donc m est élément zéro de M. M possède un zéro et la classe 0 de $\mathcal{E}(M)$ est réduite à la seule partie $\{m\}$ de $\mathcal{F}$.

- pour le produit. C'est le cas en particulier si M possède une unité 1 ; car alors $\{1\}$ classe $(f) =$ classe $(f) =$ classe (f) classe $\{1\}$.

(2) On peut adjoindre un élément 0 dans $\mathcal{E}(M)$ s'il n'en a pas. On pourra soit le considérer comme la classe de la partie ϕ (en adjoignant cette partie à $\mathcal{F}$) soit le considérer comme la classe d'un élément zéro adjoint à M.

(3) Lorsque le monoïde M est commutatif, le pseudo-treillis $\mathcal{E}(M)$ est commutatif.

Proposition 2 :

L'application de $\mathcal{F}$ dans $\mathcal{F}$ (notations de la proposition précédente) qui associe à $f \in \mathcal{F}$ la partie $\bar{f}$ des éléments maximaux de f est telle que : $f \equiv g \iff \bar{f} = \bar{g}$. Elle définit donc une représentation canonique de $\mathcal{E}(M)$ au moyen de $\mathcal{F}$. $\mathcal{E}(M)$ peut s'identifier ainsi à l'ensemble $\bar{\mathcal{F}}$ des éléments $\bar{f}$ de $\mathcal{F}$.

Il est tout à fait évident d'abord que $\bar{f} \equiv f$ car $\bar{f} \lhd f$ ($\bar{f} \subseteq f$) ; par ailleurs $f \lhd \bar{f}$ (tout mot de f est inférieur ou égal à un mot maximal de f contenu dans $\bar{f}$).

Donc si $\bar{f} = \bar{g}$ alors $f \equiv g$. Réciproquement si $f \equiv g$ tout mot maximal de f est inférieur ou égal à un mot β de g ; ce mot β est lui même inférieur ou égal à un mot α' de f donc : $\alpha \leqslant \beta \leqslant \alpha'$. Par suite (maximalité de α) : $\alpha = \beta = \alpha'$. Tout mot maximal de f est un mot de g et réciproquement. Donc $\bar{f} = \bar{g}$.

Proposition 3 :

Le pseudo-treillis $\mathcal{E}(M)$ (notation de la proposition 1) est décomposable.

Utilisons la représentation canonique précédente et supposons $a \leqslant b + c$ ($a, b, c \in \bar{\mathcal{F}}$). Soit a_1 l'ensemble des mots de a inférieurs ou égaux à au moins un mot de b. Alors $a_1 \leqslant b$. Soit a_2 l'ensemble des autres mots de a ; alors $a_2 \leqslant c$. D'où la propriété.

Remarque :

Quand on utilise cette représentation canonique, on forme $a + b$ en éliminant de la réunion de a et b les mots non maximaux. De même dans le produit $a \cdot b$ on élimine les produits $a_i\, b_j$ non maximaux.

3.2. Pseudo-treillis libre engendré par un ensemble S. Propriétés.

Comme toute structure libre, le pseudo-treillis libre engendré par S est un pseudo-treillis E tel qu'il existe une injection $q : S \to E$ et satisfaisant à la propriété universelle suivante : toute application φ de S dans un pseudo-treillis arbitraire G peut se prolonger en un homomorphisme unique $f : E \to G$. Soit encore $f \circ q = \varphi$.

On démontre (tout à fait classiquement) que l'unicité de E (à un isomorphisme près) en résulte.

Nous allons exhiber E, grâce à une construction du type défini dans le paragraphe 3.1.

Monoïde libre engendré par S et ordre factoriel associé.

Le monoïde libre engendré par S noté S^* est constitué des suites finies d'éléments de S, ou mots avec pour loi multiplicative la concaténation (ou juxtaposition).

Un mot m de S^* est dit inférieur ou égal à un mot p si, en supprimant un nombre (éventuellement nul) de lettres de m et en reconstituant dans l'ordre les lettres restantes on obtient le mot p.

Exemple :

p a r a t o n n e r r e $\leqslant$ p a r t e r r e

On vérifie qu'il s'agit bien là d'une relation d'ordre, isotone et absorbante ; donc c'est un ordre factoriel.

Proposition I :

Le pseudo-treillis $\mathcal{P}(S^*)$ associé au monoïde libre S^* muni de son ordre factoriel, est le pseudo-treillis libre engendré par S.

Nous utiliserons la représentation canonique de $\mathcal{P}(S^*)$; un élément de $\mathcal{P}(S^*)$ est une somme finie (non nulle) de mots de S^* non comparables deux à deux, vis à vis de l'ordre factoriel de S^*.

L'injection $q : S \to \mathcal{P}(S^*)$ est triviale :

$$s \in S \to q(s) = s \in \mathcal{P}(S^*)$$

Soit $\varphi : S \to G$ une application de S dans le pseudo-treillis G. Construisons $h : \mathcal{P}(S^*) \to G$.

Pour un mot $m = s_1 s_2 \ldots s_q$ de S^* considéré comme appartenant à $\mathcal{P}(S^*)$ nous poserons :

$$h(m) = \varphi(s_1)\,\varphi(s_2)\ldots\varphi(s_q)$$

Pour une somme de mots (mutuellement non comparables) nous poserons :

$$h(\Sigma\, m_i) = \Sigma\, h(m_i) \ .$$

h prolonge φ évidemment. C'est un homomorphisme. En effet si $m \leqslant p$ dans S^* alors $h(m) \leqslant h(p)$.

Donc $h(\Sigma_i m_i + \Sigma_j m_j) = h(\Sigma_i m_i) + h(\Sigma_j m_j)$

En effet les mots redondants de $\Sigma_i m_i + \Sigma_j m_j$ ont pour image par h des éléments redondants.

Pareillement puisque, m et n étant deux mots de S^*, $h(m \cdot n) = h(m)\, h(n)$ alors h est un homomorphisme pour le produit : $h(\Sigma\, m_i \cdot \Sigma\, m_j) = h(\Sigma\, m_i) \cdot h(\Sigma\, m_j)$

(Nous verrons en effet (proposition suivante) qu'aucun mot $m_i\, m_j$ n'est redondant dans $\Sigma\, m_i\ \Sigma\, m_j$).

Enfin h est unique ; en effet si $m = s_1\, s_2 \ldots s_p$ est considéré comme élément de $\mathcal{E}(S^*)$, alors il est obtenu par produit de $s_1, s_2, \ldots, s_p \in \mathcal{E}(S^*)$; tout homomorphisme h_1 de $\mathcal{E}(S^*)$ dans G, prolongeant φ vérifie obligatoirement

$h_1(s_1 \cdot s_2 \cdot \ldots \cdot s_p) = h_1(s_1)\, h_1(s_2) \ldots h_1(s_p)$

$= \varphi(s_1) \cdot \varphi(s_2) \ldots \cdot \varphi(s_p) = h(s_1\, s_2 \ldots s_p)$

Proposition 2 :

Dans la représentation canonique de $\mathcal{E}(S^*)$ au moyen de $\bar{\mathcal{F}}$, le produit (dans $\mathcal{F}$) de deux éléments de $\bar{\mathcal{F}}$ appartient à $\bar{\mathcal{F}}$.

Soient en effet $a, b \in \bar{\mathcal{F}}$; donc $a = \bar{a}$, $b = \bar{b}$; montrons que $a \cdot b = \overline{(a \cdot b)}$. Soit α un mot de a et β un mot de b ; montrons que $\alpha \cdot \beta$ est un mot maximal dans $a \cdot b$. Si cela n'était pas alors : $\alpha \cdot \beta < \gamma \cdot \delta$ avec $\gamma \in a$ et $\delta \in b$. On peut supposer $\alpha \neq \gamma$ sinon la règle de simplification donne $\beta < \delta$.
On pourra écrire alors

$\alpha \cdot \beta = \gamma_1 \cdot \delta_1$ avec $\gamma_1 \leqslant \gamma$ et $\delta_1 \leqslant \delta$ l'une des inégalités étant strictes. Supposons que ce soit la première. Alors $\gamma_1 \notin a$ donc $\gamma_1 < \alpha$ (sinon $\alpha < \gamma$: absurde) mais alors $\beta < \delta_1 \leqslant \delta$ donc $\beta < \delta$ et cela est absurde. De manière analogue l'hypothèse $\delta_1 < \delta$ est contradictoire.

Théorème :

Tout pseudo-treillis libre E est un treillis distributif relativement à l'ordre de E.

Considérons le pseudo-treillis libre E engendré par
$S = \{a, b, c, \ldots, \ell, \ldots\}$
(S non forcément fini). E est déjà un + demi treillis.

I) Considérons deux éléments μ et μ' de E qui se réduisent chacun à un mot de S^*. Nous montrerons que μ et μ' ont une borne inférieure. Nous procéderons en trois phases :

Phase de dédoublement.

Chaque lettre du mot μ sera marquée par un indice donnant l'ordre de l'occurrence de cette lettre dans le mot, (ce dernier étant lu de gauche à droite). Nous ferons de même pour les lettres de μ' en accentuant en outre les lettres de μ'.

Exemple :

$\mu = abac$ $\qquad$ $\mu' = caab$

$\mu \to a_1 b_1 a_2 c_1$ $\qquad$ $\mu' \to c'_1 a'_1 a'_2 b'$

De la sorte, les nouveaux mots écrits ont des lettres distinctes entre elles, chaque lettre ne se répétant pas dans un mot.

Phase de mixage.

Nous intercalons les lettres de μ' et dans l'ordre où elles apparaissent dans μ', de toutes les manières possibles parmi les lettres de μ. Si n est le nombre des lettres de μ et p le nombre des lettres de μ', on obtient ainsi $C^p_{n+p} = C^n_{n+p}$ nouveaux mots ; en effet la formule est vraie si $n = p = 1$. Raisonnons par récurrence sur $n + p$; les mots obtenus en mixant le mot μ à n lettres et le mot μ' à p lettres peuvent être classés en deux catégories disjointes et complémentaires la première est constituée des mots se terminant par une lettre de μ' (donc la dernière de μ') et sont au nombre de $S_{n,p-1}$; la deuxième des mots se terminant par la dernière lettre de μ donc au nombre de $S_{n-1,p}$; par suite :

$$S_{n,p} = S_{n-1,p} + S_{n,p-1} = C^p_{n+p-1} + C^{p-1}_{n+p-1} = C^p_{n+p}$$

Phase de réécriture.

Chacun des C_{n+p}^{p} mots du mixage est lu de gauche à droite et va fournir un mot par écriture de gauche à droite de la manière suivante :

- si une lettre n'a plus de suivante elle est écrite en supprimant l'indice et l'accent éventuel.

- si une lettre lue n'est pas la dernière et a une suivante distincte dans S ou égale mais avec même accentuation, elle est écrite (avec suppression de l'indice et de l'accent) et on lit la lettre suivante.

- si la lettre lue a une suivante, égale dans S mais avec une accentuation différente, on l'écrit sans indice et sans accentuation, on saute la lettre suivante et s'il n'y en a plus le processus se termine.

Exemple :

$\mu = aab$ $\mu' = caa$

Un mot du mixage de $a_1\ a_2\ b_1$ et $c'_1\ a'_1\ a'_2$ est par exemple $c'_1\ a_1\ a'_1\ a_2\ a'_2\ b_1$. Le processus de réécriture donne : caab.

Considérons la somme θ de tous les mots ainsi obtenus par réécriture des mots du mixage de μ et μ'. θ est un élément de $\mathcal{F}$ et posons $\nu = \bar{\theta}$ $(\in E)$.

ν est la borne inférieure de μ et μ'. Il est tout à fait évident que chaque mot de ν est à la fois inférieur ou égal à μ et μ'. Chaque mot mixé l'est en effet quand on supprime accent et indice. Il le reste par réécriture d'après la définition même de l'algorithme de réécriture. Les lettres confondues dans la réécriture d'un mot mixé, correspondent à des accentuations différentes signalant qu'elles proviennent d'une même lettre appartenant aux mots μ et μ'. La "réalisation" de μ et μ' dans un tel mot réécrit utilise donc des "points" communs.

Soit $\lambda \in E$ tel que $\lambda \leqslant \mu$ et $\lambda \leqslant \mu'$. Chaque mot s de λ est donc $\leqslant \mu'$ et μ. Donc les lettres de μ comme celles de μ' se réalisent (avec ordre conservé) dans les lettres de s, ces deux réalisations pouvant avoir des "points" communs. Si on dédouble ces points communs par accentuation différente on obtient (en sup primant éventuellement d'autres lettres de S "non atteintes par μ et μ') un mot du mixage de μ et μ' et le mot associé σ par réécriture est tel que $s \leqslant \sigma \leqslant \nu$. Donc ν est bien la borne inférieure de μ et μ'. Nous le noterons désormais $\mu \wedge \mu$

2) Soient alors deux éléments quelconques f et g de E

$$f = f_1 + f_2 + \ldots + f_q \quad \text{et} \quad g = g_1 + g_2 + \ldots + g_r$$

Posons :

$$f \wedge g = \sum_{j=1}^{r} \sum_{i=1}^{q} f_i \wedge g_j$$

Il est tout à fait évident que $f \wedge g \leqslant f$ et g

Soit $h \in E$ tel que :

$h \leqslant f$ et $h \leqslant g$; donc pour chaque mot h_k de h il existe un mot f_i et un mot g_j tel que $h_k \leqslant f_i$, $h_k \leqslant g_j$ par suite $h_k \leqslant f_i \wedge g_j \leqslant f \wedge g$; donc $h \leqslant f \wedge g$. $f \wedge g$ est donc bien la borne inférieure de f et g.

3) Par construction même le treillis E est distributif si $f = \sum f_i$, $g = \sum g_j$ et $h = \sum h_k$ alors

$$(f+g) \wedge h = \sum (f_i \wedge h_k) + \sum g_j \wedge h_k = f \wedge h + g \wedge h$$

3.3. Applications du théorème de Lunc dans le cas d'un pseudo-treillis libre.

Si l'on considère un réseau dans lequel on donne aux divers arcs des noms distincts, et si l'on utilise le pseudo-treillis libre engendré par ces noms, en y adjoignant les éléments unités 0 et 1, on a par fermeture transitive de la matrice de connexion les noms des chemins et des circuits simples.

Exemple :

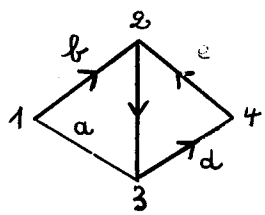


Figure 3

La matrice de connexion du réseau de la figure 3 est

$$A = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ 1 & 0 & b & a & 0 \\ 2 & 0 & 0 & c & 0 \\ 3 & a & 0 & 0 & d \\ 4 & 0 & e & 0 & 0 \end{array}$$

La fermeture transitive est (après calculs) :

$$A + A^2 + .. + A^4 = \begin{vmatrix} a^2 + bca & b + ade & a + bc & ad + bcd \\ ca & cab + cde & c & cd \\ a & ab + de & a^2 + dec + abc & f \\ eca & e & ec & ecd \end{vmatrix}$$

Cette matrice donne évidemment les chemins simples et les circuits simples complétés par les "aller-retours". D'autres applications peuvent être trouvées en théorie des automates.

Nous simplifierons dans la suite ces calculs de chemins et circuits.

3.4. Pseudo-treillis libre commutatif engendré par S.

Nous savons que le monoïde libre commutatif engendré par S s'identifie à l'ensemble $N^{(S)}$ des applications de S sans l'ensemble des entiers naturels, nulles sauf en un nombre fini de points de S, la loi multiplicative associant à deux telles applications leur somme.

Exemple :

$$S = \{a, b, c, \ldots, \ell \ldots\}$$

Les éléments du monoïde commutatif sont notés par exemple $a^{\alpha} b^{\beta}$, $b^{\beta} c^{\gamma} \ell^{\lambda}$; on les appellera des monômes commutatifs. (On n'écrit pas les lettres d'exposant 0). Ce monoïde $N^{(S)}$ est muni de l'ordre factoriel suivant ; soient $\varphi, \psi \in N^{(S)}$, nous écrirons :

$$\varphi \leqslant \psi \quad \text{si} \quad \varphi(s) \geqslant \psi(s) \qquad \forall s \in S$$

Exemple :

$$a^2 b^3 < ab^2$$

Le pseudo-treillis $\mathcal{L}(N^{(S)})$ s'appellera pseudo-treillis libre commutatif engendré par S.

Il est libre dans le sens qu'il possède la propriété universelle suivante : (a) il existe une injection q de S dans $\mathcal{L}(N^{(S)})$ (b) pour toute application φ de S dans un pseudo-treillis commutatif B, on peut trouver un homomorphisme unique f de $\mathcal{L}(N^{(S)})$ dans B tel que $f \circ q = \varphi$.

La proposition 2 précédente n'est pas valable pour ce pseudo-treillis.

Exemple :

$$(a^4 + a^2b) \in \bar{\mathcal{F}}$$

$$(b^6 + ab^4) \in \bar{\mathcal{F}}$$

or $(a^4 + a^2b)\,(b^6 + ab^4) \notin \bar{\mathcal{F}}$ car le monôme $a^4\,b^6$ est redondant ($\leqslant a^2b \cdot ab^4 = a^3\,b^5$).

Par contre le théorème précédent est satisfait car le monoïde $N^{(S)}$ est lui-même pourvu d'un ordre réticulé. Donc deux mots ont déjà une borne inférieure (exemple : $a^2\,b^3$ et ab^4 ont $a^2\,b^4$ pour borne inférieure) qui est un mot. Le théorème reste donc valable.

4) Homomorphismes. Congruences et idéaux. Pseudo-treillis de carré nul.

4.1. Homomorphismes. Congruences. Idéaux.

Dans tout ce qui suit les pseudo-treillis seront considérés avec des éléments neutres 0 et 1.

Etant donné un homomorphisme h d'un pseudo-treillis E dans un pseudo-treillis F, la relation binaire sur E, $h(x) = h(y)$ est une relation de congruence, c'est-à-dire d'équivalence notée $(x \equiv y\ (h))$ et vérifiant :

$$x \equiv y \ (h) \Longrightarrow x + z \equiv y + z \ (h)$$

$$\Longrightarrow x \cdot z \equiv y \cdot z \ (h) \quad \text{et} \quad z \cdot x \equiv z \cdot y \ (h)$$

En outre l'image homomorphe h(E) est isomorphe au quotient de E par cette congruence :

$$h(E) \overset{\sim}{\simeq} E/(h)$$

Réciproquement à toute congruence r d'un pseudo-treillis E, on peut définir le pseudo-treillis quotient E/(r) et il existe un homomorphisme canonique de E sur E/(r).

Les homomorphismes de E peuvent donc être étudiés à partir des congruences de E.

On sait [8] que l'ensemble $\mathcal{R}$ des congruences de E est un treillis complet pour l'ordre :

$$r_1 \leqslant r_2 \overset{\text{def}}{=} \left[x \equiv y \ (r_1) \Longrightarrow x \equiv y \ (r_2)\right]$$

Une relation de congruence r, peut-elle être définie par une de ses classes, par exemple la classe de 0, notée r(0)? Cela nous conduit à définir :

Définition :

On appelle idéal d'un pseudo-treillis E (avec unité) toute partie fermée, non vide stable pour l'opération +.

En d'autres termes I est un idéal si

a) $0 \in I$

b) $x, y \in I \Longrightarrow x + y \in I$

c) $x \in I \Longrightarrow \forall z \ [z \leqslant x \Longrightarrow z \in I]$

Proposition :

L'ensemble $\mathcal{I}$ des idéaux de E est un treillis complet relativement à l'inclusion. Ce treillis est en outre distributif si E est décomposable.

La première partie est tout à fait évidente, l'intersection ensembliste d'une famille quelconque d'idéaux étant un idéal l'ensemble E lui-même étant un idéal, la propriété de treillis complet en résulte.

Supposons que E soit décomposable, alors si J_1 et J_2 sont deux idéaux (donc fermés) il est tout à fait évident que $J_1 + J_2$ est fermé (prop. I.2) et stable par rapport à la somme. Or $J_1 \subseteq J_1 + J_2$ et $J_2 \subseteq J_1 + J_2$.

Par ailleurs la borne supérieure de J_1 et J_2 doit contenir $J_1 + J_2$ donc $J_1 + J_2$ est l'idéal borne supérieure de J_1 et J_2.

Il reste à montrer que $J \cap (J_1+J_2) = J \cap J_1 + J \cap J_2$
Or dans tout treillis nous avons :

$$J \cap (J_1+J_2) \supseteq J \cap J_1 + J \cap J_2$$

Montrons l'inclusion inverse ; si $x \in J \cap (J_1+J_2)$ cela veut dire que $x \in J$ et $x = x_1 + x_2$ ($x_1 \in J_1$ et $x_2 \in J_2$). Or $x_1 \leqslant x$ donc $x_1 \in J \cap J_1$; de même $x_2 \in J \cap J_2$ donc $x \in J \cap J_1 + J \cap J_2$.

La relation entre congruences et idéaux peut être résumée dans le théorème suivant dont nous rappellerons seulement le résultat [10] :

Théorème :

Si r est une congruence du pseudo-treillis E (avec unités), r(0) est un idéal. Cette application de $\mathcal{R}$ dans $\mathcal{J}$ est un Λ - homomorphisme surjectif. Plus précisément si I est un idéal, son image réciproque est un sous-treillis de congruences dont la plus fine notée ω_I et la moins fine notée δ_I sont définies respectivement par :

(1) $x \equiv y \ (\omega_I) \iff \exists\, a \in I : x + a = y + a$

(2) $x \equiv y \ (\delta_I) \iff \forall\, \lambda, \mu \in E \ [\mu \cdot x \cdot \lambda \in I \iff \mu \cdot y \cdot \lambda \in I]$

4.2. Cas des pseudo-treillis libres.

Exemple : Pseudo-treillis libre de carré nul.

Tout pseudo-treillis F est l'image homomorphe d'un pseudo-treillis libre E engendré par un ensemble générateur de F.

Il est donc intéressant de connaître les relations de congruences des pseudo-treillis libres E et par suite du théorème précédent les idéaux de E'.

Lorsqu'on se donne un idéal I d'un pseudo-treillis libre E, engendré par S, le quotient E/ω_I peut être considéré comme l'ensemble des formules de $\mathcal{F}$ dont on a supprimé les mots appartenant à l'idéal I (l'élément 0 est assimilé à la formule vide).

Le quotient de E par δ_I est un peu plus difficile à examiner. Nous noterons toutefois une petite simplification. Nous appellerons S^* le monoïde libre engendré par S et nous conviendrons que $S^* \subseteq \mathcal{F}$. Nous avons alors :

$$x \equiv y \quad (\delta_I) \Longleftrightarrow \quad \forall\, \lambda,\ \mu \in S^* \ [\mu x \lambda \in I \iff \mu y \lambda \in I]$$

En effet si $\lambda = \Sigma\, \lambda_i$ $(\lambda_i \in S^*)$ et $\mu = \Sigma\, \mu_j$ $(\mu_j \in S^*)$ sont deux éléments de E, il est évident que :

$$\lambda \times \mu \in I \iff {}_i \times \mu_j \in I \ (\forall_{i,j}).$$

Considérons un idéal I du pseudo-treillis libre E engendré par S. Si $f = \Sigma\, f_k$ appartient à I, chaque mot f_k appartient également à I. Un idéal I d'un pseudo-treillis libre E définit donc un ensemble de mots de S^* manifestement fermé par rapport à l'ordre factoriel de S^*. Réciproquement si on se donne un ensemble fermé de mots de S^* l'ensemble des sommes finies de tels mots (moyennant les règles d'absorption) forme un idéal de E.

Or le monoïde libre présente des propriétés particulières qu'il est peut être bon d'exploiter.

Deux mots de S^* sont commutativement équivalents s'ils ne diffèrent que par l'ordre des lettres (exemple ababca est commutativement équivalent à baaacb).

Définition :

Un idéal I du pseudo-treillis libre engendré par S est dit commutatif si pour tout mot y appartenant la classe des mots qui lui sont commutativement équivalents y appartient aussi.

Cette notion est mise en valeur par la proposition suivante :

Proposition :

Si I est un idéal commutatif du pseudo-treillis libre E engendré par S, alors le pseudo-treillis quotient E par δ_I est commutatif.

Pour le démontrer, il suffit de voir que dans le cas où x et y ($\in$ E) se réduisent à deux mots respectifs, commutativement équivalents alors $x \equiv y \ (\delta_I)$.

Compte tenu des remarques précédentes il suffit de prouver :

$$\forall \lambda, \mu \in S^* \ [\lambda \times \mu \in I \iff \lambda \ y \ \mu \in I]$$

Mais cela est évident : $\lambda \times \mu$ et $\lambda \ y \ \mu$ se réduisent à des mots. Comme x est commutativement équivalent à y, $\lambda \times \mu$ est commutativement équivalent à $\lambda \ y \ \mu$. Si l'un appartient à I, l'autre aussi en raison du caractère commutatif de I.

Nous pouvons alors simplifier l'équivalence modulo δ_I dans le cas où I est commutatif et nous aurons :

$$x \equiv y \quad (\delta_I) \iff \forall \lambda \in S^* \ [\lambda \times \in I \iff \lambda \ y \in I]$$

Exemple d'application. Pseudo-treillis libres de carré nul. Cas commutatif et non commutatif.

Soit E le pseudo-treillis libre engendré par S.

Considérons l'ensemble I des sommes de mots ayant tous au moins, une lettre répétée. I est manifestement un idéal, commutatif.

L'ensemble quotient de E par ω_I est par définition le pseudo-treillis libre de carré nul engendré par S.

Appelons mot multilinéaire un mot de S^* sans répétition de lettres. Alors le pseudo-treillis libre de carré nul engendré par S comporte outre les éléments 0 et 1 les sommes (finies) de mots multilinéaires de S^* (non comparables deux à deux, vis-à-vis de l'ordre factoriel de S^*).

La somme consiste à rajouter les mots et éliminer les mots les plus petits (au sens de l'ordre). Le produit consiste à développer comme dans le pseudo-treillis libre avec élimination des mots non multilinéaires.

Le pseudo-treillis quotient de E par δ_I s'appellera pseudo-treillis libre, commutatif, de carré nul engendré par S.

Il est d'abord commutatif en vertu de la proposition précédente. Nous allons montrer qu'il s'identifie à l'ensemble C des sommes finies de mots commutatifs multilinéaires (qu'on appellera des monômes) mutuellement non comparables dans la relation d'ordre factoriel de $N^{(S)}$.

Il est tout à fait évident que ce pseudo-treillis commutatif ne peut-être qu'un quotient de C. Il reste, donc à montrer que si f et g (appartenant à C) considérés comme éléments de $\mathcal{F}$ sont équivalents modulo δ_I, alors f = g.

C'est une technique booléenne, qui nous montrera ce résultat. L'équivalence modulo δ_I de f et g est équivalente à (cf. remarques précédentes) :

$\forall \lambda$ mot commutatif multilinéaire, $\lambda f \in I \iff \lambda g \in I$.

Cherchons alors comment doit être choisi le monôme λ pour que λf appartienne à I. Nous avons :

pour que λf appartienne à I il faut et il suffit que le monôme λ ait au moins une lettre commune avec tout monôme f_i de f.

Si l'on assimile f à une fonction booléenne croissante (élément du treillis distributif libre engendré par S), cette dernière condition équivant à : λ est un monôme (booléen) compatible avec l'élément dual f^*.

Par suite l'équivalence modulo δ_I de f et g est équivalente à : tout monôme compatible avec f^* est compatible avec g^* et réciproquement. Donc cela ne peut avoir lieu que si $f^* = g^*$ donc $f = g$.

Nous pouvons donc identifier le pseudo-treillis commutatif de carré nul à cet ensemble C de polynômes.

Les opérations de sommes et produits se conduiront dans C de la manière suivante :

- pour la somme, on opèrera comme dans le treillis distributif libre.

- pour le produit on tiendra compte du fait que deux monômes ayant au moins une lettre en commun, ont un produit nul.

Exemple :

$f = abc + bd + ad$ $\qquad$ $g = ac + be$

$f + g = ac + bd + ad + be$

$f \cdot g = abcd + abde$

(abcd provient du produit bd, ac)

(abde provient du produit ad, be)

(les autres produits sont nuls).

Bien entendu dans la multiplication, l'élimination des multiples doit être entreprise.

Les calculs, dans les pseudo-treillis libres commutatifs de carré nul sont extrêmement simples (légèrement plus que dans le cas des treillis distributifs libres).

Nous citerons une application importante à la théorie des chemins dans un réseau. Nous savons que si nous nommons les divers arcs d'un réseau par des lettres distinctes, tout chemin simple est un mot multilinéaire (sans répétition de lettres). Nous pouvons donc opérer dans un pseudo-treillis libre de carré nul et chercher (tout ou partie) les éléments de la fermeture transitive d'une matrice. En opérant, en commutatif, nous simplifions énormément (sur un plan programmation et codage). Bien entendu nous obtenons chaque chemin comme l'ensemble des arcs qui y figurent. Pour avoir l'ordre dans lesquels se succèdent ces arcs on utilisera (comme dans l'application de 2.2) la matrice initiale pour retrouver l'ordre.

Reprenons l'exemple (3.3). La fermeture transitive de la matrice est beaucoup plus simple à former (en commutatif de carré nul).
Nous obtenons :

abc	b + ade	a + bc	ad + bcd
ac	abc + cde	c	cd
a	ab + de	cde + abc	f
ace	e	ce	cde

Cherchons l'ordre des arcs dans le chemin ace de 4 à 1. La colonne n°1 de A ne porte que la lettre a (issue de la ligne 3). Donc le dernier arc de ace est a et on peut écrire ace $\to (ce)^3$ a où $(ce)^3$ est un chemin qui arrive au sommet 3.

La colonne 3 de A n'a que les arcs a ou c. Donc c est le dernier arc de ce. Par suite l'ordre des arcs dans ace est :

e, c, a.

Signalons également que les faux circuits (aller-retour) sont éliminés.

4.3. Propriété de pseudo-treillis principal de $\mathcal{L}(M)$ associé à un monoïde factoriel supérieurement fini. Cas des pseudo-treillis libres.

Un pseudo-treillis F est principal si tout idéal est principal c'est-à-dire engendré par un seul élément. Tout idéal est alors de la forme $a] = \{x \; ; \; x \in F \quad x \leqslant a\}$. Le pseudo-treillis libre engendré par un ensemble fini S est principal.

Nous allons démontrer en fait un résultat un peu plus général.

Définition :

Un ensemble ordonné est dit supérieurement fini si toute partie non vide admet un nombre fini (non nul) d'éléments maximaux.

Théorème I :

Si un monoïde M muni d'un ordre factoriel est engendré par une partie P supérieurement finie relativement à l'ordre induit, alors M lui-même est supérieurement fini.

Ce résultat est un cas particulier, d'un résultat plus général et assez remarquable de G.HIGMAN [14].

Conséquence :

Le monoïde libre S^* engendré par l'ensemble fini S est supérieurement fini relativement à son ordre factoriel.

En effet tout ensemble fini est supérieurement fini relativement à tout ordre.

Théorème 2 :

Le pseudo-treillis $\mathcal{E}(M)$ associé à un monoïde factoriel supérieurement fini, est complètement réticulé et tout idéal est principal.

En effet considérons une partie quelconque F de $\mathcal{E}(M)$. Chaque élément f de F est une partie finie de M. Soit G la réunion des $f \in F$. C'est une partie de M ayant donc un nombre fini non nul d'éléments maximaux ; soient $g_1, g_2, \ldots g_n$ ces éléments. A tout g_i on peut faire correspondre un $f_i \in F$ qui le contient ; alors $f_1 + f_2 + \ldots + f_n = g_1 + g_2 + \ldots + g_n$ et contient tous les éléments maximaux de F ; donc :

$$\forall f \quad f \in F \Longrightarrow f \leqslant f_1 + f_2 + \ldots + f_n .$$

Il est tout à fait évident que si g est un majorant de F alors $g \geqslant f_i$ donc $g \geqslant f_1 + f_2 + \ldots + f_n$. Par suite $f_1 + f_2 + \ldots + f_n$ est borne supérieure de F.

Donc $\mathcal{E}(M)$ est un sup-demi treillis complet ; possédant un élément nul O (la partie vide) c'est donc un treillis complet.

$\mathcal{E}(M)$ est principal car à tout idéal I on peut faire correspondre de la même manière, l'élément $f_1 + f_2 + \ldots + f_n$ y appartenant et borne supérieure de tous les éléments de I. I est donc principal.

Corollaire :

Le pseudo-treillis libre engendré par un nombre fini d'éléments est un treillis complet et tout idéal est principal.

Le pseudo-treillis n'est autre en effet que $\mathcal{E}(S^*)$. Or S^* est supérieurement fini.

Ainsi il est possible d'avoir tous les idéaux d'un pseudo-treillis libre engendré par un ensemble fini S. On peut construire, grâce à celà, une grande classe d'homomorphismes de ce pseudo-treillis.

CHAPITRE VII

CHEMINEMENTS PAR SOMMETS.
TREILLIS SERIE PARALLELE.

Nous avons vu que les pseudo-treillis rendent bien compte des problèmes de cheminements dans un réseau, lorsque les informations sont concentrées sur les arcs (c'est-à-dire sur les transitions d'un sommet à un autre). Nous masquons, ce faisant, des informations utiles sur les sommets (pré-ordres, ordres, etc...). Nous allons proposer une structure algébrique susceptible de décrire correctement les chemins (par sommets). Nous examinerons ensuite, quelques problèmes d'ordre sur les sommets d'un tel réseau en particulier dans le cas des réseaux série-parallèles.

1) Monoïde de carré nul. Gerbier de carré nul.

1.1. Monoïde de carré nul. Gerbier de carré nul.

Définition :

Un monoïde M est de carré nul s'il possède un élément nul noté 0 ($0a = a0 = 0 \ \forall a$) et si de plus : $\forall a \ \forall b \quad a \neq 1 \Rightarrow aba = aa = 0$.

Si l'on interprète un produit de facteurs comme un renseignement attaché à un chemin simple, les facteurs étant les renseignements élémentaires attachés à chaque sommet la règle de carré nul s'interprète comme le fait que 1) les sommets ne se répètent pas dans un chemin simple 2) les renseignements élémentaires attachés à deux sommets distincts sont distincts (sinon ces sommets peuvent être confondus sur un plan purement informationnel).

Monoïde libre de carré nul engendré par S.

Il est très simple de définir le monoïde libre de carré nul engendré par un ensemble S. Il est constitué des mots (suite finie de lettres de S) multilinéaires (aucune répétition de lettre), de l'élément 0 et éventuellement du mot vide 1. La règle du produit est très simple :

m•n égale 0 si m ou n est nul ou si m et n ont une lettre commune.

m•n est la juxtaposition (concaténation) des mots m et n autrement.

Lorsque S est fini et contient n éléments le monoïde libre de carré nul engendré par S noté Z(S) est fini évidemment. Il contient
$1 + n + 2!\ C_n^2 + 3!\ C_n^3 + \ldots + n!\ C_n^n$ éléments (sans compter l'élément unité 1).

Gerbier de carré nul associé à un monoïde de carré nul.

Nous désignerons par là, le gerbier des parties finies de M avec pour lois de composition l'union (notée +) (associative, commutative, idempotente) et le produit (noté •) par extension du produit de M aux parties. La partie ϕ sera confondue avec l'élément 0 de M. Lorsque M est le monoïde libre de carré nul engendré par S, le gerbier associé sera noté G(S). On l'appellera gerbier libre de carré nul engendré par S. Si S est fini G(S) se confond avec l'ensemble des parties de Z(S) et est donc fini.

1.2. Le théorème de Lunc. Application aux chemins simples d'un réseau.

Nous considérerons les matrices dont les éléments appartiennent à un gerbier G de carré nul associé à un monoïde M de carré nul.

On peut définir pareillement, la somme de deux matrices (de même format) et le produit d'une matrice par une autre.

La somme est associative, commutative et idempotente. Le produit est associatif et distributif par rapport à la somme.

Le théorème de Lunc est encore valable.

En effet A étant une matrice carrée d'ordre n la suite $S_k = A + A^2 + \ldots + A^k$ stationnera obligatoirement à partir d'un rang fini. En effet chaque élément de A est la somme d'un nombre fini d'éléments de M. Donc l'ensemble des éléments de A n'utilisent qu'un nombre fini, au total, d'éléments de M. Par suite chaque coefficient de S_k appartient au gerbier de carré nul associé à un sous-monoïde de M' de M engendré par un nombre fini d'éléments de M, donc fini. Par suite l'ordre de ce gerbier est fini et la stationnarité est atteinte au plus à l'ordre q (q étant l'ordre de ce gerbier).

Le théorème de Lunc se renforce en fait par la proposition suivante.

Proposition :

Si A est une matrice carrée à coefficients dans un gerbier de carré nu associé à un monoïde de carré nul sans unité, alors il existe un rang p à partir duquel $A^p = 0$.

En effet les éléments de A se définissent à partir d'un nombre fini d'éléments de M. Désignons ce nombre par p - 1. Il est évident que les coefficients de A^p sont des sommes de produits de p éléments (donc nuls car obligatoirement une répétition se produit).

Exemple d'application.

Soit à chercher les chemins et circuits simples d'un réseau (mixte) associé à une relation binaire non réflexive d'un ensemble donné.

Soit (exemple figure 1) la matrice 4 × 4, sur le gerbier libre engendré par {1,2,3,4}, dont le coefficient (i,j) est l'élément j du gerbier s'il y a une transition du sommet i à j et l'élément 0 autrement (en particulier pour les coefficients diagonaux).

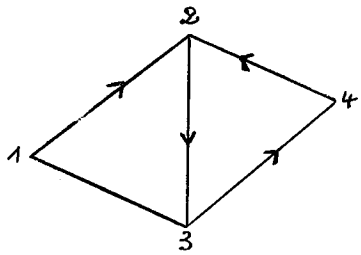


Figure 1

A =		1	2	3	4
	1	0	2	3	0
	2	0	0	3	0
	3	1	0	0	4
	4	0	2	0	0

On obtient :

$$A + A^2 = B = \begin{vmatrix} 31 + 231 & 2 & 3 + 23 & 34 \\ 31 & 0 & 3 & 34 \\ 1 & 12 + 42 & 13 & 4 \\ 0 & 2 & 23 & 0 \end{vmatrix}$$

Et enfin :

$B + B^2 =$

31 + 231	2 + 312 + 342	3 + 23	34 + 234
31	312 + 342	3	34
1 + 4231	12 + 42 + 1342	13 + 123	4 + 134
231	2	23	234

A partir de cette limite stationnaire on peut obtenir :

- les circuits de i à i.

  Exemple de 2 à 2 on obtient

  2312 et 2342

- les chemins simples de i à j ; on multiplie à gauche par i, l'élément P_{ij} de la matrice.

Exemple : de 3 à 2 on obtient :

$$3(12+42+1342) = 312 + 342$$

La méthode ainsi proposée, ressemble quelque peu, à la méthode des fermetures transitives des matrices sur un pseudo-treillis.

L'amélioration qu'on peut en attendre réside dans le fait que, la règle d'absorption n'étant pas satisfaite, la recherche des éléments redondants est un peu plus aisée (un élément est redondant s'il existe un autre identique). Nous allons toutefois, tenter de simplifier le calcul, en ne manipulant que des expressions du gerbier de carré nul organisées "linéairement" et non pas sous forme de matrices ou tableaux.

1.3. Parties fermées d'un gerbier libre de carré nul. Opérations de fermeture. Applications aux cheminements.

Dans le monoïde libre de carré nul avec unité 1, engendré par un ensemble S nous considérons la relation entre éléments non nuls :

$\mu \leqslant \nu$ s'il existe λ, θ avec $\lambda \mu \theta = \nu$.

C'est manifestement une relation d'ordre, la réflexivité et l'antisymétrie sont évidentes ainsi que la transitivité.

Nous dirons qu'un élément f du gerbier associé est fermé si contenant le mot μ il contient tout mot ν tel que $\nu \leqslant \mu$.

Opérations μ_i de fermeture.

Soit G(S) le gerbier libre de carré nul engendré par $S = \{1,2,\ldots,n\}$.

Pour chaque $i = 1, 2 \ldots n$ nous définissons :

- l'application δ_i : G(S) → G(S). C'est un homomorphisme pour la somme + vérifiant (m étant un mot (multilinéaire) du monoïde S^*) :

$\delta_i(m) = 0$ si m ne contient pas i

$\delta_i(m) = k_1\ k_2 \ldots i$ si $m = k_1\ k_2 \ldots i\ \ell_1 \ldots \ell_r$

Cette application s'appelle : section finissante en i

- l'application ω_i de G(S) → G(S). C'est encore un homomorphisme pour + tel que si m est un mot multilinéaire alors

$\omega_i(m) = 0$ si m ne contient pas i ou contient i en dernière lettre.

$\omega_i(m) = \ell_1\ \ell_2 \ldots \ell_r$ si $m = k_1\ k_2 \ldots i\ \ell_1\ \ell_2 \ldots \ell_r$

Cette application peut s'appeler ouverture commençante en i.

Exemple : $S = \{1,2,3,4,5\}$

$f = 143 + 354 + 415 + 235$

$\delta_4(f) = 14 + 354 + 4 \qquad \omega_4(f) = 3 + 15$

Nous définirons alors l'application μ_i de G(S) dans G(S) par :

$$\mu_i(f) = f + \delta_i(f) \cdot \omega_i(f)$$

Exemple précédent :

$\mu_4(f) = f + (14+354+4)\ (3+15)$

$= f + 143 + 43 = f + 43$ (143 est redondant dans f)

Proposition :

Chacune des applications μ_i est idempotente. En outre la restriction de ces applications aux éléments fermés de G(S) donne pour image des éléments fermés et deux applications μ_i et μ_j commutent sur ces éléments fermés.

Nous avons évidemment $\mu_i(f) \supseteq f$ et en outre si $f \supseteq g$ $\mu_i(f) \supseteq \mu_i(g)$ donc $\mu_i(\mu_i(f)) \supseteq \mu_i(f)$. En fait nous avons une égalité.

En effet :

$$\mu_i(\mu_i(f)) = f + \delta_i(f) \cdot \omega_i(f) + \delta_i(f+\delta_i(f)\omega_i(f)) \cdot \omega_i(f+\delta_i(f)\omega_i(f))$$

δ_i et ω_i étant des homomorphismes pour + nous avons :

$$\mu_i(\mu_i(f)) = f + \delta_i(f)\ \omega_i(f) + \left(\delta_i(f)+\delta_i(\delta_i(f)\cdot\omega_i(f))\right)\left(\omega_i(f)+\omega_i(\delta_i(f)\omega_i(f))\right)$$

Mais il est aisé de vérifier que

$\delta_i(\delta_i(f)\cdot\omega_i(f)) \subseteq \delta_i(f)$ et

$\omega_i(\delta_i(f)\cdot\omega_i(f)) \subseteq \omega_i(f)$

D'où :

$\mu_i(\mu_i(f)) = \mu_i(f)$

Montrons que l'image d'un élément fermé est fermé. Soit $m \in \mu_i(f)$, $m \notin f$ et considérons un mot $p \preccurlyeq m$; soit $\lambda\ p\ \nu = m$.

Le mot m a été formé à partir des mots de f : $p_1\ i\ p_2$ et $q_1\ i\ q_2$ comme le produit:

$$\delta_i(p_1 i p_2)\ \omega_i(q_1 i q_2) = p_1\ i\ q_2 = m = \lambda\ p\ \nu$$

- Si $i \in \lambda$ alors $\omega_i(m) = q_2 \succcurlyeq p$.

Comme $q_2 \in f$ (f est fermé) donc $p \in f$.

- De même si $i \in \nu$ alors $\delta_i(m) = p_1\ i \geqslant p$ et $p_1\ i$ appartient à f de même que p.

- Si $i \in p$ alors $p = k_1\ i\ k_2$ et on vérifie que $k_1\ i \leqslant p_1\ i$ donc appartient à f et de même $i\ k_2 \leqslant i\ q_2$ appartient à f. Donc $\delta_i(k_1 i) \cdot \omega_i(i k_2) = k_1\ i\ k_2 = p$ appartient à $\mu_i(f)$.

Il reste à prouver la commutation des opérations μ_i et μ_j sur des éléments fermés f de G(S). Il suffit pour cela de montrer :

$$\mu_i(\mu_j(f)) \supseteq \mu_j(\mu_i(f))$$

Considérons donc un mot nouveau dans $\mu_j(\mu_i f)$. Il est généré (par μ_j) à partir de deux mots de $\mu_i(f)$. Comme $\mu_i(f)$ est fermé, ce mot m peut toujours être considéré comme ayant été généré à partir des mots m_1 et m_2 de $\mu_i(f)$ du type suivant :

$$m_1 = \alpha_1\ j \qquad m_2 = j\ \beta_2 \qquad (\in \mu_i f)$$

$$m = \alpha_1\ j\ \beta_2$$

Il est évident que i n'appartient pas simultanément à α_1 et β_2. Donc trois cas se présentent

$1^{er})$ $i \notin \alpha_1$, $i \notin \beta_2$

alors m_1 et m_2 appartiennent à f (les mots propres de $\mu_i(f)$ contiennent la lettre i). Par conséquent $m \in \mu_j(f) \subseteq \mu_i(\mu_j f)$

$2^{e})$ $i \in \alpha_1$ $(i \notin \beta_2)$

Nous poserons $\alpha_1 = a_1\ i\ a_2$ et donc $m_1 = a_1\ i\ a_2\ j$. Ce mot m_1 est donc généré à partir des mots $a_1\ i$ et $i\ a_2\ j$ de f. Le mot m_2 appartient à f.

Donc $\delta_j(ia_2j)\ \omega_j(m_2) = i\ a_2\ j\ \beta_2 \quad \in \mu_j\ f$.

De même $a_1\ i \in \mu_j\ f$.

Donc $\delta_i(a_1 i)\ \omega_i(ia_2j\beta_2) = a_1\ i\ a_2\ j\ \ _2 = m$ appartient à $\mu_i(\mu_j f)$.

3^e) $i \in \beta_2 \quad (i \notin \alpha_1)$

Le raisonnement est analogue au 2^e cas.

Applications à la recherche des chemins.

Nous nous limiterons aux éléments fermés du gerbier libre de carré nul engendré par S. L'application produit des n applications μ_i (dans n'importe quel ordre) se notera μ. Nous allons montrer que si l'on part de l'expression f somme des mots du 1^{er} degré et du second degré (associés aux arcs possibles du réseau) l'expression $\mu(f)$ contient tous les chemins simples de ce réseau. Plus précisément les chemins simples de i à j sont décrits par les mots débutant à i et terminant à j.

En effet soit un chemin simple : $i_1\ i_2 \ldots i_q$. Les mots $i_1\ i_2$, $i_2\ i_3, \ldots, i_{q-1}\ i_q$ font partie de f.

Il est facile de voir que $\mu_{i_2}(f)$ contient $i_1\ i_2\ i_3$ et $\mu_{i_3}\mu_{i_2}(f)$ contient $i_1\ i_2\ i_3\ i_4$. La récurrence s'établit aisément. Donc tout chemin figure comme monôme de $\mu(f)$.

Réciproquement tout monôme de $\mu(f)$ représente un chemin. Cela est vrai pour les monômes de degré au plus deux. Si la propriété est vraie pour les monômes de degré $q - 1$ elle est vraie pour le degré q. En effet si $i_1\ i_2 \ldots i_{q-1}\ i_q$ est un tel monôme alors $i_1\ i_2 \ldots i_{q-1}$ et $i_{q-1}\ i_q$ sont des monômes de $\mu(f)$ (fermeture de $\mu(f)$) représentant des chemins l'un joignant i_1 à i_{q-1} et l'autre i_{q-1} à i_q. Le monôme initial représente alors un chemin.

Cela peut fournir un algorithme de calcul des chemins.

Exemple : (réseau figure 1)

On part de $\boxed{f = 12 + 13 + 23 + 34 + 31 + 42}$

(on a négligé les monômes du 1^{er} degré qui en fait n'interviennent pas).

On obtient $\mu_1(f) = f + \delta_1(f)\ \omega_1(f)$

$\delta_1(f) = 1 + 31 \qquad \omega_1(f) = 2 + 3$

Les nouveaux monômes sont : $\boxed{312}$

Donc $f_1 = f + 312$

$\mu_2(f_1) = f + 312 + \delta_2(f_1)\ \omega_2(f_1)$

$\delta_2(f_1) = 12 + 2 + 42 + 312$

$\omega_2(f_1) = 3$

Soit à nouveau : $\boxed{123}$ + $\boxed{423}$

L'opération μ_3 donne :

$\delta_3(f_2) = 13 + 23 + 3 + 123 + 423$

$\omega_3(f_2) = 4 + 1 + 12$

Soit à nouveau : $\boxed{134 + 234 + 231 + 1234 + 4231}$

Enfin la 4^e opération μ_4 donne :

$$\delta_4(f_3) = 34 + 4 + 134 + 234 + 1234$$

$$\omega_4(f_3) = 2 + 23 + 231$$

Soient les monômes nouveaux :

$$\boxed{342 + 1342}$$

L'intérêt de la méthode réside essentiellement dans le fait que les expressions manipulées ne sont pas organisées en matrice.

Un inconvénient réside toutefois : il y a une énorme redondance. En outre les mots (n'étant pas considérés comme commutatifs) ne peuvent être codés que par des listes ordonnées.

Dans la pratique, des méthodes voisines mais plus algorithmiques, utilisent ces techniques analogues mais recherchent une "couverture" du réseau par un certain nombre de chemins (maximaux) et à partir desquels on peut déduire tout chamin. Ces techniques souffrent toutefois du caractère non commutatif de l'enregistrement des informations.

1.4. Sur un algorithme pratique de détermination des chemins simples.

Nous allons décrire un algorithme de détermination des chemins simples d'un réseau, susceptible d'être facilement programmé. L'idée de cet algorithme, est la suivante : un chemin simple de longueur q est un ensemble (en désordre) de q + 1 sommets, dont un des sommets est le dernier dans le chemin, l'ensemble des q autres sommets constituant un chemin de longueur q - 1.

Nous déterminerons donc ces chemins, par ordre de longueur croissante. Nous supposerons que le nombre des sommets est n, chaque sommet étant défini par un entier i ($1 \leq i \leq n$). Nous considèrerons des mots binaires (éventuellement en multiple précision) d'au moins n positions binaires.

Un chemin de longueur q sera alors la donnée de trois éléments :

1) Un mot binaire de degré q + 1 (dont les 1 définissent l'ensemble des sommets).

2) Un entier définissant le dernier sommet de ce chemin.

3) Une adresse (ou référence, ou pointeur) vers un chemin déjà défini de longueur q - 1.

Nous mettrons ces trois éléments sur une même ligne, chacun étant dans une colonne. Les données relatives au réseau seront les suivantes : à chaque entier i ($1 \leq i \leq n$) on définit le mot binaire ayant un seul 1 en position i noté e_i et la liste des entiers définissant les sommets successeurs possibles du sommet i.

Supposons avoir tous les chemins de longueur q (lorsque q = 0 ces chemins se confondent avec les sommets initiaux à partir desquels on cherche les chemins) dans une certaine zone d'adresse de p à r. Considérons un index ℓ variant de p à r. En colonne 2 de la ligne ℓ, nous avons le numéro i du dernier sommet d'un certain chemin. En revenant aux données, à ce numéro i correspond une liste d'entiers $i_1, i_2, \ldots, i_k$ (successeurs possibles). Nous formerons alors l'intersection du mot binaire $1^{ère}$ colonne de la ligne ℓ successivement avec les mots binaires e_{i_1}, e_{i_2} etc... . Chaque fois que cette intersection est vide, nous formons un nouveau chemin que nous rangerons dans les lignes r + 1, r + 2,.... . Ce chemin aura en première colonne l'union des mots binaires correspondants, en deuxième le numéro i_1 (ou i_2 etc...) et en adresse référence (3^e colonne) l'adresse ℓ.

Nous obtiendrons, ainsi, s'il en est tous les chemins de longueur q +

Exemple :

Reprenant l'exemple du réseau (figure 1) à 4 sommets, les données sont :

N° du sommet	mot binaire	liste des successeurs
1	(1)	2, 3
2	(2)	3
3	(3)	1, 4
4	(4)	2

Nous cherchons les chemins simples issus de 1 et 2. Nous initialisons donc le triple tableau

Adresse	Mot binaire	Numéro de dernier sommet	Pointeur
1	(1)	1	0
2	(2)	2	0

Nous formons alors les chemins de longueur 1.

3	(12)	2	1
4	(13)	3	1
5	(23)	3	2

Puis les chemins de longueur deux :

6	(123)	3	3
7	(134)	4	4
8	(123)	1	5
9	(234)	4	5

Enfin les chemins de longueur 3 :

10	(1234)	4	6
11	(1234)	2	7

Si l'on désire alors retrouver les chemins de longueur donnée (par exemple 3) on utilise les deux dernières colonnes. Par exemple en partant de la ligne 11 en deuxième colonne, on a le sommet 2 et en troisième colonne la référence 7. On se ramène en ligne 7 où nous trouvons le sommet 4 et le n° de ligne 4 etc....

On retrouve donc la liste : 2, 4, 3, 1 qui donne (dans l'ordre inverse) le chemin 1, 3, 4, 2.

Remarque :

Dans la pratique, la première colonne ne sert qu'à la construction des chemins.

Plus exactement, seuls les éléments de la première colonne de la zone q, servent à construire les chemins de longueur q + 1. Donc il est possible (dans des réseaux à nombreux sommets) de n'utiliser pour cette première colonne qu'une mémoire de manoeuvre et ne retenir à titre de résultat que les seules deuxième et troisième colonne.

2) Réseau avec couple d'entrée-sortie. Equivalence. Réseau série parallèle.

Nous considèrerons une fois pour toute, un ensemble P de p sommets, chaque sommet étant désigné par un numéro 1, 2,...p, et nous nous intéressons aux réseaux (sans boucles) ayant P comme ensemble de sommets, uniquement sous l'angle des cheminements simples par sommets. On est alors conduit à assimiler l'ensemble de ces réseaux à l'ensemble G_p des relations binaires non réflexives sur P ou encore à celui des matrices booléennes, carrées d'ordre p, à diagonale nulle. Cet ensemble est un treillis (par inclusion), distributif.

Nous allons nous intéresser aux cheminements joignant un couple de deux sommets distincts que nous prendrons une fois pour toute (1,p).

2.1. Equivalence sur G_p à partir d'un couple (1,p) de sommets. Réseau restreint par rapport à (1,p).

Proposition 1 :

La relation entre deux réseaux R_1 et R_2 de G_p définie par : R_1 et R_2 ont les mêmes chemins simples du sommet 1 au sommet p est une relation d'équivalence sur G_p.

Il est clair qu'il s'agit bien d'une relation d'équivalence.

Définition 1 :

On appelle réseau restreint d'un réseau R de G_p à partir du couple (1,p) de sommets, le réseau (noté $\bar{R}$) de G_p défini par :

$\bar{R}(i,j) = 1$ (le sommet i est joint au sommet j) si et seulement si dans au moins un chemin simple joignant 1 à p, le sommet i précède immédiatement le sommet j.

Exemple :

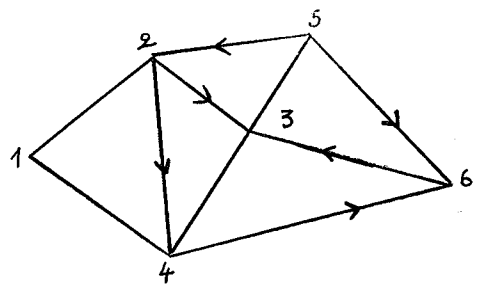


Figure 2

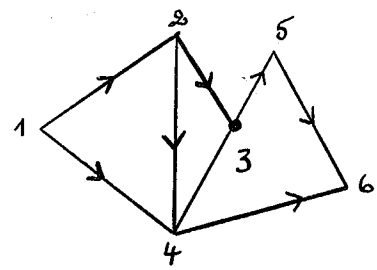


Figure 3

Le réseau R de la figure 2 a pour chemins simples joignant 1 à 6 : 12346 + 12356 + 124356 + 1246 + 14356 + 146. A partir de ces chemins on construit le réseau restreint $\bar{R}$ (figure 3).

Proposition 2 :

Deux réseaux R_1 et R_2 de G_p sont équivalents par rapport au couple (1,p) si et seulement si $\bar{R}_1 = \bar{R}_2$. En outre le réseau restreint d'un réseau donné est le plus petit de sa classe d'équivalence. Enfin chaque classe d'équivalence est convexe relativement à l'inclusion.

Le réseau restreint n'étant défini qu'à partir des chemins simples joignant 1 à p, la première partie de cette proposition est évidente.

Il est d'autre part évident que $\bar{R} \subseteq R$ et que $\bar{R} \equiv R$, ce qui assure que $\bar{R}$ est le réseau minimum de sa classe d'équivalence.

Enfin, il est facile de vérifier que si $R_1 \subseteq R_2$ les chemins simples joignant 1 à p dans R_1 sont des chemins simples dans R_2. Si donc $R_1 \subseteq R \subseteq R_2$ et si $R_1 \equiv R_2$, R a les mêmes (1,p) chemins simples que R_1 et R_2 d'où $R \equiv R_1$.

Définition 2 :

Un réseau R de G_p est parfait entre 1 et p, si tout sommet i fait partie d'au moins un chemin simple allant de 1 à p.

2.2. Détermination des réseaux maximaux (maximaux relatifs) d'une classe d'équivalence de G_p.

Soit une classe d'équivalence de G_p définie par un réseau restreint Soit R un réseau tel que $\rho \subseteq R$. On appelle réseau maximal relativement à R de classe ρ, tout réseau M maximal par inclusion, équivalent à ρ et vérifiant $M \subseteq$

On est assuré évidemment de l'existence de tels réseaux.

Nous allons donner un moyen systématique de déterminer ces réseaux. Nous pouvons supposer bien entendu que $\rho \subset R$ sinon ρ est le seul réseau répondant à la question.

Nous déterminerons alors tous les chemins entre 1 et p du réseau R. Si ces chemins sont tous des chemins de ρ alors R est le seul réseau répondant à la question. Pour chaque chemin de R étranger à ρ on peut déterminer la liste (non vide) des couples consécutifs i,j dans ce chemin, tels que $\rho(i,j) = 0$. Pour supprimer, un tel chemin, il faudra que l'un au moins des couples de cette liste soit supprimé dans R. On est donc amené à développer (en booléen) un produit de somme dont les monômes sont des produits de couples. A chaque monôme irréductible du résultat correspond un réseau maximal relativement à R équivalent à ρ.

Exemple et application.

Soit un réseau électrique de contacts, dont les branches sont orientées par des diodes. On considère ce réseau entre un couple d'entrée-sortie. Supprimer le plus grand nombre de diodes de manière que le réseau garde la même fonction de transfert.

Exemple (figure 4)

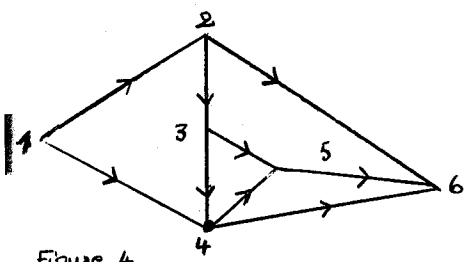


Figure 4

Le réseau est restreint et parfait entre 1 et 6. Nous cherchons donc un réseau équivalent et qui soit le plus symétrique possible.

Les chemins du réseau initial sont :

$$|26 + |46 + |456 + |2356 + |2346 + |23456$$

On considère le réseau initial symétrisé et les chemins supplémentaires sont :

$$|4326 + |4356 + |23546 + |45326$$

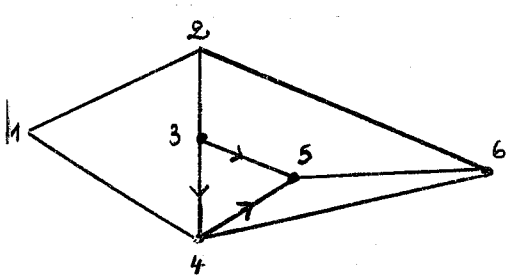
Pour supprimer le

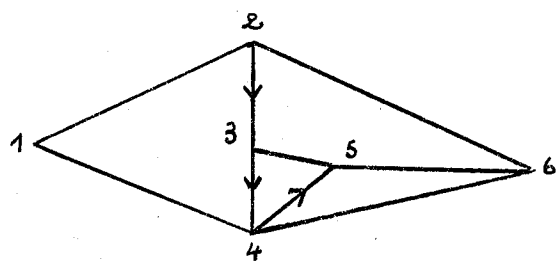
1^{er}	chemin	il	faut supprimer	43 ou 32
2^{e}	"	"	"	43
3^{e}	"	"	"	54
4^{e}	"	"	"	53 ou 32

Nous développons donc :

$$\big((43)+(32)\big)\ (43)\ (54)\ \big((53)+(32)\big) = (43)\ (54)\ (53) + (43)\ (54)\ (32)$$

Nous avons donc les deux solutions :





- Exemple analogue : on considère un réseau routier (orienté : avec sens unique). On suppose que les automobilistes entrent en 1 et sortent en p, qu'ils connaissent suffisamment les itinéraires pour ne pas faire de fausses manoeuvres et revenir à un carrefour déjà passé. On suppose enfin qu'ils peuvent tricher et prendre des sens interdits. Quel est le nombre minimum de surveillant à placer dans les diverses voies, pour pouvoir contrôler le trafic ? Ce problème est strictement le même que le précédent.

2.3. Réseau série-parallèle.

Il existe un très grand nombre de manières de définir un réseau série-parallèle par rapport à un couple d'entrée-sortie.

Nous allons profiter, des notions introduites, pour définir de tels réseaux.

Définition :

Un réseau série-parallèle de G_p, entre les sommets 1 et p est un réseau parfait R symétrique, tel que le réseau restreint $\bar{R}$ est sans circuit (ni aller retour). Le réseau $\bar{R}$ s'appellera réseau série-parallèle totalement orienté entre 1 et p.

Proposition :

La fermeture transitive d'un réseau série-parallèle $\bar{R}$ totalement orienté, entre 1 et p, définit un ordre sur l'ensemble P des sommets et nous avons $i < j$ si et seulement s'il existe au moins un chemin de 1 à p contenant i et j dans cet ordre. L'ordre ainsi défini, possède les propriétés suivantes :

(a) 1 et p sont respectivement les éléments minimum et maximum.

(b) si $i < j$ tout chemin simple joignant 1 à j a au moins un sommet commun avec tout chemin simple joignant i à p.

En effet un réseau sans circuit définit par sa fermeture transitive l'ordre : $i < j$ s'il existe un chemin de i à j. Mais le réseau étant parfait : $\forall i \quad 1 \leqslant i \leqslant p$. D'où l'existence de minimum et maximum. Considérons les chemins simples de $\bar{R}$ et supposons $i < j$ donc il existe un chemin $i\ \mu\ j$. De même on est assuré de l'existence au moins de chemins $1\ \alpha\ i$ et $j\ \beta\ p$. Alors $\delta_i(1\alpha i) \cdot \omega_i(i\mu j) \neq 0$ sinon c'est que le réseau $\bar{R}$ admet un circuit. Donc $1\ \alpha\ i\ \mu\ j$ est un chemin simple. De même on prouverait que $1\ \alpha\ i\ \mu\ j\ \beta\ p$ est un chemin simple de $\bar{R}$.

La propriété (a) de l'ordre obtenu a été vérifiée. Supposons $i < j$ et soient les chemins $m_1 = 1\ \alpha\ j$ $\quad m_2 = i\ \beta\ p$ $\quad$ et $m_3 = i\ \mu\ j$. Montrons que m_1 et m_2 se coupent. Raisonnons par l'absurde. Ces chemins m_1, m_2, m_3 sont des chemins du réseau R. Désignons par f, la somme de tous les mots désignant les chemins simples de R. Comme le réseau R est symétrique, alors $m_3^T = j\ \mu^T\ i$ (m^T mot renversé de m) appartient à f. On en conclue que l'expression $1\ \alpha\ j\ \mu^T\ i\ \beta\ p$ fait partie de f. Ce monôme est obligatoirement nul sinon $j < i$ (contredit $i < j$). Supposons (par exemple) que $\alpha\ \mu^T = 0$ soit k le premier sommet dans α qui se retrouve dans μ^T ; posons $\alpha = \alpha_1\ k\ \alpha_2$ et $\mu^T = \mu_1^T\ k\ \mu_2^T$; alors $\alpha_1\ k\ \mu_2^T$ n'est pas nul. Le mot $1\ \alpha_1\ k\ \mu_2^T\ i\ \beta\ p$ fait alors partie de f. S'il n'est pas nul, alors $k < i$ mais $m_3 = i\ \mu\ j = i\ \mu_2\ k\ \mu_1\ j$ donc $i < k$ (absurde). Donc $k\ \mu_2^T\ i\ \beta\ p$ est nul ou encore $\mu_2^T\ \beta = 0$ ($k \notin \beta$ sinon $\beta \cap \alpha \neq \phi$). Soit ℓ le dernier sommet de β qui se retrouve dans μ_2^T alors $\beta = \beta_1\ \ell\ \beta_2$ et $\mu_2^T = \mu_3^T\ \ell\ \mu_4^T$ (μ_3^T ou μ_4^T éventuellement sont des mots vides). Donc $\mu_3^T\ \ell\ \beta_2 \neq 0$ et par suite $1\ \alpha_1\ k\ \mu_3^T\ \ell\ \beta_2\ p$ est non nul et appartient à f ; donc c'est un chemin simple de $\bar{R}$ et par suite $k < \ell$. Or $\mu = i\ \mu\ j = i\ \mu_2\ k\ \mu_1\ j = i\ \mu_4\ \ell\ \mu_3\ k\ \mu_1\ j$ est aussi un chemin simple de $\bar{R}$ et donc $\ell < k$. Cela est donc absurde.

Le même raisonnement s'applique en supposant que $\mu^T\ \beta = 0$.

Remarque :

Considérons un ensemble ordonné vérifiant les conditions (a) et (b) et soient deux éléments i et j vérifiant : $i < j$. Alors l'ensemble ordonné des éléments x tels que $i \leqslant x \leqslant j$ vérifient les conditions (a) et (b) précédentes.

Réciproque :

Soit un réseau ρ sans circuit dont l'ordre associé sur l'ensemble P des sommets vérifie les conditions (a) et (b) précédentes. Alors ce réseau ρ est série-parallèle totalement orienté et il existe un réseau série-parallèle et un seul dans sa classe d'équivalence.

Nous raisonnerons par récurrence. Cela est vrai si p comporte deux éléments. D'après les mêmes remarques précédentes puisqu'il existe un sommet minimum 0 et maximum p pour l'ordre associé nous avons : $i < j$ si et seulement s'il existe au moins un chemin de 1 à p contenant d'abord i puis j. Donc ρ est un réseau parfait égal à sa restriction (1-p). Soit alors R le réseau symétrisé de ρ. Montrons que R est équivalent (1-p) à ρ. Supposons qu'un chemin simple $1\ \alpha\ p$ de R ne soit pas chemin de ρ. Il existe alors dans le mot α des couples i et j (dans l'ordre) tel que $j < i$. Considérons le 1^{er} sommet i de α donnant une telle éventualité et soit j le dernier sommet dans la suite tel que $j < i$ de sorte que $i\ \alpha\ p = 1\ \alpha_1\ i\ \alpha_2\ j\ \alpha_3\ p$. Si $j\ \alpha_3\ p$ est un chemin de ρ alors la condition (b) est mise en défaut. Sinon, on reprend le raisonnement sur $j\ \alpha_3\ p$ qui apparait comme un chemin étranger au sous réseau ρ' de ρ engendré par les éléments $x : j \leqslant x \leqslant p$ et vérifiant les conditions (a) et (b) du théorème. On aboutit à une contradiction en vertu de l'hypothèse de récurrence.

Le réseau R est donc bien série-parallèle et sa restriction (1,p) n'est autre que ρ. C'est le seul réseau symétrique de sa classe. En effet s'il y en avait un autre R_1 différent c'est que $R_1(i,j) \neq R(i,j)$ donc par exemple $R_1(i,j) = 0$ alors que $R(i,j) = 1$ or $\rho(i,j) + \rho(j,i) = R(i,j) = R_1(i,j)$ ce qui est absurde.

Remarque finale :

Le réseau restreint $\bar{R}$ associé à un réseau R série-parallèle étant sans circuit nous savons [25] qu'il n'existe qu'un réseau minimal ρ ayant même fermeture transitive que $\bar{R}$. Ce réseau ρ n'est autre que le réseau associé à la relation de couverture (ou consécutivité) de l'ordre commun défini par $\bar{R}$ et ρ.

Il est évident d'après la réciproque précédente que ρ est encore un réseau série-parallèle totalement orienté.

3) Treillis série-parallèle. Propriétés.

L'ordre sur les sommets d'un réseau série-parallèle a été étudié dans [12] où l'on a montré qu'il s'agissait d'un ordre réticulé.

Nous allons donner une nouvelle définition de cet ordre, par la condition très simple de chaîne que nous avons mise en évidence dans le paragraphe précédent. Nous essayerons, en même temps, de définir cette notion sur des ensembles infinis.

3.1. Préliminaires sur les ensembles ordonnés complets.

Définition :

Un ensemble ordonné E est complet si toute chaîne (partie totalement ordonnée) admet une borne supérieure et inférieure dans E.

Un ensemble ordonné fini est évidemment complet (les chaînes sont finies).

Un treillis complet est un ensemble ordonné complet.

Proposition I :

Si E est un ensemble ordonné complet, toute partie M non vide, ensemble des majorants de F (partie quelconque) admet un élément minimal. Si en outre cet élément minimal est unique c'est le minimum de M.

En effet considérons une chaîne C de M maximale par inclusion (il en existe, l'ensemble des chaînes de tout ordonné est un ensemble inductif).

Soit u la borne inférieure de C dans E. Montrons que $u \in C$; u en effet est le maximum de l'ensemble des minorants de C qui contient F. Donc u est un majorant de F et appartient donc à M et par suite à C (puisque C est maximale dans M). Cet élément u est minimal dans M sinon on trouverait $y \in M$ tel que $y < u$ mais alors $y \notin C$ et C ne serait pas une chaîne maximale de M.

Supposons alors que u soit le seul élément minimal de M. Alors u est le minimum de M. En effet si $x_1 \in M$ est tel que $u \not\leqslant x_1$ alors comme x_1 n'est pas minimal, on peut trouver $x_2 \in M$ avec $x_2 < x_1$. Cet élément x_2 n'est pas minimal et en outre $u \not\leqslant x_2$. En recommençant ainsi on trouverait une chaîne C_1 de M contenue dans une chaîne C maximale dans M et ne passant pas par u ; à cette chaîne C serait associé un élément minimal v de M et distinct de u ce qui contredit l'hypothèse.

Remarque :

Par dualité on a : si E est un ensemble ordonné complet et si M est l'ensemble (non vide) des minorants de F, M admet un élément maximal. Si cet élément maximal est unique c'est le maximum de M.

Proposition 2 :

Si un ensemble ordonné E est réticulé, possède un maximum I et un minimum O et est complet, alors c'est un treillis complet.

En effet soit F une partie quelconque de E et M l'ensemble (non vide grâce à l'élément I) des majorants de F. M possède un élément minimal (prop. précédente). Montrons qu'il n'y en a qu'un. Supposons que x et y soient deux éléments minimaux de M et posons : $u = x \wedge y$. Tout élément f de F est inférieur à x et y donc $f \leqslant u$. Par suite u appartient à M et comme x et y sont minimaux dans M c'est que $u = x = y$.

La démonstration est ainsi achevée : u est borne supérieure de F et par dualité on démontrerait que F admet une borne inférieure.

3.2. Treillis série-parallèle complet.

Définition :

Un ensemble ordonné E est dit série-parallèle (en abrégé SP) si

(a) E est complet et possède un élément minimum 0 et un élément maximum 1

(b) pour tout couple d'élément x, y vérifiant $x \leqslant y$ on a la propriété : toute chaîne maximale du segment $[x,1]$ a une intersection non vide avec toute chaîne maximale du segment $[0,y]$.

Remarque :

Cette définition est auto-duale.

Théorème 1 :

Tout ensemble E ordonné SP est un treillis complet.

Cela est évident si E est une chaîne.

Supposons que $x, y \in E$ soient non comparables. L'ensemble M des majorants de $\{x,y\}$ est non vide et possède donc (proposition 1 précédente) au moins un élément minimal. Montrons qu'il n'y en a qu'un. Soient z_1 et z_2 deux tels éléments. La chaîne $0 < y < z_2$ est contenue dans une chaîne maximale C_2 de $[0,z_2]$. De même la chaîne $x < z_1 < 1$ est contenue dans une chaîne maximale C_1 de $[x,1]$. Comme $x < z_2$ ces chaînes se coupent en z. On vérifie $x \leqslant z \leqslant z_2$ et en outre z est comparable à y et z_1 ; mais $z \not\leqslant y$ sinon $x \leqslant y$. Donc $y < z$ et $z \in M$. Comme z_2 est minimal alors $z = z_2$ et comme z_1 est minimal dans M et comparable à z, on en déduit que $z = z_1 = z_2$.

Conséquences :

On ne distinguera plus la notion d'ensemble ordonné SP et la notion de treillis SP.

Le dual d'un treillis SP est un treillis SP.

Notations :

Nous noterons par K la relation binaire de comparabilité et par $\bar{K}$ la relation de non comparabilité.

$$x \, K \, y \iff x \leqslant y \quad \text{ou} \quad y < x$$

$$x \, \bar{K} \, y \iff x \not\leqslant y \quad \text{et} \quad y \not< x$$

Théorème 2 :

Les propositions suivantes sont équivalentes :

(a) E est un treillis SP

(b) E est un treillis complet tel que :

$$\forall x \, \forall y \, \forall z \quad [x < y \quad \text{et} \quad z \, \bar{K} \, x \quad \text{et} \quad z \, \bar{K} \, y] \Rightarrow x \vee z = y \vee z$$

(c) proposition duale de (b)

(d) E est un treillis complet tel que :

$$\forall x \, \forall y \, \forall z \quad [x \, \bar{K} \, (y \wedge z) \quad \text{et} \quad y \, \bar{K} \, z] \Rightarrow x \, \bar{K} \, y \quad \text{et} \quad x \, \bar{K} \, z$$

(e) proposition duale de (d).

Démonstration :

(a) $\Longrightarrow$ (b) car en posant $z_1 = x \vee z$ on a $y \not\geqslant z_1$ sinon $y \geqslant z$; les chaînes $0 < z < z_1$ et $x < y < 1$ sont contenues respectivement dans des chaînes maximales de $[0,z_1]$ et $[x,1]$ se coupant en a (puisque $x<z_1$) ; a est comparable à y et z et $x \leqslant a \leqslant z_1$. Mais $a \not< y$ sinon : $z \leqslant a \Longrightarrow z \leqslant y$ et $a < z \Longrightarrow x \lneqq z$. Donc : $y \leqslant a$ d'où $y \leqslant z_1$ et $y \vee z \leqslant x \vee z$. Comme $x < y$ cela conduit à $x \vee z = y \vee z$.

(b) $\Longrightarrow$ (a)

Soit x_o et y_o vérifiant

$$\boxed{x_o < y_o} \qquad (1)$$

Considérons une chaîne maximale C_o de $[0,y_o]$.

Et une chaîne maximale C_1 de $[x_o,1]$.

Soit α la borne inférieure des éléments η de C_o vérifiant $x_o \leqslant \eta$; α appartient à C_o et $x_o \leqslant \alpha$. Si $x_o = \alpha$ les chaînes se coupent. Si $x_o < \alpha$ tout élément η de C_o tel que $\eta < \alpha$ vérifie : $\eta \not\geqslant x_o$. Nous montrerons que la chaîne maximale $C_o \cap [0,\alpha]$ coupe C_1.

Nous renoterons $\alpha = y_o$ de telle sorte que nous supposerons désormais :

$$\boxed{\forall y \ , \ y \in C_o \ , \ y \neq y_o \Longrightarrow x_o \not\leqslant y} \qquad (2)$$

Désignons alors par β la borne supérieure des éléments ξ de C_1 tels que $\xi \leqslant y_o$; β appartient à C_1 et $\beta \leqslant y_o$. Si $\beta = y_o$ les chaînes se coupent, sinon $\beta < y_o$. Alors tout élément ξ de C_1 vérifiant $\xi > \beta$ vérifie $\xi \not\leqslant y_o$. En outre les éléments y ($y \in C_o$, $y \neq y_o$) vérifient : $\beta \not\leqslant y$ sinon $x_o < y$ (contredit (2)). Nous reprendrons la notation $\beta = x_o$ et nous pouvons alors supposer :

$$\boxed{\forall x \ , \ x \in C_1 \ , \ x \neq x_o \Longrightarrow x \not\leqslant y_o} \qquad (3)$$

Soient x_1 la borne inférieure des $x \in C_1$ $x \neq x_o$ et y_1 la borne supérieure des $y \in C_o$, $y \neq y_o$. Nous avons

$$\boxed{y_1 \leqslant y_o \quad \text{et} \quad x_o \leqslant x_1} \qquad (4)$$

Nous examinerons les 4 cas possibles de (4).

A) $x_1 = x_o$ et $y_1 = y_o$

Nous avons :

$\exists\, y \quad (y \in C_o \quad y \neq y_o)$ et : $y \bar{K} x_o$

sinon $\forall y \quad y \, K \, x_o$ et comme $x_o \not\leqslant y$ on déduit $y < x_o$

Alors $y_1 \leqslant x_o$ soit $y_o \leqslant x_o$ ce qui contredit (1).

Soit y' un tel élément.

Si $\exists\, x$ et $y' \bar{K} x$ alors

$y' \vee x = y' \vee x_o \leqslant y_o \Longrightarrow x \leqslant y_o$ contredit (3)

sinon $\forall x$, $y' \, K \, x$; comme aucun x ne vérifie $x \leqslant y'$ sinon $x \leqslant y_o$ (3) c'est que $\forall x \quad y' < x \Longrightarrow y' \leqslant x_o$ or $y' \bar{K} x_o$ cela est absurde.

B) $x_1 = x_o$ et $y_1 \neq y_o$ donc $y_1 \prec y_o$

(y_o est consécutif à y_1) car C_o est maximale.

Nous avons :

$y_1 \bar{K} x_o$ car la seule comparaison serait $y_1 < x_o$ et comme $x_o < y_o$, la relation $y_1 \prec y_o$ serait mise en défaut.

Par ailleurs :

$\forall x \quad y_1 \; K \; x$ sinon $y_1 \vee x = y_1 \vee x_o \leqslant y_o$ et $x \leqslant y_o$ ce qui contredit (3).

Or aucun x ne vérifie $x \leqslant y_1$ sinon $x \leqslant y_o$ donc :
$\forall x \quad y_1 < x \Longrightarrow y_1 \leqslant x_o$ ce qui contredit $y_1 \; \bar{K} \; x_o$.

C) $x_1 \neq x_o$ donc $x_o \prec x_1$ et $y_1 = y_o$

Nous avons :

$\exists y \quad y \; \bar{K} \; x_1$

sinon $\forall y : y \; K \; x_1$ qui ne peut avoir lieu que si
$y < x_1$ $(y \geqslant x_1 \Longrightarrow y \geqslant x_o)$
Donc $y_o \leqslant x_1$.

Si $y_o = x_1$ ces chaînes se coupent si $y_o < x_1$ comme $x_o < y_o$
la relation $x_o \prec x_1$ est contredite.

Appelons y' un tel terme ; on a :

$y' \; \bar{K} \; x_o$ sinon $y' < x_o$ et $y' \; K \; x_1$

Donc $y' \vee x_o = y' \vee x_1 \leqslant y_o \Longrightarrow x_1 \leqslant y_o$ ce qui contredit (3).

D) Supposons $y_1 \prec y_o$ et $x_o \prec x_1$

Alors :

$y_1 \; \bar{K} \; x_o$ sinon c'est que $y_1 < x_o$ $(< y_o)$: la relation $y_1 \prec y_o$ est mise en défaut.

Si $y_1 \bar{K} x_1$ alors $y_1 \vee x_1 = y_1 \vee x_0 \leqslant y_0$.

Cela entraîne $x_1 \leqslant y_0$ (absurde).

Si $y_1 K x_1$ cela ne peut être que :

$y_1 < x_1$ donc $x_0 \vee y_1 = x_1$

et $x_1 \leqslant y_0$ (absurde).

Par suite de l'auto-dualité de (a) nous avons (a) $\Longleftrightarrow$ (b) $\Longleftrightarrow$ (c).

Montrons (c) $\Longrightarrow$ (d)

x en effet ne peut être plus grand que y (resp z) sinon $x \geqslant y \wedge z$; x ne peut être à la fois $< y$ et $< z$. Donc si $x < y$, $x \bar{K} z$; d'après (d) alors $z \wedge x = z \wedge y < x$ (absurde).

(d) $\Longrightarrow$ (c)

Nous avons $x < y$, $z \bar{K} x$, $z \bar{K} y$

x est comparable à $y \wedge z$ sinon d'après (d)

x est non comparable à y (absurde). Or comme $x \nleqslant y \wedge z$ sinon $x \leqslant z$ cela entraîne $y \wedge z < x$ donc $y \wedge z \leqslant x \wedge z$ d'où $y \wedge z = x \wedge z$.

Corollaire :

Tout sous-treillis complet d'un treillis SP est un treillis SP.

En particulier tout sous-treillis fini d'un treillis SP est un treillis SP.

Définition :

On appelle couple fondamental d'un treillis E un couple d'éléments (x,y) vérifiant :

(1) $x < y$

(2) Il existe a, b vérifiant $x < a < y$, $x < b < y$ tels que $a \vee b = y$ et $a \wedge b = x$.

a et b sont évidemment non comparables.

Proposition :

Si (x,y) est un couple fondamental d'un treillis SP alors le segment $[x,y]$ est complémenté.

Soit $z \in]\, x, y\, [$. Par hypothèse $\exists$ a, b $\in]\, x, y\, [$ tels que $a \vee b = y$ et $a \wedge b = x$.

Si z est comparable à a, il ne l'est pas à b. Dans ce cas $z \wedge b = a \wedge b = x$ et $z \vee b = a \vee b = y$ en vertu de (b) et (c) du théorème 2.

Si z n'est comparable ni à a ni à b, alors si $z \vee b \neq y$, $z \vee b$ n'est pas comparable à a. Par suite :

$$a \wedge (z \vee b) = a \wedge z = a \wedge b = x \qquad \text{et}$$

$$a \vee z = a \vee (z \vee b) = a \vee b = y$$

Si $z \vee b = y$ et si $z \wedge b \neq x$, $z \wedge b$ n'est pas comparable à a et de la même manière

$$a \wedge (z \wedge b) = a \wedge z = a \wedge b = x$$

$$a \vee (z \wedge b) = a \vee z = a \vee b = y$$

Théorème 3 :

Un treillis complet est SP si et seulement si deux couples fondamentaux (p,q) et (r,s) ne sont jamais enchevêtrés (c'est-à-dire $p < r < q < s$).

C.N. Si les couples fondamentaux vérifiaient $p < r < q < s$ alors en désignant par r_1 et q_1 des compléments relatifs de r et q respectivement dans $[p,q]$ et $[r,s]$, on a : $q \bar{K} q_1$ et $r_1 \bar{K} (q \wedge q_1)$ donc en vertu de la propriété (d) du théorème 2 : r_1 non comparable à q et q_1 ce qui est absurde.

CS. E est un treillis complet. Montrons la propriété (c). Soit :

$x < y$, $z \bar{K} x$, $z \bar{K} y$

Soient : $\alpha = z \wedge x$ et $\beta = z \vee x$

$\alpha' = z \wedge y$ $\beta' = z \vee y$

Si $\alpha = \alpha'$ (c) est vérifiée.

Supposons $\alpha < \alpha'$ comme $\alpha' < z < \beta \leqslant \beta'$ le non-enchevêtrement de (α,β) et (α',β') entraîne $\beta = \beta'$.

α' n'est pas comparable à x. Nous avons $\alpha' \wedge x = \alpha$. Posons $\alpha' \vee x = \alpha''$ le couple (α,α'') est fondamental et nous avons : $\alpha'' \leqslant y$ car $\alpha' < y$ et $x < y$ donc $\alpha'' < \beta'$ puisque $y < \beta'$.

Le couple (α',β') est enchevêtré avec (α,α'') car $\alpha < \alpha' < \alpha'' < \beta'$. Nous obtenons une contradiction.

3.3. Reconstitution de réseaux série-parallèles à partir d'un treillis fini SP.

On supposera que E est un treillis fini SP.

Définition 1 :

On dit que le couple (x,y) de E est permis si : (1) $x < y$; (2) il n'existe aucun couple fondamental (p,q) enchevêtré avec (x,y).

Remarque :

Il résulte de la définition que :

1er) si $x \prec y$ alors (x,y) est permis on l'appellera couple trivial.

2e) si (x,y) est fondamental alors il est permis

3e) (0,1) est toujours permis

Définition 2 :

C étant un ensemble de couples (x,y) où $x < y$, on appelle C-suite simple d'extrémité x_0, x_n toute suite $x_0, x_1, x_2, \ldots, x_n$ d'éléments de E vérifiant (1) $x_i \neq x_j$ si $i \neq j$ (2) l'un des couples (et un seulement) (x_i, x_{i+1}) ou $(x_{i+1}, x_i) \in C$.

Définition 3 :

Un ensemble c de couples ordonnés est dit génératif si :

(a) tout couple trivial $(x,y) \in c$;

(b) tout couple de c est permis ;

(c) deux couples de c ne sont jamais enchevêtrés.

Théorème :

c étant un ensemble génératif de couples ordonnés, alors toute c-suite simple $0, x_1, x_2, \ldots, 1$ d'extrémités 0,1 est croissante $(x_i < x_{i+1})$.

Réciproquement si c est un ensemble de couples ordonnés contenant tout couple trivial et si toute c-suite simple d'extrémités 0,1 est croissante, alors c est un ensemble génératif.

Proposition directe.

Soit la c-suite simple $0, x_1, x_2, \ldots, x_n, 1$. Nous avons $0 < x_1$. Supposons qu'au rang p nous ayons $0 < x_1 < x_2 < \ldots < x_p$ mais $x_{p+1} < x_p$.

Alors pour $q \geqslant p + 1$, on aurait $x_q < x_p$ sans quoi à un certain stade $x_q < x_p < x_{q+1}$ et x_q s'intercalerait de 0 à x_p entre x_r et x_{r+1} (suite simple) ; les couples (x_r, x_{r+1}) et (x_q, x_{q+1}) seraient alors enchevêtrés. Par conséquent, on aurait $1 < x_p$. Cela est absurde.

Proposition réciproque.

Montrons d'abord que les couples ne sont pas enchevêtrés. Sinon $\exists$ (p,q), (r,s) $\in$ c avec $p < r < q < s$. Alors on peut trouver une c-suite simple $0, \ldots, p, q, \ldots, r, s, \ldots, 1$ (de 0 à p, de q à r, et de s à 1, on utilise des couples triviaux). Cette suite n'est pas croissante.

Montrons à présent que les couples de c sont permis.
Sinon $\exists$ (x,y) $\in$ c avec (p,q) fondamental tel que $p < x < q < y$. Soit x_1 un complément de x dans $[p,q]$. On peut définir deux chaînes triviales

$$p\ t_1\ t_2 \ldots x\ r_n \ldots r_1\ q \quad \text{et} \quad p\ v_1\ v_2 \ldots x_1\ w_1\ w_2 \ldots q$$

n'ayant en commun que p et q.

On peut construire alors une c-suite simple :

$$0, \ldots, p\ v_1, v_2, \ldots, x_1\ w_1\ w_2, \ldots, q\ r_1\ r_2, \ldots, r_n\ xy, \ldots, 1$$

(de 0 à p et y à 1, on utilise des couples triviaux). Cette suite n'est pas croissante.

Ce dernier théorème permet de construire divers réseaux série-parallèles à partir d'un treillis fini SP. Il suffit de considérer tout ensemble C génératif de couples de E. A partir d'un tel ensemble on définit le réseau ρ de la manière suivante : $\rho(i,j) = 1 \iff (i,j) \in C$.

B I B L I O G R A P H I E

[1] BENZAKEN (Claude) : Définition et propriétés de certaines familles de fonctions booléennes croissantes, C.R.Acad. Sc. Paris, t.259, 1964, p 1369.

[2] BENZAKEN (Claude) : Les familles de fonctions booléennes déduites de certaines familles de fonctions booléennes croissantes. Critères de détermination de l'indice d'une fonction croissante, C.R.Acad. Sc. Paris, t. 260, 1965, p. 1528 - 1531.

[3] BENZAKEN (Claude) : Pour une bonne compréhension du nombre chromatique d'un graphe, à l'aide des familles de fonctions booléennes. The Fourth International Conference on Operational Research. (Theory of Graphs). Boston 1966.

[4] BENZAKEN (Claude) : Algorithmes de dualisation d'une fonction booléenne. RFTI Chiffres (9) (n°2) 1966. p 119 - 28.

[5] BENZAKEN (Claude) : Structures algébriques des cheminements. Pseudo-treillis distributifs.
(Buletinul Institului Politchnic din Iasi (XI (XV) 1 - 2) 1965).
Voir également : (Network and switching theory. Academic Press Inc. sous presse).

[6] BENZAKEN (Claude) : Treillis série-parallèle, C.R.Acad. Sc. Paris, t. 260, 1965, p. 5431 - 34.

[7] BERGE (Claude) : Théorie des graphes et ses applications. Paris, Dunod 1958.

[8] BIRKHOFF (Garett) : Lattice Theory. Amer. Math. Soc., Publ. Coll., New York, 1948.

[9] CARVALLO (M.) : Monographie des treillis et algèbre de Boole. Paris, Gauthier-Villars, 1962.

[10] DUBREIL-JACOTIN (M.L.), LESIEUR (L.), CROISOT (R.) : Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques. Cahiers Scientifiques. Gauthiers-Villars, 1953.

[11] DUFFIN (R.J.) : Topology of series-parallel retworks. J. Math. Anal. Appl. V 10 - 1965. p. 303 - 18.

[12] ELGOT (C.C.), WRIGHT (J.B.) : Series-parallel graphs and lattices. Duke Math. J., V 26 - 1959. p. 325 - 38.

[13] HEDETNIEMI (Stephen) : Homomorphisms of graphs. The University of Michigan, 1965.

[14] HIGMAN (Graham) : Ordering by divisibility in abstract algebras. Proc. London Math. Soc (3) 2, 1952, p. 326 - 36.

[15] KUNTZMANN (Jean) : Algèbre de Boole. Paris, Dunod, 1965.

[16] KUNTZMANN (Jean) : Un théorème sur les composants premiers d'une fonction booléenne et ses applications.
Automatisme, p. 18, Janvier 1964.

[17] LUNC (A.G.) : Algébraičéskié métody analiza i sintéza kontaktnyh shém. IZV. Akad. Naouk SSSR 16, 1952, p. 405 - 26.

[18] MAGHOUT (Khaled) : Sur la détermination des nombres de stabilité et du nombre chromatique d'un graphe. C.R. A.S. Paris, t.248, 1959, p. 3522.

[19] OKADA (Satio) : Algebraïc determination of loops and paths in graphs. The Fourth International Conference on Operational Research. (Theory of graphs). Boston 1966.

[20] PAIR (Claude) : Sur des algorithmes pour des problèmes de cheminement. International Seminar on graph theory and its applications. Rome 1966.

[21] POST (Emil L.) : The two-valued iterative systems of mathematical logic. Annals of math. Studies (5) Princeton University Press (1941). Kraus Reprint Corporation. New York (1965).

[22] PYNE, Mac CLUSKEY (E.J.) : The reduction of redundancy in solving prime implicant tables. IRE EC 11, Août 1962, p. 473 - 82.

[23] RIGUET (Jacques) : A quick method to find the matrix of conductances of a given switching network. Zeitshr. f. math. Logik und Grundlagen d. Math (6), 1960, p. 134 - 42.

[24] ROTH (J.P.), WAGNER (E.G.) : Algebraïc topological methods for the synthesis of switching systems : minimization of non singular boolean trees. I.B.M. Journal. Oct. 1959. p. 326 - 44.

[25] ROY (Bernard) : Cheminements et connexité dans un graphe. Applications aux problèmes d'ordonnancement. Thèse. Paris. 1961.

[26] RUDEANU (Sergiu) : On solving boolean equations in the theory of graphs. Revue Roumaine de Math. pures et appl. Tome XI (6). 1966. p. 653 - 64.

[27] SESHU (S.), REED (M.B.) : Linear graphs and electrical Networks. Addison-Vesley Pub. Comp. 1961.

[28] TISON (Pierre) : Théorie des consensus. Thèse ingénieur-docteur, Grenoble 1965.

[29] ZYKOV (A.A.) : On some properties of linear complexes. Translations of A.M.S (series one, vol. 17, Algebraïc Topology, p. 418 - 49), 1962.

INDEX TERMINOLOGIQUE

TABLE DES MATIERES

Pages

CHAPITRE V - SUR QUELQUES ALGORITHMES PRATIQUES : DUALISATION. DECOMPOSITION.

CHAPITRE VI - SUR UNE STRUCTURE ALGEBRIQUE DES CHEMINEMENTS. PSEUDO-TREILLIS.

Page

CHAPITRE VII - CHEMINEMENTS PAR SOMMETS. TREILLIS SERIE-PARALLELE.

VU

Grenoble, le

Le Président de la Thèse

VU

Grenoble, le

Le Doyen de la Faculté des Sciences

VU, et permis d'imprimer,

Le Recteur de l'Académie de GRENOBLE