Modèles de bases et spectres des fonctions booléennes

Ahmad Sharafeddin-Noury

THESE

présentée à

l'Université Scientifique et Médicale de Grenoble

et à

l'Institut National Polytechnique de Grenoble

pour obtenir le grade de

DOCTEUR DE 3ème CYCLE

Génie Informatique

par

SHARAFEDDIN - NOURY Ahmad

MODELES DE BASES ET SPECTRES DES FONCTIONS BOOLEENNES

Thèse soutenue le 17 Décembre 1980 devant la commission d'examen

C. BENZAKEN	Président
R. DAVID	
J. KUNTZMANN	Examinateurs
A. VERDILLON	
Mme G. SAUCIER	Rapporteur

Je tiens a exprimer toute ma reconnaissance à Monsieur le Professeur J. KUNTZMANN dont les conseils et suggestions m'ont permis de mener à bien ce travail,

Je remercie vivement Madame G. SAUCIER, Professeur à l'Institut National Polytechnique de Grenoble, qui m'a accueillie dans son équipe et m'a toujours témoigné sa plus grande confiance,

Je remercie Monsieur C. BENZAKEN, Professeur à l'Université Scientifique et Médicale de Grenoble et suis très sensible à l'honneur qu'il me fait en acceptant de présider le jury de cette thèse,

Je remercie vivement

Monsieur R. DAVID, Maître de Recherches au Laboratoire d'Automatisme de Grenoble,

Monsieur A. VERDILLON, Maître-Assistant à l'Université Scientifique et Médicale de Grenoble

de me faire l'honneur de participer à ce jury.

Je ne voudrais pas oublier Mesdames DUFFOURD et TREVISAN qui ont dactylographié ce travail, et le service de reprographie de l'IMAG qui en a assuré le tirage.

TABLE DES MATIERES

CHAPITRE 1 : REPRESENTATION VECTORIELLE DES FONCTIONS BOOLEENNES

INTRODUCTION

Cette thèse comporte deux parties.
Dans la première partie (Chapitre I) nous étudions une représentation vectorielle plane pour les fonctions booléennes. Cette représentation unifie quelques méthodes booléennes, à savoir :

1) La méthode de Mc Cluskey
2) L'écriture lexicographique
3) Le tableau de Karnaugh

Dans la deuxième partie de la thèse (Chapitres II à V) nous introduisons la notion de modèle et de spectre des fonctions booléennes et les utilisons pour l'étude de certaines propriétés des fonctions booléennes (ϕ-booléennes ou complètes).
Nous définissons :

a) Le modèle d'une base de la fonction booléenne : couple ordonné (m,l) où m et l représentent respectivement le nombre des monômes premiers et le nombre des lettres de base.

b) Le spectre de la fonction : ensemble de modèles des bases de la fonction.

Dans le deuxième chapitre nous donnons quelques théorèmes d'existence des fonctions ayant des bases premières de modèles donnés.

Dans le troisième chapitre nous étudions quelques propriétés générales des spectres des fonctions booléennes.

Le chapitre III traite les propriétés de la fonction $S_n^{1,1}(X)$ et applications aux fonctions $f(X) + \lambda g(X)$. Cette étude nous permettra de construire quelques fonctions ayant des spectres donnés.

Enfin, dans le chapitre V on étudie des fonctions ϕ-booléennes ou complètes pour lesquelles il n'existe pas de base première avec à la fois m minimum et l minimum (nous nommerons de telles fonctions "excentriques".

RAPPEL DES DEFINITIONS

L'algèbre de Boole est un treillis distributif et complémenté. Dans ce treillis, nous appelons produit noté multiplicativement et somme notée additivement, les opérations de borne inférieure et de borse supérieure. Les éléments nul et universel sont notés 0 et 1. Nous notons le complément par l'accentuation de la quantité sur laquelle il porte, et les quantités simples par des lettres manuscules.

$\tilde{x}$ (x ondulé) désigne indifféremment x ou x'.

Variable générale. C'est un ensemble fini de variables simples $\{x_1,x_2,\ldots,x_n\}$ qui sont ses composants. Nous désignons une variable générale par une lettre majuscule. Nous introduisons les notations suivantes.

$$X^+ = x_1+x_2+\ldots+x_n$$
$$X^\cdot = x_2.x_2\ldots x_n$$
$$X' = \{x_1',x_2',\ldots,x_n'\}$$

X^+ et $X^\cdot$ sont appelées respectivement les condensés additifs et multiplicatifs.

Une fonction booléenne $f(x_1,x_2,\ldots,x_n)$ peut être définie comme une application de $\{0,1\}^n$ dans l'ensemble ordonné $B = \{0,1\}$ muni de la relation d'ordre $0 < 1$.
L'ensemble de ces fonctions est ordonné et possède une structure de treillis de Boole dans lequel la borne supérieure de deux éléments f et g encore appelée somme est notée f+g, leur borne inférieure encore appelée produit est notée f.g et le complément d'un élément f est noté f'.

Duale d'une fonction booléenne. Nous appelons duale d'une fonction f(X), la fonction $f^*(X)$, définie par :

$$f^*(X) = f'(X')$$

Fonction paire. Une fonction f(X) est dire paire si $f(X) = f(X')$.

Fonction croissante (décroissante). Une fonction est dite croissante (décroissante) si elle est croissante (décroissante) par rapport à chacun de ses variables.

Fonction incomplète (ϕ -booléenne). On appelle fonction booléenne incomplète de la variable générale $X_n = \{x_1, x_2, \ldots, x_n\}$ tout couple $f(X_n) = (\underline{f}(X_n), \bar{f}(X_n))$ de fonctions booléennes comparables telles que $\underline{f}(A_n) \leqslant \bar{f}(A_n)$. Les fonctions $\underline{f}$ et $\bar{f}$ sont appelées borne inférieure et borne supérieure de la fonction incomplète.

Monôme. On appelle monôme tout produit non nul de variables directes ou complémentées, et "monôme d'une fonction f" tout monôme majoré par f.

Monal. On appelle monal toute somme $\neq 1$ de variables directes ou complémentées, et "monal d'une fonction f" tout monal minoré par f.

Monôme canoniques. On appelle monôme canonique de la fonction f(X), tout monôme de f, où figurent toutes les variables de X, sous forme directe ou complémentée, et forme canonique la somme de tous les monômes canoniques de la fonction.

Monômes premiers. On appelle monôme premiers d'une fonction booléenne, tout monôme inférieur à cette fonction et tel qu'aucun de ses diviseurs ne soit inférieur à cette fonction.

Variables monoformes et biformes. Une variable qui figure sous une seule forme, directe ou complémentée dans une expression, s'appelle monoforme. Une variable qui figure sous les deux formes est dite biforme.

Egalité irréductible. Soit f une fonction booléenne et $\{m_1, \ldots m_p\}$ un ensemble de monômes. L'égalité

$$f = \sum_{i=1}^{p} m_i$$

sera dite irréductible si on ne peut supprimer aucun monôme du membre de droite sans détruire l'égalité des deux membres.

Consensus. Soit $E = \{m_1, \ldots m_p\}$ un ensemble de monôme m_i dans lequel on note α_i le produit des variables de m_i monoforme dans E et β_i le produit des variables de m_i biformes dans E.

Si l'on a l'égalité irréductible

$$\sum_{i=1}^{p} \beta_i = 1$$

$\alpha = \prod_{i=1}^{p} \alpha_i$ est appelé consensus d'ordre p de E et est noté $\mathcal{C}(m_1, m_2 \ldots m_p)$. Chacun des monômes m_i est appelé générateur du consensus α.

Bases d'une fonction. On appelle base d'une fonction booléenne f, toute somme de monôme premier de f dont la somme est égale à cette fonction.

La somme de tous les monômes premiers possède cette propriété. On la nomme base complète.

On nomme base première (ou irrédondante ou irréductible) une base qui cesse d'être base si on enlève un des monômes premiers qui y figure.

Monôme premier obligatoire. C'est un monôme premier de f qui figure dans toutes les bases de f.

Monôme premier inutile de première espèce. C'est un monôme premier de f qui est majoré par la somme des monômes premiers obligatoire. Un tel monôme ne se présente pas dans une base irréductible.

Monôme premier inutile de deuxième espèce. C'est un monôme premier qui sans être majoré par la somme des monômes premiers obligatoire ne figure dans aucune base irreductible.

PREMIERE PARTIE

CHAPITRE I

REPRESENTATION VECTORIELLE DES FONCTIONS BOOLEENNES

REPRESENTATION VECTORIELLE DES FONCTIONS BOOLEENNES

Unification de quelques méthodes booléennes

Nous allons étudier une réprésentation vectorielle plane pour les fonctions booléennes. A partir de cette représentation on peut retrouver :

1) La méthode de Mc CLUSKEY.
2) L'écriture lexicographique.
3) Le tableau de KARNAUGH.

Nous proposerons également une représentation symétrique.
Pour étudier la maniabilité des représentations proposées nous étudierons le problême de la recherche des monômes premiers à partir des monômes canoniques.

1.1 Représentations vectorielles planes

Soit E un ensemble de n vecteurs $\vec{a}$, $\vec{b}$, $\vec{c}$... du plan, issus d'un même point "1" et indépendants sur le corps (0,1), c'est-à-dire tels que l'on n'ait jamais $S_1 = S_2$, S_1 et S_2 désignant deux sommes de vecteurs différents.

Soient $\vec{x}$ et $\vec{y}$ deux vecteurs de E. Nous déterminons l'extrêmité du vecteur $\vec{x} + \vec{y}$ à laquelle nous attribuons le produit xy.

Supposons F l'ensemble des points obtenus. Soient x et y deux éléments de F (par exemple x = c, z = ab).

Nous déterminons l'extrêmité du vecteur $\vec{x} + \vec{y}$, à laquelle nous attribuons le point xz (abc dans notre exemple de la figure 1.).

Cette représentation est en somme la projection du n-cube sur le plan. Elle comporte 2^n points à cause de la condition d'indépendance. Cela nous permet d'attribuer à chaque sommet de la représentation un monôme canonique à n variables.

Un monôme canonique est donné par ses lettres non accentuées. Par exemple, bd correspond au monôme canonique a'bc'd.

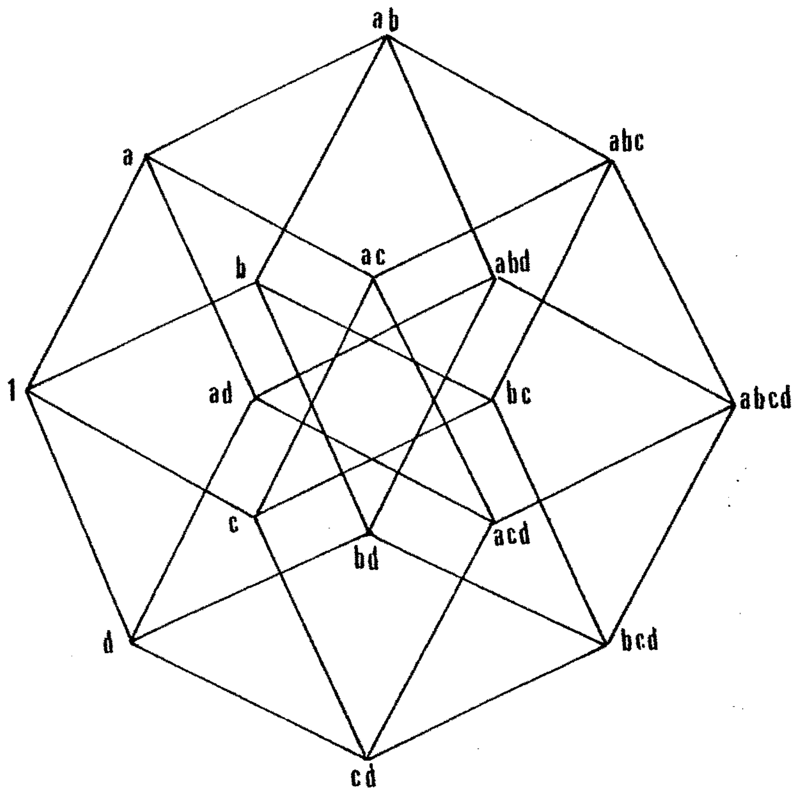


Figure 1. n=4

1.1.1 *Augmentation de la maniabilité*

Pour augmenter la maniabilité de la représentation, prenons certains vecteurs beaucoup plus grands que les autres pour obtenir des sous-systèmes distincts (figure 2).

Les traits joignant les sous-figures sont sous-entendus.

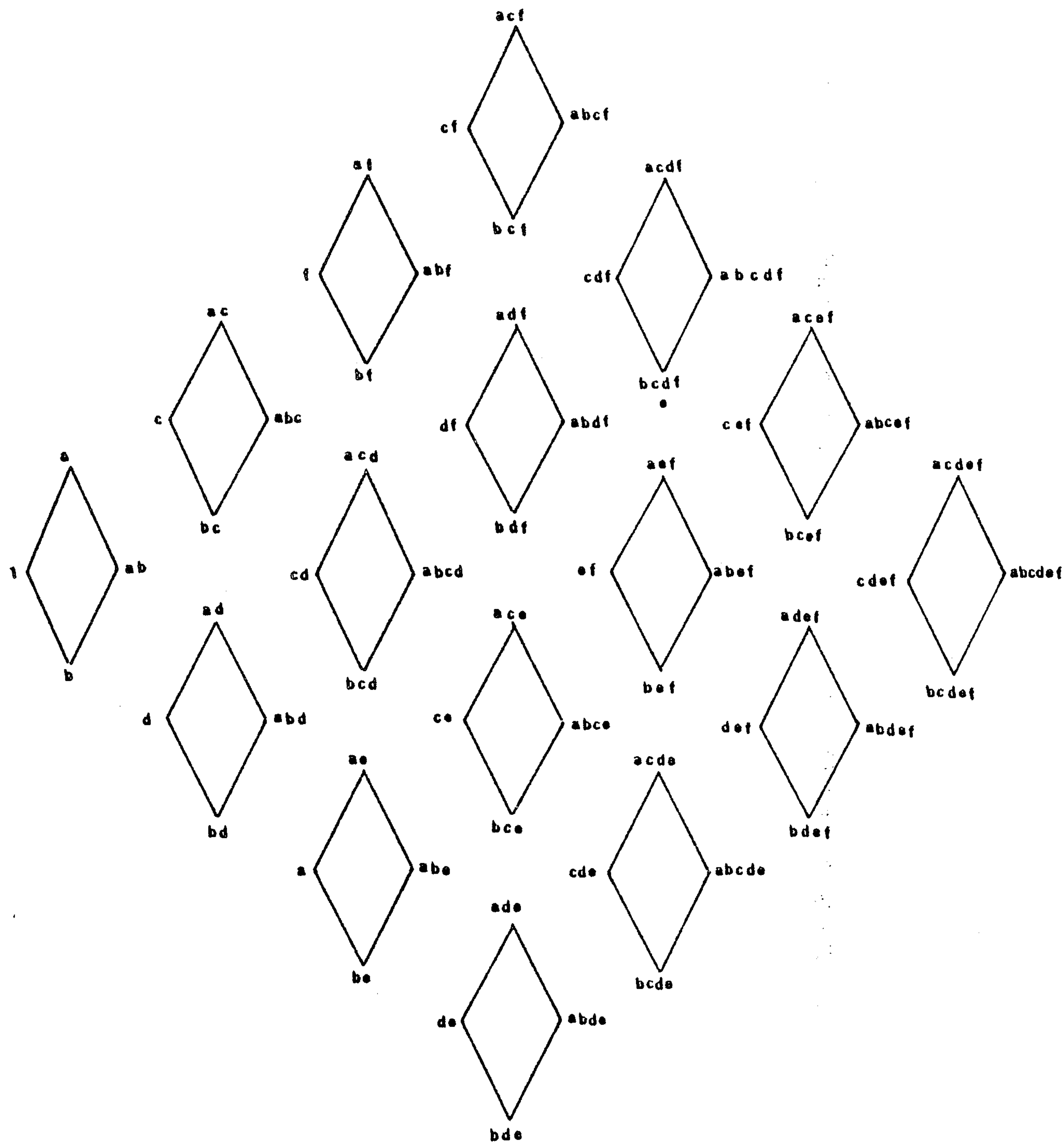

acf
cf
abcf
bcf
af
f
abf
bf
acdf
cdf
abcdf
bcdf
ac
c
abc
bc
adf
df
abdf
bdf
acef
cef
abcef
bcef
a
1
ab
b
acd
cd
abcd
bcd
aef
ef
abef
bef
acdef
cdef
abcdef
bcdef
ad
d
abd
bd
ace
ce
abce
bce
adef
def
abdef
bdef
ae
e
abe
be
acde
cde
abcde
bcde
ade
de
abde
bde

fig 2

1.2 Représentation d'un monôme

Un monôme est représenté par l'ensemble des monômes canoniques qu'il couvre.

Exemple :

Monôme ac'	abc'd	abd
	abc'd'	ab
	ab'c'd	ad
	ab'c'd'	a

Ces points forment un sous-cube dont la dimension est celle du monôme.

Nous nommerons *amont* le point qui comporte le minimum de lettres et point *aval* celui qui comporte le maximum de lettres.

Par exemple, dans le monôme précédent a est le point amont et abd est le point aval.

Nous représenterons le monôme par un vecteur dont l'origine est le point amont et l'extrêmité le point aval. Ici

$$\overrightarrow{a,\ abd}$$

une telle expression représente un monôme si et seulement si toutes les lettres du point amont figurent dans le point aval.

La règle pour retrouver l'écriture habituelle du monôme est la suivante :

- Ecrire les lettres correspondant au point amont sous forme directe.
- Ecrire les lettres ne figurant pas dans le point aval sous forme accentuée.

1.2.1 Condition pour qu'un monôme soit multiple d'un autre

Si le monôme m_2 est multiple du monôme m_1, le point amont et le point aval de m_2 doivent être formés de lettres :

- contenant celles du point amont de m_1
- contenues dans celles du point aval de m_2

Exemple

$\overrightarrow{ad,\ abd}$ est un multiple de $\overrightarrow{a,\ abcd}$

En effet, il s'agit des monômes adc' et a.

1.3 Produit de 2 monômes

Soit les deux monômes :

$$\overrightarrow{x,\ y} \quad \text{et} \quad \overrightarrow{u,\ v}$$

- Pour l'existence du produit il faut que l'aval de chaque vecteur soit plus petit que l'amont de l'autre :

$$x \geqslant v\ , \quad u \geqslant y$$

- le produit de deux vecteurs est

$$\overrightarrow{xu,\ t}$$

où

(1) t = le produit des lettres communes à y et à v.

Démontrons la partie la plus difficile : relation (1).

Soit Y et V respectivement les ensembles des lettres figurant dans y et v. Soit E l'ensemble universel.
Les ensembles des variables non accentuées des trois monômes $\overrightarrow{x,y}$, $\overrightarrow{u,v}$ et $\overrightarrow{xu,t}$ sont :

$$C_E\, Y\ ,\ C_E\, V\ ,\ C\,(Y \cap V)$$

On a :

$$(C_E\, Y) \cup (C_E\, V) = C_E\,(Y \cap V)$$

D'où la relation (1).

Remarque

On peut exprimer la règle ci-dessus de la façon suivante :

. on fait la somme des vecteurs $\overrightarrow{1,x}$, $\overrightarrow{1,u}$. Soit $\overrightarrow{1,m}$ ce vecteur;

. on fait la somme des vecteurs $\overrightarrow{y,\Pi}$ et $\overrightarrow{v,\Pi}$, Π produit de toutes les variables. Soit $\overrightarrow{M,\Pi}$ ce vecteur.

Si $\overrightarrow{m\ M}$ est un vecteur représentatif d'un monôme, c'est le vecteur représentatif du produit, sinon le produit est nul.

1.4 Monômes ma' et ma

Les deux monômes s'écrivent

$\overrightarrow{x,y}$ et $\overrightarrow{xa,ya}$ (a ne figurant pas dans y)

La somme de ces deux monômes est

m c'est-à-dire $\overrightarrow{x,ya}$

C'est cette opération que l'on utilise dans la recherche des monômes premiers à partir des monômes canoniques.

1.5 Produit d'un monôme par un monôme à une variable

Soit u,v le vecteur représentant le monôme m. Soit à représenter les monômes

ma et ma'

1er cas. Le monôme m contient a, a figure dans u et v

$ma = \overrightarrow{u,v}$ $ma' = o$

2ème cas. Le monôme m contient a', a ne figure ni dans u ni dans v

$ma = o$ $ma' = \overrightarrow{u,v}$

3ème cas. Le monôme m ne contient ni a ni a', a figure dans v mais non dans u

$ma = \overrightarrow{au,v}$ $ma' = \overrightarrow{u, \frac{v}{a}}$

Règle : *Pour multiplier par a on s'assure que a figure dans v et on remplace u par au.*
Pour multiplier par a' on s'assure que a ne figure pas dans u et on enlève a de v si cela est possible.

Produit d'un monôme par une somme de lettres directes ou accentuées

Soit à multiplier

$\overrightarrow{ab, abcd}$ par a+b'+c+d'+e+f'

En appliquant la règle ci-dessus on trouve

$\overrightarrow{ab, abcd} + \overrightarrow{abc, abcd} + \overrightarrow{ab, abc} + \overrightarrow{ab, abcd} = \overrightarrow{ab, abcd}$

1.6 Consensus

Commençons par un exemple à 5 variables

$$\begin{array}{lll} ab'c & \text{s'écrit} & \overrightarrow{a\,c\,,\ acde} = \overrightarrow{x,y} \\ dc' & & \overrightarrow{d\ ,\ abde} = \overrightarrow{u,v} \end{array}$$

c est la seule lettre qui figure dans x mais non dans v ou figure dans u mais non dans y.

Le consensus est

$$ab'd \quad \text{qui s'écrit} \quad \overrightarrow{ad\ ,\ a\,c\,de}$$

On réunit les lettres de x et u (à part c)

On prend les lettres communes à y et v, on y adjoint c.

1.6.1 *Consensus entre x'F et xG*

Supposons connus les monômes premiers de F et G. Soit x une nouvelle variable. Les monômes premiers de x'F + xG s'obtiennent en prenant

- ceux de F multipliés par x'
- ceux de G multipliés par x
- les monômes premiers de FG et en enlevant les monômes multiples d'un autre.

Nous avons appris à former le produit. Il est donc possible de construire de tels consensus.

1.7 Exemples de recherche de monômes premiers

Calculer les monômes premiers de la fonction

$$f = a'bc'd' + a'bc'd + a'b'cd' + a'b'c'd + abc'd + ab'cd' + a'b'cd + $$
$$+ abc'd' + a'b'cd' + abc'd$$

A partir des monômes canoniques on cherche les monômes premiers par réunions successives.

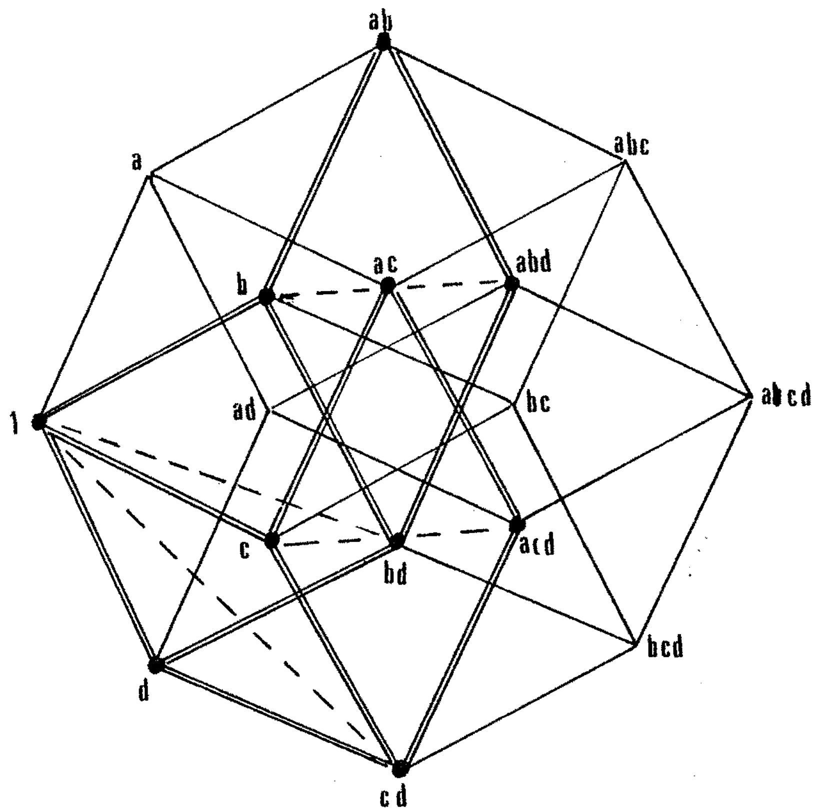


fig 3

Nous avons marqué les monômes canoniques par de gros points. Nous parcourons les points marqués dans un ordre quelconque et cherchons si on peut les joindre à un point comportant une lettre de plus. Nous obtenons ainsi tous les monômes marqué en trait double. Si un point restait isolé (il n'y en a pas ici) il correspondrait à un monôme canonique premier.

Nous reprenons les traits doubles (dans l'ordre de leurs points amont) et cherchons si on peut leur faire correspondre un autre trait double qui en différerait par une même lettre au plus à chaque extrémité, cette lettre étant située plus loin dans l'alphabet que les lettres figurant déjà dans le vecteur étudié. Nous obtenons ainsi les 4 flèches en pointillés.

Si un trait double restait inutilisé il correspond à un monôme premier (il n'y en a pas).

On continue avec les flèches en tirets et l'on n'obtient plus rien de nouveau. On a donc les monômes premiers :

$\overrightarrow{1, bd}$, $\overrightarrow{1, cd}$, $\overrightarrow{c, acd}$, $\overrightarrow{b, abd}$

c'est-à-dire en écriture ordinaire

a'c' , a'b' , cb' , bc'

L'ordre le plus commode semble être celui qui consiste à prendre les points marqués d'après leur position dans le plan.
En commençant, par exemple par la gauche, et en séparant par un trait de crayon que l'on effacera les points déjà traités des autres.

Ce genre de méthode est efficace jusqu'à 4 variables. Au delà il vaut mieux opérer autrement.

1.8 Méthode de suppression de points (ou fonctions auxiliaires)

Soit à calculer les monômes premiers de la fonction $f = \Sigma m_i$ donnée par la somme des monômes. Nous cherchons une fonction auxiliaire $g = \Sigma n_j$ sous forme de somme de monômes, telle que les deux conditions suivantes soient réalisées :

(1) $fg = o$

(2) $f+g$ est une fonction dont les monômes premiers sont faciles à calculer.

Nous obtenons les monômes premiers de f, en faisant le produit des monômes premiers de $(f+g)$ par g'.

Démonstration

a) Nous démontrons d'abord l'égalité suivante :

$f = (f+g)g'$

En effet :

$f = f(g+g') = fg + fg' = fg' = fg' + gg' = (f+g)g'$

Remarquons que la méthode consiste à ajouter des points à f pour passer à une fonction plus simple puis à les supprimer par produit.

b) D'après l'hypothèse (condition (2)) nous avons les monômes premiers de la fonction $(f+g)$. Comme g' est le produit des monômes, alors d'après le théorème des monômes premiers [16] on obtient les monômes premiers de f en faisant le produit de $(f+g)$ exprimée par ses monômes premiers par la fonction g' exprimée par le produit des monaux.

1.8.1 *Mise en oeuvre sous forme vectorielle*

Pour enlever le point représenté par def il faut multiplier par

$a+b+c+d'+e'+f'$

Pour multiplier $m = \overrightarrow{u,v}$ par cette somme on s'assure que a,b,c (lettres manquantes au point) figurent dans v et on remplace u par ua, ub, uc. On s'assure que def (lettres présentes au point) ne figurent pas dans u et on enlève d, e, f de v si possible.

1.9 Méthode d'adjonctions successives de variables

Toute expression booléenne f peut être mise sous la forme :

$$f = xf_1 + x'f_o$$

où x est une variable quelconque de f, et f_1 et f_o sont des expressions indépendantes de x.

Théorème : Soit $E_1 = \{m_1, m_2, \ldots, m_r\}$ et $E_o = \{p_1, p_2, \ldots, p_s\}$ respectivement les deux ensembles des monômes premiers de f_1 et f_o. On obtient les monômes premiers de f, en faisant le produit des deux facteurs suivants et éventuellement la suppression des multiples.

$$(m_1+m_2+\ldots +m_r+x')(p_1+p_2+\ldots +p_s+x)$$

L'expression ci-dessus s'écrit :

$$(f_1+x')(f_o+x) = f_1x+f_ox'+f_1\ f_2 = f_1x+f_ox'$$

La propriété résulte immédiatement du théorème sur les monômes premiers d'un produit [16].

Exemple 1

$$f = \overrightarrow{ac, abc} + \overrightarrow{b, ba} + \overrightarrow{abd, abcd} + \overrightarrow{c, ac} + \overrightarrow{d, bd} + 1 + cd$$

On peut écrire

les monômes contenant a

$$\overrightarrow{ac, abc} + \overrightarrow{abd, abcd}$$

ceux contenant a'

$$\overrightarrow{d, bd} + 1 + cd$$

ceux ne contenant ni a ni a'

$$\overrightarrow{b, ba} + \overrightarrow{c, ac}$$

On a

$$f = af_1 + a'f_o$$

où

$$f_1 = \overrightarrow{c,abc} + \overrightarrow{bd,abcd} + \overrightarrow{b,ab} + \cancel{\overrightarrow{c,ac}} \text{ (multiple)}$$

$$f_o = \overrightarrow{d,abd} + \overrightarrow{1,a} + \overrightarrow{cd,acd} + \overrightarrow{b,ab} + \overrightarrow{c,ac}$$

Les monômes premiers de f_1 sont :

$\overrightarrow{b,abcd}$, $\overrightarrow{c,abc}$

f_o admet les monômes premiers :

$\overrightarrow{1,abd}$, $\overrightarrow{1,acd}$

Les monômes premiers de f_of_1 sont

$\overrightarrow{c,ac}$, $\overrightarrow{b,abd}$

D'après 1.6.1 les monômes premiers de f sont

$$a(\overrightarrow{b,abcd} + \overrightarrow{c,abc}) + a'(\overrightarrow{1,abd} + \overrightarrow{1,acd}) + \overrightarrow{c,ac} + \overrightarrow{b,abd}$$
$$= \overrightarrow{ab,abcd} + \overrightarrow{ac,abc} + \overrightarrow{1,bc} + \overrightarrow{1,bd} + \overrightarrow{c,ac} + \overrightarrow{b,abd}$$

On peut dire accessoirement que cette méthode s'apparente à l'écriture lexicographique.

Exemple 2

Soit à calculer les monômes premiers de la fonction F représentée sur la figure 4.

On subdivise la représentation en 4 secteurs :

bas B, gauche G, haut H, droit D.

Les monômes premiers des sous-fonctions correspondant à ces secteurs sont :

$$B(a,b,c,d) = \overrightarrow{c,abc} + \overrightarrow{d,abd} + \overrightarrow{bc,abcd} + \overrightarrow{bd,abcd}$$
$$G(a,b,c,d) = \overrightarrow{bc,abc} + \overrightarrow{cd,acd}$$
$$H(a,b,c,d) = \overrightarrow{cd,abcd} + \overrightarrow{ad,abcd}$$
$$D(a,b,c,d) = \overrightarrow{cd,abcd}$$

D'après 1.6.1, les monômes premiers de la sous-fonction correspondant à la réunion des deux secteurs B et G sont les monômes premiers de la fonction

$$F_o(a,b,c,d,e) = e'G + eB + GB$$

après les suppressions des multiples

$$F_o = e'\,\overrightarrow{bc,abcd} + e'\,\overrightarrow{cd,acd} + e\,\overrightarrow{c,abe} + e\,\overrightarrow{d,abd} + e\,\overrightarrow{bc,abcd} +$$
$$e\,\overrightarrow{bd,abcd} + \overrightarrow{bc,abc} =$$
$$= \overrightarrow{cd,acd} + \overrightarrow{ce,abce} + \overrightarrow{de,abde} + \overrightarrow{bde,abcde} + \overrightarrow{bc,abce}$$

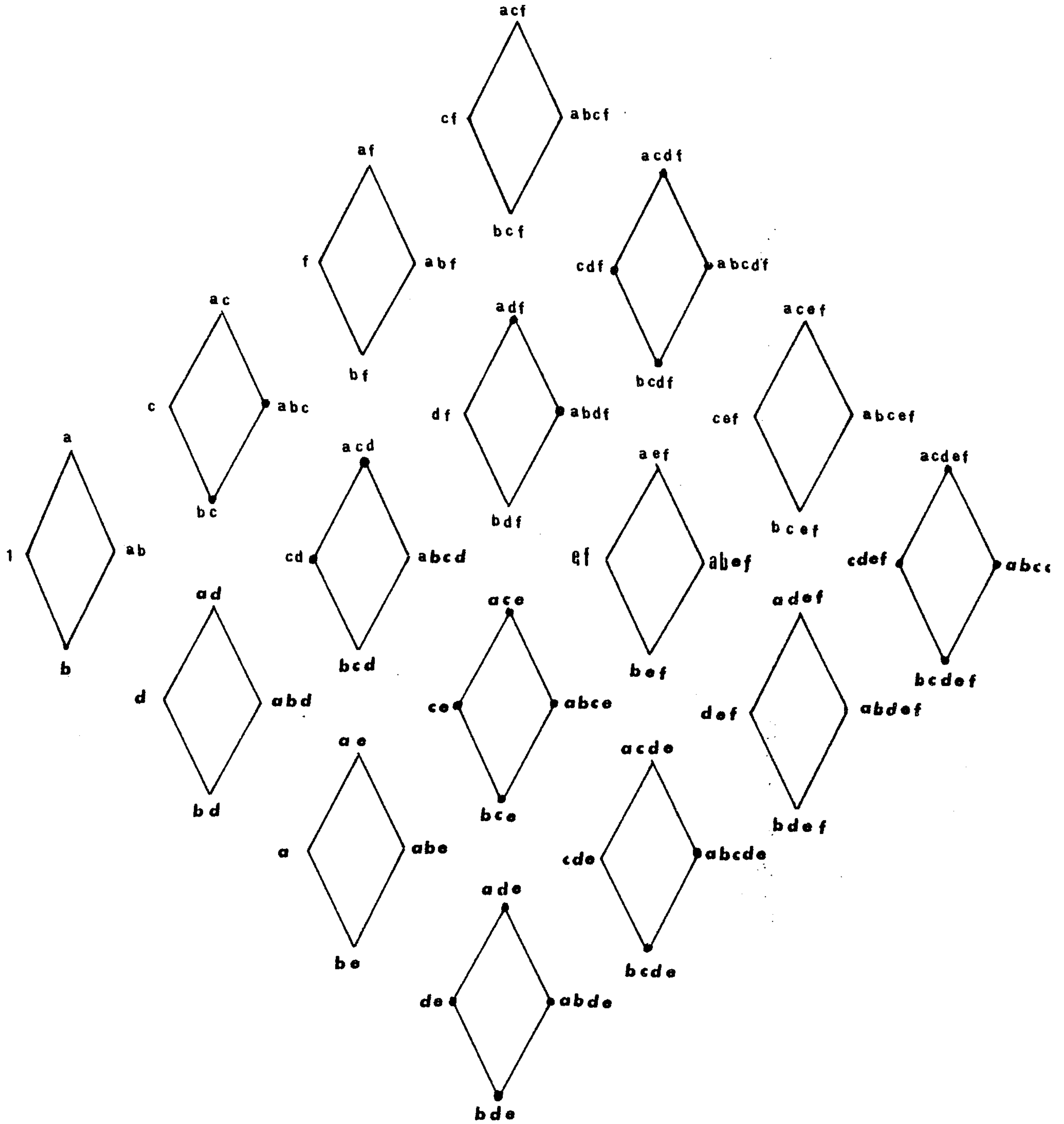

acf
cf
abcf
bcf
af
f
abf
bf
acdf
cdf
abcdf
bcdf
ac
c
abc
bc
adf
df
abdf
bdf
acef
cef
abcef
bcef
a
1
ab
b
acd
cd
abcd
bcd
aef
ef
abef
bef
acdef
cdef
bcdef
ad
d
abd
bd
ace
ce
abce
bce
adef
def
abdef
bdef
ae
abe
be
acde
cde
abcde
bcde
ade
de
abde
bde

Figure 4.

Les monômes premiers de la sous-fonction correspondant à la réunion des deux secteurs H et D sont

$$F_1(a,b,c,d,e) = e'H + eD + HD = e'\,\overrightarrow{cd,abcd} + e'\,\overrightarrow{ad,abcd} + $$
$$+ e\,\overrightarrow{cd,abcd} + \overrightarrow{cd,abcd}$$
$$= \overrightarrow{ad,abcd} + \overrightarrow{cd,abcde}$$

Les monômes premiers de la fonction f :

$$F = f'F_o + fF_1 + F_oF_1 = f'(\overrightarrow{cd,acd} + \overrightarrow{ce,abce} + \overrightarrow{de,abde} + \overrightarrow{bde,abcde}$$
$$+ \overrightarrow{bc,abce}) + f(\overrightarrow{ad,abcd} + \overrightarrow{cd,abcde}) + \overrightarrow{acd,\ acdf} + \overrightarrow{cd,acdf} +$$
$$+ \overrightarrow{bcde,abcdef}$$
$$= \overrightarrow{cd,acd} + \overrightarrow{ce,abce} + \overrightarrow{de,abde} + \overrightarrow{bde,abcde} + \overrightarrow{bc,abce} + \overrightarrow{adf,abcdf}$$
$$+ \overrightarrow{cdf,abcdef} + \overrightarrow{acd,acdf} + \overrightarrow{cd,acdf} + \overrightarrow{bcde,abcdef}$$

Le monôme $\overrightarrow{cd,acdf}$ absorbe le monôme $\overrightarrow{cd,acd}$; on a 9 monômes premiers.

1.10 Cas particuliers de la représentation générale précédente

1.10.1 Cas de Mc CLUSKEY

Considérons le cas particulier de la représentation vectorielle où les points a,b,c,... sont alignés (Figure 5).

Les points à i lettres non accentuées ($2 \leq i \leq n$) sont situés sur la droite Δ_i, homothétique dans le rapport i de la droite Δ_1 qui passe par les points à une seule lettre non accentuée (immédiat)

Les points sont partitionnés en (n+1) classes $S_n^{i,(n-i)}(X)$, $o \leq i \leq n$

On retrouve une situation analogue à celle de la méthode de Mc CLUSKEY où l'on partitionne les monômes canoniques suivant le nombre de lettres non accentuées et on cherche des réductions entre les monômes de deux groupes consécutifs.

Exemple

Calculer les monômes premiers de la fonction

abcd + a'b'cd + abcd' + a'bc'd + ab'cd + a'b'c'd' + ab'c'd + a'b'cd' + a'b'c'd + a'bcd + a'b'c'd

Dans la première étape on fait la réduction entre deux monômes de deux niveaux consécutifs (Figure 5).

On obtient les vecteurs suivants :

$\overrightarrow{1,c}$, $\overrightarrow{1,d}$, $\overrightarrow{d,cd}$, $\overrightarrow{c,cd}$,

$\overrightarrow{d,bd}$, $\overrightarrow{bd,bcd}$, $\overrightarrow{cd,bcd}$,

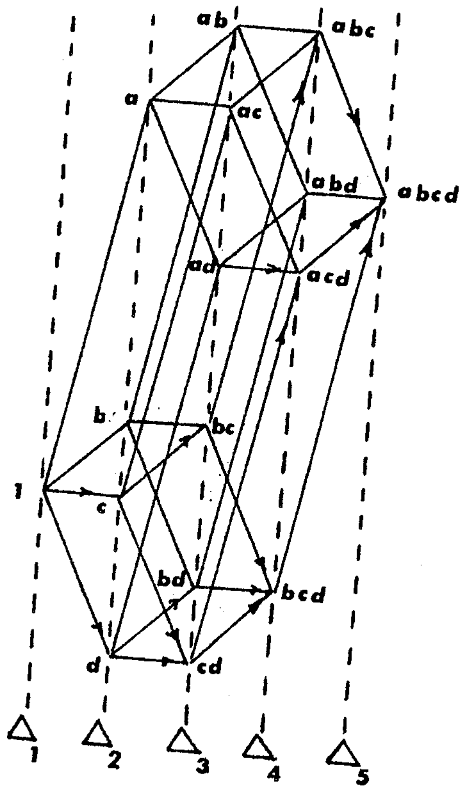
$\overrightarrow{c,bc}$, $\overrightarrow{bc,bcd}$, $\overrightarrow{d,ad}$,

$\overrightarrow{cd,acd}$, $\overrightarrow{ad,acd}$, $\overrightarrow{acd,abcd}$

$\overrightarrow{bc,abc}$, $\overrightarrow{abc,abcd}$

En deuxième étape on fait la réduction entre les vecteurs en utilisant la règle 1.4.

fig 5



On obtient les vecteurs ci-dessous : (figure 6)

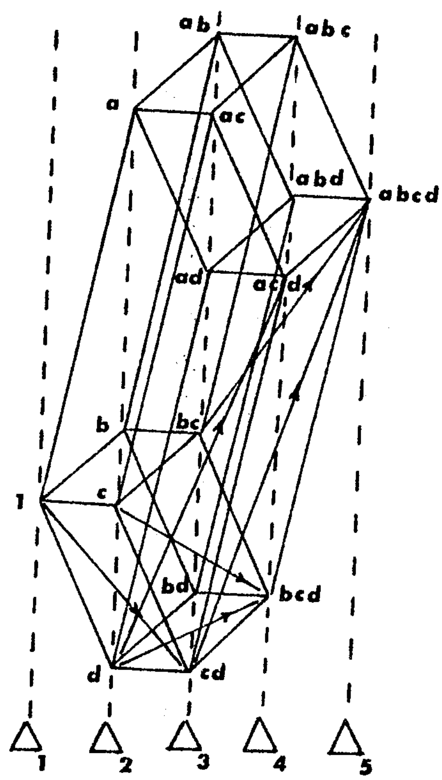
$\overrightarrow{1,cd}$, $\overrightarrow{d,bcd}$

$\overrightarrow{c,bcd}$, $\overrightarrow{d,acd}$, $\overrightarrow{cd,abcd}$, $\overrightarrow{bc,abc}$

à ces vecteurs correspondent les monômes premiers suivants :

a'b', da', ca', db', cd, bc

fig 6



Quels sont les avantages et inconvénient de ce cas particulier.

- Il est plus facile de retrouver les points en suivant les droites successives qui les contiennent. Cela est valable jusqu'à n=4.

  Pour n=6 on aura respectivement

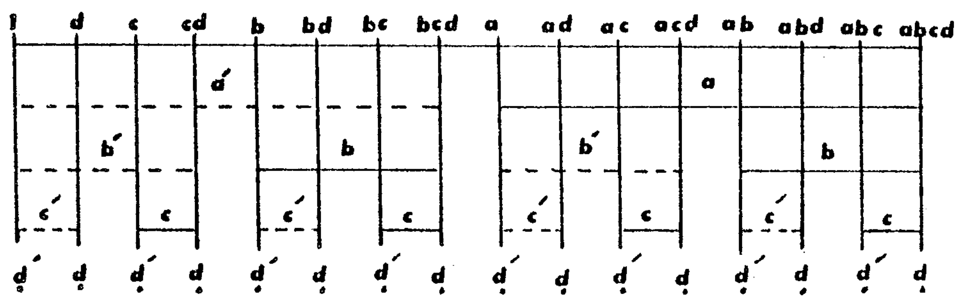
  1 6 15 20 15 6 1 points qui se représenteront dans un ordre assez complexe et la méthode sera difficile à utiliser.

1.10.2 *Représentation vectorielle à une dimension*

Dans la représentation vectorielle on peut prendre les divers vecteurs co-linéaires et de longueur..., 8,4,2,1.

Ce n'est naturellement plus une projection du cube sur le plan mais c'est une projection du cube sur la droite.

Dans la représentation vectorielle à une dimension suivante on a pris n=4.

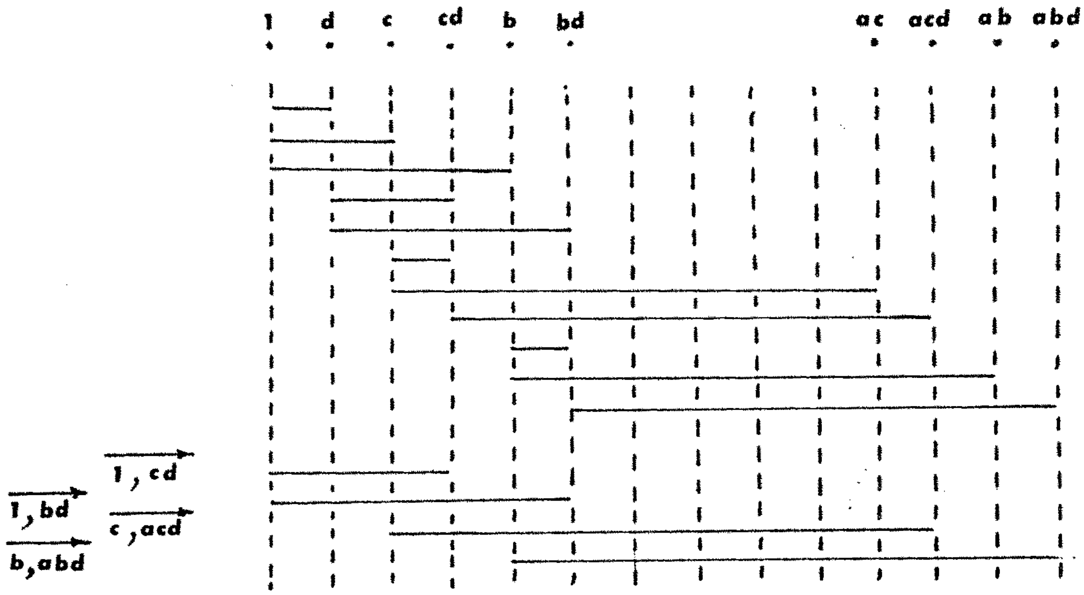


Recherche des monômes premiers

Etant donné que la représentation de la fonction n'utilise qu'une droite du plan on rend la figure plus claire en décalant vers le bas les flèches représentatives des monômes.

Exemple

Reprenons la fonction du n° 1.7



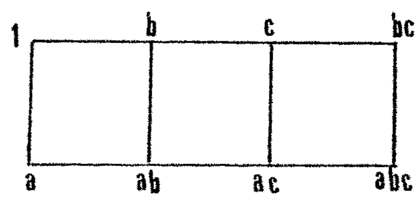
Remarque

Cette écriture à une seule dimension est très étroitement apparentée à l'écriture arborescente.

1.10.3 *Tableau de Karnaugh*

Rien ne nous empêche de choisir les vecteurs représentant les diverses variables suivant 2 directions (cela n'en est pas moins une projection du cube). Par exemple pour n=3

fig 7



Il aurait été plus naturel de présenter ceci avant la représentation à 1 dimension mais en fait cela revient à partager les variables en deux paquets pour chacun desquels on prend une représentation à une dimension (en particulier translations de 1,2,4,... et petites cases ou bien de points).

Le tableau de Karnaugh est de toutes les représentations géométriques de fonctions booléennes celle qui de loin est la plus utilisée.

On remarquera que la représentation générale donnée pour n=6 utilise deux familles de vecteurs, les vecteurs d'une même famille étant presque colinéaires.

Quels sont les avantages et inconvénients du tableau de Karnaugh ?

- Il n'exige pas de dessin préalable compliqué, tout le monde sait dessiner un tableau.

1.10.4 *Tableau de Karnaugh avec symétries*

En fait l'idée initiale du tableau de Karnaugh a été combinée avec une autre (qui à notre avis la contamine), celle de réaliser des symétries pour faciliter des rapprochements de monômes ne différant que par une variable.

Au lieu de

ab, ab', a'b, a'b'

on écrit

ab   ab'   a'b'   a'b

Des 4 monômes a b a' b' 3 correspondent à deux cases voisines. Seul b fait exception.

Le tableau de Karnaugh avec symétries s'apparente visiblement aux codes réflechis.

1.11 Représentation symétrique

Considérons l'ensemble E de n vecteurs $\vec{a}$, $\vec{b}$, $\vec{c}$,... du plan issus d'un même point "1" et l'ensemble E' de n vecteurs $\vec{a}'$, $\vec{b}'$, $\vec{c}'$,... obtenus à partir des vecteurs de E, par symétrie par rapport au point "1"(figure 8).

Soit $\vec{x} \in$ E et $\vec{y} \in$ E' tels que $x\ y \neq o$. On construit sur $\vec{x}$ et $\vec{y}$ un parallélogramme et on attribue à l'extrêmité du vecteur $\vec{x}+\vec{y}$ le produit xy.

Au vecteur $\vec{a} + \vec{b} + \vec{c}$ on fait correspondre abc

Au vecteur $\vec{a}' + \vec{b}' + \vec{c}$ on fait correspondre a'b'c etc.

On obtient la figure suivante.

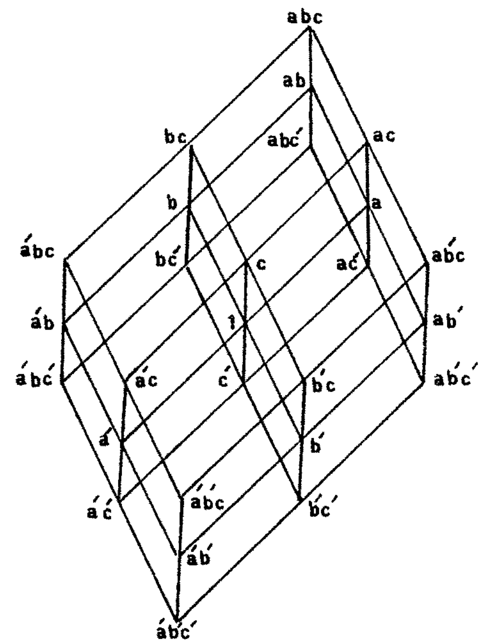


fig 8

Sur la figure 9 on a la représentation symétrique pour n=4.
On voit immédiatement qu'une telle représentation n'est guère utilisable.

Exemple pour le calcul des monômes premiers

Soit à calculer les monômes premiers de la fonction :

f = abcd + ab'cd + ab'c'd + a'b'c'd + a'b'cd + abcd' + ab'cd' +
+ ab'c'd' + a'c'c'd' + a'bc'd'

On indique sur la figure 9 l'ensemble E des points correspondant aux monômes figurant dans la fonction f (par des gros points par exemple). On cherche les milieux de chacun des couples de points de E qui sont joints par un trait rectiligne. Les points milieux constituent un ensenbme F. On cherche dans l'ensemble F, les points milieux de chacun des couples depoints qui sont joints par un trait rectiligne et ainsi de suite.

Les deux points abcd et a'bcd ont pour milieu le point acd, les deux points abcd' et ab'cd' ont le milieu acd'; les deux points acd et acd' ont pour milieu le point

ac

qui est monôme premier.

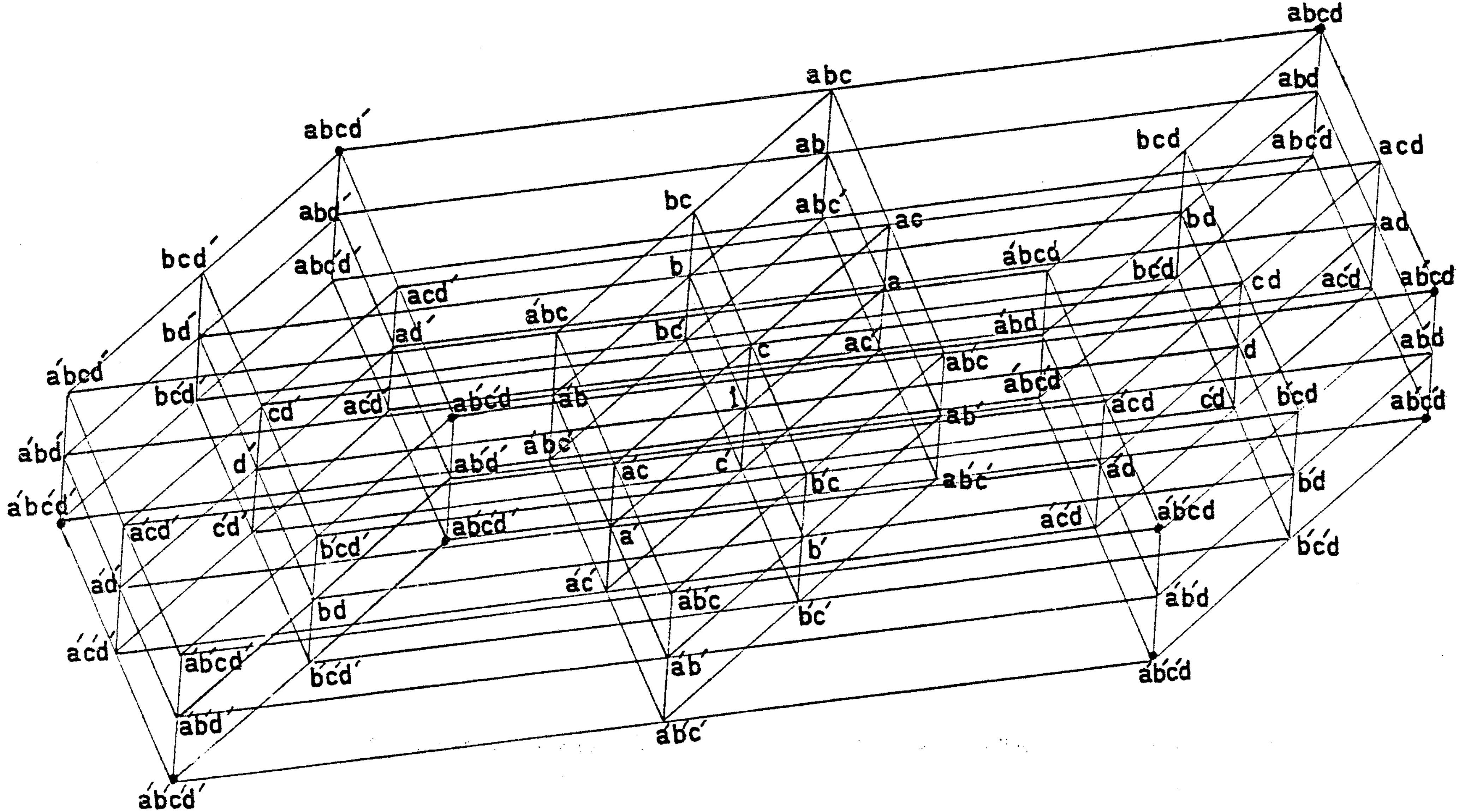


fig 9

De la même façon on a :

$ab'cd + ab'c'd + a'b'c'd + a'b'cd = b'd$

$ab'cd + ab'c'd + ab'c'd' + ab'cd' = ab'$

$ab'c'd + a'b'c'd + a'b'c'd' + ab'c'd' = b'c'$

$a\,b'c'd' + a'b'c'd' = a'c'd'$

On a les mêmes monômes premiers :

$ac,\ b'd,\ ab',\ b'c',\ a'c'd'$

Remarque

On peut obtenir la représentation symétrique (figure 8) à partir de la représentation vectorielle plane (figure 1). Sur la représentation (1), on indique d'abord chaque point par toutes les lettres (accentuées ou non). On cherche les points milieux de tous les couples de points qui sont joints. On joint tous les couples des points milieux (x,y) tel que le vecteur $\vec{xy}$ soit parallèle à un des vecteurs de l'ensemble $E = \{a,b,c,..\}$. On attribue au milieu de deux points le consensus m des deux monômes xm et x'm correspondant à ces deux points.

1.12 Nous allons appliquer les théories précédentes à la résolution d'une question qui nous intéressera dans la 2ème partie

1.12.1 *Construction d'une fonction qui possède exactement n bases premières de même modèle*

Considérons sur la représentation vectorielle à $(n+1)$ variables (sur la figure 10 on a $n=3$) un point quelconque, par exemple le point abcd. De ce point, il passe un ensemble E de $(n+1)$ arêtes.
Considérons une arête de cet ensemble, par exemple l'arête x qui a pour extrêmité les deux point abc et abcd et l'ensemble $F = E - \{x\}$.

Soit G l'ensemble de n arête de la représentation qui sont parallèles à l'arête x et passant par les extrêmités des arêtes de F et soit f l'expression booléenne correspondant à G.

L'expression booléenne correspondant à $F \cup G$ est

(1) $f+m_i \quad 1 \leqslant i \leqslant n$

où m_i est le monôme correspondant à une arête de F.

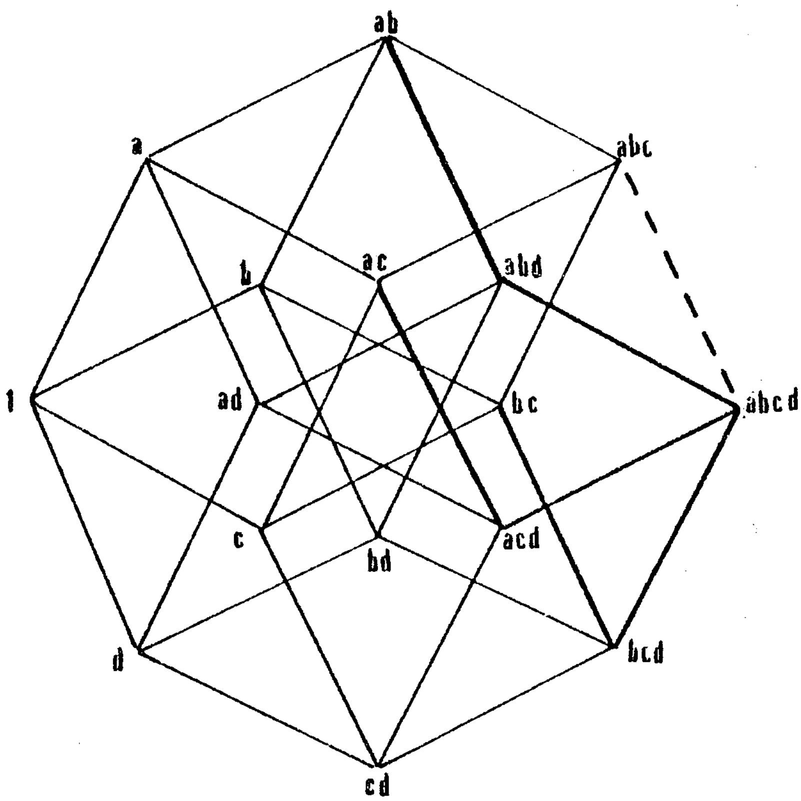


Figure 10.

Les extrémités des arêtes de G n'étant pas jointes, la fonction f n'admet qu'une seule base.

Le monôme m ne se réduit avec aucun monôme de f, alors la fonction correspondant à F $\cup$ G admet n bases premières.

Les monômes correspondants aux arêtes de F ont une variable commune d qui ne figure dans f(variable monoforme).

Les bases premières de la fonction sont de la forme

$$S_n^{n-1,1}(X) + d \prod_{i \neq j} x_i, \; i, j \in \{1,2,\dots, n\}$$

Exemple

Pour n=4 on a : abc' + ab'c + a'bc + abcd

1.12.2 *Construction d'une fonction de (n+2) variables qui possède exactement n^2 bases premières de même modèle*

Considérons la représentation vectorielle à (n+2) variables (sur la figure 11 on a n=3) et divisons la en deux représentations à (n+1) dimensions I et II.

I comporte le secteur gauche et haut.

II comporte le secteur bas et droit.

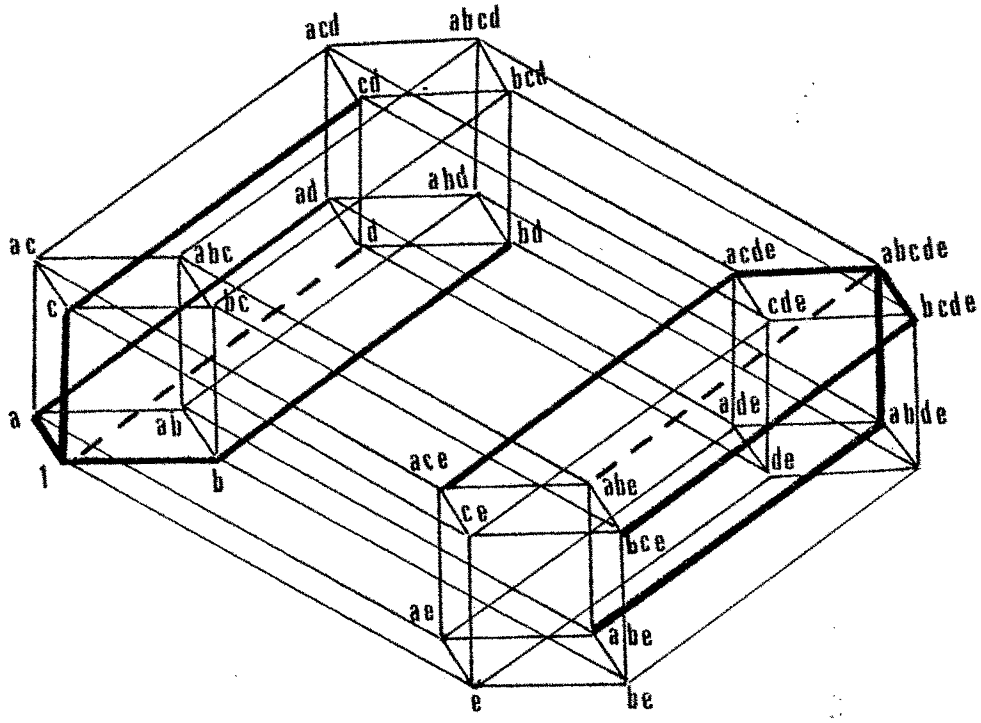


Figure 11.

Sur la représentation (I) nous construisons d'après 1.12.1 une figure F qui admet exactement n bases premières.

Soit G la symétrique de F dans la représentation à (n+2) variables.

L'expression booléenne correspondante à la figure F ∪ G admet exactement n^2 bases premières.

DEUXIEME PARTIE

MODELES DE BASES ET SPECTRES DE FONCTIONS

CHAPITRE II

MODELES DE BASES

MODELES DE BASES

Dans ce chapitre nous définissons la notion de modèle, nous donnons qualques théorèmes d'existence et nous abordons l'étude de quelques cas simples. Il s'agira toujours de fonctions booléennes complètes.

2.1 Modèle d'une base première

Nous nommerons ainsi le couple ordonné (m,l) où m et l représentent respectivement le nombre des monômes premiers et le nombre des lettres de la base.

Les fonctions "0" et "1" sont exceptionnelles. 0 et 1 sont-ils des lettres ? -Non. On rejette ces deux fonctions.

Modèles des fonctions non-constantes

Les (m,l) possibles pour des fonctions non constantes vérifient les inégalités.

(1) $l \geq m \geq 1$

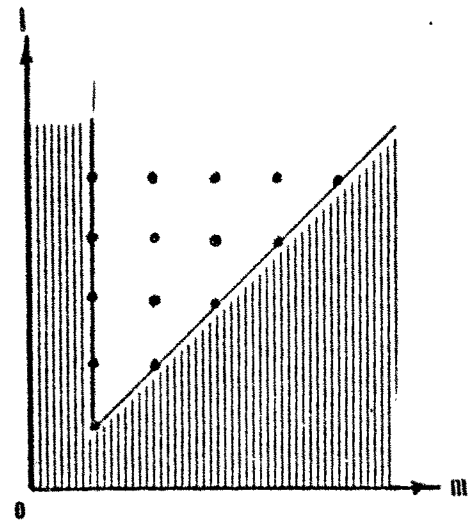
Inversement il est clair qu'on peut toujours trouver des fonctions ayant une base de modèle (m,l) lorsque m est l vérifient les conditions (1).

Exemple

$x_1 + x_2 + \dots + x_{m-1} + x_m \dots x_l$

Il sera commode de représenter le modèle d'une base par le point de coordonnée (m,l) dans le plan.

fig 1



La figure (1) représente les positions possibles de modèle d'une base.

2.2 Fonctions à une seule base

a) D'après l'exemple précédent, les conditions (1) sont nécessaires et suffisantes pour l'existence de fonctions à une seule base.

b) Y-a-t'il des (m,l) pour lesquels on peut affirmer que toute fonction ayant une base de ce modèle a une seule base.
Cela est vrai pour :
m = 1, la fonction se réduit à un monôme.
m = 2, si les deux monômes n'ont pas de consensus, la propriété est évidente, s'ils en ont un, le consensus ne peut couvrir aucun des monômes (sinon celui-ci ne serait pas premier). Il en résulte que les monômes sont obligatoire et la base est unique.
l = m, les monômes ont chacun une seule lettre. Toutes les lettres sont différentes.
l = m+1, tous les monômes sauf un ont une seule lettre. Cette lettre ne figure nulle part ailleurs. La fonction est donc monotone.
l = m+2, tous les monômes sauf un ou deux ont une seule lettre. En supprimant ces monômes à une lettre on ne change pas le nombre de bases. On est alors revenu aux cas m=1, m=2.

2.3 Fonction à plusieurs bases

Les fonctions à plusieurs bases peuvent avoir un ou plusieurs modèles. Le premier exemple ci-dessous représente une fonction à un seul modèle, le second exemple une fonction à deux modèles.

Exemple 1

La fonction représentée sur le cube (figure 2) a deux bases premières à un seul modèle.

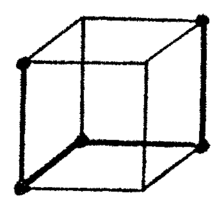
La fonction admet les deux bases premières suivantes :

xy + x'y' + xz'

xy + x'y' + y'z'

Les deux bases ont pout modèle (3,6).

fig 2



Exemple 2

Ceinture du cube (figure 3).

La fonction admet les 5 bases premières suivantes :

(1) $xy' + yz' + zx'$

(2) $x'y + y'z + z'x$

(3) $xy' + x'y + yz' + y'z$

(4) $xy' + x'y + xz' + x'z$

(5) $xz' + x'z + yz' + y'z$

Les bases (1) et (2) ont pour modèle (3,6); les bases (3), (4) et (5) ont pour modèle (4,8).

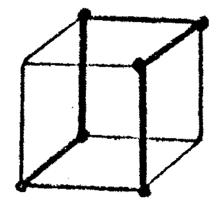


Figure 3.

2.3.1 *Théorème*

Une condition nécessaire et suffisante pour qu'il existe une fonction booléenne à plusieurs bases premières dont l'une de modèle (m,l) est :

(2) $l - 3 \geq m \geq 3$

Démonstration

Les cas qui vérifient (1) et non (2) sont $m=1$, ou 2 ou ($l=m$, $m+1$, ou $m+2$) que nous avons étudiés plus haut. Nous avons constaté qu'ils ne donnent que des fonctions à une seule base.

La condition est suffisante.

a) Remarquons d'abord que si la propriété est vraie pour (m,l) elle l'est encore pour $(m+1, l+1)$ et $(m, l+\rho m)$ (on peut multiplier tous les monômes par ρ variables différentes des variables précédentes).

b) Il existe des fonctions à plusieurs bases de modèles :

(1) $m = 3$, $l = 6$

(2) $m = 3$, $l = 7$

(3) $m = 3$, $l = 8$

Pour le cas (1) on peut citer la ceinture du cube.

Pour les cas (2) et (3) on peut citer la fonction suivante :

$abd + a'c + b'c' + bcd + ac'd + a'b'$

qui admet deux bases premières à savoir :

(1) $a'c + b'c' + abd$

(2) $a'c + b'c' + bcd + ac'd$

La première base a le modèle (3,7), l'autre a pour modèle (4,10).
En dédoublant d en d_1 d_2 on obtient une base première de modèle (3,8), l'autre a pour modèle (4,12).
Un couple (m,l) est donné, avec $l - 3 \geqslant m \geqslant 3$. Construisons une fonction à plusieurs bases premières de modèle (m,l).

On prend p, a et k tel que :

$p = m-3$

$l-m+3 = a+3\,k$

où k est un entier $\geqslant 0$ et $a \in \{6,7,8\}$.
Ensuite on construit d'après (b) une fonction dont le modèle d'une de ses bases première est (3,a).
On multiplie les monômes de cette fonction par k variables différentes des variables précédentes et on ajoute p monômes à une seule lettre.

2.3.2 *Modèle minimal*

Si parmi les modèles de base (m_i, l), d'une fonction il en existe un (m_1, l_1) tel que

$$\forall i \quad m_1 \leqslant m_i \Rightarrow l_1 \leqslant l_i$$

Ce modèle est dit modèle minimal, il est unique.
En fait, le résultat précédent est plus précis que l'énoncé que nous en avons donné.
En effet, le couple sur lequel nous avons travaillé est toujours minimal.
De plus, les solutions proposées ont des particularités qui nous permettent de dire que (2.3.1) caractérise les couples minimaux (m,l) pour lesquels il existe des fonctions ayant :

- des bases de modèles différents,
- des bases d'exactement deux modèles différents,
- des bases d'exactement deux modèles différents avec des nombres de monômes différents d'une unité.

2.4 Fonction ayant au moins un modèle avec m=3

Nous avons rencontré de telles fonctions comme exemples dans les paragraphes précédents. Nous avons toujours trouvé des bases à 3 ou 4 monômes. On peut essayer de voir si cela est général.

Soient m_1, m_2 et m_3 les trois monômes premiers. Deux de ces monômes peuvent avoir entre eux :

- ou un consensus
- ou une intersection
- ou ni l'un ni l'autre.

Si un monôme n'a ni intersection ni consensus avec les 2 autres, la fonction se décompose en un monôme et une fonction à deux monômes. Elle a donc une seule base. Lorsqu'il n'y a aucun consensus il y a aussi une seule base.

1) Nous supposerons d'abord qu'il n'existe pas de consensus $C(m_1,m_2,m_3)$

1er cas. On a 3 consensus $C(m_1,m_2)$, $C(m_2,m_3)$, $C(m_3,m_1)$.

Les monômes de départ n'ayant pas d'intersection, m_1 ne peut être couvert que par m_1 ou $C(m_1,m_2).\ C(m_2,m_3)$.

De même pour les autres. Pour former toutes les couvertures possibles, il faut développer.

$(m_1 + C(m_1,m_2).\ C(m_1,m_3)).(m_2 + C(m_2,m_1)\ C(m_2,m_3)).$

$(m_3 + C(m_3,m_1)\ C(m_3,m_2))$

ce qui donne

$m_1 . m_2 . m_3$

$m_1 . m_2 . C(m_1,m_3).\ C(m_2,m_3)$ et les permutations

$m_1 . C(m_1,m_2).\ C(m_1,m_3).\ C(m_2,m_3)$

$C(m_1,m_2).\ C(m_1,m_3).\ C(m_2,m_3)$

c'est-à-dire toujours 3 ou 4 monômes.

2ème cas. On a deux consensus $C(m_1,m_2)$ et $C(m_2,m_3)$, on a 5 monômes. Le seul moyen d'en prendre plus de 4 est de les prendre tous, mais

$m_1,m_2,m_3,\ C(m_1,m_2),\ C(m_2,m_3)$

n'est pas une base première puisque m_1,m_2,m_3 en est une.

3ème cas. On a un seul consensus $C(m_1,m_2)$

On a 4 monômes en tout.

2) Supposons maintenant l'existence du consensus $C(m_1,m_2,m_3)$.
Cela n'est possible que dans deux cas.

1er cas :

$m_1 = aX$, $m_2 = a'bY$, $m_3 = a'b'Z$

on a

$m_4 = C(m_1,m_2) = bXY$, $m_5 = C(m_1,m_3) = b'XZ$,

$m_6 = C(m_2,m_3) = a'YZ$, $m_7 = C(m_1,m_2,m_3) = XYZ$

De l'étude de consensus on déduit que m_1,m_2,m_3 est la seule base.

2ème cas.

$m_1 = aX$, $m_2 = bY$, $m_3 = a'b'Z$

on a :

$m_4 = C(m_1,m_3) = b'XZ$, $m_5 = C(m_2,m_3) = a'YZ$

$m_6 = C(m_1,\ C(m_2,m_3)) = XYZ = C(m_1,m_2,m_3)$.

L'étude des consensus montre que m_1,m_2,m_3 est la seule base.
Il serait possible de pousser plus loin cette étude et d'énumérer tous les types de fonctions ayant une base à 3 monômes, mais nous en resterons là.

2.5 Fonctions ayant exactement deux bases premières

Soit f une fonction ayant exactement deux bases premières. Nous écrivons les deux bases sous la forme :

$$\Sigma m_i + \Sigma n_j$$

$$\Sigma m_i + \Sigma p_k$$

2.5.1 *Proposition*

On a : $\forall j, k \quad n_j \cap p_k \neq \phi$

En effet, si n_j et p_k ont une intersection vide on peut remplacer n_j dans la première base par d'autres monômes premiers couvrant ses divers points sans faire appel à p_k, on a ainsi une troisième base première (contrairement à l'hypothèse).

2.5.2 *Existence de monômes premiers obligatoires dans les fonctions ayant exactement deux bases premières*

Considérons un certain monôme n_i. On peut l'obtenir comme consensus de certains m et p.

On peut alors former une base avec les n autres que n_i
les m
les p intervenant dans le consensus

qui donne n_i. Cette base n'est sans doute pas première, mais elle doit contenir une base première qui ne peut être celle des n, c'est donc celle des p. Alors le consensus qui donne n_i doit faire intervenir tous les p.

Supposons qu'il n'y ait pas de m, alors il n'y a qu'un seul consensus possible, donc un seul n. La fonction se réduit à un monôme et n'a donc pas deux bases.

Supposons qu'il y ait un seul m. Il y a alors 2 consensus possibles, celui où figure m et celui où il ne figure pas, donc 2 monômes n au plus (et de même deux monômes p au plus).

Examinons les divers cas possibles.

1er cas.

On a un n et un p.

$n = C(m,p)$, $p = C(m,n)$

Ce cas est impossible car n et $C(m,n)$ ne peuvent avoir de consensus.

2ème cas.

On a un n et deux p.

Il n'y a qu'un consensus avec n, on ne peut donc avoir deux p.

3ème cas.

On a deux n et deux p.

$p_1 = C(m,n_1,n_2)$, $p_2 = C(n_1,n_2)$
$n_1 = C(m,p_1,p_2)$, $n_2 = C(p_1,p_2)$

Le consensus $C(n_1,n_2)$ est pris par rapport à une variable a et $C(p_1,p_2)$ par rapport à une autre variable b.

On peut supposer

$$\begin{array}{l|ll} n_1 & a & b' \\ x_2 & a' & \\ p_1 & b & \\ p_2 & b' & \end{array}$$

mais p_2 contenant b', n_1 ou n_2 doit le contenir. Ce ne peut être n_2 donc c'est n_1. Mais il y a impossibilité.

car

$$n_1 = (m, p_1, p_2).$$

La lettre b figurant sous deux formes dans p_1 et p_2 ne peut figurer dans le consensus.

En conséquence, une fonction ayant exactement deux bases a au moins deux monômes premiers obligatoires.

2.5.3 *Construction de fonctions ayant exactement deux bases premières ne différant que par un monôme*

Soit f une fonction ayant plusieurs bases premières avec la propriété suivante pour les deux monômes premiers non obligatoires n et p.

Il y a des bases premières qui comportent n, il y a des bases premières qui comportent p, il y a éventuellement des bases qui comportent n et p.

Attachons à chaque monôme premier m_i de f autre que n et p une variable nouvelle x_i et construisons la fonction

$$F = (n+p) \prod_i x_i + \sum_i m_i \prod_{j \neq i} x_j$$

Les consensus entre monômes figurant dans l'expression de F sont ceux de f multipliés par $\prod_i x_i$. Il en résulte que les monômes premiers de F sont exactement ceux qui sont écrits.

Cherchons les bases premières de F. Un consensus contenant toujours $\prod_i x_i$ tous les $m_i \prod_{j \neq i} x_j$ sont obligatoires.

$\sum m_i \prod_{j \neq i} x_j$ ne couvre pas $(n+p) \prod_i x_i$ comme on le voit en faisant tout les x_i égaux à 1.

Par contre

$$(2) \quad \sum m_i \prod_{j \neq i} x_i + n \prod_i x_i$$

et

$$(3) \quad \sum m_i \prod_{j \neq i} x_i + p \prod_i x_i$$

couvrent respectivement $p \prod_i x_i$ et $n \prod_i x_i$

Par conséquent (2) et (3) sont les seules bases premières de F.

<u>Exemple</u>

Considérons la fonction ceinture du cube :

$ab'+bc'+ca'+a'b+b'c+c'a$

Prenons :

$n = ab'$, $p = b'c$

La fonction cherchée est

$$f = (ab'+b'c)\ xyzt + bc'xyz + ca'xyt + a'bxzt + c'ayzt$$

CHAPITRE III

SPECTRES DES FONCTIONS BOOLEENNES

SPECTRES DES FONCTIONS BOOLEENNES

Nous définissons la notion de spectre et en étudions quelques propriétés générales. Nous considérerons à la fois des fonctions booléennes et des fonctions ϕ-booléennes.

3.1 Spectre de la fonction

Nous nommerons ainsi l'ensemble des modèles des bases premières de la fonction.

3.1.1 *Spectre renseigné*

Le spectre est dit renseigné si pour chaque modèle on indique le renseignement, c'est-à-dire le nombre de bases ayant ce modèle.
La somme des renseignements est le nombre total de bases de la fonction.
Nous allons étudier un certain nombre d'opérations sur le spectre ou le spectre renseigné.

3.2 Addition vectorielle de spectres

On prend deux fonctions avec des variables différentes $f(X)$, $g(Y)$ et on les ajoute. Cela revient à ajouter les bases deux à deux, à ajouter vectoriellement les modèles.
C'est ce que nous appellerons :

"Ajouter vectoriellement les spectres"

Si le spectre est renseigné, le renseignement relatif à un modèle M est la somme des produits des renseignements des modèles qui fournissent M.

Remarque 1

La propriété s'étend à k fonctions.

Remarque 2

Le nombre de bases de $f(X)+g(Y)$ est le produit des nombres de bases de f et g. Nous verrons plus loin des moyens plus puissants de construire des fonctions ayant un très grand nombre de bases.

3.2.1 *Translation des spectres*

Dans le cas où g est une fonction à un seul modèle $(m,1)$ le résultat précédent devient :

Le spectre de $f(X)+g(Y)$ s'obtient en faisant subir au spectre de f la translation $(m,1)$.

Tous les renseignements de f sont multiples par le renseignement de g.

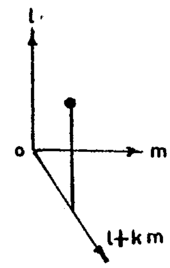
Nous avons déjà utilisé ce résultat au chapitre II.

3.2.2 *Changement d'axe sur le spectre*

En multipliant la fonction par k variables n'y figurant pas, on remplace le modèle (m,ℓ) par le modèle $(m, \ell+km)$.

Ceci peut s'interpréter ainsi :
on garde le spectre mais on remplace l'axe des m par la droite $\ell+km=0$ (en gardant l'axe des ℓ et sa graduation, ainsi que les valeurs de m).
Nous avons déjà utilisé cette propriété.

fig 1



3.2.3 *Dédoublement multiplicatif de variables monoformes*

En remplaçant dans une fonction la variable directe x par $x_1\ x_2 \ldots\ x_p$ on ne crée pas de nouvelles bases. On remplace une base de modèle (m,ℓ) par une base de modèle $(m,\ell+p\alpha)$, α désignant le nombre d'apparition de la variable x dans la base.

Démonstration

Soit

$$f = g(Y) + x\, h(Y)$$

et

$$f_p = g(Y) + x_1\ x_2 \ldots\ x_p\ h(Y)$$

Les monômes premiers de f et de f_p se correspondent par $x \leftrightarrow x_1\ x_2 \ldots\ x_p$, de même les consensus et les monômes premiers et pour finir les bases premières.
Nous avons utilisé cette propriété.

Remarque

Le dédoublement d'une variable non directe peut créer de nouvelles bases.

Exemple

Soit la fonction

(1) $xy' + x'y + z'(x+y)$

qui admet deux bases premières

$xy' + x'y + z'x$

$xy' + x'y + z'y$

En dédoublant z en uv on obtient une nouvelle fonction :

$$xy' + x'y + (u'+v')(x+y)$$

qui admet 4 bases premières à savoir :

$$xy' + x'y + u'x + v'x$$

$$xy' + x'y + u'x + v'x$$

$$xy' + x'y + u'y + v'x$$

$$xy' + x'y + uy' + v'y$$

3.3 Combinaison linéaire de fonctions

Considérons les fonctions

$$f_1(X),\ f_2(X), \ldots ,\ f_n(X)$$

des mêmes variables et la fonction :

$$f = \lambda_1\ f_1(X) + \lambda_2\ f_2(X) + \ldots + \lambda_n\ f_n(X)$$

où $\lambda_i \notin X$

En formant les consensus de monômes de cette fonction on rencontre

- des consensus de monômes de la même fonction f_i. Ils sont de la forme :

  $\lambda_i m$

- des consensus de monômes de fonctions différentes : ils sont de la forme

  $\lambda_i\ \lambda_j \ldots\ \lambda_k\ m$

un tel monôme ne peut par consensus redonner un $\lambda_i\ m_i$.
Ils ne figurent donc dans aucune base première.
Par suite les bases premières de f s'obtiennent en combinant linéairement les bases premières de $f_1,\ f_2, \ldots,\ f_n$.

Les monômes premiers de f

On déduit que les monômes premiers de la fonction f sont :

- soit de la forme λ_i m où m est un monôme premier de f,
- soit de la forme $\lambda_i\ \lambda_j \ldots\ \lambda_k$ m où m est obtenu par consensus entre les monômes des fonctions $f_i,\ f_j, \ldots,\ f_k$.

Modèles des bases premières de f

A partir des modèles :

$$(m_1,\ell_1),\ (m_2,\ell_2),\ \dots,\ (m_n,\ \ell_n)$$

On obtient le modèle :

$$(m_1+m_2+\dots+m_n,\ \ell_1+\ell_2+\dots+\ell_n+m_1+m_2+\dots+m_n)$$

et un nombre de bases égal à

$$b_1\ b_2\dots b_n$$

si b_i est le nombre de bases de f_i.

Remarque

Ceci permet de construire des fonctions ayant un très grand nombre de bases pour un nombre de variables peu élevé.

Exemple

Soit $C(X)$ la fonction ceinture du cube. La fonction

$$\lambda_1\ C(X) + \lambda_2\ C(X) + \lambda_3\ C(X)$$

admet 5^3 bases premières pour 6 variables.

3.4 Produit f(X). G(Y)

Soient les fonctions $f(X)$ et $g(Y)$. Les monômes premiers de la fonction $F = f(X)\ g(Y)$ s'obtiennent en multipliant les monômes premiers de la fonction $f(X)$ par ceux de $g(Y)$.

Soient (m_1,ℓ_1) le modèle d'une base première b_1 de $f(X)$ et (m_2,ℓ_2) le modèle d'une base première b_2 de $g(Y)$.

Alors on obtient une base première de $f(X)\ g(Y)$ en multipliant les monômes de b_1 par ceux de b_2.

En effet,

- la somme de tous ces monômes donne bien fg
- aucun monôme n'est superflu. En effet, soit $\mu\nu$ un tel monôme, on peut trouver une valeur de X telle que μ soit seul de b_1 à couvrir cette valeur et une valeur de Y telle que ν soit le seul de b_2 à couvrir cette valeur. Si l'on supprime $\mu\nu$ il y a fonc un point de fg non couvert.

Une telle base est de modèle

$$(m_1\ m_2,\ m_1\ \ell_2 + m_2\ \ell_1)$$

Remarque 1

On peut généraliser à k fonctions. On obtient :

$$(m_1\, m_2 \ldots m_k,\ \sum_j \ell_j\, \Pi_{i \neq j}\, m_i),\ i,j \in \{1,2,\ldots,k\}$$

Exemple

Considérons deux fonctions f_1 et f_2 suivantes. La première admet deux bases premières, la seconde en admet trois :

$$f_1 \begin{cases} p'qr' + pq'r + spq \\ \\ p'qr' + pq'r + spr + sqr' \end{cases}$$

$$f_2 \begin{cases} k + vx \\ k + vy + vz \\ k + vz + vt + vu \end{cases} \quad \text{avec } k = xy'z' + xz't'u' + x'z + x'z + x't + x'u$$

soit (m_1, ℓ_1) le modèle d'une base première de f_1,

on a :

$(m_1, \ell_1) \in \{(3,9), (4,12)\}$

Soit (m_2, ℓ_2) le modèle d'une base première de f_2,

On a :

$(m_2, \ell_2) \in \{(7,17), (8,19), (9,21)\}$

On a donc pour $f_1\ f_2$ des bases de modèle

$(m,\ell) \in \{(21, 104), (24, 129), (27, 144), (28, 152), (32,172), (36,192)\}$

Remarque 2

La fonction $f_1\ f_2$ a beaucoup d'autres bases. Par exemple prenons une base de f_1, à chaque monôme de cette base on associe une base de f_2. Le même raisonnement que plus haut permet de montrer qu'on obtient bien une base première de $f_1\ f_2$.

Comptons les bases ainsi obtenues pour la ceinture du cube multipliée par elle-même. On trouve

$$\left.\begin{array}{ll} 3 \text{ bases de } f_1 \text{ à 4 monômes} & 3.5^4 \\ \\ 3 \text{ bases de } f_1 \text{ à 3 monômes} & 2.5^3 \end{array}\right\} 5^3 \times 17$$

De même pour f_2 $5^3 \times 34$

Il faut enlever les bases communes, soit

bases de f_1 x bases de f_2 5^2

En tout 25 x 169 = 4225 pour 6 variables.

Mais cette fonction a encore d'autres bases.

En voici une :

	ab'	ac'	bc'	ba'	ca'	cb'
xy'	X	Y	X	Y	X	X
xz'	Y	X	X	X	Y	X
yz'	X	X	Y	X	X	X
yx'	Y	X	X	X	Y	X
zx'	X	Y	X	Y	X	X
zy'	X	X	X	X	X	Y

A partir des 10 monômes marqués Y on construit tous les autres (marqués X) par consensus successifs (l'opération de consensus porte sur deux monômes de la même ligne ou colonne séparées par une seule case où se trouve le consensus). Cette figure correspond à un pavage du plan de pas 6 dans les deux directions.

On voit facilement que cette base est première.

3.5 Fonctions à modèles proportionnels

Une fonction sera dite à modèle proportionnels si elle a plusieurs modèles et si leurs coordonnées (m_1, ℓ_1), (m_2, ℓ_2),... sont proportionnelles :

$$\frac{\ell_1}{m_1} = \frac{\ell_2}{m_2} = \dots$$

Exemples

1) Ceinture du cube

   Cette fonction a deux modèles (3,6) et (4,8) qui sont proportionnels.

2) La fonction $x'yz' + xy'z + txy$ a deux bases premières :

$$\begin{cases} x'yz' + xy'z + txy \\ x'yz' + xy'z + txz + tyz' \end{cases}$$

Les modèles des deux bases sont proportionnels.

3.6 Fonctions à modèles alignés

Nous nommerons ainsi une fonction dont les points représentatifs des modèles sont alignés.

Exemples

1) Soit $f(X)$ une fonction dont les modèles des bases sont alignés et $g(X)$ une fonction à une seule base première, alors la fonction $f(X) + g(X)$ est à modèles alignés, puisqu'on fait subir une translation au spectre de f.

2) Toute fonction à deux modèles est une fonction à modèles alignés.

3) Soit $f(X)$ une fonction à modèles alignés (proportionnels). La fonction

   (1) $f(X) + f(Y) + \ldots + f(Z)$

   est encore une fonction à modèles alignés (proportionnels).
   En particulier si $f(X)$ est à 2 modèles alignés (proportionnels).
   La fonction

   (2) $f(X_1) + f(X_2) + \ldots + f(X_n)$

   est a $(n+1)$ modèles alignés (proportionnels) équidistants.

Les points du spectre de la fonction $f(X)$ étant alignés, on peut les représenter par les extrémités des vecteurs :

$$\vec{V}_i = \vec{a} + \lambda_i \vec{b}$$

λ_i appartient à un ensemble fini E des nombres réels (on peut prendre les vecteurs $\vec{a}$ et $\vec{b}$ tels que tous les λ_i soient entiers).

De la même façon, on peut représenter les points du spectre de la fonction $f(Y)$ par les extrémités des vecteurs :

$$\vec{V}_j = \vec{a} + \lambda_j \vec{b} \quad , \lambda_j \in E$$

Les points du spectre de la fonction $f(X) + f(Y)$ sont les extrémités des vecteurs :

$$\vec{V}_i + \vec{V}_j = 2\vec{a} + (\lambda_i + \lambda_i) \vec{b}$$

qui sont évidemment alignés.
On peut facilement généraliser à k fonctions.

Si le spectre de la fonction $f(X_1)$ contient deux points A et B, alors deux points successifs quelconques du spectre de la fonction (2) sont distants de AB.
Chaque fois qu'on ajoute une nouvelle fonction, le nombre des points du spectre augmente d'une unité. Le spectre de la fonction (2) a par suite $(n+1)$ points équidistants.

4) Soit f(X) une fonction à modèles alignés (proportionnels).
La fonction

$$m\ f(X)$$

m désignant un monôme formé de k nouvelles variables est encore une fonction à modèles alignés (proportionnels).

Sur la figure (2) S_1 et S_2 représentent respectivement les spectres des deux fonctions f(X) et mf(X). Dans le cas (a) la pente du support du spectre S_1 est limité, dans le cas (b) la pente est infinie.

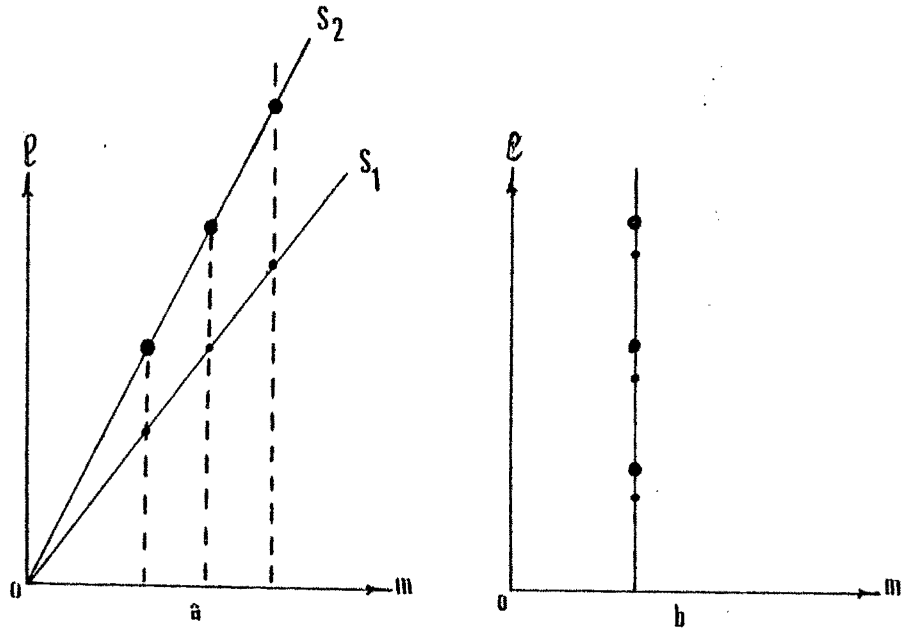


Figure 2.

5) Si les fonctions $f_1(X)$, $f_2(X)$,..., $f_n(X)$ sont des fonctions à modèles alignés (proportionnels), avec la même pente, alors la fonction :

$$f = \lambda_1\ f_2(X) + \lambda_2\ f_2(X) + \ldots + \lambda_n\ f_n(X)$$

est encore une fonction alignés (proportionnels). La pente est augmentée de 1.

Soit $(m_1,\ l_1)$ et $(m_2,\ l_2)$ deux points du spectre s_1 de la fonction $f_1(X)$. Les points correspondants dans le spectre λ_1 de la fonction $\lambda_1\ f_1(X)$ sont :

$$(m_1,\ l_1 + m_1),\ (m_2,\ l_2 + m_2)$$

La pente de Σ_1 est égale à celle de S_1 augmentée de 1.

Les spectres de toutes les fonctions $\lambda_i \; f_i(X)$ ont la même pente, par suite la fonction f est à modèles alignés avec la même pente que les fonctions $\lambda_i \; f_i(X)$.

3.7 Proposition

Si les deux fonctions f(X) et f(Y) sont à modèles alignés, alors le spectre de la fonction f(X) + g(Y) est en grille si les pentes sont différentes, à points alignés si les pentes sont égales.

Démonstration

Soient E : $\{A_1, A_2, \ldots A_p\}$ et F = $\{B_1, B_2, \ldots, B_q\}$ respectivement les spectres des fonctions f(X) et g(Y) (Figure 3). Les droites P et Q sont les supports des deux spectres.

Pour construire le spectre de la fonction f(X) + g(Y) on construit la somme vectorielle :

$$\vec{OS}_{ij} = \vec{OA}_i + \vec{OB}_i \qquad \begin{cases} i \in I = \{1,2,\ldots, p\} \\ \\ j \in J = \{1,2,\ldots, q\} \end{cases}$$

Pour une valeur fixe de $i \in I$ ou de $j \in J$, les points S_{ij} sont alignés. Ainsi le spectre de la fonction f(X) + f(Y) est en grille.

Construction plus simple

On construit la grille C formée des points C_{ij} qui sont les points de rencontre des droites $A_i \; Q_i \parallel Q$ et $B_j \; P_j \parallel P$. On construit le vecteur $\vec{OS}_{11} = \vec{OA}_1 + \vec{OB}_1$ et puis le vecteur $\vec{OO}_1 = S_{11} \; C_{11}$.

La grille C représente le spectre de la fonction f(X) + g(Y) dans le repère $m_1 O_1 \ell_1$

Nous retrouverons encore plus tard des fonctions à modèles alignés ou proportionnels.

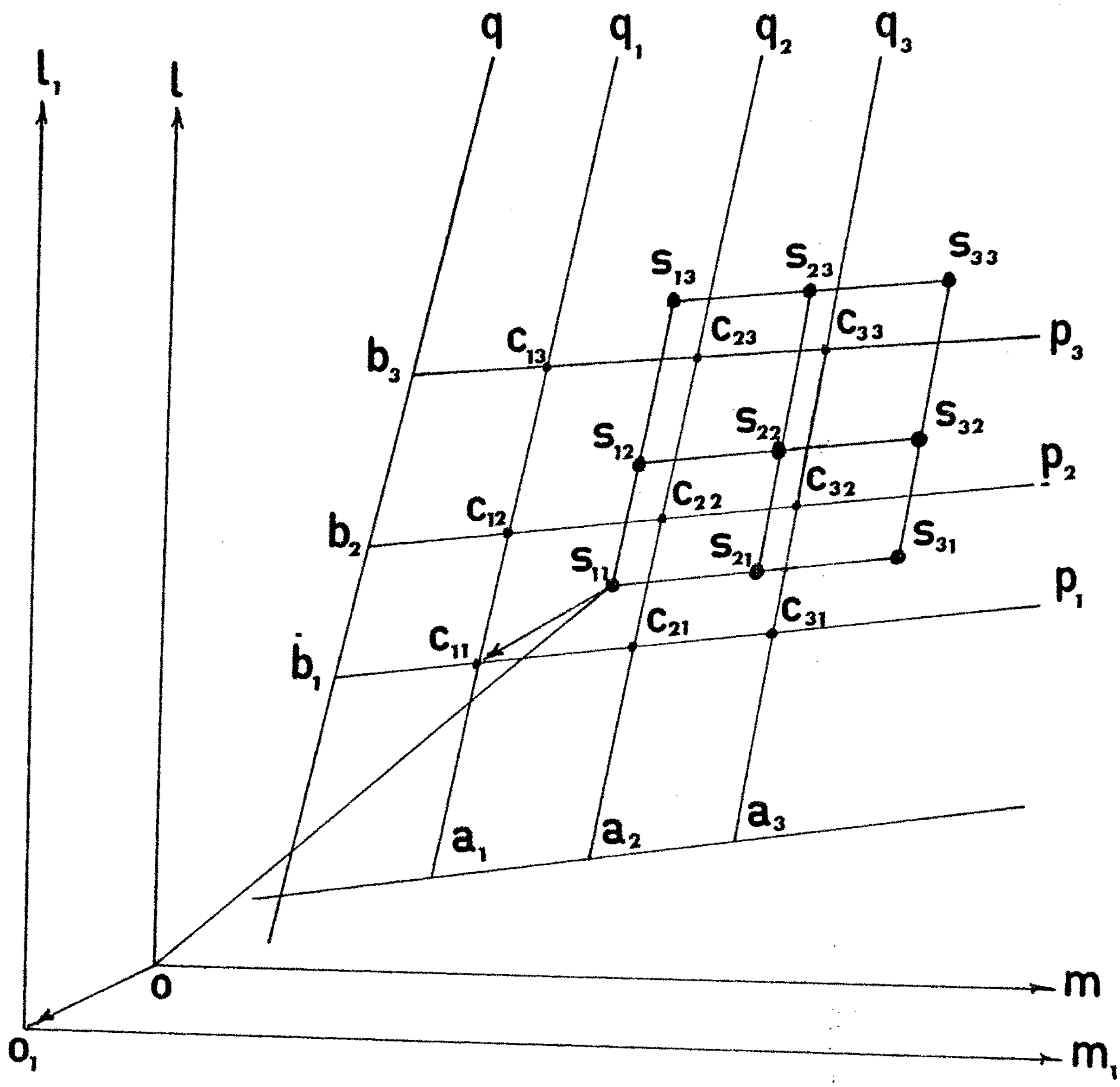


Figure 3.

3.8 Construction des fonctions ϕ-booléennes de spectres donnés

3.8.1 *Théorème*

Une condition nécessaire et suffisante pour qu'une fonction ϕ-booléenne $f = h(X_n) + \phi g(X_n)$ admette n bases premières de la forme :

$$x_i \quad , \quad 1 \leq i \leq n$$

est que :

$$h(X_n) = \prod_{i=1}^{i=n} x_i$$

$$g(X_n) = \sum_{i=1}^{i=n} x_i$$

Démonstration

La condition est nécessaire. Si une fonction ϕ-booléenne admet n bases premières x_i, alors la borne supérieure de cette fonction est :

$$\sum_{i=1}^{i=n} x_i$$

La borne inférieure de la fonction doit être couverte par chacun des monômes premiers de la borne supérieure, elle ne peut être que de la forme :

$$\prod_{i=1}^{i=n} x_i$$

La fonction est par suite de la forme

$$f = \prod_{i=1}^{i=n} x_i + \phi \sum_{i=1}^{i=n} x_i$$

La condition est suffisante. Si la fonction f est de la forme :

$$f = \prod_{i=1}^{i=n} x_i + \phi \sum_{i=1}^{i=n} x_i$$

alors elle a respectivement pour la borne supérieure et la borne inférieure les expressions suivantes :

$$\overline{f} = \sum_{i=1}^{n} x_i$$

$$\underline{f} = \prod_{i=1}^{i=n} x_i$$

Tout monôme premier x_i de $\overline{f}$ couvre la borne inférieure $\underline{f}$. La fonction admet donc n bases premières x_i, $1 \leqslant i \leqslant n$.

Toute autre base contient plusieurs x_i et par suite n'est pas première.

3.8.2 *Problème*

Construire une fonction ϕ-booléenne dont le spectre renseigné est donné.

Considérons le spectre formé par les points $A_1(m_1,l_1)$, $A_2(m_2,l_2)$,..., $A_p(m_p,l_p)$ dont les renseignements sont respectivement α, β,...Π.

Soit

$$k = \alpha+ \beta+... + \Pi$$

Formons la fonction :

$$f = \prod_{i=1}^{i=k} x_i + \phi \sum_{i=1}^{i=k} x_i$$

Cette fonction a k bases premières de la forme :

$$x_i \ , \quad 1 \leqslant i \leqslant k$$

Aux variables $x_1,x_2,..., x_\alpha$ nous attribuons α polynômes booléens sans variable accentuée, chacun comportant m_1 monômes dont la somme des lettres est l_1.

Aux variables $x_{\alpha+1}$, $x_{\alpha+2}$,..., $x_{\alpha+\beta}$ nous attribuons β polynômes, chacun comportant m_2 monômes dont la somme des lettres est l_2 et ainsi de suite (les variables étant toutes différentes).
Nous remplaçons dans f, les variables $x_1,x_2,..., x_n$ par leur polynôme correspondant et nous obtenons une fonction nouvelle F. Les variables de cette dernière étant toutes monoforme elle a exactement le spectre cherché (pas de création de nouvelle base première).

Cherchons par exemple une fonction ϕ-booléenne dont le spectre est formé de 3 points :

$$(1,1)_2,\ (2,3)_1,\ (3,8)_2$$

Les indices indiquant les renseignements.
La somme des renseignements est :

$$2+1+2 = 5$$

La fonction cherchée est

$$\prod_{i=1}^{i=5} x_i + \phi \sum_{i=1}^{i=6} x_i$$

qui admet 5 bases premières :

$$x_i \ , \quad 1 \leqslant i \leqslant 5$$

On prend :

$$x_1 = t_1$$
$$x_2 = t_2$$
$$x_3 = t_3+t_4\ t_5$$
$$x_4 = t_6+t_7+t_8\ t_9 \dots\ t_{13}$$
$$x_5 = t_{14}+t_{15}+t_{16}\ t_{17} \dots\ t_{21}$$

3.9 Le rapport des nombres de monômes et de lettres de bases d'une fonction booléenne

Pour les fonctions booléennes qu'on rencontre, les maxima n et l du rapport des nombres de monômes ou des lettres de deux bases premières n'est pas grand.
Notre but est maintenant de construire des fonctions pour lesquelles ces rapports sont grands.

3.9.1 *Construction des fonctions ϕ-booléennes dont le rapport L est grand*

Clé de parité

Nous désignerons par $f_1(X_{n-1})$ la clé de parité à n-1 variables. Cette fonction possède 2^{n-2} monômes premiers à n-1 lettres, soit $(n-1).2^{n-2}$ lettres.
Nous désignerons par $f_2(X_{n-1})$ le complémentaire de $f_1(X_{n-1})$. Cette fonction a les mêmes nombres de lettres et de monômes que la précédente.

3. 1 Construction d'une fonction ϕ-booléenne dont les rapports L et M sont grands

Considérons la fonction ϕ-booléenne à n variables

$$F(X_n) = x_n(f_1(X_{n-1}) + f_2(X_{n-1})) + x'_n\,\phi\, f_1(X_{n-1})$$

Cette fonction a pour la borne supérieure :

$$\overline{F} = x_n + f_1(X_{n-1})$$

D'où les deux bases premières :

1) x_n qui couvre $x_n\ f_1(X_{n-1})$

2) $f_1(X_{n-1})$ dont tous les monômes sont nécessaires pour couvrir $x_n f_1$.

Le rapport des nombres de monômes est 2^{n-2}.
Le rapport des nombres de lettres est $(n-1)2^{n-2}$.
Ces deux nombres sont très grands.

Construction des fonctions booléennes dont le rapport L est grand

3.9.1.2 Première construction

Soit la fonction

$$F(a_0,a_1,X_n) = a_0 \oplus a_1 + (a_0+a_1)\ f_1(X_n)$$

où $f_1(X_n)$ est la clé de parité à n variables.
En formant les consensus on constate que les seuls monômes premiers de la fonction sont :

$$a_0\ a_1',\ a_0'\ a_1,\ a_0\ m_i,\ a_1\ m_i \qquad m_i \text{ monômes de } f_1(X_n).$$

Les seules bases premières sont

$$a_0\ a_1' + a_1\ a_0' + \Sigma\ k_i\ m_i, \qquad k_i = a_0 \text{ ou } a_1$$

Cette fonction a donc 2^{2^n} bases premières pour n+3 variables, soit 2^8 bases pour 6 variables. $2^8 = 256$.
La fréquence de $\tilde{a}_0$ est maximum dans la base b_1 d'expression

$$a_0 \oplus a_1 + a_0\ f_1(X)$$

Il y a $2+2^{n-1}$ lettres $\tilde{a}_0$ dans la base b_0 et 2 lettres $\tilde{a}_1$.

La fréquence de a_1 est maximum dans la base b_{2n} d'expression :

$$a_0 \oplus a_1 + a_1\ f_1(X)$$

Il y a $2+2^{n-1}$ lettres $\tilde{a}_1$ dans la base b_2 et 2 lettres $\tilde{a}_0$.

Prenons :

$$a_0 = u_1\ u_2 \ldots\ u_p$$

Les monômes premiers de la nouvelle fonction sont ceux qui figurent dans

$$u_1\ u_2 \ldots\ u_p\ a_1' + (u_1' + u_2' + \ldots + u_p')\ a_1 + u_1\ u_2 \ldots\ u_p\ f_1(X_n) + a_1\ f_1(X_n)$$

et les bases premières sont de la forme :

$$u_1\ u_2 \ldots\ u_p\ a_1' + (u_1' + u_2' + \ldots + u_p')\ a_1 + \Sigma\ k_i\ m_i,$$

m_i monôme premier de $f_1(X_n)$

$k_i = u_1\ u_2 \ldots\ u_p$ ou a

Considérons les 2 bases :

b_1 obtenue en prenant partout $k_i = u_1\, u_2 \ldots u_p$

b_2 obtenue en prenant partout $k_i = a$

Soient (m_1, l_1) et (m_2, l_2) respectivement les modèles des deux bases.

On a

$$m_1 = m_2 = 1+p+2^{n-1}$$

$$l_1 = 2+2p+(p+n).2^{n-1}$$

$$l_2 = 2+2p+(1+n).2^{n-1}$$

On a :

$$\frac{l_1}{l_2} = \frac{2+2p+(p+n)2^{n-1}}{2+2p+(1+n)2^{n-1}}$$

Pour $p \gg n$ et n suffisamment grand, la valeur de $\frac{l_1}{l_2}$ est grande

$$\frac{l_1}{l_2} \simeq p$$

3.9.1.2 Deuxième construction

Considérons la fonction booléenne $f(X_1)$ ayant les deux bases premières :

$$x_1'\, x_3 + x_2'\, x_3' + x_1\, x_2\, x_4$$

$$x_1'\, x_3 + x_2'\, x_3' + x_2\, x_3\, x_4 + x_1\, x_3'\, x_4$$

de modèles respectifs (3,7), (4,10).

Construisons la fonction $F = f(X_1).f(X_2) \ldots f(X_n)$. D'après la proposition 3.4, parmi les bases premières de la fonction F on peut distinguer deux bases premières de modèle $(3^n,\ 7.3^{n-1})$, $(4^n,\ 10.4^{n-1})$.

Le rapport des lettres des deux bases est

$$\frac{10}{7}\left(\frac{4}{3}\right)^{n-1}$$

Ce nombre est grand avec n.

CHAPITRE IV

LA FONCTION $S_n^{1,1}$ ET APPLICATIONS AUX FONCTIONS $f + \lambda g$

LA FONCTION $S_n^{1,1}$ ET APPLICATIONS AUX FONCTIONS $f + \lambda g$

Dans ce chapitre, nous étudierons une fonction particulière et ses utilisations pour construire des fonctions ayant un spectre particulier.

4.1. Fonction symétrique

On désigne par $S_n^{i,j}$ la somme de tous les produits de i variables directes par j variables complémentées prise parmi n, une telle fonction est dite symétrique, voir [17].

4.1.1. *Fonction $S_n^{1,1}$*

D'après la définition ci-dessus on a :

$$S_n^{1,1} = \sum_{i,j} x_i\, x_j' \qquad i,j \in N = \{1,2,\ldots,n\}$$

qu'on peut encore écrire :

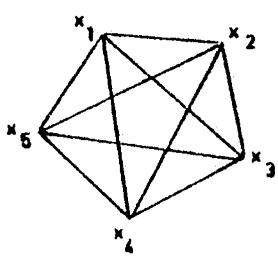
$$S_n^{1,1} = \sum_{i,j} (x_i\, x_j' + x_j\, x_i') = \sum_{i,j} (n_i \oplus n_j)$$

4.1.2. *Représentation géométrique*

Nous représentons la variable x_i par un point x_i dans le plan et la disjonction $x_i \oplus x_j$ par le segment $x_i\, x_j$:

Sur la figure (1), nous avons représenté le graphe G de la fonction $S_5^{1,1}$

fig 1



4.2.1. Théorème

Soit $C(X_n)$ la fonction $\Sigma\,(n_i \oplus n_j)$ qui correspond à un cycle couvrant tous les sommets du graphe G_n. Alors on a :

$$C(X_n) = S_n^{1,1}(X_n)$$

Démonstration

Considérons par exemple le cycle $x_1\, x_2 \ldots x_n\, x_1$, on a :

$$C(X_n) = \sum_{i=1}^{i=n} x_i \oplus x_{i+1}$$

(Par convention $x_{n+1} = x_1$)

Il suffit de démontrer que :

(1) $\qquad x_i \oplus x_j \leq C(X_n)\ , \quad \forall\ i, j \in N$

nous utilisons le raisonnement par récurrence.

Démontrons que si on a :

(2) $\qquad x_i \oplus x_{i+p} \leq C(X_n)$

on a alors :

(3) $\qquad x_i \oplus x_{i+p+1} \leq C(X_n)$

l'inégalité (2) nous permet d'écrire :

$$C(X_n) = \ldots + x_i\, x'_{i+p} + x'_i\, x_{i+p} + x_{i+p} . x'_{i+p+1} + x'_{i+p} . x_{i+p+1} + \ldots$$

On calcule les consenus des deux couples des monômes

$(x_i\, x'_{i+p},\ x_{i+p} . x'_{i+p+1})$ et $(x'_i . x_{i+p}\ ,\ x'_{i+p} . x_{i+p+1})$

et onconsidère que le consensus est inférieur ou égal à la somme de ses générateurs, on obtient l'inégalité (3).

A partir de l'inégalité (3), par récurrence on déduit l'inégalité (1).

4.2.2. Théorème.

On peut supprimer une disjonction quelconque de la fonction $C(X_n)$ correspondant à un cycle couvrant tous les sommets de G_n, sans changer la valeur de $C(X_n)$.

Démonstration :

Considérons par exemple le cycle $x_1\ x_2 \dots x_n\ x_1$. On a :

$$C(X_n) = \sum_{i=1}^{i=n} x_i \oplus x_{i+1}$$

Démontrons qu'on peut supprimer de $C(X_n)$, la disjonction

$x_j \oplus x_{j+1}$, $\forall\ j \in N$

Par l'opération consensus, on peut obtenir à partir des disjonctions

$x_{j+1} \oplus x_{j+2}$, $x_{j+2} \oplus x_{j+3}$, ... , $x_{j-1} \oplus x_j$, la disjonction $x_{j+1} \oplus x_{j+n}$

qui est égale à $x_j \oplus x_{j+1}$.

On a donc :

$$(x_{j+1} \oplus x_{j+2}) + (x_{j+2} \oplus x_{j+3}) + \dots + (x_{j-1} \oplus x_j) \geq x_j \oplus x_{j+1}$$

On peut donc supprimer la disjonction $x_j \oplus x_{j+1}$ de la fonction $C(X_n)$ sans changer la valeur de cette dernière.

Corollaire : La fonction $C(X_n)$ a le caractère majoritaire pour $n = 3,4$ (La présence de la majorité des disjonctions est équivalente à la présence de toutes les disjonctions).

Faisons la démonstration pour $n = 4$ qui est la plus difficile.

Il faut prendre 4 disjonctions parmi les 6 :

12, 13, 14, 23, 24, 34

Chaque lettre figurera en moyenne 2 fois. Si chacune figure 2 fois, on a un cycle tel que :

12 23 34 41

et la propriété est vraie.

Si l'une figure 3 fois, on a une situation telle

12 13 14 23

à partir de laquelle on peut construire 34 et 42.

Remarque : Le caractère majoritaire est perdu pour n = 5.

En effet, les 6 couples

12 13 14

23 24 34

n'utilisent pas le point 5.

Notations : Considérons l'ensemble des variables booléennes :

$$X = \{x_1, x_2, \ldots, x_n\} \quad \text{et notons :}$$

$$\begin{cases} s_{i,j} = \sum\limits_{i \neq j} x_i \\ \\ p_j = \prod\limits_{i \neq j} x_i \end{cases} \qquad i,j \in N = \{1,2,\ldots,n\}$$

on obtient n monômes et n monaux.

4.3. Proposition : On a :

$$\begin{cases} (1) \quad S_n^{1,1}(s_1,s_2,\ldots,s_n) = S_n^{1,n-1}(x_1,x_2,\ldots,x_n) \\ \\ (2) \quad S_n^{1,1}(p_1,p_2,\ldots,p_n) = S_n^{n-1,1}(x_1,x_2,\ldots,x_n) \end{cases}$$

Démonstration de la relation (1) : on a :

$$s_i \oplus s_j = \sum_{k\neq i} x_k \prod_{\ell\neq j} x'_\ell + \sum_{k\neq j} x_k \prod_{\ell\neq i} x'_\ell$$

$$= x_j \prod_{\ell\neq j} x'_\ell + x_i \prod_{\ell\neq i} x'_\ell$$

D'où la propriété.

La démonstration de la relation (2) est analogue par dualité.

4.4. <u>La forme PS de la fonction $S_n^{1,1}$</u>. On a :

$$(1) \qquad S_n^{1,1}(X) = \Big(\sum_{i=1}^{i=n} x_i\Big)\Big(\sum_{i=1}^{i=n} x_i'\Big)$$

En développant l'expression ci-dessus on trouve immédiatement :

$$\sum_{i \neq j} x_i\, x_j'$$

4.5. <u>Expression de $S_n^{1,1}$ au moyen des $x_i\, x_j'$</u>

Jusqu'à maintenant nous avons utilisé les disjonctions $x_i\, x_j' + x_j\, x_i'$.
Ce qui dans le graphe G correspond aux traits non orientés.

On peut maintenant séparer les termes $x_i\, x_j'$ et $x_j\, x_i'$

$$i \longrightarrow j \qquad\qquad i \longleftarrow j$$

que nous représenterons par des traits fléchés ce qui revient à utiliser un graphe orienté.

4.5.1. <u>*Théorème*</u> : Pour qu'une somme de termes $x_i\, x_j'$ soit égale à $S_n^{1,1}$ il faut et il suffit que le graphe orienté correspondant soit isovalent (c'est-à-dire qu'on puisse aller de tout sommet à tout autre sommet en suivant les flèches).

La propriété résulte du fait que le consensus de $x_i\, x_j'$ et $x_j\, x_k'$ est $x_i\, x_k'$, $i \neq k$.

La condition est donc suffisante. Elle est nécessaire puisque le seul moyen d'obtenir de nouveaux monômes est de former des consensus.

4.5.2. Application

Chacun des ensembles de monômes premiers suivants peuvent définir la fonction $S_n^{1,1}(X)$

$$E = \{e_1,\ e_2,\dots,e_n\} \qquad \text{avec } e_i = x_i\ x'_{i+1}$$

$$F = \{f_1,\ f_2,\dots,f_n\} \qquad \text{avec } f_i = x'_i\ x_{i+1}$$

$$G_i = E \cup F - \{e_i,\ f_i\} \qquad i \in N$$

Remarque : On a les relations :

$$S_n^{1,1}(X) = S_n^{1,1}(E) = S_n^{1,1}(F)$$

on écrit :

$$S_n^{1,1}(E) = \sum_i (e_i \oplus e_{i+1})$$

or

$$e_i \oplus e_{i+1} = x_i\ x'_{i+1} \oplus x_{i+1}\ x'_{i+2} = x_i\ x'_{i+1} + x_{i+1}\ x'_{i+2}$$

D'où

$$S_n^{1,1}(X) = S_n^{1,1}(E)$$

Par la même raison

$$S_n^{1,1}(X) = S_n^{1,1}(F)$$

4.6. Proposition : Soit la fonction booléenne :

$$f = S_n^{1,1}(X) + \lambda\ m$$

m est un monôme formé avec des lettres de X

- si m est croissant on a :

$$f = S_n^{1,1}(X) + \lambda\ X^+ \qquad (1)$$

- si m est décroissant on a :

$$f = S_n^{1,1}(X) + \lambda\ X'^+ \qquad (2)$$

- si m est mixte on a :

$$f = S_n^{1,1}(X) \qquad (3)$$

Démonstration

1) Soit $x_i\ x_j\ x_k \dots x_r\ x_s$ un monôme de $g(X)$, on effectue les opérations suivante qui nous offrent finalement le monôme λx_s :

$$C(x'_i\ x_j,\ \lambda x_i\ x_j\ x_k \dots x_r\ x_s) = \lambda x_j\ x_k \dots x_s$$

$$C(x'_j\ x_k,\ \lambda x_j\ x_k \dots x_r\ x_s) = \lambda\ x_k \dots x_s$$

$$C(x'_r\ .\ x_s,\ \lambda x_r\ x_s) = \lambda x_s$$

Ensuite, on effectue les opérations :

$$C(x'_s\ .\ x_t,\ \lambda x_s) = \lambda x_t \qquad t \in N - \{s\}$$

Les monômes obtenus : $\lambda\ x_i$ $1 \le i \le N$, absorbent les monômes en λ qui comportent plus de deux variables de X.

D'où la relation (1)

2) La démonstration de la relation (2) est analogue au cas (1)

3) Soit par exemple $x'_i\ x_j\ x'_k \dots x_k$ un monôme mixte. On a :

$$x'_i\ x_j \le S_n^{1,1}(X) \qquad \forall\ i,j \in N$$

On a donc :

$$\lambda\ x'_i\ x_j\ x'_k \dots x_r \le S_n^{1,1}(X)$$

D'où la relation (3).

4.6.1. *Proposition.*

Soit :

$$f(X) = S_n^{1,1}(X) + \lambda g(X)$$

a) Si $g(X)$ comporte uniquement des monômes mixtes, on a :

$$f(X) = S_n^{1,1}(X)$$

b) Si $g(X)$ comporte des monômes croissants et des monômes décroissants, on a :

$$f(X) = S_n^{1,1}(X) + \lambda$$

c) Si $g(X)$ comporte des monômes croissants (resp. décroissants) mais non des monômes décroissants (resp. croissants) on a :

$$f(X) = S_n^{1,1}(X) + \lambda X^+$$

$$(\text{resp. } S_n^{1,1}(X) + \lambda X'^+)$$

4.7.1. Théorème : Les monômes premiers de la fonction booléenne

$$f = h + \lambda g$$

où λ est une variable monoforme qui ne figure ni dans h, ni dans g, sont pour ceux qui ne contiennent pas λ ceux de h, pour ceux qui contiennent λ ceux de $\lambda(g+h)$ après suppression des monômes en λ multiples d'un monôme sans λ.

Démonstration : Pour un monôme m ne contenant pas λ la condition :

$$m \leq f \qquad \text{et} \qquad m \leq h$$

sont équivalentes. En effet $m \leq f$ donne pour $\lambda = 0$ $m \leq h$

En sens inverse $m \leq h \implies m \leq h + \lambda g$

Les monômes premiers de f indépendants de λ sont donc ceux de h.

Pour un monôme $m = \lambda p$ les conditions $m \leq f$ et $p \leq h+g$ sont équivalentes.
En effet $m \leq f$ entraîne pour $\lambda = 1$ $p \leq h+g$.
En sens inverse $p \leq h+g$ entraîne

$$\lambda p \leq \lambda h + \lambda g \leq h + \lambda g$$

Les monômes premiers de f contenant λ sont donc ceux de $\lambda(h+g)$.

4.7.2. Théorème : Soit la fonction booléenne :

$$f = h + \Sigma \lambda_i g_i \qquad 1 \leq i \leq p$$

où λ_i sont des variables monoformes ne figurant ni dans h ni dans les g_i.
Les monômes premiers de f sont pour ceux qui ne contiennent pas de variables monoformes, ceux de h, pour ceux qui contiennent une seule variable monoforme λ_i, ceux de $\lambda_i(g_i+h)$. Les monômes premiers qui contiennent au moins deux variables monoformes, sont des monômes premiers inutiles de deuxième espèce (immédiate).

4.8. Théorème : Les bases premières de la fonction :

$$f = h + \lambda g$$

où λ est une variable monoforme, sont de la forme :

(1) $$B_i + \lambda C_j$$

où les B_i sont les bases premières de h et les C_j sont des sommes irréductibles des monômes premiers de (g+h) tel que :

(2) $$f = B_i + \lambda C_j$$

Démonstration. Pour $\lambda = 0$, l'expression (1) devient B_i. D'après la relation (2), B_i est une base première de la fonction f pour $\lambda = 0$, par conséquent B_i est une base première de h.

On pourrait penser que si D est une base première de (g+h) tel qu'aucun monôme premier figurant dans D, multiplié par λ ne s'absorbe que par un monôme premier de h, alors $B_i + \lambda D$ (i étant fixé) est une base première pour f. L'exemple ci-dessous montre que cela n'est pas vrai. La raison en est que h couvre déjà certains points de λg. Il suffit de couvrir $\lambda h' g$.

Exemple 1 : Soit la fonction

$$f = h + \lambda g$$

avec :

$$\begin{cases} h = xy' + x'y \\ g = x + y \end{cases}$$

La fonction h a une seule base première à savoir : $xy' + x'y$.
La fonction $g+h = x + y$ a une seule base première à savoir : $x + y$.

Les monômes premiers de la fonction $\lambda(g+h)$ qui sont λx et λy ne s'absorbent pas par les monômes premiers de h, quand même l'expression $xy' + x'y + \lambda(x+y)$ n'est pas une base première pour la fonction f.

La fonction f a deux bases premières à savoir :

$$\begin{cases} h + \lambda x \\ h + \lambda y \end{cases}$$

<u>Exemple 2</u> : Calculons la base première de la fonction :

$$f = h + \lambda g$$

où

$$\begin{cases} h = ux\ (y'+v') + u'vx'y + v'z\ (u+y') \\ g = ux + u'vy + v'z \end{cases}$$

a) La fonction h a une seule base première à savoir l'expression h (aucun consensus). Tous les monômes figurant dans l'expression h sont monômes premiers essentiels.

Les monômes premiers de la fonction g sont les suivants :

$E = \{ux,\ u'vy,\ v'z,\ vxy,\ u'yz,\ xyz\}$

b) La fonction (g+h) = g a une seule base première à savoir l'expression g. Les autres monômes premiers sont inutiles.

Pour la recherche des bases premières de $h + \lambda g$ calculons les valeurs des variables booléennes $p_1, p_2, \ldots, p_6$ tel que l'on ait :

$$(1) \quad ux + u'vy + v'z = ux\ (y'+v') + u'vx'y + v'z\ (u+y') + p_1ux + p_2u'vy$$
$$+ p_3v'z + p_4vxy + p_5u'yz + p_6\ xyz$$

L'opération de consensus sur les monômes du deuxième membre de la relation ci-dessus donne :

$$\begin{cases} C(uxy',\ p_4\ vxy) = p_4\ uvx \\ C(uvx,\ uv'x) = \underline{p_4\ ux} \end{cases}$$

$$C(u'vx'y,\ p_4vxy) = \underline{p_4u'vy}$$

$$\begin{cases} C(v'y'z,\ p_5u'yz) = p_5\ u'v'z \\ C(uv'z,\ p_5u'v'z) = \underline{p_5v'z} \end{cases}$$

En considérant les résultats ci-dessus, la relation (1) devient :

$$ux + u'vy + v'z = ux\ (y' + v' + p_1\ v_1 + p_4) + u'vy\ (x'+z'+p_2+p_4) +$$
$$+ v'z\ (y' + u + p_3 + p_5u') + p_6\ xyz$$

Les 1ère et 3ème parenthèse se simplifant en :

$$y' + v' + p_1 + p_4\ , \qquad y' + u + p_3 + p_5$$

On a donc :

$$\begin{cases} p_1 + p_4 = 1 \\ p_2 + p_4 = 1 \\ p_3 + p_5 = 1 \\ \quad\; p_6 = 0 \end{cases}$$

Le système constitué par les trois premières équations du système ci-dessus est équivalent à l'équation :

$$(p_1 + p_4)\ (p_2 + p_4)\ (p_3 + p_5) = 1$$

ou

$$p_1\, p_2\, p_3 + p_1\, p_2\, p_5 + p_3\, p_4 + p_4\, p_5 = 1$$

on en déduit que :

$$p_1\, p_2\, p_3 = 1$$

$$p_1\, p_2\, p_5 = 1$$

$$p_3\, p_4 = 1$$

$$p_4\, p_5 = 1$$

On a par suite 4 bases premières de la forme :

$$h = \lambda Q_i \qquad 1 \leq i \leq 4$$

avec :

$$Q_1 = ux + u'xy + v'z$$
$$Q_2 = ux + u'vy + u'yz$$
$$Q_3 = v'z + vxy$$
$$Q_4 = vxy + u'yz$$

4.9. Théorème : Soient $g_1(X)$ et $g_2(X)$ deux fonctions booléennes données La condition nécessaire et suffisante pour qu'il existe une fonction booléenne qui ait une variable monoforme λ et qui puisse s'écrire sous les formes :

$$\mathrm{I} \qquad \begin{cases} P(X) + \lambda\, g_1(X) \\ P(X) + \lambda\, g_2(X) \end{cases}$$

est qu'elles soit de la forme :

$$P(X) + \lambda\, Q(X)$$

avec :

$$\text{II} \quad \begin{cases} P(X) \geq g_1(X) \oplus g_2(X) \\ Q(X) = g_1(X) \text{ ou } g_2(X) \text{ ou } g_1(X)\ g_2(X) \text{ ou } g_1(X) + g_2(X) \end{cases}$$

Démonstration

La condition est nécessaire : En considérant tous les jeux de valeurs des fonctions $g_1(X)$ et $g_2(X)$ on peut dresser le tableau ci-dessous :

$g_1(X)$	$g_2(X)$	$g_1(X) \oplus g_2(X)$	$P(X)$
0	0	0	$\emptyset$
0	1	1	1
1	0	1	1
1	1	0	$\emptyset$

ce qui prouve que :

$$P(X) \geq g_1(X) \oplus g_2(X)$$

La condition est suffisante. Si une fonction booléenne $f(X,\lambda)$ est de la forme $P(X) + \lambda Q(X)$ où $P(X)$ et $Q(X)$ vérifient les conditions (II), alors elle peut s'écrire sous les formes (I).

Il suffit de vérifier que

$$g_1g_2' + g_2g_1' + \lambda g_1 = g_1\ g_2' + g_2\ g_1' + \lambda g_2 = g_1\ g_2' + g_2\ g_1' + \lambda g_1\ g_2 =$$

$$g_1\ g_2' + g_2\ g_1' + \lambda(g_1+g_2)$$

Pour $\lambda = 0$ toutes ces quantités sont égales à $g_1g_2' + g_2\ g_1'$

Pour $\lambda = 1$ elles sont égales à $g_1 + g_2$

Exemples :

1) Construire une fonction qui puisse s'écrire sous les deux formes suivantes :

$$\text{I} \quad \begin{cases} P(X) + \lambda\ (x+y) \\ P(X) + \lambda\ xy \end{cases}$$

on a :

$$P(X) \quad (x+y) \oplus xy = xy' + x'y$$

Les deux formes désirées sont :

$$\text{II} \quad \begin{cases} x \oplus y + \lambda(x+y) + T(x,y) \\ x \oplus y + \lambda x\, y + T(x,y) \end{cases}$$

2) Construire une fonction qui admette deux bases premières de la forme (I) de l'expression ci-dessus.

Quel que soit T, les deux expressions (II) ne sont pas à la fois des bases premières. Par suite une telle fonction n'existe pas.

3) Construire une fonction qui admette deux bases premières de la forme

$$\text{I} \quad \begin{cases} P + txy \\ P + txz + tyz' \end{cases}$$

On a :

$$P = xy \oplus (xz + yz') + T = x'yz' + xy'z + T$$

En remplaçant dans les deux expressions (I), P par son expression, on obtient exactement deux bases premières pour $T = 0$.

On peut ajouter à la fonction P une fonction tel que $T = x'z'|x'zt'|\ldots$ Mais on ne peut pas ajouter à P, la fonction $y'z'$. Dans ce dernier cas, on obtient pour la fonction $f(x,\lambda)$ l'expression ci-dessous :

$$xy' + x'yz' + tx$$

Cette dernière fonction n'admet pas deux bases de la forme (I).

4) Construire une fonction qui admet deux bases de la forme suivant :

$$\text{I} \quad \begin{cases} P(X) + \lambda(ux + u'vy + v'z) \\ P(X) + \lambda(vxy + v'yz) \end{cases}$$

On a :

$$P(X) = uxy' + uv'x + v'y'z + u'vy + u'vx'yz' + T$$

En remplaçant dans les deux expressions (I), $P(X)$ par l'expression ci-dessus avec $T = 0$, on obtient deux bases premières.

On peut ajouter à $P(X)$ des fonctions diverses, mais on ne peut ajouter par exemple la fonction $u'vx'yz$. Dans ce dernier cas on obtient une fonction $f(X,\lambda)$ qui admet quatre bases premières.

5) Construire une fonction qui puisse s'écrire sous les formes :

$$\text{I} \quad \begin{cases} P(X) + \lambda g_1(X) \\ P(X) + \lambda g_2(X) \end{cases}$$

avec

$$\text{II} \quad \begin{cases} g_1(X) = xy + yz + zx + x'y'z' \\ \\ g_2(X) = x'y' + y'z' + z'x' + xyz \end{cases}$$

on doit avoir :

$$P(X) = g_1(X) \oplus g_2(X) + T(X) = C(X) + T(X)$$

$C(X)$ étant la fonction ceinture du cercle.

La fonction cherchée doit être de la forme :

$$C(X) + T(X) + \lambda g_i(X) \qquad i \in \{1,2\}$$

Comme la fonction $g_i(X)$ comporte des monômes croissants et des monômes décroissants, d'après la proposition 4.6.1 (b), on a :

$$C(X) + T(X) + \lambda g_i(X) = C(X) + T(X) + \lambda$$

Il n'existe donc pas de fonction qui puisse s'écrire sous la forme (I) avec les fonctions (II).

6) Construire une fonction qui puisse s'écrire sous les formes :

$$\text{I} \quad \begin{cases} P(X) + \lambda\, g'_1(X) \\ P(X) + \lambda\, g'_2(X) \end{cases}$$

avec les fonctions (II) de l'exemple ci-dessus.

On a :

$$P(X) \geq g'_2(X) \oplus g'_2(X) = C(X)$$

La fonction cherchée doit être de la forme :

$$C(X) + T(X) + \lambda\, g'_i(X) \quad , \qquad i \in \{1,2\}$$

Comme la fonction $g_i'(X)$ comporte des monômes avec lettres des deux sortes, on a donc d'après la proposition 4.6.1. (a) :

$$C(X) + T(X) + \lambda\, g_i'(X) = C(X) + T(X)$$

Il n'existe donc pas de fonction qui puisse s'écrire sous les formes désirées avec les fonctions (II).

4.10. Théorème : Une condition nécessaire et suffisante pour qu'il existe une fonction booléenne qui ait une variable monoforme λ et qui puisse s'écrire sous la forme :

$$\mathrm{I}\quad \left\{ \begin{array}{l} P(X) + \lambda\, g_1(X) \\ P(X) + \lambda\, g_2(X) \\ \cdots\cdots\cdots\cdots \\ P(X) + \lambda\, g_n(X) \end{array} \right.$$

est qu'elle soit de la forme :

$$P(X) + \lambda Q(Y)$$

avec

$$\mathrm{II}\quad \left\{ \begin{array}{l} P(X) \geq S_n^{1,1}(G(X)) \\ \text{où } G(X) = \{g_1(X),\ g_2(X),\ \ldots,\ g_n(X)\} \\ \text{et} \\ Q(Y) \text{ est une fonction croissante en } Y,\ Y \text{ est une} \\ \text{partie non vide de l'ensemble } G(X) \end{array} \right.$$

Démonstration :

La condition est nécessaire : soit $f(X,\lambda)$ une fonction booléenne qui peut s'écrire sous la forme (I). On va démontrer que :

$$P(X) \geq S_n^{1,1}(G(X))$$

On considère les deux premières expressions de (I), d'après le théorème 4.9., on a :

$$P(X) \geq g_1(X) \oplus g_2(X)$$

En raisonnant de la même façon sur tous les couples $(g_1(X), g_j(X))$ et en combinant les résultats obtenus on trouve :

$$P(X) \geq \sum_{i=2}^{i=n} (g_1(X) \oplus g_i(X)) = S_n^{1,1} (G(X))$$

<u>La condition est suffisante</u> si une fonction booléenne $f(X,\lambda)$ est de la forme $P(X) + \lambda\, Q(X)$ où $P(X)$ et $Q(X)$ vérifient les conditions (II), alors elle peut s'écrire sous les formes (I).

Considérons $g_1(X)$, $g_2(X), \ldots, g_n(X)$ comme variables, d'après la proposition 4.6.1. on peut écrire :

$$f(X,\lambda) = S_n^{1,1}(G(X)) + \lambda G^+(X)$$

La fonction ci-dessus admet des bases premières de la forme suivante (en considérant toujours $g_i(X)$, $1 \leq i \leq n$, comme variables),

$$s_j + \lambda g_i(X), \quad 1 \leq i \leq n$$

s_j est une somme minimale de $S_n^{1,1}(G(X))$

C.Q.F.D.

<u>Exemples</u>

1) Construire une fonction qui admet exactement 4 bases premières de la forme :

$$(1) \qquad P + \lambda Q_i \quad , \quad 1 \leq i \leq 4$$

avec :

$$Q_1 = ux + u'vy + v'z$$
$$Q_2 = ux + u'vy + u'yz$$
$$Q_3 = v'z + vxy$$
$$Q_4 = vxy + u'yz$$

on calcule :

$$\Sigma\ (Q_1 \oplus Q_i) \quad , \quad 2 \leq i \leq 4$$

on obtient :

$$P(X) = ux(y'+v') + u'vx'y + v'z\ (y'+u) + T$$

On remplace dans l'expression (1), P et Q_i par leur expression corre pondante (avec $T = 0$) et on vérifie qu'on a exactement 4 bases premi res (voir le théorème 4.8 et les exemples qui le suivent).

2) Construire une fonction booléenne qui puisse s'écrire sous les formes :

$$(1) \qquad P(X) + \lambda \sigma_i \quad , \quad 1 \leq i \leq n$$

où σ_i est la somme des produits i à i des variables de l'ensemble :

$$X = \{x_1, x_2, \ldots, x_n\}.$$

D'après le théorème ci-dessus on doit avoir :

$$P(X) \geq \sum_{i=1}^{i=n} \sigma_i \oplus \sigma_i$$

où

$$P(X) \geq \sigma_1 \Sigma \sigma'_i + \sigma'_1 \Sigma \sigma_i$$

comme on a :

$$\sigma_i \geq \sigma_{i+1} \quad , \quad 1 \leq i \leq n-1$$

on a donc :

$$\sigma_1 \Sigma \sigma'_i = \sigma_1 \sigma'_n \quad , \quad \sigma'_1 \Sigma \sigma_i = 0$$

$$P(X) \geq \sigma_1 \sigma'_n$$

Et d'après 4.3., on a :

$$P(X) \geq S_n^{1,1}(x_1, x_2, \ldots, x_n)$$

ainsi on a obtenu une fonction qui peut s'écrire sous la forme (I).

Les bases premières de la fonction sont :

$$p(X) + \lambda x_i$$

où p(X) est une base première de la fonction $S_n^{1,1}(X)$.

3) Construire une fonction qui admette exactement 3 bases premières sous formes:

$$I \quad \begin{cases} P(X) + \lambda x \\ P(X) + \lambda y \\ P(X) + \lambda z \end{cases}$$

on a :

$$P(X) \geq (x \oplus y) + (x \oplus z) = \text{fonction ceinture du cube}$$

La fonction ceinture du cube admettant 5 bases premières, la fonction $x \oplus y + x \oplus z + \lambda x$ admet 15 bases premières.

Par conséquent, il n'existe pas de fonction qui admette exactement 3 bases premières sous formes (I).

4) Construire une fonction qui admette exactement 3 bases premières sous formes :

$$\mathrm{I} \quad \begin{cases} P(X) + \lambda xy \\ P(X) + \lambda yz \\ P(X) + \lambda zx \end{cases}$$

on a :

$$P(X) \geq x'yz + xy'z + xyz'$$

La fonction ci-dessus a une seule base première.
En remplaçant dans les expressions (I), P(X) par son expression correspondante on obtient exactement 3 bases premières sous formes désirées.

5) Construire une fonction qui peut s'écrire sous les formes :

$$\mathrm{I} \quad \begin{cases} P(X) + \lambda x_1' \, x_2 \\ P(X) + \lambda x_2' \, x_3 \\ \cdots\cdots\cdots\cdots \\ P(X) + \lambda x_n' \, x_1 \end{cases}$$

On a :

$$P(X) \geq S_n^{1,1}(x_1' \, x_2,\ x_2' \, x_3, \ldots,\ x_n' \, x_1)$$

D'autre part :

$$x_1' \, x_2 \oplus x_2' \, x_3 = x_1' \, x_2 + x_2' \, x_3$$

l'intersection étant nulle.

On a donc :

$$S_n^{1,1}(x_1' \, x_2,\ x_2' \, x_3, \ldots,\ x_n' \, x_1) = S_n^{1,1}(X)$$

Comme on a :

$$S_n^{1,1}(X) \quad \geq \quad \lambda \, x_i' \, x_{i+1} \ , \quad \forall \ i \in N$$

une fonction qui puisse s'écrire sous la forme (I) n'existe pas .

4.11. Construction des fonctions qui admettent un nombre donné de bases premières

4.11.1. *Considérons une fonction qui admet n bases premières de la forme:*

(1) $\quad P(X) + \lambda p_j \;, \qquad j \in N$

avec

$$p_j = \prod_{i \neq j} x_i \quad , \qquad i,j \in N$$

D'après le théorème 4.10, on a :

(2) $\quad P(X) = S_n^{1,1}(p_1, p_2,\ldots,p_n)$

D'après la proposition 4.3, la relation (2) devient :

$$P(X) = S_n^{n-1,1}\;(x_1,x_2,\ldots,x_n)$$

Cette dernière fonction a une seule base puisque deux monômes quelconques de la fonction n'ont pas de consensus.

Par conséquent, la fonction en cause a exactement n bases premières.

La fonction peut s'écrire :

$$S_n^{1,n-1}(X) + \lambda\; X^{\cdot}$$

Cette fonction a été étudiée géométriquement au chapitre I.

4.11.2. *Construire une fonction qui admette exactement n bases premiers de la forme* :

$$P(X) + \lambda\; s_j \quad , \qquad j \in N$$

avec :

$$s_j = \sum_{i \neq j} x_i \quad , \qquad i,j \in N$$

on a :

$$P(X) \geq S_n^{1,1}(s_1,s_2,\ldots,s_n)$$

D'après la proposition 4.3., on a :

$$P(X) \geq S_n^{1,n-1}(X)$$

La fonction $S_n^{1,n-1}(X)$ a une seule base. La fonction en question a donc exactement n bases premières. Elle peut s'écrire :

$$S_n^{1,n-1}(X) + \lambda \Sigma x_i$$

Exemple :

$$ab'c'd' + a'bc'd' + a'b'cd' + a'b'c'd + \lambda(a+b+c+d)$$

4.11.3. Construire une fonction qui admette exactement p^q bases premières

Nous construisons d'après 4.11.1. la fonction

$$S_p^{1,p-1}(X) + \lambda X^{\cdot}$$

qui admet exactement p bases premières. Ensuites nous remplaçons λ par la somme de q variables $\lambda_1, \lambda_2, \ldots, \lambda_q$. La fonction obtenue

$$S_p^{1,p-1}(X) + \lambda_1 X^{\cdot} + \lambda_2 X^{\cdot} + \ldots + \lambda_q X^{\cdot}$$

a exactement p^q bases premières, puisque les bases premières de la fonction ci-dessus s'obtiennent en combinant linéairement les bases premières des fonctions :

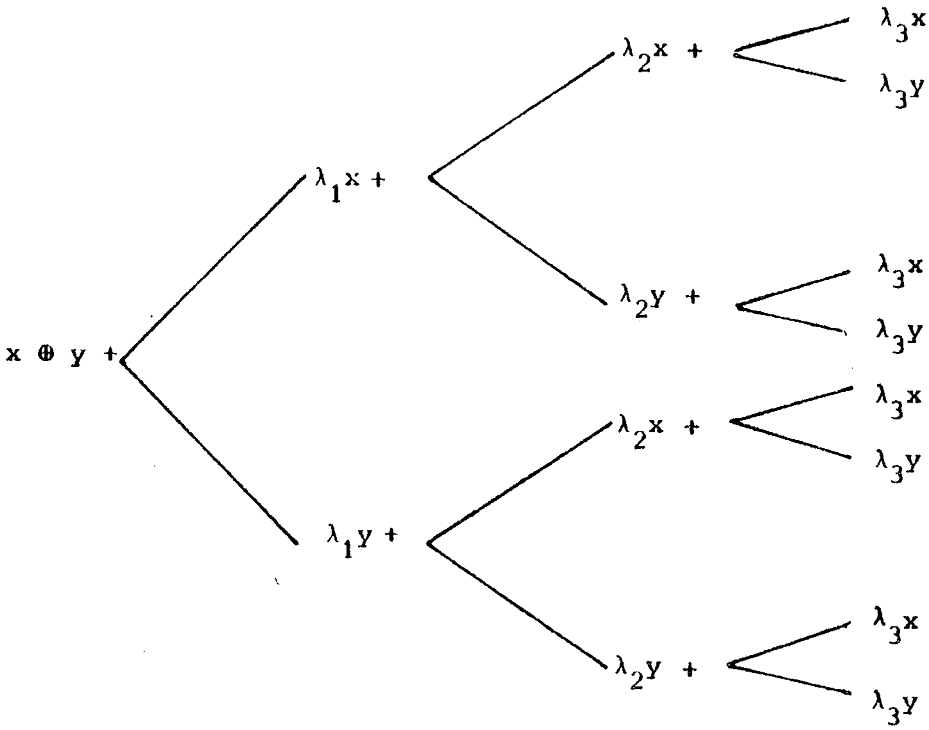
$$S_p^{1,p-1}(X) + \lambda_i X^{\cdot} , \qquad 1 \leq i \leq q$$

Exemple :

La fonction :

$$x \oplus y + (\lambda_1 + \lambda_2 + \lambda_3)\ x\ y$$

a 8 bases premières :


$x \oplus y +$
$\lambda_1 x +$
$\lambda_1 y +$
$\lambda_2 x +$
$\lambda_2 y +$
$\lambda_2 x +$
$\lambda_2 y +$
$\lambda_3 x$
$\lambda_3 y$
$\lambda_3 x$
$\lambda_3 y$
$\lambda_3 x$
$\lambda_3 y$
$\lambda_3 x$
$\lambda_3 y$

4.12. Construction d'une fonction qui peut s'écrire sous les formes

$$P(X) + \sum_i \lambda_i\, g_{ij} \quad , \qquad 1 \le i \le k, \quad 1 \le j \le \ell$$

4.12.1. Théorème. La condition nécessaire et suffisante pour qu'il existe une fonction booléenne qui ait k variables monoformes $\lambda_1, \lambda_2, \ldots \lambda_k$ et qui puisse s'écrire sous les formes :

$$P(X) + \sum_i \lambda_i G_i(X)$$

où $G_i(X) = \{g_{i1}(X), g_{i2}(X), \ldots, g_{ij}(X)\}$ est une fonction générale donnée, est qu'elle soit de la forme :

$$P(X) + \sum_{i=1}^{i=k} \lambda_i\, Q_i(Y)$$

où

$$\begin{cases} P(X) \ge \sum_{i=1}^{i=k} S_n^{1,1}\,(G_i(X)) \\ \text{et} \\ Q_i(Y) \text{ est une fonction croissante quelconque, } \underline{Y} \text{ étant} \\ \text{une partie non vide de } G_i(X) \end{cases}$$

Pour démonstration on utilise le théorème 4.7.2 et 4.10.

Exemple :

1) Construire une fonction qui admet des bases premières de la forme :

$$(I) \quad \begin{cases} P(X) + \lambda\, x_1 + \mu\, x'_1 \\ P(X) + \lambda\, x_2 + \mu\, x'_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ P(X) + \lambda\, x_n + \mu\, x'_n \end{cases}$$

on a :

$P(X) \ge S_n^{1,1}(X) + S_n^{1,1}(X') = S_n^{1,1}(X)$ (fonction paire)

La fonction cherchée est pour $P(X) = S_n^{1,1}(X)$:

$$(1) \qquad S_n^{1,1}(X) + \lambda\, Q_1(X) + \mu\, Q_2(X)$$

où $Q_1(X)$ et $Q_2(X)$ sont deux fonctions respectivement croissante et décroissante par rapport à X.

Les bases premières de la fonction (1) sont :

$$p(X) + \lambda x_i + \mu\, x'_j \quad , \qquad i,j \in \{1,2,\ldots,n\}$$

où $p(X)$ est une base première de la fonction $S_n^{1,1}(X)$

4.12.2. *Problème*

Deux fonctions $f(X)$ et $g(X)$ sont données. Ecrire la fonction $g(X)$ sous forme d'une fonction croissante $C(g_1(X), g_2(X),\dots,g_p(X))$, les fonctions $g_i(X)$ et le nombre p sont inconnus, tel que

$$S_p^{1,1}(g_1(X), g_2(X),\dots,g_p(X)) = f(X)$$

On introduit une nouvelle variable λ et on forme la fonction $f(X) + \lambda q(X)$ et on calcule les bases premières de cette dernière fonction :

$$p(X) + \lambda\, g_i(X), \qquad 1 \leq i \leq p$$

où $p(X)$ est une somme minimale de $f(X)$.

On obtient ainsi la fonction $g_i(X)$ et le nombre p.
Pour chercher l'expression de la fonction croissante C, on peut utiliser la méthode des coefficients indéterminés.

Exemple 1 :

$$\begin{cases} f = x'yz + xy' + x'z \\ y = xyz \end{cases}$$

on obtient après calcul :

$$g_1(X) = x \quad , \qquad g_2(X) = yz \quad , \ p = z$$

La fonction croissante en $g_1(X)$ et $g_2(X)$ est $g_1(X)\ g_2(X)$

Exemple 2 :

$$\begin{cases} f = xz' + x'y + x'zt + xt' \\ q = x + y + zt \end{cases}$$

On obtient après calcul :

$$g_1(X) = x \quad , \qquad g_2(X) = y \quad , \ q_3(X) = zt \quad , \ p = z$$

La fonction croissante par rapport à $g_1(X)$, $g_2(X)$ et $g_3(X)$ est

$$q_1 + q_2 + g_3$$

CHAPITRE V

FONCTIONS EXCENTRIQUES

FONCTIONS EXCENTRIQUES

On étudie ici des fonctions pour lesquelles il n'existe pas de base avec à la fois m minimum et ℓ minimum.

Nous considérerons des fonctions soit complète, soit ϕ-booléenne.

5.1. Définition

Une fonction booléenne est dite <u>excentrique</u> s'il n'existe pas pour cette fonction de base qui ait à la fois :

- un nombre minimum de monômes,
- un nombre miminum de lettres.

5.2. Exemples

1) Dans les réseaux de diodes on utilise comme fonction coût la quantité :

$$\ell + m$$

Si une fonction booléenne à n (n > 1) base pour lesquelles ℓ+ m a la même valeur, cette fonction est excentrique.
En effet, le minimum de ℓ correspond au maximum de m et inversement.

2) Quelle est la fonction booléenne excentrique la plus simple ?

a) La fonction ϕ-booléenne excentrique la plus simple est la suivante :

$$x_1\ x_2\ x_3(y_1+y_2) + \phi\,(x_1x_2x_3 + y_1 + y_2)$$

Elle admet deux bases premières :

$$x_1\ x_2\ x_3$$

$$y_1 + y_2$$

b) La fonction booléenne excentrique la plus simple est :

$$x_1x_2x_3y_1'y_2' + x_1'y_1 + x_2'y_1 + x_3'y_1 + x_4'y_1 + x_1'y_2 + x_2'y_2 + x_3'y_2 + \\ + x_4'y_2 + \lambda x_1x_2x_3x_4 + \lambda y_1 + \lambda y_2$$

dont les bases premières sont formées des termes sans λ auxquels on a ajouté :

- soit $\lambda x_1x_2x_3x_4$
- soit $\lambda y_1 + \lambda y_2$

5.3. Construction des fonctions excentriques

Nous venons de présenter les fonctions booléennes excentriques les plus simples. Nous allons construire d'autres fonctions booléennes excentriques.

5.3.1. *Construction des fonctions ϕ-booléennes excentriques*

5.3.1.1. *Exemple de DAVID* [7] Supposons la fonction ϕ-booléenne de six variables f(A,B,C,D,E,F) représentée par les tableaux de la figure (1).

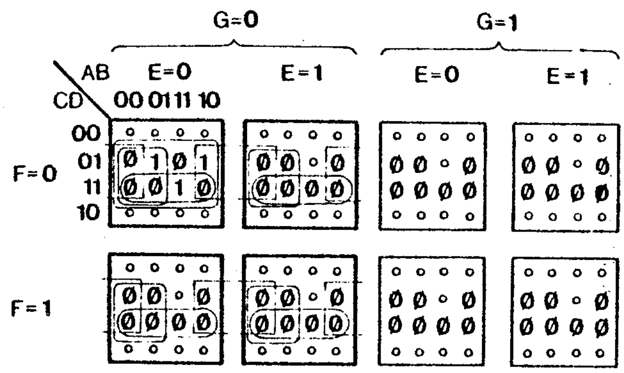


Figure 1

Sur la figure les monômes premiers de la fonction f(A,B,C,D,E,F) sont entourés.

Tous les monômes de la fonction f comportant la variable D, nous posons :

$$f = Dk$$

La fonction k, admet la borne supérieure et la borne inférieure suivantes :

$$\overline{k} = A' + B' + C + E'\ F'$$

$$\underline{k} = E'F'\ (A'BC' + ABC + A\ B'C')$$

Les monômes premiers de k sont A',B', C et E'F'. Ils sont tous couvrants. La fonction k a deux bornes premières suivantes :

$$A' + B' + C$$
$$E'F'$$

En remplaçant E' par $E_1' \cdot E_2' \ldots E_p'$, $p \geq 3$, on obtient une fonction excentrique.

<u>Remarque</u> : On peut obtenir le résultat ci-dessus en utilisant le théorème 3.8.1.

Soit la fonction ϕ-booléenne

$$xy + \phi(x+y)$$

Elle admet les deux bases premières :

$$x \quad \text{et} \quad y$$

à la base x nous attribuons le monal $A' + B' + C$

à la base y nous attribuons le monôme $E_1'\ E_2' \ldots E_p'\ F$, $p \geq 3$

(voir 5.2, exemple 2.a)

5.3.1.2. *Deuxième construction*

Soit la fonction ϕ-booléenne :

(1) $$f = f_2 + \phi\ f_1$$

avec

$$f_1 = ux + u'vy + v'z$$
$$f_2 = vxy + u'yz$$

Chacun des monômes figurant dans f_2 s'obtient par l'opération consensus, à partir de deux monômes figurant dans f_1. On a donc :

$$f_1 \geq f_2$$

La fonction f admet les 4 bases premières suivantes :

$vxy + u'yz$

$u'vy + v'z + vxy$

$ux + u'vy + u'yz$

$ux + u'vy + v'z$

En prenant :

$$x = x_1\, x_2 \ldots x_p$$
$$y = y_1\, y_2 \ldots y_p \quad , \qquad p > 2$$
$$z = z_1\, z_2 \ldots z_p$$

On obtient une nouvelle fonction ϕ-booléenne F à 4 bases premières : L'opération consensus sur les monômes de $\overline{f} = f_1$ porte sur les deux variables u et v tandis que les changements de variables portent sur les variables x, y et z. Par conséquent ces changements de variables ne peuvent pas créer de bases nouvelles.

Les bases nouvelles ont pour modèles :

(1) $(2,\ 2 + 4\ p)$

(2) $(3,\ 4 + 4\ p)$

(3) $(3,\ 4 + 4\ p)$

(4) $(3,\ 4 + 3\ p)$

pour $p > 2$ on a $2 + 4p > 4 + 3p$. La fonction F est donc excent que

5.3.1.3. *Troisième construction*

Nous considérons la fonction ϕ-booléenne :

$$f = \prod_{i=1}^{i=n} x_i + \phi \sum_{i=1}^{i=n} x_i$$

qui admet n bases premières $x_1, x_2, \ldots, x_n$ (voir le théorème 3.8.1.).

Nous remplaçons x_i par un polynôme à i monômes et ℓ_i lettres toutes différentes tel que :

(1) $\ell_{i+1} < \ell_i \quad , 1 \leq i \leq n-1$

les variables sont toutes différentes.

Nous substituons dans f, les variables x_i par leur polynômes correspondants, nous obtenons une fonction nouvelle F.

Toutes les variables de la fonction F étant monoforme, elle admet exactement n bases premières (pas de création de nouvelles bases)

Par suite des inégalités (1) la fonction F est excentrique.

5.3.2. *Construction des fonctions booléennes complètes excentriques*

5.3.2.1. *Exemple de DAVID* [7]

On construit à partir de la fonction ϕ-booléenne 5.3.3.1, une fonction booléenne excentrique. Pour cela, on ajoute une dimension X à la variable d'entrée. La fonction obtenue est 1 sur tous les points où k valait ϕ et sur ceux qui en sont déduit par translation (fig. 2).

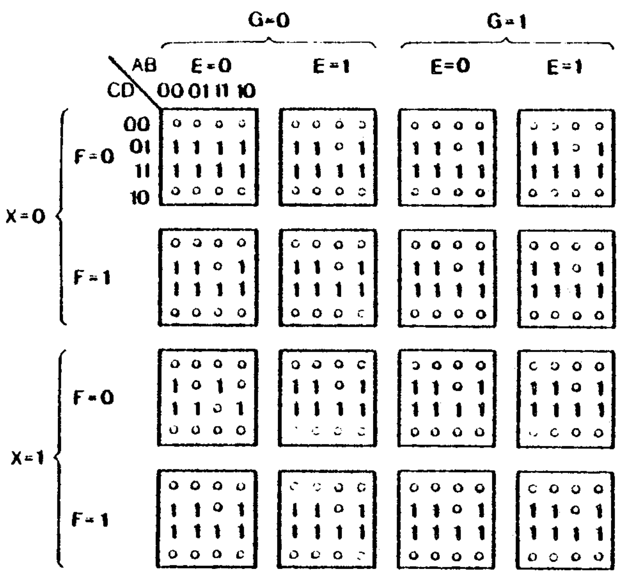


Figure 2

Soit ℓ la fonction représentée sur la figure suivante (les tableaux des deux colonnes de gauche de la figure ci-dessous).

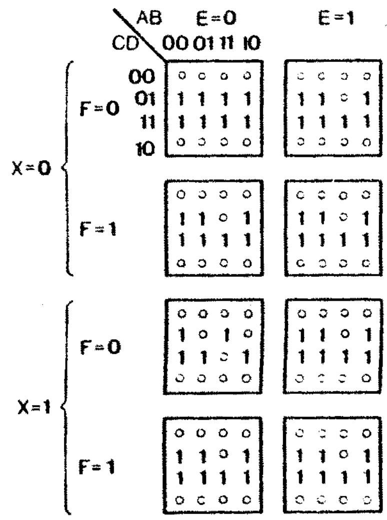


Figure 3.

Tous les monômes de la fonction ℓ comportant la variable D, nous posons :

$$\ell = Dh$$

on a :

$$h = x'\ \overline{k} + x\ \overline{k}(\underline{k})'$$

ou :

$$h = x'\ \overline{k} + \overline{k}(\underline{k})'$$

(la fonction k est définie en 5.3.1.1.)

En utilisant le théorème des monômes premiers [16], on obtient facilement les monômes premiers de la fonction $\overline{k}(\underline{k})'$ à savoir :

$abc'e'f'$, $a'b'$, $a'c$, $a'e$, $a'f$, $b'c$, $b'e$, $b'f$, ce, cf,

on a :

$a'b' + a'c + b'c \leq abc'e'f' + a'e + a'f + b'e + b'f + ce + cf$

on a donc :

$K = \overline{k}(\underline{k})' = abc'e'f' + a'e + a'f + b'e + b'f + ce + cf$

La fonction h admet les deux bases premières :

$$\begin{cases} K + x'(a'+b'+c) \\ K + x'e'f' \end{cases}$$

En prenant :

$$e' = e'_1 \, e'_2 \dots e'_q$$

on obtient une nouvelle fonction :

$$h_1 = K(a,b,c,e_1,e_2,\dots,e_q,f) + x'(a'+b'+c)$$

La fonction $K(a,b,c,e_1,e_2,\dots,e_q,f)$ a une seule base première puisque deux monômes de $K(a,b,c,e_1,e_2,\dots,e_q,f)$ n'ont pas de consensus. L'opération de consensus entre $K(a,b,c,e_1,e_2,\dots,e_q,f)$ et $x'(a'+b'+c)$ donne le monôme premier $x' \, e'_1 \, e'_2 \dots e'_q$, la fonction h_1 a donc deux bases premières suivantes :

$$K(a,b,c,e_1,e_2,\dots,e_q,f) + x'(a'+b'+c)$$

$$K(a,b,c,e_1,e_2,\dots,e_q,f) + x' \, e'_1 \, e'_2 \dots e'_q \, f$$

(pas de création de bases premières nouvelles).

En prenant $q \geq 5$ la fonction h_1 devient excentrique.

Remarque : On peut obtenir le résultat ci-dessus en utilisant le théorème 4.9.

Cherchons une fonction qui admet exactement deux bases premières de la forme :

$$P(u,v) + \lambda u$$

$$P(u,v) + \lambda v$$

s'il existe une telle fonction, on doit avoir :

$$P(u,v) = uv' + u'v$$

La fonction cherchée est :

$$f(u,v,\lambda) = uv' + u'v + \lambda Q(u,v)$$

où

$$Q(u,v) = u \,/\, v \,/\, u + v \,/\, u \,.\, v$$

La fonction $f(u,v,\lambda)$ a 4 monômes premiers uv', $u'v$, λu, λv et deux bases premières :

$$uv' + u'v + \lambda u$$

$$uv' + u'v + \lambda v$$

En prenant

$$u = a' + b' + c$$
$$v = E'_1\ E'_2\ \ldots\ E'_q \qquad q \geq 5$$
$$\lambda = x'$$

dans la fonction $f(u,v,\lambda)$ on obtient la fonction excentrique étudiée ci-dessus.
(voir 5.2., exemple 2.b)

5.3.2.2. *Deuxième construction*

La fonction génératrice de fonctions excentriques de la forme :

$$a_0 \oplus a_1 + a_0\ a_1\ f(X)$$

Considérons la fonction :

$$F(a_0,a_1,X) = a_0 \oplus a_1 + a_0\ a_1\ f(X)$$

où a_0 et a_1 sont deux variables booléennes et la fonction $f(X)$ a une base première à p monômes donnés.
La fonction $F(a_0,a_1,X)$ a 2^p bases, toutes de même modèle.

Prenons pour $f(X)$ la clé de parité à n variables dont les monômes premiers sont notés $m_1, m_2,\ldots,m_{2^{n-1}}$.
La fonction F a dans ce cas $2^{2^{n-1}}$ bases de la forme

$$a_0 \oplus a_1 + b_i \qquad 1 \leq i \leq 2^{2^{n-1}}$$

où b_i est l'expression qui figure sur la $i^{\text{ème}}$ ligne d'une matrice colonne qui s'obtient en faisant le produit matriciel A.M avec :

$$A = \left\| \begin{matrix} \overbrace{a_0 \; \cdot \; \cdot \; a_0 \; a_0 \; a_0}^{2^{n-1}} \\ a_0 \; \cdot \; \cdot \; a_0 \; a_0 \; a_1 \\ a_0 \; \cdot \; \cdot \; a_0 \; a_1 \; a_0 \\ a_0 \; \cdot \; \cdot \; a_0 \; a_1 \; a_1 \\ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ a_1 \; \cdot \; \cdot \; a_1 \; a_1 \; a_1 \end{matrix} \right\| \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \\ a \\ a \\ a \\ a \end{matrix}}\right\} 2^{2^{n-1}} \quad , \quad M = \left\| \begin{matrix} m_1 \\ m_2 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ m_{2^{n-1}} \end{matrix} \right\|$$

Les indices «0» et «1» des a représentent les nombres 0,1,2,... ..., $2^{2^{n-1}}-1$ dans la numérotation binaire.

<u>Théorème</u> : Les points du spectre de la fonction :

$$F(a_0,a_1,X) = a_0 \oplus a_1 + a_0\, a_1\, f(X)$$

où

$$\text{I} \quad \begin{cases} a_0 = u_1\, u_2 \ldots u_p \\ a_1 = v_1 + v_2 + \ldots + v_q \\ f(X) \text{ est la clé de parité} \end{cases}$$

se situent sur une droite de pente $\mu = n + \frac{q-p}{q-1}$

La droite peut être :

1 - ascendante (fig. 4a)

2 - descendante (fonction excentrique) (fig.4b)

3 - horizontale (fig. 4c)

4 - verticale (fig. 4d)

Dans tous les cas, les points du spectre sont équidistants et le spectre est renseigné. Les indices de renseignement sont les coefficients binomiaux.

Sur les figures, l'indice de renseignement de chaque base est écrit à côté du point représentatif de la base correspondante.

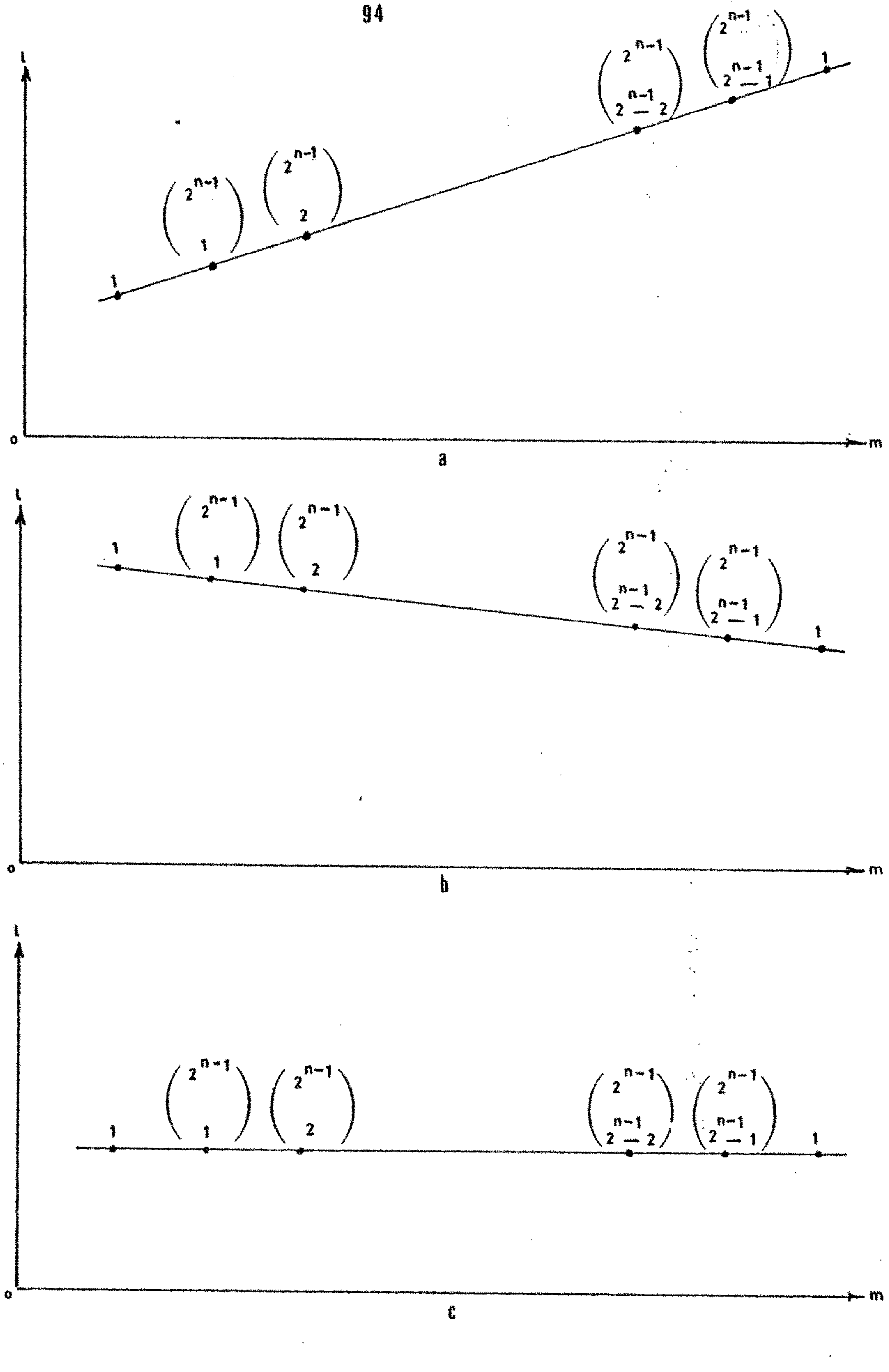


FIG 4

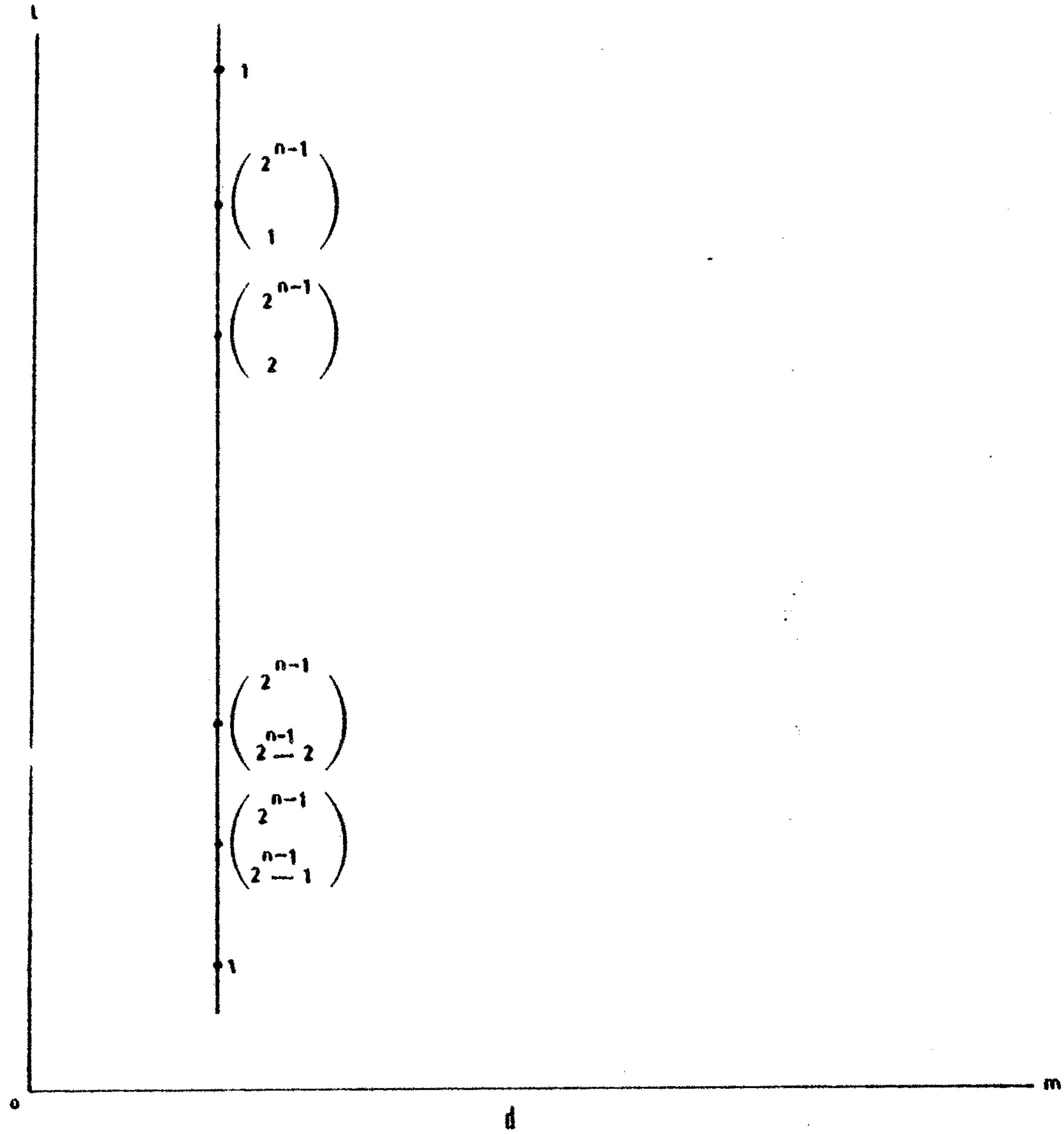


FIG 4

Démonstration

Démontrons d'abord que la fonction G obtenue à partir de la fonction F par la substitution (I) a $2^{2^{n-1}}$ bases premières.

Les monômes premiers de la fonction G sont ceux qui figure dans :

$$u_1 u_2 \dots u_p v'_1 v'_2 \dots v'_q + (u'_1+u'_2+\dots+u'_p)(v_1+v_2+\dots+v_q) + u_1 u_2 \dots u_p f(X) +$$
$$+ (v_1 + v_2 + \dots + v_q) f(X)$$

et les bases premières sont de la forme :

(II) $u_1u_2 \dots u_p v'_1v'_2\dots v'_q + (u'_1+u'_2+\dots+u'_p)(v_1+v_2+\dots+v_q)+\Sigma k_i m_i$

où

$$\begin{cases} m_i \text{ est un monôme premier de } f(X) \\ k_i = u_1\, u_2 \ldots u_p \quad \text{ou} \quad v_1 + v_2 + \ldots + v_q \end{cases}$$

La partie non changeante de l'expression (II) a une seule base première puisqu'il n'y a pas de consensus entre deux monômes de l'expression. La fonction $f(X)$ a 2^{n-1} monômes premiers, par suite la fonction G a $2^{2^{n-1}}$ bases premières.

Les bases premières de la fonction $F(a_0, a_1, X)$ comportent une expressio fixe $a_0 \oplus a_1$ et une expression changeante b_i, $1 \le i \le 2^{2^{n-1}}$. Soit E l'ensemble des expressions changeantes. Considérons l'expression b_1 :

$$b_1 = u_1\, u_2 \ldots u_p\, m_1 + u_1\, u_2 \ldots u_p\, m_2 + \ldots + u_1\, u_2 \ldots u_p\, m_{2^{n-1}}$$

Remplaçons dans k monômes premiers de b_1, le produit $u_1\, u_2 \ldots u_p$ par la somme $v_1 + v_2 + \ldots + v_q$, nous obtenons une expression changeante appartenant à E. Il y a $C^k_{2^{n-1}}$ expressions changeantes de ce genre don les bases correspondantes ont le même modèle (m_k, ℓ_k) tel que :

$$\text{III} \quad \begin{cases} m_k = 2^{n-1} - k + kq + m \\ \ell_k = 2^{n-1}\ (p+n) - k(p+n) + k(q(n+1)) + \ell \end{cases}$$

où (m, ℓ) est le modèle de l'expression irréductible

$u_1\, u_2 \ldots u_p \oplus (v_1 + v_2 + \ldots + v_q)$

Pour les bases de modèle (m_{k+1}, ℓ_{k+1}) obtenue à partir de l'expression b_1, par l'opération ci-dessus, on a :

$$\text{IV} \quad \begin{cases} m_{k+1} = 2^{n-1} - (k+1) + (k+1)q + m \\ \ell_{k+1} = 2^{n-1}\ (p+n) - (k+1)\ (p+n) + (k+1)\ (q(n+1)) + \ell \end{cases}$$

on a donc :

$$\begin{cases} m_{k+1} - m_k = q-1 \\ \ell_{k+1} - \ell_k = -(p+n) + q(n+1) \end{cases}$$

Comme les deux expressions q-1 et (n+1) q-(n+p) sont indépendant de k, par conséquent le support des points du spectre est une droite.

La continuation de la démonstration est immédiate.

Remarque. Pour $f(X) = x$ la fonction étudiée ci-dessus prend la forme

$a_0 \oplus a_1 + a_0 \, a_1 x$ étudiée précédemment.

5.3.2.3. *Troisième construction*

La fonction

$$(1) \qquad P(X) + \lambda Q(X)$$

avec :

$$\begin{cases} P(X) = uxy' + uv'x + v'y'z + u'vy + u'vx'yz' \\ Q(X) = ux + u'vy + v'z \end{cases}$$

admet exactement deux bases premières :

$$\begin{cases} P(X) + \lambda(ux + u'vy + v'z) \\ P(X) + \lambda(vxy + u'yz) \end{cases}$$

(voir 4.9 exemple 4).

En prenant :

$$(2) \begin{cases} x = x_1 \, x_2 \ldots x_p \\ y = y_1 \, y_2 \ldots y_p \\ z = z_1 \, z_2 \ldots z_p \end{cases} \qquad p > 3$$

On obtient une nouvelle fonction F à deux bases premières :

a) Soit $E = \{u,v\}$, $G = \{x,y,z\}$ et $s = m_1 + m_2$ où m_1 et m_2 figurent dans P(X).

- ou m_1 et m_2 n'ont pas de variables biforme pour s.

  exemple : $m_1 = uxy'$, $m_2 = uv'x$; pas de consensus

- ou s'ils ont une variable biforme de E (ou F) pour s, ils ont une variable biforme de F (ou E) ; pas de consensus

b) Soit $P_1(X)$ et $Q_1(X)$ respectivement les expressions obtenues à partir de $P(X)$ et $Q(X)$ après la substitution (2)

D'après (a), deux monômes de $P_1(X)$ n'ont pas de consensus. $P_1(X)$ est donc la seule base première de $P_1(X)$.

Les bases premières de $F = P_1 + \lambda Q_1$ sont de la forme $P_1 + \lambda S$ où S est une somme irréductible des monômes premiers de $P_1 + Q_1 = Q_1$

Comme dans Q(X) le dédoublement des variables se fait sur les variables directes alors les monômes premiers de Q_1 s'obtient à partir des monômes premiers de Q après la substitution (2), il n'y a donc pas de création de bases premières nouvelles.

La fonction F a donc deux bases premières qui s'obtiennent à partir des bases premières de f par la substitution (2)

Les bases premières de la fonction F ont pour modèle

$$(m+3, \ell + 3p + 7) \quad , \quad (m+2, \ell + 4p + 4)$$

(m, ℓ) est supposé le modèle de $P(X)$ après la substitution (2).

Pour $p > 3$ on a $3p + 7 > 4p + 4$

La fonction F est par suite excentrique pour $p > 3$.

CONCLUSION

Les résultats présentés dans cette thèse ne représentent qu'une première exploration d'un domaine assez peu connu.

On peut envisager de les prolonger dans diverses directions ayant à la fois un intérêt théorique et des applications pratiques dans diverses technologies.Par exemple il serait intéressant de savoir :

a) Si parmi les fonctions de n variables, il y a un grand nombre qui sont excentriques ?

b) Si les rapports $\frac{m}{m'}$, $\frac{l}{l'}$ pour la meilleure base en m et la meilleure base en m et la meilleure base en l sont susceptibles de prendre des valeurs très différentes de 1 ?

c) Si les spectres de certaines catégories de fonctions booléennes ont des propriétés particulières ?

Signalons encore à propos de la fonction $f(X) = \Sigma\, \lambda_i\, f_i(X)$ que les bases premières de f s'obtiennent en superposant les bases premières des $\lambda_i\, f_i(X)$. C'est une propriété de "linéarité", ce qui est assez rare en algèbre de Boole pour mériter d'être signalé.

Ce résultat est d'ailleurs assez isolé puisque les bases premières de $f(X) + \lambda g(X)$ obéissent à des règles beaucoup plus compliquées et qui n'en sont pas moins intéressantes (voir 4.12.2).

Ces résultats montrent que la recherche des bases premières des fonctions booléennes à part son intérêt dans le domaine technologique (recherche des expressions de coût minimal) a un intérêt théorique.

BIBLIOGRAPHIE

[1] AURIGNAC R. : "Sur la recherche des bases premières d'une fonction booléenne". C.R Acad.Sc.Paris, t.260, pp.2664-2665, 8 mars 1965.

[2] BENZAKEN C. : "Définition et propriétés de certaines familles de fonctions booléennes croissantes". C.R. Acad. Sc., t.259, pp.1369-1371, 17 août 1964.

[3] BENZAKEN C. : "Algorithme de dualisation d'une fonction booléenne". Chiffre 9 pp.119-128, 1966.

[4] BERGE C. : "Graphes et hypergraphes". Dunod-Paris, 1970.

[5] CARVALO N. : "Monographie des treillis et algèbre de Boole". Gauthier-Villard, 1962.

[6] CARVALO N. : "Principes et applications de l'analyse booléenne". Gauthier-Villard, Paris 1962.

[7] DAVID R. : "Sur l'indépendance de critères de minimisation des fonctions booléennes". Automatisme, tome XVII n°10, octobre 197.

[8] DEBRAINE P. : "Machine de traitement de l'information". Masson et Cie. Paris 1972.

[9] DESCHIZEAUX P. : "Synthèse de fonctions booléennes générales". Thèse Docteur-Ingénieur, Grenoble 1967.

[10] EDWARDS C.R, HURST S.L. : "A digital synthesis procedure under function symmetries and mapping methods". IEEE Trans. on Computers, vol.C.27 n°11, novembre 1978.

[11] FAURE R., DENIS-PAPIN, KAUFMANN N. : "Cours de calcul Booléen". Edition Albin-Michel. Paris 1970.

[12] FAURE R. , HEURGON E. : "Structures ordonnées et algèbre de Boole". Gauthier-Villard, Paris, 1971.

[13] HANSEL G. : "Résultat concernant le nombre minimal de contact nécessaire pour réaliser certaines fonctions booléennes symétriques". C.R. Acad. Sc., t.262, n°12, série A, pp.679-681, mars 1966.

[14] HARRISON M.A : "Introduction to swtiching and automata theory". Mc. Graw-Hill. 1965.

[15] KARNAUGH : "The map method for synthesis of combinational logic circuits". Communications and Electronics, 595-599, Nov. 1953.

[16] KUNTZMANN J. : "Un théorème sur les composants premiers d'une fonction booléenne et ses applications". Automatisme, p.18, Janvier 1964.

[17] KUNTZMANN J. : "Algèbre de Boole". Dunod, Paris, 1968.

[18] KUNTZMANN J., NASLIN P. : "Algèbre de Boole et machines logiques". Actes du Colloque Algèbre de Boole, Grenoble, 11-17 janvier 1965, Dunod, Paris 1967.

[19] KUNTZMANN J. : "Théorie des réseaux graphes". Dunod, Paris 1972.

[20] LAPSCHER F. : "Ensembles ordonnés et algèbre de Boole". Cours, Université Montpellier II, 1976.

[21] Mc CLUSKEY E.J. : "Minimization of boolean functions". Bell System Tech. J.35, pp.1417-1444, 1956.

[22] MENDELSON E. : "Boolean Algebra and switching circuits". Mc Graw-Hill 1976.

[23] MORRIS N.M. : "Circuits logiques". Masson, Paris 1971. Traduit en français par Lyon-Caen G.

[24] NASLIN P. : "Circuits logiques et automatiques à séquences". Dunod Paris, 3è édition 1976.

[25] NASLIN P. : "Note sur la simplification des fonctions logiques". Automatisme, Tome VII n°11, novembre 1962.

[26] PAPAKONSTANTINOU : "Minimization of modulo-2 sum of products". IEEE Transactions on Computers, vol.C-28, n°2, February 1979.

[27] PARODI M. : "Application de l'algèbre moderne à quelques problèmes de physique classique" (Chapitre II). Gauthier-Villard et Cie, Paris 1961.

[28] PERRIN J.P, DENOUETTE M., DACLIN E. : "Systèmes logiques" Dunod Paris 1967.

29 PICHAT E. : "Amélioration de l'algorithme de Mc Cluskey-Harrison pour calculer les monômes premiers d'une fonction booléenne". Automatisme, Tome XIX n°5, mai 1974.

30 PINTER C. : "Sur l'obtention des formes minimales des fonctions booléennes conjonctives". Thèse, Paris.

31 QUINE W.V. : "The problem of simplifying truth function". Amer. Math. Monthly, vol.59, pp.521-531, Octobre 1952.

32 RHYNE V.T., NOE P.S., Mc Kineey M.H., POOCH U.V. : "A new technique for fast minimization of switching functions". IEEE Transactions on Computers, vol.C-26, n°8, August 1977.

33 SAILLARD J.C. : "Etudes des formes lexicographiques des fonctions simples". Représentation à l'aide de l'opérateur u. Thèse Docteur 3è cycle, Grenoble 1968.

34 SORECHANDER : "Minimization of switching functions - A fast technique" IEEE Transactions on Computers, July 1975.

35 TISON P. : "Algèbre booléenne : théorie des consensus. Recherche des bases premières d'une fonction booléenne". Automatisme t.X, pp.229-234, juin 1965.

36 TISON P. : "Théorie des consensus". Thèse Docteur-Ingénieur, Grenoble 1965.

37 TISON P. : "Generalization of consensus theory and application to the minimization of Boolean functions". IEEE Transaction, EC-16, n°4, pp.4446-456, 1967.

38 VEITCH : "A chart method for symplifying truth function". Proc., Assoc. for Computing machinery Conf. pp.127-133, mai 1952.