REVUE FRANÇAISE D'AUTOMATIQUE INFORMATIQUE RECHERCHE OPÉRATIONNELLE. MATHÉMATIQUE

C. PAYAN

Type et graphe des distances d'une fonction booléenne

Revue française d'automatique informatique recherche opérationnelle. Mathématique, tome 6, n° R1 (1972), p. 3-14

<http://www.numdam.org/item?id=M2AN_1972__6_1_3_0>

R.A.I.R.O.
(6e année, R-1, 1972, p. 3-14)

TYPE ET GRAPHE DES DISTANCES D'UNE FONCTION BOOLEENNE

par C. PAYAN [1]

Résumé. — *On recherche dans cet article, les fonctions booléennes dont le type est caractérisé par le graphe des distances (graphe construit à partir de la fonction booléenne représentée sous forme normale disjonctive, à l'aide des distances de Hamming).*

C'est le cas des fonctions booléennes connexes (Théorème 1).

Ce résultat s'étend aux fonctions booléennes dont l'enveloppe est connexe (Théorème 2).

(L'enveloppe d'une fonction F est la plus petite fonction supérieure à F dont toutes les composantes connexes sont des cubes.)

On démontre pour terminer que le type de toute fonction booléenne est caractérisé par le graphe des distances de cette fonction et celui de la fonction complémentaire (Théorème 3).

Les fonctions booléennes seront représentées sous forme normale disjonctive.

I. DEFINITIONS

1-1. Distance

On appelle *distance* entre deux monômes canoniques le nombre de variables différentes, c'est-à-dire non complémentées dans l'un et complémentées dans l'autre ou inversement.

C'est la distance de Hamming.

1-2. Graphe des distances d'une fonction booléenne

C'est le graphe complet étiqueté défini de la façon suivante :

A chaque monôme canonique, m_i, de la fonction on fait correspondre un sommet, (m_i) du graphe.

Deux sommets quelconques sont reliés par une arête qui porte la distance entre les deux monômes représentés par ces deux sommets.

(1) Mathématiques appliquées, Informatique, Université de Grenoble.

Notation : Le graphe des distances d'une fonction booléenne F sera noté (F).

EXEMPLE : $F = x\bar{y}z + xyz + \bar{x}y\bar{z} + x\bar{y}\bar{z}$ ($\bar{x}$ désigne le complément de x).

(F)·

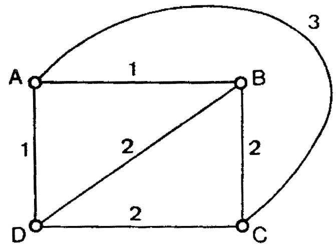


Figure 1

1-3. Graphe des distances k

C'est le graphe partiel obtenu en ne conservant que les arêtes qui portent la distance k.

1-4. Connexité

Une fonction booléenne est dite *connexe* si et seulement si son graphe des *distances-1* est connexe.

1-5. Fonctions booléennes de même type

Deux fonctions booléennes sont dites de *même type* si et seulement si on peut passer de l'une à l'autre par une bijection T de l'ensemble des variables et des variables complémentées de l'une sur l'ensemble des variables et des variables complémentées de l'autre, telle que $T(\bar{x}) = \overline{T(x)}$.

1-6. Fonctions booléennes de même type homogène [1]

Soient deux fonctions booléennes F_1 et F_2 ayant des graphes de distances (F_1) et (F_2) isomorphes.

Nous dirons que F_1 et F_2 sont de *même type homogène* si et seulement si à tout isomorphisme S de (F_1) sur (F_2) on peut associer une transformation T qui fait passer de F_1 à F_2 telle que

$$(m_2) = S[(m_1)] \Leftrightarrow m_2 = T[m_1]$$

(m_1 et m_2 sont des monômes canoniques. (m_1) et (m_2) les points associés du graphe).

(1) REMARQUE : Ceci est bien une *propriété du type.*
En effet, si à l'intérieur d'un type, 2 fonctions sont de « même type homogène », toutes les fonctions du type sont de « même type homogène ».
La démonstration est immédiate.

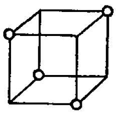
II. PROBLEME

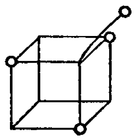
On sait que deux fonctions booléennes de même type ont des graphes de distances isomorphes.

Réciproquement, deux fonctions booléennes ayant des graphes de distances isomorphes sont-elles de même type?

Cette propriété est fausse dans le cas général comme le montrent les deux exemples suivants ·

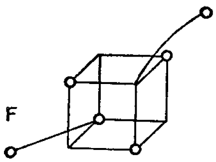
1.

F 

G 

$(xyz\bar{t} + xy\bar{z}t + x\bar{y}zt + x\bar{y}\bar{z}\bar{t})$ $(xyz\bar{t} + xy\bar{z}t + x\bar{y}zt + \bar{x}yzt)$

2

F 

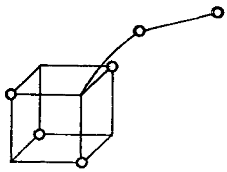
G 

Figure 2

[Dans ce deuxième exemple les cubes circonscrits à F' et à G' sont de même dimension (5) — dimension minimum étant donnés les graphes de distances (F') et (G').]

Nous allons voir que *pour certaines classes de fonctions le graphe des distances caractérise le type*

Nous ne considérerons dans ce qui suit que des fonctions ayant même nombre de variables

III. THEOREME I

« Deux fonctions booléennes *connexes*, dont les graphes des distances sont isomorphes, sont de même type homogène »

Démonstration

La démonstration se fait par récurrence sur le nombre des monômes canoniques.

La propriété est vraie pour les fonctions ayant un monôme canonique.

Supposons la vraie pour toute fonction booléenne connexe ayant $n - 1$ monômes canoniques.

Soient F_1 et F_2, 2 fonctions booléennes connexes de n monômes canoniques dont les graphes de distance sont isomorphes.

(Nous utiliserons dans la démonstration la même notation pour les monômes canoniques et les sommets correspondants du graphe des distances.) Il existe un monôme canonique $A_1 \in F_1$, tel que $f_1 = F_1 - A_1$ soit connexe.

Soit $A_2 \in F_2$, « isomorphe » de A_1.

Soit $f_2 = F_2 - A_2$.

Les graphes des distances de f_1 et f_2 sont isomorphes.

f_2 est donc connexe

f_1 et f_2 ont $n - 1$ monômes canoniques.

$\exists B_1 \in f_1$ et $B_2 \in f_2$ tels que :

— distance $(A_1, B_1) =$ distance $(A_2, B_2) = 1$

— B_1 et B_2 soient isomorphes.

Soit T_1 la transformation : $f_1 \to f_2$
telle que $B_2 = T_1(B_1)$

Soit $F_1' = T_1(F_1)$.

Soit $A_1' = T_1(A_1)$.

On a : distance $(A_1', B_2) =$ distance $(A_1, B_1) = 1$

F_1' et F_2 ont $n - 1$ monômes canoniques communs (la fonction f_2).

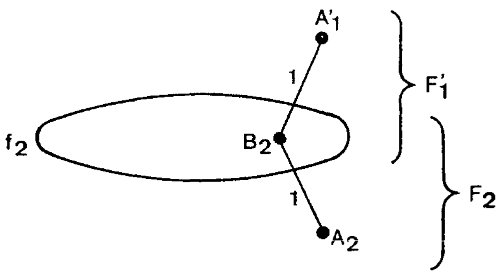


Figure 3

Distance $(A_1', A_2) =$ soit 0 (dans ce cas le problème est résolu)
$=$ soit 2

Soit, dans ce dernier cas, x_i et xj les 2 variables qui sont différentes pour A_1' et A_2.

Les monômes A_1' et A_2, sont de la forme :

$$A_1' : \tilde{x}_1, \tilde{x}_2, \ldots \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots \tilde{x}_{j-1}, \tilde{x}_{j+1}, \ldots \tilde{x}_p, \qquad \tilde{x}_i, \tilde{x}_j$$

$$A_2 : \tilde{x}_1 \text{ -------------------------------- } \tilde{x}_p, \qquad \bar{\tilde{x}}_i, \bar{\tilde{x}}_j$$

($\tilde{x}_k$ représente soit x_k soit $\bar{x}_k$)

Par exemple :

$$A_1' : 0, 0, 0, \ldots\ldots\ldots 0 \quad , \quad 0, 0$$

$$A_2 : 0, 0, 0, \ldots\ldots\ldots 0 \quad , \quad 1, 1$$

Les $n - 1$ monômes de f_2 communs à F_1' et F_2 sont de la forme :

$$\tilde{\tilde{x}}_1, \tilde{\tilde{x}}_2, \ldots, \tilde{\tilde{x}}_p \quad , \quad \tilde{x}_i, \bar{\tilde{x}}_j$$

ou

$$\tilde{\tilde{x}}_1, \tilde{\tilde{x}}_2, \ldots, \tilde{\tilde{x}}_p \quad , \quad \bar{\tilde{x}}_i, \tilde{x}_j$$

Par exemple :

$$\Phi, \Phi, \ldots\ldots\ldots \Phi, 0, 1$$

$$\Phi, \Phi, \ldots\ldots\ldots \Phi, 1, 0$$

(Ces points sont *équidistants* de A_1', et de A_2)

La transformation :

$$T_2 : \begin{bmatrix} x_i \to \bar{x}_j \\ x_j \to \bar{x}_i \end{bmatrix}$$

transforme A_1' en A_2 et laisse les $n - 1$ points de f_2 invariants.

La transformation $T_2 \circ T_1$ transforme donc F_1 en F_2 et A_1 en son isomorphe A_2.

Lemme 1

« Soient deux fonctions booléennes F et H ayant des graphes de distances isomorphes.

Si les fonctions (F) et (H) obtenues en prenant un point (monôme canonique) par composante connexe dans F et les points isomorphes dans H, sont de même type homogène

alors F et H sont de même type homogène. »

Démonstration analogue à celle du théorème 1 : récurrence sur le nombre de points des composantes connexes.

Corollaire 1

« Deux fonctions booléennes constituées de 1, 2 ou 3 composantes connexes et dont les graphes de distances sont isomorphes, sont de même type homogène.»

Démonstration : Il est facile de vérifier que deux fonctions booléennes réduites à 1, 2 ou 3 points et dont les graphes de distances sont isomorphes sont de même type homogène.

IV. EXTENSION DU THEOREME I

4-1. Définition

a) Enveloppe d'une fonction booléenne F (Notation $\tilde{F}$.):

Soit une fonction F. Son enveloppe $\tilde{F}$ est la fonction obtenue à partir de F par la transformation suivante :

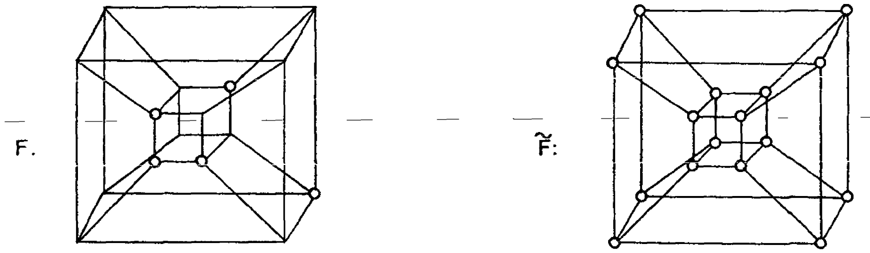
— on remplace chaque composante connexe de F par son *cube circonscrit* (plus petit cube contenant cette composante) :

— on recommence la même opération sur la nouvelle fonction obtenue;

— on continue jusqu'à stabilisation.

Exemple :

F.



$\tilde{F}$:

Figure 4

REMARQUE : L'enveloppe d'une fonction booléenne F est la plus petite fonction supérieure à F dont toutes les composantes connexes sont des cubes.

b) Opération « o »

Soit une fonction F.

F peut se mettre sous la forme : $F = \mathcal{C} \cup P$.

$\mathcal{C}$: Partie connexe de F.

$P = \{ A, B, ..., C \}$ Ensemble de monômes canoniques

On définit : $F^o = \tilde{\mathcal{C}} \cup P$

$\tilde{\mathcal{C}}$: cube circonscrit à $\mathcal{C}$.

REMARQUE : $\tilde{F}$, enveloppe de F peut être obtenue par itération de l'opération « o ».

4-2. Lemme 2

« Soient deux fonctions booléennes $F = \mathcal{C} \cup P$ et $H = \mathcal{C}' \cup P'$, ayant des graphes de distances isomorphes (isomorphisme : S ; $(\mathcal{C}') = S[(\mathcal{C})]$. $(P') = S[(P)]$.

Les fonctions $F^{\circ} = \tilde{\mathcal{C}} \cup P$ et $H^{\circ} = \tilde{\mathcal{C}}' \cup P'$ ont des graphes de distances isomorphes.

($\exists$ un isomorphisme S^{o} de (F^{o}) dans (H^{o}) dont S est une *restriction.*)

Démonstration

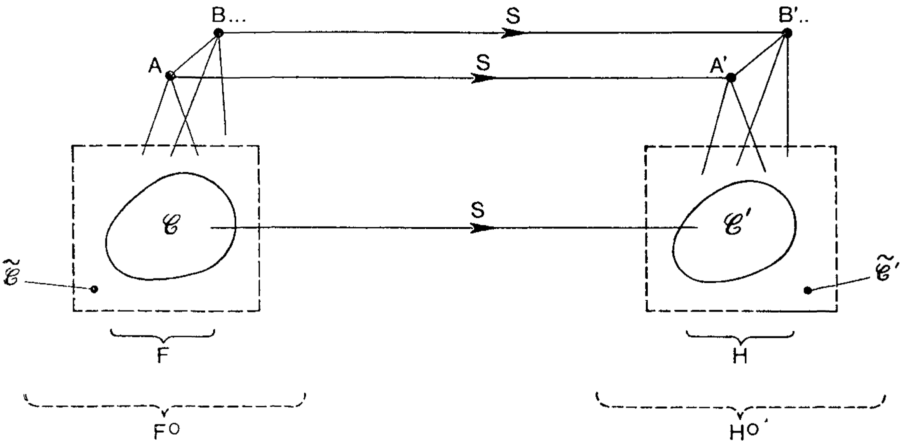


Figure 5

S : isomorphisme de (F) dans (H)

$$\begin{array}{ccc} A & \xrightarrow{S} & A' \\ \vdots & & \vdots \\ B & \xrightarrow{S} & B' \\ \vdots & & \vdots \\ \mathcal{C} & \xrightarrow{S} & \mathcal{C}' \end{array}$$

$\exists S_1$ *isomorphisme* de $\tilde{\mathcal{C}}$ dans $\tilde{\mathcal{C}}'$ tel que : [restriction de S à $\mathcal{C}$ = restriction de S_1 à $\mathcal{C}$.] (Théorème 1).

Soit S^{o} application de (F^{o}) dans (H^{o}) définie par :

$$\forall x \in S \qquad S^{o}(x) = S(x)$$
$$\forall x \in \tilde{\mathcal{C}} \qquad S^{o}(x) = S_1(x)$$

La restriction de S^0 à F est l'isomorphisme S.

Nous allons montrer que S^0 est un *isomorphisme* (c'est-à-dire une application bijective qui conserve les distances).

Conservation des distances

Notation : « Distance (x, y) » sera notée $[x, y]$.

1° $\forall x, y \in F$

$$[S^0(x), S^0(y)] = [S(x), S(y)] = [x, y]$$

2° $\forall x, y \in \tilde{\mathcal{C}}$

$$[S^0(x), S^0(y)] = [S_1(x), S_1(y)] = [x, y]$$

3° — $x \in P$ (par exemple $x = A$)

— $y \in \tilde{\mathcal{C}}$, $y \notin \mathcal{C}$.

La démonstration se fait par récurrence sur la dimension de $\tilde{\mathcal{C}}$.

La propriété est vraie pour $\tilde{\mathcal{C}}$ de dimension 0 (et 1) (dans ce cas $F^0 = F$ d'où $S^0 = S$).

Supposons la vraie pour $\tilde{\mathcal{C}}$ de dimension $n - 1$.

Soit $F = \mathcal{C} \cup P$ et $H = C' \cup P'$.

(F), $(\mathcal{C})$, (P) et (H), $(\mathcal{C}')$, (P') sont respectivement isomorphes.

$\tilde{\mathcal{C}}$ et $\tilde{\mathcal{C}}'$ de dimension n.

$\mathcal{C}$ étant *connexe* on a :

$$\left[\begin{array}{l} \bullet\mathcal{C} = \mathcal{C}_1 \cup x \cup \ldots \mid \tilde{\mathcal{C}}_1 \text{ soit de dimension } n - 1 \\ \bullet\exists x \in \mathcal{C}_1 \mid [x, x_1] = 1 \end{array}\right.$$

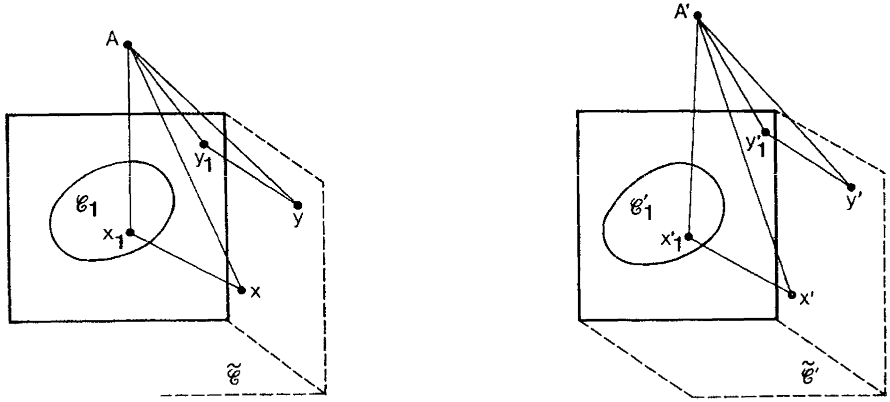


Figure 6

Soit

$$y_1 \in \tilde{\mathcal{C}}_1$$

$$y \in \tilde{\mathcal{C}} \,|\, y \notin \tilde{\mathcal{C}}_1 \text{ et } [y, y_1] = 1$$

(yy_1 parallèle à xx_1)

$$[A, x] = \text{soit } [A, x_1] + 1 \qquad (1^{er} \text{ cas})$$

$$\text{soit } [A, x_1] - 1 \qquad (2^{e} \text{ cas})$$

Dans le 1^{er} cas on a :

$$[A, y] = [A, y_1] + 1$$

$$[A', x'] = [A', x'_1] + 1 \qquad ((F) \text{ et } (H) \text{ isomorphes})$$

D'où $[A', y'] = [A', y'_1] + 1$

Or $[A, y_1] = [A', y'_1]$ (Hypothèse de récurrence)

D'où $[A, y] = [A', y']$

La démonstration est identique dans le 2^e cas.

S^o conserve donc les distances.

C'est donc une application *injective*.

Un raisonnement dans l'autre sens (de H vers F) permettrait de définir une injection de H^o dans F^o.

S^o est donc une application *bijective* qui conserve les *distances*, c'est-à-dire un isomorphisme. S est la restriction de S^o à (F).

4-3. Corollaire 2

« Si deux fonctions F et H ont des graphes de distances isomorphes (isomorphisme S), leurs enveloppes $\tilde{F}$ et $\tilde{H}$ ont des graphes de distances isomorphes. ($\exists$ un isomorphisme $\tilde{S}$ de $(\tilde{F})$ sur $(\tilde{H})$ dont S est une restriction). »

Démonstration

Ce résultat se déduit immédiatement du lemme 2 par itération de la transformation $F \rightarrow F^o$.

4-4. Théorème 2

« Deux fonctions booléennes :

— dont les enveloppes sont formées de 1, 2 ou 3 composantes connexes (1).

(1) Remarque : Ceci est vrai pour la très grande majorité des fonctions. Exemple : 22 types de fonctions à 4 variables sur 402 au total, ne vérifient pas cette condition.

— et dont les graphes de distances sont isomorphes sont de même type homogène. »

Démonstration :

Corollaire 1 et 2.

V. CARACTERISATION DU TYPE D'UNE FONCTION QUELCONQUE

5-1. Lemme 3

« Toute fonction booléenne F de dimension n, ayant plus de 2^{n-1} monômes canoniques est telle que son enveloppe $\tilde{F}$ est connexe. ($\tilde{F} =$ le n-cube circonscrit à F). »

Démonstration par récurrence sur la dimension de F :

— la propriété est vraie pour F de dimension 1 ;

— supposons la vraie pour toute fonction de dimension $n - 1$.

Soit une fonction F de dimension n, ayant plus de 2^{n-1} monômes canoniques.

$$F = xf + \bar{x}g \begin{cases} x \text{ est une variable quelconque} \\ f \text{ et } g \text{ sont des fonctions de dimension } n - 1 \end{cases}$$

xf (ou $\bar{x}g$) a plus de 2^{n-2} monômes canoniques

$\bar{x}g$ (ou xf) a au moins 1 monôme canonique

$\widetilde{xf}$ (ou $\widetilde{\bar{x}g}$) $=$ le $(n - 1)$ cube circonscrit à xf (ou $\bar{x}g$) (par hypothèse de récurrence)

$\widetilde{xf} + \bar{x}g$ (ou $xf + \widetilde{\bar{x}g}$) est donc connexe, et par suite

$\widetilde{xf} + \widetilde{\bar{x}g}$ est connexe

$\tilde{F} = \widetilde{xf + \bar{x}g} = \widetilde{\widetilde{xf} + \widetilde{\bar{x}g}}$ est donc connexe.

D'où $\tilde{F} =$ le n cube circonscrit à F.

Remarque : La propriété du lemme 3 s'étend aux fonctions booléennes dont l'enveloppe a plus de 2^{n-1} monômes canoniques C'est le cas en particulier des fonctions ayant 2^{n-1} monômes canoniques et dont une composante connexe au moins, n'est pas un cube.

En effet $\tilde{F} = \tilde{\tilde{F}}$

5-2. Lemme 4

« Pour qu'une fonction booléenne F de $x_1, x_2, \ldots, x_n$ soit une fonction *linéaire* non triviale (c'est-à-dire F de la forme $a \oplus x_i \oplus \ldots \oplus x_j$ avec $a = 0$

ou 1; $\{i, ..., j\} \subseteq \{1, ..., n\}$; $\{i, ..., j\} \neq \emptyset$) il est nécessaire et suffisant que

— F ait 2^{n-1} monômes canoniques

— $F = \tilde{F}$ (c'est-à-dire que chaque composante connexe soit un cube).

Démonstration

- Condition nécessaire évidente.
- Condition suffisante : Récurrence sur la dimension de F.

$$F = x_1 f + \bar{x}_1 g$$

Puisque $F = \tilde{F}$, le nombre de monômes canoniques appartenant respectivement à $x_1 \cdot f$ et $\bar{x}_1 \cdot g$ est respectivement soit 0 et 2^{n-1} soit 2^{n-1} et 0, soit 2^{n-2} et 2^{n-2} (lemme 3).

Dans les deux premiers cas ($F = \bar{x}_1 = 1 \oplus x_1$; $F = x_1 = 0 \oplus x_1$) le lemme est démontré.

Par hypothèse de récurrence, on a dans le 3[e] cas :

$$f = a \oplus x_i \oplus ... \oplus x_j \qquad a = 0 \text{ ou } 1$$
$$g = b \oplus x_k \oplus ... \oplus x_l \qquad b = 0 \text{ ou } 1$$
$$\{i \;...\; j\} \subseteq \{2, ...\; n\}$$
$$\{k \;...\; l\} \subseteq \{2, ...\; n\}$$

Soit $\underline{x}_i, ... \;\underline{x}_j$ des valeurs données aux variables $x_i, ... \;x_j$ telles que $f = 1$.

On a alors $f = 1$ quelque soit la valeur de $x_m \notin \{x_i ... x_j\}$. Et par suite, les composantes connexes de F étant des cubes, la valeur de la fonction g pour $x_i = \underline{x}_i, ... \;x_j = \underline{x}_j$ ne dépend pas de la valeur de x_m, $\forall\, x_m \notin \{x_i, ..., x_j\}$. g étant une fonction linéaire ($g = b \oplus x_k \oplus ... \oplus x_l$), g ne dépend pas de x_m.

On a donc $\{k ... l\} \subseteq \{i ... j\}$.

On montrerait de même que

$$\{i ... j\} \subseteq \{k ... l\}$$

D'où
$$\{i ... j\} = \{k ... l\}$$

On a donc $F = \alpha \oplus \beta x_1 \oplus x_i \oplus ... \oplus x_j$

$$\left.\begin{array}{l}\alpha = 0 \text{ ou } 1\\ \beta = 0 \text{ ou } 1\end{array}\right. \quad \text{suivant les valeurs de } a \text{ et } b$$

5-3. Lemme 5

« Le graphe des distances (F) d'une fonction booléenne linéaire F et le graphe des distances $(\bar{F})$ de la fonction complémentaire $\bar{F}$ caractérisent ensemble le type de cette fonction. »

Démonstration

Il suffit de remarquer que le type d'une fonction booléenne linéaire de n variables $F = a \oplus x_i \oplus \dots \oplus x_j$ est caractérisé par le couple $[n, p]$.

n : dimension de F

$p = | \{ i, \dots j \} |$ = nombre de variables dont dépend effectivement F.

$[(F), (\bar{F})]$ détermine n pour toute fonction booléenne,

(F) détermine p. ($n - p$ est la plus grande distance entre deux points d'une même composante connexe).

5-4. Théorème 3

« Le graphe de distances d'une fonction booléenne quelconque et le graphe des distances de la fonction complémentaire caractérisent ensemble le type de cette fonction. »

Démonstration (Théorème 2, Lemme 5).

En effet si F n'est pas une fonction linéaire, soit $\tilde{F}$ soit $\tilde{\bar{F}}$ est connexe.

VI. CONCLUSION

La recherche de l'isomorphisme de graphes complets étiquetés semble plus facile que la recherche d'un grand nombre de permutations et complémentations.

Le problème de savoir si deux fonctions sont de même type (c'est-à-dire réalisables par le même circuit) peut donc être facilité par ces résultats.

D'autre part, le lien établi entre une notion géométrique (graphe des distances) et une notion algébrique (type) est peut-être intéressant sur le plan théorique.

Je tiens à remercier ici M. P. Liddell avec qui cette étude a été abordée et M. J. Kuntzmann pour ses nombreux conseils.

BIBLIOGRAPHIE

J. KUNTZMANN, *Algèbre de Boole*, éd. Dunod, 1968.