Séminaire Dubreil.
Algèbre et théorie
des nombres

ETIENNE FICHAT

Décompositions d'une fonction de plusieurs variables

Séminaire Dubreil. Algèbre et théorie des nombres, tome 23, n° 1 (1969-1970), exp. n° 5, p. 1-20

<http://www.numdam.org/item?id=SD_1969-1970__23_1_A4_0>

Séminaire DUBREIL-PISOT
(Algèbre et théorie des nombres)
23e année, 1969/70, n° 5, 20 p.

15 décembre 1969

DÉCOMPOSITIONS D'UNE FONCTION DE PLUSIEURS VARIABLES

par Etienne PICHAT

A propos des <u>décompositions</u> d'une fonction $F(X)$ de plusieurs variables X, c'est-à-dire des expressions de $F(X)$ de la forme $G[H(A, Z), B, Z]$, où (A, B, Z) est une partition de X, deux questions se posent principalement :

1° Comment trouver les décompositions ? Dans le cas où les variables ont un nombre fini de valeurs, et étant donnée une partition (A, B, Z) des variables, un tableau permet de savoir si $F(X)$ admet une décomposition non triviale suivant cette partition ; dans le cas des fonctions booléennes, rappelons que l'écriture galoisienne, grâce à sa linéarité par rapport à chacune des variables, permet de trouver les décompositions simples d'une fonction, sans la donnée préalable de leurs partitions (PICHAT [5]).

2° Comment les décompositions d'une fonction s'agencent-elles les unes par rapport aux autres ? Ou d'un point de vue pratique, quelles décompositions est-il préférable d'utiliser pour la synthèse d'une fonction ? Des résultats remarquables sont obtenus à ce sujet en algèbre de Boole (ASHENHURST [1], CURTIS [2]) ; nous nous intéressons ici à leur généralisation à des fonctions arbitraires.

Remarquons qu'une réponse à la deuxième question aide la résolution de la première, la recherche des décompositions d'une fonction.

I. Préliminaires

I.1. Hypothèses.

Etant donné un ensemble produit arbitraire $E_1 \times E_2 \times \ldots \times E_n$, nous considérons des fonctions <u>partout définies</u> sur cet ensemble et <u>complètes</u>, c'est-à-dire des fonctions ayant une valeur ou un jeu de valeurs précisées pour tous les n-uplets de $E_1 \times E_2 \times \ldots \times E_n$.

Remarquons qu'il est toujours possible d'associer à une fonction non partout définie, ou à une fonction incomplète, une fonction partout définie et complète ; en particulier, un choix judicieux des valeurs non spécifiées d'une fonction incomplète peut faire apparaître des décompositions intéressantes.

Les fonctions considérées par la suite sont aussi supposées surjectives ; autrement dit, les données d'une fonction et de son espace-objet définissent son espace-image.

I.2. Notations.

Les lettres minuscules, excepté k, (par exemple x) désigneront des variables simples dont le domaine de définition est arbitraire ou des fonctions simples et complètes de telles variables, les lettres capitales (par exemple X) désigneront des variables générales (ensemble fini et ordonné de variables simples), ou des fonctions générales et complètes. L'ensemble des valeurs de X (ou x) est noté dom X (ou dom x) et leur nombre est noté Card dom X (ou Card dom x). Des valeurs particulières de X (respectivement x) sont notées X_1, X_2, ..., ou X_i, X_j, ... (respectivement x_1, x_2, ..., x_i, x_j, ...). Il nous arrivera d'écrire F pour $F(X)$.

I.3. Représentation tabulaire et décomposition.

(a) A une fonction $F(A, B, Z)$, on peut faire correspondre un tableau $\mathcal{T}^F_{BZ,AZ}$ (symboliquement dans le cas où les variables prennent une infinité de valeurs) dont chacune des lignes correspond à une valeur de $\{B, Z\}$, dont chacune des colonnes correspond à une valeur de $\{A, Z\}$, et dont les éléments sont les valeurs correspondantes de $F(A, B, Z)$ si elles existent, sinon (cas des fonctions non définies ou cas d'incompatibilité des arguments) des blancs.

(b) Une décomposition d'une fonction $F(A, B, Z)$ est un couple ordonné de deux fonctions G et H telles que :

$$F(A, B, Z) = G[H(A, Z), B, Z],$$

pour toutes les valeurs des variables A, B et Z. On dira aussi que $G[H(A, Z), B, Z]$ est une décomposition de $F(A, B, Z)$ suivant le triplet ordonné (A, B, Z), partition des variables de F.

Si l'ensemble Z est vide, la décomposition est dite disjointe.

Remarquons que la fonction $G(H, B, Z)$ n'est pas obligatoirement toujours définie, contrairement à F, mais c'est sans importance pour la suite. La fonction $H(A, Z)$ sera appelée fonction composante de la décomposition $G[H(A, Z), B, Z]$.

(c) Relativement au tableau représentant la fonction $F(A, B)$ et au tableau représentant sa décomposition disjointe $G[H(A), B]$ (si elle existe), on peut énoncer : Tout vecteur colonne $G(H_m, B)$ de $\mathcal{T}^G_{B,H}$ est un vecteur colonne de $\mathcal{T}^F_{B,A}$ et, inversement, tout vecteur colonne $F(A_i, B)$ de $\mathcal{T}^F_{B,A}$ est un vecteur colonne de $\mathcal{T}^G_{B,H}$.

Démonstration. - La surjectivité de H entraîne que, quelle que soit sa valeur H_m, il existe au moins une valeur A_i de A telle que $H(A_i) = H_m$, d'où

$$G(H_m , B) = G[H(A_i) , B] = F(A_i , B) .$$

Inversement,

$$F(A_i , B) = G[H(A_i) , B] = G(H_m , B) ,$$

si H_m est la valeur de $H(A_i)$.

Remarque 1. - Card dom H est supérieur ou égal au cardinal des colonnes différentes de $\mathcal{E}^F_{B,A}$, et inférieur ou égal à Card dom A .

Remarque 2. - La donnée de la décomposition non disjointe $G[H(A , Z) , B , Z]$ et celle de l'ensemble $\{G[H(A , k) , B , k] \mid k \in \text{dom } Z\}$ de décompositions disjointes sont équivalentes. Des résultats relatifs aux décompositions disjointes peuvent donc en fait être aussi généraux que ceux où interviennent des décompositions non disjointes.

I.4. Une généralisation.

Donnons une généralisation aux décompositions non disjointes, aux variables quelconques et aux fonctions générales d'un lemme de KARP [3].

LEMME 1. - Une condition nécessaire et suffisante d'existence de la décomposition

(1) $$F(A , B , Z) = G[H(A , Z) , B , Z]$$

est, pour toutes les valeurs A_i et A_j de A et pour toute valeur k de Z :

(2) $$(H(A_i , k) = H(A_j , k)) \implies (F(A_i , B , k) = F(A_j , B , k)) .$$

Démonstration. - (2) $\implies$ (1). En effet, $H(A , Z)$ étant surjectif, à toute valeur H_m de H , il correspond au moins une valeur A_i de A et une valeur k de Z telles que $H_m = H(A_i , k)$.

Définissons la fonction $G(H , B , Z)$ de la façon suivante :

$$G(H_m , B_\ell , k) = F(A_i , B_\ell , k) ,$$

pour toute valeur H_m de H , pour toute valeur B_ℓ de B , et pour toute valeur k de Z telle que $H(A , k)$ puisse prendre la valeur H_m (en particulier pour la valeur A_i de A) ; cette construction de $G(H , B , Z)$ est possible grâce à (2). Alors $G[H(A_i , k) , B_\ell , k] = F(A_i , B_\ell , k)$ pour toutes valeurs A_i , B_ℓ , k de A , B et Z respectivement, soit $G[H(A , Z) , B , Z] = F(A , B , Z)$ pour tous A , B et Z .

Inversement, (1) $\implies$ (2). En effet,

$$\begin{aligned} F(A_i , B , k) &= G[H(A_i , k) , B , k] \\ &= G[H(A_j , k) , B , k] \\ &= F(A_j , B , k) \end{aligned}$$

Etudions maintenant les décompositions multiples, échelonnées, et en chaîne, c'est-à-dire toutes les configurations possibles de deux décompositions d'une même fonction.

II. Décompositions multiples

THÉORÈME 1. - Une condition nécessaire et suffisante pour que

(3) $$F(A , B , C , Z) = N[H(A , Z) , M(B , Z) , C , Z]$$

est qu'il existe des fonctions G et K telles que

(4) $$F(A , B , C , Z) = G[H(A , Z) , B , C , Z] ,$$

(5) $$F(A , B , C , Z) = K[A , M(B , Z) , C , Z] .$$

Démonstration. - Que ce soit une condition nécessaire est évident.

Montrons qu'elle est suffisante, c'est-à-dire que, d'après le lemme 1,

$$\begin{cases} H(A_i , k) = H(A_j , k) \implies F(A_i , B , C , k) = F(A_j , B , C , k) \\ M(B_i , k) = M(B_j , k) \implies F(A , B_i , C , k) = F(A , B_j , C , k) \end{cases}$$

entraîne

$$(\{H(A_i , k) , M(B_i , k)\} = \{H(A_j , k) , M(B_j , k)\}) \implies (F(A_i , B_i , C , k) = F(A_j , B_j , C , k)) .$$

C'est évident.

Remarque. - Ce théorème est l'extension aux décompositions non disjointes, aux variables arbitraires, et aux fonctions générales, du théorème 2 de KARP [3].

III. Décompositions échelonnées

Pour relier des décompositions d'une fonction échelonnées entre elles, il est nécessaire, comme l'a fait KARP [3] pour les décompositions disjointes, de distinguer dans l'ensemble des décompositions $G[H(A , Z) , B , Z]$ d'une fonction $F(A , B, Z)$, les décompositions strictes ou décompositions $G[H(A , Z) , B , Z]$ vérifiant :

$$(H(A_i , k) = H(A_j , k)) \iff (F(A_i , B , k) = F(A_j , B , k)) .$$

Quand Z est vide, et quand A prend un nombre fini de valeurs, les décompositions strictes vérifient les propriétés équivalentes suivantes :

1° $(F(A_i , B) = F(A_j , B)) \iff (H(A_i) = H(A_j))$;

2° Card dom H est le nombre de colonnes distinctes de $\mathcal{T}^F_{B,A}$ (voir la remarque 1 de I.3) ;

3° Pour toute décomposition disjointe $K[L(A), B]$ de $F(A, B)$:

$$\text{Card dom } L \geqslant \text{Card dom } H .$$

THÉORÈME 2. - <u>Si</u>

$$F(A, B, C, Z) = G[H(A, Z), B, C, Z], \tag{6}$$

$$F(A, B, C, Z) = V[W(A, B, Z), C, Z], \tag{7}$$

<u>et si la décomposition</u> (7) <u>est stricte, alors il existe une fonction</u> M <u>telle que</u> :

$$W(A, B, Z) = M[H(A, Z), B, Z]; \tag{8}$$

<u>donc</u> $F(A, B, C, Z) = V\{M[H(A, Z), B, Z], C, Z\}$.

<u>Démonstration</u>. - $W(A, B, Z) = M[H(A, Z), B, Z]$ est, d'après le lemme 1, équivalent à :

$$H(A_i, k) = H(A_j, k) \implies W(A_i, B, k) = W(A_j, B, k) .$$

Or (6) implique

$$(H(A_i, k) = H(A_j, k)) \implies (F(A_i, B, C, k) = F(A_j, B, C, k)) ,$$

et (7) strict implique

$$(F(A_i, B, C, k) = F(A_j, B, C, k)) \implies (W(A_i, B, k) = W(A_j, B, k)) .$$

<u>Remarque</u> 1. - Ce théorème est l'extension aux décompositions non disjointes, aux variables quelconques, et aux fonctions générales, du théorème 3 de KARP [3].

<u>Remarque</u> 2.- Si la décomposition $F(A, B, C, Z) = G[H(A, Z), B, C, Z]$ est stricte, alors la décomposition $W(A, B, Z) = M[H(A, Z), B, Z]$ est stricte, et inversement.

En effet, (6) et (8) sont strictes si, respectivement,

$$(F(A_i, B, C, k) = F(A_j, B, C, k)) \implies (H(A_i, k) = H(A_j, k)) ,$$
$$(W(A_i, B, k) = W(A_j, B, k)) \implies (H(A_i, k) = H(A_j, k)) .$$

Or (7) stricte implique

$$(F(A_i, B, C, k) = F(A_j, B, C, k)) \iff (W(A_i, B, k) = W(A_j, B, k)) .$$

Remarquons que si $W(A, B, Z) = M[H(A, Z), B, Z]$ est une décomposition stricte, alors $F(A, B, C, Z) = G[H(A, Z), B, C, Z]$ est stricte, que (7) soit stricte ou non.

IV. Décompositions en chaîne.

Entre deux décompositions d'une fonction échelonnées entre elles, on n'a pu établir un lien que si l'une des deux au moins était stricte ; de même, envisager deux décompositions en chaîne d'une fonction ne peut être intéressant que si elles vérifient une certaine propriété.

<u>Définition</u>. - Une fonction $F(A , B)$ sera dite <u>injective par rapport à</u> A s'il existe une valeur B_0 de B telle que $F(A , B_0)$ est injectif (pour tout A où $F(A , B_0)$ est défini).

Dorénavant, nous considèrerons souvent des décompositions injectives, ou décompositions $G[H(A , Z) , B , Z]$, vérifiant les conditions équivalentes suivantes :

1° $G(H , B , Z)$ est injectif par rapport à H pour chaque valeur k de Z,

2° Il existe, pour chaque valeur k de Z, une valeur B_k de B telle que $G(H , B_k , k)$ est injectif,

3° Si $G[H(A , Z) , B , Z] = F(A , B , Z)$, il existe, pour tout k, une valeur B_k de B telle que, en désignant par A_i et A_j des valeurs arbitraires de A :

$$F(A_i , B_k , k) = F(A_j , B_k , k) \implies H(A_i , k) = H(A_j , k) ,$$

4° Il existe, pour tout k, une valeur B_k de B et une injection μ_k de $\operatorname{dom} H(A , k)$ dans $\operatorname{dom} G$ telle que :

$$G[H(A , k) , B_k , k] = \mu_k H(A , k) .$$

Nous devrons aussi considérer des fonctions $F(A , B , Z)$ <u>surjectives par rapport à</u> A, <u>pour toute valeur</u> k <u>de</u> Z, c'est-à-dire telles qu'il existe, pour tout k, une valeur B_k de B entraînant

$$\operatorname{dom} F(A , B_k , k) = \operatorname{dom} F(A , B , k) .$$

<u>Remarque</u> 1. - Une décomposition injective est une décomposition stricte. En effet, si $G[H(A , Z) , B , Z] = F(A , B , Z)$ est une décomposition injective, il existe, pour toute valeur k de Z, une valeur B_k de B telle que :

$$(F(A_i , B_k , k) = F(A_j , B_k , k)) \implies (H(A_i , k) = H(A_j , k)) ,$$

alors,

$$\begin{aligned}(F(A_i , B , k) = F(A_j , B , k)) &\implies (F(A_i , B_k , k) = F(A_j , B_k , k)) \\ &\implies (H(A_i , k) = H(A_j , k)) ,\end{aligned}$$

et $G[H(A , Z) , B , Z]$ est une décomposition stricte.

L'inverse n'est évidemment pas vrai.

LEMME 2. - Si

$$(9)\qquad \begin{cases} F(A , B , C , D , Z) = G[H(A , B , Z) , C , D , Z] \\ \qquad\qquad\qquad\qquad = K[A , M(B , C , Z) , D , Z] , \end{cases}$$

et s'il existe, pour chaque valeur k de Z, des valeurs A_k et D_k de A et D respectivement telles que $K(A_k , M , D_k , k)$ est injectif et $H(A_k , B , k)$ est surjectif (exactement $\mathrm{dom}\, H(A_k , B , k) = \mathrm{dom}\, H(A , B , k)$), alors il existe des fonctions V et W telles que :

$$(10)\qquad \begin{cases} F(A , B , C , D , Z) = V[W(A , B , C , Z) , D , Z] , \\ V(W , D_k , k) \text{ est injectif pour tout } k , \\ \mathrm{dom}\, W(A , B , C , Z) \subseteq \mathrm{dom}\, F(A , B , C , D , Z) , \\ W(A , B , C , k) = F(A , B , C , D_k , k) \text{ pour tout } k . \end{cases}$$

Démonstration. - Posons $W(A , B , C , k) = F(A , B , C , D_k , k)$, pour toute valeur k de Z, et démontrons (10) où, d'après le lemme 1, si A_i et A_j , B_i et B_j , C_i et C_j sont des valeurs arbitraires de A , B et C respectivement :

$$(F(A_i , B_i , C_i , D_k , k) = F(A_j , B_j , C_j , D_k , k)) \\ \Longrightarrow (F(A_i , B_i , C_i , D , k) = F(A_j , B_j , C_j , D , k)) .$$

En effet, $H(A_k , B , k)$ surjectif entraîne l'existence de la valeur B_{ik} de B telle que :

$$H(A_k , B_{ik} , k) = H(A_i , B_i , k) ,$$

d'où (9) entraîne :

$$\begin{aligned} F(A_i , B_i , C_i , D_k , k) &= G[H(A_i , B_i , k) , C_i , D_k , k] \\ &= G[H(A_k , B_{ik} , k) , C_i , D_k , k] \\ &= K[A_k , M(B_{ik} , C_i , k) , D_k , k] . \end{aligned}$$

De même, il existe une valeur B_{jk} de B telle que :

$$\begin{cases} F(A_j , B_j , C_j , D_k , k) = K[A_k , M(B_{jk} , C_j , k) , D_k , k] ; \\ H(A_k , B_{jk} , k) = H(A_j , B_j , k) . \end{cases}$$

Alors,

$$\begin{aligned} & (F(A_i , B_i , C_i , D_k , k) = F(A_j , B_j , C_j , D_k , k)) \\ \Longrightarrow\ & (K[A_k , M(B_{ik} , C_i , k) , D_k , k] = K[A_k , M(B_{jk} , C_j , k) , D_k , k]) \\ \Longrightarrow\ & (M(B_{ik} , C_i , k) = M(B_{jk} , C_j , k)) \\ \Longrightarrow\ & (K[A_k , M(B_{ik} , C_i , k) , D , k] = K[A_k , M(B_{jk} , C_j , k) , D , k]) \\ \Longrightarrow\ & (G[H(A_k , B_{ik} , k) , C_i , D , k] = G[H(A_k , B_{jk} , k) , C_j , D , k]) \\ \Longrightarrow\ & (G[H(A_i , B_i , k) , C_i , D , k] = G[H(A_j , B_j , k) , C_j , D , k]) \\ \Longrightarrow\ & (F(A_i , B_i , C_i , D , k) = F(A_j , B_j , C_j , D , k)) . \end{aligned}$$

L'injectivité de $V(W , D_k , k)$, c'est-à-dire

$$(V[W(A_i , B_i , C_i , k) , D_k , k] = V[W(A_j , B_j , C_j , k) , D_k , k]) \implies (W(A_i , B_i , C_i , k) = W(A_j , B_j , C_j , k))$$

est immédiate, puisque (10) et la définition de $W(A , B , C , Z)$ entraînent

$$V[W(A , B , C , k) , D_k , k] = F(A , B , C , D_k , k) = W(A , B , C , k) .$$

LEMME 3. - <u>Si</u>

$$(9') \quad F(A , B , C , D , Z) = G[H(A , B , Z) , C , D , Z] = K[A , M(B , C , Z) , D , Z] ,$$

<u>et s'il existe, pour chaque valeur</u> k <u>de</u> Z , <u>une valeur</u> B_{2k} <u>de</u> B <u>telle que</u> $M(B_{2k} , C , k)$ <u>est surjectif, alors il existe des fonctions</u> L <u>et</u> N <u>telles que</u>

$$(11) \quad \begin{cases} F(A , B , C , D , Z) = L[N(A , Z) , M(B , C , Z) , D , Z] , \\ \operatorname{dom} N(A , Z) \subseteq \operatorname{dom} H(A , B , Z) , \\ N(A , k) = H(A , B_{2k} , k) \ \underline{\text{pour tout}} \ k . \end{cases}$$

<u>Démonstration</u>. - Montrons d'abord l'existence de fonctions U et N telles que :

$$(12) \quad \begin{cases} F(A , B , C , D , Z) = U[N(A , Z) , B , C , D , Z] , \\ N(A , k) = H(A , B_{2k} , k) \ \text{pour tout} \ k . \end{cases}$$

En effet, si A_i et A_j sont des valeurs arbitraires de A , on a

$$\begin{aligned} &(H(A_i , B_{2k} , k) = H(A_j , B_{2k} , k)) \\ &\implies (G[H(A_i , B_{2k} , k) , C , D , k] = G[H(A_j , B_{2k} , k) , C , D , k]) \\ &\implies (K[A_i , M(B_{2k} , C , k) , D , k] = K[A_j , M(B_{2k} , C , k) , D , k]) \\ &\implies (K[A_i , M(B , C , k) , D , k] = K[A_j , M(B , C , k) , D , k]) \\ &\qquad \text{puisque } M(B_{2k} , C , k) \text{ est surjectif} \\ &\implies (F(A_i , B , C , D , k) = F(A_j , B , C , D , k)) , \end{aligned}$$

donc (12), d'après le lemme 1.

Alors le théorème 1 entraîne (11), à partir de (9') et (12).

On démontrerait semblablement :

LEMME 3'. - <u>Si</u>

$$F(A , B , C , D , Z) = G[H(A , B , Z) , C , D , Z] = K[A , M(B , C , Z) , D , Z] ,$$

<u>et s'il existe, pour chaque valeur</u> k <u>de</u> Z , <u>une valeur</u> B_{1k} <u>de</u> B <u>telle que</u> $H(A , B_{1k} , k)$ <u>est surjectif, alors il existe des fonctions</u> S <u>et</u> Q <u>telles que</u> :

$$F(A , B , C , D , Z) = S[H(A , B , Z) , Q(C , Z) , D , Z] ,$$
$$\operatorname{dom} Q(C , Z) \subseteq \operatorname{dom} M(B , C , Z) ,$$

$$Q(C\ ;\ k) = M(B_{1k}\ ,\ C\ ,\ k) \quad \underline{\text{pour tout}} \quad k\ .$$

LEMME 4. - <u>Si</u>

$$F(A\ ,\ B\ ,\ C\ ,\ D\ ,\ Z) = G[H(A\ ,\ B\ ,\ Z)\ ,\ C\ ,\ D\ ,\ Z]$$
$$= K[A\ ,\ M(B\ ,\ C\ ,\ Z)\ ,\ D\ ,\ Z]$$

<u>et s'il existe, pour chaque valeur</u> k <u>de</u> Z , <u>des valeurs</u> A_k <u>et</u> D_k <u>de</u> A <u>et</u> D <u>respectivement telles que</u> $K(A_k\ ,\ M\ ,\ D_k\ ,\ k)$ <u>est injectif, alors il existe des fonctions</u> V <u>et</u> P <u>telles que</u> :

$$M(B\ ,\ C\ ,\ Z) = V[P(B\ ,\ Z)\ ,\ C\ ,\ Z]\ ,$$
$$\mathrm{dom}\ P(B\ ,\ Z) \subseteq \mathrm{dom}\ H(A\ ,\ B\ ,\ Z)\ ,$$
$$P(B\ ,\ k) = H(A_k\ ,\ B\ ,\ k) \quad \underline{\text{pour tout}} \quad k\ ;$$

<u>donc</u>

$$F(A\ ,\ B\ ,\ C\ ,\ D\ ,\ Z) = K\{A\ ,\ V[P(B\ ,\ Z)\ ,\ C\ ,\ Z]\ ,\ D\ ,\ Z\}\ ,$$
$$K(A_k\ ,\ V\ ,\ D_k\ ,\ k) \quad \underline{\text{est injectif pour tout}} \quad k\ .$$

Démonstration. - Pour chaque valeur k de Z , il existe une injection μ_k de $\mathrm{dom}\ M(B\ ,\ C\ ,\ k)$ dans $K(A_k\ ,\ M\ ,\ D_k\ ,\ k)$ telle que :

$$K[A_k\ ,\ M(B\ ,\ C\ ,\ k)\ ,\ D_k\ ,\ k] = \mu_k\, M(B\ ,\ C\ ,\ k)\ ,$$

ou

$$G[H(A_k\ ,\ B\ ,\ k)\ ,\ C\ ,\ D_k\ ,\ k] = \mu_k\, M(B\ ,\ C\ ,\ k)\ ,$$

soit en posant $H(A_k\ ,\ B\ ,\ k) = P(B\ ,\ k)$:

$$M(B\ ,\ C\ ,\ k) = \mu_k^{-1}\, G[P(B\ ,\ k)\ ,\ C\ ,\ D_k\ ,\ k]\ ;$$

D_k dépendant uniquement de k , il existe donc une fonction V telle que

$$M(B\ ,\ C\ ,\ Z) = V[P(B\ ,\ Z)\ ,\ C\ ,\ Z]\ .$$

<u>Remarque</u> 2. - En plus de l'injectivité de $K(A_k\ ,\ M\ ,\ D_k\ ,\ k)$ pour tout k , supposons la décomposition $G[H(A\ ,\ B\ ,\ Z)\ ,\ C\ ,\ D\ ,\ Z]$ stricte ; alors $M(B\ ,\ C\ ,\ Z) = V[P(B\ ,\ Z)\ ,\ C\ ,\ Z]$ est une décomposition stricte. En effet,

$$\begin{aligned}
&(M(B_i\ ,\ C\ ,\ k) = M(B_j\ ,\ C\ ,\ k)) \\
&\quad \Longrightarrow\ (K[A\ ,\ M(B_i\ ,\ C\ ,\ k)\ ,\ D\ ,\ k] = K[A\ ,\ M(B_j\ ,\ C\ ,\ k)\ ,\ D\ ,\ k]) \\
&\quad \Longrightarrow\ (G[H(A\ ,\ B_i\ ,\ k)\ ,\ C\ ,\ D\ ,\ k] = G[H(A\ ,\ B_j\ ,\ k)\ ,\ C\ ,\ D\ ,\ k]) \\
&\quad \Longrightarrow\ (G[H(A_k\ ,\ B_i\ ,\ k)\ ,\ C\ ,\ D\ ,\ k] = G[H(A_k\ ,\ B_j\ ,\ k)\ ,\ C\ ,\ D\ ,\ k]) \\
&\quad \Longrightarrow\ (H(A_k\ ,\ B_i\ ,\ k) = H(A_k\ ,\ B_j\ ,\ k)) \\
&\quad \Longrightarrow\ (P(B_i\ ,\ k) = P(B_j\ ,\ k))\ .
\end{aligned}$$

La réunion des hypothèses des lemmes 3, 3' et 4 permet maintenant d'énoncer :

LEMME 5. - <u>Si</u> $F(A\ ,\ B\ ,\ C\ ,\ D\ ,\ Z) = G[H(A\ ,\ B\ ,\ Z)\ ,\ C\ ,\ D\ ,\ Z]$

$$= K[A\ ,\ M(B\ ,\ C\ ,\ Z)\ ,\ D\ ,\ Z]\ ,$$

<u>et s'il existe, pour chaque valeur</u> k <u>de</u> Z , <u>des valeurs</u> A_k <u>et</u> D_k <u>de</u> A <u>et</u> D <u>respectivement, et des valeurs</u> B_{1k} <u>et</u> B_{2k} <u>de</u> B <u>telles que</u> $K(A_k, M, D_k, k)$ <u>est injectif,</u> $H(A, B_{1k}, k)$ <u>et</u> $M(B_{2k}, C, k)$ <u>sont surjectifs, alors il existe des fonctions</u> L , R , N , P et Q <u>telles que</u> :

$$(13)\quad \begin{cases} M(B, C, Z) = R[P(B, Z), Q(C, Z), Z], \\ F(A, B, C, D, Z) = L\{N(A, Z), R[P(B, Z), Q(C, Z), Z], D, Z\}, \\ L[N(A_k, k), R, D_k, k],\ R[P, Q(C_0, k), k] \text{ et } R[P(B_{1k}, k), Q, k] \\ \underline{\text{sont injectifs pour tout}}\ k\ \underline{\text{et pour toute valeur}}\ C_0\ \underline{\text{de}}\ C, \\ \operatorname{dom} N(A, Z) \subseteq \operatorname{dom} H(A, B, Z), \\ \operatorname{dom} P(B, Z) \subseteq \operatorname{dom} H(A, B, Z), \\ \operatorname{dom} Q(C, Z) \subseteq \operatorname{dom} M(B, C, Z). \end{cases}$$

<u>Démonstration</u>. - $K(A_k, M, D_k, k)$ étant injectif pour toute valeur k de Z , la décomposition $K[A, M(B, C, Z), D, Z]$ est stricte d'après la remarque 1 ; le théorème 2 et le lemme 3' entraînent l'existence des fonctions U et Q telles que :

$$M(B, C, Z) = U[B, Q(C, Z), Z],$$

donc le théorème 1 et le lemme 4 entraînent l'existence de fonctions R et P telles que :

$$M(B, C, Z) = R[P(B, Z), Q(C, Z), Z],$$

soit, avec le lemme 3, de (13).

Les injectivités de $L[N(A_k, k), R, D_k, k]$, $R[P, Q(C_0, k), k]$ et $R[P(B_{1k}, k), Q, k]$ sont triviales puisque, si C_0 désigne une valeur arbitraire de C :

$$\begin{aligned} L\{N(A_k, k), R[P(B, k), Q(C, k), k], D_k, k\} \\ = F(A_k, B, C, D_k, k) = K[A_k, M(B, C, k), D_k, k], \end{aligned}$$

$$R[P(B, k), Q(C_0, k), k] = M(B, C_0, k) = \mu_k^{-1} K[A_k, M(B, C_0, k), D_k, k],$$

$$R[P(B_{1k}, k), Q(C, k), k] = M(B_{1k}, C, k) = Q(C, k).$$

THÉORÈME 3. - <u>Si</u>

$$(14)\quad \begin{aligned} F(A, B, C, D, Z) &= G[H(A, B, Z), C, D, Z] \\ &= K[A, M(B, C, Z), D, Z], \end{aligned}$$

<u>et s'il existe, pour chaque valeur</u> k <u>de</u> Z , <u>des valeurs</u> A_k <u>et</u> D_k <u>de</u> A <u>et</u> D <u>respectivement, et des valeurs</u> B_{1k} et B_{2k} <u>de</u> B <u>telles que</u> $K(A_k, M, D_k, k)$ <u>est injectif, et telles que</u> $H(A_k, B, k)$, $H(A, B_{1k}, k)$ <u>et</u> $M(B_{2k}, C, k)$ <u>sont surjectifs, alors il existe des fonctions</u> V , L , R , N , P et Q <u>telles que</u> :

$$(15)\quad \begin{cases} F(A\,,B\,,C\,,D\,,Z) = V[L\{N(A\,,Z)\,,R[P(B\,,Z)\,,Q(C\,,Z)\,,Z]\,,Z\}\,,D\,,Z]\,, \\ V(L\,,D_k\,,k)\,,\quad L[N(A_k\,,k)\,,R\,,k]\,,\quad R[P\,,Q(C_0\,,k)\,,k] \text{ et} \\ R[P(B_{1k}\,,k)\,,Q\,,k] \ \underline{\text{sont injectifs pour tout}}\ k\ \underline{\text{et pour toute valeur}} \\ C_0\ \underline{\text{de}}\ C\,. \end{cases}$$

<u>Démonstration</u>. - Le lemme 2 assure l'existence de fonctions V et W telles que :

$$(16)\quad \begin{cases} W(A\,,B\,,C\,,k) = F(A\,,B\,,C\,,D_k\,,k)\,, \\ F(A\,,B\,,C\,,D\,,Z) = V[W(A\,,B\,,C\,,Z)\,,D\,,Z]\,, \\ \text{dom } W(A\,,B\,,C\,,Z) \subseteq \text{dom } F(A\,,B\,,C\,,D\,,Z)\,, \\ V(W\,,D_k\,,k) \text{ est injectif pour tout } k\,. \end{cases}$$

La décomposition (10) stricte, d'après la remarque 1, et (14) entraînent, d'après le théorème 2, l'existence de fonctions T et U telles que :

$$(17)\quad \begin{cases} W(A\,,B\,,C\,,Z) = T[H(A\,,B\,,Z)\,,C\,,Z] \\ \qquad\qquad\qquad\quad = U[A\,,M(B\,,C\,,Z)\,,Z] \\ U(A_k\,,M\,,k) \text{ est injectif pour tout } k\,, \end{cases}$$

puisque

$$\begin{aligned} U[A_k\,,M(B\,,C\,,k)\,,k] = W(A_k\,,B\,,C\,,k) &= F(A_k\,,B\,,C\,,D_k\,,k) \\ &= K[A_k\,,M(B\,,C\,,k)\,,D_k\,,k] \end{aligned}$$

est injectif pour tout k.

Maintenant, le lemme 5 appliqué à (17) assure l'existence de fonctions L, R, N, P et Q telles que :

$$\begin{cases} W(A\,,B\,,C\,,Z) = L\{N(A\,,Z)\,,R[P(B\,,Z)\,,Q(C\,,Z)\,,Z]\,,Z\}\,, \\ L[N(A_k\,,k)\,,R\,,k]\,,\quad R[P\,,Q(C_0\,,k)\,,k] \text{ et } R[P(B_{1k}\,,k)\,,Q\,,k] \text{ sont} \\ \qquad \text{injectifs pour tout } k \text{ et pour toute valeur } C_0 \text{ de } C\,, \end{cases}$$

d'où (15) à l'aide de (17).

<u>Remarque</u> 3. - Dans le cas particulier où les décompositions sont disjointes $(Z = \emptyset)$, les lemmes et théorèmes qui précèdent ont évidemment une forme plus simple. Le théorème 3 devient, en particulier : <u>Si</u>

$$\begin{aligned} F(A\,,B\,,C\,,D) &= G[H(A\,,B)\,,C\,,D] \\ &= K[A\,,M(B\,,C)\,,D] \end{aligned}$$

<u>s'il existe des valeurs</u> A_0 <u>et</u> D_0 <u>de</u> A <u>et</u> D <u>respectivement, telles que</u> $K(A_0\,,M\,,D_0)$ <u>est injectif, et</u> $H(A_0\,,B)$ <u>est surjectif, et si</u> $H(A\,,B)$ <u>et</u> $M(B\,,C)$ <u>sont surjectifs respectivement par rapport à</u> A <u>et</u> C, <u>alors il existe des fonctions</u> V, L, R, N, P <u>et</u> Q <u>telles que</u> :

- $F(A, B, C, D) = V[L\{N(A), R[P(B), Q(C)]\}, D]$,

- $V(L, D)$, $L(N, R)$, $R(P, Q)$ sont injectifs respectivement par rapport à L, R, P et Q (pour respectivement $D = D_0$, $N = N(A_0)$, Q arbitraire et $P = P(B_0)$ si B_0 est une valeur de B rendant $H(A, B)$ surjectif).

Remarque 4. - Les hypothèses autres que (14) du théorème 3 ne sont pas symétriques en A et C ; le théorème 3 implique donc un théorème dont les hypothèses et les conclusions sont symétriques des siennes. En réunissant ces deux théorèmes, on obtient la conclusion supplémentaire suivante :

$L\{N, R[P(B_{2k}, k), Q(C_k, k), k], k\}$ est injectif pour tout k, et sa symétrique.

En effet, les hypothèses ajoutées à celles du théorème 3 sont :

Il existe, pour chaque valeur k de Z, des valeurs C_k et D_k de C et D respectivement telles que $G(H, C_k, D_k, k)$ est injectif et $M(B, C_k, k)$ est surjectif. La première entraîne :

$$
\begin{aligned}
&(L\{N(A_i, k), R[P(B_{2k}, k), Q(C_k, k), k], k\} \\
&\qquad\qquad = L\{N(A_j, k), R[P(B_{2k}, k), Q(C_k, k), k], k\}) \\
\Longrightarrow\ & (F(A_i, B_{2k}, C_k, k) = F(A_j, B_{2k}, C_k, k)) \\
\Longrightarrow\ & (G[H(A_i, B_{2k}, k), C_k, D_k, k] = G[H(A_j, B_{2k}, k), C_k, D_k, k]) \\
\Longrightarrow\ & (H(A_i, B_{2k}, k) = H(A_j, B_{2k}, k)) \\
\Longrightarrow\ & (N(A_i, k) = N(A_j, k)) .
\end{aligned}
$$

V. Dépendance

V.1. Dépendance de cardinal donné.

Généralisons la notion de dépendance d'une fonction par rapport à une de ses variables, à deux alternatives (la fonction dépend, ou ne dépend pas de la variable), en la quantifiant de la façon suivante :

Définition. - $F(A, B)$ est dit avoir une dépendance (de cardinal) n par rapport à ses variables A, si, et seulement si, quelles que soient les fonctions G et H vérifiant :

(18) $$F(A, B) = G[H(A, B), B],$$

on a :

(19) $$\min_H \operatorname{Card} \operatorname{dom} H = n .$$

Le concept d'indépendance d'une fonction par rapport à ses variables A devient alors équivalent à une dépendance égale à 1 de cette fonction par rapport à A ; une fonction dépendante de A a une dépendance supérieure à 1, et inversement.

Remarque 1. - A étant une fonction H(A , B) particulière, la dépendance de F(A , B) par rapport à A est inférieure ou égale à Card dom A ; F(A , B) pouvant être aussi considérée comme une fonction H(A , B) particulière, la dépendance de F(A , B) par rapport à A est inférieure ou égale à Card dom F(A , B) ; soit :

$$n \leqslant \min\{\text{Card dom } A \text{ , Card dom } F\} \text{ .}$$

Dans le cas où n est égal à Card dom A ou à Card dom F , nous dirons que la dépendance de F(A , B) par rapport à A est maximale ou encore que F(A , B) dépend au maximum du sous-ensemble A de ses variables. La notion classique de dépendance d'une fonction booléenne par rapport à une de ses variables (booléennes) est un exemple de dépendance maximale.

Remarque 2. - Dans le cas particulier où n = Card dom A , on ne peut donc pas remplacer A par une variable dont le cardinal de l'ensemble des valeurs est inférieur à celui de A . Mais, malheureusement, ce n'est pas parce que l'ordre de dépendance n d'une fonction par rapport à une de ses variables (générale ou non) X est inférieur à Card A que l'on peut toujours remplacer cette variable par une de ses valeurs (comme en algèbre de Boole) ou par une fonction ayant moins de valeurs et différente de la fonction de départ (il suffit de remarquer que l'ordre de dépendance d'une fonction booléenne par rapport à au moins deux de ses variables est généralement deux, et que les fonctions booléennes sont souvent pourtant non décomposables).

On peut envisager d'augmenter le nombre des valeurs d'une fonction pour que sa dépendance par rapport à certaines de ses variables A devienne égale à Card dom A . C'est ainsi que la fonction de a et de b définie par

$$\begin{array}{cc|ccc} & & & \overbrace{\quad\quad\quad}^{a} & \\ & & 0 & 1 & 2 \\ \hline b & 0 & 0 & 1 & 1 \\ & 1 & 1 & 0 & 1 \end{array}$$

a une dépendance de 2, alors que la fonction

$$\begin{array}{cc|ccc} & & & \overbrace{\quad\quad\quad}^{a} & \\ & & 0 & 1 & 2 \\ \hline b & 0 & 0 & 1 & 2 \\ & 1 & 1 & 0 & 1 \end{array}$$

a une dépendance égale à Card dom a = 3 .

Remarque 3. - $F(X)$ a une dépendance égale à Card dom F par rapport à X .

THÉORÈME 4 (Caractérisation d'une fonction dont la dépendance par rapport à une partie de ses variables est cardinal n). - Une condition nécessaire et suffisante pour que la dépendance de $F(A , B)$ par rapport à A soit n est :

$$(20) \qquad \max_B \text{Card dom } F(A , B) = n .$$

Démonstration. - La condition (20) est suffisante, car elle entraîne d'une part que toute fonction $H(A , B)$ vérifiant (18) satisfait :

$$(21) \qquad \text{Card dom } H(A , B) \geq n ,$$

d'autre part qu'il existe au moins une fonction $H^n(A , B)$ vérifiant (18) satisfaisant :

$$\text{Card dom } H^n(A , B) = n .$$

En effet, soit B_0 une valeur de B pour laquelle le maximum de (20) est atteint :

$$\text{Card dom } F(A , B_0) = n .$$

Alors (18) devient, pour B_0 ,

$$F(A , B_0) = G[H(A , B_0] , B_0] ,$$

d'où

$$\text{Card } F(A , B) \leq \text{Card dom } H(A , B_0)$$
$$n \leq \text{Card dom } H(A , B_0)$$

a fortiori (21).

Considérons une fonction $H(A , B)$ de cardinal (inférieur ou) égal à n , et vérifiant la condition suivante :

$$(H(A_i , B_k) = H(A_j , B_k)) \implies (F(A_i , B_k) = F(A_j , B_k))$$

pour toutes les valeurs B_k de B ; (20) permet d'assurer qu'une telle fonction existe. Alors le lemme 1 entraîne l'existence d'une fonction $G(H , B)$ vérifiant $G[H(A , B) , B] = F(A , B)$.

Inversement, montrons que si la dépendance de $F(A , B)$ par rapport à A est de cardinal n , alors $\max_B \text{Card dom } F(A , B) = n$.

En effet, (18) donne, pour toute fonction $H^n(A , B)$ de cardinal n , et pour $B = B_k$, $F(A , B_k) = G[H^n(A , B_k) , B_k]$, d'où

$$\text{Card dom } F(A , B_k) \leq \text{Card dom } H^n(A , B_k) \leq \text{Card dom } H^n(A , B) = n .$$

Cette borne supérieure n de Card $F(A , B_k)$ est atteinte ; sinon, à l'imitation de ce qui vient d'être fait, on pourrait construire une fonction $H(A , B)$ vérifiant (18) et de cardinal strictement inférieur à n .

Conséquence 1. - La dépendance d'une fonction $F(A , B)$ par rapport à A est supérieure ou égale à la dépendance par rapport à A de ses restrictions.

En effet, soit $\mathcal{R}F(A , B)$ une restriction de $F(A , B)$ de dépendance n par rapport à A ; alors il existe une valeur B_0 de B telle que $\text{Card dom } \mathcal{R}F(A , B_0) = n$, d'où $\text{Card dom } F(A , B_0) \geq n$.

Conséquence 2. - Si $G[H(A , B , Z) , C , Z]$ a une dépendance n par rapport à A , alors $G(H , C , Z)$ a une dépendance supérieure ou égale à n par rapport à H .

En effet, il existe des valeurs B_0 , C_0 , Z_0 de B , C et Z telles que :

$$\text{Card dom } G[H(A , B_0 , Z_0) , C_0 , Z_0] = n ,$$

d'où $\text{Card dom } G(H , C_0 , Z_0) \geq n$, et $G(H , C , Z)$ a une dépendance supérieure ou égale à n par rapport à H .

Conséquence 3. - Si $G[H(A , B , Z) , C , Z]$ a une dépendance n par rapport à A , alors $H(A , B , Z)$ a une dépendance supérieure ou égale à n par rapport à A .

En effet, il existe des valeurs B_0 , C_0 , Z_0 de B , C et Z telles que :

$$\text{Card dom } G[H(A , B_0 , Z_0) , C_0 , Z_0] = n ,$$

d'où $\text{Card dom } H(A , B_0 , Z_0) \geq n$, et $H(A , B , Z)$ a une dépendance supérieure ou égale à n par rapport à A .

Conséquence 4. - Si $F(A , B , C)$ a une dépendance n par rapport à A , alors sa dépendance par rapport à $\{A , B\}$ est supérieure ou égale à n .

En effet, il existe B_0 et C_0 tels que $\text{Card dom } F(A , B_0 , C_0) = n$, donc $\text{Card dom } F(A , B , C_0) \geq n$.

THÉORÈME 5 (Equivalence entre l'injectivité par rapport à A et la dépendance de cardinal $\text{Card dom } A$). - Etant donnée une fonction $F(A , B)$, l'existence d'une valeur B_0 de B telle que $F(A , B_0)$ est injectif entraîne que la dépendance de $F(A , B)$ par rapport à A est $\text{Card dom } A$. Inversement, si $\text{Card dom } A$ est fini et si la dépendance de $F(A , B)$ par rapport à A est $\text{Card dom } A$, alors il existe une valeur B_0 de B telle que $F(A , B_0)$ est injectif.

Démonstration. - On a obligatoirement

$$\max_B \text{Card dom } F(A , B) \leq \text{Card dom } A ,$$

borne atteinte pour $B = B_0$ puisque $F(A , B_0)$ est injectif.

L'inverse est, aussi, immédiat.

V.2. Application aux décompositions à nombre fini de valeurs.

Quand dom A est fini, les résultats précédents permettent d'énoncer qu'une condition nécessaire et suffisante pour que la dépendance d'une fonction $F(A, B)$ par rapport à l'ensemble A de ses variables, soit Card dom A, est que l'une des conditions équivalentes suivantes soit vérifiée :

1° $\max\limits_{B} \text{Card dom } F(A, B) = \text{Card dom } A$;

2° Il existe au moins une valeur B_0 de B telle que :

$$\text{Card dom } F(A, B_0) = \text{Card dom } A ;$$

3° Il existe au moins une valeur B_0 de B telle que $F(A, B_0)$ soit injectif ;

4° Il existe au moins une valeur B_0 de B et une bijection τ des valeurs de A sur les valeurs de $F(A, B_0)$ telles que $F(A, B_0) = \tau A$.

On peut utiliser la notion de dépendance pour trouver directement un résultat analogue à celui fourni par le théorème 3 dans le cas particulier où les domaines de F, H et M sont finis ; donnons-en l'énoncé dans le cas plus simple où Z est vide.

THÉORÈME 3'. - Si

$$\begin{aligned} F(A, B, C, D) &= G[H(A, B), C, D] \\ &= K[A, M(B, C), D], \end{aligned}$$

si Card dom F = Card dom H = Card dom $M = n$ fini, et si les dépendances de $F(A, B, C, D)$ par rapport à A, B et C sont n :

(a) Alors il existe des fonctions V, L, R, N, P et Q telles que :

$$F(A, B, C, D) = V[L\{N(A), R[P(B), Q(C)]\}, D],$$

$$\text{Card dom } L = \text{Card dom } R = \text{Card dom } N = \text{Card dom } P = \text{Card dom } Q = n,$$

les dépendances de $V(L, D)$ par rapport à L, de $L(N, R)$ par rapport à N et R, de $R(P, Q)$ par rapport à P et Q, de $N(A)$ par rapport à A, de $P(B)$ par rapport à B et de $Q(C)$ par rapport à C sont maximales, égales à n ;

(b) De même, il existe des fonctions S et T telles que :

$$F(A, B, C, D) = V[S\{T[N(A), P(B)], Q(C)\}, D],$$

$$\text{Card dom } S = \text{Card dom } T = \text{Card dom } N = \text{Card dom } P = \text{Card dom } Q = n,$$

les dépendances de $V(S, D)$ par rapport à S, de $S(T, Q)$ par rapport à T et Q, de $T(N, P)$ par rapport à N et P, de $N(A)$ par rapport à A, de $P(B)$ par rapport à B et de $Q(C)$ par rapport à C, sont maximales, égales à n.

<u>Démonstration</u> indirecte de (a), à partir du théorème 3. - La dépendance de $F(A , B , C , D)$ par rapport à B étant n , il existe des valeurs A_0 , C_0 et D_0 de A , C et D respectivement telles que

$$\begin{aligned} \text{Card } F(A_0 , B , C_0 , D_0) &= \text{Card } G[H(A_0 , B) , C_0 , D_0] \\ &= \text{Card } K[A_0 , M(B , C_0) , D_0] = n , \end{aligned}$$

ce qui entraîne, avec $\text{Card } H = n$,

$$\text{Card } H(A_0 , B) = n \quad \text{ou} \quad H(A_0 , B) \text{ surjectif,}$$

et, avec $\text{Card } M = n$,

$$K(A_0 , M , D_0) \text{ injectif.}$$

La dépendance de $F(A , B , C , D)$ par rapport à A étant n , il existe B_1 , C_1 et D_1 tels que :

$$\text{Card } F(A , B_1 , C_1 , D_1) = \text{Card } G[H(A , B_1) , C_1 , D_1] = n ,$$

et $H(A , B_1)$ est surjectif. De même, la dépendance n de $F(A , B , C , D)$ par rapport à C , assure l'existence d'une valeur B_2 de B telle que $M(B_2 , C)$ est surjectif.

Les hypothèses du théorème 3 sont donc vérifiées ; on montrerait de même que les hypothèses symétriques, obtenues en intervertissant A et C , sont vérifiées. Les conclusions des remarques 3 et 4 de IV sont donc valables. Il en résulte (a) en remarquant que les cardinalités de L , R , N , P et Q sont supérieures ou égales à n puisque les dépendances de $F(A , B , C , D)$ par rapport à A , B et C sont n , et qu'elles sont inférieures ou égales à n puisque

$$\begin{aligned} &\text{dom } L \subseteq \text{dom } F , \\ &\text{dom } R \subseteq \text{dom } M , \\ &\text{dom } N \subseteq \text{dom } H , \\ &\text{dom } P \subseteq \text{dom } H , \\ &\text{dom } Q \subseteq \text{dom } M . \end{aligned}$$

(b) s'obtient comme (a).

<u>Remarque</u> 4. - Le théorème 3 permet de donner des résultats plus fins que ceux mentionnés dans le théorème 3'. En particulier, si $\text{Card dom } F$ est supérieur à n , les résultats (a) sont encore valables, excepté la cardinalité et la dépendance de L . L'intérêt du théorème 3', et de ses hypothèses, réside en leur simplicité en termes de dépendance ; on peut d'ailleurs encore prendre les hypothèses plus simples, mais plus restrictives suivantes : $F(A , B , C , D)$ prend n valeurs distinctes, admet deux décompositions en chaîne à fonctions composantes prenant n valeurs distinctes, et la dépendance par rapport à chacune de ses variables est n .

<u>Remarque</u> 5. – Le théorème 3', ou son expression plus élémentaire donnée dans la remarque précédente, généralise aux fonctions de variables ayant des nombres finis de valeurs un résultat de SINGER et ASHENHURST, et confirme une conjoncture de KARP et WINOGRAD [3], partiellement parce que, si les hypothèses du théorème 3' sont vérifiées, il n'existe pas toujours de fonctions I et J telles que :

$$(22)\qquad \begin{cases} F(A\ ,\ B\ ,\ C\ ,\ D) = I[J(A\ ,\ C)\ ,\ B\ ,\ D] \\ \text{Card dom } J(A\ ,\ C) \leq \text{Card dom } F\ , \end{cases}$$

comme le montre la fonction suivante vérifiant les hypothèses du théorème 3', avec $n = 3$:

$$f(a\ ,\ b\ ,\ c) = g[h(a\ ,\ b)\ ,\ c] = k[a\ ,\ m(b\ ,\ c)]$$

f(a , b , c)	b								
	a			a			a		
c	0	1	2	1	1	1	2	2	2
	1	1	1	1	1	1	1	1	1
	2	2	2	2	2	2	2	2	2
h(a , b)	0	I	II	I	I	I	II	II	II

Ce tableau montre que la dépendance de f(a , b , c) par rapport à c est 3 et que Card dom h = 3 . Le tableau

f(a , b , c)	b								
	c			c			c		
a	0	1	2	1	1	2	2	1	2
	1	1	2	1	1	2	2	1	2
	2	1	2	1	1	2	2	1	2
m(b , c)	0	I	II	I	I	II	II	I	II

montre que la dépendance de f(a , b , c) par rapport à a est maximale et que Card dom m = 3 . Enfin

f(a , b , c)	a								
	c			c			c		
b	0	1	2	1	1	2	2	1	2
	1	1	2	1	1	2	1	1	2
	2	1	2	2	1	2	2	1	2
j(a , c)	0	I	II	III			IV		

montre que la dépendance de f(a , b,, c) par rapport à b est encore maximale. Or nous constatons que Card dom j(a , c) = 5 .

On peut vérifier que cette fonction $f(a, b, c)$ ternaire est la seule, à une permutation près des valeurs et des variables, qui vérifie les conditions du théorème 3' et qui ne vérifie pas (18). Dans le contre-exemple de THELLIEZ [7] à l'existence de (18) dans le cas des fonctions ternaires, la variable α_3 de $f(\alpha_1, \alpha_2, \alpha_3)$ peut être considérée comme une variable binaire.

VI. Conclusion

Les résultats qui viennent d'être obtenus, concernant la structure des décompositions multiples, échelonnées ou en chaîne, d'une fonction, permettent d'obtenir la proposition suivante :

Soit une fonction prenant n (nombre fini) valeurs, et à dépendance par rapport à chacune de ses variables égale à n. Considérons les fonctions composantes prenant n valeurs de ses décompositions disjointes : leurs ensembles de variables forment un treillis par rapport à la réunion et l'intersection ensemblistes.

Le principe de la démonstration est dans ASHENHURST [1] ou CURTIS [2], où est démontrée la structure de treillis dans le cas des décompositions disjointes simples des fonctions booléennes.

En conclusion, nous pouvons dire que, mise à part l'inexistence d'une certaine décomposition montrée par le contre-exemple de la remarque 5 de V.2, tous les résultats obtenus permettent de retrouver facilement ceux relatifs aux fonctions booléennes : en effet, une décomposition booléenne disjointe simple est toujours stricte si elle dépend effectivement de la fonction composante, et la dépendance d'une fonction booléenne par rapport à chacune de ses variables (effective ; sinon la variable peut être supprimée) est nécessairement deux.

Parmi les fonctions à valeurs dans un certain domaine et à variables parcourant certains domaines, la proportion de celles ayant des décompositions non triviales strictes ou vérifiant les hypothèses du théorème 3, est d'autant plus faible que ces domaines sont plus grands, et que les variables sont en plus grand nombre ; PICHAT [5] et [6] montrent par exemple que la proportion de fonctions booléennes, admettant au moins une décomposition disjointe simple non triviale, décroît très rapidement avec le nombre des variables ; par contre, les décompositions multiples ou non disjointes sont très nombreuses.

BIBLIOGRAPHIE

[1] ASHENHURST (R.). - The decomposition of switching functions, Ann. Harvard Comput. Lab., t. 29, 1959, p. 74-116.

[2] CURTIS (H. Allen). - A new approach to the design of switching circuits. - Princeton, D. Van Nostrand, 1962.

[3] KARP (Richard M.). - Functional decomposition and switching circuit design, J. Soc. for ind. and appl. Math., t. 11, 1963, p. 291-335.

[4] KUNTZMANN (J.). - Algèbre de Boole. 2e édition. - Paris, Dunod, 1968 (Bibliothèque de l'Ingénieur automaticien, 10).

[5] PICHAT (E.). - Décompositions simples de fonctions booléennes, Rev. franç. Inform. Rech. opérat., t. 2, 1968, n° 7 , p. 61-70.

[6] PICHAT (E.). - Contribution à l'algorithme non numérique dans les ensembles ordonnés (Thèse Sc. math. Grenoble, 1970).

[7] THELLIEZ (S.). - Sur la décomposition disjonctive complexe arborescente d'une fonction ternaire en vue de son application à la synthèse des structures combinatoires ternaires, C. R. Acad. Sc. Paris, t. 264, 1967, Série A, p. 419-421.

(Texte reçu le 15 décembre 1970)

Etienne PICHAT
CNAM - Inst. Inform. d'Entrepr.
1 rue Montgolfier
75 - PARIS 03