

04

**SUR LA CONSTRUCTION DES PLANS FACTORIELS
FRACTIONNÉS ET CERTAINS CODES CORRECTEURS
A L'AIDE DES CARACTÈRES DES GROUPES ABÉLIENS**

Dominique C. FOATA

Extrait de
PUBLICATIONS DE L'INSTITUT DE STATISTIQUE DE L'UNIVERSITÉ DE PARIS
Vol. XI, fascicule 1 — 1962

SUR LA CONSTRUCTION DES PLANS FACTORIELS FRACTIONNÉS ET CERTAINS CODES CORRECTEURS A L'AIDE DES CARACTÈRES DES GROUPES ABÉLIENS

Dominique C. FOATA

SOMMAIRE.

Bose a montré que la détermination du sous-groupe fondamental d'un plan d'expérience fractionné et la construction de l'alphabet d'un code correcteur d'erreurs pouvaient être réduits au même problème. Dans sa forme duale, le problème consiste à construire une matrice A , à éléments dans un corps de Galois $GF(s)$, ayant la propriété P_d que le rang de tout ensemble de d vecteurs-lignes de cette matrice A est égal à d .

Nous montrons ici comment de telles matrices peuvent être obtenues à partir de la théorie des caractères des groupes abéliens.

INTRODUCTION.

Un groupe code $C(s, n, t, k)$, s -aire, de dimension n et correcteur d'erreurs d'ordre t , est défini comme le couple formé par un sous-espace vectoriel V_k , de dimension $k \leq n$, de l'espace vectoriel E_n de dimension n sur $GF(s)$ et une application linéaire de E_n sur E_n/V_k , telle que sa restriction à Ω , l'ensemble des vecteurs de E_n n'ayant pas plus de t coordonnées non nulles, est biunivoque.

Bose [3] a montré que l'existence d'un tel $C(s, n, t, k)$ était équivalente à l'existence d'un plan factoriel fractionné $(1/s^k).s^n$, dans lequel aucune interaction d'ordre $\leq t$ n'est confondue avec une autre interaction d'ordre $\leq t$; le sous-espace vectoriel V_k pouvant être mis en correspondance biunivoque avec le sous-groupe fondamental du plan $(1/s^k).s^n$.

This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49 (638) 213. Reproduction in whole or in part is permitted for any purpose of the United States Government.

Ces deux constructions se ramènent à la détermination d'une application linéaire de E_n sur E_n/V_k , telle que la matrice A qui la représente a la propriété P_{2t} que le rang de tout ensemble de $2t$ vecteurs-lignes de A , est $2t$.

Bose et Ray-Chaudhuri [1] et [2] ont donné une méthode de construction explicite dans le cas binaire. Peterson [6] a déterminé plusieurs propriétés des codes correspondants. En particulier, il a donné la valeur exacte du rang de ces matrices. Enfin, Zierler [8] a généralisé ces résultats au cas s -aire (s puissance d'un nombre premier).

Dans la présente communication, utilisant la théorie des caractères des groupes abéliens, nous reformulons ces résultats et montrons comment ces matrices peuvent être obtenues à partir de la table des caractères des groupes cycliques. De là, prenant un groupe abélien général, nous obtenons une construction analogue et une nouvelle famille de matrices ayant la propriété P_d .

I

Dans cette section, nous donnons quelques propriétés des caractères des groupes abéliens, nécessaires pour notre construction.

Soit G un groupe abélien d'ordre g , dont les invariants sont : $h_1, h_2, \dots, h_r$. On sait que ces invariants sont caractérisés par les propriétés suivantes :

(i) G est la somme directe de r groupes cycliques $G_1, G_2, \dots, G_r$, respectivement d'ordres $h_1, h_2, \dots, h_r$.

(ii) h_{i+1}/h_i ($i = 1, 2, \dots, (r-1)$).

Ainsi, chaque élément a de G peut être représenté sous la forme :

$$a = (a_1, a_2, \dots, a_r)$$

où :

$$(0 \leq a_1 \leq h_1 - 1 ; 0 \leq a_2 \leq h_2 - 1 ; \dots ; 0 \leq a_r \leq h_r - 1)$$

Si maintenant Γ est un corps, dont la caractéristique ne divise pas $h = h_1$ et si ζ est une racine primitive de l'unité d'ordre h dans Γ ($i = 1, 2, \dots, r$), les caractères du groupe G sont donnés par :

$$\chi(u_1, u_2, \dots, u_r) : a = (a_1, a_2, \dots, a_r) \longrightarrow \zeta_1^{u_1 a_1} \zeta_2^{u_2 a_2} \dots \zeta_r^{u_r a_r}$$

$$a \in G, (0 \leq u_1 \leq h_1 - 1 ; 0 \leq u_2 \leq h_2 - 1 ; \dots ; 0 \leq u_r \leq h_r - 1).$$

Cf. Van der Waerden [7].

Comme h_i divise h , pour tout $i = 2, 3, \dots, r$, nous pouvons prendre ζ_i comme une puissance bien définie de $\zeta = \zeta_1$ et, ainsi, toutes les images des éléments de G , sous tous les caractères, seront des puissances de ζ .

Dans la table des caractères du groupe G , nous faisons la convention que les g lignes correspondent aux g éléments de G et que les g colonnes correspondent aux g caractères de G .

Rappelant la définition de la propriété P_d (définition 1), introduite par Bose et Ray-Chaudhuri [1], les précédentes conventions nous permettent de définir une propriété P_d sur les caractères : (définition 2) :

Définition 1 - Une matrice à éléments dans un corps Γ a la propriété P_d si le rang de tout ensemble de d lignes-vecteurs de cette matrice est égal à d .

Définition 2 - Un ensemble de caractères $(\chi_1, \chi_2, \dots, \chi_k)$ d'un groupe abélien G a la propriété P_d , si la sous-matrice de la table des caractères de G , formée par les k colonnes $\chi_1, \chi_2, \dots, \chi_k$, a la propriété P_d .

Maintenant, soit p un nombre premier ne divisant pas h et soit m l'ordre de p dans le système des résidus modulo h ($p^m \equiv 1 \pmod{h}$ et $p^{m'} \not\equiv 1 \pmod{h}$ pour $m' < m$). Posons, d'autre part, $c = (p^m - 1)/h$ et soit x une racine primitive du corps de Galois $GF(p^m)$. Alors x^c est une racine primitive de l'unité, d'ordre h , dans $GF(p^m)$. De là, si nous prenons $GF(p^m)$ pour le corps Γ et x^c pour ζ , tous les éléments de la table des caractères de G seront éléments de $GF(p^m)$; et nous aurons :

Proposition 1.1 - Si G est un groupe abélien, d'ordre g , dont les invariants sont $(h_1, h_2, \dots, h_r)$ et si $(\chi_1, \chi_2, \dots, \chi_k)$ est un ensemble de caractères de G ayant la propriété P_d , alors, pour tout nombre premier p (ne divisant pas g), il existe une matrice, de g lignes et k colonnes, ayant la propriété P_d , et dont les éléments appartiennent à $GF(p^m)$; m étant l'ordre de p dans le système des résidus modulo h .

Le problème est donc de construire des ensembles de caractères de G , possédant la propriété P_d pour un d donné. Cette question sera examinée plus loin. Remarquons que :

(1.2) - Si un ensemble de caractères $(\chi_1, \chi_2, \dots, \chi_k)$ d'un groupe abélien G possède la propriété P_d , alors les ensembles $(\bar{\chi}_1, \bar{\chi}_2, \dots, \bar{\chi}_k)$ et $(\chi\chi_1, \chi\chi_2, \dots, \chi\chi_k)$ possèdent la propriété P_d , pour tout caractère χ de G .

(Nous dénotons par $\bar{\chi}$ l'inverse de χ dans le groupe des caractères de G et par $\chi\chi_j$ le caractère : $a \rightarrow \chi(a)\chi_j(a)$).

En effet, si :

$$\sum_{i=1}^d \lambda_i \chi(a_i) = 0 \quad \lambda_i \in \text{corps } \Gamma$$

alors $\sum_{i=1}^d \lambda_i \bar{\chi}(a_i^{-1}) = 0$, puisque $\chi(a^{-1}) = \bar{\chi}(a)$.

De là, toute relation linéaire entre d lignes de la sous-matrice $(\chi_1, \chi_2, \dots, \chi_k)$ entraîne une relation linéaire entre d lignes de la sous-matrice $(\bar{\chi}_1, \bar{\chi}_2, \dots, \bar{\chi}_k)$.

De la même manière, si l'on a une relation :

$$\sum_{i=1}^d \lambda_i \chi(a_i) \chi_j(a_i) = 0,$$

pour $j = 1, 2, \dots, k$

et : $\lambda_i \in \Gamma$ ($i = 1, 2, \dots, d$)

alors, $\lambda_i \chi(a_i) = \mu_i$ est un élément de Γ et de là, il existe une relation :

$$\sum_{i=1}^d \mu_i \chi(a_i) = 0$$

$j = 1, 2, \dots, k$; ce qui contredit l'hypothèse de la propriété P_d .

Supposons maintenant que le nombre premier p a été choisi, une fois pour toutes, (ne divisant pas l'ordre g du groupe) et que les caractères prennent leurs valeurs dans le corps $GF(p^n)$, m étant fixé par le choix de p . Nous désignerons alors la table des caractères de G par Σ et le groupe des caractères de G , pris sous cette forme par $\Sigma(G, p, m)$.

Nous allons montrer maintenant comment, d'un ensemble de caractères de $\Sigma(G, p, m)$, possédant la propriété P_d , on peut déduire un sous-ensemble ayant la propriété P_d sur un sous-corps $GF(p^n)$ de $GF(p^n)$ (définition 4) et, représentant tout élément de $GF(p^n)$ par un vecteur à coordonnées dans $GF(p^n)$, obtenir une matrice, à éléments dans le sous-corps $GF(p^n)$ et ayant la propriété P_d .

Avant d'introduire la définition de la propriété P_d sur un sous-corps, définissons une relation d'équivalence sur les caractères :

On sait qu'à chaque diviseur n de m , correspond un sous-corps $GF(p^n)$ de $GF(p^n)$ et que le groupe de Galois de $GF(p^n)$ sur $GF(p^n)$ est le groupe cyclique Φ d'ordre $m_1 = m/n$ engendré par :

$$\alpha \longrightarrow \alpha^q ; \quad q = p^n \quad \text{et} \quad \alpha \in GF(p^n).$$

D'où la définition :

Définition 3 - Deux caractères χ_1 et χ_2 de $\Sigma(G, p, m)$ sont équivalents modulo $\Phi(n)$, s'il existe un entier k tel que :

$$\chi_1 = \chi_2^{q^k} \quad (q = p^n).$$

Comme Φ est cyclique et que $\chi^{q^{m_1}} = \chi^{p^m} = \chi$, pour tout $\chi \in \Sigma(G, p, m)$, cette relation est évidemment une relation d'équivalence. Nous dénotons les classes d'équivalence modulo $\Phi(n)$ par : $\chi_1^*, \chi_2^*, \dots, \chi_{g^*}^*$ et l'ensemble des caractères dans la classe χ^* , contenant χ , par $\{\chi^*\}$.

Définition 4 - (Propriété P_d sur un sous-corps). Un ensemble de k caractères $(\chi_1, \chi_2, \dots, \chi_k)$ de $\Sigma(G, p, m)$ a la propriété P_d sur $GF(p^n)$ (n étant un diviseur de m), si, pour tout ensemble de d vecteurs-lignes de la

sous-matrice $(\chi_1, \chi_2, \dots, \chi_k)$ de $\sum, v_{i_1}, v_{i_2}, \dots, v_{i_d}$, on ne peut avoir une relation de la forme :

$$\lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \dots + \lambda_d v_{i_d} = 0$$

avec $\lambda_1, \lambda_2, \dots, \lambda_d \in \text{GF}(p^n)$.

Nous avons alors :

Proposition 1.3 - L'ensemble $(\chi_1^*, \chi_2^*, \dots, \chi_k^*)$ de k distinctes classes modulo $\Phi(n)$ de $\sum (G, p, m)$ a la propriété P_d sur $\text{GF}(p^n)$, si et seulement si l'ensemble $(\{\chi_1^*\}, \{\chi_2^*\}, \dots, \{\chi_k^*\})$ a la propriété P_d (sur $\text{GF}(p^n)$).

En effet, supposons qu'il existe d éléments de G , $a_1, a_2, \dots, a_d$ tels que :

$$\sum_{i=1}^d \lambda_i \chi(a_i) = 0 \quad \lambda_i \in \text{GF}(p^n) \quad (i = 1, 2, \dots, d) \quad (1)$$

et que cette relation est satisfaite pour tous les caractères χ de l'ensemble : $(\{\chi_1^*\}, \{\chi_2^*\}, \dots, \{\chi_k^*\})$; alors, comme $\alpha \rightarrow \alpha^q (q = p^n)$ est un

$$\text{automorphisme de } \text{GF}(p^n), \quad \sum_{i=1}^d \lambda_i \chi(a_i) = 0 \implies \sum_{i=1}^d \lambda_i^q \chi^q(a_i) = \sum_{i=1}^d \lambda_i^{q^2} \chi^{q^2}(a_i) = \dots = \sum_{i=1}^d \lambda_i^{q^{(m_1-1)}} \chi^{q^{(m_1-1)}}(a_i) = 0.$$

D'où :

$$\sum_{i=1}^d (\lambda_i + \lambda_i^q + \dots + \lambda_i^{q^{(m_1-1)}}) \chi(a_i) = 0$$

puisque la relation (1) est satisfaite pour tous les caractères d'une même classe. Mais, d'autre part : $\mu_i = \lambda_i + \lambda_i^q + \dots + \lambda_i^{q^{(m_1-1)}}$ est un élément de $\text{GF}(p^n)$, puisque $\mu_i^q = \mu_i$ ($i = 1, 2, \dots, d$). Ainsi, nous avons trouvé une relation linéaire sur $\text{GF}(p^n)$, entre d éléments de G : $\sum_{i=1}^d \mu_i \chi(a_i) = 0$, $\mu_i \in \text{GF}(p^n)$, $i = 1, 2, \dots, d$ et cette relation est satisfaite pour tous les éléments de l'ensemble $(\{\chi_1^*\}, \{\chi_2^*\}, \dots, \{\chi_k^*\})$. De là, l'ensemble des classes $(\chi_1^*, \chi_2^*, \dots, \chi_k^*)$ ne peut avoir la propriété P_d sur $\text{GF}(p^n)$.

Si μ_i est nul pour tout $i = 1, 2, \dots, d$, alors nous pouvons multiplier tous les λ_i par un élément convenable v de $\text{GF}(p^n)$ de telle manière que la relation :

$$(v \lambda_i) + (v \lambda_i)^q + \dots + (v \lambda_i)^{q^{(m_1-1)}} = 0$$

n'est pas satisfaite pour tous les λ_i ($i = 1, 2, \dots, d$). Ceci est toujours possible, car l'équation : $\lambda + \lambda^q + \dots + \lambda^{q^{(m_1-1)}} = 0$ n'est pas satisfaite par tous les $(q^{m_1} - 1)$ éléments non-nuls de $\text{GF}(p^n)$. Ainsi, la condition est bien nécessaire.

Elle est aussi suffisante ; en effet, si l'on a une relation de la forme :

$$\sum_{i=1}^d \lambda_i \chi(a_i) = 0$$

avec $\lambda_1, \lambda_2, \dots, \lambda_d \in \text{GF}(p^n)$,

$a_1, a_2, \dots, a_d \in G$ et $\chi \in \Sigma(G, p, m)$,

alors, comme $\alpha \rightarrow \alpha^q$ est un automorphisme de $\text{GF}(p^n)$ laissant les éléments de $\text{GF}(p)$ invariants, nous avons :

$$0 = \left(\sum_{i=1}^d \lambda_i \chi(a_i) \right)^q = \sum_{i=1}^d \lambda_i^q \chi^q(a_i) = \sum_{i=1}^d \lambda_i \chi^q(a_i)$$

Ainsi, la même relation est satisfaite pour χ^q , et de là, pour $\chi^{q^2}, \chi^{q^3}, \dots, \chi^{q^{(n_1-1)}}$, c'est-à-dire pour tous les caractères de la classe χ^* contenant χ .

Corollaire 1.4 - L'ensemble de toutes les classes mod $\Phi(n)$ ($\chi_1^*, \chi_2^*, \dots, \chi_{g^*}^*$) a la propriété P_d sur $\text{GF}(p^n)$.

Prenons, en effet, toutes les classes mod $\Phi(n)$; nous épuisons tous les caractères du groupe et le résultat suit du fait que la table des caractères Σ est une matrice non-singulière.

La relation d'équivalence $\Phi(n)$ ne préserve pas la multiplication des caractères, mais elle préserve l'opération-inverse :

Si $\chi_1 = \chi_2 \bmod \Phi(n)$, alors $\chi \chi_1$ n'est pas nécessairement équivalent à $\chi \chi_2$ pour $\chi \in \Sigma(G, p, m)$. Par contre, $\chi_1^k = \chi_2^k \bmod \Phi(n)$ pour tout k . Comme tout χ vérifie $\chi^h = 1$, l'inverse $\bar{\chi}$ de χ est égal à : $\bar{\chi} = \chi^{h-1}$. D'où encore, $\bar{\chi}_1 = \bar{\chi}_2$, si $\chi_1 = \chi_2 \bmod \Phi(n)$.

Nous pouvons donc parler de la puissance k ème d'une classe χ^{*k} et aussi de son inverse χ^* .

Ainsi, par (1.2) et la proposition 1.3,

(1.5) - Si l'ensemble des classes ($\chi_1^*, \chi_2^*, \dots, \chi_k^*$) a la propriété P_d sur $\text{GF}(p^n)$, alors ($\chi_1^*, \chi_2^*, \dots, \chi_k^*$) a la propriété P_d sur $\text{GF}(p^n)$.

Les classes mod $\Phi(n)$ n'ont pas nécessairement le même nombre d'éléments. Mais ce nombre est en relation avec un corps intermédiaire, contenant $\text{GF}(p^n)$ et contenu dans $\text{GF}(p^m)$.

Nous dirons :

Définition 5 - n étant donné, diviseur de m , le caractère χ de $\Sigma(G, p, m)$ appartient au corps de Galois $\text{GF}(p^k)$, si k est le plus petit multiple de n tel que $\text{GF}(p^k)$ contient toutes les images $\chi(a)$ ($a \in G$).

Nous avons alors :

(1.6) - Si χ appartient à $\text{GF}(p^k)$, le nombre n^* de caractères de la classe χ^* est égal à : $n^* = k/n$.

Car si χ appartient à $\text{GF}(p^k)$, tous les caractères de χ^* appartiennent aussi à $\text{GF}(p^k)$. Ainsi $[\chi(a)]^{p^k} = [\chi(a)]^{q^{k_1}} = \chi(a)$ et la suite : $\chi(a)$, $\chi(a)^q, \dots, \chi(a)^{q^{m-1}}$ ne peut contenir que k_1 éléments distincts.

De là, la classe χ^* contient seulement $n^* = k_1$ caractères distincts.

II

Nous montrons maintenant comment on peut déduire d'un ensemble $(\chi_1, \chi_2, \dots, \chi_k)$ de $\sum(G, p, m)$, ayant la propriété P_d , une matrice à éléments dans un sous-corps de $\text{GF}(p^m)$ et ayant la propriété P_d .

Nous utilisons le théorème suivant (Mac Duffee [5]) :

"Soit $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ un polynôme à coefficients dans un corps F et irréductible dans F . Soit ρ une racine de ce polynôme et considérons la matrice :

$$R = \begin{bmatrix} 0 & 0 & \dots & -a_n \\ 1 & 0 & \dots & -a_{n-1} \\ 0 & 1 & \dots & -a_{n-2} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -a_1 \end{bmatrix}$$

Alors la correspondance entre les corps $F(\rho)$ et $\mathfrak{F}(\rho)$:

$$\alpha = c_0 + c_1\rho + \dots + c_{n-1}\rho^{n-1} \longleftrightarrow c_0I + c_1R + \dots + c_{n-1}R^{n-1} = A$$

est biunivoque et est un isomorphisme pour l'addition et la multiplication".

On en déduit :

(2.1) - k éléments $\alpha_1, \alpha_2, \dots, \alpha_k$ de $F(\rho)$ sont linéairement indépendants par rapport à F , si et seulement si les premières lignes des matrices correspondantes $A_1, A_2, \dots, A_k$ dans $\mathfrak{F}(\rho)$, sous l'isomorphisme $\alpha \longleftrightarrow A$, sont linéairement indépendantes.

"Seulement" est trivial. D'autre part, si une matrice de $\mathfrak{F}(\rho)$ a sa première ligne nulle, elle est entièrement nulle, puisque $\mathfrak{F}(\rho)$ est un corps.

Appliquons ce résultat à $\sum(G, p, m)$. Si n divise k , le corps $\text{GF}(p^k)$ est une extension algébrique de $\text{GF}(p^n)$ de degré $k_1 = k/n$. Ainsi chaque élément de $\text{GF}(p^k)$ peut être représenté isomorphiquement comme une matrice d'ordre k_1 , dont les éléments sont dans $\text{GF}(p^n)$. Si χ est un caractère de $\sum(G, p, m)$, appartenant à $\text{GF}(p^k)$ (définition 5), $\chi(a)$ ($a \in G$) peut être exprimé comme une matrice d'ordre $k_1 = k/n$ ($= n^*$ le nombre de caractères dans la classe χ^* , d'après 1.6).

Désignons par $P(\chi(a), n^*)$ la première ligne de cette matrice d'ordre n^* . D'après (2.1) $P(\chi(a), n^*)$ représente $\chi(a)$ isomorphiquement. D'où il vient :

Proposition 2.2 - Si un ensemble $(\chi_1, \chi_2, \dots, \chi_k)$ de caractères de $\Sigma(G, p, m)$, non équivalents mod $\Phi(n)$, a la propriété P_d sur $GF(p^n)$ (n diviseur de m), alors on peut construire une matrice de g lignes et $(n_1^* + n_2^* + \dots + n_k^*)$ colonnes, à éléments dans $GF(p^n)$, qui a la propriété P_d . De plus le rang de cette matrice est égal au nombre des colonnes $(n_1^* + n_2^* + \dots + n_k^*)$; n_i^* ($i = 1, 2, \dots, k$) étant le nombre des caractères dans χ_i^* .

En effet, si nous remplaçons chaque élément $\chi_i(a)$ de la sous-matrice $(\chi_1, \chi_2, \dots, \chi_k)$ par $P(\chi_i(a), n_i^*)$, nous obtenons une matrice A de g lignes et $(n_1^* + n_2^* + \dots + n_k^*)$ colonnes, à éléments dans $GF(p^n)$, et la propriété P_d est préservée par (2.1). D'autre part, le rang de la matrice obtenue est bien $(n_1^* + n_2^* + \dots + n_k^*)$, car, par le corollaire (1.4), l'ensemble de toutes les classes $(\chi_1^*, \chi_2^*, \dots, \chi_{g^*}^*)$ mod $\Phi(n)$ de $\Sigma(G, p, m)$ a la propriété P_d sur $GF(p^n)$ et, si nous remplaçons chaque $\chi_i^*(a)$ de la matrice correspondante $(\chi_1^*, \chi_2^*, \dots, \chi_{g^*}^*)$ par $P(\chi_i^*(a), n_i^*)$, nous obtenons une matrice carrée d'ordre g , puisque $n_1^* + n_2^* + \dots + n_{g^*}^* = g$, et non singulière, par (1.4). Le résultat suit du fait que la matrice A est un sous-ensemble des g colonnes de cette matrice.

III

Nous donnons ici quelques ensembles de caractères de groupes abéliens possédant la propriété P_d , pour un d donné. Puis, utilisant les résultats de la section 2, nous montrons comment le résultat de Bose-Chaudhuri-Peterson, dans sa forme générale, se déduit de la considération des caractères d'un groupe cyclique.

Soit donc G un groupe abélien d'ordre g et d'invariants $(h_1, h_2, \dots, h_r)$. Nous désignons ses g caractères par :

$$\zeta_1^{u_1} \zeta_2^{u_2} \dots \zeta_r^{u_r} : (a_1, a_2, \dots, a_r) \longrightarrow \zeta_1^{u_1 a_1} \zeta_2^{u_2 a_2} \dots \zeta_r^{u_r a_r}$$

(3.1) - Si G est cyclique ($r=1$), alors tout ensemble $(\zeta, \zeta^2, \dots, \zeta^d)$ a la propriété P .

En effet, tout ensemble de d lignes $a_1, a_2, \dots, a_d$ de la sous-matrice $(\zeta, \zeta^2, \dots, \zeta^d)$ a la forme :

$$\begin{bmatrix} \zeta^{a_1} \zeta^{2a_1} & \dots & \zeta^{da_1} \\ \dots & \dots & \dots \\ \zeta^{a_d} \zeta^{2a_d} & \dots & \zeta^{da_d} \end{bmatrix}$$

et c'est une matrice non-singulière, puisque son déterminant est un déterminant de Vandermonde.

Dans le cas non-cyclique, les résultats sont plus complexes. Nous avons prouvé [4] :

(3.2) - L'ensemble $(1, \zeta_1, \zeta_2, \dots, \zeta_r)$ a la propriété P_2 .

(3.3) - L'ensemble $(1, \zeta_1, \zeta_1^2, \zeta_2, \zeta_2^2, \dots, \zeta_r, \zeta_r^2)$ a la propriété P_3 .

(3.4) - L'ensemble $(1, \zeta_1, \zeta_1^2, \zeta_1^3, \zeta_1, \zeta_1; i = 1, 2, \dots, r \text{ et } j \neq i)$ a la propriété P_4 .

et si $r = 2$:

(3.5) - L'ensemble $(1, \zeta_1, \zeta_1^2, \zeta_1^3, \zeta_1^4, i = 1, 2 \text{ et } \zeta_1 \zeta_2)$ a la propriété P_5 .

(3.6) - L'ensemble $(1, \zeta_1, \zeta_1^2, \zeta_1^3, \zeta_1^4, \zeta_1^5, i = 1, 2 \text{ et } \zeta_1 \zeta_2, \zeta_1 \zeta_2^2, \zeta_1^2 \zeta_2)$ a la propriété P_6 .

Le théorème de Bose-Chaudhuri-Peterson-Zierler s'énonce alors :

(3.7) - Soit G un groupe cyclique d'ordre h , p un nombre premier ne divisant pas h , m l'ordre de p dans le système des résidus mod h et n un diviseur de m . Alors, pour d donné, nous pouvons construire une matrice de h lignes et $R(h, d, n)$ colonnes, à éléments dans $GF(p^n)$, ayant la propriété P_d . $R(h, d, n)$ est donné par le nombre des résidus mod h distincts parmi : $i q^u$ ($i = 1, 2, \dots, d; u \geq 0$) $q = p^n$.

Par (3.1) l'ensemble $(\chi_1, \chi_2, \dots, \chi_d)$ a la propriété P_d ; ($\chi_1 = \zeta^1$). De là, l'ensemble $(\chi_{i_1}^*, \chi_{i_2}^*, \dots, \chi_{i_d}^*)$ obtenu de $(\chi_1, \chi_2, \dots, \chi_d)$ en ne retenant qu'un seul représentant de chaque classe mod $\Phi(n)$, à la propriété P_d sur $GF(p^n)$ par (1.3).

Mais la congruence ; $\chi_i = \chi_j \text{ mod } \Phi(n)$ est équivalente à :

$$i = j q^k \text{ mod } h \text{ pour un certain } k$$

et : $j = i q^{k'} \text{ mod } h \text{ pour un certain } k'.$

Ainsi, les ensembles $i q^u$ ($u = 0, 1, \dots, m/n-1$) et $j q^v$ ($v = 0, 1, \dots, m/n-1$) sont les mêmes et le nombre d' des classes distinctes est égal au nombre d'ensembles distincts parmi les d ensembles : ($i q^u; u \geq 0$) $i = 1, 2, \dots, d$, ces nombres étant pris mod h .

Si nous faisons maintenant la substitution : $\chi_i^*(a) \rightarrow P(\chi_i^*(a), n_i^*)$, $i = i_1, i_2, \dots, i_d$ dans la sous-matrice $(\chi_{i_1}^*, \chi_{i_2}^*, \dots, \chi_{i_d}^*)$, la propriété P_d est conservée, par (2.2) et le nombre de colonnes obtenues est égal à $R(d, h, n) = n_{i_1}^* + n_{i_2}^* + \dots + n_{i_d}^*$ par (2.2) ; et comme n_i^* est le nombre d'éléments dans χ_i^* , c'est-à-dire le nombre de résidus mod h distincts parmi : $i q^u$, $u = 0, 1, \dots, m/n-1$, nous avons bien :

$$R(d, h, n) = \text{nombre de résidus mod } h \text{ parmi } i q^u (i = 1, 2, \dots, d; u \geq 0).$$

Je voudrais exprimer ici toute ma reconnaissance à mon bon Maître R.C. Bose, pour avoir dirigé mon travail durant mon séjour à the University of North Carolina.

REFERENCES

- [1] BOSE R.C. et RAY-CHAUDHURI D.K. - "On a class of error correcting binary group codes" Information and Control, Vol. 3, No. 1, March 1960, pp. 68-79.
- [2] BOSE R.C. et RAY-CHAUDHURI D.K. - "Further results on error correcting binary group codes" Information and Control, vol. 3, sept. 1960, pages 279-290.
- [3] BOSE R.C. - "On some connections between the design of experiments and information theory" Bulletin de l'Institut International Statistique, No. 38 (1961).
- [4] FOATA D.C. - "On the construction of Bose-Chaudhuri matrices with the help of Abelian group characters" University of North Carolina, Institute of Statistics, Mimeograph Series No. 278.
- [5] Mac DUFFEE C.C. - "An introduction to Abstract Algebra" page 109.
- [6] PETERSON W.W. - "Encoding and error correction procedures for Bose-Chaudhuri Codes" I.R.E. Trans. on Information Theory, Sept. 1960.
- [7] VAN DER WAERDEN B.L. - "Modern Algebra", vol. 2, Frederick Ungar Pub. Co., New-York.
- [8] ZIERLER NEAL - "A class of cyclic linear error correcting codes in p^n symbols" M.I.T. Lincoln Laboratory Group Report 55-19.