J.-C. Panayiotopoulos

Recherche des collections speciales maximales du groupe $G = G(2) \times G(k)$, k pair

Archivum Mathematicum, Vol. 16 (1980), No. 1, 45--50

Persistent URL: `http://dml.cz/dmlcz/107054`

ARCH. MATH. 1, SCRIPTA FAC. SCI. NAT. UJEP BRUNENSIS
XVI: 45—50, 1980

RECHERCHE DES COLLECTIONS SPECIALES MAXIMALES DU GROUPE $G = G(2) \times G(k)$, k PAIR

J-C. PANAYIOTOPOULOS, Athens

(Received April 3, 1978)

Dans ce traité nous donnons un algorythme efficace pour trouver des permutations orthogonales du groupe $G = G(2) \times G(k)$. k pair, à l'aide des graphes et de Computer. Ainsi nous avons trouvé qu'il n'existe pas quatre permutations mutuellement orthogonales de G d'ordre $n = 20$, mais des centaines de triplets orthogonaux. Pour l'ordre $n = 12$ nous avons trouvé qu'il n'existe pas d'additions orthogonales, mais des collections parallèles de nombre cardinal 4 au plus. Nous donnons des exemples d'additions orthogonales d'ordre $n = 20$ et des collections parallèles d'ordre $n = 12$ et de nombre cardinal 4. Finalement, nous exprimons une conjecture sur les additions orthogonales de G avec $k = 0 \pmod 3$.

I. INTRODUCTION

Soit le groupe $G = G(2) \times G(k)$, k pair, ainsi que:

$$G = \{(0, 0), (0, 1), \ldots, (0, k - 1), (1, 0), (1, 1), \ldots, (1, k - 1)\}$$

avec $a \pm b = (c, d) \pm (e, f) = ((c \pm e) \pmod 2), (d \pm f) \pmod k)), a, b \in G$.

Dès 1960 Knuth, Chakravarti et Bose [1] ont utilisé le groupe G à trouver cinq permutations mutuellement orthogonales d'ordre $n = 2 \times 6 = 12$, ($k = 6$).

Une condition suffissante et nécessaire pour que deux permutations A, B, de G soient orthogonales, est que l'équation $Ax - Bx = c$ ait juste une solution $x \in G$, pour chaque $c \in G$, [2].

Définition 1.1. Un ensemble de permutations de G est appellé collection orthogonale ssi les éléments de l'ensemble pris deux à deux sont orthogonaux.

Définition 1.2. Une collection orthogonale S,

$$S = \{A_1, A_2, \ldots, A_m\}$$

est une addition orthogonale, ssi $A_j = A_1 + A_{j-1}$, $j = 3, 4, \ldots, m$, $m \geq 3$.

Dans [3] est montré qu'il existe des additions orthogonales avec $m \geqq 3$ et $n \neq 0 (\bmod 3)$ et $n \neq 2k$, k impair; nous avons aussi donné des constructions et des applications importantes dont la plupart concerne le groupe G; En fin nous avons démontré dans [3] qu' il n'existe pas d'addition orthogonale avec $m \geqq 4$ du group G. Si A_m est la permutation de G telle que:

$$A_m(a_1, b_1) = (a_1^m, b_1^m), A_m(a_2, b_2) = (a_2^m, b_2^m), \dots, A_m(a_n, b_n) = (a_n^m, b_n^m)$$
$$\text{avec } (a_i, b_i) \in G \quad \text{et} \quad (a_i^m, b_i^m) \in G, \quad i = 1, 2, \dots, n,$$

alors la permutation A_m sera noté en suite:

$$A_m = \{(a_1^m, b_1^m), (a_2^m, b_2^m), \dots, (a_n^m, b_n^m)\}.$$

2. UN MEILLEUR CRITÈRE

Dire que deux permutations de G, A et B, sont orthogonales, ssi l'équation $Ax - Bx = c \in G$ a juste une solution dans G, c' est un critère qui ne permet pas l'utilisation d'un Computer pour des ordres $n \geqq 20$. Cela est clair dans [4], chapitre 13, page 481, où est cité d'une manière caractéristique que „Bose, Chakravarti, and Knuth also proposed to consider the case $n = 20$ but this proved to be too large a problem for the available computer". Cependant il y avait aussi l'oppinion qu'une condition plus vite serait nécessaire sur la question si les permutations A et B de G sont orthogonales ou s'ils ne le sont pas. Un tel critère trouvé dans [5] est le suivant:

Théorème 2.: *Une condition suffisante et nécessaire pour que les permutations A_m, A_g de G soient orthogonales est que soit valable* $(b_i^g + b_r^m) (\bmod k) \neq (b_r^g + b_i^m) (\bmod k)$ *pour chaque $i \neq r \in I = \{1, 2, \dots, n\}$ pour laquelle $a_i^g = a_i^m$ et $a_r^g = a_r^m$ or $a_i^g \neq a_i^m$ et $a_r^g \neq a_r^m$.*

Par conséquent en ayant une permutation donné A_m de G, il est possible de trouver toutes ses orthogonales. Pour la solution de ce problème nous donnons l'algorithme suivant, qui nous sera util à la suite de ce traité.

PAS 1: On prend une des permutations $n!$ de l'ensemble I. Soit W_t, $t = 1, 2, \dots, n$ la conséquence qui décrit chaque fois la permutation (p. ex. pour la permutation identitif on a $W_1 = 1, W_2 = 2, \dots, W_n = n$).

PAS 2: On transforme W_t en permutation A_g de G telle que $a_i^g = 0$ et $b_i^g = W_i - 1$ si $i \leqq k$, mais $a_i^g = 1$ et $b_i^g = W_i - k - 1$, si $i > k$.

PAS 3: Pour chaque $i = j \in I$ où on a $a_i^m = a_i^g$ et $a_j^m = a_j^g$ or $a_i^m \neq a_i^g$ et $a_j^m \neq a_j^g$ on forme S_1 et S_2 telles que:

$$S_1 = (b_i^m + b_j^g) (\bmod k), \qquad S_2 = (b_j^m + b_i^g) (\bmod k).$$

Si pour un couple quelconque $(i,j) \in I^2$ on a $S_1 = S_2$, voir PAS 1.

PAS 4: Les permutations A_m, A_g sont orthogonales. Voir PAS 1.

Cet algorithme finira evidemment si les permutations $n!$ de l'ensemble I, du PAS 1, seront épuisés. Le programme de L'algorithme en FORTRAN IV est à la disposition du chercheur.

3. COLLECTIONS ORTHOGONALES ET GRAPHES

Soit X_n l'ensemble de collections orthogonales d'ordre n. Chaque élément de X_n est appellé maximal, ssi il n'y a pas d'autre qui le contient. Un graphe est appellé une clique, si pour chaque couple de ses sommets il y a l'arête correspondante [6].

Lemme 3.1.: *Des éléments de X_n sont équivalents à un graphe non orienté.*

Démonstration. Soient $X^1, X^2 \in X_n$. Si on pose $X^{12} = X^1 \cup X^2$ et considère comme sommets x_i les éléments de X^{12} et comme arêtes (x_i, x_j) le fait que la permutation x_i est l'orthogonale de x_j, il en resulte un graphe. Ce graphe est non orienté car si x_i est l'orthogonale de x_j, alors x_j aussi est l'orthogonale de x_i; Par conséquent l'existence de l'arête (x_i, x_j) montre aussi l'existence simultanée de la (x_j, x_i).

A la suite chaque graphe de ce type sera noté par H.

Théorème 3.2.: *Une collection de permutations de G est un élément de X_n, ssi elle est équivalente á un graphe-clique, de type H.*

Démonstration. Soit $X^t \in X_n$. D'après 3.1, X^t sera équivalente à un graphe de type H. Supposons que ce graphe n'est pas une clique. Donc il existe $x_i, x_j \in X^t$ de façon que l'arête n'existe pas. Il en resulte alors que les permutations x_i, x_j ne sont pas orthogonales. Par conséquent d'après 1.1 découle que X^t n'est pas une collection orthogonale. Mais cela est absurde, puisque on a supposé que $X^t \in X_n$. Donc H est une clique. Inversement; soit H une clique. Alors chaque couple de ses sommets aura l'arête correspondante. Alors la collection constituée de ses sommets est orthogonale et par conséquent $X^t \in X_n$.

Un sous-graphe est dit intérieurement stable ssi deux de ses sommets quelconques ne se lient pas, [7].

Définition 3.3. Le sous-graphe intérieurement stable maximal de H sera nommé base de H et noté par H^*.

Définition 3.4. Deux éléments X^r, X^t de X_n sont dit parallèles ssi aucune permutation de l'un n'est pas orthogonale à la permutation quelconque de l'autre et $X^r \cap \cap X^t = \emptyset$.

Theorème 3.5. *Chaque collection orthogonale maximale contient juste un élément de la base.*

Démonstration. Les éléments de H^* sont indépendants l'un de l'autre quant à la relation d'orthogonalité. Soit X^t maximale dans H et $t_1, t_2 \in X^t$, $t_1, t_2 \in H^*$.

Il s'en suit que l'arête (t_1, t_2) n'existe pas. Donc t_1, t_2 ne sont pas orthogonals et X' n'est pas une clique; Ainsi d'après 3.2 il en resulte que $X' \notin X_n$. D'ailleurs si on suppose que $X' \cap H^* = \emptyset$, alors il existe $r \in H^*$, ainsi que $(X'U\{r\}) \in X_n$, car sinon la base sera $H^*U\{x\}$, $x \in X'$. Par conséquent la collection X' n'est pas maximale. Ainsi afin que X' soit maximale dans H, il est nécessaire qu'elle contienne juste un élément de H^*.

Finalement on doit noter que le critère 3.5 est des seuls qui existent pour les collections orthogonales maximales.

4. L'ALGORITHME

Notre problème principal est, „trouver les collections orthogonales maximales de G, *d*'ordre n". D'après 3.1, il est possible que les permutations des éléments de G constituent les sommets d'un graphe de type H. D'ailleurs d'après 3.2 en resulte que notre problème est équivalent à, „si on a un graphe H, trouver ses cliques maximales". On sait que dans la théorie des graphes afin de trouver toutes les cliques on résout le système:

$$(\hat{X} . x) * x = 0 . (1).$$

où $\hat{X}$ la négation Booléene de la matrice X de H, $(.)$ le symbole de la multiplication, $(*)$ le symbole de la multiplication Booléene et x le vecteur charactéristique de H, [7]. La difficulté y est à la construction de la matrice $X = (h_{ij})$, $i, j \in J$ où, pour simplifier au lieu de l'ensemble des permutations de H, $J \equiv \{A_1, A_2, \ldots, A_s\}$ on pose $J = \{1, 2, \ldots, s\}$. On donne les éléments de X comme il suit:

$$\begin{aligned} h_{ij} &= 1, \text{ si } A_i, A_j \text{ sont orthogonales} \\ &= 0, \text{ autrement.} \end{aligned}$$

Mais ce serait inapplicable de construire X avec toutes les permutations de G. Mais, si J contient seulement les orthogonales à l'identitive de G, alors le problème se simplifie, et, comme nous alons voir à la suite, il devient envisageable. Finalement, à cause de la nature du système (1), la relation „a, b sont orthogonals" s'extend par la relation:

„a, b sont orthogonals or $a = b$".

Cela signifie, que chaque sommet de H a une boucle. A la suite on donne l'algorythme de la solution de notre problème, dont les pas succésifs sont:

PAS 1: Donner la classe $n = 0 \pmod 4$.
PAS 2: Trouver toutes les permutations orthogonales à l'identitive de G, à aide de l'algorithme du paragraphe 2.
PAS 3: Utiliser l'algorithme du paragraphe 2 la m-ème permutation de l'ensemble J.

PAS 4: Trouver la m-ème ligne de la matrice X, ainsi que:
$h_{mi} = 1$ si les permutations m et i sont orthogonales or $i = m$, $i \in J$. Autrement poser $h_{mi} = 0$.
PAS 5: Si $m \leqq s$, retourner au PAS 3.
PAS 6: Construire la matrice $\hat{X}$.
PAS 7: Resoudre le système $(\hat{X} . x) * x = 0$.
PAS 8: Choisir les cliques maximales.

Il est évident que l'utilisation d'un Computer est une necessité. Le programme de l'algorithme en FORTRAN IV est à la disposition du chercheur.

5. APPLICATIONS

D'abord, par l'algorithme du parag. 4 une recherche expérimentale sur le groupe G par $n = 8$ a eu lieu, pour l'invention d'additions orthogonales. Ainsi nous avons trouvé 16 additions orthogonales de $m = 3$; nous en donnons une, où, pour simplifier, au lieu de $(a, b) \in G$ nous posons ab:

00	01	02	03	10	11	12	13
00	13	03	10	12	01	11	02
00	10	01	13	02	12	03	11

A la suite une recherche sur le groupe G d'ordre $n = 12$ a eu lieu pour l'invention des collections orthogonales, des additions orthogonales et des collections parallèles. Nous avons ainsi trouvé des quintuplets orthogonaux resultat qu'on avait aussi obtenu dans [1], [8]; mais nous n'avons pas trouvé aucune addition orthogonale; au contraire nous avons trouvé des collections parallèles chacune de nombre cardinal 4. Par conséquent on a:

Corolaire 5.1. Dans le groupe $G = G(2) \times G(6)$ n'existe pas d'additions orthogonales. Au contraire il existe des collections parallèles de nombre cardinal maximal quatre:

00	01	02	03	04	05	10	11	12	13	14	15
00	13	01	14	12	02	11	15	05	03	10	04
00	04	15	01	14	11	12	05	03	02	13	10
00	15	13	04	10	03	05	14	02	12	01	11
...	...	...	...	...	...	...	...	...	...	...	...
00	01	15	10	11	05	13	14	02	03	04	12
00	10	11	01	05	02	14	12	15	13	03	04
00	11	02	04	14	01	12	05	03	15	13	10
00	12	10	14	03	13	15	04	05	02	11	01

Finalement une longue recherche sur le groupe G de $n = 20$ a eu lieu. Nous avons trouvé un grand nombre de triplets orthogonaux; certains en sont des additions orthogonales. Mais nous n'avons pas trouvé aucun quadruplet orthogonal. Nous avons donc:

Corolaire 5.2. Dans le groupe $G = G(2) \times G(10)$ n'existe pas un quadruplet orthogonal.

On donne deux additions orthogonales de G avec $n = 20$:

$$\{A_3, A_2, A_1\}, \qquad \{A_3, A_4, A_5\} \qquad \text{où}$$

A_1: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19.
A_2: 00 02 04 06 08 10 12 14 16 18 19 01 03 05 07 09 11 13 15 17.
A_3: 00 09 08 07 06 15 14 13 12 11 01 10 19 18 17 16 05 04 03 02.
A_4: 00 08 06 04 02 10 18 16 14 12 11 09 07 05 03 01 19 17 15 13.
A_5: 00 07 04 01 08 05 02 09 06 03 12 19 16 13 10 17 14 11 18 15.

Actuellement la recherche concernant le groupe G avec $n = 24$ continue; mais une recherche pas complète encore (1978) n'a pas donné une addition orthogonale, tandis qu'on a pour le moment trouvé des quadruplets orthogonaux. Cela permet d'en formuler la conjecture ci-dessous:

Conjecture 5.3. Pour le groupe $G = G(2) \times G(k)$, $n = 2k$, si $k = 0 \pmod 3$ alors il n'existent pas des additions orthogonales, mais si $n \neq 0 \pmod 3$ et $n = 0 \pmod 4$ alors il existe des additions orthogonales, seulement avec $m = 3$.

RÉFÉRENCES

[1] R. C. Bose, I. M. Chakravarti, D. E. Knuth: *On Methods of Constructing Sets of Mutually Orthogonal Latin Squares Using a Computer.* Technometrics, 2, 1960, 507—516

[2] H. B. Mann: *The construction of orthogonal latin squares.* Ann. Math. Stat., 13, 1942, 418—423

[3] J-C. Panayiotopoulos: *Orthogonal additions of Abelian groups.* Aequat. Mathematicae. To appear

[4] J. Dénes, A. D. Keedwell: *Latin squares and their applications.* London 1974

[5] J-C. Panayiotopoulos: *About latin squares of standard form and of even order.* PH. D. dissertation, University of Athens 1976

[6] C. Berge: *Théorie des Graphes et ses applications.* Paris 1958

[7] V. DiGiorgio: *Application de l'Algèbre de Boole a l'étude des Graphes.* Math. et Sciences Humaines, 36, 1971, 33—58

[8] D. M. Johnson, A. L. Dulmage, N. S. Mendelsohn: *Orthomorphisms of groups and orthogonal Latin squares.* Canad. J. Math. 13, 1961, 356—372

J-C. Panayiotopoulos
Athens 708 Vatazi 16,
Greece