Agrégation externe de mathématiques
Épreuve de modélisation, option C : algèbre et calcul formel

(*Texte public*)

Résumé : On présente un problème qui se rencontre dans de nombreuses applications pratiques, et qui est connu sous le nom de “design”. Pour le résoudre, on introduira des techniques arithmétiques et matricielles, et on déduira de ces constructions multiples un résultat classique de théorie des groupes.

Mots clefs : algèbre linéaire, corps finis

► *Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Des suggestions de développement, largement indépendantes les unes des autres, vous sont proposées en fin de texte. Vous n'êtes pas tenu(e) de les suivre. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury appréciera que la discussion soit accompagnée d'exemples traités sur ordinateur.*

1. Présentation du problème

Le problème suivant est typique de nombreuses situations combinatoires : sept golfeurs passent une semaine dans un domaine qui propose deux terrains de golf. Ils décident que chacun jouera tous les jours, et que chaque jour, ils se sépareront en deux groupes : un groupe de trois qui jouera sur le premier golf, l'autre de quatre jouant sur le deuxième golf. Ils se demandent comment arranger ces groupes pour que :

— chaque golfeur puisse jouer dans le groupe de trois (donc sur le premier golf) le même nombre de fois que les autres (et de même avec le groupe de quatre) ;
— sur le premier golf, les groupes sont arrangés de façon à ce que chaque joueur joue exactement une fois contre chacun des autres.

Pour formaliser et résoudre ce problème, on est amené à introduire la notion de *design*, qui est décrite et étudiée dans les sections 2 et 3.

Une manière simple de construire des designs, et donc de résoudre des problèmes comme celui des golfeurs, est de faire appel à une classe particulière de matrices, appelées matrices de type H. Celles-ci sont introduites et étudiées dans la section 5.

2. Design

Définition 1. *Soit S un ensemble fini à v éléments et λ un entier non nul. Un $(v,k,\lambda)-$design sur S est un ensemble de b sous-ensembles à k éléments de S avec $k<v$, appelés blocs, tel que chaque paire d'éléments de S apparaisse dans exactement λ blocs.*

Par exemple, dans l'exemple des golfeurs ci-dessus, on a affaire à un $(7,3,1)-$design.

Pour qu'un design puisse exister, il faut des conditions sur v, k, et λ que nous explorons maintenant.

Théorème 1. *Soit un $(v,k,\lambda)-$design, composé de b blocs. Alors chaque élément apparaît dans exactement r blocs, avec $\lambda(v-1)=r(k-1)$ et $bk=vr$.*

En effet, supposons qu'un élément x apparaisse dans r blocs. Dans chacun de ces r blocs, il est apparié avec $k-1$ éléments. Il y a donc au total $r(k-1)$ paires dans les blocs qui contiennent x. Mais x est d'autre part appairé λ fois avec chacun des $v-1$ éléments.

D'autre part, les b blocs contiennent en tout bk éléments (en incluant les répétitions). Mais chaque élément apparait r fois dans les blocs. □

Ce résultat permet, par exemple, de voir qu'il ne peut pas exister de $(11,6,2)-$design, ou plus généralement, que s'il existe un $(v,3,1)$-design, alors $v\equiv 1$ ou $3 \bmod 6$.

3. Matrices d'incidence

Définition 2. *Soit $\mathscr{D}$ un $(v,k,\lambda)-$design sur S. On numérote les éléments de $\mathscr{D}$ et de S de façon arbitraire.*

La matrice d'incidence associée à $\mathscr{D}$ composé de b blocs est la matrice A de taille $b\times v$ telle que $A(i,j)=1$ si le i-ème bloc contient le j-ème élément, et 0 sinon.

On notera que la matrice d'incidence est définie à permutation près des lignes et des colonnes.

Notons I la matrice identité d'ordre v, J la matrice $v\times v$ dont tous les coefficients valent 1 et A^T la transposée de A. La notion de matrice d'incidence permet de donner une reformulation de la définition de (v,k,λ)-design :

Proposition 1. *Soit A une matrice $b\times v$ ne comportant que des 0 et des 1. Il est équivalent de dire :*

(1) A est la (une) matrice d'incidence d'un (v,k,λ)-design ;

(2) On a $A(1,\dots,1)^T=k(1,\dots,1)^T$ et $A^T\cdot A=(r-\lambda)I+\lambda J$.

Cette proposition permet, en particulier, d'obtenir le corollaire suivant :

Théorème 2. *Dans un (v,k,λ)-design, le nombre de blocs b est $\geqslant v$.*

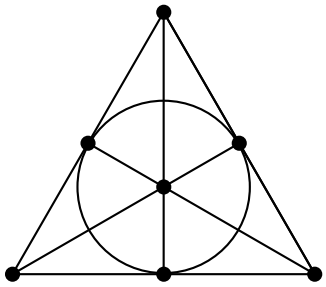
Démonstration. On vérifie que $A^T.A$ est inversible, d'où $v=\operatorname{rang}(A^T\cdot A)\leqslant\operatorname{rang}(A)$, d'où le résultat. □

4. Constructions de $(7,3,1)$-designs

4.1. *Une construction géométrique*

Proposition 2. *Soit $S_0 = \mathbb{F}_2^3 - \{(0,0,0)\}$. Les parties $\mathscr{P} - \{(0,0,0)\}$, où $\mathscr{P}$ est un sous-espace de dimension 2 du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^3$ constituent un $(7,3,1)$-design sur S_0.*

Nous noterons ce design $\mathscr{D}_0$. Il est usuellement représenté graphiquement de la manière suivante, dessin sur lequel les points représentent des points de $\mathbb{F}_2^3 - \{(0,0,0)\}$, et les segments (ainsi que le cercle) les blocs.



4.2. *Une construction arithmétique*

Proposition 3. *Soit $S_1 = \mathbb{F}_7$. Les ensembles $\{i + x^2, x \in \mathbb{F}_7^*\}$, pour i décrivant S_1, forment un $(7,3,1)$-design sur S_1.*

Ce design sera noté $\mathscr{D}_1$. Cette seconde construction amène naturellement à la question de savoir quand deux designs Δ_0 et Δ_1 sur S et S' sont isomorphes. Une notion naturelle d'isomorphisme consiste à dire que deux designs sont isomorphes si les blocs des deux designs sont les mêmes, une fois défini un "renommage" des éléments de S vers S'.

Plus formellement, un isomorphisme entre deux designs est une bijection $\phi : S \to S'$ telle que $\Delta_1 = \{\{\phi(x), x \in U\}, U \in \Delta_0\}$. On a alors :

Proposition 4. *Les deux designs $\mathscr{D}_0$ et $\mathscr{D}_1$ sont isomorphes.*

Si $S = S'$ et $\Delta_0 = \Delta_1$, nous parlerons d'automorphisme. L'ensemble des automorphismes d'un design est un groupe pour la composition, et on peut remarquer que deux designs isomorphes ont des groupes d'automorphismes isomorphes. En particulier, on a :

Théorème 3. *Le groupe des automorphismes de $\mathscr{D}_0$ et de $\mathscr{D}_1$ est isomorphe à $GL_3(\mathbb{F}_2)$.*

Démonstration. Si ϕ est une bijection de S_0, on prolonge ϕ à $\mathbb{F}_2^3$ en posant $\phi((0,0,0)) = (0,0,0)$, puis on pourra commencer par observer que l'image d'un plan par ϕ est un plan. □

Nous donnerons une seconde description de ce groupe d'automorphismes en fin de texte.

5. Matrices de type H

5.1. *Définition*

Définition 3. *On dit qu'une matrice $M \in \mathscr{M}_n(\mathbb{R})$ est une matrice de type H si*

— *ses coefficients sont tous* 1 *ou* −1
— *et ses colonnes sont orthogonales deux à deux pour le produit scalaire euclidien.*

Une caractérisation équivalente à la seconde condition est que M vérifie $M^T.M = n.I_n$.
Voyons quelques exemples de matrices de type H :

$$\begin{pmatrix} 1 \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Proposition 5. *La classe des matrices de type H est stable par multiplication de lignes ou de colonnes par* −1*, ainsi que par permutation de lignes ou de colonnes. Elle est également stable par transposition.*

Au vu de ces propriétés, on peut convenir d'une standardisation pour les matrices de type H. Une matrice de type H est dite *standardisée* si sa première ligne et sa première colonne sont constituées de +1. On peut toujours ramener une matrice de type H à cette forme en opérant la multiplication par −1 de certaines lignes et colonnes.
Une conséquence de cette standardisation est qu'une matrice de type H est de taille paire (pour $n > 1$) : compter les −1 de la seconde ligne, par exemple. Toujours en comptant, on vérifie qu'il y a $n(n-1)/2$ fois −1 et $n(n+1)/2$ fois +1 dans la matrice. On peut même montrer un peu plus :

Théorème 4. *La taille n d'une matrice de type H est* 1, 2, *ou un multiple de* 4.

On a déjà vu que, pour $n > 1$, la dimension est paire. On se ramène au cas où les $n/2$ premiers coefficients de la deuxième ligne valent 1 et les $n/2$ suivants valent −1 ; en comparant les positions des +1 et des −1 dans la troisième ligne, on trouve le résultat.

5.2. *Designs de type H*

Les matrices de type H permettent de construire les *designs de type H* comme suit.

Théorème 5. *Considérons une matrice de type H standardisée de taille* $4(n+1)$*. On efface la première ligne et la première colonne ; on remplace les* −1 *par des* 0 *dans la sous-matrice obtenue : le résultat est la matrice d'incidence d'un design* $(4n+3, 2n+1, n)$.

5.3. *Retour sur le design* $\mathscr{D}_1$

Soit $\chi : \mathbb{F}_7 \to \{\pm 1\}$ la fonction définie par

$$\chi(x) = \begin{cases} 1 & \text{s'il existe } y \in \mathbb{F}_7^* \text{ avec } y^2 = x \\ -1 & \text{sinon.} \end{cases}$$

Notons $v_0 = (0,1)$ et, pour $1 \leq i \leq 7$, $v_i = (1,i)$ un ensemble de représentants de la droite projective $\mathbb{P}^1(\mathbb{F}_7)$ dans $\mathbb{F}_7^2$. À un tel ensemble de représentants $\mathbf{v}$, on peut associer la matrice

$$M(\mathbf{v}) = (\chi(\det(v_i, v_j)))_{0 \leqslant i,j \leqslant 7}.$$

Proposition 6. *La matrice $M(\mathbf{v})$ est une matrice de type H, qu'on peut rendre standardisée en multipliant la première ligne par -1. Le design de type H correspondant est le design $\mathscr{D}_1$.*

Soit maintenant $X \in SL_2(\mathbb{F}_7)$. La matrice construite sur le même principe en utilisant $w_0 = Xv_0, \ldots, w_7 = Xv_7$ définit le même design (on a juste changé de système de représentants). À un élément de $SL_2(\mathbb{F}_7)$, on associe donc un automorphisme du design $\mathscr{D}_1$.

Enfin, $X \in SL_2(\mathbb{F}_7)$ ne peut envoyer chaque v_i sur un représentant de la même classe que si $X = \pm I_2$. On déduit de l'ensemble de ces remarques le théorème suivant : .

Théorème 6. *Le groupe des automorphismes de $\mathscr{D}_1$ contient un sous-groupe isomorphe à $PSL_2(\mathbb{F}_7) := SL_2(\mathbb{F}_7)/\{\pm I_2\}$. En conséquence, on a l'isomorphisme $GL_3(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_7)$.*

Suggestions pour le développement

► *Soulignons qu'il s'agit d'un menu à la carte et que vous pouvez choisir d'étudier certains points, pas tous, pas nécessairement dans l'ordre, et de façon plus ou moins fouillée. Vous pouvez aussi vous poser d'autres questions que celles indiquées plus bas. Il est très vivement souhaité que vos investigations comportent une partie traitée sur ordinateur et, si possible, des représentations graphiques de vos résultats.*

— Pouvez-vous, similairement à l'exemple des golfeurs du début du texte, donner la solution au problème suivant : donner une liste de sous-ensembles de $1, \ldots, 6$ avec la propriété que chaque sous-ensemble a exactement trois éléments et que chaque paire d'éléments apparaisse dans exactement deux de ces sous-ensembles ?

— Compléter certaines des preuves ou affirmations mathématiques esquissées dans le texte.

— Si A est la matrice d'incidence d'un (v,k,λ)-design, montrer que A^T est la matrice d'incidence d'un (v,r,λ)-design si et seulement si $b = v$. Ces deux designs sont-ils isomorphes ?

— Proposer une preuve du théorème 5 et en déduire des exemples de designs.

— Dans les matrices de type H, étudier si la deuxième condition de la définition 3 est équivalente à $M.M^T = n.I_n$ (donc que les lignes soient orthogonales deux à deux).

— Montrer qu'on peut numéroter les sommets de la figure de la partie 4.1 et les blocs de sorte que la matrice d'incidence correspondante soit symétrique.

— Peut-on généraliser les constructions de $\mathscr{D}_0$, $\mathscr{D}_1$ à d'autres designs ?

— Montrer que si H est une matrice de type H, alors

$$H' = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}.$$

est également une matrice de type H. En déduire une nouvelle construction d'un $(7,3,1)$-design ; est-il isomorphe aux précédents ?

— En généralisant la proposition 6, montrer que si $q = 3 \bmod 4$ est un nombre premier, il existe une matrice de type H de dimension $q+1$.

— Comment se lit l'isomorphisme entre deux designs sur la matrice d'incidence ?