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

(*Texte public*)

Résumé : On étudiera certains codes linéaires dont le polynôme des poids est stable par l'action d'un groupe afin d'en déduire des contraintes sur les poids.

Mots clefs : codes correcteurs d'erreur, groupes agissant sur un ensemble.

► *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.*

Les codes correcteurs d'erreurs jouent un rôle important dans les transmissions sur des canaux bruités. Pour juger de la capacité de détection des erreurs par un code (linéaire), on souhaite obtenir la distribution des poids des mots qu'il contient. Ceci peut se faire par une énumération, coûteuse lorsque le code contient beaucoup de mots. Cependant pour une classe particulière de codes linéaires, dits auto-orthogonaux, on peut tirer parti de propriétés de "symétrie" pour obtenir cette distribution plus aisément. C'est ce que propose d'illustrer le texte en déroulant un petit exemple.

1. Fonction de poids d'un code linéaire binaire

Dans la suite, pour $n > 0$ on considère le $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^n$ muni d'une fonction "poids" $w : \mathbb{F}_2^n \to \mathbb{N}$ qui à un vecteur $c \in \mathbb{F}_2^n$ associe le nombre de coordonnées égales à 1 dans c. On notera $\mathscr{C}$ un code linéaire binaire (c.-à-d. sur $\mathbb{F}_2$) de *paramètres* $[n,k,d]$, ce qui signifie que $\mathscr{C}$ est un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k tel que $\min_{c\in\mathscr{C}\setminus\{0\}}(w(c)) = d$. L'information sur *la distance minimale d* n'est parfois pas suffisante pour juger de la qualité d'un code : le nombre de mots de poids d compte et la distribution des mots de poids supérieur aussi. De ce fait, on peut souhaiter connaître la distribution de tous les poids des mots du code. On introduit pour cela la *fonction de poids* définie par le polynôme

$$W_{\mathscr{C}}(X,Y) = \sum_{i=0}^{n} A_i\, X^{n-i}\, Y^i \in \mathbb{C}[X,Y] \tag{1}$$

où pour tout $0 \le i \le n$, $A_i = \#\{c \in \mathscr{C},\ w(c) = i\}$.

Un tel polynôme est *homogène*, c'est-à-dire que tous ses monômes ont le même degré (à savoir n).

Exemple 1. *Pour le code* $\mathscr{C} = \{(0,0),(1,1)\}$, *on a* $W_{\mathscr{C}} = X^2 + Y^2$.

Exemple 2. *Un code $\mathscr{C}$ étant un sous-espace vectoriel, il peut être représenté par le noyau d'une matrice H de rang maximal, dite* de contrôle *pour le code $\mathscr{C}$. Par exemple le noyau de*

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

définit un code $\mathscr{H}$ de paramètres $[7,4,3]$. *En énumérant les mots du code, on obtient* $W_{\mathscr{H}} = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$.

À partir d'un code $\mathscr{C}$ de paramètres $[n,k,d]$ avec d impair, on peut construire un code $\mathscr{C}'$ de paramètres $[n+1,k,d+1]$ en considérant l'ensemble des vecteurs $c = (c_1,\dots,c_{n+1}) \in \mathbb{F}_2^{n+1}$ tels que $(c_1,\dots,c_n) \in \mathscr{C}$ et $\sum_{i=1}^{n+1} c_i = 0$. Le code $\mathscr{H}$ de l'exemple 2 donne ainsi un code de paramètres $[8,4,4]$ que nous noterons $\mathscr{S}$. Par construction, on a $W_{\mathscr{S}} = X^8 + 14X^4Y^4 + Y^8$. Une détermination directe de $W_{\mathscr{S}}$ en utilisant des propriétés de symétrie du code servira d'exemple dans la suite du texte.

2. Fonction de poids du code orthogonal

Soit $\mathscr{C}$ un code de paramètres $[n,k,d]$. À partir de $\mathscr{C}$, on peut construire le *code orthogonal* $\mathscr{C}^\perp$ qui est l'ensemble des vecteurs $c' \in \mathbb{F}_2^n$ tels que $c' \cdot c = 0$ pour tout $c \in \mathscr{C}$ où $\cdot$ désigne la forme bilinéaire symétrique canonique de $\mathbb{F}_2^n$:

$$(c'_1,\dots,c'_n)\cdot(c_1,\dots,c_n) = c'_1c_1 + \cdots + c'_nc_n. \tag{3}$$

Le code $\mathscr{C}^\perp$ est de longueur n et de dimension $n-k$. On a également le résultat suivant sur la fonction de poids du code orthogonal.

Théorème 1. *Si $\mathscr{C}$ est un code de paramètres $[n,k,d]$ alors*

$$W_{\mathscr{C}^\perp}(X,Y) = \frac{1}{2^k} W_{\mathscr{C}}(X+Y, X-Y). \tag{4}$$

La démonstration de ce théorème repose sur le lemme suivant qui est une version de la formule de sommation de Poisson. On notera dans la suite $\phi : \mathbb{F}_2 \to \{0,1\} \subset \mathbb{Z}$ la fonction définie par $\phi(0) = 0$ et $\phi(1) = 1$.

Lemme 1. *Soit $\mathscr{C}$ un code de paramètres $[n,k,d]$. Pour toute fonction $f : \mathbb{F}_2^n \to \mathbb{C}$ on définit la fonction $\hat{f} : \mathbb{F}_2^n \to \mathbb{C}$ par*

$$\hat{f}(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{\phi(u\cdot v)} f(v). \tag{5}$$

Alors

$$\sum_{u \in \mathscr{C}^\perp} f(u) = \frac{1}{2^k} \sum_{u \in \mathscr{C}} \hat{f}(u). \tag{6}$$

Démonstration. Après inversion des deux sommations du membre de droite, il suffit de remarquer que $\sum_{u\in\mathscr{C}}(-1)^{\phi(u\cdot v)} = 2^k$ si $v \in \mathscr{C}^\perp$ et 0 sinon (en effet dans ce second cas, l'étude de l'application $\pi_v : \mathscr{C} \to \mathbb{F}_2$ définie par $\pi_v(u) = u\cdot v$ montre que $u\cdot v$ prend autant de fois la valeur 0 que la valeur 1). □

Démonstration du théorème. On applique le lemme à la fonction $f(u) = x^{n-w(u)}\, y^{w(u)}$ avec $x, y \in \mathbb{C}$ et on remarque alors que pour $u = (u_1, \ldots, u_n)$ on a

$$\hat{f}(u) = \sum_{v_1\in\mathbb{F}_2} \cdots \sum_{v_n\in\mathbb{F}_2} \prod_{i=1}^{n} (-1)^{\phi(u_i v_i)}\, x^{\phi(1-v_i)}\, y^{\phi(v_i)} \tag{7}$$

$$= \prod_{i=1}^{n} \sum_{t\in\mathbb{F}_2} (-1)^{\phi(u_i t)}\, x^{\phi(1-t)}\, y^{\phi(t)} \tag{8}$$

$$= (x+y)^{n-w(u)}\,(x-y)^{w(u)} \tag{9}$$

car si $u_i = 0$ alors la somme interne de (8) vaut $x+y$ et si $u_i = 1$ elle vaut $x-y$. On en déduit le résultat. □

3. Fonction de poids d'un code auto-orthogonal

Un code $\mathscr{C}$ de paramètres $[n,k,d]$ est dit *auto-orthogonal* lorsque $\mathscr{C} = \mathscr{C}^\perp$. Ceci n'est possible que si n est pair et $k = n/2$.

Exemple 3. *Le code $\mathscr{S}$ introduit juste après l'exemple 2 est auto-orthogonal.*

Ainsi, lorsque le code $\mathscr{C}$ est auto-orthogonal, on a d'une part

$$W_{\mathscr{C}}(X,Y) = \frac{1}{2^k} W_{\mathscr{C}}(X+Y, X-Y) \tag{10}$$

et d'autre part n est pair et $k = n/2$.
Ces formules peuvent être interprétées algébriquement comme suit. Si pour une matrice $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ et pour un polynôme homogène non nul

$$f(X,Y) = \sum_{i=0}^{s} B_i\, X^i\, Y^{s-i} \in \mathbb{C}[X,Y] \tag{11}$$

on note $f.M = f(\alpha X + \beta Y, \gamma X + \delta Y)$, on dit que f est *invariant par M* si $f.M = f$. Si f est invariant par toutes les matrices M d'un groupe G, on dit que f est *invariant par G*. Lorsque G est un groupe fini, on peut produire des polynômes homogènes f invariants par G grâce au lemme suivant.

Lemme 2. *Soit $h(X,Y)$ un polynôme homogène de degré s. Si*

$$f = \frac{1}{\#G} \sum_{M\in G} h.M \tag{12}$$

est non nul alors f est invariant par G.

Dans le cas d'un code $\mathscr{C}$ auto-orthogonal, on voit que le polynôme $W_{\mathscr{C}}$ est invariant par le groupe G d'ordre 4 engendré par les matrices $M_0 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ et $J = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$. Nous allons chercher des polynômes homogènes de petit degré invariants par G. Il n'y a pas de tel polynôme de degré 1. En appliquant le lemme 2 avec $P = X^2$ et $P = Y^2$ et en effectuant des combinaisons linéaires, on obtient deux polynômes homogènes de degré 2 invariants par G, $g_1 = X^2+Y^2$ et $g_2 = Y(X-Y)$ qui sont linéairement indépendants sur $\mathbb{C}$. On peut montrer que tout autre polynôme homogène de degré 2 invariant par G est combinaison linéaire de g_1 et de g_2. On utilise pour cela le lemme suivant appliqué au $\mathbb{C}$-espace vectoriel F de dimension 3 engendré par X^2, XY, Y^2 (en réalisant G comme un sous-groupe de $GL(F)$).

Lemme 3. *Soient E un espace vectoriel de dimension finie sur $\mathbb{C}$ et H un sous-groupe fini de $GL(E)$. Le sous-espace vectoriel de E formé par les vecteurs invariants par H (c.-à-d. l'ensemble des $v \in E$ tels que $h(v) = v$ pour tout $h \in H$) est de dimension*

$$\frac{1}{\#H}\sum_{h\in H} \mathit{trace}(h). \tag{13}$$

Démonstration. On considère l'endomorphisme de E défini par $p = \frac{1}{\#H}\sum_{h\in H} h$. Puisque $p^2 = p$, cet endomorphisme est un projecteur dont l'image est l'ensemble des vecteurs invariants. □

On peut en fait prouver un peu plus :

Théorème 2. *L'ensemble des polynômes invariants par G est $\mathbb{C}[g_1, g_2] = \{F(g_1, g_2), F \in \mathbb{C}[U, V]\}$.*

Démonstration. Il suffit de montrer que tout polynôme homogène P invariant par G est un polynôme en g_1, g_2. On le prouve par récurrence sur le degré $2d$ de P ; le cas $d = 1$ vient d'être traité.

Si $P = a_{2d}X^{2d} + \cdots$, on peut remplacer P par $P - a_{2d}g_1^d$, qui est divisible par Y. Il reste à prouver que si Y divise P, alors $X - Y$ divise également P, ce que l'on obtient en faisant agir M_0 sur P. □

En utilisant ce résultat ainsi que (par exemple) les faits suivants :
— il n'y a qu'un seul mot de poids nul dans le code ;
— $\mathscr{S}$ a pour distance minimale 4 ;
— tous les mots du code sont de poids pair,
on peut retrouver $W_{\mathscr{S}}$ par des calculs élémentaires.

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.*

— On pourra démontrer les assertions laissées sans preuve dans le texte.
— On pourra retrouver les fonctions de poids des codes $\mathscr{C}$ et $\mathscr{S}$ par une énumération élémentaire à l'aide de l'outil informatique.
— On pourra expliquer comment déduire du polynôme des poids du code $\mathscr{C}'$ défini après l'exemple 2 en fonction du polynôme des poids du code $\mathscr{C}$.
— Lorsque l'on transmet un mot c d'un code linéaire $\mathscr{C} \subset \mathbb{F}_2^n$ sur un canal bruité, chaque coordonnée de c a une probabilité fixe $0 \leq p \leq 1$ d'être modifiée et ces évènements sont mutuellement indépendants. Si on note $c' = c + e$ le mot reçu, on ne détectera une modification que si $e \notin \mathscr{C}$. On pourra montrer que la probabilité qu'une erreur ait lieu et qu'elle ne soit pas détectée est $W_{\mathscr{C}}((1-p), p) - (1-p)^n$.
— On pourra détailler les calculs pour le code $\mathscr{S}$ dans la Section 3 avec l'aide de l'outil informatique.
— Pour un code auto-orthogonal, comme tous les mots sont de poids pair, la fonction de poids est invariante par un groupe G d'ordre 16 (on peut vérifier que c'est le groupe d'isométries planes de l'octogone régulier !) dont on pourra écrire des générateurs. On pourra alors vérifier en utilisant les techniques de la partie 3 que les polynômes homogènes de degré 2 invariants par G sont tous multiples de g_1 et que les polynômes homogènes de degré 8 invariants par G sont combinaison linéaires de g_1^4 et de $W_{\mathscr{S}}$.