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

(*Texte public*)

Résumé : On étudie la mise en place d'un système de transmission à base d'antennes multiples ; cela nous conduit à étudier des sous-groupes du groupe des matrices unitaires de dimension n.

Mots clefs : groupe unitaire, algèbre linéaire

► *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. Problèmatique

Avec le développement des transmissions sans-fil (*wifi*) se pose de façon prégnante la question d'améliorer leur qualité, et en particulier leur débit, dans un contexte où la multiplication des transmissions tend à augmenter les probabilités d'erreur.

Une idée qui s'est développée ces dernières années consiste à ne plus utiliser une antenne en émission et en réception, mais un ensemble de n antennes en émission et n' antennes en réception. Le texte étudie les questions pratiques soulevées par cette idée, et s'intéresse aux méthodes pour optimiser le débit d'une telle transmission.

2. Modélisation

Nous modélisons la transmission de la façon suivante. À chaque pas de temps $i \geqslant 0$, l'antenne émettrice numéro j émet un *signal* $\sigma_{ij} \in \mathbb{C}$. Lors du même pas de temps, chaque antenne réceptrice observe une superposition des signaux émis par les différentes antennes émettrices, auquel s'ajoute une erreur de transmission (“bruit”) liée à la présence d'autres équipements émetteurs, ou encore d'obstacles entre les antennes.

Dans ce texte, nous étudions le traitement du phénomène de bruit, et omettons donc le phénomène de superposition : nous nous plaçons dans le modèle idéal où $n' = n$, et, lors du pas de temps i, l'antenne réceptrice numéro j reçoit le signal $\sigma_{ij} + b_{ij}$, b_{ij} étant le bruit.

2.1. *Notation matricielle*

Au vu des notations ci-dessus, il semble naturel de grouper les pas de temps par paquets de n, et de représenter l'ensemble des transmissions intervenant entre les pas de temps an et $(a+1)n-1$ par la matrice $\Sigma_a = \left(\sigma_{i+an,j}\right)_{0\leqslant i,j\leqslant n-1}$. Le bruit est alors également modélisé par une suite de matrices B_a.

2.2. *Prise en compte du bruit*

Pour traiter le phénomène de bruit, une idée classique est d'imposer une *structure* au signal émis. Ici, nous fixons un ensemble *fini* de matrices $\mathscr{S} = \{M_1, \dots, M_{\operatorname{card}\mathscr{S}}\} \subset \mathscr{M}_n(\mathbb{C})$, et imposons aux matrices Σ_a émises d'être des éléments de $\mathscr{S}$. On supposera de plus les signaux normalisés, i.e. $\mathscr{S} \subset \mathbb{U}_n(\mathbb{C})$, où $\mathbb{U}_n(\mathbb{C})$ est le groupe des matrices $n \times n$ unitaires.

L'*information* transmise par l'émission de la matrice $\Sigma_a = M_k$ est alors simplement l'entier k. Si l'on considère que l'information constituée par un entier $k \in [1, \operatorname{card}\mathscr{S}]$ est mesurée par son nombre de chiffres binaires, on peut mesurer l'efficacité de la transmission de la façon suivante :

Définition 1. *Le "taux de transmission" obtenu dans ce modèle est* $\log \operatorname{card}\mathscr{S} / (n \log 2)$ *bits par pas de temps.*

À la réception d'une matrice M, on suppose que le bruit B_k est "faible", et on fait donc l'hypothèse que l'élément de $\mathscr{S}$ effectivement émis est celui qui est le plus proche de M, i.e. la matrice $M_k \in \mathscr{S}$ qui minimise $\|M - M_k\|_\infty$. Sous un modèle de bruit réaliste, une analyse probabiliste conduit alors au théorème suivant, dont la démonstration sort du cadre de cette épreuve :

Théorème 1. *Soit* ℓ, ℓ' *deux entiers de* $[1, \operatorname{card}\mathscr{S}]$. *La probabilité que* M_ℓ *ait été émis et que* $M_{\ell'}$ *soit la matrice de* $\mathscr{S}$ *la plus proche de la matrice reçue est une fonction décroissante de* $|\det(M_\ell - M_{\ell'})|^{1/n}$.

Dans la suite, nous allons chercher des ensembles $\mathscr{S} \subset \mathbb{U}_n(\mathbb{C})$ rendant la quantité

$$\zeta_{\mathscr{S}} := \min_{1\leqslant \ell < \ell' \leqslant \operatorname{card}\mathscr{S}} |\det(M_\ell - M_{\ell'})|^{1/n}$$

la plus grande possible, avec $\operatorname{card}\mathscr{S}$ le plus élevé possible pour maximiser le taux de transmission.

Nous allons nous restreindre au cas où $\mathscr{S}$ est un *sous-groupe* de $\mathbb{U}_n(\mathbb{C})$. On peut penser que cela permet d'obtenir de meilleures valeurs de $\zeta_{\mathscr{S}}$. En effet, si $\mathscr{S}$ est quelconque, $\zeta_{\mathscr{S}}$ est le minimum d'un ensemble de $\operatorname{card}\mathscr{S}(\operatorname{card}\mathscr{S}-1)/2$ valeurs ; si $\mathscr{S}$ est un groupe et I_n la matrice identité d'ordre n, on a

$$\zeta_{\mathscr{S}} = \min_{\substack{1\leqslant \ell \leqslant \operatorname{card}\mathscr{S} \\ M_\ell \neq I_n}} |\det(I_n - M_\ell)|^{1/n}$$

et $\zeta_{\mathscr{S}}$ est le minimum d'un ensemble de valeurs de plus petit cardinal ; on peut donc penser obtenir ainsi de plus grandes valeurs de $\zeta_{\mathscr{S}}$, ce que la pratique confirme.

On peut déjà faire la remarque suivante :

Lemme 1. *Pour que $\zeta_{\mathscr{S}} > 0$, il faut et il suffit que la seule matrice de $\mathscr{S}$ ayant 1 pour valeur propre soit I_n.*

3. Cas abélien

Dans cette partie, nous nous intéressons au cas où $\mathscr{S}$ est un groupe abélien ; commençons par un résultat classique :

Proposition 1. *Si $\mathscr{S} \subset \mathbb{U}_n(\mathbb{C})$ est un groupe abélien fini, il existe une matrice $P \in GL_n(\mathbb{C})$ telle que PM_iP^{-1} est diagonale pour tout $M_i \in \mathscr{S}$.*

Dans la suite, nous supposerons donc $M_\ell = \mathrm{diag}(\exp(2i\pi x_{\ell,k}/s))_{1\leqslant k\leqslant n}$, pour des entiers $x_{\ell,k}$ et s. On obtient alors une estimation directe de $\zeta_{\mathscr{S}}$ en fonction des $x_{\ell,k}$:

Théorème 2. *On a*

$$\zeta_{\mathscr{S}} = 2 \min_{\substack{1\leqslant \ell\leqslant s \\ M_\ell \neq I_n}} \left| \prod_{k=1}^{n} \sin(\pi x_{\ell,k}/s) \right|^{1/n}.$$

L'ensemble des $x_{\ell,k}$ est toutefois contraint : pour chaque k, $\{x_{\ell,k} \bmod s, 1 \leqslant \ell \leqslant s\}$ est un sous-groupe de $\mathbb{Z}/s\mathbb{Z}$. On déduit de cette remarque la proposition suivante :

Proposition 2. *Une condition nécessaire pour que $\zeta_{\mathscr{S}} \neq 0$ est que $\mathscr{S}$ soit cyclique.*

Réciproquement, la donnée de n racines primitives s-èmes de l'unité $\xi_1, \ldots, \xi_n$ fournit un sous-groupe $\mathscr{S}$ de $\mathbb{U}_n(\mathbb{C})$ isomorphe à $\mathbb{Z}/s\mathbb{Z}$, à savoir le sous-groupe engendré par la matrice $\mathrm{diag}(\xi_1, \ldots, \xi_n)$, pour lequel $\zeta_{\mathscr{S}} > 0$.

Pour s fixé, on peut alors former tous les ensembles $\mathscr{S}$ possibles en testant les $\varphi(s)^n$ générateurs possibles, et pour chacun évaluer sur ordinateur la valeur $\zeta_{\mathscr{S}}$ correspondante. On peut exploiter les symétries du problème pour restreindre (un peu) l'espace d'exploration. Pour un taux de transmission de 2 avec trois antennes (c'est-à-dire pour $n = 3$ et $s = 64$), le meilleur choix possible des ξ_i donne $\zeta_{\mathscr{S}} \approx 0.553$.

4. Étude d'un cas non abélien : le groupe $SL_2(\mathbb{Z}/5\mathbb{Z})$

Nous allons dans cette partie construire un sous-groupe de $\mathbb{U}_2(\mathbb{C})$ isomorphe au groupe $SL_2(\mathbb{Z}/5\mathbb{Z})$, de cardinal 120. Ce groupe est engendré par les deux éléments $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\tau = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, qui vérifient $\sigma^2 = \tau^3 = (\sigma\tau)^5 \neq I_2$, $\sigma^4 = I_2$.

Pour construire un sous-groupe de $\mathbb{U}_2(\mathbb{C})$ isomorphe à $SL_2(\mathbb{Z}/5\mathbb{Z})$, il nous suffit donc de construire des matrices S et T de $\mathbb{U}_2(\mathbb{C})$ vérifiant ces mêmes propriétés. Comme précédemment, on peut supposer que $ST = \mathrm{diag}(\eta_1, \eta_2)$, où η_i sont des racines 10-èmes de l'unité.

Cherchons S sous la forme $\begin{pmatrix} s_0 & s_1 \\ s_2 & s_3 \end{pmatrix}$. Le fait que $S^2 = (ST)^5$ soit diagonale implique

$$s_1(s_0 + s_3) = 0,\ s_2(s_0 + s_3) = 0.$$

Le choix $s_0 + s_3 \neq 0$ conduirait à une matrice S diagonale, qui commuterait avec ST, ce qui implique que le groupe engendré par S et T est commutatif, ce que $SL_2(\mathbb{Z}/5\mathbb{Z})$ n'est pas. On a donc $s_0 = -s_3$, et on vérifie qu'alors S^2 est une homothétie de rapport $s_0^2 + s_1 s_2$. Comme S^2 est d'ordre 2, on a $S^2 = -I_2$ et on en déduit que $s_0^2 + s_1 s_2 = -1$ et donc $\det S = 1$.

On cherche maintenant T sous la forme $\begin{pmatrix} t_0 & t_1 \\ t_2 & t_3 \end{pmatrix}$. De l'identité $T^3 = (ST)^5 = S^2$, on déduit que $\det T^3 = \det T^5 = 1$ et donc $\det T = 1$. Par suite en utilisant le fait $T^3 = (ST)^5$ est diagonale et en éliminant t_1 (puisque $\det T = 1$), on trouve

$$t_2((t_0 + t_3)^2 - 1) = 0.$$

Parmi les solutions possibles à cette équation, on choisit de prendre $t_0 + t_3 = 1$; on a alors

$$t_3^2 - t_3 + 1 = -t_1 t_2.$$

Remarquons que, comme $\det S = \det T = 1$, on a $\det ST = 1$ et donc $\eta_2 = \eta_1^{-1}$.

La contrainte sur ST implique $t_1 s_0 + t_3 s_1 = 0$. Le choix $t_1 = 0$ entraîne $s_1 = 0$ et les contraintes précédemment obtenues sur S et T conduisent à une contradiction avec le fait que η_1 est une racine 10-ème de l'unité distincte de 1. De même on peut montrer que $t_0 \neq 0$. En résumé, on a

$$S = \begin{pmatrix} s_0 & s_1 \\ s_2 & -s_0 \end{pmatrix}, \quad T = \begin{pmatrix} t_0 & t_1 \\ t_2 & 1 - t_0 \end{pmatrix}, \text{ avec } t_0 \neq 0, t_1 \neq 0, \text{ et } ST = \begin{pmatrix} \eta_1 & 0 \\ 0 & \eta_1^{-1} \end{pmatrix}$$

et le calcul des coefficients de ST permet de proche en proche de trouver le résultat suivant, où l'on a posé $\alpha = t_1(1 - \eta_1^2)$:

$$S = \frac{1}{1-\eta_1^2} \begin{pmatrix} \eta_1 & -\eta_1 \alpha \\ \frac{\eta_1^4 - \eta_1^2 + 1}{\alpha \eta_1} & -\eta_1 \end{pmatrix}, \quad T = \frac{1}{1-\eta_1^2} \begin{pmatrix} -\eta_1^2 & \alpha \\ -(\eta_1^4 - \eta_1^2 + 1)/\alpha & 1 \end{pmatrix}.$$

Le choix de $|\alpha|$ s'effectue en imposant que $S, T \in \mathbb{U}_2(\mathbb{C})$. Prenons par exemple $\alpha = \sqrt{\frac{1}{|1-\eta_1^2|^2} - 1}$.

On vérifie alors par énumération, grâce au lemme suivant, qu'on obtient bien un groupe de cardinal 120, *de facto* isomorphe à $SL_2(\mathbb{Z}/5\mathbb{Z})$.

Lemme 2. *Soit S, T deux éléments d'ordre fini d'un groupe G. On construit la suite d'ensembles $E_0 := \{e\}$, $E_{k+1} = E_k \cup \{MS, M \in E_k\} \cup \{MT, M \in E_k\}$. S'il existe k tel que $E_{k+1} = E_k$, le sous-groupe de G engendré par S et T est fini et égal à E_k. Réciproquement, si $< S, T >$ est fini, il existe k tel que $< S, T >= E_k = E_{k+1}$.*

La même énumération montre que $\zeta_{\mathscr{S}} \approx 0.618...$, pour un taux de transmission de ≈ 3.45 avec deux antennes.

5. Étude d'une famille de groupes non abéliens

Nous allons dans cette partie construire une famille de groupes non abéliens pour tenter d'améliorer les résultats de la partie précédente. Commençons par décrire le cadre abstrait dans lequel nous nous plaçons, en un sens le plus simple après les groupes abéliens : soit H

un groupe abélien engendré par un élément σ, et G un groupe contenant H comme sous-groupe distingué, tel que G/H soit cyclique.

Au vu des résultats du paragraphe 3, comme $H := <\sigma>$ est cyclique, on peut trouver pour tout k un sous-groupe de $\mathbb{U}_k(\mathbb{C})$ isomorphe au sous-groupe H ; on va s'intéresser au cas $k = 1$. Nous allons nous appuyer sur le sous-groupe de $\mathbb{U}_1(\mathbb{C})$ isomorphe à H pour construire un sous-groupe isomorphe à G :

Proposition 3. *Soit G un groupe, H un sous-groupe distingué de G, et notons $n = \operatorname{card} G/H$. D'un morphisme injectif $\phi : H \to \mathbb{U}_k(\mathbb{C})$ on peut déduire un morphisme injectif $\tilde{\phi} : G \to \mathbb{U}_{nk}(\mathbb{C})$.*

Démonstration. Notons $G/H = \{\overline{x}_1, \ldots, \overline{x}_n\}$. Pour tout $x \in G$, on définit $\tilde{\phi}(x)$ comme une matrice constituée de n^2 blocs $(\beta_{ij}(x))_{1 \leqslant i,j \leqslant n}$ de taille k, définis par

$$\beta_{ij}(x) = \begin{cases} 0 & x_i^{-1} x x_j \notin H \\ \phi(x_i^{-1} x x_j) & x_i^{-1} x x_j \in H. \end{cases}$$

Le fait que $\tilde{\phi}$ est un morphisme se prouve par multiplication par blocs, en notant qu'exactement un bloc par ligne ou par colonne est non nul. □

À titre d'exemple, considérons le cas où G/H est cyclique d'ordre n ; en d'autres termes, on cherche à construire un groupe G_{mn} contenant un sous-groupe cyclique distingué $H = <\sigma>$ d'ordre m et tel que $G/H = <\overline{\tau}>$ est cyclique d'ordre n. En particulier, par construction on doit avoir $\sigma^m = 1$, $\tau^n = \sigma^t$ pour un certain t et $\tau\sigma = \sigma^r\tau$ pour un certain r.

Proposition 4. *Nécessairement,* $\operatorname{pgcd}(r, m) = 1$, $r^n = 1 \bmod m$ *et* $\frac{m}{\operatorname{pgcd}(r-1,m)} | t$.

Démonstration. On doit avoir $\tau^n\sigma = \sigma^{r^n}\tau^n$ et $\tau\sigma^t = \sigma^{tr}\tau$. □

On peut dès lors poser $G_{mn} := \{\sigma^i\tau^j, 0 \leqslant i < m, 0 \leqslant j < n\}$; il reste à prouver que muni de la loi "définie" par les règles données plus haut, G_{mn} est bien un groupe de cardinal mn. Cela sort du cadre de ce texte. En tout état de cause, sur les exemples que nous étudions, nous construisons de fait un sous-ensemble de $\mathbb{U}_n(\mathbb{C})$ "isomorphe" à G_{mn} ; sur ce cas, on peut donc vérifier par énumération (cf. §7) sur chaque exemple que le sous-ensemble de $\mathbb{U}_n(\mathbb{C})$ obtenu est bien un groupe.

Exemples.

Premier cas. $m = 21$, $r = 4$, $n = 3$, $t = 7$. On obtient le sous-groupe de $\mathbb{U}_3(\mathbb{C})$ engendré par

$$A := \operatorname{diag}(\xi_{21}, \xi_{21}^4, \xi_{21}^{16}), B := \begin{pmatrix} 0 & 0 & \xi_{21}^t \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

où $\xi_{21} := \exp(2i\pi/21)$, qui conduit, par énumération, à $\zeta_{\mathscr{S}} \approx 0.77...$ pour un taux de transmission de $\approx 1.99....$

Second cas. $m = 57$, $r = 4$, $n = 9$, $t = 19$. On obtient un sous-groupe $\mathscr{S} \subset \mathbb{U}_9(\mathbb{C})$, avec $\zeta_{\mathscr{S}} \approx 0.73...$, pour un taux de transmission de $1.00031....$

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.*

— Comment la qualité d'un sous-groupe $\mathscr{S}$ change-t-elle par "changement de base" (ie. en remplaçant V_i par $P^{-1}V_iP$ pour tout i) ;
— Montrer que modifier α dans la dernière partie revient à un tel "changement de base" ;
— Interpréter le cas abélien en termes d'émission-réception : que se passe-t-il à chaque pas de temps ?
— Construire à l'aide d'un logiciel des ensembles de matrices unitaires "au hasard" et évaluer les $\zeta_{\mathscr{S}}$ obtenus ;
— Vérifier à l'aide d'un système de calcul formel que les ensembles $G_{21,4}$ et $G_{57,4}$ munis de la loi décrite sont bien des groupes ;
— Prouver que $SL_2(\mathbb{Z}/5\mathbb{Z})$ est bien engendré par σ et $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, ou de façon équivalente par σ et $\tau = \sigma^{-1}\gamma$;
— Vérifier les calculs de la partie 4 à l'aide d'un logiciel de calcul formel ; vérifier que le groupe $< S, T >$ obtenu a bien 120 éléments.
— Imiter la partie 4 pour le groupe $SL_2(\mathbb{Z}/3\mathbb{Z})$;
— Retrouver les différentes valeurs de $\zeta_{\mathscr{S}}$ annoncées dans le texte ;
— Retrouver des groupes que vous connaissez dans la famille G_{mn} ; le groupe $SL_2(\mathbb{Z}/5\mathbb{Z})$ est-il dans la famille G_{mn} ?
— Chercher les symétries du problème d'énumération dans le cas abélien ;
— Rechercher des solutions optimales en petite dimension dans le cas abélien ;
— Peut-on combiner $G \subset \mathbb{U}_n(\mathbb{C})$ et $H \subset \mathbb{U}_m(\mathbb{C})$? Comparer taux de transmission et valeurs de ζ.
— Comment prendre en compte l'effet de superposition dans le modèle ?