RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEURE
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ L'ARBI BEN M'HIDI OUM EL BOUAGHI
FACULTÉ DES SCIENCES EXACTES ET SCIENCE DE LA NATURE ET DE LA VIE
DÉPARTEMENT DES MATHÉMATIQUES ET INFORMATIQUE

Numéro d'ordre :

Mémoire de fin d'étude pour l'obtention du diplôme de Master

Filière : Mathématiques **Option :** Mathématiques appliquées

Thème

Les valeurs singulières de certaines matrices sur le corps $\mathbb{F}_4$

Présenté par :

BENGHALIA Safia

Soutenu le 06/07/2021, devant le jury :

Kellil Larbi	Président
Zekraoui Hanifa	Encadreur
Selatnia Mounia	Examinatrice

Session Juin 2021

Dédicaces *SAFIA*

Avec l'expression de ma reconnaissance je dédie ce travail à ceux qui quelques soient les termes embrassés, je n'arriverais jamais à leur exprimer mon amour sincère :

A l'homme, mon précieux offre du dieu, mon exemple éternel, mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, sans oublier de dire que si je devienne quelqu'une actuellement c'est grâce à tes efforts, tes conseils et ta surveillance qui m'a permis de terminer ce travail, à toi mon Cher Père :*Le Professeur Benghalia Abdelmadjid*, que Dieu te garde.

A la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur, je me rappelle vraiment de tous tes efforts avec moi dès mon jeune age, à toi ma Chère Mère :*Benghalia Malika*, que Dieu te garde.

Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite :

- A mes chers frères :*Abderaouf*, mon adorable petit frère :*Rafik*.

- A mes chéres sœurs : *Nadjet, Sarra, Amina*, et bien sur ma belle nièce *Ines*, et mes chers neveux *Mouad et Anes*, que Dieu vous protèges.

- A toutes mes amies en souvenir des plus beaux instants qu'on a passés ensemble, particulièrement *Djemel Chaima, Yasmine Harkat.*

- A toute ma famille *Benghalia.*

Remerciements

Je tiens tout d'abord à remercier Dieu le tout puissant de m'avoir donné la santé et la volonté d'entamer et de terminer ce mémoire.

Ensuite, je tiens à remercier infiniment Pr.*Zekraoui Hanifa* mon encadreur de ce mémoire pour son aide, ses conseils, sa gentillesse, et sa vaillance pour mon intégration dans le département, et surtout pour m'avoir confié ce sujet.

J'adresse mes vifs remerciements à toute l'équipe pédagogique du département des mathématiques et informatique, particulièrement mes enseignants : Dr.Oussaeif Taki Eddine et Dr.Rezzoug Imad pour leurs aide et leurs encouragements de terminer ce travail.

Un grand merci au Dr :*Akrour Youssouf*, de mon école précédente(L'école Normale Supérieure de Constantine) qui est toujours disponible pour répondre aux questions de manière très cordiale.

Je remercie sincèrement les membres de jury :
Président de jury : *Kellil Larbi.*
Examinatrice : *Selatnia Mounia.*
Monsieur et madame les jurys, vous me faites un grand honneur en acceptant de juger ce travail.

Merci mes chers parents, lesquels grâce à dieu et à eux je suis ici, et merci pour tout ce qu'ils ont fait et ce qu'ils sont entrain de faire pour moi.
Mes remerciements vont aussi à mes frères, mes sœurs, et mes collègues.

Résumé

L'objectif de ce mémoire est d'étudier les valeurs singulières sur le corps $\mathbb{F}_4$ (c'est un corps à quatre éléments et de caractéristique 2)afin d'étudier la décomposition des matrices en valeurs singulières. A travers cet étude nous passons par deux grandes théories de l'algèbre :

1)La théorie algébrique des nombres par l'introduction de quelques notions sur les corps algébriques et la théorie de Galois, en particulier les corps finis.

2)L'analyse matricielle par le théorème spectral, en particulier la décomposition en valeurs singulières, contrairement au théorème SVD sur le corps réel ou complexe qui affirme que toute matrice réelle ou complexe est décomposable en SVD, nous avons montré que les matrices ayant un ordre égal à 2^n(où 2 représente la caractéristique de corps) ne sont pas décomposables en valeurs singulières sur le groupe multiplicatif $\mathbb{F}_4^*$.

Dans notre étude nous avons utilisé les matrices circulantes et les matrices de comparaison des pairs sur le corps $\mathbb{F}_4$.

Mots clés :
Élément algébrique, corps fini, matrice, théorème spectral, décomposition en valeurs singulières.

ملخّص

الهدف من هذا العمل هو دراسة القيم المنفردة في الحقل $\mathbb{F}_4$ (و هو حقل به اربعة عناصر و ذي المميز ٢) من أجل دراسة تحليل المصفوفات الى قيم منفردة. خلال هذه الدراسة نستعمل نظريتين رئيسيتين في الجبر

١) نظرية الأعداد الجبرية عن طريق تقديم بعض المفاهيم في الحقول الجبرية و نظرية ڤلوا ، و لا سيما الحقول المتهية.

٢) تحليل المصفوفات بواسطة النظرية الطيفية، و لا سيما التحليل إلى قيم منفردة ، بخلاف نظرية التحليل الى قيم منفردة في الحقل الحقيقي أو المعقد الذي يوكد أن أي مصفوفة حقيقية أو معقدة قابلة للتحليل ، لقد بينا أن المصفوفات ذات الترتيب 2^n (حيث 2 تمثل مميز الحقل) غير قابلة للتحليل إلى قيم منفردة في الزمرة الجدائية $\mathbb{F}_4^*$.

استخدمنا في دراستنا المصفوفات الدائرية و المصفوفات المقارنة بين الأقران في الحقل $\mathbb{F}_4$.

الكلمات المفتاحية :

العنصر الجبري ، الحقل المتهي ، المصفوفات ، النظرية الطيفية ، التحليل الى قيم منفردة.

Abstract

The objective of this work is to study the singular values decomposition of a circulant matrix on the finite field $\mathbb{F}_4$ (this finite field is with four elements and characteristic 2) to study the decomposition of matrices into singular values. Through this study we go through two main theories of algebra :

1)The algebraic number theory by introducing some notions about the algebraic field and Galois theory, in particular finite fields.

2)Matrix analysis by the spectral theorem, in particular the decomposition into singular values. Contrary to the SVD theorem on the real or the complex field which asserts that any real or complex matrix is decomposable into SVD, we have shown that matrices having an order equal to 2^n(where 2 represents the characteristic of the field) are not decomposable into singular values on the multiplicative group $\mathbb{F}_4^*$.

In our study we used circulant matrices and pair way comparison matrices over the finite field $\mathbb{F}_4$.

Key words : Algebraic element, finite field, matrix, spectral theorem, singular value decomposition.

ACRONYMES ET NOTATIONS

- $\dfrac{K[x]}{(f(x))}$ le quotient de l'anneau $K[x]$ par l'idéal $(f(x))$.
- A^t : transposé d'une matrice A.
- A^* : l'adjointe d'une matrice A.
- $\mathbb{F}_4$:un corps à quatre éléments.
- $\overline{a}$: le conjugué d'un élément a dans le corps $\mathbb{F}_4$.
- σ : l'involution sur le corps $\mathbb{F}_4$.
- $\mathbb{F}_4^*$: le groupe multiplicatif de corps $\mathbb{F}_4$.
- $det(A)$: le déterminant d'une matrice A.
- $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Table des matières

Introduction Générale

Dans ce travail nous nous intéressons à l'étude des valeurs singulières sur le corps $\mathbb{F}_4$ permettant d'étudier la décomposition des matrices en valeurs singulières. L'étude s'articule autour de deux grandes théories de l'algèbre :la théorie algébrique des nombres et l'analyse matricielle par le théorème spectral.

La structure de corps finis intervient dans divers domaines des mathématiques [7], en particulier dans la théorie de Galois sur la résolution des équations algébriques où ils sont introduits pour la première fois. Pour cette raison, en hommage au mathématicien Français Evariste Galois(1811 - 1832), ces corps sont appelés les corps de Galois. Avec le développement de l'électronique, de l'informatique, de la transmission de l'information, de nouveaux champs d'application de l'algèbre ont vu le jour par exemple la théorie de codage et la cryptographie. Ces domaines font un grand usage de la structure de corps finis.

La décomposition en valeurs singulières d'une matrice A de type $m \times n$ est un sujet très fondamental et a des applications dans de nombreux domaines des mathématiques [7]. Les valeurs propres de A^*A sont des nombres réels non négatifs. Les valeurs singulières sont les racines carrées positives ou nulles des valeurs propres de A^*A (qui sont les mêmes que celles de AA^*).

Dans cette perspective l'étude qui sera menée concerne les valeurs singulières sur le corps $\mathbb{F}_4$. Le travail sera présenté dans ce manuscrit selon le plan suivant :

Introduction générale.

Chapitre 1 : Quelques préliminaires sur les corps finis.

Chapitre 2 : Quelques préliminaires sur le théorème spectral et la décomposition en valeurs singulières.

Chapitre 3 : Les valeurs singulières d'une matrice circulante et d'une matrice de comparaison des pairs sur le corps $\mathbb{F}_4$.

Enfin, l'étude menée se termine par une conclusion générale.

Chapitre 1

Quelques préliminaire sur les corps finis

Dans ce chapitre on s'intéresse à l'étude des corps finis en particulier ; la construction des corps finis, en illustrant l'étude par les tableaux de calculs et quelques exemples en terminant le chapitre par la notion d'un corps fini défini qui consiste à connaitre quelques notions algébriques.

1.1 les nombres algébriques

Définition 1.1. *Un corps* $\mathbb{K}$ *est un ensemble muni des opérations* $(+, \times)$ *telle que :* $-(\mathbb{K}, +, \times)$ *est un anneau commutatif unitaire.*
$-(\mathbb{K} \setminus 0_{\mathbb{K}}, \times)$ *est un groupe .*
On dit que le corps $\mathbb{K}$ *est fini si son cardinal est fini .*

Soit $\mathbb{K}$ un corps, $\mathbb{K}[x]$ l'anneau des polynômes et a un élément quelconque ; on dit que a est algébrique sur $\mathbb{K}$ s'il existe $f(x) \in K[x]$ tel que $f(a) = 0$

Remarque 1.1.1. Un élément qui n'est pas algébrique s'appelle transcendent

Exemple 1.1.1. $\sqrt{-2} + \sqrt{\sqrt{3}}$ est algébrique sur $\mathbb{Q}$

1.2 les extensions algébriques de degrés finis

Définition 1.2. *Soit* $\mathbb{K}$ *un corps,* $\mathbb{K}[x]$ *l'anneau des polynômes et a un élément algébrique sur* $\mathbb{K}$*. On dit que* $f(x) \in \mathbb{K}[x]$ *est le polynôme minimal de a si* $f(a) = 0$ *et* $f(x)$ *unitaire est* *irréductible sur $\mathbb{K}$. Le degré de $f(x)$ s'appelle le degré de l'élément algébrique a.*

1.2.1 Construction des corps primitifs

Lemme 1.1. *Soit $f(x)$ un polynôme irréductible sur $\mathbb{K}$,alors*

1- $((f(x))$ est un idéal maximal

2- $\frac{\mathbb{K}[x]}{(f(x))}$ est un corps noté $\mathbb{K}(a)$ est appelé extension primitive de $\mathbb{K}$ par l'élément algébrique a.

le degré du polynôme minimal de a s'appelle degré de l'extension noté :

$$[\mathbb{K}(a) : \mathbb{K}] = d = deg f(x)$$

3-le corps $\mathbb{K}(a)$ peut être vu comme espace vectoriel sur $\mathbb{K}$ de dimension d et l'ensemble $\{1, a, a^2, ..., a^{d-1}\}$ est sa base canonique.

1.3 Les corps finis

1.3.1 Construction des corps finis

Définition 1.3. *On appelle caractéristique de corps $\mathbb{K}$ le plus petit nombre premier p satisfaisant la condition : $p \times 1_{\mathbb{K}} = 0_{\mathbb{K}}$*

Soit $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ (pour q premier), ce corps est fini de cardinal q et de caractéristique q

Lemme 1.2. *1- Pour tout corps fini $\mathbb{K}$, il existe p premier tel que $\mathbb{F}_p$ s'injecte dans $\mathbb{K}$*

2- Il existe un entier positif n tel que le cardinal de $\mathbb{K}$ est égal à p^n.

On note $\mathbb{F}_q$ pour $q = p^n$ (p premier, $n \geqslant 1$).

Le groupe multiplicatif de corps $\mathbb{F}_q$ est cyclique d'ordre $(q-1)$, engendré par l'élément algébrique a.

Soit $f(x) \in \mathbb{F}_q[x]$ irréductible. D'après le lemme 1.1(2) l'extension primitive de $\mathbb{F}_q$ $\frac{\mathbb{F}_q[x]}{(f(x))}$ noté $\mathbb{F}_q(\alpha)$ où α est une racine de $f(x)$.

On peut donner les éléments de $\mathbb{F}_q(\alpha)$ comme suit :

$$\mathbb{F}_q(\alpha) = \{0, 1, \alpha, \alpha^2, ...\alpha^{q-1}\}$$

1.4 Calcul dans le corps fini

Soit $\mathbb{F}_q$ un corps de degré d et soit $f(x) \in \mathbb{F}_q(x)$ polynôme irréductible unitaire qui est défini comme suit :

$f(x) = a_0 + a_1x + ... + a_{d-1}x^{d-1} + a_dx^d = 0 \Longrightarrow x^d = -\sum_{i=0}^{i=d-1}(a_ix^i)$

On a :

$\forall m \in \mathbb{N}$, si $m < d$, d'après le lemme 1.1(3) $x^m \in \{1, x, x^2...x^{d-1}\}$

Si $m > d$, alors $\exists r, q < d$ tel que $m = qd + r$ d'où on a $x^m = (x^d)^q x^r$

où $x^d = -\sum_{i=0}^{i=d-1}(a_ix^i)$ et $x^r \in \{1, x, x^2...x^{d-1}\}$

Comme le polynôme primitif de $\mathbb{F}_4$ est donnée par $x^2 + x + 1$, alors l'élément primitif est α satisfaisant l'équation :

$1 + \alpha + \alpha^2 = 0$

Ce qui donne $\alpha^2 = -1 - \alpha = 1 + \alpha$ (car la caractéristique égale à 2)

Ainsi $(x + y)^2 = x^2 + y^2, \forall x, y \in \mathbb{F}_4$.

Exemple 1.4.1. Par l'équation $1 + \alpha + \alpha^2 = 0$, on obtient :

$$\begin{array}{cc} & \alpha^2 + \alpha^5 \\ = & \alpha^2 + (\alpha^2)^2\alpha \\ = & \alpha^2 + (\alpha + 1)^2\alpha \\ = & \alpha^2 + (\alpha^2 + 1)\alpha \\ = & \alpha^2 + \alpha^3 + \alpha \\ = & (\alpha^2 + \alpha) + \alpha^2\alpha \\ = & 1 + (1 + \alpha)\alpha \\ = & 1 + \alpha + \alpha^2 \quad = 0 \end{array}$$

Par l'utilisation de groupe cyclique : $\alpha^3 = 1$, on obtient :

$$\begin{array}{ccccc} \alpha^2 + \alpha^5 & = & \alpha^2 + \alpha^2\alpha^3 & & \\ & = & \alpha^2 + \alpha^2 & = & 0 \end{array}$$

Enfin on a les tableaux de calculs suivants :

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Remarque 1.4.1. D'après ce qui précède on a les résultats suivants :

1. Le groupe multiplicatif de corps $\mathbb{F}_4$ est cyclique d'ordre 3, on a :$\forall x \in \mathbb{F}_4^*, x^3 = 1$.
2. $\forall x \in \mathbb{F}_4, \overline{x}^2 = \overline{x^2}$.
3. $\forall x \in \mathbb{F}_4$, on a :

$$x + \overline{x} = \begin{cases} 0 & \text{Si } x \in \{0, 1\} \\ 1 & \text{Si } x \notin \{0, 1\} \end{cases}$$

1.5 Les corps finis définis

Définition 1.4. *Un corps $\mathbb{F}$ est dit défini positif si tout élément non nul de $\mathbb{F}$ admet une racine carrée non nul. L'élément nul est racine de lui-même.*

► Le corps $\mathbb{F}_4$ est fini défini car chaque élément de ce corps $\{0, 1, \alpha, \alpha^2\}$ admet une racine positive définie comme suit :

-La racine de l'élément 0 égale à 0.

-La racine de l'élément 1 égale à 1.

-La racine de l'élément α^2 égale à α ($\sqrt{\alpha^2} = \alpha$).

-Pour trouver la racine de l'élément α on pose :

$$\alpha = \beta^2 \text{ tel que } \beta \in \mathbb{F}_4$$

On examine l'existence de β.

-c'est clair que $\beta \neq 0$ et $\beta \neq 1$.

-Et $\beta \neq \alpha$ car :

si $\beta = \alpha \Longrightarrow \beta^2 = \alpha^2 \Longrightarrow \alpha = \alpha^2$ absurde.

-Pour $\beta = \alpha^2 = \alpha + 1$ on trouve :

$\beta^2 = (\alpha + 1)^2 = \alpha^2 + 1 = \alpha \Longrightarrow \alpha^2 + \alpha + 1 = 0$.

Donc $\beta = \alpha^2$.

Ainsi le corps $\mathbb{F}_4$ est fini défini.

Conclusion : Dans ce chapitre les définitions et les calculs que nous avons menés nous ont permis d'identifier le corps $\mathbb{F}_4$ qui est un corps fini défini qui sera étudié dans la suite de ce travail.

Chapitre 2

Quelques préliminaires sur le théorème spectral et la décomposition en valeurs singulières

Dans ce chapitre on introduit quelques préliminaires sur les outils de théorème spectral afin d'étudier la décomposition en valeurs singulières, donc on a besoin de connaitre les valeurs singulières d'une matrice qui sont les racines carrées des valeurs propres et les méthodes de décomposition en valeurs singulières(SVD).

2.1 Les valeurs propres et les vecteurs propres d'une matrice carrée

Définition 2.1. *Soit $A \in M_n(\mathbb{R})$ (ou $M_n(\mathbb{C})$). A représente une application linéaire de $\mathbb{R}^n$ dans $\mathbb{R}^n$ tel que $\mathbb{R}^n$ est muni de sa base canonique qui est définie comme suit : $\{\overrightarrow{e_1}, \overrightarrow{e_2}, \ldots\ldots, \overrightarrow{e_n}\}$ où $\overrightarrow{e_i} = (0, 0, 0, \ldots, 1, 0, 0, \ldots, 0)$, 1 est la i-ème composante.*

Si $\overrightarrow{v} \in \mathbb{R}^n$, $A\overrightarrow{v}$ désigne l'image de $\overrightarrow{v}$ par A. Comme $\overrightarrow{v}$ est de composantes $(x_1, x_2, .., x_n)$ dans la base canonique de $\mathbb{R}^n$, on écrit :

$$\mathbf{A}\overrightarrow{v} = \begin{pmatrix} a_{ij} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Définition 2.2. *Soit u une application linéaire d'un espace E de dimension n dans lui même, de matrice A dans une base donnée.*

Lemme 2.1. *Le polynôme $p(\lambda) = det(A - \lambda I)$ est un polynôme de degré n qui ne dépend que de l'application u. On l'appel polynôme caractéristique de la matrice A et par extension polynôme caractéristique de l'application linéaire u de la matrice A.*

Le nombre λ est valeur propre de la matrice A si et seulement si λ annule le polynôme caractéristique : $det(A - \lambda I) = 0$

Exemple 2.1.1. Soit la matrice A :

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$det(A - \lambda I) = \lambda^2 - 1$ les deux valeurs propres sont bien $+1$ et -1 .

Définition 2.3. *Soit u une application linéaire d'un espace E de dimension n dans lui même, on dit que le vecteur non nul x de l'espace E est un vecteur propre de u associé à la valeur propre λ si et seulement si $u(x) = \lambda x$.*

Par extension, on dit que le vecteur colonne X non nul de $\mathbb{R}^n$ est vecteur propre pour la matrice A avec la valeur propre λ si on a : $AX = \lambda X$

• *un vecteur propre associé à une valeur propre donnée n'est pas unique c'est à dire si X est un vecteur propre et β un réel non nul alors :*

$\beta AX = \beta\lambda X$

$A(\beta X) = \lambda(\beta X)$

$AY = \lambda Y$ *avec* $Y = \beta X$

βX *est aussi un vecteur propre de A associé à λ.*

Remarque 2.1.1. Une équation polynômiale de degré n a généralement n solutions mais elles ne sont pas forcément toutes distinctes.

Lorsque une même solution X apparait k fois, on dit k est l'ordre de la multiplicité de la valeur propre.

Exemple 2.1.2. Soit la matrice A :

$$\mathbf{A} = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{pmatrix}$$

$$\mathbf{P_A}(\lambda) = \mathbf{det}(\mathbf{A} - \lambda\mathbf{I}) = \begin{vmatrix} 2-\lambda & 2 & 1 \\ 1 & 3-\lambda & 1 \\ 1 & 2 & 2-\lambda \end{vmatrix}$$

Par la méthode de Gauss :

$L_3 \to L_3 - L_2$

$$\begin{vmatrix} 2-\lambda & 2 & 1 \\ 1 & 3-\lambda & 1 \\ 0 & \lambda-1 & 1-\lambda \end{vmatrix}$$

$$\begin{aligned} &= (1-\lambda)((3-\lambda)(2-\lambda) - 2 + (2-\lambda+1)) \\ &= (1-\lambda)(6 - 2\lambda - 3\lambda + \lambda^2 - 2 + 1 - \lambda) \\ &= (1-\lambda)(\lambda^2 - 6\lambda + 5) \end{aligned}$$

1 est une valeur propre d'ordre de multiplicité 2

2.1.1 Exemple de calcul de valeurs propres :

Déterminons les valeurs propres de la matrice A telle que :

$$\mathbf{A} = \begin{pmatrix} 5 & -3 \\ 6 & -4 \end{pmatrix}$$

Les valeurs propres de la matrice A sont les scalaires λ vérifiant :

$$\mathbf{det}(\mathbf{A} - \lambda\mathbf{I}) = \mathbf{0} \Leftrightarrow \begin{vmatrix} 5-\lambda & -3 \\ 6 & -4-\lambda \end{vmatrix}$$

$$= -(5-\lambda)(4+\lambda) + 18$$

$$= \lambda^2 - \lambda - 2$$

$$= (\lambda+1)(\lambda-2) = 0$$

D'où les valeurs propres sont :

$\lambda_1 = -1$ et $\lambda_2 = +2$

2.1.2 Exemple de calcul de vecteurs propres :

Cherchons les vecteurs propres de la matrice A :

$$\mathbf{A} = \begin{pmatrix} 5 & -3 \\ 6 & -4 \end{pmatrix}$$

Et est ce que ces vecteurs propres forment une base de $\mathbb{R}^2$?.

En posons X_1 et X_2 les deux vecteurs propres associés respectivement à λ_1 et λ_2 nous avons :

Pour $\lambda_1 = -1$

$$(\mathbf{A} + \mathbf{I_2})\mathbf{X_1} = \mathbf{0} \Leftrightarrow \begin{pmatrix} 6 & -3 \\ 6 & -3 \end{pmatrix} \begin{pmatrix} x_1' \\ x_1'' \end{pmatrix}$$

le système est équivalent à :

$$6x_1' - 3x_1'' = 0$$

Choix d'un vecteur propre :

$$\mathbf{X_1} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

Pour $\lambda_2 = +2$:

$$(\mathbf{A} - \mathbf{2I_2})\mathbf{X_2} = \mathbf{0} \Leftrightarrow \begin{pmatrix} 3 & -3 \\ 6 & -6 \end{pmatrix} \begin{pmatrix} x_2' \\ x_2'' \end{pmatrix} = 0$$

Le système est équivalent à :

$$3x_2' - 3x_2'' = 0$$

Choix d'un vecteur propre :

$$\mathbf{X_2} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Comme le déterminant : $\begin{vmatrix} 1 & 1 \\ 2 & 1 \end{vmatrix} \neq 0$ La famille (X_1, X_2) est une base de $\mathbb{R}^2$.

2.2 Diagonalisation d'une matrice carrée :

Définition 2.4. *On dit qu'une matrice carrée* A *est diagonalisable s'il existe une matrice diagonale* D *et une matrice inversible* P *telle que* $A = PDP^{-1}$

2.2.1 Sous espace propre :

Définition 2.5. *Soit* A *une matrice carrée d'ordre* n*,* λ *est une valeur propre de* A*.*

$E(\lambda) = \{X \in \mathbb{R}^n$ *tel que* $AX = \lambda X\}$ *est appelé sous espace propre de* A *associé à* λ*.*

$E(\lambda)$ *est un sous espace vectoriel. Pour trouver* $E(\lambda)$ *on doit résoudre le système linéaire homogène* $(A - \lambda I)X = 0$*.*

Théorème 2.2. *Une matrice carrée* A *est diagonalisable si l'une des conditions suivantes est vérifiée :*

- $P_A(\lambda)$ *admet des racines distinctes.*
- $P_A(X)$ *admet* n *racines dont quel qu'une sont confondues et l'ordre de multiplicité de chacune de ces racines est égal à la dimension de sous espace propre associé.*

2.2.2 Puissance nième d'une matrice diagonalisable :

Soit D une matrice diagonale d'ordre n telle que $A = PDP^{-1}$, alors pour tout entier k, on a :

$$A^k = PD^kP^{-1}$$

2.2.3 Le théorème spectral :

En mathématiques, et plus particulièrement en algèbre linéaire et en analyse fonctionnelle, on désigne par théorème spectral ; le cas le plus élémentaire concerne les matrices symétriques représentant les formes quadratiques en dimension finie (classification des formes quadratiques) ; le théorème spectral correspondant, démontré par Karl Weierstrass en 1858, affirme que ces matrices sont toutes diagonalisables dans les réels, par l'intermédiaire d'un changement de base orthonormée.

Théorème 2.3. *Toute matrice réelle ou complexe, auto-adjointe est diagonalisable [8].*

2.2.4 Cas des valeurs propres distinctes :

Les vecteurs propres $x_1, x_2, ..., x_n$ associés aux valeurs propres $\lambda_1, \lambda_2, .., \lambda_n$ forment une base $B_x = (x_1, x_2, ..., x_n)$. Dans cette base B_x, la matrice A' est diagonale et souvent notée par :

$$\mathbf{D} = \begin{pmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n \end{pmatrix}$$

avec $D = P^{-1}AP$.

2.2.5 Exemple de diagonalisation d'une matrice carrée d'ordre 2 :

Vérifier, à partir des résultats des deux exemples précédents que :

$D = P^{-1}AP$ avec :

$$\mathbf{A} = \begin{pmatrix} 5 & -3 \\ 6 & -4 \end{pmatrix}$$

La connaissance des valeurs propres $\lambda_1 = -1$,$\lambda_2 = 2$ et des vecteurs propres associés $X_1 = (1, 2)$ et $X_2 = (1, 1)$ conduisent à la matrice de passage P.

$$\mathbf{P} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$\mathbf{P^{-1}} = -\begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$$

avec $detP = -1$.

Et :

$$\mathbf{D} = \mathbf{P^{-1}AP} = \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 5 & -3 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 \\ 4 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}$$

La matrice diagonale est donc formée des valeurs propres.

2.3 Les valeurs singulières :

Soit $A \in \mathbb{R}^{m\times n}$ de rang r. La matrice $A^tA \in \mathbb{R}^{n\times n}$ est symétrique et semi définie positive. Soient :

► $\sigma_1^2, \sigma_2^2, ...,\sigma_n^2$ les valeurs propres de A^tA. Les r premières sont strictement positives. Les $n-r$ suivantes sont nulles.

► Les r non nulles correspondent aussi aux r valeurs propres non nulles de $AA^t \in \mathbb{R}^{m\times m}$.

► Les σ_i sont appelées les valeurs singulières de A.

► $\sigma_i = \sqrt{\sigma_i^2} \geqslant 0$. Les valeurs singulières sont toujours positives ou nulles.

2.4 Les vecteurs singuliers :

Un réel positif σ est appelé valeur singulier de M si et seulement s'il existe un vecteur unitaire u dans $\mathbb{K}^m$ et un vecteur unitaire v dans K^n tel que :

$Mv = \sigma u$ et $M^*u = \sigma v$.

Les vecteurs u et v sont appelés vecteur singulier à gauche et vecteur singulier à droite pour σ, respectivement.

2.5 L'adjointe d'une matrice :

Soit $A = (a_{ij})_{m\times n}$, alors on définit l'adjointe A^* par :

$$A^* = \overline{A}^t = \overline{(a_{ji})}_{n\times m}$$

2.6 Décomposition en valeurs singulières (SVD) :

En mathématique le procédé d'algèbre linéaire de décomposition en valeurs singulières (ou SVD de l'anglais Singular Value Decomposition)d'une matrice est un outil important de factorisation des matrices rectangulaires réelles ou complexes. Ses applications s'étendent du traitement du signal aux statistiques, en passant par la météorologie.

Théorème 2.4. *Soit M une matrice $m \times n$ dont les coefficients appartiennent au corps $\mathbb{K}$. Alors il existe une factorisation de la forme :*

$$M = U\Sigma V^*$$

Avec U une matrice unitaire $m \times m$ sur $\mathbb{K}$, Σ une matrice $m \times n$ dont les coefficients diagonaux sont des réels positifs ou nuls et tous les autres sont nuls (c'est donc une matrice diagonale dont on impose que les coefficients soient positifs ou nuls), et V^* est la matrice adjointe à V, matrice unitaire $n \times n$ sur $\mathbb{K}$. On appelle cette factorisation la décomposition en valeurs singulières de M.

· La matrice V contient un ensemble de vecteurs de base orthonormés pour M, dits «d'entrés » ou «d'analyse».

· La matrice U contient un ensemble de vecteurs de base pour M dits « de sortie».

(Les colonnes de U et de V sont respectivement vecteur singulier à gauche et à droite pour les valeurs singulières correspondantes).

· La matrice Σ contient les valeurs singulières de la matrice M

Conclusion : Dans ce chapitre on s'est familiarisé avec : les valeurs propres et les vecteur propres, la diagonalisation d'une matrice, les valeurs singulière et les vecteurs singulières ; dans le but de décomposer une matrice.

Chapitre 3

Les valeurs singulières d'une matrice circulante et d'une matrice de comparaison des pairs sur un corps a quatre éléments

Dans ce chapitre, tenant compte des théorèmes précédents, nous étudions Les valeurs singulières des matrices circulantes et des matrices de comparaison des pairs sur le corps fini $\mathbb{F}_4$, (les matrices choisies seules celles ayant un ordre égal à 2^n(où 2 représente la caractéristique de corps)) ; pour étudier la décomposition en valeurs singulières de ces matrices. Cette étude a pour objectif la comparaison des résultats qui sont obtenus avec ceux des matrices réelles ou complexes et aux matrices définis sur le même corps ($\mathbb{F}_4$) qui ont un ordre premier avec la caractéristique de corps $\mathbb{F}_4$ (par exemple les matrices circulantes d'ordre 3).

Définition 3.1. *On appelle involution sur un corps* $\mathbb{k}$ *tout automorphisme* σ *qui satisfait* $\sigma^2 = I$

- Involution sur le corps $\mathbb{F}_4$:

Soit σ le $\mathbb{F}_2$ -automorphisme du corps $\mathbb{F}_4$. Alors σ est aussi une application linéaire.
Si $\sigma \neq I$,alors :

$$\sigma(\alpha) = \alpha^2$$

$$\sigma(\alpha^2) = \alpha$$

$$\sigma(0) = 0$$

$$\sigma(1) = 1$$

On note $\overline{\alpha} = \alpha^2$, ainsi $\overline{\alpha^2} = \alpha$.

3.1 Les matrices circulantes :

Définition 3.2. *Une matrice circulante est une matrice carrée dans laquelle on passe d'une ligne à la suivante par permutation circulaire (décalage vers la droite) des coefficients.*

Une matrice circulante d'ordre n est donc de la forme :

$$\mathbf{C} = \begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \dots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \dots & c_{n-3} \\ \vdots & & & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{pmatrix}$$

3.1.1 Quelques propriétés des matrices circulantes :

- La somme de deux matrices circulantes est une matrice circulante.
- Le produit de deux matrices circulantes est une matrice circulante.
- Le produit d'une matrice circulante par un scalaire est une matrice circulante.

Exemple 3.1.1. La matrice suivante est une matrice circulante d'ordre 4 sur le corps $\mathbb{F}_4$:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & \alpha & \alpha^2 \\ \alpha^2 & 0 & 1 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ 1 & \alpha & \alpha^2 & 0 \end{pmatrix}$$

3.1.2 La décomposition en valeurs singulières de la matrice circulante :

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & \alpha & \alpha^2 \\ \alpha^2 & 0 & 1 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ 1 & \alpha & \alpha^2 & 0 \end{pmatrix}$$

Ainsi la matrice adjointe A^* de A est définie comme suit
$A^* = \overline{A}^t$ tel que :

$$\overline{\mathbf{A}} = \begin{pmatrix} 0 & 1 & \alpha^2 & \alpha \\ \alpha & 0 & 1 & \alpha^2 \\ \alpha^2 & \alpha & 0 & 1 \\ 1 & \alpha^2 & \alpha & 0 \end{pmatrix}$$

Alors :

$$\mathbf{A}^* = \begin{pmatrix} 0 & \alpha & \alpha^2 & 1 \\ 1 & 0 & \alpha & \alpha^2 \\ \alpha^2 & 1 & 0 & \alpha \\ \alpha & \alpha^2 & 1 & 0 \end{pmatrix}$$

Calculons le produit AA^* :

$$\mathbf{AA}^* = \begin{pmatrix} 0 & 1 & \alpha & \alpha^2 \\ \alpha^2 & 0 & 1 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ 1 & \alpha & \alpha^2 & 0 \end{pmatrix} \begin{pmatrix} 0 & \alpha & \alpha^2 & 1 \\ 1 & 0 & \alpha & \alpha^2 \\ \alpha^2 & 1 & 0 & \alpha \\ \alpha & \alpha^2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2\alpha^3+1 & \alpha^4+\alpha & \alpha^2+\alpha & 2\alpha^2 \\ 2\alpha^2 & 2\alpha^3+1 & \alpha^4+\alpha & \alpha^2+\alpha \\ \alpha^2+\alpha & 2\alpha^2 & 2\alpha^3+1 & \alpha^4+\alpha \\ \alpha^4+\alpha & \alpha^2+\alpha & 2\alpha^2 & 2\alpha^3+1 \end{pmatrix}$$

Comme le calcul se fait dans $\mathbb{F}_4$ alors, le caractéristique du corps et l'équation :

$$\alpha^2 + \alpha + 1 = 0$$

donnent :

$2\alpha^3 + 1 = 1$

$\alpha^2 + \alpha = 1$

$2\alpha^2 = 0$

$\alpha^4 + \alpha = \alpha\alpha^3 + \alpha = \alpha + \alpha = 0$

Ainsi,

$$\mathbf{AA}^* = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Le produit A^*A donne :

$$\mathbf{A}^*\mathbf{A} = \begin{pmatrix} 0 & \alpha & \alpha^2 & 1 \\ 1 & 0 & \alpha & \alpha^2 \\ \alpha^2 & 1 & 0 & \alpha \\ \alpha & \alpha^2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & \alpha & \alpha^2 \\ \alpha^2 & 0 & 1 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ 1 & \alpha & \alpha^2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = AA^*$$

Alors, A est normale (une matrice qui commute avec son adjointe s'appelle matrice normale).

Donc les vecteurs singulières à gauche et à droite de A sont les mêmes.

On calcule le polynôme caractéristique de AA^* :

$$\mathbf{det}(\lambda\mathbf{I} - \mathbf{AA}^*) = \mathbf{det}(\lambda\mathbf{I} + \mathbf{AA}^*) = \begin{pmatrix} \lambda+1 & 0 & 1 & 0 \\ 0 & \lambda+1 & 0 & 1 \\ 1 & 0 & \lambda+1 & 0 \\ 0 & 1 & 0 & \lambda+1 \end{pmatrix} = \lambda^4 + 4\lambda^3 + 4\lambda^2 = \lambda^4$$

Ce qui implique qu'on a une seule valeur propre $\lambda = 0$ de AA^*.

Les vecteurs propres de AA^* :

$$AA^*v = \lambda v = 0 \Longrightarrow v \in kerAA^*$$

.

Ainsi on calcule $kerAA^*$, on trouve :

$$kerAA^* = vect\{(1,0,1,0),(0,1,0,1)\}$$

Ce qui fait on a seulement deux vecteurs singulières $\{(1,0,1,0),(0,1,0,1)\}$ qui ne permettent pas à décomposer la matrice A en valeurs singulières.

Corollaire 3.1. *Contrairement aux matrices circulantes réelles, la matrice circulante définie par le vecteur* $(0, 1, \alpha, \alpha^2)$ *sur le corps* $\mathbb{F}_4$ *n'est pas décomposable en valeurs singulière.*

3.1.3 La décomposition d'une matrice circulante de vecteur général sur un corps à 4 éléments :

Dans ce cas on doit étudier la décomposition d'une matrice circulante de vecteur général sur le corps $\mathbb{F}_4$:

• le cas de 2 éléments :

$$\mathbf{C} = \begin{pmatrix} a_0 & a_1 \\ a_1 & a_0 \end{pmatrix}$$

et :

$$\mathbf{C}^* = \begin{pmatrix} \overline{a_0} & \overline{a_1} \\ \overline{a_1} & \overline{a_0} \end{pmatrix}$$

$$\mathbf{CC}^* = \begin{pmatrix} a_0 & a_1 \\ a_1 & a_0 \end{pmatrix} \begin{pmatrix} \overline{a_0} & \overline{a_1} \\ \overline{a_1} & \overline{a_0} \end{pmatrix} = \begin{pmatrix} M_0 & b_1 \\ b_1 & M_0 \end{pmatrix}$$

tel que :

$$\begin{aligned} M_0 &= a_0\overline{a_0} + a_1\overline{a_1} \\ b_1 &= a_0\overline{a_1} + a_1\overline{a_0} \end{aligned}$$

Calculons le $det(\lambda I + CC^*)$:

$$\mathbf{det}(\lambda\mathbf{I} + \mathbf{CC}^*) = \begin{pmatrix} M_0 + \lambda & b_1 \\ b_1 & M_0 + \lambda \end{pmatrix}$$

On note :

$b_0 = M_0 + \lambda$

On obtient :

$$\mathbf{det}(\lambda\mathbf{I} + \mathbf{CC}^*) = \begin{vmatrix} b_0 & b_1 \\ b_1 & b_0 \end{vmatrix} = b_0^2 + b_1^2 = 0$$

Alors : $b_0^2 + b_1^2 = (b_0 + b_1)^2 = 0 \Rightarrow b_0 + b_1 = 0 \Rightarrow b_0 = b_1$

Ce qui fait :

$a_0\overline{a_0} + a_1\overline{a_1} + \lambda = a_0\overline{a_1} + a_1\overline{a_0}$

Ainsi on a :

$\lambda = a_0\overline{a_0} + a_1\overline{a_1} + a_0\overline{a_1} + a_1\overline{a_0}$

$\lambda = (a_0 + a_1)(\overline{a_0 + a_1})$

On remarque que pour tout $x \in \mathbb{F}_4$, on a les résultats suivants :

$*$ pour $x = 0$, on a :

$$x\overline{x} = 0$$

$*$ pour $x \neq 0$, on a :

$$x\overline{x} = 1$$

Par conséquent dans tous les cas on a :

$\lambda = 1$ ou $\lambda = 0$

• Pour $\lambda = 0$

On a les résultats suivants :

$M_0 = 0$, et $b_0 = 0$.

Et comme $b_1 = b_0 = 0$.

Alors la matrice $CC^* = 0$, ce cas est inacceptable car il nous ramène à $C = 0$, or C est non nulle.

• Pour $\lambda = 1$ on a les résultats suivants :

$M_0 = 0$ ou $M_0 = 1$.

► Si $\lambda = 1$ et $M_0 = 0$:

Calculons les vecteurs propres(en sachant que les vecteurs propres sont non nuls) :

Soit $v = (x_1, x_2)$ un vecteur propre de CC^* :

$$\begin{pmatrix} 0 & b_1 \\ b_1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} b_1x_2 = x_1 ...(1) \\ b_1x_1 = x_2 ...(2) \end{cases}$$

On remplace l'équation (1) dans (2), on trouve :

$(b_1^2 + 1)x_2 = 0$

Dans ce cas $x_2 \neq 0$ car si $x_2 = 0$ on a $x_1 = 0$, or $(x_1, x_2) \neq 0$

Donc $b_1^2 + 1 = 0 \Rightarrow b_1 = 1$ ainsi $x_1 =, x_2$

Alors on a un seul vecteur propre $v = (1, 1)$ pour la valeur propre $\lambda = 1$; par conséquent la matrice CC^* n'est pas diagonalisable, d'où la matrice C n'est pas décomposable en valeurs singulières.

► Si $\lambda = 1$ et $M_0 = 1$:

$$\begin{pmatrix} 1 & b_1 \\ b_1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} x_1 + b_1 x_2 = x_1 ...(1) \\ b_1 x_1 + x_2 = x_2 ...(2) \end{cases}$$

D'après la formule (1)on a :

$b_1 x_2 = 0 \Rightarrow b_1 = 0$ (car si $x_2 = 0$ on a $x_1 = 0$, or $(x_1, x_2) \neq 0$) donc $\exists x_2 \in \mathbb{F}_4$.

D'après la formule (2)on a :

l'existence de $x_1 \in \mathbb{F}_4$.

Ce qui fait il existe deux vecteurs propres $v_1 = (1, 0)$ et $v_2 = (0, 1)$.

Donc la matrice C est décomposable en valeurs singulières dans le cas où $\lambda = 1$ et $M_0 = 1$.

c'est à dire dans le cas où l'un des coefficients égal à 0. Ainsi on a le théorème suivant :

Théorème 3.2. *Toute matrice circulante d'ordre* 2 *sur le groupe multiplicatif* $\mathbb{F}_4^*$ *n'est pas décomposable en valeurs singulières.*

On remarque, malgré $\lambda = 0$ est une racine du polynôme caractéristique de la matrice CC^*, mais elle n'est pas une valeur propre car elle ramène à $C = 0$. Ainsi on a le corollaire suivant :

Corollaire 3.3. *Contrairement au cas réel ou complexe ; les valeurs propres d'une matrice carrée sur un corps fini sont parmi les racines de son polynôme caractéristique. Mais pas nécessairement toutes les racines sont des valeurs propres.*

◄ le cas de 3 éléments :

Soit la matrice B :

$$\mathbf{B} = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_2 & a_0 & a_1 \\ a_1 & a_2 & a_0 \end{pmatrix}$$

et :

$$\mathbf{B}^* = \begin{pmatrix} \overline{a_0} & \overline{a_2} & \overline{a_1} \\ \overline{a_1} & \overline{a_0} & \overline{a_2} \\ \overline{a_2} & \overline{a_1} & \overline{a_0} \end{pmatrix}$$

$$\mathbf{BB}^* = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_2 & a_0 & a_1 \\ a_1 & a_2 & a_0 \end{pmatrix} \begin{pmatrix} \overline{a_0} & \overline{a_2} & \overline{a_1} \\ \overline{a_1} & \overline{a_0} & \overline{a_2} \\ \overline{a_2} & \overline{a_1} & \overline{a_0} \end{pmatrix} = \begin{pmatrix} M_0 & b_1 & b_2 \\ b_2 & M_0 & b_1 \\ b_1 & b_2 & M_0 \end{pmatrix}$$

tel que :

$$\begin{aligned} M_0 &= a_0\overline{a_0} + a_1\overline{a_1} + a_2\overline{a_2} \\ b_1 &= a_0\overline{a_2} + a_1\overline{a_0} + a_2\overline{a_1} \\ b_2 &= a_0\overline{a_1} + a_1\overline{a_2} + a_2\overline{a_0} \end{aligned}$$

Calculons le $det(\lambda I + BB^*)$:

$$\mathbf{det}(\lambda\mathbf{I} + \mathbf{BB}^*) = \begin{pmatrix} M_0 + \lambda & b_1 & b_2 \\ b_2 & M_0 + \lambda & b_1 \\ b_1 & b_2 & M_0 + \lambda \end{pmatrix}$$

On note :

$b_0 = M_0 + \lambda$

On obtient :

$$\mathbf{det}(\lambda\mathbf{I} + \mathbf{BB}^*) = \begin{vmatrix} b_0 & b_1 & b_2 \\ b_2 & b_0 & b_1 \\ b_1 & b_2 & b_0 \end{vmatrix} = b_0^3 + b_1^3 + b_2^3 + b_1 b_0 b_2 = 0$$

► Pour $a_i\overline{a_i} = 0$ et $a_j\overline{a_j} = 1$ et $a_k\overline{a_k} = 1 \forall j \neq i \neq k$.

On a $M_0 = 0$.

Donc, sans restreindre la généralité, on peut supposer que $a_0\overline{a_0} = 0$ cela nous donne les valeurs suivantes :

$$a_0 = 0, b_1 = a_2\overline{a_1}, b_2 = a_1\overline{a_2} = \overline{b_1}, b_0 = \lambda. \tag{3.1}$$

$det(\lambda I + BB^*) = b_0^3 + b_1^3 + b_2^3 + b_1 b_0 b_2 = 0$

D'après 3.1.3, on a :

$det(\lambda I + BB^*) = \lambda^3 + b_1^3 + \overline{b_1}^3 + \lambda b_1\overline{b_1} = 0$

Comme $\forall x \in \mathbb{F}_4$, et $x \neq 0$, on a $x\overline{x} = 1$ et $b_1\overline{b_1} = 1$ et $b_1^3 + \overline{b_1^3} = 0$ (D'après 1.4).

Alors :

$$det(\lambda I + BB^*) = \lambda^3 + \lambda = 0 \Rightarrow \lambda = 0 \text{ ou } \lambda = 1$$

• Calculons les vecteurs propres pour $\lambda = 1$

$BB^*v = \lambda v = v$

$$\begin{pmatrix} 0 & b_1 & \overline{b_1} \\ \overline{b_1} & 0 & b_1 \\ b_1 & \overline{b_1} & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Donc :

$$\Leftrightarrow \begin{cases} b_1x_2 + \overline{b_1}x_3 & = x_1 ...(1) \\ \overline{b_1}x_1 + b_1x_3 & = x_2 ...(2) \\ b_1x_1 + \overline{b_1}x_2 & = x_3 ...(3) \end{cases}$$

On remplace la formule(1) dans (2) on obtient :

$\overline{b_1}b_1x_2 + \overline{b_1}^2x_3 + x_2 + b_1x_3 = 0 \Leftrightarrow (\overline{b_1}^2 + b_1)x_3 = 0$

Comme $\overline{b_1}^2 + b_1 = 0$, alors $\exists x_3 \in \mathbb{F}_4$.

On remplace la formule(1) dans (3) on obtient :

$b_1^2x_2 + b_1\overline{b_1}x_3 + \overline{b_1}x_2 + x_3 = 0 \Leftrightarrow (b_1^2 + \overline{b_1})x_2 = 0 \Rightarrow \exists x_2 \in \mathbb{F}_4$.

Donc on a $V = (b_1x_2 + \overline{b_1}x_3, x_2, x_3) = x_2(b_1, 1, 0) + x_3(\overline{b_1}, 0, 1)$.

Ainsi il existe deux vecteurs propres $v_1 = (b_1, 1, 0)$ et $v_2 = (\overline{b_1}, 0, 1)$ pour la valeur propre $\lambda = 1$.

• Calculons les vecteurs propres pour $\lambda = 0$

$BB^*v = \lambda v = 0$

$$\begin{pmatrix} 0 & b_1 & \overline{b_1} \\ \overline{b_1} & 0 & b_1 \\ b_1 & \overline{b_1} & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} b_1x_2 + \overline{b_1}x_3 & = 0 ...(1) \\ \overline{b_1}x_1 + b_1x_3 & = 0 ...(2) \\ b_1x_1 + \overline{b_1}x_2 & = 0 ...(3) \end{cases}$$

On multiplie la formule (1) par b_1 on trouve :

$b_1^2x_2 + x_3 = 0 \Rightarrow x_3 = b_1^2x_2$.

On multiplie la formule (2) par b_1 on trouve :

$x_1 + b_1^4x_2 = 0 \to x_1 = b_1^4x_2 = b_1x_2$ (car $b_1^3 = 1$.

On multiplie la formule (3) par $\overline{b_1}$ on trouve :

$x_1 + \overline{b_1}^2x_2 = 0 \to x_1 = \overline{b_1}^2x_2$.

Donc, pour $\lambda = 0$, on a :

$x_3 = b_1^2x_2$ et $x_1 = b_1x_2 = \overline{b_1}^2x_2$.

Donc on a $V = (b_1x_2, x_2, b_1^2x_2$.

Ainsi on a le vecteur propre $(b_1, 1, b_1^2)$ pour la valeur propre $\lambda = 0$.

Donc la matrice BB^* est diagonalisable ; comme $BB^* = B^*B$ alors les vecteurs singulières à gauches et à droite pour la matrice B sont les mêmes. Par conséquent la matrice B est décomposable en valeurs singulières.

▶ Pour $a_i\overline{a_i} = 1$ et $a_j\overline{a_j} = 0$ et $a_k\overline{a_k} = 0$, $k \neq i \neq j$.

On a $M_0 = 1$, ainsi on a les valeurs suivantes :

$$b_0 = 1 + \lambda, b_1 = 0, b_2 = 0$$

.

Donc :

$det(\lambda I + BB^*) = b_0^3 + b_1^3 + b_2^3 + b_0b_1b_2 = (1 + \lambda)^3 = 0$

c'est à dire :

$1 + \lambda = 0 \Rightarrow \lambda = 1$.

Donc on a une seule valeur propre $\lambda = 1$.

• On calcule les vecteurs propres :

$$\Big(I + BB^*\Big)\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

On a

$$(\mathbf{I} + \mathbf{BB}^*) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Ce qui implique que tous les vecteurs $V = (x_1, x_2, x_3)$ sont des vecteurs propres, en particulier : $(1,0,0), (0,1,0), (0,0,1)$.

Donc la matrice BB^* est diagonalisable ; comme $BB^* = B^*B$ alors les vecteurs singulières à gauches et à droite pour la matrice B sont les mêmes. Par conséquent la matrice B est décomposable en valeurs singulières.

► Pour tous les $a_i\overline{a_i} = 1$.

On a les valeurs suivantes :

$a_i \neq 0, \forall i \in \{0,1,2\}, M_0 = 1, b_0 = 1+\lambda, b_2 = \overline{b_1}$.

Ainsi : $det(\lambda I + BB^*) = (1+\lambda)^3 + b_1^3 + \overline{b_1}^3 + (1+\lambda) = 0$

Comme l'ordre de groupe cyclique est 3 donc on a le résultat suivant :

$b_1^3 + \overline{b_1}^3 = 0.$

Alors :

$det(\lambda I + BB^*) = (1+\lambda)((1+\lambda)^2 + 1) = (1+\lambda)\lambda^2 = 0$

D'où : $\lambda = 0$ ou $\lambda = 1$.

Calculons les vecteurs propres de BB^* pour $\lambda = 0$:

$BB^*v = \lambda v = 0$

$$\begin{pmatrix} 1 & b_1 & \overline{b_1} \\ \overline{b_1} & 1 & b_1 \\ b_1 & \overline{b_1} & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} x_1 + b_1x_2 + \overline{b_1}x_3 & = 0...(1) \\ \overline{b_1}x_1 + x_2 + b_1x_3 & = 0...(2) \\ b_1x_1 + \overline{b_1}x_2 + x_3 & = 0...(3) \end{cases}$$

de (1) on a :

$x_1 = b_1x_2 + \overline{b_1}x_3$

On remplace x_1 dans la formule (2) :

$x_2 + \overline{b_1}^2x_3 + x_2 + b_1x_3 = 0$

$\Rightarrow (\overline{b_1}^2 + b_1)x_3 = 0$

Comme $\overline{b_1}^2 + b_1 = 0$, alors $\exists x_3 \in \mathbb{F}_4$.

On remplace x_1 dans la formule (3) :

$b_1^2x_2 + x_3 + \overline{b_1}x_2 + x_3 = 0$

$\Rightarrow (b_1^2 + \overline{b_1})x_2 = 0$

Comme $b_1^2 + \overline{b_1} = 0$, alors $\exists x_2 \in \mathbb{F}_4$.

Donc on a : $V = (b_1x_2 + \overline{b_1}x_3, x_2, x_3) = x_2(b_1, 1, 0) + x_3(\overline{b_1}, 0, 1)$

Ainsi il existe deux vecteurs propres $v_1 = (b_1, 1, 0)$ et $v_2 = (\overline{b_1}, 0, 1)$ pour la valeur propre $\lambda = 0$.

• Calculons les vecteurs propres pour $\lambda = 1$:

$BB^*v = \lambda v = v$

$$\begin{pmatrix} 1 & b_1 & \overline{b_1} \\ \overline{b_1} & 1 & b_1 \\ b_1 & \overline{b_1} & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} x_1 + b_1x_2 + \overline{b_1}x_3 & = x_1 \Rightarrow b_1x_2 + \overline{b_1}x_3 = 0...(1) \\ \overline{b_1}x_1 + x_2 + b_1x_3 & = x_2 \Rightarrow \overline{b_1}x_1 + b_1x_3 = 0...(2) \\ b_1x_1 + \overline{b_1}x_2 + x_3 & = x_3 \Rightarrow b_1x_1 + \overline{b_1}x_2 = 0...(3) \end{cases}$$

On multiplie la formule (1) par $\overline{b_1}$, on trouve :

$x_2 + \overline{b_1}^2 x_3 \Rightarrow x_2 = \overline{b_1}^2 + x_3$

On multiplie la formule (3) par $\overline{b_1}$, et on remplace x_1 dans cette formule on trouve :

$x_1 = \overline{b_1}^4 x_3 = \overline{b_1}x_3 = b_1^2x_3$.

Donc on a :

$V = (b_1^2x_3, \overline{b_1}^2 x_3, x_3) = x_3(b_1^2, \overline{b_1}^2, 1)$

Ainsi on a le vecteur propre $(b_1^2, \overline{b_1}^2, 1)$ pour la valeur propre $\lambda = 1$.

Par conséquent la matrice BB^* est diagonalisable ; comme $BB^* = B^*B$ alors les vecteurs singulières à gauches et à droite pour la matrice B sont les mêmes. Alors la matrice B est décomposable en valeurs singulières.

De l'étude précédente on a le théorème suivant :

Théorème 3.4. *Toute matrice circulante d'ordre* 3 *sur le corps* $\mathbb{F}_4$ *est décomposable en valeurs singulières.*

Remarque 3.1.1. L'étude de la décomposition en valeurs singulières d'une matrice circulante à 4 éléments a été déjà étudiée dans 3.1.2, et comme l'ordre des vecteurs ne change pas le résultat, alors les matrices circulantes à 4 éléments ne sont pas décomposables en valeurs singulières.

3.1.4 Les matrices de comparaison des pairs sur un corps à 4 éléments :

Définition 3.3. *Une matrice de comparaison des pairs est une matrice dont les éléments de la diagonale sont égaux à 1 et les éléments supérieurs sont les conjugués des éléments inférieurs de la matrice.*

3.1.4.1 La décomposition en valeurs singulières des matrices de comparaison des pairs

Soit la matrice de comparaison des paires définie comme suit :

$$\mathbf{A} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha \\ \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 1 & \alpha \\ \alpha^2 & \alpha & \alpha^2 & 1 \end{pmatrix}$$

Et :

$$\overline{\mathbf{A}} = \begin{pmatrix} 1 & \alpha^2 & \alpha & \alpha^2 \\ \alpha & 1 & \alpha^2 & \alpha \\ \alpha^2 & \alpha & 1 & \alpha^2 \\ \alpha & \alpha^2 & \alpha & 1 \end{pmatrix} = A^t$$

$$\overline{\mathbf{A}}^{\mathbf{t}} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha \\ \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 1 & \alpha \\ \alpha^2 & \alpha & \alpha^2 & 1 \end{pmatrix} = A$$

Donc :

$$\mathbf{A}\mathbf{A}^* = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha \\ \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 1 & \alpha \\ \alpha^2 & \alpha & \alpha^2 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha \\ \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 1 & \alpha \\ \alpha^2 & \alpha & \alpha^2 & 1 \end{pmatrix} = A^2$$

D'après les tableaux de calcul 1.4 on a le résultat suivant :

$$\mathbf{AA}^* = \begin{pmatrix} 0 & 1 & \alpha & 0 \\ 1 & 0 & 0 & \alpha \\ \alpha^2 & 0 & 0 & 1 \\ 0 & \alpha^2 & 1 & 0 \end{pmatrix}$$

Calculons le déterminant :

$$\mathbf{det}(\lambda\mathbf{I} - \mathbf{AA}^*) = det \begin{pmatrix} \lambda & 1 & \alpha & 0 \\ 1 & \lambda & 0 & \alpha \\ \alpha^2 & 0 & \lambda & 1 \\ 0 & \alpha^2 & 1 & \lambda \end{pmatrix}$$

$=\lambda[\lambda(\lambda^2 - 1) + \alpha(-\lambda\alpha^2)] - (\lambda^2 - 1) - \alpha(\alpha^2) + \alpha[(-\alpha^2) - \lambda(\lambda\alpha^2) + \alpha(\alpha^4)]$

$= \lambda(\lambda^3 - \lambda) - \lambda^2\alpha^3 - \lambda^2 + 1 - \alpha^3 - \alpha^3 - \lambda^2\alpha^3 + \alpha^6$

$=\lambda^4 - 2\lambda^2 - 2\lambda^2\alpha^3 + 1 - 2\alpha^3 + \alpha^6$

$=\lambda^4 + 1 + \alpha^6$

Alors :

$$\lambda^4 + 1 + \alpha^6 = \lambda^4 + 2 = 0$$

ce qui implique que $\lambda^4 = 0$.

c'est à dire il existe une seule valeur propre $\lambda = 0$.

Calculons les vecteurs propres :

$AA^*v = \lambda v = 0$

$$\begin{pmatrix} 0 & 1 & \alpha & 0 \\ 1 & 0 & 0 & \alpha \\ \alpha^2 & 0 & 0 & 1 \\ 0 & \alpha^2 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0$$

$$x_2 + \alpha x_3 = 0 \Longrightarrow x_2 = \alpha x_3$$
$$x_1 + \alpha x_4 = 0 \Longrightarrow x_1 = \alpha x_4$$
$$\alpha^2 x_1 + x_4 = 0 \Longrightarrow 2x_4 = 0 \quad \forall x_4 \in \mathbb{F}_4$$
$$\alpha^2 x_2 + x_3 = 0 \Longrightarrow 2x_3 = 0 \quad \forall x_3 \in \mathbb{F}_4$$

On obtient :

$(\alpha x_4, \alpha x_3, x_3, x_4) = x_4(\alpha, 0, 0, 1) + x_3(0, \alpha, 1, 0)$

Donc on a seulement deux vecteurs propres de la matrice AA^* ce qui fait la matrice AA^* n'est pas diagonalisable. D'où la matrice A n'est pas décomposable en valeurs singulières.

On remarque que AA^* est auto-adjointe sur le corps $\mathbb{F}_4$ mais n'est pas diagonalisable.

Corollaire 3.5. *Les matrices auto-adjointes sur un corps fini ne sont pas nécessairement diagonalisables.*

Conclusion : Dans ce chapitre nous avons étudié la décomposition en valeurs singulières des matrices circulantes et des matrices de comparaison des pairs. Les résultats obtenus montrent(après comparaison avec ceux des matrices réelles ou complexes) que parmi les matrices choisies seules celles ayant un ordre égal à 2^n(où 2 représente la caractéristique de corps) ne sont pas décomposables en valeurs singulières sur le groupe multiplicatif $\mathbb{F}_4^*$.

Conclusion générale et perspectives

Dans ce travail nous avons étudié les valeurs singulières de certaines matrices(les matrices circulantes et les matrices de comparaison des pairs)sur un corps fini $\mathbb{F}_4$ afin d'étudier la décomposition de ces matrices en valeurs singulières.

Pour cette étude nous sommes passés par deux grandes théories de l'algèbre : la théorie algébrique des nombres et le théorème spectral. Les résultats obtenus sont comparés à ceux des matrices réelles ou complexes qui sont décomposables en valeurs singulières. Nos résultats montrent que parmi les matrices choisies seules celles ayant un ordre égal à 2^n(où 2 représente la caractéristique de corps) ne sont pas décomposables en valeurs singulières sur le groupe multiplicatif $\mathbb{F}_4^*$.

Comme perspectives, à la suite de ce travail abordé, nous envisageons de développer les points suivants :

- Étude de la décomposition en valeurs singulières des matrices d'ordre multiple à la caractéristique de corps $\mathbb{F}_4$ comme les matrices d'ordre $6, 10$,

- Étude de la décomposition en valeurs singulières des matrices d'ordre premier avec la caractéristique de corps $\mathbb{F}_4$ comme les matrices d'ordre 7, 9 ,

- Étude permettant de généraliser nos résultats sur les matrices d'ordre 2^n $(n \geqslant 3)$,

- Étude de la décomposition en valeurs singulières des matrices sur un corps de caractéristique p premier, par exemple sur le corps $\mathbb{F}_9$.

- Application des valeurs singulières des matrices dans le processus de l'imagerie.

Bibliographie

[1] J.Baptiste and U.Hiriat Valeurs propres et vecteurs propres, diagonalisation d'une matrice carrée. -. *Université Paul Sabatier(Toulouse(3)).*

[2] T.Ben amor Diagonalisation d'une matrice carrée.-. *Université de la Manouba, l'école supérieure de l'économie numérique.*

[3] F.Dubois and M.Chloé Valeurs propres et vecteurs propres.-. , 11 janvier, 2017.

[4] P.Erin A quest for positive definite matrices over finite fields.-. *Theses and Dissertations. University of south Carolina.https ://scholarcommons.sc.edu/etd*, 2018,29.

[5] J.Guérin and N.Lahrichi and S.Le digabel Décomposition en valeurs singulières (SVD). -. *Polytechnique Montréal* , 2019.

[6] A.Riffaut Existence, unicité et construction des corps finis. -. *Cour d'algèbre*, 2013-2014.

[7] R.Rolland Introduction à l'étude des corps finis.-. https ://docplayer.fr/398766-Introduction-a-l-etude-des-corps-finis.html.

[8] H.Zekraoui Réduction des endomorphismes, formes bilinéaires et formes quadratiques. -. *Noor publishing house. 1 juillet 2018.*