République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Ben M'hidi-Oum El Bouaghi
Faculté des Sciences Exactes
et
des Sciences de la Nature et de la Vie
Département de Mathématiques et Informatique

N° d'ordre:

N° de série:

Mémoire

Présenté par

BAHRI Boubakeur

Pour l'obtention du grade de

Magistère en Algèbre

OPTION:

Elément d'Arithmétique

EXISTENCE DES INVERSES GÉNÉRALISÉS DES MATRICES SUR UN CORPS FINI

Soutenue le 21 Mars 2013

Devant le jury composé de:

Abdelhamid. Ayadi	Président	Professeur	Université d'Oum El Bouaghi
Said Guedjiba	Rapporteur	Professeur	Université de Batna
Lemnouar Noui	Examinateur	Professeur	Université de Batna
Abdelhafid Badis	Examinateur	M. C. A	Université de Khenchela
Hanifa Zekraoui	Invité	M. C. B	Université d'Oum El Bouaghi

Reconnaissances

J’aimerais remercier le Docteur ZEKRAOUI Hanifa , mon Co-encadreur, pour les suggestions secourables et pour le support constant pendant cette recherche. Je tiens aussi à remercier Mon encadreur le Professeur S. Guedjiba pour tout ce qu’il fait pour reussir ce travail, et aussi les membres du jury, le Professeur A. Ayadi, le Docteur A. Badis pour m’avoir donné l’occasion de discuter ce travail, et spécialement le Professeur L. Noui pour les questions stimulantes et les suggestions utiles.

Sommaire

Introduction

Il est bien connu qu'une matrice sur un corps a un inverse, si elle est carrée de déterminant non nul. Cependant, dans plusieurs domaines des mathématiques appliqués on a besoin de quelques types d'inverses partiels d'une matrice singulière, ou même rectangulaires. Par exemple, les solutions d'un système linéaire peuvent exister même si la matrice définissant ce système est singulière. Ce qui conduit à l'inverse ainsi nommé généralisé d'une matrice. L'inversibilité est l'une des disciplines les plus répandues en Mathématique, beaucoup de problèmes sont interprétés par une équation du type $Ax = y$, où A est une transformation linéaire donnée, qui est dans notre situation une matrice de type $m \times n$ sur $\mathbb{F}$ (un opérateur linéaire défini d'un espace vectoriel E dans un autre F de dimensions n et m respectivement) comme l'analyse numérique, l'optimisation, la théorie de contrôle, théorie de codage, la crypto système la statistique et les modèles linéaires. Devant des questions de ce type on cherche un opérateur ayant le maximum de propriétés dont l'inverse usuel réjouit, et d'une manière que cet inverse existe pour une classe aussi large d'opérateurs linéaires.

Si A est un opérateur linéaire, considérons A_0, un opérateur linéaire vérifiant $AA_0A = A$ et $A_0AA_0 = A_0$, ces propriétés, qui sont celles de l'inverse ordinaire, rendent A_0 aussi proche de l'inverse de A, ou autrement dit on est proche d'obtenir $A_0A = I_n$. Les opérateurs les plus proches de l'identité du point de vue propriétés, sont les projecteurs (l'application identique est une projection dont l'image est l'espace tout entier), pour cela,

cherchons A_0 vérifiant l'une ou les deux équations:

$$\begin{cases} A_0 A = & P_E \\ A A_0 = & P_F \end{cases}$$

où P_E et P_F sont des projecteurs vérifiant de plus $P_F\ A = A$ et (ou) $P_E\ A_0 = A_0$. La question a été connue depuis longtemps; utilisée par Fredholm (1903) pour traiter les équations intégrales, aussi par Hurwitz, Hilbert, ..., et ainsi des définitions de ce genre d'opérateurs apparaissent, donnant naissance à une terminologie variée, suivie de notations différentes, mais possédant toutes un point commun, faisant apparaître leurs propriétés proches de celles de l'inverse usuel.

Parmi la terminologie existante, citons par exemple : inverse partiel, inverse intérieur, inverse extérieur, quasi inverse, pseudo inverse, inverse généralisé,.... D'autres inverses portent les noms de leurs fondateurs, par exemple: l'inverse de Moore, l'inverse de Moore-Penrose, l'inverse de Drazin, de Duffin,...

La majorité des propriétés de l'inverse généralisé ont été traitées dans le livre de A. Ben Israël et T. N. E. Greville [1], et aussi dans le [9].

Le déroulement du mémoire:

Dans le premier chapitre on va donner quelques rappels sur la construction et les propriétés d'un corps fini, ensuite les espaces vectoriels, produit scalaire, et sous espace supplémentaire sur un corps fini.

Dans le deuxième chapitre nous donnons les conditions de l'existence de g-inverses, g-inverses réflexives, g-inverses normalisés, et enfin l'inverse de Moore-Penrose.

Dans le troisième chapitre nous exposons deux applications des g-inverses; la première application est sur la résolution d'un système linéaire $Ax = B$ où A est une matrice rectangulaire ou non inversible, l'autre est sur le crypto système où une nouvelle technique basée sur les codes correcteurs d'erreurs a été proposée par Ed Dawson et Chuan-Kun Wu.

Table des notations

$\mathbb{F}_p$ le corps des classes résiduelles modulo p.

$cara\left(\mathbb{F}_q\right)$ est le caractéristique d'un corps $\mathbb{F}_q$.

$\mathbb{F}_q$ extension finie de $\mathbb{F}_p$.

$[\mathbb{L} : \mathbb{K}]$ degré de l'extension $\mathbb{L}$ sur un corps $\mathbb{K}$.

$M_{m\times n}\left(\mathbb{F}\right)$ l'espace des matrices de type $m \times n$ sur $\mathbb{F}$.

$I = I_n$ la matrice identique d'ordre n.

$A^{(1)}$ inverse généralisée de A.

A^- g$-$réinverse de A.

$r(A)$ le rang de A.

$\ker(A)$ le noyau de A.

$\mathrm{Im}(A)$ l'espace image de A.

A^t la matrice transposée de A.

$\langle ., . \rangle$ le produit scalaire.

$W^\perp$ l'espace orthogonal d'un espace vectoriel W.

$\oplus$ la somme directe .

A^+ le Moore-Penrose inverse de A.

$\ell\left(E\right)$) l'espace vectoriel d'endomorphismes de l'espace E.

$M_{m\times n}^{\{1\}}\left(\mathbb{F}\right)$ l'ensemble des inverses généralisés des matrices appartenant à $M_{m\times n}\left(\mathbb{F}\right)$.

Chapter 1
Les corps finis

1.1 Introduction

Le premier chapitre est un chapitre introductif, où nous avons présenté quelques notions et propriétés nécessaires des corps finis et espaces vectoriels [2] , [6] . Nous avons exposé quelques propriétés d'algèbre linéaire qui sont valables lorsque le corps est infini comme $\mathbb{R}$ ou $\mathbb{C}$ mais deviennent fausses lorsque le corps est fini. Citons comme exemples: le produit scalaire, le supplémentaire orthogonal, et les vecteurs isotropes.

1.2 Préliminaires

Dans tout le contenu, $\mathbb{F}$ désigne un corps fini et les coefficients de nos matrices appartiennent à ce corps sauf exception.

Définition 1.2.1 *Un corps fini est un corps qui contient un nombre fini d'éléments.*

Exemple 1.2.1

$\frac{\mathbb{Z}}{p\mathbb{Z}} = \{0, 1, 2, ...p-1\}$ est un corps fini à p éléments. (p premier)

1.2.1 Caractéristique d'un corps fini :

Définition 1.2.2 *Soit F un corps fini tel que $|\mathbb{F}| = p$, le caractéristique de F, noté $cara\,(\mathbb{F})$ est l'ordre de 1 dans le groupe additif de $\mathbb{F}$; i.e. $cara(\mathbb{F}) = inf\{n \in N^*, n.1 = 0\}$.*

Définition 1.2.3 *Un corps premier est un corps qui ne contient aucun sous corps propre.*

Remarque 1.2.1 *Le corps fini premier est le corps* $\frac{\mathbb{Z}}{p\mathbb{Z}}$, *noté* $\mathbb{F}_p$.

Proposition 1.2.1 *Le caractéristique d'un corps fini est un entier premier.*

Preuve. Soit $cara(\mathbb{F}) = p$

1) si $p = 1$ alors $1 \times 1 = 1 \neq 0$.donc 1 n'est pas un *caractéristique.*

2) Supposons que p n'est pas premier, alors $\exists n \succ 1, n \prec p$ et $\exists\ m \prec p$,tel que $p = mn$ et $p \times 1 = 0$. Alors, $(mn) \times 1 = 0 = (\sum_{i=1}^{m} 1)(\sum_{i=1}^{n} 1)$. Comme le corps ne contient pas les diviseurs de zero, alors, $m \times 1 = 0$, ou $n \times 1 = 0$ ce qui contredit la minimalité de p vérifiant $p \times 1 = 0$. ■

R**emarque 1.2.2** $cara(\mathbb{Q}) = 0$. Ainsi tout corps contient un corps premier isomorphe à $\mathbb{Q}$ est de caractéristique nul.

1.3 Construction d'un corps fini

Lemme 1.3.1 *Tout espace vectoriel de dimension* n *sur un corps* $\mathbb{K}$ *est isomorphe à* $\mathbb{K}^n$.

Preuve. Soit $\{x_1, x_2, ..., x_n\}$ une base d'un espace vectoriel E sur $\mathbb{K}$. Alors, pour tout $v \in E$, il existe $a_1, ..., a_n \in \mathbb{K}$, tel que $v = a_1x_1 + a_1x_2 + ... + a_nx_n$. On considère l'application $\psi,\ \psi : E \longrightarrow \mathbb{K}^n$, telle que pour tout $v \in E,\ \psi(v) = (a_1, ..., a_n)$. Il est facile de vérifier que ψ est un isomorphisme.

Théorème 1.3.1 *Pour tout* p *premier, il existe un entier positif* n, *il existe un corps fini* $\mathbb{F}_q$, *extension de* $\mathbb{F}_p$ *tel que* $|\mathbb{F}_q| = p^n$.

Preuve. Pour $n = 1$, il existe $\mathbb{F}_q = \mathbb{F}_p$, et $|\mathbb{F}_q| = p$.

On suppose que $n \neq 1$, alors il existe un polynôme $f(X)$ irréductible sur $\mathbb{F}_p$ (cela est possible, car $\mathbb{F}_p$ n'est pas algébriquement clos, il suffit de voir que le polynôme $p(X) = (X - x_1)....(X - x_p) + 1$ n'a pas de racines dans $\mathbb{F}_p = \{x_1, ..., x_p\}$). Par conséquent, il existe une extension finie $\mathbb{F}_q = \frac{\mathbb{F}_p[X]}{(f(X))}$, tel que dimension de $\mathbb{F}_q$, vu comme espace vectoriel sur $\mathbb{F}_p$ est égale au degré de $f(X)$. Ainsi, $|\mathbb{F}_q| = p^n$, où $n = d^\circ f(X)$. ■

Remarque 1.3.1 Un corps fini est commutatif.

En effet, d'après la preuve précédent, un corps fini est le quotient de $\mathbb{F}_p[X]$ qui est un anneau commutatif.

Théorème 1.3.2 *Soit $\mathbb{F}_q$ un corps fini de cardinal q. Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q - 1$*

Preuve. Comme $\mathbb{F}_q^*$ est commutatif, d'après le Théorème principal des groupes abéliens finis (classement des groupes abéliens), (voir [5]), il existent des groupes cycliques $H_1, H_2, ..., H_r$, tel que

$$\mathbb{F}_q^* = H_1 \times H_2 \times ... \times H_r ,$$

et pour $i = 1, ..., r - 1$, $|H_i|$ devise $|H_{i+1}|$. On pose $N = |H_r|$, l'exposant de chaque élément de $\mathbb{F}_q^*$. Alors, pour tout $x \in \mathbb{F}_q^*$, $x^N = 1$, d'où, tout élément de $\mathbb{F}_q^*$ est racine du polynôme $X^N - 1 \in \mathbb{F}_q[X]$. Or ce polynôme admet au plus N racines. Ainsi, $\left|\mathbb{F}_q^*\right| \leq N$. Comme $|H_r| = N$ divise $\left|\mathbb{F}_q^*\right|$ (d'après le théorème de Lagrange), alors, $N = \left|\mathbb{F}_q^*\right|$, ce qui implique que H_r et $\mathbb{F}_q^*$ sont isomorphes. Par conséquent, $\mathbb{F}_q^*$ est cyclique. ■

Corollaire 1.3.1 *Soit $q = p^n$. Alors, les élément de $\mathbb{F}_q$ sont les p^n racines du polynôme $X^{p^n} - X$.* i.e. $\mathbb{F}_q$ est le corps de décomposition de $X^{p^n} - X$.

Corollaire 1.3.2 *Deux corps possèdent le même cardinal sont isomorphes.*

1.3.1 Élément primitif d'un corps fini (extension primitive)

Soit θ l'élément primitif de l'extension $\mathbb{F}_q = \frac{\mathbb{F}_p[X]}{(f(X))}$, où $d^\circ f(X) = n$, i.e. $\left\{1, \theta, ..., \theta^{n-1}\right\}$ est un $\mathbb{F}_p-$base de $\mathbb{F}_q$. Donc n est le plut petit entier pour lequel $\theta^{p^n-1} = 1$. Sinon, θ serait racine d'un polynôme de degré inférieur à n. Donc θ est aussi un générateur de $\mathbb{F}_q^*$, ce qui justifie la définition suivante:

Définition 1.3.1 *Un générateur du groupe cyclique d'un corps fini $\mathbb{F}_q$ s'appelle un élément primitif.*

Il résulte que si θ est un élément primitif de $\mathbb{F}_q$, alors $\mathbb{F}_q$ est aussi l'ensemble $\left\{0, 1, \theta, ..., \theta^{n-1}\right\}$, avec $n = \left|\mathbb{F}_q^*\right|$.

La fonction φ d'Euler définie par; $\forall n \in \mathbb{N}^*$, $\varphi(n)$ est le nombre des entiers premiers avec n de la série $1, ..., n-1$. Basé sur la formule d'inversion de Möbius, un résultat a été donné dans [5] ; pour $p_1, ..., p_s$ premiers, tels que $n = p_1^{m_1}...p_s^{m_s}$, alors

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)...\left(1 - \frac{1}{p_s}\right). \tag{1.1}$$

Il résulte directement que φ est multiplicative, et que; pour p premier,

$$\varphi(p) = p - 1, \text{ et } \varphi(p^m) = p^{m-1}(p-1). \tag{1.2}$$

À l'aide de cette fonction, nous pouvons déterminer les éléments primitifs d'un corps fini, et ainsi explicitons ce corps à l'aide de l'élément primitif.

Exemple 1.3.1 Dans les exemples suivants nous avons explicité un corps fini à l'aide de son groupe multiplicatif:

1) Élément primitif de $\mathbb{F}_3$: $|\mathbb{F}_3^*| = 2$, d'où, d'après l'équation (1.2), $\varphi(2) = 1$ élément primitif d'ordre 2; premier avec 3. D'où, $\theta = 2 \,[\mathrm{mod}\, 3]$. On peut écrire $\mathbb{F}_3 = \{0, 1, 2\}$.

2) Élément primitif de $\mathbb{F}_5$: $|\mathbb{F}_5^*| = 4 = 2^2$, d'où, d'après l'équation (1.2), $\varphi(4) = 2$ éléments primitifs d' ordre 4; premiers avec 5. D'où, $\mathbb{F}_5 = \{0, 1, 2, 2^2, 2^3\} = \{0, 1, 3, 3^2, 3^3\} \,[\mathrm{mod}\, 5]$.

3) $\mathbb{F}_4$: $\varphi(3) = 2$ éléments primitifs d'ordre 3. Soit θ l'un d'eux, alors, $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$.

4) $\mathbb{F}_9$: $|\mathbb{F}_9^*| = 8 = 2^3$, d'où, $\varphi(8) = 2^2 = 4$ éléments primitifs d'ordre 8. D'où, $\mathbb{F}_9 = \{0, 1, \theta, ..., \theta^7\}$, où θ est l'un d'eux.

5) $\mathbb{F}_{16}^*$ est isomorphe au groupe cyclique d'ordre 15 qui est à son tour, produit direct de deux groupes cycliques d'ordres 3 et 5. D'après l'équation (1.1), on a $\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$ éléments primitifs d'ordre 15. Si θ est l'un d'eux, $\mathbb{F}_{16} = \{0, 1, \theta, ..., \theta^{14}\}$, avec $\theta = \theta_1\theta_2$, où θ_1 est générateur de $\mathbb{F}_4^*$ et θ_2 est générateur du groupe cyclique d'ordre 5, en notant qu'il n'existe pas un corps d'ordre 6, car 6 n'est pas puissance d'un nombre premier.

Exemple 1.3.2 Dans les exemples suivants nous avons explicité un corps fini, vu comme extension primitive du corps $\mathbb{F}_p$.

1) $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{(f(X))}$ avec $f(X) = x^2 + x + 1$. Soit $\theta \in \mathbb{F}_4$, tel que $f(\theta) = 0$. Alors, $\theta^2 = \theta + 1$, d'où, $\mathbb{F}_4 = \{0, 1, \theta, \theta + 1\}$.

2) $\mathbb{F}_9 = \frac{\mathbb{F}_3[X]}{(f(X))}$ avec $f(X) = x^2 + x + 2$. Soit $\theta \in \mathbb{F}_9$, tel que $f(\theta) = 0$. Alors,

$\mathbb{F}_9 = \{a_0 + a_1\theta, a_0, a_1 \in \mathbb{F}_3\} = \{0, 1, 2, \theta, 2\theta, 1+\theta, 2+\theta, 1+2\theta, 2+2\theta\}$,tel que $\theta^2 = 1 + 2\theta$. Ainsi on peut avoir tous les puissances de θ.

1.3.2 Sous corps d'un corps fini

Lemme 1.3.2 *Soient p un premier, et m et n deux entiers non nuls. Alors, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, si et seulement si, m divise n.*

Preuve. Si $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, alors, $\mathbb{F}_{p^n}$ est une extension finie de $\mathbb{F}_{p^m}$, car, $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] [\mathbb{F}_{p^m} : \mathbb{F}_p] = l \times m$, ce qui implique m divise n.

Inversement, si $n = l \times m$, alors, $p^n = (p^m)^l$, d'où, $\mathbb{F}_{p^n}$ est un espace vectoriel de dimension l sur $\mathbb{F}_{p^m}$.

Lemme 1.3.3 *Tout homomorphisme de corps est injectif.*

Preuve. Soit f un *homomorphisme* d'un corps $\mathbb{K}$ dans un corps $\mathbb{K}'$. Alors, $\ker f$ est un idéal de $\mathbb{K}$. Comme $f(1) = 1$, alors $\ker f \neq \mathbb{K}$. D'où, $\ker f = \{0\}$. ■

1.4 Espace vectoriel sur un corps fini

Dans ce paragraphe, on va voir quelques propriétés qui se diffèrent lorsque on travaille sur un corps fini. Cela revient au calculs dans les corps finis: par exemple sur $\mathbb{R}$, l'exemple suivant montre que la dimension d'un sous espace dépend du caractéristique du corps.

Exemple 1.4.1

Soit T l'opérateur de l'espace V des polynômes de degré ≤ 6, qui associe à tout polynôme son dérivé. Soit $f(X) = a_0 + ...a_6X^6$. Alors, sur $\mathbb{R}$,

$$\ker(T) = \{f(X), T(f(X)) = f(X)' = 0\} \implies \{f(X) = a_0 \in \mathbb{R}\} = \mathbb{R},$$

$\dim(\ker(T)) = 1$

$\mathrm{Im}(T) = \{T(f(x)) = f(x)',\ f(x) \in V\} = \left\{\sum_{i=0}^{5} a_i x^i, a_i \in \mathbb{R}\right\}$, engendré par $B = \{1, x, x^2, x^3, x^4, x^5\}$, $\dim(\mathrm{Im}(T)) = 6$. Sur $\mathbb{F}_2$, $\ker(T)$ est engendré par $\{1, x^2, x^4, X^6\}$. $\mathrm{Im}(T)$ est engendré par $B = \{1, x^2, x^4\}$

1.4.1 Quelques résultats classiques

Soient A, B et $C \in M_{m\times n}(\mathbb{F})$ ou $\mathbb{F}$ est un corps quelconque. Alors,

1) Le théorème des dimensions:

$$\dim(\ker(A)) + \dim(\mathrm{Im}(A)) = n.$$

2) Si $B \in M_{m\times n}(\mathbb{F})$ et $C \in M_{n\times p}(\mathbb{F})$,alors,

$$r(BC) = r(C) - \dim(\ker(B) \cap \mathrm{Im}(C)) \leq \min(r(B), r(C)).$$

3) Pour toute matrice A, on a $r(A^t) = r(A)$.

4) Soient U et W deux sous espaces vectoriels d'un espace vectoriel V, alors, si $W \subset U$ et $dimW = dimU$, alors $W = U$.

1.4.2 Produit scalaire

Définition 1.4.1 *Soient $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n)$ deux vecteurs se $F = \mathbb{F}_q^n$. Le produit scalaire euclidien sur $\mathbb{F}_q^n$ est la forme bilinéaire symétrique qui à tout x et y de $(\mathbb{F}_q^n)^2$ associe l'élément $\langle x, y\rangle = x^t\, y = y^t\, x = \sum_{i=1}^{n} x_i y_i \ [\mathrm{mod}\, p]$ de $\mathbb{F}_q$. Deux vecteurs x, y sont dites orthogonaux si $\langle x, y\rangle = 0$, ils sont dites isotropes, si $\langle x, y\rangle = 0 \Rightarrow x = y$.*

1.4.3 Sous espaces orthogonaux

Définition 1.4.2 *Soit U un sous espace vectoriel de $\mathbb{F}_q^n$. Le sous espace orthogonal de U est l'ensemble $U^\perp = \{y \in \mathbb{F}_q^n, \forall x \in U; \langle x, y\rangle = 0\}$.*

On va citer quelques propriétés qu'on a besoin dans le chapitre qui vient:

Soit U un sous espace de $\mathbb{F}_q^n$, alors,

1) $dimU + dimU^\perp = n$.

2) $((U)^\perp)^\perp = U$.

3) Il existe des sous espaces vectoriels contenus dans leurs orthogonal. Dans ce cas, le sous espace vérifiant cette propriété et dit auto orthogonal. S'il est égal à son orthogonal, on l'appelle auto dual, (dans ce cas, $\dim \mathbb{F}_q^n$ est paire).

Exemple 1.4.3

1) Soient l'espace vectoriel $F = \mathbb{F}_2^3$ et $U = \{(0,0,0),(1,1,0)\}$, alors,

$U^\perp = \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\}$. On a $U \subset U^t$.

2) $V = \mathbb{F}_2^4$, $U = \{(0,0,0,0),(1,1,0,0),(0,0,1,1),(1,1,1,1)\} = U^\perp$.

1.4.4 Le supplémentaire orthogonal d'un sous espace vectoriel

Théorème 1.4.1 *Soient U et W deux sous espace vectoriels de $\mathbb{F}_q^n$. Alors, les conditions suivantes sont équivalentes :*

1) Pout *tout* $v \in \mathbb{F}_q^n$, il existe l'uniques $u \in U,\ w \in W$, tels que $v = u + w$.

2) $n = dimU + dimW$ et $U \cap W = \{0\}$.

3) Si $u + w = 0, u \in U, w \in W$, *alors* $u = w = 0$.

4) Si $\{u_1, ..., u_l\}, \{w_1, ..., w_m\}$ *sont deux bases de* U *et* W *respectivement alors,* $\{u_1, ..., u_l, w_1, ..., w_m\}$ *est une base de* $\mathbb{F}_q^n$.

Définition 1.4.3 *Soit* U *un sous espace vectoriel de* $\mathbb{F}_q^n$. *S'il existe* W *un sous espace vectoriel de* $\mathbb{F}_q^n$, *satisfaisant l'une des conditions du théorème précédent, alors,*W *s'appelle le supplémentaire de* U *dans* $\mathbb{F}_q^n$, et on note $\mathbb{F}_q^n = U \oplus W$. De plus si $W = U^\perp$, alors, W *s'appelle le supplémentaire orthogonal de* U *dans* $\mathbb{F}_q^n$, et on dit que $\mathbb{F}_q^n$ est la somme directe orthogonale de U et $U^\perp$, et on note $\mathbb{F}_q^n = U \overset{\perp}{\oplus} W$.

Exemple 1.4.4 Soient $F = \mathbb{F}_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$, $U = \{(0,0), (1,0)\}$, $U^\perp = \{(0,0), (0,1)\}$. D'où $U^\perp$ est le supplémentaire orthogonal de U, car $\{(1,0), (0,1)\}$ est une base de F, or le sous espace $W = \{(0,0), (1,1)\}$ n'a pas de supplémentaire orthogonal, car $W = W^\perp$.

1.4.5 Projection orthogonale

Définition 1.4.4 *Soit* p *un endomorphisme de* E *dans* E, e *une base orthonormée de* E *et* P *la matrice de* p *dans la base* e, *alors,* p *est un projecteur orthogonal, si et seulement si,*

1) $P^2 = P$.

2) $P^t = P$.

Définition 1.4.5 *Soit* $A \in M_{n\times n}(\mathbb{F}_q)$. *Alors,* A *est dite symétrique, si et seulement si,* $A^t = A$.

Lemme 1.4.1 *Soit* $A \in M_{n\times n}(\mathbb{F}_q)$. *Alors,* A *est symétrique, si seulement,* $\forall x, y \in (\mathbb{F}_q^n)^2$, $\langle Ax, y\rangle = \langle x, Ay\rangle$.

Lemme 1.4.2 *Soit $A \in M_{n\times n}(\mathbb{F}_q)$, telle que $A^2 = A$, alors, A est symétrique si et seulement si,* $\ker(A) = (\mathrm{Im}(A))^{\perp}$.

Preuve. Supposons que $A^2 = A$ et $\ker(A) = (\mathrm{Im}(A))^{\perp}$, alors, pour tous $x_1, x_2 \in \mathbb{F}_q^n$, on a,

$$x_1 = Ax_1 + (I_n - A)x_1,\ x_2 = Ax_2 + (I_n - A)x_2.$$

D'où,

$$Ax_1 = A^2x_1 + (A - A^2)x_1,$$

ce qui implique

$$(I_n - A)x_1,\ (I_n - A)x_2 \in \ker(A) = (\mathrm{Im}(A))^{\perp}.$$

Par conséquent,

$$\langle Ax_1, x_2\rangle = \langle Ax_1, Ax_2 + (I_n - A)x_2\rangle = \langle Ax_1, Ax_2\rangle.$$

De manière analogue, on a, $\langle x_1, Ax_2\rangle = \langle Ax_1, Ax_2\rangle$, ce qui donne $A = A^t$, d'après le lemme 1.4.1.

Inversement, supposons que $A = A^t$, $\forall\ x \in \mathbb{F}_q^n$, $y \in \ker(A)$, alors,

$$\langle Ax, y\rangle = \langle x, Ay\rangle = \langle x, 0\rangle = 0,$$

ce qui donne $\mathrm{Im}(A) \subset (\ker(A))^{\perp}$. D'après le théorème des dimensions, on obtient

$$(\ker(A))^{\perp} = \mathrm{Im}(A).$$

i.e. $\ker(A) = (\mathrm{Im}(A))^{\perp}$. ■

Chapter 2
Existence des inverses généralisées des matrices sur un corps fini

2.1 Introduction

Depuis 1970 la théorie des inverses généralisés des matrices a été systématiquement développée. La plupart des résultats ont été obtenus $\mathbb{R}$. Mais, avec le développement de la communication numérique et informatique, la méthodologie algébrique sur le corps fini a été largement exploitée.

Rohde a distingué quatre types des g-inverses sur le corps $\mathbb{R}$ où $\mathbb{C}$: g-inverse, g-inverse réflexive, g-inverse normalisé et Moore-Penrose inverse. Pearl montre dans [7] q'un g-inverse normalisé d'une matrice A sur un corps arbitraire existe si et seulement si, $r(A^tA) = r(A)$, or, A^+existe si et seulement si, $r(AA^t) = r(A^tA) = r(A)$. Dans ce chapitre, nous avons étudié les inverses généralisés sur un corps fini, les conditions nécessaires et suffisante pour l'existence des inverses généralisés, et également, la relation entre la décomposition en somme directe, en somme directe orthogonale d'un espace vectoriel sur un corps fini et l'existence de certains types d'inverses généralisés. À la fin du chapitre, nous avons montré que contrairement à $\mathbb{R}$ et $\mathbb{C}$, le nombre des inverses généralisés d'une matrice de $M_{m\times n}(\mathbb{F}_q)$ de rang r est fini et égale à q^{mn-r^2}, [4] .

Définition 2.1.1 *Soit* $A \in M_{m\times n}(\mathbb{F}_q)$. *Un* g−*inverse (inverse généralisé) de* A, *notée* $A^{(1)}$ *est une matrice* $B \in M_{n\times m}(\mathbb{F}_q)$ *satisfaisant l'équation suivante:*

$$ABA = A.$$

De plus, si B *satisfait, l'équation*

$$BAB = B,$$

alors, B *est dite* g−*inverse réflexive de* A, *notée* $A^{(12)}$. *L'inverse de Moore-Penrose noté* A^{+}, *est l'unique matrice* X *satisfaisant les équations:*

$$\begin{array}{rcll} AXA & = & A & (1) \\ XAX & = & X & (2) \\ (XA)^t & = & XA & (3) \\ (AX)^t & = & AX & (4) \end{array}$$

Une matrices satisfaisant (1), (2) *et* (3) *s'appelle* g−inverse normalisée à gauche, notée $A^{(123)}$. *Une matrices satisfaisant* (1), (2) *et* (4) *s'appelle* g−inverse normalisée à droite, notée $A^{(124)}$.

L'exemple suivant montre qu'il y a des matrices qui possèdent plus q'un g−inverse, mais, ne possèdent pas certains types d'inverses généralisés (contrairement à $\mathbb{R}$ et $\mathbb{C}$).

Exemple 2.1.1

Soit $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Sur $\mathbb{F}_2$, A possède quatre g−inverses: $B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $B_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = A^{(124)}$, $B_4 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$.

Mais, A ne possède pas l'inverse de Moore-Penrose, car $r(AA^t) = 0 \neq 1 = r(A)$.

2.2 Existence de certains types d'inverses généralisés

La preuve des théorèmes qui suivent est basée sur le lemme suivant:

Lemme 2.2.1 *Soit $A \in M_{m\times n}(F_q)$, de rang r, alors, on peut présenter A sous l'un des formes suivantes:*

1) $A = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q$ *pour* $r \leq min\{m, n\}$,

2) $A = P\,(I_r,\ 0)\,Q$ *pour* $r = m \leq n$,

3) $A = P\binom{I_r}{0} Q$ *pour* $r = n \leq m$,

ou P et Q sont deux matrices inversibles des ordres m et n respectivement.

Preuve. Soit $A \in M_{m\times n}(\mathbb{F}_q)$, de rang r. À l'aide des opérations élémentaires sur les lignes et les colonnes de A, on peut mettre A sous l'un des formes indiquées. ■

2.2.1 Existence des g−inverses d'une matrice

Théorème 2.2.1 *Pour toute matrice $A \in M_{m\times n}(\mathbb{F}_q)$, de rang r, il existe deux matrices inversibles P et Q, telles que $A = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q$. Un g−inverse de A,est une matrice $G \in M_{n\times m}(\mathbb{F}_q)$, de la forme $G = Q^{-1}\begin{pmatrix} I_r & U \\ V & W \end{pmatrix} P^{-1}$,où $U \in M_{r\times(m-r)}(\mathbb{F}_q)$, $V \in V_{(n-r)\times r}(\mathbb{F}_q)$ et $W \in M_{(n-r)\times(m-r)}(\mathbb{F}_q)$.*

Preuve. D'après le lemme 2.2.1, on prend la forme générale $A = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q$, avec $r \leq \min\{m, n\}$. Soit $G = Q^{-1}FP^{-1}$, où

$$F = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix},$$

$F_{12} \in M_{r\times(m-r)}(\mathbb{F}_q)$, $F_{21} \in M_{(n-r)\times r}(\mathbb{F}_q)$, $F_{22} \in M_{(n-r)\times(m-r)}(\mathbb{F}_q)$, alors,

$$AGA = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix}\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q,$$

si seulement si, $F_{11} = I_r$. D'où, $G = Q^{-1}\begin{pmatrix} I_r & F_{21} \\ F_{21} & F_{22} \end{pmatrix} P^{-1}$. ■

2.2.2 Existence des g−inverses réflexives d'une matrice

Théorème 2.2.2 *Toute* g−*inverse réflexive de* A *est sous l'un des formes:*

1) $A^{(12)} = Q^{-1}\begin{pmatrix} I_r & Y \\ X & XY \end{pmatrix} P^{-1}$ *pour* $r \leq \min\{m, n\}$,

2) $A^{(12)} = Q^{-1}\binom{I_r}{X} P^{-1}$ *pour* $r = m \leq n$,

3) $A^{(12)} = Q^{-1}(I_r, Y)P^{-1}$ *pour* $r = n \leq m$, *où* X *et* Y *sont deux matrices arbitraires de taille* $(m-r)\times r$ *et* $r\times(n-r)$ *respectivement.*

Preuve. C'est juste un calcul direct en mettant A sous l'une des formes du lemme 2.1.1. ■

Lemme 2.2.2 *Soit* A *une matrice. Alors,*

1) Pour $A^{(1)}$ *un* g−*inverse de* A, *on a,*

$$r(A^{(1)}) \geq r(A) = r(A^{(1)}A) = r(AA^{(1)}).$$

2) Pour $A^{(12)}$ *un* g−*inverse réflexive de* A, *on a,*

$$r(A) = r(A^{(12)}).$$

Preuve. Pour deux matrices B et C, on a, $r(BC) \leq \min\{r(B), r(C)\}$,

alors, 1)

$$r(A) \geq r(AA^{(1)}) \geq r(AA^{(1)}A) = r(A) \Longrightarrow r(A) = r(AA^{(1)}),$$

$$r(A) \geq r(A^{(1)}A) \geq r(AA^{(1)}A) = r(A) \Longrightarrow r(A) = r(A^{(1)}A),$$

d'où,

$$r(A) = r(AA^{(1)}) = r(A^{(1)}A).$$

D'autre part

$$r(A^{(1)}) \geq \ r(AA^{(1)}A) = \ r(A).$$

2) Comme A et $A^{(12)}$ sont l'un est g$-$inverse de l'autre, alors, il suffit d'appliquer la première partie à $A^{(12)}$, g$-$inverse de A, et à A g$-$inverse de $A^{(12)}$. ■

Corollaire 2.2.1 *Soit $A^{(12)}$ un g$-$inverse réflexive de A, alors,* $\mathrm{Im}(AA^{(12)}) = \mathrm{Im}(A)$ *et* $\ker(A^{(12)}A) = \ker(A)$, $\mathrm{Im}(A^{(12)}A) = \mathrm{Im}(A^{(12)})$, *et* $\ker(AA^{(12)}) = \ker(A^{(12)})$.

Lemme 2.2.3 *Soit $A^{(1)}$ un g$-$inverse de A, alors, $A^{(1)}A$, et $AA^{(1)}$ sont des projecteurs sur* $\mathrm{Im}(A^{(1)}A)$ *et* $\mathrm{Im}(A)$ *respectivement.*

Preuve. $\left(AA^{(1)}\right)^2 = \left(AA^{(1)}A\right)A^{(1)} = AA^{(1)}$, $\left(A^{(1)}A\right)^2 = A^{(1)}\left(AA^{(1)}A\right) = A^{(1)}A$.

■

Le Corollaire 2.2.1 et le lemme 2.3.2 nous permettent de décomposer les espaces $\mathbb{F}_q^n$ et $\mathbb{F}_q^m$ en somme directe des sous espaces vectoriels comme le montre le corollaire suivant:

Corollaire 2.2.2 *Soient $A \in M_{m\times n}(\mathbb{F}_q)$, et $A^{(12)}$ un g$-$inverse réflexive de A, alors,*

$$\mathbb{F}_q^n = \mathrm{Im}(A^{(12)}A) \oplus \ker(A) \text{ et } \mathbb{F}_q^m = \mathrm{Im}(A) \oplus \ker(A^{(12)}).$$

2.2.3 Existence d'une g−inverse normalisée à gauche

Théorème 2.2.3 *Soient $A \in M_{m\times n}(\mathbb{F}_q)$ et $A^{(12)}$ un g−inverse réflexive de A, alors, $A^{(12)}$ satisfait la condition (3) de la Définition 2.1.1, si et seulement si,*

$$\mathbb{F}_q^n = \ker(A) \oplus (\ker(A))^{\perp}.$$

Preuve. La nécessité : Soit $A^{(12)}$ une g-inverse réflexive de A qui satisfait la condition (3), i.e.

$$(A^{(12)}A)^t = A^{(12)}A.$$

Alors, d'après lemme 1.4.2, nous avons

$$(\ker(A^{(12)}A))^{\perp} = \mathrm{Im}(\ A^{(12)}A).$$

Or, du corollaire 2.2.1, nous avons: $\ker(A^{(12)}A) = \ker(A)$. Par suite, le corollaire 2.2.2 donne:

$$\mathbb{F}_q^n = \ker(A) \oplus (\ker(A))^{\perp}.$$

La suffisance : Supposons que la condition $\mathbb{F}_q^n = \ker(A) \oplus (\ker(A))^{\perp}$ est vérifie, alors, pour tout $z \in \mathbb{F}_q^n$, il existe l'unique $y \in \ker(A)$ et il existe l'unique $x \in (\ker(A))^{\perp}$, tels que $z = x + y$. D'où, $Az = Ax$. D'où,

$$\mathrm{Im}(A) = \left\{Ax,\ x \in (\ker(A))^{\perp}\right\}.$$

Soit S le supplémentaire de $\mathrm{Im}(A)$ dans $\mathbb{F}_q^m$. Alors, pour tout $z \in \mathbb{F}_q^m$, il existe $x \in (\ker(A))^{\perp}$, il existe $y \in S$, tels que $z = Ax + y$. Ainsi, nous définissons l'application L_B

de $\mathbb{F}_q^m$ à $\mathbb{F}_q^n$ par:

$$L_B : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n \quad z \longmapsto L_B(z)=x$$

L_B est linéaire car, pour $z = Ax + y,\ z' = Ax' + y' \in \mathbb{F}_q^m$ avec $x,\ x' \in (\ker(A))^{\perp}$ et $y,$ $y_{\prime} \in S$, on a,

$$z + z' = Ax + y + Ax' + y' = A\left(x + x'\right) + \left(y + y'\right),$$

d'où,

$$L_B(z + z') = x\ + x' = L_B(z) + L_B(z')$$

Soit $B \in M_{n\times m}\left(\mathbb{F}_q\right)$ la matrice associée à L_B, et comme pour tout $z \in \mathbb{F}_q^n$, il existe l'unique $x \in (\ker(A))^{\perp}$, tel que $Az = Ax$, et $L_B\left(Az\right) = L_B\left(Ax\right) = x$, ce qui implique

$$BAz = BAx = x,$$

d'où,

$$\left(ABA\right)z = A\left(B\left(Ax\right)\right) = Ax = Az,$$

alors, $ABA = A$. D'autre part, pour tout $z \in \mathbb{F}_q^m$, il existe $x \in (\ker(A))^{\perp}$, tel que $Bz = x$ et $BAx = x$, alors,

$$\left(BAB\right)z = BAx = x = Bz,$$

d'où, $BAB = B$, ce qui montre que B est une g$-$inverse réflexive de A. Appliquons le corollaire 2.2.1, nous avons:

$$\mathbb{F}_q^n = \ker(BA) \oplus \mathrm{Im}(BA).$$

Or, $\mathbb{F}_q^n = \ker(BA) \oplus (\ker(BA))^{\perp}$, ce qui donne

$$(\ker(BA))^{\perp} = \mathrm{Im}(BA).$$

Comme $(BA)^2 = BA$, le lemme 1.4.2 donne $(BA)^t = BA$. ■

Remarque 2.2.1 La condition $\mathbb{F}_q^n = \ker(A) \oplus (\ker(A))^\perp$ est équivalente à $r(A) = r(AA^t)$, la condition de Pearl pour l'existence d'une g−inverse normalisée d'une matrice [7].

En effet, de ce qui précède, $\mathbb{F}_q^n = \ker(A) \oplus (\ker(A))^\perp$ est équivalente à $(A^{(12)}A)^t = A^{(12)}A$, alors,

$$A = A\left(A^{(12)}A\right) = A(A^{(12)}A)^t = AA^t\left(A^{(12)}\right)^t,$$

ce qui fait

$$r(A) = r\left(AA^t\left(A^{(12)}\right)^t\right) \leq r\left(AA^t\right) \leq r(A).$$

Exemple 2.2.1
soit $A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ une matrice sur le corps fini $\mathbb{F}_2$. $r(A) = 2$, alors,
$B_1 = \{(1,1,1)\}$ est une base pour le sous espace $\ker(A)$, d'où,

$$\begin{aligned}
(\ker(A))^\perp &= \{y \in \mathbb{F}_2^3,\ \langle y, x\rangle = 0, x \in \ker(A)\} \\
&= \{y = (y_1, y_2, y_3) \in \mathbb{F}_2^3, \langle (y_1, y_2, y_3), ((1,1,1)^t\rangle = 0\} \\
&= \{y \in \mathbb{F}_2^3, y_1 + y_2 + y_3 = 0\} \\
&= \{x(1,1,0)^t + y(1,0,1)^t, x\ , y \in \mathbb{F}_2\}.
\end{aligned}$$

Comme $(1,1,0)$ et $(1,0,1)$ sont linéairement indépendants, alors, $B_2 = \{(1,1,0),(1,0,1)\}$ est une base pour le sous espace $(\ker(A))^\perp$. La famille $B = \{(1,1,1),(1,1,0),(1,0,1)\}$ est libre, ce qui donne

$$\ker(A) \oplus (\ker(A))^\perp = \mathbb{F}_2^3.$$

Donc, la matrice A possède une g−inverse réflexive qui satisfait la condition (3).

Exemple 2.2.2

Soit $A = (1, 1, 0, ..., 0)$, $AA^t = 0,\ r(A) = 1 \neq r(AA^t\ ) = 0$. Donc, la matrice A ne possède pas une g-inverse réflexive qui vérifie la condition (3).

2.2.4 Existence d'une g−inverse normalisée à droite

De la même manière que dans la preuve du théorème 2.2.3, on a le théorème suivant:

Théorème 2.2.4 *La condition nécessaire et suffisante pour que la g−inverse réflexive vérifie la condition* (4) *est que* F_q^m *a la décomposition orthogonale*

$$F_q^m = \mathrm{Im}(A) \oplus (\mathrm{Im}(A)))^{\perp}.$$

De la même manière que dans la preuve de la remarque 2.2.1, on a :

Remarque 2.2.2 La condition $\mathbb{F}_q^n = \ker(A) \oplus (\ker(A))^{\perp}$ est équivalente à

$$r(A) = r(A^t A).$$

Exemple 2.2.3

Soit $A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ sur le corps fini $\mathbb{F}_2, r(A) = 2,$

$$\begin{aligned} \mathrm{Im}(A) &= \{y = (y_1, y_2, y_3) \in \mathbb{F}_2^3, Ax = y, x \in \mathbb{F}_2^3\} \\ &= \{x(1,1,0)^t + y(1,0,1)^t, x, y \in F_2\}, \\ (\mathrm{Im}(A))^{\perp} &= \{y \in \mathbb{F}_2^3, \langle y, b\rangle = 0, b \in \mathrm{Im}(A)\} \\ &= \{y \in \mathbb{F}_2^3, \langle y, (1,1,0)\rangle = 0\} \\ &= \{y\,(1,1,1)\ \ , y \in \mathbb{F}_2\}. \end{aligned}$$

Donc, $\{(1,1,1)\}$ est une base de $(\mathrm{Im}(A))^{\perp}$. D'autre part, $\{(1,0,1),(1,1,0)\}$ une base de $\mathrm{Im}\,(A)$. L'ensemble $B = \{(1,1,1),(1,1,0),(1,0,1)\}$ est une base de $\mathbb{F}_2^3$,d'où, $\mathrm{Im}(A) \oplus (\ \mathrm{Im}(A)))^{\perp} = \mathbb{F}_2^3$. Alors, la matrice A possède une g$-$inverse réflexive qui satisfait la condition (4). Par contre la matrice $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$ ne possède aucune g$-$inverse réflexive qui satisfait la condition (4) car , $r(A) = 2 \neq 1 = r\,(A^t A)$.

2.2.5 Existence de l'inverse de Moore-Penrose

Théorème 2.2.5 *Soit A une matrice de $M_{m\times n}(\mathbb{F}_q)$. La condition nécessaire et suffisante pour que l'inverse de Moore-Penrose de A existe est que les deux décompositions suivantes soient simultanément vérifiées:*

$$\begin{aligned} \mathbb{F}_q^n &= \ker(A) \oplus (\ker(A))^{\perp} \\ F_q^m &= \mathrm{Im}(A) \oplus (\mathrm{Im}(A)))^{\perp}. \end{aligned}$$

En effet, La preuve est une conséquence immédiate de la définition de l'inverse de Moore-Penrose et les théorèmes 2.2.3 et 2.2.4.

Remarque 2.2.3 La condition du théorème 2.2.5 est équivalente à

$$r\,(A) = r\left(A^t A\right) = r\left(AA^t\right).$$

Exemple 2.2.4

Soit $A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ une matrice sur $\mathbb{F}_2, r(A) = 2,$

$$\begin{aligned} \ker(A) \cap (\ker(A))^{\perp} &= \{(0,0,0)\}, \\ \ker(A) + (\ker(A))^{\perp} &= \mathbb{F}_2^3, \\ \mathrm{Im}(A) \cap (\ \mathrm{Im}(A)))^{\perp} &= \{(0,0,0)\} \\ \mathrm{Im}(A) + (\ \mathrm{Im}(A)))^{\perp} &= \mathbb{F}_2^3. \end{aligned}$$

Donc, A possède l'inverse de Moore-Penrose.

Théorème 2.2.6 *Si l'inverse de Moore-Penrose A^+ de A existe, alors, elle est unique.*

Preuve. Supposons qu'il y a deux inverses de Moore-Penrose B et C de A. Alors, $AB = (AB)^t = B^t\ A^t = B^t\ (ACA)^t = B^t\ A^t\ C^t\ A^t = (AB)^t\ (AC)^t = ABAC = AC.$ De la même manière, $BA = CA$. D'où, $B = BAB = CAB = CAC = C.$ ■

Exemple 2.2.5

Soit $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ sur $\mathbb{F}_2$, on a $r\,(A) = r\,(A^tA) = r\,(AA^t) = 2$. Alors,

A^+ existe et $A^+ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Définition 2.2.1 *Soit $A \in M_{m\times n}(\mathbb{F}_q)$. Un $g-$reinverse de A, noté A^- est une matrice $X \in M_{n\times m}(\mathbb{F}_q)$ satisfaisant l'équation suivante: $XAX = X$ (i. e. A est un $g-$inverse de X)*

Proposition 2.2.1 *Soient $A \in M_{m\times n}(\mathbb{F}_q)$, et A^- un $g-$reinverse de A, alors,*

1) $r(A^-) \leq r(A)$

2) $(A^t)^- = (A^-)^t$

3) Si $A = [I_m, 0]Q$, où 0 est la matrice nulle de type $m \times (n-m)$, $Q \in M_{n\times n}(\mathbb{F}_q)$, inversible, alors, $A^- = Q^{-1}\begin{bmatrix} X \\ Y \end{bmatrix}$, *où* X *et* Y vérifient $X^2 = X$ et $YX = Y$.

Preuve. 1) Comme A est un g−inverse de A^-, alors,le résultat est une conséquence immédiate de 1) du Lemme 2.2.2.

2) Comme $A^-AA^- = A^-$, alors, $(A^-)^t A^t (A^-)^t = (A^-AA^-)^t = (A^-)^t$, ce qui fait $(A^-)^t$ est un g−reinverse de A^t.

3) Il, suffit d'appliquer la définition 2.2.1.

2.3 Nombre des inverses généralisés des matrices sur un corps fini

Lemme 2.3.1 *Soit* $M_{m\times n}(\mathbb{F})$ *l'espace des matrices de type* $m \times n$ *sur* $\mathbb{F}_q$. *Le cardinal de* $M_{m\times n}(\mathbb{F})$ *est* q^{mn}.

En effet, $M_{m\times n}(\mathbb{F})$ est isomorphe à $(\mathbb{F}_q)^{mn}$. D'où, le résultat.

Lemme 2.3.2 *Soit* $A\{1\}$ *et* $A\{1,2\}$ *les ensembles des g−inverses et des g-inverses réflexives d'une matrice* A *de rang* r *sur* F_q. *Alors,*

1) $|A\{1\}| = q^{nm-r^2}$.

2) $|A\{1,2\}| = q^{r(m+n-2r)}$.

Preuve. Soit $A = Q\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}P$. Alors, 1) $A^{(1)} = P^{-1}\begin{pmatrix} I_r & U \\ V & W \end{pmatrix}Q^{-1}$,

où la taille de U est $r \times (m-r)$, celle de V est $r \times (n-r)$, et la taille de W est $(n-r)\times(m-r)$. D'après le lemme 2.3.1, et les choix différents de U, V,et W, nous avons

$$|A\{1\}| = q^{r(n-r)}q^{r(m-r)}q^{(n-r)(m-r)} = q^{nm-r^2}.$$

2) $A^{(12)} = P^{-1}\begin{pmatrix} I_r & Y \\ X & XY \end{pmatrix}Q^{-1} = P^{-1}\begin{pmatrix} I_r & O \\ X & I \end{pmatrix}\begin{pmatrix} I_r & O \\ O & O \end{pmatrix}\begin{pmatrix} I_r & Y \\ O & I \end{pmatrix}Q^{-1}$,

X et Y deux matrices arbitraires de taille $(m-r)\times r$ et $r\times(n-r)$ respectivement. Ainsi,

$$|A\{1,2\}| = q^{(m-r)r}q^{r(n-r)} = q^{r(n+m-2r)}. \blacksquare$$

Exemple 2.3.1

Soit $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ une matrice sur $\mathbb{F}_2, r(A) = 1$, alors, $|A\{1\}| = 2^{2\times 2-1} = 8$, $|A\{1,2\}| = 2^{(2+2-2)} = 4$.

Pour $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, r(A) = 2$, alors, $|A\{1\}| = 2^{2\times 3-4} = 4$, $|A\{1,2\}| = 2^{2(5-4)} = 4$. Donc, $A\{1\} = A\{1,2\}$.

Chapter 3
Applications des inverses généralisées des matrices

3.1 Introduction

Dans ce chapitre nous exposons deux applications des inverses généralisés des matrices; la première application est sur la résolution d'un système linéaire $Ax = B$ où A est une matrice rectangulaire ou non inversible en utilisant les g−inverses ou les g−inverses réflexives de cette matrice, l'autre est sur le cryptosystème, où une nouvelle technique basée sur les codes correcteurs d'erreurs [6] et les g−reinverse d'une matrice a été proposée par Ed Dawson et Chuan-Kun Wu.

3.2 Résolution de l'équation $AX = B$

Beaucoup de problèmes sont interprétés par une équation du type $Ax = y$, où A est une transformation linéaire donnée, qui est dans notre situation une matrice de type $m \times n$ sur un corps fini $\mathbb{F}$. Les solutions d'un système linéaire peuvent exister même si la matrice définissant ce système est singulière ou rectangulaire.

Lemme 3.2.1 *Soient A et B deux matrices de taille $m \times n$ et $n \times 1$ respectivement.*

1) L'équation $AX = B$ admet une solution, si et seulement si,

$$\mathrm{Im}(B) \subset \mathrm{Im}(A)$$

2) Si la condition 1) est vérifiée,alors la solution générale de l'équation $AX = B$ est

$$X = A^{(1)}(AA^{(1)})B + (I - A^{(1)}A)U,$$

où $A^{(1)}$ est une g−inverse de A, et U est une matrice de taille $n \times 1$.

Preuve. 1) Soit $A^{(1)}$ une g−inverse de A, alors, $(AA^{(1)})$ est un projecteur sur $\mathrm{Im}(A)$.

Si $\mathrm{Im}(B) \subseteq \mathrm{Im}(A)$, on a $(AA^{(1)})B = B$, d'où $A(A^{(1)}(AA^{(1)})B) = B$, et il s'ensuit que $X_0 = A^{(1)}(AA^{(1)})B$ est une solution de l'équation $AX = B$.

Réciproquement, si $AX = B$ admet une solution, alors il existe une matrice X_0, telle que $AX_0 = B$. Par suite, $\mathrm{Im}(B) \subseteq \mathrm{Im}(A)$.

2) Soit X_0 une matrice, telle que $AX_0 = B$, alors, pour tout X, telle que $AX = B$, on a $A(X - X_0) = 0$. Par suite, $\mathrm{Im}(X - X_0) \subset \ker(A)$. Le Corollaire 2.2.1 donne

$$\ker(A) = \ker((A^{(1)}A)) = \mathrm{Im}((I - A^{(1)}A)).$$

On déduit qu'il existe une matrice U, telle que

$$X - X_0 = (I - A^{(1)}A)U.$$

D'où la solution générale est sous la forme

$$X = X_0 + (I - A^{(1)}A)U = A^{(1)}(AA^{(1)})B + (I - (A^{(1)}A)U.$$

Si on prend $A^{(12)}$, alors

$$X = A^{(12)}B + (I - A^{(12)}A)U.$$

Exemple 3.2.1 Soit $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ sur $\mathbb{F}_2$, $A^{(12)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$. Alors,

$\mathrm{Im}(A)$ est engendré par les vecteurs colonnes $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. L'équation $AX = B$ admet des solutions si $\mathrm{Im}(B) \subset \mathrm{Im}(A)$. Si on prend $B = c\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, avec $c \in \mathbb{F}_2$, alors, la solution générale est donnée par $X = A^{(12)}B + (I - A^{(12)}A)U$. où $U = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}, u_1, u_2, u_3 \in \mathbb{F}_2$.
Remplaçons A, $A^{(12)}$, B et U par leurs valeurs, nous obtenons

$$X = c\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left(I_3 - \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\right)\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$X = c\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} c \\ 0 \\ c + u_1 + u_2 + u_3 \end{pmatrix}.$$

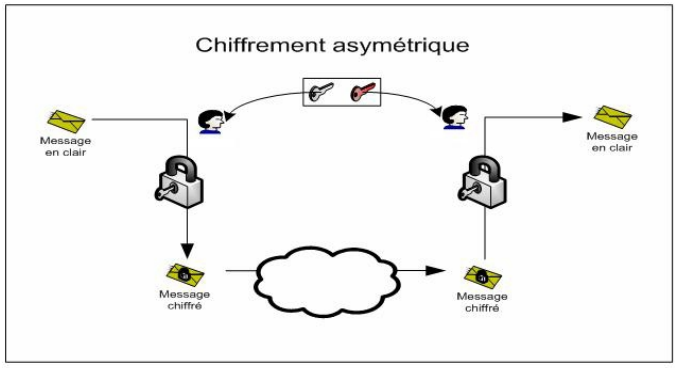
Il y a 4 solutions correspondantes à X.

3.3 Cryptosystème basé sur les codes correcteurs d'erreurs

3.3.1 Introduction

L'inverse généralisé offre un outil potentiel pour la recherche cryptographique en proposant un système de cryptographie à clé publique. Cette nouvelle technique était proposé pour la première fois par Ed Dawson et Chuan-Kun Wu [3] en 1998. Elle est similaire a celle du cryptosystème Mc-Eliece, mais en utilisant les g−reinverses des matrices. L'idée est de développer un système de chiffrement basé sur le code de correction d'erreurs par la technique d'une g−reinverse d'une matrice qui a de bonnes performances.

Le cryptosystème de Mc–Elliece fut inventé en 1978 par Robert Mc-Eliece. La première qualité qu'ont peut trouver à ce cryptosystème est sa vitesse de chiffrement et le déchiffrement qui est aussi rapide que celle des autres cryptosystèmes asymétriques, car il repose sur les calculs matriciels. Les points forts du cryptosystème Mc-Eliece sont la ra-



pidité et la sûreté, mais la taille des clés est un vrai problème. Pour le fonctionnement du cryptosystème de Mc–Elliece est la suivante:

Ahmed veut envoyer le message confidentiel YES (message claire noté plaintext) à Ali. Pour cela, il le chiffre (le message devient chiffrer noté ciphertext). Ali utilise sa clé secrète pour le déchiffrer comme le montre ce schéma :

À travers l'exemple numérique suivant nous avons analysés quelques propriètés de cette technique en comparant les résultats avec ceux de cryptosysteme de Mceliece. Avant de donner l'exemple, on va exposer L'algorithme du cryptosystème de Mc–Elliece suivant:

3.3.2 L'algorithme du cryptosystème de Mc–Elliece

- **Génération des clés**

1. Sélectionnez deux entiers positives k et n (ou $k < n$) comme taille de la matrice génératrice G.

2. Sélectionnez une matrice A de taille $k \times (n - k)$.

3. La matrice génératrice $G = [I_k, A]$.

4. Sélectionnez une matrice inversible S de dimension $k \times k$.

5. Sélectionnez une matrice de permutation P d'ordre n.

6. Calculez $G' = SGP$.

La clé publique: G'.

La clé secrète: P, G, S.

- **Le chiffrement**

1. Message clair : m.

2. Message chiffré : $c = mG' \oplus e$, où e un vecteur binaire de poids inférieur à la capacité de correction d'erreurs.

Pour obtenir le message clair m, on a

- **Le Déchiffrement**

1. Calculer $x = cP^{-1}$.

2. Calculer $y = x \oplus e_1$, où $e_1 = eP^{-1}$.

3. Trouver $m_1$de $m_1G = y$.

4. $m = m_1S^{-1}$.

3.3.3 Exemple numérique sur le Cryptosystème Mc–Elliece

- **Génération des clés**

1. Suppose $k = 4$ et $n = 7$.
2. $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.
3. $G = [I_k, A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$.
4. $S = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.
5. $P = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$.
6. $G' = SGP = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$

Du calcul ci-dessus, la clé publique est G', et la clé privée est formée de P, G et S.

Simulation

- **Le Chiffrement:**

Supposons que vous souhaitez crypter un message YES, la première des choses est de la convertir au code ASCII (8 bits), le message devient :

$$\underbrace{01011001}\underbrace{01000101}\underbrace{01010011}.$$

Comme $k = 4$, le message doit être diviser en blocs de 4 bits

$$\underbrace{0101}\ \underbrace{1001}\ \underbrace{0100}\ \underbrace{0101}\ \underbrace{0101}\ \underbrace{0011},$$

comme m_1, m_2, m_3, m_4, m_5, et m_6 respectivement. Supposons que vous prenez un vecteur Binaire aléatoire $e = (0, 0, 1, 0, 0, 0, 0)$, le processus de chiffrement pour obtenir un message chiffré c_1, c_2, c_3, c_4, c_5 et c_6 peut se faire comme suit:

$$\begin{aligned} c_i &= m_i G' \oplus e, \ \ i = 1, ..., 6. \\ c_1 &= m_1 G' \oplus e = (0,1,0,1) \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \oplus (0,0,1,0,0,0,0) = (0,1,0,1,1,1,0)\,. \end{aligned}$$

Alors,

$$c_2 = (0,1,0,0,1,0,1)\,, c_3 = (1,0,0,0,0,1,1)\,, c_4 = (0,1,0,1,1,1,0)\,, c_5 = (0,1,0,1,1,1,0)\,, .$$

$c_6 = (1,1,0,0,1,0,1)$ Alors, le message chiffré $c = c_1c_2c_3c_4c_5c_6$ est transmis.

- **Le Déchiffrement**

Lorsque le message chiffré c est accepté, le processus de déchiffrement en utilisant la clé privee P, G, et S est comme suit: (le message chiffré doit être divisé en blocs de 7 $bits$, car $n = 7$)

Pour obtenir m_1 du message chiffré c_1 :

$$x_1 = c_1 P^{-1} = (0,1,0,1,1,1,0) \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} = (1,1,0,1,0,1,0)\,,$$

$e_1 = (0,0,0,0,0,0,1)$,$e_1 = eP^{-1}$

$$y_1 = x_1 + e_1 = (1,1,0,1,0,1,1)\,.$$

De $m_{11}G = y_1$, il sera obtenu $m_{11} = (1,1,0,1)$. Ainsi,

$$m_1 = m_{11}S^{-1} = (1,1,0,1) \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (0,1,0,1).$$

De la même manière, on a

$$m_2 = (1,0,0,1), m_3 = (0,1,0,0), m_4 = (0,1,0,1), m_5 = (0,1,0,1), m_6 = (0,0,1,1).$$

Le message clair est $m = m_1 m_2 m_3 m_4 m_5 m_6$, le reconvertir a code ASCII, nous donne le message initiale YES.

3.3.4 L'algorithme du cryptosystéme de WU-DAWSON

- **Génération des clés**

1. Sélectionnez deux entiers positives k et n, ou $k < n$.

2. Sélectionnez une matrice aléatoire A qui a la taille $k \times (n-k)$.

3. La matrice génératrice est $G = [I_k, A]$, de taille $k \times n$.

4. $H_1 = [A^t, I_{n-k}]$.

5. Sélectionnez une matrice inversible S d'ordre $(n-k)$.

6. La matrice de controle est $H = SH_1$.

7. Réduire H à $H = [I_{n-k}, O]Q$, ou O est la matrice nulle de taille $(n-k) \times k$ et Q une matrice inversible d'ordre n.

8. Sélectionnez une matrice X d'ordre $(n-k)$ et Y de taille $k \times (n-k)$tels que $H^- = Q^{-1} \begin{pmatrix} X \\ Y \end{pmatrix}$, g−reinverse de H.

9. $R = H^- H$

La clé publique: G, H^-.

La clé secrète: $R = (H^- H)$.

- **Le Chiffrement:**

1. Le message clair : m.

2. Le message chiffré : $c = mG \oplus e(H^-)^t$, où e est un vecteur binaire. Alors,

$$\begin{aligned} c(I_n \oplus (H^- H)^t) &= c \oplus [(mG \oplus e(H^-)^t)(H^- H)^t] \\ &= c \oplus [mGH^t(H^-)^t \oplus e(H^{-)^t} H^t \left(H^-\right)^t] \\ &= c \oplus [0 \oplus e(H^-)^t] = c \oplus e(H^-)^t = mG. \end{aligned}$$

- **Le Déchiffrement**

Le message chiffré : c.

Le message clair: m.

1. Calculer $y = c(I_n \oplus R^t)$.

2. Trouver de $mG = y$.

3.3.5 Exemple numérique sur le Cryptosystème de Wu-Dawson:

- **Génération des clés**

1. Sélectionnez $k = 4$ et $n = 7$.
2. Sélectionnez $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$
3. $G = [I_4, A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.
4. $H_1 = [A^t, I_3] = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$.
5. Sélectionnez $S = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.
6. $H = SH_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

7. $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} = [I_{n-k}, O]Q.$

8. Sélectionnez $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, et $Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$, tels que

$$H^{-} = Q^{-1} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

9. $R = H^{-}H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$

Du calcul ci-dessus, la clé publique est formée de G et H^{-}, tandisque la clé privée est R.

Simulation:

- **Le chiffrement**

Supposons que vous souhaitez chiffrer un message $[YES]$. La première des choses le message doit être convertir en code ASCII ($8bits$), i.e :

$ASCII\ code \Longrightarrow$

$$\underbrace{01011001}\ \underbrace{01000101}\underbrace{01010011}.$$

. Le message

$$m = \underbrace{0101}\underbrace{1001}\ \underbrace{0100}\ \underbrace{0101}\ \underbrace{0101}\ \underbrace{0011}$$

divisé en blocs de 4 bits(car $k = 4$), comme $m_1, m_2, ...,$ et m_6 respectivement, i.e $m_1 = 0101, m_2 = 1001, m_3 = 0100, m_4 = 0101, m_5 = 0101$, et m_6 = 0001 qui sera crypté comme message chiffré$c_1, c_2, \ldots, c_6$. Le message chiffré c_i peut être calculé par la formule

$$c_i = m_i G \oplus e(H^-)^t,\ i = 1, ..., 6.$$

Si on a choisit un vecteur binaire $e = (0, 1, 1)$, alors,

$$c_1 = (0,1,0,1)\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \oplus (0,1,1)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}^t = (0,0,0,0,0,1,1),$$

$c_2 = (1,1,0,0,1,0,0), c_3 = (0,0,0,1,1,0,0), c_4 = (0,0,0,0,0,1,1), c_5 = (0,0,0,0,0,1,1),$.

$c_6 = (0,1,1,0,1,1,0)$ Donc,

$$c = c_1c_2c_3c_4c_5c_6 = 000001111001000001100000001100000110110110$$

est transmis au récepteur.

- **Le Déchiffrement**

Lorsque le message chiffré c est accepté, le processus de décryptage est comme suit. Le récepteur divise le texte chiffré en blocs de 7 bits (car $n = 7$) $c_1, c_2, \ldots, c_6$. En utilisant la clé privée R, on a

$$m_i G = c_i(I_7 \oplus R^t),\ i = 1, ..., 6.$$

D'où,

$$\begin{aligned} m_1 G &= (0,0,0,0,0,1,1) \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \oplus \begin{pmatrix} 1&0&1&1&1&0&0\\ 1&1&0&0&1&1&0\\ 0&0&0&0&0&0&0\\ 0&1&1&1&0&1&0\\ 0&1&1&1&0&1&0\\ 1&1&0&0&1&1&0\\ 0&1&1&1&0&1&0 \end{pmatrix}^t \\ &= (0,1,0,1,1,0,0). \end{aligned}$$

Alors, m_1 est constitut de quatre premiers colonnes (car $k = 4$) de $m_1 G$. i.e. $m_1 = (0,1,0,1)$. De la même manière,

$$m_2 = (1,0,0,1), m_3 = (0,1,0,0), m_4 = (0,1,0,1), m_5 = (0,1,0,1), m_6 = (0,0,1,1).$$

donc

$$m = m_1 m_2 \ldots m_6 = 010110010100010101010011,$$

ce qui donne le message initiale $[YES\,]$

3.3.6 Propreites de Cryptosystème de Wu-Dawson:

1).le choix de la matrice H^- avec $r(H^-) \leq r(H)$ est nécéssaire pour la sécurite de cryptosystème contre des attaques visant sa destruction car

$$C = mG \oplus e(H^-)^T = (m, e)(G^T, H^-),$$

C est combinaison lineaire de (G^T, H^-) alors le nombre de vecteurs linéairement indépendant de méssage C est égale au rang de (G^T, H^-) ,puisque

$$r(H^-) \leq r(H) = n - k$$

(par définition) donc $r(G^T, H^-) \prec n$, c'est pourquoi la matrice inverse de C n'existe pas autrement l'attaquant peut trouver la clé secrète a partir de

$$I_n \oplus (H^- H)^T = C^{-1}M.$$

1. 2). D'autres attaques sur ce cryptosystéme sont signialées comme:

   a) récuperer H à partir de H^-et comme H est g-inverse de H^-il ya q^{nm-r^2} choix pour trouver H ensuite trouver le vecteur $E = e(H^-)^T$ ce qui trés difficile,

   b) l'attaquant essaie de trouver le vecteur e. Pour cela il doit essayer 2^{n-k} choix, ce qui est couteux ce qui donne une bonne sécurite de cryptosysteme.

3.4 Comparaison entre les deux cryptosystèmes

A fin de mesurer le degré de l'efficacité d'un tel cryptosystème on doit observer ses propriétés suivantes :

(a) la securité de cryptosystème a clé publique.

(b) l'espace des clés (surtout la clé publique).

(c) la rapidité d'encodage et décodage (et leurs complexités).

(d) le taux de l'expansion de message.

Le tableau suivant donne quelques différences en ce qui concerne la taille des clés et le nombre d'opération en bits des deux cryptosystèmes; celui de Mceliece et l'autre de Wu-Dawson:

cryptosystème	W_H	Pk_1	Pk_0	C_D	R
Mceliece	$W_H(e) \leq \frac{d-1}{2}$	k^2+kn+n^2	kn	$2kn + (2n-1)n + (2k-1)k$	$\frac{n}{k}$
Wu-Dawson	$W_H(e) \geq \frac{d-1}{2}$	n^2	$2kn$	$n^3 + 3n^2 - 2n$	$\frac{n}{k}$

Pk_0 : espace de clé publique.

Pk_1 : espace de clé secret.

W_H : le poids de hamming de vecteur d'erreur.

C_D : complexité d'encodage et décodage.

R : taux d'expansion le message.

À partir de ce tableau on constate que :

1. les deux cyptosystèmes sont basés sur les codes correcteurs d'erreurs.

2. les deux cyptosystèmes possèdent un avantage de rapidité du chiffrement et déchiffrement.

3. les deux cryptosystèmes rendent le message chiffré plus long que le message clair (une caractéristique du cryptosystème basée sur la théorie des codes),cette augmentation de la longueur rend le système sensible aux erreurs de transmission.

4. On utilise la technique des g−inverses des matrices sur les corps finis, le poids de Hamming du vecteur d'erreur$W_H(e)$ est plus grand que la capacite de correction d'erreur du code utilisé au contraire de celui de Mceliece.

5. De 4), la taille de la clé publique (G, H^-) est plus petite que celle du cryptosystème de Mceliece ($G^{'} = SGP$) au même niveau de securité.

La théorie des g−inverses des matrices offre un outil potentiel pour la recherche cryptographique et il est également anticipé que cette théorie peut être utilisé pour une grande variété d'applications au cryptographie.

Bibliographie

[1] A. Ben-Israel and T.N.E.Greville, *Generalized inverse theory and applications,* Wiley New York (2003).

[2] J. L. Chabert, *Théorie de Galois et introduction à la théorie des nombres,* Cours, (2007),19-22.

[3] E. Dawson and Chuan –Kun Wu, *Generalized inverse in public key cryptosystem design,* IEE proceedings computer Digit. Tech. **145, 5,** (1998), 321-326.

[4] J. D. Fulton ,*Generalized inverse of matrices over finite field,* Discrete mathematics, **21**, (1978), 23-29.

[5] A. Kostrikin, *Introduction à l'algèbre,* Edition Mir, Moscou, (1977), 393- 394.

[6] F. Lemmermeyer :Error-correcting Codes (February 16, 2005).

[7] M. H. Pearl, *Generalized Inverses of Matrices with Entries Taken from an Arbitrary Field,* Linear Algebra and its Applications, **1,** (1968), 571-587.

[8] C. K. Wu and Ed Dawson, *Existence of Generalized Inverse of Linear Transformations over Finite Fields,* Finite fields and their Applications, **4**, (1998), 307-315.

[9] H. Zekraoui 'These '*Proprietes algebriques des G^k-inverses des matrices,* Université El-Hadj-Lakhdar, Batna, (2011).

Résumé

Un *inverse généralisé* d'une matrice A est une matrice X, sensée de satisfaire:

(i) X est définie pour une classe contenant les matrices non singulières

(ii) X est l'inverse usuel de A lorsque A est non singulière.

(iii) X possède quelques propriétés de l'inverse usuel.

La racine génétique du concept des inverses généralisés apparaît essentiellement dans le contexte de l'ainsi nommé les problèmes linéaires "mal- posé". Toutefois, il semble que cette terminologie a été premièrement mentionnée dans un manuscrit en 1903, attribué à Fredholm, où un inverse particulier généralisé, prénommé aussi "le Pseudo- inverse", d'un opérateur intégral a été donné. Depuis ce temps, ce concept a crû considérablement et devint un domaine actif de la recherche. Le but de la présente thèse est l'étude de quelques conditions d'existence des inverses généralisés des matrices finies sur un corps fini $\mathbb{F}$. En particulier, nous éxposons quelques applications des $g-$inverses des matrices au cryptosystéme

Mots clé: Matrice, inverse généralisé, projecteur, corps fini, cryptosystéme.