REPUBLIQUE DU CAMEROUN
****
Paix-Travail-Patrie
****
UNIVERSITE DE YAOUNDE I
****
ECOLE NORMALE SUPERIEURE
DE YAOUNDE I
****
DEPARTEMENT DE MATHEMATIQUES
****

N
E S

REPUBLIC OF CAMEROON
****
Peace-Work-Fatherland
****
UNIVERSITY OF YAOUNDE I
****
HIGHER TEACHER TRAINING
COLLEGE OF YAOUNDE I
****
DEPARTEMENT OF MATHEMATICS
****

CODES RANG EN CRYPTOGRAPHIE

Mémoire de Di.P.E.S II de mathématiques

De

TSASSE NEUCHY Pelvilin

***Matricule* : 09V0732**

Licencié en Mathématiques

Sous la direction de :

Dr NDJEYA Selestin

Chargé de Cours

Ecole Normale Supérieure, Université de Yaoundé I

Année académique : 2015-2016

CODES RANGS EN CRYPTOGRAPHIE

Mémoire de DIPES II de mathématiques

De

TSASSE NEUCHY PELVILIN

Matricule : **09V0732**

Licencié en Mathématiques pures

Sous la direction de :

Dr. NDJEYA SELESTIN

Chargé de Cours

Ecole Normale Supérieure, Université de Yaoundé I

Année Académique 2015-2016

♠ Dédicace ♠

Je dédie ce mémoire à mon feu père **NEUCHY Jean Pierre**

♠ Remerciements ♠

Merci au Dieu tout puissant pour les merveilles accomplies dans ma vie.

Merci à mon encadreur **Dr NDJEYA Selestin** pour ses conseils avisés, sa disponibilité et surtout pour avoir accepté de diriger ce mémoire. J'adresse également un merci particulier à tout les enseignants du département de mathématique pour la formation que j'ai reçue. Je n'oublie pas le docteur **TALE Hervé** pour toute la documentation qu'il a mis à ma disposition.

Je remercie mes parents **NEUCHY Jean Pierre** et **FOULA Véronique**, Ma tante **MANTO Jeannette**, pour l'amour dont ils n'ont cessé de me combler depuis ma tendre enfance, pour tout les efforts qu'ils ont consentis afin que je soit un homme meilleurs.

J'adresse un très grand merci à tous mes grands frères et mes sœurs, pour leur affection, pour m'avoir protégé et soutenu durant mon cursus scolaire.

Je remercie du fond de mon cœur tous mes amis et connaissances, ces étoiles de ma vie dont le sourire, l'assistance et le réconfort m'ont apporté la joie de vivre, la force et le courage d'avancer.

Je n'oublie pas mes camarades de l'ENS et enfin toutes les personnes qui de près ou de loin ont œuvré à la réussite de ce mémoire.

♠ Déclaration sur l'honneur ♠

Le présent document est une œuvre originale du candidat et n'a été soumis nulle part ailleurs en partie ou en totalité, pour une autre évaluation académique. Les contributions externes ont été dûment mentionnées et recensées en bibliographie.

Signature du candidat

TSASSE NEUCHY PELVILIN

♠ Table des matières ♠

♠ Abstract ♠

This report show the work that we have done on codes with rank metric and their application in cryptography.

The rank metric was first considerate for error control code (ECC) by **Delsarte** . The potentials applications of rank metric codes to wireless communications , public-key cryptosystems and storage equipment have motivate a steady stream of our work.

In this work, we have principally define the rank code and their properties. We have also studied the Gabidulin codes, show what this codes are MDR and presented GPT cryptosystem .

Keys words : rank, codes , cryptography, Galois fields, linear polynomials, cyphertext , plaintext

♠ Résumé ♠

Le mot cryptographie vient du grec « **cruptos** » qui signifie caché et « **grapein** » qui signifie écrire.

Elle peut se définir comme la science qui utilise les mathématiques tels que l'algèbre, pour dissimuler les données.

La cryptographie permet ainsi de sécuriser les informations, quitte à pouvoir les véhiculer à travers les réseaux douteux comme l'Internet, de façon à ce qu'elle ne puissent être reçues et déchiffrées par nul autre que le destinataire.

De nos jour elle est devenue un outil incontournable dans la sécurité informatique et englobe diverses structurations constituant les cryptosystèmes

Dans ce document, un accent particulier a été mis sur les rappels mathématiques tels que la construction des corps finis, les polynômes linéaires et la théorie du codage. Ensuite nous avons défini explicitement les codes rang et leurs propriétés tout en accordant une grande attention à une classe très utilisée des codes rang , **les codes de Gabidulin**.

La troisième partie est consacrée à l'application des codes rang à la cryptographie. Cette partie traite essentiellement des concepts de base de la cryptographie, du principe de certaines attaques en cryptographie , surtout celles orientées contre le cryptosystème GPT.

La dernière partie traite de la potée pédagogique où nous montrons en quoi le travail effectué dans ce document pourrait être utile à l'enseignement au lycée.

♠ Introduction ♠

La cryptographie est souvent désignée comme la science du secret . Elle trouve ses origines dans la volonté de cacher de l'information dans les communications qu'entretenait Jules César avec ses généraux.

De nos jours, la cryptographie s'est énormément diversifiée et possède de nombreuses applications dans les communications bancaires, dans les téléphones portables ou dans les communications internet sécurisées.

Elle repose essentiellement sur la théorie du codage ; ce qui a retenu notre attention puisque le thème que nous abordons s'intitule « codes rang en cryptographie ». Dans cet ordre d'idées nous axerons notre travail sur quatre parties principales.

Premièrement, nous ferons un rappel sur les bases mathématiques nécessaires ; ensuite nous définirons concrètement les codes rang tout en donnant quelques exemples usuelles de ces types de codes.

La troisième partie sera consacrée à l'apport de la métrique rang en cryptographie et à l'étude d'un cryptosystème basé sur la métrique rang : le cryptosystème GPT.

La quatrième partie quant à elle sera destinée à la portée pédagogique du mémoire.

⋆ ⋆ **Chapitre Un** ⋆ ⋆

RAPPELS MATHEMATIQUES ET INTRODUCTION À LA THÉORIE DU CODAGE

Dans cette partie, nous supposerons acquis les notions fondamentales sur la théorie des groupes et celles sur les anneaux.

1.1 Anneau des polynômes à une indéterminée

Soit $(A, +, .)$ un anneau unitaire. Notons par $F(\mathbb{N}, A)$ l'ensemble des applications de $\mathbb{N}$ dans A.
Pour tout $f \in F(\mathbb{N}, A)$ on note $f = (a_k)_{k\in\mathbb{N}})$ où $a_k = f(k)$
On appelle support de f l'ensemble $supp(f) = \{k \in \mathbb{N} \backslash a_k \neq 0\}$
Notons $F_0(\mathbb{N}, A)$ l'ensemble des éléments de $F(\mathbb{N}, A)$ à support finis.

Remarque 1.1.1. *$f \in F_0(\mathbb{N}, A)$ ssi $\exists n_0 \in \mathbb{N}$ tel que $\forall k \in \mathbb{N}$, $k \geq n_0 \Longrightarrow a_k = 0$*
Dans ce cas on écrit $f = (a_0\ ,\ a_1\ ,\ \ldots\ , a_n\ , 0\ ,\ 0 \ldots . 0\ , 0\ , 0\ , 0)$

l'addition et la multiplication dans $F_0(\mathbb{N}, A)$

Soient $f = (a_k)_k$ et $g = (b_k)_k$ deux éléments de $F_0(\mathbb{N}, A)$
On définit :

- $f + g = (c_k)_k$ avec $c_k = a_k + a_k$
- $f \times g($ ou $f.g\ ) = (d_k)_k$ où $d_k = \sum_{i+j=k} a_i b_j$

L'application nulle est notée 0 lorsque aucune confusion n'est à craindre. C'est l'élément neutre pour l'addition.

L'application $e = (1,\ 0\ ,0\ ,\ ...0\ ,0\ ,0\ ,0)$ est l'élément neutre pour la multiplication.

$(F_0(\mathbb{N}, A), +, \times, 0, e)$ est un anneau unitaire (il est commutatif si A est commutatif).

Définition 1.1.1 (**L'indéterminée**). .

On appelle indéterminée l'application $X = (0,\ 1,\ 0,\ 0,\ 0,\ ...,0\ \ 0,\ 0)$

On a :

- $X^2 = (0,\ 0,\ 1,\ 0,\ 0,\ ...,0\ \ 0,\ 0)$
- $X^3 = (0,\ 0,\ 0,\ 1,\ 0,\ ...,0\ \ 0,\ 0)$
- De façon générale, $\forall n \in \mathbb{N}\ X^n = (d_k)_{k\in\mathbb{N}}$ $\begin{cases} d_k = 0 & \text{si } k \neq n \\ 1 & si\ k = n \end{cases}$

Dans le cas particulier où $n = 0$, on pose $X^0 = e$

Ainsi $\forall f \in F_0(\mathbb{N}, A)$ on peut écrire $f = \sum_{k=0}^{n} a_k X^k$

quand $a_n \neq 0$ on dit que a_n est le coefficient dominant et que f est de dégré n.

f est appelée *polynôme à une indéterminé à coefficients dans A.*. Son dégré est noté $deg(f)$

$F_0(\mathbb{N}, A, +, \times, 0, e)$ est noté simplement $A[X]$ pour dire *l'anneau des polynômes à une indéterminée à coefficients dans A*.

Corollaire 1.1.1. .

* *si f et $g \in A[X]$ tel que le coefficient dominant de g est inversible, alors il existe $q,\ r\ \in A[X]$ tel que $f = gq + r$ et $deg(r) < deg(g)$.*

* *si A est un corps commutatif, alors $A[X]$ est un anneau euclidien.*

En effet :

– *$A[x]$ est un anneau commutatif unitaire*

– *l'application*

$$\begin{array}{rccc} \sigma & : & A[X]\backslash\{0\} & \longrightarrow & \mathbb{N} \\ & & f & \longmapsto & deg(f) \end{array}$$

vérifie

1. $\forall f, g\ \in A[X]\backslash 0$, $deg(f, g) \leq deg(f)$
2. $\forall f, g\ \in A[X] g \neq 0, \exists\ !\ h,\ r\ \in A[X]/f = gh + r$
   Avec $r = 0$ ou $deg(r) < deg(g)$

* *Si A est un corps, alors $A[X]$ est un anneau factoriel. De ce fait, tout polynôme g de $A[X]$ peut s'écrire sous la forme $g = g_1^{\alpha_1}.g_2^{\alpha_2}\cdots g_r^{\alpha_r}$ où g_i est irréductible dans $A[X]$ et $\alpha_i \in \mathbb{N}^*$*

1.2 Rappels sur la théorie des corps finis

Définition 1.2.1. *Un corps est un anneau unitaire où tout élément non nul est inversible. Lorsque l'anneau est commutatif, le corps est dit commutatif.*

Dans toute la suite, sauf mention contraire, tous les anneaux qu'on utilisera seront commutatifs et unitaires.

1.2.1 Caractéristique d'un corps

Soit $(A,+,.)$ un anneau . On pose $W = \{k \in \mathbb{N}^* \backslash \{1\} \ , \ k.1_A = 0\}$

On appelle *caractéristique* de A l'entier $p = \begin{cases} 0 & si \quad w = \emptyset \\ minW & sinon \end{cases}$

Théorème 1.1. .

i) Tout anneau commutatif unitaire et infini possède un sous anneau isomorphe à $(\mathbb{Z},+,.)$

ii) Tout anneau commutatif et unitaire de caractéristique p possède un sous anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$

iii) Si A est un domaine d'intégrité de caractéristique non nul p, alors p est premier

Démonstration. .

i) Considérons l'application

$$\begin{array}{rccc} \phi & : & (\mathbb{Z},+,.) & \longrightarrow & (A,+,.) \\ & & k & \longmapsto & k.1_A \end{array}$$

ϕ est un automorphisme d'anneau injectif car *caract(A)* $= 0$. Ainsi $Ker(\phi) = 0$. Or d'après le premier théorème d'isomorphisme $Im(\phi) \cong \mathbb{Z}/Ker(\phi) = \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

ϕ étant un homomorphisme, $Im(\phi)$ est un sous anneau de A. Ainsi $\mathbb{Z}$ est isomorphe à un sous anneau de A

ii) Soit A un anneau commutatif unitaire de caractéristique fini p .

Nous considérons l'application ϕ définie si dessus.

Montrons que $Ker(\phi) = p\mathbb{Z}$:

- $p\mathbb{Z} \subset Ker(\phi)$ car *caract(A)* $= p$ est
- Soit $k \in Ker(\phi)$. Alors par division euclidienne, il existe $(q,r) \in \mathbb{Z}^2$ tel que $k = pq + r$ avec $0 \leq r < p$.

  Ainsi

$$\begin{aligned} r.1_A1 &= (k-pq).1_A \\ &= k.1_A - pq1_A \quad r.1_A = 0 \Longrightarrow r = 0 \text{ car } p = min\{s \in \mathbb{N}^*/s.1_A = 0\} \\ &= 0 \end{aligned}$$

D'où $k \in p\mathbb{Z}$. Ainsi $Ker(\phi) \subset p\mathbb{Z}$.

iii) Supposons que il existe $r, s \in \mathbb{N}^*$ tel que $p = r.s$. Alors

$p1_A = (r.s)1_A = (r1_A).(s.1_A) = 0$

Ainsi $r1_A = 0$ ou $s1_A = 0$ car A est intègre. Ce qui contredit la minimalité de p

p est donc premier .

□

Corollaire 1.2.1. .

C_1 *Si* $\mathbb{K}$ *est un corps de caractéristique* p *non nul, alors* p *est premier*

C_1 *Tout corps de caractéristique* p *possède un sous corps isomorphe à* $\mathbb{Z}_p$.

On adoptera la notation $\mathbb{F}_q$ où bien $GF(q)$ pour désigner un corps fini à q éléments

1.2.2 Propriétés des corps finis

Proposition 1.1. .

P_1 *Si* $\mathbb{L}$ *est un sous corps d'un corps* $\mathbb{K}$*, alors* $\mathbb{K}$ *a une structure d'espace vectoriel sur le corps* $\mathbb{L}$

P_2 *Si* $\mathbb{K}$ *est un corps fini de caractéristique* $p \neq 0$*, alors le cardinal de* $\mathbb{K}$ *est une puissance de* p

P_3 *Tout les corps fini de même cardinal sont isomorphes*

P_4 *Le cardinal de tout sous-corps d'un corps fini est un diviseur du cardinal du corps*

P_5 *L'ordre de tout élément d'un corps fini est un diviseur du cardinal du corps*

P_6 *Le groupe des inversible* $\mathbb{F}_q^*$ *d'un corps fini est* $\mathbb{F}_q$ *est cyclique de cardinal* $q-1$

Preuve 1.2.1. .

P_1 $(\mathbb{K}, +, .)$ est un groupe *Abélien*. Puisque $\mathbb{L}$ est un sous corps de $\mathbb{K}$, on déduit que pour tout $\alpha,\ \beta\ \in \mathbb{L}$ et $x,\ y\ \in \mathbb{K}$ on a

1. $\alpha(x+y) = \alpha.x + \alpha.y$
2. $(\alpha+\beta)x = \alpha.x + \beta.x$
3. $(\beta.\alpha).x = \beta(\alpha.x)$
4. $1_{\mathbb{K}}.x = x$

P_2 Soit $\mathbb{K}$ un corps fini de $caract(\mathbb{K}) = p$. D'après le corollaire si dessus, $\mathbb{K}$ possède un sous corps isomorphe à $\mathbb{Z}_p$ qui est $\mathbb{F} = \{k1_{\mathbb{K}}/\ k = 1, 2, 3 \cdots p\}$

D'après P_1, $\mathbb{K}$ est un $\mathbb{F} - sous\ espace$ vectoriel .

$\mathbb{K}\ fini \implies dim(\mathbb{K})\ est\ finie$. Posons $n = dim(\mathbb{K})$; on déduit que $card(\mathbb{K}) = p^n$.

P_3 Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps tel que $card(\mathbb{K}) = card(\mathbb{L})$. $\mathbb{K}$ $et\mathbb{L}$ étant fini, ils sont forcement de caractéristique non nul . Car sinon ils posséderaient chacun un sous anneau isomorphe à $(\mathbb{Z}, +, .)$; ce qui serait absurde puisque $\mathbb{Z}\ est\ infini$.

Désignons par p la caractéristique de $\mathbb{K}$ et par q celle de $\mathbb{L}$. $p\ et\ q$ sont premiers ;

d'après ce qui précède, $\mathbb{K}\ est\ un\ \mathbb{Z}_p - espace\ vectoriel$ et $\mathbb{L}\ est\ un\ \mathbb{Z}_q - espace\ vectoriel$. Ainsi $card(\mathbb{K}) = p^n$ et $card(\mathbb{L}) = q^m$ où $n = dim(\mathbb{K})$ $m = dim(\mathbb{L})$

$\mathbb{K}\ et\ \mathbb{L}$ étant de même cardinal, on a $p^n = q^m$.

D'où $p = q$ car $p\ et\ q$ sont des nombres premiers .

Ainsi $m = n$; par suite, $dim(\mathbb{K}) = dim(\mathbb{L})$ et $\mathbb{K}\ et\ \mathbb{L}$ sont des $\mathbb{Z}_p - espace\ vectoriel$. D'où $\mathbb{K} \cong \mathbb{L}$

P_4 Soit $\mathbb{F}_q$ un corps fini, $\mathbb{L}$ un sous corps de F_q. Les classe a gauche suivant $\mathbb{L}$ pour l'addition forment une partition de $\mathbb{F}_q$. On déduit par le théorème de Lagrange que $\mathbb{L}$ divise q

P_5 Soit $\mathbb{K}$ un corps fini ; $x \in \mathbb{K}$. On considère le groupe multiplicatif $(\mathbb{K}, \bullet)$. Soit (x) le sous groupe engendré par x. En considérant les classe à gauche suivant (x), le théorème de Lagrange assure que l'ordre de x divise p^n

P_6 Soit γ un élément d'ordre maximal m . Montrons que $\forall\ x\ \in \mathbb{F}_q^*$, l'ordre de x divise m.

Posons $d = pgcd(m, n)$; alors il existe m', n' premiers entre eux tel que

$m'n' = \dfrac{mn}{d} = ppcm(m, n)$ avec m' et n' divisant respectivement $m\ et\ n$.

Soit $x_1 = x^d$ et $\gamma_1 = \gamma^d$. Alors x_1 et x_2 sont d'ordre n' et m' respectivement.

Posons $z = x_1\gamma_1$; $z^{m'n'} = 1$. Soit $r \in \mathbb{N}$ tel que $z^r = 1$. On a $1 = z^{rm'} = (x_1\gamma_1)^{rm'} = x_1^{rm'}$. Ainsi n' divise rm' car n' est l'ordre de x_1. Et comme $m'\ et\ n'$ sont premiers entre eux, il vient que $n'\ divise\ r$. De même,on montre que $m'\ divise\ r$; puisque $m'\ et\ n'$ sont premiers entre eux, il vient que $n'm'$ divise r . D'où $|z| = n'm' = \dfrac{nm}{d} \geq m$.

γ étant un élément d'ordre maximal, on déduit que $|z| = m$.

$m = m'n' = \dfrac{nm}{d} \Longrightarrow m = \dfrac{nm}{d}$;

il suit que $n = d$ et que n *divise* m

Or l'équation $x^m - 1 = 0$ admet au plus m racines distinctes dans $\mathbb{F}_q^*$. Puisque tous les éléments de $\mathbb{F}_q^*$ sont racines de cette équation, on déduit que $q - 1 \leq m$.

Par ailleurs, d'après le théorème de Lagrange, l'ordre de γ divise l'ordre de $\mathbb{F}_q^*$ qui vaut $q - 1$.

D'où $m = q - 1$. Ainsi, $\mathbb{F}_q^*$ est **cyclique** .

Remarque 1.2.1. $1,\ \gamma,\ \gamma,\ \cdots,\ \gamma^{m-1}$, sont également, les racines de l'équation $x^m - 1 = 0$

Ainsi, $\mathbb{F}_q^* = \{1,\ \gamma,\ \gamma,\ \cdots,\ \gamma^{m-1}\}$

Proposition 1.2. *Tout corps fini $\mathbb{F}_q$ admet « un élément primitif » γ ; c'est à dire un élément d'ordre $q - 1$.*

De ce fait, tout élément non nul de $\mathbb{F}_q$ est une puissance de γ .

$$\mathbb{F}_q = \{0,\ 1,\ \gamma,\ \gamma,\ \cdots,\ \gamma^{q-2}\} = \{x \in \mathbb{F}_q / x^q - x = 0\}$$

Proposition 1.3. *Dans un corps fini $\mathbb{F}_q$ de caractéristique p. Toute puissance de p se distribue sur les termes d'une somme.*

Preuve 1.2.2. .

- Soient $a,\ b\ \in F_q$.

$$\begin{aligned}(a+b)^p &= \sum_{i=0}^{p} C_p^i a^p b^{p-i} \\ &= a^p + \sum_{i=1}^{p-1} pC_{p-1}^i a^i b^{p-i} + b^p\end{aligned}$$

  $\mathbb{F}_q$ étant de caractéristique p, les termes $pC_{p-1}^{i-1} a^i b^{p-i}$ $1 \leq i \leq p-1$ sont tous nuls .

  D'où $(a+b)^p = a^p + b^p$

- à partir de ce qui à été fait ci-dessus, on déduit que $\forall k \in \mathbb{N}$ on a $(a_1 + a_2 \cdots a_k)^p = a_1^p + a_2^p \cdots a_k^p$
- par récurrence sur la puissance k de p, on déduit que

$$(a_1 + a_2 \cdots a_r)^{p^k}) = a_1^{p^k} + a_2^{p^k} \cdots a_r^{p^k}$$

❑

Corollaire 1.2.2. .

➠ *Les éléments de $\mathbb{F}_p$ s'identifient dans un corps fini de caractéristique p aux racines de $x^p - x$.*

Pour la preuve, $\mathbb{F}_p$ étant un corps, il suffit de remplacer q par p dans la ***Proposition 1.2*** *ci-dessus.*

➠ *On peut simplifier les puissances $p^{ième}$ de polynômes à coefficients dans $\mathbb{F}_p$.*

En fait, $P(x)^p = (\sum_n a_n x^n)^p = \sum_n (a_n)^p x^{np}$.

Puisque les a_n sont dans $\mathbb{F}_p$, on obtient $P(x)^p = \sum_n a_n (x^p)^n = P(x^p)$.

Critère de Fröbenius : $\boxed{P(x)^p = P(x^p) \quad si\ et\ seulement\ si \quad P \in \mathbb{F}_p[x]}$

Olivier RIOUL *Corps finis, page 15, Septembre 2011, Telecom ParisTech*

1.3 Extension de corps

Soit $\mathbb{K}$ *et* k deux corps. On dit que $\mathbb{K}$ est une extension de k si k est isomorphe à un sous corps de K . Notation $\mathbb{K}|k$ ou $(\mathbb{K} : k)$

Soit $\mathbb{K}$ une extension de k .

$\mathbb{K}$ peut être identifier à un sous $k - espace$ vectoriel.

Exemple 1.3.1. .

Si $\mathbb{F}_q$ est un corps de caractéristique p, $\mathbb{F}_q$ est une extension de $\mathbb{F}_p$.

Définition 1.3.1. .

a) ***Éléments algébriques d'une extension***

Soit $\alpha \in \mathbb{K}$. α est ***algébrique*** *s'il existe $P \in k[X]$, $P \neq 0$, tel que $\tilde{P}(\alpha) = 0$ ($\tilde{P}$ fonction polynôme associé à P). Dans le cas contraire, α est dit* ***transcendant****.*

Si $\forall \alpha \in \mathbb{K}$, α est algébrique, alors l'extension $\mathbb{K}$ de k est appelée extension algébrique.

b) ***Degré d'une extension***

On appelle degré de l'extension $\mathbb{K}$ de k, la dimension du $k-$espace vectoriel $\mathbb{K}$. On note $[\mathbb{K} : k]$.

Lorsque $[\mathbb{K} : k]$ est fini, $\mathbb{K}$ est une extension fini.

c) ***Polynôme minimal d'un élément algébrique.***

Soit $\mathbb{K}$ une extension d'un corps k , $k(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n)$ le sous corps engendré par k et $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n\}$;

$k[\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n]$ le sous anneau engendré par k et $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n\}$; $\alpha_1 \cdots \alpha_n \in \mathbb{K}$

Proposition 1.4. *Si α est un élément algébrique de $\mathbb{K}$, alors $k[\alpha] = k(\alpha)$.*

Preuve 1.3.1. .

- par définition, on a $k[\alpha] \subset k(\alpha)$
- Montrons que $k(\alpha) \subset k[\alpha]$

  Considérons l'application $\begin{array}{rccc} \Omega: & k[X] & \longrightarrow & k[\alpha] \\ & P & \longmapsto & \Omega(P) = \tilde{P}(\alpha) \end{array}$

  Ω est un *épimorphisme* d'anneaux.

  ✪ $Ker(\Omega) \neq \emptyset$ car α est algébrique.

  On sait que $ker(\Omega)$ est un idéal de $k[X]$ qui est principal. Donc il existe $\zeta \in k[X]$ tel que $Ker(\Omega) = (\zeta)$

  ✪ ζ est irréductible.

  En effet supposons $\exists P, Q \in k[x]$ tel que $deg(P) \geq 1, \quad deg(Q) \geq 1$ et $\zeta = PQ$.
  Alors $\zeta(\alpha) = P(\alpha)Q(\alpha) = 0$ car $\zeta \in Ker(\Omega)$
  $\mathbb{K}$ *intgre* $\Rightarrow$ $P(\alpha) = 0 \quad ou \quad Q(\alpha) = 0$. Ainsi $P \in Ker(\Omega) = (\zeta) \quad ou \quad Q(\Omega) \in (\zeta)$; ce qui est impossible vu que $deg(P) < deg(\zeta)$ et $deg(Q) < deg(\zeta)$. Donc ζ est **irréductible**.

  On sait que ζ irréductible $\Rightarrow$ (ζ) est maximal dans la classe des idéaux propres et principaux de $k[X]$.
  $k[X]$ étant principal, tout ses idéaux sont principaux. Et par suite (ζ) est un idéal maximal de $k[X]$; d'où $k[X]/(\zeta)$ est un corps .

  ✪ Le premier théorème d'isomorphisme assure que $k[X]/(\zeta) \cong Im(\Omega) = k[\alpha]$.
  D'où $k[\alpha]$ est un corps. Puisque $k[\alpha]$ est un corps contenant k et α il contient forcement $k(\alpha)$. Ce qui achève la démonstration.
  Le polynôme ζ ci-dessus est appelé polynôme minimal de α .

Définition 1.3.2. *Soit α un élément algébrique d'une extension K d'un corps k . On appelle polynôme minimal de α le polynôme normalisé(i.e de coefficient dominant 1) et de degré minimal non nul ζ de $k[X]$ tel que $\zeta(\alpha) = 0$.*

Proposition 1.5. *Toute extension finie $(\mathbb{K} : k)$ est algébrique.*

Démonstration. Puisque $\mathbb{K}$ est finie, $\forall \alpha \in \mathbb{K} \setminus \{0\}$, il existe $n \in \mathbb{N}^*$ tel que $1, \alpha, \alpha^2, \alpha^3 \cdots \alpha^n$ soient liés sur k. De ce fait, il existe $a_1, a_2, \cdots, a_n \in k$ tel que $\sum_{0 \leq i \leq n} a_i \alpha^i = 0$. Ce qui montre que α est racine

du polynôme non nul $\sum_{0\leq i\leq n} x_i\alpha^i = 0$ ❑

1.3.1 Corps de rupture, corps de décomposition, Extension normale, Extension séparable

Définition 1.3.3. .

a) ***Extension simple***

Une extension $\mathbb{K}$ d'un corps k est dit simple si il existe $c \in \mathbb{K}$ tel que $\mathbb{K} = k(c)$.

b) ***Corps de rupture***

*Soit k un corps , $f \in k[X]$. f irréductible sur k . On appelle **corps de rupture** de f toute extension simple $k' = k(\theta)$ de k dans laquelle f admet θ comme racine de f.*

Exemple 1.3.2. $f(x) = x^2 - 5 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$. L'extension simple $\mathbb{Q}(\sqrt{5})$ est un corps de rupture de f.

c) ***Corps de décomposition*** *Soit k un corps et $f \in [X]$, $deg(f) > 0$. On appelle corps de décomposition de f ou corps des racines de f sur k, toute extension K de k telle que :*

i) *f se décompose entièrement en facteurs linéaires* $f(x) = \mu\prod_{i=1}^{n}(x - \alpha_i)$ $\alpha_i \in \mathbb{K},\ \mu \in k.$

ii) *$\mathbb{K}$ minimal (pour l'inclusion) parmi les extension de k dans lesquelles f vérifie **i**. En d'autre termes $\mathbb{K} = k(\alpha_1, \alpha_2, \cdots \alpha_n)$*

d) ***Extension normale***

Une extension $(\mathbb{K} : k)$ est dite normale si :

i) *$\mathbb{K}$ est algébrique .*

ii) *Tout polynôme irréductible sur k ayant une racine dans $\mathbb{K}$ admet une décomposition en facteurs linéaires dans $\mathbb{K}$.*

e) ***Extension séparable*** *Soit F un corps et $f \in F[X]$, irréductible. f est dit séparable si toutes ses racines sont **simples**.*

*Un polynôme non contant $f \in F[X]$ est dit **séparable** si tous ses facteurs irréductibles sont séparables.*

Soit $(\mathbb{K} : k)$ une extension . Un élément β de $\mathbb{K}$ est dit séparable son polynôme minimal est séparable.

Lorsque tout les éléments d'une extension $(\mathbb{K} : k)$ sont séparables, l'extension est dite séparable.

1.3.2 Irréductibilité des polynômes

On rappel que si A est un corps, $A[X]$ est un anneau euclidien et factoriel.

Définition 1.3.4. ***(Polynôme irréductible)*** *Soit $P \in A[X]$, A un anneau commutatif unitaire. On dit que P est irréductible lorsque les deux conditions suivantes sont vérifiées :*

i) *P n'est pas inversible*

ii) *P ne possède aucun diviseurs propre.*

Remarque 1.3.1. La condition **(ii)** signifie que les seuls diviseurs de P sont les éléments inversibles et les éléments associés $A[X]$.

Quelques critères usuels d'irréductibilité des polynômes

C_1 *Un polynôme de degré 2 ou 3 sur un corps est irréductible s'il n'admet pas de racines*

C_2 *Soit k un corps ; $P \in k[X]$ est irréductibles si et seulement siil n'admet pas racine dans toute extension de degré inférieur à $(deg)/2$ extension .*

Exemple 1.3.3. $X^5 + X^2 - 1$ est irréductible sur $\mathbb{F}_2$; donc irréductible sur $\mathbb{F}_{2^2}$ qui est une extension de degré 2 de $\mathbb{F}_2$

Vérification :

✪ $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ α élément primitif de $\mathbb{F}_4$ dont le polynôme minimale est $x^2 + x + 1$.

De l'égalité $\alpha^2 + \alpha + 1 = 0$ nous permet de remarquer que

- $\alpha^2 + \alpha + 1 + \alpha + 1 = \alpha + 1 \Longleftrightarrow \alpha^2 + 2\alpha + 2 = \alpha + 1 \Longleftrightarrow \alpha^2 = \alpha + 1$
- On a :
$$\begin{aligned} \alpha^2 + \alpha + 1 = 0 &\Rightarrow \alpha^2 + \alpha + 1 + 1 = 1 \\ &\Rightarrow \alpha^2 + \alpha + 2 = 1 \\ &\Rightarrow \alpha^2 + \alpha = 1 \end{aligned}$$
- $\alpha^3 = 1,\ \alpha^4 = \alpha,\ \alpha^5 = \alpha^2$

✪ On vérifie sans peine avec ce qui précède que :

$\forall x \in \{0, 1, \alpha, \alpha^2\} = \mathbb{F}_4, \quad P(x) \neq 0$

C_3 ***Critère d'Eisenstein***

Soit $q \in \mathbb{Z}[X]$, $\quad q(X) = a_n X^n + a_{n-1} X^n + \cdots + a_1 X + a_0$

Soit p un entier premier.

Si :

– $p^2 \nmid a_0$ *et* $p \nmid a_n$

– $p/a_i \ \forall i = 0, 1, \cdots, n-1$

Alors p est irréductible sur $\mathbb{Q}$

C_4 *$x^2 + X + 1$ est l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$. Donc tout polynôme n'admettant pas de racines dans $\mathbb{F}_2$ et distincts de $(X^2 + X + 1)^2 = 1 + X^2 + X^4$ est irréductible.*

C_5 *Les polynômes irréductibles unitaires de degré 2 sont $X^2 + 1, \quad X^2 - X + 1, \quad X^2 + X - 1$ Donc tout polynôme de degré 4 sans racines dans $\mathbb{F}_3$ et non divisible par un de ces polynômes est irréductible.*

C_6 *Soit k un corps et $\mathbb{K}$ une extension de degré m premier avec le degré le degré un polynôme P. Si P est irréductible sur k alors il l'est également sur $\mathbb{K}$*

1.4 Construction des corps finis

$\mathbb{F}_q$ est un corps fini de caractéristique p .

On sait que $\mathbb{F}_q$ est une extension de $\mathbb{F}_p$

Proposition 1.1. *Tout élément non nul α de $\mathbb{F}_q$ possède un polynôme minimal M_α tel que $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/M_\alpha(x)$*

Par abus de notation, on écrira tout simplement, $\mathbb{F}_p[\alpha] = \mathbb{F}_p[x] mod(M_\alpha(x))$

Démonstration. Soit $\alpha \in \mathbb{F}_q$:

✪ $\mathbb{F}_p[\alpha] = \{P(\alpha), \quad P \in \mathbb{F}_p[x]\}$

Le corps $\mathbb{F}_q$ est fini et pourtant il existe une infinité d'expression polynômiale de la forme $P(\alpha) = \sum_{i=1}^{n} a_i \alpha^i \quad n \in \mathbb{N}^*$ à l'intérieur de $\mathbb{F}_p[\alpha]$

Puisque $\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_q$, on déduite que $\mathbb{F}_p[\alpha]$ est fini. Ainsi il existe au moins un polynôme $P_0 \in \mathbb{F}_p[x]$ tel que $P_0(\alpha) = 0$

En effet $\mathbb{F}_p[\alpha]$ étant fini, il existe forcement deux polynômes $P(x)$ *et* $Q(x)$ dans $\mathbb{F}_p[x]$ tel que $P(x) \neq Q(x)$ et $P(\alpha) = Q(\alpha)$. En posant $P_0(x) = P(x) - Q(x)$. On obtient que $P_0(\alpha) = 0$. Notons par $M_\alpha(x)$ le polynôme minimale de α

✪ D'après la proposition **1.4** ci-dessus , on peut dire que α est un élément algébrique de $\mathbb{F}_q$. Donc $\mathbb{F}_p[\alpha]$ est un corps. De la preuve **1.3.1** on déduite que $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/(M_\alpha(x))$.

□

Remarque 1.4.1. Si d est le degré du polynôme minimal de α alors $\mathbb{F}_p[\alpha]$ est un corps fini de cardinal p^d .

Démonstration. On sait que $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/(M_\alpha(x))$. Soit $P \in \mathbb{F}_p[x]$.
Par division euclidienne, il existe Q et $R \in \mathbb{F}_p[x]$ tel que $P = M_\alpha.Q + R$ avec $deg(R) < deg(M_\alpha)$
Ainsi $deg(R) < d$. Posons $R(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r$ où $r = deg(R)$ *et* $a_i \in \mathbb{F}_p$.
$P(\alpha) = M_\alpha(\alpha)Q(\alpha) + R(\alpha) = R(\alpha)$ car $M_\alpha(\alpha) = 0$.
D'où $P(\alpha) = R(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r \quad a_i \in \mathbb{F}_p$.
$\mathbb{F}_p[\alpha]$ est un $\mathbb{F}_p - espace$ vectoriel dont une base est $\{1, \alpha_1, \alpha_2 \cdots, \alpha_d\}$. Donc cardinal de $\mathbb{F}_p$ est p^d. □

Construction pratique des corps finis

Soit $\mathbb{F}_q$ un corps fini de caractéristique p et γ un élément primitif de $\mathbb{F}_q$.

Proposition 1.6. *Si $d = deg(M_\gamma(x))$, alors $q = p^d$ et on a $\mathbb{F}_q = \{0, 1, \gamma, \gamma^2, \cdots \gamma^{q-2}\} = \mathbb{F}_p[\gamma]$*

Démonstration.
- Par définition de $\mathbb{F}_p[\gamma]$, $\mathbb{F}_p[\gamma] \subseteq \mathbb{F}_q$.
- Puisque $|\gamma| = q - 1$, on a $\mathbb{F}_q = \{0, 1, \gamma, \gamma^2, \cdots \gamma^{q-2}\}$. Les éléments de $\mathbb{F}_q$ étant les puissances de γ il suit que $\mathbb{F}_q \subseteq \mathbb{F}_p[\gamma]$. D'où $\mathbb{F}_p[\gamma] = \mathbb{F}_q$.
  Le cardinal de $\mathbb{F}_p[\gamma]$ étant égale à p^d, on déduit que $q = p^d$ ❑

A présent, considérons un corps fini $\mathbb{F}_q$. Où $q = p^m$
Soit γ un élément primitif de $\mathbb{F}_q$. D'après ce qui précède, on a forcement $m = deg(M_\gamma(x))$. Or γ étant un polynôme primitif, $\gamma^{q-1} = 1$. Ainsi on peut trouver le polynôme minimal de γ parmi les facteurs de $x^{q-1} - 1 = 0$.
En posant $\gamma = x \ mod(M_\gamma(x))$, on obtient $\mathbb{F}_q = \mathbb{F}_p[\gamma] = \mathbb{F}_p[x]mod(M_\gamma(x)) = \{0, 1, \gamma, \cdots, \gamma^{q-2}\}$.
Chaque élément de $\mathbb{F}_q$ correspond à un polynôme en γ de degré inférieur à m modulo $M_\gamma(x)$.
□

Remarque 1.4.2. $\mathbb{F}_q$ est en fait complètement caractérisé par la table de correspondance donnant les $\gamma^i = P_i(\gamma)$ où $P_i(x) = \sum_n a_n x^n$ est de degré inférieur à m. Pour écrire cette table, il suffit de calculer successivement les γ^i pour $i = 0, 1, \cdots, q-2$ en multipliant par γ et en réduisant modulo $M_\gamma(x)$ à chaque fois .

Quelques exemples de construction de corps fini

a) *Cas des corps fini $\mathbb{F}_{2^m}$ où $1 \leq m \leq 16$.*

Le tableau suivant donne la liste de quelques polynômes primitifs sur $\mathbb{F}_2$ de degré $1 \leq m \leq 16$ permettant de construire les corps finis $\mathbb{F}_{2^m}$

x^2+x+1	x^3+x+1	x^4+x+1	x^5+x^2+1
x^6+x+1	x^7+x^2+1	$x^8+x^4+x^3+x^2+1$	x^9+x^4+1
$x^{10}+x^3+1$	$x^{11}+x^2+1$	$x^{12}+x^6+x^4+x+1$	$x^{13}+x^4+x^3+x+1$
$x^{14}+x^{10}+x^6+x+1$	$x^{15}+x+1$	$x^{16}+x^{12}+x^3+x+1$	

1.5 Les polynômes linéaires

La théorie des polynômes linéaires date de 1932 *et est due à Oystein Ore ([17] et [18]). Celui -ci donne plusieurs algorithmes de calculs sur les polynômes linéaires. Les polynôme linéaires sont utilisés dans la conception des codes MDR[4] en métrique rang.*
Dans ce paragraphe, on considère $\mathbb{F}_{q^n}$ comme un $\mathbb{F}_q - espace\ vectoriel$ de dimension n.

Définition 1.5.1. *Un polynôme linéaire(ou $q-polynôme$) sur $\mathbb{F}_{q^n}$ est un polynôme de la forme $P(X) = a_k X^{q^k} + a_{k-1}X^{q^{k-1}} + \cdots a_l X^{q^l} + \cdots a_1 X^q + a_0 X$ où $a_0,\ a_1,\ \cdots a_k$ sont des éléments de $\mathbb{F}_{q^n}$.*

Si $a_k \neq 0$, l'entier k est appelé le $q-$degré de P ou simplement le degré de P .
Pour la suite, nous adopterons la notation $[l] = q^l$, l'entier l étant pris modulo n.

1.5.1 Propriété des polynômes linéaires

Proposition 1.2. .

Muni des lois $+$ et $\circ$(composition des applications) l'ensemble des q-polynômes est un sous-anneau non commutatif de $\mathcal{L}(\mathbb{F}_{q^n})$ ensemble des applications $\mathbb{F}_q$-linéaires de $\mathbb{F}_{q^n}$ de lui-même.

Démonstration. Notons par $\mathcal{P}(q)$ l'ensemble des polynômes q-linéaire sur $\mathbb{F}_{q^n}$.

✪ Montrons que X^q est linéaire.

$\mathbb{F}_{q^n}$ étant de caractéristique q, $\forall \alpha \in \mathbb{F}_q, \quad , a, b \in \mathbb{F}_{q^n}$ on a $(\alpha a + b)^q = \alpha^q a^q + b^q$

$\alpha \in \mathbb{F}_q \Rightarrow \alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha$

D'où $(\alpha a+b)^q = \alpha a^q + b^q$.

Ainsi X^q est $\mathbb{F}_q-$linéaire

✪ Montrons par récurrence sur $k \in \mathbb{N}^*$ que X^{q^k} est $\mathbb{F}_q$ -linéaire

- pour $k=0$ on obtient X qui est $\mathbb{F}_q$-linéaire
- Pour $k=1$ on a X^q qui est $\mathbb{F}_q-$linéaire d'après ce qui précède.
- Soit $k \in \mathbb{N}^*$; supposons X^{q^k} linéaire .

Soient $a,\ b\ \in \mathbb{F}_{q^n},\ \alpha \in \mathbb{F}_q$

$$\begin{aligned}
(\alpha a+b)^{q^{k+1}} &= ((\alpha a+b)^{q^k})^q \\
&= (\alpha^{q^k} \times a^{q^k} + b^{q^k})^q \qquad \textit{par hypothèse de récurrence} \\
&= \alpha^{q^{k+1}} \times a^{q^{k+1}} + b^{q^{k+1}} \\
&= \alpha^{q^k-1} \times \alpha \times a^{q^{k+1}} + b^{q^{k+1}} \\
&= \alpha^{(q-1)(1+q+q^2+\cdots+q^{k-1})} \times \alpha \times a^{q^{k+1}} + b^{q^{k+1}} \\
&= 1 \times \alpha \times a^{q^{k+1}} + b^{q^{k+1}} \\
(\alpha a+b)^{q^{k+1}} &= \alpha a^{q^{k+1}} + b^{q^{k+1}}
\end{aligned}$$

D'où $X^{q^{k+1}}$ est linéaire.

Conclusion : $\forall k \in \mathbb{N} * X^{q^k}$ est linéaire.

Le polynôme $P(X) = a_k X^{q^k} + a_{k-1}X^{q^{k-1}} + \cdots + a_1 X^q + a_0 X$ est donc linéaire

$\mathcal{P}(q)$ est une partie de non vide de $\mathcal{L}(\mathbb{F}_{q^n})$.

✪ Montrons que $\mathcal{P}(q)$ est un sous anneau de $\mathcal{L}(\mathbb{F}_{q^n})$

1. Soient A , B deux éléments de $\mathcal{P}(q)$. $A = \sum_{i=0}^{k} a_i X^{[i]} \qquad B = \sum_{j=0}^{k'} b_j X^{[j]}$

   Sans nuire à la généralité, supposons que $k \leq k'$

   $B - A = \sum_{i=0}^{k} (b_i - a_i) X^{[i]} + \sum_{i=k+1}^{k'} b_i X^{[i]}$. Posons $c_i = \begin{cases} b_i - a_i & si \quad 0 \leq i \leq k \\ b_i & si \quad k+1 \leq i \leq k' \end{cases}$

   On obtient $B - A = \sum_{i=0}^{k'} c_i X^{[i]}$ qui est un $q-$polynôme.

   D'où $B - A \in \mathcal{P}(q)$

2. Montrons que $A \circ B \in \mathcal{P}(q)$

$$\begin{aligned} A \circ B &= \sum_{i=0}^{k} a_i (\sum_{j=0}^{k'} b_j X^{[j]})^{[i]} \\ &= \sum_{i=0}^{k} a_i (\sum_{j=0}^{k'} b_j^{[i]} X^{[j+i]}) \\ &= \sum_{i=0}^{k} \sum_{r=i}^{k'+i} a_i b_{r-i}^{[i]} X^{[r]} \end{aligned}$$

En faisant varier r de 0 à $k+k'$, et en regroupant les facteurs de $X^{[0]},\ X^{[1]},\ X^{[2]},\ \cdots X^{[k+k']}$.

- Pour $r = 0$ on a $(a_0 b_0^{[0]})X^{[0]}$ car $i = 0$
- $r = 1$ on a $(a_0 b_1^{[0]} + a_1 b_0^{[1]})X^{[1]}$ car $i \in \{0, 1\}$
- $r = 2$ on a $(a_0 b_2^{[0]} + a_1 b_1^{[1]} + a_2 b_0^{[2]})X^{[2]}$
- $r = 3$ on a $(a_0 b_3^{[0]} + a_1 b_2^{[1]} + a_2 b_1^{[2]} + a_3 b_0^{[3]})X^{[3]}$

  $\vdots$

  $\vdots$

- $r = k$ on a $(a_0 b_k^{[0]} + a_1 b_{k-1}^{[1]} + \cdots\cdots + a_k b_0^{[k]})X^{[k]}$

  Posons $a_j = 0$ si $j > k$ et $b_{r-j} = 0$ si $r - j > k'$, On obtient

  $A \circ B = \sum_{r=0}^{k+k'} (\sum_{j=0}^{r} a_j b_{r-j}^{[j]}) X^{[r]}$

Ainsi $A \circ B = \sum_{r=0}^{k+k'} c_r X^{[r]}$ où $c_r = \sum_{j=0}^{r} a_j b_{r-j}^{[j]}$ $\star$

Ce qui nous permet de déduire que $\mathcal{P}(q)$ est un sous-anneau de $(\mathcal{L}(\mathbb{F}_{q^n}), +, \circ)$

□

Avec $\star$, on obtient que $B \circ A = \sum_{r=0}^{k+k'} c'_r X^{[r]}$ *où* $c'_r = \sum_{j=0}^{r} b_j a_{r-j}^{[j]}$

D'où $A \circ B \neq B \circ A$

Ce qui prouve que $(\mathcal{P}(q), +, \circ)$ n'est pas commutatif pour la loi $\circ$

Exemple 1.5.1 (**L'application trace** de $\mathbb{F}_{q^n}$)**.** .

$$\begin{aligned} T_n : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\ x &\longmapsto \sum_{i=0}^{n-1} x^{q^i} \end{aligned}$$

T_n est un polynôme linéaire sur F_{q^n} de $q-$degré $n-1$

Proposition 1.3 (**Noyau des polynômes linéaires**)**.** .

Si *P est un polynôme linéaire de q-degré $k \neq 0$, alors dim $ker(P) \leq k$*

Si *E est un sous-espace vectoriel de $\mathbb{F}_{q^n}$ de dimension k non nul, il existe un q-polynôme de degré k s'annulant sur E.*

Démonstration. .

- Soit P un q-polynôme de degré k ; $P(X) = a_k X^{[k]} + a_{k-1}X^{[k-1]} + \cdots + a_1 X^{[1]} + a_0 X$
  où $[i] = q^{i \ mod(n)}$.
  Le degré de P sur $\mathbb{F}_q[X]$ est q^k. Ainsi P possède au plus q^k racines distinctes sur $\mathbb{F}_{q^n}$.
  Or on sait que $ker(P)$ est un $\mathbb{F}_q$- sous-espace vectoriel de $\mathbb{F}_{q^n}$.
  Ainsi cardinal de $Ker(P) = q^{dim(Ker(P))}$
  D'où $q^{dim(Ker(P))} \leq q^k$, c'est-à-dire $\boxed{dim\ Ker(P) \leq k}$
- Soit E un $\mathbb{F}_q$ sous-espace vectoriel de dimension k ; $\mathcal{B} = \{e_1, \cdots, e_k\}$ une $\mathbb{F}_q - base$ de E.
  Posons :

  1) $P_1(X) = X^q - e_1^{q-1}X$. Alors P est un P_1 est un $q - polynôme$ de de degré 1 qui s'annule en e_1.
  2) $P_2(X) = (X^q - P_1(e_2)^{q-1}X) \circ P_1$ P_2 est un $q-$polynôme de degré 2 qui s'annule en e_2 et e_1.

  ⋮

  ⋮

  k) successivement, on arrive à $P_k(X) = (X^q - p_{k-1}(e_k)^{q-1}X) \circ P_{k-1}(X) \circ \cdots P_1(X)$ est un q-polynôme de degré k qui s'annulant sur $\{e_1, e_2, \cdots, e_k\}$ et par conséquent sur E entier.

□

1.6 théorie algébrique du codage

La théorie du codage voit le jour dans les années 1946 *grâce aux travaux de* ***HAMMING****[11]. Par suite,* ***Claude SHANNON****[3] formalise cette théorie comme une branche mathématique, permettant ainsi à ce concept de devenir un outil presque incontournable en informatique. En effet, la théorie des codes fournie une immense panoplie d'astuces, de techniques et d'algorithmes permettant de véhiculer une information via un canal bruité*[1] *de la manière la plus rapide possible.*

1. *canal de transmission sensible à des perturbations*

1.6.1 Alphabet et codes

De façon générale, pour écrire des textes on a besoin des symboles d'un alphabet.

Définition 1.6.1. ***Un alphabet*** *est tout simplement un ensemble fini de symboles.*

Exemple 1.6.1. $\Omega = \{\mathcal{A}, \mathcal{B}, \mathcal{C}, \cdots \mathcal{Z}\}$ est un alphabet de longueur 26.
$\Theta = \{0, 1\}$ est un alphabet de longueur 2.

Lorsqu'un alphabet possède m symboles, ils peuvent être identifié aux éléments de
$\mathbb{Z}_m = \{O, 1, 2, \cdots, m-1\}$

Définition 1.6.2. ***Un mot*** *sur un alphabet Ω est une suite de symbole de Ω. La longueur d'un mot est le nombre de symboles qui le constituent.*

On adoptera parfois la notation vectorielle pour désigner un mot sur un alphabet donné.

Définition 1.6.1. *Un* ***code*** *C sur un alphabet Ω est un ensemble de mots constitués de symboles pris dans Ω. Les éléments d'un code sont appelés les* ***mots codes*** *ou* ***bloc code****.*

Exemple 1.6.2. Le code **ASCII**[2] Dans le code **ASCII**, les mots formés sont de longueur 8 sur l'alphabet $\Theta = \{0, 1\}$.
$C = \{00010000, 00001000, 11001000, \cdots 10000101\}$

1.6.2 Déchiffrabilité d'un code

Pour communiquer un message, $c = c_1c_2\cdots c_n$ via un canal[3]*, on le traduit sous la forme $x_1x_2\cdots x_n = f(c_1)f(c_2)\cdots f(c_n)$. Une condition nécessaire pour que le message c soit reçu sans ambiguïté est la bijectivité de f . Cette condition n'est malheureusement pas suffisante comme le montre l'exemple ci-dessous :*
Considérons le codage sur les lettres de l'alphabet $\Omega = \{\mathcal{A}, \mathcal{B}, \mathcal{C}, \cdots \mathcal{Z}\}$ par les entiers $0, 1, 2\cdots, 25$.
On obtient $f(\mathcal{A}) = 0,\ f(\mathcal{B}) = 1,\ f(\mathcal{C}) = 2, \cdots f(\mathcal{J}),\ f(\mathcal{K}) = 10,\ f(\mathcal{Z}) = 25$
Le mot de code 1209 peut par exemple correspondre à plusieurs messages différents ; à savoir $\mathcal{BUJ}$ ou $\mathcal{MAJ}$ ou $\mathcal{BCAJ}$. Il est donc nécessaire d'ajouter des nouvelles contraintes sur le code pour qu'un message quelconque puisse être déchiffré sans ambiguïté.

Définition 1.6.3 (Code uniquement déchiffrable)**.** .
On note Ω^+ l'ensemble des mots sur Ω. Un code C sur Ω est dit ***uniquement déchiffrable*** *ou* ***non***

2. *American Standard Code for Information Interchange* 3. téléphone, internet,réseau sans fil

ambigu *si pour tout* $x = x_1x_2\cdots x_n \in \Omega^+$, *il existe au plus une sequence* $c = c_1c_2\cdots c_m \in C^+$ *tel que* $c = c_1c_2\cdots c_m = x_1x_2\cdots x_n$

Théorème 1.2. *Un code* C *sur* Ω *est uniquement déchiffrable si et seulement sipour tout* $c = c_1c_2\cdots c_n$ *et* $d = d_1d_2\cdots d_m$ *de* C^+ ,
$c = d \Longrightarrow\ (n = m \text{ et } c_i = d_i\ 1 \leq i \leq n)$

Dans toute la suite, sauf mention contraire, les codes utilisés sont uniquement déchiffrables. L'alphabet considéré sera un corps fini $\mathbb{F}_q$ *ou bien isomorphe à* $\mathbb{F}_q$.

1.6.3 La distance de Hamming [11]

Définition 1.6.4. Def 1 : ***La distance de Hamming*** *de deux vecteurs* $x,\ y\ \in \mathbb{F}_q^n$ *est le nombre de coordonnées dont* x *et* y *diffèrent. On la note* $d_H(x, y)$

Def 2 : *On appelle* ***distance d'un code*** C *notée* $d(C)$ *la plus petite distance entre deux mots -code de* C *distincts*

$$d(C) = min\{d_H(x, y),\ x, y \in C,\ x \neq y\}$$

Lorsque aucune confusion n'est à craindre, $d_H(C)$ *sera noté simplement* d.

Def 3 : *On appelle code de type* (n, M, d) *tout code* C *dont la distance minimale est* d, *qui possède* M *mots-code distincts et chacun de ces mots-code étant de longueur* n .

Théorème 1.3. *Soit* C *un* (n, M, d) *code sur* $\mathbb{F}_q$, $s, t \in \mathbb{N}, s \leq n$

i) *Le code* C *peut détecter jusqu'à* s *erreurs dans un mot code si* $d(C) \geq s + 1$

ii) C *peut corriger jusqu'à* t *erreurs sur un mot-code si et seulement si* $d(C) \geq 2t + 1$

Démonstration. .

Soit y un message reçu et x le message envoyé réellement.

Supposons que x et y diffèrent de r coordonnées. On a $d_H(x, y) = r$

i) Si $r \leq s$ alors $d_H(x, y) \leq s$. $y \notin C$ car sinon on aurait $s + 1 \leq d \leq d_H(x, y) \leq s \Rightarrow\ s + 1 \leq s$ ce qui est absurde. Le message erroné y est donc détecté

ii) Supposons à présent que $r \leq t$

Comme au i), on montre que $y \notin C$.

Supposons qu'il existe $x' \in C$, $x' \neq x$ tel que $d_H(x, y) = d_H(x', y) = r$

Alors l'inégalité triangulaire entraine que

$d_H(x,x') \leq d_H(x,y) + d_H(y,x') \leq 2t$

D'où $2t+1 \leq d \leq 2t$. Impossible ! puisque $2t+1 > 2t$.

Ainsi x est l'unique mot de C tel que $d_H(x,y) = r$. On peut donc décoder y à l'aide de x.

□

Corollaire 1.6.1. *Si C est un code sur $\mathbb{F}_q$ de distance d, alors C peut détecter au plus **d-1** erreurs et corriger au plus $\lfloor \frac{d-1}{2} \rfloor$ erreur détectées.*

Démonstration. .

- ✪ Soit x un message envoyé et y le message reçu. On suppose que y à au moins d erreurs. Alors $d_H(x,y) \geq d$; or pour tout x, $x' \in C$ $x \neq x'$, $d_H(x,x') \geq d$. Ainsi les erreurs sur y ne serons pas détectées.
- ✪ Par contre, si y contient au plus $d-1$ erreurs, le i) du théorème assure que les $d-1$ erreurs serons détectées *(il suffit de poser $s = d-1$)*
- ✪ D'après ii), $t \leq \frac{d-1}{2}$. La plus grande valeur de t est $\lfloor \frac{d-1}{2} \rfloor$. D'où le résultat.

□

Quelques problèmes en théorie du codage

La théorie du codage est sujette à plusieurs problèmes,notamment celui du déchiffrement d'un message reçu en générale et de la génération des codes optimaux en particulier. En effet, étant donné un code (n, M, d) , l'on aimerait que ce dernier satisfasse les propriétés suivantes :

i) *une petite valeur de n pour une transmission rapide.*

ii) *une grande valeur de d afin de pouvoir corriger le plus d'erreurs possibles.*

iii) *une grande valeur de M afin de pouvoir transmettre le plus de message possibles.*

Une question cruciale se pose ! Comment optimiser un (n, M, d) code afin qu'il puissent vérifier les 3 conditions sus citées ?

En d'autre termes, étant donné une longueur n de mots - code donnée et une distance minimale d, quel est le plus large code C qu'on peut fabriquer ?

A cet effet, beaucoup d'algorithmes d'optimisation sont proposés dans [11] et [27]

1.6.4 Les codes linéaires

On désire transmettre des éléments d'un corps fini $\mathbb{F}_q^k$ de longueur k à travers un canal numérique (internet , téléphone, satellite, réseau wifi etc...). La première opération est l'opération d'encodage, qui consiste à associer à chaque éléments de $\mathbb{F}_q^k$ un mot-code de longueur $n \geq k$ appartenant à $\mathbb{F}_q^n$. Pour cela, on se sert d'une application linéaire injective de $\mathbb{F}_q^k$ dans $\mathbb{F}_q^n$ dont l'image C est un sous espace vectoriel de $\mathbb{F}_q^n$ appelé ***code linéaire*** *de longueur n et de dimension k.*

Dans ce mémoire, nous ne nous intéresserons pas particulièrement à la fonction d'encodage mais plus tôt à son image qui est le code C sur $\mathbb{F}_q$. La documentation relative aux fonctions d'encodage se trouvent dans [15]

Définition 1.6.2 (**Codes linéaires**). .
On dit qu'un code C sur un corps fini $\mathbb{F}_q$ est un code linéaire de longueur n si C est un sous-espace vectoriel de $\mathbb{F}_q^n$.
Les caractéristiques d'un tel code sont notées (n, k, d) où $k = dim(C)$ et $d = d(C)$

Définition 1.6.3 (**Poids de Hamming**). .
Le poids de Hamming d'un vecteur x de $\mathbb{F}_q^n$ est le nombre de coordonnées non nulles de x. Il est noté $\omega(x)$

Proposition 1.4. *Soit C un code sur $\mathbb{F}_q$.*

$$d(C) = min\{\omega(x), x \neq 0, x \in C\}$$

Preuve 1.6.1. Il suffit de remarquer que C étant un sous-espace vectoriel, on a $\forall x,\ y \in C, \quad x - y \in C$

Remarque 1.6.1 (**Avantages que procurent les codes linéaires**). [25]

A_1 les propriétés algébriques **d'addition**, **de soustraction**, **multiplication interne** et de **division** sur $\mathbb{F}_q$ facilitent la manipulation des mots du code

A_2 Lorsque C à M mot du code, on a besoin que de C_M^2 comparaisons pour déterminer $d(C)$, ce qui est parfois un travail fastidieux. Avec les codes linéaires, la relation $d(C) = \omega(C)$ nous permet de déterminer $d(C)$ en examinant seulement le poids des $M - 1$ mots de C.

A_3 On à plus besoin de lister tous les mots-code afin de le spécifier . Lorsque C est un $(n, k) - code$ il suffit de déterminer une base de C formée de k mots-code.

Remarque 1.6.2. Ces types de codes présentent un léger inconvénient à cause du fait qu'on ne peut les définir que lorsque le cardinal du corps de base est une puissance de nombre premier.

Définition 1.6.4 (**Matrice génératrice**). *Soit C un $(n,k)-$code linéaire. On dit qu'une matrice G est une matrice génératrice de C lorsque les lignes de G forment une base de C*

Remarque 1.6.3. G est de taille k×n

1.6.5 Équivalence des code linéaires

C est un $(n,k,d)-$code linéaire de matrice génératrice G à coefficient dans $\mathbb{F}_q$, C' un autre code linéaire de matrice G' également à coefficients dans $\mathbb{F}_q$

Proposition 1.5. *Les Codes C et C' sont dit équivalents si la matrice G' de C peut être obtenue de G à l'aide d'au moins une des transformations suivantes :*

C_1 *Permutation des colonnes de G*

C_2 *Multiplication d'une ou plusieurs colonnes de G par des scalaires non nuls*

R_1 *Permutation des lignes de G*

R_2 *Multiplication d'une ou plusieurs lignes de G par des scalaires non nuls*

R_3 *Addition à une ligne de G, d'une autre ligne ayant été multipliée par un scalaire*

Remarque 1.6.4. .

i) Si la transformation fait intervenir uniquement $R_1,\ R_2,\ ou\ R_3$ alors $C = C'$ puisque les lignes de G' sont des combinaisons linéaires de celles de G.

ii) Si la transformation a fait intervenir C_1 ou C_2 alors C' n'est pas forcement identique à C

iii) C_1 et C_2 peuvent être jumelées en une transformation appelée **transformation monomiale**. Il s'agit en fait d'un isomorphisme

$$\begin{array}{rccc} \mathcal{T}\ : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & u = (u_1, u_2, \dots u_n) & \longmapsto & (\lambda_1 u_{\sigma(1)}, \lambda_2 u_{\sigma(2)}, \dots, \lambda_n u_{\sigma(n)}) \end{array}$$

où σ est une permutation de $\{1, 2, \dots, n\}$ et les $\lambda_i\ 1 \leq i \leq n$ étant des éléments de $\mathbb{F}_q \setminus 0$

Démonstration. iii).

✪ Soit $\alpha \in \mathbb{F}_q,\ a,\ b \in \mathbb{F}_q^n\ ;\ a = (a_1, \cdots, a_n)\ et\ b = (b_1,\ b_2,\ \dots,\ b_n)$

$\mathcal{T}(\alpha a + b) = \mathcal{T}(c_1, c_2, \dots c_n)$ où $c_i = \alpha a_i + b_i$

$\mathcal{T}(c_1, \cdots, c_n) = (\lambda_1 c_{\sigma(1)}, \cdots, \lambda_n c_{\sigma(n)})$

Puisque σ ne permute que les positions des c_i, on déduit que

$\mathcal{T}(\alpha a+b)=\mathcal{T}(\ \lambda_1(\alpha a_{\sigma(1)}+b_{\sigma(1)}),\cdots,\lambda_n(\alpha a_{\sigma(n)}+b_{\sigma(n)})\ )$

D'où $\mathcal{T}(\alpha a+b)=\alpha\mathcal{T}(a)+\mathcal{T}(b)$. Donc $\mathcal{T}$ est une application linéaire.

✪ Soit $x\in Ker(\mathcal{T})$

Soit $x\in Ker(\mathcal{T})$, $x=(x_1,\ldots,x_n)$

$$\begin{aligned}\mathcal{T}(x)=0 &\iff \lambda_i x_{\sigma(i)}=0 \qquad 1\le i\le n\\ &\iff x_{\sigma(i)}=0 \qquad (1\le i\le n) \quad \text{car les } \lambda_i \text{ sont tous non nuls}\\ &\iff x_i=0 \qquad 1\le i\le n\\ &\iff x=(0,0,\cdots,0)\end{aligned}$$

D'où $\mathcal{T}$ est un automorphisme de $\mathbb{F}_q^n$ □

Proposition 1.6. *Si C est un $(n,k,d)-$code linéaire sur $\mathbb{F}_q$ et C' un code équivalent à C, alors C' est un (n,k,d)-code linéaire sur $\mathbb{F}_q$*

Démonstration. Sans nuire à la généralité supposons que C' est obtenu en deux étapes :

1^{ire} **étape :** On obtient de C le code C_1 par au moins une des transformations $R_1,\ R_2,\ R_3$.

2^{ire} **étape :** C_2 obtenu de C_1 par une transformation monomiale $\mathcal{T}$

on obtient $C\iff C_1\iff C_2=C'$.

D'après la remarque ci-dessus, $C=C_1$

Il suffit donc de montrer que C_2 est de type (n,k,d).

Soit $\mathcal{B}=\{b_1,\ldots,b_k\}$ une base de C_1. $\mathcal{T}$ étant un isomorphisme, il suit que $\{\mathcal{T}(b_1),\cdots,\mathcal{T}(b_k)\}$ est une base de C_2. D'où $dim(C_2)=k$.

montrons que $d(C_2)=d$

- $\forall x,\ y\ \in C_2,\ x\neq y\ \mathcal{T}^{-1}(x)$ et $\mathcal{T}^{-1}(y)$ sont dans C. Puisque l'application $\mathcal{T}$ conserve les valeurs des différents indices, on a

$d_H(x,y)=d_H(\ \mathcal{T}(\mathcal{T}^{-1}(x)),\mathcal{T}(\mathcal{T}^{-1}(y)\ )=d_H(\ \mathcal{T}^{-1}(x),\mathcal{T}^{-1}(y)\ )\ \ge d(C)$ D'où $d(C_2)\ge d(C)$

- $\forall c_1$ et $c_2\ \in C$, on a $c_1=\mathcal{T}^{-1}(\mathcal{T}(c_1))$, $c_1=\mathcal{T}^{-1}(\mathcal{T}(c_2))$

$d_H(c_1,c_2)=d_H(\ \mathcal{T}^{-1}(\mathcal{T}(c_1),\mathcal{T}^{-1}(\mathcal{T}(c_2))\ )\ge d(C_2)$

$$d(C)=d(C_2)$$

Conclusion : C' est un code linéaire de type (n,k,d). □

Remarque 1.6.5. L'ordre des transformations successives pour parvenir à C' importe peu car à chaque étapes, le code obtenu est toujours équivalent à C.

Définition 1.6.5 (**Matrice systématique d'un code**). .

Soit G la matrice génératrice d'un code (n, k, d). On dit que G est sous forme systématique ou standard s'il existe une matrice A de taille $k \times (n-k)$ tel que $G = [I_k|A]$ (où $\mathrm{I_k}$ matrice identité de taille $k \times k$)

Théorème 1.4. *Tout (n, k, d) code linéaire C sur $\mathbb{F}_q$ est équivalent à un code (n, k, d) dont la matrice est sous forme systématique.*

Démonstration. Soit G la matrice génératrice de C.

- Grâce à une transformation monomiale sur G, on obtient une matrice de la forme $[X|Y]$ où X est inversible de taille $k \times k$.

  Une telle transformation est toujours possible puisque $Rg(G) = k$.
- Par échélonage à l'aide des transformations $R_1,\ R_2,\ R_3$ on transforme X en $I_{k\times k}$ et simultanément la matrice Y en une matrice A, tel que $[X|Y] \Longleftrightarrow [I_k|A]$

□

1.6.6 Code dual et matrice de contrôle

Pour commencer, définissons d'abord le produit scalaire suivant :

$$\begin{array}{rcl} \mathbb{F}_q^n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q \\ (u, v) & \longmapsto & u_1v_1 + \cdots + u_nv_n \end{array} \qquad \text{avec } u = (u_1, \ldots, u_n) \quad , \quad v = (v_1, \ldots, v_n)$$

*Soit C un $(n, k) - code$ linéaire. L'ensemble $C^\perp = \{x \in \mathbb{F}_q^n / u.x = 0\}$ est appelé **code dual** de C. $C^\perp$ est un $(n, n-k) - code$ linéaire sur $\mathbb{F}_q$.*

Démonstration. .

➠ $C^\perp$ est un sous-espace vectoriel de $\mathbb{F}_q^n$.

En fait, pour tout $\alpha\_in\mathbb{F}_q$ $x,\ y\ \in C^\perp$ et $u \in C$, on a

$u.(\alpha x + y) = \alpha u.x + u.y = 0$ par définition de $C^\perp$.

D'où $\alpha x + y\ \in C^\perp$. Ce qui signifie que $C^\perp$ est un sous-espace vectoriel de $\mathbb{F}_q$. C'est-à-dire un code linéaire sur $\mathbb{F}_q$

➠ Montrons que $dim(C^\perp) = n - k$

Si $dim(C) = 1$, alors $C = \mathbb{F}_q.a \qquad a \in \mathbb{F}_q^n \setminus \{0\}$

Supposons $a = (a_1, a_2, \ldots, a_n)$. Soit $x \in C^\perp$.

$$a.x = 0 \iff a_1x_1 + \cdots + a_nx_n = 0$$
$$\iff x_1 = \alpha_1x_2 + \cdots + \alpha_nx_n \qquad où\ \alpha_i = -a_ia_1^{-1}, \quad 2 \le i \le n$$

On obtient $x = \begin{pmatrix} \alpha_1x_2 + \cdots + \alpha_nx_n \\ x_2 \\ x_3 \\ x_4 \\ \vdots \\ x_n \end{pmatrix} = x_2 \underbrace{\begin{pmatrix} \alpha_2 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{e_1} + x_3 \underbrace{\begin{pmatrix} \alpha_2 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{e_2} + \cdots + x_n \underbrace{\begin{pmatrix} \alpha_n \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}}_{e_{n-1}}$

On déduite dans ce cas que $\mathcal{B} = \{e_1,\ e_2,\ \cdots,\ e_{n-1}\}$ est une base de $C^\perp$.

Si $2 \le k \le n$, supposons que la matrice génératrice G de C est standard.

$$G = [I_k|A_{n-k}]$$
$$= \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & a_{11} & a_{12} & \cdots & a_{1(n-k)} \\ 0 & 1 & 0 & \cdots & 0 & a_{21} & \cdots & \cdots & \cdots \\ 0 & 0 & 1 & \cdots & 0 & \vdots & \cdots & \cdots & \cdots \\ \vdots & \cdots\cdots & \cdots & 0 & 0 & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 1 & a_{k1} & \cdots & \cdots & a_{k(n-k)} \end{array}\right]$$

Ainsi, $x \in C^\perp$ si et seulement si $[I_k|A].x^\top = 0 \iff \begin{cases} x_1 + \sum_{j=1}^{n-k} a_{1j}x_{k+j} = 0 \\ x_2 + \sum_{j=1}^{n-k} a_{2j}x_{k+j} = 0 \\ \vdots \\ x_k + \sum_{j=1}^{n-k} a_{kj}x_{k+j} = 0 \end{cases}$

On obtient un système de k équations homogènes indépendantes à n inconnues. Ce qui nous permet de déduire que l'ensemble des solutions est un sous-espaces de dimension $n-k$. Donc $dim(C^\perp) = n-k$ □

Définition 1.6.5. *On appelle matrice de contrôle d'un code (n, k) C, la matrice H de $C^\perp$*

Remarque 1.6.6. .

- R_1 G est de type $k \times n$ et H de type $(n-k) \times n$
- R_2 $G.H^\top = 0$
- R_3 $u \in C^\perp \iff G.u^\perp = 0$
- R_4 $v \in C \iff H.v^\perp$

$\boxed{R_5}$ $C = (C^{\perp})^{\perp}$ (**en fait** $\mathbf{C} \subset (\mathbf{C}^{\perp})^{\perp}$ **et** $\mathbf{dim}(\mathbf{C}^{\perp})^{\perp} = \mathbf{n} - \mathbf{dim}(\mathbf{C}^{\perp}) = \mathbf{n} - (\mathbf{n} - \mathbf{k}) = \mathbf{k} = \mathbf{dim}(\mathbf{C})$)

Théorème 1.5 ([25]). *Si* $G = [I_k|A]$ *alors* $H = [-A^{\top}|I_{n-k}]$

Démonstration. $H = [-A^{\top}|I_{n-k}] \Rightarrow Rg(H) = n - k$. De plus $[I_k|A] \times [-A^{\top}|I_{n-k}]^{\top} = 0$; ainsi les linges de H engendrent un sous espace vectoriel de dimension $n - k$ qui est entièrement contenu dans $C^{\perp}$ d'après la remarque $\boxed{R_3}$. D'où H est une matrice de contrôle de C □

Définition 1.6.6 ([25]). *La matrice de contrôle* H *est dite sous forme standard d si* $H = [B|I_{n-k}]$ *où* B *est de type* $(n - k) \times k$

1.7 Décodage des codes linéaires

Il existe plusieurs méthodes de décodage des codes linéaires. Les plus connues sont ***le décodage au maximum de vraisemblance, le décodage borné, décodage en liste, le décodage par tableau standard****.*

Dans cette section, C *est un* $(n, k, d) -$ *code linéaire sur* $\mathbb{F}_q$, $y \in \mathbb{F}_q^n$, $x \in C$ *et* t *est un entier naturel non nul .*

✪ Décodage au maximum de vraisemblance

Cette méthode consiste à rechercher à partir d'un mot y *pouvant contenir des erreurs, le mot* x *de* C *qui se rapproche le plus de* y *au sens de Hamming.*

Cela revient à rechercher x *tel que* $d_H(x, y) = d_H(y, C)$*. Il s'agit en fait de trouver le mot qui a été le plus probablement envoyé par l'expéditeur via un canal symétrique*[4]

✪ Décodage borné

Ici il s'agit de trouver s'il existe, un mot x *de* C *vérifiant* $d_H(x, y) \leq t$. t *fixé*

✪ Décodage en liste

Ce type de décodage consiste en la recherche d'un ensemble de mots $x \in C$ *tel que* $d_H(x, y) \leq t$ *où* t *est fixé.*

4. Un canal est dit q-symétrique si chacun des q symboles de son alphabet a la même probabilité $p(p < \frac{1}{2})$ de subir une erreur lors de sa transmission. Si un symbole est reçu, chacun des $q - 1$ erreurs possibles peuvent survenir manière identique (Une documentation plus approfondie se trouve dans [25])

Remarque 1.7.1. Le décodage borné est en général plus rapide et plus précis que le décodage au maximum de vraisemblance ou bien le décodage en liste. Cependant si $t \leq \lfloor \frac{d}{2} \rfloor$, alors le décodage en liste et le décodage borné sont équivalents, *(voir la preuve (ii) 1.6.3 du **théorème 1.3** de la page 19)* Par contre, si $t > \frac{d}{2}$ le décodage en liste est plus efficace vu que t excède la capacité de correction du code *(**théorème 1.3**)*

✪ Décodage par tableau standard

Définition 1.7.1. *Soit H une matrice de contrôle de C et $y \in \mathbb{F}_q^n$ un mot quelconque. On appelle **syndrome** de y le mot code $\boldsymbol{S(y)} = H.y^\top$*

***Principe** :*

Si on a $y = x + e$ avec $x \in C$ alors

$$\begin{aligned} H.y^\top &= H(x+e)^\top \\ &= H.x^\top + H.e^\top \\ &= 0 + He^\top \end{aligned}$$

Ainsi , lorsque x est solution du problème du décodage borné 1.7 (page 26) , c'est-à-dire si $y = x + e$ avec $\omega(e) = t \leq \lfloor (d-1)/2) \rfloor$ (ω poids de Hamming 1.6.3) alors on peut retrouver x à l'aide d'un mot de poids faible et de même syndrome que y.

a) Algorithme du décodage par tableau standard

Input : G, $y = (y_1, \cdots, y_n)$, t

. **Output** : $x \in C$, tel que, $d(x, y) \leq t$

Pré calcul :

Calcul de la matrice de parit H associe la matrice gnratrice G.

Pour chaque mot e $\in \mathbb{F}_q$ de poids infrieur ou *é*gale t, calculer $H.e^\top$ et l'ajouter la liste des syndromes L.

Décodage : Calculer $Hy^\top$ et rechercher dans la liste L, un mot e admettant le m*ê*me syndrome

si e existe, renvoyer $c = y - e$ sinon, renvoyer « pas solution »

Décodage par ensemble d'information

Définition 1.7.2 (Ensemble d'information)**.** *C est un (n, k, d) code linéaire sur $\mathbb{F}_q$ de matrice génératrice G. Une partie I de $[1, n]$ est appelée ensemble d'information pour le code C si I est*

de cardinal k et la restriction de G aux colonnes d'indices $i \in I$ forme une matrice inversible.

Proposition 1.7. *Si $I = [1, k]$ est un ensemble d'information d'un code C de type (n, k, d), alors il existe une unique matrice génératrice de C de la forme $[I_k|A]$ et une unique matrice de parité de la forme $[Q|I_{n-k}]$ où $Q = -R^\top$ (confère **proposition 1.5 sur les matrice équivalentes**)*

Proposition 1.8. *Si $I = \{i_1, \cdots, i_k\}$ est un ensemble d'information du code C. Et $(x_1, \cdots, x_k)$ un vecteur quelconque de $\mathbb{F}_q^k$, alors il existe un unique mot $c \in C$ tel que pour $j \leq k$, on ait $c_j = x_j$. De plus on peut calculer c a partir d'une matrice génératrice de C par simple inversion matricielle. (confère [2])*

⋆ ⋆ Chapitre Deux ⋆ ⋆

Les codes rang

2.1 Introduction et historique de la métrique rang

La norme la plus connue en théorie du codage est ***poids de Hamming****[11] d'un vecteur pris dans un corps fini. Au fil des années, plusieurs autres métriques ont été implémentés à l'instar de la* ***métrique rang****. En effet le concept de métrique rang fut introduit par Loo-Keng Hua[16] comme étant " la distance arithmétique ". Ensuite, Philipe Delsartre définit la distance rang sur un ensemble de forme bilinéaires et propose une construction de codes par représentation sous forme bilinéaire mais sans aucun algorithme de décodage. Plu tard, Ernst- Gabidulin[4] à introduit la distance rang pour les espaces vectoriels sur les* ***extensions*** *de corps . Il est considéré aujourd'hui comme l'une des personnes qui ont révolutionnées la conception des cryptosystèmes à base de la métrique rang, notamment grâce à ses travaux sur la construction des codes* ***MDR****[4] et des cryptosystèmes* ***GPT***[1] *à l'aide des polynômes linéaires .*

2.2 Intérêt d'utilisation de la métrique rang

L'une des idées maitresses qui ont impulser la recherche dans cette branche nouvelle de la cryptographique est la réduction de la taille des clés publiques des cryptosystèmes à l'aide de la métrique rang.

Les algorithmes classiques de décodage général en métrique de Hamming utilisent la méthode du type ensemble d'information qui consiste à déplacer une fenêtre sur le mot reçu et à espérer que l'erreur se situe en dehors. En métrique rang, cette méthode est inapplicable. Cependant, des algorithmes assez intéressant de décodage en métrique rang ont été proposés par Ourvski et Johanson [19], avec une complexité bien plus élevée que ce que nous propose la métrique de Hamming. C'est ainsi que

1. **GPT** : du à leurs auteurs Gabidulin, Paramonov et Tretjakov *en 1991*

progressivement, on parvient de nos jours à construire des codes rang dont la matrice génératrice est assez petite mais dont le décodage n'est pas envisageable si l'on ne connait pas la structure algébrique de ces codes.

2.3 Définition des codes rangs

2.3.1 La métrique rang

Soient N, n, q des entiers naturels non nuls,q premier, $\mathbb{F}_q$ un corps fini et $\mathbb{F}_{q^N}$ une extension de $\mathbb{F}_q$ de degré N.

Notons par $\mathbb{F}_q^{N\times n}$ l'ensemble des matrices N lignes et n colonnes à entrées dans $\mathbb{F}_q$; $\Omega = \{\omega_1, \omega_2, \cdots, \omega_N\}$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^N}$.

Soit $v \in \mathbb{F}_{q^N}^n$, $v = (v_1, v_2, \cdots, v_n)$.

Les coordonnées v_j, $\quad 1 \leq j \leq n$ de v peuvent être vues comme des vecteurs colonnes de $\mathbb{F}_q$ ayant pour composantes les coefficients v_{ij} dans la base Ω . $v_j = \sum_{i=1}^{N} v_{ij}\omega_i$

En outre $v = (v_1, v_2, \cdots, v_n)$ peut être assimilé à la matrice $M = \begin{pmatrix} v_{11} & v_{11} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \cdots & \cdots & \vdots \\ v_{N1} & \cdots & \cdots & v_{Nn} \end{pmatrix} \qquad v_{ij} \in \mathbb{F}_q$

Proposition 2.1. *les $\mathbb{F}_q$-espaces vectoriel $\mathbb{F}_{q^N}^n$ et $\mathbb{F}_q^{N\times n}$ sont isomorphes via l'application*

$$\begin{array}{rccc} \Phi : & \mathbb{F}_{q^N}^n & \longrightarrow & \mathbb{F}_q^{N\times n} \\ & v = (v_1, v_2, \cdots, v_n) & \longmapsto & M = \begin{pmatrix} v_{11} & v_{11} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \cdots & \cdots & \vdots \\ v_{N1} & \cdots & \cdots & v_{Nn} \end{pmatrix} \qquad v_{ij} \in \mathbb{F}_q \end{array}$$

Proposition 2.1. *L'application :*

$$\begin{array}{rccll} d : & \mathbb{F}_{q^N}^n \times \mathbb{F}_{q^N}^n & \longrightarrow & \mathbb{N} & \text{où } Rg(\Phi(x) - \Phi(y)|\mathbb{F}_q) \text{ est le rang de la} \\ & (x, y) & \longmapsto & d(x, y) = Rg(\Phi(x) - \Phi(y)|\mathbb{F}_q) & \text{matrice } \Phi(x) - \Phi(y) \text{ sur } \mathbb{F}_q \end{array}$$

est une distance sur $\mathbb{F}_{q^N}^n$.

Démonstration. Soient a, b, c trois éléments de $\mathbb{F}_{q^N}^n$. $A = \Phi(a)$, $B = \Phi(b)$ *et* $C = \Phi(c)$

i) $d(a,b) \geq 0$ puisque le rang est un entier naturel

ii) $d(a,b) = 0 \iff Rg(A-B|\mathbb{F}_q) = 0 \iff A - B = [0]_{N\times n} \iff A = B \iff a = b$

iii) Soient $A_1,\ A_2,\ A_3, \cdots A_n$ les colonnes de A, $B_1,\ B_2, \cdots B_n$ celle de B

$$\begin{aligned} d(a,b) &= Rg(A-B|\mathbb{F}_q) \\ &= dim\ vect(A_1 - B_1, A_2 - B_2, \cdots, A_n - B_n >) \\ &= dim\ vect(B_1 - A_2, B_2 - A_2, \cdots, B_n - A_n) \\ &= Rg(B-A|\mathbb{F}_q) \end{aligned}$$

$$d(a,b) = d(b,a)$$

iv) Soit C_i $1 \leq i \leq n$ les colonnes de C. Montrons que $d(a,c) \leq d(a,b) + d(b,c)$

$Rg(A-C|\mathbb{F}_q) = dim\ vect(A_1 - C_1, A_2 - C_2, \cdots, A_n - C_n)$

Or pour $i = 1, 2, \cdots,\ n \quad A_i - C_i = A_i - B_i + B_i - C_i$. Ce qui permet de déduire que

$vect(A_i - C_i, \quad 1 \leq i \leq n) \subseteq vect(A_i - B_i,\ \ 1 \leq i \leq n) + vect(B_i - C_i,\ \ 1 \leq i \leq n)$

D'où

$dim\ vect(A_i - C_i,\ \ 1 \leq i \leq n) \leq dim\ vect(A_i - B_i,\ \ 1 \leq i \leq n) + dim\ vect(B_i - C_i,\ \ 1 \leq i \leq n)$

$$\Updownarrow$$

$$Rg(A-C|\mathbb{F}_q) \leq Rg(A-B|\mathbb{F}_q) \leq Rg(B-C|\mathbb{F}_q)$$

Ce qui prouve que $d(a,c) \leq d(a,b) + d(b,c)$ ❑

Conclusion : d est une distance sur $\mathbb{F}_{q^N}^n$

Propriété 2.3.1. *La métrique rang est plus grossière que la métrique de Hamming.*

$$\forall x \in \mathbb{F}_{q^N}^n,\ Rg(x) \leq \omega(x) \qquad (\omega \cong \textit{poids de Hamming})$$

Dans la suite, on adoptera la notation $d(x,y) = Rg(x-y|\mathbb{F}_q)$ *au lieu* $Rg(\Phi(x) - \Phi(y)|\mathbb{F}_q)$

Démonstration. Si x possède p coordonnées non nulles, on a $\omega(x) = p$. Ces p coordonnées peuvent être liées dans $\mathbb{F}_{q^N}$. D'où $Rg(x|\mathbb{F}_q) \leq p$ ❑

Définition 2.3.1 (Code rang). *Soit* $\mathbb{F}_{q^N}$ *une extension de* $\mathbb{F}_q$ *de degré* N*. On appelle code rang de longueur* n *tout sous-espace vectoriel de* $\mathbb{F}_{q^N}^n$ *;* (Les codes rang sont les codes linéaires)

La distance minimale d'un code rang C est la quantité $d(C) = min\{Rg(x-y|\mathbb{F}_q),\ x \neq y,\ x,\ y\ \in C\}$

Remarque 2.3.1. $d(C) = min\{Rg(x|fq), x \in C \setminus \{0\}\}$

Exemple 2.3.1. .

Construisons un code rang C de type $(3,2,1)$ sur $\mathbb{F}_4 = \{0,1,\gamma,\gamma^2\}$. Où γ est un élément primitif de $\mathbb{F}_4$ avec pour polynôme primitif x^2+x+1. $\mathbb{F}_{2^2}$ est une extension de $\mathbb{F}_2$ de degré 2 .

Considérons le code rang C sur $\mathbb{F}_4$ de matrice génératrice

$G = \begin{pmatrix} 1 & \gamma & \gamma \\ 0 & 1 & \gamma^2 \end{pmatrix}$

Soit $\mathcal{B} = \{1,\gamma\}$ une $\mathbb{F}_2$-base de $\mathbb{F}_4$. Alors $C = im(f)$ où

$$\begin{array}{rccc} f\ : & \mathbb{F}_4^2 & \longrightarrow & \mathbb{F}_4^3 \\ & (x,y) & \longmapsto & (x,y).G \end{array}$$

$f(0,1) = (0,1,\gamma^2)$;

Dans la base $\mathcal{B}$, $0 = (0,0),\ 1 = (1,0),\ \gamma^2 = 1+\gamma = (1,1)$

Ainsi la forme matricielle du mot code $(0,1,\gamma^2)$ est $\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

$Rg(\ (0,1,\gamma^2)\ )|\mathbb{F}_2) = 2$

mettons la matrice de G sous forme systématique :

Par une transformation sur les lignes de G ,on obtient une matrice du code C sous forme systématique $\begin{pmatrix} 1 & 0 & \gamma^2 \\ 0 & 1 & \gamma \end{pmatrix}$

La matrice de contrôle de C est $H = (-\gamma^2\ \gamma\ 1)$ *(H est une matrice de type $(n-k)\times n$ d'après la remarque 1.6.6 de la page 25 , c'est-à-dire de type 1×1 puisque $n=3$ et $dim(C)=2$)*

2.3.2 Borne de Singleton - Borne de Gilbert Varshamov

a) Sphère et Boules en métrique rang

Définition 2.3.2. *Soit t un entier fixé, $x \in \mathbb{F}_{q^N}^n$.*

*On appelle **sphère de centre** x et de rayon t l'ensemble $\mathcal{S}(x,t) = \{\ y \in \mathbb{F}_{q^N}^n\ / Rg(y-x) = t\ \}$.*

*L'ensemble $\mathcal{B}(x,t) = \{\ y \in \mathbb{F}_{q^N}^n\ /\ Rg(y-x) \leq t\ \}$ désigne **la boule de centre** t.*

Proposition 2.2. *Les cardinaux de $\mathcal{S}(x,t)$ et de $\mathcal{B}(x,t)$ ne dépendent pas de x*

Preuve. :Elle découle du fait que les applications

$$\begin{array}{rccc} g\ : & \mathcal{S}(x,t) & \longrightarrow & \mathcal{S}(0,t) \\ & y & \longmapsto & y-x \end{array} \quad et \quad \begin{array}{rccc} f\ : & \mathcal{S}(x,t) & \longrightarrow & \mathcal{B}(0,t) \\ & y & \longmapsto & y-x \end{array} \quad sont\ bijectives$$

□

Dans la suite , on notera par $\mathcal{S}(n, N, q, t)$ le cardinal de la sphère de rayon t sur $\mathbb{F}_{q^N}^n$ et par $\mathcal{B}(n, N, q, t)$ celui des boules de rayon t.

Proposition 2.3. $\mathcal{S}(n, N, q, t) = \prod_{j=0}^{t-1} \frac{(q^n - q^j)(q^N - q^j)}{q^t - q^j}$

De plus $\mathcal{B}(n, N, q, t) = \sum_{i=0}^{t} \mathcal{S}(n, N, q, t)$

La quantité $\prod_{j=0}^{t-1} \frac{q^N - q^j}{q^t - q^j}$ *est appelée* ***binôme de Gauss*** *et est notée* $\begin{bmatrix} m \\ t \end{bmatrix}_q$ *. Elle représente le nombre de sous espace vectoriel de dimension t sur* $\mathbb{F}_{q^N}$ *.*

Preuve. *cf [22] pages* ***2-4*** par **P Loidreau** □

b) Borne de singleton

Proposition 2.4 (**Borne de singleton**). .

Soit C un code rang de type (n, k, d) *sur* $\mathbb{F}_q^N$*. Alors*

$$\boxed{\mathsf{d} \leq \mathsf{n} + 1 - \mathsf{k}}.$$

Démonstration. Notons par d_H la distance de hamming (section 1.6.3 (page 19) de C .

Soit M le sous-espace vectoriels de vecteurs dont les $k-1$ dernières coordonnées sont nulles.

$$\begin{aligned} dim(C \cap Q) &= dim(C) + dim(M) - dim(C + M) \\ &= k + n - k + 1 - dim(C + M) \\ &= n + 1 - dim(C + M) \\ &\geq 1 \end{aligned}$$

Donc il existe $x \in C$ tel que $\omega(x) \leq n - k + 1$. Ainsi $d_H \leq n - k + 1$.

La métrique rang étant plus grossière que la métrique de Hamming (***propriété*** *2.3.1 page 31*), il vient que $d \leq d_H \leq n - k + 1$. □

Remarque 2.3.2. Si C est un code rang sur $\mathbb{F}_{q^N}$ de dimension k et de distance minimale d, alors : $|C| \leq q^{\min\{\ N(n-d+1),\ n(N-d+1)\ \}}$

En particulier , si $n > N$ on obtient $d \leq 1 + \lfloor \frac{(n-k)N}{n} \rfloor$

Preuve. cf [14] pages **5-11** □

Définition 2.3.3 (**Code MDR** [2]). .

Un $(n, k, d) - code\ rang$ *est dit* ***MDR*** *si* $\boldsymbol{d = n\text{-}k\text{+}1}$

2. **MDR** : *Maximum distance Rang*

Borne de Gilbert-Varshamov

Proposition 2.5 (**Borne de Gilbert-Varshamov**). .

Il est possible de construire un code rang linéaire $C(n,k,d)$ lorsque $\mathcal{B}(n,N,q,d) < q^{N(n-k)}$

La borne de **Gilbert-Varshamov** d'un code rang sur $\mathbb{F}_{q^N}$ notée **GVR(n,k,m,q)** est le plus petit entier $\tilde{d}$ tel que $\mathcal{B}(n,N,q,\tilde{d}) \geq q^{N(n-k)}$.

Cette borne permet d'assurer l'existence de code rang pour certains paramètres adéquats.

Étant donné un code rang C de matrice duale H, **GVR(n,k,m,q)** correspond au plus petit rang pour lequel pour l'on peut dire avec certitude tout syndromes s, il existe au moins un mot x de rang r tel que $Hx^\top = s$

2.3.3 Codes de Gabidulin[4]

Dans cette partie, $k \leq n \leq N$ et $g = (g_1, g_2, \cdots, g_n) \in \mathbb{F}_{q^N}^n$ tel que $\{g_1, g_2, \cdots, g_n\}$ est une famille libre sur $\mathbb{F}_q$.

Proposition 2.6. . *L'ensemble*

$Gab(g,k,n) = \{ \ (P(g_1), P(g_2), \cdots, P(g_n)), \ P$ *est un* $q-$*polynôme sur* $\mathbb{F}_{q^N}$ *tel que* $deg_q(P) \leq k-1 \ \}$

vérifie les propriétés suivantes :

① ***Gab(g,k,n)*** *est un sous espace vectoriel de* $\mathbb{F}_{q^N}^n$ *de dimension* **k**

② $\forall x \in$ ***Gab(g,k,n)***, ***Rg(x / $\mathbb{F}_q$)*** $\geq$ ***n-k+1***

Preuve. .

① La structure de sous-espace vectoriel de $Gab(g,k,n)$ découle du fait que l'ensemble des q-polynômes est un sous espace vectoriel de l'ensemble des applications linéaire sur $\mathbb{F}_{q^N}$.

Montrons que *dim Gab(g,k,n) = k*

À partir de la définition de $Gab(g,k,n)$, on déduit que

$Gab(g,k,n) = \{ \ (a_0, a_1, \cdots, a_{k-1}).G \ , \quad (a_0, a_1, \cdots, a_{k-1}) \in \mathbb{F}_{q^N}^{k-1} \ \}$

où $G = \begin{pmatrix} g_1 & g_2 & \cdots & \cdots & g_n \\ g_1^q & g_2^q & \cdots & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & \cdots & g_n^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & \cdots & g_n^{q^{k-1}} \end{pmatrix}$

Avec cette notation, on remarque que les lignes de G sont également les éléments de $Gab(g,k,n)$ *(Il suffit de considérer successivement les $q-$polynômes $X,\ X^q,\ X^{q^2},\cdots,X^{q^{k-1}}$)* et en constituent une famille génératrice. De plus ces lignes sont linéairement indépendantes.

En effet, supposons qu'il existe une famille de scalaires non tous nuls $\alpha_0,\ \alpha_1,\cdots,\alpha_{k-1}$ pris dans $\mathbb{F}_{q^N}$ tel que

$\alpha_0(g_1,g_2,\cdots,g_n)+\alpha_1(g_1^{q^2},g_2^{q^2},\cdots,g_n^{q^2})+\cdots+\alpha_{k-1}(g_1^{q^{k-1}},g_2^{q^{k-1}},\cdots,g_n^{q^{k-1}})=(0,0,0,0,0,\cdots,0)$

Ceci équivaut à $\begin{cases} \sum_{i=0}^{k-1}\alpha_i g_1^{[i]} &= 0 \\ \vdots & \\ \sum_{i=0}^{k-1}\alpha_i g_n^{[i]} &= 0 \end{cases}$

Posons $P_\alpha(X)=\alpha_{k-1}X^{[k-1]}+\alpha_{k-2}X^{[k-1]}+\cdots+\alpha_1X^{[1]}+\alpha_0X$

P_α est un $q-$polynôme de degré $k-1$ s'annulant sur $\{g_1,g_2,\cdots,g_n\}$ qui est une famille libre de $\mathbb{F}_{q^N}$ .Ce qui entraine que $<g_1,g_2,\cdots,g_n>\subseteq Ker(P_\alpha)$.

D'où $dim\ <g_1,g_2,\cdots,g_n>\leq\ dim\ Ker(P_\alpha)\leq k-1$ d'après la **proposition** 1.3 page 16 .

On obtient $n\leq k-1$; ce qui est impossible puisque $k\leq n\leq N$.

Donc $\alpha_{k-1}=\alpha_{k-2}=\cdots=\alpha_0=0$

Les k lignes de G forment une famille libre génératrice de $Gab(g,k,n)$. D'où $dim\ Gab(g,k,n)=k$

② Soit $x\in Gab(g,k,n)$ de rang r.

Montrons que $\mathbf{r\geq n-k+1}$.

$x\in Gab(n,k,g)\Rightarrow$ Il existe un q-polynôme P_x de degré inférieur ou égale à $k-1$ tel que $x=(\ P_x(g_1),\ P_x(g_2),\cdots,\ P_x(g_n)\ )$.

Puisque $Rg(x\mid\mathbb{F}_q)=r$, x possède au moins $n-r$ colonnes liée dans sa représentation matricielle sur $\mathbb{F}_q^{N\times n}$. Or ces colonnes sont exactement les $P_x(g_i)\quad 1\leq i\leq n$ vue comme vecteur de $\mathbb{F}_q^N$.

Sans nuire à la généralité, supposons que les $n-r$ dernières colonnes soient liées aux r premières.

✪ $\begin{cases} P_x(g_{r+1})=a_1^{(r+1)}P_x(g_1)+\cdots+a_r^{(r+1)}P_x(g_r) \\ P_x(g_{r+2})=a_1^{(r+2)}P_x(g_1)+\cdots+a_r^{(r+2)}P_x(g_r) \\ \vdots \\ P_x(g_n)=a_1^{(n)}P_x(g_1)+\cdots+a_r^{(n)}P_x(g_r) \end{cases} \Longleftrightarrow \begin{cases} P_x(\ a_1^{(r+1)}g_1+\cdots+a_r^{(r+1)}g_r-g_{r+1}\ )=0 \\ P_x(\ a_1^{(r+2)}g_1+\cdots+a_r^{(r+2)}g_r-g_{r+2}\ )=0 \\ \vdots \\ P_x(\ a_1^{(n)}g_1+\cdots+a_r^{(n)}g_r-g_n\ )=0 \end{cases}$

avec $a_j^{(i)}$ des éléments de $\mathbb{F}_{q^N}$.

Posons $f_1 = a_1^{(r+1)}g_1 + \cdots + a_r^{(r+1)}g_r - g_{r+1}$, $f_2 = a_1^{(r+2)}g_1 + \cdots + a_r^{(r+2)}g_r - g_{r+2}$ $\cdots$ $\cdots$
$f_{n-r} = a_1^{(n)}g_1 + \cdots + a_r^{(n)}g_r - g_n$

L'équivalence ✪ devient $P_x(f_1) = 0,\ P_x(f_2) = 0,\ P_x(f_3) = 0, \cdots\cdots p_x(f_{n-r}) = 0$

$f_1,\ f_2,\ f_3,\ \cdots, f_{n-r}$ sont des éléments de $Ker(P_c)$. En utilisant le fait que $\{g_1, g_2, \cdots, g_n\}$ est libre sur $\mathbb{F}_q$, on déduit que $\{f_1,\ f_2,\ f_3,\ \cdots, f_{n-r}\}$ est une famille libre de $n-r$ vecteurs de $Ker(P_x)$; Par suite, $dim\ < f_1,\ f_2,\ f_3,\ \cdots, f_{n-r} > \leq dim\ Ker(P_x) \leq k-1$.

C'est-à-dire $n - r \leq k - 1$. D'où $r \geq n - k + 1$

□

Définition 2.3.4 (**Codes de Gabidulin**). .

*On appelle **codes de Gabidulin** de **longueur** n, de **dimension** k et de **support** g le code rang obtenu par évaluation des q-polynôme degré inférieur à k sur les coordonnées de g.*

$Gab(g, k, n) = \{\ (\ P(g_1), P(g_2), \cdots, P(g_n)\ ),\ P$ *est un* $q-$*polynôme sur* $\mathbb{F}_{q^N}$ *tel que* $deg_q(P) \leq k-1\ \}$

Proposition 2.7. *Les codes de Gabidulin sont les **codes MDR***

Preuve : notons par d la distance minimale de $Gab(g, k, n)$. D'après la proposition 2.6 page 34 $Gab(g, k, n)$ est un code rang sur $\mathbb{F}_{q^N}$ et d vérifie $\mathbf{d \geq n - k + 1}$.
Grâce à la borne de singleton ***(proposition2.4)*** on a $d \leq n - k + 1$

d'où $\boxed{\mathbf{d= n\text{-}k+1}}$

□

Proposition 2.8 (**dual d'un code de Gabidulin**). .

Si $C = Gab(g, k, n)$ est un code de Gabidulin, alors le code dual C' est aussi un code de Gabidulin de dimension $n - k$, de longueur n et de support h obtenu par résolution de système de n équations $(\ \sum_{j=1}^{n} h_j g_j^{[i+1+k-n]}\ )_{i=1,2,\cdots,n-2}$

*(une preuve de cette proposition est fait par **Gabidulin** dans [5] page 1-12)*

2.4 Décodage des codes rangs

Avec la métrique de Hamming, il est facile d'évaluer l'écart entre le mot y reçu et le mot x qui a été réellement envoyer. Plus cet écart est petit, plus le mot y est proche de x. C'est sur ce principe que repose le décodage par maximum de vraisemblance. Cette méthode de décodage est presque impossible

en métrique rang. En effet, si l'on désigne par e l'erreur et qu'on pose $e = y - x$,.
Il peut très bien arrivé que $Rg(e) = 1$ et $\omega(e) = 5$, c'est-à-dire $d(x, y) = 1$ alors que le, x et y diffèrent d'au moins 5 coordonnées.

Notons tout de même que, diverses méthodes de détection d'erreurs ou de décodages existent en métrique rang. Dans cette section, nous nous évertuerons à donner quelques unes d'entre elles.

Proposition 2.1. *Soit $s \in \mathbb{N}^*$, C un code rang de longueur n sur $\mathbb{F}_{q^N}$. Si $d(C) \geq s + 1$, alors C peut détecter jusqu'à s erreurs sur un mot code reçu.*

Démonstration. Soit x un mot code envoyé via un canal symétrique(4).
Supposons que le mot y reçu diffère de x par t coordonnées, $t \leq s$. Posons $y = x + e$ où e est l'erreur survenue. On a $e = y - x$.
Le poids de Hamming de e est $\omega(e) = t$
D'après la propriété 2.3.1 $Rg(e|\mathbb{F}_q) \leq \omega(e) = t \leq s$; d'où $Rg(e|\mathbb{F}_q) \leq s$.
$e \notin C$; en fait si e était dans C, on aurait $s + 1 \leq d(C) \leq Rg(e|\mathbb{F}_q) \leq t \leq s$, c'est-à-dire $s + 1 \leq s$.
Ce qui est impossible. Ainsi l'erreur e est détectée. □

2.4.1 Correction d'erreurs à l'aide de la métrique rang

Théorème 2.1. *Soient C un (n, k, d) code rang sur $\mathbb{F}_{q^N}$, e une erreur de rang $r = Rg(e) \leq \lfloor \frac{d-1}{2} \rfloor$ et $c \in C$, tel que $y = c + e$*

i) *c est l'unique élément de C tel que $d(y, c') = r$*

ii) *Soit C' le code engendré par la matrice $G' = \begin{pmatrix} G \\ y \end{pmatrix}$ $y = (y_1, \cdots, y_n)$.*

Les vecteurs non nuls de C' de rang minimum sont de la forme de la forme αe, $\alpha \in \mathbb{F}_{q^N}$

Démonstration. **i)** La preuve est analogue à celle de la **théorème** 1.3

ii) D'après (i), y et e ne sont pas dans C.

Sans nuire à la généralité, supposons que $G = \begin{pmatrix} g11 & g_{12} & \cdots & g_{1n} \\ g_{21} & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ g_{k1} & \cdots & \cdots & g_{kn} \end{pmatrix}$ alors $G' = \begin{pmatrix} g11 & g_{12} & \cdots & g_{1n} \\ g_{21} & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ g_{k1} & \cdots & \cdots & g_{kn} \\ y_1 & y_2 & \cdots & y_n \end{pmatrix}$

Montrons que $C' = C \bigoplus \mathbb{F}_{q^N}.e$:

D'après la définition de G' , *pour tout* $x \in C'$, il existe $\alpha \in \mathbb{F}_{q^N}$ et $c_x \in C$

tel que $x = c_x + \alpha y = c_x + \alpha c + \alpha e$. D'où $C' \subseteq C \bigoplus \mathbb{F}_{q^N}.e$

En outre , on peut remarquer que le vecteur $-c + c + e$ est dans C' et par suite e appartient à C'.

De plus pour $\alpha = 0$, on a $x = c_x$. Ainsi $C \subseteq C'$

Conclusion $C' = C \bigoplus \mathbb{F}_{q^N}$

✪ Soit $x \in C$, on sait qu'il existe $\alpha \in \mathbb{F}_{q^N}$ et $c_0 \in C$ tel que $x = c_0 + \alpha e$

Supposons x est de rang minimum alors $Rg(x) \leq Rg(e) \leq \dfrac{d-1}{2}$ car $e \in C'$

Or $Rg(x) \leq \dfrac{d-1}{2} \leq d(C)$ $\Rightarrow x \notin d(C)$

Supposons $c_0 \neq 0$ et $\alpha \neq 0$ alors

$$\begin{aligned} c = x - \alpha.e &\implies d \leq Rg(c) \leq Rg(x) + Rg(\alpha e) \\ &\implies d \leq \frac{d-1}{2} + \frac{d-1}{2} \qquad (\ Rg(\alpha e) = Rg(e)\ si\ \alpha \neq 0) \\ &\implies d \leq d-1 \qquad absurde \end{aligned}$$

Donc $c = 0$ et $x = \alpha.e$

□

On peut donc décoder C en utilisant un algorithme de recherche de mots de poids faibles sur C'. Lorsqu'on a obtenu $e' = \alpha e$, on retrouver facilement la valeur α en utilisant le fait que $He'^{\top} = \alpha H y^{\top}$ où H est la matrice duale de G

Comment rechercher les mots de poids faibles sur C' ?

Avant de répondre à cette question, énonçons d'abord le théorème suivant :

Théorème 2.2. *Les mots de* $\mathbb{F}_{q^N}^n$ *de rang inférieurs ou égale à* t *sont de la forme* $(\beta_1\ \beta_2\ \cdots \beta_t)\mathbf{Q}$ *où* $\{\beta_1,\ \beta_2,\ \cdots, \beta_t\}$ *est une famille d'éléments de* $\mathbb{F}_{q^N}$ *libre sur* $\mathbb{F}_q$ *et* Q *est une matrice* $t \times n$ *a coefficients dans* $\mathbb{F}_q$

Démonstration. .

$\Rightarrow$) Soit $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_{q^N}^n$ tel que $Rg(x|\mathbb{F}_q) \leq t$.

Où $x_j = \sum_{i=1}^{N} x_{ij}\omega_i \quad 1 \leq j \leq n$, avec $\{\omega_1, \omega_2, \cdots, \omega_N\}$ une $\mathbb{F}_q$ - base de $\mathbb{F}_{q^N}$ ❤

Montrons que x **peut s'écrire sous la forme** $(x_1\ x_2\ \cdots x_t) \left[\ I_{t\times t} \ \middle|\ A_{t\times(n-t)}\ \right]$

- En déroulant x sous forme matricielle, par rapport à la base $\{\omega_1, \omega_2, \cdots, \omega_N\}$,

  on a $X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ x_{N1} & x_{N2} & \cdots & \cdots & x_{Nn} \end{pmatrix}$.

  Puisque $Rg(x|\mathbb{F}_q) \leq t$, X possède au moins $n-t$ colonnes liées.

  Sans nuire à la généralité, supposons que les $n-t$ dernières colonnes soient liées et s'expriment comme combinaisons linéaire des t premières. On a :

  $x_{t+1} = \sum_{j=1}^{t} a_r^{(t+1)} x_j = \sum_{i=1}^{N} (\sum_{j=1}^{t} x_{ij} a_j^{(t+1)}) \omega_i$ *(d'après la ligne ❤)*

  $$Ainsi, \quad x_{t+1} = \left(\sum_{j=1}^{t} a_r^{(t+1)} x_{1j}, \ \sum_{j=1}^{t} a_r^{(t+1)} x_{2j}, \cdots, \sum_{j=1}^{t} a_r^{(t+1)} x_{nj} \right)$$

  $$= \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1t} \\ x_{21} & x_{22} & \cdots & x_{2t} \\ \vdots & \vdots & \ddots & x_{3t} \\ \underbrace{x_{N1}}_{x_1} & \underbrace{x_{N2}}_{x_2} & \cdots & \underbrace{x_{Nt}}_{x_t} \end{pmatrix} \begin{pmatrix} a_1^{(t+1)} \\ a_2^{(t+1)} \\ \vdots \\ a_t^{(t+1)} \end{pmatrix}$$

  $x_{t+1} = (x_1 \ x_2 \ \cdots x_t) \begin{pmatrix} a_1^{t+1} \\ a_2^{t+1} \\ \vdots \\ a_t^{(t+1)} \end{pmatrix}$. De façon analogue, on a $x_j = (x_1 \ x_2 \cdots \ x_t) \begin{pmatrix} a_1^{(j)} \\ a_2^{(j)} \\ \vdots \\ a_t^{(j)} \end{pmatrix}$

  Ainsi, le vecteur $(x_{t+1}, \ x_{t+2}, \cdots, x_n)$ peut s'écrire encore

  $$(x_{t+1}, \ x_{t+2}, \cdots, x_n) = (x_1 \ x_2 \cdots x_t) \begin{pmatrix} a_1^{(t+1)} & a_1^{(t+2)} & \cdots & a_1^{(n)} \\ a_2^{(t+1)} & a_2^{(t+2)} & \cdots & a_2^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ a_t^{(t+1)} & a_t^{(t+2)} & \cdots & a_t^{(n)} \end{pmatrix}$$

  En définitive, on obtient

  $$(x_1, \ x_2, \ \cdots, x_t, \ x_{t+1}, \ x_{t+2}, \cdots, x_n) = (x_1 \ x_2 \cdots x_t) \left[\begin{array}{ccccc|cccc} 1 & 0 & 0 & \cdots & 0 & a_1^{(t+1)} & a_1^{(t+2)} & \cdots & a_1^{(n)} \\ 0 & 1 & 0 & \cdots & 0 & a_2^{(t+1)} & a_2^{(t+2)} & \cdots & a_2^{(n)} \\ 0 & 0 & 1 & \cdots & 0 & a_3^{(t+1)} & a_3^{(t+2)} & \cdots & a_3^{(n)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_t^{(t+1)} & a_t^{(t+2)} & \cdots & a_t^{(n)} \end{array} \right]$$

(⇐ **Réciproquement**

Soit $x = (\beta_1\ \beta_2 \cdots\ \beta_t)Q$, où les $\beta_1, \cdots \beta_t$ sont libres sur $\mathbb{F}_q$ et $Q = \begin{pmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{t1} & \cdots & q_{tn} \end{pmatrix} \quad q_{ij} \in \mathbb{F}_q$

On a : $x = (\ \sum_{i=1}^{t} \beta_i q_{i1},\ \sum_{i=1}^{t} \beta_i q_{i2}, \cdots, \sum_{i=1}^{t} \beta_i q_{in}\ )$

Le rang de x sur $\mathbb{F}_q$ est la dimension du sous espace vectoriel engendré par les colonnes de la matrice X associée à x ; où $X = (\ C_1\ C_2 \cdots\ C_n\ )$ et les colonnes C_i vérifient

$C_1 = q_{11}\underbrace{\begin{pmatrix} \beta_{11} \\ \beta_{21} \\ \vdots \\ \beta_{N1} \end{pmatrix}}_{\beta_1} + \cdots + q_{t1}\underbrace{\begin{pmatrix} \beta_{1t} \\ \beta_{2t} \\ \vdots \\ \beta_{Nt} \end{pmatrix}}_{\beta_t}$ c'est-à-dire $C_1 = q_{11}\beta_1 + q_{21}\beta_2 \cdots + q_{t1}\beta_t$.

De même $C_2 = q_{12}\beta_1 + q_{22}\beta_2 \cdots + q_{t2}\beta_t$; successivement, on parvient à $C_n = q_{1n}\beta_1 + q_{2n}\beta_2 \cdots + q_{tn}\beta_t$.

Les colonnes de X sont donc les combinaisons linéaires des $\beta_1,\ \beta_2, \cdots, \beta_t$ vus comme vecteur colonnes de $\mathbb{F}_q^N$. On déduit que $vect(\{C_1, C_2, \cdots, C_n\}) \subseteq <\ \beta_1,\ \beta_2, \cdots, \beta_t\ >$

D'où $dim(\ vect(\{C_1, C_2, \cdots, C_n\})\ ) \leq dim(<\ \beta_1,\ \beta_2, \cdots, \beta_t\ >)$ et par suite $Rg(x \mid \mathbb{F}_q) \leq t$

□

La recherche des mots de rang faible de C' *(C' étant définie au (ii) du théorème 2.1 de la page 37)* se fait en 3 étapes :

① Quitte à effectuer une permutation, on suppose que $[1, k+1]$ forme un ensemble d'information du code C'.

on note par $G' = \left[\ I_{k+1} \ \middle|\ R\ \right]$ et $H' = \left[\ -R^\top \ \middle|\ I_{n-k-1}\ \right]$ les matrices génératrices et duale de C' associée à cet ensemble d'information.

② Sachant que les mots de rang $t \leq \lfloor \frac{d-1}{2} \rfloor$ sont de la forme $x = (\beta_1 \cdots \beta_t)Q$ *(voir théorème 2.2 ci-dessus)* ; on pose $Q = \left[\ Q_1 \ \middle|\ Q_2\ \right]$

Lorsque x est pris dans C' il vient que $x.H'^\top = 0$; c'est-à-dire $(\beta_1 \cdots \beta_t)\left[\ Q_1 \ \middle|\ Q_2\ \right] H'^\top = 0$.

Ce qui équivaut à $(\beta_1 \cdots \beta_t)\left[\ Q_1 \ \middle|\ Q_2\ \right]\left[\begin{array}{c} -R \\ \hline I_{n-k-1} \end{array}\right] = 0$

D'où $(\beta_1 \cdots \beta_t)(Q_2 I_{n-k-1} - Q_1 R) = 0$. Ainsi , les mots de C' de rang $t \leq \lfloor \frac{d-1}{2} \rfloor$ vérifient l'équation

$$(\beta_1\ \beta_2 \cdots \beta_t)(Q_2 - Q_1 R) = 0, \quad \textit{les } \beta_i \textit{ libres sur } \mathbb{F}_q \tag{2.1}$$

C'est une équation dont les inconnues sont $\beta_1 \cdots \beta_t$ et la matrice Q.

③ **résolution de l'équation 2.1**

Pour y parvenir, on peut :

méthode 1 énumérer les familles libres $\{\beta_1 \cdots \beta_t\}$. *(on doit énumérer au plus $q^{(N-t)(t-1)}$ familles d'après [2] page **79**)*

Pour chacune d'entre elles, on tente de résoudre dans $\mathbb{F}_q$ l'équation 2.1 dont l'inconnue est Q

méthode 2 chercher une matrice $V = Q_2 - Q_1 R$ qui ne soit pas de rang maximale *(d'après [2] page 80, on doit dans ce cas énumérer un ensemble de $q^{t(k+1)}$ matrice et tester le rang de chacune).*

Lorsque une matrice de rang au plus t-1 est trouvée, on résout l'équation 2.1 ci-dessus.

Corollaire 2.4.1 (**Décodage d'Ourivski et Johanson [19]**). .

Soit C un code linéaire (n,k) de distance rang d, $y \in \mathbb{F}_{q^N}$ un mot de longueur n et $t \leq \lfloor \frac{d-1}{2} \rfloor$. Alors on peut trouver un mot de C' à distance rang au plus t du mot y de deux manière :

❶ *Par énumération des base en $o(\ (k+t)^3 q^{(t-1)(m-t)+2\ }\ )$*

❷ *Par énumération des coordonnées en $o(\ (k+t)^3 t^3 q^{(t-1)(k+1)\ }\ )$*

2.4.2 Décodage des codes de Gabidulin

Plusieurs méthodes peuvent être utilisées pour décoder les codes de Gabidulin l'une d'entre elles est exposée par **Philippe GABORIT** dans [20] et est basée sur la caractérisation du noyau des polynômes linéaires.

approche de Philippe GABORIT

Théorème 2.3. .

Ici $N = n$.

Le code $C = \boldsymbol{Gab}(g,k,n)$ peut corriger jusqu'à $\frac{n-k}{2}$ erreurs .

Preuve. .

Soit c un mot code de C ; $c = (P_c(g_1), \cdots, P_c(g_n))$, $P_c \in \mathcal{P}_{k-1}$; e une erreur de rang $Rg(e \mid \mathbb{F}_q) = r$, $e = (e_1, e_2, \cdots, e_n)$

De support $E = \{E_1, \cdots, E_r\}$ tel que $e_i = \sum_{j=1}^{r} e_{ij} E_j$

Supposons que le mot y reçu soit $y = c + e = (P_c(g_1) + e_1, \cdots, P_c(g_n) + e_n)$.

E est un sous espace vectoriel de $\mathbb{F}_{q^n}$ de dimension r ; ce qui entraine qu'il existe un unique polynôme

monique Q de degré r s'annulant sur E (***proposition 1.3)*** . Ainsi, déterminer Q revient à déterminer E. On peut écrire y comme un $q-$polynôme Y de degré au plus n , $Y = \sum_{i=0}^{n-1} Y_i X^{q^i}$ de sorte que $y_i = Y(g_i)$ $1 \leq i \leq n$.

Puisque Q s'annule sur E , on a $Q \circ Y = Q \circ P_c + 0$ sur E .

Or $Q \circ P$ est de q-degré $r+k-1$. Ce implique $\deg_q(Q \circ Y) \leq r+k-1$. Ainsi les $n-(k+k)$ coefficients des puissances de $Q \circ Y$ correspondant aux X^{q^i} où $i \geq r+k$ sont nuls.

On est donc ramener à résoudre $n-(r+k)$ équations à r inconnues (les Y_i) et cette résolution est possible si $r \leq n-(r+k)$; c'est-à-dire $r \leq \dfrac{m-k}{2}$ □

approche de Pierre Loidreau - Cedric Faure

À cause de leurs structure, on sert de plus en plus de la reconstitution des polynômes linéaires pour décoder les codes de Gabidulin. C'est dans ce sens que **Pierre Loidreau** propose dans [21] un algorithme de décodage pour les codes de Gabidulin, s'inspirant de celui de **Berlekamp - Welch** pour les codes de **Reed Salomon** par reconstruction du polynôme de position d'erreurs du mot reçu. D'après d'après **Cédric Faure**([2] page **80 - 83**), ce problème est difficile à résoudre au delà de la capacité de correction du code de Gabidulin **Gab(g,k,n)** qui est $\lfloor \dfrac{n-k}{2} \rfloor$ *(puisqu'ils sont **MDR**).* Ce qui justifie d'avantage leur utilisation en cryptographie.

Le problème en question s'énonce comme suit :

Étant donné un code $C = \mathbf{Gab}(g,k,n)$ sur $\mathbb{F}_{q^N}$, $t \in \mathbb{N}$ et y un mot code de $\mathbb{F}_{q^N}^n$, comment trouver tous les couples (Q,P) de polynômes linéaires non nuls tels que $deg_q(Q) \leq t$, $\quad deg_q(P) \leq k-1$ vérifiant $Q(y_i) = Q \circ P(g_i)$ $1 \leq i \leq n$?

Dans la suite , on utilisera la notation **RPL(y,g,k,t)** pour désigner le problème de reconstitution de polynômes linéaire associé au code $C = \mathbf{Gab}(g,k,n)$ sur $\mathbb{F}_{q^N}$.

Proposition 2.9. .

*Les polynômes linéaires P pour lesquels il existe Q tel que (Q,P) est solution de **RPL**(y,g,k,t) sont exactement ceux associés à un mot de **Gab**(g,k,n) dont la distance à y est inférieur ou égale à t.*

Preuve. .

⇒) Si (Q,P) est solution de **RPL**(y,g,k,t) , alors pour $i = 1, 2, \cdots, n$ on a $Q(y_i) = Q \circ P(g_i)$.
Posons $e_i = y_i - P(g_i)$. Il suit que $vect(e_1, e_2, \cdots, e_n) \subseteq Ker(Q)$
D'après la proposition 1.3 , $dim\ vect(e_1, e_2, \cdots, e_n) \leq \dim\ Ker(Q) \leq t$
donc $Rg(e \mid \mathbb{F}_q) \leq t$. D'où $d(y, P(g)) \leq t$

$\Leftarrow$) Réciproquement, si $y = P(g) + e$ avec $Rg(e \mid \mathbb{F}_q) \leq t$ alors grâce à la proposition 1.3 il existe un q-polynôme V non nul de q-degré plus petit que t tel que $V(e_i) = 0$, ce qui implique $V(y_i) = V \circ P(g_i)$

Donc (V, P) est solution de **RPL**(y,g,k,t) .

□

La résolution du problème **RPL**(y,g,k,t) conduit donc à une équation de la forme

$$V(y_i) = V \circ P(g_i) \quad 1 \leq i \leq n \tag{2.2}$$

où $deg_q(V) \leq t$, $\quad deg_q(P) \leq k-1$

À ce sujet, **Cédric FAURE** propose dans [2] page **80-85** une méthode de résolution de l'équation 2.2 :

- on pose $M = V \circ P$.

  L'équation 2.2 devient

  $$V(y_i) = M(g_i) \quad 1 \leq i \leq n,\ V \neq 0 \tag{2.3}$$

  dont les inconnues sont $V(X) = \sum_{i=0}^{t} v_i X^{[i]}$ et $M(X) = \sum_{i=0}^{k+t-1} m_i X^{[i]}$ *(on peut se référer à la proposition 1.2)*

  Attention ! toute solution du problème **RPL**(y,g,k,t) est solution de l'équation 2.2 mais la réciproque n'est pas toujours vraie .

- On pose $\mathcal{V} = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_t \end{pmatrix}$, $\mathcal{M} = \begin{pmatrix} m_0 \\ m_1 \\ \cdots \\ m_{k+t-1} \end{pmatrix}$, $\mathcal{S} = \begin{pmatrix} g_1 & g_1^q & \cdots & g_1^{[k+t-1]} & -y_1 & -y_1^{[1]} & \cdots & -y_1^{[t]} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n & g_n^{[1]} & \cdots & g_n^{[k+t-1]} & -y_n & -y_n^{[1]} & \cdots & -y_n^{[t]} \end{pmatrix}$

  Ces notations permettent de traduire le système 2.3 sous forme matricielle

  $$\mathcal{S} \times \begin{pmatrix} \mathcal{M} \\ \mathcal{V} \end{pmatrix} = 0 \tag{2.4}$$

  Les solutions de 2.4 forment un $\mathbb{F}_{q^N}$-espace vectoriel F.

  Trois cas se distinguent suivant la dimension de F :

  Si dim(F) = 0 alors le vecteur nul est la seule solution de l'équation 2.4. Ce qui conduit au polynôme nul. Or V doit être non nul.

  Il suit que **RPL**(y,g,k,t) n'a pas de solution si **dim(F) = 0**

Si dim(F) = 1 Pour avoir une solution au problème **RPL**(y,g,k,t) , on choisit un élément $\begin{pmatrix} \mathcal{M} \\ \mathcal{V} \end{pmatrix}$ de F et on effectue la division euclidienne à gauche. On obtient $M = V \circ Q + R$. Si $R \neq 0$ alors **RPL**(y,g,k,t) n'a pas de solution. Par contre, si $R = 0$, on déduit que **RPL**(y,g,k,t) admet comme solution le couple (V, Q)

Si dim(F)$= s \geq$**2** le système 2.4 a q^{Ns} solution dont certaines n'ont à priori rien à voir avec celle de **RPL**(y,g,k,t) . La meilleur solution est d'essayer $q^{N(s-1)}$ solution non colinéaires et de regarder lesquelles sont solution de **RPL**(y,g,k,t) .

⋆ ⋆ Chapitre Trois ⋆ ⋆

Application des codes rangs à la cryptographie

Le mot **cryptographie** vient du mot « Cruptos » qui signifie *caché* et « Grapein » qui signifie *écrire* . Elle peut se définir comme la science qui utilise les mathématiques, plus précisément **l'algèbre** pour dissimuler des données. La cryptographie permet ainsi de sécuriser les informations, quitte à pouvoir les véhiculer à travers les réseaux douteux tels que l'Internet, de façon à ce qu'elles ne puissent être reçues et déchiffrer par nul autre que le destinataire.

C'est une science qui évolue sans cesse avec les avancées technologiques. De nos jours, elle est devenue un outil incontournable dans la **sécurité informatique** et englobe diverses structurations constituant les cryptosystèmes 3.1.2.

Dans le cadre de notre travail, nous avons évoqué quelques uns de ces cryptosystèmes ,tout en accordant une atention particulière ceux mettant en jeux les codes rang tel que le cryptosystème de **GPT**.

3.1 Les fondements de la cryptographie

Définition 3.1.1 (**Chiffrement**). .

On appelle chiffrement le procédé qui consiste à dissimuler un message clair ***plaintext***[1] *de façon à cacher sa substance*[2] *. Dans le langage courant, on parle de cryptographie de données. Logiquement, le chemin inverse qui permet de passer du texte* ***chiffré*** *au texte clair est appelé* ***déchiffrement****.*

Le texte chiffré est appelé ***cryptogramme*** *ou* ***cyphertext***

Définition 3.1.2 (**Cryptosystème**). .

Un cryptosystème est l'ensemble formé par un algorithme cryptographique, toutes les clés possibles et

1. **message clair ou plaintext** : qui peut être compris sans aucune ambiguïté 2. **substance** : son contenu, sa véritable interprétation ou signification

tous les protocoles[3] *qui le font fonctionner.*

C'est en fait la donnée d'un 5-uplet $(\mathcal{M},\ \mathcal{C},\ \mathcal{K},\ \mathcal{D}_{\mathcal{K}},\ \mathcal{E}_{\mathcal{K}})$ *où*

- $\mathcal{M}$ *est l'ensemble des messages clairs*
- $\mathcal{C}$ *ensemble des messages cryptés*
- $\mathcal{K}$ *ensemble des clés*
- $\mathcal{E} = \{\mathsf{E}_k\ :\ \mathcal{M} \longmapsto \mathcal{C},\ k \in \mathcal{K}\}$ E_k *est une fonction de chiffrement de clé* k.
- $\mathcal{D} = \{\mathsf{D}_l : \mathcal{C}\ \longmapsto\ \mathcal{M},\ l \in \mathcal{K}\}$ D_l *est une fonction de déchiffrement de clé* l.
- *À chaque clé de cryptage* $c \in \mathcal{K}$*, est associé une clé de déchiffrement* $d \in \mathcal{K}$ *tel que* $\mathsf{D}_d(\mathsf{E}_c(m)) = m \quad \forall m \in \mathcal{M}$

3.2 Cryptosystème symétriques - cryptosystème à clés sécrètes

La cryptographie revêt deux principaux types de protocoles à savoir les **cryptosystèmes symétrique** et les **cryptosystème à clé publique**.

3.2.1 cryptosystèmes symétrique

Un cryptosystème est dit symétrique lorsque à tout clé de chiffrement e, la clé de déchiffrement d peut être facilement calculé à partir de e.

Dans un tel cryptosystème, la clé e doit être cachée pour éviter que n'importe qui connaissant e ne puisse obtenir la clé de déchiffrement.

Exemple 3.2.1. .

- **Le cryptosystème de césar**.

  Ici $\mathcal{M} = \mathcal{C} = \{\mathsf{A},\ \mathsf{B},\ \cdots,\ \mathsf{Z}\}$, $\mathcal{Z} = \{0,\ 1, \cdots,\ 25\}$.

  Chaque lettre correspond à un entier modulo 26 : $\mathsf{A} \to 1,\ \mathsf{B} \to 2,\ \cdots,\ \mathsf{Z} \to 25$

  $E_e\ :\ \mathcal{M}\ \longrightarrow\ \mathcal{M}$ $\qquad$ $D_e\ :\ \mathcal{M}\ \longrightarrow\ \mathcal{M}$

  $x\ \longmapsto\ x + e\ mod(26)$ $\qquad$ $x\ \longmapsto\ x + e\ mod(26)$

- **cryptosystème DES**[4](Data Encryption Standard)

3. **Protocole** : ensemble des messages clairs, des messages cryptés, des clés possibles 4. DES : *Il à été publié en 1975 Il et adopté par le NBS en 1977 comme standard de cryptage pour les applications non classifiées. Il reprend les principes et une partie du système de cryptage d'IBM dénommé LUCIFER.*

✪ **AES**[5] :(Advanced Encrytion Standard) ; c'est une version améliorée du **DES**

(réf [27] **page 96-99**)

Remarque 3.2.1. .

Ce type de chiffrement à l'avantage d'être très rapide. Il est particulièrement utile pour chiffrer des données qui ne vont aller nulle part.

Cependant, utilisé comme moyen de transmission des données sécurisées peut être onéreux simplement en raison de la difficulté de la distribution des clés.

3.2.2 Cryptosystèmes à clés publique

Pour pallier aux problèmes évoqués dans la remarque ci-dessus, l'on préfère utiliser les cryptosystème à clé publique. Ces types de cryptosystèmes ont été mis au point par **Whitfield Diffie** et **Martin Hellman** en 1975 .

La sécurité que procure les cryptosystèmes à clés publique réside dans le fait qu'il est mathématiquement impossible de déduire une clé de déchiffrement à l'aide d'une clé publique. Cependant, cette impossibilité est assez relative ! vu que parfois, elle dépend de la puissance de calcul des machines utilisées pour attaquer le cryptosystème.

Comme exemples de cryptosystème à clé publique, on peut citer le Elgamal[6], le cryptosystème RSA[7] , le cryptosystème Diffle-Nellmann[8], le cryptosystème DSA[9]

(réf [27], page **101-109**)

Pour augmenter la sécurité dans les cryptosystème à clé publique, l'on utilise parfois les **chiffrements randomisés** [12]. En effet , les cryptosystème à clé publique sont le plus souvent utilisés pour chiffrer n'importe quel message. Il est donc nécessaire d'introduire un aléa pour que les chiffrements différents d'un message en clair fixé ne produisent jamais deux cryptogramme identique, bien qu'on ait utilisé la même clé de chiffrement.

Définition 3.2.1 (**Chiffrement par blocs**). *Un protocoles est dit à chiffrement par blocs si son espace des clés et son espace des messages en clair sont tous deux constitué de mots de code de longueur n fixée .*

5. AES *de J. Daemen et V. Rijmen, basé sur le même principe que le DES avec une clé plus longue (128 à 256 bits), plus structuré et avec des fonctionnalités plus étendues. AES a été retenu en 2000 après un appel d'offre international.*

6. cryptosystème Elgamal :*du nom de l'inventeur* **Tasher Elgamal** 7. RSA : **Ron Rivest - Adi Shamir - Leonard Aldeman** 8. le cryptosystème Diffle-Hellmann : nommé ainsi à cause de ses inventeurs **Diffle** et **Hellmann** 9. le cryptosystème DSA : *Digital Signature Algorithm* par **David Kravitz**

Ce type de chiffrement est souvent couplé avec une fonction de ***Hachage*** *permettant de fragmenter un message clair de longueur quelconque sur un alphabet donné en une succession de message de longueur identique* $n \in \mathbb{N}$.

La documentation relative aux fonctions de **Hachage** se trouve dans [9]

3.3 Principe de certaines attaques en cryptographie

Tout d'abord, rappelons la règle de **Kerckhoff** qui stipule que la ***la sécurité du cryptosystème repose sur le secret des clés et non celui des algorithmes de chiffrement*** . En fait il est inutile de dissimuler le cryptosystème utilisé car avec les avancés technologiques actuelles, un pirate peut toujours le connaître par simple analyse d'un cryptogramme intersecté.
Pour cette raison, nous supposerons dans cette section que l'attaquant connait le cryptosystème utilisé.
Les types d'attaques les plus courantes sont :

Attaque sur texte chiffré ou**attaque brutale**

Cette attaque est la plus « faible » [10] en générale. Ici l'attaquant connait un cryptogramme. À partir de ce cryptogramme il essaie successivement toutes les clés possible et recherche le **plaintext** parmis les résultats obtenu et ayant un sens pour lui.

Une façon de faire face a ce type d'attaque est d'augmenter la **longueur** [11] de la clé secrète.

Exemple 3.3.1 (réf [27]). .

Pour une clé de **64 bits**, il existe $1.844 * 10^{19}$ combinaisons différentes. Sur un ordinateur calculant un milliard de clés par seconde il faudra **584** ans pour être sûr de trouver la clé

Attaque à clair connu

L'attaquant a à sa disposition un plaintext et le cryptogramme associé ; il s'en sert pour essayer de déchiffrer d'autre cryptogrammes.

Attaque à clair choisi

L'attaquant chiffre des messages de son choix ; mais ignore la clé de déchiffrement. Il essaye donc de déchiffrer ses propres cryptogrammes.

Pour avoir une liste plus détaillée, se référer à [12] ou [27] page 90

10. c'est une notion assez relative, car elle dépend de la puissance de calcul de l'attaquant. 11. **Longueur de la clé** :*une clé d'une longueur de* ***128*** *bits oblige par exemple l'attaquant à tester exactement* $2^{128} - 1$ *combinaisons possibles au pire des cas*

3.4 sécurité en cryptographie

Selon les normes internationale, un « bon » protocole cryptographique doit satisfaire les conditions suivantes :

☞ **Assurer la confidentialité**

Un cryptosystème devrait être imperméable à la divulgation du contenu de l'information transitant sur le canal.

☞ **Assurer l'intégrité**

L'information reçu ne devrait avoir été transmis par nul autre que son auteur véritable.

☞ **La non-répudiation**

On distingue trois niveaux pour la propriété de non répudiation :

- ***non-répudiation d'origine***
  l'émetteur ne peut nier avoir écrit le message
- ***non-répudiation de réception***
  le receveur ne peut nier avoir reçu le message.
- ***non-répudiation de transmission***
  l'émetteur du message ne peut nier avoir envoyé le message.

☞ **Authentification**

Il s'agit ici de pouvoir être en mesure d'identifier des personnes lors d'un échange de données et de certifier leurs identités.

3.5 Cryptosystème basé sur la métrique rang : Le cryptosystème GPT

Le cryptosystème **GPT** est l'une des premières implémentations de la métrique rang en cryptographie. C'est une adaptation à la métrique rang du cryptosystème de **Mc Eliece**. Il a été mis au point par **Gabilin**, **Paramonov** et **Tretjakov** en **1991**(dans [6]). Comme la plupart des cryptosystème il fait l'objet de diverses attaques structurelles telle que les attaques de **Gibson**[13] ou celles **d'Overberck**[24], poussant la communauté scientifique en général, et ses concepteurs en particulier à l'améliorer incessamment. Ainsi **Gabidulin** et **Ourivski** présentent dans [8] une version

généralisé du cryptosystème, utilisant une matrice de distorsion dont le but est de brouiller le plus possible la clé sécrète, rendant ainsi le système plus résistant aux attaques sus évoquées.

3.5.1 Présentation du cryptosystème GPT

Génération de la clé publique

$k,\ n,\ N$ sont dans $\mathbb{N}$, $k \leq n \leq N$ et $g = (g_1, g_2, \cdots, g_n) \in \mathbb{F}_{q^N}^n$ tel que $\{g_1, g_2, \cdots, g_n\}$ est une famille libre sur $\mathbb{F}_q$.

La clé publique est notée G_{pub} et est donnée par la formule

$$G_{pub} = SG_kP \tag{3.1}$$

La matrice G_k est donnée par $G_k = \begin{pmatrix} g_1 & g_2 & \cdots & \cdots & g_n \\ g_1^q & g_2^q & \cdots & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & \cdots & g_n^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & \cdots & g_n^{q^{k-1}} \end{pmatrix}$

S est une matrice carrée de taille $k \times k$ sur $\mathbb{F}_{q^N}$ est appelé la matrice brouilleuse de lignes.

Elle est utilisée pour détruire toute structure visible de la matrice G_k par mixage de lignes.

$P = [p_{ij}]$ joue le même rôle que la matrice S mais plutôt sur les colonnes de G_k. Elle est de taille $n \times n$ et à carré non singulière ($P^2 \neq I$).

Si P est une matrice à entrées dans $\mathbb{F}_q$, alors G_kP a la même structure que la matrice G_k avec une première ligne différente de celle de G_k. Dans ce cas, il y a équivalence entre les clés publique $G_{pub} = SG_kP$ et $G'_{pub} = SG_k$. La matrice P est donc facultative.

Par contre, si les entrées de la matrice P sont dans $\mathbb{F}_{q^N}$ alors les matrice G_k et G_kP ont des structures différentes ; ce qui rend le décryptage un peu plus difficile, augmentant ainsi la sécurité du système.

Suite aux attaques de **Gibson** et d' **Overberck**, **Gabidulin** et **Ourivski** ont associé à la matrice G_k une matrice de **"distorsion"** X de taille $k \times t_1$, à entrée dans $\mathbb{F}_{q^N}$, et de rang t_1. La nouvelle clé publique est

$$G_{pub} = S[X|G_k]P \qquad ou\ bien \qquad G_{pub} = S[G_k|X]P \tag{3.2}$$

Cette fois si P est de type $(n + t_1) \times (n + t_1)$ à entrées dans $\mathbb{F}_q$ et à carré non singulier.

Résumé :

- Les clés publiques sont la matrice G_{pub} et la capacité de correction du code $(n-k)/2$
- La clé sécrète est la décomposition précise de G_{pub} . C'est-à-dire le quadruplet $(S,\ X,\ G_k, P)$

Le processus de chiffrement

Il est analogue à celui du système de **Mc Eliece** classique.

Étant donné un message m,

On génère une erreur aléatoire, e de rang $(n-k)/2$

On chiffre le message m en calculant $c = mG_{pub} + e$

Processus de déchiffrement

On suppose que le message reçu est effectivement $c = mG_{pub} + e$.

On effectue le calcule $cP^{-1} = (mS[G_k|X]P + e)P^{-1}$

En tronquant les t_1 dernières colonnes de cP^{-1} un algorithme de décodage du code C de matrice génératrice G_k, permet d'obtenir mS et par suite m.

3.5.2 Attaque structurelle sur le cryptosystème GPT

Comme nous l'avons mentionné plus haut, le cryptosystème GPT fait l'objet de diverse formes d'attaques. Plusieurs autres variantes du dit cryptosystème ont été développée pour contrer l'attaque de Gibson. Dans [26] **Berger** et **Loidreau** propose l'utilisation d'un sous-code d'un code de Gabidulin. A. V. Ourivski, E. M. Gabidulin, B. Honary, et B. Ammar proposent dans [1] l'utilisation de code rang réductibles combinés à une matrice de distorsion.

L'attaque d'Overbeck sur le système GPT

C'est l'une des attaques structurelles la plus célèbre sur le cryptosystème **GPT**. Elle fut conçue et présenté par **Raphaël Overbeck** dans [24]. Cette célébrité vient du fait que, le principe de la dite attaque peut être généralisé à tout système utilisant les codes de Gabidulin, puisqu'il est basé sur les propriétés intrinsèque de ces types de codes . Les détails relatifs à l'attaque d'Overbeck se trouve dans [2] page **90-95** ou bien dans [24].

L'attaque d'Overbeck n'est pas insurmontable. En effet grâce aux travaux de issus de [1], [10] ou de [2], on peut très bien s'en prémunir

- ✔ Par augmentation de la taille des paramètres du système
- ✔ par conception de système basé sur le problème de reconstitution des polynômes linéaires

♠ PORTÉE PÉDAGOGIQUE ♠

On peut se demander en quoi est-ce que le travail que nous avons effectué est utile à l'enseignement au lycée ?

En allégeant un peut le savoir savant qui se trouve dans ce mémoire, on peut utiliser les connaissances qui y sont développées pour :

- L'enseignement de l'algèbre au lycée ; par exemple ,
  - les notions sur lois de composition internes des groupes
  - édifier d'avantage les élèves sur les cas spécifiques de l'anneau des polynômes à coefficients dans $\mathbb{R}$ et par suite sur l'anneau des polynômes à coefficients dans $\mathbb{C}$ en classe de b**Tle**.
  - Introduire quelques éléments fondamentaux sur le concept des corps finis.

Pour ce qui est du volet cryptographie de notre travail, nous pensons qu'elle pourrait aussi être utile aux élèves du lycée.
En effet les jeunes sont de plus en plus en contact avec internet, soit pour effectuer les recherches ou pour communiquer à travers les réseaux sociaux.
Il serait prudent de commencer à les édifier sur les bases de la cryptographie et surtout des dangers qui les guettes tels que l'usurpation d'identité ou bien le piratage de boites e-mail etc $\cdots$
Par ailleurs, vu qu'en classe de Tle, les élèves ont déjà quelques connaissances en programmation « **WEB** » (conception des fichiers **html**), on peut aussi les initier dans leurs cours d'informatique au chiffrement des mots de l'alphabet français avec des exemples basiques comme le chiffrement de César ou bien le chiffrement par permutation des lettres de l'alphabet.

♠ Conclusion ♠

Dans le cadre de notre travail, après un rappel sur la théorie des anneaux, des corps finis, des polynômes linéaires et sur la théorie du codage, nous avons principalement explicité les codes rang, leurs propriétés et quelques méthodes d'encodage et de décodage à l'aide de ces types de codes. Ceci nous a conduit à l'étude d'une classe particulière de codes rang, **les codes de Gabidulin** et le cryptosystème associé qui est le **cryptosystème GPT**.

Bien qu'assez novice dans ce vaste océan de connaissance que revêt la cryptographie en général et celle basée sur la métrique rang en particulier, notre étude du cryptosystème GPT standard nous a montré une certaine vulnérabilité face à certaines attaques structurelles, surtout celle **d'Overbeck**. Cependant le cryptosystème GPT est sans cesse en évolution ; de nos jours, il existe une riche documentation à ce sujet et l'on observe depuis quelques années des versions meilleurs de ce cryptosystème grâce aux travaux d'auteurs tels que Philippe Gaborit, Olivier RUATTA, Gille ZEMOR et Gaetan MURAT, sur le problème **RPL** ou bien sur les codes **low rank parity check (LRPC**) avec des algorithmes de décodage probabilistes performants.

Tout en évitant une comparaison frontale avec la métrique de Hamming, nous pensons que la métrique rang semble être une alternative intéressante pour la cryptographie basée sur les code correcteurs , car elle à la propriété de neutraliser les attaques par ensemble d'information comme le montre les travaux de **Gabidulin**, **Paramonov** et **Tretjakov** dans [7].

Notons que, l'implémentation des codes rang en informatique semble encore assez ardue. De plus les seuls codes connus , facilement déchiffrables dérivent des codes de Gabidulin. Ainsi pour explorer d'avantage la métrique rang, il serait nécessaire de se diversifier et de mettre à jour d'autres familles de codes rang complètement différents. En outre, le décodage optimal des codes rang en générale et des codes de Gabidulin en particulier constituent à l'heure actuelle un véritable chalenge dans le domaine de la cryptographie et une piste recherche très prometteuse qui pourrait peut-être révolutionner ce domaine.

♠ Bibliographie ♠

[1] **A. V. Ourivski, E. M. Gabidulin, B. Honary,** and **B. Ammar.** Reducible rank codes and their applications to cryptography. *IEEE Transactions on Information Theory, 49(12) :3289–3293, 2003.*

[2] **Cédric FAURE** Études de systèmes cryptographiques construits à l'aide de codes correcteurs, en métrique de Hamming et en métrique rang *17 mars 2009*

[3] **Claude.E SHANNON** : Communication Theory of Secrecy Systems. Bell system technical journal, *28 :656–715, 1949.*

[4] **E.M GABIDULIN** : "Theory of codes with maximum rank distance",*Problems on Informatique Transmission, Vol 21, N° 1, PP. 1-12, Jan 1985.*

[5] **E.M Gabidulin** Theory of Codes with Maximal Rank Distance *Problems of Information Transmission, 21 :1–12, July 1985.*

[6] **E .M. Gabidulin, A. V. Paramonov,** and **O. V. Tretjakov.** Ideals over a Non-Commutative Ring and their Application in Cryptology. *LNCS, 573 :482 – 489, 1991.*

[7] **E.M Gabidulin**,**A.V Paramonov**, **O.V Tretjakov** Ideals over a non Commutative Ring and their Application in cryptologie. *EUROCRYPT 1991, PP : 482-489*

[8] **E. M. Gabidulin** and **A. V. Ourivski**. Modified GPT PKC with Right Scrambler. *In Daniel Augot and Claude Carlet, editors, Proceedings of the 2nd International workshop on Coding and Cryptography, WCC 2001, pages 233–242, 2001.*

[9] **Fouque Pierre-Alain**, Fonctions de Hachage *Avril 2014*

[10] **Gaetan Murat.** Résultants de polynômes de Ore et Cryptosystèmes de McEliece sur des Codes Rang faiblement structurés. *Ordinateur et société [cs.CY]. Université de Limoges, 2014. Fran¸cais. <NNT : 2014LIMO0061>. <tel-01161777>*

[11] **HAMMING** Error Detecting and Error correcting Codes. *Copyright, 1950, American telephone and telegraph company*

[12] ; **Johannes Buchman** Introduction à la cryptographie

[13] **J. K. Gibson**. Severely Denting the Gabidulin Version of the McEliece Public-Key Cryptosystem. *Designs, Codes and Cryptography, 6 :37–45, 1995.*

[14] **Maximilien Gadouleau** and **Zhiyuan Yan**- Department of Electrical and Computer Engineering *Lehigh University, PA 18015, USA E-mails : magc, yan@lehigh.edu*

[15] **Nicolas BRUYÈRE** : Élément de la théorie des corps fini : application aux codes correcteurs, *Université de Rouen Agrégation de mathématiques 2005-2006*

[16] **Loo-Keng** "A theorem on matrices over a sfield and its applications ", *Chinese mathematical society, vol 1, N° 2, PP 109-163, year 1951*

[17] **O. Ore**. On a special class of Polynomials. *Transactions of the American Mathematical Society, 35 :559–584, 1933.*

[18] **O. Ore**. Contribution to the theory of finite fields. *Transactions of the American Mathematical Society, 36 :243–274, 1934.*

[19] **Ourivski And Johanson** New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications. Problems of Information Transmission, 38(3) :237–246, *September 2002..*

[20] **Philippe GABORIT** Introduction to rank-based cryptography *University of Limoges, France 2013*

[21] **P.Loidreau**- Métrique rang et cryptographie*mémoire d'HDR, 2007*

[22] **P.Loidreau** -Properties of Codes in Rank Metric,*http ://arxiv.org/qbs/cs /0610057*

[23] **P. Delsarte**, "Bilinear Forms over a Finite Field, with Applications to Coding Theory", *Journal of Combinatorial Theory A, vol. 25 PP.226-241,1978*

[24] **R. Overbeck**. Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes. *Journal of Cryptology, 21 :280–301, 2008.*

[25] **RAYMOND HILL** : A first Course in Coding Theory. *University of Salford, 1986*

[26] **T. P. Berger** and **P. Loidreau**. How to Mask the Structure of Codes for a Cryptographic use. *Designs, Codes and Cryptography, 35 :63–79, 2005.*

[27] **Yves Denneulin, Jean-Guillaume Dumas, Gregory Mounié, Jean-Louis Roch** :THEORIE DES CODES(Compression, cryptage, Correction),*2005*