REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET
DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
Faculté de Mathématiques

THESE
Présenté pour l'obtention du diplôme de DOCTORAT
EN: MATHEMATIQUES
Spécialité : Algèbre et Théorie des Nombres
par

GUENDA KENZA

SUR L'EQUIVALENCE DES CODES

Soutenue publiquement, le 22/04/2010 devant le jury composé de :

Mr. Benali BENZAGHOU	Prof.	USTHB	Président
Mr. Lemnouar NOUI	Prof.	Université de Batna	Directeur de thèse
Mr. Thierry BERGER	Prof.	Université de Limoges	Examinateur
Mr. Albdelhafid BERRACHEDI	Prof.	USTHB	Examinateur
Mr. Hacène BELBACHIR	MCA	USTHB	Examinateur
Mr. Farid BENCHERIF	MCA	USTHB	Examinateur
Mr. Sadek BOUROUBI	Prof.	USTHB	Examinateur
Mr. Toufik ZAIM	MCA	Université de Oum-Bouagui	Examinateur

Résumé

Cette thèse nous a permis de résoudre certains problèmes ouverts [2, 12] et de donner des solutions partielles à certains problèmes NP-durs en théorie des codes [25]. Nous donnons explicitement le nombre des codes cycliques. Ce nombre est nécessaire pour analyser l'efficacité de l'algorithme d'équivalence des codes cycliques proposé par Skersys [65]. Nous avons déterminé les propriétés des classes cyclotomiques, grâce auxquelles nous avons pu donner la dimension d'une classe de code BCH intéressante [49]. Nous avons donné des bornes optimales pour la distance minimale de ces codes, et dans certains cas nous l'avons calculée. En utilisant nos résultats nous avons donné de nouvelles tables pour la distance minimale. Cette partie a fait l'objet d'une publication parue [31]. Nous avons caractérisé les codes affine-invariants maximaux. C'est la réponse à la question ouverte posée par T. P. Berger [12]. Nous avons aussi répondu à la question ouverte posée par Aly et al. [2] sur l'existence des splitting, lorsque l'ordre multiplicatif de q modulo n est pair. Dans la deuxième partie de cette thèse, nous nous sommes intéressés au lien existant entre les codes classiques et les codes quantiques. La théorie des codes quantiques est une nouvelle discipline en pleine évolution. Grâce à ce lien nous avons construit de nouvelles familles de codes BCH quantiques, de codes Affine-

invariants quantiques et de codes duadiques quantiques. Certaines familles construites sont trés intéressantes du point de vue correctabilité. Nous donnons aussi de nouvelles tables de codes quantiques. Une partie de ce travail a fait l'objet d'une autre publication parue [32].

Remerciements

Je suis en premier lieu redevable à Lemnouar Noui pour le choix judicieux du sujet de cette thèse, pour le respect et la confiance qu'il a montré à mon égard, ainsi que pour les nombreux courriels de sa part qui ont orienté, corrigé mes recherches et m'ont encouragé malgrès la distance qui nous séparait.

Je n'ai pas eu l'occasion de remercier Benali Benzaghou pour m'avoir fait découvrir le monde magnifique de la théorie des nombres, à travers ses cours de graduation et post-graduation. Je souhaite lui exprimer toute ma gratitude pour cela et pour m'avoir fait l'honneur de présider le jury de cette thèse.

Je remercie Thierry P. Berger pour m'avoir accueilli au sein de son équipe, pour sa grande disponibilité, ses encouragements, ainsi que pour avoir toujours répondu à mes questions.

Je remercie également Haçane Belbachir pour ses encouragements et pour avoir accepté de faire partie des membres de jury de cette thèse.

C'est un grand honneur pour moi d'avoir parmi les membres de jury de cette thèse Farid Bencherif, un brillant enseignant dont je garde une image extraordinaire en tant qu'ancienne étudiante, mais aussi un aussi éminent chercheur algébriste.

Je remercie Abdelhafid Berrachedi pour avoir mis à ma disposition sa bibliographie personnelle sur la théorie des codes, pour sa gentillesse, ses discussions encourageantes et aussi pour avoir fait partie des membres de jury de cette thèse.

Je ne serais comment remercier Sadek Boroubi pour ses dicussions enrichissantes, pour son soutient, ses encouragements et pour avoir fait partie des membres de jury de cette thèse.

Je remercie Toufik Zaim pour l'honneur qu'il me fait en acceptant de faire partie des membres de jury de cette thèse et d'avoir accepté de se déplacer de Oum Bouagui, malgrés ses nombreuses préoccupations.

Un grand merci pour les membres du conseils scientifique Faculté de Mathématiques, USTHB, qui m'ont sélectionné pour finaliser cette thèse au sein de l'équipe PC12 Limoges qui n'a pu que m'être bénéfique sur le plan scientifique.

Un chaleureux merci à mes amies Isma Bouchemakh, Hafida Guerbyenne et Schahrazad Selmane pour leurs amitiés et pour m'avoir entrainé dans leur passion pour la recherche.

Je n'oublierai surtout pas de remercier tout le groupe d'enseignants et amis pour les divers discutions passionantes sur le chemin de nos classes.

Que notre personnel administratif ; Hafsa, Sabah, Djamila Karima, Hafida, Farida, Slimane et d'autres, trouvent l'expression de ma gratitude pour le travail qu'ils font.

Je ne pourrais oublier de remercier mes amis du DMI Limoges, Abdelkader Necer, Idriss Boularasse, François Laubie, François Arnault, Aurore Bernard, Sinaly Traoré, Christophe Chabot et Katherine pour leur gentillesses

et discussions enrichissantes.

Je suis redevable à mes amies de Limoges, Viviane Anglard, Halima Geoffroy, Meriem Heraoua et à leurs familles pour leurs amitiés et les moments de joie et plaisir partagés avec eux.

Enfin je remercie vivement mes amies, Souhila, Fatiha, Fadila, Baya, Naima, Rachida, Zahra, Malika, Samia, Nawel, Lila, Ouahiba, ...pour leurs complicités et pour avoir toujours partagé avec moi les moments de joie ainsi que les moments difficiles.

Que tous les membres de ma famille trouvent l'expression de mon affection et ma gratitude pour leur amour, leur confiance, leurs encouragements et leur soutients.

Merci enfin à tous ceux que j'ai omis. Qu'ils veuillent bien me pardonner cet oubli !

Kenza Guenda

Table des matières

Notations

$\mathbb{F}_q$ =: Le corps fini à q éléments.

$\min(E)$ =: Le plus petit élément de E.

Pour a et $b \in \mathbb{N}$ et p un nombre premier,

$p^a//b$ =: a est la plus grande puissance de p qui divise b.

$\mathbb{Z}_n$ =: $\mathbb{Z}/n\mathbb{Z}$.

C_i =: La $i$ème classe cyclotomique mod n.

$ppcm(a, b)$ =: Le plus petit commun multiple de a et b.

$[n]$ =: L'ensemble $\{1, \ldots, n\}$.

$q \equiv \square \mod n$ =: q est un résidu quadratique modulo n.

$\phi(.)$ =: La fonction indicatrice d'Euler.

S_n =: Le groupe symétrique d'un ensemble à n éléments.

Introduction

We know accurately only when we know little,

with knowledge doubt increase.

J. W. Von Goethe

Les codes correcteurs d'erreurs sont des objets qui sont proposés comme solution aux problèmes de transmission sur un canal à bruit. Dans le cas classique, l'émetteur, le receveur et le canal sont des entités classiques et dans le cas quantique ce sont des entités quantiques.

Les codes cycliques qui sont étudiés dans cette thèse sont parmi les plus anciens codes, les plus étudiés et les plus utilisés en pratique. Leur fiabilité est dûe à leur grand pouvoir de correction et à l'existence d'algorithmes efficaces pour les décoder. Malgré cela, plusieurs de leurs propriétés sont restées inconnues [19]. Dans cette thèse nous nous sommes intéressés à déterminer certaines de ses propriétés. L'étude de ces propriétés et le lien qui existe avec les codes quantiques nous a permis de construire de nouvelles familles de codes quantiques.

Il est bien connu que le problème de l'équivalence des codes est un problème aussi difficile que le célèbre problème d'isomorphisme des graphes [53]. Dans sa thèse [65] G. Skersys a proposé un algorithme pour déterminer l'équivalence

des codes cycliques, seulement l'efficacité de l'algorithme en question dépend essentiellement du nombre des codes cycliques. Ce nombre n'a été donné que dans un cas trés particulier dans [65]. Dans cette thèse nous donnons explicitement une forme plus générale que celle de Skersys pour ce nombre. Cela nous a été possible en utilisant certains résultats de la théorie des nombres élémentaire.

L'étude des propriétés des classes cyclotomiques nous a permis de déterminer les paramètres d'une classe de codes BCH intéressante, comme elle a été qualifiée par F. J. Macwilliams et N. J. A. Sloane [49]. Ce sont les codes BCH de longueur $n = p^m + 1$ avec $m > 1$. Bien que nous n'ayons considéré que les codes BCH au sens strict, il est à remarquer que nos résultats s'appliquent par une simple généralisation à certains codes $B_q(n, \delta, \alpha, b)$ au sens non-strict avec $n = q^m + 1$, $m > 1$, b et δ vérifiant $b + \delta - 2 < q$.

Le problème de la détermination de la valeur exacte de la distance minimale n'a pas été résolu pour plusieurs familles de codes, en particulier pour les codes BCH. Il a même été démontré par Dumer et al. [25] que l'approximation de la distance minimale des codes linéaires est un problème NP-dur. Nous avons donné des bornes optimales et dans certains cas nous avons donné la distance minimale exacte pour nos codes BCH [32]. Sans ces bornes, la recherche exhaustive pour trouver le mot de plus petit poids peut être inefficace et dans la plupart des cas impossible.

Dans la même optique, nous avons considéré la classe des codes affine-invariants. En construisant sur les travaux de T. P. Berger nous avons caractérisé les codes affines-invariants maximaux, considérés leurs dualités et calculé leur groupe de permutations.

La dernière classe des codes cycliques considérée est la classe des codes duadiques. Notre intérêt à cette classe vient de sa caractéristique intéressante de dualité et du lien qui existe avec les codes cycliques auto-duaux. Nous avons donné des conditions sur l'existence des splittings, qui alors a des déductions sur les problèmes de dualité pour ces codes ; spécialement l'existence des codes auto-orthogonaux dans le cas Euclidien et l'existence des splitting lorsque l'ordre multiplicatif de n modulo q est pair. Cette partie a été donnée comme réponse à la question ouverte posée par Aly et al. [2].

À cause de ses propriétés étranges, comme la superposition des états, le non-clonage, l'intrication, etc, on pourrait croire que la théorie quantique n'a rien à voir avec la théorie classique. Cependant ce n'est pas le cas ; à partir des codes classiques on peut toujours construire la machinerie mathématique pour la construction et l'analyse des codes quantiques et vis-versa [14, 20]. Cela a permis de montrer que les deux théories sont similaires. Nous avons tiré profit de ce lien existant entre les deux théories pour construire de nouvelles familles de codes quantiques de chacune des classes des codes cycliques citées précédemment. Certaines de ces familles sont trés intéressantes du point de vue capacité de correction.

Dans cette thèse, en plus de certains résultats qui n'ont pas encore été publiés (concernant le nombre de codes cycliques et les codes BCH quantiques) nous détaillons les articles [31, 32].

Au chapitre 1, nous rappelons les définitions et les propriétés élémentaires des codes linéaires.

Les codes cycliques ont fait l'objet du second chapitre. Nous avons commencé par le lien entre la factorisation de $x^n - 1$ et les racines n-ièmes de

l'unité, puis nous avons donné les propriétés des classes cyclotomiques. Nous avons rappelé les définitions concernant l'équivalence et le groupe de permutations, puis nous avons clôturé par des formules et des exemples qui donnent le nombre des classes cyclotomiques et donc le nombre des codes cycliques.

Dans le troisième chapitre nous avons introduit les définitions et les propriétés des codes quantiques, spécialement les codes stabilisés et la construction CSS. Ce procédé permet la construction des codes quantiques à partir des codes classiques d'une manière trés élégante.

Les codes BCH classiques et quantiques ont fait l'objet du quatrième chapitre. Dans ce chapitre nous avons déterminé en premier lieu la dimension des codes BCH classique, puis par généralisation des théorèmes de Farr et de Peterson [49] nous avons donné des bornes sur la distance minimale de ces codes, et dans certains cas nous avons calculé cette distance minimale. Grâce à la construction CSS ainsi que la propriété d'emboîtement des codes BCH, il nous a été possible de construire de nouveaux codes quantiques. Nous clôturons ce chapitre par des exemples de codes quantiques construits et par la comparaison avec les tables existantes concernant ce sujet.

Dans le cinquième chapitre nous caractérisons les codes affine-invariants maximaux. Comme le groupe de permutations est l'un des paramètres les plus importants d'un code, nous avons calculé le groupe de permutations de ces codes. La relation de dualité établie nous a permis de construire une nouvelle famille de codes quantiques.

Les codes duadiques ont fait l'objet du sisième chapitre. Nous commençons ce chapitre par des définitions et des préliminaires concernant ces codes, ensuite nous donnons des conditions sur l'existence des splitting et nous

construisons de nouveaux codes quantiques à partir de ces codes.

Pour alléger la littérature, nous avons rassemblé les outils mathématiques concernant la théorie des codes quantiques et la théorie de la complexité dans des appendices, où nous avons rappelé la théorie concernant les espaces de Hilbert, le produit tensoriel, comme nous avons redémontré d'une manière trés simple le théorème du non-clonage. Nous avons aussi introduit les notions de base de la théorie de complexité.

Nous clôturons ce manuscrit par une conclusion générale et des perspectives de cette thèse.

Chapitre 1

Les codes linéaires : définitions et propriétés

I don't consider this algebra, but this
doesn't mean that algebraists can't do it.
Garett Birkhoff

1.1 Les codes correcteurs d'erreurs

Dés 1946 Richard Hamming avait travaillé sur un modèle de calculateur à cartes perforées de faible fiabilité. Si, durant la semaine, des ingénieurs pouvaient corriger les erreurs, les périodes chômées comme les fins de semaines voyaient les machines s'arrêter invariablement sur des bogues. La frustration de Hamming le conduit à inventer le premier code correcteur véritablement efficace. Cette période correspond à la naissance de la théorie de l'information. Claude Shannon formalise cette théorie comme une branche

des mathématiques. Hamming développe les prémisses de la théorie des codes et décrit sa solution comme un exemple.

Les codes correcteurs d'erreurs sont un outil visant à améliorer la fiabilité des transmissions sur un canal bruité. La méthode utilisé consiste à envoyer sur le canal, plus de données que la quantité d'information à transmettre. Une redondance est ainsi introduite. Si cette redondance est structuré de manière exploitable, il est alors possible de corriger d'éventuelles erreurs introduites par le canal. On peut alors, malgré le bruit, retrouver l'intégralité des informations transmises au départ.

Définition 1.1.1 *Soit A un alphabet (souvent on considère les corps finis), et soit $\mathcal{A}$ l'ensemble des vecteurs formés à partir de A. Un code C est un sous ensemble de vecteurs de $\mathcal{A}$. Un élément de C est appelé mot du code.*

Dans la suite de ce chapitre nous introduisons les codes linéaires et leurs propriétés. Ces codes sont les plus intéressants et les plus utilisés en pratique. De plus ils sont étroitement liés à la construction des codes quantiques.

1.2 Les codes linéaires

Soit $\mathbb{F}_q$ un corps fini à q éléments. Tout sous ensemble C de $\mathbb{F}_q^n$ est appelé **code** de longueur n sur $\mathbb{F}_q$. On peut considérer $\mathbb{F}_q^n$ comme étant un $\mathbb{F}_q$-espace vectoriel de dimension n sur $\mathbb{F}_q$ et donc on peut considérer des sous espaces vectoriels de $\mathbb{F}_q^n$. Un sous espace vectoriel C de $\mathbb{F}_q^n$ de dimension k est appelé un $[n, k]$ **code linéaire**. Les vecteurs de C sont appelés **mots du code**.

La matrice G dont les lignes forment une base de C est dite **matrice génératrice** de C. Comme C est de dimension k et de longueur n, alors G

est de type $k \times n$. La matrice G définit complètement le code C du fait que :

$$C = \{\mathsf{x}G \,|\, \mathsf{x} \in \mathbb{F}_q^k\}.$$

On peut définir sur $\mathbb{F}_q^n$ une métrique $d(.,.)$ appelée **distance de Hamming**, dennée par :

$$d(\mathsf{x}, \mathsf{y}) = |\{i \mid x_i \neq y_i\}|,$$

où $\mathsf{x} = (x_1, \ldots, x_n)$ et $\mathsf{y} = (y_1, \ldots, y_n)$ sont des vecteurs de $\mathbb{F}_q^n$.

Le **poids de Hamming** d'un mot x qu'on note $w(\mathsf{x})$ est le nombre de coordonnés non nulles de x, i.e.,

$$w(\mathsf{x}) = d(\mathsf{x}, 0).$$

La **distance minimale** d'un code $C \subset \mathbb{F}_q^n$ est donnée par

$$d(C) = \min \{d(\mathsf{x}, \mathsf{y}) \,|\, \mathsf{x}, \mathsf{y} \in C, \mathsf{x} \neq \mathsf{y}\}.$$

Le **poids minimal** d'un code C est

$$\omega(C) = \min \{\omega(\mathsf{x}) \mid \mathsf{x} \in C, \mathsf{x} \neq 0\}.$$

Un $[n, k]$ code linéaire C de distance minimale d est appelé un $[n, k, d]$-code.

Remarque 1.2.1 *Pour un code linéaire la distance minimale et le poids minimal sont égaux.*

Il existe un lien important entre la capacité de correction d'un code linéaire et sa distance minimale ; il a été démontré (voir par exemple [49, Ch. 1]) qu'un code linéaire C de distance minimale d peut corriger jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs et détecter $d-1$ erreurs.

1.2.1 Les bornes sur les paramètres

Il existe quelques bornes et restrictions sur les paramètres d'un code ; soient la longueur, la dimension et la distance minimale. La plus simple des bornes, mais aussi la plus importante est la borne dite de **Singleton** :

$$k + d \leq n + 1. \tag{1.1}$$

La borne de Singleton est le cas linéaire pour la borne dite **Borne de Griesmer** donnée par le théorème suivant.

Théorème. 1.2.2 *([49] p. 547) Soit C un $[n, k, d]$ code sur $\mathbb{F}_q$, alors*

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil.$$

Puisque $\lceil d/q^0 \rceil = d$ et $\lceil d/q^i \rceil \geq 1$ pour $i \in [k-1]$, alors la borne de Griesmer implique celle de Singleton.

Une autre importante borne sur les paramètres et qui résoud l'un des problèmes les plus importants en théorie des codes ; pour n, k et d donnés est ce qu'il existe un $[n, k, d]$ code sur $\mathbb{F}_q$?

Le théorème suivant appelé **empilement des sphères** ou **borne de Hamming** donne la réponse.

Théorème. 1.2.3 *([36, théorème 1.12.1]) Pour des entiers n, k, d, il existe un $[n, k, d]$ code sur $\mathbb{F}_q$ dés lors que :*

$$q^k \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq q^n.$$

1.3 La dualité des codes linéaires

1.3.1 Le dual Euclidien

À chaque code linéaire C on peut associer un code linéaire donné par la définition suivante.

Définition 1.3.1 *Soit un code linéaire $C \subset \mathbb{F}_q^n$ de dimension k. Le* ***code dual Euclidien*** *ou simplement, code dual de C est l'orthogonal de C pour le produit scalaire usuel défini sur $\mathbb{F}_q^n \times \mathbb{F}_q^n$ par*

$$\langle \mathsf{x}, \mathsf{y} \rangle = \sum_{i=1}^{n} x_i y_i,$$

où $\mathsf{x} = (x_1, \ldots, x_n)$ et $\mathsf{y} = (y_1, \ldots, y_n)$. Ce code est noté $C^\perp$ et il est défini par

$$C^\perp = \{\mathsf{x} \in \mathbb{F}_q^n,\ \langle \mathsf{x}, \mathsf{y} \rangle = 0,\ \forall \mathsf{y} \in C\}.$$

Le code dual $C^\perp$ est un code linéaire de dimension $k^\perp = n - k$. Sa matrice génératrice H est appelée **matrice de contrôle de parité** de C, car elle vérifie :

$$C = \{\mathsf{x} \in \mathbb{F}_q^n \mid H\mathsf{x}^T = 0\}. \tag{1.2}$$

La distance minimale de $C^{\perp}$ est appelée distance duale et notée $d^{\perp}$.

1.3.2 Le dual Hermitien

Si on considère des codes sur $\mathbb{F}_{q^2}$, alors nous pouvons considérer le produit scalaire Hermitien. Le code dual par rapport à ce produit scalaire est un code linéaire noté par $C^{\perp h}$ et appelé **dual Hermitien**. Il est défini par :

$$C^{\perp h} = \{\mathsf{x} \in \mathbb{F}_{q^2}^n, \sum_{i=1}^{n} x_i y_i^q = 0\,, \forall \mathsf{y} \in C\}.$$

1.3.3 Les codes auto-duaux

Un code linéaire est dit **auto-orthogonal au sens Euclidien** s'il vérifie $C \subset C^{\perp}$. Il est dit **auto-dual au sens Euclidien** s'il vérifie $C = C^{\perp}$. Dans ce cas, C doit être un $[n, n/2]$ code avec n pair. Cette propriété vient du fait que pour un code linéaire C on a

$$\dim C + \dim C^{\perp} = n.$$

De ce qui précède, on en déduit qu'un $[n, k]$ code linéaire est auto-dual si et seulement s'il est auto-orthogonal avec $k = n/2$.

Un code linéaire est dit **auto-orthogonal au sens Hermitien** s'il vérifie $C \subset C^{\perp h}$. Il est dit **auto-dual au sens Hermitien** s'il vérifie $C = C^{\perp h}$.

1.4 L'étendu d'un code linéaire

À chaque code linéaire C on peut associer le code linéaire $\hat{C}$ définie par :

$$\hat{C} = \{(x_0, \ldots, x_n) \,|\, (x_1, \ldots, x_n) \in C \text{ tel que } x_0 = -\sum_{i=1}^{n} x_i\}.$$

Le code $\hat{C}$ est appelé code étendu[1] de C. Le code $\hat{C}$ est linéaire et admet pour paramètres $[n+1, k, \hat{d}]$ avec $\hat{d} = d$ ou $d+1$.

Dans le cas binaire, si d est impaire alors $\hat{d} = d + 1$.

[1]Cette façon d'étendre les codes est la plus usuelle. Cependant, il existe d'autres manières pour étendre un code de telle sorte à préserver certaines de ses propriétés, voir juste par exemple Huffman et Pless [36, lemme 6.6.17].

Chapitre 2

Codes cycliques, classes cyclotomiques et équivalence

In Galois Fields, full of flowers,
primitive elements dance for hours
climbing sequentially through the trees
and shouting occasional parities
S. B. Weinstein

2.1 Introduction

Comme les codes considérés dans cette thèse sont basés sur les codes cycliques, nous avons consacré ce chapitre à ces derniers. Nous avons énoncé des résultats donnés dans [36, 47, 49, 59, 65], et prouvé certains de nos résultats parus dans [31, 32] en vue de les utiliser dans les chapitres suivants. Nous considérons aussi dans ce chapitre le problème de l'équivalence des

codes et le nombre des codes cycliques.

2.2 La Factorisation de $x^n - 1$

2.2.1 Les racines n-ièmes de l'unité

Dans cette section on s'intéresse à la factorisation du polynôme $x^n - 1$; avec les codes cycliques de longueur n sur $\mathbb{F}_q$.

Soit $\mathbb{F}_q$ un corps fini de caractéristique p et $n = mp^h$, avec $(m, p) = 1$, alors le polynôme $x^n - 1$ admet la décomposition suivante :

$$x^n - 1 = x^{mp^h} - 1 = (x^m - 1)^{p^h}.$$

Pour cela on se restreint au cas où n et q sont relativement premiers.
On dénote par $\mathbb{F}_{q^s}$ le corps de décomposition de $x^n - 1$ sur $\mathbb{F}_q$, c'est l'extension de $\mathbb{F}_q$ qui contient toutes les racines du polynôme $x^n - 1$. Comme $(n, q) = 1$, la dérivée de $x^n - 1$ est égale à nx^{n-1} et donc $x^n - 1$ n'a aucune racine double, donc il admet n racines distinctes dans $\mathbb{F}_{q^s}$. Ces racines sont appelées **racines n-ièmes de l'unité** sur $\mathbb{F}_q$, elles forment le sous groupe E^n de $\mathbb{F}_{q^s}^*$ de cardinal n. Comme $\mathbb{F}_{q^s}^*$ est cyclique alors E^n est cyclique d'ordre n. Un élément primitif de E^n est appelé **racine primitive n-ième de l'unité**. Donc si α est une racine primitive $n$ième de l'unité, on a alors :

$$\alpha \in \mathbb{F}_{q^s} \Rightarrow \alpha^{q^s} = \alpha \Rightarrow \alpha^{q^s - 1} = 1 \Rightarrow n/(q^s - 1).$$

L'entier s est appelé **l'ordre** de q modulo n et on le note par $s = \mathrm{ord}_n q$, c'est

le plus petit entier qui vérifie $q^s \equiv 1 \mod n$.

Puisque tout groupe cyclique d'ordre n admet $\phi(n)$ éléments d'ordre n, alors il existe exactement $\phi(n)$ racines primitives n-ièmes de l'unité sur $\mathbb{F}_q$. En particulier puisque $\phi(n) > 0$, donc il existe une racine primitive n-ième de l'unité sur $\mathbb{F}_q$ pour tout entier positif n qui est relativement premier à q.

Le résultat suivant nous permet de trouver les racines primitives n-ièmes de l'unité.

Proposition 2.2.1 *([59]) Soit β un élément primitif du corps de décomposition $\mathbb{F}_{q^s}$ de $x^n - 1$, alors les racines primitives n-ièmes de l'unité sur $\mathbb{F}_q$ sont exactement les éléments de l'ensemble suivant :*

$$\{\beta^k \mid k = \frac{q^s - 1}{n} u, u < n, (u, n) = 1\}.$$

D'après la proposition 2.2.1, si on a un élément primitif β de $\mathbb{F}_{q^s}$ avec $s = \mathrm{ord}_n q$, alors on obtient une racine primitive $n$ième de l'unité $\alpha = \beta^{\frac{q^s-1}{n}}$, donc les racines de $x^n - 1$ sont données par

$$1, \alpha, \ldots, \alpha^{n-1},$$

d'ù la décomposition de $x^n - 1$ dans $\mathbb{F}_{q^s}$:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i). \tag{2.1}$$

Puisque les α^i sont distinctes, alors $x^n - 1$ n'est rien d'autre que le produit des polynômes minimaux de ces racines. On rappele la définition du polynôme

minimal.

Définition 2.2.2 *Soit $\gamma \in \mathbb{F}_{q^s}$. Le polynôme minimal de γ sur $\mathbb{F}_q$ est le polynôme unitaire de plus bas degré $M_\gamma(x)$ dans $\mathbb{F}_q[x]$, vérifiant $M_\gamma(\gamma) = 0$*

Proposition 2.2.3 *([49] p. 106) Soint $\gamma \in \mathbb{F}_{q^s}$ et $M_\gamma(x)$ son polynôme minimal. Alors* $\deg M_\gamma(x) = d$ *si et seulement si d est le plus petit entier positif vérifiant $\gamma^{q^d} = \gamma$.*

De la définition de l'ordre de q modulo l et de la proposition 2.2.3 nous déduisons le corollaire suivant.

Corollaire 2.2.4 *Si $\gamma \in \mathbb{F}_{q^s}$ tel que l est l'ordre de γ, alors*

$$\deg M_\gamma(x) = ord\ {}_l q.$$

La proposition suivante donne la forme de $M_\gamma(x)$.

Proposition 2.2.5 *([59] p. 310) Soit α une racine primitive n-ième de l'unité de $\mathbb{F}_{q^s}$ et $\gamma = \alpha^j$. Alors le polynôme minimal de γ est donné par,*

$$M_\gamma(x) = \prod_{i=0}^{ord_l q - 1} (x - \alpha^{jq^i}). \tag{2.2}$$

La forme de $M_\gamma(x)$ donnée par la proposition 2.2.5 nous suggère de noter $M_\gamma(x)$ simplement par $M_j(x)$. À l'ensemble $\{\alpha^j, \alpha^{jq}, \ldots, \alpha^{jq^{\mathrm{ord}\ {}_l q - 1}}\}$ nous pouvons associer l'ensemble

$$C_j = \{j, jq, \ldots, jq^{\mathrm{ord}\ {}_l q - 1}\} \bmod n.$$

Cet ensemble est appelé la classe cyclotomique de j modulo n, et alors $r = \mathrm{ord}_l\, q$ est le plus petit entier positif tel que $jq^r = j \mod n$. Les entiers j et l sont reliés par le fait que l est l'ordre de $\gamma = \alpha^j$ i.e.,

$$l = \frac{n}{(n, j)}.$$

Remarque 2.2.6 *L'ordre de q modulo n vérifie les propriétés suivantes :*

1. *Si $n > 1$, alors $\mathrm{ord}_n\, q$ est l'ordre de q dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.*
2. *Si m est tel que $q^m = 1 \mod n$ alors $\mathrm{ord}_n\, q$ divise m.*

De la proposition 2.2.5 et de l'équation (2.1) nous obtenons la factorisation suivante de $x^n - 1$:

$$x^n - 1 = \prod_{j \in K} M_j(x),$$

où K est un ensemble de représentants modulo n.

Remarque 2.2.7 *Si α est une racine primitive nième de l'unité, son polynôme minimale est M_1 et donc $\mathrm{ord}_n\, q = |C_1| = deg\ M_1$.*

2.3 Les propriétés des classes cyclotomiques

Dans cette section nous considérons quelques propriétés des classes cyclotomiques utiles pour la suite. Nous redémontrons certains résultats de [31, 32].

Lemme 2.3.1 *Pour tout $j \in \mathbb{Z}_n := \{0, \ldots, n-1\}$, le cardinal de C_j est un diviseur du cardinal de C_1, et deg M_j divise deg M_1.*

Preuve 2.3.2 *Soit $j \in \mathbb{Z}_n$ tel que $\gamma = \alpha^j$ du corollaire 2.2.4, nous avons*

$$deg\ M_j = ord_{\ l} q,$$

où $l = \frac{n}{(n,j)}$ est l'ordre de γ. Puisque l divise n, alors $ord_{\ l}(q)$ divise $ord_{\ n}(q)$. Cependant, d'après la remarque 2.2.7 on a $\mathrm{ord}_n\, q = |C_1| = deg\ M_1$, d'où le résultat.

Définition 2.3.3 *Soient $i \in \mathbb{Z}_n$ et C_i la classe cyclotomique de i modulo n sur $\mathbb{F}_q$. Alors C_i est dite* ***réversible*** *si elle satisfait,*

$$C_i = C_{-i}.$$

Dans ce qui suit nous démontrons le lemme suivant.

Lemme 2.3.4

Si C_1 est réversible, alors $\forall j \in \mathbb{Z}_n, C_j$ est réversible.

Preuve 2.3.5 *Si C_1 est réversible, alors il existe k, $1 \leq k \leq \mathrm{ord}_n(q)$ tel que $q^k \equiv -1 \mod n$, il s'ensuit que $jq^k \equiv -j \mod n$, d'où $C_j = C_{-j}$.*

Lemme 2.3.6 *S'il existe $i > 0$ tel que $q^i \equiv -1 \mod n$, alors C_1 est réversible.*

Preuve 2.3.7 *Puisque $C_1 = \{1, q, \ldots, q^{r-1}\} \mod n$, où $r = \mathrm{ord}_n\, q$, alors il suffit de vérifier l'existence d'un entier k, $1 \leq k \leq \mathrm{ord}_n\, q$, tel que $q^k \equiv -1 \mod n$. Nous avons $i \equiv j \mod n$. Pour $j > 0$ il suffit de prendre $k = j$. Pour $j < 0$ il suffit de prendre $k = j + \mathrm{ord}_n\, q > 0$.*

Corollaire 2.3.8 *Toutes les classes cyclotomiques modulo $n = q^m + 1$ sont réversibles.*

Preuve 2.3.9 *Nous avons $q^m \equiv -1 \mod n$, alors d'après le lemme 2.3.6 la classe C_1 est réversible, donc d'après le lemme 2.3.4 toutes les classes sont réversibles.*

Lemme 2.3.10 *Soient q la puissance d'un nombre premier, m un entier positif plus grand que 1 et $n = q^m + 1$, alors la cardinalité de C_1 modulo n est $2m$.*

Preuve 2.3.11 *De la remarque 2.2.7 nous avons $|C_1| = ord\ _n(q)$, avec $ord\ _n(q)$ le plus petit entier t vérifiant $q^t \equiv 1 \mod n$. Puisque $q^{2m} \equiv 1 \mod (q^m + 1)$, nous avons à prouver que $2m$ est le plus petit entier tel que $q^{2m} \equiv 1 \mod (q^m + 1)$. Supposons qu'il existe un entier $1 \leq r < 2m$ tel que $q^r \equiv 1 \mod (q^m + 1)$, alors r divise $2m$. Puisque $q^r = k(q^m + 1) + 1$, alors $r > m$ ce qui implique que r est tel que $1 < m < r < 2m$ et r divise $2m$; il n'existe aucun entier qui satisfait ces conditions.*

Il est bien connu de la théorie des nombres élémentaire [47] que si $(s, n) = 1$, alors le nombre d'éléments de C_s est égale à $\text{ord}\ _n(q)$. Le lemme suivant affirme que lorsque $n = q^m + 1$ avec $m > 1$, cela est aussi vrai pour tout $s < q$ sans la restriction $(s, n) = 1$.

Lemme 2.3.12 *Si q est la puissance d'un nombre premier, m un entier positif plus grand que 1 et $n = q^m + 1$, alors toutes les classes cyclotomiques,*

$$C_s = \{sq^l \mod n \,|\, l \in \mathbb{N}\},$$

tel que $1 \leq s < q$ *ont le même cardinal* $|C_s| = 2m$.

Preuve 2.3.13 *Soit* $1 \leq s < q$, *par le lemme 2.3.10* $|C_1| = 2m$. *Si on suppose que* $|C_s| = i < 2m$, *alors* i *divise* $2m$. *De plus* i *est le plus petit entier qui vérifie*

$$sq^i \equiv s \mod n, \text{ alors } s(q^i - 1) \equiv 0 \mod (q^m + 1)$$

et donc $s \geq (q^m + 1)/(q^i - 1)$.

Si $i \leq m-1$, *nous avons* $s \geq (q^m+1)/(q^i-1) \geq (q^m+1)/(q^{m-1}-1 > q$, *ce qui est impossible puisque* $s < q$.

Si $i = m$, *nous avons alors* $sq^m = s + k(q^m + 1)$ *et* $sq^m = -s + s(q^m + 1)$, *en sommant les deux égalités, on obtient :*

$$2sq^m = (k + s)(q^m + 1).$$

Puisque $(q^m, q^m + 1) = 1$, *alors* $2s \equiv 0 mod\ (q^m + 1)$, *puisque* $2s \geq q^m + 1$ *ce qui est impossible puisque* $s < q$ *et* $m > 1$.

Puisque $i < 2m$ *et* i *divise* $2m$ *il n'existe aucun autre cas pour* i.

Lemme 2.3.14 *Soient* q *la puissance d'un nombre premier,* m *un entier positif plus grand que* 1, $n = q^m + 1$, s *et* s' *deux entiers distincts tels que* $1 \leq s, s' < q$, *alors les classes cyclotomiques* C_s *et* $C_{s'}$ *sont disjointes.*

Preuve 2.3.15 *Supposons l'existence de deux entiers distincts* s *et* s' *tels que* $1 \leq s, s' < q$ *et* $C_s = C_{s'}$, *alors il existe* $1 \leq i < 2m$ *et* $1 \leq j < 2m$, *tels que* $s \equiv q^i s' \mod n$ *et* $s' \equiv q^j s \mod n$. *Donc* i *et* j *doivent être différents*

de $2m$*, sinon on aura* $s \equiv q^{2m}s' \mod n$*, ce qui implique* $s \equiv s' \mod n$*. Cela est impossible puisque* $s, s' < q$*.*

Maintenant $q^i s' \equiv s \mod n \iff q^i s' - s = k(q^m + 1)$*, avec* $k \in \mathbb{N}^*$*, car si* $k < 0$ *on obtient* $q > s = q^i s' - k(q^m + 1) \geq q^i + q^m + 1$*. Ce qui est impossible pour n'importe quelle valeur de* i*. Par conséquent*

$$q^i s' - s = k(q^m + 1), \text{ avec } k \in \mathbb{N}^*,$$

alors $q^i s' \geq kq^m$*, et alors* $s' > q^{m-i}$*, ce qui est impossible pour* $i \leq m - 1$*.*

Par le même argument il est impossible d'avoir $j \leq m - 1$*.*

Pour $m \leq i \leq 2m - 2$ *nous avons :*

$$q^i s' = s + k(q^m + 1) \text{ et } q^m s = -s + s(q^m + 1),$$

en additionnant les deux égalités on obtient que

$$q^m(s + q^{i-m}s') = (s + k)(q^m + 1),$$

par conséquent q^m *divise* $s + k$ *et*

$$s + q^{i-m}s' \equiv 0 \mod (q^m + 1)$$

Ce qui donne $s + q^{i-m}s' \geq q^m + 1$*. Puisque* $s' < q$ *on obtient que*

$q > s > q^m - q^{i-m+1} + 1 \geq q^m - q^{m-1} + 1$*, ce qui est absurde.*

Par le même argument il est impossible d'avoir $m \leq j \leq 2m - 2$*.*

Si $i = 2m - 1$*,* $j = 2m - 1$*, alors on a* $q^{2m-1}s' = s + k(q^m + 1)$*, en multipliant*

par q les deux membres de l'égalité on obtient que $q^{2m}s' = sq + knq$, mais $q^{2m} \equiv 1 \mod n$ et alors on déduit que $s' \equiv sq \mod n$, et $s \equiv s'q \mod n$, et alors $s' \equiv s'q^2 \mod n$ et $s \equiv sq^2 \mod n$ i.e., $|C_{s'}| = 2$ et $|C_s| = 2$, absurde.

2.4 Les codes cycliques

Un code linéaire de longueur n est dit cyclique s'il est invariant par le décalage circulaire à droite,

$$(a_0, \ldots, a_{n-1}) \longrightarrow (a_{n-1}, a_1, \ldots, a_{n-2}).$$

En considérant l'anneau des polynômes $\mathbb{F}_q[x]$ et son anneau quotient

$$R_n = \mathbb{F}_q[x]/(x^n - 1),$$

si on ignore la multiplication on peut construire un isomorphisme de groupe.

$$\mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1)$$

$$(a_0, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

Le décalage à droite n'est rien d'autre que la multiplication par x et alors un code cyclique C est un idéal de R_n. Puisque R_n est un anneau principal, alors C est un idéal principal engendré par un polynôme $g(x)$. Donc un mot $\mathsf{c} = (c_0, \ldots, c_n)$ de C peut être interprété par le polynôme $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ avec $g(x)$ un diviseur de $c(x)$.

Nous résumons les propriétés des codes cycliques dans le lemme suivant.

Lemme 2.4.1 *([49] p. 190) Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, alors on a les propriétés sivantes :*

1. *Il existe un unique polynôme $g(x)$ de degré minimal dans C tel que, $C = \langle g(x) \rangle$ i.e., C est engendré par le polynôme $g(x)$.*
2. *$g(x)$ est un diviseur de $x^n - 1$.*
3. *La dimension de C est $n - r$, où $r = deg\ g$.*

Soit C un code cyclique engendré par $g(x)$ et α une racine primitive nième de l'unité, on appelle **ensemble de définition** du code C, un sous ensemble de $\mathbb{Z}_n = \{1, \ldots, n\}$ défini par :

$$T_C = \{i \in \mathbb{Z}_n \,|\, g(\alpha^i) = 0\}.$$

Quelques propriétés de l'ensemble de définition d'un code cyclique sont données par la proposition suivante.

Proposition 2.4.2 *([49] p. 196) Soit T_C l'ensemble de définition d'un code cyclique C engendré par g, alors on a :*

1. *$T_C = \cup C_j$, la réunion est sur toutes les classes cyclotomiques C_j telle que M_j divise g.*
2. *$deg\ g = |T_C|$ et alors $\dim C = n - |T_C|$.*
3. *$C = \{f(x) \mod (x^n - 1) \,|\, f(\alpha^i) = 0 \,\forall\, i \in T\}$.*

Le dual Euclidien d'un code cyclique $C =< g(x) >$ est un code cyclique qui vérifie les propriétés données par le lemme suivant.

Lemme 2.4.3 *([36, Théorème 4.4.9] p. 196) Soit C un code cyclique engendré par le polynôme g de degré r, et ayant pour ensemble de définition T, alors le code $C^{\perp}$ dual de C est un code cyclique engendré par $g^{\perp} = h^* = x^{n-r}h(x^{-1})$, avec $h(x) = \frac{x^n-1}{g(x)}$. De plus $C^{\perp}$ admet pour ensemble de définition l'ensemble suivant :*

$$T^{\perp} = \{s \in \mathbb{Z}_n \,|\, n - s \notin T\} = \mathbb{Z}_n \setminus (-T). \tag{2.3}$$

Le dual Hermitien d'un code cyclique $C =< g(x) >$ est un code cyclique. Ses propriétés sont données par le lemme suivant.

Lemme 2.4.4 *([39] p. 27) Soit C un code cyclique engendré par le polynôme g, d'ensemble de définition T, le code $C^{\perp h}$ dual Hermitien de C est un code cyclique engendré par*

$$\prod_{i \in \mathbb{Z}_n \setminus (-qT)} (x - \alpha^i). \tag{2.4}$$

Du lemme 2.4.4 on peut déduire que l'ensemble de définition $T^{\perp h}$ de $C^{\perp h}$ est égale à

$$T^{\perp h} = \mathbb{Z}_n \setminus (-qT). \tag{2.5}$$

2.5 L'équivalence des codes

Un automorphisme (d'espace vectoriel) d'un code linéaire C est un automorphisme de $\mathbb{F}_q^n$ qui laisse C globalement invariant. En fait en théorie des codes, les automorphismes intéressants sont ceux qui conservent la distance de Hamming [52]. De tels automorphismes sont appelés automorphismes

isométriques de $\mathbb{F}_q^n$, leurs groupe est noté H. Le résultat suivant a été prouvé par A. Monpetit et peut être trouvé dans [8, 36].

Proposition 2.5.1 *([8, proposition 1.1]) Le groupe des automorphismes isométriques H de $\mathbb{F}_q^n$ est le produit semi-direct $\mathbb{F}_q^{*n} \ltimes S_n$, c'est à dire*

$$H = \{(a, \sigma) \, : \, a \in \mathbb{F}_q^{*n}, \sigma \in S_n\}, \tag{2.6}$$

et $(b, \tau) \circ (a, \sigma) = (\sigma^{-1}(b)a, \tau \circ \sigma)$

Les matrices de ces automorphismes sont ce que l'on appelle des matrices $n \times n$ **monomiales** : ces matrices ont un seul coefficient non nul par ligne et par colonne.

Définition 2.5.2 *Soient C un code linéaire de longueur n sur un corps fini $\mathbb{F}_q$, le groupe d'automorphismes de C noté $Aut(C)$ est le groupe constitué des automorphismes isométiques de $\mathbb{F}_q$, qui laisse C invariant.*

Soit σ une permutation de S_n, on associe au code C le code linéaire $\sigma(C)$ définit par :

$$\sigma(C) = \{(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) \,|\, (x_1, \ldots, x_n) \in C\}.$$

Le groupe de permutations $Per(C)$ d'un code linéaire de longueur n est un sous groupe du groupe S_n qui laisse le code C invariant, autrement le groupe de permutations c'est :

$$Per(C) = \{\sigma \in S_n \,|\, \sigma(C) = C\}. \tag{2.7}$$

Remarque 2.5.3 *Le groupe de permutations d'un code linéaire C vérifi les propriétés suivantes :*

1. *$Per(C)$ est contenu dans $Aut(C)$. En fait, si $\sigma \in Per(C)$, $\alpha \in \mathbb{F}_q^*$, $a = (\alpha, \ldots, \alpha) \in \mathbb{F}_q^{*n}$, alors $(a, \sigma) \in Aut(C)$. On en déduit immédiatement*

$$\mathbb{F}_q^* \times Per(C) \subset Aut(C).$$

Le produit $\mathbb{F}_q^* \times S_n$ est direct car, pour tout $\sigma \in S_n$ si $b = (\beta, \ldots, \beta)$,

$$\sigma^{-1}(b) = b \text{ et } (b, \tau) \circ (a, \tau) = (ba, \tau \circ \sigma).$$

2. *Lorsque C est un code binaire, c'est à dire un code sur $\mathbb{F}_2$, alors le groupe $Per(C)$ peut être identifié avec $Aut(C)$; cela vient du fait que dans (2.6) le groupe*

$$H = \{(1, \sigma) \, : \, 1 \in \mathbb{F}_2^{*n}, \sigma \in S_n\} \simeq S_n.$$

On dit que deux codes C et C' sont équivalents par permutation (ou simplement équivalent s'il n'y a pas de confusion), s'il existe une permutation $\sigma \in S_n$ tel que $C' = \sigma(C)$.

Deux codes équivalents ont les mêmes paramètres et les mêmes propriétés, c'est pour cette raison que les algorithmes d'équivalence des codes trouvent divers applications dans les problèmes de reconnaissances des codes, spécialement dans le cryptosystème de McEliece avec toutes ces variantes. Le problème de l'équivalence des codes trouve aussi des applications dans le problème de décodage des codes [52]. Il est à noter que le problème de

décodage des codes pour certaines familles de codes est NP-complet [10]. G. Skersys dans sa thèse [65] a proposé un algorithme pour résoudre le problème de l'équivalence des codes cycliques, l'algorithme en question utilise la recherche arrière et est basé sur la méthode des partitions de J. S. Leon [46]. L'efficacité de l'algorithme de Skersys dépend essentiellement du comportement asymptotique de la dimension moyenne du hull des codes cycliques de longueur n sur $\mathbb{F}_q$. Cette dimension moyenne est égale à

$$Edimh_q(n) = \frac{\sum_{C \in C(n,q)} \dim \mathcal{H}(C)}{|C(n,q)|},$$

où $C(n,q)$ désigne l'ensemble des codes cycliques de longueur n sur $\mathbb{F}_q$ et $\mathcal{H}(C) = C \cap C^{\perp}$, appelé **le hull** du code C.

Les raisons précédentes ont suscité notre intérêt au calcul du nombre des codes cycliques donné dans la section suivante.

2.6 Le nombre des codes cycliques

Le nombre $c_q(n)$ désigne le nombre de classes cyclotomiques modulo n dans $\mathbb{F}_q$. Le résultat suivant donnée par Skersys [65] p. 138 découle directement de la proposition 2.2.5 ; du fait que chaque classe cyclotomique correspond à un polynôme minimal qui divise $x^n - 1$.

Lemme 2.6.1 *Soient q une puissance d'un nombre premier p, et n un nombre premier avec p, et $s \geq 0$. Le nombre des codes cycliques de longueur n sur $\mathbb{F}_q$ est égal à*

$$2^{c_q(n)}.$$

Il est bien connu [59] que le nombre de polynômes minimaux irréductibles d'ordre l sur $\mathbb{F}_q$ est égale à

$$\frac{\phi(l)}{\mathrm{ord}_l(q)}. \tag{2.8}$$

En utilisant l'équation (2.8) et la décomposition de $x^n - 1$ en produit de polynômes cyclotomiques, G. Skersys [65] a donné le résultat suivant :

Lemme 2.6.2 *([65] p. 139) Soient q une puissance d'un nombre premier p et n un entier positif non nul tel que $(n, q) = 1$; alors le nombre de classes cyclotomiques modulo n sur $\mathbb{F}_q$ est*

$$c_q(n) = \sum_{l/n} \frac{\phi(l)}{\mathrm{ord}_l(q)}. \tag{2.9}$$

Il n'est pas du tout évident de manipuler la formule (2.9) comme ça a été mentionner par G. Skersys [65] p. 139 " Il est difficile de manipuler une telle formule, et nous avons réussi à l'expliciter dans un cas trés particulier."

Dans ce qui suit nous allons donner explicitement la formule (2.9) dans un cas plus général. Pour cela nous avons besoin du lemme suivant.

Lemme 2.6.3 *([22], p. 87) Soient $r \geq 2$ et u congru à 1 modulo p. Alors $u^{p^{r-1}}$ est congru à 1 modulo p^r. Pour que $u \mod p^r$ soit un élément d'ordre p^{r-1} du groupe $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$, il faut et il suffit qu'on ait u non congru à $1 \mod p^2$.*

Lemme 2.6.4 *Soit z le plus grand entier tel que p^z divise $q^t - 1$, et p^{z+1} ne divise pas $q^t - 1$, avec t l'ordre multiplicatif de q modulo p. Alors si $z = 1$ on a : $\mathrm{ord}_{p^r} q = p^{r-1}t$.*

Preuve 2.6.5 *Pour $u = q^t$, u non congru à $1 \mod p^2$ est équivalent à $z = 1$, alors dans ce cas du lemme 2.6.3 on obtient que q^t est d'ordre $p^{r-1} \mod p^r$*

pour tout entier r ; c'est-à-dire

$$\left(q^t\right)^{p^{r-1}} \equiv 1 \mod p^r,$$

et par suite $ord_{p^r}(q) = tp^{r-1}$.

Proposition 2.6.6 *Soient* α *un entier positif et* $n = t^\alpha$ *où* t *est un nombre premier impair, tel que* $(t, q) = 1$, *et* $\mathrm{ord}_t(q) \neq \mathrm{ord}_{t^2}(q)$. *Alors on a :*

$$c_q\left(t^\alpha\right) = 1 + \frac{\alpha(t-1)}{\mathrm{ord}_t\left(q\right)}.$$

Preuve 2.6.7 *Puisque les diviseurs de* t^α *sont les puissances de* t, *alors la formule (2.9) devient,*

$$c_q\left(t^\alpha\right) = \sum_{l/t^\alpha} \frac{\phi\left(l\right)}{\mathrm{ord}_l\left(q\right)} = \sum_{i=0}^{\alpha} \frac{\phi\left(t^i\right)}{\mathrm{ord}_{t^i}\left(q\right)}.$$

D'autre part d'après le lemme 2.6.4, on a q^r *est d'ordre* $t^{i-1} \mod t^i$ *pour tout entier i ;*

$$\left(q^r\right)^{t^{i-1}} \equiv 1 \mod t^i$$

et par suite

$$\mathrm{ord}_{t^i}(q) = rt^{i-1}. \tag{2.10}$$

D'où

$$c_q\left(t^\alpha\right) = \sum_{i=0}^{\alpha} \frac{\phi\left(t^i\right)}{\mathrm{ord}_{t^i}\left(q\right)} = 1 + \sum_{i=1}^{\alpha} \frac{\left(t-1\right)t^{i-1}}{rt^{i-1}} = 1 + \frac{\alpha\left(t-1\right)}{r}.$$

Remarque 2.6.8 *L'inégalité* $\mathrm{ord}_t(q) \neq \mathrm{ord}_{t^2}(q)$ *est essentielle dans la pro-*

position 2.6.6, sinon on ne peut pas appliquer le lemme 2.6.3. Cependant les nombres premiers qui ne verifient pas cette inégalité sont vraiment rares [35] p. 207. Juste par exemple, pour $q = 2, 4, 8$ *ou* 16 *et* $3 \leq t \leq 3 \times 10^9$*, les seules solutions sont* $t = 1093$ *ou* 3511*, en plus* $t = 3$ *est une solution avec* $q = 8$*. Pour* $q = 3, 9$ *ou* 27 *et* $3 \leq t \leq 2^{30}$*, les seules solutions sont* $t \in \{11, 1006003\}$*. Pour* $q = 5$ *ou* 25 *et* $3 \leq t < 2^{29}$*, les seules solutions sont* $t \in \{20771, 40487, 53471161\}$*. Pour* $q = 7$ *on a comme solution* $t \in \{5, 491531\}$*. Pour* $q = 11$ *on a* $t = 71$*. Pour* $q = 17$ *ou* 19 *et* $3 \leq t < 2^{27}$ *les seules solutions sont* $t \in \{3, 46021, 48947\}$ *pour* $q = 17$ *et* $t \in \{3, 7, 13, 43, 137, 63061489\}$ *pour* $q = 19$*. Pour* $q = 23$ *et* $3 \leq t < 2^{26}$ *les solutions sont* $t \in \{13, 2481757, 13703077\}$*. Pour* $q = 29$ *et* $3 \leq p \leq 2^{28}$ *il n'existe pas de solutions.*

Soient p_1 et p_2 deux nombres premiers impairs et $n = p_1^{a_1} p_2^{a_2}$ un produit de leurs puissances, et q la puissance d'un nombre premier tel que $(n, q) = 1$. On note $r_1 = \mathrm{ord}_{p_1}(q)$, $r_2 = \mathrm{ord}_{p_2}(q)$, $r = ppcm(r_1, r_2)$, et on suppose que $r_1 \neq \mathrm{ord}_{p_1^2}(q)$ et $r_2 \neq \mathrm{ord}_{p_2^2}(q)$.

D'après la proposition 2.6.2

$$c_q(n) = \sum_{l/n} \frac{\phi(l)}{\mathrm{ord}_l(q)} = 1 + c_q(p_1^{a_1})^* + \ c_q(p_2^{a_2})^* + R_q\left(p_1^{a_1} p_2^{a_2}\right),$$

où

$$\begin{aligned} c_q(p_1^{a_1})^* &= \sum_{i=1}^{a_1} \frac{\phi\left(p_1^i\right)}{\mathrm{ord}_{p_1^i}(q)} \\ c_q(p_2^{a_2})^* &= \sum_{j=1}^{a_2} \frac{\phi\left(p_2^j\right)}{\mathrm{ord}_{p_2^j}(q)}, \\ R_q\left(p_1^{a_1}p_2^{a_2}\right) &= \sum_{l/p_1^{a_1}p_2^{a_2}, l\neq p_1^i, l\neq p_2^j} \frac{\phi(l)}{ord_l(q)}. \end{aligned}$$

D'autre part, d'après la proposition 2.6.6 on a

$$c_q(p_1^{a_1})^* = \frac{a_1(p_1-1)}{r_1} \quad \text{et} \quad c_q(p_2^{a_2})^* = \frac{a_2(p_2-1)}{r_2}.$$

Le calcul explicite de $R_q\left(p_1^{a_1}p_2^{a_2}\right)$ est donné dans la proposition suivante :

Proposition 2.6.9 *Le nombre de classes cyclotomiques modulo $p_1^{a_1}p_2^{a_2}$ sur $\mathbb{F}_q$ est égal à :*

$$c_q(p_1^{a_1}p_2^{a_2}) = 1 + \frac{a_1(p_1-1)}{r_1} + \frac{a_2(p_2-1)}{r_2} + R_q\left(p_1^{a_1}p_2^{a_2}\right),$$

où $R_q\left(p_1^{a_1}p_2^{a_2}\right) =$

$$\begin{cases} \frac{a_1 a_2 (p_1-1)(p_2-1)}{r} & si\ (p_1, r_2) = 1\ et\ (p_2, r_1) = 1 \\ \frac{a_2 (p_1^{a_1}-1)(p_2-1)}{r} & si\ p_1^j // r_2, j \geq a_1\ et\ (p_2, r_1) = 1 \\ \frac{a_1 (p_2^{a_2}-1)(p_1-1)}{r} & si\ p_2^i // r_1, i \geq a_2\ et\ (p_1, r_2) = 1 \\ \frac{(p_1^{a_1}-1)(p_2^{a_2}-1)}{r} & si\ p_1^j // r_2, p_2^i // r_1, j \geq a_1\ et\ i \geq a_2 \\ \frac{[(p_1^{j+1}-1)+(a_1-j-2)(p_1-1)p_1^j][(p_2^{i+1}-1)+(a_2-i-2)(p_2-1)p_2^i]}{r} & si\ p_1^j // r_2,\ p_2^i // r_1, j \leq a_1,\ et\ i \leq a_2 \\ \frac{(p_2^{a_2}-1)[(p_1^{j+1}-1)+(a_1-j-2)(p_1-1)p_1^j]}{r} & si\ p_1^j // r_2\ , j \leq a_1, p_2^i // r_1\ et\ i \geq a_2 \\ \frac{(p_1^{a_1}-1)[(p_2^{i+1}-1)+(a_2-i-2)(p_2-1)p_2^i]}{r} & si\ p_1^j // r_2\ , j \geq a_1, p_2^i // r_1\ et\ i \leq a_2. \end{cases}$$

Preuve 2.6.10 *Si* $r_1 = \mathrm{ord}_{p_1}(q)$ *et* $r_2 = \mathrm{ord}_{p_2}(q)$ *alors* $\mathrm{ord}_{p_1 p_2}(q) = ppcm(r_1, r_2)$.

Si on suppose en plus que $r_1 \neq \mathrm{ord}_{p_1^2}(q)$ *et* $r_2 \neq \mathrm{ord}_{p_2^2}(q)$

alors $\mathrm{ord}_{p_1^j p_2^i}(q) = ppcm(\mathrm{ord}_{p_1^j}(q), \mathrm{ord}_{p_2^i}(q)) = ppcm(p_1^{j-1} r_1, p_2^{i-1} r_2)$. *Il s'en suit les différents cas suivants :*

Premier cas :

Si $(p_1, r_2) = 1$ *et* $(p_2, r_1) = 1$ *alors pour* $1 \leq t \leq a_1$ *et* $1 \leq l \leq a_2$ *nous obtenons*

$$ord_{p_1^t p_2^l}(q) = ppcm(p_1^{t-1} r_1, p_2^{l-1} r_2) = p_1^{t-1} p_2^{l-1} r \tag{2.11}$$

et par suite

$$\begin{aligned}
&R_q\left(p_1^{a_1} p_2^{a_2}\right) = \\
&\phi(p_1)\left(\frac{\phi(p_2)}{r} + \frac{\phi(p_2)\, p_2}{ppcm(r_1, p_2 r_2)} + \ldots + \frac{\phi(p_2)\, p_2^{a_2-1}}{ppcm(r_1, p_2^{a_2-1} r_2)}\right) \\
&+\phi\left(p_1^2\right)\left(\frac{\phi(p_2)}{ppcm(p_1 r_1, r_2)} + \frac{\phi(p_2)\, p_2}{ppcm(p_1 r_1, r_2 p_2)} + \ldots + \frac{\phi(p_2)\, p_2^{a_2-1}}{ppcm(r_1 p_1, p_2^{a_2-1} r_2)}\right) \\
&\vdots \\
&+\phi\left(p_1^{a_1}\right)\left(\frac{\phi(p_2)}{ppcm(p_1^{a_1-1} r_1, r_2)} + \frac{\phi(p_2)\, p_2}{ppcm(p_1^{a_1-1} r_1, r_2 p_2)} + \ldots + \frac{\phi(p_2)\, p_2^{a_2-1}}{ppcm(p_1^{a_1-1} r_1, p_2^{a_2-1} r_2)}\right).
\end{aligned}$$

Tenant compte de la relation (2.11) on obtient :

$$R_q\left(p_1^{a_1} p_2^{a_2}\right) = \frac{a_1 a_2 (p_1 - 1)(p_2 - 1)}{r}.$$

Deuxième et troisième cas :

Si $p_1^j // r_2$ *avec* $j \geq a_1$ *et* $(p_2, r_1) = 1$ *alors pour* $1 \leq t \leq a_1$ *et* $1 \leq l \leq a_2$ *on obtient*

$$\mathrm{ord}_{p_1^t p_2^l}(q) = ppcm(p_1^{t-1} r_1\, , p_2^{l-1} r_2) = r p_2^{l-1} \tag{2.12}$$

et donc

$$\begin{aligned} R_q\left(p_1^{a_1}p_2^{a_2}\right) &= \phi\left(p_1\right)\left(\frac{\phi\left(p_2\right)}{r}+\ldots+\frac{\phi\left(p_2\right)p_2^{a_2-1}}{ppcm(r_1,p_2^{a_2-1}r_2)}\right) \\ &\quad +\phi\left(p_1^2\right)\left(\frac{\phi\left(p_2\right)}{ppcm(p_1r_1,r_2)}+\ldots+\frac{\phi(p_2)p_2^{a_2-1}}{ppcm(r_1p_1,p_2^{a_2-1}r_2)}\right) \\ &\quad \vdots \\ &\quad +\phi\left(p_1^{a_1}\right)\left(\frac{\phi\left(p_2\right)}{ppcm(p_1^{a_1-1}r_1,r_2)}+\ldots+\frac{\phi\left(p_2\right)p_2^{a_2-1}}{ppcm(p_1^{a_1-1}r_1,p_2^{a_2-1}r_2)}\right). \end{aligned}$$

Tenant compte de la relation (3) *on a*

$$R_q\left(p_1^{a_1}p_2^{a_2}\right)=\frac{a_2(p_1^{a_1}-1)(p_2-1)}{r}.$$

De la même manière on obtient le troisième cas.

Quatrième cas :

Si $p_1^j//r_2$ *avec* $j\geq a_1$ *et* $p_2^i//r_1$ *avec* $i\geq a_2$ *alors pour* $1\leq t\leq a_1$ *et* $1\leq l\leq a_2$ *on obtient*

$$\mathrm{ord}_{p_1^tp_2^l}(q)=ppcm(p_1^{t-1}r_1,p_2^{l-1}r_2)=ppcm(r_1,r_2)=r;$$

donc

$$\begin{aligned} R_q\left(p_1^{a_1}p_2^{a_2}\right) &= \frac{1}{r}\left[\phi\left(p_1\right)+\ldots+\phi\left(p_1^{a_1}\right)\right]\left[\phi\left(p_2\right)+\ldots+\phi\left(p_2^{a_2}\right)\right] \\ &= \frac{1}{r}(p_1^{a_1}-1)(p_2^{a_2}-1). \end{aligned}$$

Cinquième cas :

$p_1^j//r_2$ *avec* $j\leq a_1$ *et* $p_2^i//r_1$ *avec* $i\leq a_2$, *alors pour* $1\leq t\leq a_1$ *et*

$1 \leq l \leq a_2$ *on obtient*

$$\mathrm{ord}_{p_1^t p_2^l}(q) = ppcm(p_1^{t-1} r_1, p_2^{l-1} r_2) = \begin{cases} p_1^{t-1} p_2^{l-1} r & si \;\; t-1 \gneq j \;\; et \; l-1 \gneq i \\ r p_2^{l-(i+1)} & si \;\; t-1 \leq j \;\; et \; l-1 \gneq i \\ r & si \; t-1 \leq j \;\; et \; l-1 \leq i \\ r p_1^{t-(j+1)} & si \; t-1 \gneq j \;\; et \; l-1 \leq i. \end{cases}$$

Donc

$$\begin{aligned} & R_q\left(p_1^{a_1} p_2^{a_2}\right) \\ &= \phi(p_1)\left[\frac{\phi(p_2)}{r} + \ldots + \frac{\phi\left(p_2^{i+1}\right)}{r} + \frac{\phi\left(p_2^{i+2}\right)}{p_2 r} + \ldots + \frac{\phi\left(p_2^{a_2}\right)}{p_2^{a_2-(i+1)} r}\right] \\ &\quad + \phi\left(p_1^2\right)\left[\frac{\phi(p_2)}{r} + \ldots + \frac{\phi\left(p_2^{i+1}\right)}{r} + \frac{\phi\left(p_2^{i+2}\right)}{p_2 r} + \ldots + \frac{\phi\left(p_2^{a_2+1}\right)}{p_2^{a_2-(i+1)} r}\right] \\ &\quad \vdots \\ &\quad + \phi\left(p_1^{j+1}\right)\left[\frac{\phi(p_2)}{r} + \ldots + \frac{\phi\left(p_2^{i+1}\right)}{r} + \frac{\phi\left(p_2^{i+2}\right)}{p_2 r} + \ldots + \frac{\phi\left(p_2^{a_2+1}\right)}{p_2^{a_2-(i+1)} r}\right] \\ &\quad + \phi\left(p_1^{j+2}\right)\left[\frac{\phi(p_2)}{r p_1} + \ldots + \frac{\phi\left(p_2^{i+1}\right)}{r p_1} + \frac{\phi\left(p_2^{i+2}\right)}{p_1 p_2 r} + \ldots + \frac{\phi\left(p_2^{a_2+1}\right)}{p_1 p_2^{a_2-(i+1)} r}\right] \\ &\quad \vdots \\ &\quad + \phi\left(p_1^{a_1}\right)\left[\frac{\phi(p_2)}{r p_1^{a_1-(j+1)}} + \ldots + \frac{\phi\left(p_2^{i+1}\right)}{r p_1^{a_1-(j+1)}} + \frac{\phi\left(p_2^{i+2}\right)}{p_1^{a_1-(j+1)} p_2 r} \cdots \frac{\phi\left(p_2^{a_2+1}\right)}{p_1^{a_1-(j+1)} p_2^{a_2-(i+1)} r}\right]. \end{aligned}$$

Donc on obtient :

$$\begin{aligned} & R_q\left(p_1^{a_1}p_2^{a_2}\right) \\ = \; & \frac{1}{r}\phi\left(p_1\right)\left(1+p_1+\ldots+p_1^j\right)\left[\phi\left(p_2\right)\left(1+p_2+\ldots p_2^i\right)+\phi\left(p_2\right)p_2^i(a_2-i-2)\right] \\ & +\frac{1}{r}p_1^j\phi\left(p_1\right)\left[a_1-(j+2)\right]\left[\phi\left(p_2\right)\left(1+p_2+\ldots+p_2^i\right)+\phi\left(p_2\right)p_2^i(a_2-(i+2))\right]. \end{aligned}$$

D'où

$$R_q\left(p_1^{a_1}p_2^{a_2}\right)=\frac{1}{r}\left[p_1^{j+1}-1+p_1^j\left(p_1-1\right)\left(a_1-j-2\right)\right]\left[p_2^{i+1}-1+p_2^i\left(p_2-1\right)\left(a_2-i-2\right)\right].$$

Sixième et septième cas :

Si $p_1^j//r_2$ *avec* $j \leq a_1$ *et* $p_2^i//r_1$ *avec* $i \geq a_2$, *alors pour* $1 \leq t \leq a_1$ *et* $1 \leq l \leq a_2$ *on obtient :*

$$\mathrm{ord}_{p_1^t p_2^l}(q) = ppcm(p_1^{t-1}r_1, p_2^{l-1}r_2) = \begin{cases} r & si\ t-1 \leq j \\ p_1^{t-1-j}r & si\ t-1 \geq j. \end{cases}$$

Donc

$$\begin{aligned} R_q\left(p_1^{a_1}p_2^{a_2}\right) &= \phi\left(p_1\right)\left[\frac{\phi\left(p_2\right)}{r}+\ldots+\frac{\phi\left(p_2^{a_2}\right)}{r}\right] \\ &\quad \vdots \\ &\quad +\phi\left(p_1^{j+1}\right)\left[\frac{\phi\left(p_2\right)}{r}+\ldots+\frac{\phi\left(p_2^{a_2}\right)}{r}\right] \\ &\quad +\phi\left(p_1^{j+2}\right)\left[\frac{\phi\left(p_2\right)}{rp_1}+\ldots+\frac{\phi\left(p_2^{a_2}\right)}{rp_1}\right] \\ &\quad \vdots \\ &\quad +\phi\left(p_1^{a_1}\right)\left[\frac{\phi\left(p_2\right)}{rp_1^{a_1-(j+1)}}+\ldots+\frac{\phi\left(p_2^{a_2}\right)}{p_1^{a_1-(j+1)}r}\right] \\ &= (p_1^{j+1}-1)(\frac{p_2^{a_2}-1}{r})+(\frac{p_2^{a_2}-1}{r})\left[p_1^j\phi\left(p_1\right)\left(a_1-j-2\right)\right]. \end{aligned}$$

Donc

$$Rq\left(p_1^{a_1}p_2^{a_2}\right)=(\frac{p_2^{a_2}-1}{r})\left[(p_1^{j+1}-1)+p_1^j\left(p_1-1\right)\left(a_1-j-2\right)\right].$$

Le septième cas se traite de la même manière.

Exemple 2.6.11 *En appliquant les résultats de cette section nous donnons N (le nombre des codes cycliques de longueur n sur $\mathbb{F}_q$).*

Quelques exemples de calcul du nombre des codes cycliques.

q	n	N	q	n	N	q	n	N	q	n	N
3	5	2^2	11	2	2^2	13	2	2^2	13	77	2^{11}
3	7	2^2	11	3	2^6	13	3	2^3	13	11^2	2^3
3	5^2	2^3	11	5	2^5	13	4	2^4	29	3	2^2
3	35	2^5	11	7	2^3	13	5	2^2	29	5	2^3
5	2	2^2	11	10	2^{10}	13	6	2^6	29	7	2^{29}
5	3	2^2	11	15	2^{10}	13	7	2^4	29	9	2^3
5	4	2^4	11	21	2^6	13	11	2^2	29	15	2^8
5	9	2^3	11	5^2	2^9	13	12	2^{12}	29	21	2^{36}
5	27	2^4	11	5^3	2^{13}	13	14	2^8	29	35	2^{43}
5	81	2^5	11	5^4	2^{17}	13	15	2^7	29	45	2^{13}

Chapitre 3

La théorie des codes quantiques

Anyone who says that they can contemplate
quantum mechanics without becoming dizzy
has not understood the concept in the least.
Niels Bohr

3.1 Introduction

Bien que le développement de la mécanique quantique moderne date du début du siècle et la théorie des codes correcteurs d'erreurs date depuis la fin des années 40, l'idée de combiner les deux n'est survenue que vers les années 80. À cette date il est devenue possible de manipuler et d'observer des objets quantiques individuellement (atomes, molécules, photons, etc...), alors les physiciens Richard Feynman et Paul Benioff ont commencé à étudier la relation entre la physique et les processus d'informatique. Feynman dans [26] a prouvé qu'un système quantique de R particules ne peut pas être simulé

par un ordinateur classique sans que l'efficacité de la simulation ne soit retarder d'une manière exponentielle. Feynman a aussi eu l'idée d'éliminer ce retard en construisant un ordinateur qui fonctionne selon les lois de la mécanique quantique. Un modèle de l'information quantique a été construit par Benioff [5], mais Deutsch [24] a prouvé que le modèle de Benioff peut être simulé par un ordinateur classique, en revanche il a donné de solides bases à la théorie de l'information quantique en introduisant un modèle qui décrit un ordinateur quantique universel[1]. Ça a été le début de l'aire de l'informatique quantique. La performance de celle ci découle de la combinaison des deux lois principales de la mécanique quantique, qui sont l'intrication et la superposition linéaire des états. Cette combinaison est responsable du parallélisme quantique qui diffère fondamentalement des parallélismes classiques. Après quelques résultats dans ce domaine purement théorique, Peter Shor [64] en costruisant sur les travaux de Simon a fait une révolution dans ce domaine. Il a présenté un algorithme qui avait un intérêt pratique pour les ordinateurs basés sur les principes de la mécanique quantique. L'algorithme en question permis la factorisation d'entiers en un temps polynomial. Cette découverte a été suivit par d'autres solutions à des problèmes connues tels que, l'ordre d'un entier, la période, etc ... Ceci a eu pour effet que plusieurs équipes de chercheurs ce sont dévoué à ce domaine de recherche de pointe. Malgré cela il reste des doutes sur l'utilité de l'information quantique.

C. H. Bennett [6] a commenté :“ la situation actuelle et les doutes sur la faisabilité des ordinateurs quantiques sont similaires à ceux qui existaient

[1]Actuellement certains chercheurs étudient la possibilité de construire un ordinateur hybride.

dans les années 40 vis à vis des ordinateurs (classiques)..." !!!. Quant à D. V. Mackay il pense que la réalisation réel d'un ordinateur quantique peut être nécessite une cinquantaine d'année, car à l'heure actuelle on ne sait manipuler que quelques qu-bits (10 qu-bits en 2005 à IQC Waterloo). Cependant cela n'a pas empêché toute une armada d'équipes de chercheurs à travers le monde d'essayé d'apporter leurs contributions à ce domaine de recherche.

3.2 Le bit, le *qu*-bit et le *qu*-dit

Un qu-bit décrit l'état dans le plus simple système quantique ; comme le bit est l'unité de base de l'information classique, le qu-bit est l'unité de base de l'information quantique. Dans le cas classique la valeur 0 d'un bit dans un ordinateur est représenté physiquement par un condensateur non chargé. La valeur 1 par un condensateur chargé. Dans le cas quantique on peut utiliser la polarisation des photons pour transmettre de l'information. En effet, lorsque l'on fait passé la lumière à travers un filtre polarisant, les photons seront absorbés ou trasmis selon leur polarisation :

- Si le photon est polarisé parallèlement à l'angle d'orientation du filtre, alors ce photon sera transmis sans changement de polarisation.
- Si le photon est polarisé perpendiculairement à l'angle d'orientation du filtre, alors ce photon sera absorbé.
- Si le photon est polarisé selon une direction intermédiaire, alors ce photon sera transmis avec une probabilité $\cos^2(\alpha)$, où α est l'angle de polarisation du photon mesuré par rapport à l'angle d'orientation du filtre. C'est à dire que si le photon est polarisé suivant un angle de γ

et que le filtre est orienté selon un angle de β, alors $\alpha = \gamma - \beta$. Si le photon est transmis alors sa nouvelle polarisation correspond à l'angle d'orientation du filtre.

Ces propriétés permettent d'utiliser un photon polarisé pour réaliser le concept de bit quantique ou qu-bit. Pour un système de photons polarisé on décide tout à fait arbitrairement d'attribuer la valeur $|0>$ à un photon polarisé suivant ox et la valeur $|1>$ à un photon polarisé suivant oy[2], un photon polarisé suivant un angle de $\gamma = 45°$ sera représenté par $\cos(\gamma)|0> + \sin(\gamma)|1> = (|0> + |1>)/\sqrt{2}$ i.e., un photon polarisé à 45° est une superposition d'un photon polarisé suivant *ox* et d'un photon polarisé suivant *oy*. Autrement un bit ne peut prendre que la valeur 0 ou 1, alors qu'un qu-bit peut prendre toutes les valeurs entre $|0>$ et $|1>$.

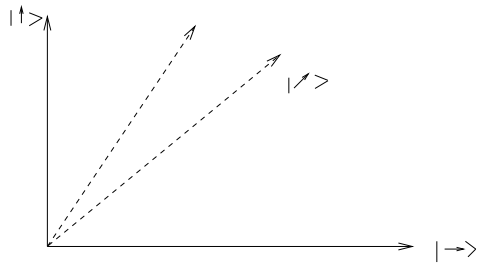

FIG. 3.1 – Le principe de la superposition linéaire des états.

On peut aussi choisir d'utiliser un système qui représente le spin d'une particule de spin $\frac{1}{2}$ (e.g. électron) ou bien les niveaux d'énergie de certains atomes. De tels systèmes sont en fait des idéalisations. Dans la nature en

[2]La notation $|. >$ est dûe à Dirac, on verra dans l'appendice d'où elle découle.

général le nombre d'états de base d'une microparticule est supérieur à deux, cependant nous devons ignorer certains degrés de liberté afin d'obtenir un système à deux niveaux effectifs.

Lorsque le nombre d'états de base est supérieur à deux, on parle du digit quantique *qu*-aire, nommé en abréviation *qu*-dit.

3.3 L'information quantique

3.3.1 Les problèmes de l'information quantique

Théoriquement, le principe de superposition des états permet à l'information quantique de voyager plus rapidement que la lumière. Cependant la réalisation pratique est beaucoup plus ardue. Cela est dû aux conditions sévères imposés aux systèmes physiques (photons ou électrons ...) utilisés pour représenter les *qu*-dits ; ils doivent être manipulables individuellement, mais en grand nombre. Ils doivent être initialisés dans un état quantique précis. On doit pouvoir mesurer leurs états finals pour lire le résultat du calcul. Ils doivent intéragir fortement entre eux, pour réaliser la dynamique conditionnelle des portes logiques quantiques. Finalement ils doivent être totalement isolés du milieu extérieur. L'interaction des *qu*-bits avec l'environnement **décohérence** est responsable de la destruction de l'interaction des états et de la superposition nécessaire pour obtenir une rapidité meilleur que le cas classique. Cette décohérence même si elle reste faible à l'échelle d'un *qu*-dit individuel devient trés rapide lorsque elle s'attaque à la superposition d'un grand nombre de *qu*-dits.

3.3.2 Les codes correcteurs : solution pour la décohérence

Le schéma usuel d'envoyer l'information dans le cas classique consiste à ajouter une certaine redondance en faisant des copies conformes du message en vue de le protéger. Cela n'est plus possible dans le cas quantique à cause du théorème du non-clonage[3]. Cependant comme on va le voir on peut utiliser pour cela les codes correcteurs d'erreurs quantiques.

L'hypothèse conventionel était que si un seul qu-dit est en décohérence, alors tout le système est en décohérence, ce qui détruit l'intéraction des états et donne nécessairement des résultats faux [69]. En supposant que la décohérence affecte les qu-dits en mémoire indépendament, ce qui ressemble à l'hypothèse de l'indépendance des erreurs dans le cas classique, Shor [63] a montré qu'on peut utiliser le schéma du défaut toléré (fault-tolerent) comme solution à la décohérence ; au moins en principe il existe un code qui protège efficacement les états à condition que le taux d'erreurs par opération soit plus petit qu'une valeur seuil p. Au fait avec cette hypotèse on peut effectuer sans échec un nombre d'opérations de l'ordre $\mathcal{O}(p^a)$, avec a une constante positive [23].[4] L'hyphothèse de Shor permet de considérer la probabilité pour que le résultat obtenu soit correct, comme étant une somme de toutes les probablités sur les qu-dits. Il reste cependant deux problèmes ; Le taux maximum d'erreurs admissibles par opération est trés faible beaucoup plus faible que ce qui est facilement réalisable en théorie classique. De plus la redondance est beaucoup plus forte que dans le cas classique.

[3]Voir l'Appendice pour ça

[4]Knill et al. [44] ont prouvé théoriquement l'existence de larges codes quantiques qui peuvent être utilisé pour transférer l'information sans bruit.

3.4 Les codes correcteurs quantiques

L'état d'un qu-dit est un vecteur non nul du $\mathbb{C}$ espace vectoriel $\mathbb{C}^q$. Cet espace vectoriel est équipé d'une base orthonormale. On note ses éléments par $|x>$, où x est un élément du corps fini $\mathbb{F}_q$. L'état d'un système à n qu-dits (appelé aussi n qu-dits) est alors un vecteur non nul dans l'espace de Hilbert $\mathbb{C}^{q^n} = \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$. Alors une base orthonormale de $\mathbb{C}^{q^n}$ est donnée par $\{|\mathsf{w}>: \mathsf{w} \in \mathbb{F}_q^n\}$ où $|\mathsf{w}>= |w_1> \otimes \ldots \otimes |w_n>$ (Une base orthonormale de $\mathbb{C}^{q^n}$ eat aussi appelée registre de taille n).[5] Cela a pour effet qu'un état général d'un système à n qu-dits est donné par

$$|\psi>= \sum_{\mathsf{x} \in \mathbb{F}_q^n} \alpha_{\mathsf{x}} |\mathsf{x}>; \sum |\alpha_{\mathsf{x}}|^2 = 1.$$

La probabilité d'observer un système dans un état $|\mathsf{x}>$ est donnée par $|\alpha_{\mathsf{x}}|^2$. Les coefficients $|\alpha_{\mathsf{x}}|$ sont appelés amplitudes et la fonction $\psi(\mathsf{x}) = \alpha_{\mathsf{x}}$ est appelé la fonction onde. La condition sur les amplitudes assure que la probablité d'obtenir un certain résultat soit égale à 1.

Exemples :

1. L'espace de Hilbert $\mathbb{C}^2$ de dimension 2 admet pour base orthonormale $\{|0>, |1>\}$ et alors un état général d'un seul qu-bit est donné par :

$$a_0|0> + a_1|1> \tag{3.1}$$

où $|a_0|^2 + |a_1|^2 = 1$.

L'observation d'un qu-bit à l'état (3.1) donne $|0>$ ou $|1>$ avec une

[5] Par fois les éléments de la base sont simplement notés $|\mathsf{w}>= |w_1> \ldots |w_n>$.

probabilité $|a_0|^2$, respectivement $|a_1|^2$.

2. L'espace de Hilbert $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ de dimension 4 admet pour base orhtonormale :

   $$\{|00>=|0>\otimes|0>, |01>=|0>\otimes|1>, |10>=|1>\otimes|0>, |11>=|1>\otimes|1>\}.$$

   Un état général à 2 qu-bits est de la forme

   $$a_0|00> + a_1|01> + a_2|10> + a_3|11>,$$

   où $|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1$

D'une importante propriété du produit tensoriel découle la définition suivante.

Un état z dans $\mathbb{C}^{q^{m+n}} = \mathbb{C}^{q^m} \otimes \mathbb{C}^{q^n}$ est dit **décomposable** s'il peut se mettre sous la forme $\mathsf{z} = \mathsf{x} \otimes \mathsf{y}$, sinon il est dit **intriqué (enchevêtré)** (entangled).

Exemples :

1. On considère l'état $|\psi>=\frac{1}{2}(|00> + |01> + |10> + |11>)$, alors

   $$|\psi>=\frac{1}{2}(|0>|0> + |0>|1> + |1>|0> + |1>|1>),$$

   d'où $|\psi>=\frac{1}{\sqrt{2}}(|0>+|1>)\frac{1}{\sqrt{2}}(|0>+|1>)$, ce qui veut dire que $|\psi>$ est un état décomposable.

2. L'état $|\phi>=\frac{1}{\sqrt{2}}(|00>+|11>)$ est enchevêtré car supposons que

   $$|\phi>=(a_0|0>+a_1|1>)(b_0|0>+b_1|1>)$$

$$= a_0b_0|00> + a_0b_1|01> + a_1b_0|10> + a_1b_1|11>,$$

pour certains nombres complexes a_0, a_1, b_0, b_1, alors ils vérifient

$$\begin{aligned} a_0b_0 &= \frac{1}{\sqrt{2}} \\ a_0b_1 &= 0 \\ a_1b_0 &= 0 \\ a_1b_1 &= \frac{1}{\sqrt{2}}, \end{aligned}$$

ce qui est absurd.

L'état $|\phi> = \frac{1}{\sqrt{2}}(|00> + |11>)$ est appelée paire EPR, cette appellation est en honneur à Einstein, Podolsky, Rosen. La paire EPR est trés importante dans les protocole quantique.

Lorsque les qu-bits sont enchevêtrés il n'est pas possible d'observer un état d'un qu-bit enchevêtré sans détruire le reste du système. C'est ce qui donne théoriquement la puissance des ordinateurs quantiques.

Dans ce qui suit nous donnons la définition d'un code correcteur d'erreur.

Définition 3.4.1 *Un code q-aire quantique Q de longueur n et de taille K est un sous espace de dimension K de $\mathbb{C}^{q^n}$. Le code Q est utilisé pour encoder $\log_q K$ qu-dits en n qu-dits. Dans ce cas le code Q est noté par $((n, K))_q$. Lorsque $K = q^k$, par analogie au cas classique, on note Q par $[[n, k]]_q$.*

Exemples :

1. Nous pouvons encoder $|0> \mapsto |000>$ et $|1> \mapsto |111>$ et alors un état

$|\phi>=\alpha|0>+\beta|1>\mapsto|\psi>=\alpha|000>+\beta|111>$. Il est à noter que $|\psi>$ est un état enchevêtré ; ce n'est pas une copie de $|\phi>$.

2. Le code connu par " code répété de Shor à 9 qu-dits" $[[9,1]]_2$ permet d'encoder

$$|0>\mapsto|\overline{0}>=(|000>+|111>)(000>+|111>)(|000>+|111>),$$

et

$$|1>\mapsto|\overline{1}>=(|000>-|111>)(000>-|111>)(|000>-|111>).$$

Les états $(|000>+|111>)(000>+|111>)(|000>+|111>)$, et $(|000>-|111>)(000>-|111>)(|000>-|111>)$ forment une base du $[[9,1]]_2$ code de Shor. Ce code est donc un sous espace de $\mathbb{C}^{2^{\otimes 9}}$ de dimension 2.

Les exemples précédents de codes ne violent pas le théorème du non-clonage, puisque chaque mots de ces codes est une superposition linéaires des deux états $|\overline{0}>$ et $|\overline{1}>$, dit zéro logique et un logique. On a

$$\alpha|\overline{0}>+\beta|\overline{0}>\neq[\alpha(|000>+|111>)+\beta(|000>-|111>)]^{\otimes 3}.$$

Comme un code quantique Q est un sous espace de l'espace de Hilbert $\mathbb{C}^{q^n}$, alors $Q^\perp$ est un espace de Hilbert et vérifie :

$$\mathbb{C}^{q^n}=Q\oplus Q^\perp.$$

On appelle la projection de Q l'application linéaire $P : x_Q + x_{Q^\perp} \longrightarrow x_Q$, avec$Q^\perp$ désignat le dual du code Q par rapport au produit scalaire de l'espace de Hilbert (voir l'appendice). La projection est un opérateur auto-adjoint[6] et vérifie $P^2 = P$.
L'opérateur $I - P$ est une projection de $Q^\perp$.

Un projecteur peut être facilement construit en choisissant une base orthonormale $\{|\alpha_1 > |, \ldots, |\alpha_K >\}$ de Q en formant la matrice suivante[7] :

$$\sum_{i=1}^{K} |\alpha_i >< \alpha_i|,$$

Après avoir encoder l'état $|\phi >$ de sorte à obtenir un état $|\psi >$ de Q (on dit qu'on a préparé l'état $|\psi >$ de Q), on envoi l'information et on obtient l'état $E|\psi >$ avec E l'opérateur erreur, un mesurement est effectué (en prenant $PE|\psi >$) pour détecter si le bruit a pris $|\psi >$ en dehors de Q i.e., dans $Q^\perp$. Donc formellement l'erreur E est détectable si on a :

$$PEP = c_E P.$$

Ce qui est équivalent à

$$< c_1|E|c_2 >= \lambda_E < c_1, c_2 >, \tag{3.2}$$

pour tout $c_1, c_2 \in Q$. Si on choisit une base orthonormale de Q, $\{|c_1 >, |c_2 > , \ldots\}$, alors l'égalité (3.2) devient $< c_i|E|c_j >= \lambda_{i,j}\delta_{i,j}$.

[6]Voir appendice pour cette définition.
[7]Voir l'appendice pour la définition de la matrice de densité.

Remarque 3.4.2 *Si un code quantique peut détecter toutes les erreurs dans un certain sous ensemble $\mathcal{D}$ de $\mathcal{G}_n$, alors il peut détecter toutes les erreurs qui sont dans le sous espace vectoriel engendré par $\mathcal{D}$, cela est dû à la linéarité de la mécanique quantique.*

Soit S un ensemble d'erreurs on dit que Q est S correcteur si et seulement si pour tout $|\psi >\neq |\phi >$ dans Q et pour tout E_i et E_j dans S on a :

$$E_i|\psi >\neq E_j|\phi > .$$

Il a été prouvé par Bennett et al. [7] qu'un code Q est S correcteur si et seulement s'il est S^*S code détecteur[8].

3.4.1 Les bases d'erreurs

En théorie classique les seules erreurs sont les erreurs de positions dûe au flip, en théorie quantique nous avons plusieurs types d'erreurs.

Exemple 3.4.3 *La représentation en coordonnés des qu-bits est :*

$$|0 >= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2, |1 >= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2.$$

Ça induit les représentations en coordonnées suivantes.

[8] $S^*S = \{A^*B/A, B \in S\}$.

$$|01>=|0>\otimes|1>=\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\begin{pmatrix}0\\1\end{pmatrix}\\0\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

De même on peut avoir $|00>=\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$,

$$|11>=\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\ et\ |10>=\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

L'erreur de position ou le bit flip correspond à $|0>\mapsto|1>$ *et* $|1>\mapsto|0>$.

En utilisant la représentation en coordonnées de $|0>$ *et* $|1>$, *le bit flip de* $|\psi>$ *correspond à* $X|\psi>$ *où* $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

L'erreur de phase correspond à $|0>\mapsto|0>$ *et* $|1>\mapsto-|1>$, *pour* $|\psi>$ *ça correspond à* $Z|\psi>$ *où* $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$.

Une erreur combiné $|0>\mapsto i|1>$ *et* $|1>\mapsto -i|0>$, *pour* $|\psi>$ *ça correspond à* $Y|\psi>$ *où* $Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, *puisque* $Y=iXZ$.

Les matrices X,Y,Z *et* $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ *sont appelés* ***matrices de Pauli***

et les opérateurs associés à ces matrices les opérateurs de Pauli.

La matrice de $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
est dite matrice de Hadamard, elle transforme $|0>$ en $|0> + |1>$ et $|1>$ en $|0> - |1>$. Le produit tensoriel de X et Y est :

$$X \otimes Y = \begin{pmatrix} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}.$$

On peut supposer que les erreurs sur chaque qu-bit sont indépendantes et que X, Y, Z ont la même probabilité, puisque il a été démontrer [43] que tout code qui corrige ce type d'erreurs peut corriger un modèle arbitraire d'erreurs.

Donc explicitement les erreurs ont l'effet suivant :

$$\begin{aligned} I|\psi> &\quad \text{Prob. } 0.25 \quad \text{(pas d'erreur)}. \\ X|\psi> &\quad \text{Prob. } 0.25 \quad \text{(bit flip)}. \\ Y|\psi> &\quad \text{Prob. } 0.25 \quad \text{(bit-phase flip)}. \\ Z|\psi> &\quad \text{Prob. } 0.25 \quad \text{(phase flip)}. \end{aligned}$$

Les matrices de Pauli sont importantes puisque les erreurs peuvent être exprimées comme une combinaison linéaire de ces matrices. En plus elles forment une base de l'espace des 2×2 matrices. Ce qui donne que toute

erreur sur un qu-bit $|\phi> \mapsto E|\phi>$ peut être exprimée comme combinaison linéaire des matrices de Pauli ;

$$\phi \mapsto (aI + bX + cY + dZ)|\phi> = aI|\phi> + bX|\phi> + cY|\phi> + dZ|\phi> .$$

Le processus de correction peut être modelé par une transformation linéaire qui enchevêtre l'état érroné $M|\psi>$ avec un "ancilla" $|A>$ et transforme la combination a un état correcte

$$M|\psi> \otimes A \longmapsto |\psi> \otimes A_M.$$

Si l'application $M \mapsto A_M$ est injective, alors le code est dit non dégénéré, sinon il est dit dégénéré[9].

Exemple 3.4.4 *Le code donné par :* $|0> \mapsto |000>$ *et* $|1> \mapsto |111>$ *permet de corriger les erreurs d'un unique bit-flip suivantes :*

$X \otimes I \otimes I, I \otimes X \otimes I, I \otimes I \otimes X.$

Le produit tensoriel de t de ces matrices forment une base de l'espace des matrices $2^t \times 2^t$ à coefficients complexe.

On peut étendre le principe précédent d'erreurs aux cas q-aire en faisant une généralisation comme suit :
Soient a et b deux éléments dans $\mathbb{F}_q$. On définit les opérateurs unitaires[10]

[9] On reviendra à la notion de dégénérescence dans le cas des codes stabilisés.

[10] Les lois de la mécanique quantique exigent que toute transformation sur un système quantique doit être linéaire, en plus pour préserver la normalisation tout opérateur de l'espace de Hilbert qu'on considère doit être unitaire

$X(a)$ et $Z(b)$ sur $\mathbb{C}^q$ par

$$X(a)|x>=|a+x>,\ Z(b)|x>=\omega^{tr(bx)}|x>,$$

tr désigne la fonction trace de $\mathbb{F}_q$ sur $\mathbb{F}_p$, et $\omega = \exp(2\pi i/p)$[11]. L'opérateur $X(a)$ correspond à l'erreur de position et l'opérateur $Z(b)$ correspond à l'erreur de phase. On considère l'ensemble $\mathcal{E} = \{X(a)Z(b)|a, b \in \mathbb{F}_q\}$, alors $\mathcal{E}$ vérifie :

1. L'opérateur identité est dans $\mathcal{E}$.
2. Le produit de deux éléments de $\mathcal{E}$ est un autre élément multiplié par un scalaire.
3. $Tr(A^*B) = 0$ pour A et B distincts dans $\mathcal{E}$.

Grace à la dernière propriété on peut montrer que $\mathcal{E}$ est une base d'erreur de $\mathbb{C}^q$.

Lemme 3.4.5 *Si $\mathcal{E}_1$ et $\mathcal{E}_2$ sont deux bases d'erreurs, alors*

$$\mathcal{E} = \{E_1 \otimes E_2 | E_1 \in \mathcal{E}_1,\ E_2 \in \mathcal{E}_2\}$$

est une base d'erreur.

Au fait la preuve vient directement de la définition.

Maintenant si $\mathsf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^n}$, alors $X(\mathsf{a}) = X(a_1) \otimes X(a_2) \otimes \ldots \otimes X(a_n)$ et $Z(\mathsf{a}) = Z(a_1) \otimes Z(a_2) \otimes \ldots \otimes Z(a_n)$ et alors on obtient le corollaire suivant.

[11] On choisit ω ainsi pour que les opérateurs de la base d'erreur soient normalisés.

Corollaire 3.4.6 *L'ensemble* $\mathcal{E}_n = \{X(\mathsf{a})Z(\mathsf{b})|\, \mathsf{a}, \mathsf{b} \in \mathbb{F}_q^n\}$ *est une base d'erreurs sur l'espace* $\mathbb{C}^{q^n}$

3.5 Les codes stabilisés

Les codes stabilisés sont importants en pratique car la plupart des codes correcteurs utilisés pour le schéma du défaut toléré utilisent ce formalisme [27], en particulier les codes CSS sont des codes stabilisés. En plus tout code quantique Q^* peut être contenu dans un code stabilisé Q et la capacité de détection et de correction de Q^* est borné par celle de Q.

On considère le groupe $\mathcal{G}_n$ défini par

$$\mathcal{G}_n = \{\omega^c X(\mathsf{a})Z(\mathsf{b})|\mathsf{a}, \mathsf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}.$$

$\mathcal{G}_n$ est appelé **le groupe d'erreurs associé à la base d'erreurs** $\mathcal{E}_n$. C'est un groupe, d'ordre pq^{2n} et il est engendré par les matrices de $\mathcal{E}_n$. Soit $\mathcal{S}$ un sous groupe abelien[12] de $\mathcal{G}_n$, un code quantique est dit **stabilisé** par $\mathcal{S}$, si c'est un sous espace de $\mathbb{C}^{q^n}$ qui vérifie

$$Q = \cap_{E \in \mathcal{S}} \{\upsilon \in \mathbb{C}^{q^n} \mid E\upsilon = \upsilon\}. \tag{3.3}$$

Autrement Q est l'intersection des espaces propres des éléments de $\mathcal{S}$ qui sont associés à la valeur propre 1, et donc le code Q peut être décrit en terme d'opérateurs d'erreurs de son stabilisateur puisque ces opérateurs n'affectent

[12]La condition sur le groupe d'être abelien est une condition nécessaire sinon le code costruit sera un code trivial.

pas les mots du code. En plus si $\mathcal{S}$ est d'ordre s, alors Q a pour dimension $tr(P) = q^{n-s+1}$ [4].

Exemples :

1. Si on considère l'état $|\psi >= \alpha|000 > +\beta|111 >$, il est invariant par les opérateurs $Z \otimes Z \otimes I$ et $Z \otimes I \otimes Z$, car $|\psi >= Z \otimes Z \otimes I|\psi >$ et $|\psi >= Z \otimes I \otimes Z|\psi >$.
2. Le code de Shor répété $[[9, 1, 3]]_2$, admet pour groupe stabilliseur le groupe d'éléments :

$$
\begin{aligned}
&Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I,\\
&I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I,\\
&I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I,\\
&I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I,\\
&I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I,\\
&I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes Z,\\
&X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I,\\
&I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X
\end{aligned}
$$

Remarque 3.5.1 *Pour un code stabilisé par $\mathcal{S}$ l'opérateur projection P peut être donné sous la forme*

$$P = \frac{1}{|\mathcal{S}|} \sum_{E \in \mathcal{S}} E. \tag{3.4}$$

Pour trouver une base du code stabilisé par un groupe $\mathcal{S}$, on considère n'importe quelle base $\{|a >\}$ de l'espace de Hilbert et on calcule $P|a >$. Si $P|a >= |a >$ on garde $|a >$ comme étant un élément de la base du code stabilisé.

Un code Q stabilisé par le groupe $\mathcal{S}$ peut détecter toutes les erreurs de $\mathcal{G}_n$ qui sont des multiples par scalaire d'eléments de $\mathcal{S}$ ou celles qui ne commutent pas avec les éléments de $\mathcal{S}$. En particulier une erreur dans $\mathcal{G}_n$ qui n'est pas détectable par Q doit commuter avec tous les éléments du groupe $\mathcal{S}$.

Soit $E = \omega^c X(a)Z(b) = \omega^c E_1 \otimes \ldots \otimes E_n$ un élément du groupe d'erreurs $\mathcal{G}_n$. Le poids de E noté $wt(E)$ est défini par :

$$wt(E) = |\{E_i \neq I\}|,$$

en particulier le poids de αI est nul.

Comme dans le cas classique on a l'inégalité suivante :

$$wt(EE') \leq wt(E) + wt(E').$$

Exemple 3.5.2 *Soit $E \in \mathcal{P}_4$, tels que $E = X \otimes I \otimes X \otimes Y$, alors $wt(E) = 3$.*

Définition 3.5.3 *On dit qu'un code quantique Q admet pour distance minimale d, s'il peut détecter toutes les erreurs dans $\mathcal{G}_n$ de poids inférieur à d, mais ne peut pas détecter quelques erreurs de poids d.*

Un code quantique Q est **pur jusqu'à** t si son groupe stabiliseur ne contient pas de matrices de poids plus petit que t. Le code Q est dit **pur** s'il est pur jusqu'à sa distance minimale. Sinon il est **dégénéré**. Cette notion n'a pas d'équivalent en théorie classique.

Exemple 3.5.4 *Le code de Shor répété est un code dégénéré qui peut corriger une erreur.*

Lemme 3.5.5 *(Ashikhmin-Knill[4]) Un code quantique de distance minimale d peut détecter $d-1$ erreurs et corriger $\frac{d-1}{2}$ erreurs.*

Nous avons aussi la version de la borne de Singleton dans le cas quantique donnée par le lemme suivant.

Lemme 3.5.6 *(La borne de Singleton quantique [43]) Soit Q un $[[n,k,d]]_q$ code quantique, alors les paramètres n,k,d vérifient*

$$k+2d \leq n+2,$$

Si on a l'égalité alors Q est pur.[13]

3.6 De la théorie classique à la théorie quantique

On pourait croire que la théorie quantique n'a rien à voir avec la théorie classique à cause des propriétés étranges, comme la superposition des états, le théorème du non-clonage et l'intrication. Cependant ce n'est pas le cas à partir des codes classiques on peut toujours construire la machinerie mathématique pour la construction et l'analyse des codes quantiques et vis-versa [**?**, 20]. Cela a permis de montrer que les deux théories sont similaires. Une simple, surprenante et élégante construction de codes quantiques a été introduite en 1996 par Calderbank et Shor [14] et Steane [67] pour les codes binaires [14].

[13] À cause de cette borne le plus petit code qui peut corriger une erreur est le code $[[5,1,3]]$.

[14] Il existe d'autres constructions de codes quantiques dérivés des codes classiques par la construction topologique [41] ou en utilisant les subsystèmes [56]

Elle a été appelée dés lors la CSS construction. Cela a été généralisé pour les autres caractéristiques par différentes manières [29, 40, 50]. Cette construction donne le lien le plus direct entre les deux théories, en plus les codes CSS ont des propriétés les plus appropriées et utilisées pour le schéma du défaut toléré. Ces codes sont aussi appelés codes additifs, puisqu'ils sont liés aux codes additifs ($\mathbb{F}_p$-linéaire). On rappele qu'une partie C de $\mathbb{F}_{p^r}^n$ est dite $\mathbb{F}_p$-linéaire sur $\mathbb{F}_{p^r}$ si c'est un espace vectoriel par rapport au corps $\mathbb{F}_p$, alors si k est la dimension de C sur $\mathbb{F}_p$, C admet p^{kr} mots.

Le paragraphe suivant sera consacré au développement de la CSS dans le cas q-aire, nous adoptons l'approche de Kim et al. [40]. Avant cela rappelons que pour $(\mathsf{a}|\mathsf{b})$ et $(\mathsf{a}'|\mathsf{b}')$ dans $\mathbb{F}_q^{2n}$, on définit le produit scalaire suivant :

$$(\mathsf{a}|\mathsf{b}) * (\mathsf{a}'|\mathsf{b}') = tr_{q/p}(\mathsf{a}\mathsf{b}' - \mathsf{a}'\mathsf{b}),$$

la fonction tr désigne la trace de $\mathbb{F}_q$ sur $\mathbb{F}_p$.

Proposition 3.6.1 *(Ashikhmin-Knill[4]) Soit $C \subset \mathbb{F}_q^{2n}$ un $\mathbb{F}_p$-linéaire code admettant p^k mots. Soit $C^{\perp *}$ le dual de C par rapport au produit $*$. Si $C \subset C^{\perp *}$, alors il existe un code quantique $[[n, n-k/r, d]]_q$ où $d = d(C^{\perp *} \setminus C)$.*

Pour $\mathsf{x}, \mathsf{y} \in \mathbb{F}_{q^2}^n$ on définit $\mathsf{x} \circ \mathsf{x} = \sum(x_i y_i^q - x_i^q y_i)$ c'est une forme $\mathbb{F}_q$-bilinéaire. Pour chaque $\gamma_0 \in \mathbb{F}_q$ on choisit $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ tel que $\gamma^q = \gamma_0 - \gamma$

Lemme 3.6.2 *Soit $D \subset \mathbb{F}_q^{2n}$ un $\mathbb{F}_q$-linéaire code satisfaisant que $D \subset D^{\perp \circ}$ où $D^{\perp \circ}$ est le dual de D par rapport à $\circ$. On définit l'application $\mathbb{F}_q$-linéaire suivante $f : \mathbb{F}_{q^2}^n \mapsto \mathbb{F}_q^{2n}$, $f(x_1, \ldots, x_n) = (x_1^{(1)}, \ldots, x_n^{(1)} | x_1^{(2)}, \ldots, x_n^{(2)})$ où $x_i = x_i^{(1)} + \gamma x_i^{(2)}$, pour $i \in [n]$. Alors $f(D) \subset f(D^{\perp \circ}) = (f(D^{\perp}))^{\perp *}$ où $(f(D))^{\perp *}$ désigne le dual de $f(D)$ par rapport à $*$.*

Proposition 3.6.3 *Soient $C_1 \subset C_2 \subset \mathbb{F}_q^n$ des codes $\mathbb{F}_q$-linéaire, tels que $C_2^\perp \subset C_1^\perp$. Soit ω un élément primitif de $\mathbb{F}_q^2$ et $D = \omega C_1 + \omega^q C_2^\perp \subset \mathbb{F}_q^2 n$. Alors on a $D^{\perp\circ} = \omega^q C_1^\perp + \omega C_2$, d'où $D \subset D^{\perp\circ}$ et $d(D^{\perp\circ} \setminus D) = \min\{d(C_2 \setminus C_1, d(C_1^\perp \setminus C_2^\perp)\}$.*

Les résultats précédents sont utilisés pour la preuve du théorème suivant.

Théorème. 3.6.4 *Soient $q = p^r$ avec p un nombre premier et $r \geq 1$. $C_1 = [n, k_1, d_1]$ et $C_2 = [n, k_2, d_2]$ deux codes $\mathbb{F}_q$-linéaires de $\mathbb{F}_q^n$, tels que $C_1 \subset C_2$. Alors il existe un code stabilisé $[[n, k_2 - k_1, d_Q]]_q$ code quantique où $d_Q = \min wt\{(C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\} \geq d_* = \min(d_1^\perp, d_2)$. Ce code est pur jusqu'à d_*.*

Preuve 3.6.5 *Soit $D = \omega C_1 + \omega^q C_2^\perp$. Alors par la proposition 3.6.3 et lemme 3.6.2 nous obtenons que $f(D) \subset (f(D))^{\perp *}$. $f(D)$ est un $\mathbb{F}_q$ code linéaire de $\mathbb{F}_q^2$, alors c'est un code $\mathbb{F}_p$-linéaire avec p^r éléments, où $m = r(k_1 + n - k_2)$, donc en appliquant la proposition 3.6.1 pour $C = f(D)$. On obtient le résultat.*

En appliquant le théorème 3.6.4 pour $C_1 = C^\perp$ et $C_2 = C$, on peut déduire directement le corollaire suivant.

Corollaire 3.6.6 *Si un code linéaire C de paramètres $[n, k, d]$ contient son dual $C^\perp$, alors il existe un code quantique avec les paramètres $[[n, 2k-n, d_Q \geq d]]_q$, qui est pur jusqu'à d.*

Si on considère des codes sur $\mathbb{F}_{q^2}$, alors nous pouvons considérer le produit scalaire Hermitian, dans ce cas aussi on peut construire des codes classiques linéaires des codes quantiques en utillisant la la dualité Hermitiènne.

Corollaire 3.6.7 *S'il existe un code linéaire C de paramètres $[n,k,d]_{q^2}$, vérifiant $C \subset C^{\perp_h}$. Alors il existe un $[[n, n-2k, \geq d]]_q$ code quantique pur jusqu'à d.*

Preuve 3.6.8 *Voir [29, Corollaire 2].*

3.6.1 Construction systématique des codes CSS

Le procédé expliqué dans la remarque 3.5.1 pour trouver le code stabilisé peut être trés long à cause du fait que le groupe stabiliseur croît d'une façon exponentielle avec le groupe générateur. Cependant il existe un procédé plus simple pour trouver ces codes CSS ; en effet, soient C_1 et C_2 deux codes classiques de paramètres $[n,k_1]$ et $[n,k_2]$ tels que C_1 et $C_2^{\perp}$ corrigent t erreurs et $C_2 \subset C_1$. On définit un $[[n, k_1 - k_2]]$ code quantique capable de corriger des erreurs sur t qu-dits. Le code est appelé CSS code et il est donné par la construction suivante :

On considère un mot x de C_1, et on définit l'état quantique suivant

$$|x + C_2 >= \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y> .$$

Soit x' un mot de C_1 tels que $x - x' \in C_2$, alors il est facile de voir que $|x + C_2 >= |x' + C_2 >$ et alors l'état $|x + C_2 >$ dépend de C_1/C_2, alors le code CSS est défini comme étant l'espace vectoriel engendré par l'ensemble

$$\{|x + C_2 > \ | x \in C_1\}.$$

Le nombre de classes est $|C_1|/|C_2|$, alors la dimension du CSS code (C_1, C_2)

est $|C_1|/|C_2| = q^{k_1-k_2}$ et alors un CSS code est un $[[n, k_1 - k_2]]$ code quantique. Un état général est de la forme :

$$|\psi >= \sum_{x \in C_1} \alpha_x \sum_{y \in C_2} |x + y> . \tag{3.5}$$

Exemple 3.6.9 *Un célèbre code construit par la CSS construction est le code dit de Steane. Il a été construit avec $C_1 = [7, 4, 3]$ code de Hamming et $C_2 = C_1^{\perp} \subset C_1$: La matrice de contrôle de C_1 est*

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

On peut obtenir un code quantique de paramètres $[[7, 1, 3]]$ qui peut corriger une erreur sur un qu-bit. On détermine les mots du code C_2 et on déduit

$|0 + C_2 >= \frac{1}{\sqrt{8}}[|0000000 > +|1010101 > +|0110011 > +|0001111 > +|1011010 > +|0111100 > +|1101001 > +|0000000 >]$.

On peut prendre comme mot de C_1 qui n'est pas dans C_2 le mot $(1, 1, 1, 1, 1, 1, 1)$ on le note 1, on obtient alors $C_2 \subset C_1$ et $|1 + C_2 >= \frac{1}{\sqrt{8}}[|1111111 > +|0101010 > +|1001100 > +|0011001 > +$
$|1110000 > +|0100101 > +|1000011 > +|0010110 >]$.

Il est visible que l'écriture précédente de la base d'un code est déjà ardue en longueur 7 et dimension 2, que serait elle pour des longueurs et dimensions élevés ?

Nous savons qu'un code stabilisé est entièrement défini par son groupe stabiliseur, cependant le procédé de trouver ce stabiliseur peut être long et le

temps pour le trouver augmente d'une façon exponentielle en fonction de la dimension, c'est pour cela que Calderbank et al. [14] ont introduit un simple procédé en utilisant une équivalence entre les codes linéaires et les codes quantiques stabilisés pour trouver le groupe stabiliseur d'un code construit à partir d'un code linéaire. L'idée est de construire la matrice suivante à partir des matrices de contrôle de $H(C_2^{\perp})$ et $H(C_1)$, comme suit :

$$\left(\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right)$$

Alors dans les lignes de $H(C_2^{\perp})$ on remplace 1 par X et 0 par I et dans les lignes de $H(C_1)$ on remplace 1 par Z et 0 par I. La condition exigée sur les codes $C_2 \subset C_1$ permet d'assurer la commutativité du groupe stabiliseur qui est équivalente à $H(C_2^{\perp})H(C_1)^T = 0$, or nous avons

$$H(C_2^{\perp})H(C_1)^T = [H(C_1)G(C_2)]^T = 0.$$

Exemple 3.6.10 *Le code de Steane donné dans l'exemple 3.6.9 admet pour matrice (de contrôle) la matrice de la forme suivante :*

$$(C_1|C_2) = \left(\begin{array}{ccccccc|ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

Le groupe stabiliseur du code de Steane est engendré par

$$\{IIIXXXX, XIXIXIX, IIIZZZZ, IZZXXZZ, ZIZIZIZ\}.$$

Chapitre 4

Les codes BCH classiques et quantiques

Mathematicians stand on each

other's shoulders .

C. F. Gauss

Soit α une racine primitive $n$ième de l'unité sur $\mathbb{F}_q$, un code cyclique C de longueur n sur $\mathbb{F}_q$ est appelé code BCH[1] de distance construite $\delta \geq 1$, s'il existe $b \in \mathbb{N}$ tels que le polynôme générateur g vérifie :

$$g(\alpha^b) = \cdots = g(\alpha^{b+\delta-2}) = 0.$$

Alors C est engendré par

$$g(x) = ppcm\{M_b(x), M_{b+1}(x), \ldots, M_{b+\delta-2}(x).\} \tag{4.1}$$

[1]Cette appelation est dûe aux auteurs qui les ont construits R. C. Bose, D. K. Ray-Chaudhuri et A. Hocquenghem.

On note ce code $B_q(n, \delta, b)$, ou simplement $B_q(n, \delta)$ si $b = 1$. Dans ce dernier cas, il est dit BCH **au sens strict**. Lorsque α est un élément primitif du corps i.e., quand $n = q^s - 1$, alors $B_q(n, \delta, \alpha, b)$ est appelé code BCH **primitif**. La classe des codes BCH est l'une des plus anciennes classe de codes et les plus utilisés en pratique, car malgré qu'elle soit mauvaise asymptotiquement, pour des longueurs finies elle a un trés bon comportement. En plus les codes BCH sont simples à encoder et relativement simple à décoder, en plus ils ont une grande capacité de correction [49, Cha. 9, p. 258]. Malgré cela plusieurs de leurs propriétés sont restées inconnues [19].

Dans ce chapitre nous nous sommes intéressés à déterminer les paramètres d'une classe de codes BCH qualifiée par Macwilliams et Sloane dans [49, Cha. 9, p. 258] comme "interesting non-primitive BCH codes". Nous donnons en détail les résultats déjà parus dans [32]. Bien que nous ne considérons que les codes BCH au sens strict, il est à remarquer que ces résultas peuvent être généralisés aux codes $B_q(n, \delta, \alpha, b)$ au sens non-strict avec $n = q^m + 1$, $m > 1$, b et δ vérifiant $b + \delta - 2 < q$.

Récement Aly et al. [3] ont étudié de près les propriétés des codes BCH non nécessairement primitifs. Ils ont considéré la dimension, la distance minimale et l'auto-orthogonalité. En utilisant une généralisation du théorème de Farr [49] ils ont donné une borne sur la distance minimale. Nous généralisons le même théorème à nos codes et nous donnons une autre borne en faisant la généralisation du théorème de Peterson [49], cela nous a permis de donner exactement la distance minimale dans certains cas et de dériver une autre borne qui dans certains cas est beaucoup meilleur que les deux premières.

Tous les résultats de [3] sont basés sur le lemme et le théorème suivants.

Nous les énonçons en vue de prouver que nos codes BCH ne peuvent pas être considérés par [3].

Lemme 4.0.11 *([3, lemme 09]) Soit q la puissance d'un nombre premier, n un entier positif tel que $pgcd(n,q) = 1$ et $q^{\lceil m'/2 \rceil} < n \leq q^{m'} - 1$ avec $m' = \mathrm{ord}_n\, q$. Si x et y sont des entiers distincts vérifiants :*

$$1 \leq x, y \leq \min\{\lfloor nq^{\lceil m'/2 \rceil}/(q^{m'} - 1) - 1 \rfloor, n - 1\}, \tag{4.2}$$

tels que $x, y \neq 0 \mod q$, alors les classes cyclotomiques de x et y sont distinctes.

Théorème. 4.0.12 *([3, Théorème 1]) Soit q la puissance d'un nombre premier tels que $pgcd(n,q) = 1$, avec $m' = \mathrm{ord}_n\, q$, alors un code BCH au sens strict de longueur $q^{\lceil m'/2 \rceil} < n \leq q^{m'} - 1$ sur $\mathbb{F}_q$, de distance construite δ vérifiant :*

$$2 \leq \delta \leq \min\{\lfloor nq^{m'/2}/(q^{m'} - 1) \rfloor, n\} \tag{4.3}$$

admet pour dimension

$$k = n - m' \lceil (\delta - 1)(1 - 1/q) \rceil.$$

Pour $n = q^m + 1$ avec $m > 1$, d'après le lemme 2.3.10 on trouve que $m' = \mathrm{ord}_n\, q = 2m$. Si on substitue la valeur de n et m' dans les inégalités à droite des équations 4.2 et 4.3 du lemme 4.0.11 du théorème 4.0.12, on trouve successivement les valeurs 0 et 1 ; chose qui ne peut avoir lieu, car cela veut dire que les équations 4.2 et 4.3 deviennent $1 \leq x, y \leq 0$ et $2 \leq \delta \leq 1$.

4.0.2 La dimension des codes BCH

Comme un code BCH est un code cyclique, alors il est engendré par un polynôme g. Du théorème 2.4.1 nous avons que la dimension k est égale à $n-$ deg g. Puisque le générateur d'un code $B_q(n,\delta)$ est $g = ppcm(M_1,\ldots,M_{\delta-1})$, souvent il n'est pas facile de trouver le générateur de $B_q(n,\delta)$, puisqu'on peut avoir $M_i = M_j$ pour $i \neq j$.

Théorème. 4.0.13 *([49]) Pour un code $B_q(n,\delta,b)$ de longueur n et distance construite δ, nous avons :*

$$dim(B_q(n,\delta,b) \geq n - (\delta-1)\,\mathrm{ord}_n\, q.$$

La borne donnée par le théorème 4.0.13 est souvent large et insuffisante, d'où la nécessité de trouver la dimension exacte pour ces codes. Bien évidemment, nous pouvons calculer la dimension de $B_q(n,\delta,b)$ si on connait le polynôme générateur, ce qui n'est pas toujours évident comme nous l'avons expliqué plus haut.

Dans le théorème suivant nous donnons la dimension de nos code BCH.

Théorème. 4.0.14 *Soit q la puissance d'un nombre premier, et m un entier plus grand que 1. Alors un code $B_q(n,\delta)$ de longueur $n = q^m+1$ et de distance construite δ tel que $2 \leq \delta \leq q$ admet pour dimension,*

$$k = q^m + 1 - 2m(\delta-1).$$

Preuve 4.0.15 *Les lemmes 2.3.12 et 2.3.14, donnent que les classes cyclotomiques C_j pour $j < q$ sont disjointes et de cardinalité $2m$. Comme à chaque*

polynôme minimal M_j de α^j correspond une classe cyclotomique C_j ; on en deduit que les polynômes minimals sont distincts et chacun de degré $2m$. Ce qui donne que le polynôme générateur de $B_q(n, \delta)$ est

$$g = \prod_{i=1}^{\delta-1} M_i,$$

et son degré est $2m(\delta - 1)$. Alors,

$$dim\ B_q(n, \delta) = q^m + 1 - 2m(\delta - 1).$$

Comme le dual d'un $[n, k]$ code cyclique est un $[n, n - k]$ code cyclique on obtient directement du théorème 4.0.14 le corollaire suivant.

Corollaire 4.0.16 *Le code dual $B_q(n, \delta)^\perp$ a pour dimension*

$$k^\perp = 2m(\delta - 1).$$

4.0.3 La distance minimale des codes BCH

Il existe des algorithmes probablistiques pour la détermination de la distance minimale de grands codes [15, 45], cependant le problème de la détermination de la valeur exacte de la distance minimale n'a pas été résolue pour plusieurs familles de codes, en particulier pour les codes BCH. Ça a même été démontré par Dumer et al. [25] que l'approximation de la distance minimale des codes linéaires est un problème NP-dur. Dans [36, 49, 59] et dans d'autres ouvrages sous certaines conditions le problème est partiellement résolu ou des bornes ont été données. Ces bornes permettent en utilisant des

algorithmes de recherche de trouver physiquement le mot du plus petit poids quand on ne peut pas le faire mathématiquement[2]. Une étude comparative de ces méthodes pour les codes BCH primitifs a été donnée par S. K. Houghten et J. L. Wallis dans [34]. Évidemment les bornes de Singleton et Griesmer s'appliquent, mais souvent ces bornes sont larges ; il existe une autre borne dite **la borne** BCH donnée par le lemme suivant.

Lemme 4.0.17 *([49, Théorème 8.7]) Soit C un code cyclique de longueur n. Si le polynôme générateur de C admet s racines consécutifs, alors la distance minimale d de C vérifie,*

$$d \geq s + 1.$$

Du lemme 4.0.17 nous pouvons déduire que la distance minimale d d'un code $BCH(n, \delta, b)$ vérifie :

$$d \geq \delta.$$

Dans la suite de ce paragraphe nous donnons des bornes supérieures pour la distance minimale de nos codes BCH.

Pour $n = q^m + 1$ et $\delta \leq q$ en utilisant la borne de Singleton et le résultat du théorème 4.0.14 nous obtenons le la borne suivante :

$$\delta \leq d_{\min} \leq 2m(\delta - 1) + 1. \tag{4.4}$$

Le théorème suivant qui est une conséquence du théorème 4.0.14 nous permet d'améliorer la borne (4.4). Il est à noter que ce résultat est la généralisation

[2]La recherche exhaustive du mot de plus petit poids n'est pas faisable, du fait que si k est la dimension du code C, alors C contient q^k mots, d'où l'importance des bornes supérieures et inférieures sur d.

du théorème dit de Farr donné dans [49] p. 259 aux cas non binaires et non primitifs.

Théorème. 4.0.18 *Soit $B_q(n, \delta)$ un code BCH de longueur $n = q^m + 1$ et de distance construite $\delta \leq q$, tels que*

$$\sum_{i=0}^{2(\delta-1)} \binom{q^m+1}{i} (q-1)^i > q^{2m(\delta-1)}, \tag{4.5}$$

alors nous avons

$$d_{min} \leq 4(\delta - 1). \tag{4.6}$$

Preuve 4.0.19 *Supposons que $d_{min} \geq 4(\delta-1)+1$, du théorème 4.0.14 la dimension est $q^m+1-2m(\delta-1)$. Par le théorème d'empilement des sphères nous avons :*

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{q^m+1}{i} (q-1)^i \leq q^{2m(\delta-1)},$$

cela donne l'inégalité suivante :

$$\sum_{i=0}^{2(\delta-1)} \binom{q^m+1}{i} (q-1)^i \leq q^{2m(\delta-1)},$$

contradiction.

Quelques fois il est possible de donner exactement la distance minimale des codes BCH comme nous le faisons dans la généralisation suivante du théorème de Peterson aux cas non-binaires. La preuve est similaire à la preuve du [49, Théorème 9.2.3], nous avons remarqué[3]qu'elle peut être étendu à nos

[3]La plupart des résultats donnés dans [49] sont établis pour les codes binaires, en admettant qu'ils peuvent être généralisés aux autres caractéristiques, or ce n'est pas toujours le cas comme ça à été démontré plusieurs fois ; cela est dû aux propriétés de $\mathbb{F}_2$.

codes BCH.

Théorème. 4.0.20 *Un code BCH noté C qui est de longueur $n = b\delta$ et de distance construite δ admet pour distance minimale exactement δ.*

Preuve 4.0.21 *Comme nous avons supposé que le code C admet pour distance construite δ, alors d'après le lemme 4.0.17 on a $d_C \geq a$. Soit α une racine primitive nième de l'unité tels que $\alpha^{ib} \neq 1$. Puisque*

$$(x^n - 1) = (x^b - 1)(1 + x^b + x^{2b} + \ldots + x^{(\delta-1)b}),$$

les éléments $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ ne sont pas racines de $x^b - 1$, alors elles doivent être des racines de $1 + x^b + x^{2b} + \ldots + x^{(\delta-1)b}$, ce qui donne un mot de poids δ dans C et donc $d_C = \delta$.

Dans le cas où m est impair, ce qui implique que $q + 1$ divise $q^m + 1$. Alors dans ce cas le code $B_q(n, \delta)$ contient un mot de poids $q+1$; la distance minimale est donc inférieure ou égale à $q + 1$ ce qui nous donne une autre borne, dans certains cas elle est meilleure que les précédentes.

Corollaire 4.0.22 *La distance minimale d'un code BCH de longueur $n = q^m + 1$, avec m impair et de distance construite $\delta \leq q$ est au plus*

$$q + 1. \tag{4.7}$$

Remarque 4.0.23 *Il est évident que si q est impair alors tous les codes $B(q^m + 1, 2)$ ont pour distance minimale $d = 2$; du fait que $q^m + 1$ est pair et donc divisible par 2, donc d'après le théorème 4.0.20 $d = 2$.*

Dans le but de comparer les bornes données précédemment à la borne de Griesmer et à la distance minimale exacte d déduite du théorème 4.0.20 ou calculé en utilisant la recherche exhaustive, nous donnons la table numérique suivante. Nous utilisons aussi le fait que $BCH(n, \delta + 1) \subset BCH(n, \delta)$ et alors nous avons $d_{BCH(n,\delta)} \leq d_{BCH(n,\delta+1)}$. Dans certains cas ce fait nous a permis de trouver des bornes étroites ou de donner exactement d. la notation $(\times)$ veut dire que la borne (4.7) n'est pas vérifiée. La notation (?) veut dire que nous n'avons pas pu trouvé exactement d ou une borne étroite. Cependant nous avons les bornes (4.6) et (4.7) ou les bornes de Griesmer et BCH.

q	δ	m	Borne (4.6)	Griesmer	Borne (4.7)	d
5	2	2	4	4	$\times$	2
		3	4	5	6	2
		4	4	7	$\times$	2
		5	4	10	6	2
		7	4	12	6	2
5	4	2	12	10	$\times$	7
		3	12	15	6	6
		4	12	20	$\times$	$5 \leq d$
		5	12	24	6	$5 \leq d \leq 6$
		6	12	29	$\times$	?
		7	12	34	6	$4 \leq d \leq 6$

q	δ	m	Bound 4.6	Griesmer bound	Bound 4.7	d
5	5	3	16	20	6	6
		4	16	26	×	?
		5	16	33	6	6
		6	16	39	×	?
7	3	2	8	7	×	5
		3	8	11	8	4
		4	8	14	×	$4 \leq d \leq 8$
		5	8	18	8	4
		6	8	21	×	$3 \leq d \leq 5$
		7	8	25	8	$3 \leq d \leq 4$
7	4	2	12	11	×	5
		3	12	11	8	4
		4	12	16	×	?
		5	12	21	8	4
		6	12	27	×	$4 \leq d \leq 5$
		7	12	31	8	4
7	5	2	16	14	×	5
		3	16	14	8	$5 \leq d \leq 8$
		4	16	21	×	?
		5	16	28	8	$5 \leq d \leq 8$
		6	16	35	×	5

q	δ	m	Bound 4.6	Griesmer bound	Bound 4.7	d
7	6	2	20	18	$\times$	9
		3	20	27	8	$6 \leq d \leq 8$
		4	20	35	$\times$	?
		5	20	44	8	$6 \leq d \leq 8$
		6	20	52	$\times$	?
11	3	2	8	8	$\times$	5
		3	8	11	12	3
		4	8	15	$\times$	?
		5	8	19	12	3
11	4	2	12	12	$\times$	6
		3	12	17	12	4
		4	12	21	$\times$	?
		5	12	28	12	4
11	5	2	16	15	$\times$	$6 \leq d$
		3	16	22	12	$5 \leq 6$
		4	16	30	$\times$	?
		5	16	37	12	$5 \leq d \leq 6$
11	6	2	20	19	$\times$	?
		3	20	28	12	6
		4	20	37	$\times$	?
		5	20	46	12	6

q	δ	m	Bound 4.6	Griesmer bound	Bound 4.7	d
13	5	2	16	15	×	5
		3	16	23	14	?
		4	16	30	×	?
		5	16	38	14	?
		6	16	43	×	5
13	6	2	20	19	×	?
		3	20	28	14	?
		4	20	38	×	?

4.0.4 La distance minimale du dual d'un BCH

Le dual d'un code BCH est un code cyclique qui en général n'est pas un code BCH. L'approximation de la distance minimale $d^{\perp}$ du code dual d'un code cyclique a fait l'objet de plusieurs travaux, la quasi-totalité de ces travaux utilisent le nombre de points rationnels d'une courbe algébrique. Le théorème suivant découle d'un résulat de Weil et Serre sur le nombre de points rationnels d'une courbe algébrique, cela a été adapté pour le cas des codes cycliques par J. Wolfmann [70].

Lemme 4.0.24 *[**La borne de Weil**] Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, $n\nu = q^{m'} - 1$, où $q^{m'}$ est l'ordre de F le corps de décomposition de $x^n - 1$. Soit $T^{\perp}$ l'ensemble de définition de $C^{\perp}$ et J un ensemble de représentants des classes cyclotomiques de $T^{\perp}$. Soit θ le plus grand élément de J, si tout éléments de J est premier à p alors $d^{\perp}$ satisfait :*

Si $0 \in T$ alors,

$$\frac{q^{m'-1}(q-1)}{\nu}-\frac{(\theta\nu-1)(q-1)}{2\nu q}\lfloor 2q^{m'/2}\rfloor \leq d^{\perp} \leq \frac{q^{m'-1}(q-1)}{\nu}+\frac{(\theta\nu-1)(q-1)}{2\nu q}\lfloor 2q^{m'/2}\rfloor$$

Si $0 \notin T$ *alors,*

$$\frac{q^{m'-1}(q-1)-1}{\nu}-\frac{(\theta\nu-1)(q-1)}{2\nu q}\lfloor 2q^{m'/2}\rfloor \leq d^{\perp} \leq \frac{q^{m'-1}(q-1)}{\nu}+\frac{(\theta\nu-1)(q-1)}{2\nu q}\lfloor 2q^{m'/2}\rfloor \tag{4.8}$$

En utilisant le lemme 4.0.24 Augot et Levy-dit-vehel ont donné des bornes plus précises sur certaines classes de codes BCH primitifs sur les corps premiers ; en particulier pour $\delta = 2$ en appliquant les résultats du [18, Théorème.4], on trouve que pour ces codes on a :

$$d^{\perp} \geq p^m - p^{m-1}. \tag{4.9}$$

Pour le cas non-primitif, malgré que le lemme 4.0.24 donne un excellent outil pour le calcul des bornes, vérifier ses hypothèses n'est pas toujours évident. Dans le paragraphe suivant nous allons donner explicitement la borne 4.8 sur $d^{\perp}$ pour la famille de codes BCH construite plus haut sur les corps premiers ; i.e. ; $q = p$ un nombre premier.

D'après le corollaire 2.3.8 toutes les classes cyclotomiques modulo $q^m + 1$ sont réversibles, alors dans ce cas l'ensemble de définition de $BCH(p^m+1, \delta)_p$ d'après l'équation 5.4.3 est égale à

$$T^{\perp} = \mathbb{Z}_n \setminus T. \tag{4.10}$$

Donc si J désigne un ensemble de représentants de classes cyclotomiques de $T^{\perp}$, puisque on est dans le cas $q = p$ les seuls $i \in \mathbb{Z}_n$ représentants des classes cyclotomiques et qui ne sont pas premiers avec p sont les puissances de p, or la classe de 1 contient toutes les puissances de p, alors l'équation 4.10 implique que $T^{\perp}$ et J ne contiennent aucune puissances de p, ce qui donne que tous les éléments de J sont premiers à p. Il est aussi claire que dans ce cas $m' = 2m$ et $\nu = p^m - 1$. De plus comme chaque classe est réversible alors on peut représenter toute classe dans $\mathbb{Z}_n$ par $i \leq \frac{p^m+1}{2}$, et donc si on considère que C est un code $B(p^m + 1, \delta \leq p)_p$, du fait que $T^{\perp} = \mathbb{Z}_n \setminus T$ on obtient que $\theta = \frac{p^m+1}{2}$. Donc en appliquant le lemme 4.0.24 on trouve les bornes suivantes.

$$\frac{[p^{2m-1}(p-1)-1]-(p^{2m}-3)(p-1)p^{m-1}}{p^m-1} \leq d^{\perp} \leq \frac{[p^{2m-1}(p-1)-1]+(p^{2m}-3)(p-1)p^{m-1}}{p^m-1}.$$

On remarque que la borne inférieure est négative et que la borne supérieure est beaucoup plus large que la borne de Singleton. Cependant nous pensons que par un choix bien approprié de courbes algébriques on peut trouver un résultat similaire au lemme 4.0.24 qui soit efficace pour le calcul de $d^{\perp}$ dans le cas non-primitif.

Remarque 4.0.25 *De l'équation (4.10), nous pouvons déduire que si un code cyclique C de longueur n sur $\mathbb{F}_q$ a toutes ses classes réversibles, alors on a :*

$$C \cap C^{\perp} = \{0\}. \tag{4.11}$$

De l'égalité (4.11), nous obtenons que nos codes BCH ne sont ni auto-orthogonaux ni contiennent leurs duaux.

4.1 Les codes BCH quantiques

Comme nos codes ne sont ni auto-orthogonaux, ni contiennent leurs duaux à cause de la remarque 4.0.25, l'idée d'obtenir les codes quantiques de ces codes en utilisant la CSS construction et le fait qu'ils soient emboités est différentes de celles présentées dans [3, Théorèmes 19,21], [68] et dans [28] puisqu'ils utilisent l'auto-orthogonalité dans [3, 68] et dans [28] ils utilisent la construction sur une extension de $\mathbb{F}_{2^l}$ et le fait que leurs codes contiennent leurs duaux.

Lemme 4.1.1 *On considère les codes $C_1 = BCH(q^m+1, \delta_1)$ respectivement $C_2 = BCH(q^m+1, \delta_2)$ de distance minimale d_1 respectivement d_2 et tels que $\delta_2 \geq \delta_1$, alors il existe un code quantique de paramètres $[[q^m+1, 2m(\delta_2 - \delta_1), d^*]]_q$ où $d^* = \min\{d(C_1 \setminus C_2), d(C_2^\perp \setminus C_1^\perp)\} \geq \min(d_{C_2^\perp}, d_{C_1)}$.*

Preuve 4.1.2 *Le résultat découle directement du théorème 3.6.4 et du fait que si $\delta_2 \geq \delta_1$, alors $C_2 = BCH(q^m+1, \delta_2) \subset C_1 = BCH(q^m+1, \delta_1)$. La dimension découle du théorème 4.0.14.*

Corollaire 4.1.3 *Soit q une puissance d'un nombre premier, on considère les codes $C_1 = B(q^m+1, 2)_q$ et $C_2 = B(q^m+1, \delta)_q$ tels que $3 \leq \delta \leq q$, alors il existe un code quantique de paramètres $[[q^m+1, 2m(\delta-2), min\{2, d(C_2^\perp \setminus C_1^\perp\}]]$.*

Preuve 4.1.4 *D'après le théorème 4.0.14 les codes C_1 et C_2 ont pour dimensions $k_1 = q^m+1-2m$ respectivement $k_2 = q^m+1-2m(\delta-1)$, en plus ces codes vérifient $B(q^m+1, \delta)_q \subset B(q^m+1, 2)_q$, alors d'après le théorème 3.6.4 il existe un codes quantique de paramètres $[[q^m+1, 2m(q-2), d^*]]_q$ avec*

$d^* = \min\{d(C_1 \setminus C_2), d(C_2^{\perp} \setminus C_1^{\perp})\}$, *or d'après le théorème 4.0.20 et la remarque 4.0.23 le code* $B(q^m + 1, 2)_q$ *a pour distance minimale 2. En plus d'après la borne BCH le code* $B(q^m + 1, \delta)_q$ *a au moins pour distance minimale* δ*, d'où le résultat.*

Remarque 4.1.5 *Malgré que les codes quantiques donnés par le corollaire 4.1.3 ont une distance minimale* ≤ 2*. Donc ces codes ne corrigent aucune erreur et dans les meilleurs cas peuvent détecter une erreur, nous pensons qu'on peut montrer que ces codes sont d'une grande importance non pas du point de vue correctablité mais en les utilisant en faisant une généralisation des travaux de E. M. Rains [58] à* $\mathbb{F}_{q^2}$ *pour trouver le groupe d'automorphisme des codes linéaires et peut être de certains codes quantiques. En plus si on utilise un canal à effacement, on sait qu'un code de distance minimale d peut corriger* $d - 1$ *erreurs, alors par chacun de ces codes on peut corriger une erreur.*

Lemme 4.1.6 ([39]) *Supposons qu'il existe un code quantique Q de paramètre* $[[n, k, d]]_q$ *, alors nous avons l'existence des codes suivants :*

- *Si* $k > 0$*, alors il existe un code* $[[n + 1, k, d]]_q$ *qui est dégénéré.*
- *Si Q est pur avec* $n \geq 2$ *et* $d \geq 2$*, alors il existe un code pur de paramètres* $[[n - 1, k + 1, d - 1]]_q$*.*
- *Si* $k > 1$ *ou si* $k = 1$ *avec Q pur, alors il existe un code de paramètre* $[[n, k - 1, d^* \geq d]]_q$*, pur jusqu'à d.*

4.1.1 Les tables des codes BCH quantiques

La table suivante donne des exemples des codes quantiques $Q = CSS(C_1, C_2)$ construits précédement, nous n'avons considéré que les cas où les distances

minimales des codes C_1 et C_2 vérifient $d_1 < d_2$ et $d_2^\perp < d_1^\perp$ et cela pour limiter le temps pour trouver la distance $d_Q = \min(d_1, d_2^\perp)$, ce qui veut dire que les codes Q listés dans la table sont tous des codes purs.

$C_1 = [n_1, k_1, \delta_1, d_1]_q$	$C_2 = [n_2, k_2, \delta_2, d_2]_q$	$Q = CSS(C_1, C_2) = [[n, k, , d]]_q$
$[26, 22, 2, 2]_5$	$[26, 14, 4, 7]_5$	$[[26, 8, 2]]_5$
$[26, 18, 3, 5]_5$	$[26, 14, 4, 7]_5$	$[[26, 4, 5]]_5$
$[26, 18, 3, 5]_5$	$[26, 10, 5, 10]_5$	$[[26, 8, 5]]_5$
$[26, 18, 3, 5]_5$	$[26, 6, 8, 13]_5$	$[[26, 10, 4]]_5$
$[26, 18, 3, 5]_5$	$[26, 10, 7, 10]_5$	$[[26, 8, 5]]_5$
$[26, 18, 3, 5]_5$	$[26, 10, 6, 10]_5$	$[[26, 10, 4]]_5$
$[26, 18, 3, 5]_5$	$[26, 2, 9, 13]_5$	$[[26, 16, 2]]_5$
$[26, 10, 5, 10]_5$	$[26, 2, 13, 13]_5$	$[[26, 8, 2]]_5$
$[26, 10, 5, 10]_5$	$[26, 2, 11, 13]_5$	$[[26, 8, 2]]_5$
$[50, 46, 2, 2]_7$	$[50, 42, 3, 5]_7$	$[[50, 4, 2]]_7$
$[50, 46, 2, 2]_7$	$[50, 38, 4, 5]_7$	$[[50, 8, 2]]_7$
$[50, 46, 2, 2]_7$	$[50, 34, 5, 5]_7$	$[[50, 12, 2]]_7$
$[50, 46, 2, 2]_7$	$[50, 30, 6, 9]_7$	$[[50, 16, 2]]_7$
$[50, 34, 5, 5]_7$	$[50, 2, 25, 25]_7$	$[[50, 32, 2]]_7$
$[50, 42, 3, 5]_7$	$[50, 38, 4, 5]_7$	$[[50, 4, 5]]_7$
$[50, 42, 3, 5]_7$	$[50, 30, 6, 9]_7$	$[[50, 12, 5]]_7$
$[82, 78, 2, 2]_9$	$[82, 74, 3, 5]_9$	$[[82, 4, 2]]_9$
$[82, 74, 3, 5]_9$	$[82, 70, 4, 6]_9$	$[[82, 4, 5]]_9$
$[82, 74, 3, 5]_9$	$[82, 66, 5, \geq 7]_9$	$[[82, 8, 5]]_9$
$[82, 70, 4, 6]_9$	$[82, 66, 5, \geq 7]_9$	$[[82, 4, 6]]_9$

$C_1 = [n, k_1, \delta_1, d_1]_q$	$C_2 = [n, k_2, \delta_2, d_2]_q$	$Q = CSS(C_1, C_2) = [[n, k, d]]_q$
$[122, 118, 2, 2]_{11}$	$[122, 114, 3, 5]_{11}$	$[[122, 4, 2]]_{11}$
$[122, 118, 2, 2]_{11}$	$[122, 110, 4, 6]_{11}$	$[[122, 8, 2]]_{11}$
$[122, 118, 2, 2]_{11}$	$[122, 106, 5, 6]_{11}$	$[[122, 12, 2]]_{11}$
$[122, 118, 2, 2]_{11}$	$[122, 102, 6, \geq 6]_{11}$	$[[122, 16, 2]]_{11}$
$[122, 106, 5, 6]_{11}$	$[122, 2, 61, 61]_{11}$	$[[122, 104, 2]]_{11}$
$[122, 114, 3, 5]_{11}$	$[122, 110, 4, 6]_{11}$	$[[122, 4, 5]]_{11}$
$[122, 114, 3, 5]_{11}$	$[122, 106, 5, 6]_{11}$	$[[122, 8, 5]_{11}$
$[122, 114, 3, 5]_{11}$	$[122, 106, 6, \geq 6]_{11}$	$[[122, 20, 5]]_{11}$
$[122, 114, 5, 6]_{11}$	$[122, 106, 6, \geq 6]_{11}$	$[[122, 8, 6]]_{11}$
$[126, 120, 2, 2]_5$	$[126, 108, 4, 6]_5$	$[[126, 112, 2]]_5$
$[126, 114, 3, 3]_5$	$[126, 102, 5, 6]_5$	$[[126, 12, 3]]_5$
$[126, 114, 3, 3]_5$	$[126, 108, 4, 6]_5$	$[[126, 6, 3]]_5$
$[126, 96, 7, 7]_5$	$[126, 60, 14, 14]_5$	$[[126, 36, 7]]_5$
$[170, 154, 5, 5]_{13}$	$[170, 134, 10, 10]_{13}$	$[[170, 20, 5]]_{13}$
$[170, 154, 5, 5]_{13}$	$[170, 122, 13, \geq 13]_{13}$	$[[170, 32, 5]]_{13}$
$[170, 134, 10, 10]_{13}$	$[170, 122, 13, \geq 13]_{13}$	$[[170, 12, 10]]_{13}$
$[170, 134, 10, 10]_{13}$	$[170, 114, 17, 17]_{13}$	$[[170, 20, 10]]_{13}$
$[170, 114, 17, 17]_{13}$	$[170, 62, 34, 34]_{13}$	$[[170, 52, 10]]_{13}$
$[290, 254, 10, 10]_{17}$	$[290, 246, 12, \geq 12]_{17}$	$[[290, 8, 10]]_{17}$
$[290, 254, 10, 10]_{17}$	$[290, 226, 17, \geq 17]_{17}$	$[[290, 28, 10]]_{17}$
$[290, 254, 10, 10]_{17}$	$[290, 186, 29, 29]_{17}$	$[[290, 68, 10]]_{17}$

Dans la table suivante, nous donnons des exemples des codes quantiques construits de nos codes BCH sur $\mathbb{F}_4$. La dernière colonne désigne les bornes

supérieures et inférieures sur la distance minimale pour des codes existants de même paramètres dans la table de M. Grassl [30] qui est donnée sur $\mathbb{F}_4$ et pour des codes de longueurs maximale 128.

$C_1 = [n, k_1, \delta_1, d_1]_q$	$C_2 = [n, k_2, \delta_2, d_2]_q$	$Q = [[n, k, d]]_q$	Bornes de [30]
$[17, 13, 2, 4]_4$	$[17, 5, 6, 9]_4$	$[[17, 8, 4]]_4$	4
$[17, 9, 3, 5]_4$	$[17, 5, 6, 9]_4$	$[[17, 4, 5]]_4$	5
$[65, 59, 2, 3]_4$	$[65, 9, 16, 39]_4$	$[[65, 50, 3]]_4$	4-5
$[65, 53, 3, 5]_4$	$[65, 9, 16, 39]_4$	$[[65, 46, 5]]_4$	5-6
$[65, 53, 3, 5]_4$	$[65, 41, 6, 11]_4$	$[[65, 12, 5]]_4$	13-19
$[65, 59, 2, 3]_4$	$[65, 3, 25, 39]_4$	$[[65, 56, 2]]_4$	3
$[65, 41, 6, 11]_4$	$[65, 23, 10, 13]_4$	$[[65, 18, 8]]_4$	10-17
$[65, 41, 6, 11]]_4$	$[65, 11, 13, 13]_4$	$[[65, 30, 6]]_4$	8-12
$[257, 249, 2, 4]_4$	$[257, 241, 3, 5]_4$	$[[257, 8, 4]]_4$	
$[257, 249, 2, 4]_4$	$[257, 233, 4, \geq 5]_4$	$[[257, 16, 4]]_4$	

Remarque 4.1.7 *Nous pouvons utiliser le lemme 4.1.6 pour obtenir des tables précédentes de nouveaux codes quantiques comme ça a été le cas d'un grand nombre des codes donnés dans [30], nous mentionnons juste par exemple que sur* $\mathbb{F}_5$ *on a l'existence des codes* $[[25, 9, 4]]_5$, $[[27, 8, 5]]_5$ *qui sont dérivés du code* $[[26, 8, 5]]_5$, *le premier code est pur et le second est dégénéré. De même nous avons l'existence des codes* $[[27, 10, 4]]_5$ *et* $[[25, 11, 3]]_5$ *obtenus du code* $[[26, 10, 4]]_5$. *Sur* $\mathbb{F}_4$ *nous avons l'existence du code* $[[66, 46, 5]]_4$ *obtenu du code* $[[65, 46, 5]]_4$.

Chapitre 5

Les codes affine-invariants maximaux classiques et quantiques

L'algèbre est généreuse ; souvent
elle donne plus qu'on lui demande.
J. L. D'Alembert

Certains résultat de ce chapitre ont fait l'objet d'une section de l'article [31].

5.1 Introduction

La classe des codes affines-invariants est l'une des classes les plus abondante dans la nature. Elle regroupe particulièrement les codes BCH primitifs, les codes de Reed–Solomon, les codes de Reed–Muller, etc... Ce chapitre sera dédié à l'étude de ces codes, plus particulièrement les codes affines-invariants

maximaux classiques et quantiques.

Pour la suite nous avons besoin de rappeler quelques sous groupes du groupe de permutations $Sym(G)$ où G est $G = \mathbb{F}_{p^m}$.

Soit r un diviseur de m et $m_r = m/r$. Comme ça a été donné dans [48] toute application de G dans lui même admet une représentation sous forme polynomial à coefficient dans G de degré au plus $p^m - 1$. Les polynômes associés aux applications $\mathbb{F}_{p^r}$-linéaires sont de la forme

$$f(x) = \sum_{i=0}^{m_r-1} f_i x^{p^{ri}},\ f_i \in G.$$

Puisque le corps $\mathbb{F}_{p^m}$ contient le sous-corps $\mathbb{F}_{p^r}$, et alors $\mathbb{F}_{p^m}$ peut être considérer comme un espace vectoriel de dimension m_r sur $\mathbb{F}_{p^r}$. Les éléments du groupe linéaire sont alors les permutations qui peuvent s'écrire sous la forme

$$\sigma(g) = \sum_{i=0}^{m_r-1} f_i g^{p^{ri}}.$$

Pour chaque diviseur r de m nous considérons les sous groupes linéaire et affine d'un espace vectoriel de dimension m_r sur $\mathbb{F}_{p^m}$ comme groupes de permutations de G suivants :

$$Gl(m_r, p^r) = \{\sigma \in Sym(G) \,|\, \sigma(g) = \sum_{i=0}^{m_r-1} f_i g^{p^{ri}}, f_i \in G\} \tag{5.1}$$

$$AGl(m_r, p^r) = \{\sigma \in Sym(G) \,|\, \sigma(g) = \sigma'(g) + b, \sigma' \in Gl(m_r, p^r)\}$$

Lorsque r est égale à 1, nous appelons le groupe $GL(m, p)$ groupe général linéaire. Le groupe $AGL(m, p)$ est appelé le groupe général affine.

Lorsque r est egal à m, le groupe linéaire $GL(1, p^m)$ est isomorphe au groupe mltiplicatif du corps G car $m_r = 1$ de la frome 5.3.1 on obtient $GL(1, p^r) = \{\sigma \in Sym(G)/\sigma(g) = ag, a \in G^*\}$.

Nous appelons le groupe affine le groupe :

$$AGL(1, p^m) = \{\sigma \in Sym(G)/\sigma(g) = ag + b, a \in G^*, b \in G\}.$$

Le groupe de Galois de G (ou groupe d'automorphismes du corps G) est le groupe d'automorphismes défini par :

$$Gal(G) = \{\gamma_{p^l} \in Sym(G) \,|\, \gamma_{p^l}(g) = g^{p^l}, l \in [o, m-1]\}.$$

5.2 Les codes affine-invariants classiques

Soit $q = p^r$ la puissance d'un nombre premier p, $K = \mathbb{F}_{p^r}$ et $G = \mathbb{F}_{p^m}$ les corps finis avec p^r éléments, respectivement p^m éléments et $m = rm_r$. Un code cyclique C de longueur $n = p^m - 1$ est dit maximal si son ensemble de définition contient une seule classe cyclotomique.

Au code C nous associons le code $\hat{C}$, l'étendu de C défini dans la Section 1.4. Puisque le code $\hat{C}$ est de longueur p^m, le corps G peut être pris comme le corps de base et alors les coordonnés d'un mot peuvent être indexées par des éléments du corps G. Ce qui donne que le code $\hat{C}$, peut être considéré comme un sous espace de l'algèbre de groupe $A = K[\{G, +\}]$, qui

est l'algèbre de groupe additive de G sur K,

$$A = \{\sum_{g\in G} x_g X^g, x_g \in K\}.$$

Les opérations dans A sont données par

$$a\sum_{g\in G} x_g X^g + b\sum_{g\in G} y_g X^g = \sum_{g\in G}(ax_g + by_g)X^g,\ a, b \in K,$$

et

$$\sum_{g\in G} x_g X^g \times \sum_{g\in G} y_g X^g = \sum_{g\in G}(\sum_{h+k=g} x_h y_k)X^g.$$

le zéro et l'unité de A sont $\sum_{g\in G} 0X^g$ and X^0.

Dans le concept précédent le code étendu $\hat{C}$ dans A est défini par :

$$\hat{C} = \{\sum_{g\in G} x_g X^g | \phi_s(x) = 0, s \in \hat{T}\},$$

où l'ensemble $\hat{T} = T \cup \{0\}$ est dit ensemble de définition de $\hat{C}$, et ϕ est l'application K-linéaire de A à G défini par :

$$\phi_s(\sum_{g\in G} x_g X^g) = \sum_{g\in G} x_g g^s.$$

Un code étendu $\hat{C}$ de longueur p^m est dit **affine-invariant** si son groupe de permutations contient le groupe des permutations affines $AGL(1, p^m)$.

Soient s et t deux éléments de $S = [0, p^m - 1]$, on considère leurs écritures en base p-adique, alors si $s = \sum_{i=0}^{m-1} s_i p^i$, $t = \sum_{i=0}^{m-1} t_i p^i$, on définit un ordre partiel

sur $S = [0, p^m - 1]$ par :

$$s \prec t \iff s_i \leq t_i, \forall i = 0, \ldots, m-1, s_i \in [0, p-1]. \tag{5.2}$$

L'ordre partiel donné dans (5.2) permet de caractériser les codes affine-invariants par leur ensemble de définition, comme le montre le résultat suivant bien connu [17, 37].

Proposition 5.2.1 *Soit $\hat{C}$ l'étendu d'un code cyclique, ayant pour ensemble de définition $\hat{T}$, alors $\hat{C}$ est affine-invariant si et seulement si $\hat{T}$ satisfait*

$$\forall t \in \hat{T}, \forall s \in S, s \prec t \Rightarrow s \in \hat{T}.$$

Comme conséquence nous obtenons.

Proposition 5.2.2 *Un code cyclique étendu maximal de A est affine-invariant si et seulement si*

$$\hat{T} = C_{p^j} \cup \{0\}.$$

Preuve 5.2.3 *Soit $\hat{T}$ l'ensemble de définition d'un code cyclique étendu maximal. Il est clair que $\hat{T} = C_{p^j} \cup \{0\}$ avec $0 \leq j \leq m-1$, alors pour $s \in S$ et $t \in \hat{T}$ nous ne pouvons avoir $s \prec t$ que pour $s = t$. Alors par la proposition 5.2.1, l'ensemble $\hat{T}$ est l'ensemble de définition d'un code affine-invariant.*

Réciproquement, soient $\hat{T} = C_t \cup \{0\}$ l'ensemble de définition d'un code cyclique étendu maximal qui est affine invariant, $t = \sum_{i=0}^{m-1} s_i p^i$, l'expansion p-adique de t et soit j le plus petit entier $\{0, \ldots, m-1\}$ tels que $s_j \neq 0$, alors

nous avons $p^j \prec t$. Par la proposition 5.2.1 nous obtenons que $p^j \in \hat{T}$. Alors $C_{p^j} \cup \{0\} \subset \hat{T}$. Puisque le code est maximal nous obtenons que $\hat{T} = C_{p^j} \cup \{0\}$.

Lemme 5.2.4 *la classe $C(p^j)$ admet pour cardinal $\frac{m}{r}$.*

Preuve 5.2.5 *Nous avons ord $_{p^m-1} p^r = \frac{m}{r}$. Maintenant soit $t = |Cl(p^j)|$ alors t divise $\frac{m}{r}$ en plus t est le plus petit entier qui vérifie*

$$p^j (p^r)^t \equiv p^j \mod (p^m - 1). \tag{5.3}$$

Alors de (5.3) on obtient que $p^{rt} - 1 = w(p^m - 1)$ pour un entier w, ce qui donne $w = 1$ et $t = \frac{m}{r}$.

Remarque 5.2.6 *Une conséquence du lemme 5.2.4 est que pour des paramètres fixés p, m, r, le nombre des codes affine-invariants maximaux est r.*

5.3 Le groupe de permutations des codes affine-invariants maximaux

Le résultat suivant est dû à T. P. Berger et P. Charpin [11].

Proposition 5.3.1 *Soit $\hat{C}$ un code affine-invariant d'ensemble de définition $\hat{T}$. Alors il existe un diviseur e de m et un diviseur l de e tels que le groupe de permutations de $\hat{C}$ soit engendré par le groupe générale affine $AGL(m/e, p^e)$ et γ_{p^l}. L'entier l est le plus petit entier tel que $\hat{T}$ soit invariant par multiplication par p^l modulo $p^m - 1$ et e le plus petit entier tel que la condition*

suivante soit vérifiée :

$$\forall t \in T, j \prec t \Rightarrow t + j(p^e - 1) \in T. \tag{5.4}$$

Donc la détermination de $Per(\hat{C})$ d'un code affine-invariant revient à la détermination des entiers e et l donnés dans le théorème 5.3.1. D'après Berger [12] "la détermintation des entiers e et l est facile pour un code précis, mais plus délicate pour une famille de codes".

Dans le théorème suivant on donnera le groupe de permutations des codes affines-invariants maximaux.

Théorème. 5.3.2 *Le groupe de permutations d'un code affine-invariant maximal est engendré par $AGl(m/r, p^r)$ et l'application Frobenius γ_{p^r}.*

Preuve 5.3.3 *D'après la proposition 5.2.2 on a l'ensemble de définition d'un code affine-invariant maximal est de la forme $\hat{T} = C(p^j) \cup \{0\}$. Alors pour $s \in S$ et $t \in \hat{T}$, on ne peut avoir $s \prec t$ que si $s = t$. Alors de l' équation (5.4) on obtient $e = r$. Alors dans ce cas d'après la proposition 5.3.1 on obtient que l est un diviseur de r.*

Maintenant on montre que $l = r$; en effet supposons que $l < r$, alors pour tout $t = p^j$, si $p^l p^j \in C(t) \Rightarrow p^{l+j} \equiv p^{j+\alpha r} \mod p^m - 1$, avec $0 \leq \alpha \leq \frac{m}{r} - 1$. Cela est équivalent à

$$p^{l+j} \equiv p^{j+\alpha r} + k(p^m - 1).$$

Puisque $l < r$, cela est équivalent à avoir

$$p^l(p^{\alpha r-l} - 1) = k(p^m - 1),$$

ce qui est absurde puisque $\alpha \leq \frac{m}{r} - 1$.

Les codes cycliques étendus dont l'ensemble de définition est $\cup Cl(p^j)$ sont affine-invariants, cela peut être démontrer en utilisant la proposition 5.2.1 et puisque aussi dans ce cas chaque élément ne peut être relaté qu' à lui même. Par une preuve similaire au théorème 5.3.2 on peut montrer qu'aussi dans ce cas nous avons $e = l = r$; autrement le groupe de permutations de ces codes est engendré par le groupe affine $AGl(m/r, p^r)$ et l'application Frobenius γ_{p^r}.

5.4 Les codes affine-invariants quantiques

Dans cette section, nous allons construire une famille de codes quantiques à partir des codes affine-invariant maximaux et cela en utilisant la CSS construction.

Par le corollaire 3.6.6, si un code $[n, k, d]$ C contient son dual $C^\perp$, alors il existe un code quantique de paramètres $[[n, 2k - n, d_Q \geq d]]_q$, pur jusqu'à d. Maintenant nous donnons le lemme suivant qui nous informe quand est ce qu'un code affine-invariant maximal peut contenir son dual. Il est à noter que le dual d'un code affine-invariant est aussi un code affine-invariant.

Lemme 5.4.1 *Soit $\hat{C}$ un code étendu affine-invariant maximal $[p^m, p^m - 1 - \frac{m}{r}, d]$, alors si $p > 3$ ou $m > 2$ ou $r \neq 1$ nous avons $\hat{C}^\perp \subset \hat{C}$.*

Preuve 5.4.2 *Soit $T^{\perp}$ l'ensemble de définition de $\hat{C}^{\perp}$. De l'équation (2.3) $T^{\perp} = \{s \in \mathbb{Z}_n \,|\, n - s \notin T\}$. Pour avoir $\hat{C}^{\perp} \subset \hat{C}$ il suffit d'avoir $T \subset T^{\perp}$, qui est alors equivalent au résultat suivant.*

$$s \in T \Rightarrow p^m - 1 - s \notin T. \tag{5.5}$$

Soit $T = C_{p^j}$, pour simplicité nous considérons $s = p^j$; le cas géneral peut être déduit. Supposons que $p^m - 1 - p^j \in T$, alors il existe $0 \leq \alpha \leq \frac{m}{r} - 1$ tel que $p^m - 1 - p^j = p^{\alpha r + j} \mod (p^m - 1)$. Cela est équivalent à $p^j(1 + p^{\alpha r}) = k(p^m - 1)$ pour un certain $k \geq 1$. Alors $1 + p^{\alpha r} = k'(p^m - 1)$ pour uun certain $k' \geq 1$, cela implique que

$$1 + p^{\alpha r} \geq p^m - 1. \tag{5.6}$$

Puisque $\alpha \leq \frac{m}{r} - 1$, alors (5.6) donne $2 \geq p^{m-r}(p^r - 1)$, cela n'est possible que pour $(r = m = 1, p \leq 3)$ ou $(r = 1, m = 2, p = 2)$. Alors avec les hypothèses $p > 3$ ou $m > 2$ ou $r \neq 1$ nous avons $\hat{C}^{\perp} \subset \hat{C}$.

Du lemme 5.4.1 et de la CSS construction nous obtenons le résultat suivant.

Théorème. 5.4.3 *Soit $q = p^r$ avec p un nombre premier, m un nombre positif entier et $n = p^m - 1$. Si $p > 3$ ou $m > 2$ ou $r \neq 1$, alors il existe un code quantique avec des paramètres*

$$[[p^m, p^m - 2 - 2\frac{m}{r}, \frac{m}{r} + 2 \geq d_Q \geq d_A]]_q,$$

avec d_A la distance minimale du code étendu affine-invariant maximal.

Preuve 5.4.4 *La proposition 5.2.2 et le lemme 5.4.1 impliquent l'existence d'un code affine- invariant* $\hat{C}$ *avec les paramètres* $[p^m, p^m - 1 - \frac{m}{r}, d_A]$ *et qui contient son dual. Alors par le théorème 3.6.4, nous avons l'existence d'un* $[[p^m, p^m - 2 - 2\frac{m}{r}, d_Q \geq d_A]]_q$ *code quantique. La borne de Singleton quantique donne :* $d_Q \leq 2 + \frac{m}{r}$.

Corollaire 5.4.5 *Supposons que* $r = 1$ *et (*$p > 3$ *ou* $m > 2$*), alors il existe un code quantique qui est pur et de paramètres* $[[p^m, p^m - 2 - 2m, m + 2 \geq d_Q = d_A]]_p$, *avec* d_A *la distance minimale du code étendu affine-invariant maximal.*

Preuve 5.4.6 *Supposons que* $r = 1$ *et (*$p > 3$ *ou* $m > 2$*), du théorème 5.4.3 nous déduisons l'existence d'un code quantique de paramètres* $[[p^m, p^m - 2 - 2m, m+2 \geq d_Q \geq d_A]]_p$. *De la Remarque 5.2.6 il existe un unique code affine-invariant code* $\hat{C}$, *qui est l'étendu d'un code BCH de distance construite 2. Alors par la borne 4.9 la distance minimale de* $\hat{C}^{\perp}$ *est* $d = p^m - p^{m-1}$ *or* $d = p^m - p^{m-1} + 1$, *alors du théorème 3.6.4 le code quantique est pur ;* $d_Q = d_A$.

Chapitre 6

Les codes duadiques quantiques

In most sciences one generation tears down what another.. .In mathematics only each generation builds a new storey on top of the old structure.

H. Hankel

Les résultat de ce chapitre ont fait l'objet d'une section de l'article [31].

6.1 Définitions et préliminaires

Soient q la puissance d'un nombre premier et n un entier impair premier avec q. L'entier m est divisible par p^α, mais n'est pas divisible par $p^{\alpha+1}$.

Pour un entier s premier avec n on appelle **multiplicateur** une application $\mu_s : \frac{\mathbb{F}_q[x]}{x^n-1} \longmapsto \frac{\mathbb{F}_q[x]}{x^n-1}$ définie par :

$$\mu_s(c(x)) = c(x^s)(\mod (x^n - 1)).$$

Au fait l'application μ_s est un automorphisme de $\frac{\mathbb{F}_q[x]}{x^n-1}$. Si C est un code cyclique, on définit $\mu_s(C) = \{\mu_s(c(x)) = c(x^s) | c(x) \in C\} = \{c(x^s) \,|\, c(x) \in C\}$. μ_s induit aussi une permutation sur $\mathbb{Z}_n$, définie par :

$$\mu_s : i \longmapsto is \mod n.$$

L'ensemble de définition de $\mu_s(C)$ est donné par le lemme suivant :

Lemme 6.1.1 *[36, corollaire 4.4.5] Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, ayant pour ensemble de définition T, alors $\mu_s(C)$ est un code cyclique d'ensemble de définition $s^{-1}T$.*

Dans ce qui suit on donnera un rappele des définitions et des propriétés connues sur les codes duadiques. On commence par la définition du splitting donnée comme suit :

Soient S_1 et S_2 des réunions de classes cyclotomiques modulo n, tels que :

1. $S_1 \cap S_2 = \emptyset$,
2. $S_1 \cup S_2 = \mathbb{Z}_n \setminus \{0\}$ et
3. $\mu_s(S_i \mod n) = S_{(i+1) \mod 2}$.

Le triplet μ_s, S_1, S_2 est appelé **splitting** modulo n. Ce splitting donne un quadriplet de codes ; deux codes cycliques sur $\mathbb{F}_q$, D_1 et D_2 ayant pour ensembles de définitions respectifs S_1 et S_2 et qui sont appelés **les codes duadiques odd-like** et deux codes cycliques C_1 et C_2 sur $\mathbb{F}_q$ admettant pour ensembles de définitions respectifs $\{0\} \cup S_1$ et $\{0\} \cup S_2$ et qui sont appelés **les codes duadique even-like**.

De la dernière propriété nous obtenons que $|S_1| = |S_2|$, et alors $|S_i| = \frac{n-1}{2}$ ce qui justifie le choix de n impair.

Autrement, si on considère une racine primitive $n$ième de l'unité α de $\mathbb{F}_q$, les codes D_i sont des codes cycliques de polynômes générateurs

$$g_i = \prod_{j \in S_i} (x - \alpha^j),$$

les codes C_i ont pour polynômes générateurs $g_i(x-1)$ et alors $\dim D_i = \frac{n+1}{2}$ et $\dim C_i = \frac{n-1}{2}$.

Remarque 6.1.2 *Nous avons une caractéristique des mots des codes D_i et C_i, en effet :*

$$\forall \mathsf{x} = (x_1, \ldots, x_n) \in D_i, \textit{ alors } \mathsf{x} \textit{ vérifie } \sum x_i \neq 0$$

$$\forall \mathsf{x} = (x_1, \ldots, x_n) \in C_i, \textit{ alors } \mathsf{x} \textit{ vérifie } \sum x_i = 0.$$

Le théorème suivant prouvé par M. Smid [66] donne une condition nécessaire et suffisante sur l'existence des codes duadiques sur $\mathbb{F}_q$.

Théorème. 6.1.3 *Les codes duadiques de longueur n sur $\mathbb{F}_q$ existent si et seulement si $q \equiv \square \mod n$, i.e., si $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, alors il existe un code duadique sur $\mathbb{F}_q$ si et seulement si $q \equiv \square \mod p_i$ avec $i \in [s]$.*

Les codes duadiques sont une généralisation des codes dits **résidus quadratiques**, construit comme suit :

Soient n un nombre premier impair tel que $q = \square \mod n$, $S_1 = \{0 <$

$i < n \,|\, i = \square \mod n\}$ et $S_2 = \{0 < i < n \,|\, i = \square \mod n\}$, pour un $a \in S_2$ $\mu_a : S_1 \leftrightarrow S_2$ est un splitting modulo n et les codes correspondants sont appelés les codes résidus quadratiques, (car le produit de deux non résidues est un résidu).

Les codes duadiques sont importants en pratique à cause de leurs distances minimales qui est large et aussi à cause de leurs lien avec les codes auto-duaux, ce lien est donné par le théorème suivant.

Théorème. 6.1.4 *([66])*

Soit C un code cyclique de longueur n sur $\mathbb{F}_q$. Supposons que l'étendu de C soit un code auto-dual, alors C est un code duadique et le splitting est donné par μ_{-1}.

Nous avons le résultat suivant sur la distance minimale des codes duadiques.

Lemme 6.1.5 *Soient D_1 et D_2 une paire de codes duadiques odd-like de longueur n sur $\mathbb{F}_q$. Alors D_1 et D_2 ont la même distance minimale d et on a :*

(i) $d^2 \geq n$,

(ii) $d^2 - d + 1 \geq n$, si le splitting est donné par μ_{-1}.

Preuve 6.1.6 *Voir [36, Théorème 7].*

Le résultat suivant dû à [66] donne une autre borne sur la distance minimale.

Lemme 6.1.7 *Soit $n = p^m$ un entier impair tel que $t = \mathrm{ord}_p(q^2)$. Soit z tel que $p^z \mid\mid q^{2t} - 1$. Alors tous les codes duadiques de longueurs p^m, avec $m > z$ ont une distance minimale $\leq p^z$.*

Si nous considérons le corps $\mathbb{F}_{q^2}$, alors on peut parler du dual Hermitien, en plus nous avons l'existence de codes duadiques sur $\mathbb{F}_{q^2}$ pour tout entier n impair premier avec q^2.

Le résultat suivant est dû à Rushanan [60, théorème 4.4].

Lemme 6.1.8 *Soient C_i et D_i, respectivement even-like et les odd-like codes duadiques sur $\mathbb{F}_{q^2}$, avec $i \in [2]$, alors $C_i^{\perp h} = D_i$ si et seulement il existe un q^2-splitting donné par μ_{-q}, i.e., $-qS_i \equiv S_{(i+1 \mod 2)} \mod n$*

6.2 L'existence des splittings

Dans cette section, nous donnons des conditions suffisantes sur l'existence des splittings μ_{-1} et μ_{-q}. Comme conséquences nous déduisons des résultats et des propriétés des codes duadiques sur $\mathbb{F}_q$ et $\mathbb{F}_{q^2}$.

6.2.1 μ_{-1} splitting

Le problème d'existence du μ_{-1} est un ancien problème, la solution est liée à l'existence des codes duadiques cycliques comme dans notre cas ou plus généralement les codes duadiques d'algèbre de groupe. Récemment la réponse a été donné dans [1], comme nous nous intéréssons qu'au cas cyclique notre preuve est différente et plus simple que celle donnée dans [1].

Il est évident que si une classe cyclotomique est fixé par μ_{-1} est alors réversible.

Théorème. 6.2.1 *Soit un entier n impair et q la puissance d'un nombre premier impair, alors μ_{-1} donne un splitting si et seulement si* $\mathrm{ord}_n(q)$ *est*

impair.

Preuve 6.2.2 *Rushanan [60] à montrer que si* $\mathrm{ord}_n(q)$ *est impair, alors* μ_{-1} *donne un splitting. Nous proposons de montrer l'inverse. Pour cela nous considérons deux cas.*

1. *Si* $n = p$ *est un nombre premier, nous supposons que* $\mathrm{ord}_n(q)$ *est pair* $q^{2w} \equiv 1 \bmod n$. *Alors* $q^w \equiv -1 \bmod n$. *Alors du lemme 2.3.6 nous obtenons que* C_1 *est réversible. Donc par le corollaire 2.3.8, toutes les classes* C_j *sont réversible.*

2. *Si* $n = p^\alpha$, *nous montrons l'implication suivante,*

$$\mathrm{ord}_{p^\alpha}(q) \text{ est pair } \Rightarrow \mathrm{ord}_p(q) \text{ est pair.}$$

Supposons que $\mathrm{ord}_{p^\alpha}(q)$ *est pair et que* $\mathrm{ord}_p(q)$ *est impair, alors il existe* $i > 0$ *impair tels que* $q^i \equiv 1 \mod p \Leftrightarrow q^i = 1 + kp$. *Ce qui donne* $q^{ip^{\alpha-1}} = (1+kp)^{p^{\alpha-1}} \equiv 1 \mod p^\alpha$, *cela est dû au fait que* $(1+kp)^{p^{\alpha-1}} \equiv (1 + kp^\alpha \mod p^{\alpha+1})$. *Alors*

$$q^{ip^{\alpha-1}} \equiv 1 \mod p^\alpha. \tag{6.1}$$

Nous avons i *impair et* $p^{\alpha-1}$ *impair, alors* $\mathrm{ord}_{p^\alpha}(q)$ *est impair (car* $\mathrm{ord}_{p^\alpha} q | ip^{\alpha-1}$*) ; ce qui est absurde. Donc* $\mathrm{ord}_p(q)$ *ne peut être que pair, et alors il existe un entier* j *tel que* $0 < j < \mathrm{ord}_p(q)$, *et* $q^j \equiv -1 \mod p$, *alors de l'équation (6.1) nous avons,* $q^{jp^{\alpha-1}} \equiv -1 \mod p^\alpha$, *en appliquant le lemma 2.3.6 on trouve que* C_1 *est réversible. Donc par le corallaire 2.3.8 toutes les classes cyclotomiques sont fixées par* μ_{-1}.

3. *Si* $n = p_1 p_2$ *avec* $(p_1, p_2) = 1$ *et* $(p_1, q) = (p_2, q) = 1$, *alors* $\mathrm{ord}_n(q) = ppcm(\mathrm{ord}_{p_1}(q), \mathrm{ord}_{p_2}(q))$ *est pair, donc* $\mathrm{ord}_{p_1}(q)$ *ou* $\mathrm{ord}_{p_2}(q)$ *doit être pair. Supposons que* $\mathrm{ord}_{p_1}(q)$ *est pair, alors il existe* $1 \leq k \leq \mathrm{ord}_{p_1}(q)$ *tel que* $q^k \equiv -1 \mod p_1$. *Alors* $q^k(n - p_2) \equiv -(n - p_2) \mod n$, *avec* $k \leq \mathrm{ord}_{p_1}(q)$. *Ce qui veut dire qu'il existe au moins une classe qui est réversible ;* $C_{(n-p_2)}$. *D'où* μ_{-1} *ne peut donner un splitting.*

4. *Si* $n = p_1^{\alpha_1} p_2^{\alpha_2}$ *avec* $(p_1, p_2) = 1$ *et* $(p_1, q) = (p_2, q) = 1$, *nous savons que* $\mathrm{ord}_n\, q = ppcm(\mathrm{ord}_{p_1{}^{\alpha_1}}(q), \mathrm{ord}_{p_2{}^{\alpha_2}}(q))$. *Alors si* $\mathrm{ord}_{p_1^{\alpha_1} p_2^{\alpha_2}}(q)$ *est pair nous avons ou bien* $\mathrm{ord}_{p_1}(q)$ *ou* $\mathrm{ord}_{p_2}(q)$ *qui soit pair. Et alors il suffit de répéter le processus du cas 3. D'où la généralisation à tout n tels que* $\mathrm{ord}_n(q)$ *est pair.*

Du théorème 6.2.1 et de l'équation (2.3), nous pouvons déduire directement le corollaire suivant.

Corollaire 6.2.3 *Si* $\mathrm{ord}_n(q)$ *est pair il ne peut exister de codes cycliques de longueur n sur* $\mathbb{F}_q$ *ou cycliques étendus qui soient auto-orthogonaux ou qui contiennent leurs duaux.*

6.2.2 μ_{-q} splitter

Maintenant nous montrons le lemme suivant qui nous donne quelques propriétés de $\mathrm{ord}_n(q)$.

Lemme 6.2.4 *Soit q une puissance d'un nombre premier et n un entier positif, tel que* $pgcd(n, q) = 1$, *alors on a :*

1. *Si* $\mathrm{ord}_n(q)$ *est impair, alors* $\mathrm{ord}_n(q^2) = \mathrm{ord}_n(q)$.

2. *Si* $\mathrm{ord}_n(q)$ *est pair, alors* $\mathrm{ord}_n(q^2) = \frac{\mathrm{ord}_n(q)}{2}$.

Preuve 6.2.5 1. *Soit* $r = \mathrm{ord}_n(q)$ *et* $r' = \mathrm{ord}_n(q^2)$, *alors* $r|2r'$, *puisque* r *est impair alors* $r|r'$. *D'autre part nous avons,* $q^{2r} \equiv 1 \mod n$, *et alors* $r'|r$. *D'où* $r = r'$.

2. *Soit* $r = \mathrm{ord}_n(q)$ *et* $r' = \mathrm{ord}_n(q^2)$. *Alors on a* $q^{2r'} \equiv 1 \mod n$ *ce qui implique que* $r|2r'$. *Puisque* r *est pair, alors* $q^{2(\frac{r}{2})} \equiv q^r \equiv 1 \mod n$, *donc* $r'|\frac{r}{2}$. *D'où* $r' = \frac{r}{2}$.

Lemme 6.2.6 *Soit* $n = \prod p_i^{m_i}$ *la factorisation d'un entier impair* n, *où chaque* $m_i > 0$, *et tels que* $p_i \equiv -1 \mod 4$, *alors* $\mathrm{ord}_n(q^2)$ *est impair.*

Preuve 6.2.7 *Nous savons que* $\mathrm{ord}_n(q^2) = ppcm(\mathrm{ord}_{p_i^{m_i}}(q^2))$, *en plus du lemme 2.6.4 nous avons :*

$$\mathrm{ord}_{p_i^{m_i}}(q^2) = p_i^{m_i - z_i} t_i,$$

avec $t_i = \mathrm{ord}_{p_i}(q^2)$ *et* z_i *est tels que* $p_i^{z_i} \mid\mid q^{t_i} - 1$. *Alors pour compléter la preuve il suffit de montrer que* $\mathrm{ord}_{p_i}(q^2)$ *est impair si* $p_i \equiv -1 \mod 4$. *Nous allons considérer deux cas :*

1. $q \equiv \square \mod p_i$, *alors* $\mathrm{ord}_{p_i}(q)$ *divise* $\frac{p_i - 1}{2}$. *Cela implique que* $\mathrm{ord}_{p_i}(q)$ *est impair car sinon* $p_i \equiv 1 \mod 4$. *Donc du lemme 6.2.4* $\mathrm{ord}_{p_i}(q^2)$ *est impair.*

2. *Si* q *n'est pas un carré modulo* p_i, *alors* $\mathrm{ord}_{p_i}(q) = p_i - 1$ *est pair. Alors du lemme 6.2.4 on obtient* $\mathrm{ord}_{p_i}(q^2) = \frac{p_i - 1}{2}$. *La dernière quantité doit être impair, sinon nous obtenons que* $p_i \equiv 1 \mod 4$.

La proposition suivante donne le splitting, lorsque $\mathrm{ord}_{p^m}(q^2)$ est pair.

Proposition 6.2.8 *Soient q une puissance d'un nombre premier, p un nombre premier impair premier avec q tel que $\mathrm{ord}_{p^m}(q)$ soit pair. Alors μ_q donne un splitting de p^m sur $\mathbb{F}_{q^2}$. Si $\mathrm{ord}_{p^m}(q^2)$ est pair, alors μ_{-q} donne aussi un splitting de p^m sur $\mathbb{F}_{q^2}$.*

Preuve 6.2.9 *Puisque l'ordre est pair, nous avons $q^{2w} \equiv 1 \bmod p^m$, ce qui donne $q^w \equiv -1 \bmod p^m$. Suppososns que μ_q fixes une certaine q^2-ary classe cyclotomique C_x, $1 \leq x \leq p^m - 1$. Alors nous avons que $qC_x = C_x$. Il existe un certain entier i tels que $qx = xq^{2i}$. Or $x(q^{2i-1} - 1) \equiv \mathrm{mod} p^m$. Puisque $p \nmid x$, $q^{2i-1} \equiv 1 \bmod p^m$. Par hypothèse $\mathrm{ord}_{p^m}(q)$ est pair, dans ce cas $2 \mid (2i-1)$, absurde. Donc μ_q ne fixe aucune classe. Alternativement μ_q donne un splitting de p^m.*

Maintenant, supposons que $\mathrm{ord}_{p^m}(q^2)$ est pair, du lemme 6.2.4 nous avons que $4 \mid \mathrm{ord}_{p^m}(q)$. Alors $q^{4w} \equiv 1 \bmod p^m$, ce qui implique que $q^{2w} \equiv -1 \bmod p^m$, et donc du corollaire 2.3.8 nous obtenons que μ_{-1} fixes toutes les q^2-ary classes cyclotomiques. Supposons que μ_{-q} ne donne pas un splitting, alors $\mu_{-q}(C_x) = C_x$ pour un certain $1 \leq x \leq p^m - 1$. Mais cela implique que $\mu_{-q}(C_x) = \mu_q(\mu_{-1}(C_x)) = \mu_q(C_x) = C_x$. Mais on savait déja que μ_q ne fixe aucune classe cyclotomique. Alors μ_{-q} aussi ne peut fixé aucune classe cyclotomique et par conséquent donne un splitting de p^m.

6.3 Les codes quantiques duadiques

Maintenant en utilisant les résultats de proposition 6.2.8, nous avons construit la famille suivante des codes quantiques.

Théorème. 6.3.1 *On considère un entier $n = p^m$ impair premier avec q et tels que $\mathrm{ord}_{p^m}(q^2)$ soit pair. Alors il existe un code quantique de paramètre $[[n, 1, d^*]]_q$ vérifiant $d^{*2} \geq n$.*

Preuve 6.3.2 *De la proposition 6.2.8 il existe un splitting de n donné par μ_{-q}, ce qui veut dire qu'en utilisant le lemme 6.1.8 nous obtenons que $C_i \subset C_i^{\perp h} = D_i$. Alors par le corollaire 3.6.7 il existe un code quantique de paramètres $[[n, n-(n-1), d^* \geq d]]_q$ avec $d^{*2} \geq n$.*

6.3.1 Codes duadiques quantiques dégénérés

Dans cette section en utilisant les résultats précédents nous dérivons des codes duadiques quantiques avec une large distance minimale.

Théorème. 6.3.3 *Soit $n = p^m$ un entier impair tel que $t = \mathrm{ord}_p(q^2)$ est pair. Soit $p^z \mid\mid q^{2t} - 1$. Alors pour $m > 2z$, il existe un $[[n, 1, d^* > d]]_q$ code quantique dégénéré, avec $d^{*2} \geq n$.*

Preuve 6.3.4 *En supposant que $n = p^m$ soit premier avec q, nous avons l'existence d'un code duadique sur $\mathbb{F}_{q^2}$, en plus de l'hypothèse $p^z \mid\mid q^{2t} - 1$ nous pouvons déduire du lemme 6.1.7 que la distance d du code duadique vérifie*

$$d \leq p^z. \tag{6.2}$$

De la proposition 6.2.8 on obtient l'existence d'un splitting de n donné par μ_{-q}, ce qui veut dire qu'en utilisant le lemme 6.1.8 nous obtenons que $C_i \subset C_i^{\perp h} = D_i$. En plus, en appliquant le corollaire 3.6.7 on trouve l'existence d'un code quantique de paramètres $[[n, n-(n-1), d^* \geq d]]_q$ avec $d^{*2} \geq n$,

or par hypothèse $n = p^m > p^{2z}$*, et donc de l'equation 6.2, nous obtenons que* $d < d^*$*, ce qui veut dire que le code quantique est dégénéré.*

Appendice A

Our difficulty is not in the proofs,

but in learning what to prove.

Emil Artin

6.4 Espace de Hilbert

Un espace vectoriel complexe H est appelé espace de Hilbert s'il admet un produit scalaire défini ci dessous et s'il est complet par rapport à la norme induite par le produit scalaire. En mécaniqe quantique un vecteur d'un espace de Hilbert est noté $|x>$.

Le produit scalaire est une application de $H \times H$ à valeur dans $\mathbb{C}$ qui à tout couple d'ordonnées de vecteurs $|x>$ et $|y> \in H$ on associe un nombre complexe $(|x>, |y>)$ appelé produit scalaire de $|x>$ et $|y>$, (cette notation du produit scalaire n'est pas celle utilisé en mécanique quantique, plus tard nous ferons le lien). Un produit scalaire doit vérifier les axiomes suivants :

1. $(|x>, |y>) = (|y>, |x>)^*$ (le signe * désigne le conjugué complexe)

2. pour tout $|x>, |y>, |z> \in H$, $\alpha \in \mathbb{C}$ on a

$$(|x>, \alpha|y+z>) = \alpha(|x>, |y>) + (|x>, |z>)$$

3. $(|x>, |x>) \geq 0, \forall |x> \in H$.

4. $(|x>, |x>) = 0 \iff |x> = 0$.

Le produit scalaire sur un espace de Hilbert induit une norme donnée par :

$$||x|| = \sqrt{(|x>, |x>)}.$$

Comme tous les espaces de Hilbert de même dimension sont isomorphe, on note H_n un espace de Hilbert de dimension n. Une base orthonormale de H_n est constitué par n vecteurs $|x_i>$, vérifiant $(|x_i>, |x_j>) = \delta_{i,j}$, (symbole de Kronecker).

Si on considère la base orthonormale $\{|x_1>, \ldots, |x_n>\}$ de H_n, alors les états $|x>$ et $|y>$ de H_n peuvent être représentés par $|x> = x_1|x_1> + \ldots + x_n|x_n>$ et $|y> = y_1|x_1> + \ldots + y_n|x_n>$, on peut vérifier que $x_i = (|x_i>, |x>)$ et que $y_j = (|x_j>, |y>)$. Cela induit un produit scalaire défini par,

$$(|x>, |y>) = \sum_{i=1}^{n} x_i^* y_j < (|x_i>, |x_j>) = \sum_{i=1}^{n} x_i^* y_i.$$

Soit Q un sous espace d'un espace de Hilbert H, nous pouvons définir l'orthogonale de Q par rapport au produit scalaire de H par :

$$Q^{\perp} = \{y \in H | (|y>, |x>) = 0 \ , \forall |x> \in H\}.$$

L'espace $Q^{\perp}$ est un sous espace de H, dit **le complément orthogonal de** Q. Lorsque l'espace de Hilbert est de dimension fini n, alors tout sous espace de H_n est un espace de Hilbert, dans ce cas on a le résultat suivant.

Lemme 6.4.1 *Si Q est un sous espace d'un espace de Hilbert de dimension fini n, alors on a $H_n = Q \oplus Q^{\perp}$.*

6.4.1 Les opérateurs

La mécanique quantique moderne est essentiellement basé sur les opérateurs linéaires. Un opérateur linéaire sur un espace de Hilbert H est une application linéaire $T : H \mapsto H$.

L'ensemble des opérateurs linéaires noté $L(H)$ a la structure d'un espace vetoriel normé. La norme est donné par

$$||T|| = \sup_{|||x>||=1} ||T|x > ||.$$

Supposons qu'on a un opérateur linéaire $T : H \mapsto H$, alors il existe un opérateur linéaire unique T^* défini pour tout $|x >, |y > \in H$ par la contrainte

$$(|x >, T|y >) = (T^*|x >, |y >).$$

L'opérateur T^* est appelé l'opérateur adjoint de T. Si on a $T = T^*$, alors T est dit auto-adjoint. De la définition d'un opérateur adjoint, on peut montrer au fait que si A et B sont deux opérateurs sur H, alors ils vérifient :

$$(AB)^* = B^*A^*. \tag{6.3}$$

De (6.3) on peut déduire que AB est auto-adjoint si A et B commutent. L'opérateur T est dit unitaire s'il vérifie : $T^* = T^{-1}$.

Exemple 6.4.2 *L'opérateur de Hadamard appelé aussi transformation de Hadamard, est l'opérateur unitaire suivant :*

$$\begin{aligned} |0> &\mapsto \tfrac{1}{\sqrt{2}}(|0> + |1>) \\ |1> &\mapsto \tfrac{1}{\sqrt{2}}(|0> - |1>) \end{aligned}$$

Dans la base $\{|0>, |1>\}$*, cette opérateur admet pour matrice*

$$\mathcal{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

On retrouve la matrice de Hadamard du group de pauli.

Considérons maintenant un registre de taille n*, initialement dans l'état* $|0>$*, et appliquons la transformation de Hadamard à chaque sous-registre de taille 1 :*

$$\mathcal{H}^n : |0> \rightarrow \frac{1}{\sqrt{2}}(|0> + |1>) \otimes \ldots \otimes \frac{1}{\sqrt{2}}(|0> + |1>) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i> .$$

Une caractéristique des opérateurs unitaires est le fait qu'ils préservent le produit scalaire, i.e.,

$$(T|x>, T|y>) = (|x>, |y>).$$

L'inverse est vraie i.e., tout opérateur qui préserve le produit scalaire est unitaire.

Comme à chaque produit scalaire on associe une norme, alors on peut montrer qu'un opérateur $T : H \mapsto H$ est unitaire si et seulement si, il préserve la norme.

Un opérateur T auto-adjoint est dit **positif** s'il vérifie

$$(|x>, T|x>) \geq 0 \text{ pour tout } |x> \in H.$$

Remarque 6.4.3 *Si on a une base* $\{|e_1>, \ldots, |e_n>\}$ *de* H_n*, alors tout opérateur peut être représenter par une matrice* M *de type* (n, n) *à coefficients complexe. Alors l'opérateur* T^* *admet pour matrice associé la matrice transposé du conjugué complexe de* M*.*

Si $\{|x_1>, \ldots, |x_n>\}$ *et* $|y_1>, \ldots, |y_n>\}$ *sont deux bases orthonormales de* H_n*, alors on peut montrer qu'on a*

$$\sum_{i=1}^{n}(|x_i>, T|x_i>) = \sum_{i=1}^{n}(|y_i>, T|y_i>).$$

Définition 6.4.4 *Pour toute base orthonormale on appelle trace de l'opérateur* T *la quantité suivante :*

$$Tr(T) = \sum_{i=1}^{n}(|x_i>, T|x_i>).$$

6.4.2 La représentation spectrale des opérateurs

Lemme 6.4.5 *Les valeurs propres d'un opérateur auto-adjoint sont réels.*

Un opérateur A est dit normal s'il vérifie

$$A^*A = AA^*.$$

Il est claire qu'un opérateur auto-adjoint est normal.

Théorème. 6.4.6 *([51, Théorème]) Tout opérateur normal est diagonalisable, par rapport à une base orthonormale.*

Remarque 6.4.7 *Comme les opérateurs auto-adjoints sont normaux, alors ils sont diagonnalisables, en plus d'après le lemme 6.4.5 les valeurs propres des opérateurs auto-adjoints sont réels. Ce résultat est trés utile dans la représentation de ces opérateurs.*

6.4.3 Matrice de densité

On considère un espace de Hilbert H_n et $\{|b_1>, \ldots, |b_n>\}$ une base orthonormale fixée de H_n. Un vecteur $|x>= x_1|b_1> + \ldots + x_n|b_n>$ peut être vu comme un vecteur colonne $(x_1, \ldots, x_n)^T$. On définit le dual de $|x>$ comme étant le vecteur $<x|$, par

$$<x| = (x_1^*, \ldots, x_n^*),$$

et alors pour tout $|x>= x_1|b_1> + \ldots + x_n|b_n>$ et $|y>= y_1|b_1> + \ldots + y_n|b_n>$, la représentation matricielle de $<x|(|y>)$ est donnée par :

$$< x|(|y >) = (x_1^*, \ldots, x_n^*) \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix} = \sum_{i=1}^{n} x_i^* y_i = (|x >, |y >).$$

Inspiré du mot **bracket**, le vecteur $< x|$ est dit le vecteur **bra** et le vecteur colonne $|y >$, est dit vecteur **ket**. Toujours dans le formalisme de Dirac on note

$$(< x|(|y >)) \equiv < x, y >= (|x >, |y >).$$

On définit l'opérateur linéaire suivant : $|x >< y| : H_n \mapsto H_n$ par :

$$(|x >< y|)(|z >) \equiv |x >< y|z >=< y|z > |x > .$$

On peut vérifier qu'on a :

$$(|x >< y|)^* = |y >< x|.$$

Exemple 6.4.8 *La matrice de Pauli X peut être donnée sous la forme suivante :* $|0 >< 1| + |1 >< 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (10) + \begin{pmatrix} 1 \\ 0 \end{pmatrix} (01) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Le groupe de Pauli $\mathcal{P}_n = \{\pm u_1 \otimes \ldots \otimes u_n, \pm i u_1 \otimes \ldots \otimes u_n \,|u_i \in \{I, X, Y, Z\}\}$. Une erreur dans un n-qu bit est un élément de $\mathcal{P}_n$.

En utilisant la représentation matricielle pour tout état $|x >= x_1|b_1 >$

$+ \ldots + x_n|b_n >$ on définit la **matrice densité de** $|x >$ par :

$$|x > \otimes < x| = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} \otimes (x_1*, \ldots, x_n*) = \begin{pmatrix} |x_1|^2 & x_1x_2^* & \ldots & x_1x_n^* \\ x_2x_1^* & |x_1|^2 & \ldots & x_2x_n^* \\ \cdots & \cdots & \vdots & \cdots \\ x_nx_1^* & x_nx_2^* & \ldots & |x_n|^2 \end{pmatrix}$$

La matrice à droite est calculée par rapport la loi du produit tensoriel des matrices qu'on explique plus loin dans ce chapitre.

On peut démontrer que $|x > \otimes < x|$ qu'on note tout simplement $|x >< x|$ est une matrice qui représente une projection sur l'espace engendré par $|x >$.

La matrice de densité admet les importantes propriétés suivantes :

- Puisque $|||x > || = 1$, alors la trace de la matrice $|x >< x|$ est égale à 1.
- Comme projection, la matrice $|x >< x|$ est auto-adjointe.
- La matrice $|x >< x|$ est positive puisque $(|x >< x|)^2 = |x >< x|$.

D'une manière plus général on définit l'opérateur linéaire $|x >< y| : H \mapsto H$ par :

$$(|x >< y|)(|z >) \equiv |x >< y|z >=< y|z > |x > .$$

Les propriétés précédentes de la matrice densité permettent de montrer que l'application qui envoie un état unitaire à une matrice de densité est bijective, cela justifie la définition suivante de la notion d'état.

Définition 6.4.9 *Un état d'un système quantique est un opérateur de H_n qui est adjoint, positif ayant pour trace 1. Un tel opérateur est dit opérateur densité.*

Toute matrice associée à un opérateur densité est une matrice de densité. La représentation spectrale simplifie l'étude des matrices de densité, en effet :

Si ρ est une matrice de densité qui admet pour valeurs propres $\lambda_1, \ldots, \lambda_n$, alors on peut trouver une base orthonormale $\{|x_1>, \ldots, |x_n>\}$ tels que :

$$\rho = \lambda_1 |x_1><x_1| + \ldots + \lambda_n |x_n><x_n|. \tag{6.4}$$

La représentation spectrale (6.4) induit que chaque matrice de densité est au fait une combinaison linéaire des projections de dimension 1. D'après la remarque 6.4.7 les valeurs propres d'un opérateur auto-adjoints sont réels, ce qui donne que les valeurs propres d'une matrice de densité sont réels, en plus on a

$$\sum_{i=1}^{n} \lambda_i = Tr(\rho) = 1.$$

De plus puisque ρ est positif, alors $\lambda_i =< x_i|\rho|x_i >\geq 0$. Ce qui donne, que toute matrice de densité à la forme d'une distribution de probabilité. Il est vraie que toute distribution de probabilité $\{p_1, \ldots, p_n\}$ de vecteurs orthogonaux définie toujours une matrice de densité.

$$\rho = p_1 |x_1><x_1| + \ldots + p_n |x_n><x_n|. \tag{6.5}$$

Souvent en littérature quantique la matrice de densité d'un système quantique est donné par (6.5). ρ est dit pure si $\rho = |\psi><\psi|$ sinon il est dit mélangé.

Souvent un opérateur linéaire de $H_n \mapsto H_n$ est dit **porte quantique** (gate).

Exemple 6.4.10 *L'opération "non-contrôlé" (controlled-not gate ou (Cnot))* $U_{cnot} \in L(\mathbb{C}^2 \otimes \mathbb{C}^2)$ *est définie par :*

$$U_{cnot}|i> |j>= |i> |i \oplus j(\mod 2)> .$$

$U_{cnot}|00>= |00>$, $U_{cnot}|01>= |01>$, $U_{cnot}|11>= |10>$, $U_{cnot}|10>= |11>$.

La matrice associé à U_{cnot} *est la matrice suivante :*

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

6.4.4 L'évolution dans le temps d'un système quantique

On pourrait se demander comment l'état $|\psi>$ change en fonction du temps. Le postulat suivant de la mécanique quantique donne une déscription d'un tel changement.

Postulat 2 L'évolution d'un système quantique fermé est décrite par un opérateur unitaire :

$$U_t : \ H_n \longrightarrow H_n \tag{6.6}$$

$$|\psi'(t_2)> \ = U_t|\psi(t_1)>, \tag{6.7}$$

ce qui veut dire que l'état $|\psi>$ du système au temps t_1 est relié à l'état $\psi'>$ du système au temps t_2 par un opérateur unitaire U qui dépend du temps t_1 et t_2, seulement la mécanique quantique ne donne pas l'opérateur unitaire qui d'ecrit la dynamique du système.

Théorème. 6.4.11 *(Théorème de Stone) On considère $U(t)$ l'opérateur qui décrit la dynamique du système, alors il existe un unique opérateur H auto-adjoint qui vérifie :*

$$U(t) = e^{-it}H.$$

Une conséquence du postulat 2 et du théorème 6.4.11 est le postulat suivant de la mécanique quantique.

Postulat 2' L'évolution en temps d'un état d'un système quantique clos est décrite par l'équation de Schrödinger

$$ih\frac{d|\psi>}{dt} = H|\psi>,$$

h est une constante dite la constante de Planck qui peut être déterminée expérimentalement, mais il est usuel de faire absorber h par H, dit le Hamiltonien du système. Cet Hamiltonien décrit l'énergie totale du système, et ses valeurs propres sont les niveaux d'énergie du système.

6.5 Le théorème du non-clonage

Le non-clonage est dû à Dieks, W. K. Wooters et W. H. Zurek ça prouve qu'il ne peut pas exister d'opérateur unitaire U dans $H_n \otimes H_n$ qui vérifie :

$$U(|x> |a>) = |x> |x>$$

pour $|a>$ un élément de la base de H_n. Autrement, on ne peut pas faire des copies des état inconnues. Car supposons qu'il existe un opérateur de clonage et soient $|\phi>$ et $|\psi>$ deux états distincts alors :

$$|\phi> \mapsto |\phi> |\phi>, \tag{6.8}$$

$$|\psi> \mapsto |\psi> |\psi>, \tag{6.9}$$

alors l'opérateur envoie l'état $|\phi> + |\psi>$ vers l'état suivant :

$$(|\phi> + |\psi>)(|\phi> + |\psi>) = |\phi> |\phi> + |\psi> |\psi> + |\phi> |\psi> + |\psi> + |\phi>, \tag{6.10}$$

mais comme tous les opérateurs quantiques sont linéaires alors des équations (6.8) et (6.9) nous obtenons :

$$|\phi> + |\psi> \mapsto |\phi> |\phi> + |\psi> |\psi>,$$

ce qui contredit (6.10), à moins que $|\phi>$ et $|\psi>$ sont orthogonaux.

6.6 Le produit tensoriel

Soient V_1 et V_2 deux espaces vectoriels, on appelle produit tensoriel de V_1 et V_2 un espace vectoriel W muni d'une application

$$\begin{aligned} V_1 \times V_2 &\longrightarrow W = V_1 \otimes V_2 \\ (x_1, x_2) &\longmapsto x_1 \otimes x_2, \end{aligned} \tag{6.11}$$

vérifiant :

1. $(a_1 x_1 + a_2 x_2) \otimes b = (a_1 \otimes b) x_1 + (a_2 \otimes b) x_2$

   $a \otimes (b_1 x_1 + b_2 x_2) = (a \otimes b_1) x_1 + (a \otimes b_2) x_2$

   i.e., $x_1 \otimes x_2$ dépend linéairement de chacune des variables x_1 et x_2.

2. Si e_{i_1} est une base de V_1 et e_{i_2} est une base de V_2 la famille des produits $(e_{i_1} \otimes e_{i_2})$ est une base de W.

Un tel espace vectoriel est unique (à isomorphisme prés). On le note : $V_1 \otimes V_2$.

La dimension du produit tensoriel $V_1 \otimes V_2$ est :

$$\dim(V_1 \otimes V_2) = \dim V_1 \dim V_2.$$

6.7 Le produit tensoriel des matrices

Le produit tensoriel aussi connu sous le nom du produit de Kronecker d'une matrice A de type (n, m) et d'une matrice B de type (k, l) donne la

matrice de type (nk, lm) suivante :

$$A \otimes B = \begin{pmatrix} Ab_{00} & Ab_{01} \cdots & Ab_{0l-1} \\ Ab_{10} & Ab_{11} \cdots & Ab_{1l-1} \\ \vdots & \vdots & \vdots \\ Ab_{k-10} & Ab_{k-11} \cdots & Ab_{k-1l-1} \end{pmatrix}$$

Le produit tensoriel d'un vecteur collone u de longueur n et d'un vecteur collone v de longueur k est donc donné par :

$$\mathsf{u} \otimes \mathsf{v} = \begin{pmatrix} \mathsf{u}v_1 \\ \mathsf{u}v_2 \\ \vdots \\ \mathsf{u}v_k \end{pmatrix}$$

Appendice B

6.8 Rappels de la théorie de complexité

Dans cette section on s'intéresse à rappeler quelques définitions et résultats classiques à la base de la théorie de la complexité.

Définition 6.8.1 *Un problème est une question à laquelle on veut apporter une réponse. Tout problème comporte dans sa description des paramètres formels, en donnant des valeurs à ces paramètres on obtient une instance du problème. Résoudre un problème c'est donner une réponse à toutes ses instances possibles.*

Définition 6.8.2 *Un algorithme de résolution d'un problème* Π *donné est une procédure, décomposable en un nombre fini opérations élémentaires, transformant une chaîne de caractères représentant les données de n'importe quel exemple du problème* Π *en une chaîne de caractères représentant les résultats de* Π.

Il arrive souvent que des algorithmes conçus pour résoudre le même problème diffèrent fortement entre eux. Ces différences peuvent être bien plus importantes que celles dues au matériel, aux logiciels ou encore aux programmeurs.

Il faut donc trouver un moyen pour juger l'efficacité d'un algorithme et pour comparer plusieurs algorithmes entre eux sans tenir compte des machines utilisées.

Définition 6.8.3 *Le temps d'exécution d'un algorithme est le nombre d'opérations élémentaires nécessaire pour résoudre un problème. La complexité d'un algorithme mesure le temps d'éxécution en fonction de sa taille (le nombre de cases nécessaires pour stocker toutes les données). Soit $f(T)$ la durée pour résoudre un problème de taille T, si $f(T) = \mathcal{O}(g(T))$ où g est un polynôme alors le problème est dit de complexité polynomiale, sinon il est dit de complexité exponentielle.*

6.8.1 Complexité des problèmes

La théorie de la complexité permet de classer les problèmes de décision (un problème de décision est un problème pour lequel la réponse est oui ou non) en deux classes faciles et difficiles en fonction de la complexité des algorithmes qui existent pour les résoudres.

Cependant, il est aussi possible d'associer à chaque problème d'optimisation, un problème de décision en introduisant un seuil k correspondant à la fonction objectif f. Le problème de décision devient ;" existe-t-il une solution réalisable (S) tel que $(f(S) \leq k($ ou $\geq k)$?".

Définition 6.8.4 *Un problème est dit facile s'il existe un algorithme polynomial pour le résoudre. Sinon le problème est dit difficile.*

Définition 6.8.5 *La complexité d'un problème est la complexité (dans le pire des cas) du meilleur algorithme connu pour le résoudre.*

6.8.2 Classes de complexité

- **La classe P (Polynomial)** : Un problème est dit appartenir à la classe P s'il existe un algorithme polynomial en taille des données pour le résoudre.
- **La classe NP (Non-deterministic polynomial)** : Cette classe réunit les problèmes de décision pour lesquels la réponse oui peut être décidée par un algorithme non-déterministe en un temps polynomial par rapport à la taille de l'instance. Un algorithme est dit non-déterministe s'il compte des instructions de choix. Pour ces algorithmes, si à chaque instruction le bon choix est effectué, le temps de calcul est polynomial. Si au contraire tous les choix sont énumérés, l'algorithme devient déterministe et son temps d'execution devient exponentiel.

  Pour montrer qu'un problème est dans la classe NP, il suffit de trouver un algorithme qui vérifie si une solution donnée est valide en temps polynomial.

  Un problème A est dit **réductible** à un problème B s'il existe un algorithme résolvant A utilisant un algorithme résolvant B.

  Dans le cas où l'algorithme résolvant A est polynomial en considérant l'appel à celui qui résoud B comme une opération élémentaire, la réduction est dite **polynomial**.
- **La classe NP-Complet** : La classe NP-Complet est une sous classe des problèmes NP. Un problème est NP-Complet quand tous les problèmes appartenant à NP lui sont polynomialement réductibles. Si on trouve un algorithme polynomial pour un problème NP-Complet, on trouve

alors automatiquement une résolution polynomiale de tous les problèmes de la classe NP.

- **La classe NP-Dur** : La classe NP-Dur est une sous classe des problèmes d'optimisation, telle que tous problème d'optimisation combinatoire peut se réduire polynomialement à ses problèmes.

Conclusion et Perspectives

Ce travail a permis de résoudre certains problèmes ouverts dans la théorie des codes, spécialement la déterminantion du nombre des codes cycliques qui est lié aux algorithmes d'équivalence, la détermination des propriétés des codes BCH non-primitifs, la caractérisation des codes affine-invariants maximaux, le calcul de leur groupe de permutations, l'existence des codes duadiques lorsque l'ordre multiplicatif de q modulo n est pair et finalement les problèmes de dualités pour ces codes. Nous avons construit de nouvelles familles de codes quantiques, dont certaines sont trés intéressantes du point de vue correctablilité. Nos outils pour cela ont été la théorie des nombres élémentaire, les propriétés des classes cyclotomiques et certaines propriétés combinatoires dans les corps finis.

Nous proposons des questions dont certaines sont un prolongement possible de notre travail, d'autres sont indépendantes.

- La classification des groupes de permutations des codes cycliques.
- Est ce qu'on peut trouver d'autres méthodes pour construire des codes quantiques intéréssants à partir des codes classiques.
- Il est bien connu que la classe des codes BCH primitifs est mauvaise asymptotiquement [38]. Est ce que c'est le cas pour nos codes BCH et

est ce que les codes quantiques construits à partir de cette classe sont bons asymptotiquement ?

- Montrer que les codes affines-invariants maximaux et les codes affines invariants tels que leur ensemble de définition est de la forme $\cup C(p^j) \cup \{0\}$, sont les seules codes qui admettent pour groupe de permutations le groupe engendré par le groupe affine et le Frobenius.

Bibliographie

[1] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, *Duadic Group Algebra Codes,* Proc. IEEE Intern. Sym. Inform. Theory, Seattle, USA, 2096-2100, 2006.

[2] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, *Remarkable degenerate quantum stabilizer codes derived from duadic codes*, Proc. IEEE Intern. Sym. Inform. Theory, Seattle, USA, 1114-1118, 2006.

[3] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, *On Quantum and Classical BCH Codes*, IEEE Trans. Inform. Theory, 53(3), Mar. 2007.

[4] A. Ashikhmin, E. Knill, *Nonbinary quantum stabilizer codes,* IEEE Trans. Inform. Theory 47 3065-3072, 2001.

[5] P. A. Benioff, *Quantum mechanical hamiltonian models of discrete processes that erase their own histories : Application to turing machines,* Internat. J. Theor. Physics 21 :3/4, 177- 202, 1982.

[6] C. H. Bennett, *Comments by C. H. Bennett,* Proc. Army Research Office Conference on Quantum Computer and Cryptography, Tucson, Feb. 1995.

[7] C. H. Bennett, D. DiVincenzo, J. Smolin and W. Wooters, *Mixed state entenglement and quantum error correction,* Phy. Rev. A 54, 3824-3851, 1996.

[8] T. P. Berger, *Sur le groupes d'automorphismes des codes cycliques étendus primitifs affine-invariants,* Thèse de Doctorat d'État, Université de Limoges,

Sep. 1991.

[9] T. P. Berger, *On the automorphism groups of affine invariant codes* Design, Codes and Cryptography, 7, 215-221, 1996.

[10] T. P. Berger, P. L. Cayrel, P. Gaborit and A. Otmani, *Reducing key lengths with quasi-cyclic alternat codes,* Code-Based Cryptography 2008.

[11] T. P. Berger and P. Charpin, *The permutation groups of affine invariant extended cyclic codes* IEEE Trans. Inform. Theory, 42, 2194-2309, 1996.

[12] T. P. Berger, *Groupes d'automorphismes et de permutations des codes affine-invariants,* Habilitation à diriger des recherches, Université de Limoges, Sep. 1996.

[13] T. P. Berger and P. Charpin, *The automorphism groups of BCH codes and of some affine-invariant codes over extension fields,* Design, Codes and Cryptography, 18, 29-53, 1999.

[14] A. R. Calderbank, E. M. Rains, P. Shor and N. J. A. Sloane, *Quantum error correction and orthogonal geometry,* Phy. Rev. Lett 78, 405-408, 1997.

[15] A. Canteaut and F. Chabaud, *A new algorithm for finding minimum-weight words in a linear code : Application to McEliec's cryptosystem and to narrow sens BCH codes of lenght 511,* IEEE Trans. Inform. Theory, 44 N(1), 367-378, 1998.

[16] C. Chabot, K. Guenda and B. Kadri, *Facotrization step in the list-decoding algorithm,* Submitted to Studia Informatica, 2009.

[17] P. Charpin, *Codes Cycliques étendus invariants sous le groupe affine,* Thèse de Doctorat d'État, Université de Paris VII, Jan. 1987.

[18] P. Charpin and F. Levy-Dit-Vehel, *On Self-Dual Affine-Invariant Codes,* J. Combin. Theory, 67(2), Aug. 1997.

[19] P. Charpin, *Open problems on cyclic codes, Handbook of coding theory*, Vol. I, II, Elsevier, 1998.

[20] R. Cleve, *Quantum stabilizer codes and classical codes,* Phys. Review, A, V9560, N3, p. 4054-4059, 1997.

[21] G. Cohen, S. Encheva and S. Litsyn, *On binary construction of quantum codes,* IEEE. Trans. Inf. Theory 45, (7) p. 2495-2498, 1999.

[22] M. Demazure, *Cours D'Algèbre : Primalité. Divisibilité. Codes.* Cassini, Paris, 1997.

[23] D. P. Divencenzo, P. W. Shor, *Fault-Tolerant Error Correction with Efficient Quantum Codes,* Phys. Rev. Lett. 77, 3260-3263, 1996.

[24] D. Deutsch, *Quantum theory, the church-turing principle and the universal quantum computer,* Proc. R. Soc. London, A 400, 97-117. 1985.

[25] I. Dumer, D. Micciancio and M. Sudan, *Hardness of approximating the minimum distance of a linear code*, IEEE Trans. Information Theory 49(1), Jan. 2003.

[26] R. P. Feynman, *Simulating physics with computers,* Internat J. Theor. Phys., 21 : 6/7, 467-488, 1982.

[27] D. Gottesman, Ph.D. Thesis, California Institute of Technology, Pasadena, CA. 1997.

[28] M. Grassl, T. Beth, *Quantum BCH codes,* Internat. J. Quant. Information, 2(1), 757-775, 2004.

[29] M. Grassl, T. Beth and M. Rötteler, *On optimal quantum codes,* Internat. J. Quantum Information, 2(1) : 757-775, 2004.

[30] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes.* Online available at http ://www.codetables.de. Accessed on 2009-04-2.

[31] K. Guenda, *Quantum Duadic and Affine Invariant Codes.* Internat. J. Quantum Information, 2(1) : 757-775, Feb. 2009.

[32] K. Guenda, *Dimension and Minimum Distance of a Class of BCH Codes,* Ann. Sci. Math. Québec 1 : 57-62, 2008.

[33] M. Hirvensalo, *Quantum computing,* Springer 2004.

[34] S. K. Houghten and J. L. Wallis, *A comparative study of search thechniques applied to the minimum distance problem of BCH codes,* Proceedings 6Th IASTED International Conference on Artificial Intelligence and Soft Computing, Banff, July 2002.

[35] W. C. Huffman, V. Job and V. Pless, *Multiplier and generalized multipliers of cyclic objects and cyclic codes,* J. Combin. Theory A (62) 183-215 1993.

[36] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes,* Cambridge, 2003.

[37] T. Kasami, S. Lin and W. W. Peterson, *Some results on cyclic codes which are invariant under the affine group and their application,* Inform. Control, 11 : 475-496, 1967.

[38] T. Kasami, S. Lin and W. W. Peterson, *An upper bound on k/n for affine-invariant codes with fixed d/n,* IEEE Trans. Inform. Theory, IT-15, 174-176, 1969.

[39] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, *Non-binary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory, 52(11), 4892-4916, 2006.

[40] J. L. Kim and J. Walker, *Nonbinary Quantum error-correcting codes from algebraic curves,* Discr. Math, 308 (14), 3115-3124, 2008.

[41] A. Kitaev, *Topological quantum codes and anyons, Quantum computation : a grand mathematical chal- lenge for the twenty-* , Math., vol. 58, Amer. Math. Soc., Providence, RI, 2002, pp. 267.

[42] E. Knill, *Group representation error bases and quantum codes,* Los Alomos National Laboratory report LAUR-962807, 1996.

[43] E. Knill and R Laflamme, *A Theory of Quantum Error correcting codes,* LANL e-print quant-ph/9604034.

[44] E. Knill R. Laflamme and L. viola, *Theory of quantum error correction for general noise,* Phys. Rev. Letters, V. 48 (11), 2525-2528, Mar. 2000. *Non-binary quantum error-correcting codes from algebraic curves,* Disc. Mathematics 3115-3124, 2008. Trans. Inform. Theory, 47 3065-3072, 2001.

[45] J. S. Leon, *A probabilistic algorithm for computing minimum weight of large error-correcting codes,* IEEE Trans. Inform. Theory, 34, 1354-11358, 1988.

[46] J. S. Leon, *Permutation Group Algorithms Based on Partitions, I : Theory and Algorithms.* J. Symbolic Computation 12, 1991, 533-583.

[47] W. J. LeVeque, *Elementary theory of numbers,* Dover, New York, 1990.

[48] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications,* Cambridge University Press 1986.

[49] F. J. Macwilliams and N.J.A Sloane, *The theory of error correcting-codes,* Benjamin, Inc. Amsterdam, North-Holland, 1977.

[50] R. Matsumoto and T. Uyematsu, *Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes,* IEICE Trans. Fundamentals v. E83-A N 10 october 2000.

[51] M. A. Nielsen and I. A. Chuang, *Quantum computation and quantum information,* Cambridge, London, 2000.

[52] O. Papini, *Etude de techniques de décodage par permutation,* Thèse de 3ième cycle, Université de Toulon 1984.

[53] E. Pertrand and R. M. Roth, *Is code equivalence easy to decide*, IEEE Trans. Inform. Theory, 43(5), Sep. 1997.

[54] V. Pless, *Q Codes,* J. Combin. Theory. Ser. A, 43, 1986.

[55] V. Pless, *Duadic Codes Revisited,* Congressus Numerantium, 59 : 225-233, 1987.

[56] D. Poulin, *Stabilizer formalism for Operator Quantum error correction,* IEEE Trans. Inform, 45(1), 266-271, Jan. 1999.

[57] J. Preskill, *Lecture notes for physics,* Quantum Information, 1998.

[58] E. M. Rains, *Quantum code of minimum distance two,* IEEE Trans. Inform, 45(1), 266-271, Jan. 1999.

[59] S.Roman, *Coding and information theory.* Springer Verlag, New-York, 1992.

[60] J. J. Rushanan, *Topics in Integral Matrices and Abelian Group Codes,* Ph.D. Thesis, California Institute of Technology, 1986.

[61] J. J. Rushanan, *Duadic codes and difference sets,* J. Combin. Theory Ser. A, 57 : 254-261, 1991.

[62] P. K. Sarvepalli and A. Klappenecker, *Nonbinary Quantum Reed-Muller Codes* , arXiv : quant-ph/0502001 v1, Jan. 2005.

[63] P. W. Shor, *Scheme for reducing decoherence in quantum memory*, Phys. Rev. A, 2 : 2493-2496, 1995.

[64] P. W. Shor, *Polynomial-algorithm for prime factorization and discret logarithm on a quantum computer* SIAM J. Comp. 26(5) 1484-1509, 1997.

[65] G. Skersys, *Calcul du groupe d'automorphismes des codes. Détermination du groupe d'automorphismes,* Ph.D thesis, LACO, Limoges, October, 1999.

[66] M. H. M. Smid, *Duadic codes,* IEEE. Trans. Inform. Theory, 29(2), 1983.

[67] P. Steane, *Multiple particle interference and quantum error correction*, Proc. R. Soc. London A, 452 : 2551-76, 1996.

[68] A. M. Steane, *Enlargement of Calderbamk Shor Steane quantum codes,* IEEE. Trans. Inform. Theory, 45(7), 2492-2495, 1999.

[69] W. G. Unruh, *Maintaining coherence in quantum computer,* Phys. Rev. A 51, 992-997, 1995.

[70] J. Wolfman, *New bounds on cyclic codes from algebraic curves ,* in "Lecture Notes in Computer Science". 388 : 47-62, Springer-Verlag, 1989.