Université Paris 8

École doctorale Cognition, Langage, Interaction - ED 224
Laboratoire Analyse, Géométrie et Applications - UMR 7539

Thèse

Doctorat en mathématiques

Interactions entre Combinatoire Additive et Théorie des Codes

---

Auteur: Martin SCOTTI

Directeur: Wolfgang SCHMID
Co-directeur: Martino BORELLO

Présentée et soutenue publiquement le 8 octobre 2025

Devant un jury composé de :

Alain Couvreur	Inria Saclay	Président
Leo Storme	Universiteit Gent	Rapporteur
Gilles Zémor	Université de Bordeaux, IMB	Rapporteur
Gianira Alfarano	Université de Rennes 1, IRMAR	Examinatrice
Eimear Byrne	University College Dublin	Examinatrice
Sihem Mesnager	Université Paris 8, LAGA	Examinatrice
Wolfgang Schmid	Université Paris 8, LAGA	Directeur de thèse
Martino Borello	Université Paris 8, LAGA	Co-directeur de thèse

Contents

Résumé en français

Après de rapides rappels, nous étudions les codes minimaux et les codes intersectants en métrique de Hamming, puis nous introduisons les codes intersectants en métrique rang $\mathbb{F}_{q^m}$-linéaire.

Dans le cas des codes minimaux, nous prouvons une borne inférieure asymptotique sur la longueur minimale d'un code minimal, et nous nous intéressons aux codes les plus courts possibles dans le cas binaire.

Dans le cas des codes intersectants en métrique de Hamming, nous donnons une interprétation géométrique de ces codes dans l'espace projectif. De cette interprétation géométrique, nous affinons les bornes existantes sur la plus petite longueur d'un code intersectant, et nous donnons de nouvelles constructions explicites de petite taille de codes intersectants.

Après avoir rappelé le lien entre les codes intersectants et la constante de Davenport, nous en donnons une généralisation à n'importe quelle valeur de q. Cela nous permet de généraliser les bornes sur cette constante, et de donner des constructions explicites de longues suites qui n'ont pas deux sous-suites disjointes à somme nulle.

Puisque la constante de Davenport a un lien avec la théorie de la factorisation dans les corps de nombres, nous établissons une interprétation de la constante de Davenport correspondant aux codes intersectants. Nous montrons alors un lien avec l'action du groupe de Galois sur le groupe de classes.

Enfin, nous introduisons les codes intersectants en métrique rang. Nous montrons qu'il existe une caractérisation géométrique des q-systèmes correspondant à ces codes, et après avoir étudié leur propriétés, nous donnons des bornes sur les rangs admissibles pour ces q-systèmes.

Abstract in english

After a brief review of basic notions, we investigate minimal codes and intersecting codes in the Hamming metric. We then introduce intersecting codes in the rank metric (for $\mathbb{F}_{q^m}$-linear codes).

For minimal codes, we prove an asymptotic lower bound on the minimum length of a minimal code and investigate the shortest possible codes in the binary case.

For intersecting codes in the Hamming metric, we provide a geometric interpretation of these codes in projective space. From this geometric perspective, we refine existing bounds on the smallest possible length of an intersecting code and present new explicit constructions of short intersecting codes.

After recalling the connection between intersecting codes and the Davenport constant, we generalize it for any value of q. This allows us to extend bounds on this constant and provide explicit constructions of long sequences without two disjoint zero-sum subsequences.

Since the Davenport constant is linked to factorization theory in number fields, we establish an interpretation of the Davenport constant corresponding to intersecting codes. We then demonstrate a connection with the action of the Galois group on the class group.

Finally, we introduce intersecting codes in the rank metric. We show that there is a geometric characterization of the q-systems corresponding to these codes. After studying their properties, we derive bounds on the admissible ranks for these q-systems.

Remerciements

Mes remerciements vont tout d'abord à Leo Storme et à Gilles Zémor, qui ont accepté d'être les rapporteurs de cette thèse. Leurs commentaires et conseils m'ont permis d'améliorer considérablement la qualité de cette thèse. Les quelques coquilles et contrepèteries qui restent sont entièrement de ma responsabilité.

Je remercie également Sihem Mesnager, Eimear Byrne, et Gianira Alfarano d'avoir été examinatrices, et pour les nombreuses et belles discussions que j'ai pu avoir avec chacune d'entre elles, sur les mathématiques ou sur tout ce qui les entoure.

J'aimerais aussi exprimer ma profonde gratitude à Wolfgang Schmid, pour son dévouement et sa disponibilité, ainsi que pour m'avoir guidé dans ma recherche tout aussi bien que dans mes autres responsabilités au sein de l'université. Avec Martino Borello, il a su créer un environnement de recherche dans lequel je me suis pleinement épanoui.

Martino Borello a été pour moi bien plus que ce que le simple terme de co-directeur de thèse laisse entendre. Il m'a transmis son goût pour les approches géométriques de problèmes mathématiques (que l'on retrouve tout au long de ce travail), et j'en suis venu à partager (parfois avec un peu moins de talent) beaucoup de ses intuitions sur des questions mathématiques. Il m'a aussi transmis un petit bout de culture culinaire italienne[1]. Martino a également eu un grand impact sur ma vision de questions plus personnelles, comme sur le sens de l'activité de recherche, ou encore sur les grandes questions de la vie. J'ai beaucoup mûri à ses côtés, et je le remercie très affectueusement pour l'influence qu'il a eu sur moi.

Cette thèse n'aurait pas été possible sans Alain Couvreur. Avant d'être le chercheur accueillant et toujours prêt à discuter que j'ai connu dans les retraites Barracuda et à l'Inria Saclay, Alain avait été mon professeur de théorie des codes en M2 MPRI. Ses cours (tout autant que ceux de Pascal Molin, que j'avais suivi avec passion un semestre auparavant) m'ont fait découvrir un domaine des mathématiques dont je connaissais à peine l'existence, à une époque où j'avais échoué à entrer dans le monde de la recherche en théorie analytique des nombres. La théorie des codes a été pour moi une seconde vie mathématique, dans un moment où je commençais à faire le deuil de mes ambitions de recherche. Alain a gracieusement accepté d'être le président du jury lors de ma soutenance, ce pour quoi je le remercie chaleureusement.

C'est ainsi en grande partie à Wolfgang, Martino et Alain que je dois l'accomplissement de mon rêve de faire de la recherche en mathématiques, et je leur dédie cette belle thèse.

Les doctorants, postdocs et chercheurs permanents de l'ANR Barracuda ont été une grande famille étendue de recherche pour moi. Merci en particulier à Jade et Elena pour leur séminaire

[1] De manière très grossière et injuste, on peut classer les Italiens en deux catégories : ceux qui font des chichis sur la nourriture, et ceux qui n'en font pas. Martino appartient à la première catégorie. En mon expérience c'est de ce genre de personnes exigentes que l'on apprend le plus de choses. Je tiens également à dire que Martino refuse toujours de goûter à ma carbonara, malgré mes meilleurs efforts. Je l'ai vu en préparer une, et on a la même recette.

CAIPI (et pour leurs karaokés), merci à Maxime, Clément, Hugues, Christophe, Candice, Emmanuel, Marc, Bastien, Ruben, Camille, Alix, Dounia, et à tous les autres.

Une grande partie de mon travail a été réalisée au sein de l'équipe Grace à l'Inria Saclay, dirigée par Alain Couvreur. J'y ai été chaleureusement accueilli par tous les membres, et je remercie Bruno, Thomas, Rakhi, Hugo, Pierre, Rati, Lola, Nihan, Estelle, Christophe, Daniel, Maxence, Olivier, Ben, et François. J'ai pu participer avec joie aux sessions du séminaire Godzilla (pour les #youngpeople), ainsi qu'au séminaire régulier de l'équipe. Je remercie tout particulièrement Valentina, ma petite sœur de recherche, pour sa gentillesse et son humour.

Je souhaite remercier affectueusement les équipes de recherche des universités de Caserte, de Naples, et de Delft, qui m'ont invité pour des séjours de recherche, et auprès desquelles je me suis toujours senti comme chez moi. Le monde de la recherche serait significativement moins joyeux sans vous. A Ferdinando, Olga, Paolo, Chiara, Giuseppe, Rocco, Giovanni, Alessandro, Anurag, Ananth, merci.

Au début de mon doctorat, ces mathématicien.ne.s (et d'autres) n'étaient que des noms que je lisais au début des articles en me disant "Qu'est-ce que c'est intéressant ! Quelle bonne idée ! J'aimerais vraiment avoir des idées aussi bonnes un jour...". J'ai été très touché de rencontrer toute ces personnes dans les différentes conférences auxquelles j'ai assisté, et de voir l'étendue de leur culture mathématique et de leur gentillesse. Une liste exhaustive de noms pourrait facilement couvrir toute une page.

On dit quelquefois que ceux qui savent faire quelque chose le font, et les autres l'enseignent. Dans cette perspective, j'ai eu l'occasion d'enseigner l'analyse complexe et la combinatoire deux années de suite. Je remercie vivement les étudiants qui ont suivi ces cours pour leur intérêt manifeste, leurs questions curieuses, et pour leur patience quand mes explications n'étaient pas assez claires. Professeur, quel beau métier !

Les professeurs de mathématiques que j'ai eu au cours de ma vie m'ont donné une culture mathématique solide, et ont toujours encouragé ma passion, chacun à sa propre manière. A MM. Brisset, Gard, Martin, Hermann, Ehinger, Kasperczak, Mansuy, et Roudneff, merci de tout cœur.

Je remercie également tous les ami.e.s qui ont été à mes côtés durant cette période, qui ont parfois écouté avec patience mes élucubrations mathématiques. Merci infiniment à Henri, Etienne, Virginio, Antoine, Axel, Baptiste, Marthe, Jacques, Brieuc, Michael, Lucas, Matthias, Arthur, Darelle, Son, Eloïse, Hanna, Anna, Leo, Robert et tous les autres.

Dans ce groupe d'amis, mes anciens camarades du Master MIC de l'Université Paris 7 occupent une place particulière. Merci beaucoup à Daphné, ainsi qu'à Marina, Marc, et Pierre-Augustin pour les sorties et les visites, pour les déjeuners et les dîners, et pour votre présence constante.

A Isabelle, Elvire, Jean-Christophe, Pierre-Alexis, merci de m'avoir si souvent invité à

déjeuner, à diner, à partir en vacances avec vous, et pour tous les autres moments à discuter et à rire ensemble.

Je remercie également chaleureusement Gioconda, Sabrina, Bruno, Selyan et Camil, ainsi que Elisabeth, Camillo, Stefan, Manuela, Christina, Gregor, Lena et Florian pour leur gentillesse, leur générosité et leur soutien. J'ai aussi une pensée pour Hans et Livio, qui ne sont plus là mais dont le souvenir m'anime encore.

Merci à mes parents, Maria et Lucien. Merci d'avoir su encourager ma passion pour les mathématiques en m'achetant régulièrement des livres de vulgarisation. Merci d'avoir su éveiller et entretenir ma curiosité scientifique. Merci aussi pour tout le reste, bien évidemment (sauf pour le fait de ne pas m'avoir fait découvrir plus tôt les joies culinaires des épices). Je suis fier d'être votre fils.

Merci aussi à ma petite sœur, Veronica, qui a toujours été à mes côtés, et qui est probablement la seule personne que je connaisse qui n'a pas fait des mathématiques parce que c'était trop facile pour elle. Quelques semaines avant ma soutenance, elle a en plus eu l'outrecuidance de devenir docteur avant moi, et qui plus est en médecine, c'est-à-dire un domaine qui sert vraiment dans la vie de tous les jours. Je lui souhaite bonne chance et beaucoup de bonheur, malgré sa tendance à me battre à Mario Kart DS.

Pour finir, je souhaite remercier tendrement ma moitié, Daphné, pour son amour et sa gentillesse à toute épreuve, pour sa présence tant dans les bons moments que dans les mauvais, et pour m'avoir suggéré la lettre κ dans mon mémoire de master en 2022.

Introduction : quatre langages, trois directions

L'objectif de cette thèse est de développer les liens entre la théorie des codes et la combinatoire additive sur des groupes abéliens finis. Il n'est pas surprenant que de tels liens puissent servir d'axes de recherche, au vu de la proximité mathématique immédiate des deux domaines (dans les deux cas nous avons affaire à de la combinatoire et de l'algèbre finie). L'objet de combinatoire additive sur lequel nous concentrerons notre attention est la constante de Davenport et ses variantes, dont l'étude peut être regroupée sous le terme générique de *problèmes de suites à somme nulle*.

La plupart des résultats de cette thèse sont tirés de nos travaux [19,62,63], ainsi que d'un article en préparation sur les codes intersectants en métrique rang, avec Martino Borello, Daniele Bartoli et Giuseppe Marino, *Linear rank-metric intersecting codes* [13].

Commençons par introduire quelques notions de théorie des codes et de combinatoire additive. Le lecteur intéressé pourra se référer à [38] pour une introduction plus complète à la théorie des codes.

En métrique de Hamming, le support d'un vecteur $x \in \mathbb{F}_q^n$ est $\sigma(x) = \{i \mid x_i \neq 0\}$, et son poids de Hamming est $\mathrm{wt}(x) = |\sigma(x)|$. Un $[n,k,d]_q$-code linéaire est un sous-espace de dimension k de $\mathbb{F}_q^n$ dont tous les vecteurs non nuls ont poids de Hamming au moins d.

En métrique rang, on ne considère plus des vecteurs, mais des matrices, et le poids d'un mot de code est son rang. Nous travaillerons dans le cas où notre espace de matrices est $\mathbb{F}_{q^m}$-linéaire, que l'on peut alors assimiler à un sous-espace vectoriel de dimension k de $\mathbb{F}_{q^m}^n$. Si tous les vecteurs non nuls du sous-espace correspondent à des matrices de rang au moins d, on parle de $[n,k,d]_{q^m/q}$-code en métrique rang.

En métrique rang comme en métrique de Hamming, une matrice génératrice d'un code $\mathcal{C}$ de dimension k dans $\mathbb{F}_q^n$ (ou $\mathbb{F}_{q^m}^n$) est une matrice G à k lignes et n colonnes, telle que $\mathrm{rowspan}(G) = \mathcal{C}$. Une matrice de parité de $\mathcal{C}$ est une matrice H telle que $\mathcal{C} = \ker(H) = \{c \mid H \cdot c = 0\}$.

En combinatoire additive, notre objet central est la constante de Davenport d'un groupe abélien fini. Etant donné un groupe abélien fini G, et une suite $a_1, \dots, a_n$ d'éléments de G (les répétitions sont permises), une sous-suite à somme nulle est une sous-suite $a_{i_1}, \dots, a_{i_r}$ telle que $\sum_{j=1}^{r} a_{i_j} = 0_G$. Il est clair que pour un groupe abélien fini, une suite assez longue doit avoir une sous-suite (non vide) à somme nulle. La constante de Davenport de G, notée $\mathrm{D}(G)$, est le plus petit entier ℓ tel que toute suite de longueur au moins ℓ admet une sous-suite (non vide) à somme nulle. Le lecteur intéressé pourra trouver une introduction plus développée à la combinatoire additive dans [32].

L'idée centrale, qui sert de base à tout notre travail, est la suivante.

Proposition 0.0.1. Soit $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$ une matrice et $\mathcal{C} = \ker H \subset \mathbb{F}_q^n$. Un élément $c \in \mathcal{C}$ correspond à une suite à somme nulle (pondérée par les coefficients de c) de colonnes de H

$$\sum_{i=1}^{n} c_i H_i = 0,$$

où H_i désigne la i-ème colonne de H.

Notons que les colonnes de H appartiennent à $\mathbb{F}_q^{n-k}$, qui est un groupe abélien fini, ce qui permet d'entrevoir un lien entre théorie des codes et constante de Davenport.

Notre travail est divisé en trois chapitres. Le premier est consacré aux codes minimaux (en métrique de Hamming), le deuxième aux codes intersectants en métrique de Hamming, et le troisième aux codes intersectants en métrique rang.

Dans le domaine particulier de la théorie des codes, nous utiliserons fréquemment une approche géométrique. L'idée générale est d'associer à une matrice génératrice d'un $[n, k, d]_q$-code $\mathcal{C}$ en métrique de Hamming un ensemble de points de l'espace projectif $\mathrm{PG}(k-1, q)$. Les propriétés géométriques de cet ensemble de points sont intimement reliées aux propriétés du code $\mathcal{C}$. Ainsi, la géométrie projective devient un nouveau langage dans lequel nous pouvons exprimer les problèmes que nous étudions dans le cadre de la théorie des codes et de la combinatoire additive.

Une approche similaire existe également en métrique rang. A une matrice génératrice on associe un q-système, c'est-à-dire un sous-espace $\mathbb{F}_q$-linéaire de $\mathbb{F}_{q^m}^k$, obtenu en faisant le $\mathbb{F}_q$-span des colonnes. A un q-système correspond également un sous-ensemble de $\mathrm{PG}(k-1, q^m)$, que l'on appelle un *ensemble linéaire*.

Notre étude des codes intersectants permet d'établir des liens entre certaines généralisations de la constante de Davenport et la théorie des codes. Il s'avère qu'il est même possible de déterminer des liens explicites avec la théorie de la factorisation dans les corps de nombres.

Nous avons porté une attention particulière à cette partie de notre travail, afin d'y donner un cadre le plus complet possible.

Notre exposition est divisée en cinq chapitres. Pour commencer, deux chapitres introductifs présentent l'essentiel des prérequis en théorie des codes et en combinatoire additive sous une forme synthétique. Puisque, comme nous l'avons vu plus haut, notre travail touchera à de nombreux champs d'étude mathématique, le champ des prérequis est assez large.

Codes minimaux et ensembles générateurs d'hyperplans

Les codes minimaux sont un objet classique de théorie des codes, étudiés par exemple dans [3, 4,6,8,9,14,18,26,41,51,52]. Ils ont de nombreuses applications, en particulier pour un protocole cryptographique de secret partagé, ainsi que pour l'étude des ensembles saturants (qui sont intimement reliés à l'étude du problème du recouvrement).

Ils sont définis comme suit.

Définition. Soit $\mathcal{C}$ un $[n,k,d]_q$-code, et $c \in \mathcal{C} \setminus \{0\}$ un mot de code non nul. On dit que c est minimal si

$$\forall c' \in \mathcal{C} \setminus \{0\}, \quad \sigma(c') \not\subset \sigma(c).$$

On dit que $\mathcal{C}$ est minimal si tous les mots de code (non nuls) de $\mathcal{C}$ sont minimaux.

Notre travail s'inscrit dans la lignée de l'approche géométrique découverte simultanément en 2019 dans [3,66]. Selon ces travaux, il existe une bijection entre les classes d'équivalence de codes minimaux et les classes d'équivalence projectives d'ensembles de points de l'espace projectif avec la propriété de pouvoir engendrer tout hyperplan. Pour ce premier travail en langue francaise, nous avons choisi d'appeler ces ensembles des *ensembles générateurs d'hyperplans*. Ceux-ci ont été introduits pour la première fois en 2011 dans [31].

Nous voulons étudier la fonction $m(k,q)$, qui désigne le plus petit entier n tel qu'il existe un $[n,k]_q$-code minimal. Nous nous intéressons au régime où q est fixé et k est grand.

Grâce aux travaux cités plus haut, il est connu que cette fonction $m(k,q)$ est bornée par le haut et par le bas par des fonctions de la forme ckq, où $c > 0$. Cependant, il n'est pas connu à ce jour si $\lim_{k\to\infty} m(k,q)/k$ existe. Dans [6], les auteurs établissent le résultat suivant.

Théorème.

$$m(k,q) \geq (k-1)(q+1).$$

Notre travail nous permet d'établir le théorème suivant.

Théorème ([62], Théorème 3.3., et [16], Théorème 1.4.)**.**

$$\liminf_{k\to\infty} m(k,q) \geq (q+\varepsilon(q)) \cdot k,$$

où ε est une fonction croissante qui vérifie

$$1.5204 \leq \varepsilon(2) \leq \varepsilon(q) \leq \sqrt{2} + \frac{1}{2}.$$

L'une des conséquences immédiates de notre résultat est que, à q fixé, il ne peut exister qu'un nombre fini de codes minimaux pour lesquels $n = (k-1)(q+1)$.

Il est donc naturel de s'intéresser à ces codes particuliers, ce que nous faisons dans la suite de notre chapitre dans le cas particulier où $q = 2$. Nous montrons que de tels codes n'existent pas quand $k \in \{7, 8, 9, 11\}$, et n'existent pas non plus quand $k = 5 \pmod 8$.

Dans la suite du chapitre, nous nous intéressons à divers résultats sur les codes minimaux et sur les ensembles générateurs d'hyperplans, en particulier une construction explicite présentée dans [7], et les nombreuses applications des codes minimaux, par exemple pour l'étude des ensembles saturants.

Codes intersectants en métrique de Hamming

Les codes intersectants en métrique de Hamming sont définis comme suit.

Définition. Un code $\mathcal{C}$ est dit intersectant si

$$\forall c, c' \in \mathcal{C} \setminus \{0\}, \quad \sigma(c) \cap \sigma(c') \neq \varnothing.$$

On constate rapidement que la définition d'un code intersectant coïncide avec celle d'un code minimal quand $q = 2$. Tout code minimal est intersectant, mais l'inverse n'est pas vrai quand $q > 2$.

Les codes intersectants ont été fréquemment étudiés dans la littérature, par exemple dans [27,29,58,60,64]. Si beaucoup de travaux ne s'intéressent qu'au cas $q = 2$, qui est le plus directement utile pour des applications, les codes intersectants pour d'autres valeurs de q ont également été étudiés. Des applications des codes intersectants au transfert inconscient et à d'autres problèmes ont été données par exemple dans [17,22,30].

Notre approche sera assez similaire à celle pour les codes minimaux.

Premièrement, après avoir exploré quelques propriétés élémentaires des codes intersectants, nous verrons qu'ils correspondent aux ensembles non-2-cohyperplanaires (N2C), qui sont les ensembles de points de $\mathrm{PG}(k-1, q)$ qui ne sont pas contenus dans l'union de deux hyperplans.

On conçoit aisément que de tels ensembles doivent avoir une taille minimale, qui correspond à la longueur minimale d'un code intersectant de dimension k sur $\mathbb{F}_q$. Nous notons cette taille minimale $i(k, q)$ par analogie avec la fonction $m(k, q)$ définie plus haut.

En utilisant des méthodes analogues à celles du précédent chapitre, nous établissons les théorèmes suivants, qui donnent des bornes inférieures sur $i(k, q)$.

Théorème.

$$i(k,q) \geq 2k-1,$$

et l'égalité n'est satisfaite que par les codes MDS.

Théorème.

$$\liminf_{k\to\infty} \frac{i(k,q)}{k} \geq 2 + \frac{1}{q-1}.$$

Théorème. Pour $q \leq 17$, il est possible de donner de meilleures bornes inférieures asymptotiques que celles du théorème précédent, elles sont résumées dans le Tableau 1.

q	$\liminf_{k\to\infty} \frac{i(k,q)}{k}$
2	3.5276
3	2.8272
4	2.5713
5	2.4342
7	2.2862
8	2.2411
9	2.2060
11	2.1547
13	2.1185
16	2.0802
17	2.0703

Table 1: Borne inférieure sur la longueur asymptotique des codes intersectants

Les bornes inférieures sur $i(k,q)$ exposées ici peuvent être interprétées comme des résultats d'inexistence, i.e. il n'existe pas de codes intersectants plus courts que telle valeur. Les bornes supérieures sur $i(k,q)$ correspondent, elles, à des résultats d'existence, i.e. il existe des codes intersectants avec telle longueur. Ces résultats d'existence peuvent prendre deux formes : soit probabiliste et non explicite, soit explicite (correspondant à un choix explicite de points sur une courbe algébrique, comme expliqué dans [58]).

Voici le résultat probabiliste, déjà bien connu dans la littérature [27].

Théorème. Si

$$n \geq \frac{2}{\log_q(\frac{q^2}{2q-1})}\ k$$

alors il existe un $[n,k,d]_q$-code intersectant. Par conséquent on a

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq \frac{2}{\log_q(\frac{q^2}{2q-1})}.$$

Dans le cas des constructions explicites, nous utilisons l'argument de graphes expanseurs et de codes AG proposé dans [7] pour les codes minimaux et donnons une construction explicite analogue pour des codes intersectants. La valeur de la constante $\alpha(q,t)$ correspond à une borne supérieure (issue d'une construction explicite)

$$\limsup_{k\to\infty} \frac{i(k,q^2)}{k} \leq \alpha(q,t).$$

q	t	$\alpha(q,t)$
3^2	86	299.5378
4^2	39	110.0490
5^2	27	71.8927
7^2	20	48.6300
8^2	18	43.7121
9^2	17	40.4255
11^2	15	36.2747
13^2	14	33.7937
16^2	13	31.5103
$17^2 \leq q \leq 19^2$	13	~ 30
$23^2 \leq q \leq 27^2$	12	~ 28
29^2	12	27.7441
$31^2 \leq q \leq 32^2$	11	~ 27
$37^2 \leq q \leq 49^2$	11	~ 26
$53^2 \leq q \leq 83^2$	11	~ 25

Table 2: Plus petites valeurs de $\alpha(q,t)$ pour q carré et petit

Cette construction explicite n'est cependant pas optimale, et en combinant les arguments de Randriambololona dans [58] avec de la concaténation, nous donnons des constructions explicites très courtes de codes intersectants, qui sont parfois plus courtes que la borne probabiliste.

Théorème. Les bornes suivantes, issues de constructions *explicites* (utilisant parfois de la concaténation), sont vérifiées:

- Si q est un carré et $q \geq 25$, alors

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq 2 + \frac{2}{\sqrt{q}-2};$$

- Si $q = p^{2m+1}$ est une puissance impaire d'un nombre premier (avec $m \geq 1$, c'est-à-dire que q n'est pas premier) et si $q \geq 32$, alors

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq \frac{4}{2 - \frac{1}{p^m-1} - \frac{1}{p^{m+1}-1}},$$

- Si q est un nombre premier vérifiant $q \geq 11$, alors

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq 3 + \frac{3}{q-2}.$$

Pour les valeurs restantes de q, les bornes sont indiquées dans le Tableau 3, avec les paramètres du code interne utilisé pour faire la concaténation avec des codes AG.

q	Paramètres du code interne	Borne supérieure pour $\limsup_{k\to\infty} i(k,q)/k$	Borne probabiliste
2	$[15,6]_2$	5.8334	4.8189
3	$[10,5]_3$	4.3561	3.7382
4	$[5,3]_4$	4.1667	3.3539
5	$[5,3]_5$	3.9025	3.1507
7	$[7,4]_7$	3.5745	2.9331
8	$[3,2]_8$	3.5	2.8666
9	$[3,2]_9$	3.4286	2.8148
16	$[3,2]_{16}$	3.2143	2.6266
27	$[3,2]_{27}$	3.12	2.5146

Table 3: Bornes supérieures obtenues avec des codes AG pour les valeurs exceptionnelles de q

Après ces études en termes de théorie des codes, nous passons à une étude dans le langage de la combinatoire additive et de la constante de Davenport.

Nous proposons une généralisation de la constante de Davenport qui permet de conserver le lien avec la théorie des codes pour tout q. Si le lien était simple quand $q = 2$, ce n'est pas le cas pour d'autres valeurs. Une première généralisation a été proposée dans [47], dans le cas particulier où q est premier. Nous introduisons un système d'endomorphismes, noté $\mathcal{Q}_h$, dont l'action sur C_p^{hr} correspond à l'action scalaire de $\mathbb{F}_q$ sur $\mathbb{F}_q^r$.

En notant $q = p^h$, nous notons D_2^h notre constante de Davenport d'ordre 2 généralisée. Nous montrons alors des théorèmes qui permettent de passer d'énoncés sur D_2^h à des énoncés sur $i(k,q)$.

Théorème. Soit $E_{p^{hr}}$ le groupe abélien élémentaire d'ordre p^{hr}, où p est premier et h, r sont des entiers positifs. Alors $\mathrm{D}_2^h(E_{p^{hr}})$ est le plus petit entier n tel que tous les $[n, n-r]_{p^h}$ codes ne sont pas intersectants. Par conséquent

$$\mathrm{D}_2^h(E_{p^{hr}}) = \min\{m \geq r+1 \mid m < i(m-r, p^h)\}.$$

Lemme. Soit $\alpha \leq \liminf_{k\to\infty} i(k,p^h)/k$, et $\beta \geq \limsup_{k\to\infty} i(k,p^h)/k$. Alors

$$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq \frac{\alpha}{\alpha - 1}$$

et

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq \frac{\beta}{\beta-1}.$$

Nous donnons une formulation équivalente sur D_2^h des bornes sur $i(k,q)$ présentées plus haut.

Puisque la constante de Davenport a un lien avec la théorie de la factorisation, nous donnons une interprétation de notre constante de Davenport généralisée dans le langage du groupe de classes d'un corps de nombres. La voici.

Théorème. Soit p un premier et $h, r \geq 0$ des entiers. Soit K un corps de nombres tel que $\mathrm{Cl}(\mathcal{O}_K) = E_{p^{hr}}$.

La petite constante pondérée de Davenport d'ordre 2, notée $\mathrm{d}_2^h(\mathrm{Cl}(\mathcal{O}_K))$, est le plus grand nombre $\ell \in \mathbb{N}$ tel qu'il existe ℓ idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ tels que tout produit

$$\prod_{i=1}^{\ell} \mathfrak{q}_i,$$

où $\mathfrak{q}_i$ est un idéal dans la classe de $\varphi_i([\mathfrak{p}_i])$, avec $\varphi_i \in \mathcal{Q}_h$, n'est pas divisible par le produit de deux idéaux principaux non triviaux.

Nous verrons enfin que l'action de $\mathcal{Q}_h$ peut être interprétée comme l'action du groupe de Galois sur le groupe de classes dans certains cas (par exemple quand $q-1$ est un nombre premier de Mersenne).

Codes intersectants en métrique rang

Après nous être intéressés aux codes intersectants en métrique de Hamming, nous nous demanderons ce qu'il en est en métrique rang.

L'objectif d'une étude des codes intersectants en métrique rang est de participer au développement de la théorie géométrique des q-systèmes, qui sont la contrepartie des codes non-dégénérés en métrique rang $\mathbb{F}_{q^m}$-linéaire.

Il doit être noté qu'il n'est pas clair de savoir quelle définition donner aux codes intersectants en métrique rang, étant donné que plusieurs définitions candidates sont *a priori* cohérentes. Nous choisissons de demander aux supports de deux mots de code non nuls d'avoir une intersection non triviale, en définissant le support d'un mot de code comme étant le rowspan d'une matrice représentative du mot de code dans n'importe quelle $\mathbb{F}_q$-base.

Avec cette définition, nous montrons un théorème de caractérisation géométrique. Un q-système 2-générable est un sous-espace $\mathbb{F}_q$-linéaire $\mathcal{U} \subset \mathbb{F}_{q^m}^k$ tel qu'il existe deux hyperplans $\mathcal{H}, \mathcal{H}'$ tels que

$$\mathcal{U} = \mathcal{H} \cap \mathcal{U} + \mathcal{H}' \cap \mathcal{U}.$$

On montre alors le théorème de caractérisation géométrique suivant.

Théorème. Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code non-dégénéré en métrique rang. Les assertions suivantes sont équivalentes.

1. Le code $\mathcal{C}$ est intersectant en métrique rang.
2. Pour tout $A \in GL(n,q)$, le code $\mathcal{C} \cdot A$ est intersectant en métrique de Hamming.
3. Pour tout $A \in GL(n,q)$, et pour tout $[n,k,d]_q$-système $\mathcal{S} \subset \mathrm{PG}(k-1,q^m)$ obtenu à partir des colonnes d'une matrice génératrice de $\mathcal{C} \cdot A$, l'ensemble $\mathcal{S}$ est N2C.
4. Le $[n,k,d]_{q^m/q}$-système $\mathcal{U}$ correspondant au code $\mathcal{C}$ n'est pas 2-générable.

L'étude des codes intersectants peut alors être menée avec les outils géométriques des q-systèmes. Nous montrons alors les théorèmes suivants.

Théorème. Soit $U \subset \mathbb{F}_{q^m}^k$ un q-système de rang n. Si $n \geq 2m-2$, alors U est 2-générable.

Théorème. Si $n \leq 2m-2k+1$, il existe un q-système $U \subset \mathbb{F}_{q^m}^k$ de rang n qui ne soit pas 2-générable.

Pour finir, nous concluons notre étude par un examen des q-systèmes de rang n avec $2m-2k+1 < n < 2m-2$ dans le cas particulier $k=3$.

Part I

Prérequis

Chapter 1

Théorie des codes

Elwood: It's 106 miles to Chicago, we've got a full tank of gas, half a pack of cigarettes, it's dark and we're wearing sunglasses.
Jake: Hit it.

- The Blues Brothers

L'objectif de ce chapitre introductif est de présenter la théorie des codes linéaires.

Les codes ont une importance cruciale dans le domaine de la transmission d'information. Ce domaine ne recouvre pas seulement l'ensemble des communications entre humains ou entre ordinateurs, mais aussi le stockage de données (qui peut être vu comme une communication depuis le passé à destination du futur).

En théorie de l'information, une communication est modélisée comme l'envoi d'un message constitué d'une suite de symboles, mettons $m = (m_1, \ldots, m_n)$, dans un *canal bruité*. Ce canal bruité modifie quelques symboles et produit en sortie un message alternatif $m' = (m'_1, \ldots, m'_n)$, en quelque sorte on peut dire que le canal a brouillé l'écoute. Le destinataire de la communication doit deviner m à partir de m'. Pour cela, il convient de choisir au préalable un message m contenant une certaine dose de *redondance* (que nous quantifierons avec précision plus bas). S'il y a assez de redondance, la donnée du message reçu m' doit permettre de retrouver m.

Nous invitons le lecteur intéressé à se référer à [38], qui donne une introduction bien plus approfondie que la courte présentation que nous donnons de la théorie des codes dans ce travail.

Il convient, pour commencer, de fixer quelques conventions d'écriture, que nous utiliserons dans toute la suite de notre exposé.

Dans toute la suite, q désigne une puissance d'un nombre premier. Pour tout tel q, il existe un unique corps fini à q éléments, que nous noterons $\mathbb{F}_q$.

1.1 Introduction à la métrique de Hamming

La métrique de Hamming est une métrique nommée d'après le mathématicien américain Richard Hamming. Comme nous allons le voir, elle est particulièrement adaptée aux problématiques de communication.

1.1.1 Les codes linéaires et la métrique de Hamming

Définition 1.1.1. Soit $x \in \mathbb{F}_q^n$ un vecteur. Son *support*, noté $\sigma(x)$, est

$$\sigma(x) = \{i \mid x_i \neq 0\}.$$

Définition 1.1.2. Soit $x \in \mathbb{F}_q^n$. Son *poids de Hamming* est

$$\mathrm{wt}(x) = |\sigma(x)|.$$

Le poids de Hamming induit une distance sur $\mathbb{F}_q^n$, appelée *distance de Hamming*:

$$d(x, y) = \mathrm{wt}(y - x).$$

Définition 1.1.3. La *boule de Hamming* de rayon r et de centre x_0 dans $\mathbb{F}_q^n$ est l'ensemble

$$B_H(x_0, r) = \{x \in \mathbb{F}_q^n \mid \mathrm{wt}(x - x_0) \leq r\}.$$

Le cardinal d'une boule de Hamming ne dépend pas de son centre.

Définition 1.1.4. Un code linéaire est un sous-espace vectoriel $\mathcal{C}$ de $\mathbb{F}_q^n$. Sa *dimension* est

$$k = \dim_{\mathbb{F}_q}(\mathcal{C}),$$

et sa *distance minimale* est

$$d = \min_{c,c' \in \mathcal{C}} \{d_H(c, c')\} = \min_{c \in \mathcal{C} \setminus \{0\}} \mathrm{wt}(c).$$

On dit qu'un tel code est un code de paramètres $[n, k, d]_q$, ou un $[n, k, d]_q$-code.

Remarque 1.1.5. Il existe également des codes *non-linéaires*, qui sont simplement des sous-ensembles de $\mathbb{F}_q^n$.

Les codes linéaires sont un cas particulier des *codes* en général. Dans toute cette thèse nous ne considérerons que des codes linéaires.

Définition 1.1.6. L'espace des matrices à k lignes et n colonnes et à coefficients dans un corps $\mathbb{K}$ est noté $\mathcal{M}_{k \times n}(\mathbb{K})$.

Définition 1.1.7. Soit $\mathcal{C}$ un $[n,k,d]_q$-code. Une *matrice génératrice* de $\mathcal{C}$ est une matrice $G \in \mathcal{M}_{k\times n}(\mathbb{F}_q)$ telle que $\mathcal{C} = \text{rowspan}(G)$:

$$\forall c \in \mathcal{C},\ \exists x \in \mathbb{F}_q^k, \quad c = x \cdot G.$$

Une *matrice de parité* de $\mathcal{C}$ est une matrice $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$ telle que $\mathcal{C} = \ker(H)$:

$$\forall x \in \mathbb{F}_q^n, \quad x \in \mathcal{C} \iff H^t x = 0.$$

Remarque 1.1.8. Un code linéaire n'a (sauf cas triviaux) pas de matrice génératrice et de matrice de parité uniques. D'autre part, en appliquant le pivot de Gauss, on peut écrire une matrice génératrice sous la forme

$$G = (I_k \mid A),$$

où $A \in \mathcal{M}_{k\times(n-k)}(\mathbb{F}_q)$.

Définition 1.1.9. Une isométrie de $\mathbb{F}_q^n$ est une application linéaire $\psi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ qui préserve la distance de Hamming:

$$\forall x \in \mathbb{F}_q^n, \quad \text{wt}(\psi(x)) = \text{wt}(x).$$

Définition 1.1.10. Deux $[n,k,d]_q$-codes $\mathcal{C}$ et $\mathcal{C}'$ sont dits *équivalents* s'il existe une isométrie $\psi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ telle que $\mathcal{C}' = \psi(\mathcal{C})$.

Deux codes équivalents ont les mêmes paramètres: si $\mathcal{C}$ est un $[n,k,d]_q$-code et si $\mathcal{C}' \sim C$, alors $\mathcal{C}'$ est aussi un $[n,k,d]_q$-code.

1.1.2 Communication et codes asymptotiquement bons

Définition 1.1.11. Soit $\mathcal{C}$ un code de paramètres $[n,k,d]_q$. Son *taux d'information* est la quantité $R = k/n$, et son *taux de correction* est $\delta = d/n$.

Remarque 1.1.12. Il est difficile de parler des codes correcteurs sans mentionner leur utilité pratique. Nous exposons ici très brièvement la manière principale dont ils sont employés.

Soit $\mathcal{C}$ un code de paramètres $[n,k,d]_q$. Notons $\tau = \lfloor \frac{d-1}{2} \rfloor$. Puisque la distance minimale de $\mathcal{C}$ est d, des boules de Hamming de rayon τ centrées en les mots de code de $\mathcal{C}$ ont intersection nulle.

Cela permet le protocole de communication qui suit. Deux interlocuteurs se mettent d'accord sur un code $\mathcal{C}$ ainsi que sur une manière de faire correspondre des messages potentiels à des mots de code. On envoie un mot de code c dans le canal bruité (décrit plus haut), qui renvoie un vecteur $x = c + e$, où e est un vecteur aléatoire. En supposant que le canal bruité ne fait pas plus de τ erreurs, i.e. si $\text{wt}(e) \leq \tau$, le vecteur reçu x est dans la boule de Hamming centrée en c. Pour retrouver c, il suffit donc simplement d'identifier de quelle boule il s'agit.

On comprend que si d est grand, alors le rayon de correction τ l'est également, et que beaucoup d'erreurs peuvent être corrigées. D'autre part, si le taux d'information R est grand, le nombre de symboles utiles dans le message transmis est élevé: il y a peu de redondance.

Dans l'idéal on veut que R soit élevé (pour que le message soit transmis le plus efficacement possible), et que δ soit élevé (pour corriger le plus d'erreurs possibles). Cependant, comme nous le verrons dans la section suivante, R et δ ne peuvent pas être tous les deux élevés.

Cette dernière observation motive la définition suivante.

Définition 1.1.13. Une famille de codes *asymptotiquement bons* est une famille de codes $\mathcal{F}$ qui contient une suite de codes $(C_s)_{s\in\mathbb{N}}$ de paramètres $[n_s, k_s, d_s]_q$ vérifiant

$$n_s \to \infty, \quad R_s \geq R > 0, \quad \delta_s \geq \delta > 0.$$

1.1.3 La concaténation

La concaténation est une méthode pour combiner des codes linéaires sur des corps différents.

Soit $\mathcal{I}$ un $[n, k, d]_q$-code et soit $\mathcal{O}$ un $[N, K, D]_{q^k}$-code. En remarquant que $\mathbb{F}_{q^k} \simeq \mathbb{F}_q^k$ et que le code $\mathcal{I}$ définit une injection naturelle de $\mathbb{F}_q^k$ dans $\mathbb{F}_q^n$, notons $\phi : \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ une injection dont l'image est $\mathcal{I}$. La concaténation de $\mathcal{I}$ et $\mathcal{O}$ est alors

$$\mathcal{I}\square_\phi\mathcal{O} := \{(\phi(c_1), \ldots, \phi(c_N)) \mid (c_1, \ldots, c_N) \in \mathcal{O}\}.$$

Le code $\mathcal{I}\square_\phi\mathcal{O}$ est un code sur $\mathbb{F}_q$, de longueur Nn et de dimension Kk. Sa distance minimale vérifie $d(\mathcal{I}\square_\phi\mathcal{O}) \geq Dd$.

Essentiellement, la concaténation consiste à considérer les coordonnées de $\mathcal{O}$, qui sont des éléments de $\mathbb{F}_{q^k}$, comme des vecteurs de $\mathbb{F}_q^k$, que l'on peut injecter dans $\mathbb{F}_q^n$ au moyen d'un autre code correcteur, sur $\mathbb{F}_q$. Du point de vue de la correction d'erreurs, on introduit de la redondance au niveau de chaque symbole.

1.2 Bornes classiques

Avant de développer les outils de la théorie des codes, il est judicieux de mentionner les q-analogues des coefficients binomiaux.

Proposition 1.2.1. Le nombre de sous-espaces de dimension k de $\mathbb{F}_q^n$ est

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Cette notion est le premier exemple de q-analogue, dont la définition, informelle, est la suivante : le q-analogue d'une notion de combinatoire sur un ensemble fini de cardinal n est la

notion de combinatoire correspondante pour un espace vectoriel de dimension n sur le corps fini $\mathbb{F}_q$. Souvent, en faisant tendre q vers 1 dans les formules, on retrouve la formule initiale pour la combinatoire sur l'ensemble fini (c'est par exemple le cas avec les q-analogues des coefficients binomiaux mentionnés plus haut).

Les q-analogues occuperont une place importante dans nos considérations en métrique rang.

1.2.1 Les boules de Hamming

Beaucoup des bornes utilisent des résultats classiques sur les boules de Hamming. Nous nous permettons donc de les rappeler.

Théorème 1.2.2. Le cardinal d'une boule de Hamming de rayon r dans $\mathbb{F}_q^n$ est

$$\mathrm{Vol}_q(r,n) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

On notera sans souci que le cardinal d'une boule de Hamming ne dépend pas de son centre.

Définition 1.2.3. L'entropie q-aire est la fonction $H_q(t) = -t \log_q(\frac{t}{q-1}) - (1-t)\log_q(1-t)$.

L'utilité principale de la fonction H_q réside dans la proposition suivante.

Proposition 1.2.4. Soit $0 \leq p \leq 1 - \frac{1}{q}$ et $n \in \mathbb{N}$ tel que $pn \in \mathbb{N}$. Alors

1. Soit $n \in \mathbb{N}$. Si $pn \in \mathbb{N}$, alors

$$\mathrm{Vol}_q(pn, n) \leq q^{n \cdot H_q(p)}.$$

2. Soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que si $n \geq N$ alors

$$\mathrm{Vol}_q(pn, n) \geq q^{n \cdot (H_q(p) - \varepsilon)}.$$

En somme, cette proposition affirme que le $q^{n \cdot H_q(p)}$ est une bonne approximation asymptotique de $\mathrm{Vol}_q(pn, n)$, le cardinal d'une boule de Hamming.

1.2.2 Bornes sur les paramètres d'un code linéaire

Théorème 1.2.5 (Borne de Singleton)**.** Soit $\mathcal{C}$ un code de paramètres $[n, k, d]_q$. Ses paramètres vérifient

$$k + d \leq n + 1.$$

Les codes dont les paramètres atteignent la borne de Singleton sont appelés *codes MDS* (pour "maximum distance separable"). Ces codes ont une interprétation remarquable en géométrie projective (comme nous allons le voir plus bas). Puisque ces codes sont optimaux du point de vue du taux d'information et du taux de correction, il sont d'un intérêt particulier pour les questions de communication.

L'une des familles de codes MDS les plus connues est celle des *codes de Reed-Solomon*, construits comme suit. On sélectionne n éléments différents $a_1, \ldots, a_n \in \mathbb{F}_q$. Le code de Reed-Solomon de longueur n et de dimension k est alors le code d'évaluation

$$RS_{n,k} = \{(f(a_1), \ldots, f(a_n)) \mid f \in \mathbb{F}_q[X], \deg(f) < k\}.$$

Proposition 1.2.6. La distance minimale du code $RS_{n,k}$ est $n - k + 1$.

Les codes de Reed-Solomon sont utiles mais présentent le désavantage d'imposer $n \leq q$ (il est possible de construire une version un peu plus générale qui ne nécessite que $n \leq q+1$, mais cette longueur reste bornée). En particulier, cela implique qu'il n'est pas possible d'utiliser seulement des codes de Reed-Solomon pour construire des codes asymptotiquement bons.

Théorème 1.2.7 (Borne de Plotkin)**.** Soit $\mathcal{C}$ un code de paramètres $[n, k, d]_q$. Ses paramètres vérifient

$$\delta = \frac{d}{n} \leq \frac{q^k - q^{k-1}}{q^k - 1}.$$

Théorème 1.2.8 (Borne de Hamming)**.** Soit $\mathcal{C}$ un $[n, k, d]_q$-code, et notons $t = \lfloor \frac{d-1}{2} \rfloor$. Alors

$$q^k \cdot |\mathrm{Vol}_q(t, n)| \leq q^n.$$

1.2.3 Bornes asymptotiques

Les bornes présentées à la section précédente ont des versions asymptotiques, i.e. lorsque la longueur n des codes considérés tend vers l'infini. Nous allons abondemment utiliser ces bornes asymptotiques dans les chapitres suivants dans le cas des codes minimaux et des codes intersectants.

Nous allons présenter ces bornes sous la forme de fonctions majorantes q-aires, définies comme suit.

Définition 1.2.9. Une fonction $f : [0, 1] \to [0, 1]$ est une fonction majorante q-aire si pour tout $0 \leq \delta \leq 1$, il n'existe aucune suite de codes de paramètres $[n_s, k_s, d_s]_q$ tels que $n_s \to \infty$, $\frac{d_s}{n_s} \to \delta$, et $\frac{k_s}{n_s} \to f(\delta)$.

Un exemple simple est celui de la borne de Singleton. En effet, si $k + d \leq n + 1$, alors $R + \delta \leq 1 + \frac{1}{n}$. On en déduit que R ne peut être supérieur (asymptotiquement, dans le sens exact défini plus haut) à $1-\delta$. Par conséquent, la borne de Singleton est associée naturellement à la fonction majorante q-aire $f(x) = 1 - x$.

Théorème 1.2.10 (Borne de Hamming asymptotique)**.** La fonction suivante est une fonction majorante q-aire:

$$f(\delta) = 1 - H_q(\delta/2).$$

Théorème 1.2.11 (Borne de Plotkin asymptotique)**.** La fonction suivante est une fonction majorante q-aire:

$$f(\delta) = 1 - \frac{q-1}{q}\delta.$$

Ces bornes sont relativement simples à établir à partir des bornes non-asymptotiques énoncées plus haut.

L'étude des schémas d'association (que nous n'aborderons pas dans cette thèse) conduit à la borne MRRW déduite du programme linéaire de Delsarte.

Théorème 1.2.12. La fonction suivante est une fonction majorante q-aire:

$$M_q(\delta) = H_q\left(\frac{1}{q}\left(q - 1 - (q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}\right)\right).$$

Cette borne a été montrée pour la première fois par McEliece, Rodemich, Rumsey, et Welch [50] (d'où son nom) dans le cas binaire, puis généralisée pour n'importe quelle valeur de q par Aaltonen [1].

Dans le cas où $q = 2$, c'est la meilleure fonction majorante binaire connue à ce jour.

On notera que toutes ces fonctions sont des bornes asymptotiques d'*inexistence*, i.e. aucune famille de codes ne peut avoir ses paramètres asymptotiques au-dessus du graphe de la fonction.

Gilbert et Varshamov ont établi indépendamment[1] une borne d'existence qui vient compléter notre compréhension des paramètres possibles d'un code.

Théorème 1.2.13. Soit $0 \leq \delta \leq 1 - \frac{1}{q}$, et $\varepsilon > 0$. Pour tout $R \geq 1 - H_q(\delta) - \varepsilon$, il existe une suite de codes de paramètres $[n_s, R \cdot n_s, \delta \cdot n_s]_q$ avec $n_s \to \infty$.

La borne de Gilbert-Varshamov correspond donc à la *fonction minorante q-aire* $f(x) = 1 - H_q(x)$, dans la mesure où pour tout couple $(\delta, R) \in [0,1]^2$ avec $R < f(\delta)$, il existe une

[1] Gilbert était un théoricien des codes américain, et Varshamov était soviétique. Gilbert a prouvé une version non-linéaire de la borne en 1952 et Varshamov a prouvé la version linéaire en 1957. Une des conséquences de la guerre froide a été de diviser la recherche selon les lignes politiques des deux "blocs". Pour ma part, je trouve qu'il est correct d'attribuer à la borne les deux noms.

famille de codes asymptotiquement bons dont les paramètres convergent vers (δ, R). Comme nous pouvons le voir dans le théorème suivant, un code linéaire sur $\mathbb{F}_q$ pris au hasard est proche de la borne de Gilbert-Varshamov avec forte probabilité. Dans cette mesure, la borne indique le comportement asymptotique des paramètres d'un code aléatoire.

Théorème 1.2.14. Soit $0 \leq \delta \leq 1 - \frac{1}{q}$, et soit $\varepsilon > 0$. Soit $\mathcal{C}$ un code sur $\mathbb{F}_q$ de longueur n et de dimension $k \leq n \cdot (1 - H_q(\delta) - \varepsilon)$. Alors

$$\mathbb{P}(d(\mathcal{C}) > n \cdot \delta) \geq 1 - q^{-\varepsilon n}.$$

Pour résumer la situation, une famille de codes est asymptotiquement bonne si elle contient une suite de codes de paramètres $[n_s, k_s, d_s]_q$ avec $n_s \to \infty$, $\frac{k_s}{n_s} \to R > 0$ et $\frac{d_s}{n_s} \to \delta > 0$. S'il est impossible d'atteindre les couples $(R, \delta) \in [0,1]^2$ tels que $R > f(\delta)$, où f est une fonction majorante q-aire, il est possible d'atteindre tous les paramètres (δ, R) vérifiant $R \leq g(\delta)$, où $g(x) = 1 - H_q(x)$ est la fonction correspondant à la borne de Gilbert-Varshamov. Qui plus est, un code aléatoire a des paramètres proches du graphe de g.

1.3 Les codes AG

1.3.1 Présentation

Définition 1.3.1. Une courbe X est une variété projective lisse de dimension 1.

Définition 1.3.2. Un *diviseur* est un élément du groupe abélien libre engendré par un nombre fini de points de la courbe, noté $\mathrm{Div}(X)$.

Tout diviseur est donc de la forme

$$D = \sum_P n_P P,$$

avec $n_P \in \mathbb{Z}$, et cette somme est finie. Le *support* d'un diviseur est l'ensemble des points P pour lesquels $n_P \neq 0$ (c'est donc un ensemble fini).

Définition 1.3.3. Un diviseur $D = \sum_P n_P P$ est *effectif* si $\forall P, \quad n_P \geq 0$.

Etant donnés deux diviseurs D_1 et D_2, on note $D_2 \geq D_1$ si $D_2 - D_1$ est effectif.

Définition 1.3.4. L'*espace de Riemann-Roch* associé à un diviseur $D \in \mathrm{Div}(X)$ est

$$\mathcal{L}(D) = \{f \in F^\times \mid div(f) \geq -D\} \cup \{0\},$$

où F est le corps de fonctions associé à la courbe X. C'est un espace vectoriel $\mathbb{F}_q$-linéaire, et on note sa dimension $\ell(D) = \dim_{\mathbb{F}_q} L(D)$.

Théorème 1.3.5. Soit X une courbe de genre g, et D un diviseur sur X. Alors

$$\ell(D) \geq \deg(D) + 1 - g.$$

De plus, si $\deg(D) \geq 2g - 2$, alors l'inégalité ci-dessus devient une égalité.

Définition 1.3.6. Soit $D \in \mathrm{Div}(X)$, et $G \in \mathrm{Div}(X)$ tel que les supports de D et G soient disjoints. Le code de Goppa généralisé $C(G, D)$ est l'image du morphisme

$$\begin{array}{rccc} \phi_{G,D}: & \mathcal{L}(D) & \longrightarrow & \mathbb{F}_q^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

Le noyau de $\phi_{G,D}$ est $\mathcal{L}(D - G)$. Par conséquent, si $\ell(D - G) = 0$, alors $\dim C(G, D) = \ell(D)$. Cela est par exemple le cas quand $\deg(D) < \deg(G)$.

1.3.2 Bornes sur les codes AG

Définition 1.3.7. Soit $\mathcal{C}$ un $[n, k, d]_q$-code. Son *défaut de Singleton* est

$$\Delta = 1 - \frac{k + d}{n + 1}.$$

Intuitivement, si $\Delta = 0$, alors le code est MDS, tandis que si Δ est proche de 1, le code a des paramètres *mauvais*.

Dans le même esprit que celui exposé en début de chapitre, il est clair qu'il est intéressant de construire des codes à faible défaut de Singleton.

Définition 1.3.8. La *constante d'Ihara* de $\mathbb{F}_q$ est

$$A(q) = \limsup_{g(X) \to \infty} \frac{n(X)}{g(X)},$$

où X parcourt l'ensemble des courbes sur $\mathbb{F}_q$, $n(X) = |X(\mathbb{F}_q)|$ est le nombre de points rationnels de X et $g(X)$ est le genre de X.

L'une des raisons de l'importance de la constante d'Ihara en théorie des codes est le théorème suivant. Pour une discussion plus approfondie sur les codes AG et la constante d'Ihara, nous invitons le lecteur à consulter [38, Chapitre 15].

Théorème 1.3.9. Soit $0 \leq R \leq 1$ et $0 \leq \delta \leq 1$ tels que $R + \delta = 1 - A(q)^{-1}$. Alors il existe une construction explicite de codes de paramètres $[n, R \cdot n, \delta \cdot n]_q$.

En d'autres termes, il est possible de construire des familles de codes asymptotiquement bons à condition que leur défaut de Singleton soit supérieur ou égal à $A(q)^{-1}$. On comprend

donc que dans l'objectif d'avoir des constructions explicites de codes avec les meilleurs paramètres possibles, on voudrait que la valeur de $A(q)$ soit grande.

Théorème 1.3.10 (Borne de Drinfeld-Vladut)**.**

$$A(q) \leq \sqrt{q} - 1.$$

Théorème 1.3.11. Si q est un carré, alors

$$A(q) = \sqrt{q} - 1.$$

Théorème 1.3.12 (Théorème 1.1., [15])**.** Si $q = p^{2m+1}$ alors

$$A(q) \geq 2 \cdot \left(\frac{1}{p^m - 1} + \frac{1}{p^{m+1} - 1} \right)^{-1}.$$

Quand q est un nombre premier, les bornes inférieures sur la constante d'Ihara ne sont pas assez bonnes pour construire des codes AG asymptotiquement bons, nous n'examinerons donc pas ce cas.

Les codes AG sont l'un des rares moyens disponibles dans la littérature pour construire explicitement des codes asymptotiquement bons. De ce fait, toutes les constructions explicites de codes asymptotiquement bons qui seront examinées dans cette thèse utiliseront des codes AG.

1.4 La métrique rang : Le cas $\mathbb{F}_{q^m}$-linéaire

Dans cette section, nous donnons une rapide présentation de la métrique rang et des codes dans cette métrique.

Le point de départ est de remarquer que le *rang* d'une matrice vérifie les axiomes classiques de norme, en particulier l'inégalité triangulaire

$$\mathrm{rk}(A + B) \leq \mathrm{rk}(A) + \mathrm{rk}(B).$$

On peut dès lors parler de la *métrique rang* sans abus de langage.

A partir de ce constat, il est possible de construire des codes en métrique rang de deux manières. La première est de considérer un sous-espace $\mathbb{F}_q$-linéaire de $\mathcal{M}_{m\times n}(\mathbb{F}_q)$, muni de la *métrique rang*. La deuxième est de considérer des codes sur $\mathbb{F}_{q^m}$, et c'est celle que nous allons développer dans toute la suite.

Considérons Γ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^m}$. Pour tout vecteur $x \in \mathbb{F}_{q^m}^n$, on peut écrire la matrice $\mathrm{Mat}_\Gamma(x) \in \mathcal{M}_{m\times n}(\mathbb{F}_q)$ représentant les coordonnées de x dans la base Γ.

Définition 1.4.1. Le rang de $x \in \mathbb{F}_{q^m}^n$ est le rang de la matrice $\mathrm{Mat}_\Gamma(x)$.

On notera que le rang de $\mathrm{Mat}_\Gamma(x)$ ne dépend pas de Γ. En effet, si Γ' est une autre $\mathbb{F}_q$-base de $\mathbb{F}_{q^m}$, alors $\mathrm{Mat}_{\Gamma'}(x) = A \cdot \mathrm{Mat}_\Gamma(x)$, où A est une matrice inversible, qui n'a donc aucun impact sur le rang.

Définition 1.4.2. Un code $\mathcal{C}$ en métrique rang est un sous-espace vectoriel de $\mathbb{F}_{q^m}^n$. Sa *longueur* est n, sa dimension est $k = \dim_{\mathbb{F}_{q^m}}(\mathcal{C})$ et sa distance minimale est $d(\mathcal{C}) = \min_{c \in \mathcal{C} \setminus \{0\}} \mathrm{rk}(c)$. On dit que $\mathcal{C}$ est un $[n, k, d]_{q^m/q}$-code.

Définition 1.4.3. Deux codes $\mathcal{C}$ et $\mathcal{C}'$ de longueur n sur $\mathbb{F}_{q^m}$ sont équivalents s'il existe une isométrie linéaire $\psi : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ (i.e. ψ préserve le rang) telle que $\mathcal{C}' = \psi(\mathcal{C})$.

De manière équivalente, $\mathcal{C}$ et $\mathcal{C}'$ sont équivalents s'il existe $A \in \mathrm{GL}(n, q)$ telle que

$$\mathcal{C}' = \mathcal{C} \cdot A = \{c \cdot A \mid c \in \mathcal{C}\}.$$

Comme en métrique de Hamming, deux codes équivalents en métrique rang ont nécessairement les mêmes paramètres.

La définition suivante n'est pas la définition classique, mais c'est la plus utile. Son équivalence avec la définiton classique est établie dans [5].

Définition 1.4.4. Soit $\mathcal{C}$ un code en métrique rang et soit G une matrice génératrice de $\mathcal{C}$. On dit que $\mathcal{C}$ est non-dégénéré si les colonnes de G sont $\mathbb{F}_q$-linéairement indépendantes.

Définition 1.4.5. Soit $x \in \mathbb{F}_{q^m}^n$. Son *support* (en métrique rang) est

$$\sigma(x) = \mathrm{rowspan}(\mathrm{Mat}_\Gamma(x)),$$

avec Γ une $\mathbb{F}_q$-base quelconque de $\mathbb{F}_{q^m}$.

Proposition 1.4.6. Soit Γ et Γ' deux $\mathbb{F}_q$-bases de $\mathbb{F}_{q^m}$. On a alors

$$\forall x \in \mathbb{F}_{q^m}^k, \quad \mathrm{rowspan}(\mathrm{Mat}_\Gamma(x)) = \mathrm{rowspan}(\mathrm{Mat}_{\Gamma'}(x)).$$

Preuve. Notons $B_\Gamma^{\Gamma'}$ la matrice de changement de base de Γ vers Γ', de sorte qu'on ait

$$\mathrm{Mat}_{\Gamma'}(x) = B_\Gamma^{\Gamma'} \cdot \mathrm{Mat}_\Gamma(x).$$

Puisque $B_\Gamma^{\Gamma'}$ est inversible, et agit à gauche sur $\mathrm{Mat}_\Gamma(x)$, on a bien

$$\mathrm{rowspan}(\mathrm{Mat}_{\Gamma'}(x)) = \mathrm{rowspan}(\mathrm{Mat}_\Gamma(x)).$$

□

Cette proposition justifie le fait de ne pas spécifier le choix de Γ dans la définition du support.

Proposition 1.4.7. Soit $x \in \mathbb{F}_{q^m}$. On a

$$\forall \lambda \in \mathbb{F}_{q^m} \setminus \{0\}, \quad \sigma(\lambda \cdot x) = \sigma(x).$$

Preuve. Cette proposition peut aisément se déduire de la précédente en voyant la multiplication par λ comme un endomorphisme inversible et $\mathbb{F}_q$-linéaire de $\mathbb{F}_{q^m}$, que l'on peut donc représenter par une matrice inversible. □

En général, il n'y aura pas de confusion sur le support en métrique de Hamming et le support en métrique rang car le contexte rendra clair que nous utilisons l'un ou l'autre, même s'ils se notent tous les deux σ. Dans les rares cas où il peut y avoir confusion, nous noterons σ_{rk} le support en métrique rang.

1.4.1 La borne de Singleton et les codes de Gabidulin

Les codes en métrique rang existent en deux "régimes". Le premier est celui où $n \leq m$, et où les codes de Gabidulin, l'analogue en métrique rang des codes de Reed-Solomon existent.

Nous commençons par donner un analogue de la borne de Singleton en métrique rang.

Proposition 1.4.8 (Borne de Singleton en métrique rang)**.** Soit $\mathcal{C}$ un $[n, k, d]_{q^m/q}$-code. Alors

$$km \leq \max(m, n) \cdot \min(n - d + 1, m - d + 1).$$

Les codes qui atteignent cette borne sont appelés *codes MRD* (maximum rank distance). Si l'étude des codes MRD en général constitue un domaine actif de recherche, les codes de Gabidulin en constituent un exemple simple à construire. Il s'agit du q-analogue des codes de Reed-Solomon présentés plus haut.

Nous commençons par définir les polynômes linéarisés.

Définition 1.4.9. Soit $P(X) = a_0 + a_1 X + \cdots + a_k X^k \in \mathbb{F}_{q^m}[X]$. Le *polynôme linéarisé* associé à P est l'application $\mathbb{F}_q$-linéaire $\tilde{P} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ définie par

$$\tilde{P}(X) = (P \circ \pi_q)(X) = a_0 + a_1 X^q + a_2 X^{q^2} + \cdots + a_k X^{q^k}.$$

Soit $n \leq m$, et soient $a_1, \ldots, a_n \in \mathbb{F}_{q^m}$ des éléments $\mathbb{F}_q$-linéairement indépendents. Le code de Gabidulin est

$$Gab_{n,k} = \{(\tilde{P}(a_1), \ldots, \tilde{P}(a_n)) \mid P \in \mathbb{F}_{q^m}[X], \deg(P) < k\}.$$

Notons qu'une matrice génératrice de $Gab_{n,k}$ est

$$G = \begin{pmatrix} a_1 & \dots & a_n \\ a_1^q & \dots & a_n^q \\ \vdots & \vdots & \vdots \\ a_1^{q^{k-1}} & \dots & a_n^{q^{k-1}} \end{pmatrix}.$$

Ce type de matrices s'appelle *matrice de Moore*, elle est de rang maximal si et seulement si $a_1, \dots, a_n$ sont $\mathbb{F}_q$-linéairement indépendants.

Le code de Gabidulin $Gab_{n,k}$ a pour paramètres $[n, k, n-k+1]_{q^m/q}$, c'est un code MRD.

1.5 Codes et géométrie projective

Dans cette section nous introduisons la méthode géométrique, qui sera le point de départ de notre recherche sur les codes minimaux et intersectants.

1.5.1 Codes projectifs

Définition 1.5.1. Soit $\mathcal{C}$ un $[n, k, d]_q$-code, et notons G une matrice génératrice de $\mathcal{C}$. Si toutes les colonnes de G sont non-nulles, alors le code $\mathcal{C}$ est un *code non-dégénéré*.

Le titre de cette section laisse bien entendu entendre que nous allons travailler dans l'espace projectif. Définissons-le.

Définition 1.5.2. Soit $\sim$ la relation d'équivalence sur $\mathbb{F}_q^k \setminus \{0\}$ définie par $x \sim y$ si x et y sont colinéaires. L'espace projectif est alors

$$\mathrm{PG}(k-1, q) = (\mathbb{F}_q^k \setminus \{0\}) / \sim .$$

Définition 1.5.3. L'image d'un hyperplan $\mathcal{H} \subset \mathbb{F}_q^k$ dans l'espace projectif est appelée *hyperplan projectif* (ou simplement hyperplan lorsque le contexte ne prête pas à confusion). Similairement, l'image d'un sous-espace $\mathcal{E} \subset \mathbb{F}_q^k$ de codimension s est appelée *sous-espace projectif* de codimension s.

Nous utiliserons également sporadiquement[2] l'espace affine, défini comme suit.

Définition 1.5.4. L'*espace affine* de dimension $k-1$ est

$$\mathrm{AG}(k-1, q) = \mathrm{PG}(k-1, q) \setminus \mathcal{H},$$

où $\mathcal{H}$ est n'importe quel hyperplan de $\mathrm{PG}(k-1, q)$.

[2] C'est-à-dire une seule fois.

Dans la suite, certaines de nos constructions explicites de codes utiliseront des ensembles de droites projectives (i.e. des sous-espaces projectifs de codimension $k-2$).

Définition 1.5.5. Soit $\mathcal{L}$ un ensemble de droites projectives de $\mathrm{PG}(k-1,q)$. On dit que $\mathcal{L}$ est un *ensemble de droites dispersées*[3] si pour tout sous-espace projectif $\mathcal{V} \subset \mathrm{PG}(k-1,q)$ de codimension 2, il existe $\ell \in \mathcal{L}$ telle que $\ell \cap \mathcal{V} = \varnothing$.

1.5.2 Le lien entre théorie des codes et géométrie projective

Prenons un code projectif $\mathcal{C}$ et notons G l'une de ses matrices génératrices. Puisque chaque colonne de G est non nulle, il est possible de lui associer le point de l'espace projectif qui correspond à sa classe d'équivalence. En faisant cela pour chaque colonne, on obtient une collection de points de l'espace projectif, avec possiblement des répétitions.

Puisqu'un point est répété dans l'espace projectif si et seulement si deux colonnes de G sont colinéaires, on peut imposer au code d'éviter cela.

Définition 1.5.6. Soit $\mathcal{C}$ un $[n,k,d]_q$-code, et G une matrice génératrice de $\mathcal{C}$. Si les colonnes de G ne sont pas colinéaires deux à deux, alors le code $\mathcal{C}$ est un code *projectif*.

Remarquons que cette définition est cohérente car elle ne dépend pas du choix de la matrice génératrice G. En effet, un code $\mathcal{C}$ n'est pas projectif s'il existe deux coordonnées i,j et un scalaire $\lambda \in \mathbb{F}_q$ tels que $\forall c \in \mathcal{C}, \quad c_i = \lambda \cdot c_j$, ce qui ne dépend pas de G.

Dans la suite, nous n'examinerons que le cas des codes projectifs (on notera sans peine que tous les codes projectifs sont des codes non dégénérés).

La proposition suivante relie les poids de Hamming des mots de code de $\mathcal{C}$ aux propriétés géométriques de l'ensemble projectif obtenu à partir d'une matrice génératrice.

Proposition 1.5.7. Soit $\mathcal{C}$ un code projectif, et soit $\mathcal{S}$ l'ensemble de points obtenu à partir d'une matrice génératrice G de $\mathcal{C}$. Tout mot de code $c \in \mathcal{C} \setminus \{0\}$ est de la forme $x \cdot G$, avec $x \in \mathbb{F}_q^k$. Notons $P_i \in \mathcal{S}$ le point obtenu à partir de la i-ème colonne de G. On a alors

$$P_i \in \langle x \rangle^\perp \iff c_i = 0,$$

et le poids de Hamming de c est donc

$$\mathrm{wt}(c) = |\{P \in \mathcal{S} \mid P \notin \langle x \rangle^\perp\}|.$$

[3] Encore une traduction littéraire plutôt que litérale. En effet, le terme anglais pour désigner ces ensembles de droites est "set of lines with avoidance property", que j'aurais volontiers traduit par "ensemble de droites avec propriété d'évitement" si ce n'était pas horriblement moche. Puisque ceci est ma thèse, j'appelle ces ensemble comme je veux et je choisis le terme "dispersées".

On peut affirmer qu'un hyperplan $\langle x\rangle^\perp$ correspond à $q-1$ mots de code (colinéaires). Les propriétés géométriques de $\mathcal{S}$ décrivent donc totalement les supports du code $\mathcal{C}$. Cette interprétation géométrique sera capitale pour notre étude de familles particulières de codes définies à partir de propriétés de leurs supports.

Proposition 1.5.8. Soit $\mathcal{C}$ un $[n,k,d]_q$-code projectif, et notons $\mathcal{S}$ l'ensemble de points associé à l'une des matrices génératrices de $\mathcal{C}$. Alors

$$d = \min_{\mathcal{H}} |\{P \notin \mathcal{H} \mid P \in \mathcal{S}\}|,$$

où le minimum est pris sur les hyperplans projectifs.

Cette proposition motive la définition d'un $[n,k,d]_q$-système projectif.

Définition 1.5.9. Un $[n,k,d]_q$-système projectif est un ensemble $\mathcal{S} \subset \mathrm{PG}(k-1,q)$ de cardinal $|\mathcal{S}|$ tel que

$$n-d = \max_{\mathcal{H}} |\{P \in \mathcal{H} \mid P \in \mathcal{S}\}|,$$

où le maximum est pris sur les hyperplans projectifs.

De la même manière que deux codes peuvent être équivalents, deux $[n,k,d]_q$-systèmes peuvent l'être aussi.

Définition 1.5.10. Pour $\phi \in GL(k,q)$ on note $\tilde{\phi}$ la bijection induite par ϕ sur $\mathrm{PG}(k-1,q)$. Soit $\mathcal{S} \subset \mathrm{PG}(k-1,q)$ et $\mathcal{S}' \subset \mathrm{PG}(k-1,q)$. On dit que $\mathcal{S}$ et $\mathcal{S}'$ sont *équivalents* s'il existe $\phi \in GL(k,q)$ tel que $\mathcal{S}' = \tilde{\phi}(\mathcal{S})$.

On notera tout naturellement que si $\mathcal{S} \sim \mathcal{S}'$ et si $\mathcal{S}$ est un $[n,k,d]_q$-système, alors $\mathcal{S}'$ est également un $[n,k,d]_q$-système.

On peut alors affirmer le théorème suivant.

Théorème 1.5.11 (Théorème 1.1.6., [67])**.** Il y a une bijection entre les classes d'équivalence de codes projectifs et les classes d'équivalences de $[n,k,d]_q$-systèmes.

1.5.3 Les q-systèmes et les ensembles linéaires

Les codes non-dégénérés en métrique rang possèdent des propriétés géométriques remarquables, que nous présentons ici.

Définition 1.5.12. Un $[n,k,d]_{q^m/q}$-système (ou q-système lorsque le contexte ne prête pas à confusion) est un sous-espace $\mathbb{F}_q$-linéaire $\mathcal{U} \subset \mathbb{F}_{q^m}^k$, tel que $\dim_{\mathbb{F}_q}(\mathcal{U}) = n$, $\langle \mathcal{U}\rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$, et

$$n-d = \max\{\dim_{\mathbb{F}_q}(\mathcal{H}\cap\mathcal{U}) \mid \mathcal{H} \text{ hyperplan } \mathbb{F}_{q^m}\text{-linéaire de } \mathbb{F}_{q^m}^k\}.$$

Notons $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code non-dégénéré en métrique rang, et G une matrice génératrice de $\mathcal{C}$. Notons $\mathcal{U} \subset \mathbb{F}_{q^m}^k$ l'espace vectoriel $\mathbb{F}_q$-linéaire engendré par les colonnes de G. Puisque $\mathcal{C}$ est non-dégénéré, $\dim_{\mathbb{F}_q}(\mathcal{U}) = n$. Comme montré dans [5], le poids d'un mot $c = x \cdot G$, avec $x \in \mathbb{F}_{q^m}^k$, est

$$\mathrm{rk}(c) = n - \dim_{\mathbb{F}_q}(\mathcal{U} \cap \langle x \rangle_{\mathbb{F}_{q^m}}^{\perp}).$$

L'espace $\mathcal{U}$ est donc bien un $[n,k,d]_{q^m/q}$-système.

L'étude des codes non-dégénérés en métrique rang $\mathbb{F}_{q^m}$-linéaire peut donc être conduite dans les termes de la géométrie des q-systèmes.

Définition 1.5.13. Soit U un $[n,k,d]_{q^m/q}$-système, et M un sous-espace $\mathbb{F}_{q^m}$-linéaire de $\mathbb{F}_{q^m}^k$. Le *poids* de M est

$$\mathrm{wt}_U(M) = \dim_{\mathbb{F}_q}(U \cap M) \leq \dim_{\mathbb{F}_q}(M).$$

Proposition 1.5.14. Soit U un $[n,k,d]_{q^m/q}$-système, et M un sous-espace $\mathbb{F}_{q^m}$-linéaire de $\mathbb{F}_{q^m}^k$ de codimension s. Alors

$$\mathrm{wt}_U(M) \geq n - sm.$$

Preuve. D'après la formule de Grassmann on a

$$\begin{aligned}
\mathrm{wt}_U(H) &= \dim_q(M \cap U) = \dim_q(M) + \dim_q(U) - \dim_q(M+U) \\
&\geq \dim_q(M) + \dim_q(U) - \dim_q(V) \\
&= m(k-s) + n - km \\
&= n - sm.
\end{aligned}$$

□

Définition 1.5.15. Soit $\mathcal{U}$ un $[n,k,d]_{q^m/q}$-système. On dit que $\mathcal{U}$ est h-éparpillé[4] si tout sous-espace $\mathbb{F}_{q^m}$-linéaire de $\mathbb{F}_{q^m}^k$ de dimension h a poids au plus h.

Les codes MRD non-dégénérés avec $n \leq m$ sont exactement ceux qui correspondent aux ensembles $k-1$-éparpillés (on dit aussi éparpillés par rapport aux hyperplans).

En métrique rang, les q-systèmes sont généralement suffisants dans le cadre de la recherche que nous développons dans cette thèse. Dans un intérêt culturel, il est toutefois important de mentionner l'existence des ensembles linéaires, introduits pour la première fois par Lunardon dans [45].

[4] Il s'agit de la première présentation de cette notion en français, j'ai donc choisi de traduire l'anglais "h-scattered" littéralement. Je trouve le terme "éparpillé" assez amusant mais très approprié dans ce contexte.

Définition 1.5.16. Soit $\mathcal{U}$ un $[n,k,d]_{q^m/q}$-système. L'ensemble linéaire qui lui est associé est

$$L_{\mathcal{U}} = \{\pi(x) \mid x \in \mathcal{U} \setminus \{0\}\} \subset \mathrm{PG}(k-1, q^m),$$

où π est la fonction qui à un vecteur non nul de $\mathbb{F}_{q^m}^k$ associe sa classe d'équivalence dans $\mathrm{PG}(k-1,q^m)$.

Proposition 1.5.17. Soit $\mathcal{U}$ un $[n,k,d]_{q^m/q}$-système et $L_{\mathcal{U}}$ l'ensemble linéaire associé. On a

$$|L_{\mathcal{U}}| \leq \frac{q^n - 1}{q-1}.$$

La théorie des ensembles linéaires est très riche et un sujet actif de recherche. Le lecteur intéressé pourra par exemple consulter les travaux [12,46,56,69] pour s'en rendre compte.

Chapter 2

Problèmes de suites à somme nulle et applications à la factorisation

Habe nun, ach! Philosophie,
Juristerei and Medizin,
Und leider auch Theologie
Durchaus studiert, mit heißem Bemühn.
Da steh' ich nun, ich armer Tor,
Und bin so klug als wie zuvor!

- Goethe, *Faust*

L'objectif de ce chapitre est d'introduire la constante de Davenport, ainsi que ses variantes et quelques autres problèmes mathématiques auxquels elle est naturellement reliée.

2.1 La constante de Davenport

Dans toute cette section, G désignera un groupe abélien fini quelconque et C_n désignera un groupe cyclique à n éléments. En règle générale, nous utiliserons la notation additive et noterons l'élément neutre 0_G, même si nous pourrons parfois utiliser la notation multiplicative quand c'est utile.

Une suite d'éléments de G est la donnée d'éléments $a_1, \ldots, a_s \in G$, possiblement avec des répétitions.

Une suite est dite *à somme nulle* si elle vérifie

$$\sum_{i=1}^{s} a_i = 0_G.$$

Une sous-suite de $a_1, \ldots, a_s$ est une suite de la forme $a_{i_1}, \ldots, a_{i_r} \in G$, tels que $1 \leq i_1 < \cdots < i_r \leq s$.

On notera en particulier que la sous-suite vide (i.e. avec $s = 0$) est une sous-suite à somme nulle.

Comme le montre la proposition suivante, si s est suffisamment grand, une suite admet nécessairement une sous-suite non vide à somme nulle.

Proposition 2.1.1. Soit G un groupe abélien fini. Soit $a_1, \ldots, a_s \in G$ une suite de G. Si $s \geq |G|$, alors la suite contient une sous-suite non vide à somme nulle.

Preuve. Considérons les sous-suites de la forme $u_0 = 0$, $u_1 = a_1$, $u_2 = a_1 + a_2$, etc. Si $u_i = u_j$, avec $i < j$, alors $u_j - u_i$ est une sous-suite non vide à somme nulle. Or, puisque $s + 1 > |G|$, et puisque les éléments u_i sont des éléments de G, d'après le principe des tiroirs, il existe deux tels indices i et j. □

Cette proposition justifie l'existence de la *constante de Davenport*, définie comme suit.

Définition 2.1.2. Soit G un groupe abélien fini. La *constante de Davenport* de G, notée $\mathrm{D}(G)$, est le plus petit entier ℓ vérifiant

$$\forall s \geq \ell,\ \forall a_1, \ldots, a_s \in G,\ \exists (\varepsilon_1, \ldots, \varepsilon_s) \in \{0;1\}^s \setminus \{0^s\},\quad \sum_{i=1}^{s} \varepsilon_i a_i = 0_G.$$

En d'autres termes, $\mathrm{D}(G)$ est le plus petit entier ℓ tel que toute suite de longueur ℓ doit avoir une sous-suite à somme nulle.

Remarque 2.1.3. Une définition équivalente de $\mathrm{D}(G)$ est la suivante: $\mathrm{D}(G)$ est *le plus grand* entier ℓ tel qu'il existe une suite *à somme nulle* de cardinal ℓ sans sous-suite propre à somme nulle.

Remarque 2.1.4. Dans la littérature, la constante de Davenport est quelquefois définie comme le plus grand entier ℓ tel qu'il existe une suite de longueur ℓ sans sous-suite à somme nulle.

Cette constante est notée $d(G)$, et on a bien évidemment

$$d(G) + 1 = \mathrm{D}(G).$$

On rappelle le théorème de structure des groupes abéliens fini, que nous utiliserons maintes fois dans toute la suite.

Théorème 2.1.5. Soit G un groupe abélien fini non trivial. Alors il existe des entiers $1 < n_1 \mid n_2 \mid \cdots \mid n_r$ tels que

$$G \simeq C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}.$$

Définition 2.1.6. Soit G un groupe abélien fini, de la forme

$$G \simeq C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}.$$

Le nombre n_r est appelé l'*exposant* de G, il est noté $\exp(G)$. C'est le plus grand ordre d'un élément de G. Le nombre r est appelé le *rang* de G.

On notera que le rang du groupe trivial est 0, et son exposant est 1.

Ce théorème permet de construire des suites sans sous-suite à somme nulle, de la manière suivante.

On commence par remarquer que la suite $g, \ldots, g$ contenant $n-1$ fois un générateur $g \in C_n$ n'a pas de sous-suite à somme nulle. Cela implique $d(C_n) \geq n-1$, donc $\mathrm{D}(C_n) \geq n$. Cependant, puisque $\mathrm{D}(C_n) \leq n$, on obtient $\mathrm{D}(C_n) = n$.

Pour le groupe $G = C_{n_1} \oplus C_{n_2}$, on peut prendre la suite composée de $n_1 - 1$ fois un élément g_1 d'ordre n_1 puis de $n_2 - 1$ fois un élément g_2 d'ordre n_2 tel que $G = \langle g_1 \rangle \oplus \langle g_2 \rangle$. Pour les mêmes raisons, elle n'a pas de sous-suite à somme nulle, et on obtient

$$\mathrm{D}(G) \geq n_1 + n_2 - 1.$$

En généralisant cette construction, on définit la quantité D^* comme suit.

Définition 2.1.7. Soit $G \simeq C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$ un groupe abélien fini.

$$\mathrm{D}^*(G) = 1 + \sum_{i=1}^{r} (n_i - 1).$$

De la discussion qui précède on déduit la proposition suivante.

Proposition 2.1.8. Soit G un groupe abélien fini.

$$\mathrm{D}(G) \geq \mathrm{D}^*(G).$$

Notons en particulier que le choix des coefficients $n_1, \ldots, n_r$ issu du théorème de structure est celui qui produit égalelent la constante D^* la plus grande : on pourrait tout à fait choisir d'autres décompositions $G \sim C_{n'_1} \oplus \cdots \oplus C_{n'_r}$, mais elles produiraient une valeur de D^* inférieure.

Cette proposition donne une première idée de la taille de $\mathrm{D}(G)$, mais pour être certain que l'ordre de grandeur est correct, il faut donner une borne supérieure. La voici.

Théorème 2.1.9. Soit G un groupe abélien fini. Notons $m = \exp(G)$. Alors

$$d(G) \leq m\left(1 + \ln \frac{|G|}{m}\right).$$

Cette borne supérieure ne diffère de la borne inférieure que d'un facteur environ égal à $\ln(m)$, ce qui indique que ces deux théorèmes donnent une idée à peu près exacte de l'ordre de grandeur de $\mathrm{D}(G)$.

Cette borne constitue la meilleure borne supérieure générale connue à ce jour (il y a bien évidemment de meilleures bornes pour des cas particuliers). Il n'est pas évident de déterminer comment l'améliorer. Nous avons consacré notre stage de master à différentes idées d'amélioration, toutes infructueuses.

2.2 Les bornes d'Olson

Dans cette section nous examinons les cas où la borne inférieure $\mathrm{D}^*(G)$ est égale à $\mathrm{D}(G)$. Les deux résultats exposés ici sont dûs à Olson [54,55].

Définition 2.2.1. Un p-groupe est un groupe fini G dont l'ordre est de la forme $|G| = p^r$, où p est un nombre premier.

Théorème 2.2.2. Soit G un groupe abélien fini. Si G est un p-groupe, alors

$$\mathrm{D}(G) = \mathrm{D}^*(G).$$

Preuve. Pour faciliter la preuve nous allons noter le groupe $G \simeq \prod_{i=1}^{r} C_{p^{\alpha_i}}$ multiplicativement.

Nous allons montrer que pour toute suite $g_1, \ldots, g_k \in G$ avec $k \geq 1 + \sum_{i=1}^{r}(p^{\alpha_i} - 1)$, on a l'égalité suivante dans l'anneau $\mathbb{Z}[G]$:

$$\prod_{i=1}^{k}(1 - g_i) = 0 \pmod{p} \tag{2.1}$$

Pour $g \in G$ examinons les sous-suites de $g_1, \ldots, g_k$ dont le produit vaut g, notons $E(g)$ le nombre de ces sous-suites de longueur paire et $O(g)$ le nombre de sous-suites de longueur impaire. 2.1 implique alors que $E(g) - O(g) = 0 \pmod{p}$ si $g \neq 1$ et $E(1) - O(1) = -1 \pmod{p}$, ce qui montre en particulier que $O(1) = E(1) = 0$ est impossible et implique donc l'existence d'une sous-suite de produit nul.

Montrons donc 2.1. Notons $x_1, \ldots, x_r$ une "base" de G, où $\mathrm{ord}(x_i) = p^{\alpha_i}$. Si $g_l \in G$ se décompose en $g_l = uv$ en utilisant l'égalité $1 - g_l = 1 - uv = (1 - u) + u(1 - v)$ on peut écrire

:

$$\prod_{i=1}^{k}(1-g_i) = (1-g_1)\dots(1-g_{l-1})(1-u)(1-g_{l+1})\dots(1-g_k)$$
$$+ u(1-g_1)\dots(1-g_{l-1})(1-v)(1-g_{l+1})\dots(1-g_k)$$

En répétant cette opération on obtient, en décomposant tous les g_i en produits d'éléments de notre base $(x_i)_i$:

$$\sum_{\sigma} a_\sigma J_\sigma = 0 \pmod p$$

où les a_σ sont des éléments de G, et les J_σ sont tous des produits de la forme

$$J_\sigma = (1-x_1)^{f_1}\dots(1-x_r)^{f_r},$$

où les f_i dépendent de σ et vérifient $\sum_{i=1}^{r} f_i = k$.

Puisque $k > \sum_{i=1}^{r}(p^{\alpha_i}-1)$ il existe un indice i pour lequel $f_i \geq p^{\alpha_i}$. Pour cet indice i on a alors $(1-x_i)^{p^{\alpha_i}} = 0 \pmod p$, car $x_i^{p^{\alpha_i}} = 1$ et les autres coefficients binomiaux sont divisibles par p. On en déduit finalement $(1-x_i)^{f_i} = 0 \pmod p$, et donc $J_\sigma = 0 \pmod p$ pour tout σ, donc enfin 2.1 et le théorème. □

Théorème 2.2.3. Soit $G = H \times K$ un groupe abélien, où $h = |H|$ divise $k = |K|$. Alors $D(G) \leq h + k - 1$.

Pour prouver ce théorème nous avons besoin d'un petit lemme.

Lemme 2.2.4. Soit p un nombre premier. Une suite $a_1, \dots, a_s$ de $C_p \times C_p$ de longueur $s \geq 3p-2$ admet une sous-suite de somme nulle de longueur au plus p.

Preuve. Notons pour commencer que $\mathrm{D}(C_p^2) = 2p-1$ et $\mathrm{D}(C_p^3) = 3p-2$ (cela découle du résultat sur les p-groupes). Plongeons C_p^2 dans C_p^3 et prenons $x \in C_p^3 \setminus C_p^2$. La suite $xa_1, \dots, xa_s$ est de longueur $3p-2$ et possède donc une sous-suite de somme nulle, qui est donc de longueur p ou $2p$, pour annuler x.

Si la longueur est p alors nous avons fini. Si la longueur est $2p$, notons sans perte de généralité cette sous-suite $a_1, \dots, a_{2p}$. On utilise alors $\mathrm{D}(C_p^2) = 2p-1$ pour garantir l'existence d'une sous-suite de somme nulle strictement plus petite dans C_p^2. Il suffit alors de considérer soit cette suite soit sa complémentaire pour obtenir une sous-suite de somme nulle, car $a_1 + \dots + a_{2p} = 0$. □

Nous sommes à présent en mesure de prouver le théorème.

Preuve. Nous allons faire une récurrence sur h. Si $h = 1$ la Proposition 2.11 donne la borne voulue.

Supposons donc $h > 1$, et notons p un nombre premier divisant h (et donc k). Notons H_1 et K_1 des sous-groupes de respectivement H et K, tous les deux d'indice p. Notons également $h_1 = |H_1|$ et $k_1 = |K_1|$ (donc $h = ph_1$ et $k = pk_1$).

Posons $Q = H_1 \times K_1$. Le théorème est vrai pour Q par hypothèse de récurrence, et $G/Q \simeq C_p^2$. Soit $a_1, \ldots, a_s$ une suite de G avec $s \geq h + k - 1 = p(h_1 + k_1 - 2) + 2p - 1$.

Le lemme garantit l'existence d'une sous-suite de longueur au plus p dont la somme est dans Q, notons S_1 l'ensemble de ses indices. En itérant ce processus on obtient des ensembles disjoints d'indices $S_1, \ldots, S_u$, tous de cardinal au plus p.

En posant $u_j = \sum_{i \in S_j} a_i$ on a $u_j \in S_j$. Cela peut être fait tant qu'il reste au moins $3p-2$ indices, c'est-à-dire au moins $l = h_1 + k_1 - 2$ fois : chaque étape élimine au plus p indices, mais après $h_1 + k_1 - 3$ fois, il en reste au moins $3p - 1 > 3p - 2$.

Il reste donc $2p - 1$ éléments dans la suite des a_i. Puisque $\mathrm{D}(C_p^2) = 2p - 1$, ces éléments admettent une sous-suite de somme nulle :

$$u_{l+1} = \sum_{i \in S_{l+1}} a_i \in Q.$$

Puisque $l + 1 = \mathrm{D}(Q)$, une sous-suite de $u_1, \ldots, u_{l+1}$ est à somme nulle, ce qui donne une sous-suite de $a_1, \ldots, a_s$ à somme nulle. □

Pour le cas des groupes de rang $r = 3$, savoir si $\mathrm{D}^*(G)$ est toujours égal à $\mathrm{D}(G)$ est un problème ouvert, voir [32].

Dans le cas où $r \geq 4$, il existe un nombre infini de groupes qui ne vérifient pas $\mathrm{D}^*(G) = \mathrm{D}(G)$, comme établi dans [34].

2.3 Les généralisations de la constante de Davenport

Il existe plusieurs généralisations de la constante de Davenport.

L'une des manières de généraliser cette constante est d'introduire un système de *poids*, de la manière suivante. On définit un ensemble de poids $A \subset \{1, \ldots, \exp(G) - 1\}$ et on dit qu'une suite $a_1, \ldots, a_s$ a une sous-suite à somme nulle s'il existe une sous-suite $a_{i_1}, \ldots, a_{i_r}$ telle que

$$\exists (\varepsilon_1, \ldots, \varepsilon_r) \in A^r, \quad \sum_{j=1}^{r} \varepsilon_i a_{i_j} = 0_G.$$

Etant donné un groupe abélien fini G et un ensemble de poids A, la constante de Davenport pondérée, notée $\mathrm{D}^A(G)$ est alors le plus petit entier $\ell > 0$ tel que toute suite de ℓ éléments de G a une sous-suite à somme nulle (pondérée).

En prenant $A = \{1\}$, on retrouve la définition classique de la constante de Davenport.

Divers auteurs ont étudié des cas particuliers, par exemple $A = \{1, -1\}$ [48] ou $A = \{1, \ldots, \exp(G) - 1\}$ [47]. Dans ce dernier cas, on parle de constante de Davenport avec poids maximaux.

Une autre généralisation concerne les constantes de Davenport multiples.

Définition 2.3.1. Soit G un groupe abélien fini, et soit $a_1, \ldots, a_s \in G$ une suite. Deux sous-suites $a_{i_1}, \ldots, a_{i_r}$ et $a_{j_1}, \ldots, a_{j_t}$ sont *disjointes* si les ensembles $I = \{i_1, \ldots, i_r\}$ et $J = \{j_1, \ldots, j_t\}$ sont disjoints.

Définition 2.3.2. Soit G un groupe abélien fini, et soit j un entier. La constante de Davenport d'ordre j, notée $\mathrm{D}_j(G)$, est le plus petit entier ℓ tel que toute suite de longueur ℓ admet j sous-suites à somme nulle *disjointes*.

On note bien évidemment que $\mathrm{D}_1(G) = \mathrm{D}(G)$.

A première vue, il n'est pas très facile de cerner l'ordre de grandeur de $\mathrm{D}_j(G)$. La proposition suivante est particulièrement utile à cet égard.

Proposition 2.3.3.

$$\mathrm{D}(G) \leq \mathrm{D}_j(G) \leq j \cdot \mathrm{D}(G).$$

Preuve. Tout d'abord, on a bien $\mathrm{D}(G) \leq \mathrm{D}_j(G)$ comme conséquence directe de la définition de D_j : s'il y a $j \geq 1$ sous-suites à somme nulle disjointes, il y en a bien une.

D'autre part, une suite de longueur $j \cdot \mathrm{D}(G)$ doit avoir une sous-suite à somme nulle sur les $\mathrm{D}(G)$ premiers indices, puis une autre sur les $\mathrm{D}(G)$ suivants, et ainsi de suite. Puisque toutes ces suites sont disjointes, on obtient bien j sous-suites à somme nulles disjointes. □

Intuitivement, on s'attend plutôt à avoir $\frac{\mathrm{D}_j(G)}{\mathrm{D}(G)} \sim j$ (voire un peu moins). Nous aurons l'occasion de voir à quel point cette intuition est vérifiée dans le chapitre sur les codes intersectants.

2.4 Anneaux de Dedekind et groupes de classes

La constante de Davenport d'un groupe de classes d'un anneau de Dedekind a une signification arithmétique. Dans cette section, nous commençons par introduire le groupe de classes.

Nous passerons assez rapidement sur les concepts généraux, une introduction plus détaillée (avec des preuves) peut être consultée dans l'ouvrage classique de Neukirch [53].

2.4.1 Une présentation des anneaux de Dedekind

Définition 2.4.1. Un anneau A est un anneau de Dedekind s'il vérifie (toutes) les conditions suivantes:

- A est intègre;
- A est intégralement clos;
- A est noethérien;
- $\mathrm{Spec}(A) = \mathrm{Spm}(A)$, où $\mathrm{Spec}(A)$ désigne l'ensemble des idéaux premiers de A, et où $\mathrm{Spm}(A)$ désigne l'ensemble des idéaux maximaux.

Définition 2.4.2. Un idéal fractionnaire de A est une partie de $K = Frac(A)$ de la forme $d^{-1} \cdot \mathcal{I}$, où $\mathcal{I}$ est un idéal de A.

On remarque aisément que la multiplication d'idéaux de A peut être étendue aux les idéaux fractionnaires: si $I = a^{-1}\mathcal{I}$ et $J = b^{-1}\mathcal{J}$ sont des idéaux fractionnaires, alors leur produit

$$I \cdot J = (ab)^{-1}\mathcal{I}\mathcal{J}$$

l'est aussi.

On définit donc naturellement la notion d'idéal fractionnaire inversible.

Définition 2.4.3. Soit A un anneau et I un idéal fractionnaire de A. Cet idéal est *inversible* s'il existe un idéal fractionnaire J tel que $I \cdot J = A$.

On note également que l'inverse d'un idéal fractionnaire (quand il existe) est unique.

Les anneaux de Dedekind vérifient de nombreuses propriétés en lien avec la factorisation, nous présentons ici les plus importantes.

Proposition 2.4.4. Soit A un anneau de Dedekind. Tout idéal fractionnaire de A est inversible. L'ensemble des idéaux fractionnaires forme donc un groupe multiplicatif.

Proposition 2.4.5. Soit A un anneau de Dedekind. Tout idéal $\mathcal{I}$ de A peut s'exprimer de manière unique (à l'ordre des facteurs près) comme un produit d'idéaux premiers de A, à savoir

$$\mathcal{I} = \prod_{i=1}^{n} P_i^{\alpha_i}.$$

Définition 2.4.6. Soit A un anneau de Dedekind et $P \in \mathrm{Spm}(A)$. La *valuation* en P est l'application v_P qui associe à tout idéal $\mathcal{I} \subset A$ le nombre de fois que P apparaît dans la décomposition (unique) de $\mathcal{I}$ en produit d'idéaux premiers.

2.4.2 Les corps de nombres

Jusqu'ici, la Définition 2.4.1 a l'air assez anodine, mais elle permet en fait de retrouver une théorie de la factorisation dans certains anneaux. Cette réalisation est d'importance majeure pour l'étude de l'arithmétique dans l'anneau des entiers d'un corps de nombres.

Rappelons pour commencer quelques notions élémentaires de théorie algébrique des nombres.

Définition 2.4.7. Un *corps de nombres* est une extension algébrique de $\mathbb{Q}$.

Théorème 2.4.8 (Théorème de l'élément primitif)**.** Tout corps de nombres est de la forme $K = \mathbb{Q}(\alpha)$, où $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$.

Définition 2.4.9. L'anneau des entiers d'un corps de nombres K est l'ensemble $\mathcal{O}_K$ des éléments de K qui sont racines d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.

L'anneau $\mathcal{O}_K$ peut ne pas être factoriel. Par exemple, si $K = \mathbb{Q}(i\sqrt{5})$, alors l'anneau des entiers est $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$, qui n'est pas factoriel. En effet, on a

$$6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}).$$

Heureusement, cela ne signifie pas qu'il faut abandonner tout espoir de développer une théorie de la factorisation dans les anneaux d'entiers d'un corps de nombres.

Théorème 2.4.10. Soit K un corps de nombres. Son anneau d'entiers $\mathcal{O}_K$ est un anneau de Dedekind.

Cela signifie que nous pouvons utiliser la théorie de factorisation des anneaux de Dedekind pour les corps de nombres.

2.4.3 Idéaux principaux et groupe de classe

Soit K un corps de nombres. On a vu que son anneau d'entiers $\mathcal{O}_K$ n'est pas factoriel en général. Cela implique que $\mathcal{O}_K$ n'est pas principal: en effet, tout anneau principal est factoriel. Pour les anneaux de Dedekind, la réciproque est vraie également : un anneau de Dedekind est principal si et seulement s'il est factoriel.

On note $\mathrm{Frac}(\mathcal{O}_K)$ l'ensemble des idéaux fractionnaires de $\mathcal{O}_K$. Muni de la structure multiplicative définie dans la sous-section précédente, $\mathrm{Frac}(\mathcal{O}_K)$ admet une structure de groupe. De même on note $\mathrm{Prin}(\mathcal{O}_K)$ le sous-groupe des idéaux fractionnaires principaux.

Définition 2.4.11. Le *groupe de classes* d'un anneau de Dedekind D est

$$\mathrm{Cl(D)} = \mathrm{Frac(D)}/\mathrm{Prin(D)}.$$

Proposition 2.4.12. Le groupe de classes de l'anneau des entiers d'un corps de nombres est un groupe abélien fini.

On remarquera aisément que $\mathrm{Cl}(\mathcal{O}_K)$ est le groupe trivial si et seulement si $\mathcal{O}_K$ est principal et donc factoriel. De ce point de vue, l'étude du groupe de classes permet de déterminer *de quelle manière* (et à quel point) la décomposition en facteurs premiers dans $\mathcal{O}_K$ n'est pas vérifiée.

2.4.4 Les applications de la constante de Davenport au groupe de classes

Nous allons voir à présent que le groupe de classes et la constante de Davenport sont intimement liés.

Nous commençons par noter qu'il est bien établi que pour chaque classe du groupe de classes d'idéaux $\mathrm{Cl}(\mathcal{O}_K)$, il existe un idéal premier $\mathfrak{p} \subset \mathcal{O}_K$ qui soit dans cette classe[1].

La motivation originale derrière l'étude de la constante de Davenport est précisément son lien avec la factorisation (voir par exemple [54]).

Lemme 2.4.13. La constante de Davenport $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre d'idéaux premiers (comptés avec multiplicités) apparaissant dans la factorisation d'un idéal engendré par un élément irréductible $x \in \mathcal{O}_K$. De manière équivalente, la petite constante de Davenport $\mathrm{d}(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre d'idéaux premiers tels que leur produit n'est pas divisible par un idéal principal non trivial.

Preuve. Soit $(x) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ la factorisation unique (x) en produit d'idéaux premiers. L'image de cette factorisation dans $\mathrm{Cl}(\mathcal{O}_K)$ (que nous notons ici de manière additive) est une identité de la forme

$$0_{\mathrm{Cl}(\mathcal{O}_K)} = [\mathfrak{p}_1] + \cdots + [\mathfrak{p}_n]$$

car (x) est un idéal principal. Notons que l'identité ci-dessus signifie que $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_n]$ est une suite à somme nulle de $\mathrm{Cl}(\mathcal{O}_K)$. Si cette suite à somme nulle peut être décomposée en 2 sous-suites à somme nulle disjointes, alors (x) est le produit de 2 idéaux premiers non triviaux, ce qui signifique que x ne peut pas être irréductible. Par conséquent la suite à somme nulle a longueur au plus $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$.

Réciproquement, considérons une suite à somme nulle dans $\mathrm{Cl}(\mathcal{O}_K)$ de longueur $n = \mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$ qui n'a pas 2 sous-suites disjointes à somme nulle une telle suite doit exister d'après la définition de la constante de Davenport). Une telle suite est de la forme

$$0_{\mathrm{Cl}(\mathcal{O}_K)} = [\mathfrak{a}_1] + \cdots + [\mathfrak{a}_n].$$

Chaque classe de $\mathrm{Cl}(\mathcal{O}_K)$ est représentée par un idéal premier de $\mathcal{O}_K$. Chaque $[\mathfrak{a}_n]$ peut donc être représenté par un idéal premier, mettons $\mathfrak{p}_i$. Soit $x \in \mathcal{O}_K$ un générateur de l'idéal principal $\prod_{i=1}^{n} \mathfrak{p}_i$. Puisqu'il n'y a pas 2 sous-suites à somme nulle disjointes, x doit être irréductible, et sa factorisation unique en idéaux premiers a longueur exactement $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$.

Par conséquent, $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$ est bien le plus grand nombre d'idéaux premiers apparaissant dans la factorisation d'un idéal engendré par un élément irréductible, ce qui termine la preuve. □

[1] A ma connaissance, la manière la plus simple d'établir ce résultat est d'utiliser le théorème de Chebotarev et la théorie du corps de classes. Développer tout cet arsenal théorique ici serait excessif par rapport à l'usage que nous en ferons par la suite, nous utiliserons donc ces résultats sans les examiner en détail.

2.5 Quelques bases sur les extensions de corps

Dans cette section nous prenons K une extension galoisienne de $\mathbb{Q}$, de groupe de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ et de degré $n = |G|$. Etant donné un premier $p \in \mathbb{Z}$, on souhaite décomposer l'idéal $(p) = p\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$:

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}.$$

Le lemme des restes chinois donne

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}\mathcal{O}_K.$$

Les indices e_i sont appelés *indices de ramification*. Puisque chaque idéal premier $\mathfrak{p}_i$ est maximal dans $\mathcal{O}_K$ (car $\mathcal{O}_K$ est un anneau de Dedekind), $\mathcal{O}_K/\mathfrak{p}_i\mathcal{O}_K$ est un corps (que l'on appelle *corps résiduel*). Le corps $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$ admet une injection naturelle dans $\mathcal{O}_K/\mathfrak{p}_i\mathcal{O}_K$, qui a donc une structure de $\mathbb{F}_p$-espace vectoriel. On note $f_i = [\mathcal{O}_K/\mathfrak{p}_i\mathcal{O}_K : \mathbb{Z}/p\mathbb{Z}]$ la dimension de cette extension, et on l'appelle *degré d'inertie*.

On a alors en général, quand l'extension est séparable, l'identité suivante:

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i.$$

Dans notre cas particulier cependant, les extensions que nous examinerons seront galoisiennes!

Le groupe de Galois G agit transitivement sur les idéaux $\mathfrak{p}_i$. Par conséquent, tous les e_i sont égaux. On note e cette valeur commune. De même, le groupe de Galois induit un isomorphisme entre les corps résiduels $\mathcal{O}_K/\mathfrak{p}_i\mathcal{O}_K$, qui ont donc tous le même degré d'inertie, que nous notons désormais f. On obtient donc

$$n = [K : \mathbb{Q}] = efg.$$

Définition 2.5.1. Si $e = f = 1$, on dit que p est *totalement décomposé*. Si $e = g = 1$, on dit que p est *inerte*. Enfin, si $f = g = 1$, on dit que p est *totalement ramifié*.

On rappelle un autre résultat qui est d'importance culturelle pour la théorie de la factorisation des idéaux dans les anneaux d'entiers.

Proposition 2.5.2. Pour une extension $K/\mathbb{Q}$ algébrique, il n'y a qu'un nombre fini de nombres premiers $p \in \mathbb{Z}$ qui sont ramifiés, c'est-à-dire tel que $\exists 1 \leq i \leq g, \quad e_i > 1$.

Remarque 2.5.3. Notons que la théorie de la ramification ne considère pas seulement des extensions de $\mathbb{Q}$, mais bel et bien le cas général d'un corps de nombres K et d'une extension

L/K:

$$\begin{array}{ccc} \mathcal{O}_K & \hookrightarrow & \mathcal{O}_L \\ \downarrow & & \downarrow \\ K & \hookrightarrow & L \end{array}$$

Dans cette thèse, nous ne nous arrêterons que sur le cas simple d'une extension $K/\mathbb{Q}$, qui suffit amplement pour développer nos exemples.[2]

[2]Cette remarque n'est en aucun cas motivée par le souhait de montrer que je sais faire un diagramme commutatif en LaTeX.

Part II

Résultats principaux

Chapter 3

Codes minimaux et ensembles générateurs d'hyperplans

Verse-nous ton poison pour qu'il nous réconforte !
Nous voulons, tant ce feu nous brûle le cerveau,
Plonger au fond du gouffre, Enfer ou Ciel, qu'importe ?
Au fond de l'Inconnu pour trouver du nouveau !

- Charles Baudelaire, *Les fleurs du mal*

Dans ce chapitre, nous utilisons les techniques géométriques exposées au premier chapitre dans le cas particulier des codes minimaux. Nous verrons qu'ils correspondent à un objet géométrique particulier: les *ensembles générateurs d'hyperplans.*[1]

3.1 Une définition abstraite des codes minimaux

Définition 3.1.1. Soit P un ensemble à ordre partiel. Un *support* est une application $\sigma : \mathbb{F}_q^n \to P$ vérifiant

$$\forall x \in \mathbb{F}_q^n \quad \forall \lambda \in \mathbb{F}_q^\times \quad \sigma(\lambda \cdot x) = \sigma(x),$$

[1] Les ensembles générateurs d'hyperplans ont été définis pour la première fois en 2011, sous le nom de *strong blocking sets*, et ont été étudiés par d'autres auteurs sous les noms *cutting blocking set* et *hyperplane generating set*. Cette thèse est à ma connaissance le premier travail en français sur ce sujet, je dois donc donner une bonne traduction française à cet objet. J'ai choisi *ensemble générateur d'hyperplans*, qui correspond le mieux à ma propre représentation mentale et qui est assez naturel à prononcer en français.

et

$$\forall x \in \mathbb{F}_q^n \quad \sigma(0) \leq \sigma(x).$$

Cette définition se veut aussi générale que possible, et permet de définir les codes minimaux d'une manière très générale.

Définition 3.1.2. Soit $\mathcal{C} \subset \mathbb{F}_q^n$ un code. Un mot de code $c \in \mathcal{C}$ est *minimal* par rapport à σ si

$$\forall c' \in \mathcal{C} \setminus \{0\}, \quad \sigma(c') \subsetneq \sigma(c).$$

Le code $\mathcal{C}$ est *minimal* par rapport à σ si tout mot de code non nul $c \in \mathcal{C} \setminus \{0\}$ est minimal par rapport à σ.

De manière équivalente, un code minimal est un code dont l'ensemble des supports de mots de code forme une *antichaine*: ils ne sont pas comparables deux à deux avec la relation d'ordre.

3.2 Codes minimaux en métrique de Hamming

En métrique de Hamming, la Définition 3.1.2 peut être reformulée comme suit.

Définition 3.2.1. Un code $\mathcal{C}$ est *minimal* si pour toute paire de mots de code non nuls $c, c' \in \mathcal{C} \setminus \{0\}$ vérifie

$$\sigma(c) \subseteq \sigma(c') \iff \exists \lambda \in \mathbb{F}_q, \quad c = \lambda c'.$$

Historiquement, les codes minimaux ont d'abord été étudiés dans le cas binaire (i.e. $q = 2$). Dans ce cas, les codes minimaux sont exactement les codes intersectants, que nous examinerons dans le chapitre suivant.

En particulier, en appliquant le Théorème 4.1.4, cela veut dire qu'un $[n, k, d]_q$-code minimal vérifie toujours $d \geq k$, mais nous verrons plus bas que nous pouvons montrer des inégalités bien plus fortes.

3.2.1 Quelques bornes élémentaires

Proposition 3.2.2 ([9], Lemme 2.1. (2.))**.** Soit $\mathcal{C}$ un $[n, k, d]_q$-code minimal. Pour tout mot de code $c \in \mathcal{C}$ on a

$$\mathrm{wt}(c) \leq n - k + 1.$$

Théorème 3.2.3 ([9], Lemme 2.1. (3.))**.** Soit $\mathcal{C}$ un $[n, k, d]_q$-code, et notons $d \leq w \leq n$ son poids de Hamming maximal. Si

$$\frac{w}{d} < \frac{q}{q-1},$$

alors $\mathcal{C}$ est un code minimal.

Le Théorème 3.2.3 est nommé *condition de Ashikhmin-Barg*. Il permet de construire beaucoup de familles de codes minimaux: par exemple, une des conséquences immédiates est que tout code à poids constant est un code minimal. Similairement, il est facile de vérifier si un code à deux poids est un code minimal.

Dans [52], cette condition est utilisée pour construire des codes minimaux avec un ensemble de poids restreints. Il est important de noter que si la condition d'Ashikhmin-Barg est suffisante, elle n'est pas nécessaire: il existe en effet une famille infinie de codes minimaux qui ne satisfont pas la borne, comme établi dans [37].

Théorème 3.2.4 ([23], Théorème 2.)**.** Soit $\mathcal{C}$ un $[n,k,d]_q$-code. Si $\mathcal{C}$ est minimal, alors

$$n \geq \log_2(q) \cdot k.$$

Proposition 3.2.5 ([26], Corollaire 1.)**.** Soit $\mathcal{C}$ un $[n,k,d]_q$-code tel que $k \geq 2$. Si $\mathcal{C}$ est minimal, alors

$$d \leq k + q - 2.$$

Proposition 3.2.6 ([6], Théorème 2.8.)**.** Soit $\mathcal{C}$ un $[n,k,d]_q$-code. Si $\mathcal{C}$ est minimal, alors

$$d \geq (q-1)(k-1) + 1.$$

3.2.2 Une interprétation géométrique : les ensembles générateurs d'hyperplans

Définition 3.2.7. Soit $\mathcal{S} \subset \mathrm{PG}(k-1,q)$. On dit que $\mathcal{S}$ est un *ensemble générateur d'hyperplans* si pour tout hyperplan $\mathcal{H} \subset \mathrm{PG}(k-1,q)$, l'intersection de $\mathcal{H}$ avec $\mathcal{S}$ engendre $\mathcal{H}$:

$$\langle \mathcal{S} \cap \mathcal{H} \rangle = \mathcal{H}.$$

De manière équivalente, $\mathcal{S}$ est un ensemble générateur d'hyperplans si tout hyperplan peut être engendré par $k-1$ points de $\mathcal{S}$.

La motivation derrière l'étude de ces ensembles est le théorème suivant.

Théorème 3.2.8 ([3], Théorème 3.4., [66], Théorème 14.)**.** Soit $\mathcal{C}$ un code et soit $\mathcal{S}$ l'ensemble de points associé à l'une de ses matrices génératrices. Le code $\mathcal{C}$ est un code minimal si et seulement si $\mathcal{S}$ est un ensemble générateur d'hyperplans.

Preuve. Notons G une matrice génératrice de $\mathcal{C}$ dont les colonnes correspondent aux points de $\mathcal{S}$.

Supposons que $\mathcal{S}$ soit un ensemble générateur d'hyperplans. Soit $x \in \mathbb{F}_q^k \backslash \{0\}$, et $\mathcal{H} = \langle x \rangle^\perp$. Notons également $x' \in \mathbb{F}_q^k \setminus \{0, x\}$, et $\mathcal{H}' = \langle x' \rangle^\perp$. Puisque $\mathcal{S}$ est un ensemble générateur d'hyperplans, il existe $P \in \mathcal{S} \cap \mathcal{H} \backslash \mathcal{S} \cap \mathcal{H}'$. Par symétrie, il existe également $P' \in \mathcal{S} \cap \mathcal{H}' \backslash \mathcal{S} \cap \mathcal{H}$.

Par conséquent, $\mathcal{S} \cap \mathcal{H}$ et $\mathcal{S} \cap \mathcal{H}'$ ne sont pas comparables pour l'inclusion, ce qui implique que $\sigma(xG)$ et $\sigma(x'G)$ ne sont également pas comparables pour l'inclusion. Par conséquent $\mathcal{C}$ est un code minimal.

Inversement, supposons que $\mathcal{S}$ ne soit pas un ensemble générateur d'hyperplans. Alors pour un certain hyperplan $\mathcal{H} = \langle x \rangle^\perp$, avec $x \in \mathbb{F}_q^k$, on a $\mathcal{S} \cap \mathcal{H} \subset \mathcal{U}$, où $\mathcal{U} \subset \mathrm{PG}(k-1,q)$ est un sous-espace projectif de codimension 2. Notons alors $\mathcal{H}'$ un hyperplan projectif contenant $\mathcal{U}$ mais distinct de $\mathcal{H}$, et notons $x' \in \mathbb{F}_q^k$ tel que $\mathcal{H}' = \langle x' \rangle^\perp$. On a alors $\mathcal{S} \cap \mathcal{H} \subset \mathcal{S} \cap \mathcal{U} \subset \mathcal{S} \cap \mathcal{H}'$, et par conséquent, on a également $\sigma(x'G) \subset \sigma(xG)$. Cependant, x et x' ne peuvent pas être colinéaires, car $\mathcal{H}$ et $\mathcal{H}'$ sont distincts. Par conséquent, le code $\mathcal{C}$ n'est pas minimal. □

Ce résultat permet de donner une interprétation géométrique simple des codes minimaux. Beaucoup des propriétés des codes minimaux que nous déterminerons par la suite se comprennent le plus clairement quand on les interprète du point de vue de la géométrie projective.

3.3 Bornes sur la taille des ensembles générateurs d'hyperplans

Les ensembles générateurs d'hyperplans vérifient la proposition élémentaire suivante.

Proposition 3.3.1. Soit $\mathcal{S} \subset \mathcal{S}' \subset \mathrm{PG}(k-1,q)$. Si $\mathcal{S}$ est un ensemble générateur d'hyperplans, alors $\mathcal{S}'$ l'est aussi.

Preuve. Soit $\mathcal{H}$ un hyperplan projectif de $\mathrm{PG}(k-1,q)$. Alors $(\mathcal{S} \cap \mathcal{H}) \subset (\mathcal{S}' \cap \mathcal{H})$, et si $\mathcal{S} \cap \mathcal{H}$ engendre $\mathcal{H}$, alors il en est de même pour $\mathcal{S}' \cap \mathcal{H}$. □

On comprend intuitivement qu'un ensemble générateur d'hyperplans doit être assez grand. Par conséquence, la question naturelle à poser du point de vue de la recherche est la suivante: Quelle est la plus petite taille d'un ensemble générateur d'hyperplans dans $\mathrm{PG}(k-1,q)$? Notons qu'il pourrait y avoir plusieurs ensembles générateurs d'hyperplans qui atteignent la taille minimale.

Ces considérations mènent à la définition suivante.

Définition 3.3.2. La taille minimale d'un ensemble générateur d'hyperplans dans $\mathrm{PG}(k-1,q)$ est notée $m(k,q)$. C'est également la longueur minimale d'un code minimal de dimension k sur $\mathbb{F}_q$.

Dans la suite, les bornes sur la taille minimale des ensembles générateurs d'hyperplans ou sur la longueur minimale d'un code minimal seront présentées en utilisant la fonction $m(k,q)$.

Définition 3.3.3. Un ensemble $B \subseteq \mathrm{AG}(k-1,q)$ est appelé *ensemble bloquant affine* s'il intersecte tout hyperplan affine de $\mathrm{AG}(k-1,q)$.

Théorème 3.3.4 ([40])**.** Soit $\mathcal{B} \subseteq \mathrm{AG}(k-1,q)$ un ensemble bloquant affine. Alors $|B| \geq (q-1)(k-1)+1$.

Théorème 3.3.5 ([6], Théorème 2.14.)**.**

$$m(k,q) \geq (q+1)(k-1).$$

Puisque nous allons nous intéresser en détail au cas d'égalité de ce théorème, nous nous permettons d'en restituer une preuve, qui servira de base pour nos considérations dans la Section 3.4.

Preuve. Soit S un ensemble générateur d'hyperplans de $\mathrm{PG}(k-1,q)$. Soit H un hyperplan de $\mathrm{PG}(k-1,q)$ d'intersection maximale avec S. Notons $S_H = S \backslash H$. Puisque S est un ensemble générateur d'hyperplans, S_H est un ensemble bloquant affine. Soit S'_H un ensemble bloquant affine minimal par rapport à l'inclusion contenu dans S_H. D'après le Théorème 3.3.4, on a $|S'_H| \geq 1+(k-1)(q-1)$. D'autre part, la minimalité de S'_H implique que pour tout $P \in S'_H$ il existe un hyperplan U tel que $U \cap S'_H = \{P\}$. Il existe un hyperplan Z contenant $H \cap U$ mais distinct de H et de U, et tel que $|Z \cap (S_H \setminus U)| \geq k-1$, car $|S_H \setminus U| \geq (q-1)(k-1)$, et car les $q-1$ hyperplans contenant $H \cap U$ distincts de H et de U forment une partition de $S_H \setminus U$.

On a donc:

$$\begin{aligned} |H \cap S| \geq |Z \cap S| &\geq |Z \cap S_H| + |Z \cap S \cap H| = |Z \cap (S_H \setminus U)| + |U \cap (S \cap H)| \\ &= |Z \cap (S_H \setminus U)| + |S \cap H| + |(S \setminus H) \setminus U| - |S \setminus U| \\ &\geq (k-1) + |S \cap H| + (k-1)(q-1) - |S \setminus U| \end{aligned}$$

et donc $|S \setminus U| \geq q(k-1)$. Puisque $|S \cap U| \geq (k-1)$, on obtient $|S| = |S \cap U| + |S \setminus U| \geq (k-1)(q+1)$. □

D'autre part, la meilleure borne supérieure connue sur $m(k,q)$ est la borne suivante.

Théorème 3.3.6.

$$m(k,q) \leq \left\lceil \frac{2k}{\log_q(\frac{q^4}{q^3-q+1})} \right\rceil \cdot (q+1) \simeq 2(q+1)k.$$

Cette borne est issue d'une construction probabiliste impliquant des droites de $\mathrm{PG}(k-1,q)$, présentée simultanément dans [4] et [16].

Corollaire 3.3.7. La famille des codes minimaux est asymptotiquement bonne.

On comprend bien que l'objectif de tout ce qui suit sera d'explorer les propriétés de la fonction $m(k,q)$ et de développer une bonne compréhension géométrique des ensembles

générateurs d'hyperplans. Avant de rentrer dans les détails des preuves, je veux donner ici une vision d'ensemble de l'état de l'art, ainsi que mes intuitions sur les ensembles générateurs d'hyperplans.

D'un point de vue assez abstrait et très intuitif, un ensemble générateur d'hyperplans doit avoir des points *hautement non alignés*. Ma compréhension intuitive est qu'un tel ensemble doit présenter le moins de structure possible. Cela est difficile à réconcilier avec notre culture mathématique, qui adore les ensembles (algébriques, géométriques, etc.) avec beaucoup de structure. Beaucoup de structures géométriques élémentaires sont à éviter, en particulier lorsque les points sont "trop alignés".

La seule chose sur laquelle les chercheurs semblent être d'accord (et je partage cette opinion) est qu'il est pratique de considérer des ensembles de droites plutôt que des ensembles de points. Cette idée est assez logique: en effet, toute droite doit intersecter tout hyperplan pour des raisons élémentaires de dimension. Par conséquent, un ensemble de droites aura beaucoup d'intersections avec les divers hyperplans, ce qui facilite grandement la construction d'ensembles générateurs d'hyperplans.

En pratique, puisque tout ensemble de droites dispersées est un ensemble générateur d'hyperplans (l'inverse n'est pas vrai: il peut y avoir des ensembles de droites non dispersées mais qui forment un ensemble générateur d'hyperplans), on choisit de construire des ensembles de droites dispersées, ce qui (en l'état actuel de nos connaissances) est déjà suffisamment complexe.

J'ai passé beaucoup de temps à essayer d'améliorer la borne supérieure probabiliste du Théorème 3.3.6, et pour l'instant je n'en pas été capable. Il s'agit de l'un de ces problèmes qui "résistent", et où chaque idée prometteuse se heurte à une difficulté imprévue.

De mon point de vue, la difficulté principale vient du fait que les constructions qui impliquent des droites qui se croisent "souvent" sont mauvaises et ne peuvent pas produire des familles de droites dispersées. Par exemple, une famille de droites qui passent toutes par un point commun serait la pire version de cette idée (on imagine facilement un tel "faisceau de droites", personnellement j'imagine un tipi): n'importe quel espace de codimension 2 qui contient le point intersectera toutes les droites, et la famille ne peut pas être dispersée.

En somme, il faudrait faire avec les droites exactement ce que l'on fait avec les points, c'est-à-dire les choisir de manière à ce qu'elles soient le plus dispersées possible. Cela est très difficile à obtenir avec une construction qui a la moindre structure, parce qu'une construction structurée tend à produire des droites qui s'intersectent.

Plus bas, nous verrons une construction explicite avec des graphes expanseurs. Les droites de cette construction s'intersectent, et la construction en souffre considérablement (même si elle demeure excellente): la constante explicite est assez grande par rapport à la borne supérieure probabiliste du Théorème 3.3.6.

3.3.1 Notre borne inférieure asymptotique

Notre objectif dans [62] est d'améliorer la borne inférieure du Théorème 3.3.5. Notre méthode consiste à chercher quels paramètres asymptotiques $(R, \delta) \in [0,1]^2$ peuvent être atteints par une suite de codes minimaux dont les longueurs tendent vers l'infini.

Observons pour commencer que la borne $d \geq (q-1)(k-1)+1$ du Théorème 3.3.5 peut s'interpréter comme une borne asymptotique. En effet, elle équivaut à la fonction *majorante* q-aire

$$b(\delta) = \delta/(q-1).$$

Notons évidemment que cette fonction n'est valide que pour les codes minimaux. L'avantage de ce point de vue est qu'elle délimite une région assez petite de $[0,1]^2$, et que l'intersection de cette fonction avec une fonction majorante q-aire classique de théorie des codes nous donnera une borne supérieure sur R (qui correspond à l'ordonnée du point d'intersection de b et de notre fonction majorante q-aire bien choisie).

Théorème 3.3.8 ([62], Théorème 3.3., et [16], Théorème 1.4.)**.**

$$\liminf_{k\to\infty} m(k,q) \geq (q+\varepsilon(q)) \cdot k,$$

où ε est une fonction croissante qui vérifie

$$1.5204 \leq \varepsilon(2) \leq \varepsilon(q) \leq \sqrt{2} + \frac{1}{2}.$$

Preuve. La fonction majorante q-aire correspondant à la borne MRRW est

$$M_q(\delta) = H_q\left(\frac{1}{q}\left(q-1-(q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}\right)\right).$$

Nous voulons vérifier que l'ordonnée du point d'intersection des graphes de M et de $b(\delta) = \delta/(q-1)$ est inférieure à $(q+\varepsilon(q))^{-1}$. Puisque M_q est décroissante, et puisque pour $\delta = \delta_c(q) = \frac{q-1}{q+\varepsilon(q)}$ la borne supérieure sur le taux d'information est $R \leq \frac{\delta_c(q)}{q-1} = \frac{1}{q+\varepsilon(q)}$, il suffit de vérifier que $M_q(\delta_c(q)) \leq \frac{1}{q+\varepsilon(q)}$, ou, de manière équivalente, que

$$M_q\Big(\frac{q-1}{q+\varepsilon(q)}\Big)(q+\varepsilon(q)) \leq 1.$$

Notons

$$A(q) = \frac{1}{q}\left(q-1-(q-2)\delta_c(q) - 2\sqrt{(q-1)\delta_c(q)(1-\delta_c(q))}\right) = \frac{q-1}{q(q+\varepsilon(q))} \cdot C(q),$$

où $C(q) = \varepsilon(q) + 2 - 2\sqrt{\varepsilon(q)+1}$.

La valeur de $(q+\varepsilon(q))H_q(A(q))$ est alors

$$(q+\varepsilon(q))H_q(A(q)) \leq \frac{q-1}{q} \cdot C(q) \cdot \log_q \Big(\frac{e}{C(q)} q(q+\varepsilon(q)) \Big).$$

Nous voulons montrer que $(q+\varepsilon(q))H_q(A(q)) \leq 1$, si bien qu'il suffit d'établir

$$\frac{q-1}{q} \cdot C(q) \cdot \log_q \Big(\frac{e}{C(q)} q(q+\varepsilon(q)) \Big) \leq 1. \tag{3.1}$$

Soit $\varepsilon(q)$ tel que (3.1) soit une égalité. Une évaluation numérique donne $\varepsilon(2) \geq 1.5204$.

Supposons à présent que nous ayons montré que ε est croissante jusqu'à la puissance première ℓ, et notons $C_\ell = \varepsilon(\ell) + 2 - 2\sqrt{\varepsilon(\ell)+1}$. Il suffit de montrer que

$$\forall q \geq \ell \quad \frac{q-1}{q} \cdot C_\ell \cdot \log_q \Big(\frac{e}{C_\ell} q(q+\varepsilon(\ell)) \Big) \leq 1.$$

Un calcul direct permet de montrer que la fonction

$$f(x) = \frac{x-1}{x} \cdot C_\ell \cdot \frac{\ln\Big(\frac{e}{C_\ell} x(x+\varepsilon(\ell)) \Big)}{\ln(x)}$$

est décroissante. Puisque $f(\ell) = 1$, pour toute puissance première q plus grande que ℓ, on a $f(q) < 1$, c'est-à-dire $\varepsilon(q) > \varepsilon(\ell)$. Par conséquent ε est une fonction croissante.
Pour finir, un calcul direct donne

$$\lim_{q \to \infty} \varepsilon(q) = \sqrt{2} + \frac{1}{2}.$$

□

Remarque 3.3.9. En raison de la manière dont ε est définie dans la preuve ci-dessus, ses valeurs sont suboptimales. Si nous avions défini $\varepsilon(q)$ comme étant la valeur telle que $H_q(A(q))(q+\varepsilon(q)) = 1$, on aurait obtenu les bornes inférieures asymptotiques telles qu'elles apparaissent dans le Tableau 3.1.

Nous avons choisi la définition suboptimale précisément pour prouver que ε est croissante, en jugeant que l'écart n'est pas trop grand. Je suis fermement persuadé que la valeur réelle de ε est également croissante.

L'écart entre notre définition de ε et la borne inférieure réelle est indiqué dans le tableau ci-dessous.

Remarque 3.3.10. Il serait possible d'améliorer le Théorème 3.3.8 si l'on parvenait à trouver une meilleure fonction majorante q-aire. Bien évidemment, il est seulement nécessaire que cette fonction corresponde à une borne sur les codes minimaux.

q	$\liminf_{k\to\infty} \frac{m(k,q)}{k} - q$	$\varepsilon(q)$
2	1.5276	1.5204
3	1.5516	1.5450
4	1.568	1.5624
5	1.5805	1.5757
7	1.5987	1.5951
8	1.6057	1.6025

Table 3.1: Écart entre le ε du théorème et la valeur réelle de la borne inférieure.

Par exemple, si pour $q = 2$ la borne de Gilbert-Varshamov $f(x) = 1 - H_2(x)$ est bien une fonction majorante binaire, ce qui est encore un problème ouvert mais paraît plausible à mes yeux aussi bien qu'aux yeux de tous les théoriciens des codes auxquels j'ai posé la question, on en déduira immédiatement une borne inférieure significativement plus forte sur la valeur asymptotique de $m(k, 2)$.

Remarque 3.3.11. Il est regrettable que la preuve du Théorème 3.3.8 ne soit pas le fruit d'une compréhension géométrique des ensembles générateurs d'hyperplans. Mon impression est qu'elle surgit comme simple conséquence de théorèmes de théorie des codes, sans donner davantage d'information sur la structure géométrique des ensembles générateurs d'hyperplans, comme le fait par exemple la preuve du Théorème 3.3.5.

3.4 Le cas d'égalité quand $q = 2$

Dans la section précédente nous avons établi que la borne inférieure $m(k, q) \leq (k - 1)(q + 1)$ n'est pas optimale quand k est grand. Dans [6], les auteurs établissent que la borne n'est pas optimale pour $2 \leq k \leq \sqrt{q} + 2$ (sauf si $q = 2$ et $k = 3$). Dans cette section, nous nous intéressons au cas d'égalité quand k est petit et $q = 2$.

Il est clair qu'il n'y a qu'un nombre fini de codes minimaux atteignant la borne inférieure à q fixé. Il est donc clair que ces codes minimaux doivent posséder des caractéristiques particulières. Notre objectif est de développer notre compréhension de ces codes remarquables.

Nous commencerons par nous intéresser à la preuve du Théorème 3.3.5, et nous déduirons des résultats de structure forts sur les codes minimaux qui atteignent la borne inférieure.

3.4.1 Quelques résultats de structure

Pour obtenir des ensembles générateurs d'hyperplans de taille minimale, une grande partie des inégalités de la preuve du Théorème 3.3.5 doivent être des égalités. Prenons donc $q = 2$ et considérons un ensemble générateur d'hyperplans $\mathcal{S} \subseteq \mathrm{PG}(k - 1, q)$ de taille $(k - 1)(q + 1) = 3(k-1)$. On doit avoir $\mathcal{S}_H = \mathcal{S}'_H$, et chacun doit avoir cardinal exactement $(k-1)(q-1)+1 = k$.

On doit également avoir $|\mathcal{S} \cap U| = k - 1$. En particulier, $|\mathcal{S} \cap U| = k - 1$ doit être vérifié indépendamment du choix d'un point P et du choix de l'hyperplan U, ce qui implique qu'il y a exactement k tels points, et par conséquent exactement k hyperplans U pour lesquels $|\mathcal{S} \cap U| = k - 1$.

Les points d'un ensemble générateur d'hyperplans correspondent aux colonnes d'une matrice génératrice. Si nous considérons que les k points de $\mathcal{S}_H$ correspondent aux k premières colonnes, alors le mot de code correspondant à l'hyperplan H est

$$c_H = (\underbrace{1, \ldots, 1}_{k \text{ times}}, \underbrace{0, \ldots, 0}_{2k-3 \text{ times}}).$$

Le mot de code correspondant à un hyperplan U_j (où P est le point correspondant à la j-ème colonne de la matrice génératrice) est

$$c_{U_j} = (1, \ldots, 1, 0, 1, \ldots, 1) \cdot b_{U_j},$$

où le 0 est en j-ème position et b_{U_j} est un mot de code correspondant aux derniers $2k - 3$ indices, de poids de Hamming $w_H(b_{U_j}) = k - 1$.

Puisque les mots de code $c_H + c_{U_j}$ sont en forme échelonnée, ils sont linéairement indépendants. De plus, puisqu'il y a exactement k tels mots de code, ils forment les lignes de la matrice génératrice suivante

$$G = \begin{pmatrix} I_k & R \end{pmatrix} \tag{3.2}$$

avec $R \in \mathcal{M}_{k,2k-3}(\mathbb{F}_q)$.

Chaque ligne de R doit avoir poids de Hamming $k - 1$, et puisque c_H est un mot de code qui ne peut être engendré qu'en sommant toutes les lignes, toutes les colonnes de R doivent avoir poids de Hamming pair.

Nous venons donc de montrer le résultat suivant.

Proposition 3.4.1. Soit $\mathcal{C}$ un code minimal de paramètres $[n, k, d]_2$, avec $n = 3(k-1)$. Alors $\mathcal{C}$ est équivalent à un code engendré par une matrice génératrice de la forme (3.2), où chaque ligne a poids de Hamming k et chaque colonne de R a poids de Hamming pair. De plus, $d = k$.

Notre objectif est de déterminer s'il est possible pour des matrices de la forme (3.2) d'être des matrices génératrices de codes binaires minimaux. Dans tout ce qui suit, nous noterons $N = k - 1$ pour simplifier la notation.

Considérons donc une matrice de la forme (3.2). La sous-matrice R a $N + 1$ lignes et $2N - 1$ colonnes. Notons $R_j \subseteq \{1, \ldots, 2N - 1\}$ le support de la j-ème ligne. Puisque chaque ligne de R a poids de Hamming N, chaque sous-ensemble correspondant $R_j \subset \{0, \ldots, 2N-1\}$

doit avoir cardinal

$$|P_j| = N.$$

Le code minimal $\mathcal{C}$ correspondant à cette matrice génératrice aura distance minimale $N+1$, et puisque le poids de Hamming de chaque mot de code $c \in \mathcal{C}$ vérifie la Proposition 3.2.2, le poids de Hamming d'un mot de code ne peut excéder $2N$.

Lemme 3.4.2. Un code minimal binaire $\mathcal{C}$ de paramètres $[3N, N+1]$ correspond à une famille de $N+1$ sous-ensembles de $\{1, \ldots, 2N-1\}$ qui ont tous cardinal N et dont les intersections deux à deux ont cardinal compris entre $\frac{N-1}{2}$ et $\frac{N+1}{2}$, et tels que la différence symétrique de tous les $N+1$ sous-ensembles est l'ensemble vide.

Preuve. Notons $A\Delta B = (A \cup B) \setminus (A \cap B)$ la différence symétrique des ensembles A et B. Considérons G une matrice de la forme (3.2), telle que G est une matrice génératrice d'un code équivalent à $\mathcal{C}$. Ajouter la i-ème et la j-ème ligne de G produit un mot de code de poids $2 + |R_i \Delta R_j|$ (le terme 2 vient du bloc I_k de G). Ajouter le mot de code c_H à cette somme produit un mot de code de poids $N - 1 + |R_i \Delta R_j|$.

Puisque ces mots de code doivent avoir poids de Hamming compris entre $N+1$ et $2N$, on en déduit naturellement des bornes sur le cardinal des différences symétriques $|R_i \Delta R_j|$: $N + 1 \leq 2 + |R_i \Delta R_j|$ donne $|R_i \Delta R_j| \geq N - 1$, tandis que $N - 1 + |R_i \Delta R_j| \leq 2N$ donne $|R_i \Delta R_j| \leq N + 1$, de sorte qu'on obtient $N - 1 \leq |R_i \Delta R_j| \leq N + 1$.

Puisque $|R_i \Delta R_j| = 2N - 2|R_i \cap R_j|$ on obtient

$$\frac{N-1}{2} \leq |R_i \cap R_j| \leq \frac{N+1}{2}. \tag{3.3}$$

Pour finir, puisque le mot de code c_H ne peut être engendré qu'en sommant toutes les lignes de G, les dernières $2N-1$ colonnes doivent avoir poids de Hamming pair, i.e. la différence symétrique des sous-ensembles R_i est l'ensemble vide. □

En particulier, quand $N = k - 1$ est pair, il n'y a qu'une seule valeur possible pour le cardinal de l'intersection entre deux sous-ensembles R_i et R_j.

Remarquons que raisonner en termes de poids de Hamming donne des conditions supplémentaires sur les poids de Hamming des différences symétriques des sous-ensembles correspondant aux indices de 3 lignes de R, et ainsi de suite.

3.4.2 Le cas où N est pair

Quand N est pair, on peut prendre $R_1 = \{1, \ldots, N\}$ et $R_2 = \{N/2 + 1, \ldots, N + N/2\}$ sans perte de généralité au vu de la discussion plus haut.

Pour chaque nouveau sous-ensemble $I \subseteq \{1, \dots, 2N-1\}$ on note

$$\begin{aligned} a_I &= |I \cap (R_1 \setminus R_2)|, \\ b_I &= |I \cap (R_1 \cap R_2)|, \\ c_I &= |I \cap (R_2 \setminus R_1)|, \\ d_I &= |I \cap \big(\{1, \dots, 2N-1\} \setminus (R_1 \cap R_2)\big)|. \end{aligned}$$

Le lemme suivant présente quelques restrictions sur les valeurs que peuvent prendre $a_I, \dots, d_I$.

Lemme 3.4.3. Soit $\mathcal{C}$ un code binaire minimal de dimension $k \geq 3$, dont un code équivalent admet une matrice génératrice de la forme (3.2). Si R_1, R_2, et I sont les supports de 3 lignes de la sous-matrice R, alors les $a_I, \dots, d_I$ définis plus haut vérifient $a_I = c_I$, $b_I = d_I$ et $|a_I - b_I| \leq 1$.

Preuve. Notons pour commencer que $a_I + b_I = |R_1 \cap I| = N/2 = |R_2 \cap I| = b_I + c_I$, ce qui donne $a_I = c_I$. De plus, puisque $a_I + b_I + c_I + d_I = N = a_I + 2b_I + c_I$, on a également $b_I = d_I$.

Posons $s = b_I + d_I$. La différence symétrique des trois ensembles a cardinal $N+s-(N-s) = 2s$. La somme des trois lignes correspondantes produit un mot de code $c = c_{P_1+P_2+I}$ dont le poids de Hamming est $w_H(c) = 3 + 2s$. Puisque $w_H(c) = 3 + 2s \geq N + 1$ à cause des conditions sur les poids, on obtient $s \geq N/2 - 1$.

Remarquons $c + c_H$ est également un mot de code, de poids de Hamming $N - 2 + 2s = N + 2s - 2$. L'autre inégalité sur les poids donne $N + 2s - 2 \leq 2N$, ce qui donne $s \leq N/2 + 1$. Cela signifie que $N/2 - 1 \leq b_I + d_I \leq N/2 + 1$, ce qui implique également que $N/2 - 1 \leq a_I + c_I \leq N/2 + 1$.

Pour finir, puisque $a_I = c_I$ et $b_I = d_I$ on obtient $|a_I - N/4| \leq 1/2$ et $|b_I - N/4| \leq 1/2$, ce qui donne $|a_I - b_I| \leq 1$. □

Ce lemme est particulièrement utile, puisqu'il permet de restreindre considérablement quels nouveaux sous-ensembles choisir une fois qu'on a déjà choisi les deux premiers. Notons que tout nouveau sous-ensemble doit satisfaire les conditions du lemme pour n'importe quel choix de R_i, R_j parmi les sous-ensembles déjà sélectionnés. En particulier, quand N grandit, on s'attend à ce que ce soit de plus en plus difficile.

Proposition 3.4.4. Il n'existe aucun code minimal binaire de paramètres $[18, 7]$.

Preuve. Dans ce cas particulier on a $R_1 = \{1, 2, 3, 4, 5, 6\}$ et $R_2 = \{4, 5, 6, 7, 8, 9\}$. Nous nous intéressons aux colonnes correspondant aux indices 10 et 11, on sait en particulier que chacune doit avoir poids de Hamming pair d'après le Lemme 3.4.3. A cause du Lemme 3.4.3,

les seules valeurs possibles pour d_I sont 1 et 2. Nous divisons les sous-ensembles qui satisfont les conditions énoncées au Lemme 3.4.3 en 3 familles, selon leur intersection avec $\{10, 11\}$:

$$A = \{I \subseteq \{1, \ldots, 2N-1\} \mid I \cap \{10, 11\} = \{10\}\}$$

$$B = \{I \subseteq \{1, \ldots, 2N-1\} \mid I \cap \{10, 11\} = \{11\}\}$$

$$C = \{I \subseteq \{1, \ldots, 2N-1\} \mid I \cap \{10, 11\} = \{10, 11\}\}$$

Pour que les lignes se somment à 0, il faut que 3 des sous-ensembles viennent d'une seule famille et 1 de chaque autre. Supposons pour commencer que 3 des sous-ensembles sont dans la famille A (par symétrie cela couvrira également le cas où ces sous-ensembles sont dans B). Alors leur différence symétrique est $\{4, 5, 6, 10\}$ et la différence symétrique de tous les cinq sous-ensembles est $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, ce qui produit un mot de code de poids de Hamming $5 + |S| = 5 + 10 = 15$, tandis que le poids maximal est au plus $2N = 12$, une contradiction.

Par conséquent les 3 sous-ensembles sont dans la famille C.

Dans ce cas on peut vérifier que leur différence symétrique doit être $\{1, 2, 3, 7, 8, 9, 10, 11\}$ et donc la différence symétrique des cinq mots de code doit être $S' = \{10, 11\}$, ce qui, additionné à c_H, donne un mot de code de poids de Hamming $(7 - 5) + |S'| = 2 + 2 = 4$, tandis que le poids minimal autorisé est $N + 1 = 7$ (puisque la distance minimale est $d = 7$ d'après le Lemme 3.4.3), ce qui donne encore une contradiction. □

Proposition 3.4.5. Il n'existe aucun code minimal binaire de paramètres $[24, 9]$.

Preuve. Ici, après avoir choisi R_1 et R_2, le Lemme 3.4.3 force tous les sous-ensembles restants I à vérifier $d_I = 2$. Puisque d_I est calculé en considérant l'intersection de I avec $\{13, 14, 15\}$, et puisqu'il y a 7 sous-ensembles restants, ils forment une matrice 7×3 dont chaque colonne a un nombre pair de 1, et donc il y a au moins une colonne avec au moins 3 fois le 0.

Dans le langage des sous-ensembles, cela signifie qu'il doit y avoir 3 sous-ensembles contenant (sans perte de généralité) $\{13, 14\}$. Sans perte de généralité supposons que le premier est I. Puisque $a_I = b_I = c_I = d_I = 2$ sans perte de généralité on choisit $I = \{1, 2, 5, 6, 9, 10, 13, 14\}$. Maintenant, en appliquant le Lemme 3.4.3 de deux sous-ensembles déjà sélectionnés, on déduit que le seul sous-ensemble restant qui contient $\{13, 14\}$ est $J = \{3, 4, 5, 6, 11, 12, 13, 14\}$, tandis que nous en voulons au moins deux pour trouver trois sous-ensembles contenant $\{13, 14\}$, une contradiction. □

Proposition 3.4.6. Il n'existe aucun code minimal binaire de paramètres $[30, 11]$.

Preuve. Ceci a été prouvé par une recherche numérique en 248 secondes sur un unique

processeur Intel i5 (9e génération), à l'aide d'un programme en Sagemath, en utilisant une méthode similaire au cas $N = 10$.

En pratique il est possible de restreindre la recherche encore davantage : après avoir éliminé des sous-ensembles en appliquant le Lemme 3.4.3, on peut diviser les sous-ensembles restants en classes d'équivalence en fonction de leurs intersections avec les ensembles déjà présents dans notre liste. Il est alors possible de ne tester qu'un seul représentant pour chaque classe d'équivalence, ce qui accélère considérablement la recherche.

On déduit rapidement qu'il est impossible pour 11 sous-ensembles de satisfaire les conditions tous en même temps, ce qui implique le théorème. □

Théorème 3.4.7. Si $N = 4 \pmod 8$, il n'existe aucun code binaire minimal de paramètres $[3N, N + 1]$.

Preuve. Une des conséquences directes de la preuve du Lemme 3.4.3 est que pour $N = 0 \pmod 4$, on a $a_I = b_I = c_I = d_I = N/4$ pour chaque nouveau sous-ensemble I. Considérons la sous-matrice de taille $N - 1 \times N/4$ correspondant aux indices $\{3N/2 + 1, \ldots, 2N - 1\}$ (i.e. ceux qui correspondent aux d_I). Chacune de ses lignes est la fonction indicatrice des $N - 1$ sous-ensembles restants dans $\{3N/2 + 1, \ldots, 2N - 1\}$, et donc chaque ligne de cette sous-matrice contient précisément $N/4$ fois le chiffre 1.

Pour $N = 4 \pmod 8$, il est clair que $N/4$ est impair. Puisque N est pair, $N - 1$ est également impair. Par conséquent, la sous-matrice dans son entier contient un nombre impair de 1, et ses lignes ne peuvent donc pas se sommer à 0, ce qui contredit la Proposition 3.4.1. □

Comme noté dans les précédentes sous-sections, il n'y a pas de codes minimaux binaires de paramètres $[3N, N + 1]$ quand N est assez grand. Cela implique que ces codes n'existent que pour un nombre fini de valeurs de N. Nous avons vu que de tels codes n'existent pas pour certaines valeurs de N, à savoir $N = 6$, $N = 8$, $N = 10$ et tous les N congrus à $4 \pmod 8$, il est naturel de poser la question suivante.

Question 3.4.8. Est-ce qu'il existe un code minimal binaire de paramètres $[3N, N + 1]$ si $N \geq 4$ est pair?

Nous nous attendons bien évidemment à une réponse négative, mais en l'absence de preuve pour les cas manquants rien ne peut être affirmé avec certitude.

3.4.3 Le cas où N est impair

Quand N est impair, la situation est considérablement plus complexe, parce que le cardinal de l'intersection de deux sous-ensembles de taille N peut avoir deux valeurs différentes.

Cela implique que lorsque l'on sélectionne un sous-ensemble de cardinal N dans $\{1, \ldots, 2N-1\}$, mettons $\{1, \ldots, N\}$ (sans perte de généralité), il devient bien plus difficile d'éliminer des sous-ensembles de cardinal N pour les lignes suivantes. Par conséquent, il est bien plus facile

pour une famille de $N+1$ sous-ensembles de cardinal N dans $\{1,\dots,2N-1\}$ de satisfaire le Lemme 3.4.2.

En effet, quand k est pair (et donc N impair) il existe des exemples de codes minimaux de longueur $3(k-1)$ avec $k \in \{2,4,6\}$ (par exemple dans [11]), tandis que la sous-section plus haut montre que cela est plus rare quand k est impair. La proposition suivante montre que même ces cas particuliers de codes minimaux courts sont rares.

Proposition 3.4.9. Pour $N = 7$ il n'existe aucun ensemble générateur d'hyperplans de taille $3N = 21$.

Preuve. Ceci a été prouvé par une recherche numérique en 802 secondes sur un unique processeur Intel i5 (9e génération), à l'aide d'un programme en Sagemath, en utilisant une méthode similaire au cas $N = 10$. □

3.5 Constructions explicites d'ensembles générateurs d'hyperplans

Tout ce que nous avons exposé jusqu'ici n'indique pas de quelle manière construire des ensembles générateurs d'hyperplans. Dans cette section nous exposons les meilleurs résultats connus à ce jour.

Nous commençons par le tétraèdre, un exemple relativement simple, exposé par exemple dans [3].

Exemple 3.5.1 (Le tétraèdre)**.** Considérons k points $V_1,\dots,V_k$ de $\mathrm{PG}(k-1,q)$ en position générale (i.e. qui engendrent $\mathrm{PG}(k-1,q)$ tout entier). Pour tous $i,j \in \{1,\dots,k\}, i<j$, prenons la droite $\ell_{i,j}$ passant par V_i et V_j. L'ensemble

$$\mathcal{T} = \bigcup_{i\neq j} \ell_{i,j}.$$

est appelé *tétraèdre*, et est un ensemble générateurs d'hyperplans.

Le tétraèdre a taille exactement $k + (q-1)\cdot\frac{k(k-1)}{2}$, ce qui est quadratique en k. Cela donne donc en particulier la borne supérieure

$$m(k,q) \leq k + (q-1)\cdot\frac{k(k-1)}{2},$$

qui est très mauvaise si on la compare avec les bornes supérieures linéaires en k obtenues plus haut.

Dans [18], les auteurs donnent des constructions explicites de codes minimaux de longueur en $O(q^4k)$.

Avant de donner les meilleures constructions asymptotiques, nous restituons les meilleures constructions explicites en petite dimension, i.e. dans le cas où la valeur exacte de $m(k,q)$ est déterminée explicitement.

3.5.1 Constructions optimales en petite dimension

Déterminer la valeur exacte de $m(k,q)$ pour des petites valeurs de k et q est possible, mais quand k grandit, ce problème devient très difficile au vu du grand temps de calcul nécessaire. Pour des valeurs de k assez petites, il est même possible de classifier entièrement la structure géométrique des ensembles générateurs d'hyperplans. Dans le cas particulier $q = 2$ et $k = 4$, ce travail a été réalisé par Smaldore dans [65].

Dans les deux tableaux ci-dessous, nous présentons les meilleurs résultats dont nous avons connaissance sur $m(k,q)$, y compris quelques valeurs exactes. Beaucoup de ces valeurs ont été obtenues par Kurz dans [42], en particulier pour $q = 2$ et $k \geq 7$. La borne $m(10,2) \leq 30$ a été établie par Cohen et Zémor dans [27]. Les bornes sur $m(6,3)$ établies ici sont obtenues dans [16]. Nous invitons le lecteur intéressé à se référer à ces travaux pour d'avantages de détails sur les méthodes utilisées.

k	2	3	4	5	6	7	8	9
$m(k,2)$	3	6	9	13	15	20	24	26
Référence	folklore	folklore	[3]	[3]	[25]	[42]	[42]	[42]

Table 3.2: Les premières valeurs de $m(k,2)$

k	10	11	12
$m(k,2)$	$28 \leq \cdot \leq 30$	$31 \leq \cdot \leq 35$	$33 \leq \cdot \leq 40$
Référence	[27,42]	[42]	[42]

Table 3.3: Les prochaines valeurs de $m(k,2)$

k	2	3	4	5	6
$m(k,3)$	3	9	14	19	$22 \leq \cdot \leq 24$
Référence	folklore	[3]	[3]	[16]	[16]

Table 3.4: Les premières valeurs de $m(k,3)$

Quelques autres résultats existent dans la littérature, nous citons en particulier celui-ci.

Théorème 3.5.2 (Théorème 3.1., [10]).

- Si $q \leq 8$, alors

$$m(3,q) = 3q.$$

- Si $q \geq 9$ est un carré, alors
$$m(3,q) = 2q + 2\sqrt{q} + 2.$$
- Si $q \geq 23$ est de la forme $q = p^{2a+1}$, alors
$$m(3,q) \geq 2q + p^a \left\lceil \frac{p^{a+1}+1}{p^a+1} \right\rceil + 2.$$
- Si $q \in \{11, 13, 17, 19\}$, alors
$$m(3,q) \geq \frac{5q+7}{2}.$$

3.5.2 Les graphes expanseurs

Dans cette partie nous présentons une construction explicite de codes minimaux asymptotiquement bons, de longueur asymptotique $O(kq)$ dans $\mathrm{PG}(k-1,q)$. Elle est exposée dans [8]. Nous la présentons ici pour montrer l'un des meilleurs résultats sur la théorie des codes minimaux, et parce que nous réutiliserons cette méthode dans le chapitre suivant pour le cas des codes intersectants.

Nous commençons par présenter les graphes expanseurs, qui sont l'ingrédient essentiel de la construction.

Définition 3.5.3. Soit $\mathcal{G} = (V, E)$ un graphe avec n sommets, mettons $V = \{u_1, \ldots, u_n\}$. La matrice d'adjacence $A_\mathcal{G}$ de $\mathcal{G}$ est la matrice de taille $n \times n$ et dont les coefficients sont

$$a_{i,j} = |\{\text{arêtes reliant } u_i \text{ et } u_j\}|.$$

Puisque cette matrice est symétrique, elle est clairement diagonalisable sur $\mathbb{R}$. Notons $\lambda_1(\mathcal{G}) \geq \lambda_2(\mathcal{G}) \geq \ldots \geq \lambda_n(\mathcal{G})$ ses valeurs propres. Rappelons que si le graphe $\mathcal{G}$ est t-régulier, alors $\lambda_1(\mathcal{G}) = t$. On note également

$$\lambda(\mathcal{G}) = \max\{|\lambda_2(\mathcal{G})|, \ldots, |\lambda_n(\mathcal{G})|\}.$$

Définition 3.5.4. Un (n,t,λ)-*graphe* $\mathcal{G}$ est un graphe t-régulier à n sommets tel que $\lambda(\mathcal{G}) \leq \lambda$. Un graphe t-régulier $\mathcal{G}$ avec $\lambda(\mathcal{G}) \leq 2\sqrt{t-1}$ est appelé *graphe de Ramanujan*.

Théorème 3.5.5 (Alon-Bopanna)**.** Pour tout (n,t,λ)-graphe,

$$\lambda \geq 2\sqrt{t-1} - o(1)$$

quand $n \to \infty$.

Dans [7], l'auteur établit le théorème suivant.

Théorème 3.5.6 (Théorème 1.3, [7]). Pour tout degré t, pour tout ε et tout $n \geq n_0(t, \varepsilon)$ suffisament grand, où nt est pair, il y a une construction explicite d'un (n, t, λ)-graphe avec

$$\lambda \leq 2\sqrt{t-1} + \varepsilon.$$

L'un des ingrédients fondamentaux de notre construction est l'intégrité d'un graphe. Il s'agit d'un invariant de graphe (comme le nombre chromatique par exemple), et est définie comme suit.

Définition 3.5.7. Soit $\mathcal{G} = (V, E)$ un graphe simple et connexe. Pour tout sous-graphe $\mathcal{H}$, notons $\kappa(\mathcal{H})$ la plus grande taille d'une composante connexe de $\mathcal{H}$. L'*intégrité* de $\mathcal{G}$ est l'entier

$$\iota(\mathcal{G}) = \min\{|S| + \kappa(\mathcal{G} - S) \mid S \subseteq V\}.$$

Proposition 3.5.8 (Corollaire 3.4, [7]). Tout (n, t, λ)-graphe $\mathcal{G}$ vérifie

$$\iota(\mathcal{G}) \geq n \cdot \frac{t-\lambda}{t+\lambda}.$$

Le lien entre la théorie des graphes expanseurs et les ensembles de droites dispersées, montré dans [8], est le suivant.

Proposition 3.5.9 (Lemme 4.4, [8]). Soit $\mathcal{M} = \{P_1, \ldots, P_n\} \subseteq \mathrm{PG}(k-1, q)$ un $[n, k, d]_q$-système projectif et $\mathcal{G} = (\mathcal{M}, E)$ un graphe. Si

$$\iota(\mathcal{G}) \geq n - d + 1,$$

alors l'ensemble de droites

$$\mathcal{L}(\mathcal{M}, \mathcal{G}) = \{\langle P_i, P_j \rangle \mid P_i P_j \in E\}$$

est dispersé.
Par conséquent, si $\mathcal{G}$ est un (n, t, λ)-graphe et si

$$\frac{t-\lambda}{t+\lambda} \geq 1 - \delta + \frac{1}{n},$$

alors les droites de $\mathcal{L}(\mathcal{M}, \mathcal{G})$ sont dispersées.

En utilisant des codes AG bien choisis, et en optimisant les paramètres des graphes expanseurs, les auteurs de [8] en déduisent des constructions explicites de codes minimaux de longueur environ $20k(q+1)$.

3.6 Applications

Dans [22], Brassard, Crépeau et Santha utilisent des codes minimaux pour concevoir un protocole de transfert inconscient.

Supposons que deux personnes, Alice et Bob, veulent mettre en œuvre le protocole suivant: Alice détient deux vecteurs de k bits $x_0, x_1 \in \mathbb{F}_2^k$, et Bob a un bit $b \in \mathbb{F}_2$. Bob veut connaître x_b sans révéler b à Alice, et Alice veut que Bob obtienne de l'information sur au plus l'un des vecteurs. On suppose que Alice et Bob ont accès à un protocole qui effectue du transfert inconscient dans le cas où $k = 1$.

L'idée naïve consistant à répéter ce protocole k fois (à chaque étape, on donne le choix entre $x_{0,i}$ et $x_{1,i}$) ne marche pas, car Bob peut apprendre des bits de x_0 et de x_1.

Avec la donnée d'un $[n, k]_2$-code minimal, les auteurs donnent un protocole pour du transfert inconscient sur k-bits qui utilise le transfert inconscient sur 1 bit exactement n fois. Plus n est petit, plus le protocole sera efficace. Par conséquent, dans ce contexte, il est clairement intéressant d'avoir accès à de bonnes construction explicites de codes minimaux.

La notion de rayon de recouvrement d'un code est reliée à l'étude des ensembles saturants, un objet classique de géométrie projective. Ils sont définis comme suit.

Définition 3.6.1. Soit $S \subset \mathrm{PG}(k-1, q)$. Si ρ est le plus petit entier tel que tout point $Q \in \mathrm{PG}(k-1, q) \setminus S$ vérifie $Q \in \langle P_1, \ldots, P_{\rho+1} \rangle$ (où les P_i sont des points de S), alors l'ensemble S et dit ρ-saturant.

Les ensembles générateurs d'hyperplans sont en fait un exemple d'ensembles saturants, comme expliqué dans [31].

Théorème 3.6.2 ([31], Théorème 3.2.)**.** Tout ensemble générateur d'hyperplans dans une sous-géométrie $\mathrm{PG}(k-1, q)$ de $\mathrm{PG}(k-1, q^{k-1})$ est un ensemble $(k-2)$-saturant dans $\mathrm{PG}(k-1, q^{k-1})$.

Un autre concept apparenté aux codes minimaux est celui de code *trifférent*, examiné par exemple dans [16] et [43]. Un code trifférent est un code $\mathcal{C}$ sur $\mathbb{F}_3$ tel que pour n'importe que choix de 3 mots de code distincts $c_1, c_2, c_3 \in \mathcal{C}$, il existe une coordonnée i pour laquelle $\{c_{1,i}, c_{2,i}, c_{3,i}\} = \{0, 1, 2\}$.

Dans le cas des codes linéaires, les codes trifférents sont exactement les codes minimaux.

3.7 Une rapide présentation de la métrique rang

Dans cette section nous développons les résultats principaux sur les codes minimaux en métrique rang $\mathbb{F}_{q^m}$-linéaire. Si nous resterons brefs, nous voulons insister sur l'analogie entre

l'étude des codes minimaux en métrique rang et celle des codes intersectants en métrique rang. Nous tenterons en effet de donner des explications aux similarités aussi bien qu'aux différences que nous constaterons.

Définition 3.7.1. Soit $\mathcal{C}$ un code $\mathbb{F}_{q^m}$-linéaire en métrique rang. On dit que $\mathcal{C}$ est *minimal* si deux mots de code non nuls $c, c' \in \mathcal{C}$ vérifient

$$\sigma_{\mathrm{rk}}(c) \subset \sigma_{\mathrm{rk}}(c') \iff \exists \lambda \in \mathbb{F}_{q^m}, \quad c = \lambda \cdot c'.$$

L'interprétation géométrique des codes minimaux en métrique rang, établie dans [5], est la suivante.

Théorème 3.7.2. Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code en métrique rang et soit $\mathcal{U}$ l'un des q-systèmes correspondants à $\mathcal{C}$. Le code $\mathcal{C}$ est minimal si et seulement si $L_{\mathcal{U}}$ est un ensemble générateur d'hyperplans.

Cette interprétation est surprenante: les ensembles générateurs d'hyperplans sont l'objet de géométrie projective relié aux codes minimaux aussi bien en métrique de Hamming qu'en métrique rang[2]!

Notons que le choix d'une matrice génératrice n'est pas important pour déterminer si $L_{\mathcal{U}}$ est un ensemble générateur d'hyperplans.

L'étude géométrique des q-systèmes correspondant aux codes minimaux permet d'obtenir plusieurs propriétés, que nous présentons ici.

Proposition 3.7.3 ([5], Corollaire 5.9.)**.** Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code minimal. Soit $c \in \mathcal{C}$ un mot de code. Alors

$$\mathrm{wt}_{\mathrm{rk}}(c) \leq n - k + 1.$$

On en déduit le théorème suivant.

Théorème 3.7.4 ([5], Corollaire 5.10.)**.** Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code minimal. Alors

$$n \geq k + m - 1.$$

Outre cette borne inférieure, l'interprétation géométrique permet également de déduire des bornes supérieures sur la longueur des codes minimaux en métrique rang.

Théorème 3.7.5 ([5], Proposition 6.2.)**.** Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code avec $n \geq (k-1)m + 1$. Alors $\mathcal{C}$ est minimal.

Théorème 3.7.6 ([5], Théorème 6.11.)**.** Soit $k, m \geq 2$. Pour tout choix de paramètres n, k, m, q tels que $n \geq 2k + m - 2$, il existe un $[n,k]_{q^m/q}$-code minimal en métrique rang.

[2] Il se trouve que les codes minimaux ont également été définis en métrique somme-rang, mais la présentation de cette métrique complexe n'est pas pertinente dans le cadre de ce travail.

Pour une discussion plus approfondie de ce sujet, nous invitons le lecteur à se référer à [5]. En particulier, on notera que le Théorème 3.7.4 et le Théorème 3.7.6 déterminent les longueurs possibles pour un code minimal en métrique rang, en laissant seulement $k-1$ valeurs de n où l'existence est encore inconnue. Cette "zone grise" a fait l'objet de travaux ultérieurs, en particulier pour $k = 3$, où des constructions explicites de longueur $n = m + 2$ ont été découvertes [5,49].

Chapter 4

Codes intersectants en métrique de Hamming

The mathematician's patterns, like the painter's or the poet's must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics.

- G.H. Hardy, *A mathematician's apology*

Dans ce chapitre nous abordons l'étude des codes intersectants. Ces codes sont bien connus dans la littérature, on pourra par exemple voir [17,27,29,60,61,64]. Dans beaucoup de travaux antérieurs, les codes intersectants ont été considérés principalement dans le cas $q = 2$, dans lequel leur définition est équivalente à celle des codes minimaux.

Les liens avec la combinatoire additive qui apparaîtront dans ce chapitre concernent bel et bien les codes intersectants. Nous proposons une généralisation de la constante de Davenport qui permet de conserver son lien avec les codes intersectants en introduisant un système de pondération par des endomorphismes. De plus, nous verrons qu'il est parfois possible d'interpréter l'action de ce groupe d'endomorphisme comme étant l'action du groupe de Galois sur le groupe de classes dans le cas de corps de nombres bien choisis, ce qui donne une motivation supplémentaire à notre travail.

4.1 Définition et premières propriétés

Définition 4.1.1. Un $[n, k, d]_q$-code $\mathcal{C}$ est *intersectant* si

$$\forall c, c' \in \mathcal{C} \setminus \{0\}, \quad \sigma(c) \cap \sigma(c') \neq \varnothing.$$

Quand $q = 2$, cette définition coïncide avec celle des codes minimaux, comme évoqué au

chapitre précédent.

Proposition 4.1.2. Soit $\mathcal{C}$ un $[n,k,d]_q$-code et H une matrice de parité de $\mathcal{C}$. Le code $\mathcal{C}$ est intersectant si et seulement si pour toute partition de H en deux blocs (de colonnes), l'un des blocs a rang maximal.

Preuve. Notons H_I et H_J ces deux blocs, où I et J sont des parties disjointes et complémentaires de $\{1,\dots,n\}$. Si H_I et H_J ont tous les deux une dépendance linéaire de colonnes, alors il existe des mots de code $c_I \in \mathcal{C}$ et $c_J \in \mathcal{C}$ disjoints (car $I \cap J = \varnothing$) et non nuls, par conséquent $\mathcal{C}$ n'est pas intersectant.

Réciproquement, si $\mathcal{C}$ n'est pas intersectant, il existe deux mots de code $c, c' \in \mathcal{C} \setminus \{0\}$ tels que $\sigma(c) \cap \sigma(c') = \varnothing$. Ces deux mots de code à supports disjoints correspondent à deux ensembles (disjoints) de colonnes de H qui ont chacun une dépendance linéaire. Par conséquent, il est possible de diviser H en deux blocs, dont aucun n'a rang maximal. □

Lemme 4.1.3. Soit $\mathcal{C}$ un $[n,k,d]_q$-code. Si $2d > n$, alors $\mathcal{C}$ est intersectant.

Preuve. Soit $c, c' \in \mathcal{C} \setminus \{0\}$ deux mots de code non nuls. D'après le principe des tiroirs, puisque $\mathrm{wt}(c) + \mathrm{wt}(c') \geq 2d > n$, il existe un indice $1 \leq i \leq n$ tel que $c_i \neq 0$ et $c'_i \neq 0$. Par conséquent $\sigma(c) \cap \sigma(c') \neq \varnothing$ et le code $\mathcal{C}$ est donc intersectant. □

Théorème 4.1.4. Soit $\mathcal{C}$ un $[n,k,d]_q$-code. Si $\mathcal{C}$ est intersectant, alors

$$d \geq k.$$

Preuve. Pour tout sous-ensemble $I \subset \{1,\dots,n\}$ tel que $|I| \leq k-1$, il existe un mot de code $c \in C \setminus \{0\}$ tel que $\forall i \in I, \quad c_i = 0$ (en appliquant le pivot de Gauss aux coordonnées de I.

Si $d = k-1$, alors il existe un mot de code c' tel que $\mathrm{wt}(c') = d = k-1$. Il suffit alors de prendre la construction du dessus avec $I = \sigma(c')$ et le couple c, c' vérifiera $\sigma(c) \cap \sigma(c') = \varnothing$, ce qui contredit le fait que $\mathcal{C}$ est intersectant. □

Lemme 4.1.5. Soit $\mathcal{C}$ un $[N,K,D]_{q^k}$-code intersectant et $\mathcal{I}$ un $[n,k,d]_q$-code intersectant. Alors $\mathcal{I}\square\mathcal{C}$ est un $[Nn, Kk, \geq Dd]_q$-code intersectant.

Il est possible de montrer une borne qui ressemble à celle de Plotkin.

Théorème 4.1.6. Pour $1 \leq t \leq k$, on a

$$i(k,q) \geq k + \frac{q^t - 1}{q^t - q^{t-1}}(k-t). \tag{4.1}$$

Preuve. Soit $G = (I_k \mid A)$ une matrice génératrice de $\mathcal{C}$. Nous allons considérer t lignes de G. Notons $\mathcal{V}$ la famille des combinaisons linéaires des t lignes de A correspondantes. Nous

voulons calculer la somme des poids des vecteurs de $\mathcal{V}$, que nous appellerons poids total de $\mathcal{V}$, noté $\mathrm{w}(\mathcal{V})$. Puisque les t lignes sont linéairement indépendantes, il y a $q^t - 1$ vecteurs dans $\mathcal{V}$ (avec multiplicités). Puisque tout mot de code correspondant à un vecteur de $\mathcal{V}$ a au plus t coordonnées non nulles parmi les k premières, chaque vecteur de $\mathcal{V}$ a poids de Hamming au plus $d - t \geq k - t$ (la dernière inégalité vient du Théorème 4.1.4). Par conséquent

$$\mathrm{w}(\mathcal{V}) \geq (q^t - 1)(k - t).$$

D'autre part, tout vecteur de $\mathcal{V}$ a longueur exactement $n - k$, et pour chaque coordonnée il y a au plus $q^t - q^{t-1}$ vecteurs de $\mathcal{V}$ qui sont non nuls en cette coordonnée. Le poids total est donc au plus

$$\mathrm{w}(\mathcal{V}) \leq (n - k)(q^t - q^{t-1}).$$

Il suffit alors de combiner les deux inégalités pour finir la preuve. □

Corollaire 4.1.7. Soit $\mathcal{C}$ un $[n, k, d]_q$-code. Si $\mathcal{C}$ est intersectant, alors

$$n \geq 2k - 1.$$

Preuve. Il suffit d'appliquer le Théorème 4.1.6 avec $t = 1$. □

4.2 Une interprétation géométrique

Nous avons vu au chapitre précédent que les codes minimaux non-dégénérés correspondent aux ensembles générateurs d'hyperplans dans l'espace projectif. La question dans le cas des codes intersectants est alors de savoir s'il existe une caractérisation des codes intersectants dans le langage de la géométrie projective. Nous allons montrer que c'est bel et bien le cas.

Définition 4.2.1. Soit $\mathcal{S} \subset \mathrm{PG}(k-1, q)$. On dit que $\mathcal{S}$ est *j-cohyperplanaire* s'il existe j hyperplans $\mathcal{H}_1, \ldots, \mathcal{H}_j$ de $\mathrm{PG}(k-1, q)$ tels que $\mathcal{S} \subset \bigcup_{i=1}^{j} \mathcal{H}_i$. On dit que $\mathcal{S}$ est *non-j-cohyperplanaire* si $\mathcal{S}$ n'est pas *j-cohyperplanaire*.

Dans toute la suite, par souci de simplicité et de concision nous noterons N2C pour désigner non-2-cohyperplanaire.

Théorème 4.2.2. Soit $\mathcal{C}$ un $[n, k, d]_q$-code non-dégénéré et soit $\mathcal{S} \subset \mathrm{PG}(k-1, q)$ l'ensemble de points obtenu à partir d'une une matrice génératrice de $\mathcal{C}$. Le code $\mathcal{C}$ est intersectant si et seulement si $\mathcal{S}$ est non-2-cohyperplanaire.

Preuve. Soit G une matrice génératrice de $\mathcal{C}$, et $\mathcal{S} = \{P_1, \ldots, P_n\} \subset \mathrm{PG}(k-1, q)$ l'ensemble des points projectifs correspondant aux colonnes de G. Notons $c = xG$ et $c' = x'G$ deux mots

de code non nul. Notons que $\sigma(c) = \{1 \leq i \leq n \mid P_i \notin \langle x \rangle^\perp\}$ et $\sigma(c') = \{1 \leq i \leq n \mid P_i \notin \langle x' \rangle^\perp\}$.

Par conséquent

$$\sigma(c) \cap \sigma(c') \neq \varnothing \iff \exists P \in \mathcal{S}, \quad P \notin \langle x \rangle^\perp \cup \langle x' \rangle^\perp.$$

On en déduit que $\mathcal{C}$ est intersectant si et seulement si $\mathcal{S}$ est N2C. □

Cette notion est la première interprétation géométrique des codes intersectants. De la même manière que la notion d'ensemble générateur d'hyperplans permet de montrer plusieurs propriétés des codes minimaux, le développement de la théorie des ensembles N2C permet de montrer facilement beaucoup de propriétés simples des codes intersectants.

Proposition 4.2.3. Soit $\mathcal{L}$ un ensemble de droites dispersées et soit $\mathcal{S} \subset \mathrm{PG}(k-1, q)$ tel que pour tout $\ell \in \mathcal{L}$,

$$|\mathcal{S} \cap \ell| \geq 3.$$

Alors $\mathcal{S}$ est N2C.

Preuve. Supposons par l'absurde qu'il existe deux hyperplans $\mathcal{H}, \mathcal{H}' \subset \mathrm{PG}(k-1, q)$ tels que $\mathcal{S} \subset \mathcal{H} \cup \mathcal{H}'$. Notons $\mathcal{V} = \mathcal{H} \cap \mathcal{H}'$. Puisque $\mathcal{V}$ est de codimension 2 et puisque $\mathcal{L}$ est un ensemble de droites dispersées, il existe une droite $\ell \in \mathcal{L}$ telle que $\ell \cap \mathcal{V} = \varnothing$.

Examinons à présent l'intersection de ℓ avec les hyperplans $\mathcal{H}$ et $\mathcal{H}'$. Cette intersection est nécessairement non nulle, mais seuls deux cas de figure sont possibles: soit $\ell \subset \mathcal{H}$, auquel cas $|\ell \cap \mathcal{H}| = q+1$, soit $|\ell \cap \mathcal{H}| = 1$. Le premier de ces deux cas est impossible. En effet, si $\ell \subset \mathcal{H}$, alors $\ell \cap \mathcal{V} \neq \varnothing$, une contradiction. Par conséquent $|\ell \cap \mathcal{H}| = 1$, et de même $|\ell \cap \mathcal{H}'| = 1$.

Puisque $|\mathcal{S} \cap \ell| \geq 3$, il existe nécessairement un point $P \in \mathcal{S}$ qui n'est pas contenu dans l'union des hyperplans $\mathcal{H} \cup \mathcal{H}'$. Par conséquent l'ensemble de points $\mathcal{S}$ est bien N2C. □

4.2.1 Bornes sur les paramètres des codes intersectants

Il est désormais possible de donner des preuves géométriques de quelques résultats que nous avons déjà obtenus. Ces preuves viennent compléter notre compréhension des codes intersectants.

Théorème 4.2.4. Soit $\mathcal{C}$ un $[n, k, d]_q$-code intersectant. Alors

$$k \leq d.$$

Preuve. Soit $\mathcal{S} \in \mathrm{PG}(k-1, q)$ l'ensemble de points obtenu à partir d'une matrice génératrice de $\mathcal{C}$. Puisque la distance minimale du code est d, le nombre minimal de points en dehors d'un hyperplan est également d. Soit $\mathcal{H}$ un hyperplan tel que $|\mathcal{S} \setminus (\mathcal{S} \cap \mathcal{H})| = d$. Il existe un hyperplan $\mathcal{H}'$ qui contient les d points qui restent si $d \leq k-1$. Pour que $\mathcal{S}$ soit N2C, il faut donc que $d \geq k$. □

Théorème 4.2.5. Soit $\mathcal{C}$ un $[n,k,d]_q$-code intersectant. Alors

$$n \geq 2k-1.$$

Preuve. Soit $\mathcal{S} \in \mathrm{PG}(k-1,q)$ l'ensemble de points obtenu à partir d'une matrice génératrice de $\mathcal{C}$. Si $n \leq 2(k-1)$, il est possible de prendre un hyperplan $\mathcal{H}$ passant par les $k-1$ premiers points, et un autre hyperplan $\mathcal{H}'$ passant par les $k-1$ autres points. On aurait alors $\mathcal{S} \subset \mathcal{H} \cup \mathcal{H}'$, ce qui est impossible car $\mathcal{S}$ est N2C. Par conséquent $n \geq 2k-1$ par l'absurde. □

Notons qu'il est également possible de montrer ce théorème en utilisant la borne de Singleton et l'inégalité $k \leq d$.

De la même manière que pour les ensembles générateurs d'hyperplans, on notera que les ensembles N2C sont stables par inclusion: si $\mathcal{S} \subset \mathcal{S}' \subset \mathrm{PG}(k-1,q)$ et que $\mathcal{S}$ est N2C, alors $\mathcal{S}'$ l'est aussi. Il est donc naturel de se demander quels sont les plus petits ensembles N2C possibles, ou, de manière équivalente, quelle est la plus petite longueur admissible d'un code intersectant de dimension k donnée.

Définition 4.2.6. La plus petite longueur d'un code intersectant de dimension k sur $\mathbb{F}_q$ est notée $i(k,q)$. Il s'agit également du plus petit cardinal d'un ensemble N2C de $\mathrm{PG}(k-1,q)$.

Le Théorème 4.2.5 peut se reformuler de la façon suivante: $i(k,q) \geq 2k-1$. Notons également que quand $q=2$, les codes intersectants coïncident avec les codes minimaux. On a donc $i(k,2) = m(k,2)$ pour tout $k \geq 2$.

Il est possible d'adapter la borne probabiliste que nous avons rencontrée dans le chapitre précédent au cas des codes intersectants.

Théorème 4.2.7. Si

$$n \geq \frac{2}{\log_q(\frac{q^2}{2q-1})}\ k$$

alors il existe un $[n,k,d]_q$-code intersectant. Par conséquent on a

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq \frac{2}{\log_q(\frac{q^2}{2q-1})}.$$

Preuve. Notons

$$\mathcal{B}_n = \{\{x,y\} \subseteq \mathbb{F}_q^n \mid \sigma(x) \cap \sigma(y) = \emptyset\}.$$

Pour chaque coordonnée $i \in \{1,\ldots,n\}$ d'une paire de vecteurs $\{x,y\}$ de $\mathcal{B}_n$ il y a trois possibilités:

$$(x_i \neq 0 \wedge y_i = 0) \vee (x_i = 0 \wedge y_i \neq 0) \vee (x_i = 0 \wedge y_i = 0).$$

On en déduit $|\mathcal{B}_n| = (2(q-1)+1)^n = (2q-1)^n$.

Notons

$$\mathcal{F}_{n,k} = \{\mathcal{C} \subseteq \mathbb{F}_q^n \mid \dim \mathcal{C} = k\},$$

dont le cardinal est clairement $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Chaque paire de vecteurs de $\mathcal{B}_n$ est contenue dans exactement $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q$ éléments de $\mathcal{F}_{n,k}$. Un code de $\mathcal{F}_{n,k}$ est intersectant si et seulement s'il ne contient aucun élément de $\mathcal{B}_n$. Puisqu'il y a au plus

$$(2q-1)^n \cdot \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q$$

codes de $\mathcal{F}_{n,k}$ qui contiennent un élément de $\mathcal{B}_n$, si

$$(2q-1)^n \cdot \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q \leq \begin{bmatrix} n \\ k \end{bmatrix}_q$$

alors il existe des codes intersectants de paramètres $[n,k]_q$. Un calcul direct montre que cela est impliqué par $q^{n\log_q(2q-1)+2(k-n)} \leq 1$, d'où le résultat. □

On en déduit immédiatement le corollaire suivant.

Corollaire 4.2.8. La famille des codes intersectants est asymptotiquement bonne.

Preuve. Le Théorème 4.2.7 et le Théorème 4.2.4 montrent qu'il existe une famille de codes intersectants de paramètres

$$\left[\frac{2}{\log_q(\frac{q^2}{2q-1})} \; k, d \geq k \right]_q.$$

Cette famille est clairement asymptotiquement bonne. □

Remarque 4.2.9. Notons que $\frac{2}{\log_q(\frac{q^2}{2q-1})} \sim 2 + 2/\ln(q)$.

4.2.2 Bornes inférieures asymptotiques

Notons que d'après le Théorème 4.1.4, les paramètres d'un code intersectant doivent être dans la région

$$\{(\delta, R) \in \mathbb{R}^2_{\geq 0} \mid R \leq \delta\}.$$

De manière équivalente, la fonction $g(x) = x$ est une fonction majorante q-aire pour les codes intersectants.

Similairement à notre travail sur les codes minimaux, nous pouvons utiliser cette méthode pour donner des bornes inférieures sur $\liminf_{k\to\infty} \frac{i(k,q)}{k}$.

Théorème 4.2.10.

$$\liminf_{k\to\infty} \frac{i(k,q)}{k} \geq 2 + \frac{1}{q-1}.$$

Preuve. La borne de Plotkin asymptotique [39, Theorem 2.10.2] correspond à la fonction majorante q-aire

$$f(x) = 1 - \frac{q}{q-1}\, x.$$

L'intersection des graphes de cette fonction et de g est le point $\left(\frac{q-1}{2q-1}, \frac{q-1}{2q-1}\right)$. Ce point induit une borne supérieure sur le taux d'information d'un code intersectant et donne donc la borne voulue. □

Remarque 4.2.11. Il est également possible de prouver ce résultat directement à partir du Théorème 4.1.6, en faisant tendre t vers l'infini.

En utilisant la borne MRRW [39, Theorem 2.10.6] au lieu de la borne de Plotkin, il est possible de montrer une borne supérieure plus forte. Contrairement au cas des codes minimaux, cette borne sera meilleure seulement quand $q \leq 17$.

Théorème 4.2.12. La borne MRRW donne une meilleure borne supérieure sur le taux d'information des codes intersectants que la borne de Plotkin quand $q \leq 17$. En d'autres termes, si et seulement si $q \geq 19$, on a:

$$M_q\left(\frac{q-1}{2q-1}\right) \geq \frac{q-1}{2q-1}.$$

Preuve. La preuve de ce résultat est une adaptation de la preuve du Théorème 3.3.8.

On rappelle que la borne MRRW correspond à la fonction majorante q-aire

$$M_q(x) = H_q\left(\frac{1}{q}\left(q - 1 - (q-2)x - 2\sqrt{(q-1)x(1-x)}\right)\right),$$

où

$$H_q(x) = -x \log_q\left(\frac{x}{q-1}\right) - (1-x)\log_q(1-x)$$

est l'entropie q-aire.

Nous commençons par calculer $A(x) = \frac{1}{q}\left(q - 1 - (q-2)x - 2\sqrt{(q-1)x(1-x)}\right)$ avec $x = \frac{q-1}{2q-1}$. Cela donne

$$A\left(\frac{q-1}{2q-1}\right) = \frac{(q-1)(\sqrt{q}-1)^2}{q(2q-1)}.$$

Nous voulons déterminer pour quelles valeurs de q on a

$$M_q\left(\frac{q-1}{2q-1}\right) \geq \frac{q-1}{2q-1}.$$

Pour simplifier la notation, notons $B(q) = q(2q-1) - (q-1)(\sqrt{q}-1)^2$, $C(q) = (2q-1)q$ et $D(q) = (q-1)(\sqrt{q}-1)^2$, et posons $g(x) = x\log_q(x)$. Notons que $B(q)$, $C(q)$ et $D(q)$ sont

tous positifs. Un calcul direct montre que l'inégalité ci-dessus équivaut à

$$g(B(q)) - (q-1)g\left(\frac{D(q)}{q-1}\right) + g(C(q)) \geq q(q-1).$$

Puisque g est convexe, et puisque $D(q) = C(q) - B(q)$, nous pouvons affirmer la borne suivante:

$$g(C(q)) - g(B(q)) \geq D(q)g'(B(q)) = D(q)\log_q(eB(q)).$$

Il suffit donc d'établir

$$D(q)\log_q(eB(q)) - D(q)\log_q((\sqrt{q}-1)^2) \geq q(q-1)$$

ce qui se simplifie pour donner

$$(\sqrt{q}-1)^2 \log_q\left(\frac{eB(q)}{(\sqrt{q}-1)^2}\right) \geq q.$$

Puisque $(\sqrt{q}-1)^2 \leq q$, pour que l'inégalité soit vérifiée il suffit de montrer que

$$\begin{aligned}(\sqrt{q}-1)^2 \log_q\left(\frac{eB(q)}{q}\right) &\geq q \\ (\sqrt{q}-1)^2 \log_q(eq) &\geq q \\ q &\geq 2\sqrt{q}(\ln(q)+1) \\ 1 + \frac{1}{2}\cdot\sqrt{q} &\geq \ln(q)\end{aligned}$$

En notant $f(x) = 1 + \frac{1}{2}\cdot\sqrt{x} - \ln(x)$, on vérifie aisément que f est croissante pour $x \geq 16$.

En particulier, on montre aisément que $f(144) > 0$, c'est-à-dire que dès que $q \geq 144$ on a bien

$$M_q\left(\frac{q-1}{2q-1}\right) \geq \frac{q-1}{2q-1}.$$

Pour les valeurs restantes de q, à savoir $19 \leq q \leq 144$, le théorème peut être vérifié par un calcul direct. □

Dans le Tableau 4.1 ci-dessous, nous restituons les meilleures bornes inférieures obtenues avec le Théorème 4.2.12.

q	$\liminf_{k\to\infty} \frac{i(k,q)}{k}$
2	3.5276
3	2.8272
4	2.5713
5	2.4342
7	2.2862
8	2.2411
9	2.2060
11	2.1547
13	2.1185
16	2.0802
17	2.0703

Table 4.1: Borne inférieure sur la longueur asymptotique des codes intersectants

Remarque 4.2.13. Dans le cas particulier $q = 2$, cette borne est déjà donnée dans [25]. Il est donc possible de comprendre le Théorème 4.2.12 comme une généralisation de ce résultat.

En plus de la borne de Plotkin et la borne MRRW, il est possible d'utiliser une borne donnée par Aaltonen dans [2, (8)], qui correspond à la fonction majorante q-aire

$$A(x) = 1 - \frac{q}{q-2}\log_q(q-2)x.$$

La borne inférieure asymptotique que l'on en déduit sur $i(k,q)$ est meilleure que celle des deux précédentes propositions dès que $q \geq 16$.

Théorème 4.2.14.

$$\liminf_{k\to\infty} \frac{i(k,q)}{k} \geq 1 + \frac{q\log_q(q-2)}{q-2}.$$

Preuve. La preuve est identique à celle du Théorème 4.2.10. □

4.3 Constructions explicites

4.3.1 Quelques constructions élémentaires

Exemple 4.3.1 (Arcs avec au moins $2k-1$ points). Un *arc* de $\mathrm{PG}(k-1,q)$ est un ensemble de points avec la propriété que n'importe quel sous-ensemble de k d'entre eux engendrent $\mathrm{PG}(k-1,q)$ tout entier. Il est connu que les arcs de $\mathrm{PG}(k-1,q)$ correspondent aux codes MDS de dimension k sur $\mathbb{F}_q$. Un arc $\mathcal{A}$ avec au moins $2k-1$ points est nécessairement N2C: le nombre maximal de points de $\mathcal{A}$ contenus dans n'importe quel hyperplan est $k-1$, par définition. Par conséquent, si $|\mathcal{A}| > 2(k-1)$, pour toute paire d'hyperplans $\mathcal{H}_1, \mathcal{H}_2$ il existe toujours un point de $\mathcal{A}$ qui n'est pas contenu dans $\mathcal{H}_1 \cup \mathcal{H}_2$.

Exemple 4.3.2 (Le tétraèdre clairsemé[1])**.** Considérons k points $V_1, \dots, V_k$ de $\mathrm{PG}(k-1,q)$ en position générale (i.e. qui engendrent $\mathrm{PG}(k-1,q)$ tout entier). Pour tous $i,j \in \{1,\dots,k\}, i < j$, prenons un point $P_{i,j}$ sur la droite $\langle V_i, V_j\rangle$, $P_{i,j} \notin \{V_i, V_j\}$. L'ensemble

$$\mathcal{T} = \{V_1,\dots,V_k\} \cup \{P_{i,j} \mid i,j \in \{1,\dots,k\}, i<j\}$$

est appelé *tétraèdre clairsemé*.

Un tel ensemble est N2C. En effet, l'intersection de $\mathcal{T}$ avec n'importe quel hyperplan $\mathcal{H}$ ne peut pas contenir tous les points $V_1,\dots,V_k$. Si $\mathcal{T}\cap\mathcal{H}$ ne contient pas V_i, en particulier, il ne contient pas non plus n'importe quelle droite passant par V_i, et en particulier aucune des droites $\langle V_i, V_j\rangle$. Pour chacune de ces droites, il y a au moins un point distinct de V_i qui n'est pas contenu dans $\mathcal{H}$ (sinon la droite entière serait contenue dans $\mathcal{H}$). Par conséquent nous avons identifié un ensemble de points qui ne sont pas contenus dans $\mathcal{H}$ et qui engendrent tout l'espace. Cela signifie qu'aucun autre hyperplan $\mathcal{H}'$ ne pourra couvrir tous les points restants à lui seul, ce qui implique que le tétraèdre clairsemé est N2C.

Nous nous sommes également intéressés aux petites valeurs de la fonction $i(k,q)$, dont nous donnons un résumé dans le Tableau 4.2 ci-dessous. Quand nous écrivons $[n_1,n_2]$, cela signifie que $i(k,q)$ est inconnu mais est contenu dans cet intervalle. Les couleurs indiquent l'argument utilisé pour établir la borne inférieure ou supérieure.

Table 4.2: Valeurs de $i(k,q)$ pour de petits q et k

q \ k	2	3	4	5	6	7	8	9
2	3	6	9	13	15	20	24	26
3	3	6	9	10	13	[17, 18]	[19, 21]	[21, 30]
4	3	5	8	10	[12, 13]	[15, 16]	[17, 21]	[21, 25]
5	3	5	8	10	[12, 13]	[15, 17]	[18, 21]	[20, 25]
7	3	5	7	10	[12, 13]	14	[17, 21]	[19, 25]
8	3	5	7	9	[12, 13]	[14, 15]	[16, 21]	[19, 25]
9	3	5	7	9	12	[14, 15]	[16, 21]	[18, 25]

Pour la première ligne du Tableau 4.2, nous citons le travail de Kurz dans [42], où ces valeurs sont données dans le contexte des codes minimaux.

Les bornes inférieures sont toutes en bleu et sont tirées du Théorème 4.1.4 et de l'archive des codes avec les meilleurs paramètres connus dans Magma. Les bornes supérieures en orange [2] sont obtenues avec des constructions utilisant de la concaténation et le Lemme 4.1.5. Les bornes en vert [3] viennent de recherche exhaustive en Magma, en prenant un $[n,k-1,d]_q$-

[1] A mon sens, c'est la plus belle traduction possible de l'anglais "sparse".
[2] i.e. les bornes supérieures dans les colonnes $k=8$ et $k=9$
[3] i.e. les bornes supérieures dans les colonnes $k=6$ et $k=7$

code intersectant optimal et en construisant un $[n, k, d]_q$-code aléatoire à partir du premier, ou en prenant tout simplement les codes avec les meilleurs paramètres connus en MAGMA.

4.3.2 Graphes expanseurs

Dans cette partie, nous allons adapter la construction explicite de codes minimaux obtenue dans [8] et présentée au chapitre précédent au cas des codes intersectants. Nous construirons une suite explicite de codes intersectants asymptotiquement bons.

Cette suite est moins bonne que celle utilisant des codes AG présentée juste après, mais je choisis de la présenter pour deux raisons. La première est que la construction explicite de codes intersectants que je présenterai au prochain chapitre s'inspire fortement de celle-ci. La seconde est que cette construction est une construction géométrique, dans le sens où l'on construit directement un ensemble générateur d'hyperplans.

Théorème 4.3.3. Supposons qu'il existe une construction de $[n, Rn, \delta n]_q$-systèmes projectifs et un entier t tel que

$$\frac{t - 2\sqrt{t-1}}{t + 2\sqrt{t-1}} > 1 - \delta.$$

Alors il existe une famille *explicite* d'ensembles N2C de cardinal tendant vers

$$\left(1 + \frac{t}{2}\right) n,$$

quand $n \to \infty$.

Preuve. Soit $\varepsilon > 0$ et choisissons $n \geq n_0(t, \varepsilon)$ de manière à ce que nt soit pair. Notons $\mathcal{M}$ le $[n, Rn, \delta n]_q$-système projectif. D'après le Théorème 3.5.6, il existe une construction explicite d'un (n, t, λ)-graphe avec $\lambda = 2\sqrt{t-1} + \varepsilon$. Notons ce graphe $\mathcal{G}_{n,t} = (V_{n,t}, E_{n,t})$. Selon nos hypothèses on peut choisir ε suffisamment petit et n suffisamment grand pour avoir

$$\frac{t - \lambda}{t + \lambda} \geq 1 - \delta + \frac{1}{n}.$$

Par conséquent $\mathcal{L}(\mathcal{M}, \mathcal{G}_{n,t})$ est un ensemble de droites dispersées.

D'après la Proposition 4.2.3, en prenant 3 points sur chaque droite de $\mathcal{L}(\mathcal{M}, \mathcal{G}_{n,t})$, on obtient un ensemble N2C. Pour obtenir le plus petit ensemble N2C, on sélectionne chaque sommet ainsi qu'un point de chaque droite (différent des sommets du graphe) de $\mathcal{G}_{n,t}$. Cela donne $n + nt/2$ points. □

Donnons un exemple d'application du Théorème 4.3.3. Par souci de simplicité, nous ne considérerons que le cas où q est un carré, parce que les codes AG sont alors optimaux, et la formule pour le défaut de Singleton est la plus simple (ce qui facilite les calculs). Considérons

une famille de codes AG de paramètres $[n, Rn, \delta n]_q$ telle que

$$R + \delta = 1 - \frac{1}{\sqrt{q} - 1}.$$

Notons que le cardinal de l'ensemble N2C ainsi obtenu est

$$\left(1 + \frac{t}{2}\right) n = \frac{1 + t/2}{R} \cdot k,$$

où k est la dimension du code AG. D'après le Théorème 4.3.3, t doit satisfaire

$$\frac{t - 2\sqrt{t-1}}{t + 2\sqrt{t-1}} > 1 - \delta = R + \frac{1}{\sqrt{q} - 1}.$$

En posant

$$R(q, t) = \frac{t - 2\sqrt{t-1}}{t + 2\sqrt{t-1}} - \frac{1}{\sqrt{q} - 1}$$

et

$$\alpha(q, t) = \frac{1 + t/2}{R(q, t)},$$

notre objectif est de minimiser la valeur de $\alpha(q, t)$. Notons que puisque t est le degré d'un somme, on doit avoir $t \in \mathbb{N}$, ce qui limite significativement nos moyens d'optimisation à q fixé.

Quand $q \to \infty$, le second terme dans l'expression de $R(q, t)$ tend vers 0. Cela donne une expression explicite de $\alpha(q, t)$ qui ne dépend pas de q, et pour laquelle on vérifie aisément que la valeur minimale est atteinte pour $t = 10$. On obtient donc une construction explicite d'ensembles N2C avec

$$R(q, 10) = \frac{1}{4} - \frac{1}{\sqrt{q} - 1}$$

et

$$\alpha(q, 10) = \frac{6}{R(q, 10)} \to 24,$$

quand $q \to \infty$.

En calculant la valeur de $\alpha(q, t)$ quand t est entier, on peut vérifier que pour $q \geq 89^2$, $t = 10$ donne la plus petite valeur de $\alpha(q, t)$. Pour de plus petites valeurs de q, les meilleurs valeurs de t et de $\alpha(q, t)$ sont données dans le Tableau 4.3. Pour $q = 4$ le défaut de Singleton est 1 donc $R > 0$ est impossible, ce qui implique que notre construction est inefficace dans ce cas.

4.3.3 Codes AG

Dans cette partie, nous présentons la meilleure construction explicite de codes intersectants que nous connaissons. L'idée de base, due à Xing, est la suivante.

q	t	$\alpha(q,t)$
3^2	86	299.5378
4^2	39	110.0490
5^2	27	71.8927
7^2	20	48.6300
8^2	18	43.7121
9^2	17	40.4255
11^2	15	36.2747
13^2	14	33.7937
16^2	13	31.5103
$17^2 \leq q \leq 19^2$	13	~ 30
$23^2 \leq q \leq 27^2$	12	~ 28
29^2	12	27.7441
$31^2 \leq q \leq 32^2$	11	~ 27
$37^2 \leq q \leq 49^2$	11	~ 26
$53^2 \leq q \leq 83^2$	11	~ 25

Table 4.3: Plus petites valeurs de $\alpha(q,t)$ pour q carré et petit

Théorème 4.3.4 (Critère de Xing, [68] Théorème 3.5, avec $s = 2$)**.** Soit X une courbe algébrique et $D \in Div(X)$ de degré $\deg(D) < n$. Supposons que

$$l(2D - G) = 0,$$

où $G \in Div(X)$ a support disjoint de P. Alors le code de Goppa $C(G, D)$ a dimension $l(D)$ et est intersectant.

En s'appuyant sur ce résultat, dans [58], Randriambololona établit le résultat suivant.

Théorème 4.3.5 (Theorem 2, [58])**.** Supposons que $A(q) \geq 4$. Alors il existe une famille asymptotiquement bonne de codes intersectants de taux d'information

$$R = \frac{1}{2} - \frac{1}{2A(q)}.$$

Remarque 4.3.6. La preuve du Théorème 4.3.5 repose sur des arguments complexes de géométrie algébrique. Une manière plus simple de construire des codes AG intersectants serait de considérer des familles de codes AG avec $\delta > 1/2$, qui sont intersectants d'après le Lemme 4.1.3. Le meilleur taux d'information possible en utilisant cette méthode est

$$R = \frac{1}{2} - \frac{1}{A(q)}.$$

Par conséquent, le Théorème 4.3.5 peut être vu comme une amélioration de cette méthode plus simple.

Le Théorème 4.3.5 donne souvent la meilleure construction explicite connue de codes intersectants sur $\mathbb{F}_q$. Cependant, quand q est petit, ou un nombre premier, $A(q) \leq 4$. Dans ces cas, il devient nécéssaire d'utiliser de la concaténation pour construire des familles explicites de codes intersectants asymptotiquelent bons.

Remarque 4.3.7. Avant de rentrer dans les détails, il est important de faire une observation supplémentaire. Le plus haut taux d'information d'un code intersectant non trivial est atteint par le code de paramètres $[3, 2, 2]_q$ (sur n'importe quel corps $\mathbb{F}_q$), qui correspond à trois points distincts sur la droite projective. De plus, un code AG intersectant construit avec le théorème ci-dessus doit avoir un taux d'information inférieur à $1/2$. Cela signifie en particulier que toute concaténation d'un code intersectant non-trivial avec une famille de codes AG intersectants produit une famille de codes intersectants dont le taux d'information est au plus $1/3$. Par conséquent, si sur un corps $\mathbb{F}_q$ il existe une famille de codes AG intersectants dont le taux d'information est supérieur à $1/3$, alors aucune construction utilisant de la concaténation ne pourra produire une famille de codes intersectants à taux plus élevé.

Avec ces quelques remarques, nous sommes enfin prêts pour notre théorème.

Théorème 4.3.8. Les bornes suivantes, issues de constructions *explicites* (utilisant parfois de la concaténation), sont vérifiées:

- Si q est un carré et $q \geq 25$, alors
$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq 2 + \frac{2}{\sqrt{q}-2};$$
- Si $q = p^{2m+1}$ est une puissance impaire d'un nombre premier (avec $m \geq 1$, c'est-à-dire que q n'est pas premier) et si $q \geq 32$, alors
$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq \frac{4}{2 - \frac{1}{p^m-1} - \frac{1}{p^{m+1}-1}},$$
- Si q est un nombre premier vérifiant $q \geq 11$, alors
$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq 3 + \frac{3}{q-2}.$$

Pour les valeurs restantes de q, les bornes sont indiquées dans le Tableau 4.4, avec les paramètres du code interne utilisé pour faire la concaténation avec des codes AG.

Remarque 4.3.9 (Comparaison avec la borne probabiliste du Théorème 4.2.7)**.** Les bornes du Théorème 4.3.8 sont plus fortes que la borne probabiliste dans les cas suivants:

q	Paramètres du code interne	Borne supérieure pour $\limsup_{k\to\infty} i(k,q)/k$	Borne probabiliste
2	$[15,6]_2$	5.8334	4.8189
3	$[10,5]_3$	4.3561	3.7382
4	$[5,3]_4$	4.1667	3.3539
5	$[5,3]_5$	3.9025	3.1507
7	$[7,4]_7$	3.5745	2.9331
8	$[3,2]_8$	3.5	2.8666
9	$[3,2]_9$	3.4286	2.8148
16	$[3,2]_{16}$	3.2143	2.6266
27	$[3,2]_{27}$	3.12	2.5146

Table 4.4: Bornes supérieures obtenues avec des codes AG pour les valeurs exceptionnelles de q

- si $q \geq 49$ est un carré;
- si $q \geq 128$ est une puissance impaire d'un premier.

Par conséquent les bornes supérieures asymptotiques issues du Théorème 4.3.8 sont les meilleurs pour presque toutes les cas où q n'est pas premier. De plus, ces bornes supérieures asymptotiques sont *constructives* : les codes qui les atteignent peuvent être construits explicitement en temps polynomial, comme explicité dans [58].

Remarque 4.3.10. Dans le cas binaire, les codes intersectants coïncident avec les codes minimaux. Nous avons exposé beaucoup de constructions explicites de codes minimaux asymptotiquement bons, et le lecteur intéressé peut les examiner dans [8,11,27]. A ma connaissance, la construction explicite la plus courte est celle de Cohen et Zémor [27]. La construction donnée dans le Tableau 4.4 est une amélioration et représente à ma connaissance la plus courte construction *explicite* de codes minimaux sur $\mathbb{F}_2$.

4.4 Liens avec la constante de Davenport

Dans cette section, nous explicitons le lien entre les codes intersectants et la constante de Davenport.

4.4.1 L'action multiplicative de $\mathbb{F}_q$

Si la constante de Davenport d'un groupe de la forme C_2^r a bien une interprétation en termes de théorie des codes, ce n'est pas naturellement le cas quand nous parlons de codes sur $\mathbb{F}_q$ en général. Dans cette partie notre objectif est de généraliser le théorème suivant.

La constante de Davenport d'un groupe de la forme C_2^r a une interprétation naturelle en termes de théorie des codes, la voici.

Soit $H \in \mathcal{M}_{r\times n}(\mathbb{F}_2)$ la matrice de parité d'un $[n, n-r]_2$-code $\mathcal{C}$. Un mot de code de $\mathcal{C}$ correspond naturellement à une suite à somme nulle de colonnes de H, qui sont des éléments de $\mathbb{F}_2^r \simeq C_2^r$.

Cette remarque n'est pas originale, elle fait par exemple déjà l'objet de discussions dans [57] et dans [28].

On note aisément qu'il existe deux sous-suites à somme nulle disjointes si et seulement s'il existe deux mots de codes non intersectants. Ainsi, la valeur de la constante de Davenport double $\mathrm{D}_2(C_2^r)$ est exactement la plus grande longueur n d'un code de dimension $n-r$ sur $\mathbb{F}_2$ qui ne soit pas intersectant. Quand n devient petit, le rapport $n/(n-r)$ grandit, et à partir d'un moment, il commence à y avoir des codes intersectants. La valeur de $\mathrm{D}_2(C_2^r)$ est le plus petit entier n tel qu'il n'y a pas de codes intersectants (et donc l'existence de deux sous-suites à somme nulle disjointes). Nous venons donc d'établir le théorème suivant.

Théorème 4.4.1.

$$\mathrm{D}_2(C_2^r) = \min\{m \geq r+1 \mid m < i(m-r, 2)\}.$$

Si nous voulons préserver cette relation entre la constante de Davenport et la théorie des codes, nous devons introduire un système de poids pour la constante de Davenport.

Soit p un nombre premier, et examinons une matrice de parité H d'un code $\mathcal{C}$ de paramètres $[n, n-r]_p$. Pour les mêmes raisons que précédemment, un mot de code de $\mathcal{C}$ correspond à une suite à somme nulle de colonnes de H pondérée par des poids dans $\{0, 1, \ldots, p-1\}$. On comprend aisément le sens d'un tel système de poids (selon l'introduction à la Section 2.3) en termes de répétitions de colonnes.

A ce stade, on devine aisément le lien entre les codes intersectants sur $\mathbb{F}_p$ et la constante de Davenport. Avant de l'énoncer explicitement, il convient d'en introduire une généralisation que nous n'avons pas abordée dans le cadre de la Section 2.3.

Définition 4.4.2. Soit $j \in \mathbb{N}$ un entier strictement positif, G un groupe abélien fini, et $A = \{1, \ldots, \exp(G) - 1\}$. La constante d'ordre 2 de Davenport maximalement pondérée de G, notée $\mathrm{D}_2^f(G)$, est le plus petit entier ℓ tel que pour toute suite de ℓ éléments $a_1, \ldots, a_\ell$ de G, il existe j sous-suites disjointes à somme nulle A-pondérées, de la forme

$$\sum_{i=1}^{r} \varepsilon_i a_{j_i} = 0_G,$$

où les ε_i sont des éléments de A.

Cette constante de Davenport est étudiée dans [47], avec une attention particulière portée aux cas particuliers correspondant à quelques valeurs petites de p.

Avec cette définition, on obtient sans peine le théorème suivant, par analogie avec le cas particulier où G est de la forme C_2^r, qui correspond au Théorème 4.4.1.

Théorème 4.4.3. Soit p un nombre premier. On a

$$\mathrm{D}_2^f(C_p^r) = \min\{m \geq r+1 \mid m < i(m-r,p)\}.$$

Si l'on veut maintenant poursuivre ce raisonnement avec les codes intersectants sur $\mathbb{F}_q$, où $q = p^h$, on se heurte à la difficulté suivante: les coefficients de $\mathbb{F}_q$ ne peuvent pas être interprétés comme des répétitions d'éléments de C_p^{hr} lorsque q n'est pas premier. Par conséquent, il faut introduire une notion de poids plus générale encore que les "poids maximaux" qui correspondent à l'ensemble $A = \{1, \ldots, \exp(G) - 1\}$.

4.4.2 Notre généralisation

Nous sommes à présent en mesure de définir correctement et précisément notre généralisation de la constante de Davenport pleinement pondérée. Nous commençons par rappeler la définition de la constante de Davenport $\mathcal{W}$-pondérée, où $\mathcal{W}$ est un ensemble non vide d'endomorphismes de G. Elle a été introduite pour la première fois dans [70], et le lecteur intéressé pourra également consulter [36].

Définition 4.4.4. Soit G un groupe abélien fini et soit $\mathcal{W}$ un ensemble non vide d'endomorphismes de G, que nous appelons un *ensemble de poids* pour G. Soit $a_1, \ldots, a_n \in G$ une suite d'éléments de G. Une sous-suite à somme nulle $\mathcal{W}$-pondérée est une suite $a_{i_1}, \ldots, a_{i_r}$, avec $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, vérifiant

$$\sum_{j=1}^{r} \varepsilon_i(a_{i_j}) = 0,$$

où $\varepsilon_i \in \mathcal{W}$.

Définition 4.4.5. Soit $j \in \mathbb{N} \setminus \{0\}$. La constante de Davenport $\mathcal{W}$-pondérée d'ordre j, notée $\mathrm{D}_j^{\mathcal{W}}(G)$, est le plus petit entier ℓ tel que toute suite de ℓ éléments de G ait j sous-suites à somme nulle $\mathcal{W}$-pondérée disjointes.

Similairement, la petite constante de Davenport $\mathcal{W}$-pondérée d'ordre j, notée $\mathrm{d}_j^{\mathcal{W}}(G)$, est le plus grand entier ℓ tel qu'il existe une suite de ℓ éléments de G qui n'ait pas j sous-suites à somme nulle $\mathcal{W}$-pondérée.

Si G est un p-groupe abélien élémentaire d'ordre p^{hr}, c'est-à-dire quand

$$G = E_{p^{hr}} = \underbrace{C_p \oplus \ldots \oplus C_p}_{hr \text{ times}},$$

le groupe abélien élémentaire d'ordre p^{hr} (ici p est un nombre premier et h et r sont des entiers strictement positifs), il est possible de considérer un isomorphisme de groupes $E_{p^{hr}} \cong \mathbb{F}_q^r$, où

$q = p^h$. Bien évidemment, un tel isomorphisme ne concerne que la partie additive. Plus bas, nous utilisons l'action scalaire de $\mathbb{F}_q$ sur $\mathbb{F}_q^r$ pour introduire un ensemble de poids qui peut être vu comme la généralisation des poids maximaux pour les groupes abéliens d'ordre p étudiés plus haut dans le cas des p-groupes abéliens élémentaires.

Définition 4.4.6. Pour $G = E_{p^{hr}}$ un groupe abélien élémentaire d'ordre p^{hr}, considérons un isomorphisme de groupes $\varphi : E_{p^{hr}} \to \mathbb{F}_q^r$. Notons

$$\mathcal{Q}_h = \{m_x : y \mapsto \varphi^{-1}(x\varphi(y)) \in \mathrm{End}(E_{p^{hr}}) \mid x \in \mathbb{F}_q\}$$

l'ensemble des poids induits par la multiplication scalaire de $\mathbb{F}_q = \mathbb{F}_{p^h}$.

Si l'ensemble de poids $\mathcal{Q}_h$ dépend en principe de notre choix d'isomorphisme φ, il est clair que ce n'est pas le cas pour la valeur des constantes de Davenport associées. C'est pourquoi nous n'incluons pas φ dans l'écriture de $\mathcal{Q}_h$.

Plus bas nous étudions la constante de Davenport $\mathcal{Q}_h$-pondérée $\mathrm{D}_j^{\mathcal{Q}_h}(E_{p^{hr}})$. Pour simplifier la notation, nous la notons simplement $\mathrm{D}_j^h(E_{p^{hr}})$.

Remarque 4.4.7. La constante de Davenport maximalement pondérée de $\mathcal{C}_p^r$ est exactement $r+1$. En effet, on peut voir ce problème comme un problème d'algébre linéaire sur $\mathbb{F}_p^r$, où il existe une base de cardinal r mais $r+1$ vecteurs sont nécéssairement liés.

Théorème 4.4.8. Soit $E_{p^{hr}}$ le groupe abélien élémentaire d'ordre p^{hr}, où p est premier et h, r sont des entiers positifs. Alors $\mathrm{D}_2^h(E_{p^{hr}})$ est le plus petit entier n tel que tous les $[n, n-r]_{p^h}$ codes ne sont pas intersectants. Par conséquent

$$\mathrm{D}_2^h(E_{p^{hr}}) = \min\{m \geq r+1 \mid m < i(m-r, p^h)\}.$$

Preuve. Soit $m = \mathrm{D}_2^h(E_{p^{hr}}) - 1$. Par définition, il existe une suite $a_1, \ldots, a_m \in E_{p^{hr}}$ qui n'admet pas deux sous-suites à somme nulle pondérées disjointes. Notons que m doit être supérieur à r d'après la Remarque 4.4.7. Avec l'isomorphisme $E_{p^{hr}} \cong \mathbb{F}_{p^h}^r$, chaque a_i peut être vu comme un vecteur colonne Soit H la matrice définie par

$$H = \left[\begin{array}{c|c|c} & & \\ a_1 & \cdots & a_m \\ & & \end{array}\right].$$

La matrice H est de rang maximal, parce que sinon il y aurait une suite de longueur $\mathrm{D}_2^h(E_{p^{hr}})$ qui n'admet pas deux sous-suites à somme pondérée nulle disjointes, ce qui contredit la définition: il suffit de considérer $b \notin \langle a_1, \ldots, a_m \rangle$ et la suite étendue $a_1, \ldots, a_m, b$.

Soit $\mathcal{C}$ le $[m, m-r]_{p^h}$ de matrice de parité H. Un mot de code de $\mathcal{C}$ correspond à une sous-suite de $a_1, \ldots, a_m$ à somme nulle pondérée par des poids dans $\mathcal{W}$. D'après l'hypothèse

ci-dessus, $\mathcal{C}$ est un code intersectant. Par conséquent

$$m \geq i(m-r, p^h).$$

On en déduit

$$\mathrm{D}_2^h(E_{p^{hr}}) = \max\{m > r \mid m \geq i(m-r, p^h)\} + 1,$$

qui est équivalent au théorème. □

Exemple 4.4.9. Soit E_{16} le groupe abélien élémentaire d'ordre 16. Soit $h = 1$ et $r = 4$. On a alors $\{m \geq 5 \mid m < i(m-4, 2)\} = \{8, 9, \ldots\}$ (voir le Tableau 4.2), si bien que $\mathrm{D}_2(E_{16}) = 8$. D'autre part, si $h = 2$ et $r = 2$, alors $\{m \geq 3 \mid m < i(m-2, 4)\} = \{6, 7, \ldots\}$ (voir encore le Tableau 4.2), de sorte que $\mathrm{D}_2^2(E_{16}) = 6$.

Exemple 4.4.10. Soit E_{1024} le groupe abélien élémentaire d'ordre 1024. On a alors $\{m \geq 11 \mid m < i(m-10, 2)\} = \{17, 18, \ldots\}$ (voir le Tableau 4.2), et donc $\mathrm{D}_2(E_{1024}) = 17$. D'autre part, si $h = 2$ et $r = 5$, on a $\{m \geq 6 \mid m < i(m-5, 4)\} = \{11, 12, \ldots\}$ (voir encore le Tableau 4.2), de sorte que $\mathrm{D}_2^2(E_{1024}) = 11$.

4.4.3 Bornes asymptotiques sur $\mathrm{D}_2^h(E_{p^{hr}})$

Soit p un premier et $h \in \mathbb{N}$. Notons $q = p^h$. Nous nous intéressons au comportement asymptotique de $\mathrm{D}_2^h(E_{p^{hr}})$ quand r tend vers l'infini.

Lemme 4.4.11. Soit $\alpha \leq \liminf_{k\to\infty} i(k, p^h)/k$, et $\beta \geq \limsup_{k\to\infty} i(k, p^h)/k$. Alors

$$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq \frac{\alpha}{\alpha - 1}$$

et

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq \frac{\beta}{\beta - 1}.$$

Preuve. Soit $\varepsilon > 0$ et soit r suffisamment grand pour que pour tout $m \geq r+1$, on ait tout à la fois

$$i(m-r, p^h) \leq (\beta + \varepsilon) \cdot (m - r) \text{ et } i(m-r, p^h) \geq (\alpha - \varepsilon) \cdot (m - r).$$

D'après le Théorème 4.4.8,

$$\mathrm{D}_2^h(E_{p^{hr}}) = \min\{m \geq r+1 \mid m < i(m-r, q)\}.$$

Par conséquent $\mathrm{D}_2^h(E_{p^{hr}}) < i(\mathrm{D}_2^h(E_{p^{hr}}) - r, q) \leq (\beta + \varepsilon) \cdot (\mathrm{D}_2^h(E_{p^{hr}}) - r)$, dont on déduit

$$\mathrm{D}_2^h(E_{p^{hr}}) \geq r \cdot \frac{\beta + \varepsilon}{\beta - 1 + \varepsilon}.$$

De même, on déduit l'autre borne en remarquant que

$$\mathrm{D}_2^h(E_{p^{hr}}) - 1 \geq i(\mathrm{D}_2^h(E_{p^{hr}}) - 1 - r, q) \geq (\alpha - \varepsilon) \cdot (\mathrm{D}_2^h(E_{p^{hr}}) - 1 - r),$$

ce qui donne

$$\mathrm{D}_2^h(E_{p^{hr}}) \leq 1 + r \cdot \frac{\alpha - \varepsilon}{\alpha - 1 - \varepsilon}.$$

□

En utilisant ce lemme, on peut transformer nos bornes asymptotiques sur $i(k, q)$ dans le contexte des codes intersectants en bornes asymptotiques sur $\mathrm{D}_2^h(E_{p^{hr}})$ dans le cas de la constante de Davenport.

De même, les constructions explicites de codes intersectants correspondent de manière naturelle à des constructions explicites de longues suites sans sous-suite à somme nulle: de la matrice génératrice d'un code AG intersectant, on déduit une matrice de parité, dont les colonnes seront les éléments de notre longue suite.

Théorème 4.4.12. Pour tout premier p et tout entier h, on a

$$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq 2 - \frac{1}{p^h},$$

ainsi que

$$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq \frac{q + 2 + q\log_q(q-2)}{q\log_q(q-2)}.$$

De plus, pour $p^h \leq 17$, cette borne est améliorée dans le Tableau 4.5.

p	h	$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r}$
2	1	1.3956
2	2	1.6364
2	3	1.8057
2	4	1.9257
3	1	1.5472
3	2	1.8291
5	1	1.6972
7	1	1.7774
11	1	1.8660
13	1	1.8940
17	1	1.9343

Table 4.5: Borne supérieure asymptotique sur la constante de Davenport pondérée d'ordre 2

Preuve. Il suffit d'appliquer le Lemme 4.4.11 en utilisant les valeurs de α obtenues dans les Théorèmes 4.2.10 et 4.2.14. Pour des petites valeurs de q, il est possible d'améliorer α en examinant le Tableau 4.1 et en appliquant le Lemme 4.4.11 (ces valeurs correspondent à la borne MRRW). □

Théorème 4.4.13. Soit p un premier et $h \in \mathbb{N}$ un entier. On a:

- si $h = 1$ ou $p^h \in \{4, 8, 9, 16, 25, 27, 32, 125\}$,

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq \frac{2}{\log_{p^h}(2p^h - 1)};$$

- si $h = 2m$ est pair et $p^h \notin \{4, 9, 16, 25\}$, alors

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq 2 - \frac{2}{p^m};$$

- si $h = 2m + 1$ est impair et $p^h \notin \{8, 27, 32, 125\}$, alors

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq 2 - \frac{2}{2\frac{(p^m-1)(p^{m+1}-1)}{(p^{m+1}+p^m-2)} + 1}.$$

Preuve. Il suffit d'appliquer le Lemme 4.4.11 en utilisant la valeur de β issue du Théorème 4.2.7 ou du Théorème 4.3.8. □

Remarque 4.4.14. Quand $h = 1$, nous obtenons les mêmes bornes asymptotiques que celles présentées dans [47].

Remarque 4.4.15. Notons que le Théorème 4.4.12 et le Théorème 4.4.13 peuvent être considérés comme des améliorations de la Proposition 2.3.3 pour $j = 2$. En effet, notons que la Proposition 2.3.3 est également vraie pour les versions pondérées de la constante de Davenport. De plus, puisque $\mathrm{D}_1^h(E_{p^{hr}}) = r + 1$, comme énoncé dans la Remarque 4.4.7, une version pondérée et asymptotique de la Proposition 2.3.3 est

$$1 \leq \liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq 2.$$

Des améliorations similaires pour d'autres valeurs de j sont exposés en détail dans [47].

Remarquons que puisque le Théorème 4.3.8 donne des constructions explicites de codes intersectants courts, en utilisant le Lemme 4.4.11, il est possible de les transformer en constructions explicites de longues suites d'éléments de $E_{p^{hr}}$ qui n'admettent pas deux sous-suites à somme pondérée nulle disjointes. Ceci est affirmé dans une forme précise dans la remarque suivante.

Remarque 4.4.16. Soit p un premier et h et r des entiers positif. Il existe des suites *explicites* de longueur ℓr d'éléments de $E_{p^{hr}}$ qui n'ont pas 2 sous-suites à somme pondérée nulle disjointes avec

- $\ell = 2 - \frac{2}{p^m}$, si $p \geq 5$, $h = 2m$ et $p^h \geq 25$;
- $\ell = 2 - \frac{2}{2\frac{(p^m-1)(p^{m+1}-1)}{(p^{m+1}+p^m-2)}+1}$, si $h = 2m+1$ et $p^h \geq 32$;
- $\ell = \frac{3p-3}{2p-1}$, si $p \geq 11$ et $h = 1$.

Les cas restants sont donnés dans le Tableau 4.6.

p	h	ℓ	Borne probabiliste
2	1	1.206	1.261
3	1	1.297	1.365
2	2	1.315	1.424
5	1	1.344	1.464
7	1	1.388	1.517
2	3	1.4	1.535
3	2	1.411	1.551
2	4	1.451	1.614
3	3	1.471	1.660

Table 4.6: Valeur de ℓ dans les cas exceptionnels

4.5 Liens avec la théorie de la factorisation

Dans cette section, nous nous intéressons au lien entre la constante de Davenport (et ses généralisations) et la théorie de la factorisation. En développant les résultats obtenus dans notre introduction au groupe de classes (au deuxième chapitre), nous voulons faire émerger des liens entre les codes intersectants et la théorie de la factorisation. Nous commençons bien évidemment par une interprétation en termes de factorisation des différentes constantes de Davenport.

Pour tout idéal $\mathcal{I} \subset \mathcal{O}_K$, l'idéal $\mathcal{I}^{\exp(\mathrm{Cl}(\mathcal{O}_K))}$ est principal. En particulier, un idéal de la forme $(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n)^{\exp(\mathrm{Cl}(\mathcal{O}_K))}$ est toujours principal.

Au vu du Lemme 2.4.13, la question suivante est naturelle: considérant un idéal $\mathcal{I} \subset \mathcal{O}_K$, quelles puissances de $\mathcal{I}$ sont divisibles par un idéal principal non trivial? Un exemple intéressant est le cas où $\mathcal{I}$ est de la forme

$$\mathcal{I} = \prod_{i=1}^{n} \mathfrak{p}_i,$$

où $\mathfrak{p}_i$ sont des idéaux premiers. Si $\mathcal{I}^k$ est divisible par un idéal principal non trivial, alors il doit exister un produit

$$\prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i},$$

(avec $0 \leq \alpha_i \leq k$) qui est un idéal principal non trivial. Ce produit peut bien évidemment être interprété comme une sous-suite à somme nulle à poids dans $\{1, \ldots, k\}$, dans le groupe de classes $\mathrm{Cl}(\mathcal{O}_K)$. La constante de Davenport maximalement pondérée est un cas particulier de cette question générale, à savoir le cas $k = \exp(\mathrm{Cl}(\mathcal{O}_K)) - 1$.

Lemme 4.5.1. Les différentes constantes de Davenport peuvent être interprétées comme suit:

- Pour tout $k \in \mathbb{N}$, la petite constante de Davenport pondérée $\mathrm{d}^{\{1,\ldots,k\}}(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre $\ell \in \mathbb{N}$ tel qu'il existe ℓ idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ tels que le produit

  $$(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell)^k$$

  n'est pas divisible par un idéal principal non trivial.

- La petite constante de Davenport maximalement pondérée $\mathrm{d}^f(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre $\ell \in \mathbb{N}$ tel qu'il existe ℓ idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ tels que le produit

  $$(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell)^{\exp(\mathrm{Cl}(\mathcal{O}_K))-1}$$

  n'est pas divisible par un idéal principal non trivial.

- La petite constante d'ordre 2 de Davenport $\mathrm{d}_2(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre $\ell \in \mathbb{N}$ tel qu'il existe ℓ idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ tels que le produit

  $$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell$$

  n'est pas divisible par le produit de deux idéaux principaux non triviaux (ou, de manière équivalente, ce produit n'est divisible que par des idéaux principaux engendrés par une élément irréductible).

- La petite constante d'ordre 2 de Davenport maximalement pondérée $\mathrm{d}_2^f(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre $\ell \in \mathbb{N}$ tel qu'il existe ℓ idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ tels que le produit

  $$(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell)^{\exp(\mathrm{Cl}(\mathcal{O}_K))-1}$$

  n'est pas divisible par le produit de deux idéaux principaux non triviaux (ou, de manière équivalente, ce produit n'est divisible que par des idéaux principaux engendrés par un élément irréductible).

4.5.1 Le cas où le groupe de classe est un groupe abélien élémentaire

Dans ce qui suit, nous allons nous intéresser au cas où $\mathrm{Cl}(\mathcal{O}_K)$ est un groupe abélien fini élémentaire, à savoir de la forme $E_{p^{hr}}$.

Comme dans la section précédente, on note $q = p^h$, et on peut considérer l'action multiplicative de $\mathbb{F}_q$ sur $E_{p^{hr}}$. Notons qu'il n'y a pas de manière unique de définir cette action multiplicative (parce qu'il n'y a pas d'isomorphisme canonique $\mathbb{F}_q^r \cong E_{p^{hr}}$). Cependant, nos résultats ne dépendent pas du choix de l'isomorphisme.

Nous obtenons alors le théorème suivant.

Théorème 4.5.2. Soit p un premier et $h, r \geq 0$ des entiers. Soit K un corps de nombres tel que $\mathrm{Cl}(\mathcal{O}_K) = E_{p^{hr}}$.

La petite constante pondérée de Davenport d'ordre 2, c'est-à-dire $\mathrm{d}_2^h(\mathrm{Cl}(\mathcal{O}_K))$ est le plus grand nombre $\ell \in \mathbb{N}$ tel qu'il existe ℓ idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ tels que tout produit

$$\prod_{i=1}^{\ell} \mathfrak{q}_i,$$

où $\mathfrak{q}_i$ est un idéal dans la classe de $\varphi_i([\mathfrak{p}_i])$, avec $\varphi_i \in \mathcal{Q}_h$, n'est pas divisible par le produit de deux idéaux principaux non triviaux.

Preuve. Ici également, la preuve est une adaptation de celle du Lemme 2.4.13 à la définition de la petite constante pondérée de Davenport d'ordre 2. □

Remarque 4.5.3. Il est remarquable que la propriété ci-dessus ne dépend pas du choix de l'action multiplicative. Il serait très intéressant d'obtenir une interprétation de cet invariant en termes de théorie des nombres. Plus bas, nous montrerons un lien avec l'action du groupe de Galois sur le groupe de classes, qui coïncide avec notre action multiplicative dans certains cas particuliers que nous examinerons.

Notons qu'on ne sait pas encore si tout groupe abélien est le groupe de classes de l'anneau d'entiers d'un corps de nombres: il s'agit d'un problème ouvert. Cependant, dans [24], Claborn montre que tout groupe abélien fini est le groupe de classes d'un anneau de Dedekind. Pour donner quelques exemples correspondant aux résultats énoncés plus haut, nous utilisons la construction explicite présentée dans [35, Theorem 2], ainsi que des calculs explicites en Magma.

Exemple 4.5.4. Prenons

$$\alpha = 5 \cdot 13 \cdot 29 \cdot 41 \cdot 61$$

et $K = \mathbb{Q}(\sqrt{\alpha})$. Le groupe de classes est $\mathrm{Cl}(\mathcal{O}_K) \cong E_{16}$. D'après l'Exemple 4.4.9 on sait que $\mathrm{d}_2(E_{16}) = \mathrm{D}_2(E_{16}) - 1 = 7$, et $\mathrm{d}_2^2(E_{16}) = \mathrm{D}_2^2(E_{16}) - 1 = 5$. Par conséquent il existe

7 idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_7$ tels que leur produit n'est pas divisible par le produit de deux idéaux principaux non triviaux, et 5 idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$ tels que tout produit de la forme

$$\prod_{i=1}^{5} \mathfrak{q}_i,$$

où $\mathfrak{q}_i$ est un idéal dans la classe de $\varphi_i([\mathfrak{p}_i])$, avec $\varphi_i \in \mathcal{Q}_2$, n'est pas divisible par le produit de deux idéaux principaux non triviaux.

Exemple 4.5.5. Prenons

$$\alpha = 316861 \cdot 451897 \cdot 455333 \cdot 476977 \cdot 490549 \cdot 523793 \cdot 560641 \cdot 724481 \cdot 736993 \cdot 828829 \cdot 916621$$

et $K = \mathbb{Q}(\sqrt{\alpha})$. Le groupe de classes est $\mathrm{Cl}(\mathcal{O}_K) \cong E_{1024}$. D'après l'Exemple 4.4.10 on a $\mathrm{d}_2(E_{1024}) = \mathrm{D}_2(E_{1024}) - 1 = 16$ et $\mathrm{d}_2^2(E_{1024}) = D_2^2(E_{1024}) - 1 = 10$.

Par conséquent il existe 16 idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_{16}$ tels que leur produit n'est pas divisible par le produit de deux idéaux principaux non triviaux, ainsi que 10 idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_{10}$ tels que tout produit

$$\prod_{i=1}^{10} \mathfrak{q}_i,$$

où $\mathfrak{q}_i$ est un idéal appartenant à la classe $\varphi_i([\mathfrak{p}_i])$, où $\varphi_i \in \mathcal{Q}_2$, n'est pas divisible par le produit de deux idéaux principaux non triviaux.

4.5.2 L'action du groupe de Galois sur le groupe de classes

Dans [21, Theorem 7.1], il est établi que le monoïde des normes des anneaux d'entiers des corps de nombres galoisiens admet un morphisme de transfert vers les monoïdes de suites pondérées à somme nulle, où les poids correspondent aux éléments du groupe de Galois. Une généralisation supplémentaire de ce travail est donnée dans [33].

L'étude des suites à somme nulle dans le groupe de classe pondérées par des poids issus de l'action du groupe de Galois sur le groupe de classe est donc naturelle. Du point de vue de la théorie de la factorisation, elle ne nécessite aucune justification supplémentaire.

L'action de $\mathcal{Q}_h$ correspond précisément à l'action multiplicative de $\mathbb{F}_q$ sur $E_{p^{hr}}$. Le groupe multiplicatif de $\mathbb{F}_q$ est isomorphe à C_{q-1}. Les orbites de cette action multiplicative ont toutes cardinal $q-1$: l'action est libre sur $\mathbb{F}_q^r \setminus \{0\}$. Le théorème suivant vient compléter cette discussion.

Théorème 4.5.6. Soit p un premier, et $h, r \in \mathbb{N}$, et posons $q = p^h$. Soit K un corps de nombres, dont le groupe de Galois est $\mathrm{Gal}(K/\mathbb{Q}) = C_{q-1}$ et le groupe de classes est $\mathrm{Cl}(\mathcal{O}_K) = E_{p^{hr}}$. Si l'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathrm{Cl}(\mathcal{O}_K) \setminus \{0\}$ est libre, alors il existe un isomorphisme

$\varphi : E_{p^{hr}} \to \mathbb{F}_q^r$ tel que l'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur le groupe de classe est exactement la même que celle de $\mathcal{Q}_h$.

Preuve. Notons pour commencer que l'action du groupe de Galois sur le groupe de classe préserve l'addition.

Soit σ un générateur du groupe de Galois. Notons que $E_{p^{hr}} \cong \mathbb{F}_p^{hr}$ en tant qu'espace vectoriel sur $\mathbb{F}_p$. Il est clair que σ correspond à un endomorphisme de $\mathbb{F}_p^{hr}$, que nous notons également σ. Puisque $x^q - x = 0$ annule σ et σ est d'ordre $q-1$, l'anneau des endomorphismes $\mathbb{F}_p[\sigma]$ est isomorphe à $\mathbb{F}_q$.

Puisque l'orbite de chaque élément non nul v a ordre $q-1$, la fonction

$$f(\sigma) = f_0 + f_1\sigma + \ldots + f_{h-1}\sigma^{h-1} \mapsto f(\sigma)(v) = f_0 v + f_1\sigma(v) + \ldots + f_{h-1}\sigma^{h-1}(v)$$

est une bijection de $\mathbb{F}_p[\sigma]$ vers $\{0\} \cup \omega(v)$, et est également un isomorphisme d'espaces vectoriels sur $\mathbb{F}_p$. Avec cette bijection, nous pouvons munir $\{0\} \cup \omega(v)$ d'une structure multiplicative qui le rend isomorphe à $\mathbb{F}_q$.

Notons à présent v_1 un élément non nul de $\mathrm{Cl}(\mathcal{O}_K)$. Considérons un élément non nul $v_2 \in \mathrm{Cl}(\mathcal{O}_K) \setminus \omega(v_1)$. Les deux ensembles $\{0\} \cup \omega(v_1)$ et $\{0\} \cup \omega(v_2)$ sont isomorphes à $\mathbb{F}_q$. Les orbites sont disjointes. On en déduit que $W = \langle \omega(v_1), \omega(v_2) \rangle \cong \mathbb{F}_q^2$. De plus, W est stable sous l'action du groupe de Galois. Nous pouvons continuer en choisissant un élément non nul qui n'est pas contenu dans W et ainsi de suite, jusqu'à ce qu'on obtienne r éléments, mettons $v_1, \ldots, v_r$. De cette manière, on obtient finalement $\langle \omega(v_1), \ldots, \omega(v_r) \rangle \cong \mathbb{F}_q^r$. □

Remarque 4.5.7. Si $p = 2$ et $q - 1 = 2^h - 1$ est un nombre premier de Mersenne, alors l'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathrm{Cl}(\mathcal{O}_K) \setminus \{0\}$ est libre. En fait, il est connu que tout premier $\ell \in \mathbb{Z}$ produit la décomposition suivante:

$$(\ell) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$$

et er divise $q-1$. Par conséquent, soit $e = 1$ et $r = q-1$, de sorte que ℓ est totalement décomposé, ou bien $e = q-1$ et $r = 1$, et alors ℓ est totalement ramifié, ou encore $e = r = 1$, et ℓ est inerte. Notons en particulier que quand $(\ell) = (\mathfrak{p})^{q-1}$ (c'est-à-dire quand ℓ est totalement ramifié), l'idéal $\mathfrak{p}$ est principal.

En l'état actuel de nos connaissances, il est inconnu en général pour quelle valeurs de p, h, r il existe un corps de nombres qui vérifie les hypothèses du Théorème 4.5.6. Nous développons cependant un exemple dans l'un des cas simples évoqués dans la Remarque 4.5.7.

Exemple 4.5.8. Soit $p(x) = x^3 - x^2 - 2562x + 48969$ et soit $K = \mathbb{Q}[\alpha]$ le corps de nombres cubique obtenu en prenant l'extension $\mathbb{Q}$ avec une racine de $p(x)$. On a

$$\mathrm{Gal}(K/\mathbb{Q}) = C_3 \text{ et } \mathrm{Cl}(\mathcal{O}_K) = E_{16}.$$

De plus, $q-1=3$ est un nombre premier de Mersenne. Dans ce cas, comme dans l'Exemple 4.5.4, il existe 7 idéaux premiers $\mathfrak{p}_1,\ldots,\mathfrak{p}_7$ tels que leur produit n'est pas divisible par le produit de deux idéaux principaux non triviaux, ainsi que 5 idéaux premiers $\mathfrak{p}_1,\ldots,\mathfrak{p}_5$ tels que tout produit

$$\prod_{i=1}^{5}\mathfrak{q}_i,$$

où $\mathfrak{q}_i$ est un idéal de la classe de $\sigma([\mathfrak{p}_i])$, avec $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, n'est pas divisible par le produit de deux idéaux principaux non triviaux.

Remarque 4.5.9. Il existe des corps de nombres qui satisfont les hypothèses du Théorème 4.5.6 et qui ne sont pas de degré premier (comme dans la remarque 4.5.7). Un exemple est le corps $K=\mathbb{Q}[\alpha]$ où

$$\alpha^6-\alpha^5+22\alpha^4+11\alpha^3+1038\alpha^2-1993\alpha+16649=0.$$

Dans ce cas on a

$$\mathrm{Gal}(K/\mathbb{Q})=C_6 \text{ et } \mathrm{Cl}(\mathcal{O}_K)=E_{49}.$$

L'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathrm{Cl}(\mathcal{O}_K)\setminus\{0\}$ est libre et les 8 orbites d'ordre 6 sont celles des 8 classes suivantes: $[\mathfrak{p}_\ell]$ où $\ell\in\{47,59,107,127,131,151,173,193\}$ et $\mathfrak{p}_\ell$ est un facteur de (ℓ).

Il serait certainement intéressant d'examiner davantage les extensions de corps qui satisfont les hypothèses du Théorème 4.5.6, ainsi que d'examiner les codes qui correspondraient à une action non libre.

Chapter 5

Codes intersectants en métrique rang

En métrique rang $\mathbb{F}_{q^m}$-linéaire, m joue le rôle de q.

- Martino Borello

L'objectif de ce chapitre est de donner un q-analogue des codes intersectants étudiés au chapitre précédent. De ce point de vue, le travail esquissé ici est semblable à celui effectué dans [5] pour les codes minimaux en métrique rang.

Nous allons nous appuyer sur la théorie géométrique des codes en métrique rang $\mathbb{F}_{q^m}$-linéaire développée par exemple dans [59]. Notre idée générale est de donner une caractérisation géométrique des codes intersectants en métrique rang.

Cette caractérisation géométrique devra nécéssairement être exprimée en termes de q-systèmes. L'étude de ces q-systèmes particuliers, que nous appellerons 2-générables dans la suite, permettra de donner des constructions explicites de codes intersectants, ainsi que de montrer des bornes sur leurs paramètres.

5.1 Définition et premières propriétés

Rappelons que la définition de support d'un vecteur $x \in \mathbb{F}_{q^m}^n$ est $\sigma(x) = \mathrm{rowspan}(\mathrm{Mat}_\Gamma(x))$, dans n'importe quelle $\mathbb{F}_q$-base Γ de $\mathbb{F}_{q^m}$. Le choix de cette définition est motivée au premier chapitre dans la section dédiée aux codes en métrique rang.

Définition 5.1.1. Un code $\mathcal{C}$ est intersectant si $\forall c, c' \in \mathcal{C} \setminus \{0\}$ on a

$$\sigma(c) \cap \sigma(c') \neq \{0\}.$$

Dans le cas de la métrique de Hamming, nous avons vu au chapitre précédent que cela implique l'existence d'une coordonnée i telle que $c_i \neq 0$ et $c'_i \neq 0$. Dans le cas de la métrique rang, le support d'un mot de code est un sous-espace de $\mathbb{F}_q^n$. L'interprétation est donc que l'intersection des supports de c et c' est non triviale.

Proposition 5.1.2. Soit $\mathcal{C}$ un code intersectant en métrique rang, et soit $\mathcal{C}'$ un code équivalent à $\mathcal{C}$. Alors $\mathcal{C}'$ est également un code intersectant.

Preuve. Notons pour commencer que puisque $\mathcal{C}'$ est équivalent à $\mathcal{C}$, il existe $A \in GL(n,q)$ tel que $C' = \{c \cdot A \mid c \in \mathcal{C}\}$. Soit $c, c' \in \mathcal{C}$. Puisque $\mathcal{C}$ est intersectant, on a bien $\sigma(c) \cap \sigma(c') \neq \varnothing$, et en particulier $\exists x \in (\sigma(c) \cap \sigma(c')) \setminus \{0\}$. D'autre part, $c \cdot A$ et $c' \cdot A$ sont des mots de code de $\mathcal{C}'$. Puisque $\sigma(c \cdot A) = \sigma(c) \cdot A$, on a alors clairement $x \cdot A \in \sigma(c \cdot A)$ et $x \cdot A \in \sigma(c' \cdot A)$, donc $\sigma(c \cdot A) \cap \sigma(c' \cdot A) \neq \varnothing$, ce qui implique que $\mathcal{C}'$ est intersectant. □

Proposition 5.1.3. Soit $\mathcal{C}$ un code intersectant en métrique rang. Alors $\mathcal{C}$ est intersectant en métrique de Hamming.

Preuve. Supposons que $\mathcal{C}$ ne soit pas intersectant en métrique de Hamming. Alors il existe $c, c' \in \mathcal{C} \setminus \{0\}$ tels que

$$\sigma(c) \cap \sigma(c') = \varnothing.$$

Soit Γ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^m}$. On remarque que les colonnes non nulles de $\mathrm{Mat}_\Gamma(c)$ sont exactement celles indexées par $\sigma(c)$. Il en va de même pour les colonnes de $\mathrm{Mat}_\Gamma(c')$. On en déduit qu'un vecteur de $\sigma_{\mathrm{rk}}(c) \cap \sigma_{rk}(c')$ doit nécéssairement être nul sur les colonnes indexées par $\sigma(c')$, mais également sur les colonnes indexées $\sigma(c)$ (ainsi que sur les colonnes qui ne sont indexées ni par $\sigma(c)$ ni par $\sigma(c')$). Par conséquent, $\sigma_{\mathrm{rk}}(c) \cap \sigma_{rk}(c') = \{0\}$, et $\mathcal{C}$ n'est donc pas intersectant en métrique rang. □

Nous donnons une condition suffisante pour qu'un code soit intersectant en métrique rang.

Théorème 5.1.4. Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code en métrique rang. Si $2d > n$, alors $\mathcal{C}$ est intersectant en métrique rang.

Preuve. Soit $c, c' \in \mathcal{C} \setminus \{0\}$. Il est clair que $\dim_{\mathbb{F}_q} \sigma(c) \geq d$, et que $\dim_{\mathbb{F}_q} \sigma(c') \geq d$. Par conséquent, puisque $\sigma(c)$ et $\sigma(c')$ sont des sous-espaces de $\mathbb{F}_q^n$, et puisque $2d > n$, on a bien $\sigma(c) \cap \sigma(c') \neq \varnothing$ d'après la formule de Grassmann, et donc $\mathcal{C}$ est intersectant. □

Exemple 5.1.5. Soit $\mathcal{C}$ un $[3,2,2]_{8/2}$ engendré par

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

où $\alpha^3 = \alpha + 1$ est un élément primitif dans $\mathbb{F}_8$. Le support de tout mot non nul est un sous-espace de dimension 2 de $\mathbb{F}_2^3$. D'après la formule de Grassmann, deux tels sous-espaces doivent avoir une intersection de dimension au moins 1.

Remarque 5.1.6. Dans le régime $n \leq m$, un code MRD est intersectant si et seulement si $2d > n$. Ses paramètres sont en effet $[n, k, n-k+1]_{q^m}$.

Si $2d > n$, alors le code est clairement intersectant en métrique rang d'après le théorème ci-dessus.

Si le code est intersectant, alors on a $d \geq k$, ce qui implique $2d \geq k+d = n-k+k+1 = n+1$, soit $2d > n$.

On notera également que dans le cas des codes MRD, la condition $2d > n$ est équivalente à $n \geq 2k-1$.

Remarque 5.1.7. En métrique rang, la comparaison des codes intersectants avec les codes minimaux est plus ténue qu'en métrique de Hamming.

En effet, si tout code minimal est intersectant en métrique de Hamming, cela n'est certainement pas vrai en métrique rang. Le meilleur exemple de ce phénomène est le code de matrice génératrice

$$G = \begin{pmatrix} I_k & \alpha \cdot I_k & \alpha^2 \cdot I_k & \cdots & \alpha^{m-1} \cdot I_k \end{pmatrix},$$

avec α un élément primitif de $\mathbb{F}_{q^m}$. Notons en particulier que le q-système associé à ce code est de rang maximal, à savoir $n = km$.

Tous les mots de code de ce code ont même poids [5,59], ce qui implique qu'il est minimal. Cependant, ce code n'est clairement pas intersectant pour $k \geq 2$. En effet, si e_1, e_2 sont les deux premiers éléments de la base canonique de $\mathbb{F}_{q^m}^k$, on observe facilement que

$$\sigma(e_1 G) \cap \sigma(e_2 G) = \{0\}.$$

Malgré ces différences, nous allons observer une similarité : selon les valeurs de n, i.e. le rang du q-système, il existe un régime pour lequel les codes intersectants ne peuvent pas exister, une zone grise, et un régime dans lequel on sait que les codes intersectants existent. Cela est similaire pour les codes minimaux : il existe également un régime dans lequel on sait que les codes minimaux existent, une zone grise, et un régime dans lequel on sait que les codes minimaux n'existent pas. De ce point de vue, notre travail s'apparente à celui mené dans [5].

5.2 Une interprétation géométrique

De la même manière que les codes minimaux et intersectants en métrique de Hamming ont une interprétation géométrique, que nous avons étudiée dans les précédents chapitres, nous voulons déterminer une interprétation géométrique des codes intersectants en métrique rang.

Au vu de la discussion de la métrique rang au premier chapitre, il est naturel de penser que l'analogue géométrique des codes intersectants en métrique rang prendra la forme d'une propriété particulière sur les q-systèmes ou sur les ensembles linéaires.

La voici.

Définition 5.2.1. Soit $\mathcal{U}$ un $[n,k,d]_{q^m/q}$-système. On dit que $\mathcal{U}$ est 2-générable s'il existe deux hyperplans $\mathbb{F}_{q^m}$-linéaires $\mathcal{H}_1, \mathcal{H}_2$ de $\mathbb{F}_{q^m}^k$ tels que

$$\mathcal{U} = \mathcal{H}_1 \cap \mathcal{U} + \mathcal{H}_2 \cap \mathcal{U}.$$

On pourrait aisément généraliser cette propriété et proposer des q-systèmes j-générables, avec $j \geq 1$. Cependant, cette généralisation est excessive au vu de l'utilisation que nous comptons en faire dans le présent travail.

On remarque immédiatement que si un q-système $\mathcal{U}$ est 2-générable, alors

$$n \leq \mathrm{wt}_{\mathcal{U}}(\mathcal{H}_1) + \mathrm{wt}_{\mathcal{U}}(\mathcal{H}_2).$$

En particulier il existe un hyperplan $\mathcal{H}$ dont le poids vérifie

$$\mathrm{wt}_{\mathcal{U}}(\mathcal{H}) \geq n/2.$$

Par conséquent, si pour tout hyperplan $\mathcal{H}$ on a $\mathrm{wt}_{\mathcal{U}}(\mathcal{H}) < \frac{n}{2}$, alors $\mathcal{U}$ n'est pas 2-générable.

Proposition 5.2.2. Soit $\mathcal{U}$ un $[n,k,d]_{q^m/q}$-système. Si $n \leq 2k-2$, alors $\mathcal{U}$ est 2-générable.

Preuve. Si $n \leq 2k-2$, notons $(u_1, \ldots, u_n)$ une $\mathbb{F}_q$-base de $\mathcal{U}$. On peut alors prendre $\mathcal{H}_1$ un hyperplan contenant $u_1, \ldots, u_{k-1}$ et $\mathcal{H}_2$ un hyperplan contenant $u_k, \ldots, u_n$. Avec ce choix de $\mathcal{H}_1, \mathcal{H}_2$, on a bien

$$\mathcal{U} = \mathcal{H}_1 \cap \mathcal{U} + \mathcal{H}_2 \cap \mathcal{U},$$

ce qui implique que $\mathcal{U}$ est 2-générable. □

Théorème 5.2.3. Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code non-dégénéré en métrique rang. Les assertions suivantes sont équivalentes.

1. Le code $\mathcal{C}$ est intersectant en métrique rang.
2. Pour tout $A \in GL(n,q)$, le code $\mathcal{C} \cdot A$ est intersectant en métrique de Hamming.
3. Pour tout $A \in GL(n,q)$, et pour tout $[n,k,d]_q$-système $\mathcal{S} \subset \mathrm{PG}(k-1, q^m)$ obtenu à partir des colonnes d'une matrice génératrice de $\mathcal{C} \cdot A$, l'ensemble $\mathcal{S}$ est N2C.
4. Le $[n,k,d]_{q^m/q}$-système $\mathcal{U}$ correspondant au code $\mathcal{C}$ n'est pas 2-générable.

Preuve. Commençons par montrer que les deux premières assertions sont équivalentes.

(1) ⇒ (2) : Nous avons bien vu que si $\mathcal{C}$ est intersectant en métrique rang, alors il l'est aussi en métrique de Hamming, et tout code de la forme $\mathcal{C} \cdot A$ avec $A \in GL(n,q)$ est intersectant

en métrique rang. Par conséquent, tout code de la forme $\mathcal{C} \cdot A$ est intersectant en métrique de Hamming.

(2) $\Rightarrow$ (1) : Si $\mathcal{C}$ n'est pas intersectant, il existe deux mots de code $c, c' \in \mathcal{C}$ tels que $\sigma(c) \cap \sigma(c') = \varnothing$. Soit $B \subset \mathbb{F}_q^n$ une $\mathbb{F}_q$-base de $\sigma(c)$, et $B' \subset \mathbb{F}_q^n$ une $\mathbb{F}_q$-base de $\sigma(c')$. Puisque $\sigma(c) \cap \sigma(c') = \varnothing$, il est clair que B et B' sont linéairement indépendantes, et leur union peut être complétée pour donner une base $\mathcal{B}$ de $\mathbb{F}_q^n$. Notons $A \in \mathrm{GL}(n, q)$ la matrice de changement de base de $\mathcal{B}$ vers la base canonique. Il est alors clair que $c \cdot A$ et $c' \cdot A$ ne s'intersectent pas en métrique de Hamming, et que le code $\mathcal{C} \cdot A$ n'est donc pas intersectant en métrique de Hamming. On en conclut que les assertions 1 et 2 sont bien équivalentes.

D'après le Théorème 4.2.2, il est clair que les assertions 2 et 3 sont équivalentes. Il s'agit donc pour finir de montrer que les assertions 3 et 4 le sont.
(3) $\Rightarrow$ (4) : si $\mathcal{U}$ est 2-générable, alors il a une base contenue dans deux hyperplans de $\mathbb{F}_{q^m}^k$, et il existe une matrice inversible $A \in \mathrm{GL}(n, q)$ telle que les colonnes de $G \cdot A$ sont les vecteurs de cette base. Il est clair que l'ensemble de points $\mathcal{S} \subset \mathrm{PG}(k-1, q^m)$ obtenu à partir de ces colonnes est contenu dans deux hyperplans projectifs (qui sont les images des hyperplans de $\mathbb{F}_{q^m}^k$ correspondants).
(4) $\Rightarrow$ (3) : Fixons une matrice génératrice G de notre code intersectant $\mathcal{C}$, et considérons le q-système $\mathcal{U}$ formé par les combinaisons $\mathbb{F}_q$-linéaires des colonnes de G. Notons également que l'action de $\mathrm{GL}(n, q)$ laisse invariant le q-système $\mathcal{U}$. Si l'ensemble $\mathcal{S}$ n'est pas N2C, alors il est contenu dans deux hyperplans de $\mathrm{PG}(k-1, q^m)$, et donc $\mathcal{U}$ admet une base contenue dans deux hyperplans de $\mathbb{F}_{q^m}^k$, i.e. $\mathcal{U}$ est 2-générable. Par conséquent, les assertions 3 et 4 sont équivalentes, ce qui conclut. □

Corollaire 5.2.4. Si un $[n, k, d]_{q^m/q}$ code est intersectant, alors $n \geq 2k - 1$.

Preuve. Cela est une conséquence directe du Théorème 5.2.3 et de la Proposition 4.2.5. □

Remarque 5.2.5. Il est important de remarquer que la propriété de 2-générabilité n'est pas stable par inclusion, contrairement à la définition des ensembles générateurs d'hyperplans et des ensembles N2C examinés dans les chapitres précédents.

En effet, si l'on prend le code de Gabidulin de paramètres $[5, 3, 3]_{32/2}$, alors il n'y a pas de manière d'ajouter une colonne à la matrice génératrice qui donne encore un code intersectant.

5.3 Bornes sur les paramètres des q-systèmes 2-générables

Dans cette section, nous explorons les bornes sur les paramètres des codes intersectants que nous pouvons déduire de notre caractérisation géométrique.

Proposition 5.3.1. Soit U un q-système 2-générable de $\mathbb{F}_q$-dimension n dans $V = \mathbb{F}_{q^m}^k$. Alors pour tout sous-espace $\mathbb{F}_{q^m}$-linéaire M de codimension s on a

$$\mathrm{wt}_U(M) \geq n - sm. \tag{5.1}$$

De plus, si H est un hyperplan de $\mathbb{F}_{q^m}^k$, alors

$$\mathrm{wt}_U(H) \leq n - k.$$

Preuve. La première inégalité est une conséquence directe de la formule de Grassmann. On a en effet

$$\begin{aligned}\mathrm{wt}_{\mathcal{U}}(\mathcal{M}) &= \dim_{\mathbb{F}_q}(\mathcal{M} \cap \mathcal{U}) = \dim_{\mathbb{F}_q}(\mathcal{M}) + \dim_{\mathbb{F}_q}(\mathcal{U}) - \dim_{\mathbb{F}_q}(\mathcal{M} + \mathcal{U}) \\ &\geq \dim_{\mathbb{F}_q}(\mathcal{M}) + \dim_{\mathbb{F}_q}(\mathcal{U}) - \dim_{\mathbb{F}_q}(\mathcal{V}) \\ &= m(k-s) + n - mk.\end{aligned}$$

Pour la seconde inégalité, supposons qu'il existe un hyperplan H' tel que $\mathrm{wt}_U(H) \geq n-k+1$, avec U non inclus dans H'. Alors il y a au plus $k-1$ vecteurs $\mathbb{F}_q$-linéairement indépendants qui sont dans un autre hyperplan, mettons $\bar{H}$. Par conséquent on a

$$U = \langle U \cap H' \rangle_q \oplus \langle U \cap \bar{H} \rangle_q,$$

et donc U est 2-générable. □

L'une des conséquences immédiates est la suivante.

Corollaire 5.3.2. Soit U un q-système qui ne soit pas 2-générable. Alors $n \geq 2k-1$ et $k \leq m$.

Preuve. Soit $\underline{u}_1, \ldots, \underline{u}_{k-1}$ des vecteurs $\mathbb{F}_q$-linéairement indépendants de U. Alors ils sont inclus dans un hyperplan H. D'après (5.1), on obtient

$$n - m \leq \mathrm{wt}_U(H) \leq n - k,$$

i.e. $n \geq 2k-1$. La seconde inégalité est alors une conséquence immédiate de la proposition précédente. □

Théorème 5.3.3. Soit $\mathcal{C}$ un $[n,k,d]_{q^m/q}$-code intersectant. Alors

$$k \leq d \leq m.$$

Preuve. L'assertion $k \leq m$ est une conséquence triviale du corollaire.

En ce qui concerne $k \leq d$, on observe que la distance minimale en métrique rang est

$$d = d_R = \min_{A \in GL(n,q)} d_H(\mathcal{C} \cdot A) \geq k,$$

ce qui est vrai selon 4.1.4 tout code de la forme $\mathcal{C} \cdot A$ est intersectant en métrique de Hamming □

Corollaire 5.3.4. Si $n = 2k - 1$, et si $n \leq m$, alors un $[n, k, d]_{q^m/q}$-code intersectant est un code MRD.

Preuve. Quand $n \leq m$, la borne de Singleton est $k + d \leq n + 1$. D'après le théorème précédent, on a $k \leq d$, ce qui combiné avec la borne de Singleton donne $2k \leq k+d \leq n+1$. Si $n = 2k-1$, alors nécéssairement les deux inégalités sont des égalités, et le code est MRD. □

Théorème 5.3.5. Soit $2 \leq k \leq \lfloor \frac{m+1}{2} \rfloor$. Il existe un code intersectant non dégénéré de paramètres $[n, k, > \frac{n}{2}]_{q^m/q}$ pour tout

$$n \in \{m, \ldots, 2m - 2k + 1\}.$$

Preuve. Nous allons utiliser les q-systèmes.

Soit $\mathcal{W}$ un $[m, k]_{q^m/q}$ système qui soit éparpillé par rapport aux hyperplans (par exemple correspondant à un code de Gabidulin de paramètres $[m, k, m - k + 1]_{q^m/q}$). Soit $\overline{\mathcal{W}}$ un sous-espace $\mathbb{F}_q$-linéaire de $\mathbb{F}_{q^m}^k$ de dimension $r \leq m(k-1)$ et tel que $\mathcal{W} \cap \overline{\mathcal{W}} = \{0\}$.

Posons $\mathcal{U} = \mathcal{W} \oplus \overline{\mathcal{W}}$. Alors $n := \dim_{\mathbb{F}_q} \mathcal{U} = m + r$.

Nous voulons montrer que $\mathcal{U}$ n'est pas 2-générable quand $r \leq m - 2k + 1$.

Supposons que $r \leq m - 2k + 1$ et qu'il existe un hyperplan $\mathcal{H}$ tel que $\mathrm{wt}_{\mathcal{U}}(\mathcal{H}) \geq \frac{n}{2}$. Alors

$$\begin{aligned}
w_{\mathcal{W}}(\mathcal{H}) &= \dim_{\mathbb{F}_q}(\mathcal{H} \cap \mathcal{W}) \\
&= \dim_{\mathbb{F}_q}(\mathcal{H} \cap \mathcal{U} \cap \mathcal{W}) \\
&= \dim_{\mathbb{F}_q}(\mathcal{H} \cap \mathcal{U}) + \dim_{\mathbb{F}_q}(\mathcal{W}) - \dim_{\mathbb{F}_q}((\mathcal{H} \cap \mathcal{U}) + \mathcal{W}) \\
&\geq \dim_{\mathbb{F}_q}(\mathcal{H} \cap \mathcal{U}) + \dim_{\mathbb{F}_q}(\mathcal{W}) - \dim_{\mathbb{F}_q}(\mathcal{U}) \\
&\geq \frac{m+r}{2} + m - (m+r) \\
&= \frac{m-r}{2} \\
&\geq \frac{m-(m-2k+1)}{2} \geq k,
\end{aligned}$$

ce qui contredit le fait que $\mathcal{W}$ est éparpillé par rapport aux hyperplans. Par conséquent $\mathrm{wt}_{\mathcal{U}}(\mathcal{H}) < \frac{n}{2}$ pour tout hyperplan $\mathcal{H}$, de sorte que $\mathcal{U}$ n'est pas 2-générable. De plus, le poids de tout mot de code du code associé est au moins $n - \frac{n}{2} = \frac{n}{2}$. □

Remarque 5.3.6. Dans la preuve ci-dessus, pour obtenir la contradiction, on a besoin d'avoir $m-r > 2(k-1)$, ce qui donne bien $r < m-2k+2$, i.e. $r \leq m-2k+1$. Pour des valeurs de r plus grandes, le raisonnement suivi ne permet pas de conclure que U n'est pas 2-générable.

Proposition 5.3.7. Soit U un q-système de rang $n = 2m$ dans $\mathbb{F}_{q^m}^k$. Alors U est 2-générable.

Preuve. D'abord, remarquons que $|L_{\mathcal{U}}| \leq \frac{q^{2m}-1}{q-1}$. Ceci implique que $L_{\mathcal{U}}$ ne peut pas intersecter tous les sous-espaces $\mathbb{F}_{q^m}$-linéaires de codimension 2. En effet, si $L_{\mathcal{U}}$ intersectait chaque sous-espace de ce type, ce serait un ensemble 2-bloquant, et on sait d'après [20] que les ensembles 2-bloquants ont une taille d'au moins $q^{2m}+q^m+1$.

Ainsi, il existe un sous-espace $\mathbb{F}_{q^m}$-linéaire $\mathcal{M}$ de codimension 2 dans $\mathbb{F}_{q^m}^k$ dont l'intersection avec $\mathcal{U}$ est triviale. Soient $\mathcal{H}_1$ et $\mathcal{H}_2$ deux hyperplans distincts tels que $\mathcal{M} = \mathcal{H}_1 \cap \mathcal{H}_2$; alors

$$\mathrm{wt}_{\mathcal{U}}(\mathcal{H}_i) = \dim_{\mathbb{F}_q}(\mathcal{H}_i \cap \mathcal{U}) = \dim_{\mathbb{F}_q} \mathcal{H}_i + \dim_{\mathbb{F}_q} \mathcal{U} - \dim_{\mathbb{F}_q}(\mathcal{H}_i + \mathcal{U}) \geq m(k-1) + 2m - mk = m$$

pour $i \in 1, 2$. De plus,

$$(\mathcal{U} \cap \mathcal{H}_1) \cap (\mathcal{U} \cap \mathcal{H}_2) = \mathcal{U} \cap (\mathcal{H}_1 \cap \mathcal{H}_2) = \mathcal{U} \cap \mathcal{M} = \{0\},$$

de sorte que $\mathcal{U} = \langle \mathcal{U} \cap \mathcal{H}_1 \rangle \oplus \langle \mathcal{U} \cap \mathcal{H}_2 \rangle$, et donc $\mathcal{U}$ est 2-générable. □

Proposition 5.3.8. Soit U un q-système de rang $n > 2m$. Alors U est 2-générable.

Preuve. L'espace $\mathbb{F}_q$-linéaire $\mathcal{U}$ contient un espace $\mathbb{F}_q$-linéaire $\mathcal{W}$ de dimension $2m$. Soit $\mathcal{M}$ un sous-espace $\mathbb{F}_{q^m}$-linéaire de codimension 2 dans $\mathbb{F}_{q^m}^k$ dont l'intersection avec $\mathcal{W}$ est triviale (qui existe d'après le même argument que plus haut). Notons que $\mathcal{W} \oplus \mathcal{M} = \mathbb{F}_{q^m}^k$, de sorte que $\mathcal{U} + \mathcal{M} = \mathbb{F}_{q^m}^k$. Par conséquent, d'après la formule de Grassmann, on a

$$\mathrm{wt}_{\mathcal{U}}(\mathcal{M}) = n - 2m.$$

Soient $\mathcal{H}_1$ et $\mathcal{H}_2$ deux hyperplans tels que $\mathcal{M} = \mathcal{H}_1 \cap \mathcal{H}_2$. Alors

$$\mathrm{wt}_{\mathcal{U}}(\mathcal{H}_i) \geq n - m,$$

pour $i \in \{1, 2\}$. On a alors

$$\begin{aligned}
\dim_{\mathbb{F}_q}(\mathcal{U} \cap \mathcal{H}_1 + \mathcal{U} \cap \mathcal{H}_2) &= \dim_{\mathbb{F}_q} \mathcal{U} \cap \mathcal{H}_1 + \dim_{\mathbb{F}_q} \mathcal{U} \cap \mathcal{H}_2 - \dim_{\mathbb{F}_q} \mathcal{U} \cap \mathcal{H}_1 \cap \mathcal{H}_2 \\
&= \mathrm{wt}_{\mathcal{U}}(\mathcal{H}_1) + \mathrm{wt}_{\mathcal{U}}(\mathcal{H}_2) - \mathrm{wt}_{\mathcal{U}}(\mathcal{M}) \\
&\geq n - m + n - m - n + 2m = n.
\end{aligned}$$

Par conséquent, on a bien $\mathcal{U} = \mathcal{U} \cap \mathcal{H}_1 + \mathcal{U} \cap \mathcal{H}_2$, et donc $\mathcal{U}$ est 2-générable. □

Proposition 5.3.9. Soit U un q-système de rang $2m-1$ dans $\mathbb{F}_{q^m}^k$. Alors U est 2-générable.

Preuve. Soit $\mathcal{H}$ un hyperplan de $\mathbb{F}_{q^m}^k$. D'après (5.1), on a $\mathrm{wt}_{\mathcal{U}}(\mathcal{H}) \geq m-1$. Soit $\mathcal{M}$ un sous-espace $\mathbb{F}_{q^m}$-linéaire de codimension 2 dans $\mathbb{F}_{q^m}^k$ dont l'intersection avec $\mathcal{U}$ est triviale (qui existe d'après le même argument que plus haut). On a alors $(\mathcal{U}\cap\mathcal{H}_1)\cap(\mathcal{U}\cap\mathcal{H}_2)=\{0\}$ pour toutes les paires d'hyperplans différents $\mathcal{H}_1,\mathcal{H}_2$ contenant $\mathcal{M}$, de sorte que les intersections de $\mathcal{U}\setminus\{0\}$ avec tous les hyperplans contenant $\mathcal{M}$ forment une partition de $\mathcal{U}\setminus\{0\}$. Si tous les q^m+1 hyperplans contenant $\mathcal{M}$ ont poids $m-1$ dans $\mathcal{U}$, alors

$$(q^{m-1}-1)(q^m+1) < |\mathcal{U}|-1 = q^{2m-1}-1,$$

une contradiction. Par des arguments simples de cardinalité, il existe un hyperplan $\mathcal{H}$ contenant $\mathcal{M}$ de poids m dans $\mathcal{U}$, et tous les autres ont poids $m-1$. En particulier, on a $\mathcal{U}=\mathcal{U}\cap\mathcal{H}+\mathcal{U}\cap\mathcal{H}'$, avec $\mathcal{H}'$ choisi parmi n'importe lequel des autres hyperplans contenant $\mathcal{M}$. □

Proposition 5.3.10. Soit U un q-système de rang $2m-2$ dans $\mathbb{F}_{q^m}^k$. Alors U est 2-générable.

Preuve. Soit $\mathcal{H}$ un hyperplan de $\mathbb{F}_{q^m}^k$. D'après (5.1), on a $\mathrm{wt}_{\mathcal{U}}(\mathcal{H}) \geq m-2$. Soit $\mathcal{M}$ un sous-espace $\mathbb{F}_{q^m}$-linéaire de codimension 2 dans $\mathbb{F}_{q^m}^k$ dont l'intersection avec $\mathcal{U}$ est triviale (qui existe d'après le même argument que plus haut). Encore une fois, les intersections de $\mathcal{U}\setminus\{0\}$ avec tous les hyperplans contenant $\mathcal{M}$ forment une partition de $\mathcal{U}\setminus\{0\}$. S'il existe un hyperplan contenant $\mathcal{M}$ de poids m, alors $\mathcal{U}$ est 2-générable. Supposons que tous les q^m+1 hyperplans contenant $\mathcal{M}$ ont poids $m-1$ ou $m-2$ dans U. Soit a et b le nombres d'hyperplans contenant $\mathcal{M}$ de poids respectivement $m-1$ et $m-2$ dans $\mathcal{U}$. Alors la seule solution du système

$$\begin{cases} a(q^{m-1}-1)+b(q^{m-2}-1) = q^{2m-2}-1 \\ a+b = q^m+1, \end{cases}$$

est $a=q+1$ et $b=q^m-q$. Par conséquent, il existe au moins 2 hyperplans contenant $\mathcal{M}$ de poids $m-1$ dans $\mathcal{U}$, qui est donc bien 2-générable. □

Remarque 5.3.11. Il est important de remarquer qu'il est impossible de poursuivre cette ligne de raisonnement pour $n=2m-3$ voire au-delà, parce qu'il existe des solutions au système plus haut qui permettent l'existence d'hyperplans dont les poids sont trop petits.

On peut résumer la situation ainsi. Un code $\mathbb{F}_{q^m}$-linéaire en métrique rang est intersectant si et seulement si le q-système associé n'est pas 2-générable.

Or, un q-système U dans $\mathbb{F}_{q^m}^k$ qui n'est pas 2-générable vérifie nécéssairement $n<2m-2$. De plus, il existe des codes de métrique de rang intersectants non dégénérés de paramètres $[n,k,d]_{q^m/q}$ pour $n\in 2k-1,\ldots,2m-2k+1$ (avec $2\leq k\leq\frac{m+1}{2}$).

Il reste donc une *zone grise*, à savoir $2m-2k+2 \leq n \leq 2m-3$, pour laquelle les résultats exposés plus hauts ne permettent pas de déduire s'il existe ou pas un q-système qui ne soit pas 2-générable.

Pour $k = 2$, la zone grise est vide. Il est donc intéressant de considérer la plus grande dimension. Dans la sous-section suivante, nous nous concentrerons sur le cas $k = 3$ et $m = 5$.

5.4 L'étude de la zone grise quand $k = 3$

Quand $k = 3$, les valeurs de n pour lesquelles il est *a priori* inconnu s'il existe des q-systèmes qui ne soient pas 2-générables sont $n = 2m - 4$ et $n = 2m - 3$. Nous allons examiner leur existence en utilisant l'espace projectif, et en nous intéressant à l'ensemble linéaire $L_{\mathcal{U}}$ associé au q-système considéré.

Cette approche est intéressante pour une première étude de la zone grise pour deux raisons. La première est le nombre réduit de valeurs de n à considérer. La deuxième est que l'espace projectif en question n'est rien d'autre que le plan projectif $\mathrm{PG}(2, q^m)$, qui est relativement simple à concevoir du point de vue géométrique.

Proposition 5.4.1. Soit $\mathcal{U}$ un q-système dans $\mathbb{F}_{q^m}^3$ qui ne soit pas 2-générable. Alors $L_{\mathcal{U}} \neq \mathrm{PG}(2, q^m)$.

Preuve. Supposons que $L_{\mathcal{U}} = \mathrm{PG}(2, q^m)$. Alors on a

$$q^{2m} + q^m + 1 = L_{\mathcal{U}} \leq \frac{q^n - 1}{q - 1} = q^{n-1} + \cdots + q + 1,$$

ce qui implique $2m \leq n - 1$ et donc $n \geq 2m + 1$, ce qui est impossible si $\mathcal{U}$ n'est pas 2-générable. □

Grâce à cette proposition, pour chercher des q-systèmes de rang 3 qui ne soient pas 2-générables, on pourra supposer qu'il existe un point $P \in \mathrm{PG}(2, q^m) \setminus L_{\mathcal{U}}$.

Le théorème suivant donne alors une condition suffisante pour qu'un q-système soit 2-générable.

Théorème 5.4.2. Soit $\mathcal{U}$ un q-système de rang n dans $\mathbb{F}_{q^m}^3$, et soit $P \in \mathrm{PG}(2, q^m) \setminus L_{\mathcal{U}}$. S'il existe deux droites distinctes ℓ_1, ℓ_2 passant par P et telles que

$$\mathrm{wt}_{\mathcal{U}}(\ell_1) + \mathrm{wt}_{\mathcal{U}}(\ell_2) = n,$$

alors $\mathcal{U}$ est 2-générable.

Preuve. Si on a $\mathrm{wt}_{\mathcal{U}}(\ell_1) + \mathrm{wt}_{\mathcal{U}}(\ell_2) = n$, alors les hyperplans correspondant aux droites ℓ_1, ℓ_2 vérifient $\mathcal{H}_1 \cap \mathcal{H}_2 \cap \mathcal{U} = \{0\}$ puisque $P \notin L_{\mathcal{U}}$. Par conséquent, on a bien

$$\mathcal{U} = \mathcal{U} \cap \mathcal{H}_1 + \mathcal{U} \cap H_2,$$

et $\mathcal{U}$ est 2-générable. □

Ce théorème nous donne donc une méthode géométrique pour déterminer si un code est intersectant.

Nous allons voir que $m = 5$ est le premier entier pour lequel la question de la zone grise est pertinente.

Puisque $m \geq k$, on commence par examiner $m = 3$. La zone grise est donc $n = 2$, qui est impossible car $k = 3$, et $n = 3$, pour lequel le code n'est rien d'autre que l'espace entier, et n'est pas intersectant.

Pour le cas $m = 4$, la zone grise est constituée de $n = 4$ et $n = 5$. Pour $n = 4$, on doit avoir un $[4, 3, 3]_{q^4/q}$-code intersectant, ce qui viole la borne de Singleton. Pour $n = 5$, on doit avoir un $[5, 3, \geq 3]_{q^4/q}$, ce qui viole également la borne de Singleton.

Nous nous intéressons donc au cas $m = 5$, pour lequel la zone grise est constituée de $n = 6$ et $n = 7$.

Quand $n = 7$, d'après la Proposition 5.3.1, les poids admissibles pour le poids d'une ligne ℓ passant par P, noté $\mathrm{wt}_{\mathcal{U}}(\ell)$ sont $\{2, 3, 4\}$. D'après [44, Theorem 5.3], il y a $q^2 + 1$ droites de poids 4 dans $\mathcal{U}$. Soit ℓ l'une de ces droites, et soit P un point sur cette droite. Si toutes les autres droites passant par P ont poids 2 dans $\mathcal{U}$, on a

$$q^4 - 1 + (q^2 - 1)q^5 < |U| - 1 = q^7,$$

une contradiction. Par conséquent il existe une autre droite passant par P de poids 3, ce qui conclut d'après le Théorème 5.4.2.

Par conséquent il n'existe pas de q-système 2-générable pour $k = 3$, $m = 5$ et $n = 7$.

Le cas $n = 6$ est considérablement plus difficile à traiter. Pour l'heure, il s'agit encore d'un problème ouvert, qui est en cours d'examination. Un tel code intersectant devrait avoir paramètres $[6, 3, 3]_{q^5/q}$, mais son existence reste incertaine.

Bibliography

[1] M. Aaltonen. Linear programming bounds for tree codes (corresp.). *IEEE Transactions on Information Theory*, 25(1):85–90, 1979.

[2] M. Aaltonen. A new upper bound on nonbinary block codes. *Discrete Mathematics*, 83(2):139–160, 1990.

[3] G. N. Alfarano, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Advances in Mathematics of Communications*, 16(1):115–133, 2022.

[4] G. N. Alfarano, M. Borello, and A. Neri. Outer strong blocking sets. *The Electronic Journal of Combinatorics*, 31(2), 2024.

[5] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Linear cutting blocking sets and minimal codes in the rank metric. *Journal of Combinatorial Theory, Series A*, 192:105658, 2022.

[6] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Three combinatorial perspectives on minimal codes. *SIAM Journal on Discrete Mathematics*, 36(1):461–489, 2022.

[7] N. Alon. Explicit expanders of every degree and size. *Combinatorica*, 41:447 – 463, 2020.

[8] N. Alon, A. Bishnoi, S. Das, and A. Neri. Strong blocking sets and minimal codes from expander graphs. *Transactions of the American Mathematical Society*, 377(08):5389–5410, 2024.

[9] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.

[10] S. Ball and A. Blokhuis. On the size of a double blocking set inpg(2,q). *Finite Fields and Their Applications*, 2:125–137, 1996.

[11] D. Bartoli and M. Borello. Small strong blocking sets by concatenation. *SIAM Journal on Discrete Mathematics*, 37(1):65–82, 2023.

[12] D. Bartoli, M. Borello, and G. Marino. Saturating linear sets of minimal rank. *Finite Fields and Their Applications*, 95:102390, 2024.

[13] D. Bartoli, M. Borello, G. Marino, and M. Scotti. Linear rank-metric intersecting codes, 2025.

[14] D. Bartoli, A. Cossidente, G. Marino, and F. Pavese. On cutting blocking sets and their codes. *Forum Math.*, 34(2):347–368, 2022.

[15] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth. Towers of function fields over non-prime finite fields. *Moscow Mathematical Journal*, 15, 02 2012.

[16] A. Bishnoi, J. D'haeseleer, D. Gijswijt, and A. Potukuchi. Blocking sets, minimal codes and trifferent codes. *Journal of the London Mathematical Society*, 109, 2023.

[17] S. R. Blackburn. Frameproof codes. *SIAM Journal on Discrete Mathematics*, 16(3):499–510, 2003.

[18] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *Journal of Algebraic Combinatorics*, 53(2):327–341, 2021.

[19] M. Borello, W. Schmid, and M. Scotti. The geometry of intersecting codes and applications to additive combinatorics and factorization theory. *Journal of Combinatorial Theory, Series A*, 214:106023, 2025.

[20] R. Bose and R. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the hamming and the macdonald codes. *Journal of Combinatorial Theory*, 1(1):96–104, 1966.

[21] S. Boukheche, K. Merito, O. Ordaz, and W. A. Schmid. Monoids of sequences over finite abelian groups defined via zero-sums with respect to a given set of weights and applications to factorizations of norms of algebraic integers. *Communications in Algebra*, 50(10):4195–4217, 2022.

[22] G. Brassard, C. Crépeau, and M. Santha. Oblivious transfers and intersecting codes. *IACR Cryptol. ePrint Arch.*, 1996:10, 1996.

[23] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *International Conference on Information Security and Cryptology*, pages 34–46. Springer, 2013.

[24] L. Claborn. Every abelian group is a class group. *Pacific Journal of Mathematics*, 18:219–222, 1966.

[25] G. D. Cohen and A. Lempel. Linear intersecting codes. *Discrete Mathematics*, 56:35–43, 1984.

[26] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *IMA International Conference on Cryptography and Coding*, pages 85–98. Springer, 2013.

[27] G. D. Cohen and G. Zémor. Intersecting codes and independent families. *IEEE Transactions on Information Theory*, 40(6):1872–1881, 1994.

[28] G. D. Cohen and G. Zemor. Subset sums and coding theory. *Astérisque*, 258:327–339, 1999.

[29] G. D. Cohnen, S. Encheva, S. Litsyn, and H. G. Schaathun. Intersecting codes and separating codes. *Discrete Applied Mathematics*, 128(1):75–83, 2003.

[30] C. Crépeau and M. Sántha. Efficient reduction among oblivious transfer protocols based on new self-intersecting codes. In *Sequences II: Methods in Communication, Security, and Computer Science*, pages 360–368. Springer, 1993.

[31] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Advances in Mathematics of Communications*, 5(1):119, 2011.

[32] W. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: A survey. *Expositiones Mathematicae*, 24(4):337–369, 2006.

[33] A. Geroldinger, F. Halter-Koch, and Q. Zhong. On monoids of weighted zero-sum sequences and applications to norm monoids in galois number fields and binary quadratic forms. *Acta Mathematica Hungarica*, 168(1):144–185, 2022.

[34] A. Geroldinger and R. Schneider. On davenport's constant. *Journal of Combinatorial Theory, Series A*, 61(1):147–152, 1992.

[35] F. Gerth. Number fields with prescribed ℓ-class groups. *Proceedings of the American Mathematical Society*, 49(2):284–288, 1975.

[36] D. J. Grynkiewicz. *Structural additive theory*, volume 30. Springer, 2013.

[37] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. *Finite Fields and Their Applications*, 54:176–196, 2018.

[38] W. C. Huffman, J. Kim, and P. Sole. *Concise Encyclopedia of Coding Theory*. CRC Press, 2021.

[39] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2010.

[40] R. E. Jamison. Covering finite fields with cosets of subspaces. *Journal of Combinatorial Theory, Series A*, 22(3):253–266, 1977.

[41] G. Katona and J. Srivastava. Minimal 2-coverings of a finite affine space based on GF(2). *Journal of statistical planning and inference*, 8(3):375–388, 1983.

[42] S. Kurz. Divisible minimal codes. *arXiv preprint arXiv:2312.00885*, 2023.

[43] S. Kurz. Trifferent codes with small lengths. *Examples and Counterexamples*, 5:100139, 2024.

[44] S. Lia, G. Longobardi, G. Marino, and R. Trombetti. Short rank-metric codes and scattered subspaces. *SIAM Journal on Discrete Mathematics*, 38(4):2578–2598, 2024.

[45] G. Lunardon. Normal spreads. *Geom. Dedicata*, 75(3):245–261, 1999.

[46] G. Lunardon. MRD-codes and linear sets. *Journal of Combinatorial Theory, Series A*, 149:1–20, 2017.

[47] L. E. Marchan, O. Ordaz, I. Santos, and W. A. Schmid. Multi-wise and constrained fully weighted davenport constants and interactions with coding theory. *Journal of Combinatorial Theory, Series A*, 135:237–267, 2015.

[48] L. E. Marchan, O. Ordaz, and W. A. Schmid. Remarks on the plus–minus weighted davenport constant. *International Journal of Number Theory*, 10(05):1219–1239, 2014.

[49] G. Marino, A. Neri, and R. Trombetti. Evasive subspaces, generalized rank weights and near mrd codes. *Discrete Mathematics*, 346(12):113605, 2023.

[50] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch. New upper bounds on the rate of a code via the delsarte-macwilliams inequalities. *IEEE Transactions on Information Theory*, 23(2):157–166, 1977.

[51] S. Mesnager, Y. Qi, H. Ru, and C. Tang. Minimal linear codes from characteristic functions. *IEEE Transactions on Information Theory*, 66(9):5404–5413, 2020.

[52] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Transactions on Information Theory*, 66(4):2296–2310, 2019.

[53] J. Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[54] J. E. Olson. A combinatorial problem on finite abelian groups, i. *Journal of Number Theory*, 1(1):8–10, 1969.

[55] J. E. Olson. A combinatorial problem on finite abelian groups, ii. *Journal of Number Theory*, 1(2):195–199, 1969.

[56] V. Pepe. On subspaces defining linear sets of maximum rank. *Journal of Algebra*, 2025.

[57] A. Plagne and W. A. Schmid. An application of coding theory to estimating Davenport constants. *Designs, Codes and Cryptography*, 61:105–118, 2010.

[58] H. Randriambololona. (2, 1)-separating systems beyond the probabilistic bound. *Israel Journal of Mathematics*, 195:171–186, 2013.

[59] T. H. Randrianarisoa. A geometric approach to rank metric codes and a classification of constant weight codes. *Des. Codes, Cryptogr.*, 88(7):1331–1348, 2020.

[60] C. T. Retter. Intersecting Goppa codes. *IEEE Transactions on Information Theory*, 35(4):822–828, 1989.

[61] Y. L. Sagalovich and A. G. Chilingarjan. Separating systems and new scopes of its application. 2009.

[62] M. Scotti. On the lower bound for the length of minimal codes. *Discrete Mathematics*, 347(1):113676, 2024.

[63] M. Scotti. Recent advances on minimal codes, 2024.

[64] N. J. Sloane. Covering arrays and intersecting codes. *Journal of Combinatorial Designs*, 1(1):51–63, 1993.

[65] V. Smaldore. All minimal $[9, 4]_2$-codes are hyperbolic quadrics. *Examples and Counterexamples*, 3:100097, 2023.

[66] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Transactions on Information Theory*, 67(6):3690–3700, 2021.

[67] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991.

[68] C. Xing. Asymptotic bounds on frameproof codes. *IEEE Transactions on Information Theory*, 48(11):2991–2995, 2002.

[69] C. Zanella and F. Zullo. Vertex properties of maximum scattered linear sets of $pg(1, q^n)$. *Discrete Mathematics*, 343(5):111800, 2020.

[70] X. Zeng and P. Yuan. Weighted Davenport's constant and the weighted EGZ theorem. *Discrete mathematics*, 311(17):1940–1947, 2011.