Mémoire de master

Codes abéliens et combinatoire additive sur des groupes finis
Martino Borello & Wolfgang Schmid

Martin Scotti

Printemps 2022

1 Synthèse

Le contexte général

Dans ce rapport, nous étudions certains liens possibles entre la théorie des codes abéliens et le problème de la constante de Davenport d'un groupe abélien fini.

Un code abélien est un idéal d'un anneau de polynômes multivariés (les codes cycliques en sont un cas particulier, qui correspond au cas où il n'y a qu'une variable). La constante de Davenport d'un groupe abélien fini est la longueur de la plus longue suite sans sous-suite de somme nulle.

Connaître la constante de Davenport avec précision est un enjeu en théorie algébrique des nombres, où elle permet d'étudier le problème de la non-unicité de la factorisation dans certains corps de nombres (voir [GHK06] pour plus de détails). Elle est aussi utilisée par exemple dans la preuve de l'infinité des nombres de Carmichael (voir [AGP95]).

De nombreuses bornes sont connues sur la constante de Davenport, nous nous intéressons ici à la meilleure borne supérieure générale (i.e. sans hypothèses supplémentaires sur le groupe), prouvée pour la première fois en 1969 par van Emde Boas et Kruyswijk.

D'autres preuves existent, et dans un article de 1990, Meshulam donne une preuve basée sur un théorème d'incertitude, c'est cet article qui nous intéresse dans ce mémoire.

Le problème étudié

On connaît précisément la constante de Davenport lorsque le groupe G est d'exposant premier, et également dans le cas où le rang (i.e. le cardinal de la plus petite famille génératrice) est inférieur à 2. Les cas plus complexes sont un sujet actif de recherche (voir par exemple [GS92] ou même [Liu20] pour une contribution plus récente).

Pour l'instant la borne mentionnée plus haut affirme que pour un groupe abélien fini

G d'exposant m, sa constante de Davenport $d(G)$ vérifie

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

Un théorème d'incertitude en analyse harmonique relie le support d'une fonction avec celui de sa transformée de Fourier, la "philosophie générale" commune à ces théorèmes étant que parmi une fonction et sa transformée de Fourier, au moins l'une a un grand support (i.e. elles ne peuvent pas toutes les deux avoir un support petit).

Dans son article de 1990, Meshulam montre d'abord un théorème d'incertitude : il suppose d'abord que le support d'une fonction n'inclut aucun élément de $T_s = \{0,1\}^s \backslash \{0^s\}$, puis il utilise cette restriction sur supp f pour établir une borne inférieure sur supp $\hat{f}$. Enfin, il utilise ce théorème d'incertitude pour montrer la borne sur la constante de Davenport ci-dessus.

Des principes d'incertitude très similaires existent en théorie des codes (et sont un champ de recherche actif) : dans [EKL17] les auteurs montrent qu'une généralisation d'un théorème d'incertitude impliquerait que la famille de codes cycliques est asymptotiquement bonne. Ces techniques sont développées et généralisées dans les articles récents [BS22] et [BWZ22], et il est vraisemblable que l'étude de principes d'incertitudes donne encore des nouveaux résultats en théorie des codes.

Un premier objectif est donc de reformuler le théorème d'incertitude de Meshulam dans les termes de théorie des codes. Dès lors, nous voulons appliquer des techniques de la théorie des codes pour voir dans quelle mesure il est possible d'améliorer les résultats de Meshulam : modification du corps de base, groupement des racines d'un polynôme multivarié en classes d'équivalence (sous l'action du groupe de Galois) pour faire augmenter la dimension, etc.

La contribution proposée

Un premier résultat est que la preuve de Meshulam peut être entièrement reformulée dans les termes de la théorie des codes. Cette reformulation permet de mieux comprendre la preuve de Meshulam à certains endroits.

En particulier dans des cas simples la théorie des codes donne des résultats plus forts que ceux de Meshulam : sous certaines hypothèses un code cyclique dont on sait que la dimension est supérieure à 2 a en fait une dimension beaucoup plus grande.

Nous cherchons donc à généraliser les techniques de théorie des codes qui donnent ces résultats (concrètement on étudie l'action du groupe de Galois sur des racines d'un polynôme multivarié) et à les appliquer dans le contexte précis du théorème d'incertitude de Meshulam (où les hypothèses sur le sous-groupe sont fortes).

Les arguments en faveur de sa validité

Le théorème d'incertitude de Meshulam a pu être amélioré ou étendu dans des cadres plus restreints, où l'on dispose d'hypothèses supplémentaires (naturelles pour le cadre de la

théorie des codes et pour l'utilisation du groupe de Galois, ou pour le reste de la preuve de Meshulam).

Cependant nous n'avons pas été capables d'utiliser ces améliorations pour donner une meilleure borne sur la constante de Davenport, et il est vraisemblable que la preuve de Meshulam ne peut pas être améliorée de cette manière. Cela est dû au fait que la preuve de Meshulam n'omet pas de compter des racines obtenues avec l'action du groupe de Galois, et au fait que tous les sous-groupes d'un groupe abélien fini ont une décomposition en somme de classes cyclotomiques.

Le bilan et les perspectives

A ce stade plusieurs pistes de recherche s'ouvrent. Il est par exemple possible d'examiner d'autres théorèmes d'incertitude, voire d'étudier la distance minimale des codes abéliens impliqués dans la démonstration de Meshulam, dans les deux cas soit pour améliorer la borne sur la constante de Davenport, soit comme des problèmes indépendants. Inversement, des outils combinatoires peuvent être utilisés pour obtenir des résultats en théorie des codes, mais nous n'avons pas encore exploré cette piste.

2 Notions élémentaires

2.1 Code de groupe

Dans le présent mémoire nous examinerons des codes de groupe, dans le cas particulier où le groupe est abélien et fini.

Définition 2.1 (G-code)**.** *Soit G un groupe fini, et F un corps. Un G-code sur F est un idéal de l'algèbre de groupe*

$$FG = \left\{ \sum_{g \in G} a_g g \mid a_g \in F \right\}.$$

Si $\mathcal{C}$ est un idéal de FG, c'est aussi en particulier un sous-espace vectoriel de FG vu comme espace vectoriel, de ce fait on peut utiliser les définitions et notations connues de théorie des codes.

On note $dim(\mathcal{C})$ la dimension de $\mathcal{C}$ comme F-espace vectoriel. Soit $x \in \mathcal{C}$, on note $wt(x)$ son poids de Hamming (i.e. le nombre de coefficients de x non nuls). On note encore $d(\mathcal{C}) = min_{x \in \mathcal{C}}\, wt(x)$ la distance minimale de $\mathcal{C}$.

Soit $f : G \to F$ une fonction. Cette fonction a un représentant dans l'algèbre de groupe FG, il s'agit de $\sum_{g \in G} f(g) \cdot g$. Inversement, tout élément de FG peut être vu comme une

fonction de G dans F. Dans la suite, nous ferons souvent la confusion entre la fonction et l'élément de l'algèbre de groupe pour alléger les notations.

FG est un espace vectoriel, mais il possède une structure supplémentaire : le produit de convolution, défini dans FG par

$$\sum_{g\in G} f(g)g \cdot \sum_{g\in G} h(g)g = \sum_{g\in G} g\Big(\sum_{ab=g} f(a)h(b)\Big)$$

Cette multiplication fait de FG une algèbre de groupe. Muni de cette multiplication, on demande que $\mathcal{C}$ soit un idéal de FG.

Dans tout ce mémoire on ne considérera que le cas où $car(F) \nmid |G|$, et où G est un groupe abélien fini. FG est alors un anneau principal : c'est une conséquence du théorème de Maschke [GC13], où FG est vu comme la représentation régulière de G sur F. Cela implique que tout code est généré par un unique élément. Les codes abéliens auront donc tous la même forme : il seront générés par une fonction $f : G \to F$, et on aura $\mathcal{C} = fFG$.

Il est aussi utile à ce stade d'introduire le produit scalaire dans FG, défini par

$$\langle f \mid h\rangle = \sum_{g\in G} f(-g)h(g)$$

et que nous utiliserons abondemment dans la suite.

Exemple 2.2 (Codes cycliques)**.** *Un code cyclique est un sous-espace vectoriel de $F[X]/\langle X^m - 1\rangle$ stable par multiplication par X, donc par tout polynôme, donc un idéal de $F[X]/\langle X^m - 1\rangle \simeq FC_m$ où C_m désigne le groupe cyclique à m éléments.*

2.2 Le groupe dual

Définition 2.3 (Groupe dual)**.** *Soit G un groupe abélien fini d'exposant m, et F un corps possédant des racines primitives m-ièmes. On note $\hat{G}$ le groupe des homomorphismes de G dans F (muni de la loi $(\chi \cdot \chi')(g) = \chi(g) \times \chi'(g)$), c'est le groupe dual de G.*

Le théorème de structure des groupes abéliens fini (une conséquence du théorème de Maschke [GC13]) permet de décomposer tout groupe abélien fini en produit de groupes cycliques :

$$G \simeq \prod_{i=1}^{r} C_{n_i}$$

avec $n_1 \mid n_2 \mid \cdots \mid n_r$.

Définition 2.4. *En notant $G \simeq \prod_{i=1}^{r} C_{m_i}$ par exemple en utilisant le théorème de structure des groupes abéliens finis (et $m = ppcm(m_i) = \exp(G)$), on définit le produit scalaire :*

$$\forall g, h \in G \quad g \cdot h = \sum_{i=1}^{r} g_i h_i \pmod{m}$$

où la multiplication $g_i \cdot h_i$ est celle héritée de la structure d'anneau de $\mathbb{Z}/m_i\mathbb{Z}$ (que l'on confond ici avec le groupe cyclique C_{m_i}).

Proposition 2.5. *Soit $\zeta \in F$ une racine primitive m-ième de l'unité. Alors $\phi_\zeta : g \mapsto \chi_g$ où $\chi_g(h) = \zeta^{g \cdot h}$ définit un isomorphisme de groupe $G \simeq \hat{G}$.*

Cet isomorphisme n'est pas canonique (car il dépend du choix de ζ).

Les caractères, en tant que fonctions, peuvent être vus comme des éléments de l'algèbre de groupe FG. En tant que tels, ils possèdent des propriétés d'orthogonalité intéressantes.

Proposition 2.6. *Soit χ et χ' deux caractères de FG. Alors*

$$\langle \chi \mid \chi' \rangle = \delta_{\chi,\chi'} \cdot |G|$$

$$\chi \times \chi' = \delta_{\chi,\chi'} \cdot |G| \cdot \chi$$

Preuve. En annexe. □

On en déduit la proposition suivante :

Proposition 2.7. *Les caractères forment une base orthogonale de FG.*

Preuve. Puisque $dim(FG) = |G| = |\hat{G}|$, il suffit de montrer que les caractères sont libres. Si $a = \sum_{i=1}^{r} \lambda_i \chi_i = 0$ alors $0 = \langle a \mid \chi_i \rangle = \lambda_i$, et les caractères sont donc bien libres. □

Notons qu'en général on a, en notant I et J deux ensembles de caractères,

$$\Big(\sum_{i \in I} \lambda_i \chi_i\Big) \times \Big(\sum_{j \in J} \mu_j \chi_j\Big) = \sum_{i \in I \cap J} \lambda_i \mu_i \chi_i$$

Cela signifie que si $\langle f \mid \chi \rangle \neq 0$, alors $Vect(\chi)$, qui est un espace de dimension 1, vérifie $Vect(\chi) \subset \langle f \rangle$. Il s'agit alors de savoir quels sont les caractères sur lesquels l'idéal $\langle f \rangle$ sera défini.

2.3 Transformée de Fourier

La transformée de Fourier permet de déterminer quels caractères participent à la décomposition de f en caractères.

Définition 2.8 (Transformée de Fourier)**.** *La transformée de Fourier de $f : G \to F$ est*

$$\hat{f} : \hat{G} \to F$$

définie par

$$\hat{f}(\chi) = \langle \chi \mid f \rangle = \sum_{g \in G} \bar{\chi}(g) f(g)$$

On a alors

$$f = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \cdot \chi$$

En utilisant l'isomorphisme $G \simeq_\zeta \hat{G}$ on peut donner une définition légèrement différente, et plus pratique pour l'examen de FG.

Définition 2.9 (Transformée de Fourier)**.** *La transformée de Fourier de $f : G \to F$ est*

$$\hat{f} : G \to F$$

définie par

$$\hat{f}(x) = \sum_{y \in G} f(y) \zeta^{-x \cdot y}$$

La transformée inverse donne alors

$$f(x) = \frac{1}{|G|} \sum_{y \in G} \hat{f}(y) \zeta^{x \cdot y}$$

Tout ce travail de décomposition en caractères permet d'expliciter naturellement le lien entre la dimension d'un code (i.e. un idéal) et la transformée de Fourier de son générateur (on rappelle que l'idéal est principal), résumé dans le lemme suivant.

Lemme 2.10. *Soit $f : G \to F$ le générateur d'un G-code sur F. Alors*

$$dim\langle f \rangle = |\operatorname{supp} \hat{f}|$$

Preuve. De la discussion sur les caractères il est clair que $\hat{f}(\chi) \neq 0$ équivaut à $Vect(\chi) \subset \langle f \rangle$, et puisque $Vect(\chi) \cap \langle f \rangle$ est soit $\{0\}$ soit $Vect(\chi)$ selon que $\hat{f}(\chi)$ vale respectivement 0 ou non, on en déduit l'égalité $dim\langle f \rangle = |\operatorname{supp} \hat{f}|$: la transformée de Fourier permet de compter les caractères linéaires impliqués dans la décomposition de f. □

2.4 La constante de Davenport

Le problème de la constante de Davenport est le suivant : étant donné un groupe abélien fini G, déterminer la longueur de la plus longue suite sans sous-somme nulle.

Plus formellement, on note

$$d(G) = \max\{s \in \mathbb{N} \mid \exists a_1, \ldots, a_s \in G \quad \forall \epsilon \in \{0,1\}^s \quad \big(\sum_{i=1}^{s} a_i \epsilon_i = 0 \implies \epsilon = 0\big)\}$$

et ce nombre s'appelle la constante de Davenport de G.

La littérature examine également la quantité $d(G)+1$, notée en général $D(G)$ et souvent aussi appelée constante de Davenport (selon les auteurs et le point de vue). Elle correspond au plus petit entier s tel que toute suite de s éléments de G a une sous-somme nulle. Pour plus de clarté, dans ce mémoire seul $d(G)$ sera appelé constante de Davenport.

Il s'agit dans un premier moment d'étudier quelques bornes simples sur $d(G)$. Il convient de commencer par une borne supérieure élémentaire.

Proposition 2.11. *Soit G un groupe abélien fini, et $a_1, \ldots, a_s$ une suite d'éléments de G sans sous-somme nulle. Alors $s < |G|$.*

Preuve. Notons $u_0 = 0$ et $u_i = a_1 + \cdots + a_i$ une nouvelle suite d'éléments de G. Si pour $i < j$ on a $u_i = u_j$ alors $0 = u_j - u_i = \sum_{k=i+1}^{j} a_k$ et la suite des a_i possède une sous-somme nulle. Par conséquent les u_i sont tous différents, donc $s \leq |G| - 1$, donc $s < |G|$. □

Il existe beaucoup d'autres bornes supérieures, mais toutes sont significativement plus dures à montrer. Le présent mémoire montre que pour un groupe G d'exposant m on a

$$d(G) \leq m(1 + \log \frac{|G|}{m})$$

Cette borne a été montrée de nombreuses fois, avec des méthodes diverses. C'est la meilleure borne supérieure valable pour tout groupe abélien fini (sans autres hypothèses supplémentaires).

Examinons à présent quelques bornes inférieures sur $d(G)$.

Proposition 2.12. *Soit $G = C_n$ un groupe cyclique d'ordre n. Alors $d(G) = n - 1$.*

Preuve. Il suffit de considérer la suite constante égale à 1, répété $n - 1$ fois. Aucune de ses sous-sommes n'est nulle, et elle atteint la borne supérieure montrée à la proposition précédente, donc elle est de longueur maximale. □

Un argument similaire permet de montrer que lorsque l'on utilise le lemme des restes chinois pour écrire un groupe abélien fini sous forme de produit de groupes cycliques

$$G \simeq \prod_{i=1}^{r} C_{n_i}$$

avec $n_1|n_2|\dots|n_r$, alors on a

$$d(G) \geq \sum_{i=1}^{r}(n_i - 1)$$

Cette borne inférieure est une égalité dans le cas où G est un p-groupe et dans le cas où G est de rang 2. Les deux sous-sections suivantes en restituent des démonstrations de J.E.Olson [Ols69a], [Ols69b] datant de 1969.

2.5 Le cas des p-groupes abéliens

Théorème 2.13. *Soit $G \simeq \prod_{i=1}^{r} C_{p^{\alpha_i}}$. Alors*

$$D(G) \leq 1 + \sum_{i=1}^{r}(p^{\alpha_i} - 1)$$

Preuve. En annexe. □

2.6 Le cas des groupes abéliens de rang 2

Théorème 2.14. *Soit $G = H \times K$ un groupe abélien, où $h = |H|$ divise $k = |K|$. Alors $D(G) \leq h + k - 1$.*

Corollaire 2.15. *Soit $G \simeq C_{n_1} \times C_{n_2}$ un groupe abélien fini de rang 2 (on suppose que $n_1 \mid n_2$). Alors*

$$d(G) = n_1 - 1 + n_2 - 1$$

Preuve du corollaire. La construction exposée plus haut donne un exemple de suite de longueur $n_1 - 1 + n_2 - 1$, ce qui indique que $d(G) \geq n_1 - 1 + n_2 - 1$. Inversement, d'après le théorème, on a $d(G) = D(G) - 1 \leq n_1 - 1 + n_2 - 1$. □

La démonstration du théorème est donnée en annexe.

3 L'article de Meshulam

Dans cette section nous restituons simplement le contenu de l'article de Meshulam [Mes90]. Nous l'examinerons plus en détail dans la suite en quête d'améliorations.

Définissons récursivement $\alpha(m, s)$ par $\alpha(m, 0) = 1$, et $\alpha(m, s) = \lceil \frac{m}{m-1}\alpha(a, s-1) \rceil$. Notons que $\alpha(m, i) = i + 1$ quand $i < m$, puis pour des grandes valeurs de s, $\alpha(m, s)$ adopte un comportement asymptotique exponentiel.

Théorème 3.1. *Soit F un corps fini avec des racines primitives m-ièmes de l'unité, et soit $f : \mathbb{Z}_m^s \to F$ vérifiant $f(0) = 1$ et $\forall \epsilon \in \{0,1\}^s \setminus 0^s \quad f(\epsilon) = 0$. Alors on a*

$$|\operatorname{supp} \hat{f}| \geq \alpha(m, s)$$

Avant de commencer la preuve nous montrons un petit lemme.

Lemme 3.2. *Soit $B_1, \dots, B_k$ des ensembles de cardinalité au moins u. Alors*

$$\Big|\bigcup_{i=1}^{k} B_i\Big| + \Big|\bigcap_{i=1}^{k} B_i\Big| \geq \frac{k}{k-1}u$$

Preuve du lemme. Notons $C_i = B_i \setminus (\cap_{i=1}^{k} B_i)$ et $|\cap_{i=1}^{k} B_i| = v$. En remarquant que $\cap_{i=1}^{k} C_i = \emptyset$ on obtient

$$(u-v)k \leq \big|\{(x,i) \mid x \in C_i\}\big| \leq \Big|\bigcup_{i=1}^{k} C_i\Big|(k-1)$$

On en déduit enfin

$$\Big|\bigcup_{i=1}^{k} B_i\Big| + \Big|\bigcap_{i=1}^{k} B_i\Big| = \Big|\bigcup_{i=1}^{k} C_i\Big| + 2v \geq \frac{k}{k-1}(u-v) + 2v \geq \frac{k}{k-1}u$$

□

Nous sommes à présent en mesure de montrer le théorème.

Preuve du théorème. Nous allons faire une récurrence sur s.

Supposons pour commencer que $s = 1$. $|\operatorname{supp} \hat{f}| = 1$ si et seulement si $f(x)$ est de la forme $C\zeta^{x \cdot x_0}$ (i.e. un caractère multiplié par un scalaire non nul), ce qui est impossible car alors $f(1) \neq 0$. Donc $|\operatorname{supp} \hat{f}| \geq 2 = \alpha(m, 1)$.

Supposons à présent que $s > 1$. Pour $y \in \mathbb{Z}_m$ on définit $f_y : \mathbb{Z}_m^{s-1} \to F$ en posant $f_y(x) = f(x, y)$. Pour $a \in \mathbb{Z}_m^{s-1}$ on définit $g_a : \mathbb{Z}_m \to F$ en posant $g_a(y) = \hat{f}_y(a)$. On a alors

$$\forall (a,b) \in \mathbb{Z}_m^{s-1} \times \mathbb{Z}_m \quad \hat{f}(a,b) = \sum_{x \in \mathbb{Z}_m^{s-1}} \sum_{y \in \mathbb{Z}_m} f(x,y)\zeta^{-x\cdot a - y \cdot b} = \sum_{y \in \mathbb{Z}_m} \hat{f}_y(a)\zeta^{-y\cdot b} = \hat{g_a}(b)$$

Par conséquent

$$|\operatorname{supp} \hat{f}| = \sum_{a \in \mathbb{Z}_m^{s-1}} |\operatorname{supp} \hat{g_a}| \tag{3.1}$$

Pour $0 \leq i \leq m-1$ on définit $h_i(x) = f_0(x) - \zeta^i f_1(x)$. Clairement $h_i : \mathbb{Z}_m^{s-1} \to F$ vérifie l'hypothèse de récurrence (i.e. les conditions du théorème avec $s-1$), donc $A_i = \operatorname{supp} \hat{h}_i$ vérifie $|A_i| \geq \alpha(m, s-1)$.

Puisque $A_i = \{a \in \mathbb{Z}_m^{s-1} \mid f_0(a) \neq \zeta^i f_1(a)\} = \{a \in \mathbb{Z}_m^{s-1} \mid g_a(0) \neq g_a(1)\}$ on peut faire deux observations.

$$a \in A_i \implies g_a \neq 0 \implies |\operatorname{supp} \hat{g_a}| \geq 1 \tag{3.2}$$

$$a \in \bigcap_{i=1}^{m} A_i \implies g_a \neq C\zeta^{yy_0} \implies |\operatorname{supp} \hat{g_a}| \geq 2 \tag{3.3}$$

On obtient donc, en utilisant le lemme avec $u = \alpha(m, s-1)$:

$$|\operatorname{supp} \hat{f}| = \sum_{a \in \mathbb{Z}_m^{s-1}} |\operatorname{supp} \hat{g_a}| \geq \Big|\bigcup_{i=1}^{m} A_i\Big| + \Big|\bigcap_{i=1}^{m} A_i\Big| \geq \lceil \frac{m}{m-1}\alpha(m, s-1)\rceil = \alpha(m, s)$$

□

Avant d'examiner les répercussions sur la constante de Davenport, il nous reste un petit lemme.

Lemme 3.3.

$$\forall s \geq m-1 \quad \alpha(m, s) \geq \frac{m}{e}\Big(\frac{m}{m-1}\Big)^s$$

Preuve. Puisque $\alpha(m, m-1) = m$ on a :

$$\alpha(m, s) \geq \alpha(m, m-1)\Big(\frac{m}{m-1}\Big)^{s-(m-1)} = m\Big(\frac{m}{m-1}\Big)^s\Big(\frac{m}{m-1}\Big)^{-(m-1)} \geq \frac{m}{e}\Big(\frac{m}{m-1}\Big)^s$$

□

Pour tout sous-groupe H de $\mathbb{Z}_m^s$ on note $H^\perp = \{a \in \mathbb{Z}_m^s \mid \forall h \in H \quad a \cdot h = 0\}$. On a ainsi $H^{\perp\perp} = H$ et $\hat{\mathbb{1}}_H = |H|\mathbb{1}_{H^\perp}$, comme le montrent les deux propositions suivantes.

Proposition 3.4. *Soit $H < \mathbb{Z}_m^s$. Alors*

$$H^{\perp\perp} = H$$

Preuve. On a pour commencer $H \subset H^{\perp\perp}$. En effet, $\forall x \in H^\perp \quad \forall h \in H \quad h \cdot x = 0$.

Nous allons montrer que

$$G/H \simeq H^\perp \tag{3.4}$$

ce qui impliquera le résultat voulu. En effet on aura alors $|G| = |H| \cdot |H^\perp|$ et $|G| = |\hat{G}| = |H^\perp| \cdot |H^{\perp\perp}|$, donc au final $|H| = |H^{\perp\perp}|$ donc, puisque $H \subset H^{\perp\perp}$, $H = H^{\perp\perp}$.

Pour prouver (3.4), il suffit de remarquer qu'un morphisme de G dans $F^\times$ qui s'annule sur H est déterminé par un morphisme de G/H dans $F^\times$, d'après le premier théorème d'isomorphisme. □

Proposition 3.5. *Soit $H < \mathbb{Z}_m^s$. Alors*

$$\hat{\mathbb{1}}_H = |H|\mathbb{1}_{H^\perp}$$

Preuve. Nous allons utiliser l'isomorphisme $\hat{G} \simeq_\zeta G$ introduit à la proposition 2.5, c'est-à-dire ϕ_ζ.

Notons $f = \phi_\zeta \circ \hat{\mathbb{1}}_H : G \to F^\times$. Si $x \in H^\perp$ on a :

$$\begin{aligned} f(x) &= \sum_{y \in H} \zeta^{-x \cdot y} \\ &= \sum_{y \in H} \zeta^0 \\ &= |H| \end{aligned}$$

D'autre part si $x \notin H^\perp$, on note $H = \langle h_1, \ldots, h_r \rangle$ une décomposition de H en générateurs, avec $k_i = ord(h_i) | m$, et on obtient :

$$\begin{aligned} f(x) &= \sum_{y \in H} \zeta^{-x \cdot y} \\ &= \prod_{i=1}^{r} \sum_{k=1}^{k_i} \zeta^{k h_i \cdot x} \end{aligned}$$

Puisque $x \notin H^\perp$, il existe un h_j tel que $x \cdot h_j = a \neq 0$. Mais alors pour un tel h_j on aura $\sum_{k=1}^{k_i} \zeta^{k h_i \cdot x} = \sum_{k=1}^{k_i} \zeta^{ka} = 0$, donc tout le produit vaut 0. □

Maintenant nous sommes en mesure de montrer la borne de Meshulam.

Théorème 3.6 (Borne de Meshulam sur la constante de Davenport)**.** *Soit $G = \prod_{i=1}^{r} C_{m_i}$ un groupe abélien d'exposant m et $s = s(G)$ sa constante de Davenport. Alors*

$$s \leq m\Big(1 + \log \frac{|G|}{m}\Big)$$

Preuve. Soit $a_1, \ldots, a_s$ une suite sans sous-somme nulle. Notons $a_i = (a_{i,1}, \ldots, a_{i,r})$, et posons $b_j = (a_{1,j}, \ldots, a_{s,j}) \in \mathbb{Z}_m$. Alors puisque $\forall j \quad ord(b_j) \mid m_j$, le groupe $H = \langle b_j \rangle_j \subset \mathbb{Z}_m^s$ est d'ordre au plus $\prod_{i=1}^{r} m_i = |G|$.

Puisque la suite des a_i n'a pas de sous-somme nulle, $H^\perp \cap \{0,1\}^s = 0^s$. En effet, si $\exists \epsilon \in \{0,1\}^s \cap H^\perp$ alors $\epsilon \cdot b_j = 0$ pour tout $1 \leq j \leq r$, et donc que $\sum_{i=1}^{s} a_i \epsilon_i = 0$. Puisque la suite a_i n'a pas de sous-somme nulle, $\epsilon = 0$.

Puisque $H^\perp \cap \{0,1\}^s = 0^s$, cela signifie que $\hat{\mathbb{1}}_{H^\perp}$ vérifie les conditions du théorème d'incertitude de Meshulam, ce qui donne:

$$\frac{m}{e}\Big(\frac{m}{m-1}\Big)^s \leq \alpha(m,s) \leq |\operatorname{supp} \hat{\mathbb{1}}_{H^\perp}| = |\operatorname{supp}(|H| \cdot \mathbb{1}_H)| = |H| \leq |G| \tag{3.5}$$

et donc

$$s \leq m\Big(1 + \log \frac{|G|}{m}\Big)$$

□

4 Les classes cyclotomiques de caractères

Dans cette section nous allons nous intéresser à des classes d'équivalence de caractères.

Reprenons quelques instants notre étude des caractères.

4.1 Motivation

En théorie des codes cycliques l'algèbre $\mathbb{F}_q[X]/\langle X^n - 1\rangle$ se décompose en utilisant les facteurs irréductibles de $X^n - 1$ dans $\mathbb{F}_q[X]$ (et le lemme des restes chinois). On obtient alors l'isomorphisme

$$\mathbb{F}_q[X]/\langle X^n - 1\rangle \simeq \prod_{\substack{P(X)|X^n-1 \\ P\ irr.}} \mathbb{F}_q[X]/\langle P(X)\rangle$$

Dans cette décomposition on notera que si les racines primitives n-ièmes de l'unité sont contenues dans le corps $\mathbb{F}_q$ alors les facteurs irréductibles sont de degré 1. Dans le cas contraire des facteurs de degré plus grand apparaissent : ce sont des polynômes dont les racines sont conjuguées (i.e. stables sous l'action du groupe de Galois).

Nous voulons obtenir des facteurs regroupant autant de racines que possible, c'est pourquoi nous nous placerons dans un corps "petit" (pour que l'extension contenant les racines primitives ait un grand groupe de Galois).

Dans le cas des codes cycliques la décomposition en facteurs de degré 1 équivaut au choix d'un caractère, et la décomposition en facteurs irréductibles sur un "petit" corps équivaut à étudier l'action du groupe de Galois sur ces racines, qui équivaut à son tour à l'action du groupe de Galois sur les caractères.

L'objet de la présente section est de généraliser cette étude des codes cycliques aux codes abéliens, afin d'obtenir une décomposition de FG en modules irréductibles de degré(s) le(s) plus grand possible(s).

4.2 Généralités sur les caractères

Nous nous plaçons dans le cas où F est un corps de cardinal q, et $G = \mathbb{Z}_m^s$, avec $q \nmid m$. Par conséquent il existe une extension de F (que l'on notera E) qui possède des racines primitives m-ièmes de l'unité.

Un caractère est un morphisme de groupes de G dans $E^\times$. Vu en tant qu'élément de l'algèbre de groupes EG il a la forme :

$$\chi = \sum_{g \in G} \chi(g) g$$

En reprenant l'isomorphisme ϕ_ζ entre G et $\hat{G}$ défini plus haut on peut écrire le caractère sous la forme :

$$\chi_{(a_1,\ldots,a_s)} = \sum_{(g_1,\ldots,g_s)\in\mathbb{Z}_m^s} \zeta^{a_1 g_1 + \cdots + a_s g_s}$$

Exemple 4.1. *Prenons $G = C_3^2$ et $F = \mathbb{F}_2$. On a alors $FG \simeq \mathbb{F}_2[X,Y]/\langle X^3-1, Y^3-1\rangle$. Le caractère correspondant à l'élément $(1,2)$ est alors celui muni des coefficients égaux à l'évaluation en $X_1 = \zeta^1$ et $X_2 = \zeta^2$:*

$$\begin{aligned}\chi_{(1,2)} &= 1 + \zeta X + \zeta^2 X^2 + \zeta^2 Y + XY + \zeta X^2 Y + \zeta Y^2 + \zeta^2 XY^2 + X^2Y^2 \\ &= (1 + XY + X^2Y^2)(1 + \zeta X + \zeta^2 X^2)\end{aligned}$$

Comme on peut l'observer sur l'exemple, les caractères admettent une factorisation, où l'un des facteurs ne contient aucune racine de l'unité : ses coefficients sont toujours 1 et ses éléments correspondent au noyau du caractère. L'autre facteur correspond aux différents cosets du noyau.

Il convient également à ce stade de montrer en quoi ces exemples sont une reformulation naturelle de ce que l'on sait déjà dans le cadre des codes cycliques. Soit $G = C_n$ le groupe cyclique d'ordre n, et $C = fFG$ un code cyclique engendré par une fonction f.

Supposons que F contienne toutes les racines n-ièmes de l'unité. ζ^a est une racine de f si et seulement si $\chi_a \notin \operatorname{supp} \hat{f}$. On a alors également $FG \simeq \prod_{i=1}^n F[X]/\langle X - \zeta^i\rangle$, et donc $fFG \simeq \prod_{\zeta^i \in \operatorname{supp} \hat{f}} F[X]/\langle X - \zeta^i\rangle$. En général, l'étude des racines du polynôme multivarié f peut donc se faire par le moyen des caractères. Elle détermine toute la structure du code engendré par f.

4.3 L'action du groupe de Galois sur les caractères

Si $E \neq F$ alors $Gal(E/F)$ n'est pas trivial et il est engendré par l'endomorphisme $\sigma : x \mapsto x^q$ (si q est premier c'est l'endomorphisme de Frobenius).

Le caractère $\chi : G \to E$ est alors l'objet de l'action du groupe de Galois, par exemple $\sigma \circ \chi : G \to E$ est aussi un caractère. On note alors $[\chi]_q$ la classe d'équivalence de χ engendrée par cette action de groupe.

Proposition 4.2. *La somme des caractères d'une même classe cyclotomique est une fonction de G dans F.*

Preuve. Soit $\chi : G \to E$ un caractère. En écrivant

$$S = \sum_{\chi' \in [\chi]_q} \chi' = \sum_{k=0}^{|[\chi]_q|-1} \sigma^k \circ \chi$$

on a bien que $\sigma(S) = S$ donc $S \in FG$. □

On remarque de plus que la transformée de Fourier d'une fonction $f : G \to F$, qui donne la valeur du coefficient du caractère, commute avec l'action du groupe de Galois :

$$\begin{aligned}\hat{f}(\sigma \circ \chi) &= \sum_{g \in G} f(g) \cdot \sigma \circ \chi(-g) \\ &= \sum_{g \in G} \sigma \circ f(g) \cdot \sigma \circ \chi(-g) \\ &= \sigma \circ \sum_{g \in G} f(g) \cdot \sigma\chi(-g) \\ &= \sigma \circ \hat{f}(\chi)\end{aligned}$$

En pratique nous examinons les caractères sous leur forme donnée par l'isomorphisme entre G et $\hat{G}$. L'action du groupe de Galois est alors simple à décrire :

Proposition 4.3. *Soit $\chi \in \hat{G}$ tel que $\chi = \phi_\zeta((a_1, \ldots, a_s))$.*

$$\phi_\zeta^{-1}(\sigma \circ \chi) = q \cdot (a_1, \ldots, a_s) = (qa_1, \ldots, qa_s)$$

Preuve. En annexe. □

Exemple 4.4. *Prenons $F = \mathbb{F}_2$ et $G = C_7$. Considérons $\zeta \in \mathbb{F}_{64}$ une racine primitive 7-ième de l'unité, et le caractère $\chi = \phi_\zeta(1)$. Alors*

$$\begin{aligned}\chi &= 1 + \zeta X + \zeta^2 X^2 + \zeta^3 X^3 + \zeta^4 X^4 + \zeta^5 X^5 + \zeta^6 X^6 \\ \sigma \circ \chi &= 1 + \zeta^2 X + \zeta^4 X^2 + \zeta^6 X^3 + \zeta X^4 + \zeta^3 X^5 + \zeta^5 X^6 \\ \sigma^2 \circ \chi &= 1 + \zeta^4 X + \zeta X^2 + \zeta^5 X^3 + \zeta^2 X^4 + \zeta^6 X^5 + \zeta^3 X^6 \\ (id + \sigma + \sigma^2) \circ \chi &= 1 + (\zeta + \zeta^2 + \zeta^4)(X + X^2 + X^4) + (\zeta^3 + \zeta^5 + \zeta^6)(X^3 + X^5 + X^6)\end{aligned}$$

La valeur de $\zeta + \zeta^2 + \zeta^4$ (et celle de $\zeta^3 + \zeta^5 + \zeta^6$) dépend de ζ, selon la racine choisie l'une des deux expressions vaudra 1 et l'autre 0. La somme des caractères de cette classe cyclotomique vaudra donc soit $1 + X + X^2 + X^4$ soit $1 + X^3 + X^5 + X^6$.

Un exemple supplémentaire est donné en annexe.

Ces examples sont présents pour montrer que la proposition suivante est naturelle. Elle peut s'interpréter comme un lemme de structure sur les classes cyclotomiques.

Proposition 4.5. *Soit $\chi = \phi_\zeta(g)$ un caractère d'une extension de FG (dépendant du choix d'une racine ζ primitive m-ième de l'unité). Si l'on note $Cyc_{\zeta,g}$ la somme des caractères d'une classe cyclotomique on a la forme suivante :*

$$Cyc_{\zeta,g} = |[\chi]_q| \mathbb{1}_{Ker(\chi)} + \sum_{k \in C_m \setminus \{0\}} c_{k,\zeta} \mathbb{1}_{\chi^{-1}(\zeta^k)}$$

avec $c_{k,\zeta} = \sum_i \zeta^{kq^i}$.

Une approche directe serait alors de déterminer quelles classes cyclotomiques rentreront dans l'expression de l'indicatrice d'un sous-groupe $H < \mathbb{Z}_m^s$ ne contenant aucun élément de $T_s = \{0,1\}^s \setminus \{0^s\}$:

$$\mathbb{1}_H = \sum_i \lambda_i \cdot Cyc_{\zeta,\chi_i} \tag{4.1}$$

L'un des problèmes que nous rencontrons à ce stade est que pour divers corps finis et diverses valeurs de m, les coefficients $c_{\zeta,k}$ peuvent prendre beaucoup de valeurs (pas seulement 1, 0 ou -1). Cette approche directe a donc a priori peu de chances de donner des résultats exploitables. Nous verrons à la dernière partie pourquoi elle ne peut pas aboutir.

5 Retour sur l'article de Meshulam

Dans cette section nous réexaminons la preuve du théorème d'incertitude de Meshulam à l'aide des classes cyclotomiques de caractères.

Nous allons nous placer dans le cas où $f : \mathbb{Z}_m^s \to F$ est l'indicatrice d'un sous-groupe $H < \mathbb{Z}_m^s$, qui de plus vérifie $H \cap T_s = \emptyset$.

Nous reprenons les notations de Meshulam, et allons les examiner plus en détail.

Dans toute cette partie on notera q le cardinal de F.

5.1 Formulation en termes de théorie des codes

On considère le code $fF\mathbb{Z}_m^s$, et on note de nouveau E une extension de F qui contient des racines primitivs m-ièmes. Si $s = 1$, alors le code engendré par f est cyclique. S'il est de dimension 1, alors f est un caractère, ce qui est impossible car alors $f(1) \neq 0$, ce qui contredit la condition sur f. Par conséquent $dim\langle f \rangle \geq 2$.

En fait on peut faire beaucoup mieux en exploitant les classes cyclotomiques. Si q est primitif modulo m (i.e. $ord_m(q) = m-1$), alors $X^m - 1 = (X-1)(X^{m-1} + \cdots + 1)$ dans $F[X]$, ce qui signifie qu'un code qui est de dimension supérieure à 1 est soit de dimension $m-1$ soit de dimension m.

Cet exemple est l'une de nos motivations pour l'étude des classes cyclotomiques, l'espoir étant que l'on peut reproduire cet exemple (on est passés de $\alpha(m,1) = 2$ comme borne inférieure à $m-1$!).

Par la suite, Meshulam prend $y \in \mathbb{Z}_m$ et considère f_y. Quand on évalue f en une multi-racine de l'unité $(\zeta^{a_1}, \ldots, \zeta^{a_{s-1}}, \zeta^{a_s})$, on décompose le calcul (en notant ev_a l'évaluation en a) :

$$\begin{aligned} ev_{(\zeta^{a_1},\ldots,\zeta^{a_{s-1}},\zeta^{a_s})}(f(X_1,\ldots,X_s)) &= ev_{\zeta^{a_s}}(f_0(\zeta^{a_1},\ldots,\zeta^{a_{s-1}}) + \cdots + f_{m-1}(\zeta^{a_1},\ldots,\zeta^{a_{s-1}})X_s^{m-1}) \\ &= f_0(\zeta^{a_1},\ldots,\zeta^{a_{s-1}}) + \cdots + f_{m-1}(\zeta^{a_1},\ldots,\zeta^{a_{s-1}})\zeta^{(m-1)\cdot a_s} \\ &= g_{a_1,\ldots,a_{s-1}}(0) + g_{a_1,\ldots,a_{s-1}}(1)\zeta^{a_s} + \cdots + g_{a_1,\ldots,a_{s-1}}(m-1)\zeta^{(m-1)\cdot a_s} \end{aligned}$$

Il s'agit donc tout simplement de déterminer les caractères qui composent le code cyclique suivant (en notant $a = (a_1, \dots, a_{s-1})$) :

$$g_a(0) + g_a(1)X_s + \cdots + g_a(m-1)X_s^{m-1} \in E[X_s]/\langle X_s^m - 1\rangle$$

On a ainsi décomposé le problème de compter les caractères composant f (i.e. le support de sa transformée de Fourier) au problème de compter la dimension de m^{s-1} codes cycliques.

On notera que le code $gE\mathbb{Z}_m$ est à défini sur l'extension E et non pas sur le "petit" corps initial F. Cela signifie qu'il sera impossible d'utiliser l'action du groupe de Galois pour augmenter la dimension du code $gE\mathbb{Z}_m$.

L'action du groupe de Galois nous permet cependant de faire quelques observations sur les g_a.

Proposition 5.1.

$$dim\langle g_a\rangle = dim\langle g_{qa}\rangle$$

Preuve. Supposons que $\zeta^i \in \operatorname{supp} \hat{g_a}$. C'est-à-dire que $\hat{f}(a,i) \neq 0$. Mais alors l'action du groupe de Galois donne $\hat{f}(qa, qi) \neq 0$, ce qui implique donc $\zeta^{qi} \in \operatorname{supp} g_{qa}$. Puisque q est premier avec m, la multiplication par q est une bijection dans $\mathbb{Z}_m$, il y a une bijection entre le support de $\hat{g_a}$ et celui de $\hat{g_{qa}}$, ce qui signifie que les dimensions des codes cycliques concernés sont égales. □

Ce résultat est une première simplification, il signifie qu'un caractère ne vient jamais seul. On peut l'utiliser pour la reformulation suivante du lemme d'incertitude de Meshulam.

Théorème 5.2. *Soit G un groupe abélien et fFG un code, où $f = \mathbb{1}_H$ avec $H < G$ vérifiant $H \cap T_s = \emptyset$. Notons κ le PGCD des cardinals des classes cyclotomiques modulo m qui ne sont pas la classe de 0. Alors*

$$dim\langle f\rangle \geq 1 + \kappa\lceil\frac{\alpha(m,s) - 1}{\kappa}\rceil$$

Preuve. D'après la proposition précédente, le support de $\hat{f}$ est distribué sur les classes cyclotomiques de $\mathbb{Z}_m^s$. Notons que la classe $(0; \dots; 0)$ est nécéssairement présente : en effet $\hat{f}(x) = |H|$ si $x \in H^\perp$ (et 0 sinon), or $0 \in H^\perp$ indépendamment de H, et $|H| \neq 0$ grâce à l'hypothèse $q \nmid |G|$.

Les autres caractères sont nécéssairement dans des classes cyclotomiques sur $\mathbb{Z}_m^s$ non triviales. Or toute classe cyclotomique est de la forme $\{(a_1, \dots, a_s), (qa_1, \dots, qa_s), \dots\}$. Par conséquent son cardinal est un multiple de celui des classes de a_1, de a_2, etc. jusqu'à a_s. En particulier c'est un multiple de κ.

Par conséquent non seulement $\dim\langle f\rangle$ est de la forme $1+\kappa$, mais ce nombre est supérieur à $\alpha(m,s)$ par le théorème de Meshulam (et l'expression du théorème donne précisément le prochain nombre qui est 1 modulo κ). □

Notons également que sans supposer que f est l'indicatrice d'un sous-groupe on obtient de la même manière le théorème suivant.

Théorème 5.3. *Soit G un groupe abélien et fFG un code, où $f : G \to F$. Notons κ le PGCD des cardinals des classes cyclotomiques modulo m qui ne sont pas la classe de 0. Si $\sum_{g\in G} f(g) = 0$ alors*

$$dim\langle f\rangle \geq \kappa\lceil\frac{\alpha(m,s)}{\kappa}\rceil$$

et si $\sum_{g\in G} f(g) \neq 0$ alors

$$dim\langle f\rangle \geq 1 + \kappa\lceil\frac{\alpha(m,s)-1}{\kappa}\rceil$$

Preuve. Ici la seule distinction est selon la valeur de $\hat{f}(0)$, i.e. si le caractère nul apparaît ou pas. Si c'est le cas on est exactement dans le cas de la démonstration précédente (on a simplement enlevé l'hypothèse que f est l'indicatrice d'un sous-groupe, dont on se servait que pour la valeur de $\hat{f}(0)$). Sinon on sait que le caractère nul n'apparaît pas et que par conséquent, puisque les caractères viennent par classes cyclotomiques, qui sont toutes de cardinal multiple de κ. Ainsi $dim\langle f\rangle$ est un multiple de κ et supérieur à $\alpha(m,s)$, d'où le résultat. □

5.2 Utilisation de la structure de groupe de $H^\perp$

Comme son nom l'indique, dans cette partie nous examinons les possibilités offertes par l'observation que $\hat{f} = |H| \cdot \mathbb{1}_{H^\perp}$, en particulier le fait que H et $H^\perp$ sont des sous-groupes de $\mathbb{Z}_m^s$.

Une première interprétation des fonctions h_i définies dans la preuve de Meshulam permet de comprendre leur rôle.

Proposition 5.4. *Soit $f : G \to F$ et $h_i : \mathbb{Z}_m^{s-1} \to E$ définie par $h_i(x) = f_0(x) - \zeta^i f_1(x)$. Alors $a \in \operatorname{supp}\hat{h}_i(x) \implies \exists j \neq -i \quad \hat{f}(a,j) \neq 0$*

Preuve. En annexe. □

Cette proposition éclaire l'approche de Meshulam : le rôle des fonctions h_i n'est pas tant de déterminer, étant donné $a \in \mathbb{Z}_m^s$, quels caractères de la forme (a,i) sont dans le support de $\hat{f}$ que de déterminer *s'il y a* un caractère de la forme (a,i) (sans pouvoir déterminer pour quelle valeur de i il existe).

Dans ce contexte, les assertions (3.2) et (3.3) trouvent un équivalent naturel. Si $a \in \operatorname{supp}\hat{h}_i$ alors il y a un caractère de la forme (a,j) donc $|\operatorname{supp}\hat{g}_a| \geq 1$. D'autre part si $a \in \cap_{i=1}^m \operatorname{supp}\hat{h}_i$ non seulement il y a un caractère de la forme (a,j) mais aussi un deuxième (ce qui se voit en considérant $i = -j$), donc $|\operatorname{supp}\hat{g}_a| \geq 2$.

Il est également intéressant de noter une dernière propriété des fonctions g_a.

Proposition 5.5. *Soit $g_a = \sum_{i=1}^{m} \lambda_i \chi_i$. Alors pour tout i, le coefficient λ_i est soit nul soit vaut $|H|$.*

Preuve. C'est une conséquence du fait que si $f = \mathbb{1}_H$, alors $\hat{f} = |H| \cdot \mathbb{1}_{H^\perp}$ et de l'observation $\lambda_i = \hat{g}_a(i) = \hat{f}(a, i)$. □

A ce stade il devient possible d'exploiter la structure de groupe de $H^\perp$.

Définition 5.6. *Un sous-groupe $H < \mathbb{Z}_m^s$ vérifiant $H \cap T_s = \emptyset$ est dit T_s-maximal s'il n'existe pas de sous-groupe $H' < \mathbb{Z}_m^s$ contenant H strictement, et vérifiant $H' \cap T_s = \emptyset$.*

L'intérêt de cette proposition est justifié par la proposition suivante, qui assure que les sous-groupes T_s maximaux permettent de s'approcher le plus d'une quelconque borne inférieure sur $\operatorname{supp} \hat{\mathbb{1}}_H$.

Proposition 5.7. *Soit $\mathbb{1}_H : \mathbb{Z}_m^s \to F$ l'indicatrice d'un sous-groupe H vérifiant $H \cap T_s = \emptyset$. Alors H est T_s-maximal si et seulement s'il n'existe aucun $H' < \mathbb{Z}_m^s$ T_s-maximal tel que $\operatorname{supp} \hat{\mathbb{1}}_{H'} \subsetneq \operatorname{supp} \hat{\mathbb{1}}_H$.*

En un sens, seuls les sous-groupes T_s-maximaux nous intéressent dans toute la suite, puisque toute borne inférieure sur $\operatorname{supp} \hat{\mathbb{1}}_H$ valable pour tous les $H < \mathbb{Z}_m^s$ sera aussi valable pour tous les autres sous-groupes.

Cette définition introduite, nous pouvons désormais affirmer que les caractères présents dans les g_a doivent être bien espacés pour que le sous-groupe leur correspondant soit T_s-maximal.

Proposition 5.8. *Soit $H < \mathbb{Z}_m^s$ T_s-maximal, et $f = \mathbb{1}_H$. Supposons que m ne soit pas premier. Si $i \in \operatorname{supp} \hat{g}_a$ alors $i + 1 \notin \operatorname{supp} \hat{g}_a$ et $i - 1 \notin \operatorname{supp} \hat{g}_a$.*

Preuve. Si $i \in \operatorname{supp} \hat{g}_a$ et $i + 1 \in \operatorname{supp} \hat{g}_a$, alors $\{(a, i), (a, i + 1)\} \subset H^\perp$. Puisque $H^\perp$ est un groupe, $(0, 1) = (a, i + 1) - (a, i) \in H^\perp$. Par conséquent, par définition de $H^\perp$, $\forall h \in H \quad h_s = 0$.

Cela signifie que $H = H_0$. Or puisque m n'est pas premier, il est possible de construire H' strictement plus grand que H, et tel que $H' \cap T_s = \emptyset$: il suffit de prendre $H' = H + \langle (0, \ldots, 0, p) \rangle$ avec $p \neq 1$ un diviseur strict de m. Ainsi H n'est pas T_s-maximal, donc la proposition est montrée par l'absurde.

Le cas $i - 1$ se traite de la même manière. □

Une petite généralisation permet de montrer le corollaire

Corollaire 5.9. *Soit $H < \mathbb{Z}_m^s$ T_s-maximal, et $f = \mathbb{1}_H$. Supposons que m ne soit pas premier. Alors si $i \in \operatorname{supp} \hat{g}_a$, pour tout k premier avec m, $i + k \notin \operatorname{supp} \hat{g}_a$.*

Preuve. Avec le même raisonnement on obtient que $(0, k) \in H^\perp$.

Mais alors, puisque k est premier avec m, en notant d un inverse de k, on a aussi $d \cdot (0, k) = (0, 1) \in H^\perp$, et le reste de la preuve est identique. □

D'après cette petite discussion, $\operatorname{supp} \hat{g}_0$ doit être un sous-groupe de $H^\perp$. Cela implique que les éléments du support de $\hat{g}_0$ sont dans une progression arithmétique de raison d, avec $d \mid m$.

Proposition 5.10. *Soit $a \in \mathbb{Z}_m^{s-1}$. Alors soit $\operatorname{supp} \hat{g}_a = \emptyset$ soit $|\operatorname{supp} \hat{g}_a| = |\operatorname{supp} \hat{g}_0|$.*

Preuve. Si $\operatorname{supp} \hat{g}_a \neq \emptyset$ alors $\forall i \in \operatorname{supp} \hat{g}_a \quad \forall x \in \operatorname{supp} \hat{g}_0 \quad i + x \in \operatorname{supp} \hat{g}_a$. □

En particulier, si m n'est pas premier, alors la condition (3.3) de Meshulam implique $|\operatorname{supp} \hat{g}_a| \geq p$, où p est le plus petit diviseur non trivial de m ! D'après cette preuve, les coefficients non nuls de g_a (quand ils existent) forment toujours un coset de l'ensemble des coefficients non nuls de g_0, donc sont espacés régulièrement (dans une suite arithmétique de raison $d \mid m$).

A ce stade indiquons que nous pouvons montrer une autre amélioration du théorème d'incertitude de Meshulam. La discussion précédente n'est pas nécéssaire pour cette preuve, mais elle en éclaire les limites.

Théorème 5.11. *Soit $H < \mathbb{Z}_m^s$ vérifiant $H \cap T_s = \emptyset$. Alors $|H^\perp| \geq \alpha(m, s)$ et $|H^\perp| \mid m^s$.*

Preuve. La première assertion est le théorème de Meshulam, tandis que la seconde est une conséquence du théorème de Lagrange sur le cardinal d'un sous-groupe, puisque $H^\perp < \mathbb{Z}_m^s$. □

5.3 Les limites de ces deux approches

Si les théorèmes constituent bien des améliorations modestes sur le théorème d'incertitude de Meshulam, il est probable que nos techniques ne permettent pas (encore) de l'améliorer suffisament pour obtenir une meilleure borne sur la constante de Davenport.

Il est en effet nécéssaire d'améliorer le théorème 3.1 (et non le 3.6) pour obtenir une meilleure borne sur la constante de Davenport. En reprenant les notations du théorème 3.6, si $\epsilon \in H^\perp \cap \{0,1\}^s$ alors $\sum_{i=1}^s \epsilon_i a_i = 0$. En effet, on a $\forall 1 \leq j \leq r \quad b_j \cdot \epsilon = 0$, ce qui implique que $\left(\sum_{i=1}^s \epsilon_i a_i \right)_j = 0$ coordonnée par coordonnée.

Par conséquent toute suite sans sous-somme nulle correspond à un sous-groupe $H < \mathbb{Z}_m^s$ tel que $H^\perp \cap \{0,1\}^s = \{0\}^s$, et une bonne borne supérieure sur s viendra d'une amélioration de la borne inférieure sur $|H|$.

Reprenons un instant le calcul (3.5) dans la preuve de Meshulam.

$$\frac{m}{e}\left(\frac{m}{m-1}\right)^s \leq \alpha(m,s) \leq |\operatorname{supp} \hat{\mathbb{1}}_{H^\perp}| = |\operatorname{supp}(|H| \cdot \mathbb{1}_H)| = |H| \leq |G|$$

Il montre que toute amélioration sur $\alpha(m, s)$ doit permettre de dépasser au moins une valeur possible de $|H|$ pour permettre d'améliorer la constante de Davenport. Si la nouvelle valeur de $\alpha(m, s)$ ne permet pas d'éliminer certaines valeurs de $|H|$ potentiels, on n'obtiendra aucune amélioration.

Or puisque $\mathbb{1}_H$ est une fonction à valeurs dans le "petit corps" F et non pas son extension E, l'action du groupe de Galois sur $\mathbb{1}_H$ est triviale. Cela signifie en particulier que toutes les classes cyclotomiques de caractères qui apparaîtront dans le support de la transformée de Fourier de $\mathbb{1}_H$ sont pleines, donc qu'on ne peut pas éliminer des sous-groupes $H < \mathbb{Z}_m^s$ simplement en sachant que les classes cyclotomiques doivent être entières.

En ce sens, on notera également que le théorème 5.11 est donc la meilleure amélioration du théorème d'incertitude de Meshulam, puisque le 5.3 ne permet que de compléter des classes cyclotomiques déjà existantes, et non pas d'en créer de nouvelles.

Il reste encore l'espoir que la méthode de Meshulam ne compte qu'un seul caractère par classe cyclotomique, et qu'ainsi il soit possible de multiplier sa borne $\alpha(m, s)$ par au moins κ (le PGCD du cardinal des classes cyclotomiques non triviales), ce qui donnerait une amélioration importante de la borne sur la constante de Davenport.

La méthode de Meshulam est détaillée à la proposition 5.4 : étant donné $a \in \mathbb{Z}_m^{s-1}$ il parvient à déterminer s'il existe $i \in \mathbb{Z}_m$ tel que $(a, i) \in H^\perp$, sans pouvoir déterminer avec précision de quel i il s'agit.

D'après la discussion suivant la proposition 5.10, il y a deux cas de figure possibles : $|\operatorname{supp} \hat{g}_0|$ vaut soit 1, soit $1 \neq d \mid m$. Dans le premier cas, la méthode de Meshulam trouve tous les caractères à $a \in \mathbb{Z}_m^s$ donné, donc tous les caractères, et explorer les classes cyclotomiques n'apporte rien de nouveau.

Dans le second cas, la méthode de Meshulam prédit 2 caractères à $a \in \mathbb{Z}_m^s$ donné, alors qu'il y en a en fait $d \geq 2$. Cela est particulièrement intéressant dans les cas où m est le produit de deux grands nombres premiers, car alors il y a de bonnes chances pour que d soit grand.

Cependant, le lemme 3.2 amélioré qui en résulterait ne permet pas d'améliorer les choses : si les B_i sont tous de cardinal au moins u, pour $1 \leq i \leq k$, alors

$$\Big|\bigcup_{i=1}^{k} B_i\Big| + (d-1)\Big|\bigcap_{i=1}^{k} B_i\Big| \geq \frac{k}{k-1}u$$

est toujours la meilleure borne possible.

Enfin, le cas $|\operatorname{supp} \hat{g}_0| > 1$ arrive peu souvent, bien qu'il permettrait à l'étape s_0 où il se produit de multiplier $\alpha(m, s_0 - 1)$ par d. Toutefois, même si une telle amélioration était possible, on ne peut pas l'utiliser dans l'hypothèse de récurrence, car h_i (sur laquelle on l'applique) ne vérifie pas les hypothèses du théorème 5.11.

Enfin, avec les techniques dont nous disposons, il est impossible de prédire quand le phénomène $|\operatorname{supp} \hat{g}_0| > 1$ se produit, ni combien de fois.

Nous ne pouvons donc pas améliorer la constante de Davenport avec les méthodes développées dans le présent rapport, malgré les améliorations sur le théorème d'incertitude de Meshulam. Soit une amélioration est impossible, soit (à notre avis plus probablement) elle employera des techniques que nous n'avons pas examinées.

6 Annexe

Proposition 6.1. *Soit χ et χ' deux charactères de FG. Alors*

$$\langle \chi \mid \chi' \rangle = \delta_{\chi,\chi'} \cdot |G|$$
$$\chi \times \chi' = \delta_{\chi,\chi'} \cdot |G| \cdot \chi$$

Preuve. Montrons d'abord l'orthogonalité des caractères :

$$\begin{aligned}\langle \chi \mid \chi' \rangle &= \sum_{g \in G} \bar{\chi}(g)\chi'(g) \\ &= \sum_{g \in G} (\bar{\chi} \cdot \chi')(g) \\ &= \delta_{\chi,\chi'} \cdot |G|\end{aligned}$$

En utilisant cette relation on peut alors écrire

$$\begin{aligned}\chi \times \chi' &= \sum_{g \in G} \Big(\sum_{h \in G} \chi(gh^{-1})\chi'(h) \Big) g \\ &= \sum_{g \in G} \chi(g) \Big(\sum_{h \in G} \chi(h^{-1})\chi'(h) \Big) g \\ &= \sum_{g \in G} \chi(g) \Big(\sum_{h \in G} \bar{\chi}(h)\chi'(h) \Big) g \\ &= \Big(\sum_{h \in G} \bar{\chi}(h)\chi'(h) \Big) \cdot \chi \\ &= \langle \chi \mid \chi' \rangle \cdot \chi \\ &= \delta_{\chi,\chi'} \cdot |G| \cdot \chi\end{aligned}$$

□

Théorème 6.2. *Soit $G \simeq \prod_{i=1}^{r} C_{p^{\alpha_i}}$. Alors*

$$D(G) \leq 1 + \sum_{i=1}^{r} (p^{\alpha_i} - 1)$$

Preuve. Pour faciliter la preuve nous allons noter le groupe G 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 $\mathbb{Z}[G]$:

$$\prod_{i=1}^{k} (1 - g_i) = 0 \pmod{p} \tag{6.1}$$

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 (6.1). Notons $x_1, \ldots, x_r$ une "base" de G, où $ord(x_i) = p^{\alpha_i}$. 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 :

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

En répétant cette opération on obtient (en décomposant tous les g_i en produits déléments 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 $J_\sigma = (1-x_1)^{f_1}\ldots(1-x_r)^{f_r}$, 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 (6.1) et le théorème. □

Théorème 6.3. *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 6.4. *Soit p un nombre premier. Une suite $a_1, \ldots, a_s$ 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 du lemme. Notons pour commencer que $D(C_p^2) = 2p-1$ et $D(C_p^3) = 3p-2$ (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 $xa_1, \ldots, xa_s$ 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 $a_1, \ldots, a_{2p}$. On utilise alors $D(C_p^2) = 2p-1$ 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 $a_1 + \cdots + a_{2p} = 0$. □

Preuve du théorème. 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 $D(C_p^2) = 2p-1$, ces éléments admettent une sous-suite de somme nulle :

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

Puisque $l + 1 = D(Q)$, 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. □

Proposition 6.5. *Soit $\chi \in \hat{G}$ tel que $\chi = \phi_\zeta((a_1, \ldots, a_s))$.*

$$\phi_\zeta^{-1}(\sigma \circ \chi) = q \cdot (a_1, \ldots, a_s) = (qa_1, \ldots, qa_s)$$

Preuve.

$$\begin{aligned} \sigma \circ \chi_{(a_1,\ldots,a_s)}((b_1, \ldots, b_s)) &= \sigma(\zeta^{a_1b_1+\cdots+a_sb_s}) \\ &= \zeta^{q(a_1b_1+\cdots+a_sb_s)} \\ &= \zeta^{qa_1b_1+\cdots+qa_sb_s} \\ &= \chi_{(qa_1,\ldots,qa_s)}((b_1, \ldots, b_s)) \end{aligned}$$

□

Exemple 6.6. *Prenons $F = \mathbb{F}_2$ et $G = C_5$. Considérons $\zeta \in \mathbb{F}_{16}$ une racine primitive*

5-*ième de l'unité, et le caractère* $\chi = \phi_\zeta(1)$. *Alors*

$$\begin{aligned}
\chi &= 1 + \zeta X + \zeta^2 X^2 + \zeta^3 X^3 + \zeta^4 X^4 \\
\sigma \circ \chi &= 1 + \zeta^2 X + \zeta^4 X^2 + \zeta X^3 + \zeta^3 X^4 \\
\sigma^2 \circ \chi &= 1 + \zeta^4 X + \zeta^3 X^2 + \zeta^2 X^3 + \zeta X^4 \\
\sigma^3 \circ \chi &= 1 + \zeta^3 X + \zeta X^2 + \zeta^4 X^3 + \zeta^2 X^4 \\
\sum_{k=0}^{|[\chi]_q|-1} \sigma^k \circ \chi &= 0 + X + X^2 + X^3 + X^4
\end{aligned}$$

Proposition 6.7. *Soit* $f : G \to F$ *et* $h_i : \mathbb{Z}_m^{s-1} \to E$ *définie par* $h_i(x) = f_0(x) - \zeta^i f_1(x)$. *Alors* $a \in \operatorname{supp} \hat{h}_i(x) \implies \exists j \neq -i \quad \hat{f}(a, j) \neq 0$

Preuve. Notons pour commencer que $\hat{h}_i(a) = g_a(0) - \zeta^i g_a(1)$. D'autre part, puisque g_a est un code cyclique, il est une combinaison linéaire de caractères, de la forme $\chi_j = 1 + \zeta^j X_s + \cdots + \zeta^{j(m-1)} X_s^{m-1}$. En notant $g_a = \sum_{j=1}^m \lambda_j \chi_j$ on obtient $g_a(0) = \sum_{j=1}^m \lambda_j$ et $g_a(1) = \sum_{j=1}^m \lambda_j \zeta^j$. Alors

$$\begin{aligned}
\hat{h}_i(a) &= g_a(0) - \zeta^i g_a(1) \\
&= \sum_{j=1}^{m} \lambda_j (1 - \zeta^{i+j}) \\
&= \sum_{j \in [\![1, m-1]\!] \setminus \{-i\}} \lambda_j (1 - \zeta^{i+j})
\end{aligned}$$

Si $\hat{h}_i(a)$ est non nul, alors cela signifie que l'un des λ_j (pour $j \neq -i$) est non nul, ce qui donne $\hat{f}(a, j) = \lambda_j \neq 0$, et donc $(a, i) \in \operatorname{supp} \hat{f}$. □

References

[AGP95] William Alford, Andrew Granville, and Carl Pomerance. There are infinitely many Carmichael numbers. *Annals of Mathematics*, 139:703–722, 1995.

[BS22] Martino Borello and Patrick Solé. The uncertainty principle over finite fields. *Discrete Mathematics*, 345(1):112670, 2022.

[BWZ22] Martino Borello, Wolfgang Willems, and Giovanni Zini. On ideals in group algebras : an uncertainty principle and the Schur product. *Forum Mathematicum*, 0, 2022.

[EKL17] Shai Evra, Emmanuel Kowalsi, and Alexander Lubotsky. Good cyclic codes and the uncertainty principle. *Enseignement mathématique*, 63:305–332, 2017.

[GC13] Jérôme Germoni and Philippe Caldero. *Histoires hédonistes de groupes et de géométries: Volume 1.* Calvage et Mounet, Montrouge, 05 2013.

[GHK06] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations: a survey.* Springer US, Boston, MA, 2006.

[GS92] Alfred Geroldinger and Rudolf Schneider. On Davenport's constant. *Journal of Combinatorial Theory, Series A*, 61(1):147–152, 1992.

[Liu20] Chao Liu. On the lower bounds of Davenport constant. *Journal of Combinatorial Theory, Series A*, 171:105162, 2020.

[Mes90] Roy Meshulam. An uncertainty inequality and zero subsums. *Discrete Mathematics*, 84(2):197–200, 1990.

[Ols69a] John E. Olson. A combinatorial problem on finite abelian groups, I. *Journal of Number Theory*, 1(1):8–10, 1969.

[Ols69b] John E. Olson. A combinatorial problem on finite abelian groups, II. *Journal of Number Theory*, 1(2):195–199, 1969.