école normale supérieure paris—saclay

université PARIS-SACLAY

Ensembles $B_2[g]$ dans les n premiers carrés.

Approches diverses.

La pie, Claude Monet, 1868

Remerciements

Nous tenons à remercier chaleureusement Robin Riblet et Alexandre Bailleul pour nous avoir accompagnés tout au long de ce stage. Leur disponibilité, leurs conseils avisés et la qualité de leurs explications ont été déterminants dans l'avancement de ce travail. Nous leur sommes reconnaissants de nous avoir guidés avec patience sur des questions parfois ardues, et d'avoir su nous laisser l'autonomie nécessaire pour explorer par nous-mêmes certaines pistes de recherche.

ENSEMBLES $B_2[g]$ DANS LES n PREMIERS CARRÉS

FRANÇOIS BOSIO, JACQUES TARR

RÉSUMÉ. On dit que A est un ensemble $B_2[g]$ lorsque pour tout $k \in \mathbb{N}^*$, k s'écrit comme la somme de deux éléments de A d'au plus g manières différentes. On établit une majoration et une minoration non triviales du cardinal du plus grand ensemble $B_2[g]$ dans les n premiers carrés.

Dans un premier temps, on applique la méthode du grand crible, adaptée pour une norme 4 sur l'espace des polynômes trigonométriques, afin d'exploiter les relations d'ordres classiques qui interviennent entre l'énergie additive et le cardinal en question. Cela nous permet d'obtenir une nouvelle majoration non triviale de ce dernier.

Dans un second temps, on exploite des résultats de combinatoire des hypergraphes pour construire un grand sous ensemble $B_2[g]$ des n premiers carrés. Cela nous permet d'obtenir une nouvelle minoration non triviale du cardinal étudié.

Introduction & État de l'Art

La notion d'ensemble de Sidon, aussi appelé ensemble B_2, dérive de problèmes de combinatoire additive introduits et étudiés par S. Sidon par exemple en 1932 dans [9]. Un ensemble de Sidon A est une partie $\mathbb{N}^*$ telle que deux paires distinctes d'éléments de A n'ont jamais la même somme.

La notion d'ensemble de Sidon se généralise en la notion d'ensemble $B_2[g]$ qui impose que chaque entier naturel s'écrit d'au plus g manières comme somme de deux éléments de l'ensemble considéré. Les ensembles de Sidon sont le cas particulier $g = 1$.

Dans [3] P. Erdös et N. Alon exposent en 1985 de premières bornes sur le cardinal maximal $|A_n|$ d'un sous ensemble de Sidon de l'ensemble des n premiers carrés. Ils exposent en effet que $|A_n|$ est grand devant $n^{2/3-\varepsilon}$ pour tout $\varepsilon > 0$ et que $|A_n|$ est au plus de l'ordre de $\dfrac{n}{\ln(n)^{1/4}}$.

Ils laissent ouverte la question de la possibilité de mieux estimer $|A_n|$ et demandent par exemple si $|A_n| = n^{1-o(1)}$. Ceci constitue le problème 773 d'Erdös [1].

La borne inférieure a été améliorée en 1995 par H. Lefmann et T. Thiele pour montrer que $|A_n|$ est au moins de l'ordre de $n^{2/3}$ *(Éliminant donc le $-\varepsilon$ parasite)*.

La borne supérieure, elle, se trouve avoir été améliorée au cours même de ce stage comme mentionné ci-dessous dans la deuxième section.

Dans le cadre de ce stage, nous avons cherché à étendre le problème d'estimer $|A_n|$ en l'estimation de $|A_n(g)|$ le plus grand cardinal d'un sous ensemble $B_2[g]$ dans les n premiers carrés.

On a d'abord approfondi la méthode du grand crible. En la combinant avec des théorèmes taubériens, on a obtenu la première majoration non triviale de $|A_n(g)|$. L'idée essentielle reposait sur la structure rigide des n premiers carrés, en remarquant qu'ils sont toujours des résidus quadratiques modulo p, pour tout nombre premier p.

De plus, l'inégalité du grand crible, initialement démontrée par V. Brun, établit une inégalité entre la norme L^2 et la norme L^∞ de polynômes trigonométriques. Nous avons montré qu'elle pouvait être adaptée afin d'obtenir une inégalité reliant des normes L^4. Cette adaptation était particulièrement intéressante, car la norme L^4 est intimement liée à l'énergie additive, un objet omniprésent en combinatoire additive et très naturel à considérer dans le cadre de notre étude. Ainsi, en choisissant convenablement le crible, on élimine suffisamment d'éléments pour obtenir une inégalité de grand crible adaptée à la norme L^4, ce qui permet de majorer $|A_n(g)|$.

On a ensuite tenté d'adapter des arguments de B. Lindström afin de raffiner cette borne supérieure, mais sans succès.

Date: juin 2026.

En parallèle, on a étudié plusieurs approches pour la minoration de $|A_n(g)|$.

Une première piste pour la minoration a consisté à spécifier, dans le contexte qui nous intéresse, un résultat très général de J. Komlós, M. Sulyok & E. Szemerédi exposé dans [10] qui permettait naturellement de comparer le cardinal du plus grand sous ensemble $B_2[g]$ d'une partie finie à celui du plus grand sous ensemble $B_2[g]$ dans l'intervalle d'entiers de même taille. La minoration ainsi obtenue n'est jamais que de l'ordre de $\sqrt{n}$ donc moins bonne que l'état de l'art et ce raisonnement n'est ici exposé qu'en annexe.

Une autre piste considérée un temps partait d'un recouvrement des $g(q^2+q+1)$ premiers entiers par des sous ensembles $B_2[g]$, obtenus à partir des ensembles de Singer. La piste consistait par exemple à se demander si un de ces sous-ensembles rencontrait souvent les carrés. Par manque d'idée pertinente pour détecter les carrés dans un tel sous-ensemble cette piste n'a pas mené à grand chose et n'est pas développée ci-dessous.

Finalement la piste fructueuse développée ci-dessous consiste en une généralisation de la méthode développée dans [11]. Cet article trouve un grand sous ensemble B_2 inclus dans $\square_n$ en montrant l'existence d'une grande partie indépendante d'un hypergraphe 4-uniforme bien construit. On adapte la même méthode en l'appliquant sur un hypergraphe $2(g+1)$-uniforme bien construit pour obtenir un grand sous ensemble $B_2[g]$.

La première section expose les définitions de base du sujet et quelques notions pertinentes qui lui sont associées.

La deuxième section expose les résultats de majoration que l'on a obtenus. On y montre notamment l'existence d'une constante $C>0$ telle que $|A_n(g)| \leqslant C\sqrt{g}\frac{n}{\sqrt{\ln(n)}}$.

La troisième section expose enfin les résultats de minoration que l'on a obtenus. On y montre notamment l'existence, pour tout $g \geqslant 1$, d'une constante $C_g > 0$ telle que $|A_n(g)| \geqslant C_g n^{\alpha_g}\ln(n)^{\gamma_g}$ avec $\alpha_g = \frac{2g}{2g+1}$ et $\gamma_g = \frac{2-2^g}{2g+1}$.

1. Définitions & Notations Générales

Définition 1.0.1. *Pour $g \in \mathbb{N}^*$, une partie $A \subseteq \mathbb{N}^*$ est dite $B_2[g]$ si pour tout entier naturel k il existe au plus g paires $\{a,b\}$ (éventuellement dégénérées en singleton) d'éléments de A telles que $a+b=k$.*

On notera $r_{A+A}(k)$ le nombre de couples $(a,b) \in A^2$ tels que $a+b=k$. On pourra constater que si A est un ensemble $B_2[g]$ on a pour tout k, $r_{A+A}(k) \leqslant 2g$.

On introduit un outil classique de la combinatoire additive :

Définition 1.0.2. *Pour $A \subseteq \mathbb{N}^*$ on appelle énergie additive de A le nombre de "collisions de A" :*

$$E(A) = |\{(a,b,c,d) \in A^4 \,;\, a+b=c+d\}|.$$

On remarquera que $E(A) = \sum_{i=1}^{+\infty} r_{A+A}^2(i)$. En particulier si A est un ensemble $B_2[g]$: $E(A) \leqslant 2g|A|^2$.

Étant donnée une partie finie $A \subseteq \mathbb{N}^*$, on note $\|A\|_g$ le cardinal maximal d'un sous ensemble $B_2[g]$ de A.

Notons pour $n \in \mathbb{N}^*$ $\square_n = \{1^2, \dots, n^2\}$ l'ensemble des n premiers carrés. Notre objectif dans le cadre de ce stage est d'estimer $\|\square_n\|_g$ quand $n \to +\infty$.

Pour $n, g \geqslant 1$ on notera $A_n(g)$ un sous ensemble $B_2[g]$ de $\square_n$ de cardinal $\|\square_n\|_g$.

On pourra constater que tant que l'on ne s'intéresse qu'à l'ordre de grandeur de $\|\square_n\|_g$ le fait d'inclure ou non les paires dégénérées en singletons dans la contrainte sur le nombre de collisions dans la définition des ensembles $B_2[g]$ n'a pas vraiment d'importance.

En effet déclarons qu'une partie $A \subseteq \mathbb{N}^*$ est $B_2[g]^*$ si tout entier naturel s'écrit d'au plus g manières comme somme de deux éléments **distincts** de A. Notons pour une partie finie $A \subseteq \mathbb{N}^*$ $\|A\|_g^*$ le cardinal maximal d'un sous ensemble $B_2[g]^*$ de A. On a :

Proposition 1.0.1. *Pour tout $A \subseteq \mathbb{N}^*$ finie on a :*

$$\|A\|_g^*/2 \leqslant \|A\|_g \leqslant \|A\|_g^*.$$

la proposition 1.0.1 peut être montrée à partir du fait suivant :

Proposition 1.0.2. *Soit A un ensemble fini et $\to$ une relation binaire sur A telle que tout élément de A admet au plus un successeur pour $\to$.*

On suppose qu'il n'existe pas de boucle pour $\to$ (c'est-à-dire qu'on ne peut pas trouver $a_1, \dots, a_p \in A$ tels que $a_1 \to \cdots \to a_p \to a_1$).

Il existe une partie $B \subseteq A$ avec $|B| \geqslant |A|/2$ telle que $\forall a, b \in B, a \not\to b$.

Démonstration. Pour $a \in A$ on définit la hauteur $h(a)$ de a comme le cardinal maximal h d'une chaîne $a = a_0 \to a_1 \to \cdots \to a_{h-1}$.

On constate alors que si $a, b \in A$ vérifient $a \to b$ on a $h(a) = h(b) + 1$. En particulier les hauteurs de a et de b sont alors de parités opposées.

On partitionne $A = A_0 \sqcup A_1$ où A_0 est l'ensemble des éléments de hauteur paire.

À partir de là il existe $i \in \{0, 1\}$ tel que $|A_i| \geqslant |A|/2$, et puisque les hauteurs de tous les éléments de A_i sont de même parité, aucun élément de A_i n'est successeur d'un autre élément de A_i. □

Remarque 1.0.1. *Les hypothèses sur $\to$ dans la proposition 1.0.2 signifient exactement que $\to$ est la relation "est le fils de" pour une certaine structure de forêt d'arbres enracinés apposée sur A.*

La proposition 1.0.2 repose donc simplement sur l'idée que dans un arbre on peut partitionner l'ensemble des sommets selon la parité de leurs distances à un élément fixé.

L'inégalité non triviale de la proposition 1.0.1 découle immédiatement du :

Lemme 1.0.1. *Si $A \subseteq \mathbb{N}^*$ est un ensemble $B_2[g]^*$ fini, il existe un sous-ensemble $B_2[g]$ $B \subseteq A$ tel que $|B| \geqslant |A|/2$.*

Démonstration. Puisque A est $B_2[g]^*$, les seuls entiers qui peuvent être représentés de strictement plus de g manières comme somme de deux éléments de A sont les doubles d'éléments de A auxquels cas ils sont représentables d'exactement $g + 1$ manières comme somme de deux éléments de A.

On définit sur A $a \to b$ par "$2a$ est somme de deux éléments distincts de A et b est le plus petit élément impliqué dans une telle somme".

Ainsi tout élément de A admet au plus un successeur pour $\to$ et comme $a \to b$ implique $b < a$, $\to$ est sans boucle.

Considérons alors B donné par la proposition 1.0.2 et vérifions qu'il s'agit d'un sous ensemble $B_2[g]$, ce qui se réduit à vérifier qu'aucun double d'élément de B n'est représenté par $g + 1$ sommes de deux éléments de B. En effet si $a \in B$:

— soit a n'a pas de successeur au sens de $\to$ auquel cas $2a$ admet exactement une représentation comme somme de deux éléments de A et donc, de même, $2a$ admet exactement une représentation comme somme de deux éléments de B ;

— soit a a un successeur au sens de $\to$ lequel n'appartient pas à B et donc $2a$ admet au moins une représentation de moins comme somme de deux éléments de B que comme somme de deux éléments de A. Il s'ensuit bien que $2a$ admet au plus g représentations comme somme de deux éléments de B.

□

2. Majoration de $\|\square_n\|_g$

On expose dans cette section les résultats de majoration obtenus en explorant la piste d'utiliser les idées de la théorie du crible pour obtenir des informations sur la taille d'un sous ensemble $B_2[g]$ de $\square_n$.

La théorie du grand crible est d'abord explorée par Brun dans ses travaux sur la conjecture de Goldbach, puis encore plus poussée par Linnik en 1941. L'inégalité du grand crible a été énormément raffinée par toute une équipe de mathématiciens dans les années 1960 (Bombieri, Renyi, Roth, Davenport, Halberstam, Gallagher, Montgomery, Vaughan …)[7]. Le théorème général repose sur la définition d'un ensemble δ-bien espacé modulo 1.

2.1. **Concepts clés**

On note $\mathcal{Q}$ l'ensemble des quadratfrei et μ la fonction de Möbius. Dans la première partie, p désignera toujours un nombre premier. Lorsqu'on écrit :

$$\sum_{p \leqslant Q} \text{ ou } \prod_{p|Q}$$

cela veut dire qu'on somme sur les nombres premiers plus petits que Q ou qu'on prend le produit sur les premiers qui divisent Q. Pour tout $p \geqslant 3$, on note $\mathfrak{Q}_p$ l'ensemble des résidus quadratiques de $\mathbb{F}_p = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$. On notera désormais $\mathcal{C}$ le crible suivant :

$$\mathcal{C} = (\mathcal{P}_\mathcal{C}, \Omega_\mathcal{C} = \bigcup_{p \in \mathcal{P}_\mathcal{C}} \{\Omega_{p,\mathcal{C}}\}) \text{ avec } \mathcal{P}_\mathcal{C} = \{3 \leqslant p \leqslant n^2\} \text{ et } \Omega_{p,\mathcal{C}} = \mathbb{F}_p \backslash \mathfrak{Q}_p.$$

Pour tout $p \in \mathcal{P}_\mathcal{C}$, on note $\omega_\mathcal{C}(p) = \#\Omega_{p,\mathcal{C}} = \frac{p-1}{2}$. On note $\mathcal{E}$ l'espace des polynômes trigonométriques, c'est-à-dire l'espace vectoriel engendré par la base $\mathcal{B} = \text{vect}_\mathbb{C}((e_n)_{n\in\mathbb{Z}})$, avec pour tout $n \in \mathbb{Z}$, $e_n : t \mapsto \exp(2\pi i n t)$. $\mathcal{E}$ est un espace préhilbertien pour le produit hermitien $\langle \cdot, \cdot \rangle$ suivant, dont les éléments de $\mathcal{B}$ forment une base orthonormée :

$$\forall (f,g) \in \mathcal{E}^2,\ \langle f, g \rangle = \int_0^1 f(t)\overline{g(t)}\, dt.$$

Pour tout $f \in \mathcal{E}$, on note $\sigma(f) = \{n \in \mathbb{Z}, \langle f, e_n \rangle \neq 0\}$. On note $A_n(g)$ un des plus grand $B_2[g]$ de $\square_n$. Le but de ce rapport est, dans un premier temps, d'estimer la taille de $A_n(g)$ en fonction de n et de g. Par hypothèse, pour tout $m \in \mathbb{N}^*$, $r_{A_n(g)+A_n(g)}(m) \leqslant 2g$. On obtient alors la borne supérieure :

$$E(A_n(g)) \leqslant 2g \sum_{a \in A_n(g)+A_n(g)} r_{A_n(g)+A_n(g)}(a) = 2g|A_n(g)|^2.$$

L'énergie additive peut être vue comme la norme L^4 d'un élément de $\mathcal{E}$. Posons $f_n(t) = \sum_{a \in A_n(g)} e_a(t)$. Alors :

$$\int_0^1 |f_n(t)|^4\, dt = \int_0^1 \left| \sum_{a \in A_n(g)+A_n(g)} r_{A_n(g)+A_n(g)}(a) e_a(t) \right|^2 dt = E(A_n(g)).$$

Par l'identité de Parseval. On cherche alors une inégalité analogue à celle du grand crible arithmétique avec des normes 4. On détaille ici les résultats de base du grand crible arithmétique.

2.2. **Résultats fondamentaux sur le grand crible pour la norme L^2**

L'inégalité du grand crible repose de façon cruciale sur la notion d'espace δ-bien espacées :

Définition 2.2.1. *Soit $\delta > 0$. On dit que $X \subseteq \mathbb{R}$ finie est δ-bien espacé modulo 1 si pour tout $(x,y) \in X^2$ avec $x \neq y$, on a :*

$$\|x - y\|_\mathbb{Z} \geqslant \delta.$$

Avec $\|x\|_\mathbb{Z}$ la distance de x à $\mathbb{Z}$.

Le résultat suivant, de Montgomery et Vaughan publié en 1973, est celui qu'on va utiliser ici.

Théorème 2.2.1. *Soit $f \in \mathcal{E}$, $\delta > 0$ et X une partie δ-bien espacée modulo 1. On suppose que $\sigma(f)$ est inclus dans un intervalle de $\mathbb{Z}$ de longueur $N \geqslant 1$. Alors :*

$$\sum_{x \in X} |f(x)|^2 \leqslant \left(N + \frac{1}{\delta}\right) \int_0^1 |f(t)|^2\, dt.$$

De cette inégalité on tire l'inégalité du grand crible, qui va être l'outil principal de cette partie que l'on va chercher à adapter à la norme L^4 :

Théorème 2.2.2. *Soit $f \in \mathcal{E}$, $\mathcal{C}$ un crible et $Q \geqslant 1$. On suppose que $\sigma(f) \subseteq \mathcal{C}(I)$ avec I un segment de longueur $N \geqslant 1$. Alors :*

$$\|f\|_\infty^2 \leqslant \frac{Q^2+N}{\lambda_{\mathcal{C}}(Q)} \int_0^1 |f(t)|^2 \, dt.$$

Avec $\lambda_{\mathcal{C}}(Q) = \sum_{q \leqslant Q} \mu(q)^2 \prod_{p|q} \frac{\omega_{\mathcal{C}}(p)}{p - \omega_{\mathcal{C}}(p)}$.

Cette inégalité découle du théorème 2.2.1 appliqué à l'ensemble $\mathcal{F}_Q = \{p/q,\ p \leqslant q \leqslant Q,\ p \wedge q = 1, (p,q) \in \mathbb{N} \times \mathcal{Q}\}$, qui est $1/Q^2$-bien espacé modulo 1. Il faut également deux lemmes dont on va inclure les démonstrations pour que les arguments ensuite soient bien compris :

Dans cette partie, fixons p un nombre premier et $\mathcal{C}$ un crible. On pose $\tilde{f} : x \mapsto f(x/p)$, qui est clairement une fonction p-périodique. Si on restreint alors notre étude à $\mathbb{F}_p$, il est clair qu'on peut la décomposer dans la base des caractères de ce dernier. Ainsi, pour tout $x \in \mathbb{Z}$:

$$\tilde{f}(x) = \sum_{k=0}^{p-1} b_k \chi_k,\ b_k = \langle \chi_k, \tilde{f} \rangle.$$

Avec un petit abus de langage où l'on traite les χ_k comme des applications de $\mathbb{Z} \to \mathbb{C}^*$ p-périodiques additives au lieu de morphismes de $\mathbb{F}_p \to \mathbb{C}^*$. Si $f \in E$ avec $(c_n(f))_{n\in\mathbb{Z}}$ ses coordonnées dans la base canonique, on a alors :

$$\forall k \in [\![0, p-1]\!],\ b_k = \frac{1}{p} \sum_{j=0}^{p-1} \overline{\chi_k}\left(\frac{j}{p}\right) f\left(\frac{j}{p}\right) = \sum_{n\in\mathbb{Z}} c_n(f) \langle \chi_k, e_j \rangle.$$

Ici, il est clair que $\langle \chi_k, e_j \rangle = 1$ si $k \equiv j[p]$ et 0 sinon. On en tire donc le résultat suivant :

Proposition 2.2.1. *Soit $f \in E$ tel que $\sigma(f) \subseteq \mathcal{C}(\mathbb{Z})$. Alors :*

$$\frac{\omega_{\mathcal{C}}(p)}{p - \omega_{\mathcal{C}}(p)} |f(0)|^2 \leqslant \sum_{j=1}^{p-1} \left| f\left(\frac{j}{p}\right) \right|^2.$$

Démonstration. Si $p \notin \mathcal{P}_{\mathcal{C}}$ le résultat est évident. Sinon, supposons que $p \in \mathcal{P}_{\mathcal{C}}$ et observons qu'avec la remarque précédente :

$$\tilde{f} = \sum_{k=0}^{p-1} b_k \chi_k, \text{ avec } b_k = \sum_{n\in\mathbb{Z}, n\equiv k[p]} c_n(f).$$

Il s'ensuit que $b_k = 0$ si $\overline{k}_p \in \Omega_{p,\mathcal{C}}$. On en tire que :

$$|f(0)|^2 = |\tilde{f}(0)|^2 = \left| \sum_{k=0}^{p-1} b_k \mathbb{1}(\overline{k}_p \notin \Omega_{p,\mathcal{C}}) \right|^2 \leqslant (p - \omega_{\mathcal{C}}(p)) \sum_{k=0}^{p-1} |b_k|^2.$$

d'après l'inégalité de Cauchy-Schwarz. Or, cette dernière somme étant égale à $\langle \tilde{f}, \tilde{f} \rangle$ par l'identité de Parseval, on en tire l'inégalité :

$$|f(0)|^2 \leqslant \frac{p - \omega_{\mathcal{C}}(p)}{p} \sum_{j=0}^{p-1} \left| f\left(\frac{j}{p}\right) \right|^2.$$

Et en soustrayant le premier terme de la somme des deux côtés, on a le résultat. □

Il est important de remarquer une chose ici : cette inégalité est incroyablement flexible ! En effet, c'est nous qui imposons les valeurs de $\omega_{\mathcal{C}}(p)$, quels p nous intéressent, et la seule restriction qui en réalité va nous servir est l'inclusion $\sigma(f) \subseteq \mathcal{C}(\mathbb{Z})$.

Généralisons cette inégalité pour $q \in \mathcal{Q}$. Posons :

$$g_{\mathcal{C}}(q) = \prod_{p|q} \frac{\omega_{\mathcal{C}}(p)}{p - \omega_{\mathcal{C}}(p)}.$$

Ce produit, qui vaut 1 lorsque $q = 1$ et 0 si et seulement s'il existe un élément de $\mathcal{P}\backslash\mathcal{P}_{\mathcal{C}}$ qui divise q, va jouer un rôle central dans ce texte. En effet, on a alors la généralisation de la proposition précédente :

Proposition 2.2.2. *Soit $q \in \mathcal{Q}$ différent de 1. Alors, pour tout $f \in E$ tel que $\sigma(f) \subseteq \mathcal{C}(\mathbb{Z})$:*

$$g_{\mathcal{C}}(q)|f(0)|^2 \leqslant \sum_{\substack{1 \leqslant j \leqslant q-1 \\ j \wedge q = 1}} \left| f\left(\frac{j}{q}\right) \right|^2.$$

Démonstration. On va le montrer par récurrence sur le nombre de facteurs premiers de q, à savoir $\omega(q)$. On vient de traiter le cas $\omega(q) = 1$, c'est-à-dire $q \in \mathcal{P}$. Soit donc $n \in \mathbb{N}^*$ et supposons le résultat montré pour tout $\omega(q) \leqslant n$. Soit $q \in \mathcal{Q}$ tel que $\omega(q) = n$ et $p \in \mathcal{P}$ tel que $p \wedge q = 1$. On pose $q' = pq$. Alors on a l'égalité des deux ensembles suivants :

$$\{k \in [\![1, q' - 1]\!], k \wedge q' = 1\} = \{kp + qj,\ j \in [\![1, p-1]\!], k \wedge q = 1\}.$$

En effet, on vérifie immédiatement l'inclusion de l'ensemble à droite dans l'ensemble à gauche, et pour l'inclusion inverse on emploie un argument de cardinalité ; l'ensemble de gauche est de cardinal $\varphi(q') = \varphi(p)\varphi(q) = (p-1)\varphi(q)$, qui est le cardinal de l'ensemble de droite. Il s'ensuit que :

$$\sum_{\substack{1 \leqslant k \leqslant q'-1 \\ k \wedge q' = 1}} \left| f\left(\frac{k}{q'}\right) \right|^2 = \sum_{j=1}^{p-1} \sum_{\substack{1 \leqslant k \leqslant q-1 \\ k \wedge q = 1}} \left| f\left(\frac{k}{q} + \frac{j}{p}\right) \right|^2.$$

On applique alors l'hypothèse de récurrence à $x \mapsto f\left(x + \dfrac{j}{p}\right)$, qui vérifie bien les hypothèses nécessaires. On en tire que pour tout $j \in [\![1, p-1]\!]$:

$$g_{\mathcal{C}}(q) \left| f\left(\frac{j}{p}\right) \right|^2 \leqslant \sum_{\substack{1 \leqslant k \leqslant q-1 \\ k \wedge q = 1}} \left| f\left(\frac{k}{q} + \frac{j}{p}\right) \right|^2.$$

On applique alors la proposition 2.2.1 en sommant sur $1 \leqslant j \leqslant p-1$ et la multiplicativité de $g_{\mathcal{C}}$ pour conclure. □

2.3. Inégalité du grand crible pour L^4

On adapte dans cette partie les inégalités du grand crible pour la norme 4. Toutes les assertions concernant f_n sont justifiées par la suite d'inclusions :

$$A_n(g) \subseteq \square_n \subseteq \mathcal{C}([\![1, N^2]\!]).$$

Proposition 2.3.1. *Soit X une partie δ-bien espacée modulo 1 pour un $\delta > 0$. Alors :*

$$\sum_{x \in X} |f_n(x)|^4 \leqslant \left(2n^2 + \frac{1}{\delta}\right) \int_0^1 |f_n(t)|^4 \, dt.$$

Démonstration. C'est le théorème 2.2.1 appliqué en prenant $f = f_n^2$. $\sigma(f) \subseteq [\![1, 2n^2]\!]$ d'où le résultat. □

Lemme 2.3.1. *On reprend les hypothèses de la proposition 2.2.1. Alors pour tout p premier :*

$$\frac{\omega_{\mathcal{C}}(p)^2}{(p-1)(p-\omega_{\mathcal{C}}(p))^2}|f(0)|^4 \leqslant \sum_{k=1}^{p-1}\left|f\left(\frac{k}{p}\right)\right|^4.$$

Démonstration. On a déjà grâce à la proposition 2.2.1 que pour tout p premier :

$$\frac{\omega_{\mathcal{C}}(p)}{p-\omega_{\mathcal{C}}(p)}|f(0)|^2 \leqslant \sum_{k=1}^{p-1}\left|f\left(\frac{k}{p}\right)\right|^2 \Longrightarrow \frac{\omega_{\mathcal{C}}(p)^2}{(p-\omega_{\mathcal{C}}(p))^2}|f(0)|^4 \leqslant (p-1)\sum_{k=1}^{p-1}\left|f\left(\frac{k}{p}\right)\right|^4.$$

D'après Cauchy-Schwarz, d'où le résultat. □

On pose désormais, pour tout $Q \geqslant 1$:

$$\tilde{\lambda}_{\mathcal{C}}(Q) = \sum_{q\leqslant Q}\mu(q)^2\tilde{g}_{\mathcal{C}}(q) \text{ avec } \tilde{g}_{\mathcal{C}}(q) = \prod_{p|q}\frac{\omega_{\mathcal{C}}(p)^2}{(p-1)(p-\omega_{\mathcal{C}}(p))^2}.$$

On a alors le résultat suivant :

Lemme 2.3.2. *On reprend les notations de la proposition 2.2.2. Alors :*

$$\tilde{g}_{\mathcal{C}}(q)|f(0)|^4 \leqslant \sum_{\substack{1\leqslant j\leqslant q-1\\ j\wedge q=1}}\left|f\left(\frac{j}{q}\right)\right|^4.$$

Démonstration. On raisonne par récurrence d'exactement la même manière que dans la démonstration de la proposition 2.2.2. □

Avec ceci, on peut finaliser notre raisonnement avec cette inégalité finale :

Proposition 2.3.2. *On a l'inégalité suivante, valable pour tout $Q \geqslant 1$:*

$$|f_n(0)|^4 \leqslant \frac{2n^2+Q^2}{\tilde{\lambda}_{\mathcal{C}}(Q)}\int_0^1 |f_n(t)|^4\,dt.$$

Démonstration. On utilise le fait que l'ensemble $\mathcal{F}_Q$ soit $1/Q^2$-bien espacé modulo 1. On prend $f = f_n$ dans le lemme 2.3.2 et on somme sur les quadratfrei inférieurs à Q, différents de 1 :

$$|f(0)|^4 \sum_{\substack{q\leqslant Q\\ q\in\mathcal{Q}\setminus\{1\}}}\tilde{g}_{\mathcal{C}}(q) \leqslant \sum_{x\in\mathcal{F}_Q\setminus\{0\}}|f(x)|^4.$$

En ajoutant $|f(0)|^4$ des deux côtés et en mobilisant la proposition 2.3.1, on obtient :

$$\tilde{\lambda}_{\mathcal{C}}(Q)|f(0)|^4 \leqslant \left(2n^2+Q^2\right)\int_0^1 |f(t)|^4\,dt.$$

D'où le résultat. □

Cette proposition s'agence bien avec les remarques de la partie préliminaire ; l'intégrale vaut l'énergie additive, donc est majorée par $2g|A_n(g)|^2$, et en remarquant que $|f_n(0)|^4 = |A_n(g)|^4$ on obtient alors la majoration suivante :

Proposition 2.3.3. *On a la majoration suivante, valable pour tout $Q \geqslant 1$:*

$$|A_n(g)| \leqslant \sqrt{2g}\frac{\sqrt{2n^2+Q^2}}{\sqrt{\tilde{\lambda}_{\mathcal{C}}(Q)}}.$$

On est donc amené, comme il est toujours le cas dans la théorie du crible, à examiner la quantité $\tilde{\lambda}_{\mathcal{C}}(Q)$ lorsque $Q \to \infty$. Un choix naturel va être de prendre $Q = n \leqslant n^2$ et donc on va pouvoir écrire cette quantité assez facilement car on ne considère que des nombres premiers $p \leqslant Q$, donc dans l'ensemble $\mathcal{P}_{\mathcal{C}}$, tout en tenant compte du fait que $2 \notin \mathcal{P}_{\mathcal{C}}$.

2.4. Estimation de $\tilde{\lambda}_{\mathcal{C}}(Q)$

Il est important de faire une remarque : notre crible $\mathcal{C}$ ne considère pas $2 \in \mathcal{P}$ car tous les éléments de $\mathbb{F}_2$ sont des résidus quadratiques, et donc notre crible tuerait tout l'ensemble $[\![1, N^2]\!]$. Heureusement, comme le lemme suivant le montre, cela ne va pas nous poser de problème :

Lemme 2.4.1. *On introduit :*

$$\Lambda_{\mathcal{C}}(Q) = \sum_{q \leqslant Q} \mu(q)^2 \prod_{p|q} \frac{p-1}{(p+1)^2}.$$

Alors on a l'inégalité suivante :

$$\frac{9}{10}\Lambda_{\mathcal{C}}(n) \leqslant \tilde{\lambda}_{\mathcal{C}}(n).$$

Démonstration. Remarquons que :

$$\tilde{\lambda}_{\mathcal{C}}(n) = \sum_{q \leqslant n} \mu(q)^2 \prod_{p|q} \frac{p-1}{(p+1)^2} \mathbb{1}(q \equiv 1[2]).$$

Ainsi :

$$\Lambda_{\mathcal{C}}(n) = \tilde{\lambda}_{\mathcal{C}}(n) + \frac{1}{9} \sum_{2q \leqslant Q} \mu(2q)^2 \prod_{p|q} \frac{p-1}{(p+1)^2} \leqslant \frac{10}{9}\tilde{\lambda}_{\mathcal{C}}(n).$$

D'où le résultat. □

On va donc chercher à estimer $\Lambda_{\mathcal{C}}(n) = \sum_{q \leqslant n} \lambda(q)$, avec $\lambda(q) = \mu(q)^2 \prod_{p|q} \frac{p-1}{(p+1)^2}$. On définit alors $\Lambda : \mathbb{C} \to \mathbb{C}$ pour tout $s = \sigma + i\tau$ avec $\sigma > 1$:

$$\Lambda(s) = \sum_{q=1}^{\infty} \frac{\lambda(q)}{q^s}.$$

Λ est la série de Dirichlet correspondant à la suite $(\lambda(q))_{q \geqslant 1}$. La convergence est assurée dans le domaine $\sigma > 1$ car la suite $(\lambda(q))_{q \geqslant 1}$ est bornée. On a alors le résultat suivant :

Proposition 2.4.1. *Il existe une fonction holomorphe $D : \{\sigma + i\tau,\ \sigma > 1/2\} \to \mathbb{C}$ telle que :*

$$\forall Re(s) > 1,\ \Lambda(s) = \zeta(s+1)D(s).$$

Avec ζ la fonction zêta de Riemann.

Démonstration. On remarque que dans le domaine $\sigma > 1$ on peut voir Λ comme un produit eulérien :

$$\Lambda(s) = \prod_{p \in \mathcal{P}} \left(1 + \frac{p-1}{p^s(p+1)^2}\right).$$

On pose alors $D(s) = \Lambda(s)/\zeta(s+1)$, qui est au moins méromorphe sur $\sigma > 1$. En prenant l'écriture en produit eulérien de ζ, on trouve :

$$\forall \mathrm{Re}(s) > 1,\ D(s) = \prod_{p\in\mathcal{P}} \left(1 + \frac{p-1}{(p+1)^2} p^{-s}\right)(1-p^{-1-s}) = \prod_{p\in\mathcal{P}} \left(1 - \frac{3p+1}{p^s(p(p+1)^2)} - \frac{p-1}{(p+1)^2 p^{2s+1}}\right).$$

Il s'ensuit que le produit converge uniformément sur tout compact de la région $\sigma > -1/2$ et donc D est holomorphe dans cette région, d'où le résultat. □

On utilise maintenant un théorème taubérien, conséquence du théorème taubérien de Wiener-Ikehara [6] :

Théorème 2.4.1. *Soit $G(s) = \sum_{q=1}^{\infty} \frac{g(q)}{q^s}$ une série de Dirichlet à coefficients non négatifs. Supposons que $G(s) = \zeta(s)^k A(s)$ avec $k \in \mathbb{N}^*$ et A une série de Dirichlet qui converge absolument sur $\sigma > 1$, qui peut être prolongé holomorphiquement sur $\sigma \geqslant 1$ avec $A(1) \neq 0$. Alors, lorsque $Q \to \infty$:*

$$\sum_{q\leqslant Q} g(q) = \frac{R}{(k-1)!} Q(\ln(Q))^{k-1} + \mathcal{O}(Q(\ln(Q))^{k-2}).$$

Avec R le résidue de G en 1.

Appliquons ce théorème à la suite $h(q) = q\lambda(q)$. D'après la proposition 2.4.1, on a :

$$H(s) = \sum_{q=1}^{\infty} \frac{h(q)}{q^s} = \Lambda(s-1) = \zeta(s)D(s-1).$$

On voit que A satisfait les conditions du théorème 2.4.1, avec $k = 1$, $A(s) = D(s-1)$ qui converge absolument sur $\sigma > 1/2$ et $R = D(0)$. Ainsi :

$$\sum_{q\leqslant Q} q\lambda(q) = D(0)Q + \mathcal{O}\left(\frac{Q}{\ln(Q)}\right).$$

On conclut alors avec le lemme suivant :

Lemme 2.4.2. *Soit $(a_q)_{q\geqslant Q}$ une suite de réels positifs telle que :*

$$S(Q) = \sum_{q\leqslant Q} q a_q \sim CQ.$$

Pour un $C > 0$. Alors $\sum_{q\leqslant Q} a_q \sim C\ln(Q)$..

Démonstration. Quitte à diviser par C on considère le cas $\sum_{q\leqslant Q} q a_q \sim Q$. On mobilise ainsi une sommation d'Abel :

$$\sum_{q\leqslant Q} a_q = \frac{S(Q)}{Q} + \int_1^Q \frac{S(t)}{t^2}\, dt = \int_1^Q \frac{C}{t}\, dt + o\left(\int_1^Q \frac{C}{t}\, dt\right).$$

D'après les hypothèses et les théorèmes de comparaison d'intégrales divergentes. □

On en déduit alors la proposition suivante :

Proposition 2.4.2. *On a $\Lambda_{\mathcal{C}}(n) \sim \alpha\ln(n)$ avec $\alpha = \prod_{p\in\mathcal{P}} \left(1 - \frac{4}{(p+1)^2}\right)$.*

Démonstration. Conséquence directe du lemme 2.4.2 et du théorème 2.4.1. □

On en tire alors le théorème suivant, conséquence de tout ce qui précède en prenant $Q = n$ dans la proposition 2.3.3 :

Théorème 2.4.2. *Il existe une constante universelle $M > 0$ telle que, pour tout $g, n \geqslant 1$:*

$$|A_n(g)| \leqslant \frac{M\sqrt{g}n}{\sqrt{\ln(n)}}.$$

Démonstration. On reprend l'inégalité de la proposition 2.3.3 et on emploie le lemme 2.4.1. Il existe alors une constante $a > 0$ telle que :

$$|A_n(g)| \leqslant \frac{a\sqrt{g}n}{\sqrt{\Lambda_{\mathcal{C}}(n)}}.$$

Or, $\Lambda_{\mathcal{C}}(n) \sim \alpha \ln(n)$, d'où le résultat. □

.

2.5. **Autres avancées**

Seulement quelques jours après qu'on a trouvé la majoration ci-dessus, E. Croot et deux de ses élèves [12] ont réussi à raffiner ce dernier avec des idées classique de combinatoire additive. Même s'ils disent qu'ils se sont inspiré d'un article sur le crible [5], les techniques utilisées sont assez élémentaires.

Proposition 2.5.1. *(Croot et. al, 2026) Il existe une constante $c > 0$ tel que :*

$$|A_n(1)| \leqslant n \exp\left(\frac{-c\ln(n)}{\ln(\ln(n))}\right).$$

La démonstration se généralise difficile pour les $|A_n(g)|$, et constitue une partie majeure de l'article de Croot.

Démonstration. Soit $\varepsilon > 0$. On suppose que $|A_n(1)| > n^{1-\varepsilon}$ sinon on a terminé. On pose alors d le produit de t nombres premiers de l'intervalle $[\ln(n), 2\ln(n)]$, avec :

$$t = \left\lfloor \frac{(1-2\varepsilon)\ln(n)}{\ln(\ln(n))} \right\rfloor.$$

On remarque alors que $d \leqslant 2^t \ln(n)^t = n^{1-2\varepsilon+o(1)}$ donc pour n assez grand $d < |A_n(1)|$, un fait qu'on mobilisera à la toute fin de la démonstration. On introduit ainsi deux nouvelles quantités :

(*i*) Pour tout $r \in [\![0, d-1]\!]$, $A(r,d) = |\{a \in A_n(1),\ a \equiv r[d]\}|$.

(*ii*) Pour tout $k \in \mathbb{Z}$, $r(k) = \{(a, a') \in A_n(1), a - a' = k\}$.

Alors on a les 3 propriétés suivantes :

(*i*) $|A_n(1)| = \sum_{r=0}^{d-1} |A(r,d)|$.

(*ii*) $r(k) \in \{0,1\}$ pour tout $k \in \mathbb{Z}$ car $A_n(1)$ est un ensemble de Sidon.

(*iii*) $\sum_{\substack{|k| \leqslant n^2 \\ k|d}} r(k) = \sum_{r=0}^{d-1} A(r,d)^2 - |A_n(1)|$ en comptant.

On note $\mathcal{R}$ l'ensemble des $r \in [\![0, d-1]\!]$ tel que $A(r,d) \neq 0$. Le théorème des restes chinois garantit ${}^{\mathbb{Z}}/_{d\mathbb{Z}} \cong \prod_{p|d} \mathbb{F}_p$, et puisque $A_n(1)$ peut occuper au plus $(p+1)/2$ résidus dans chaque $\mathbb{F}_p$ ($p \geqslant 3$), on en déduit que :

$$|\mathcal{R}| \leqslant \prod_{p|d} \frac{p+1}{2} = \frac{d(1+o(1))}{2^t}.$$

On applique alors Cauchy-Schwarz à la somme de la propriété (*i*) pour obtenir :

$$|A_n(1)|^2 \leqslant |R| \sum_{r=0}^{d-1} |A(r,d)|^2 \leqslant \frac{d(1+o(1))}{2^t} \sum_{\substack{|k| \leqslant n^2 \\ k|d}} r(k) + \frac{|A_n(1)|d(1+o(1))}{2^t}.$$

Or, les propriétés *(ii)* et *(iii)* impliquent que $\sum_{\substack{|k| \leqslant n^2 \\ k|d}} r(k) \leqslant \frac{2n^2}{d}$. Ainsi :

$$\frac{2^{t-1}|A_n(1)|^2}{d} << \frac{2^t(|A_n(1)|^2 - (d+o(1))|A_n(1)|)}{d(1+o(1))} \leqslant \frac{2n^2}{d}.$$

Et le résultat s'ensuit. □

Croot et al. réussissent à généraliser ce dernier résultat, mais cela nécessite beaucoup d'artillerie lourde concernant le crible, afin d'obtenir la proposition suivante :

Proposition 2.5.2. *Il existe une constante $c > 0$ tel que pour tout $n, g \geqslant 1$:*

$$|A_n(g)| \leqslant g^{1/4} n^{1 - \frac{c}{\ln(\ln(n))}}.$$

2.6. **Remarques**

Les bornes supérieures trouvées ici sont meilleures que celle obtenue par un argument classique. En effet, montrons en quelques lignes la proposition suivante :

Proposition 2.6.1. *Il existe une constante universelle $C > 0$ telle que, pour tout $n, g \geqslant 1$:*

$$|A_n(g)| \leqslant \sqrt{g} \frac{Cn}{\ln(n)^{1/4}}.$$

Démonstration. On a :

$$|A_n(g)|^2 = \sum_{a \in A+A} r_{A_n(g)+A_n(g)}(a) \leqslant 2g|A_n(g) + A_n(g)| \leqslant 2g|\square_n + \square_n|.$$

Notons $\Pi_\square(m)$ le nombre d'entiers $\leqslant m$ qui peuvent s'écrire comme la somme de deux carrés. D'après le théorème de Bernays [2], il existe une constante $b > 0$ telle que :

$$\Pi_\square(m) \sim \frac{bm}{\sqrt{\ln(m)}}.$$

Ainsi, il existe une constante $C > 0$ telle que, pour tout $n, g \geqslant 1$:

$$|A_n(g)|^2 \leqslant g \frac{C2n^2}{\sqrt{2\ln(n)}}.$$

On en déduit le résultat en prenant la racine. □

3. **Minoration de $\|\square_n\|_g$**

La première piste qui a été suivie pour le travail de minoration, avant que l'on ait connaissance du meilleur résultat connu sur le cardinal maximal des ensembles de Sidon dans $\square_n$, a été une adaptation des arguments de l'article [10] laquelle donne une minoration de $\|\square_n\|_g$ par $\frac{1}{4}\|\{1, \ldots, n\}\|_g$.

On obtient ainsi que $\|\square_n\|_g$ est au moins de l'ordre de $\sqrt{n}$ ce qui est bien moins bon que les résultats de [3] ou [11].

On met en annexe 4.2 la démonstration produite dans le cadre de cette première piste et on consacre cette section au meilleur résultat de minoration que l'on a été donné de trouver en généralisant l'argument de [11] qui montre que $\|\Box_n\|_1$ est au moins de l'ordre de $n^{2/3}$.

3.1. La méthode hypergraphique

On va, suivant le chemin tracé par [11], exploiter des résultats de combinatoires sur des hypergraphe et notamment exploiter la notion d'hypergraphe uniforme et linéaire.

Un **hypergraphe** $\mathcal{G} = (V, \mathcal{E})$ est la donnée d'un ensemble V et d'un ensemble $\mathcal{E}$ inclus dans $\mathcal{P}(V)$.

Les éléments de V sont appelés **sommets** de l'hypergraphe $\mathcal{G}$ et les éléments de $\mathcal{E}$ sont appelés **arêtes** (ou *hyperarêtes*). Lorsque toutes les arêtes d'un hypergraphe sont de même cardinal $k \in \mathbb{N}$, l'hypergraphe est dit k**-uniforme**.

Le **degré** $deg(v)$ d'un sommet $v \in V$ est défini comme le nombre d'arêtes auxquelles v appartient. $Deg(\mathcal{G})$ désigne alors le degré maximal d'un sommet de $\mathcal{G}$ (lorsque cela est bien défini, notamment lorsque $\mathcal{G}$ est fini).

Un **2-cycle** de $\mathcal{G}$ est une paire d'arêtes $\{E_1, E_2\}$ ($E_1 \neq E_2$) avec $|E_1 \cap E_2| \geqslant 2$. On note $c_2(\mathcal{G})$ le nombre de 2-cycles de $\mathcal{G}$ et, pour $i \geqslant 2$, $c_{2,i}(\mathcal{G})$ le nombre de deux cycles $\{E_1, E_2\}$ tels que $|E_1 \cap E_2| = i$.

Un hypergraphe est qualifié de **linéaire** s'il ne contient aucun 2-cycle.

Partant d'une partie $A \subseteq V$, on définit le sous graphe de $\mathcal{G}$ induit par A comme l'hypergraphe dont les sommets sont les éléments de A et les arêtes les éléments de $\mathcal{E}$ inclus dans A. A est dite **indépendante** (pour $\mathcal{G}$) si le sous graphe induit par A ne contient pas d'arête.

On note (lorsque cela est bien défini) $I(\mathcal{G})$ le cardinal maximal d'une partie indépendante de V.

On va, comme dans [11], chercher à exploiter le résultat suivant sur les hypergraphes uniformes et linéaires (non démontré ici, provenant de [8]) :

Théorème 3.1.1. *Soit $k \geqslant 3$, il existe des constantes $\lambda_k, \tau_k > 0$ telles que si $\mathcal{G} = (V, \mathcal{E})$ est un hypergraphe linéaire et k-uniforme avec $|V| = n \in \mathbb{N}$ et $Deg(\mathcal{G}) \leqslant t^{k-1}$ pour un certain $t \geqslant \tau_k$, alors :*

$$I(\mathcal{G}) \geqslant \lambda_k \frac{n}{t} \ln(t)^{\frac{1}{k-1}}.$$

On va aussi utiliser le lemme de probabilités suivant pouvant être obtenu par l'inégalité de Chernoff :

Lemme 3.1.1. *Si $(X_i)_{i\in\mathbb{N}}$ est une suite de variables aléatoire de Bernoulli avec $X_i \rightsquigarrow \mathcal{B}(n_i, p_i)$ tel que $n_i p_i \xrightarrow[i\to+\infty]{} +\infty$ et si $\delta \in]0;1[$, on a :*

$$\mathbb{P}(X_i < (1-\delta) n_i p_i) \xrightarrow[i\to+\infty]{} 0.$$

Pour construire un grand sous ensemble $B_2[g]$ inclus dans $\Box_n$, on va chercher à utiliser le théorème 3.1.1 pour obtenir une grande partie indépendante d'un hypergraphe bien construit.

En étudiant les points clefs de la démonstration pour $g = 1$ proposée dans [11] on conjecture et démontre le résultat général suivant qu'on cherchera ensuite à appliquer dans notre contexte.

Théorème 3.1.2. *Soit $k \geqslant 3$ et, pour chaque $n \geqslant 1$, $\mathcal{G}_n = (V_n, \mathcal{E}_n)$ un hypergraphe fini et k-uniforme.*
On suppose trouver deux suite $(p_n)_{n\in\mathbb{N}} \in [0;1]^{\mathbb{N}}$ et $(t_n)_{n\in\mathbb{N}} \in (R_+^*)^{\mathbb{N}}$ telles que :

(1) $p_n|V_n| \xrightarrow[n\to+\infty]{} +\infty$

(2) $t_n \xrightarrow[n\to+\infty]{} +\infty$

(3) pour tout $i \in \{2, \dots, k-1\}$, $c_{2,i}(\mathcal{G}_n) p_n^{2k-i-1} = O(|V_n|)$

(4) $|\mathcal{E}_n|(\frac{p_n}{t_n})^{k-1} = O(|V_n|)$.

Il existe alors une constante $C > 0$ telle que, pour n suffisamment grand, on a :

$$I(\mathcal{G}_n) \geqslant C|V_n| \frac{p_n}{t_n} \ln(t_n)^{\frac{1}{k-1}}.$$

Démonstration. Remarquons que quitte à multiplier $(p_n)_{n\in\mathbb{N}}$ par une constante dans $]0;1]$ on peut supposer avoir pour tout $i \in \{2,\dots,k-1\}$ l'inégalité asymptotique :

$$c_{2,i}(\mathcal{G}_n)p_n^{2k-i-1} \leqslant \frac{1}{16(k-2)}|V_n|. \tag{0}$$

Puis, quitte à multiplier $(t_n)_{n\in\mathbb{N}}$ par une constante strictement positive, on peut supposer avoir l'inégalité asymptotique :

$$|\mathcal{E}_n|\left(\frac{p_n}{t_n}\right)^{k-1} \leqslant \frac{1}{32k}|V_n|. \tag{0'}$$

Soit $n \geqslant 1$. On va chercher, en utilisant une méthode probabiliste, à trouver une partie de V_n telle que le sous graphe qu'elle induit contienne beaucoup de sommets, peu d'arêtes et peu de 2-cycles.

On définit R_n comme le sous-ensemble aléatoire de V_n défini en choisissant, indépendamment pour chaque élément de V_n, de le prendre comme élément de R_n avec probabilité p_n.

Ainsi, $|R_n| \rightsquigarrow \mathcal{B}(|V_n|, p_n)$ et donc, par le lemme 3.1.1 et l'hypothèse 1. :

$$\mathbb{P}\left(R_n < \frac{1}{2}p_n|V_n|\right) \xrightarrow[n\to+\infty]{} 0.$$

En particulier, si n est suffisamment grand, on a :

$$\mathbb{P}\left(R_n < \frac{1}{2}p_n|V_n|\right) \leqslant \frac{1}{4}. \tag{1}$$

Notons $\mathcal{G}'_n = (R_n, \mathcal{E}'_n)$ le sous graphe induit par R_n. L'on a, pour $2 \leqslant i \leqslant k-1$:

$$\mathbb{E}(c_{2,i}(\mathcal{G}'_n)) = c_{2,i}(\mathcal{G}_n)p_n^{2k-i}.$$

Et donc si on suppose n suffisamment grand pour vérifier (0) on a $\mathbb{E}(c_2(\mathcal{G}'_n)) \leqslant \frac{1}{16}p_n|V_n|$.

L'inégalité de Markov montre alors que :

$$\mathbb{P}\left(c_2(\mathcal{G}'_n) > \frac{1}{4}p_n|V_n|\right) \leqslant 4\frac{\mathbb{E}(c_2(\mathcal{G}'_n))}{p_n|V_n|} \leqslant \frac{1}{4}. \tag{2}$$

Enfin remarquons que l'on a : $\mathbb{E}(|\mathcal{E}'_n|) = |\mathcal{E}_n|p_n^k$ et donc par l'inégalité de Markov :

$$\mathbb{P}(|\mathcal{E}'_n| > 4|\mathcal{E}_n|p_n^k) \leqslant \frac{1}{4}. \tag{3}$$

Par (1), (2) et (3) on obtient que, dès que n est suffisamment grand :

$$\mathbb{P}\left(\left(|R_n| \geqslant \frac{1}{2}p_n|V_n|\right) \cap \left(c_2(\mathcal{G}'_n) \leqslant \frac{1}{4}p_n|V_n|\right) \cap \left(|\mathcal{E}'_n| \leqslant 4|\mathcal{E}_n|p_n^k\right)\right) \geqslant 1 - \frac{1}{4} - \frac{1}{4} - \frac{1}{4} = \frac{1}{4} > 0.$$

On peut dès lors trouver $V_n^* \subseteq V_n$, dont on note $\mathcal{G}_n^* = (V_n^*, \mathcal{E}_n^*)$ le sous graphe induit, telle que :

— $|V_n^*| \geqslant \frac{1}{2}p_n|V_n|$

— $c_2(\mathcal{G}_n^*) \leqslant \frac{1}{4}p_n|V_n|$

— $|\mathcal{E}_n^*| \leqslant 4|\mathcal{E}_n|p_n^k$

Au sens de cet hypergraphe on a :

$$\sum_{v\in V_n^*}\deg(v) = \sum_{v\in V_n^*}\sum_{E\in\mathcal{E}_n^*}\mathbb{1}_E(v) = \sum_{E\in\mathcal{E}_n^*}\sum_{v\in V_n^*}\mathbb{1}_E(v) = k|\mathcal{E}_n^*| \leqslant 4k|\mathcal{E}_n|p_n^k$$

.

Si on note T_n le nombre de sommets de cet hypergraphe de degré supérieur à t_n^{k-1} on a alors que :

$$T_n t_n^{k-1} \leqslant 4k|\mathcal{E}_n|p_n^k.$$

Et donc, en supposant n suffisamment grand pour vérifier (0') :

$$T_n \leqslant 4k|\mathcal{E}_n|\left(\frac{p_n}{t_n}\right)^{k-1} p_n \leqslant \frac{1}{8}p_n|V_n|.$$

Notons alors $\mathcal{G}_n^\dagger = (V_n^\dagger, \mathcal{E}_n^\dagger)$ un sous graphe induit par une partie de V_n^* obtenue en retirant à V_n^* un élément chaque deux cycles de $\mathcal{G}_n^*$ et tous les éléments de degré supérieur à t_n^{k-1} au sens de $\mathcal{G}_n^*$.

On a :

$$|V_n^\dagger| \geqslant |V_n^*| - c_2(\mathcal{G}_n^*) - T_n \geqslant \left(\frac{1}{2} - \frac{1}{4} - \frac{1}{8}\right) p_n|V_n| = \frac{1}{8}p_n|V_n|.$$

et $\mathcal{G}_n^\dagger$ est un hypergraphe linéaire k-uniforme qui vérifie $Deg(\mathcal{G}_n^\dagger) \leqslant t_n^{k-1}$.

Ainsi, si on suppose n suffisamment grand pour vérifier toutes les inégalités asymptotiques précédemment établies et pour avoir $t_n \geqslant \tau_k$, en appliquant le théorème 3.1.1 sur $\mathcal{G}_n^\dagger$ on obtient que :

$$I(\mathcal{G}_n) \geqslant I(\mathcal{G}_n^\dagger) \geqslant \frac{\lambda_k}{8}|V_n|\frac{p_n}{t_n}\ln(t_n)^{\frac{1}{k-1}}.$$

□

Remarque 3.1.1. *Dans ce qui va suivre, on va établir la condition 3. simplement en vérifiant la condition plus forte : $c_2(\mathcal{G}_n)p_n^k = o(|V_n|)$.*

Remarque 3.1.2. *Si l'on connaît les constantes de dominations dans les conditions 3. et 4., la constante C peut être choisie comme fonction uniquement de ces constantes et de k.*

Remarque 3.1.3. *Les conditions 1. et 2. sont semblablement plus fortes que nécessaires pour aboutir à un résultat.*
Mais dans la pratique pour obtenir une minoration intéressante il est bon que ces conditions soient vérifiées, nous n'alourdirons pas ici ni l'énoncé ni la preuve en recherchant les conditions optimales.

Fixons $g \geqslant 1$. On définit pour $n \geqslant 1$ l'hypergraphe $2(g+1)$- uniforme $\mathcal{G}_n = (V_n, \mathcal{E}_n)$ par :

$$V_n = \{1, 2, \ldots, n\}.$$

$$\mathcal{E}_n = \left\{ \{a_1, b_1, a_2, b_2, \ldots, a_{g+1}, b_{g+1}\} \subseteq V_n \text{ (de cardinal 2(g+1))} ;\ a_1^2 + b_1^2 = a_2^2 + b_2^2 = \cdots = a_{g+1}^2 + b_{g+1}^2 \right\}.$$

[11] affirme alors (dans le cas $g = 1$) que trouver un sous ensemble $B_2[g]$ de $\square_n$ revient à trouver une partie indépendante de $\mathcal{G}_n$.

C'est faux au sens où l'on a défini les ensembles $B_2|g]$ mais c'est juste que [11] s'intéresse en fait aux ensembles $B_2[g]^*$. Ce n'est pas un problème puisque, on rappelle la proposition 1.0.1, $\|\square_n\|_g$ et $\|\square_n\|_g^*$ sont du même ordre de grandeur.

(On constate bien que trouver une partie $B_2|g]^*$ de $\square_n$ se rapporte à trouver une partie indépendante de $\mathcal{G}_n$).

Notre objectif à partir de là est d'utiliser le théorème 3.1.2 pour obtenir une grande partie indépendante de $\mathcal{G}_n$ ainsi défini.

3.2. **Les estimations utiles**

Moralement, pour obtenir des minorations intéressantes à partir du Théorème 3.1.2 on veut avoir des majorations des ordres de grandeur de $|\mathcal{E}_n|$ et des $c_{2,i}(\mathcal{G}_n)$ de sorte à ensuite trouver des suites $(p_n), (t_n)$ telles que les rapports $\frac{p_n}{t_n}$ soient aussi grands que possibles mais que les hypothèses 3. et 4. (qui bornent supérieurement les valeurs pouvant être prises par respectivement p_n et $\frac{p_n}{t_n}$) soient tout de même vérifiées.

On va donc chercher à estimer $|\mathcal{E}_n|$ et $c_2(\mathcal{G}_n)$. Pour ce faire on va définir r_2 comme l'application qui à un entier naturel associe le nombre de façons de l'écrire comme la somme de deux carrés d'entiers naturels distincts. On va aussi définir D comme l'application qui à un entier naturel associe son nombre de diviseurs. le théorème des deux carrés de Fermat garantit que $r_2(n) = O(D(n))$. On va être amené à utiliser les résultats suivants connus sur le comportement asymptotique de D et de r_2 :

Proposition 3.2.1. *On a :*

(1) Pour tout $\varepsilon > 0$, $D(n) = o(n^\varepsilon)$.

(2) En conséquence, pour tout $\varepsilon > 0$, $r_2(n) = o(n^\varepsilon)$.

(3) Pour tout $\alpha \in \mathbb{N}^*$, $\sum_{i=1}^{n} r_2^\alpha(i) = O(n \ln(n)^{2^{\alpha-1}-1})$.

Le point 3. de la proposition 3.2.1 est un cas particulier d'un résultat montré dans [4]. On indique en annexe 4.3 une démonstration du point 1.

Commençons par une domination de $|\mathcal{E}_n|$:

Proposition 3.2.2. $|\mathcal{E}_n| = O(n^2 \ln(n)^{2^g-1})$.

Démonstration.

$$|\mathcal{E}_n| \leqslant \sum_{i=1}^{2n^2} \binom{r_2(i)}{g+1} = O\left(\sum_{i=1}^{2n^2} r_2(i)^{g+1}\right) = O\left(n^2 \ln(n)^{2^g-1}\right).$$

□

Et pour ce qui est de $c_2(\mathcal{G}_n)$:

Proposition 3.2.3. *Pour tout $\varepsilon > 0$, $c_2(\mathcal{G}_n) = o(n^{2+\varepsilon})$.*

Démonstration. On va ici raisonner par récurrence sur g et donc le temps seulement de cette démonstration on ne considère pas g fixé et on note donc les hypergraphes considérés $\mathcal{G}_n^{(g)} = (V_n^{(g)}, \mathcal{E}_n^{(g)})$ plutôt que juste $\mathcal{G}_n = (V_n, \mathcal{E}_n)$.

On pose, pour tout $g, n \geqslant 1$ $c_2^{(g)}(n) = c_2(\mathcal{G}_n^{(g)}) + |\mathcal{E}_n^{(g)}|$ le nombre de 2-cycles de $\mathcal{G}_n^{(g)}$ au sens large (c'est-à-dire en incluant les paires d'arêtes dégénérées en singletons).

On va montrer par récurrence sur g que pour tout $g \geqslant 1$, pour tout $\varepsilon > 0$, $c_2^{(g)}(n) = o(n^{2+\varepsilon})$, ce résultat étant bien sur plus fort que ce que l'on cherche à montrer.

Initialisation

Pour le cas $g = 1$, on redonne l'argument exposé dans [11] :

Soit $\varepsilon > 0$. On sait par la proposition 3.2.2 que $|\mathcal{E}_n^{(1)}| = o(n^{2+\varepsilon})$.

On a aussi que $c_{2,3}(\mathcal{G}_n^{(1)}) \leqslant 4 \cdot 6 \cdot |\mathcal{E}_n^{(1)}| = o(n^{2+\varepsilon})$.

En effet, si $E = \{a_1, a_2, a_3, a_4\} \in \mathcal{E}_n^{(1)}$, toute autre arête intersectant E en exactement 3 sommets peut être obtenu à partir de E en retirant un a_i pour $i \in \{1, 2, 3, 4\}$ puis en ordonnant $\{1, \ldots, i-1, i+1, \ldots, 4\} = \{j_1, j_2, j_3\}$ et en ajoutant à $E_1 \setminus \{a_i\}$: $\sqrt{a_{j_1}^2 + a_{j_2}^2 - a_{j_3}^2}$.

Il ne reste plus qu'à montrer que $c_{2,2}(\mathcal{G}_n^{(1)}) = o(n^{2+\varepsilon})$.

On remarque qu'un 2-cycle $\{E_1, E_2\}$ avec $|E_1 \cap E_2| = 2$ est d'une deux formes suivantes :

(1) $E_1 = \{a, b, c, d\}$ et $\{a, b, c', d'\}$ avec $a^2 + b^2 = c^2 + d^2 = c'^2 + d'2$

(2) $E_1 = \{a, c, b, d\}$ et $E_2 = \{a, c', b, d'\}$ avec $a > b$, $a^2 + c^2 = b^2 + d^2$ et $a^2 + c'^2 = b^2 + d'^2$.

Dans ce cas on a donc $a^2 - b^2 = (d' + c')(d' - c')$.

En fixant E_1, le nombre d'arêtes E_2 qui font de $\{E_1, E_2\}$ un 2-cycle de la forme 1. est majoré par $r_2(\max_{x\in E_1}\ x^2 + \min_{x\in E_1}\ x^2)$.

Le nombre d'arêtes E_2 qui font de $\{E_1, E_2\}$ un 2-cycle de la forme 2. est majoré par le nombre de façons de choisir a, b et c' (le choix de c' imposant le choix de d') donc par $4 \max_{a,b\in E_1\ ;\ a>b} D(a^2 - b^2)$.
Ainsi :

$$c_{2,2}(\mathcal{G}_n^{(1)}) \leqslant |\mathcal{E}_n^{(1)}| \left[\max_{1\leqslant i\leqslant 2n^2}\ r_2(i) \ +\ 4 \max_{1\leqslant i\leqslant n}\ D(i) \right].$$

Or d'après la proposition 3.2.2 on a $|\mathcal{E}_n^{(1)}| = o(n^{2+\varepsilon/2})$ et d'après la proposition 3.2.1 $\max_{1\leqslant i\leqslant 2n^2}\ r_2(i) = O(n^{\varepsilon/2})$ et $\max_{1\leqslant i\leqslant n}\ D(i) = O(n^{\varepsilon/2})$.

D'où :

$$c_{2,2}(\mathcal{G}_n^{(1)}) = o(n^{2+\varepsilon}).$$

Hérédité

Supposons maintenant le résultat vrai pour $g - 1 \geqslant 1$ et montrons le pour g.

Soient $a_1, b_1, a_2, b_2, \ldots, a_{g+1}, b_{g+1} \in V_n^{(g)}$ deux à deux distincts tels que $a_1^2 + b_1^2 = a_2^2 + b_2^2 = \cdots = a_{g+1}^2 + b_{g+1}^2$. Soient $a'_1, b'_1, a'_2, b'_2, \ldots, a'_{g+1}, b'_{g+1}$ vérifiant la même hypothèse. On suppose que $|\{a_1, b_1, a_2, b_2, \ldots, a_{g+1}, b_{g+1}\} \cap \{a'_1, b'_1, a'_2, b'_2, \ldots, a'_{g+1}, b'_{g+1}\}| \geqslant 2$.

On constate, puisque $g + 1 \geqslant 3$ qu'il existe $i, j \in \{1, 2, \ldots, g + 1\}$ tels que :

$$|\{a_1, b_1, \ldots, a_{i-1}, b_{i-1}, a_{i+1}, b_{i+1}, \ldots, a_{g+1}, b_{g+1}\} \cap \{a'_1, b'_1, \ldots, a'_{j-1}, b'_{j-1}, a'_{j+1}, b'_{j+1}, \ldots, a'_{g+1}, b'_{g+1}\}| \geqslant 2$$

On en déduit que :

$$c_2^{(g)}(n) \leqslant c_2^{(g-1)}(n) \left(\max_{1\leqslant i\leqslant 2n^2}\ r_2(i) \right)^2. \tag{1}$$

En effet, au vu du constat précédent, tout 2-cycle (au sens large) de $\mathcal{G}_n^{(g)}$ peut être construit à partir d'un 2-cycle (au sens large) de $\mathcal{G}_n^{(g-1)}$ en ajoutant à chaque arête de ce deux cycle deux éléments dont la somme des carrés donne le même résultat que la somme des carrés du plus petit et du plus grand élément de l'arête.

Soit $\varepsilon > 0$. Comme $\max_{1\leqslant i\leqslant 2n^2}\ r_2(i) = O(n^{\varepsilon/3})$ d'après la proposition 3.2.1 et $c_2^{(g-1)}(n) = o(n^{2+\varepsilon/3})$ par hypothèse de récurrence, l'inégalité (1) permet bien de conclure que :

$$c_2^{(g)}(n) = o(n^{2+\varepsilon}).$$

□

Remarque 3.2.1. *L'estimation de $c_{2,2}(\mathcal{G}_n^{(1)})$ dans la démonstration du Théorème 3.2.3 est la seule étape de tout le raisonnement exposé dans cette section qui utilise le fait de travailler spécifiquement sur les carrés (on y utilise la factorisation de la différence de deux carrés).*

En effet, si on note $A = \{n^2\ ;\ n \in \mathbb{N}\}$ tous les autres arguments reposent uniquement sur des estimations de l'ordre de grandeur des éléments de A et de la suite r_{A+A}.

3.3. Obtention d'un grand $B_2[g]$

Maintenant que l'on dispose de ces estimations on va chercher à appliquer le théorème 3.1.2 en cherchant $(p_n), (t_n)$ convenables de la forme :

$$p_n = n^{-\alpha+\varepsilon} \ln(n)^{-\beta} \text{ et } t_n = n^{\varepsilon}.$$

avec $\alpha \in]0; 1[$, $\beta \geqslant 0, \varepsilon > 0$ et en cherchant à prendre α et β aussi petits que l'on peut.

On a :

$$|\mathcal{E}_n| \left(\frac{p_n}{t_n}\right)^{2g+1} = O\left(n^{2-(2g+1)\alpha} \ln(n)^{2^g-1-(2g+1)\beta}\right).$$

Ainsi pour remplir la condition 4. il suffit d'avoir $2-(2g+1)\alpha \leqslant 1$ *i.e.* $\alpha \geqslant \dfrac{1}{2g+1}$ et $2^g-1-(2g+1)\beta \leqslant 0$ *i.e.* $\beta \geqslant \dfrac{2^g-1}{2g+1}$.

On constate que prendre $\alpha = \dfrac{1}{2g+1}$ et $\beta = \dfrac{2^g-1}{2g+1}$ convient aussi pour vérifier la condition 3. pourvu que l'on prenne ε suffisamment petit.

On a en effet alors pour tout $\delta > 0$:

$$c_2(\mathcal{G}_n) p_n^{2(g+1)} = o(n^{2+\delta-\frac{2(g+1)}{2g+1}+2(g+1)\varepsilon}) = o(n^{1-\frac{1}{2g+1}+2(g+1)\varepsilon+\delta}).$$

et donc dès que $2(g+1)\varepsilon+\delta \leqslant \dfrac{1}{2g+1}$ (on peut trouver un δ convenable dès que $\varepsilon < \dfrac{1}{2(g+1)(2g+1)}$) on a :

$$c_2(\mathcal{G}_n) p_n^{2(g+1)} = o(n).$$

.

On peut donc enfin démontrer le :

Théorème 3.3.1. *Soit $g \geqslant 1$, il existe une constante C_g telle que l'on a pour tout $n \geqslant 1$:*

$$\|\square_n\|_g \geqslant C_g n^{\alpha_g} \ln(n)^{\gamma_g}$$

avec $\alpha_g = \frac{2g}{2g+1}$ et $\gamma_g = \frac{2-2^g}{2g+1}$.

Démonstration. Bien sur il est suffisant de vérifier la même inégalité avec $\|\square_n\|_g^*$ plutôt que $\|\square_n\|$

En posant pour $n \geqslant 1$: $p_n = n^{-\frac{1}{2g+1}+\frac{1}{4(g+1)(2g+1)}} \ln(n)^{-\frac{2^g-1}{2g+1}}$ et $t_n = n^{\frac{1}{4(g+1)(2g+1)}}$, on a bien *(et on rappelle que $|V_n| = n$)* que :

(1) $np_n \xrightarrow[n\to+\infty]{} +\infty$

(2) $t_n \xrightarrow[n\to+\infty]{} +\infty$

(3) $c_2(\mathcal{G}_n) p_n^{2(g+1)} = o(n)$

(4) et $|\mathcal{E}_n| \left(\dfrac{p_n}{t_n}\right)^{2g+1} = O(n)$.

Ainsi, en appliquant le théorème 3.1.2, on trouve une constante $C > 0$ tel que pour n suffisamment grand :

$$\|\square_n\|_g^* = I(\mathcal{G}_n) \geqslant Cn \left(n^{-\frac{1}{2g+1}} \ln(n)^{-\frac{2^g-1}{2g+1}}\right) \ln^{n^{\frac{1}{2(2g+1)}}} \frac{1}{2g+1} = \left(\frac{1}{2(2g+1)}\right)^{\frac{1}{2g+1}} Cn^{\frac{2g}{2g+1}} \ln(n)^{\frac{2-2^g}{2g+1}}.$$

D'où le théorème 3.3.1. (Bien sur une fois qu'on a l'inégalité pour n suffisamment grand on peut la rendre vraie pour tout n en adaptant la constante.) □

On constate avec satisfaction que $\alpha_g \xrightarrow[g\to+\infty]{} 1$ même si $\gamma_g \xrightarrow[g\to+\infty]{} -\infty$. Et, naturellement, le cas $g = 1$ redonne le résultat de [11].

Références

[1] *773| Erdös Problems*. URL : https://www.erdosproblems.com/773 (visité le 26/06/2026).

[2] P. BERNAYS. *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht quadratischen Discriminante*. Universitäts-Buehdruckerei, 1912. URL : https://books.google.fr/books?id=GFFLAAAAMAAJ.

[3] N. ALON & P. ERDÖS. "An Application of Graph Theory to Additive Number Theory". In : *European Journal of Combinatorics* 6 (1985), p. 201-203. DOI : https://doi.org/10.1016/S0195-6698(85)80027-5.

[4] V. BLOMER & A. GRANVILLE. "Estimates for representation numbers of quadratic forms". In : *Duke Mathematical Journal* 135 (2006), p. 261-302. DOI : https://doi.org/10.1215/S0012-7094-06-13522-6.

[5] B. HANSON. "Additive correlation and the inverse problem for the large sieve". In : *Mathematical Proceedings of the Cambridge Philosophical Society* 168.2 (2018), 211–217. ISSN : 1469-8064. DOI : 10.1017/s0305004118000518. URL : http://dx.doi.org/10.1017/S0305004118000518.

[6] J. SAHOO & A. VATWANI M. RAM MURTY. "A simple proof of the Wiener–Ikehara Tauberian Theorem". In : *Expositiones Mathematicae* 42.3 (2024), p. 125570. ISSN : 0723-0869. DOI : https://doi.org/10.1016/j.exmath.2024.125570. URL : https://www.sciencedirect.com/science/article/pii/S0723086924000379.

[7] *RMS 135-4 (Juillet–Août–Septembre 2025) : Revue de la filière Mathématiques - 135*. Revue de la filière Mathématiques. rue des écoles, 2026. ISBN : 9782379190698. URL : https://books.google.fr/books?id=dOTEEQAAQBAJ.

[8] R. A. DUKE & H. LEFMANN & V. RÖDL. "On Uncrowded Hypergraphs". In : *Random Structures & Algorithms* 6 (1995), p. 209-212. DOI : https://doi.org/10.1002/rsa.3240060208.

[9] S. SIDON. "Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen". In : *Mathematische Annalen* 106 (1932), p. 536-539. DOI : https://doi.org/10.1007/BF01455900.

[10] J. KOMLÓS & M. SULYOK & E. SZEMERÉDI. "Linear Problems in Combinatorial Number Theory". In : *Acta Mathematica Academiae Scientarum Hungaricae* 26 (1975), p. 113-121. DOI : https://doi.org/10.1007/BF01895954.

[11] H. LEFMANN & T. THIELE. "Points sets with distinct distances". In : *Combinatorica* 15 (1995), p. 379-408. DOI : https://doi.org/10.1007/BF01299744.

[12] E. CROOT & J. MAO & C. H. YIP. "A COMBINATORIAL LARGE SIEVE FOR SIDON SETS, DISTANCES, AND NORM FORMS". In : (2026). arXiv : 2603.14654 [math.NT]. URL : https://arxiv.org/abs/2603.14654.

4. Annexes

4.1. Orthogonalité des caractères sur un groupe abélien fini

On note G un groupe abélien fini (gaf) et $\widehat{G} = \hom(G, \mathbb{C}^*)$ son dual, dont on va appeler les éléments *caractères* de G. Il est claire que ce dernier forme un groupe pour la multiplication. Notre but sera, dans un premier temps, de montrer que $G \cong \widehat{G}$, puis de montrer que l'ensemble des caractères sur G est un réalité une base orthonormale de $\mathbb{C}^G$ pour un produit scalaire hermitien qu'on précisera.

Pour montrer que $G \cong \widehat{G}$, il faut d'abord traiter le cas où G est cyclique, qui est assez facile. En effet, soit $\chi \in \widehat{G}$, et $x \in G$ qui l'engendre. Alors χ est uniquement défini à partir de x, car tout élément de G est une puissance de x. De plus, en notant $n = |G|$, $\chi(x^n) = \chi(x)^n = 1$ par le théorème de Lagrange, donc $\chi(x) \in \mathbb{U}_n$. On a alors n choix distincts pour $\chi(x)$. On en déduit que le morphisme :

$$\phi : \begin{cases} \widehat{G} \to \mathbb{U}_n \\ \chi \mapsto \chi(x) \end{cases}$$

est en réalité un isomorphisme de groupes. Puisque $\mathbb{U}_n \cong G$ on en déduit par transitivité que $\widehat{G} \cong G$.

On montre ensuite le lemme suivant pour conclure avec le théorème de structure des gaf :

Proposition 4.1.1. *Soit G_1, G_2 deux gaf. Alors $\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$*

Démonstration. Pour tout $(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2$, on note $\chi_1 \otimes \chi_2 : G_1 \times G_2 \to \mathbb{C}^*$ l'application :

$$(\chi_1 \otimes \chi_2)(g_1, g_2) = \chi_1(g_1)\chi_2(g_2).$$

Alors $\psi : \widehat{G}_1 \times \widehat{G}_2 \to \widehat{G_1 \times G_2}$, $(\chi_1, \chi_2) \mapsto \chi_1 \otimes \chi_2$ est un isomorphisme de groupes. En effet :

$$\ker \psi = \{(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2,\ \forall (g_1, g_2) \in G_1 \times G_2,\ \chi_1(g_1)\chi_2(g_2) = 1\}.$$

On en tire que si $(\chi_1, \chi_2) \in \ker \psi$ alors en prenant $g_2 = e_2$ élément neutre de G_2, pour tout $g_1 \in G_1$, $\chi_1(g_1) = 1$. Donc χ_1 est le morphisme triviale et de même χ_2 aussi. Donc ψ est injectif. Pour la surjectivité, On prend $\chi \in \widehat{G_1 \times G_2}$ et on pose $\chi_1(g_1) = \chi(g_1, e_2)$ pour tout $g_1 \in G_1$ et $\chi_2 = \chi(e_1, g_2)$ pour tout $g_2 \in G_2$. Alors on a bien $\psi(\chi) = \chi_1 \otimes \chi_2$. □

On va maintenant admettre la version faible du théorème de structure des groupes abéliens finis qui s'énonce de la manière suivante :

Théorème 4.1.1. *Soit G un gaf. Alors il existe $r \in \mathbb{N}^*$ et $d_1, \dots, d_r$ des entiers naturels tels que $d_1 | d_2 | \dots | d_r$ et :*

$$G \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{d_r\mathbb{Z}}.$$

En admettant ceci, on peut conclure avec la proposition suivante, qui est fondamentale à la théorie de l'analyse harmonique sur les gaf :

Proposition 4.1.2. *Soit G un gaf. Alors $G \cong \widehat{G}$. En particulier, $|G| = |\widehat{G}|$.*

Démonstration. On applique la proposition 4.1.1 et le théorème 4.1.1 :

$$\widehat{G} \cong \widehat{{}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{d_r\mathbb{Z}}} \cong \widehat{{}^{\mathbb{Z}}/_{d_1\mathbb{Z}}} \times \cdots \times \widehat{{}^{\mathbb{Z}}/_{d_r\mathbb{Z}}} \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{d_r\mathbb{Z}} \cong G.$$

D'où le résultat. □

On va donc montrer que les éléments de $\widehat{G}$ forment une base de $\mathbb{C}^G$ dans un sens bien précis. Pour montrer que les caractères forment une famille libre, on veut définir un produit scalaire sur $\widehat{G}$. Faisons d'abord la remarque suivante :

Proposition 4.1.3. *Soit χ un caractère non trivial d'un gaf G. Alors :*

$$\sum_{g\in G}\chi(g)=0.$$

Démonstration. Il suffit de remarquer que puisque χ est non trivial, on dispose de $h\in G$ tel que $\chi(h)\neq 1$. De ce fait, puisque $g\mapsto hg$ définit une bijection :

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

D'où le résultat. □

On est alors amené à définir un produit scalaire hermitien sur l'espace $\mathbb{C}^G$ de la façon suivante :

Définition 4.1.1. *On définit $\langle\cdot,\cdot\rangle$ le produit scalaire hermitien suivant sur $\mathbb{C}^G$:*

$$\forall(f,h)\in\mathbb{C}^G,\ \langle f,h\rangle=\frac{1}{|G|}\sum_{g\in G}\overline{f(g)}h(g).$$

Pour ce produit scalaire, on a alors le résultat suivant :

Proposition 4.1.4. *Les éléments de $\widehat{G}$ forment une famille orthogonale pour $\langle\cdot,\cdot\rangle$. En particulier, la famille est libre dans $\mathbb{C}^G$.*

Démonstration. Si $\chi\neq\chi'$ sont deux caractères de G alors $\overline{\chi}\chi'=\chi^{-1}\chi'\in\widehat{G}$ car tout caractère est à valeurs dans $\mathbb{U}$. Ainsi, en notant $\phi=\overline{\chi}\chi'$, $\phi\in\widehat{G}$ et est non triviale. On en tire :

$$\langle\chi,\chi'\rangle=\frac{1}{|G|}\sum_{g\in G}\phi(g)=0.$$

D'après la 4.1.3. Un calcul direct nous fournit :

$$\langle\chi,\chi\rangle=\frac{1}{|G|}\sum_{g\in G}|\chi(g)|^2=\frac{1}{|G|}\sum_{g\in G}1=1.$$

D'où le résultat. □

On va alors montrer que le résultat qu'on voulait est vrai, à savoir que $\widehat{G}$ forme une base de $\mathbb{C}^G$.

Proposition 4.1.5. *$\widehat{G}$ est une base de $\mathbb{C}^G$.*

Démonstration. $\dim(\mathbb{C}^G)=|G|=|\widehat{G}|$ d'après la 4.1.2, et puisque la famille $(\mathbb{1}_g)_{g\in G}$ est une base de $\mathbb{C}^G$ de cardinal $|G|$. Or, les caractères forment une famille libre de $\mathbb{C}^G$ et il y en a $|\widehat{G}|$, d'où le résultat. □

On a donc la décomposition qu'on cherchait. En effet, pour tout $f\in\mathbb{C}^G$, on a alors :

$$f=\sum_{\chi\in\widehat{G}}\langle\chi,f\rangle\chi.$$

Fait qu'il fallait absolument mobiliser pour les démonstrations qu'on vient de faire. Il nous reste seulement à montrer le théorème de structure des groupes abéliens finis, qu'on a admis pour achever cette démonstration. Montrons le :

Démonstration. (du théorème 4.1.1 :) On commence avec le lemme de prolongement des caractères sur un gaf.

Lemme : Soit G un gaf et $H < G$. Alors tout caractère de H se prolonge en un caractère de G.

Preuve : Soit χ un caractère de $H < G$. Si $H = G$ il n'y a rien à dire. Sinon, prenons $x \in G \backslash H$ et notons $K = \langle H, x\rangle = \{x^k h,\ h \in H\}$. On va prolonger χ en un caractère de K et en itérant le processus un nombre fini de fois, on finira par avoir prolongé χ sur G tout en entier.

Un caractère χ' prolongeant χ sur K est défini uniquement par $\chi'(x)$ car il coïncide avec χ sur H. La difficulté repose sur le fait que la définition de χ' doit absolument être cohérente avec celle de χ, ce qui nous conduit à considérer $\{k \in \mathbb{Z},\ x^k \in H\}$. C'est un sous groupe non trivial de $\mathbb{Z}$ car $x^{|G|} \in H$ d'après Lagrange et est donc de la forme $m\mathbb{Z}$ avec $m \geqslant 2$. Posons $\gamma = \chi(x^m)$ et on choisit un $\alpha \in \mathbb{U}$ tel que $\alpha^m = \gamma$. On définit alors χ' pour tout $h \in H$ et $k \in \mathbb{Z}$:

$$\chi'(x^k h) = \alpha^k \chi(h).$$

On vérifie que cela définit bien un caractère compatible avec la définition de χ. En faisant une descente finie sur le cardinal de G on a le résultat. □

On va vouloir montrer le théorème $4.1.1$ par récurrence sur le cardinal du gaf. Pour ce faire, il faut commencer quelque part ; montrons donc le lemme suivant :

Lemme : Soit G un gaf. Alors il existe $x \in G$ tel que l'ordre de x soit $\exp(G)$.

Démonstration. Pour tout $G \in G$, on note $\omega(g)$ l'ordre de g. Montrons d'abord que si u, v sont deux éléments de G tels que $\omega(u) \wedge \omega(v) = 1$, alors $\omega(uv) = \omega(u)\omega(v)$. En effet, on considère $g \in \langle u\rangle \cap \langle v\rangle$. Alors $\langle g\rangle$ est un sous groupe de $\langle u\rangle$ et $\langle v\rangle$ donc l'ordre de g divise à la fois celui de u et v, et donc leur PGCD. On en tire que $g = e$, et donc pour tout $(k, p) \in \mathbb{Z}^2$, $u^k \neq v^p$ sauf si $u^k = v^p = e$.

On a alors $(uv)^k = u^k v^k = e$ si et seulement si $u^k = v^{-k}$, ce qui est possible si et seulement si $u^k = v^{-k} = e$, donc $\omega(u)|\omega(uv)$ et $\omega(v)|\omega(uv)$. Les deux étant premiers entre eux, on en tire que $\omega(u)\omega(v)|\omega(uv)$. Or, puisque $(uv)^{\omega(u)\omega(v)} = 1$ on a $\omega(uv)|\omega(u)\omega(v)$, d'où le résultat. □

Montrons désormais le lemme. Soit $x \in G$ d'ordre maximal. Il faut montrer que l'ordre de tout $y \in G$ divise celui de x. Fixons $y \in G$ et notons $n = \omega(x)$ et $m = \omega(y)$. Il s'agit de montrer que pour tout nombre premier p, $v_p(m) \leqslant v_p(n)$. Ainsi, pour p fixé, on note $m = p^a r$ et $n = p^b s$ avec $p \wedge r = p \wedge s = 1$. Alors x^{p^b} est d'ordre s et y^r est d'ordre p^a. Avec ce qu'on vient de montrer, on a alors $\omega(x^{p^b} y^r) = p^a s \leqslant p^b s$ par hypothèse de la maximalité de l'ordre de x. Donc $a \leqslant b$, d'où le résultat. □

Nous sommes désormais armés pour montrer le théorème 4.1.1.

Soit G un gaf. Alors il existe $r \in \mathbb{N}^*$ et $d_1, \ldots, d_r$ des entiers naturels tel que $d_1|d_2| \ldots |d_r$ et :

$$G \cong {}^{\mathbb{Z}}\!/_{d_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{d_r\mathbb{Z}}.$$

Démonstration. On raisonne par récurrence sur la taille de G. Si $|G| = 1$ ou $|G| = 2$ c'est évident. Supposons alors que la propriété est vérifiée pour tout groupe de taille $1, 2, \ldots, n-1$ et prenons G un groupe de cardinal n, $n \geqslant 3$. Alors il existe $y \in G$ tel que son ordre soit l'exposant de G. On note $\omega(y) = m$ et H le groupe engendré par y. Soit $\tilde{\chi}$ un caractère bijectif de H sur $\mathbb{U}_m$ que l'on prolonge en un caractère χ de G. On va montrer que :

$$G \cong H \times \ker \chi.$$

On pose donc $\phi : H \times \ker(\chi) \to G$ qui à (h, k) associe hk. Alors ϕ est injectif. En effet, si $hk = e$ alors $k \in H \cap \ker(\chi) = \{e\}$ car on a supposé $\chi_{|H}$ bijectif. Donc $h = k = e$. χ est injectif.

Pour montrer que χ est surjectif, on remarque que puisque l'ordre de tout élément de G divise m χ est à valeurs dans $\mathbb{U}_m$. Or, puisque $\chi_{|H}$ est un isomorphisme, on en tire que les $(h \ker \chi)_{h \in H}$ forment une partition de G par le premier théorème d'isomorphisme, d'où le résultat.

Donc $|\ker(\chi)| = |G|/|H| < n$, donc il existe $r \geqslant 2$ et $d_1| \ldots |d_{r-1}$ tel que :

$$G \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{d_{r-1}\mathbb{Z}} \times H \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{d_{r-1}\mathbb{Z}} \times {}^{\mathbb{Z}}/_{m\mathbb{Z}}.$$

Par cette isomorphisme, on peut exhiber un élément $g \in G$ pour lequel l'élément correspondant dans le produit ci-dessus soit $(0, \ldots, 1, 0)$ donc d'ordre d_{r-1}, donc $d_{r-1}|m$, d'où le résultat. □

4.2. **Premier résultat de minoration**

[10] montre que pour toute une classe de problèmes de combinatoire additive consistant à chercher, dans un ensemble donné, un grand sous ensemble respectant certaines contraintes (classe à laquelle appartient la recherche de grands ensemble de Sidon par exemple), l'intervalle $\{1, \ldots, n\}$ est l'ensemble de taille n dans lequel la solution est aussi petite que possible, à un facteur constant près dépendant du problème.

Le problème étant que le facteur constant près est à priori très mauvais.

En sélectionnant les points pertinents de la preuve de [10], que l'on redémontre et améliore, et en gardant en tête que l'on travaille spécifiquement sur la comparaison entre $\|\square_n\|_g$ et $\|\{1, \ldots, n\}\|_g$, on arrive à obtenir dans le cas qui nous intéresse $\frac{1}{4}$ comme constante.

Autrement dit, on montre ici que $\|\square_n\|_g$ est minorée par une expression asymptotiquement équivalente à $\|\{1, \ldots, n\}\|$.

Lemme 4.2.1. *Si $q \in \mathbb{N}^*$ et pour $1 \leqslant i \leqslant n$ on dispose d'un entier a_i dont on écrit la division euclidienne par q : $a_i = h_i q + r_i$ et que l'on suppose toujours avoir $r_i < \frac{q}{2}$ alors $\|\{a_1, \ldots, a_n\}\|_g \geqslant \|\{r_1, \ldots, r_n\}\|_g$.*

Démonstration. Remarquons déjà, pour i, j, k, l que si $a_i + a_j = a_k + a_l$ alors $r_i + r_j = r_k + r_l$. En effet on a alors :

$$\begin{aligned} r_i + r_j &= a_i + a_j - h_i q - h_j q \\ &= a_k + a_l - h_i q - h_j q \\ &= q(h_k + h_l - h_i - h_j) + r_k + r_l. \end{aligned}$$

donc $r_i + r_j - r_k - r_l = q(h_k + h_l - h_i - h_j)$. Or, $|r_i + r_j - r_k - r_l| < q$ et $q(h_k + h_l - h_i - h_j) \in q\mathbb{Z}$.

Donc $r_i + r_j = r_k + r_l$.

On se donne alors $i_1, \ldots, i_m$ tels que les $r_{i_1}, \ldots, r_{i_m}$ sont 2 à 2 distincts et tels que $\{r_{i_1}, \ldots, r_{i_m}\}$ est un sous ensemble $B_2[g]$ de $\{r_1, \ldots, r_n\}$ de cardinal maximal.

On propose alors que $\{a_{i_1}, \ldots, a_{i_m}\}$ est un ensemble $B_2[g]$, justifiant donc l'inégalité annoncée.

En effet, si $k, l \in \{1, \ldots, m\}$:

$$|\{\{k', l'\}\ ;\ a_{i_{k'}} + a_{i_{l'}} = a_{i_k} + a_{i_l}\}| \leqslant |\{\{k', l'\}\ ;\ r_{i_{k'}} + r_{i_{l'}} = r_{i_k} + r_{i_l}\}| \leqslant g.$$ □

Pour tout entier naturel $n \in \mathbb{N}$ on note q_n le plus petit nombre premier strictement supérieur à n.

Par le critère de Bertrand on a $q_n \leqslant 2n$ mais asymptotiquement on sait même que q_n est équivalent à n et même par exemple que $q_n = n + O(n^{0,525})$.

Lemme 4.2.2. *Pour $n \in \mathbb{N}^*$ il existe au moins $n/2$ entiers $0 < k_1 < \cdots < k_m \leqslant \dfrac{q_{2n} - 1}{2}$ tels que $\|\square_n\|_g \geqslant \|\{k_1, \ldots, k_m\}\|_g$.*

Démonstration. En effet, remarquons déjà que si $0 \leqslant b \leqslant a \leqslant n$ on a $a^2 - b^2 = (a - b)(a + b)$, ces deux facteurs étant plus petits que $2n$, $a^2 - b^2$ n'est pas divisible par q_{2n} ; les résidus des $n + 1$ *(en incluant 0)* premiers carrés modulos q_{2n} sont 2 à 2 distincts.

On remarque de plus que :

$$\sum_{1 \leqslant k \leqslant n} \sum_{t \in \mathbb{F}_{q_{2n}}} \mathbb{1}\left(t\overline{k^2} \in \left\{\overline{1}, \ldots, \overline{\frac{q_{2n} - 1}{2}}\right\}\right) = n\frac{q_{2n} - 1}{2}$$

et donc il existe un t tel qu'au moins $\frac{n}{2}$ des n premiers carrés aient un résidu modulo q_{2n} strictement inférieur à $2n$. Notons ceux-ci $a_1, \ldots, a_m$, on conclut par le lemme précédent en prenant les résidus modulo q de $ta_1, \ldots, ta_m$.

□

Lemme 4.2.3. *Si n est un entier naturel non nul et $A \subseteq \{1, \ldots, n\}$ on a* $\|A\| \geqslant \dfrac{|A|}{2n-1}\|\{1, \ldots, n\}\|_g$

Démonstration. Prenons B une partie $B_2[g]$ de $\{1, \ldots, n\}$ de cardinal maximal, on remarque que :

$$\sum_{-n<i<n} \sum_{a \in A} \mathbb{1}(a \in B + i) = |A| \times |B| = |A| \times \|\{1, \ldots, n\}\|_g$$

Il existe donc un i tel qu'au moins $|A|\|\{1, \ldots, n\}\|_g/(2n-1)$ des éléments de A sont dans $(B+i) \cap \mathbb{N}^*$ qui est un ensemble $B_2[g]$. Ces éléments constituent donc une partie $B_2[g]$ de A d'où l'inégalité annoncée.

□

Proposition 4.2.1. *Pour $n \in \mathbb{N}^*$, $\|\square_n\|_g \geqslant \frac{1}{2q_{2n}}\|\{1, \ldots, n\}\|_g$.*

Démonstration. On se donne $A = \{k_1, \ldots k_m\}$ tel que donné par le lemme 4.2.2 puis on applique sur A le lemme 4.2.3 (avec A et $\frac{q_{2n}-1}{2}$) pour obtenir :

$$\|\square_n\|_g \geqslant \|A\| \geqslant \frac{|A|}{q_{2n}-1} \left\| \left\{1, \ldots, \frac{q_{2n}-1}{2}\right\} \right\|_g \geqslant \frac{n}{2(q_{2n}-1)}\|\{1, \ldots, n\}\|_g \geqslant \frac{n}{2q_{2n}}\|\{1, \ldots, n\}\|_g$$

□

En utilisant le développement asymptotique, mentionné ci-dessus, du plus petit premier succédant un entier on obtient :

$$\|\square_n\|_g \geqslant \frac{1}{4}\|\{1, \ldots, n\}\|_g \left(1 + O\left(\frac{1}{n^{0,475}}\right)\right).$$

4.3. $D(n) = o(n^\varepsilon)$ pour tout $\varepsilon > 0$

Il s'agit de montrer ce résultat pour établir une minoration de la section 3.

Soit $\varepsilon > 0$. On constate à l'aide de la formule de décomposition en facteurs premiers que pour tout $n \geqslant 2$:

$$n = \prod_{p|n} p^{v_p(n)}.$$

On peut obtenir la formule explicite suivante de d_n :

$$D(n) = \prod_{p|n} (v_p(n) + 1).$$

Avec $v_p(n)$ la valuation p-adique de n. Ainsi :

$$\frac{D(n)}{n^\varepsilon} = \prod_{p|n} \frac{v_p(n)+1}{p^{\varepsilon v_p(n)}}.$$

Où $v_p(n)$ désigne la valuation p-adique et le produit parcourt les nombres premiers divisant n. On est donc amené à étudier les fonctions $f_p : \mathbb{R} \to \mathbb{R}$:

$$f_p(x) = \frac{x+1}{p^{x\varepsilon}}.$$

Pour tout $p \in \mathcal{P}$, $f_p \in \mathcal{C}^\infty(\mathbb{R})$ et de dérivée :

$$f_p'(x) = \frac{p^{x\varepsilon} - (x+1)\varepsilon \ln(p) p^{x\varepsilon}}{p^{2\varepsilon x}}.$$

On vérifie donc que f_p est croissante puis décroissante sur $\mathbb{R}$ et atteint son maximum en $x = 1/(\varepsilon \ln(p)) - 1$. Or, puisque $\mathcal{P}$ est infini, il existe un certain $p_\varepsilon \in \mathcal{P}$ tel que pour tout $p \geqslant p_\varepsilon$ premier, $\sup_{x \geqslant 0} f_p(x) = f_p(0) = 1$ puisque $1/(\varepsilon \ln(p)) - 1 \to -1$ lorsque $p \to \infty$. Ainsi :

$$0 \leqslant \frac{D(n)}{n^\varepsilon} \leqslant \prod_{p \leqslant p_\varepsilon} f_p\left(\frac{1}{\varepsilon \ln(p)} - 1\right) := M_\varepsilon.$$

D'où le résultat, car $D(n) = O(n^\varepsilon)$ pour tout $\varepsilon > 0$ implique que $D(n) = o(n^\varepsilon)$ pour tout $\varepsilon > 0$.