1 Objectif

On note $G = Sl_2(\mathbb{F}_p)$, $\pi : Sl_2(\mathbb{Z}) \to G$.

Théorème 1 (Bourgain-Gamburd, à paraître à *Annals of Math.*). *Soit S un sous-ensemble fini, symétrique, de $Sl_2(\mathbb{Z})$, qui engendre un sous-groupe libre, non cyclique. Alors, pour p assez grand, $\pi(S)$ engendre G, et les graphes de Cayley* $\mathrm{Cay}(G, \pi(S))$ *constituent un expanseur.*

2 Schéma de la preuve

Il s'agit d'une réduction au théorème d'Helfgott.

1. Il suffit de majorer la norme ℓ^2 de la marche en temps logarithmique.
2. Un argument très court dû à Margulis permet de minorer le tour de taille du sous-groupe engendré par $\pi(S)$. Combiné avec la classification des sous-groupes propres de G (ils ont automatiquement des relations courtes), cela entraîne que $\pi(S)$ engendre G. On donne ensuite une version quantitative de ces deux énoncés : la marche aléatoire visite modérément chaque sommet, et même, visite peu un sous-groupe propre.
3. La combinatoire additive montre qu'une mesure de norme ℓ^∞ trop petite et de norme ℓ^2 trop grande est concentrée sur un translaté d'un ensemble de faible triplement.
4. Le théorème d'Helfgott affirme qu'un tel ensemble est contenu dans un sous-groupe propre, contradiction.

3 Rôle de la norme ℓ^2 de la marche

On note $2k = |S|$, $\mu = \frac{1}{2k} \sum_{s \in S} \delta_{\pi(s)}$, $\mu^{(\ell)} = \mu \star \mu \star \cdots \star \mu$ ℓ fois.

Lemme 2 *Pour prouver le théorème 1, il suffit de trouver des constantes $\sigma > 0$ et $C < +\infty$ telles que, pour p assez grand et pour $\ell = C \log_{2k} p$, $\| \mu^{(\ell)} \|_2 < p^{-1-\sigma}$.*

Preuve. Soit A la matrice d'incidence du graphe de Cayley $\mathrm{Cay}(G, \pi(S))$, $2k = \lambda_0 > \lambda_1 \geq \cdots$ ses valeurs propres. Alors les colonnes de la matrice $(\frac{1}{2k} A)^\ell$ sont des permutations du vecteur $\mu^{(\ell)}$, d'où

$$\mathrm{mult}(\lambda_1) \lambda_1^{2\ell} \leq \mathrm{trace}(A^{2\ell}) = |G| (2k)^{2\ell} \| \mu^{(\ell)} \|_2^2 .$$

D'après Frobenius, $\mathrm{mult}(\lambda_1) \geq \frac{p-1}{2}$. Il vient

$$\begin{aligned} \lambda_1 &\leq 2k \left(\frac{2(p^3 - p)}{p-1} \| \mu^{(\ell)} \|_2^2 \right)^{1/2\ell} \\ &< 2k \, 3^{1/2\ell} p^{-\sigma/2C \log p} = 2k (2k)^{-\sigma/2C} 3^{1/2\ell} < 2k, \end{aligned}$$

pour p assez grand.

Remarque. Remarquer le rôle joué par le théorème de Frobenius. Il permet de gagner un facteur $1/2$. Sans cela, il faudrait montrer que $\| \mu^{(\ell)} \|_2 < p^{-3/2}$. Or on arrive, dans la suite, à majorer $\| \mu^{(\ell)} \|_2$ par $p^{-\theta}$ pour tout $\theta < 3/2$, mais pas mieux.

4 Tour de taille

On appelle *rayon d'injectivité* le plus grand entier n tel que deux points du graphe à distance $< n$ soient reliés par un unique chemin minimisant (le tour de taille vaut alors $2n$ ou $2n + 1$).

Lemme 3 (Margulis). *On utilise la norme d'opérateur sur les matrices. Soit* $\alpha = \max\{\| s \| \mid s \in S\}$. *Le rayon d'injectivité du graphe de Cayley* $\mathrm{Cay}(\pi(\langle S\rangle), \pi(S))$ *est au moins égal à* $i = \lfloor \log_\alpha(p/2) \rfloor$.

Preuve. Si n est le rayon d'injectivité, alors il existe deux mots réduits distincts w et w', de même longueur n, tels que $\pi(w) = \pi(w')$. Alors $w \neq w'$ dans le groupe libre $\langle S\rangle$, donc dans $Sl_2(\mathbb{Z})$. Chaque coefficient de $w - w'$ est divisible par p, et l'un d'entre eux est non nul, donc $\| w - w' \|^2 \geq p^2$. L'un des deux, soit w, satisfait $\| w \| \geq p/2$. Or $w = s_1 s_2 \cdots s_n$ entraîne $\| w \| \leq \alpha^n$, soit $n \geq \log_\alpha(p/2)$.

5 Génération

Lemme 4 (Gamburd). *Pour* p *assez grand,* $\pi(S)$ *engendre* G.

Preuve. Sinon, $\pi(S)$ engendre un sous-groupe propre G_0. D'après Dickson, les sous-groupes de $Sl_2(\mathbb{F}_p)$ sont ou bien de 60-torsion, ou bien métabéliens. La 60-torsion entraîne $i \leq 30$, contredisant le lemme précédent. Sinon, si a, b, c, d sont 4 éléments de $\langle S\rangle$ engendrant un sous-groupe libre, la relation

$$1 = [[a,b],[c,d]] = aba^{-1}b^{-1}cdc^{-1}d^{-1}bab^{-1}a^{-1}dcd^{-1}c^{-1}$$

entraîne $i \leq 8 \max\{|a|, |b|, |c|, |d|\}$.

6 Norme ℓ^∞ de la marche

Voici une conséquence quantitative de la minoration du rayon d'injectivité.

Lemme 5 *Il existe une constante* $\gamma > 0$ *telle que, pour tout* $g \in G$, *pour* $\ell \geq i$, $\mu^{(\ell)}(g) < p^{-\gamma}$.

Preuve. On écrit $\mu^{(\ell)} = \mu^{(i)} \star \mu^{(\ell-i)}$, d'où

$$\| \mu^{(\ell)} \|_\infty \leq \| \mu^{(i)} \|_\infty \| \mu^{(\ell-i)} \|_1 = \| \mu^{(i)} \|_\infty .$$

$\mu^{(i)}(g)$ est la probabilité d'arriver en g en partant de 1 en i pas. Or dans la boule de centre 1 et de rayon i, le graphe est un arbre régulier de valence $2k$, donc on peut utiliser des résultats classiques (Kesten 1959),

$$\mu^{(i)}(g) \leq \sqrt{\mu^{(2i)}(1)} \leq (\frac{\sqrt{2k-1}}{k})^i = (\frac{p}{2})^{\log_\alpha(\sqrt{2k-1}/k)}.$$

7 La marche visite peu les sous-groupes de G

En affinant l'argument qui prouve que $\pi(S)$ engendre G, on montre que la marche, non seulement n'est pas contenue dans un sous-groupe propre, mais en plus charge peu les sous-groupes propres de G.

Lemme 6 *Il existe une constante* $\delta > 0$ *telle que, pour tout sous-groupe propre* $G_0 \subset G$, *pour tout* $\ell \geq i$, $\mu^{(\ell)}(G_0) < p^{-\delta}$.

Preuve. On se ramène au cas où $\ell = 2\ell_0 = i/16$.

$$\begin{aligned}\mu^{(\ell)}(G_0) &= \sum_{y\in G} \mu^{(\ell-\ell_0)}(y)\mu^{(\ell_0)}(y^{-1}G_0)\\ &\leq \max_{y\in G} \mu^{(\ell_0)}(y^{-1}G_0)\\ &= \mu^{(\ell_0)}(b^{-1}G_0)\mu^{(\ell_0)}(G_0 b).\end{aligned}$$

Or

$$\begin{aligned}\mu^{(2\ell_0)}(G_0) &= \sum_{y\in G} \mu^{(\ell_0)}(y)\mu^{(\ell_0)}(y^{-1}G_0)\\ &\geq \sum_{y\in G_0 b} \mu^{(\ell_0)}(y)\mu^{(\ell_0)}(y^{-1}G_0)\\ &= \mu^{(\ell_0)}(bG_0)^2,\end{aligned}$$

car $y \in G_0 b \Rightarrow y^{-1}G_0 = b^{-1}G_0$. Par conséquent, $\mu^{(\ell)}(G_0) \leq \sqrt{\mu^{(2\ell_0)}(G_0)}$, et il suffit donc de majorer $\mu^{(i/16)}(G_0)$.

Pour les sous-groupes d'ordre ≤ 60, l'inégalité $\mu^{(i/16)}(G_0) < p^{-\delta}$ résulte de la majoration de la norme ℓ^∞. Supposons donc G_0 métabélien. Soit

$$\mathcal{G}_0 = \{a \in \langle S\rangle \,|\, |a| \leq \frac{i}{16},\, \pi(a) \in G_0\}.$$

Si a, $b \in \langle S\rangle$ sont de longueurs $\leq i/16$, et si $\pi(a)$ et $\pi(b) \in [G_0, G_0]$, alors $\pi(a)$ et $\pi(b)$ commutent, donc a et b commutent, et appartiennent à un même sous-groupe cyclique Z du groupe libre $\langle S\rangle$. Considérons l'application

$$\mathrm{comm} : (a,b) \mapsto [a,b], \quad \mathcal{G}_0 \times \mathcal{G}_0 \to \{c \in Z \,|\, |c| \leq \frac{i}{4}\}.$$

Soit $c \in Z$, $|c| \leq i/4$ (il n'y a que Ci choix pour c, où C est une constante absolue). Soient a, b, $b' \in \langle S\rangle$, de longueurs $\leq i/16$, tels que $[a,b] = [a,b'] = c$. Alors $ba^{-1}b^{-1} = b'a^{-1}b'^{-1}$, donc $b'b^{-1}$ commute avec a, donc $b'b^{-1}$ et a appartiennent à un même sous-groupe cyclique. Autrement dit, étant donnés a et c, il n'y a que Ci choix pour un b tel que $\mathrm{comm}(a,b) = c$. Cela donne $|\mathrm{comm}^{-1}(c)| \leq Ci|\mathcal{G}_0|$, d'où $|\mathcal{G}_0|^2 \leq |\mathcal{G}_0|C^2 i^2$, soit $|\mathcal{G}_0| \leq C^2 i^2$. Par conséquent,

$$\begin{aligned}\mu^{(i/16)}(G_0) &= \tilde{\mu}^{(i/16)}(\mathcal{G}_0)\\ &\leq |\mathcal{G}_0| \parallel \tilde{\mu}^{(i/16)} \parallel_\infty\\ &\leq C^2 i^2 (\frac{\sqrt{2k-1}}{k})^{i/16}\\ &< p^{-\delta}.\end{aligned}$$

(On a noté $\tilde{\mu}$ la marche sur le groupe libre $\langle S\rangle$).

8 Réduction à une propriété de la convolution

Il nous faut un mécanisme qui, étant donnée une mesure ν sur G qui satisfait $\parallel \nu \parallel_\infty < p^{-\gamma}$ et pour tout sous-groupe propre $G_0 \subset G$, $\nu^{(2)}(G_0) < p^{-\delta}$, garantisse qu'une puissance ν^m de ν, m borné, satisfait $\parallel \nu^m \parallel_2 < p^{-1-\sigma}$. L'exposant m est nécessaire. Par exemple, pour $\ell \leq i/2$, grâce à la borne sur la rayon d'injectivité, on connaît exactement

$$\parallel \mu^\ell \parallel_2 = \sqrt{\mu^{2\ell}(1)} = \sqrt{\tilde{\mu}^{2\ell}(1)} \sim (\frac{\sqrt{2k-1}}{k})^\ell \ell^{-3/2},$$

qui est majoré par une puissance négative de p, mais sans doute pas par p^{-1}. C'est ce qui motive le lemme suivant.

Lemme 7 *Pour tous $\gamma > 0$, $\delta > 0$ et $\sigma < 1/2$, il existe $\epsilon(\gamma, \delta, \sigma) > 0$ tel que, pour toute mesure de probabilité ν sur G, si*
- $\| \nu \|_\infty < p^{-\gamma}$,
- *pour tout sous-groupe propre $G_0 \subset G$, $\nu^{(2)}(G_0) < p^{-\delta}$,*
- $\| \nu \|_2 > p^{-1-\sigma}$,

alors $\| \nu \star \nu \|_2 < p^{-\epsilon} \| \nu \|_2$.

Cela fait notre affaire. En effet, si $\mu^{(i)}$ ne satisfait pas aux hypothèses du lemme 7, on a gagné. Sinon,

$$\| \mu^{(i)} \|_2 \leq \| \mu_\infty^{(i)} \| |G|^{1/2} < p^{\frac{3}{2}-\gamma}.$$

On lui applique le lemme 7. On trouve que $\| \mu^{(2i)} \|_2$ a diminué d'un facteur $p^{-\epsilon}$. On recommence tant que $\mu^{(2^r i)}$ satisfait aux hypothèses du lemme 7. Au bout d'au plus $n = \frac{5}{2\epsilon}$ étapes, on trouve $\ell = 2^n i$ pour lequel la mesure $\mu^{(\ell)}$ satisfait $\| \mu^{(\ell)} \|_2 < p^{-1-\sigma}$.

9 Intervention de la combinatoire additive

On explique la preuve du lemme 7 dans le cas où $\nu = \frac{1}{|A|}\chi_A$ pour un sous-ensemble $A \subset G$. Dans ce cas, $\| \nu \|_2^2 = \frac{1}{|A|}$ et

$$\| \nu \star \nu \|_2^2 = \frac{1}{|A|^4} E(A, A),$$

où E est l'énergie définie comme suit.

Définition 8 (Tao). *Soient A, $B \subset G$. L'*énergie multiplicative *de A et B est*

$$\begin{aligned} E(A, B) &= \| \chi_A \star \chi_B \|_2^2 \\ &= |\{(a, b, c, d) \in A \times B \times A \times B \,|\, ab = cd\}|. \end{aligned}$$

Remarque 9 *Pour tous A, B,*

$$E(A, B) \leq |A||B| \min\{|A|, |B|\} \leq |A|^{3/2}|B|^{3/2}.$$

Lorsque G est commutatif et $A = B$, l'égalité a lieu si et seulement si A est un translaté d'un sous-groupe.

En effet,

$$\begin{aligned} \| \chi_A \star \chi_B \|_1 &= \| \chi_A \|_1 \| \chi_B \|_1 = |A||B|, \\ \| \chi_A \star \chi_B \|_\infty &\leq \min\{|A|, |B|\} \leq \sqrt{|A||B|}, \end{aligned}$$

d'où $\| \chi_A \star \chi_B \|_2^2 \leq |A||B| \min\{|A|, |B|\} \leq (|A||B|)^{3/2}$.

L'égalité $E(A, A) = |A|^3$ entraîne que pour tout $g \in A \cdot A$, le nombre de paires $(a, a') \in A \times A$ telles que $aa' = g$ est égal à $|A|$. Autrement dit, pour tout $a \in A$, $a^{-1}g \in A$. Dans le cas commutatif, on peut translater A (cela ne change pas l'énergie), supposer que A contient l'élément neutre, et alors A est un (translaté à gauche de) sous-groupe.

Autrement dit, au moins dans le cas commutatif, l'inégalité $\| \nu \star \nu \|_2 > p^{-\epsilon} \| \nu \|_2$, pour $\nu = \frac{1}{|A|}\chi_A$, soit $E(A, A) > p^{-2\epsilon}|A|^3$, exprime que A est proche d'être une classe à gauche d'un sous-groupe. Cet énoncé un peu vague peut être rendu précis et quantitatif. Dans le cas commutatif, c'est un théorème de Balog-Szemerédi-Gowers. Il est remarquable que ce théorème s'étende au cas général.

Définition 10 *Soit G un groupe. Soit $K > 1$. Un sous-ensemble $H \subset G$ est appelé* K-sous-groupe approché *s'il est symétrique ($H = H^{-1}$) et s'il existe un ensemble symétrique $X \subset H \cdot H$ tel que $|X| \leq K$ et $H \cdot H \subset X \cdot H$.*

Théorème 11 (Tao, à paraître à *Combinatorica*, Theorem 5.4). *Il existe une constante C telle que, pour tout $K > 1$, pour tout groupe G, si $E(A,B) \geq \frac{1}{K}|A|^{3/2}|B|^{3/2}$, alors il existe un CK^C-sous-groupe approché $H \subset G$ tel que $|H| \leq K^C|A|^{1/2}|B|^{1/2}$ et des éléments g et $g' \in G$ tels que $|A \cap (gH)| \geq \frac{1}{K^C}|A|$ et $|B \cap (g'H)| \geq \frac{1}{K^C}|B|$.*

La combinatoire additive ne s'arrête pas là, elle joue un rôle important dans le théorème d'Helfgott.

10 Intervention du triplement

Un K-sous-groupe approché satisfait à la condition de triplement

$$|H \cdot H \cdot H| \leq K^2|H|.$$

En effet, $H \cdot H \cdot H \subset X \cdot X \cdot H$.

Théorème 12 (Helfgott, à paraître à *Annals of Math.*). *Pour tout $\eta > 0$, il existe $c = c(\eta)$ et $\kappa = \kappa(\eta) > 0$ tels que si p est assez grand et si $H \subset G = Sl_2(\mathbb{F}_p)$ satisfait $|H| < p^{3-\eta}$ et*

$$|H \cdot H \cdot H| < c|H|^{1+\kappa},$$

alors H est contenu dans un sous-groupe propre de G.

On peut terminer la preuve du lemme 7 dans le cas simple. Supposons que $\nu = \frac{1}{|A|}\chi_A$ satisfasse aux hypothèses du lemme 7. Alors

- $\frac{1}{|A|} < p^{-\gamma}$, i.e. $|A| > p^{\gamma}$.
- pour tout sous-groupe propre G_0, $\frac{1}{|A|}|A \cap G_0| < p^{-\delta}$.
- $\frac{1}{\sqrt{|A|}} > p^{-1-\sigma}$, i.e. $|A| < p^{3-\eta}$, avec $\eta = 1 - 2\sigma$.

On raisonne par l'absurde. On suppose de plus que $E(A,A) > p^{-2\epsilon}|A|^3$. Le théorème de Tao fournit un $Cp^{C\epsilon}$-sous-groupe approché $H \subset G$ tel que $|H| \leq p^{C\epsilon}|A|$ et un élément $g \in G$ tel que $|A \cap (gH)| \geq p^{-C\epsilon}|A|$. H satisfait $|H \cdot H \cdot H| \leq C^2p^{2C\epsilon}|H|$. Si $\epsilon < \kappa\gamma/(\kappa + 2C\kappa + 4C)$, alors $|H \cdot H \cdot H| \leq c|H|^{1+\kappa}$. D'après le théorème d'Helfgott, H est contenu dans un sous-groupe propre G_0 de G. En particulier,

$$\nu(gG_0) \geq \nu(gH) = \frac{1}{|A|}|A \cap gH| > p^{-C\epsilon},$$

ce qui entraîne que $\nu^{(2)}(G_0) > p^{-2C\epsilon}$. Si $\epsilon < \delta/2C$, cela contredit l'hypothèse.

11 Extraction d'ensembles de grande énergie

Parmi les ensembles de niveau de ν, on va en sélectionner deux, notés A et B, tels que $E(A,B) > p^{-\epsilon}|A|^{3/2}|B|^{3/2}$. Dans les deux versions du texte de Bourgain et Gamburd, ce point comporte des erreurs de détails.

Lemme 13 *Soit G un groupe. Soit ν une mesure de probabilité sur G telle que $\| \nu \star \nu \|_2 > \frac{1}{K} \| \nu \|_2$. On pose $J = \lceil \log_2(4K|G|) \rceil$. Il existe A et $B \subset G$ tels que*

1. $E(A,B) > \dfrac{1}{2^4K^2J^4}|A|^{3/2}|B|^{3/2}$.

2. $|A| < 2^5 K^2 J^4 \parallel \nu \parallel_2^{-2}$.

3. *pour tout* $A' \subset A$, $\nu(A') > \dfrac{|A'|}{4KJ^2|A|}$.

Preuve. On se débarrasse d'abord des très petites valeurs de la fonction ν. On pose $A_- = \{g \in G \,|\, \nu(g) < 2^{-J}\}$ et $\nu_- = \chi_{A_-}\nu$, $\nu_+ = \nu - \nu_-$. On majore

$$\parallel \nu_- \parallel_1 \leq |G| 2^{-J} \leq \frac{1}{4K},$$

puis

$$\parallel \nu \star \nu_- \parallel_2 \leq \parallel \nu \parallel_2 \parallel \nu_- \parallel_1 \leq \frac{1}{4K} \parallel \nu \parallel_2,$$

$$\parallel \nu_+ \star \nu_- \parallel_2 \leq \parallel \nu_+ \parallel_2 \parallel \nu_- \parallel_1 \leq \frac{1}{4K} \parallel \nu \parallel_2,$$

d'où, comme

$$\nu \star \nu = \nu_+ \star \nu_+ + \nu_+ \star \nu_- + \nu_- \star \nu,$$

$$\parallel \nu \star \nu \parallel_2 \leq \parallel \nu_+ \star \nu_+ \parallel_2 + \frac{1}{2K} \parallel \nu \parallel_2 .$$

L'hypothèse $\parallel \nu \star \nu \parallel_2 > \frac{1}{K} \parallel \nu \parallel_2$ entraîne donc que $\parallel \nu_+ \star \nu_+ \parallel_2 > \frac{1}{2K} \parallel \nu \parallel_2 \geq \frac{1}{2K} \parallel \nu_+ \parallel_2$.

Pour simplifier encore la mesure, on pose $\tilde{\nu} = \sum_{j=1}^{J} 2^{-j} \chi_{A_j}$ où, pour $j = 1, \ldots, J$, $A_j = \{g \in G \,|\, 2^{-j} \leq \nu(g) < 2^{-j+1}\}$. Alors $\tilde{\nu} \leq \nu_+ \leq 2\tilde{\nu}$, donc $\parallel \tilde{\nu} \star \tilde{\nu} \parallel_2 > \frac{1}{4K} \parallel \tilde{\nu} \parallel_2$.

On écrit

$$\begin{aligned} \parallel \tilde{\nu} \star \tilde{\nu} \parallel_2 &= \parallel \sum_{1 \leq j_1, j_2 \leq J} 2^{-j_1 - j_2} \chi_{A_{j_1}} \star \chi_{A_{j_2}} \parallel_2 \\ &\leq \sum_{1 \leq j_1, j_2 \leq J} 2^{-j_1 - j_2} \parallel \chi_{A_{j_1}} \star \chi_{A_{j_2}} \parallel_2 . \end{aligned}$$

Il existe $1 \leq j_1, j_2 \leq J$ tels que

$$J^2 2^{-j_1 - j_2} \parallel \chi_{A_{j_1}} \star \chi_{A_{j_2}} \parallel_2 \geq \parallel \tilde{\nu} \star \tilde{\nu} \parallel_2 . \tag{1}$$

On pose $A = A_{j_1}$, $B = A_{j_2}$, $\alpha = j_1$ et $\beta = j_2$.

1. Estimation d'énergie. On minore

$$\begin{aligned} \parallel \tilde{\nu} \parallel_2^2 &= \sum_{j=1}^{J} 2^{-2j} |A_j| \\ &\geq 2^{-2\alpha} |A| + 2^{-2\beta} |B| \\ &\geq 2^{-\alpha-\beta} |A|^{1/2} |B|^{1/2}. \end{aligned}$$

Comme $\parallel \tilde{\nu} \star \tilde{\nu} \parallel_2 > \frac{1}{2^2 K} \parallel \tilde{\nu} \parallel_2$, il vient

$$2^{-\alpha-\beta} |A|^{1/2} |B|^{1/2} \leq 2^4 K^2 J^4 2^{-2\alpha-2\beta} \parallel \chi_A \star \chi_B \parallel_2^2 . \tag{2}$$

Comme $\tilde{\nu} \leq \nu$ qui est une mesure de probabilités, $|A_j| \leq 2^j$. Cela donne

$$|A|^{3/2} |B|^{3/2} \leq 2^4 K^2 J^4 E(A, B).$$

2. Majoration de la taille. D'après la remarque 9,

$$\begin{aligned} E(A,B) &\leq |B|^2|A| \\ &\leq 2^{\alpha+2\beta}. \end{aligned}$$

En injectant l'inégalité (1),

$$J^4 2^{-2\alpha-2\beta} E(A,B) \geq \| \tilde{\nu} \star \tilde{\nu} \|_2^2,$$

on trouve

$$|A| \leq 2^{\alpha} \leq J^4 \| \tilde{\nu} \star \tilde{\nu} \|_2^{-2} < 2^4 J^4 K^2 \| \tilde{\nu} \|_2^{-2} \leq 2^4 J^4 K^2 \| \nu_+ \|_2^{-2} .$$

Reste à minorer $\| \nu_+ \|_2$ en fonction de $\| \nu \|_2$. Comme $\nu < 2^{-J}$ sur A_-,

$$\| \nu_- \|_2^2 \leq \| \nu_- \|_\infty \| \nu_- \|_1 < 2^{-2J}|G| \leq \frac{1}{2^4 K^2} \| \nu \|_2^2,$$

d'où $\| \nu_+ \|_2^2 > \frac{1}{2} \| \nu \|_2^2$, et enfin $|A| < 2^5 J^4 K^2 \| \nu_+ \|_2^{-2}$.

3. Minoration de la taille. On reprend l'inégalité (2),

$$|A|^{1/2}|B|^{1/2} \leq 2^4 K^2 J^4 2^{-\alpha-\beta} E(A,B).$$

D'après la remarque 9,

$$E(A,B) \leq |A|^{3/2}|B|^{3/2}.$$

On trouve

$$1 \leq 2^4 K^2 J^4 2^{-\alpha-\beta}|A||B| = 2^4 K^2 J^4 \tilde{\nu}(A)\tilde{\nu}(B),$$

soit

$$\tilde{\nu}(A)\tilde{\nu}(B) \geq \frac{1}{2^4 K^2 J^4}.$$

Quitte à échanger A et B, on peut supposer que $\tilde{\nu}(A) \geq \tilde{\nu}(B)$. Dans ce cas, $\tilde{\nu}(A) \geq 1/4KJ^2$. Si $A' \subset A$, comme $\tilde{\nu}$ est constante sur A,

$$\nu(A') \geq \tilde{\nu}(A') = \frac{|A'|}{|A|}\tilde{\nu}(A) \geq \frac{|A'|}{4KJ^2|A|}.$$

12 Preuve du lemme 7

Supposons, par l'absurde, que $\| \nu \star \nu \|_2 > p^{-\epsilon} \| \nu \|_2$. Le lemme 13 fournit deux ensembles A et B tels que $E(A,B) \geq p^{-2\epsilon}|A|^{3/2}|B|^{3/2}$ (à un terme inoffensif en $\log p$ près). Le théorème de Tao fournit un $Cp^{2C\epsilon}$-sous-groupe approché $H \subset G$ tel que $|H| \leq p^{C\epsilon}|A|^{1/2}|B|^{1/2}$ et des éléments g et $g' \in G$ tels que $|A \cap (gH)| \geq p^{-C\epsilon}|A|$ et $|B \cap (g'H)| \geq p^{-C\epsilon}|B|$.

Noter que $|H| \leq p^{2C\epsilon}|A| \leq p^{4C\epsilon} \| \nu \|_2^{-2}$. Avec l'hypothèse $\| \nu \|_2 > p^{-1-\sigma}$,

$$|H| \leq p^{2+2\sigma+2C\epsilon}.$$

Comme on suppose $\sigma < 1/2$, l'exposant est < 3 si ϵ est assez petit.

D'après le lemme 13-3, $\nu(A) \geq p^{-\epsilon}/10(\log p)^2$. Il vient, à des termes logarithmiques près,

$$p^{-\epsilon} \leq \nu(A) \leq \| \nu \|_\infty |A|,$$

d'où $|A| \geq p^{\gamma-\epsilon}$, puis

$$|H| \geq p^{-2C\epsilon}|A| \geq p^{\gamma-\epsilon-2C\epsilon}.$$

Noter que $p^{4C\epsilon} < |H|^{\kappa}$ dès que $\epsilon < \kappa\gamma/(\kappa + 2C\kappa + 4C)$. C'est pourquoi H satisfait $|H \cdot H \cdot H| \leq C^2 p^{4C\epsilon}|H| < c|H|^{1+\kappa}$ pour p assez grand. D'après le théorème d'Helfgott, H est contenu dans un sous-groupe propre G_0 de G. En particulier,

$$\nu(gG_0) \geq \nu(gH) \geq \nu(A \cap gH) \geq \frac{|A \cap gH|}{4\,p^{\epsilon}|A|} > p^{-(C+1)\epsilon},$$

ce qui entraîne que $\nu^{(2)}(G_0) > p^{-2(C+1)\epsilon}$. Si $\epsilon < \delta/(2C+2)$, cela contredit l'hypothèse.

13 Triplement et sous-groupes approchés

Comme le montre le théorème d'Helfgott, le faible triplement est une hypothèse très forte. En fait, le triplement caractérise les sous-groupes approchés. Il s'agit du corollaire 3.10 de l'article de Tao à paraître à *Combinatorica*. Dans les groupes commutatifs, le doublement caractérise déjà les sous-groupes approchés, mais ce n'est pas le cas en général.

Théorème 14 (Tao). *Il existe une constante C qui a l'effet suivant. Soit $K > 1$. Soit G un groupe, $A \subset G$ un sous-ensemble qui satisfait à la condition de petit triplement $|A \cdot A \cdot A| \leq K|A|$. Posons $H_0 = A \cup \{1\} \cup A^{-1}$. Alors $H = H_0 \cdot H_0 \cdot H_0$ est un CK^C-sous-groupe approché qui contient A et tel que $|H| \leq CK^C|A|$. En particulier, si A est symétrique et contient 1, alors $A \cdot A \cdot A$ est un sous-groupe approché.*

Preuve. (schématique). Par récurrence sur n, on montre que $|A^{\pm} \cdot A^{\pm} \cdots A^{\pm}| \leq K^{C(n)}|A|$. Pour cela, il est commode d'utiliser l'inégalité triangulaire satisfaite par la *distance de Ruzsa*

$$d(A, B) = \log \frac{|A \cdot B^{-1}|}{|A|^{1/2}|B|^{1/2}}.$$

Par exemple, le triplement pour A entraîne que $d(A \cdot A, A^{-1}) \leq \log K$. De même, $|A \cdot A| \leq |A \cdot A \cdot A| \leq K|A|$ entraîne que $d(A, A^{-1}) \leq \log K$. Par l'inégalité triangulaire, $d(A \cdot A, A) \leq 2 \log K$, ce qui signifie que $|A \cdot A \cdot A^{-1}| \leq K^2|A|$. Et ainsi de suite...

Cela entraîne que $|H| \leq CK^C|A|$ et $|H_0 \cdot H \cdot H| \leq CK^C|A|$.

Ensuite (lemme de recouvrement de Ruzsa), on construit un $Y \subset H \cdot H$ tel que $H \cdot H \subset H_0^{-1} \cdot H_0 \cdot Y \subset H \cdot Y$, avec $|Y| \leq CK^C$. Pour cela, il suffit de choisir Y maximal parmi les sous-ensembles de $H \cdot H$ tels que les $H_0 y$, $y \in Y$, soient deux à deux disjoints.

Enfin, on pose $X = Y \cup Y^{-1}$ et on vérifie que $H \cdot H \subset H \cdot X$.