Recouvrements de réseaux euclidiens

Soline Arnoulx de Pirey, Paul-Enée Le Goff, Kanañ Marteil-Agarwal

Sous la direction de M. François Charles (DMA-ENS)

Table des matières

1 Introduction

Pour marquer son territoire, le chevreuil se frotte aux arbres pour y laisser une marque et son odeur. Ces marques sont perceptibles par les autres animaux jusqu'à une distance de 5 mètres. Il doit donc créer une grille de marques adaptée, pour recouvrir la forêt de sorte à ce qu'aucun point de son territoire ne soit à plus de 5 mètres d'un arbre de la grille. Comment doit-il faire ? Et si du haut de son intellect animal limité il choisissait une grille au hasard, quelle est la probabilité qu'il réalise une grille adaptée ? Dans ce mémoire, nous nous proposons de présenter et d'expliquer

l'article *New bounds on the density of lattice coverings* (2022) par Or Ordentlich, Oded Regev et Barak Weiss. Celui-ci répond à notre dernière question sur le chevreuil en montrant un résultat probabiliste sur les recouvrements d'un espace en n dimensions par des réseaux euclidiens.

Nous commencerons par introduire rigoureusement ce qu'est un réseau, et munir cet l'espace des réseaux d'une structure et d'une loi de probabilité (sections 1.1, 1.2, 1.3). Un fois ces bases posées, nous pourrons énoncer clairement le résultat que nous voulons démontrer (section 1.4). Ensuite, nous présenterons l'intuition globale de la preuve (partie 2), pour motiver les outils que nous utiliserons dans les deux dernières parties (partie 3), pour démontrer le théorème (partie 4).

1.1 Généralités sur les réseaux

Dans toute cette partie, nous fixons $n, r \in \mathbb{N}^*$ des entiers non nuls, nous travaillons dans $\mathbb{R}^n$.

Un réseau euclidien est :

Définition 1 (réseau euclidien)**.** Soit $(e_i)_{1\leq i\leq r}$ une famille libre de $\mathbb{R}^n$. Le réseau euclidien engendré par la famille (e_i) est :

$$L(e_i)_{1\leq i\leq r} = \{\sum_{k=1}^{r} \lambda_i e_i, (\lambda_i)_{1\leq i\leq r} \in \mathbb{Z}^r\}. \tag{1}$$

En posant $B = (e_1, ..., e_r)$ la matrice de la famille (e_i), (1) devient :

$$L(e_i)_{1\leq i\leq r} = \{BX, X \in \mathbb{Z}^r\} = B\mathbb{Z}^r. \tag{2}$$

Un réseau euclidien hérite naturellement de la structure de groupe de $\mathbb{Z}$: c'est un groupe additif commutatif.

Puisque nous travaillons dans $\mathbb{R}^n$, nous nous permettrons d'appeler *réseau* un *réseau euclidien* sans ambiguïté.

Remarque 1. On appelle r le rang du réseau. En pratique, on ne parlera dans ce mémoire que de réseaux de rang n, où n est la dimension de l'espace.
La famille (e_i) est appelée base du réseau, elle n'est pas du tout unique. Deux matrices $B, B' \in GL_n(\mathbb{R})$ engendrent le même réseau ssi $\exists U \in Gl_n(\mathbb{Z}), B' = UB$
Une base d'un réseau L est une base de $Vect(L)$, mais la réciproque est fausse, celà est dû au fait que $\mathbb{Z}$ n'est pas un corps.

Définition 2 (Sur-réseau)**.** Soit $L, L' \subset \mathbb{R}^n$ des réseaux de rang n.
L' est un sur-réseau de L ssi $L \subset L'$.

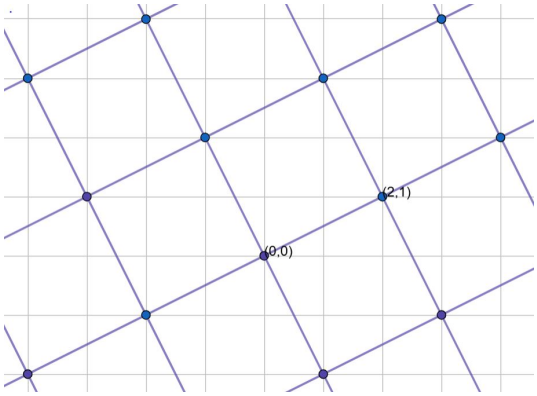

FIGURE 1 – Le réseau bleu est un sur-réseau du réseau gris, et ces deux réseaux sont de rang 2 dans le plan.

Définition 3 (Domaine fondamental)**.** Soit $(e_i)_{1\leq i\leq n} \in \mathbb{R}^n$ une famille libre et L le réseau engendré par B (défini par (1)). Le domaine fondamental subordonné à (e_i) de L est :

$$\mathcal{P}_{(e_i)}(L) = \{\sum_{k=1}^{n} x_i e_i, (x_i)_{1\leq i\leq n} \in [0,1[^n\}. \tag{3}$$

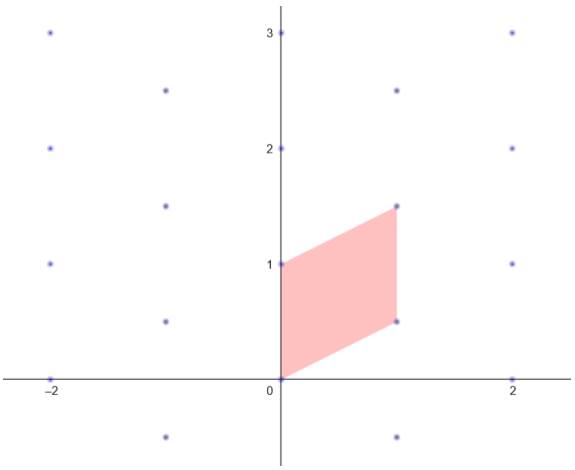

FIGURE 2 – Réseau en deux dimension et un domaine fondamental en rouge

Remarque 2. La définition du domaine fondamental est étroitement liée au choix de la base, ce qui est particulièrement désagréable. Nous allons donc définir une quantité, invariante par choix de base : le covolume.

Définition 4 (covolume)**.** Soit L un réseau, et B une base de L. Alors $|\det(B)|$ est appelé covolume de L.

Remarque 3. Le covolume est une grandeur indépendante de la base choisie. En effet, si B, B' sont des bases de L, alors $\exists U \in GL_n(\mathbb{Z}), B' = UB$ et $det(U) = \pm 1$.

Remarque 4. Le covolume est aussi la mesure de l'espace fondamental (pour la mesure de Lesbegue). Celà se montre en fixant une base B du réseau, et en orthogonalisant cette base, par Gram Schmidt, nous obtenons : $det(B) = \prod_{i=1}^{n} \|b_i\|$, ce qui nous donne le résultat.

Il existe donc plusieurs façons de voir un réseau : soit nous nous intéressons à une base, soit nous oublions la base pour ne voir que la structure de groupe. Micciancio et Goldwasser montrent dans [Mic02] que les réseaux sont exactement les sous-groupes discrets de l'espace euclidien :

Propriété 1 (réseau euclidien, définition équivalente)**.** Soir $L \subset \mathbb{R}^n$, L est un réseau ssi :

$$\begin{cases} 0 \in L \\ \forall x, y \in L, x - y \in L \\ \inf_{x,y \in L, x \neq y} d(x, y) > 0, \text{avec } d \text{ la distance euclidienne.} \end{cases} \tag{4}$$

Remarque 5. Le rang du réseau est la dimension de $Vect(L)$

1.2 Recouvrement euclidien

Définition 5 (Recouvrir)**.** Soit L un réseau, et $\mathcal{K}$ un convexe. On dit que $(L, \mathcal{K})$ recouvrent $\mathbb{R}^n$ ssi $\mathbb{R}^n = L + \mathcal{K}$.

Voici un exemple de recouvrement à l'aide de boules, toujours en deux dimensions :

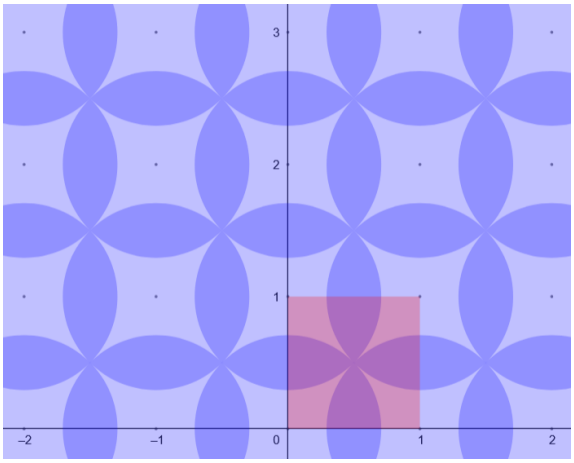

FIGURE 3 – Recouvrement à l'aide de boules (de rayon $\frac{\sqrt{2}}{2}$) et du réseau $\mathbb{Z}^2$

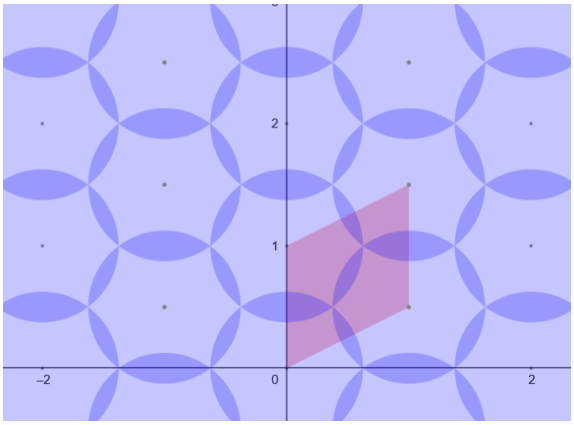

FIGURE 4 – Recouvrement plus fin de $\mathbb{R}^2$ à l'aide de boules, mais avec un réseau différent.

On peut s'intéresser au volume nécessaire d'un dilaté de la boule de rayon 1 pour recouvrir l'espace. Pour la figure 3, ce volume minimal est environ $1,57$ (i.e. $\frac{\pi}{2}$). En comparaison, le réseau de la figure 4, aussi de covolume 1, permet de recouvrir l'espace avec des boules de volume $1,23$ seulement. Nous voyons qu'en fonction du réseau, il faut plus ou moins dilater un convexe d'intérieur non vide (ici la boule de rayon 1) pour recouvrir tout l'espace.

Le but de ce mémoire est de montrer que, pour tous les convexes d'intérieur non vide et pour beaucoup de réseaux, il suffit de dilater un peu le convexe pour qu'il recouvre l'espace (théorème 2) . Pour réussir à formaliser ce résultat, il faut quantifier ce que "beaucoup de réseaux" veut dire, pour se faire, nous allons munir l'espace des réseaux d'une loi de probabilité.

1.3 Ensemble des réseaux et mesure de Haar-Sigel

Dans cette partie, nous allons munir l'ensemble des réseaux d'une structure pour le munir d'une loi de probabilité.

Définition 6 (Réseaux de covolume c)**.** Posons $\mathcal{L}_{n,c}$ l'ensemble des réseaux de $\mathbb{R}^n$ de covolume c.

En particulier, nous nous intéresserons à des réseaux renormalisés, de covolume 1.

On peut voir l'ensemble des réseaux de covolume 1 comme le quotient $\mathrm{SL_n}(\mathbb{R})/\mathrm{SL_n}(\mathbb{Z})$. En effet, un réseau de rang n comme un ensemble $g\mathbb{Z}^n$ avec g inversible et de déterminant 1 (c'est le covolume), et on remarque que $gu\mathbb{Z}^n = g\mathbb{Z}^n$ si $u \in \mathrm{SL_n}(\mathbb{Z})$.

Théorème 1. On identifie $\mathcal{L}_{n,1}$ à $\mathrm{SL_n}(\mathbb{R})/\mathrm{SL_n}(\mathbb{Z})$ via l'isomorphisme :

$$\begin{array}{rccc} \phi & : & \mathrm{SL_n}(\mathbb{R})/\mathrm{SL_n}(\mathbb{Z}) & \to & \mathcal{L}_{n,1} \\ & & cl(B) & \mapsto & L(B) \end{array} \tag{5}$$

Cet isomorphisme permet de munir l'ensemble des réseaux d'une topologie : la topologie quotient.

Nous pouvons donc considérer $\mathcal{L}_{n,1}$ comme un groupe quotient grâce à l'isomorphisme ϕ^{-1} vers $\mathrm{SL_n}(\mathbb{R})/\mathrm{SL_n}(\mathbb{Z})$. Pour parler de probabilité, nous devons munir cet espace d'une mesure finie. Dans tout ce mémoire, nous allons utiliser la mesure de Haar-Sigel, contruite dans [Sgl45] par Siegel. Cette mesure est invariante par translation dans $SL_n(\mathbb{Z})$ et finie. Nous choisissons de la renormaliser pour qu'elle soit une mesure de probabilité.

Remarque 6 (notation)**.** On notera, jusqu'à la fin de ce mémoire, $\mu_{n,1}$ ou μ_n la mesure de probabilité de Haar-Siegel sur $\mathcal{L}_{n,1}$, et $\mu_{n,c}$ la mesure correspondante sur $\mathcal{L}_{n,c}$.

1.4 Résultat

Définition 7. Soit L un réseau de $\mathbb{R}^n$, $\mathcal{K}$ un borélien convexe de $\mathbb{R}^n$. Posons :

$$\Theta_{\mathcal{K}}(L) = \inf\{vol(\lambda\mathcal{K}), \lambda > 0, \lambda\mathcal{K} + L = \mathbb{R}^n\} \tag{6}$$

où *vol()* est le volume d'un borélien, calculé grâce à la mesure de Lebesgue.

Voici maintenant le résultat principal de l'article, dont nous présenterons une preuve dans la section 4.

Théorème 2. Il existe des constantes strictement positives c_1, c_2, c_3 et c_4 telles que pour tout $n \geq 1$, $M \in \left[c_3 n^2, c_4 n^3\right]$ et $\mathcal{K}$ convexe borélien d'intérieur non vide,

$$\mu_{n,1}\left(\Theta_{\mathcal{K}}(L) > M\right) < c_1 e^{-\frac{c_2 M}{n^2}} \tag{7}$$

Ce résultat est un résultat asymptotique sur la dépendance en M et n de la probabilité, les constantes ne seront pas explicitées. Elles peuvent l'être si besoin, ce travail fut effectué par Rogers dans [Rog58]. On remarque que la borne ne dépend pas de la forme du convexe $\mathcal{K}$. Le résultat est donc très général, mais n'est pas optimal pour tous les convexes.

Remarque 7. Ce résultat affirme que plus un convexe est gros, plus la probabilité qu'il ne permette pas de recouvrir l'espace est faible, avec une dépendance exponentiellement décroissante en le volume du convexe. Cette majoration est plus faible à mesure que n augmente, donc plus l'espace est de haute dimension plus il est difficile de le recouvrir.

Nous pouvons énoncer un corollaire remarquable de ce théorème, dont nous ne détaillerons pas la preuve (celle-ci se retrouve dans [Ord22]).

Corollaire 3. Il existe une constante strictement positive c telle que pour tout $n \geq 1$ et $\mathcal{K}$ borélien convexe d'intérieur non vide,

$$\inf\left\{\Theta_{\mathcal{K}}(L), L \in \mathcal{L}_{n,1}\right\} < cn^2. \tag{8}$$

Ainsi, pour tout convexe, il existe un réseau suffisamment bien adapté pour recouvrir l'espace à l'aide d'un dilaté du convexe de volume seulement quadratique en n la dimension de l'espace. De nouveau, ce résultat est général car ne dépend pas de la forme du convexe, et améliore une borne générale précédemment trouvée par Rogers [Rog59], mais est moins bonne qu'une borne trouvée pour le cas des boules, en $n(log(n))^c$ ([Rog59]).

2 Idée de la preuve

Le but de cette partie est de motiver les outils que nous allons utiliser pour démontrer le résultat, et de donner les grandes idées de la preuve. Elle n'est volontairement pas rigoureuse. Une démonstration détaillée est donnée dans les parties suivantes.

Soit $\mathcal{K} \subset \mathbb{R}^n$ un borélien convexe d'intérieur non vide. Nous cherchons donc à montrer que pour beaucoup de réseaux L, $L + \lambda\mathcal{K} = \mathbb{R}^n$ pour λ pas trop grand. Le défi est de réussir à trouver une méthode qui permette de construire beaucoup de L tels que $L + \lambda\mathcal{K} = \mathbb{R}^n$, et un critère pour savoir si $L + \lambda\mathcal{K}$ recouvre $\mathbb{R}^n$.

Nous commencerons par remarquer que $L + \lambda\mathcal{K}$ est un espace périodique en chaque direction du réseau, donc que nous pouvons nous ramener à une étude du domaine fondamental. Dans ce domaine fondamental, nous cherchons à savoir si $\lambda\mathcal{K}$ couvre tout l'espace. Il faut non seulement que $\lambda\mathcal{K}$ soit de volume pas trop petit (ce qui n'est pas trop difficile à demander, étant donné que nous pouvons encore le dilater et que $\mathcal{K}$ est d'intérieur non vide), mais ce n'est pas suffisant. Comme le montre les deux figures ci-dessous, il est possible de construire des convexes de grand volume qui ne couvrent pas le domaine fondamental en entier :

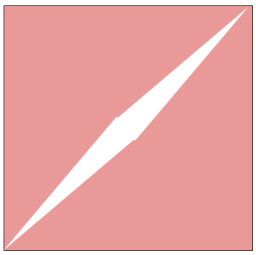

FIGURE 5 – Ensemble de grand volume dans le domaine fondamental, mais qui ne possède pas pour autant toutes les directions

En effet, dans cet exemple, nous avons construit un convexe de volume proche de 1, mais qui ne couvrait pas tout l'espace... car ils ne possédait pas toutes les directions ! Cette remarque nous invite naturellement à étudier la propriété $\ll$ posséder toutes les directions $\gg$, il s'agit du problème de Kakeya.

2.1 Le problème de Kakeya

Définition 8 (Problème de Kakeya)**.** Le problème de Kakeya se demande quelle est l'aire minimale d'une région de $\mathbb{R}^n$ dans laquelle on peut faire tourner continûment une aiguille de taille 1 d'un tour complet.

Une région (d'aire non minimale) très simple est donnée par le cercle :

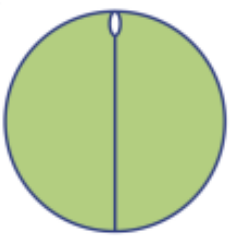

FIGURE 6 – Solution la plus simple, d'aire $\frac{\pi}{4} \approx 0,785$
source : accromath.uqam.ca

Des solutions plus optimales ont été trouvées par la suite :

FIGURE 7 – Solution convexe d'aire $\approx 0,704$
source : accromath.uqam.ca

FIGURE 8 – Solution convexe d'aire $\approx 0,577$
source : accromath.uqam.ca

De nombreuses améliorations non convexes ont été proposées :

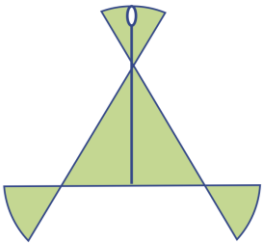

FIGURE 9 – Solution d'aire $\approx 0,412$
source : accromath.uqam.ca

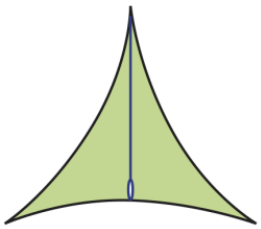

FIGURE 10 – Solution d'aire $\approx 0,392$
source : accromath.uqam.ca

Jusqu'à ce que Besicovich fabrique un ensemble de Kakeya d'aire arbitrairement petite à l'aide de fractales :

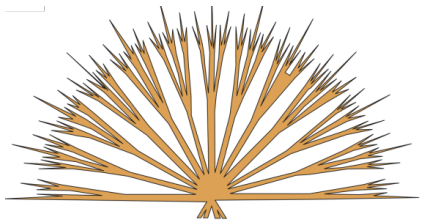

FIGURE 11 – Ensemble de Besicovitch
source : accromath.uqam.ca

Ce résultat compromet la réussite de notre intuition d'utiliser des ensembles de Kakeya pour voir si $\mathcal{K}$ possède toutes les directions : en effet, si $\mathcal{K}$ peut être aussi petit qu'on veut, nous ne pourrons pas le dilater par une constante en étant sûrs qu'il recouvre tout l'espace. Il nous faudrait une minoration du volume de $\mathcal{K}$... ce qui n'est pas le cas !

De récentes recherches dans ce domaine [KLSS11] ont montré que les ensembles de Kakeya sur de corps finis (des $\mathbb{F}_p^n$ avec p premier, vus comme des espaces vectoriels) avaient des cardinaux minorés par une constante. Si nous pouvions passer de $\mathbb{R}^n$ à $\mathbb{F}_p^n$, notre piste a plus de chances d'aboutir !

2.2 La correspondance de Hecke

Ce passage du continu au discret s'appelle la correspondance de Hecke [COU01]. Elle nous permet travailler avec un nouveau réseau dans $\mathbb{F}_p^n$. Une étude des ensembles de Kakeya dans $\mathbb{F}_p^n$ nous permet de dire que pour $K' \subset \mathbb{F}_p^n$, si K' est grand, il y a beaucoup de 2-plans dont tous les translatés rencontrent K' (*i.e.*, K' est grand dans toutes les directions !). C'est cette propriété qui nous permettra, entre autres, de conclure que $L + \lambda\mathcal{K} = \mathbb{R}^n$, en fabriquant K' à partir de $\lambda\mathcal{K}$.

2.3 Théorème de Rogers

Pour appliquer cette propriété, encore faut-il trouver un K' de volume assez grand. On exploite pour cela un résultat antérieur, dû à Rogers (dans[Rog58]). Il nous assure que pour beaucoup de réseaux, $L + \mathcal{K}$ recouvre une grosse partie du domaine fondamental. En projetant cette propriété dans $\mathbb{F}_p^n$, cela veut dire qu'on peut trouver un K', qui dépend de J, qui soit très grand.

3 Outils

Dans cette partie, nous allons définir les outils introduits précédemment et démontrer les propriétés fondamentales qui nous permettrons de démontrer (7).

3.1 Critère élémentaire

Commençons par énoncer un critère élémentaire, qui permet d'affirmer qu'un réseau et un convexe recouvrent $\mathbb{R}^n$. Pour cela, nous allons nous intéresser au tore $\mathbb{R}^n/L$, où L est vu comme un sous groupe distingué (puisque abélien) de $\mathbb{R}^n$.

Remarque 8 (notation)**.** Nous appelons $\pi_L := \mathbb{R}^n \to \mathbb{R}^n/L$ la projection de $\mathbb{R}^n$ sur le tore, et m_L : la mesure de probabilité de Haar sur le groupe additif $\mathbb{R}^n/L$

Propriété 2 (Critère élémentaire)**.** Soit $J \subset \mathbb{R}^n$ un convexe borélien d'intérieur non vide. Si $m_L(\pi_L(J)) > \frac{1}{2}$, alors $L + 2J = \mathbb{R}^n$

Démonstration. Comme une mesure de Haar est invariante par translation par un élément du groupe, pour tout $x \in \mathbb{R}^n/L$, on a $m_L(x + \pi_L(-J)) = m_L(\pi_L(-J)$.

Or, $m_L(\pi_L(-J)) = m_L(\pi_L(J))$ (propriété héritée de la mesure de Lebesgue). Ainsi,

$$m_L(x + \pi_L(-J)) = m_L(\pi_L(J)) > \frac{1}{2}$$

Or $m_L(\mathbb{R}/L) = 1$, donc $(x+\pi_L(-J)) \cap \pi_L(J) \neq \emptyset$ *i.e.* il existe $z_1, z_2 \in \pi_L(J)$ tels que $x - z_1 = z_2$. Donc $x = z_1 + z_2 \in \pi_L(2J)$, et ce pour x quelconque dans $\mathbb{R}^n/L$. D'où $L + 2J = \mathbb{R}^n$. □

3.2 Théorème de Rogers

Pour un réseau $L \in \mathcal{L}_n$ soit $\mathbb{T}_L \stackrel{\text{def}}{=} \mathbb{R}^n/L$ le tore quotient, soit m_L la mesure de probabilité de Haar sur $\mathbb{T}_L$, et soit $\pi_L : \mathbb{R}^n \to \mathbb{T}_L$ la projection sur le quotient $\mathbb{R}^n \backslash L$. Soit $\mathrm{Vol}(\cdot)$ la mesure de Lebesgue sur $\mathbb{R}^n$. Pour un ensemble mesurable $J \subset \mathbb{R}^n$, et un reseau $L \subset \mathbb{R}^n$, soit

$$\varepsilon(J, L) \stackrel{\text{def}}{=} 1 - m_L\left(\pi_L(J)\right)$$

De manière équivalente, $\varepsilon(J, L)$ est la densité de points de $\mathbb{R}^n$ pas couverts par $L + J$.

Soit également

$$\eta = \eta_n \stackrel{\text{def}}{=} \frac{n}{4} \log\left(\frac{27}{16}\right) - 3 \log n.$$

Rogers a alors montré, dans [Rog58] :

Théorème 4 (Rogers)**.** Il existe une constante $c_{Rog} > 0$ telle que, pour tout $n \in \mathbb{N}$, pour tout ensemble mesurable $J \subset \mathbb{R}^n$ avec

$$V \stackrel{\text{def}}{=} \mathrm{Vol}(J) \leq \eta$$

on ait

$$\left| \int_{\mathcal{L}_n} (J, L) d\mu_n(L) - e^{-V} \right| < c_{Rog} \cdot e^{-\eta}.$$

Ce théorème se réécrit, en utilisant l'inégalité de Markov :

Corollaire 5. Avec les mêmes hypothèses et notations, pour tout $\kappa > 0$,

$$\mu_n\left(\{L \in \mathcal{L}_n : (J, L) > \kappa\}\right) < \frac{1}{\kappa}\left(e^{-V} + c_{Rog}\, e^{-\eta}\right)$$

Remarque 9. Il nous assure donc que pour beaucoup de réseaux, $L+J$ recouvre une grosse partie du domaine fondamental. En projetant cette propriété dans $\mathbb{F}_p^n$, cela veut dire qu'on peut trouver un K', qui dépend de J, qui soit très grand.

N'oublions pas que ce théorème est une amélioration car il permet de dire que la probabilité que $L+\lambda J$ *recouvre* tout l'espace est grande, et non que $L+\lambda J$ recouvre presque l'espace. Il reste donc à montrer que $L+\lambda J$ vérifie les hypothèses d'une propriété élémentaire pour en déduire le résultat.

Dans ce mémoire, nous utiliserons une adaptation du corollaire 5 :

Théorème 6. Soit J un convexe borélien d'intérieur non vide de volume V. Alors :

$$\Pr(\varepsilon(J,L) > e^{-V/2}) < c_0 e^{-V/2}$$

avec $c_0 := 1 + c_{Rog}$, en utilisant $\kappa = e^{-V/2}$ et en se souvenant que $V \leq \eta$.

Démonstration. Idée de la preuve (tirée de [Rog58], théorème 1) :

Soit J un borélien de mesure finie, L un réseau de déterminant 1. On note $\alpha(L,\cdot)$ la fonction caractéristique des points qui ne sont pas dans $L+J$.

On note ρ la fonction caractéristique de J. On peut alors utiliser une série infinie d'inclusion-exclusion pour trouver que :

$$a(A,x) = 1 + \sum_{k=1}^{n} \frac{(-1)^k}{k!} \sum_{\substack{g_1,\ldots,g_k \in L \\ \text{distinct}}} \prod_{r=1}^{k} p(g_r + x).$$

On va ensuite simplifier cette somme en restreignant les sommes aux ensembles de points ne se trouvant pas dans un sous-espace affine de faible dimension.

On intègre ensuite sur l'espace des réseaux, en utilisant des résultats antérieurs de Siegel, Schmidt et Rogers pour encadrer des intégrales.

Lorsque V est petit (*i.e.* inférieur à η) alors les termes d'ordre élevés décroissent rapidement, ce qui permet de conclure. □

3.3 Correspondances de Hecke

Dans cette partie, nous allons étudier comment passer d'un réseau sur $\mathbb{R}^n$ à un réseau sur $\mathbb{F}_p^n$, où p est un nombre premier et $\mathbb{F}_p$ est le corps à p éléments. On notera $\pi_p := g\mathbb{Z}^n \to g\big(\mathbb{F}_p\big)^n$ la réduction modulo p des coordonnées. Pour ce faire, nous étudierons un cas particulier des correspondances de Hecke, étudiés notamment dans [COU01]. Ces correspondances seront des sur-réseaux associés à un réseau L, p plus fins que lui selon deux directions, avec p un nombre premier. Leur étroit lien avec les plans de $\mathbb{F}_p^n$ nous permettra d'utiliser le résultat lié au problème de Kakeya discret où interviennent ces mêmes plans.

Pour la suite, définissons donc les notions suivantes :

Définition 9. Soit $L \subset \mathbb{R}^n$ un réseau. Posons $\Lambda_{p,2}(L) = \{L' \text{ sur-réseau de L tels que } L'/L \cong (\mathbb{F}_p)^2\}$.

Cette définition a le défaut de n'être pas constructive, et pour mieux appréhender cette notion, nous donnerons une caractérisation utile, faisant intervenir les plans de $\mathbb{F}_p^n$. La définition des grassmaniennes nous permettra de la formaliser :

Définition 10 (grassmannienne de rang r)**.** Soit $\mathbb{K}^n$ espace vectoriel sur le corps $\mathbb{K}$ de dimension $n \in \mathbb{N}^*$. La grassmannienne de $\mathbb{K}^n$ de rang r, notée $\mathrm{Gr}_{n,r}(\mathbb{K})$ est :

$$\mathrm{Gr}_{n,r}(\mathbb{K}) = \{F < \mathbb{K}^n, \dim(F) = r\}$$

Cette caractérisation nous permettra de démontrer le résultat suivant, qui est l'objet de cette partie.

Théorème 7 (Correspondance de Hecke)**.** Choisir $L' \in \mathcal{L}_{n,p^{-2}}$ selon la distribution $\mu_{n,p^{-2}}$ revient à choisir indépendamment $S \in \mathrm{Gr}_{n,2}(\mathbb{F}_p)$ selon la distribution uniforme, $L = g\mathbb{Z}^n \in \mathcal{L}_{n,1}$ selon $\mu_{n,1}$ et poser $L' := p^{-1}g\pi_p^{-1}(S)$.

Prenons un exemple de réseaux L et L' pour mieux visualiser :

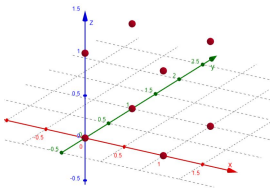

FIGURE 12 – Le réseau de base le plus simple, $L = \mathbb{Z}^n$, et alors $g = I_3$

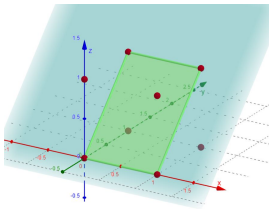

FIGURE 13 – On prend $p = 2$ et S le plan vert (d'équation $y = z$), au sein du domaine fondamental

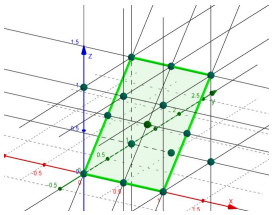

FIGURE 14 – Le nouveau réseau $L' = \frac{1}{2}\pi_2^{-1}(S)$ est alors un sur-réseau de L

On peut donc bien se ramener à une correspondance de Hecke choisie au hasard avec

$$\Pr\left(\Theta_{\mathcal{K}}(L) \leq M\right) = \Pr\left(\Theta_{\mathcal{K}}(L') \leq \frac{M}{p^2}\right)$$

avec le membre de droite selon la loi de probabilité produit de la loi uniforme sur la grassmanienne de rang 2 et de la loi de $\mu_{n,1}$ d'après le théorème.

Énonçons la caractérisation attendue :

Lemme 8. Soit $L = g\mathbb{Z}^n \in \mathcal{L}_{n,1}$, avec $g \in \mathrm{SL}_n(\mathbb{R})$. Alors :

$$\Lambda_{p,2}(L) = \{p^{-1}g\pi_p^{-1}(S) : S \in \mathrm{Gr}_{n,2}(\mathbb{F}_p)\}$$

Démonstration. En effet, l'inclusion réciproque s'effectue en remarquant que $L \subset p^{-1}g\pi_p^{-1}(S) \subset \frac{1}{p}L$ et donc $p^{-1}g\pi_p^{-1}(S)/L \cong \frac{1}{p}S \cong (\mathbb{F}_p)^2$.

Démontrons l'inclusion directe. Pour $L' \in \Lambda_{p,2}\big(L\big)$, on a $L'/L \cong (\mathbb{F}_p)^2$ donc $pg^{-1}L'/p\mathbb{Z}^n \cong (\mathbb{F}_p)^2$, d'où :

$$\pi_p(pg^{-1}L')/\pi_p(p\mathbb{Z}^n) \cong (\mathbb{F}_p)^2, \textit{ ie } \pi_p(pg^{-1}L') \cong (\mathbb{F}_p)^2$$

Or $\pi_p(pg^{-1}L')$ est un ensemble de combinaison linéaires à coefficients dans $\mathbb{F}_p$ de vecteurs linéairement indépendants, donc il est de dimension 2 et $\exists S \in \mathrm{Gr}_{n,2}(\mathbb{F}_p)$ tel que

$$\pi_p(pg^{-1}L') = S$$

□

Preuve du théorème. Dans cette démonstration, nous notons $C_c(\mathcal{L}_{n,p^{-2}})$ l'ensemble des fonctions sur $\mathcal{L}_{n,p^{-2}}$ à valeurs dans $\mathbb{R}$ continues à support compact.
Grâce à la caractérisation des correspondances de Hecke (8), nous montrons plutôt l'égalité de distribution suivante :

$$\forall f \in C_c(\mathcal{L}_{n,p^{-2}}), \int f \, d\mu_{n,p^{-2}} = \int \left(\frac{1}{N} \sum_{L' \in \Lambda_{p,2}\big(L\big)} f(L') \right) d\mu_{n,1}$$

En remarquant que $\varphi : f \longmapsto \int \left(\frac{1}{N} \sum_{L' \in \Lambda_{p,2}\big(L\big)} f(L') \right) d\mu_{n,1}$ est une forme linéaire positive, le théorème de représentation de Riesz donne l'existence d'une mesure de Radon ν sur $\mathcal{L}_{n,p^{-2}}$ telle que $\varphi = f \mapsto \int f \, d\nu$. Montrons que $\nu = \mu_{n,p^{-2}}$.

On définit $f_i := \mathbb{1}_{K_i}$ avec $\big(K_i\big)_{i \in \mathbb{N}}$ une suite exhaustive croissante de compacts de $\mathcal{L}_{n,p^{-2}}$. On a la convergence simple $f_i \to 1$, car $\mathcal{L}_{n,p^{-2}}$ est de mesure 1.

Comme $\frac{1}{N} \sum_{L' \in \Lambda_{p,2}\big(L\big)} f_i(L') \in [0,1]$ et converge vers 1 pour tout L, on a par convergence dominée

$$\varphi(f_i) \to \int 1 \, d\mu_{n,1} = 1$$

$$\varphi(f_i) \to \int 1 \, d\nu$$

par convergence simple. Donc ν est une mesure de probabilité.

Par unicité à dilatation près de la mesure de Haar, il reste à montrer que $\forall g \in \mathrm{SL}_n(\mathbb{R})$ et $\forall A \subset \mathcal{L}_{n,p^{-2}}$, $\nu(gA) = \nu(A)$. De façon équivalente :

$$\forall g \in \mathrm{SL}_n(\mathbb{R}), \forall f \in C_c(\mathcal{L}_{n,p^{-2}}), \int f \circ g \, d\nu = \int f \, d\nu$$

En effet, on a

$$\begin{aligned} \int f \circ g \, d\nu &= \int \left(\frac{1}{N} \sum_{L' \in \Lambda_{p,2}\big(L\big)} f(gL') \right) d\mu_{n,1}(L) \\ &= \int \left(\frac{1}{N} \sum_{L'' \in \Lambda_{p,2}\big(gL\big)} f(L'') \right) d\mu_{n,1}(L) \end{aligned}$$

$$= \int \left(\frac{1}{N} \sum_{L'' \in \Lambda_{p,2}\left(gL\right)} f(L'') \right) d\mu_{n,1}(gL) = \int f \, d\nu$$

□

3.4 Problème de Kakeya

Dans toute cette partie, nous noterons $q = p^n$ avec $n \in \mathbb{N}^*, p$ premier $\mathbb{F}_q$ un corps à q éléments. Nous regarderons $\mathbb{F}_q^n$ comme un $\mathbb{F}_q$-espace vectoriel de degré n.

Nous rappelons la définition :

Définition 11 (grassmannienne de rang r)**.** Soit $\mathbb{K}^n$ espace vectoriel sur le corps $\mathbb{K}$ de dimension $n \in \mathbb{N}^*$. La grassmannienne de $\mathbb{K}^n$ de rang r, notée $\mathrm{Gr}_{n,r}(\mathbb{K})$ est :

$$\mathrm{Gr}_{n,r}(\mathbb{K}) = \{F < \mathbb{K}^n, \dim(F) = r\}$$

Définition 12 (ϵ-ensemble de Kakeya de rang r)**.** Soit $K \subset \mathbb{F}_q^n$. K est un ϵ-ensemble de Kakeya de rang r ssi $|\{l \in \mathrm{Gr}_{n,r}(\mathbb{F}_q^n), \exists x \in \mathbb{F}_q^n, l + x \subset K\}| \geq \epsilon |\mathrm{Gr}_{n,r}(\mathbb{F}_q)|$.

Remarque 10. Un 1-ensemble de Kakeya est appelé ensemble de Kakeya. Il est aussi possible de définir les ensembles de Kakeya pour un espace vectoriel E sur un corps infini de la façon suivante : $K \subset E$ est de Kakeya ssi $\forall l \in \mathrm{Gr}_{n,r}(E), \exists x \in E, l + x \subset K$.

Le but de cette partie est de montrer l'inégalité :

$$\mathcal{S} > (1 - \epsilon)|\mathrm{Gr}_{n,2}(\mathbb{F}_q)|$$

avec $\mathcal{S} = \{S \in \mathrm{Gr}_{n,2}(\mathbb{F}_q), \forall x \in \mathbb{F}_q^n, (x + S) \cap K' \neq \emptyset\}$, pour $K' \subset \mathbb{F}_q^n$, sous certaines hypothèses.

Nous allons nous intéresser à des encadrements de cardinaux d'ϵ-ensembles de Kakeya de rang r quelconque, pour en déduire, dans le cas r=2, la minoration voulue.

Le premier lemme permet de construire, à partir d'un ϵ-ensemble de Kakeya, un δ-ensemble de Kakeya dont on peut contrôler le cardinal.

Lemme 9. Soit $0 < \epsilon < \delta < 1, K \subset \mathbb{F}_q^n$ un ϵ-ensemble de Kakeya de rang r. Alors il existe $\mathcal{A} \subset \mathbb{F}_q^n$ un δ-ensemble de Kakeya de rang r tel que :

$$|\mathcal{A}| \leq \lceil \frac{\ln(1-\delta)}{\ln(1-\epsilon)} \rceil |K|$$

Démonstration. Pour $K' \subset \mathbb{F}_q^n$, on pose :

$$\mathcal{B}_{K'} = \{S \in \mathrm{Gr}_{n,r}(\mathbb{F}_q), \exists x \in \mathbb{F}_q^n, S + x \subset K'\}$$

Cet ensemble permet de déterminer si K' est un ϵ-ensemble de Kakeya : c'est le cas ssi $|\mathbb{B}_{K'}| \geq \epsilon |\mathrm{Gr}_{n,r}(\mathbb{F}_q^n)|$.
Soit $g \in GL_n(\mathbb{F}_q^n), S \in \mathrm{Gr}_{n,r}(\mathbb{F}_q^n)$. Notons que $S \in \mathcal{B}_{K'}$ ssi $gS \in \mathcal{B}_{gK'}$.
Soit $\mathcal{N} \subset GL_n(\mathbb{F}_q^n)$ un ensemble fini de matrices inversibles. Posons :

$$\mathcal{A}(\mathcal{N}, K') = \bigcup_{g \in \mathcal{N}} gK'$$

Alors

$$|\mathcal{A}(\mathcal{N},K')| \leq |\mathcal{N}||K'| \text{ et } \bigcup_{g\in\mathcal{N}} g\mathcal{B}_{K'} \subset \mathcal{B}_{\mathcal{A}(\mathcal{N},K')}$$

Nous allons construire notre δ-ensemble de Kakeya $\mathcal{A}$ comme un certain $\mathcal{A}(\mathcal{N},K)$. Il suffirait de trouver un $\mathcal{N} \subset GL_n(\mathbb{F}_q^n)$ qui vérifie :

$$|\mathcal{N}| \leq \lceil \frac{\log(1-\delta)}{\log(1-\epsilon)} \rceil \text{ et } |\bigcup_{g\in\mathcal{N}} g\mathcal{B}_K| \geq \delta |\mathrm{Gr}_{n,r}(\mathbb{F}_q)|$$

Nous allons montrer qu'un tel ensemble existe par une méthode probabiliste. Plaçons nous sur $\Omega = GL_n(\mathbb{F}_q^n)$ et on tire indépendamment $N = \lceil \frac{\log(1-\delta)}{\log(1-\epsilon)} \rceil$ matrices, notées $g_1, g_2, ...g_N$ selon la loi uniforme. $\forall S \in \mathrm{Gr}_{n,r}(\mathbb{F}_q), \forall i \in 1 \ ; \ N$ posons E_S^i l'évènement $S \notin g_i\mathcal{B}_K$. Les $(E_S^i)_{1\leq i\leq N}$ sont indépendantes et identiquement distribuées, donc

$$E_S = \bigcap_{i=1}^{N} E_s^i \text{ vérifie } Pr(E_S) = Pr(E_S^1)^N$$

Puis :

$$Pr(E_S^1) = Pr(g_1^{-1}S \notin \mathcal{B}_K) = 1 - \frac{|\mathcal{B}_K|}{|\mathrm{Gr}_{n,r}(\mathbb{F}_q)|} \leq 1 - \epsilon$$

Car K est un ϵ-ensemble de Kakeya. D'où :

$$Pr(E_S) \leq (1-\epsilon)^N \leq 1 - \delta$$

Par définition de N. Donc

$$\mathbb{E}(|\bigcup_{i=1}^{N} g_i\mathcal{B}_K|) = \mathbb{E}(\sum_{S\in\mathrm{Gr}_{n,r}(\mathbb{F}_q)} \mathbb{1}_{S\in\bigcup_{i=1}^{N} g_i\mathcal{B}_K}) = \sum_{S\in\mathrm{Gr}_{n,r}(\mathbb{F}_q)} (1 - Pr(E_S)) \geq \delta|\mathrm{Gr}_{n,r}(\mathbb{F}_q)|$$

Nous en déduisons qu'il existe $\mathcal{N}$ qui vérifie les propriétés demandées. □

Nous aurons aussi besoin d'une minoration du cardinal d'un ϵ-ensemble de Kakeya. Cette minoration est forte quand ϵ est proche de 1, et assez faible si ϵ est proche de 0. La démonstration de ce lemme est faite dans par Ordentlich, Regev, et Weiss dans [Ord22], elle est inspirée de celle de Swastik Kopparty, Vsevolod, Shubhangi Saraf et Madhu Su-dan dans [KLSS11].

Lemme 10. Soit $0 < \delta \leq 1, K \subset \mathbb{F}_{||}{}^n$. Si K est un δ-ensemble de Kakeya de rang r, alors :

$$|K| \geq (1 + \frac{(q-1)q^{-r}}{\delta})^{-n} q^n$$

Lemme 11. Soit $0 < \epsilon < 1, K \subset \mathbb{F}_q^n$. Si K est un ϵ-ensemble de Kakeya de rang r, alors :

$$|K| > \epsilon(1 + 2(q-1)q^{-r})^{-n} q^n$$

Démonstration. Notons que si $\epsilon \geq 1/2$, le lemme est prouvé par (10). Il reste à montrer le cas où $\epsilon < 1/2$. Sans perte de généralité, supposons que $0 < \epsilon < 1/2$. Pour $\epsilon < \delta < 1$,

$$|K| \geq (\lceil \frac{\log(1-\delta)}{\log(1-\epsilon)} \rceil)^{-1} (1 + \frac{(q-1)q^{-r}}{\delta})^{-n} q^n$$

En effet, si par l'absurde l'inégalité nétait pas vérifiée, on pourrait fixer par (9) un δ-ensemble de Kakeya $\mathcal{A}$ tel que :

$$|\mathcal{A}| \leq \lceil \frac{\log(1-\delta)}{\log(1-\epsilon)} \rceil |K| < (1 + \frac{(q-1)q^{-r}}{\delta})^{-n} q^n$$

ce qui contredit (10). En choisissant $\delta = 1/2$, nous avons :

$$\lceil \frac{\log(1-\delta)}{\log(1-\epsilon)} \rceil = \lceil \frac{\log(2)}{-\log(1-\epsilon)} \rceil < 1 - \frac{\log(2)}{\log(1-\epsilon)} < \frac{\log(1-\delta)}{\log(1-\epsilon)} < \frac{1}{\epsilon}$$

Ce qui conclut, en injectant ce résultat dans l'inégalité du début, avec $\delta = 1/2$. □

Lemme 12. Soit $K \subset \mathbb{F}_q^n$ un ϵ-ensemble de Kakeya de rang r=2, alors $\frac{|K|}{q^n} \geq \epsilon e^{-2n/q}$.

Démonstration. $|K| > \epsilon(1 + 2(q-1)q^{-2})^{-n} q^n$ par (11). Puis

$$(1 + 2(q-1)q^{-2})^n = (1 + 2/q - 2/q^2)^n \leq (1 + 2/q)^n = ((1 + 2/q)^{q/2})^{2n/q} \leq e^{2n/q}$$

□

Théorème 13. Soit $K' \subset \mathbb{F}_q^n$ tel que $\frac{|K'|}{q^n} > 1 - \epsilon e^{-2n/q}$ alors

$$\mathcal{S} = \{S \in \mathrm{Gr}n, 2(\mathbb{F}_q), \forall x \in \mathbb{F}_q^n, (x+S) \cap K' \neq \emptyset\}, K' \subset \mathbb{F}_q^n \tag{9}$$

vérifie :

$$|\mathcal{S}| > (1-\epsilon)|\mathrm{Gr}n, 2(\mathbb{F}_q^n)| \tag{10}$$

Démonstration. En considérant $K = \mathbb{F}_q^n \backslash K'$, nous avons l'inégalité demandée ssi K est un ϵ-ensemble de Kakeya. Si, par l'absurde, ce n'était pas le cas, (12) serait contredit. □

4 Preuve du théorème

Dans toute cette partie, nous fixons p un nombre premier tel que $n \leq p \leq 2n$, $\mathcal{K}$ un convexe borélien d'intérieur non vide et $M > 0$. Nous préciserons au fil de la preuve l'intervalle auquel M doit appartenir.

4.1 Préliminaires

Choisissons aléatoirement, d'une part, $L \subset \mathbb{R}^n$ un réseau de covolume 1 selon $\mu_{n,1}$, avec $g \in GL_n(\mathbb{R})$ une base du réseau et d'autre part, $S \in \mathrm{Gr}_{n,2}(\mathbb{F}_p)$ selon la distribution uniforme.

Posons $L' = p^{-1} g \pi_p^{-1}(S)$, et remarquons que $L \subset L' \subset \frac{1}{p} L$. De plus, par (7), nous avons :

$$\Pr\left(\Theta_{\mathcal{K}}(L) \leq M\right) = \Pr\left(\Theta_{\mathcal{K}}(L') \leq \frac{M}{p^2}\right) \tag{11}$$

Notons tout au long de la preuve, nous identifions par isomorphisme $\mathbb{F}_p^n$ et $\pi_L(\frac{1}{p}L)$.

Puisque nous avons dilaté le réseau, nous allons aussi devoir travailler avec un convexe dilaté. Ainsi, définissons J :

$$J \text{ dilaté de } \mathcal{K}, \text{de volume V, avec } V := p^{-2}\big(1 + \frac{2}{p}\big)^{-n} M \tag{12}$$

Il serait plus agréable de travailler en sachant que le réseau L et le convexe J recouvrent déjà une grande partie de $\mathbb{R}^n$. Nous pouvons supposer cela grâce à (5). Plus précisément, nous considèrerons plutôt dans cette partie la probabilité conditionnelle :

$$\Pr\left(\Theta_{\mathcal{K}}(L) \leq M \;\middle|\; \varepsilon(J, L) \leq e^{-V/2}\right) \geq 1 - c_0 e^{-V/2} \geq 1 - c_0 e^{-c_2 M/n^2} \tag{13}$$

Ainsi, supposons dorénavant que L vérifie :

$$\varepsilon(J, L) \leq e^{-V/2} \tag{14}$$

On sait que cet événement a une probabilité supérieure à $1 - c_0 e^{-V/2} \geq 1 - c_0 e^{-c_2 M/n^2}$ par définition de V (12), ce qui est de l'ordre du résultat attendu.

Le lemme sur les ensembles de Kakeya (13) nous permettra de préciser le fait qu'un J assez grand sera grand selon toutes les directions. Rappelons ce théorème, en gardant en tête que K' est qualitativement une discrétisation de J dans le domaine fondamental. Pour $K' \subset \mathbb{F}_p^n$ tel que $\frac{|K'|}{p^n} \geq 1 - \varepsilon e^{-2n/q}$,

$$\Pr\left(\forall x \in \mathbb{F}_p^n, (x + S) \cap K' \neq \emptyset\right) > 1 - \varepsilon$$

en remarquant qu'il nous donne une minoration d'une probabilité sur le choix de S selon la distribution uniforme sur $\mathrm{Gr}_{n,2}(\mathbb{F}_p)$. C'est ce que nous voulons, et en définissant bien les ε et K', nous devrons trouver une condition $\forall x \in \mathbb{F}_p^n, (x + S) \cap K' \neq \emptyset$ impliquant $\Theta_{\mathcal{K}}(L') \leq \frac{M}{p^2}$.

Pour obtenir le résultat voulu, nous devons avoir un ε de l'ordre de $e^{-V/2}$ (d'après la remarque précédente : $c_0 e^{-V/2} \leq c_0 e^{-c_2 M/n^2}$).

4.2 Choix de K'

Par le choix de p et ε de l'ordre de $e^{-V/2}$, nous devons, pour appliquer (13) trouver K' tel que $\frac{|K'|}{p^n} \geq 1 - e^{-V/2}$. Or l'hypothèse de Rogers (14) nous donne :

$$m_L(\pi_L(J)) \geq 1 - e^{-V/2} \tag{15}$$

On voudrait donc naturellement définir $K' := \mathbb{F}_p^n \cap \pi_L(J)$, on voudrait $\frac{|K'|}{p^n} \geq m_L(\pi_L(J))$.

Cela n'est pas être vrai dans le cas général, car on peut construire des ensembles de grand volume qui ne rencontrent pas un certain ensemble discret, mais on peut montrer :

$$\exists u \in \mathbb{R}^n/L, \frac{1}{p^n} \mid (u + \mathbb{F}_p^n) \cap \pi_L(J) \mid \geq m_L(\pi_L(J)) \tag{16}$$

En effet, supposons par l'absurde que $\forall u \in \mathbb{R}^n/L$, $\frac{1}{p^n} \mid (u + \mathbb{F}_p^n) \cap \pi_L(J) \mid < m_L(\pi_L(J))$. Alors :

$$\frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} \mathbb{1}_{\pi_L(J)-x}(u) < m_L(\pi_L(J))$$

Donc en intégrant contre la mesure m_L, on a

$$\frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} m_L(\pi_L(J) - x) < m_L(\pi_L(J))$$

Or par définition de la mesure de Haar, $m_L(\pi_L(J)-x) = m_L(\pi_L(J))$, donc $m_L(\pi_L(J)) < m_L(\pi_L(J))$: c'est absurde.

Posons alors

$$K' := \big(u + \mathbb{F}_p^n\big) \cap \pi_L(J) - u \subset \mathbb{F}_p^n \ . \tag{17}$$

4.3 Utilisation du théorème de Kakeya

Nous avons donc $\frac{|K'|}{p^n} \geq m_L(\pi_L(J))$.

Nous appliquons donc (10) avec $\varepsilon := e^{-V/2} e^{2n/p} \leq e^2 e^{-V/2}$ (qui est bien de l'ordre escompté) ce qui nous donne :

$$\Pr\left(\forall x \in \mathbb{F}_p^n, (x + S) \cap K' \neq \emptyset\right) > 1 - \varepsilon \tag{18}$$

$$ie \ \Pr\left(\forall x \in \mathbb{F}_p^n, (u + x + S) \cap \pi_L(J) \neq \emptyset\right) > 1 - \varepsilon \tag{19}$$

Montrons que cet événement implique $\Theta_{\mathcal{K}}(L') \leq \frac{M}{p^2}$.

Soit $y \in u + \mathbb{F}_p^n$. L'événement dont il est question donne l'existence d'un $s \in S$ tel que $y - s \in \pi_L(J)$, donc $y \in \pi_L(J) + S$. Ainsi, dans tout l'espace, comme $L' = \pi_p^{-1}(S)$ (remarquons que l'identification de $\pi_L(\frac{1}{p}L)$ avec $\mathbb{F}_p^n$ nous permet de remplacer $\frac{1}{p}gS$ par S et donc simplifier la définition de L'), on a

$$u + \frac{1}{p}L \subset L' + J$$

On rappelle que par le critère élémentaire (2), puisque nous pouvons supposer que $V > 2\log 2$ et donc $m_L(\pi_L(J)) > 1 - e^{-V/2} > \frac{1}{2}$, nous avons $L + 2J = \mathbb{R}^n$.

Donc

$$\mathbb{R}^n = u + \frac{1}{p}\big(L + 2J\big) \subset L' + \left(1 + \frac{2}{p}\right) J$$

Donc

$$\Theta_{\mathcal{K}}(L') \leq \left(1 + \frac{2}{p}\right)^n V = \frac{M}{p^2}$$

Ainsi, par tout ce qui précède, on a montré

$$\Pr\left(\Theta_{\mathcal{K}}(L) \leq M \;\middle|\; \varepsilon(J, L) \leq e^{-V/2}\right) > 1 - e^2 e^{-V/2} \tag{20}$$

4.4 Conclusion

Ainsi, on a :

$$\Pr\Big(\Theta_{\mathcal{K}}(L) \leq M\Big) \geq \Pr\Big(\big(\Theta_{\mathcal{K}}(L) \leq M\big) \cap \big(\varepsilon(J, L) \leq e^{-V/2}\big)\Big)$$

i.e

$$\Pr\Big(\Theta_{\mathcal{K}}(L) \leq M\Big) \geq \Pr\left(\Theta_{\mathcal{K}}(L) \leq M \;\middle|\; \varepsilon(J, L) \leq e^{-V/2}\right) \Pr\Big(\varepsilon(J, L) \leq e^{-V/2}\Big)$$

Donc, par (5) et (20) :

$$\Pr\Big(\Theta_{\mathcal{K}}(L) \leq M\Big) > (1 - c_0 e^{-V/2})(1 - e^2 e^{-V/2}) \tag{21}$$

Donc

$$\Pr\Big(\Theta_{\mathcal{K}}(L) \leq M\Big) > 1 - c_1 e^{-V/2} > 1 - c_1 e^{-\frac{c_2 M}{n^2}}$$

par choix de V et de p, avec par exemple $c_1 = c_0 + e^2$.

Finalement,

$$\Pr\Big(\Theta_{\mathcal{K}}(L) > M\Big) < c_1 e^{-\frac{c_2 M}{n^2}} \tag{22}$$

pour $M \in \big[c_3 n^2, c_4 n^3\big]$, avec c_1, c_2, c_3 et c_4 indépendants de n, $\mathcal{K}$ et M. □

5 Bibliographie

[Ord22] Ordentlich, O., Regev, O., Weiss, B. (2022). New bounds on the density of lattice coverings. *Journal of the American Mathematical Society*, 35(1), 295-308.

[Rog58] Rogers, C.A. (1958), Lattice Coverings of Space : The Minkowski–Hlawka Theorem. *Proceedings of the London Mathematical Society*, s3-8 : 447-465.

[Ber11] Bergeron, N. (2011). *Le spectre des surfaces hyperboliques*. Harlequin.

[Mic02] Micciancio, D., Goldwasser, S. (2002). *Complexity of lattice problems : a cryptographic perspective* (Vol. 671). Springer Science Business Media.

[KLSS11] Swastik Kopparty, Vsevolod F. Lev, Shubhangi Saraf, Madhu Sudan (2011). *Kakeya-type sets in finite vector spaces*

[Sgl45] Carl Ludwig Siegel (1945). *Annals of mathematics* Vol46 (340-347)

[COU01] Laurent Clozel, Hee Oh, Emmanuel Ullmo (2001). Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2) :327–351