Théorie des nombres, combinatoire additive, analyse de Fourier et interactions. Mémoire de HDR de Anne de Roton

Anne de Roton

Université de Lorraine Ecole doctorale IAEM

Résumé de travaux

présenté pour obtenir

l'**Habilitation à Diriger des Recherches**

en

Mathématiques

par

Anne de Roton

Théorie des nombres, combinatoire additive, analyse de Fourier et interactions.

Date de soutenance : 14 juin 2018

Jury :

Christine Bachoc	Université de Bordeaux	Examinatrice
Jörg Brüdern	Université Georg August de Göttingen	Rapporteur
Cécile Dartyge	Université de Lorraine	Examinatrice
Laurent Habsieger	CNRS	Rapporteur
Hervé Queffelec	Université de Lille 1	Examinateur
Imre Ruzsa	Institut Alfréd Rényi de Mathématiques	Rapporteur
Oriol Serra	Universitat Politècnica de Catalunya	Examinateur
Thomas Stoll	Université de Lorraine	Examinateur

À Jean-Pierre Kahane

Remerciements

Merci tout d'abord infiniment à Jörg Brüdern, Laurent Habsieger et Imre Ruzsa, qui ont accepté d'écrire un rapport sur ce travail et qui lui ont porté un regard bienveillant. Merci à eux et à Christine Bachoc, Cécile Dartyge, Hervé Queffelec, Oriol Serra et Thomas Stoll d'avoir accepté de participer au jury de mon habilitation. Je suis très heureuse de partager avec eux ce moment qui prolonge les discussions mathématiques et amicales que nous avons pu avoir ces dernières années. Merci aussi à David Dos santos d'avoir accepté de me parrainer pour cette habilitation.

J'ai eu la chance de faire de belles rencontres mathématiques et humaines dans ma vie professionnelle. Les membres du jury en sont un exemple, mais aussi mes co-auteurs que je remercie vivement, avec par ordre d'apparition (mais non de parution !) : Michel Balazard dont je mesure aujourd'hui la patience et le dévouement alors qu'il dirigeait ma thèse, Bahman Saffari, Harold Shapiro et Gérald Tenenbaum avec lesquels j'ai fait mes premières armes postdoctorales, Szilárd Révész, Harald Helfgott qui m'a accompagnée vers la combinatoire additive, Alain Plagne et Pablo Candela avec lesquels j'ai le plaisir de poursuivre mes recherches, Diego González-Sánchez et Paul Péringuey.

Je n'oublie bien sûr pas les membres de l'Institut Elie Cartan, anciens et nouveaux, parmi lesquels je compte des amis très chers. Je profite au quotidien d'un environnement professionnel chaleureux et les discussions animées du midi, les papotages de bureau et les débats autour d'un café sont un attrait certain de mon travail. Je pense aussi bien sûr aux théoriciens des nombres de notre petite communauté que j'ai plaisir à retrouver colloque après colloque, aux mathématiciens de tous horizons qui ont croisé ma route.

La recherche est pour moi indissociable de l'enseignement et je remercie mes étudiants qui tout au long de ces années m'ont apporté beaucoup de joie, à commencer par Gautier Hanna et Robin Riblet dont j'ai eu ou j'ai la chance de suivre les travaux en thèse et les CPU, en particulier Séréna qui a tant fait pour cette formation.

Merci aux obstinés de tout poil sans lesquels mes colères seraient vaines : merci aux physiciens, mathématiciens, informaticiens, linguistes, philosophes, sociologues, psychologues, biologistes et autres littéraires qui ne se résignent pas !

Merci infiniment à Alex et Pierre qui me donnent force et bonheur chaque jour.

Enfin, je tiens à remercier Jean-Pierre Kahane dont l'amitié bienveillante m'a guidée ces dernières années. Son regard espiègle et chaleureux me manque chaque jour et aujourd'hui plus encore. Je lui dédie ce travail modeste. Cela peut paraître présomptueux mais nous partagions cette absence totale de respect pour la hiérarchie, aussi suis-je persuadée qu'il ne m'en voudrait pas.

Liste des travaux et publications

À paraître dans des revues internationales à comité de lecture :

— P. Candela, D. González-Sánchez, A. de Roton, *A Plünnecke-Ruzsa inequality in compact abelian groups*, arxiv : 1712.07615, à paraître dans Revista Matemática Iberoamericana.

— P. Candela, A. de Roton, *On sets with no sumset in the circle*, arXiv : 1709.04501, à paraître dans Quaterly Journal of Mathematics.

Parues dans des revues internationales à comité de lecture :

— A. de Roton, *Small sumsets in* $\mathbb{R}$ *: full continuous* $3k-4$ *Theorem, critical sets*, Journal de l'école polytechnique, Tome 5 (2018), p. 177-196.

— A. de Roton, B. Saffari, H. Shapiro et G. Tenenbaum, *Sur le principe d'incertitude pour les familles orthonormales de* $L^2(\mathbb{R})$, l'Enseignement Mathématique (2) **62** (2016), 285-300.

— A. Plagne, A. de Roton, *Maximal sets with no solutions to x+y=3z*, Combinatorica **36** (2016), pp. 229-248.

— A. de Roton, S. Révész, *Generalization of the effective Wiener-Ikehara Theorem*, Int. J. Number Theory **9** (2013), pp. 1091-1128.

— H. Helfgott, A. de Roton, *Improving Roth's theorem in the primes*, Int. Math. Res. Notices **4** (2011), pp. 767-783.

— M. Balazard, A. de Roton, *Sur un critère de Báez-Duarte pour l'hypothèse de Riemann*, Int. J. Number Theory **6** (2010), pp. 883-903.

— A. de Roton, *Une approche séquentielle de l'hypothèse de Riemann généralisée*, J. Number Theory **129** (2009), pp. 2647-2658.

— A. de Roton, *Généralisation du critère de Beurling-Nyman à la classe de Selberg*, Transactions of the AMS, **359** (2007), n°12, 6111-6126 (electronic) .

— A. de Roton, *On the mean square of the error term for an extended Selberg's class*, Acta Arithmetica **126** (2007), 27-55.

— A. de Roton, *Une approche hilbertienne de l'hypothèse de Riemann généralisée*, Bulletin de la SMF **134** (2006), 417-445.

— A. de Roton, *Généralisation du critère de Beurling-Nyman à la classe de Selberg*, C. R. Acad.Sci. Paris, Ser. I **340** (2005), 191-194.

Autres publications :

— M. Balazard, A. de Roton, *Notes de lecture de l'article "Partial sums of the Möbius function" de Kannan Soundararajan*, arXiv : 0810.3587

— Cours CIMPA d'analyse de Fourier discrète : théorème de Roth dans les entiers et les premiers (2013). http ://cel.archives-ouvertes.fr/cel-00963631.

Table des matières

Introduction

La thèse de doctorat *Généralisation du critère de Beurling-Nyman à la classe de Selberg*, écrite sous la direction de Michel Balazard, était consacrée à l'étude de certains critères pour l'hypothèse de Riemann généralisée aux fonctions de la classe de Selberg.
La classe de Selberg [Sel92] est une classe de fonctions caractérisées par des propriétés analytiques et arithmétiques. Ce sont en particulier des séries de Dirichlet absolument convergentes dans le demi-plan $\Re(s) > 1$, prolongeables méromorphiquement à $\mathbb{C}$ avec un pôle éventuel en 1, satisfaisant une équation fonctionnelle mettant en évidence une symétrie par rapport à la droite $\Re(s) = 1/2$ (dite droite critique) et admettant un développement en produit Eulérien. Cette classe est conjecturalement l'ensemble des fonctions L associées à une forme automorphe et son introduction est donc une tentative de définition axiomatique de telles fonctions. L'hypothèse de Riemann généralisée affirme que les zéros non triviaux des fonctions de la classe de Selberg sont sur la droite critique.

Le critère de Beurling et Nyman [Beu55] établit un lien entre l'hypothèse de Riemann pour la fonction ζ de Riemann et la densité de certains sous-espaces fonctionnels engendrés par des contractées de la fonction partie fractionnaire. Il a été précisé par Báez-Duarte, Balazard, Burnol et Saias dans plusieurs articles parus entre 1998 et 2003 [BD03, BS00, BDBLS00, Bur02]. Les articles [0] et [3] principalement issus de la thèse ont permis de généraliser une partie de ces travaux aux fonctions de la classe de Selberg. Le critère de Beurling et Nyman repose sur une correspondance, via la transformation de Mellin, entre l'espace $L^2(\mathbb{R})$ et un espace de Hardy, entre la fonction partie fractionnaire et la fonction zêta de Riemann. Le déplacement du problème dans les espaces de Hardy permet d'utiliser de nombreux outils d'analyse fonctionnelle. Une des difficultés de l'adaptation du critère de Beurling et Nyman à la classe de Selberg réside en l'étude des fonctions complémentaires qui sont les analogues de la fonction partie fractionnaire pour zêta. L'article [2] est consacré à une telle étude. Dans [4], c'est l'aspect séquentiel, étudié initialement pour la fonction zêta de Riemann par Báez-Duarte, de ce problème, qui est développé. On trouve une suite d'un espace fonctionnel qui, sous l'hypothèse de Riemann pour une fonction F de la classe de Selberg, converge vers la fonction indicatrice de l'intervalle $[0, 1]$ en assurant une certaine vitesse de convergence. Les aspects hilbertiens de ce critère ont été développés dans [1] où l'on obtient une majoration de la vitesse de convergence. Ce dernier travail utilise la structure euclidienne de $L^2(0, 1)$ et l'action de certains opérateurs, adaptant ainsi le travail de Burnol. Dans [5], travail en collaboration avec Michel Balazard ultérieur à la thèse, nous avons poursuivi l'étude séquentielle du critère de Báez-Duarte pour la fonction zêta de Riemann en améliorant les majorations connues.

Ces travaux faisaient fortement appel à l'outil classique en théorie analytique des nombres qu'est l'analyse complexe ainsi qu'à l'analyse fonctionnelle. Ils ont aussi constitué une première approche des interactions entre analyse de Fourier et théorie des nombres à travers notamment l'utilisation des transformations de Fourier et de Mellin et l'évaluation de fonctions oscillantes et de sommes d'exponentielles. Cette thématique a aussi été développée dans les travaux ultérieurs que nous allons présenter ici.

Dans ce mémoire, nous présentons les travaux [9, 6, 8, 10, 11]. Le premier de ces articles [9] a été écrit en collaboration avec Bahman Saffari, Harold S. Shapiro et Gérald Tenenbaum. Le second [6] est le

fruit d'une collaboration avec Harald A. Helfgott, le troisième [8] provient d'une collaboration avec Alain Plagne et le dernier [11] avec Pablo Candela. L'article [10] n'est pas issu d'une collaboration. Hormis [9], tous ces travaux sont consacrés à l'étude des structures additives d'ensembles, ce qui constitue ce que l'on appelle aujourd'hui la combinatoire additive. Notons que l'analyse de Fourier joue un rôle important dans ces travaux, c'est en particulier un outil essentiel dans [6] et [11]. C'est pourquoi nous avons choisi d'inclure [9], consacré à un principe d'incertitude pour les familles de $L^2(\mathbb{R})$, dans ce mémoire.

Notons que [7] et [5], écrits respectivement en collaboration avec Szilard S. Révész et Michel Balazard, auraient également pu être insérés dans ce mémoire. L'article [7] fournit en effet un théorème taubérien qui donne des informations asymptotiques sur une fonction dont la transformée de Laplace vérifie certaines propriétés. Il améliore le théorème taubérien classique de Wiener-Ikehara. Notre amélioration est double : nous affaiblissons les hypothèses nécessaires à l'obtention d'une estimation de la transformée de Laplace d'une fonction et nous donnons un terme d'erreur explicite. Dans [5], on précise le critère de Báez-Duarte pour l'hypothèse de Riemann [BD03]. Cet article fait appel à des techniques fines d'analyse complexe empruntées à [Sou09] et utilise intensivement la transformée de Mellin. Il s'agit donc aussi dans ces deux travaux d'extraire des informations sur un objet mathématique à partir d'éléments connus sur sa transformée (de Fourier, de Laplace ou de Mellin). Toutefois, [7] et [5] sont plus proches de nos travaux antérieurs [0-4] et en particulier des méthodes d'analyse complexe alors utilisées et il nous a semblé plus cohérent de nous restreindre dans ce mémoire à des thématiques plus homogènes.

L'article [12] écrit en collaboration avec Pablo Candela et Diego González-Sánchez, se situe pour sa part bien dans la thématique de la combinatoire additive puisque l'on obtient un théorème de Plünnecke-Ruzsa dans un groupe abélien compact. Il nous a néanmoins semblé que son insertion serait un retour trop précoce sur ce travail que nous venons d'achever.

Ce mémoire portera donc essentiellement sur la recherche de structures additives dans des ensembles et sur l'utilisation de la transformée de Fourier dans ce contexte. Le passage d'un contexte discret à un contexte continu, et réciproquement, sera aussi un thème récurrent de cette présentation.

Dans un premier temps, nous nous sommes intéressés à la structure des ensembles sans solution à une équation linéaire donnée. Ce type de problème est fréquemment abordé dans la littérature. La recherche d'ensemble sans somme (sans solution à l'équation $x + y = z$), sans progression arithmétique (sans solution à l'équation $x + y = 2z$) ou d'ensembles de Sidon (sans solution à l'équation $x + y = z + t$) en sont des exemples bien connus.

Dans [Ruz93] et [Ruz95], Ruzsa mène une étude générale des ensembles d'entiers sans solution à une équation linéaire de la forme $a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$, où $a_1, a_2, \cdots, a_k$ et b sont des entiers fixés. Il distingue deux types d'équations : les équations invariantes pour lesquelles l'ensemble des solutions est invariant par multiplication et par translation par un entier (donc $b = 0 = \sum_{i=1}^{k} a_i$) et les autres équations qui seront dites non-invariantes. Les équations invariantes possèdent dans tout ensemble non vide des solutions que l'on appelera « triviales » (par exemple (x, x, x) pour l'équation $x + y = 2z$ ou (x, y, y, x) pour l'équation $x + y = z + t$) et Ruzsa montre qu'il n'existe pas d'ensemble de densité positive sans solution non triviale à une équation linéaire invariante alors qu'un tel ensemble existe pour une équation non invariante. Son résultat pour les équations invariantes généralise le théorème de Roth [Rot53] qui traitait de l'équation $x + y = 2z$.

Dans [6,8], nous nous sommes intéressés aux équations de la forme $x + y = kz$ avec k un entier supérieur à 1.

Le cas $k = 2$ qui correspond aux ensembles sans progression arithmétique non triviale, est la seule équation invariante de cette forme. C'est à cette équation que nous nous sommes intéressés dans [6]. Nous présentons ce travail au chapitre 2 en étudiant les sous-ensembles de nombres premiers sans progression arithmétique non triviale, prolongeant ainsi le travail de Green dans [Gre05]. Notons que Łaba

et Pramanik donnent dans [LaP09] un analogue continu des résultats de Green pour les ensembles de mesure de Lebesgue nulle. Ce dernier travail fait intervenir des hypothèses sur la dimension de Hausdorff et la dimension de Fourier des sous-ensembles de réels étudiés. Les techniques utilisées dans le contexte discret par Green et dans le contexte continu par Łaba et Pramanik sont similaires et l'analyse de Fourier joue dans ces études ainsi que dans [6] un rôle essentiel. Dans [6], nous avons utilisé des méthodes de crible et un théorème de tranfert lié à l'analyse de Fourier pour améliorer quantitativement de résultat de Green. La difficulté principale lorsque l'on travaille avec les nombres premiers est que cet ensemble est de densité nulle. Il faut alors utiliser le caractère aléatoire de la distribution des nombres premiers (en dehors des obstructions liées à leur définition) pour pouvoir transposer le résultat sur les ensemble de densité positive à ce contexte.

Le chapitre 3 est consacré aux équations $x+y = kz$ avec $k \geq 3$ donc à des équations non invariantes. Pour ce type d'équations, on peut trouver des ensembles sans solution de mesure de Lebesgue positive si on considère des ensembles de réels et de densité positive si on considère des ensembles bornés d'entiers. Pour $k \geq 4$, c'est le passage du cadre continu au cadre discret qui a permis de déterminer la structure des ensembles d'entiers maximaux sans solution [CG96, BHK$^+$05]. Dans le cas $k = 3$ en revanche, il y a une rupture entre le cadre discret, où l'ensemble des nombres impairs constitue un ensemble de densité maximale sans solution [CG97], et le cadre continu comme l'ont montré Matolcsi et Ruzsa [MR13]. Nous exposons en particulier dans le chapitre 3 la méthode (issue de [8]) qui a permis la détermination des ensembles de réels maximaux sans solution à l'équation $x + y = 3z$. Les méthodes employées dans ce chapitre sont essentiellement combinatoires. L'évaluation de la taille des ensembles sommes y est utilisée et c'est ce qui a motivé les recherches présentées aux chapitres 4 et 5.

Étant donnés deux sous-ensembles A et B d'un groupe additif, on peut définir l'ensemble somme $A + B$ comme l'ensemble des éléments du groupe qui s'écrivent comme somme d'un élément de A et d'un élément de B. Si A et B sont des intervalles de $\mathbb{R}$, alors la mesure de l'ensemble de Lebesgue de $A + B$ est la somme des mesures de A et B. C'est aussi vrai (en remplaçant la mesure de Lebesgue par la mesure de Haar sur $\mathbb{T}$) si A et B sont des intervalles de $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ lorsque la somme des mesures de Haar de A et B ne dépasse pas 1. Pour des sous-ensembles quelconques de $\mathbb{R}$ ou $\mathbb{T}$, la somme des mesures de A et B devient un minorant de la mesure de $A + B$ (pourvu que $A + B$ ne couvre pas le cercle si A et B sont des sous-ensembles de $\mathbb{T}$). Les chapitres 4 et 5 sont consacrés à la caractérisation des sous-ensembles de $\mathbb{R}$ ou $\mathbb{T}$ pour lesquels la mesure de $A + B$ est proche du minimum donné par la somme des mesures de A et B. Les résultats obtenus poursuivent le travail de Ruzsa dans [Ruz91] et s'inscrivent dans la tradition des théorèmes inverses en combinatoire additive. On donne en particulier au chapitre 4 des analogues continus pour des ensembles de réels des théorèmes $3k - 4$ de Freiman, Bardaji-Grynkiewicz, Stanchescu et Lev-Smeliansky [Fre59, Fre62, Fre09, BG10, Sta96, LS95] ainsi que d'autres résultats qui n'ont pas encore d'analogues discrets dans $\mathbb{Z}$. Ces résultats sont issus de [10]. Notons que dans un travail en cours en collaboration avec Paul Péringuey, nous établissons les analogues discrets de ces résultats.

Au chapitre 5, consacré aux résultats de [11], nous démontrons un analogue continu pour des sous-ensembles de $\mathbb{T}$ des résultats de Serra-Zémor [SZ09] et Grynkiewicz [Gry13] et donnons deux applications aux structures des ensembles de réels de constante de doublement proche de 3 et à la description des sous-ensembles de $\mathbb{T}$ sans solution à l'équation $x + y = 3z$. Notons que dans ce dernier chapitre encore, l'analyse de Fourier joue un rôle essentiel.

Expliquons ici brièvement le rôle de l'analyse de Fourier dans les problèmes de combinatoire additive que nous avons abordés.

La transformée de Fourier permet d'abord, grâce aux relations d'orthogonalité entre caractères, de détecter des relation linéaires. Ainsi, au chapitre 2, le nombre de progressions arithmétiques dans un

ensemble A peut-il s'exprimer en fonction d'une somme sur les coefficients de Fourier de la fonction indicatrice de A.

Ensuite, les coefficients de Fourier servent de mesure d'uniformité. La philosophie générale est que si les coefficients de Fourier en dehors de 0 d'une fonction indicatrice sont petits alors l'ensemble concerné se comporte en terme de propriétés additives comme on l'attendrait en moyenne d'un ensemble de même taille. Tout ceci est formalisé au chapitre 2. Alternativement, un grand coefficient de Fourier traduit une concentration sur une progression arithmétique et révèle donc une certaine structure, idée utilisée aux chapitres 2 et 5.

Enfin, $A+B$ est le support de $\mathbf{1}_A * \mathbf{1}_B$ et la formule $\widehat{f * g} = \hat{f}\hat{g}$ fait qu'il est souvent plus facile de se placer du côté des transformées de Fourier pour étudier les convolutions donc les sommes d'ensembles.

La transformée de Fourier permet de révéler des structures additives. Il existe donc un lien fort entre la taille d'une transformée de Fourier et la physiologie de la fonction d'origine. Des résultats appelés ≪ principes d'incertitude ≫ permettent de mettre ce type de liens en lumière. Par exemple un résultat de Hardy stipule que si pour une fonction f de $L^2(\mathbb{R})$ non nulle, $\hat{f}$ est négligeable en l'infini devant $e^{-x^2/2}$ alors f ne peut l'être.

Au chapitre 1 qui présente les résultats de [9], on donne un principe d'incertitude pour une famille $\{g_n\}_{n\in\mathbb{Z}}$ de fonctions de $L^2(\mathbb{R})$. Ce principe, dû à Shapiro, montre que la majoration uniforme simultanée de $\{g_n\}_{n\in\mathbb{Z}}$ et $\{\widehat{g}_n\}_{n\in\mathbb{Z}}$ par une fonction de $L^2(\mathbb{R})$ force la compacité de la famille. On discute des limites et de l'optimalité de ce résultat en tentant de répondre à la question suivante : jusqu'à quel point une majoration uniforme simultanée de $\{g_n\}_{n\in\mathbb{Z}}$ et $\{\widehat{g}_n\}_{n\in\mathbb{Z}}$ peut-elle s'approcher de $L^2(\mathbb{R})$ lorsque $\{g_n\}_{n\in\mathbb{Z}}$ est une base orthonormale ou une famille orthonormale infinie de $L^2(\mathbb{R})$?

Par soucis de clarté, nous avons choisi de numéroter les références aux articles auquels nous avons contribué et citons les autres références bibliographiques par les initiales du ou des auteurs, éventuellement complétées par une date. De même, les théorèmes présentant des résultats auquels nous avons contribué seront numérotés en numérotation latine, les autres résultats sont numérotés par l'écriture en chiffres arabes usuelle. À chaque début de chapitre, les noms des mathématiciens ayant contribué aux résultats présentés dans le chapitre et les publications associées sont cités. Il est bien évident que le ≪ nous ≫ employé désigne le collectif d'auteurs précités.

Chapitre 1

Un principe d'incertitude pour les familles de $L^2(\mathbb{R})$

Ce chapitre porte sur des travaux réalisés en collaboration avec Bahman Saffari, Harold S. Shapiro et Gérald Tenenbaum. Ils ont donné lieu à la publication [9].

Un principe d'incertitude en analyse harmonique est un résultat qui énonce, pour une fonction f de $L^2(\mathbb{R})$ non nulle, l'impossibilité que f et $\widehat{f}$ soient simultanément petites, ce dernier terme restant à préciser. Par exemple, f et $\widehat{f}$ ne peuvent être simultanément à support compact. Plus précisément, Hardy a montré que f et $\widehat{f}$ ne peuvent être toutes deux négligeables devant $e^{-x^2/2}$ à l'infini. Il existe de nombreux résultats de ce type et le lecteur pourra en consulter un panorama dans [FS97] ou [HJ94].

Le type de principe d'incertitude auquel on s'est intéressé dans [9] ne concerne pas une unique fonction mais une classe de fonctions. Nous avons montré qu'on ne peut dominer f et $\widehat{f}$ à l'infini par une fonction de carré intégrable uniformément pour toutes les fonctions d'une famille orthonormale infinie. Ce principe avait fait l'objet d'une note de travail non publiée de Shapiro datée de 1991 dans laquelle Shapiro a énoncé et démontré le résultat suivant.

Théorème 1 (Shapiro) *Soit $\{g_n\}_{n=1}^{\infty}$ une famille orthonormale infinie de $L^2(\mathbb{R})$. Alors il n'existe pas de fonction dans $L^2(\mathbb{R})$ dominant à la fois les g_n et leurs transformées de Fourier*

$$\widehat{g_n}(t) := \int_{\mathbb{R}} g_n(x) e^{-itx} \mathrm{d}x.$$

Le résultat de Shapiro est en fait plus précis, ll affirme que pour toute suite orthonormale $\{g_n\}_n$ infinie de $L^2(\mathbb{R})$, on a

$$\lim_{\xi\to\infty} \sup_{n\in\mathbb{N}} \int_{|x|>\xi} \left(|g_n(x)|^2 + |\widehat{g_n}(x)|^2\right) \mathrm{d}x > 0. \tag{1.1}$$

La démonstration de ce résultat repose sur une variante du théorème de Fréchet-Kolmogorov qui caractérise la compacité relative d'une famille de fonctions de $L^2(\mathbb{R})$. L'idée principale est que la majoration des fonctions et de leurs tranformées de Fourier implique la compacité de la famille considérée.

Une version quantitative du théorème de Shapiro est donnée dans [JP07] puis simplifiée et généralisée en dimension finie quelconque dans [Mal10].

L'article [9] a fourni la première publication d'une démonstration du principe d'incertitude de Shapiro. Il a également répondu à plusieurs questions posées par Shapiro dans sa note non publiée en reprenant sa construction de bases orthonormales de $L^2(\mathbb{R})$ à partir de la base $\{e^{2i\pi nx}\}_{n\in\mathbb{Z}}$ de $L^2(\mathbb{T})$ et d'une bijection strictement croissante de $\mathbb{R}$ sur $]0,1[$.

L'une de ces questions est la suivante : étant donnée une famille orthonormale infinie, dans quelle mesure peut-on donner une majoration uniforme des g_n et des $\widehat{g_n}$ par des fonctions proches de $L^2(\mathbb{R})$, c'est à dire dont la décroissance en l'infini est la plus grande possible ?

1.1 Construction d'une famille de bases orthonormales de $L^2(\mathbb{R})$

Si $F \in \mathcal{C}^1(\mathbb{R},]0,1[)$ (F continûment dérivable) est une bijection strictement croissante, l'image $\{g_n\}_{n\in\mathbb{Z}}$ par F de la base orthonormale $\{e^{2\pi inx}\}_{n\in\mathbb{Z}}$, donnée par

$$g_n(x) := e^{2\pi inF(x)}\sqrt{F'(x)} \qquad (x \in \mathbb{R}), \tag{1.2}$$

est une base orthonormale de $L^2(\mathbb{R})$. L'orthonormalité de cette famille découle immédiatement de celle de la base $\{e^{2i\pi nx}\}_{n\in\mathbb{Z}}$ de $L^2(\mathbb{T})$ dont elle est issue. Le caractère complet de la famille se vérifie simplement en considérant un vecteur de $L^2(\mathbb{R})$ orthogonal à tous les vecteurs g_n et en utilisant la complétude de la base $\{e^{2i\pi nx}\}_{n\in\mathbb{Z}}$ de $L^2(\mathbb{T})$ via un changement de variable. Cette construction de base de $L^2(\mathbb{R})$ était proposée dans la note de Shapiro.
Une telle famille vérifie pour tout $n \in \mathbb{Z}$

$$|g_n(x)| = \sqrt{F'(x)},$$

donc la famille $\{g_n\}_{n\in\mathbb{Z}}$ est majorée uniformément par $\sqrt{F'(x)}$, une fonction de $L^2(\mathbb{R})$. Le principe d'incertitude de Shapiro assure qu'il ne peut exister une aussi bonne majoration uniforme pour la famille $\{\widehat{g_n}\}_{n\in\mathbb{Z}}$ mais il est légitime de s'interroger sur la décroissance uniforme maximale que l'on peut obtenir pour cette dernière famille.

Pour cela, examinons les fonctions $\widehat{g_n}$. Notons que

$$\widehat{g_n}(t) := \int_{\mathbb{R}} g_n(x)e^{-itx}\mathrm{d}x = \int_{\mathbb{R}} \sqrt{F'(x)}e^{i\varphi_{n,t}(x)}\mathrm{d}x$$

avec $\varphi_{n,t}(x) = 2\pi nF(x) - tx$. Fixons a un réel et posons $\Phi_{n,t}(x) = \int_a^x e^{i\varphi_{n,t}(u)}\mathrm{d}u$. Si $F \in C^2(]a,b[)$, une simple intégration par parties permet de montrer

$$\begin{aligned}\int_a^b \sqrt{F'(x)}e^{i\varphi_{n,t}(x)}\mathrm{d}x &= \int_a^b \sqrt{F'(x)}\mathrm{d}\Phi_{n,t}(x)\\ &= \sqrt{F'(b)}\Phi_{n,t}(b) - \int_a^b \Phi_{n,t}(x)\frac{F''(x)}{2\sqrt{F'(x)}}\mathrm{d}x.\end{aligned}$$

En supposant de plus que F'' est de signe fixe sur $]a,b[$, on obtient

$$\int_a^b \sqrt{F'(x)}e^{i\varphi_{n,t}(x)}\mathrm{d}x \ll \max\left(\sqrt{F'(b)}, \sqrt{F'(a)}\right)\sup_{]a,b[}|\Phi_{n,t}(x)|. \tag{1.3}$$

Nous nous sommes donc ramenés à la recherche d'une majoration de l'intégrale oscillante $|\Phi_{n,t}|$. Rappelons ici des estimations classiques d'intégrales oscillantes (voir Théorèmes I.6.2 et I.6.3 de [Ten95]). Si $f \in \mathcal{C}^2(]a,b[,\mathbb{R})$ (deux fois continûment dérivable) et si f'' est de signe constant sur $]a,b[$, alors

$$\left|\int_a^b e^{2\pi if(x)}\mathrm{d}x\right| \leq \min\left(\frac{1}{\pi\inf_{x\in]a,b[}|f'(x)|}, \frac{4}{\sqrt{\pi\inf_{x\in]a,b[}|f''(x)|}}\right). \tag{1.4}$$

Plaçons nous sur un intervalle $]a,b[$ sur lequel F'' est de signe fixe. La majoration (1.4) implique immédiatement

$$\sup_{x\in]a,b[} |\Phi_{n,t}(x)| \ll \min\left(\frac{1}{\inf_{x\in]a,b[}|2\pi nF'(x)-t|}, \frac{1}{\sqrt{\inf_{x\in]a,b[}(2\pi n|F''(x)|)}}\right). \tag{1.5}$$

Après ces considérations générales, nous pouvons examiner quelques cas particuliers.

1.2 Premier exemple : une décroissance unilatérale exponentielle

Nous avons obtenu dans [9] le résultat suivant.

Théorème I (de Roton, Saffari, Shapiro, Tenenbaum) *Il existe une base orthonormale* $\{g_n\}_{n\in\mathbb{Z}}$ *de* $L^2(\mathbb{R})$ *pour laquelle on a*

$$|g_n(x)| = e^{-|x|/2} \qquad (x\in\mathbb{R})$$

et

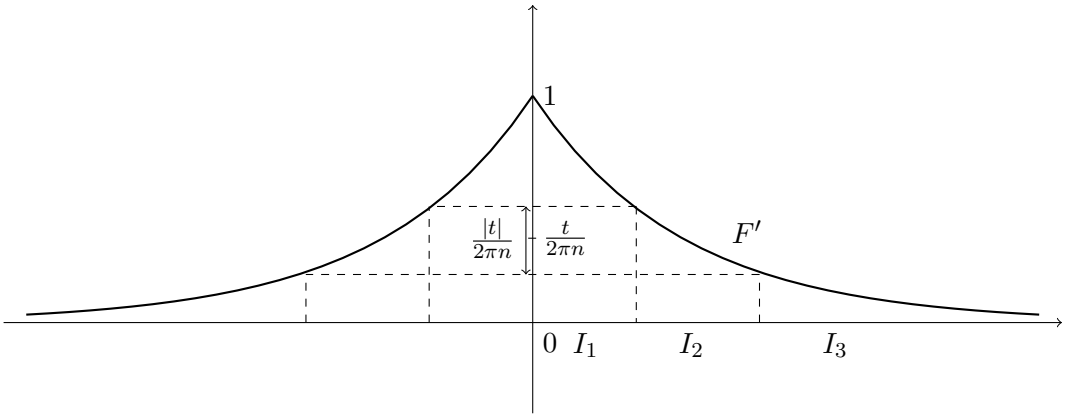
$$\sup_{n\in\mathbb{Z}} |\widehat{g_n}(t)| \ll 1/\sqrt{1+|t|} \qquad (t\in\mathbb{R}). \tag{1.6}$$

Les fonctions g_n sont définies par la formule (1.2) à partir de la fonction $F(x)=\int_{-\infty}^x e^{-|v|}dv$. La fonction F est infiniment dérivable sur $\mathbb{R}^*$ et ses dérivées sur cet ensemble vérifient $F'(x)=e^{-|x|}=|F''(x)|$. De plus F'' est de signe fixe sur chacun des deux intervalles $\mathbb{R}^{+*}$ et $\mathbb{R}^{-*}$. Plaçons nous sur l'un de ces deux intervalles et notons $]a,b[$ l'intervalle choisi.

Si t et n sont de signes opposés, alors $\inf_{x\in]a,b[}|2\pi nF'(x)-t|\geq|t|$ et $\sup_{x\in]a,b[}|\Phi_{n,t}(x)|\ll 1/|t|$ par (1.5).
Sinon, comme $F'=|F''|$ sur $]a,b[$, l'intervalle $]a,b[$ peut être divisé en au plus trois intervalles I_1, I_2, I_3 pour lesquels au moins l'une des deux minorations $\inf_{x\in I_k}|2\pi nF'(x)-t|\geq|t|/2$ ou $\inf_{x\in I_k}|2\pi nF''(x)|>|t|/2$ est vérifiée. Les majorations (1.5) et (1.3) permettent donc d'obtenir successivement les estimations suivantes.

$$\sup_{x\in\mathbb{R}^*}|\Phi_{n,t}(x)|\ll 1/\sqrt{t} \text{ pour } t\geq 1, \quad \text{et} \quad \widehat{g_n}(t)\ll\frac{1}{\sqrt{1+|t|}} \text{ pour } t\in\mathbb{R}.$$

La figure suivante illustre ce cas particulier.



1.3 Décroissance unilatérale arbitraire

La méthode employée au paragraphe précédent permet de généraliser le résultat obtenu en démontrant l'existence d'une base orthonormale de $L^2(\mathbb{R})$ dominée à une constante multiplicative près par une fonction arbitraire de $L^2(\mathbb{R})$ et satisfaisant néanmoins (1.6).

Théorème II (de Roton, Saffari, Shapiro, Tenenbaum) *Soit G une fonction positive de $L^2(\mathbb{R})$ telle que la borne inférieure de G sur tout compact de $\mathbb{R}$ soit non nulle. Il existe une base orthonormale $\{g_n\}_{n\in\mathbb{Z}}$ satisfaisant*

$$\sup_{n\in\mathbb{Z}} |g_n(x)| \ll G(x) \qquad (x \in \mathbb{R})$$

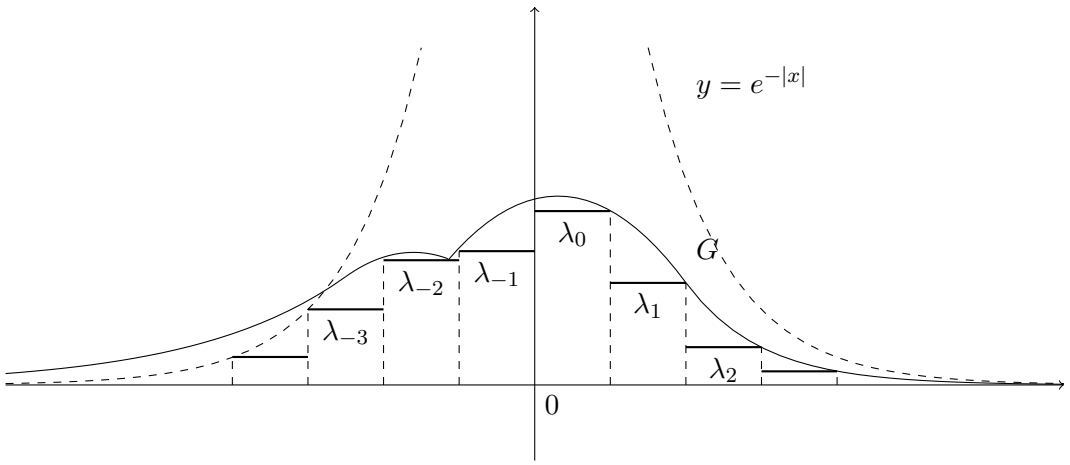
et

$$\sup_{n\in\mathbb{Z}} |\widehat{g_n}(t)| \ll 1/\sqrt{1+|t|} \qquad (t \in \mathbb{R}).$$

Pour obtenir ce résultat, posons

$$\lambda_m := \min\Big(\inf_{m\le x<m+1} G(x), e^{-|m|}\Big) \quad (m \in \mathbb{Z}), \quad L := \sum_{m\in\mathbb{Z}} \lambda_m^2$$

(la figure suivante illustre cette définition).



Désignant par w la fonction continue définie par

$$w(x) := \min(1, x^+)^2 \quad \text{où} \quad x^+ = \max(x, 0),$$

nous choisissons

$$F(x) := \frac{1}{L}\sum_{m\in\mathbb{Z}} \lambda_m^2 w(x-m) \quad (x \in \mathbb{R}).$$

Ainsi, F est une bijection strictement croissante de $\mathbb{R}$ sur $]0,1[$, de classe C^2 sur $\mathbb{R}\setminus\mathbb{Z}$. La suite $\{g_n\}_{n\in\mathbb{Z}}$ définie par

$$g_n(x) := \begin{cases} e^{2\pi i n F(x)}\sqrt{F'(x)} & (x \in \mathbb{R}\setminus\mathbb{Z}), \\ 0 & (x \in \mathbb{Z}) \end{cases}$$

est une base orthonormale de $L^2(\mathbb{R})$. De plus, pour m, $n \in \mathbb{Z}$, $m \le x < m+1$, on a

$$|g_n(x)| \le \sqrt{F'(x)} = \lambda_m\sqrt{2(x-m)/L} \ll \lambda_m \ll G(x).$$

D'autre part, un calcul simple permet de montrer :

$$|\widehat{g_n}(t)| \leq \sqrt{2/L} \sum_{m\in\mathbb{Z}} \lambda_m \left| \int_0^1 e^{i\varphi_{m,n}(t,v)} \sqrt{v} dv \right|$$

où l'on a posé

$$\varphi_{m,n}(t,v) := 2\pi n \frac{\lambda_m^2}{L} v^2 - vt.$$

Un raisonnement similaire à celui du paragraphe précédent permet de montrer

$$\left| \int_0^1 e^{i\varphi_{m,n}(t,v)} \sqrt{v} dv \right| \ll \frac{1}{\sqrt{|t|+1}}$$

et donc $|\widehat{g_n}(t)| \ll 1/\sqrt{|t|+1}$.

1.4 Optimalité de la borne $1/\sqrt{|t|}$

Dans les deux exemples précédents, on montrait pour g_n définis par (1.2) et certains choix de F, que $|\widehat{g_n}(t)| \ll 1/\sqrt{|t|+1}$.
Notons d'abord que cette majoration n'est pas valable pour toute fonction F, comme le montre le choix de $F(x) = \frac{1}{\pi}\int_{-\infty}^{x} \frac{dv}{1+v^2} = \frac{1}{2} + \frac{\arctan x}{\pi}$ pour lequel on obtient

$$\widehat{g_n}(2n) = \frac{(-1)^n \Gamma(1/3)}{2^{1/3}\sqrt{\pi} 3^{1/6} n^{1/3}} + O\Big(\frac{1}{\sqrt{n}}\Big) \qquad (n \geq 1).$$

On comprend ici aisément ce qui limite la décroissance de $|\widehat{g_n}(2n)|$. En effet, on a

$$|2\pi n F'(x) - 2n| = \frac{2|n|x^2}{1+x^2} \leq 2|n|x^2$$

et

$$|2\pi n F''(x)| = \frac{4|nx|}{(1+x^2)^2} \leq 4|nx|$$

donc ces deux fonctions de x sont simultanément petites au voisinage de 0. La régularité de la fonction F et l'égalité $|2\pi n F^{(3)}(0)| = 4|n|$ permettent tout de même d'avoir une majoration en $1/n^{1/3}$ pour $\widehat{g_n}(2n)$.

D'autre part, nous montrons dans [9] que la majoration $|\widehat{g_n}(t)| \ll 1/\sqrt{|t|+1}$ ne peut être améliorée pour un large choix de fonction F.

Théorème III (de Roton, Saffari, Shapiro, Tenenbaum) *Soit $F \in \mathbb{C}^2(\mathbb{R},]0,1[)$ une bijection strictement croissante. Supposons que F' est strictement positive sur $\mathbb{R}$, que F'' ne s'annule qu'un nombre fini de fois et qu'il existe $x_0 > 0$, $\eta > 0$, tels que, pour tout $x \in \mathbb{R} \setminus [-x_0, x_0]$, on ait*

$$F(x+h) = F(x) + hF'(x) + \frac{1}{2}h^2 F''(x) + O_x(|h|^{2+\eta}) \qquad (|h| \leq 1).$$

Alors, il existe une suite $\{t_n\}_{n=1}^{\infty} \in (\mathbb{R}^+)^{\mathbb{N}^*}$ telle que $\lim_{n\to\infty} t_n = \infty$ et

$$\limsup_{n\to\infty} \sqrt{t_n}\, \big|\widehat{g_n}(t_n)\big| > 0.$$

La démonstration de ce résultat repose sur des arguments similaires à ceux que nous avons employés dans les paragraphes précédents. Sous les hypothèses du théorème III, on peut exhiber une bijection θ d'un intervalle $]-\infty, u]$ sur un intervalle $[v, +\infty[$ telle que pour tout $z \in]-\infty, u]$, $F'(z) = F'(\theta(z))$ et $\forall x \in]u, v[,\ F'(x) > \sup_{\mathbb{R}\setminus]u,v[} F'$.

Soit $z < u$ un réel suffisamment petit. Nous posons

$$t_n = t_n(z) := 2\pi n F'(z) \qquad (n \geq 1),$$

de sorte que

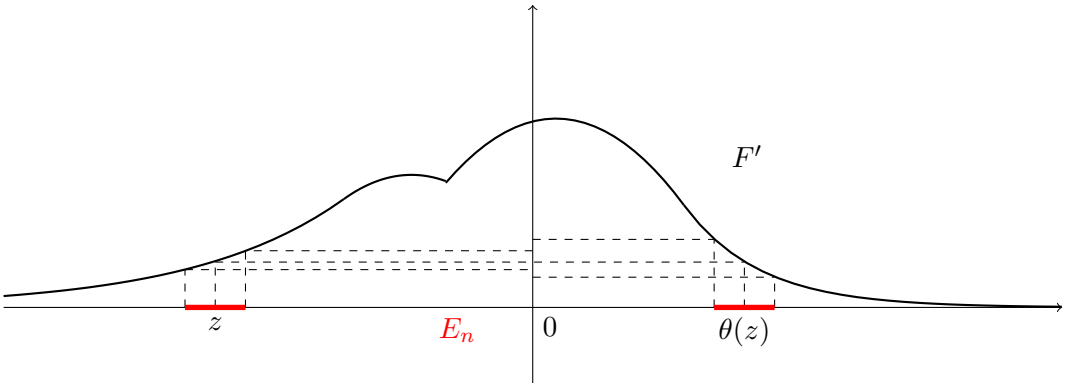
$$\widehat{g_n}(t_n) = \int_{\mathbb{R}} e^{i\varphi_n(x)} \sqrt{F'(x)} dx,$$

avec $\varphi_n(x) := 2\pi n\{F(x) - xF'(z)\}$ $(x \in \mathbb{R})$ et donc

$$\varphi_n'(x) = 2\pi n\{F'(x) - F'(z)\} \qquad (x \in \mathbb{R}).$$

Soit $\varepsilon \in]0, 1/2[$. Posons $\delta_n := n^{-(1/2-\epsilon)}$ et

$$E_n = [z - \delta_n, z + \delta_n] \cup [\theta(z) - \delta_n, \theta(z) + \delta_n].$$



Pour n suffisamment grand, nous obtenons $|\varphi_n'(x)| > 2\pi C(z) n\delta_n$ pour $x \notin E_n$ et donc pour tout intervalle $]a, b[$ de $\mathbb{R} \setminus E_n$ sur lequel F'' ne s'annule pas, on a

$$\Phi_n(x) := \int_a^x e^{i\varphi_n(t)} dt \ll \frac{1}{n\delta_n} = \frac{1}{n^{1/2+\epsilon}} \qquad (a \leq x \leq b).$$

Comme F'' ne possède qu'un nombre fini de changements de signe, il s'ensuit par (1.3) que la contribution du domaine $\mathbb{R} \setminus E_n$ à l'intégrale $\widehat{g_n}(t_n)$ est $\ll n^{-1/2-\epsilon}$.

Il reste alors à évaluer la contribution des deux intervalles composant E_n. Pour $x \in \mathbb{R}$, posons

$$I_n(x) := \int_{-\delta_n}^{\delta_n} e^{i\varphi_n(x+h)} \sqrt{F'(x+h)} dh.$$

L'écriture du développement asymptotique de F au voisinage de z suivie d'un changement de variable dans l'intégrale permettent de montrer

$$I_n(z) = \Big\{1 + O\Big(\frac{1}{n^\varepsilon}\Big)\Big\} \sqrt{\frac{F'(z)}{nF''(z)}} e^{i\varphi_n(z) + i\pi/4}$$

et

$$I_n(\theta(z)) = \Big\{1 + O\Big(\frac{1}{n^\varepsilon}\Big)\Big\} \sqrt{\frac{F'(z)}{nF''(\theta(z))}} e^{i\varphi_n(z) - i\pi/4}.$$

La majoration annoncée dans le Théorème III découle alors de la non annulation de la limite de la somme de ces deux contributions lorsque n tend vers l'infini.

Le théorème III pourrait amener à l'idée qu'une majoration de la forme $\left|\widehat{g_n}(t_n)\right| \ll 1/\sqrt{1+|t|}$ est optimale pour toute famille orthonormale $\{g_n\}_{n\in\mathbb{Z}}$ de $L^2(\mathbb{R})$. L'exemple suivant prouve qu'il n'en est rien.
Considérons la fonction $L(x) := \max(1, \sqrt{\log x})$. Il existe une suite $\{\lambda_n\}_{n=1}^{\infty}$ d'éléments de $[1, \infty[$ telle que la suite de fonctions

$$g_n(x) := \frac{\mathbf{1}_{[\lambda_n, \lambda_{n+1}[}(x)}{\sqrt{x}L(x)} \qquad (n \geq 1)$$

soit une famille orthonormale de $L^2(\mathbb{R})$. De plus

$$\sup_n |g_n(x)| \leq u(x) = \frac{1}{\sqrt{x}L(x)}$$

et on peut montrer

$$|\widehat{g_n}(t)| \ll \begin{cases} \frac{1}{t} & \text{si } t \geq 1 \\ \frac{1}{\sqrt{t}L(1/t)} & \text{si } 0 < t < 1 \end{cases}.$$

Ainsi, nous avons construit une famille orthonormale infinie de $L^2(\mathbb{R})$ vérifiant

$$\sup_n |g_n(x)| + \sup_n |\widehat{g}_n(x)| \ll u(x) + \frac{u(1/x)}{x} \qquad (x > 0).$$

Cet exemple montre que la « barrière » en $1/\sqrt{t}$ pour la majoration uniforme des $\left|\widehat{g_n}\right|$ peut être dépassée. De plus, un large choix de fonction L à décroissance lente permettrait d'obtenir un résultat identique. Notons cependant, que nous ne parvenons à franchir cette barrière qu'au prix de plusieurs concessions : la famille ainsi construite n'est pas une base, la majoration uniforme des g_n n'est plus dans $L^2(\mathbb{R})$ et la majoration uniforme des $\left|\widehat{g_n}\right|$ n'est pas de carré intégrable au voisinage de l'origine.

Plusieurs questions demeurent donc : peut-on franchir la « barrière » en $1/\sqrt{t}$ pour la majoration uniforme des $\left|\widehat{g_n}\right|$ tout en garantissant une majoration uniforme des g_n par une fonction de $L^2(\mathbb{R})$? Peut-on construire une base de $L^2(\mathbb{R})$ qui satisfasse à ces contraintes ? Peut-on obtenir sous ces mêmes contraintes une majoration uniforme des $\left|\widehat{g_n}\right|$ de carré intégrable au voisinage de l'origine ?

Chapitre 2

Ensembles d'entiers sans progression arithmétique

Ce chapitre porte sur des travaux réalisés en collaboration avec Harald A. Helfgott. Ils ont donné lieu à la publication [6].

Ce chapitre aborde la question de l'existence de solutions à une équation linéaire donnée dans un ensemble E. Commençons par la question suivante : quand peut-on dire qu'un ensemble E contient des progressions arithmétiques non triviales, autrement dit qu'il existe des élements distincts x et y dans E tels que $(x+y)/2$ est un élément de E ? Dans le cas d'un ensembles d'entiers, Roth a répondu à cette question en 1953 [Rot53] en montrant que tout sous ensemble d'entiers de densité positive contient des progression arithmétiques de longueur trois non triviales. Il montre plus précisément que, pour N assez grand, tout ensemble d'entiers inférieurs à N de cardinal supérieur à $cN/\log\log N$ contient des progressions arithmétiques non triviales. Son résultat quantitatif a été successivement amélioré par Szemeredi [Sze90], Heath-Brown [HB87], Bourgain [Bou99, Bou08], Sanders [San11, San12] et Bloom [Blo12]. On sait à présent que tout sous-ensemble d'entiers inférieurs à N de cardinal supérieur à $cN(\log\log N)^5/\log N$ contient des progressions arithmétiques non triviales. Des recherches récentes de Bloom et Sisask confirment que ce sujet est toujours au centre des intérêts des chercheurs en combinatoire additive.

La question de l'existence de progressions arithmétiques dans un ensemble d'entiers est liée à la conjecture d'Erdös-Turán suivante.

Conjecture 1 (Erdös-Turán) *Soit A un ensemble d'entiers positifs. Si la série $\sum_{n\in A}\frac{1}{n}$ diverge, alors A contient des progressions arithmétiques arbitrairement longues.*

Le théorème de Roth est un premier pas vers cette conjecture dans le cas où A est un ensemble assez dense d'entiers. Étant donné un ensemble E de densité nulle contenant une infinité de progressions arithmétiques, on peut se demander s'il existe un énoncé analogue au théorème de Roth dans E, autrement dit : dans quel type d'ensemble E d'entiers peut-on dire que tout sous-ensemble de E de densité relative positive contient des progressions arithmétiques ?

Van der Corput [vdC39] a démontré en 1939 que l'ensemble des nombres premiers contenait une infinité de progressions arithmétiques. Notons d'autre part que la série des inverses des nombres premiers est bien divergente. C'est en 2005 que Green démontre [Gre05] que dans l'ensemble des nombres premiers un analogue du théorème de Roth existe (rappelons que le nombre de nombres premiers inférieurs à N est de l'ordre de $N/\log N$ et que le meilleur résultat quantitatif du théorème de Roth ne permet pas d'atteindre un tel ensemble). Green donne plus précisément le résultat quantitatif suivant :

pour N assez grand, tout sous- ensemble de nombres premiers inférieurs à N de cardinal supérieur à $c(N/\log N)(\log_5 N/\log_4 N)^{1/2}$ contient des progressions arithmétiques non triviales (ici $\log_k$ désigne le logaritme népérien itéré k fois).

Dans un travail en collaboration avec Harald Helfgott [6], nous avons amélioré ce résultat quantitatif en utilisant des techniques de cribles et d'analyse de Fourier. Nous avons obtenu qu'une cardinalité supérieure à $c(N/\log N)\log_3 N/(\log_2 N)^{1/3}$ était suffisante pour assurer l'existence de progressions arithmétiques.

Théorème IV (Helfgott, de Roton) *Soit A un ensemble de nombres premiers. Alors il existe deux constantes C et N_0 pour lesquelles le fait que la densité relative de $A \cap [1, N]$ dans les nombres premiers plus petits que N soit supérieure à $C \log\log\log N/(\log\log N)^{1/3}$ pour un certain $N \geq N_0$ implique l'existence de progressions arithmétiques non triviales de longueur 3 dans A.*

Depuis [6], Naslund a proposé une amélioration quantitative du théorème de Roth dans les nombres premiers [Nas15]. Dans [Nas15], le changement principal consiste à utiliser la norme L^{2q} de la partie principale de la fonction indicatrice normalisée de A plutôt que sa norme quadratique. Comme il existe très peu de nombres premiers p pour lesquels $p, p + k_1, p + k_2, \cdots p + k_l$ sont simultanément premiers, Naslund obtient une très bonne majoration pour cette norme. Il peut ensuite appliquer un théorème de transfert similaire au théorème V (voir paragraphe 2.2.1) avec une norme L^{2q} au lieu d'une norme quadratique et utiliser un ensemble de Bohr plus grand que celui que nous utilisons.

Citons également les travaux de Henriot [Hen17] dans lesquels l'auteur étend notre résultat de [6] à tout système linéaire invariant de complexité 1.

2.1 Ensembles sans progression arithmétique dans les entiers

2.1.1 La stratégie générale de Roth : une concentration sur les progressions arithmétiques

Pour comprendre les idées mises en oeuvre dans les démonstrations du théorème de Roth dans les nombres premiers, il faut revenir à la démonstration originale de Roth dans les entiers. L'idée initiale consiste à mettre en évidence une concentration sur des progressions arithmétiques. Plus précisément, si N est un grand nombre premier et si A est un sous-ensemble de $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ (on passe rapidement d'un ensemble borné d'entiers à un ensemble de $\mathbb{Z}/N\mathbb{Z}$ modulo quelques précautions techniques) de densité α, on s'attend à ce que le nombre de progressions arithmétiques de longueur 3 dans A soit de l'ordre de $\alpha^3 N^2$. Si en revanche A ne contient que des progressions triviales, alors ce nombre est $|A| = \alpha N$, soit très éloigné du nombre attendu. Cela signifie que l'ensemble A n'est pas « uniforme », selon la terminologie de Tao, mais qu'il est au contraire « structuré ». Roth exprime cette structure en montrant que A se concentre sur une progression arithmétique assez grande. Il considère alors le sous-ensemble de A inclus dans cette progression arithmétique, qui est à nouveau sans progression non triviale mais de densité supérieure à α. On a donc une concentration, autrement dit un gain de densité (*density increment*). Itérant l'argument, la densité de A sur les progressions considérées augmente, ce qui induit une contradiction lorque la densité dépasse 1. Il faut bien sûr garantir que la taille de la progression arithmétique n'a pas trop diminué et c'est ce qui conditionne la taille de α en fonction de N.

La concentration de A sur une grande progression arithmétique lorsque A ne contient pas de progression non triviale, s'obtient en utilisant que la fonction indicatrice de A a un grand coefficient de Fourier. Ce passage utilise l'orthogonalité des caractères et la détection des relations linéaires par l'analyse de Fourier. Nous détaillons ci-dessous cette idée, centrale dans [Gre05] et [6].

2.1.2 Le rôle des coefficients de Fourier

Établissons dès à présent quelques conventions de notation. Dans tout ce chapitre, $e(x)$ désignera $e^{2i\pi x}$ et, si G est un groupe fini et $f : G \to \mathbb{C}$ une application, on notera

$$\mathbb{E}_{n\in G} f(n) = \frac{1}{|G|}\sum_{n\in G} f(n). \tag{2.1}$$

L'orthogonalité des caractères assure pour tout entier ξ

$$\mathbb{E}_{n\in\mathbb{Z}_N} e(-\xi n/N) = \begin{cases} 1 & \text{si } \xi \equiv 0 \bmod N, \\ 0 & \text{sinon.} \end{cases}$$

Définissons à présent une fonctionnelle permettant de compter les progressions de longueur 3. Pour $f, g, h : \mathbb{Z}_N \to \mathbb{C}$ des applications, on définit

$$\Lambda_3(f,g,h) := \mathbb{E}_{n,r\in\mathbb{Z}_N} f(n)g(n+r)h(n+2r) = \frac{1}{N^2}\sum_{n,r\in\mathbb{Z}_N} f(n)g(n+r)h(n+2r).$$

Notons que $N^2\Lambda_3(\mathbf{1}_A, \mathbf{1}_A, \mathbf{1}_A)$ compte le nombre de progressions arithmétiques de longueur 3 dans A. En introduisant pour $f : \mathbb{Z}_N \to \mathbb{C}$, la transformée de Fourier de f définie par

$$\hat{f}(\xi) = \frac{1}{N}\sum_{n\in\mathbb{Z}_N} f(n)e(-n\xi/N) = \mathbb{E}_{n\in\mathbb{Z}_N} f(n)e(-n\xi/N),$$

et en utilisant la formule d'inversion de Fourier et l'orthogonalité des caractères, on obtient

$$\Lambda_3(f,g,h) = \sum_{\xi\in\mathbb{Z}_N} \hat{f}(\xi)\hat{g}(-2\xi)\hat{h}(\xi).$$

En particulier, si A est de densité α, une utilisation de l'inégalité de Cauchy-Schwarz permet de montrer

$$\left|\Lambda_3(\mathbf{1}_A, \mathbf{1}_A, \mathbf{1}_A) - \alpha^3\right| \leq \alpha \sup_{\xi\neq 0} |\hat{\mathbf{1}}_A(\xi)|.$$

Ainsi, si A ne contient que des progressions triviales, alors $\Lambda_3(\mathbf{1}_A, \mathbf{1}_A, \mathbf{1}_A) = \alpha/N$, qui est très petit devant α^3 et donc $\mathbf{1}_A$ doit avoir un gros coefficient de Fourier, ce qui permet de montrer que A se concentre sur une grande progression arithmétique (on parle de biais linéaire).

Notons ici que si les coefficients de Fourier de $\mathbf{1}_A$ en dehors de 0 sont petits, alors A doit contenir un nombre de progressions arithmétiques proche de la valeur attendue. On dit alors que les coefficients de Fourier sont une mesure d'uniformité pour ce problème.

2.1.3 Nombre de progressions arithmétiques : une version quantitative du théorème de Roth

Il existe une version quantitative du théorème de Roth (et des améliorations qui ont suivies) qui donne une minoration du nombre de progressions de longueur 3 dans A en fonction de sa densité. Une telle version a été utilisée dans [Gre05] et [6] pour démontrer le théorème de Roth dans les nombres premiers. L'argument originel est du à Varnavides [Var59]. Ce résultat peut être énoncé comme suit :

Théorème 2 (Roth-Varnavides) *Soient N un grand nombre premier et $\alpha > 0$ un réel. Il existe une constante $h(\alpha)$ strictement positive telle que tout sous-ensemble A de $\mathbb{Z}_N$ de densité α contient au moins $N^2 h(\alpha)$ progressions arithmétiques de longueur 3 distinctes.*

Une valeur explicite de la constante $h(\alpha)$ peut être donnée, elle dépend de la version quantitative du théorème de Roth que l'on utilise. Ainsi, si on utilise le meilleur résultat à notre disposition aujourd'hui [Blo12], on peut prendre $h(\alpha) = c_0\alpha\exp(-c_1/\alpha(\log(1/\alpha))^5)$ où c_0 et c_1 sont des constantes absolues. C'est le résultat antérieur de Bourgain [Bou08] qui avait été utilisé dans [6], c'était à l'époque le meilleur résultat quantitatif disponible. Son remplacement par la borne actuelle aurait permis d'obtenir, sans rien changer à l'argumentation que tout sous ensemble de nombres premiers inférieurs à $N \geq N_0$ de cardinal supérieur à $K(N/\log N)\sqrt{(\log_3 N)^5/\log_2 N}$, où K est une constante absolue, contient des progressions arithmétiques non triviales, ce qui aurait amélioré le résultat de [6].

Le théorème 2 permet, en considérant l'ensemble $A = \{n \in \mathbb{Z}_N \ : \ f(n) \geq \alpha/2\}$ d'obtenir un énoncé un peu plus général donnant une minoration de $\Lambda_3(f,f,f)$ pour toute fonction $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{R}^+$ bornée de moyenne supérieure à $\alpha > 0$. C'est ce type de résultat que Green a utilisé dans [Gre05].

Lemme 2.1.1 (Green) *Soit N un grand nombre premier. Pour tout réel $\alpha \in (0,1)$ et tout réel positif M, il existe une constante $c(\alpha, M)$ pour laquelle, si $f : [1,N] \to [0,M]$ est une application satisfaisant $\mathbb{E}_{n\in\mathbb{Z}_N} f(n) \geq \alpha$, on a $\Lambda_3(f,f,f) > c(\alpha,M)$. De plus, on peut choisir $c(\alpha,M) = \left(\frac{\alpha}{2}\right)^3 h\left(\frac{\alpha}{2M}\right)$ avec h la fonction introduite au théorème 2.*

Néanmoins contrôler la norme infinie d'une fonction peut s'avérer difficile et une utilisation de l'inégalité de Cauchy-Schwarz permet de se contenter d'une majoration en norme quadratique. C'est ce que nous avons utilisé dans [6] :

Lemme 2.1.2 (Helfgott, de Roton) *Soient α, c des réels positifs et $f : \mathbb{Z}_N \to \mathbb{C}$ une application telle que $\mathbb{E}_{\mathbb{Z}_N} f \geq \alpha$ et $\|f\|_{L^2} \leq c$. Alors*

$$\Lambda_3(f,f,f) \geq \left(\frac{\alpha}{2}\right)^3 h\left(\left(\frac{\alpha}{2c}\right)^2\right).$$

Ce type de résultat est appelé « principe de transfert », il permet de se ramener à une utilisation du théorème de Roth dans les entiers.

2.2 Les ensembles de densité nulle

Le cas des ensembles d'entiers de densité nulle ne se prête pas directement au traitement que l'on vient de décrire et nécessite l'utilisation d'un théorème de transfert plus sophistiqué. Examinons le cas d'un sous-ensemble de nombres premiers de densité relative positive et notons $\mathcal{P}_N$ l'ensemble des nombres premiers inférieurs à N, $\mathcal{P}$ étant l'ensemble des nombres premiers. Étant donné un sous-ensemble A de $\mathcal{P}$ de densité relative positive dans $\mathcal{P}$, on pose $A_N = A \cap \mathcal{P}_N$. Si on choisit $f = \mathbf{1}_{A_N}$, alors la moyenne de f sur $\mathbb{Z}/N\mathbb{Z}$ tend vers 0 car A est de densité nulle dans $\mathbb{Z}$, ce qui ne permet pas d'utiliser l'un des lemmes énoncés ci-dessus. Si on choisit de normaliser la fonction indicatrice en posant $f = \frac{N}{|\mathcal{P}_N|}\mathbf{1}_{A_N}$, alors la fonction f est bien de moyenne positive mais n'est plus bornée, ni en norme infinie, ni en norme quadratique.

2.2.1 Approximation de f : la stratégie générale

Un moyen pour contourner ce problème consiste à approcher la fonction f (fonction indicatrice normalisée) par une fonction f_1 qui satisfait les hypothèses d'un des lemmes de transfert (bornée au moins en norme 2 et de moyenne positive). Ici, lorsqu'on parle d'approximation, on entend que la fonctionnelle $\Lambda_3(f,f,f)$ ne doit pas être trop altérée par le changement de f en f_1. C'est ce qui va nous guider dans le choix de f_1.

L'idée consiste alors à décomposer f en deux parties $f = f_1 + f_2$, où $f_1 = f * \sigma$. On choisit alors σ de manière à ce que f_1 satisfasse les hypothèses du théorème de Roth et que $\Lambda_3(f_1, f_1, f_1)$ soit proche de $\Lambda_3(f, f, f)$. Cette dernière condition se traduira par le fait que les coefficients de Fourier de f_2 en dehors de 0 sont petits, f_2 sera donc la partie uniforme de f.

La formule

$$\Delta := |\Lambda_3(f, f, f) - \Lambda_3(f_1, f_1, f_1)| \leq \sum_k |\hat{f}(-2k)\hat{f}(k)^2||1 - \hat{\sigma}(-2k)\hat{\sigma}(k)^2| \tag{2.2}$$

amène naturellement à choisir σ de sorte que $\hat{\sigma}(k)$ soit proche de 1 lorsque $\hat{f}(k)$ est grand. On commence donc, pour $\varepsilon > 0$, par définir le spectre-ε de f par

$$R := \{k \in \mathbb{Z}_N \ , \ |\hat{f}(k)| \geq \varepsilon\}$$

et l'ensemble de Bohr de fréquence R et de rayon ε par

$$B = \{n \in \mathbb{Z}_N \ : \ \forall k \in R, \ \|nk/N\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon\},$$

où pour x réel, $\|x\|_{\mathbb{R}/\mathbb{Z}}$ désigne la distance de x à l'entier le plus proche. On définit aussi la fonction caractéristique de B normalisée, $\beta : \mathbb{Z}_N \to \mathbb{C}$ par $\beta = \frac{N}{|B|}\mathbf{1}_B$. Les ensembles de Bohr sont des outils classiques en analyse de Fourier. Une propriété immédiate de β est que ses coefficients de Fourier sur R sont proches de 1, plus précisément

$$\forall k \in R, \quad |\hat{\beta}(k) - 1| \ll \varepsilon. \tag{2.3}$$

Par ailleurs, le principe des tiroirs permet d'obtenir une minoration de la taille de B :

$$|B| \gg \varepsilon^r N \quad \text{ avec } r = |R|. \tag{2.4}$$

Choisissant $\sigma = \beta * \beta$, on assure l'uniformité de f_2 c'est à dire que les coefficients de Fourier de f_2 hors de 0 sont petits. Cette propriété provient du fait que $\hat{f}_2 = \hat{f}(1 - \hat{\sigma})$ et que $\hat{\sigma}(k)$ est proche de 1 lorsque $\hat{f}(k)$ est grand. Il faut cependant une hypothèse de majoration d'une norme p (pour un $p \in]2, 3[$) de $\hat{f}$ pour pouvoir conclure que Δ défini en (2.2) est petit. On utilise en effet l'inégalité de Hölder qui permet de majorer Δ à l'aide d'une norme p de $\hat{f}$ et de la norme infinie de $\hat{f}_2$.

La fonction σ étant normalisée, nous observons que $\mathbb{E}f_1 = \mathbb{E}f \geq \alpha$ selon la notation introduite en (2.1). Il reste à montrer que f_1 est bornée. Pour cela, il suffit que f soit majorée par une fonction ν uniforme.
Le résultat de ces réflexions est le principe de transfert énoncé par Green et Tao dans [GT06].

Théorème 3 (Principe de transfert, Green-Tao) *Soit N un grand nombre premier et $f : Z_N \to \mathbb{R}^+$ une fonctions vérifiant les conditions suivantes :*

1. $\mathbb{E}f \geq \alpha$,
2. $\|\hat{f}\|_p \leq M$ *pour un* $p \in]2, 3[$ *et un* $M > 0$,
3. $f \leq \nu$ *avec* $\sup_{k \in \mathbb{Z}_N} |\hat{\nu} - \mathbf{1}_0(k)| \leq \eta$ *pour un* $\eta > 0$.

Alors $\Lambda_3(f, f, f) \geq c(\alpha)/2 + O_{\alpha,M,p}(\eta)$.

C'est ce type de résultat que Green a utilisé dans [Gre05] pour démontrer le théorème de Roth dans les nombres premiers. Nous avons utilisé dans [6] un principe de transfert moins contraignant. Il peut s'énoncer comme suit :

Théorème V (Helfgott-de Roton) *Soit N un grand nombre premier et $f : Z_N \to \mathbb{R}^+$ une fonction vérifiant les conditions suivantes :*

1. $\alpha \leq \mathbb{E}f \leq 1$,
2. $\exists\, p \in]2,3[,\ \exists\, M > 0,\ \|\hat{f}\|_p \leq M$,
3. $\|f_1\|_2 \leq c$ *avec* $f_1 = f * \beta$ *où* $\beta = \frac{N}{|B|}\mathbf{1}_B$ *et* B *et l'ensemble de Bohr défini précédemment.*

Alors $\Lambda_3(f,f,f) \geq \left(\frac{\alpha}{2}\right)^3 h\left(\left(\frac{\alpha}{2c}\right)^2\right) - O_p(M^p \varepsilon^{3-p})$.

2.2.2 Vers une majoration uniforme pour les nombres premiers

Suivant la stratégie du principe de transfert, il nous faut majorer la fonction indicatrice normalisée des nombres premiers par une mesure uniforme. C'est clairement une nécessité si on veut obtenir le point 3 du théorème 3 mais c'est aussi ce que l'on utilise pour obtenir une majoration de la norme p de $\hat{f}$, ce qui est requis dans les deux théorèmes de transfert (théorème 3 et théorème V).

Cela ne peut être fait directement car les nombres premiers ne sont pas bien répartis dans les progressions arithmétiques de petit module. Par exemple, il n'existe pas de nombre premier (en dehors de 2 et 3) congru à 0, 2, 3 ou 4 modulo 6. Une première étape est donc nécessaire pour passer d'un ensemble de nombres premiers à un ensemble d'entiers dont on pourra trouver une majoration par une mesure uniforme. Cette étape est l'utilisation de ce qui est communément appelé « l'astuce W » (*W-trick*) depuis l'utilisation que Green en a fait dans [Gre05]. Elle consiste à se restreindre à l'intersection des nombres premiers avec une progression arithmétique de grande raison afin de passer d'un sous-ensemble de nombres premiers, qui donc n'ont pas de petits diviseurs, à un sous-ensemble d'entiers.

Plus précisément, pour un entier z choisi ultérieurement, on pose $W = \prod_{p \leq z} p$. Si A est un sous-ensemble de nombres premiers inférieurs à N' de densité relative au moins α, alors il est aisé de voir qu'il existe une progression arithmétique $P(b) = \{b + nW \,:\, 1 \leq n \leq N'/W\}$ de raison W dans laquelle A est de densité relative au moins $\alpha \log z / \log N'$. Ceci permet de considérer l'ensemble d'entiers $A_0 = \{n \,:\, b + nW \in A, :\, 1 \leq n \leq N\}$ de densité au moins $\alpha \log z / \log N$ dans $\mathbb{Z}_N$. Toute progression arithmétique de longueur 3 non triviale dans A_0 donnera une progression non triviale dans A. Nous laissons ici encore de côté quelques détails techniques qui permettent de considérer A_0 comme un sous-ensemble de $\mathbb{Z}/N\mathbb{Z}$ avec N un grand nombre premier de l'ordre de N'/W de manière à ne pas ajouter de progression dans A_0 qui ne correspondrait pas à une progression dans A.

Désignons à présent par f la fonction indicatrice normalisée de A_0 et montrons qu'elle vérifie les hypothèses d'un théorème de transfert. On a clairement $\mathbb{E}f \geq \alpha$ et il suffit montrer que l'on contrôle bien une norme p de $\hat{f}$ et que soit f est majorée par une mesure uniforme, soit $f * \beta$ est bornée en norme quadratique.
Remarquons dans un premier temps que $0 \leq f(n) \leq \lambda(n)$, où $\lambda : \mathbb{Z} \to \mathbb{R}$ est définie par

$$\lambda = \frac{\log N}{N \log z}\mathbf{1}_X \quad \text{avec} \quad X = \{n : 1 \leq n \leq N \text{ et } b + nW \text{ est premier}\}. \tag{2.5}$$

Dans [Gre05], Green utilise que le passage de A à A_0 ne conserve que les grands pics de la transformée de Fourier des nombres premiers et il utilise la méthode du cercle pour obtenir une majoration de la norme infinie de $\hat{\lambda}$. Il obtient alors une nouvelle preuve d'un théorème de restriction pour les nombres premiers établi dans un premier temps par Bourgain dans [Bou89]. Dans [6], nous observons plus directement le fait que les éléments de X peuvent avoir de petits diviseurs. Cela nous permet d'utiliser le crible enveloppant développé par Ramaré dans [Ram95] et initié dans [RR01]. Nous pouvons ainsi choisir un W plus grand que celui que Green utilisait, ce qui conduit à une première amélioration exponentielle. Nous n'avons néanmoins pas pu supprimer totalement cette astuce W, malgré nos efforts en ce sens.

Une application du théorème de Green et Tao sur le crible enveloppant [GT06] permet d'obtenir la majoration de la norme p de $\hat{f}$ nécessaire à l'application d'un des deux théorèmes de transfert.

Nous disposons donc à présent d'une application $f : \mathbb{Z}_N \to \mathbb{R}$ satisfaisant les deux premières hypothèses des théorèmes de transfert 3 et V. Afin de pouvoir appliquer le théorème de transfert V, il nous reste à majorer la norme quadratique de f_1.

2.2.3 Majoration de la norme quadratique de f_1

Cette partie de [6] est celle qui se démarque le plus des travaux préexistant, en particulier de [Gre05]. La majoration de la norme quadratique de f repose sur l'idée suivante : en convolant la fonction indicatrice normalisée de X, λ, avec β, on diminue fortement la norme quadratique de λ. Cela repose sur le fait que, pour k non nul, on dispose d'une bonne majoration (essentiellement $\ll \frac{k}{\phi(k)} \frac{N}{(\log N)^2}$ où ϕ est la fonction indicatrice d'Euler) du nombre de nombres premiers $p \leq N$ tels que $p+k$ est aussi premier. La seule chose que l'on utilise sur β est que β n'est pas concentré sur un trop petit ensemble, c'est à dire que l'ensemble de Bohr B n'est pas trop petit. La restriction à une classe de congruence modulo W permet de neutraliser le facteur $\frac{k}{\phi(k)}$ potentiellement problématique.

Notons d'abord que l'on a

$$\|f_1\|_2 = \|f * \beta\|_2 \leq \|\lambda * \beta\|_2 = \mathbb{E}_{m_1}\mathbb{E}_{m_2}\beta(m_1)\beta(m_2)\mathbb{E}_n\lambda(n+m_1)\lambda(n+m_2).$$

Maintenant, une utilisation de l'inégalité de Brun-Titchmarsh pour les terme diagonaux et du crible de Selberg pour les autres termes permet de montrer la majoration

$$\mathbb{E}_n\lambda(n+m_1)\lambda(n+m_2) \ll \begin{cases} \log N/(\log z) & \text{si} \quad m_1 = m_2, \\ \prod_{p|(m_1-m_2),\, p>z} \frac{p}{p-1} & \text{si} \quad m_1 \neq m_2. \end{cases} \tag{2.6}$$

Ceci amène la majoration

$$\|f_1\|_2 \ll \frac{1}{N}\left(\frac{\log N}{|B|\log z} + 1\right).$$

On obtient donc $\|f_1\|_2 \ll 1/N$ dès que $|B| \gg \log N/\log z$. En utilisant la taille des ensembles de Bohr et en prenant toutes les contraintes en compte on obtient le résultat de [6] .

Chapitre 3

Ensembles sans k-somme

Ce chapitre porte sur des travaux réalisés en collaboration avec Alain Plagne. Ils ont donné lieu à la publication [8].

3.1 Introduction

Le chapitre précédent était consacré à la majoration de la taille maximale des sous-ensembles de nombres premiers sans solution à l'équation $x + y = 2z$. Cette équation est une équation invariante au sens de la terminologie rappelée en introduction, c'est à dire invariantes par translation et multiplication. Ce chapitre sera consacré à l'étude d'équations non invariantes (par translation). Le cas des équations non invariantes se traite de manière très différente du cas des équations invariantes. Concentrons-nous sur les équations de la forme $x + y = kz$. Commençons par le cas le plus simple des sous-ensembles d'entiers positifs inférieurs à N sans somme, c'est à dire sans solution à l'équation $x + y = z$ (voir par exemple [DFST99]). Dans ce cas la taille maximale d'un ensemble sans somme ne peut dépasser $\lceil N/2 \rceil$ et deux types d'ensembles maximaux se distinguent :

— L'ensemble $\{\lceil (N+1)/2 \rceil, \cdots, N\}$ ne peut contenir de solution pour des questions de taille (la somme de deux entiers supérieurs à $N/2$ est nécessairement supérieure à N) ; ce premier type d'ensemble est de type « combinatoire ».

— L'ensemble des entiers impairs, lui aussi maximal, ne contient pas de somme pour une raison de congruence (la somme de deux entiers impairs est paire) ; ce second type d'ensemble est de type « arithmétique ».

Dans le cas des ensembles sans somme, la taille des ensembles combinatoires maximaux et des ensembles arithmétiques maximaux est la même. Cette distinction entre les types d'ensembles maximaux de retrouve dans l'étude des ensembles maximaux sans k-somme, c'est à dire sans solution à l'équation $x + y = kz$.

Pour $k = 3$ (et $n \neq 4$), Chung et Goldwasser [CG97] démontrent une conjecture d'Erdős annonçant que $\lceil N/2 \rceil$ est la taille maximale d'un ensemble d'entiers inférieurs à N sans 3-somme. Ils montrent aussi que pour $N \geq 23$, l'ensemble des entiers impairs (donc un ensemble de nature arithmétique) est le seul ensemble attaignant cette taille.

Pour $k \geq 4$, Chung et Goldwasser [CG96] découvrent un sous-ensemble de $\{1, 2, \ldots, N\}$ sans k-somme de taille asymptotiquement équivalente à

$$\sim \left(1 - \frac{2}{k}\right) \frac{k^4 - 4}{k^4 - 2k^2 - 4} N$$

lorsque N tend vers l'infini et conjecturent que cette taille asymptotique est bien celle d'un ensemble maximal sans k-somme. C'est Baltz, Hegarty, Knape, Larsson et Schoen qui démontrent finalement cette conjecture dans [BHK$^+$05] (une autre preuve en est donnée dans [DL06]) et décrivent précisément les ensembles maximaux. Notons que les ensembles maximaux construits sont la réunion de trois ensembles d'entiers consécutifs (on parlera d'intervalles d'entiers).

Ces ensembles maximaux sont de nature combinatoire et c'est en étudiant le problème continu analogue des ensembles sans k-somme dans $[0,1]$ dans [CG96] que Chung et Goldwasser ont pu énoncer leur conjecture (partant d'un ensemble A de réels de $[0,1]$ sans k-somme, on obtient un ensemble $\mathcal{A}$ d'entiers inférieurs à N sans k-somme en prenant les entiers de l'ensemble obtenu en dilatant A par N).

Ceci motive la recherche de la mesure de Lebesgue maximale d'un sous-ensemble de $[0,1]$ sans solution à l'équation $x+y=kz$. Laissons de côté le cas $k=1$ qui est simple à étudier, le cas $k=2$ qui a été discuté au chapitre précédent et et examinons le cas $k\geq 3$. Rappelons que le cas $k\geq 4$ a été résolu dans [CG96] et que nous avons étudié avec Alain Plagne le cas $k=3$ dans [8], poursuivant ainsi le travail de Matolcsi et Ruzsa dans [MR13].

Comme nous le verrons au chapitre suivant, le fait de travailler avec des ensembles de réels introduit une difficulté liée à la notion de mesurabilité. En effet, rien n'assure la mesurabilité de la somme de deux ensembles mesurables. Dans le cadre de ce chapitre, on peut contourner cette difficulté en considérant la mesure le Lebesgue intérieure λ_* plutôt que la mesure de Lebesgue λ. Dans la suite de ce chapitre nous ne reviendrons donc pas sur cette difficulté.

3.2 Les ensembles sans k-somme pour $k\geq 4$

Supposons pour commencer $k\geq 4$ et expliquons la construction d'un sous-ensemble de $[0,1]$ sans k-somme que l'on montrera maximal par la suite. Notons avant tout que le fait qu'un ensemble A ne contienne pas d'éléments x, y et z tels que $x+y=kz$ peut s'interpréter en terme ensembliste par

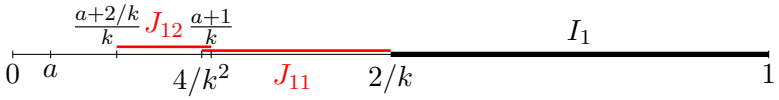
$$(A+A)\cap(k\cdot A)=\emptyset \quad \text{ou encore} \quad \left(\frac{1}{k}\cdot(A+A)\right)\cap A=\emptyset, \tag{3.1}$$

où pour un réel positif α, on note $\alpha\cdot A=\{\alpha x,\ x\in A\}$ et où $A+A$ désigne l'ensemble somme défini par $A+A=\{a+a',\ a,a'\in A\}$.

3.2.1 Construction d'un gros ensemble sans k-somme

On cherche un sous-ensemble A de $[0,1]$ sans k-somme. Si $\sup(A)\neq 1$, on constate que l'ensemble A' obtenu en dilatant A par $1/\sup(A)$ est aussi un ensemble sans k-somme et que sa mesure est plus grande que celle de A. Si A est un ensemble maximal dans $[0,1]$, on doit donc avoir $\sup(A)=1$. On note alors $a=\inf A$ et on applique un algorithme glouton en partant de 1, en descendant vers 0 et en prenant dans l'ensemble A tous les réels x rencontrés tant qu'il n'y a pas d'obstruction à les prendre.

La première obstruction rencontrée est en $2/k$ car $1+1=k\cdot 2/k$. Si on a pris dans A l'intervalle $I_1=]2/k,1]$, il faut exclure l'intervalle $J_{11}=\left]\frac{1}{k}(2/k+2/k),\frac{1}{k}(1+1)\right]=]4/k^2,2/k]$. D'autre part, si $a=\inf A$, il faut aussi exclure l'intervalle $J_{12}=\left]\frac{1}{k}(a+2/k),\frac{1}{k}(a+1)\right]$. Si $k\geq 4$, alors quelle que soit la valeur de a (rappelons tout de même que $0\leq a\leq 1$), on a $4/k^2\leq(a+1)/k\leq 2/k$ donc J_{11} et J_{12} sont d'intersection non vide (ou « collés » l'un à l'autre) et on doit en fait exclure l'intervalle $J_1=\left]\frac{1}{k}(a+2/k),\frac{2}{k}\right]$ de A (rappelons que l'on a pris $]2/k,1]$ dans A donc $a\leq 2/k$).



À présent, à gauche de $b = \frac{1}{k}(a + 2/k)$, l'influence de l'intervalle I_1 n'est plus opérante, puisque $\frac{1}{k}(\inf A + \inf I_1) \geq b$, et on peut donc chercher un sous-ensemble maximal de $[0, b]$ sans k-somme. En continuant à utiliser l'algorithme glouton, on choisit de prendre dans A l'intervalle $I_2 =]2b/k, b[$ et d'exclure l'intervalle $J_2 = \left]\frac{1}{k}(a + 2b/k), \frac{2b}{k}\right[$. À gauche de cet intervalle, l'influence de I_2 est à son tour inopérante et on peut donc itérer le procédé. On procède ainsi tant que a est bien inférieur aux valeurs prises dans A et on obtient pour A, aux points extrémaux des intervalles près, une réunion d'intervalles de la forme

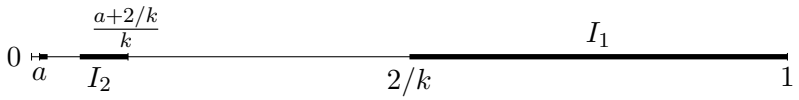
$$A = \bigcup_{i=1}^{n-1}]2x_i/k, x_i[\cup]a, x_n[$$

avec $a \geq 2x_n/k$, $x_1 = 1$ et $x_{i+1} = \frac{1}{k}(a + 2x_i/k)$ donc $x_{i+1} = \frac{a}{k}\frac{1-(2/k^2)^i}{1-2/k^2} + (2/k^2)^i$. La mesure d'un tel ensemble est $(1 - 2/k)\sum_{i=1}^{n} x_i - (a - 2x_n/k)$. Elle est maximale lorsque $a = 2x_n/k$ et $n = 3$, c'est à dire lorsque A est, aux points extrémaux des intervalles près, l'ensemble

$$\mathcal{A}_k =]a, x_3[\cup \left]\frac{2}{k}x_2, x_2\right[\cup \left]\frac{2}{k}, 1\right[$$

avec $a = \frac{2}{k}x_3$ donc $a = \frac{8}{k(k^4-2k^2-4)}$ et donc

$$\mathcal{A} = \left]\frac{8}{k(k^4-2k^2-4)}, \frac{4}{k^4-2k^2-4}\right[\cup \left]\frac{4(k^2-2)}{k(k^4-2k^2-4)}, \frac{2(k^2-2)}{k^4-2k^2-4}\right[\cup \left]\frac{2}{k}, 1\right[.$$



3.2.2 Optimalité de l'ensemble construit

Pour montrer dans le cas $k \geq 4$ que l'ensemble ainsi construit est de mesure maximale, on utilisera des résultats postérieurs à [CG96]. À la lumière des travaux de [MR13] et de nos travaux en collaboration avec Alain Plagne [8], on dégage en effet une généralité qui nous semble-t-il permet de mieux exposer les idées.
On considère un ensemble mesurable $A \subset [0, 1]$ sans k-somme de borne supérieure 1, on pose $a = \inf A$, $A_1 = A \cap [2/k, 1]$ et $\varepsilon = 1 - 2/k - \lambda(A_1)$. On peut alors montrer, en notant $x_2 = \frac{1}{k}(a + 2/k)$ que

$$\lambda\left(A \cap [x_2, 1]\right) \leq 1 - 2/k - (1 - 3/k)\varepsilon \tag{3.2}$$

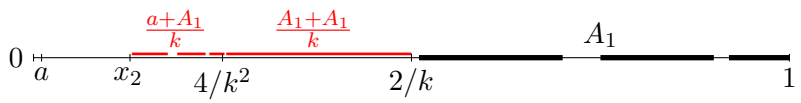
Ce fait se démontre de la manière suivante :

— on commence par remarquer que $\frac{1}{k}(A_1 + A_1)$ est inclus dans $[4/k^2, 2/k]$ et contient l'ensemble $\frac{2}{k} \cdot A_1$ donc l'ensemble $\frac{1}{k}(A_1 + A_1)$ est de mesure intérieure au moins $\frac{2}{k}\lambda(A_1) = \frac{2}{k}(1 - 2/k - \varepsilon)$. Il est d'intersection vide avec A, donc on a nécessairement

$$\lambda(A \cap [4/k^2, 2/k]) \leq \left(\frac{2}{k} - \frac{4}{k^2}\right) - \frac{1}{k}\lambda_*(A_1 + A_1) \leq \frac{2}{k}\varepsilon.$$

— on remarque de même que $\frac{1}{k}(a + A_1)$ est inclus dans $\frac{1}{k}(a + [2/k, 1])$ et d'intersection vide avec A si $a \in A$ (sinon on prend une suite d'éléments de A qui converge vers a et la conclusion demeure) donc $\lambda(A \cap [a/k + 2/k^2, (1 + a)/k]) \leq \frac{1}{k}\varepsilon$.

— dans le cas $k \geq 4$, les intervalles $\frac{1}{k}(a + [2/k, 1])$ et $[4/k^2, 2/k]$ sont d'intersection non vide et on conclut donc $\lambda(A \cap [a/k + 2/k^2, 2/k]) \leq \frac{3}{k}\varepsilon$ d'où $\lambda(A \cap [x_2, 1]) \leq 1 - \frac{2}{k} - \left(1 - \frac{3}{k}\right)\varepsilon$.



Nous utilisons un autre résultat intermédiaire qui donne une majoration de la taille d'un ensemble A sans k-somme en fonction de ses bornes inférieure et supérieure. Si A est un ensemble mesurable borné de $\mathbb{R}$ sans k-somme, alors :

$$\lambda(A) \leq \frac{k-1}{k+1} \sup A - \frac{1}{k+1} \inf A. \tag{3.3}$$

Dans [MR13], ce lemme était démontré dans le cas $k = 3$ mais sa généralisation au cas $k \geq 3$ est immédiate. Pour démontrer cette majoration, on remarque que $1/k \cdot (A + A)$ et A sont deux ensembles disjoints inclus dans l'intervalle $[2 \inf A/k, \sup A]$, ce qui implique

$$\sup A - \frac{2}{k} \inf A \quad \geq \quad \lambda_* \left(\frac{1}{k} \cdot (A + A) \right) + \lambda(A). \tag{3.4}$$

Appliquons la minoration de Ruzsa [Ruz91] pour la mesure de la somme de deux ensembles bornés et mesurables de réels :

$$\lambda_*(A + A) \geq \min \left(3\lambda(A), \lambda(A) + \sup A - \inf A \right). \tag{3.5}$$

Si $k \geq 3$, alors la majoration (3.3) découle de la majoration $\lambda(A) \leq \frac{1}{2}(\sup A - \inf A)$. Nous supposerons donc que nous sommes dans le cas $\lambda(A) > \frac{1}{2}(\sup A - \inf A)$ pour lequel (3.5) devient $\lambda_*(A + A) \geq \lambda(A) + \sup A - \inf A$ et (3.4) implique

$$\sup A - \frac{2}{k} \inf A \quad \geq \quad \frac{1}{k} \left(\lambda(A) + \sup A - \inf A \right) + \lambda(A),$$

et la majoration annoncée.

Nous disposons à présent de tous les éléments nécessaires à la démonstration du résultat suivant de Chung et Goldwasser [CG96].

Théorème 4 (Chung-Goldwasser) *Soit k un réel supérieur ou égal à 4. Définissons l'ensemble $\mathcal{A}_k$, union de trois intervalles, par*

$$\mathcal{A}_k = \left] \frac{2}{k} x_3, x_3 \right[\cup \left] \frac{2}{k} x_2, x_2 \right[\cup \left] \frac{2}{k} x_1, x_1 \right[$$

avec $x_3 = \frac{4}{k^4 - 2k^2 - 4}$, $x_2 = \frac{2(k^2-2)}{k^4-2k^2-4}$ et $x_1 = 1$. Si A est un sous-ensemble mesurable de $[0, 1]$ sans k-somme, alors

$$\lambda(A) \leq \lambda(\mathcal{A}_k) = \left(1 - \frac{2}{k} \right) \frac{k^4 - 4}{k^4 - 2k^2 - 4}.$$

De plus, si $\lambda(A) = \left(1 - \frac{2}{k}\right) \frac{k^4-4}{k^4-2k^2-4}$ et si A est maximal au sens de l'inclusion parmi les sous- ensembles sans k-somme de $[0, 1]$, alors A est l'un des sept ensembles obtenus comme union de $\mathcal{A}_k$ et d'un ensemble de trois points $\{u, v, w\}$ avec

$$(u, v, w) \in \left(\left\{ \frac{2}{k} x_3, x_3 \right\} \times \left\{ \frac{2}{k} x_2, x_2 \right\} \times \left\{ \frac{2}{k} x_1, x_1 \right\} \right) \setminus \left(\frac{2}{k} x_3, x_2, \frac{2}{k} x_1 \right).$$

Achevons à présent l'exposé de la démonstration. Rappelons que l'on a montré (3.2), i.e si $x_2 = \frac{2}{k^2} + \frac{a}{k}$, l'inégalité

$$\lambda\left(A \cap [x_2, 1]\right) \leq 1 - \frac{2}{k} - \left(1 - \frac{3}{k}\right)\varepsilon.$$

On peut supposer que $\lambda(A) \geq 1 - 2/k$, sans quoi la majoration $\lambda(A) \leq \lambda(\mathcal{A}_k)$ est immédiate. Posons $b = \sup\left(A \cap [0, x_2]\right)$ et définissons η par

$$\lambda\left(A \cap \left[\frac{2}{k}b, b\right]\right) = b\left(1 - \frac{2}{k}\right) - \eta.$$

L'inégalité (3.2) appliquée à l'ensemble A dilaté par $1/b$ permet d'obtenir la majoration

$$\lambda\left(A \cap \left[\frac{2b}{k^2} + \frac{a}{k}, b\right]\right) \leq b\left(1 - \frac{2}{k}\right) - \left(1 - \frac{3}{k}\right)\eta.$$

Ajoutant ces deux contributions on obtient la majoration

$$\begin{aligned}\lambda(A) &\leq (1+b)\left(1 - \frac{2}{k}\right) - \left(1 - \frac{3}{k}\right)(\varepsilon + \eta) + \lambda\left(A \cap \left[0, \frac{2}{k^2}b + \frac{a}{k}\right]\right) \\ &\leq (1+b)\left(1 - \frac{2}{k}\right) + \lambda\left(A \cap \left[0, \frac{2}{k^2}b + \frac{a}{k}\right]\right).\end{aligned}$$

Dans le cas où $A \cap \left[0, \frac{2}{k^2}b + \frac{a}{k}\right] = \emptyset$, cette majoration est meilleure que celle attendue. On peut donc supposer $A \cap \left[0, \frac{2}{k^2}b + \frac{a}{k}\right] \neq \emptyset$.

D'après (3.3), on a pour tout $c \geq a$

$$\lambda\left(A \cap [0, c]\right) \leq \min\left(c - a, \frac{k-1}{k+1}c - \frac{1}{k+1}a\right).$$

Appliquant cette inégalité à $c = \sup\left(A \cap \left[0, \frac{2}{k^2}b + \frac{a}{k}\right]\right)$, on obtient

$$\lambda(A) \leq (1+b)\left(1 - \frac{2}{k}\right) + \min\left(c - a, \frac{k-1}{k+1}c - \frac{1}{k+1}a\right). \tag{3.6}$$

En utilisant $b \leq x_2 = \frac{2}{k^2} + \frac{a}{k}$ et $c \leq x_3 = \frac{2}{k^2}x_2 + \frac{a}{k}$, on obtient

$$\lambda(A) \leq (1+x_2)\left(1 - \frac{2}{k}\right) + \min\left(x_3 - a, \frac{k-1}{k+1}x_3 - \frac{1}{k+1}a\right).$$

Le majorant est maximal lorsque $a = \frac{8}{k(k^4-2k^2-4)}$ et on obtient alors

$$\lambda(A) \leq \left(1 - \frac{2}{k}\right)\frac{k^4 - 4}{k^4 - 2k^2 - 4}.$$

D'autre part, l'égalité implique que l'on a égalité dans toutes les inégalités précédentes et donc en particulier

$$a = \frac{8}{k(k^4 - 2k^2 - 4)}, \quad b = x_2 = \frac{2}{k^2} + \frac{a}{k}, \quad c = x_3 = \frac{2}{k^2}b + \frac{a}{k}, \quad \lambda(A \cap [a, c]) = c - a \quad \text{et} \quad \varepsilon = \eta = 0,$$

autrement dit $A = \mathcal{A}_k$ à un ensemble de mesure nulle près. Il en découle que si A est un ensemble sans k-somme maximal au sens de l'inclusion parmi les ensembles de mesure maximale, alors A contient l'intérieur des $\mathcal{A}_k$ et est contenu dans leur adhérence. Une étude des points du bord des intervalles composant A permet de conclure que A est nécessairement l'un des ensembles décrits précédemment.

3.3 Les ensembles sans 3 somme

3.3.1 Énoncé des résultats

Le cas $k = 3$ est plus difficile à traiter que le cas $k \geq 4$ dont nous venons de parler. Rappelons que dans le cas discret, Chung et Goldwasser [CG97] ont démontré que pour N assez grand l'ensemble des entiers impairs, de densité $1/2$, était le seul ensemble maximal d'entiers inférieur à N sans 3-somme. Dans le contexte continu des sous-ensembles de $[0, 1]$, on peut remarquer que la construction opérée dans le cas $k \geq 4$ donne pour $k = 3$ l'ensemble composé de trois intervalles suivant

$$\mathcal{A}_3 = \left(\frac{8}{177}, \frac{4}{59}\right) \cup \left(\frac{28}{177}, \frac{14}{59}\right) \cup \left(\frac{2}{3}, 1\right) \tag{3.7}$$

et que cet ensemble ne contient pas de solution à l'équation $x + y = 3z$. Cet ensemble, de mesure $77/177 = 0.4350\ldots$, a été introduit dans [CG96] où la conjecture suivante a été formulée :

Conjecture 2 (Chung, Goldwasser) *Soit A un sous-ensemble mesurable sans 3-somme de $[0, 1]$. Alors*

$$\lambda(A) \leq \lambda(\mathcal{A}_3) = \frac{77}{177} \sim 0,43502\ldots.$$

De plus, si $\lambda(A) = 77/177$ et si A est maximal au sens de l'inclusion parmi les sous- ensembles sans 3-somme de $[0, 1]$, alors A est l'un des sept ensembles obtenus comme union de $\mathcal{A}_3$ et d'un triplet de points, un point extremal pour chaque intervalle définissant $\mathcal{A}_3$ excepté $(8/177, 14/59, 2/3)$.

Plus tard, les calculs de Matolcsi et Ruzsa [MR13] ont consolidé cette conjecture et les auteurs de [MR13] ont démontré que la mesure d'un sous-ensemble sans 3-somme de $[0, 1]$ satisfait

$$\lambda(A) \leq \frac{28}{57} = 0.49122\ldots.$$

Ce résultat était le premier à démontrer une majoration plus petite que $1/2$. C'est tout à fait notable dans la mesure ou cela démontre que dans le cas des ensembles sans solution à l'équation $x + y = 3z$, il y a rupture entre le cas continu (où un ensemble maximal est de densité $< 1/2$) et le cas discret (où un ensemble maximal est de densité $1/2$). On comprend ici que cette différence de comportement est due au fait que dans le cas discret les ensembles maximaux sont de nature arithmétique et ne possèdent donc pas d'analogue continu direct.

Dans [8], nous avons démontré la conjecture de Chung et Goldwasser énoncée dans [CG96].

Nous avons choisi dans cette partie consacrée au cas $k = 3$ d'écrire des calculs valables pour $k \geq 3$ sans spécifier $k = 3$. Ce cas spécifique ne simplifie en rien l'argumentation et il nous a semblé plus facile de suivre les calculs avec un k non spécifié, on garde ainsi trace de l'origine des quantités qui apparaissent.

3.3.2 Les différences avec le cas $k \geq 4$.

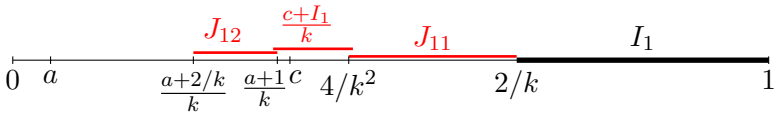
Revenons à l'argumentation développée dans le cas $k \geq 4$ et voyons pourquoi une telle argumentation ne s'applique plus dans le cas $k = 3$.

Considérons donc un ensemble mesurable $A \subset [0, 1]$ sans k-somme de borne supérieure 1, de borne inférieure a, on pose $A_1 = A \cap [2/k, 1]$ et $\varepsilon = 1-2/k-\lambda(A_1)$. Les majorations $\lambda(A \cap [4/k^2, 2/k]) \leq \frac{2}{k}\varepsilon$ et $\lambda(A \cap [a/k + 2/k^2, (1 + a)/k]) \leq \frac{1}{k}\varepsilon$ montrées précédemment restent valables. Toutefois, on n'a plus nécessairement $(1 + a)/k \geq 4/k^2$ comme dans le cas $k \geq 4$, ce qui signifie qu'il peut y avoir un espace entre l'intervalle J_{11} et l'intervalle J_{12} et que cet espace contient potentiellement des éléments

de A. Une deuxième difficulté est liée au fait que cette fois-ci $1-3/k$ n'est pas strictement positif et donc, même dans le cas où l'espace entre J_{11} et J_{12} ne contiendrait pas d'éléments de A, l'inégalité $\lambda([x_2,1]) \leq 1-2/k-(1-3/k)\varepsilon$ qui redeviendrait valable, ne suffirait plus à conclure que $\varepsilon = 0$ est le cas optimal.

Afin de dépasser ces difficultés, nous allons utiliser deux idées : l'une consiste à utiliser la minoration de Ruzsa (3.5) plutôt que la minoration classique de la taille d'une somme dans l'estimation de la mesure de $A_1 + A_1$, la seconde consiste à examiner l'influence qu'aurait la présence d'éléments de A dans l'intervalle J_{13} entre J_{11} et J_{12}.

Pour comprendre la seconde idée, imaginons que A contienne l'intervalle $]2/k, 1]$. Alors, comme on l'a vu précédemment, les intervalles $]4/k^2, 2/k]$ et $](a+2/k)/k, (a+1)/k[$ ne contiennent pas d'éléments de A. S'il existe un élément c de A compris entre $1/k$ et $4/k^2$, comme $\frac{1}{k}(c+2/k) < c$ et $\frac{1}{k}(c+1) > 4/k^2 > c$ si $k \geq 3$, l'intervalle $\frac{1}{k}(c+]2/k, 1[)$ contient c et donc si A contient l'intervalle $]2/k, 1]$, c ne peut être un élément de A. Dans le cas où on ne suppose plus que A contient l'intervalle $]2/k, 1]$, on va utiliser une idée similaire pour dire que l'intervalle $]1/k, 4/k^2[$ ne peut contenir que très peu d'éléments de A (un ensemble de petite mesure).



3.3.3 Optimalité de $\mathcal{A}_3$

Venons-en au cas général. Considérons à nouveau un ensemble mesurable $A \subset [0,1]$ sans k-somme de borne supérieure 1 et notons comme précédemment $a = \inf A$, $A_1 = A \cap]2/k, 1]$ et $\varepsilon = 1-2/k-\lambda(A_1)$. Définissons également l'ensemble $\overline{A_1} = [2/k, 1] \setminus A_1$ dont la mesure est donc ε. Comme noté précédemment, puisque A et $\frac{1}{k}(a+A_1)$ sont d'intersection vide si $a \in A$, on obtient, quitte à prendre une suite d'élements de A qui converge vers a si $a \notin A$,

$$A \cap \left]\frac{a}{k} + \frac{2}{k^2}, \frac{1+a}{k}\right[\subset \frac{1}{k}(a + \overline{A_1}). \tag{3.8}$$

De plus, s'il existe des éléments de A entre $1/k$ et $4/k^2$, en notant $c = \inf(A \cap]1/k, 4/k^2[)$, on a

$$A \cap]1/k, 4/k^2] \subset A \cap [c, 4/k^2] \subset \frac{1}{k}(c + \overline{A_1}). \tag{3.9}$$

D'autre part, en utilisant (3.5), on a

$$\lambda_*(A_1 + A_1) \geq \min(3\lambda(A_1), \lambda(A_1) + \operatorname{diam}(A_1))$$

donc si $\operatorname{diam}(A_1) = 1-2/k$ et $\lambda(A_1) \geq \frac{1}{2}(1-\frac{2}{k})$, alors

$$\lambda\left(A \cap \left[\frac{4}{k^2}, \frac{2}{k}\right]\right) \leq \frac{2}{k} - \frac{4}{k^2} - \frac{1}{k}\lambda_*(A_1 + A_1) \leq \frac{1}{k}\varepsilon. \tag{3.10}$$

Rassemblant (3.8), (3.9) et (3.10), on obtient dans le cas $\operatorname{diam}(A_1) = 1-2/k$ et $\lambda(A_1) \geq \frac{1}{2}(1-\frac{2}{k})$,

$$\lambda\left(A \cap \left[\frac{a}{k} + \frac{2}{k^2}, 1\right]\right) \leq 1 - \frac{2}{k} - \left(1 - \frac{3}{k}\right)\varepsilon,$$

ce qui montre dans ce cas encore la validité de l'équation (3.2) déjà utilisée dans le cas $k \geq 4$. Le reste de la démonstration est alors similaire à ce que l'on a fait pour $k \geq 4$. Il faut juste être un peu plus précis pour montrer que l'égalité n'est possible que si $\varepsilon = 0$.

Dans le cas où $\lambda(A_1) \geq \frac{1}{2}\operatorname{diam}(A_1)$ et $\operatorname{diam}(A_1) < 1-2/k$, il faut poser $\varepsilon_1 = 1-2/k-\operatorname{diam}(A_1)$, $\varepsilon_2 = \varepsilon - \varepsilon_1$ et considérer un découpage idoine plus fin mais les idées restent les mêmes.

Il reste alors à étudier le cas $\lambda(A_1) < \frac{1}{2}\operatorname{diam}(A_1)$. Pour cela, on utilise un résultat de Matolcsi et Ruzsa [MR13]. Ce résultat était énoncé pour $k = 3$ mais s'étend sans difficulté au cas $k \geq 3$. Il donne une majoration de la mesure d'un ensemble sans k-somme en fonction de la mesure de son intersection A_1 avec l'intervalle $]2/k, 1]$. Si A est un sous-ensemble mesurable de $[0, 1]$ sans k-somme ($k \geq 3$) et si $A_1 = A \cap]2/k, 1]$ alors

$$\lambda(A) \leq \frac{2}{k+3} + \frac{k}{k+3}\lambda(A_1). \tag{3.11}$$

La démonstration de ce résultat repose sur le fait que $\frac{1}{k}(A + A)$ et $A \setminus A_1$ sont deux sous-ensembles disjoints de l'intervalle $[2a/k, 2/k]$ et sur l'utilisation de la minoration de Ruzsa (3.5).

La minoration (3.11) permet aisément de montrer que dans le cas où $\lambda(A_1) \leq \frac{1}{2}\operatorname{diam}(A_1)$, on a une majoration de la mesure de A meilleure que celle attendue. On peut donc se placer dans l'autre cas, déjà traité.

Notons toutefois que la question se pose à nouveau à l'étape suivante. On est en effet amenés à chercher un minorant pour $\lambda_*(A_2 + A_2)$ où $A_2 = A \cap [2x_2/k, x_2]$ mais dans ce cas encore, si l'ensemble A_2 a une mesure plus petite que la moitié de son diamètre, on obtient une meilleure majoration que celle espérée.

Ceci permet de prouver que, si A est un sous-ensemble mesurable de $[0, 1]$ sans 3-somme, alors $\lambda(A) \leq \lambda(\mathcal{A}_3) = 77/177$ et si de plus $\lambda(A) = 77/177$ alors $A \Delta \mathcal{A}_3 = \emptyset$. Il faut alors examiner les ensembles de mesure nulle pour conclure.

Chapitre 4

Ensembles de petite somme

4.1 Introduction

Soit G un groupe commutatif dont la loi sera notée $+$. On supposera G localement compact et on notera μ sa mesure de Haar. Étant donnés A et B deux sous-ensembles non vides de G, on définit l'ensemble somme $A+B$ par $A+B=\{a+b,\, a\in A,\, b\in B\}$. Au chapitre précédent, nous avons utilisé des minorations de la mesure de l'ensemble somme pour déterminer la mesure maximale d'un ensemble sans solution à une équation linéaire donnée. Nous cherchons dans ce chapitre à déterminer une minoration de la mesure de Haar de l'ensemble somme $A+B$ en fonction des mesures de A et de B et la structure des ensembles A et B pour lesquels la taille de $A+B$ est proche du minorant obtenu.

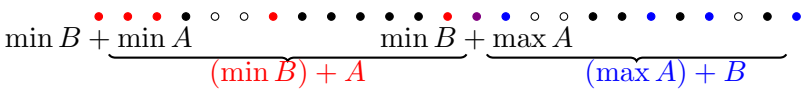
Une minoration immédiate de la taille de la somme est $\max(\mu(A),\mu(B)) \leq \mu(A+B)$. Lorsque $A\subset B$ et B est un sous-groupe de G, le minorant $\max(\mu(A),\mu(B))$ est atteint. Toutefois, cette minoration peut être améliorée dans certains cas.

4.1.1 Premières minorations dans le cas discret

Commençons par rappeler quelques résultats dans le cas où G est un groupe discret. On s'intéresse plus précisément aux cas des entiers relatifs ($G=\mathbb{Z}$) et au cas des résidus modulo un entier n ($G=\mathbb{Z}/n\mathbb{Z}$). Dans le cas où G est un groupe discret, la mesure de Haar est la mesure de comptage et on notera $|A|$ la mesure de A, c'est à dire le nombre d'éléments de A.
La recherche de minorations pour la taille de la somme de deux ensembles finis d'entiers et la carcatérisation des ensembles pour lesquels la taille de la somme est proche du minorant a maintenant une longue histoire. Commençons par une minoration élémentaire. Si A et B sont des sous-ensembles finis de $\mathbb{Z}$ alors :

$$|A+B| \geq |A|+|B|-1. \tag{4.1}$$

En particulier $|A+A|\geq 2|A|-1$.
Un simple dessin illustre parfaitement ce résultat qui se passe alors de démonstration ($\min B+A$ est en rouge, $\max A+B$ est en bleu, les points de $A+B$ sont les points « pleins »).



Cette première minoration est optimale dans le cas où A et B sont des progressions arithmétiques de même pas, c'est en fait le seul cas d'égalité. On peut aussi décrire les ensembles pour lesquels l'égalité est « presque atteinte ». Pour établir certains de ces résultats, il est utile de rechercher une minoration de la taille de la somme modulo un entier n de deux ensembles d'entiers. Les théorèmes de Cauchy-Davenport et Kneser [Kne53] énoncent de telles minorations. Notons dans un premier temps que l'ensemble $A+B$ modulo n ne peut pas occuper plus de place que le groupe $\mathbb{Z}/n\mathbb{Z}$. Si toutefois il n'occupe pas le groupe tout entier, on retrouve modulo n une minoration similaire à celle que l'on avait dans les entiers lorsque n est premier. C'est le théorème de Cauchy-Davenport : si A et B sont deux ensembles non vides de $\mathbb{Z}/n\mathbb{Z}$ et **si n est un nombre premier**, alors

$$|A+B| \geq \min(|A|+|B|-1, n). \tag{4.2}$$

Dans le cas où n est un entier composé, on peut trouver un sous-groupe propre H de $\mathbb{Z}/n\mathbb{Z}$ et si on choisit $A=B=H$, on a $H+H=H$ et la taille de $H+H$ est donc exactement la taille de H. Dans ce cas, on ne peut donc pas trouver d'analogue du théorème de Cauchy-Davenport mais il existe un énoncé plus général, le théorème de Kneser, qui donne une minoration de la taille d'un ensemble somme dans $\mathbb{Z}/n\mathbb{Z}$ faisant intervenir le sous-groupe stabilisateur de $A+B$.

Revenons au cas des entiers. Pour des ensembles A et B « quelconques », on s'attend à ce que la taille de la somme soit beaucoup plus grande que le minorant donné dans (4.1). Il est donc légitime de s'interroger sur la structure des ensembles pour lesquels la minoration est presque atteinte. De tels questionnements ont amené les mathématiciens à établir des théorèmes dits « théorèmes inverses » donnant des informations structurelles sur les ensembles A et B pour lesquels $A+B$ est petit. Le lecteur pourra consulter [TV06] ou [Nat96] pour plus d'information sur ce domaine.

En 1959, Freiman [Fre59] démontre qu'un ensemble A d'entiers pour lequel on a $|A+A| \leq 3|A|-4$ est inclus dans une progression arithmétique de taille au plus $|A+A|-|A|+1$. Ce résultat, souvent appelé théorème $(3k-4)$ de Freiman, a donné lieu à de nombreuses généralisations et précisions. Une des généralisations, opérée par Freiman lui-même dans [Fre62] puis précisée par Lev et Smeliansky dans [LS95] et Stanchescu dans [Sta96], a consisté à établir un résultat analogue lorsque la somme de deux ensembles distincts est considérée. Sous l'hypothèse $|A+A| \leq 3|A|-4$, on peut aussi donner une information sur la structure de $A+A$. Dans [Fre09], Freiman obtient en effet que l'ensemble $A+A$ doit contenir une progression arithmétique de taille au moins $2|A|-1$. Une version du théorème $(3k-4)$ donnant la structure de l'ensemble somme a aussi été donnée pour des ensembles A et B distincts dans [BG10]. Une version exhaustive et optimale de ce théorème pour les entiers peut être trouvée dans [Gry13] au chapitre 7. Nous la reproduisons ici.

Théorème 5 *Soient A et B deux sous-ensembles finis non vides d'entiers. On note $d=\operatorname{pgcd}(A+B)$. On suppose que l'une au moins des hypothèses suivantes est vérifiée :*

i) $|A+B| \leq |A|+|B|-3+\min(|A|,|B|)-\delta(A,B)$ *;*

ii) ou $\operatorname{diam}(B) \leq \operatorname{diam}(A)$, $\operatorname{pgcd}(A) \leq 2d$ *et* $|A+B| \leq |A|+2|B|-3-\delta(A,B)$ *;*

où l'on a noté $\operatorname{diam}(A)=\max A-\min A$, $\operatorname{diam}(B)=\max B-\min B$ *et* $\delta(A,B)=\begin{cases}1 & \text{si } A\subset B,\\ 0 & \text{sinon.}\end{cases}$

Alors

1. *A est inclus dans une progression arithmétique de pas d et de longueur $|A+B|-|B|+1$,*
2. *B est inclus dans une progression arithmétique de pas d et de longueur $|A+B|-|A|+1$,*
3. *$A+B$ contient une progression arithmétique de pas d et de longueur $|A|+|B|-1$.*

On trouve dans la littérature beaucoup d'autres résultats sur les ensembles d'entiers de petite somme. Citons le célèbre théorème de Freiman-Ruzsa [Ruz94] qui donne des informations structurelles sur les ensembles d'entiers de petite constante de doublement. Plus précisément, si A est un ensemble d'entiers tel que $|A+A| \leq K|A|$, alors A est contenu dans une progression arithmétique générale de dimension d et de taille au plus $K'|A|$ avec K' et d dépendant de K. De nombreux travaux ont cherché à donner des majorations de K' et d les plus précises possibles. Notons que plus la taille de la somme $A+A$ est loin de sa valeur minimale possible, moins la description de l'ensemble A est précise. Dans ce qui suit, nous nous intéresserons à des sommes de taille très proche de la taille minimale possible.

4.1.2 Le cas réel

Le cas réel présente certaines difficultés qui n'étaient pas présentes dans le cas discret. La première de ces difficultés est que la somme de deux ensembles de réels (Lebesgue) mesurables n'est pas nécessairement mesurable, comme l'a démontré Sierpiński dans [Sie20]. La somme de deux ensembles fermés étant un ensemble fermé, ce problème peut être résolu dans certains cas en considérant la mesure intérieure de Lebesgue plutôt que la mesure de Lebesgue. Ce sera le cas pour les résultats que nous énonçons dans ce chapitre et par soucis de clarté, nous ne reviendrons pas sur cette difficulté dans la mesure où elle se limite à des détails techniques. Cependant, certaines difficultés liées au contexte discret disparaissent dans le cas continu et certaines idées sont plus intuitives dans ce dernier contexte. Notons par exemple que les détails techniques liés dans le cas discret au fait que la mesure d'un point n'est pas nulle n'interviennent plus. Ainsi l'analogue continu de (4.1) s'énonce-t-il plus simplement.

Notant λ la mesure de Lebesgue sur $\mathbb{R}$ et λ_* la mesure de Lebesgue intérieure sur $\mathbb{R}$, si A et B sont deux sous-ensembles non vides, bornés et mesurables de réels, alors

$$\lambda_*(A+B) \geq \lambda(A) + \lambda(B). \tag{4.3}$$

De plus on a égalité si et seulement si A et B sont respectivement inclus dans des intervalles I et J avec $\lambda(I) = \lambda(A)$ et $\lambda(J) = \lambda(B)$.
Nous avons noté que dans le cadre discret, lorsqu'on cherchait un minorant de la taille de $A+B$ modulo un entier n, la nature arithmétique de n, et donc l'existence éventuelle de sous-groupes propres dans $\mathbb{Z}/n\mathbb{Z}$, jouait un rôle important. Dans le contexte continu de $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, tout se passe comme si dans le cas discret, on ne considérait que les modules premiers. Une difficulté majeure du cadre discret est donc évitée dans ce nouvau contexte. Plus précisément, le théorème de Raikov [Rai39] donne un analogue continu du théorème de Cauchy-Davenport qui s'appliquait pour les sommes modulo un nombre premier. Notons μ la mesure de Haar sur $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ et μ_* la mesure de Haar intérieure, alors

$$\mu_*(A+B) \geq \min(1, \mu(A) + \mu(B)). \tag{4.4}$$

pour tous sous ensembles non vides mesurables A et B de $\mathbb{T}$.

On l'a vu précédemment, étant donnés deux sous-ensembles A et B de réels, la minoration $\lambda_*(A+B) \geq \lambda(A) + \lambda(B)$ est optimale lorsque A est un intervalle. Ruzsa [Ruz91] donne néanmoins une meilleure minoration faisant intervenir le diamètre d'un des ensembles. Si A est un ensemble borné de réel, on appelle diamètre de A et on note $\mathrm{diam}(A)$ le réel $\mathrm{diam}(A) = \sup A - \inf A$.

Théorème 6 (Ruzsa) *Soient A et B deux sous-ensembles mesurables de réels tels que $\lambda(B) \leq \lambda(A)$. Alors*

$$\lambda_*(A+B) \geq \min(\lambda(A) + 2\lambda(B), \mathrm{diam}(A) + \lambda(B))$$

Ce théorème permet d'obtenir une version continue du théorème $3k-4$ de Freiman. Nous avons même obtenu un analogue continu de la version exhaustive de ce théorème (Théorème 5) dans [10]. Il fera

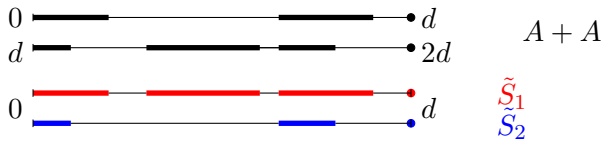
l'objet du théorème VIII. Soulignons ici que les idées de la démonstration sont beaucoup plus faciles à comprendre dans le cas continu. L'une des raisons à cela est que dans le cadre continu on dispose du théorème de Raikov (dans le cas discret, cela reviendrait à faire comme si tous les entiers étaient premiers !), l'autre raison est que l'on peut illustrer graphiquement la démonstration dans le cadre continu et que cela simplifie grandement l'argumentation, en particulier dans la description de la structure de $A+B$.
Notons enfin que cette dernière interprétation graphique mène naturellement à des résultats de structure sur les ensembles de petite somme qui n'ont pas nécessairement d'analogues discrets dans la littérature.

4.2 Les minorations de Ruzsa

Afin de comprendre les idées dans les démonstrations de nos résultats, il est nécessaire de revenir sur l'argumentation de Ruzsa dans [Ruz91]. Nous exposons ci-dessous les idées principales dans le cas $A=B$. Nous signalerons rapidement les aménagements à apporter dans le cas général.
Supposons que A est un sous-ensemble fermé et borné de réels, de mesure strictement positive, de borne inférieure 0. Par invariance par translation de la mesure de Lebesgue, on peut bien supposer $\inf A = 0$ sans perte de généralité. Le fait de travailler avec la mesure de Lebesgue intérieure permet de plus de restreindre la démonstration aux ensembles fermés.
Comme dans la démonstration du théorème de Raikov, la première idée (mise en oeuvre par Ruzsa) consiste à travailler modulo un réel, ici le réel $d=\mathrm{diam}(A)=\sup A-\inf A$. Notons $\mathbb{T}_d=\mathbb{R}/d\mathbb{Z}$ et μ_d la mesure de Haar associée. Définissons les ensembles $\tilde{S}_1$ et $\tilde{S}_2$, considérés comme des sous-ensembles de $\mathbb{T}_d=\mathbb{R}/d\mathbb{Z}$ suivants :

$$\tilde{S}_1=\{x\in[0,d[:\ x\in A+A \,\text{ou}\, x+d\in A+A\};\quad \tilde{S}_2=\{x\in[0,d[:\ x\in A+A \,\text{et}\, x+d\in A+A\}$$

et illustrons cette définition par un dessin.



Remarquons que $\lambda(A)=\mu_d(A \bmod d)$ et, puisque $A+A\subset[0,2d]$, $\lambda(A+A)=\mu_d(\tilde{S}_1)+\mu_d(\tilde{S}_2)$. Or $0,d\in A$ donc $A \bmod d\subset\tilde{S}_2$ et $\mu_d(\tilde{S}_2)\geq\lambda(A)$. D'autre part, en opérant une dilatation dans l'inégalité de Raikov (4.4), on obtient $\mu_d(\tilde{S}_1)=\mu_d(A \bmod d+A \bmod d)\geq\min(d,2\lambda(A))$.
Ces éléments permettent d'obtenir la minoration

$$\lambda(A+A)\geq\lambda(A)+\min(d,2\lambda(A)),$$

ce qui démontre le théorème de Ruzsa dans le cas $A=B$.

Dans le cas $A\neq B$, les idées sont similaires. Après s'être ramené à des ensembles fermés bornés de minimum 0, on raisonne modulo $d_A=\mathrm{diam}\,A$ et on considère les ensembles

$$\tilde{S}_k=\{x\in[0,d_A[:\ |\{l\in\mathbb{Z}\ :\ x+ld_A\in A+B\}|\geq k\}$$

$$\text{et}\ \ \tilde{B}_k=\{x\in[0,d_A[:\ |\{l\in\mathbb{Z}\ :\ x+ld_A\in B\}|\geq k\}.$$

On observe que

$$\lambda(A+B)=\sum_{k\geq1}\mu_{d_A}(\tilde{S}_k),\quad \lambda(B)=\sum_{k\geq1}\mu_{d_A}(\tilde{B}_k). \tag{4.5}$$

Puisque $0, d_A \in A$, on a de plus $\tilde{B}_k \subset \tilde{S}_{k+1}$. Ceci implique

$$\lambda(A+B) \geq \lambda(B) + \mu_{d_A}(\tilde{S}_1).$$

On distingue alors deux cas. Dans le premier cas, $\mu_{d_A}(\tilde{S}_1) = d_A$ et $\lambda(A+B) \geq \mathrm{diam}(A) + \lambda(B)$. Dans le cas contraire, on a pour tout entier k, $\mu_{d_A}(\tilde{S}_k) < d_A$ (rappelons que $\tilde{S}_{k+1} \subset \tilde{S}_k$) et l'inclusion $A + \tilde{B}_k \subset \tilde{S}_k$ et l'inégalité de Raikov (4.4) impliquent l'inégalité $\mu_{d_A}(\tilde{S}_k) \geq \lambda(A) + \mu_{d_A}(\tilde{B}_k)$. Cette inégalité, combinée à $\tilde{B}_k \subset \tilde{S}_{k+1}$ donc $\mu_{d_A}(\tilde{B}_k) \leq \mu_{d_A}(\tilde{S}_{k+1})$, et aux égalités (4.5), permet d'obtenir

$$\lambda(A+B) \geq \frac{K_B+1}{K_B}\lambda(B) + \frac{K_B+1}{2}\lambda(A), \tag{4.6}$$

avec $K_B = \max\{k \in \mathbb{N} : \tilde{B}_k \neq \emptyset\}$.

Ruzsa utilise (4.6) pour démontrer une minoration dépendant du ratio $\lambda(B)/\lambda(A)$. Plus précisément, si $K \in \mathbb{N}^*$ et $\delta \in \mathbb{R}$ sont définis par

$$\frac{\lambda(B)}{\lambda(A)} = \frac{K(K-1)}{2} + K\delta, \quad 0 \leq \delta < 1, \tag{4.7}$$

alors il obtient la minoration

$$\lambda(A+B) \geq \lambda(B) + \min(\mathrm{diam}(A), (K+\delta)\lambda(A)). \tag{4.8}$$

Cette minoration est une conséquence directe de (4.6) et de l'étude de la fonction de la variable entière K_B du membre de droite qui atteint son minimum en $K_B = K$.

Nous avons utilisé dans [10] l'observation simple suivante : K_B est nécessairement inférieur ou égal à $\mathrm{diam(B)/diam(A)}$. Cette remarque permet d'obtenir une amélioration de (4.8) dans le cas $\mathrm{diam(B)/diam(A)} \leq \mathrm{K}$.

La minoration de Ruzsa dans le cas $\lambda(B) \leq \lambda(A)$ (donc $K = 1$ ou $(K, \delta) = (2, 0)$ dans (4.8)) et notre observation faisant intervenir le quotient des diamètres permettent d'obtenir la minoration

$$\lambda_*(A+B) \geq \min(\lambda(A) + 2\lambda(B), \mathrm{diam}(A) + \lambda(B))$$

lorsque $\lambda(B) \leq \lambda(A)$ ou $\mathrm{diam(B)} \leq \mathrm{diam(A)}$.

D'autre part, nous pouvons décrire les ensembles extrémaux pour lesquels la minoration de Ruzsa est atteinte.

Théorème VI (de Roton) *Soient A et B des ensembles fermés bornés de réels tels que $\lambda(A), \lambda(B) \neq 0$. On suppose*

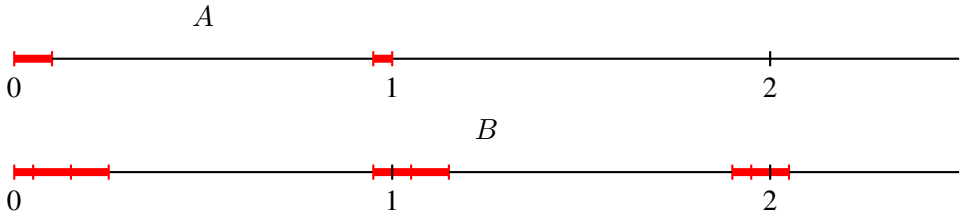
$$\lambda(A+B) = \lambda(B) + (K+\delta)\lambda(A) < \lambda(B) + \mathrm{diam(A)}$$

où K et δ sont définis dans (4.7)*. Alors A et B sont des sous-ensembles de mesure totale dans des translatés des ensembles A' et B' définis par*

$$A' = [0, a_+] \cup [d_A - a_-, d_A]; \quad B' = \bigcup_{k=1}^{K} [(k-1)(d_A - a_-), (k-1)d_A + (K-k)a_+ + \delta a]$$

avec $a_+, a_- \geq 0$, $a_+ + a_- = a = \lambda(A)$ et $d_A = \mathrm{diam A}$.

Les couples (A, B) d'ensembles extremaux auront donc la forme suivante (ici, $K = 3$ et $d_A = 1$).



La démonstration de ce résultat se décompose en trois étapes que nous ne reproduisons pas ici dans leur intégralité. Nous essaierons plutôt d'illustrer chaque étape de la preuve par des exemples pour en dégager les idées.

On se ramène d'abord facilement à des ensembles A et B fermés, bornés de minimum 0 et tels que le diamètre de A est $d_A = 1$ (donc μ_{d_A} est à présent noté μ). On suppose $\lambda(A+B) = \lambda(B) + (K+\delta)\lambda(A) < \lambda(B) + 1$. La première étape consiste à revenir sur la démonstration de la minoration de Ruzsa et donc à raisonner avec les ensembles modulo $d_A = 1$. On obtient facilement que les hypothèses du théorème VI impliquent $\mu(\tilde{S}_1) < 1$, $K_B = K$, et

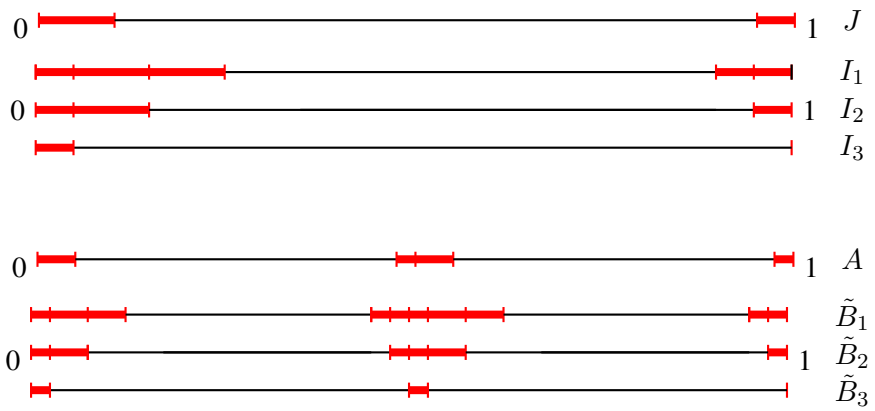
$$\begin{cases} \mu(\tilde{S}_k) = \mu(\tilde{B}_{k-1}) & (2 \le k \le K+1) \\ \mu(\tilde{S}_k) = \mu(\tilde{B}_k) + \mu(A) & (1 \le k \le K) \\ \mu(\tilde{S}_k) = 0 & (k \ge K+2) \end{cases} \tag{4.9}$$

La seconde égalité et l'inclusion $\tilde{B}_k + A \subset \tilde{S}_k$ pour $1 \le k \le K$, indiquent que l'on se trouve dans le cas d'égalité pour l'inégalité de Raikov (4.4) et la caractérisation que Kneser a donné dans [Kne56] des ensembles pour lesquels cette égalité était vraie permet d'affirmer qu'il existe un entier m_k et deux intervalles fermés I_k et J_k de $\mathbb{T}$ tels que $m_k\tilde{B}_k \subset I_k$, $m_k A \subset J_k$ et $\mu(I_k) = \mu(\tilde{B}_k)$, $\mu(J_k) = \mu(A)$.
On obtient aisément que $J = J_k$ et $m = m_k$ ne dépendent pas de k, ce qui, en posant $a = \lambda(A)$, implique, après quelques calculs et en utilisant (4.7)

$$m\tilde{B}_k \sim I_k = I_K + (K-k)J, \text{ avec } \mu(I_K) = \delta a \text{ et } \mu(J) = a,$$

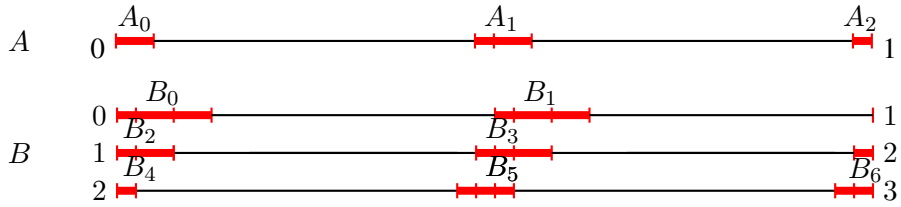
où le sympole $\sim$ signifie que les deux ensembles sont égaux à un ensemble de mesure nulle près.

On illustre dans le dessin ci-dessous la forme des intervalles J et I_k et des ensembles A et $\tilde{B}_k$ modulo $d_A = 1$ (ici, $K = 3$ et $m = 2$).

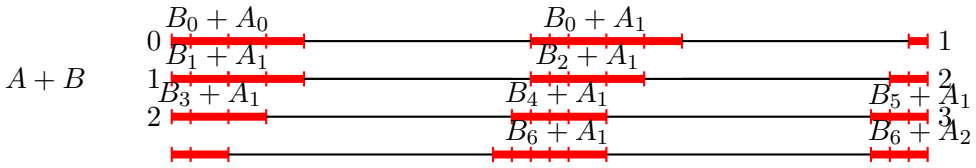


La seconde étape de la démonstration consiste à démontrer que m ne peut être égal qu'à 1 et que donc $A \sim J$ et $\tilde{B}_k \sim I_k$. D'après la définition de I_1, B est inclus dans l'union des intervalles $\frac{k}{m} + \frac{1}{m}I_1$. Pour $k \ge 1$, on note B_k l'intersection de B avec l'intervalle $\frac{k}{m} + \frac{1}{m}I_1$ et on désigne par $\mathcal{L}$ l'ensemble

des indices k pour lesquels B_k est non vide et par L le maximum de $\mathcal{L}$.
Nous montrons d'abord que $|\mathcal{L}| = Km$. La minoration $|\mathcal{L}| \geq Km$ provient des définitions de K et I_K et du fait que $m\tilde{B}_K \sim I_K$. La majoration est obtenue en utilisant l'hypothèse $\lambda(A+B) = \lambda(B) + (K+\delta)\lambda(A)$ et l'inclusion $A_i + B_j \subset S_{i+j}$ pour $j \in \mathcal{L}$ (avec pour $k \in \mathbb{N}$, $A_k = A \cap \left(\frac{k}{m} + \frac{1}{m}J\right)$ et $S_k = (A+B) \cap \left(\frac{k}{m} + \frac{1}{m}(I_1 + J)\right)$).
Pour illustrer cette majoration, reprenons l'exemple du dessin précédent (la forme de A est donc fixée par les données de m et J, à un ensemble de mesure nulle près) et supposons que $\mathcal{L}$ contient $Km+1$ entiers et que A et B sont de la forme suivante.



La somme $A+B$ contient l'ensemble représenté ci-dessous (dans ce cas particulier, on a même égalité entre $A+B$ et cet ensemble).



Si $m \geq 2$, alors $\lambda(A_1) = \lambda(A)/m$ et cet ensemble inclus dans $A+B$ est de mesure au moins

$$\begin{aligned}\lambda(B) + |\mathcal{L}|\lambda(A_1) + \lambda(A_0) + \lambda(A) - \lambda(A_0) - \lambda(A_1) &= \lambda(B) + \lambda(A) + (|\mathcal{L}| - 1)\lambda(A_1) \\ &\geq \lambda(B) + \lambda(A) + Km\lambda(A_1) \\ &\geq \lambda(B) + (K+1)\lambda(A),\end{aligned}$$

ce qui contredit les hypothèses. On a donc, si $m \geq 2$ exactement Km ensembles B_k non vides. Comme $m\tilde{B}_K \sim I_K$, chaque ensemble B_k non vide contient donc un translaté de $\frac{1}{m}I_K$. Comme d'autre part, si $m \geq 2$ l'ensemble $(A_0 + B_0) \cup \bigcup_{\ell \in \mathcal{L}} (A_1 + B_\ell) \cup \bigcup_{\ell=2}^{m} (A_\ell + B_L)$, où L est le maximum de $\mathcal{L}$, est inclus dans $A+B$, on obtient en comparant les mesures une contradiction et le fait que $m = 1$.

Dans la dernière étape de la démonstration, on montre que l'on doit en fait avoir $L = K-1$ (les B_k non vides correspondent à des indices k successifs) et que l'on doit avoir $S_k = B_k + A_0 = B_{k-1} + A_1$ à un ensemble de mesure nulle près. Le raisonnement est alors très semblable à celui fait dans la première étape de la démonstration.

4.3 Représentation graphique pour les ensembles de grande densité

Le paragraphe précédent traitait de la structure des ensembles de petite somme pour lesquels la somme $A+B$ modulo d_A, le diamètre de A, n'occupait pas tout le cercle $\mathbb{T}_{d_A}$. Nous allons ici étudier le cas des sommes qui, à un ensemble de mesure nulle près, remplissent tout le cercle modulo d_A, autrement dit pour lesquelles $\mu_{d_A}(A+B) = d_A$.

La principale nouveauté de [10] a consisté à donner une interprétation graphique de la densité des ensembles et à utiliser cette interprétation graphique pour lier la taille de la somme des ensembles à leur structure.

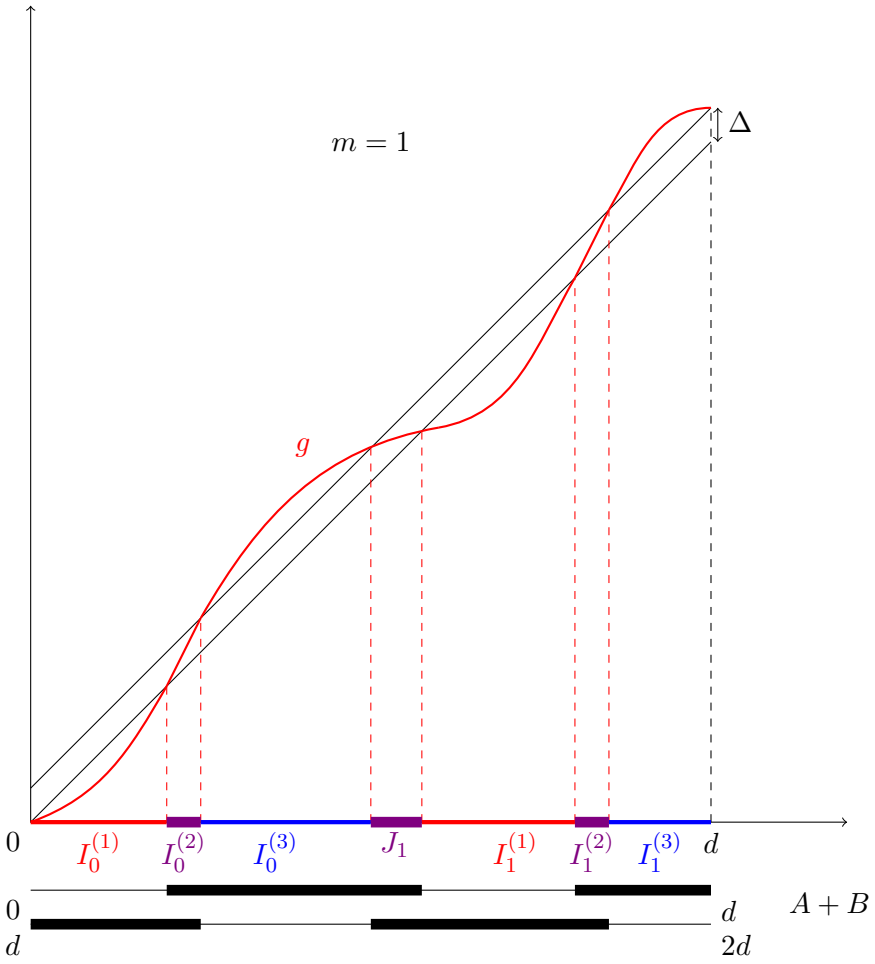
Pour simplifier l'exposé, nous supposerons que A et B sont des ensembles fermés et bornés de même diamètre d et nous les translaterons de manière à avoir $\min(A) = \min(B) = 0$ et $\max(A) = \max(B) = d$. Définissons à présent sur $[0, d]$ la fonction g par $g(x) = \lambda(A \cap [0, x]) + \lambda(B \cap [0, x])$. Supposons $\lambda(A) + \lambda(B) > d$, donc en particulier, d'après l'inégalité de Raikov (4.4), $\mu_d(A + B) = d$. Posons $\Delta = \lambda(A) + \lambda(B) - d$ et notons que Δ est strictement positif sous nos hypothèses.

Une propriété lie la taille de la fonction g en x à l'appartenance de x à la somme $A + B$. En effet, si $x \in [0, d]$ vérifie $g(x) > x$, alors $x \in A + B$. Cela provient du fait que si $x \notin A + B$ alors pour tout $y \in [0, x]$, soit y n'appartient pas à A, soit $x - y$ n'appartient pas à B. Symétriquement, si $x \in [0, d]$ vérifie $g(x) < x + \Delta$, alors $x + d \in A + B$.
Nous disposons alors d'une fonction g définie sur $[0, d]$, continue, croissante, 2-Lipschitzienne telle que $g(0) = 0$ et $g(d) = \lambda(A) + \lambda(B) = d + \Delta$. Traçant le graphe de cette fonction et les deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ d'équations respectives $y = x$ et $y = x + \Delta$, on peut diviser l'intervalle $[0, d]$ en trois zones comme suit :

- Z_1 est l'ensemble fermé des $x \in [0, d]$ tels que $g(x) \leq x$,
- Z_2 est l'ensemble ouvert des $x \in [0, d]$ tels que $g(x) > x$ et $g(x) < x + \Delta$,
- Z_3 est l'ensemble fermé des $x \in [0, d]$ tels que $g(x) \geq x + \Delta$.

D'après la remarque précédente, les ensembles Z_2, Z_3, $d + Z_1$ et $d + Z_2$ sont inclus dans $A + B$. D'autre part, la famille $\{Z_1, Z_2, Z_3\}$ forme une partition de $[0, d]$, ce qui confirme que $\mu_d(A + B) = d$, donc que $A + B$ remplit tout le cercle $\mathbb{T}_d$ modulo d.

Maintenant intervient la continuité de g. Pour passer de Z_1 à Z_3 et réciproquement, il faut traverser Z_2. Comme $0 \in Z_1$ et $d \in Z_3$, il y a au moins un passage « en montée » de Z_1 à Z_3 et si m est le nombre de « descentes » (passages de Z_3 à Z_1) pour g, alors on a $m + 1$ « montées » et on alterne les montées et les descentes (Notons ici que la fonction g reste croissante même dans ce que nous appelons les descentes). Ainsi si m est le nombre de descentes pour g, l'intervalle $[0, d]$ peut être partitionné en $4m + 3$ intervalles consécutifs comme le dessin ci-dessous (pour lequel $m = 1$) l'illustre :



Les intervalles rouges sont dans Z_1, les bleus dans Z_3 et les violets dans Z_2. En particulier, d'après les remarques précédentes, les $2m + 1$ intervalles noirs sous le graphe sont inclus dans $A + B$.

Remarquons de plus que chaque montée et chaque descente induit un passage dans la zone Z_2 qui ne peut pas être trop court (pour filer la métaphore alpestre, le caractère Lipschitzien de g donne une majoration de la pente et donc une minoration de la distance à parcourir pour garantir une certaine élévation). On montre ainsi qu'à chaque montée correspond un intervalle I inclus dans Z_2 de longueur au moins Δ et à chaque descente correspond un intervalle J inclus dans Z_2 tel que $\lambda(J \cap B^c) \geq \Delta$.

Cette remarque implique en particulier que chacun des $2m + 1$ intervalles noirs inclus dans $A + B$ est de longueur au moins 2Δ.

Le cas de diamètres distincts ($\mathrm{diam(A)} = \mathrm{d_A} \neq \mathrm{diam(B)} = \mathrm{d_B}$) est plus difficile à appréhender. Il fait intervenir la fonction g pour laquelle on a toujours

$$g(x) > x \Rightarrow x \in A + B$$

mais aussi la fonction h définie par $h(x) = g_A(x + d_A - d_B) + g_B(x)$ pour laquelle on a

$$h(y) < y + \lambda(A) + \lambda(B) - d_B \Rightarrow y + d_A \in A + B.$$

Il faut alors « jongler » avec un décalage partiel des courbes. Cependant, si la démonstration est moins intuitive dans ce cas général, le principe reste le même que celui que l'on vient d'exposer.

Avec ces ingrédients, on obtient aisément un théorème de structure pour les ensembles de grande densité.

Théorème VII (de Roton, 2016) *Soient A et B des sous-ensembles mesurables bornés de $\mathbb{R}$ tels que $d_A = \mathrm{diam}(A) \geq d_B = \mathrm{diam}(B)$ et $\Delta = \lambda(A) + \lambda(B) - d_A > 0$.*
Soit $m \in \mathbb{N}$ tel que

$$\lambda(A+B) < \lambda(A) + 2\lambda(B) + (m+1)(\Delta + d_A - d_B)$$

Alors la somme $A+B$ contient l'union d'au plus $2m+1$ intervalles disjoints $K_1, ..., K_{2n+1}$ $(n \leq m)$, tous de longueur au moins $2\Delta + d_A - d_B$, tels que la mesure de cette union d'intervalles est au moins $d_A + (2n+1)\Delta + n(d_A - d_B)$.

Ici encore, nous donnons le schéma de preuve dans le cas $d_A = d_B$ et nous posons $d = d_A = d_B$. Rappelons que $\lambda(A+B) = \mu_d(\tilde{S}_1) + \mu_d(\tilde{S}_2)$ avec $\tilde{S}_1$ la somme $A+B$ modulo d qui remplit $\mathbb{T}_d$ (donc $\mu_d(\tilde{S}_1) = d$) et $\tilde{S}_2$ l'ensemble des éléments x de $[0, d[$ tels que $x, x+d \in A+B$. Comme $B \subset \tilde{S}_2$ et $Z_2 \subset \tilde{S}_2$, on a $\lambda(A+B) \geq \lambda(B) + d + \lambda(B^c \cap Z_2)$. À chaque « descente » de Z_3 à Z_1 on trouve un sous-ensemble de $Z_2 \cap B^c$ de longueur au moins Δ. Notant n le nombre de passages de Z_3 à Z_1, nous obtenons donc $\lambda(A+B) \geq \lambda(B) + D + n\Delta$. Ainsi nécessairement $n \leq m$ et d'après les remarques précédentes, on obtient l'inclusion de $2n+1$ intervalles de longueur au moins 2Δ chacun dans $A+B$.

Dans le cas où les diamètres de A et B (respectivement d_A et d_B) sont différents, on montre qu'à chaque « descente » correspond un sous-ensemble de $Z_2 \cap B^c$ de longueur au moins $\Delta + d_A - d_B$.

4.3.1 L'analogue continu du théorème $3k-4$

Les éléments que nous avons développés dans ce chapitre nous permettent de démontrer une version continue du théorème $3k-4$ pour les entiers dans sa forme la plus exhaustive.

Théorème VIII (de Roton, 2016) *Soient A et B deux sous-ensembles mesurables et bornés de réels. On suppose que $\lambda(A), \lambda(B) \neq 0$. Si de plus l'une au moins des hypothèses suivante est vérifiée :*

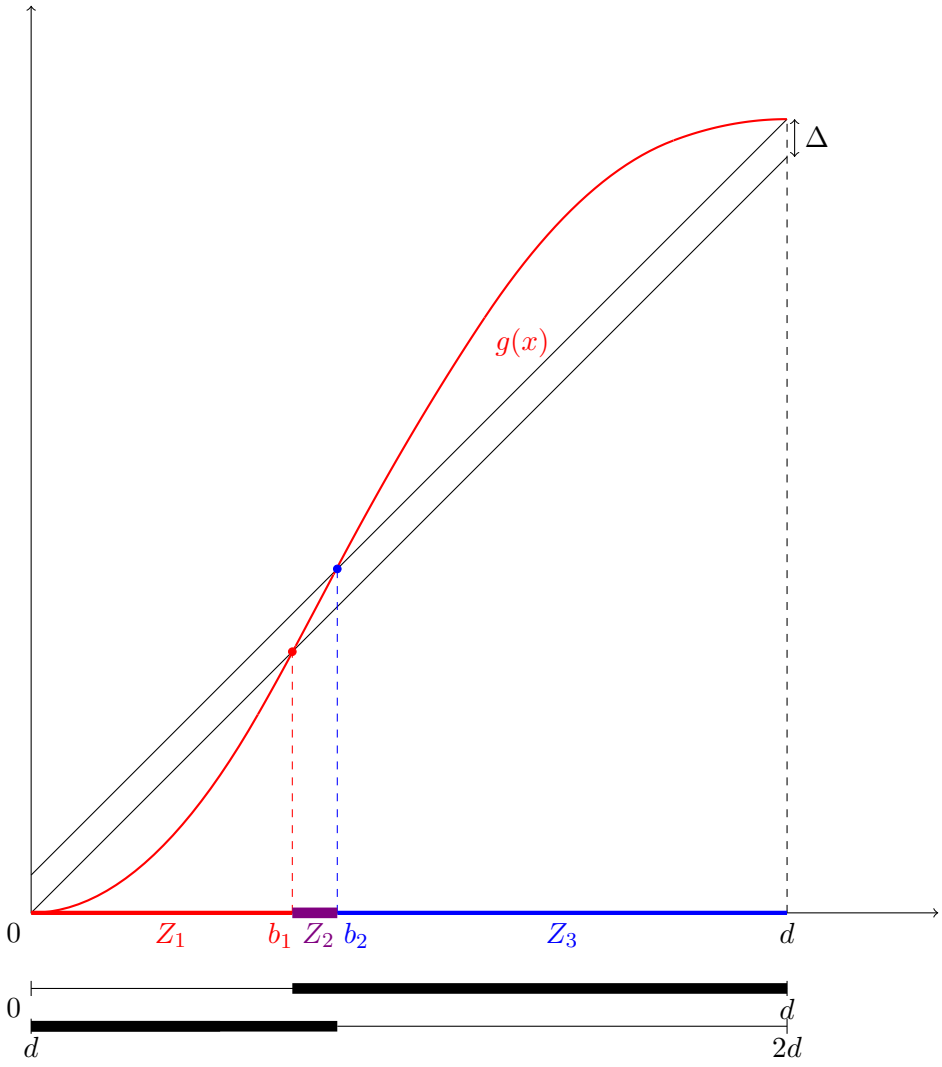
i) $\lambda_*(A+B) < \lambda(A) + \lambda(B) + \min(\lambda(A), \lambda(B))$ *;*

ii) ou $\mathrm{diam}(B) \leq \mathrm{diam}(A)$ *et* $\lambda_*(A+B) < \lambda(A) + 2\lambda(B)$ *;*

alors

1. $\mathrm{diam}(A) \leq \lambda_*(A+B) - \lambda(B)$,
2. $\mathrm{diam}(B) \leq \lambda_*(A+B) - \lambda(A)$,
3. *et il existe un intervalle I de longueur au moins $\lambda(A) + \lambda(B)$ inclus dans $A+B$.*

La première partie du théorème (conséquences 1 et 2) découle de l'étude menée dans le paragraphe sur les minorations de Ruzsa. La troisième conséquence provient des observations graphiques que nous avons faites pour les ensembles de grande densité. En effet, sous les hypothèses du théorème, on doit avoir $\Delta = \lambda(A) + \lambda(B) - d > 0$ et comme $\lambda(A+B) < d + \lambda(B) + \Delta$, il n'y a pas de « descente » pour g et la forme de g doit être conforme au dessin suivant.



Cela implique en particulier que l'intervalle $I = (b_1, b_2 + d)$, de longueur au moins $d + \Delta = \lambda(A) + \lambda(B)$ est inclus dans $A + B$.

Dans le cas où A et B n'ont pas le même diamètre, il faut pour cette partie de la preuve considérer les deux fonctions g et h déjà définies, ce qui complique l'exposé de l'argumentation mais les idées sont essentiellement les mêmes.

4.3.2 Structure des ensembles critiques

Les arguments de la preuve du théorème VIII permettent de comprendre la structure des ensembles fermés bornés A et B pour lesquels $d_B \leq d_A$ et $\lambda(A + B) = d_B + \lambda(A) < \lambda(A) + 2\lambda(B)$, c'est à dire des ensembles critiques de grande densité pour lesquels on a égalité dans l'inégalité de Ruzsa.

Dans le cas des entiers, Freiman a mis en évidence dans [Fre09] une similitude dans les structures de A et $A + A$ lorsque $|A + A| = \mathrm{diam}(A) + |A| - 1 < 3|A| - 4$. Notre résultat donne un analogue continu de celui de Freiman pour les entiers et le prolonge au cas d'ensembles A et B distincts. À notre connaissance, un tel résultat pour les entiers n'existe pas dans la littérature. L'énoncé étant technique, nous nous contentons ici de le reproduire pour le cas $A = B$. Le cas général se trouve dans [11].

Théorème IX (de Roton) *Soit A un ensemble fermé borné de réels de minimum 0 tel que $\lambda(A+A) = d_A + \lambda(A) < 3\lambda(A)$. Alors il existe deux réels positifs b et c tels que $b+c \leq d_A$, l'intervalle $I =]b, d_A - c[$ est de longueur au moins $2\lambda(A) - d_A = \Delta$ et les ensembles A et $A+A$ s'écrivent, à un ensemble de mesure nulle près*

$$A = (A_1 \cup]b, d_A - c[\cup (d_A - A_2)), \quad A + A = (A_1 \cup]b, 2d_A - c[\cup (2d_A - A_2))$$

avec $A_1 \subset [0, b]$, $A_2 \subset [0, c]$.

De plus, la mesure de A_1 et de A_2 près de 0 doit être petite. On peut en fait montrer qu'il existe c_1 et c_2 tels que $\lambda(A_1 \cap [0, x]) \leq x^2/c_1$ pour $x \leq c_1$ et $\lambda(A_2 \cap [0, x]) \leq x^2/c_2$ pour $x \leq c_2$.

Expliquons ici les idées principales de la démonstration dans le cas $A = B$. Rappelons l'inégalité

$$\lambda(A + A) \geq d_A + \lambda(A) + \lambda(Z_2 \cap A^c)$$

que nous avons déjà utilisée. Sous les hypothèses du théorème IX, on a donc $\lambda(Z_2 \cap A^c) = 0$ autrement dit $Z_2 \subset A$ à un ensemble de mesure nulle près. D'autre part, $A + A$ doit être, à un ensemble de mesure nulle près, l'union de $A_1 = A \cap [0, b]$, $]b, 2d - c[$ et $d + A_2 = d + (A \cap [d - c, d])$. L'idée est donc que A ne doit pas « grossir » par addition sur les bords $[0, b]$ et $[d - c, d]$. Cela implique que la taille de A au bord de l'intervalle $[0, d]$ tend vers 0 au moins quadratiquement en la distance au bord. La preuve de ce résultat est technique. Elle fait appel à la minoration de Ruzsa (4.8). Lidée principale consiste à noter $A_u = A \cap [0, u]$ et à minorer la mesure de $A_{(n+1)u}$ en fonction de celle A_{nu} et A_u en utilisant à chaque étape le ratio $\lambda(A_{nu})/\lambda(A_u)$ et (4.8).

Notons que ce résultat est presque optimal, comme le montre l'exemple suivant.

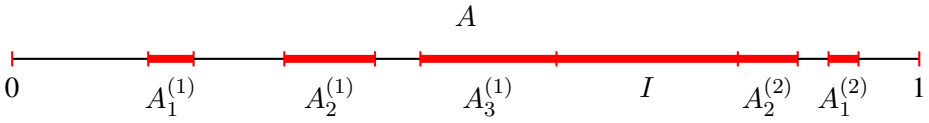
Soient δ, a_1 et a_2 des réels positifs et n, m des entiers positifs satisfaisant à

$$(n-1)a_1 + (m-1)a_2 = 1 - 2\delta < 1. \tag{4.10}$$

Définissons l'ensemble $A \subset [0, 1]$ suivant :

$$A := \left(\bigcup_{k=0}^{n-1} A_k^{(1)} \right) \cup I \cup \left(\bigcup_{k=0}^{m-1} A_k^{(2)} \right)$$

avec $A_k^{(1)} = \left[ka_1 \left(1 - \frac{1}{n}\right), ka_1 \right]$, $A_k^{(2)} = \left[1 - ka_2, 1 - ka_2 \left(1 - \frac{1}{m}\right) \right]$ et
$I = [(n-1)a_1, 1 - (m-1)a_2]$.



L'ensemble A est un sous-ensemble fermé de $[0, 1]$ de mesure $\frac{1}{2} + \delta$ par (4.10) et de diamètre 1. De plus.

$$A + A = \left(\bigcup_{k=0}^{n-1} A_k^{(1)} \right) \cup [(n-1)a_1, 2 - (m-1)a_2] \cup \left(\bigcup_{k=0}^{m-1} A_k^{(2)} \right)$$

donc $\lambda(A+A) = 1 + \lambda(A) = d_A + \lambda(A) < 3\lambda(A)$.
Pour $x = \ell a_1$ avec $\ell \leq n-1$, on a

$$\lambda(A \cap [0,x]) = \frac{a_1}{n} \sum_{k=1}^{\ell} k = \frac{\ell a_1(\ell+1)}{2n} = x\frac{\ell+1}{2n}.$$

Ainsi $c_1 := \sup\{x \,:\, \lambda(A \cap [0,x]) \leq \frac{1}{2}x\} = (n-1)a_1$ et

$$\lambda(A \cap [0,x]) = x\frac{\ell a_1 + a_1}{2na_1} = \frac{x(x+a_1)}{2(c_1+a_1)} \geq \frac{x^2}{2c_1}.$$

Pour $x = a_1$ en particulier, on a $\lambda(A \cap [0,x]) = \frac{x^2}{(c_1+x)}$, ce qui montre l'optimalité de notre minoration au voisinage du bord.

Chapitre 5

Structure des ensembles de petite somme dans le cercle

Ce chapitre porte sur des travaux réalisés en collaboration avec Pablo Candela. Ils ont donné lieu à la publication [12].

Pour décrire les ensembles bornés de réels de constante de doublement plus petite que 3, nous avons utilisé une caractérisation des sous-ensembles de $\mathbb{T}$ de constante de doublement plus petite que 2. Plus généralement, en travaillant modulo le diamètre de l'ensemble, on peut passer d'une description des sous-ensembles de $\mathbb{T}$ de constante de doublement plus petite que K à une description des ensembles bornés de réels de constante de doublement plus petite que $K+1$. Le même phénomène est à l'oeuvre pour les entiers, avec une complexité plus importante engendrée par la non primalité éventuelle du diamètre.

C'est cette simple observation qui a motivé notre recherche de structure pour les sous-ensembles de $\mathbb{T}$ de constante de doublement plus petite que 3. Nous avons cependant aussi utilisé nos résultats pour donner une majoration non triviale de la taille d'un sous-ensemble de $\mathbb{T}$ sans 3-somme.

5.1 Le cas discret

Commençons par rappeler les résultats connus dans $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. Nous les utiliserons pour démontrer des résultats similaires dans $\mathbb{T}$. La recherche d'un analogue du théorème $3k-4$ de Freiman, qui concerne des ensembles d'entiers, dans d'autres groupes, en particulier dans $\mathbb{Z}/p\mathbb{Z}$, a fait l'objet de nombreux articles dans la littérature. Citons par exemple [Fm61, Gry13, Nat96, Rd06, SZ09]. Dans [Gry13], Grynkiewicz énonce une conjecture qui donnerait un théorème $3k-4$ (dans sa version complète) dans $\mathbb{Z}/p\mathbb{Z}$.

Conjecture 3 (Grynkiewicz) *Soient p un nombre premier et r un entier positif. Si A et B sont deux sous-ensembles non vides de $\mathbb{Z}/p\mathbb{Z}$ tels que $|A| \geq |B|$ et*

$$|A+B| = |A| + |B| + r - 1 \leq \tfrac{1}{2}(p + |A| + |B|) - 2, \quad \textit{et} \quad r \leq |B| - 3, \tag{5.1}$$

alors il existe des intervalles $I, J, K \subset \mathbb{Z}/p\mathbb{Z}$ et un élément $n \in \mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ tels que $n\cdot A \subset I$, $n\cdot B \subset J$, $n\cdot(A+B) \supset K$, et $|I| \leq |A| + r$, $|J| \leq |B| + r$, $|K| \geq |A| + |B| - 1$.

Précisons avant tout la terminologie employée dans cette conjecture : on appelle intervalle de $\mathbb{Z}_p$ toute progression arithmétique de pas 1 dans $\mathbb{Z}/p\mathbb{Z}$ et on note $n \cdot A$ l'ensemble $\{na,\, a \in A\}$. La conclusion annoncée par cette conjecture peut donc être formulée ainsi : A et B sont respectivement inclus dans des progressions arithmétiques de même pas et de longueurs respectives $|A| + r$ et $|B| + r$, $A + B$ contient

une progression arithmétique de même pas et de longueur $|A| + |B| - 1$.
Dans [SZ09], une conjecture antérieure de Serra et Zémor énonçait un résultat similaire dans le cas particulier $A = B$, mais sans la conclusion sur la structure de $A + A$. La conjecture de Serra et Zémor avait déjà été démontrée pour des ensembles de petite taille dans [GR06, BLR98].
Notons que dans le contexte de $\mathbb{Z}_p$, la majoration $|A+B| \leq \frac{1}{2}(p+|A|+|B|) - 2$ qui n'apparaissait pas dans le cas des entiers, est nécessaire comme le démontre un exemple de Serra et Zémor dans [SZ09].

Dans [Gry13, Conjecture 19.5], Grynkiewicz énonce une version symétrique (et équivalente) de la conjecture 3.

Conjecture 4 *Soient p un nombre premier, r un entier positif et A_1, A_2, A_3 trois sous-ensembles de $\mathbb{Z}_p$ tels que*

$$|A_1|, |A_2|, |A_3| > r + 2, \qquad |A_1| + |A_2| + |A_3| > p - r, \qquad |A_1 + A_2 + A_3| < p. \tag{5.2}$$

Alors il existe des intervalles I_1, I_2, I_3 de $\mathbb{Z}_p$ et un élément $n \in \mathbb{Z}_p \setminus \{0\}$ tels que $n \cdot A_j \subset I_j$ et $|I_j| \leq |A_j| + r$ pour $j = 1, 2, 3$.

Un résultat de Grynkiewicz [Gry13, Theorem 21.8] permet de montrer cette conjecture (et donc la conjecture 3) sous l'hypothèse supplémentaire $0 \leq r \leq cp - 1.2$ avec $c = 3.1 \cdot 10^{-1549}$. Dans le cas $A = B$, le résultat antérieur de Serra et Zémor [SZ09] permet obtenir l'inclusion de A dans une progression arithmétique de longueur $|A| + r$ sous l'hypothèse $r = \varepsilon|A|$ avec $0 \leq \varepsilon \leq 10^{-4}$ et $p \geq 2^{94}$.

5.2 Le cas continu

Dans la suite de ce chapitre, on note μ la mesure de Haar sur $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ et $\underline{\mu}$ la mesure de Haar intérieure.
La recherche d'analogues du théorème $3k-4$ de Freiman dans $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ remonte au moins à 1973, date de la parution des travaux de Freiman, Judin, et Moskvin [MFmJ73].

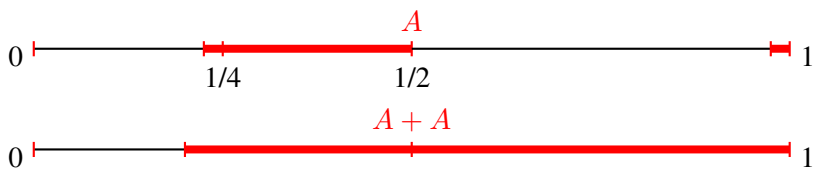
Dans [Bil98], Bilu propose une conjecture [Bil98, Conjecture 1.2] donnant la structure des sous-ensembles de $\mathbb{T}^d$ de petite somme. Dans le cas de la dimension 1, i.e. pour $\mathbb{T}$, cette conjecture s'énonce ainsi :

Conjecture 5 (Bilu) *Si $A, B \subset \mathbb{T}$ vérifient $\alpha = \underline{\mu}(A) \geq \underline{\mu}(B) = \beta$ et $\underline{\mu}(A+B) < \min(\alpha + 2\beta, 1)$, alors il existe des intervalles fermés $I, J \subset \mathbb{T}$ et un entier strictement positif n tels que $n \cdot A \subset I$, $n \cdot B \subset J$, et $\mu(I) \leq \underline{\mu}(A+B) - \underline{\mu}(B)$, $\mu(J) \leq \underline{\mu}(A+B) - \underline{\mu}(A)$.*

Bilu [Bil98, Theorem 1.4] démontre cette conjecture sous la condition supplémentaire $\alpha/\tau \leq \beta \leq \alpha \leq c(\tau)$, où c est une constante positive dépendant de $\tau \geq 1$. Notons cependant que cette conjecture ne peut être valide sans condition supplémentaire pour des réels α et β de $]0, 1[$ arbitraires comme le montre l'exemple suivant.
Pour $\delta \in]0, 1/8[$, considérons l'ensemble

$$A = \left]\tfrac{1}{4} - \delta,\ \tfrac{1}{2}\right] \cup \left]1 - \delta,\ 1\right] \subset \mathbb{T}.$$

Nous le représentons ci-dessous, ainsi que la somme $A + A$, comme des sous-ensembles de $[0, 1]$.



Pour un tel ensemble, $\mu(A) = \frac{1}{4} + 2\delta$, et $\mu(A+A) = 2\mu(A) + 2\left(\frac{1}{8} - \delta\right) = \frac{3}{4} + 2\delta = \frac{1}{2} + \mu(A) < 3\mu(A)$ mais quelle que soit la valeur de l'entier positif n, l'ensemble $n \cdot A$ ne peut être inclus dans un intervalle de $\mathbb{T}$ de longueur $\mu(A + A) - \mu(A) = \frac{1}{2}$. Cet exemple est une adaptation au contexte continu d'un exemple de Serra et Zémor [SZ09] dans $\mathbb{Z}_p$.

Nous énonçons dans le contexte continu l'analogue de la conjecture 3.

Conjecture 6 *Soit ρ un réel de $]0, 1[$. Soient $A, B \subset \mathbb{T}$ deux ensembles tels que*

$$\underline{\mu}(A + B) \;=\; \underline{\mu}(A) + \underline{\mu}(B) + \rho \;<\; \tfrac{1}{2}\big(1 + \underline{\mu}(A) + \underline{\mu}(B)\big), \quad \textit{et} \quad \rho < \underline{\mu}(B) \leq \underline{\mu}(A).$$

Alors il existe des intervalles fermés I, J de $\mathbb{T}$, un intervalle K de $\mathbb{T}$ ouvert et un entier positif n tels que $n \cdot A \subset I$, $n \cdot B \subset J$, $K \subset n \cdot (A + B)$, et $\mu(I) \leq \underline{\mu}(A) + \rho$, $\mu(J) \leq \underline{\mu}(B) + \rho$, $\mu(K) \geq \underline{\mu}(A) + \underline{\mu}(B)$.

Comme dans le cas discret, on peut donner un énoncé symétrique équivalent à cette conjecture.

Conjecture 7 *Soit ρ un réel de $]0, 1[$. Soient A_1, A_2, A_3 des sous-ensembles de $\mathbb{T}$ tels que*

$$\underline{\mu}(A_1), \underline{\mu}(A_2), \underline{\mu}(A_3) > \rho, \quad \underline{\mu}(A_1) + \underline{\mu}(A_2) + \underline{\mu}(A_3) > 1 - \rho, \quad \underline{\mu}(A_1 + A_2 + A_3) < 1. \tag{5.3}$$

Alors il existe des intervalles fermés $I_1, I_2, I_3 \subset \mathbb{T}$ et un entier positif n tels que $n \cdot A_j \subset I_j$ et $\mu(I_j) \leq \underline{\mu}(A_j) + \rho$ pour $j = 1, 2, 3$.

Lors de plusieurs discussions avec l'un ou l'autre des auteurs de [11], Imre Ruzsa avait suggéré qu'un énoncé symétrique de ce type de résultat était préférable. Ce n'est qu'après cet entretien que nous avons eu connaissance, ainsi que Ruzsa, de l'énoncé symétrique donné par Grynkiewicz dans [Gry13] pour $\mathbb{Z}/p\mathbb{Z}$.

Dans un travail en collaboration avec Pablo Candela [11], nous avons démontré les conjectures 6 et 7 pour de petites valeurs de ρ.

Théorème X (Candela, de Roton) *Sous l'hypothèse supplémentaire $\rho < c = 3.1 \cdot 10^{-1549}$, les conjectures 6 et 7 sont vraies.*

Notons que la borne $c = 3.1 \cdot 10^{-1549}$ provient directement du résultat de Grynkiewicz dans $\mathbb{Z}_p$. Dans le cas $A = B$, en utilisant le résultat de Serra et Zémor plutôt que celui de Grynkiewicz, on obtient le résultat suivant.

Théorème XI (Candela, de Roton) *Soit ε un réel tel que $0 \leq \varepsilon \leq 10^{-4}$. Soit A un sous-ensemble de $\mathbb{T}$ vérifiant $\underline{\mu}(A) > 0$ et*

$$\underline{\mu}(A + A) = (2 + \varepsilon)\underline{\mu}(A) < \frac{1}{2} + \underline{\mu}(A).$$

Alors il existe un intervalle I fermé de $\mathbb{T}$, un intervalle K ouvert de $\mathbb{T}$ et un entier positif n tels que $n \cdot A \subset I$, $K \subset n \cdot (A + A)$, $\mu(I) \leq \underline{\mu}(A + A) - \underline{\mu}(A)$ et $\mu(K) \geq 2\underline{\mu}(A)$.

Dans [Bil98], Bilu obtient un résultat pour les petits sous-ensembles de petite somme dans $\mathbb{T}^d$ en se ramenant à un ensemble de réels de petite somme et en utilisant un argument de rectification. Nous utilisons certaines de ses idées dans [11] mais la philosophie générale est très différente. Nous expliquons ici quelques idées (très simplifiées, les arguments originaux sont complexes) de la démonstration de Bilu mais par soucis de simplicité, nous nous restreignons au cas d'un seul ensemble $A \subset \mathbb{T}$ de constante de doublement plus petite que 3.

Bilu introduit, pour un irrationel $\theta \in \mathbb{T}$, l'ensemble d'entiers $\mathcal{B}(\theta, A) = \{n \in \mathbb{Z} : \theta n \in A\}$. Grâce au théorème de Weyl, il montre que cet ensemble d'entiers a une petite constante de doublement et il lui applique le théorème inverse de Freiman-Ruzsa pour les entiers. Il en déduit qu'il existe un entier m et un réel $\varepsilon > 0$ tels que pour tout entier n de $\mathcal{B}(\theta, A)$, $\|nm\theta\|_{\mathbb{Z}} \leq \varepsilon$ (cette étape essentielle est ardue). Par le théorème de Kronecker et par l'irrationalité de θ, il obtient $mA \subset [-\varepsilon, \varepsilon]$. Ici, ε dépend de $\alpha = \mu(A)$. Si α est suffisamment petit, mA est inclus dans un intervalle de longueur $< 1/2$ et sa somme se comporte donc comme une somme dans $\mathbb{R}$. Bilu repasse aux entiers, peut considérer une somme dans $\mathbb{Z}$ plutôt que dans $\mathbb{Z}_p$ et utilise alors le théorème $3k-4$ de Freiman pour les entiers. Ce dernier argument est un argument de rectification et repose sur le fait que α est petit. Bilu conclut sa démonstration en commençant par considérer des ensembles ouverts de Jordan, pour lesquels la discrétisation donne une image fidèle de l'ensemble, puis des ensembles fermés et en passant enfin au cas général. Nous empruntons à Bilu certains arguments de cette dernière partie dans [11] pour passer des ensembles simples aux ensembles quelconques.

5.3 Les idées de la démonstration

Nous exposons ici les idées principales de notre démonstration dans [11] de la conjecture 7 avec l'hypothèse supplémentaire $\rho < c = 3.1 \cdot 10^{-1549}$. La valeur de cette constante c provient du théorème de Grynkiewicz [Gry13, Theorem 21.8] qui établit la conjecture 3 sous l'hypothèse supplémentaire $0 \leq r \leq cp - 1.2$.

5.3.1 Discrétisation

La première étape consiste à utiliser un argument de discrétisation. Étant donné un sous-ensemble A de $\mathbb{T}$ et un nombre premier p, on définit l'ensemble $A_p = A \cap \frac{1}{p}\mathbb{Z}_p$. Afin que l'ensemble A_p donne une image fidèle de l'ensemble A, on se restreint dans un premier temps à des ensembles que l'on appellera simples et qui sont des unions finis d'intervalles de $\mathbb{T}$. Pour se convaincre de la nécessité d'une telle restriction, on peut réfléchir au peu d'information que A_p donnerait sur un ensemble de $\mathbb{T}$ qui ne contiendrait que des irrationnels.

Soit donc ρ un réel de $]0, 1[$ et A_1, A_2, A_3 des sous-ensembles simples de $\mathbb{T}$ tels que

$$\underline{\mu}(A_1), \underline{\mu}(A_2), \underline{\mu}(A_3) > \rho, \quad \underline{\mu}(A_1) + \underline{\mu}(A_2) + \underline{\mu}(A_3) > 1 - \rho, \quad \underline{\mu}(A_1 + A_2 + A_3) < 1. \tag{5.4}$$

Considérons les ensembles $A_{j,p} = (A_j)_p$. Nous appliquons le théorème de Grynkiewicz aux sous ensembles $pA_{1,p}$, $pA_{2,p}$, $pA_{3,p}$ de $\mathbb{Z}_p$ avec r un entier proche de ρp. On obtient alors pour p suffisamment grand l'existence de trois intervalles $I_{1,p}$, $I_{2,p}$, $I_{3,p}$ de $\frac{1}{p}\mathbb{Z}_p$ et d'un entier $n \in -]p/2, p/2[$ tels que $n \cdot A_{j,p} \subset I_{j,p}$ et $\frac{1}{p}|I_{j,p}| \leq \frac{1}{p}|A_{j,p}| + \frac{r}{p} \sim \mu(A_j) + \rho$. Nous passons ici sous silence les détails techniques liés à cette discrétisation.

Revenant à la définition de $A_{j,p}$, on remarque que $A_j \subset A_{j,p} + [-1/(2p), 1/(2p)]$, ce qui implique

$$n \cdot A_j \subset n \cdot A_{j,p} + \left[-\tfrac{|n|}{2p}, \tfrac{|n|}{2p}\right] \subset I_{j,p} + \left[-\tfrac{|n|}{2p}, \tfrac{|n|}{2p}\right].$$

Notant I_j l'intervalle fermé $I_{j,p} + \left[-\frac{|n|}{2p}, \frac{|n|}{2p}\right]$, nous avons donc montré $n \cdot A_j \subset \mu(I_j)$ avec

$$\mu(I_j) \leq \frac{1}{p}|I_{j,p}| + \tfrac{|n|}{p} \sim \mu(A_j) + \rho + \tfrac{|n|}{p}. \tag{5.5}$$

Jusqu'ici, le seul argument utilisé est un argument classique de discrétisation. À présent, nous avons besoin de pouvoir contrôler le terme $\frac{|n|}{p}$. En effet, on cherche à obtenir la conclusion $\mu(I_j) \lesssim \mu(A_j) + \rho$ et

rien ne dit *a priori* que le terme $\frac{|n|}{p}$ disparait lorsque p tend vers l'infini. Il nous faut donc contrôler la taille de $|n|$ lorsque les ensembles A_j sont des ensembles simples, c'est à dire des unions finies d'intervalles ouverts de $\mathbb{T}$. Nous allons établir une majoration de $|n|$ qui dépendra du nombre d'intervalles composant les ensembles A_j. Pour cela, nous faisons appel à l'analyse de Fourier.

5.3.2 Analyse de Fourier pour le contrôle de n

Soit A un ensemble de réels qui est l'union de m intervalles ouverts de $\mathbb{T}$. Alors, quitte à prendre p un nombre premier assez grand, l'ensemble $B = pA_p$ est l'union de m intervalles de $\mathbb{Z}_p$.

Si J est un intervalle de $\mathbb{Z}_p$, alors un simple calcul permet de montrer, pour tout $s \in \mathbb{Z}_p \setminus \{0\}$, la majoration

$$|\widehat{\mathbf{1}_J}(s)| \leq \frac{1}{p}\frac{2}{|1-e^{2i\pi s/p}|} \leq \frac{1}{2|s|_p},$$

où $|s|_p$ est la valeur absolue du représentant dans l'intervalle $]-p/2, p/2[$ de la classe de s modulo p. La première inégalité provient du calcul de la somme des termes consécutifs d'une suite géométrique, la seconde de l'inégalité classique $|1-e^{2i\pi\theta}| \geq 4|\theta|$ pour $\theta \in]-1/2, 1/2[$. Par conséquent, si B est l'union de m intervalles disjoints, par linéarité de la transformée de Fourier, on a pour tout $s \in \mathbb{Z}_p \setminus \{0\}$, la majoration

$$|\widehat{\mathbf{1}_B}(s)| \leq \frac{m}{2|s|_p}. \tag{5.6}$$

Cette majoration permet en particulier de majorer $|s|_p$ si s est une fréquence en laquelle le coefficient de $\widehat{\mathbf{1}_B}$ est grand.

Nous combinons cette première observation avec le fait que si $n \cdot B$ est inclus dans un petit intervalle I de $\mathbb{Z}_p$ (pour un $n \in \mathbb{Z}_p \setminus \{0\}$), alors le coefficient de Fourier de $\widehat{\mathbf{1}_B}$ en n doit être grand. En effet, supposons $n \cdot B \subset I$ et $|I| < p/2$. Alors

$$\begin{aligned}\widehat{1_B}(n) &= \tfrac{1}{p}\sum_{j\in\mathbb{Z}_p} 1_B(j)\, e^{2\pi i \frac{nj}{p}} = \tfrac{1}{p}\sum_j 1_{n\cdot B}(j)\, e^{2\pi i \frac{j}{p}} \\ &= \tfrac{1}{p}\sum_j 1_I(j)\, e^{2\pi i \frac{j}{p}} + \tfrac{1}{p}\sum_j (1_{n\cdot B}(j) - 1_I(j))\, e^{2\pi i \frac{j}{p}}.\end{aligned}$$

En majorant la dernière somme trivialement par $\frac{1}{p}|I \setminus n\cdot B|$ et en opérant des calculs similaires aux calculs précédents, on obtient

$$|\widehat{1_B}(n)| \geq \tfrac{1}{p}\left(\frac{|1-e^{2\pi i \frac{|I|}{p}}|}{|1-e^{2\pi i \frac{1}{p}}|} + |B| - |I|\right) > \tfrac{1}{p}\big(|B| - (1-\tfrac{2}{\pi})|I|\big). \tag{5.7}$$

Rappelons qu'au paragraphe précédent, nous étions arrivés à la conclusion : $n\cdot A_{j,p} \subset I_{j,p}$ et $\frac{1}{p}|I_{j,p}| \leq \frac{1}{p}|A_{j,p}| + \frac{r}{p} \sim \mu(A_j) + \rho$. Quitte à choisir j minimisant la mesure de A_j et p assez grand, on obtient $|I_{j,p}| \leq p(\mu(A_j)+\rho) < p/2$. Nous appliquons (5.7) à $B = A_{j,p}$ puis (5.6) et obtenons $|n| \leq 2m/\mu(A_j)$. L'entier n est donc borné et le terme $|n|/p$ qui nous gênait tend bien vers 0 lorsque p tend vers l'infini.

Ceci permet de montrer le résultat pour des ensembles simples.

5.3.3 Passage à des ensembles quelconques

Dans l'argumentation précédente, la structure des ensembles A_j comme union finie d'intervalles ouverts jouait un rôle essentiel. Nous allons néanmoins étendre notre résultat à des ensembles quelconques.

Commençons par nous restreindre au cas d'ensembles A_1, A_2, A_3 fermés dans $\mathbb{T}$.
Notant $I_\delta =]-\delta, \delta[$ pour tout $\delta > 0$, nous commençons par approcher tout ensemble A fermé de $\mathbb{T}$ par l'ensemble $A + I_\delta$. Notons que A étant fermé borné, donc compact, et $A + I_\delta$ étant un recouvrement ouvert de A, il existe un ensemble A' qui est une union d'un nombre fini de traslatés de I_δ, donc un ensemble simple, tel que $A \subset A' \subset A + I_\delta$. Quitte à prendre δ suffisamment petit, on peut sous les hypothèses de la conjecture 7 avec $\rho < c$, appliquer le résultat démontré aux ensembles simples A'_1, A'_2 et A'_3 ainsi construits. Ceci garantit l'existence d'un entier n non nul et de trois intervalles fermés $I_1, I_2, I_3 \subset \mathbb{T}$ pour lesquels $n \cdot A_j \subset I_j$ et $\mu(I_j) \leq \mu(A_j) + \rho$ pour $j \in \{1, 2, 3\}$. On ne détaille pas ici les aspects techniques de la démonstration durant laquelle il faut, à chaque étape, préciser les dépendances en δ.

Venons-en au cas général et supposons que A_1, A_2, A_3 sont des sous-ensembles de $\mathbb{T}$ vérifiant $\underline{\mu}(A_1) = \min_{j=1}^3 \underline{\mu}(A_j) > \rho$, $\underline{\mu}(A_1) + \underline{\mu}(A_2) + \underline{\mu}(A_3) > 1 - \rho$ et $\underline{\mu}(A_1 + A_2 + A_3) < 1$ avec $\rho < c$.
Comme la mesure considérée est une mesure intérieure, l'idée naturelle pour étendre notre résultat à des ensembles quelconques consiste à approcher chaque ensemble A_j par un ensemble fermé F_j de mesure très proche de la mesure intérieure de A_j, puis à appliquer le résultat déjà démontré pour les ensembles fermés à F_1, F_2 et F_3. Cette approche permet d'obtenir l'existence d'un entier n non nul et de trois intervalles fermés $I_1, I_2, I_3 \subset \mathbb{T}$ pour lesquels $n \cdot F_j \subset I_j$ et $\mu(I_j) \leq \mu(F_j) + \rho$ pour $j \in \{1, 2, 3\}$.
Ce raisonnement ne permet toutefois pas de conclure. En effet, rien ne dit que $n \cdot A_j$ est inclus dans $n \cdot F_j$. C'est l'inclusion inverse que l'on a. Pour garantir que $n \cdot A_j$ est proche de $n \cdot F_j$, il faut une construction plus sophistiquée. Nous l'avons essentiellement empruntée à Bilu dans [Bil98].
Étant donné un ensemble $A \subset \mathbb{T}$, on peut pour tout $\varepsilon > 0$ et tout entier n positif, trouver un ensemble fini $E_n \subset A$ tel que $A \subset E_n + [-\varepsilon/n, \varepsilon/n]$ (c'est un argument de compacité). Si F est un sous-ensemble fermé de A, l'ensemble $A' = F \cup E_n$ vérifie alors $n \cdot A \subset n \cdot A' + [-\varepsilon, \varepsilon]$ et $\mu(A') = \mu(F)$.
Si nous appliquons ceci à chaque couple d'ensembles (A_j, F_j), nous obtenons trois ensembles fermés A'_1, A'_2 et A'_3 tels que pour tout $j \in \{1, 2, 3\}$, $F_j \subset A'_j \subset A_j$, $n \cdot A_j \subset n \cdot A'_j + [-\varepsilon, \varepsilon]$, $\mu(A'_j) = \mu(F_j)$ et $n \cdot F_j \subset I_j$. On ne peut toujours pas conclure, il faudrait que ce soit $n \cdot A'_j$ qui soit inclus dans I_j. On pourrait envisager d'appliquer notre résultat pour les ensembles fermés A'_j directement mais A'_j ne peut être défini qu'une fois n fixé.

Pour contourner cette difficulté, on va construire un ensemble fermé A' qui vérifie $\mu(A') = \mu(F)$, $n \cdot A \subset n \cdot A' + [-\varepsilon, \varepsilon]$ et $\mu(A') = \mu(F)$, non plus pour un seul entier n mais pour un nombre fini de n et on va s'assurer que les entiers n qui seront susceptibles de convenir sont bien en nombre fini.
Reprenons donc le raisonnement. Soit F_1 un sous-ensemble fermé de A_1 dont la mesure est très proche de la mesure intérieure de A_1. D'abord le Lemme 4.2.1 de [Bil98] permet d'affirmer que l'ensemble X des entiers n tels que $\mu(n \cdot F_1) \leq \underline{\mu}(A_1) + \rho$ est fini. Ensuite, en posant $A'_1 = F_1 \cup \left(\bigcup_{n \in X} E_n\right)$, on a $n \cdot A_1 \subset n \cdot A'_1 + [-\varepsilon, \varepsilon]$ pour tout $n \in X$ et $\mu(A'_1) = \mu(F_1) \sim \mu(A_1)$. De même, on construit A'_2 et A'_3 tels que pour $j = 2, 3$ on ait $n \cdot A_j \subset n \cdot A'_j + [-\varepsilon, \varepsilon]$ pour tout $n \in X$ et $\mu(A'_j) \sim \mu(A_j)$.
Appliquant maintenant notre résultat aux ensembles fermés A'_j, on obtient l'existence de trois intervalles fermés I'_1, I'_2 et I'_3 et d'un entier n non nul tels que $n \cdot A'_j \subset I_j$ et $\mu(I_j) \leq \mu(A'_j) + \rho$ pour $j \in \{1, 2, 3\}$. En particulier $n \in X$, ce qui entraîne $n \cdot A_j \subset I_j = I'_j + [-\varepsilon, \varepsilon]$ et le résultat.

On démontre ainsi le théorème X. La conclusion donnant des informations sur la structure de A sous les hypothèses du théorème XI se montre de la même manière en utilisant la résultat de Serra et Zémor plutôt que celui de Grynkiewicz. Pour obtenir la structure de $A + A$, le théorème de Serra et Zémor ne donnant pas d'information à ce sujet, nous avons utilisé les résultats de [10].

5.4 Ensembles sans k-somme dans $\mathbb{T}$

Soit k un entier positif donné. Le théorème XI obtenu au paragraphe précédent permet d'obtenir une majoration non triviale pour la mesure d'un sous-ensemble A de $\mathbb{T}$ Haar-mesurable sans k-somme, c'est à dire sans solution à l'équation $x + y = kz$. Notons

$$d_k(\mathbb{T}) = \sup\{\mu(A) : A \text{ est un sous-ensemble de } \mathbb{T} \text{ Haar mesurable sans } k\text{-somme}\}.$$

Notons d'abord que si A est un ensemble Haar-mesurable sans k-somme, alors $(A + A) \cap k \cdot A = \emptyset$ donc par l'inégalité de Raikov (4.4)

$$3\mu(A) \leq \underline{\mu}(A + A) + \mu(k \cdot A) = \underline{\mu}((A + A) \cup k \cdot A) \leq 1, \text{ donc } \mu(A) \leq 1/3. \tag{5.8}$$

Comme l'intervalle $]\frac{1}{3}, \frac{2}{3}[$ est sans (1-)somme, on obtient immédiatement $d_1(\mathbb{T}) = 1/3$. Le cas $k = 2$ est un cas à part dans la mesure où l'équation $x + y = 2z$ est invariante et dans ce cas, on a $d_1(\mathbb{T}) = 0$. Supposons désormais $k \geq 3$. Le Théorème XI nous permet d'améliorer la majoration (5.8) comme suit.

Théorème 7 *Soit $\varepsilon > 0$ un réel pour lequel le Théorème XI est valable, et soit $k \geq 3$ un entier. Alors $d_k(\mathbb{T}) \leq \max\{\frac{1}{3+\varepsilon}, \frac{1+k\varepsilon}{k+2}\}$.*

Avec la valeur de ε donnée par Serra et Zémor, on obtient donc $d_k(\mathbb{T}) \leq \frac{1}{3+10^{-4}}$ pour $k \geq 3$.

La démonstration repose sur une disjonction de cas : si la somme $A+A$ est de mesure intérieure au moins $(2 + \varepsilon)\mu(A)$, alors en raisonnant comme pour l'équation (5.8), on montre que $\mu(A) \leq 1/(3 + \varepsilon)$; dans le cas contraire, on peut appliquer le théorème XI avec ε. Plaçons-nous dans ce second cas et supposons A fermé, donc $A + A$ mesurable. Il existe donc un intervalle I de mesure $\mu(I) \leq \mu(A + A) - \mu(A)$ et un entier positif tels que $n \cdot A \subset I$. Nous allons montrer que cet intervalle I est presque sans k-somme.

Afin de préciser ce « presque », introduisons la notion de préimage. Si X est un sous-ensemble de $\mathbb{T}$ et n un entier positif, on définit l'ensemble $n^{-1}X = \{t \in \mathbb{T} : n\,t \in X\}$. Notons que $X \subset \mathbb{T}$ est sans k-somme si et seulement si $X \cap k^{-1}(X + X) = \emptyset$. Notons aussi que dans le cas où l'on s'est placé, l'intervalle I vérifie $A \subset n^{-1}I$. L'avantage de la préimage $n^{-1}D$ par rapport à l'image $n \cdot C$ est que la mesure $n^{-1}D$ est égale à la mesure de D alors que la mesure de $n \cdot C$ peut être jusque n fois supérieure à la mesure de C.

Nous allons montrer $\mu\big(I \cap k^{-1}(I + I)\big) \leq 2\varepsilon\,\mu(I)$. Pour cela, introduisons l'ensemble $B = n^{-1}I$. On a

$$\mu(B \setminus A) = \mu(B) - \mu(A) = \mu(I) - \mu(A) \leq \varepsilon\,\mu(A) \leq \varepsilon\,\mu(I) \tag{5.9}$$

et, puisque $\mu(I) \leq \mu(A + A) - \mu(A) \leq (1 + \varepsilon)\mu(A) \leq \mu(A) + \varepsilon\mu(I)$, on a

$$\mu\big((B + B) \setminus (A + A)\big) = \mu\big(n^{-1}(I + I)\big) - \mu(A + A) = 2\mu(I) - \mu(A + A) \leq \varepsilon\,\mu(I). \tag{5.10}$$

Or, puisque $A \cap (k^{-1}(A + A)) = \emptyset$, on a

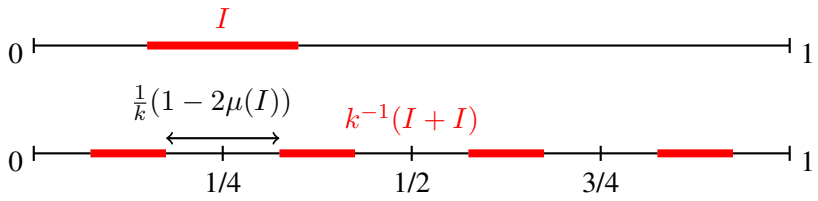
$$\begin{aligned} B \cap k^{-1}(B + B) \;&\subset\; \big[B \cap k^{-1}(A + A)\big] \cup k^{-1}\big[(B + B) \setminus (A + A)\big] \\ &\subset\; (B \setminus A) \cup k^{-1}\big[(B + B) \setminus (A + A)\big], \end{aligned}$$

donc $\mu\big(I \cap k^{-1}(I + I)\big) \leq 2\varepsilon\,\mu(I)$.

Nous voici donc ramenés à la recherche d'une majoration pour la mesure d'un intervalle de $\mathbb{T}$ « presque » sans k-somme. Notons d'abord qu'un intervalle I de $\mathbb{T}$ sans k-somme ne peut être de mesure supérieure à $1/(k + 2)$ car $k \cdot I$ et $I + I$ sont des sous-ensembles disjoints de $\mathbb{T}$ de mesures respectives

$k\mu(I)$ et $2\mu(I)$. Ce majorant est par ailleurs atteint par l'intervalle $I = \left[\frac{2}{k^2-4}, \frac{k}{k^2-4}\right[$ qui est sans k-somme.
Nous montrons qu'un intervalle « presque » sans k-somme ne peut être de mesure beaucoup plus grande que $1/(k+2)$. Plus précisément, si $\mu\big(I \cap k^{-1}(I+I)\big) \leq 2\varepsilon\mu(I) < \mu(I)$, alors $\mu(I) \leq \frac{1+k\varepsilon}{k+2}$.
En effet, $I+I$ est un intervalle fermé de $\mathbb{T}$ de mesure $2\mu(I)$, et $k^{-1}(I+I)$ est l'union de k copies de $I+I$ contractées par un facteur $1/k$, en progression arithmétique de pas $1/k$. Le complément de $k^{-1}(I+I)$ est donc l'union de k intervalles ouverts de mesure $\frac{1}{k}(1-2\mu(I))$ et I ne peut couvrir beaucoup de ces intervalles puisque la mesure de $I \cap k^{-1}(I+I)$ est petite. cela implique que I ne peut pas être trop étendu et donne donc la majoration de $\mu(I)$ attendue.

Plutôt que de détailler ces arguments, nous les illustrons par un dessin pour lequel on a choisit $k = 4$.



D'après la correspondance établie dans [CS11] entre ce problème dans $\mathbb{T}$ et son analogue dans $\mathbb{Z}_p$, le théorème 7 implique un résultat analogue dans $\mathbb{Z}_p$.

5.5 Ensembles de constante de doublement proche de 3 dans $\mathbb{R}$

À la lecture du chapitre 4, un principe général se dégage : toute information structurelle sur les ensembles de $\mathbb{T}$ de constante de doublement inférieure à c donne une information structurelle sur les sous-ensembles de réels de constante de doublement inférieure à $1+c$. En effet, soit A un ensemble borné de réels. On se ramène aisément à un sous-ensemble fermé de $[0,1]$ de diamètre 1. On note $\tilde{A}$ l'ensemble $A \bmod 1$. Si nous reprenons de plus les notations introduites au chapitre 4, on observe comme précédemment que l'on a

$$\lambda(A+A) = \mu(\tilde{S}_1) + \mu(\tilde{S}_2)$$

où $\tilde{S}_1 = \tilde{A} + \tilde{A}$ et $\tilde{S}_2 = \{x \in [0,1[: \ x \in A+A, \ 1+x \in A+A\}$ sont considérés comme des sous-ensembles de $\mathbb{T}$. Notons par ailleurs que comme $0, 1 \in A$, on a aussi $\tilde{A} \subset \tilde{S}_2$, d'où l'implication suivante :

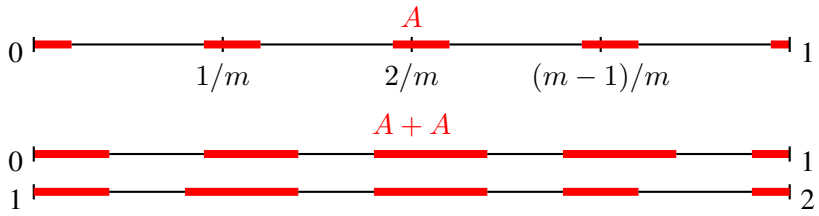
$$\lambda(A+A) \leq (3+c)\lambda(A) \Rightarrow \mu(\tilde{A}+\tilde{A}) \leq (2+c)\mu(\tilde{A}).$$

Cette simple remarque permet d'avoir des informations structurelles pour les ensembles de $\mathbb{R}$ de petite constante de doublement mais ce processus fait perdre de l'information. En effet, dire que $\lambda(A+A)$ est petit c'est à la fois dire que $\mu(\tilde{A}+\tilde{A})$ est petit, ce que nous exploitons mais aussi dire que $\tilde{S}_2 \setminus \tilde{A}$ est petit, ce qui n'est pas utilisé.
On le comprend bien en examinant le cas $c = 0$. Si $A \subset \mathbb{R}$ vérifie $\lambda(A+A) = 3\lambda(A)$, alors $\tilde{A} \subset \mathbb{T}$ vérifie $\mu(\tilde{A}+\tilde{A}) = 2\mu(\tilde{A})$, et d'après le théorème de Kneser [Kne56] on sait qu'il existe un entier positif m et un intervalle $\tilde{I}$ de $\mathbb{T}$ tel que $m \cdot \tilde{A} \subset \tilde{I}$ et $\mu(\tilde{I}) = \mu(\tilde{A})$. Si on en reste à cette observation, on obtient que A est, à un ensemble de mesure nulle près, une réunion de $m+1$ intervalles de la forme suivante :

$$A_m = \left[0, \frac{1}{m}a_+\right] \cup \bigcup_{k=1}^{m-1} \left[\frac{k}{m} - \frac{1}{m}a_-, \frac{k}{m} + \frac{1}{m}a_+\right] \cup \left[1 - \frac{1}{m}a_-, 1\right],$$

avec $0 \leq a_-, a_+$ et $a_- + a_+ = \lambda(A)$. Cependant, on a alors $\lambda(A+A) = \left(4 - \frac{1}{m}\right)\lambda(A)$, comme l'illustre le dessin suivant.

Sur cette illustration, on a choisi $m = 4$.



Ainsi, si $\lambda(A + A) = 3\lambda(A)$, on doit avoir $m = 1$, ce qui implique que A_0 est une réunion de deux intervalles de $\mathbb{R}$ de la forme $[0, a_+] \cup [1 - a_-, 1]$.

Le cas d'une constante de doublement (un peu) plus grande que 3 va se régler de la même manière. Si A est un sous-ensemble fermé de $[0, 1]$ de diamètre 1 vérifiant $\lambda(A + A) \leq (3 + c)\lambda(A)$, alors $\tilde{A}$ vérifie $\mu(\tilde{A} + \tilde{A}) \leq (2 + c)\mu(\tilde{A})$. On applique alors les résultats connus dans le cercle pour trouver la structure de $\tilde{A}$ donc de A. On obtiendra que A est inclus dans un ensemble A_m avec $a_+ + a_-$ assez proche de $\lambda(A)$. On examine ensuite la taille de la somme dans $\mathbb{R}$ pout obtenir une majoration de la taille de m donc du nombre d'intervalles composant A_m.

On obtient ainsi le résultat suivant.

Théorème 8 *Soit $\varepsilon \in [0, 1[$ un réel pour lequel le théorème XI est valable. Soit A un ensemble fermé de $[0, 1]$ de diamètre 1, vérifiant $\lambda(A + A) \leq (3 + \varepsilon)\lambda(A)$ et $0 < \lambda(A) < \frac{1}{2(1+\varepsilon)}$. Alors il existe un entier positif $m \leq \frac{1+\varepsilon}{1-\varepsilon}$ tel que $m \cdot A \bmod 1$ est inclus dans un intervalle fermé I de $\mathbb{T}$ tel que $\mu(I) \leq (1 + \varepsilon)\lambda(A)$.*

La conjecture de Bilu impliquerait la validité de ce théorème pour tout $\varepsilon \in [0, 1[$ sous l'hypothèse $0 < \lambda(A) < 1/4$. Son résultat implique déjà la validité de ce théorème pour tout $\varepsilon \in [0, 1[$ pourvu que $\lambda(A)$ soit suffisamment petit. Notons par ailleurs que si $\varepsilon < 1/3$, ce qui est le cas pour les valeurs pour lesquelles nous savons montrer la validité du théorème XI, alors $m = 1$, ce qui signifie que A est inclus dans une réunion de deux intervalles de la forme $[0, a_+] \cup [1 - a_-, 1]$ avec $a_+ + a_- \leq \lambda(A + A) - \lambda(A)$.

Notons par ailleurs que ce résultat permet de donner une version explicite d'un théorème de Eberhard, Green and Manners [EGM14, Theorem 6.2] qui affirme que pour un ensemble $A \subset [0, 1]$ ouvert satisfaisant à $\lambda(A + A) \leq 4\lambda(A) - \delta$, il existe un intervalle I de longueur $\lambda(I) \gg_\delta 1$ tel que $\lambda(A \cap I) \geq (\frac{1}{2} + \frac{\delta}{7})\lambda(I)$. Notre résultat permet d'obtenir $\lambda(I) \geq \min(\delta/4, \delta^2)$ si $\lambda(A) < \frac{\mathrm{diam}(A)}{4} + \frac{\delta}{2}$ et $\delta > \lambda(A)(1 - \varepsilon)$, avec ε tel que le théorème XI s'applique. Sous la conjecture de Bilu, on obtient en particulier une version effective de [EGM14, Theorem 6.2] pour tout ensemble A tel que $\lambda(A) \leq \frac{\mathrm{diam}(A)}{4}$.

Liste de publications

[0] A. de Roton, *Généralisation du critère de Beurling-Nyman à la classe de Selberg*, C. R. Acad.Sci. Paris, Ser. I **340** (2005), 191-194.

[1] A. de Roton, *Une approche hilbertienne de l'hypothèse de Riemann généralisée*, Bulletin de la SMF **134** (2006), 417-445.

[2] A. de Roton, *On the mean square of the error term for an extended Selberg's class*, Acta Arithmetica **126** (2007), 27-55.

[3] A. de Roton, *Généralisation du critère de Beurling-Nyman à la classe de Selberg*, Transactions of the AMS, **359** (2007), n°12, 6111-6126 (electronic) .

[4] A. de Roton, *Une approche séquentielle de l'hypothèse de Riemann généralisée*, J. Number Theory **129** (2009), pp. 2647-2658.

[5] M. Balazard, A. de Roton, *Sur un critère de Báez-Duarte pour l'hypothèse de Riemann*, Int. J. Number Theory **6** (2010), pp. 883-903.

[6] Harald Andrés Helfgott et Anne de Roton, *Improving Roth's theorem in the primes*, International Math. Research Notices **4** (2011), pp. 767–783.

[7] S. Révész, A. de Roton, *Generalization of the effective Wiener-Ikehara Theorem*, Int. J. Number Theory **09** (2013), pp. 1091-1128.

[8] Alain Plagne et Anne de Roton, *Maximal sets with no solution to* $x + y = 3z$, Combinatorica **36** No 2 (2016), pp. 229–248.

[9] Anne de Roton, Bahman Saffari, Harold S. Shapiro et Gérald Tenenbaum, *Sur le principe d'incertitude pour les familles orthonormales de* $L^2(\mathbb{R})$, Enseignement Mathématique **62** (2016), no. 1-2, pp. 285–300.

[10] A. de Roton, *Small sumsets in* $\mathbb{R}$ *: full continuous* $3k-4$ *theorem, critical sets*, Tome 5 (2018), p.177-196.

[11] Pablo Candela et Anne de Roton, *On sets with no sumset in the circle*, prépublication disponible sur Arxiv.

[12] P. Candela, D. González-Sánchez, A. de Roton, *A Plünnecke-Ruzsa inequality in compact abelian groups*, à paraître dans Revista Matemática Iberoamericana.

Bibliographie

[BD03] Luis Báez-Duarte. A strengthening of the Nyman-Beurling criterion for the Riemann hypothesis. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 14(1) :5–11, 2003.

[BDBLS00] Luis Báez-Duarte, Michel Balazard, Bernard Landreau, and Eric Saias. Notes sur la fonction ζ de Riemann. III. *Adv. Math.*, 149(1), 2000.

[Beu55] Arne Beurling. A closure problem related to the Riemann zeta-function. *Proc. Nat. Acad. Sci. U.S.A.*, 41 :312–314, 1955.

[BG10] Itziar Bardaji and David J. Grynkiewicz. Long arithmetic progressions in small sumsets. *Integers*, 10 :A28, 335–350, 2010.

[BHK$^+$05] Andreas Baltz, Peter Hegarty, Jonas Knape, Urban Larsson, and Tomasz Schoen. The structure of maximum subsets of $\{1, \ldots, n\}$ with no solutions to $a + b = kc$. *Electron. J. Combin.*, 12 :Research Paper 19, 16, 2005.

[Bil98] Yuri Bilu. The $(\alpha + 2\beta)$-inequality on a torus. *J. London Math. Soc. (2)*, 57(3) :513–528, 1998.

[Blo12] Thomas F. Bloom. Translation invariant equations and the method of Sanders. *Bull. Lond. Math. Soc.*, 44(5) :1050–1067, 2012.

[BLR98] Y. F. Bilu, V. F. Lev, and I. Z. Ruzsa. Rectification principles in additive number theory. *Discrete Comput. Geom.*, 19(3, Special Issue) :343–353, 1998. Dedicated to the memory of Paul Erdős.

[Bou89] J. Bourgain. On $\Lambda(p)$-subsets of squares. *Israel J. Math.*, 67(3) :291–311, 1989.

[Bou99] J. Bourgain. On triples in arithmetic progression. *Geom. Funct. Anal.*, 9(5) :968–984, 1999.

[Bou08] Jean Bourgain. Roth's theorem on progressions revisited. *J. Anal. Math.*, 104 :155–192, 2008.

[BS00] Michel Balazard and Eric Saias. The Nyman-Beurling equivalent form for the Riemann hypothesis. *Expo. Math.*, 18(2) :131–138, 2000.

[Bur02] Jean-François Burnol. A lower bound in an approximation problem involving the zeros of the Riemann zeta function. *Adv. Math.*, 170(1) :56–70, 2002.

[CG96] Fan R. K. Chung and John L. Goldwasser. Maximum subsets of $(0, 1]$ with no solutions to $x + y = kz$. *Electron. J. Combin.*, 3(1) :Research Paper 1, approx. 23 pp. (electronic), 1996.

[CG97] Fan R. K. Chung and John L. Goldwasser. Integer sets containing no solution to $x+y = 3z$. In *The mathematics of Paul Erdős, I*, volume 13 of *Algorithms Combin.*, pages 218–227. Springer, Berlin, 1997.

[CS11] P. Candela and O. Sisask. On the asymptotic maximal density of a set avoiding solutions to linear equations modulo a prime. *Acta Math. Hungar.*, 132(3) :223–243, 2011.

[DFST99] Jean-Marc Deshouillers, Gregory A. Freiman, Vera Sós, and Mikhail Temkin. On the structure of sum-free sets. II. *Astérisque*, (258) :xii, 149–161, 1999. Structure theory of set addition.

[DL06] Karl Dilcher and Lutz G. Lucht. On finite pattern-free sets of integers. *Acta Arith.*, 121(4) :313–325, 2006.

[EGM14] Sean Eberhard, Ben Green, and Freddie Manners. Sets of integers with no large sum-free subset. *Ann. of Math. (2)*, 180(2) :621–652, 2014.

[Fm61] G. A. Freĭ man. Inverse problems in additive number theory. Addition of sets of residues modulo a prime. *Dokl. Akad. Nauk SSSR*, 141 :571–573, 1961.

[Fre59] G. A. Freĭman. The addition of finite sets. I. *Izv. Vysš. Učebn. Zaved. Matematika*, 1959(6 (13)) :202–213, 1959.

[Fre62] G. A. Freĭman. Inverse problems of additive number theory. VI. On the addition of finite sets. III. *Izv. VysŠ. Učebn. Zaved. Matematika*, 1962(3 (28)) :151–157, 1962.

[Fre09] Gregory A. Freiman. Inverse additive number theory. XI. Long arithmetic progressions in sets with small sumsets. *Acta Arith.*, 137(4) :325–331, 2009.

[FS97] Gerald B. Folland and Alladi Sitaram. The uncertainty principle : a mathematical survey. *J. Fourier Anal. Appl.*, 3(3) :207–238, 1997.

[GR06] Ben Green and Imre Z. Ruzsa. Sets with small sumset and rectification. *Bull. London Math. Soc.*, 38(1) :43–52, 2006.

[Gre05] Ben Green. Roth's theorem in the primes. *Ann. of Math. (2)*, 161(3) :1609–1636, 2005.

[Gry13] David J. Grynkiewicz. *Structural additive theory*, volume 30 of *Developments in Mathematics*. Springer, Cham, 2013.

[GT06] Ben Green and Terence Tao. Restriction theory of the Selberg sieve, with applications. *J. Théor. Nombres Bordeaux*, 18(1) :147–182, 2006.

[HB87] D. R. Heath-Brown. Integer sets containing no arithmetic progressions. *J. London Math. Soc.*, 35(2) :385–394, 1987.

[Hen17] Kevin Henriot. On systems of complexity one in the primes. *Proc. Edinb. Math. Soc. (2)*, 60(1) :133–163, 2017.

[HJ94] Victor Havin and Burglind Jöricke. *The uncertainty principle in harmonic analysis*, volume 28 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1994.

[JP07] Philippe Jaming and Alexander M. Powell. Uncertainty principles for orthonormal sequences. *J. Funct. Anal.*, 243(2) :611–630, 2007.

[Kne53] Martin Kneser. Abschätzung der asymptotischen Dichte von Summenmengen. *Math. Z.*, 58 :459–484, 1953.

[Kne56] Martin Kneser. Summenmengen in lokalkompakten abelschen Gruppen. *Math. Z.*, 66 :88–110, 1956.

[LaP09] Izabella Ł aba and Malabika Pramanik. Arithmetic progressions in sets of fractional dimension. *Geom. Funct. Anal.*, 19(2) :429–456, 2009.

[LS95] Vsevolod F. Lev and Pavel Y. Smeliansky. On addition of two distinct sets of integers. *Acta Arith.*, 70(1) :85–91, 1995.

[Mal10] Eugenia Malinnikova. Orthonormal sequences in $L^2(\mathbf{R}^d)$ and time frequency localization. *J. Fourier Anal. Appl.*, 16(6) :983–1006, 2010.

[MFmJ73] D. A. Moskvin, G. A. Freĭ man, and A. A. Judin. Inverse problems of additive number theory and local limit theorems for lattice random variables. pages 148–162, 1973.

[MR13] Máté Matolcsi and Imre Z. Ruzsa. Sets with no solutions to $x + y = 3z$. *European J. Combin.*, 34(8) :1411–1414, 2013.

[Nas15] Eric Naslund. On improving Roth's theorem in the primes. *Mathematika*, 61(1) :49–62, 2015.

[Nat96] Melvyn B. Nathanson. *Additive number theory*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[Rai39] D. Raikov. On the addition of point-sets in the sense of Schnirelmann. *Rec. Math. [Mat. Sbornik] N.S.*, 5(47) :425–440, 1939.

[Ram95] Olivier Ramaré. On snirel'man's constant. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 22(4) :645–706, 1995.

[Rd06] Ø ystein J. Rø dseth. On Freiman's 2.4-Theorem. *Skr. K. Nor. Vidensk. Selsk.*, (4) :11–18, 2006.

[Rot53] K. F. Roth. On certain sets of integers. *J. London Math. Soc.*, 28 :104–109, 1953.

[RR01] Olivier Ramaré and Imre Z. Ruzsa. Additive properties of dense subsets of sifted sequences. *J. Théor. Nombres Bordeaux*, 13(2) :559–581, 2001.

[Ruz91] Imre Z. Ruzsa. Diameter of sets and measure of sumsets. *Monatsh. Math.*, 112(4) :323–328, 1991.

[Ruz93] Imre Z. Ruzsa. Solving a linear equation in a set of integers. I. *Acta Arith.*, 65(3) :259–282, 1993.

[Ruz94] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.*, 65(4) :379–388, 1994.

[Ruz95] Imre Z. Ruzsa. Solving a linear equation in a set of integers. II. *Acta Arith.*, 72(4) :385–397, 1995.

[San11] Tom Sanders. On Roth's theorem on progressions. *Ann. of Math. (2)*, 174(1) :619–636, 2011.

[San12] Tom Sanders. On certain other sets of integers. *J. Anal. Math.*, 116 :53–82, 2012.

[Sel92] Atle Selberg. Old and new conjectures and results about a class of Dirichlet series. In *Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989)*, pages 367–385. Univ. Salerno, Salerno, 1992.

[Sie20] Wacław Sierpiński. Sur la question de la mesurabilité de la base de m. hamel. *Fund. Math.*, 1 :105–111, 1920.

[Sou09] K. Soundararajan. Partial sums of the Möbius function. *J. Reine Angew. Math.*, 631 :141–152, 2009.

[Sta96] Yonutz Stanchescu. On addition of two distinct sets of integers. *Acta Arith.*, 75(2) :191–194, 1996.

[SZ09] Oriol Serra and Gilles Zémor. Large sets with small doubling modulo p are well covered by an arithmetic progression. *Ann. Inst. Fourier (Grenoble)*, 59(5) :2043–2060, 2009.

[Sze90] E. Szemerédi. Integer sets containing no arithmetic progressions. *Acta Math. Hungar.*, 56(1-2) :155–158, 1990.

[Ten95] Gérald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*, volume 1 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, second edition, 1995.

[TV06] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[Var59] P. Varnavides. On certain sets of positive density. *J. London Math. Soc.*, 34 :358–360, 1959.

[vdC39] J. G. van der Corput. über Summen von Primzahlen und Primzahlquadraten. *Math. Ann.*, 116(1) :1–50, 1939.