

Ensembles invariants par $\times 2$ et $\times 3$

Nicolas de Saxcé

22 novembre 2022

Résumé

Après quelques millénaires de tâtonnements, l'écriture décimale s'est peu à peu imposée pour les nombres entiers et réels : l'apprentissage du calcul en base 10 est maintenant un point essentiel de l'instruction à l'école primaire. Il est assez naturel de se demander à quoi ressembleraient les nombres dont l'écriture décimale nous est si familière, s'ils étaient écrits dans une autre base. Le but de cet article est de présenter certaines questions posées par Furstenberg à ce propos dans les années 60, et les progrès récents de Hochman, Shmerkin et Wu dans ce domaine.

Introduction

Tout nombre réel $x \in [0, 1[$ peut se définir par son écriture en binaire : il existe une suite d'entiers $a_n \in \{0, 1\}$ tels que

$$x = \sum_{n \geq 1} a_n 2^{-n}.$$

On écrit alors $x = 0, a_1 a_2 a_3 \dots$, en base 2. Bien que cette écriture soit particulièrement adaptée à l'informatique, nous préférons pour notre usage courant le système décimal, suivant lequel on peut écrire $x = 0, b_1 b_2 b_3 \dots$ en base 10, c'est-à-dire, pour certains entiers $b_i \in \{0, \dots, 9\}$,

$$x = \sum_{n \geq 1} b_n 10^{-n}.$$

Ainsi par exemple, nous avons plus l'habitude de

$$\pi = 3, 14 \dots \quad \text{en base 10}$$

que de

$$\pi = 11, 001001 \dots \quad \text{en base 2.}$$

De façon plus générale, si p et q sont deux entiers distincts — par exemple $p = 2$ et $q = 3$ — on peut s'intéresser à l'écriture d'un réel x dans chacune de ces deux bases, et chercher à comprendre les liens entre ces deux écritures.

Naturellement, si p et q sont des puissances d'un même entier, c'est-à-dire si l'on peut écrire $p = r^k$ et $q = r^l$ pour un certain entier r , les écritures dans les bases p et q correspondent simplement aux blocs de longueur k et l de l'écriture en base r , de sorte qu'elles sont très similaires. Par exemple, si peu de chiffres (ou de blocs de chiffres de longueur donnée) apparaissent dans l'écriture de x en base $p = r^k$, ce sera aussi le cas en base $q = r^l$. Lorsque p et q ne sont pas des puissances d'un même entier — on dit qu'ils sont *multiplicativement indépendants* — le problème est beaucoup plus subtil.

Dans les années 1960, Furstenberg [5, 4] a obtenu les premiers résultats remarquables sur ce sujet, et énoncé une série de conjectures dont l'étude a ouvert de nouvelles voies à explorer, à l'interface entre la théorie géométrique de la mesure et les systèmes dynamiques. Nous nous proposons dans cet article de donner une introduction à ces problèmes, depuis les observations fondatrices de Furstenberg, et jusqu'aux travaux récents de Hochman et Shmerkin [6], puis de Shmerkin [10] et Wu [11], qui ont résolu par l'affirmative plusieurs des conjectures de Furstenberg.

Mais commençons par décrire le problème de façon plus géométrique. Si l'on identifie le segment $[0, 1[$ au cercle $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ des réels modulo 1, l'écriture en base p décrit l'orbite du point x par la multiplication par p modulo 1. Concrètement, si l'on découpe le cercle en p intervalles d'égale longueur $\mathbb{T} = I_0 \cup I_1 \cup \dots \cup I_{p-1}$, le développement $x = 0, a_1 a_2 \dots$ donne la suite des positions des éléments de l'orbite $(p^n x)_{n \geq 0}$ dans cette partition.

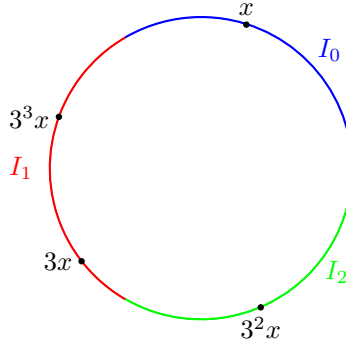


FIGURE 1 – Orbite par $\times 3$ de $x = 0,0121\dots$ en base 3 ($x = 0,197\dots$ en base 10)

Par exemple, dire que tout bloc de chiffres apparaît dans l'écriture de x en base p revient à dire que l'orbite de x par $\times p$ est dense dans \mathbb{T} . À l'opposé, l'écriture de x en base p est périodique à partir d'un certain rang si et seulement si l'orbite de x par $\times p$ est finie ; cela équivaut d'ailleurs à ce que x soit rationnel.

Évidemment, de façon analogue, l'écriture en base q correspond à l'opération $\times q$ de multiplication par q . D'un point de vue dynamique, on cherche donc à comprendre comment interagissent les deux transformations $\times p$ et $\times q$ sur

le cercle \mathbb{T} . La première observation remarquable de Furstenberg concerne les fermés invariants simultanément par ces deux transformations.

th:basic

Théorème 1 (Furstenberg). *Si p et q sont multiplicativement indépendants, le cercle \mathbb{T} est l'unique fermé infini invariant par les opérations $\times p$ et $\times q$.*

Au vu de cet énoncé, Furstenberg a aussi formulé une conjecture analogue pour les mesures invariantes. Rappelons qu'une mesure μ est dite *diffuse* si elle est sans atome, i.e. si pour tout x dans \mathbb{T} , $\mu(\{x\}) = 0$.

conj:mes

Conjecture 1 (Furstenberg). *Si p et q sont multiplicativement indépendants, la mesure de Lebesgue est l'unique probabilité diffuse invariante par $\times p$ et $\times q$.*

Cette conjecture reste aujourd'hui un des problèmes ouverts les plus importants en systèmes dynamiques. Sous une hypothèse supplémentaire d'entropie strictement positive, cette conjecture a été résolue par Rudolph [9] lorsque p et q sont premiers entre eux, puis par Johnson [7] lorsque p et q sont seulement multiplicativement indépendants.

Il n'est pas évident d'explicitier les conséquences des énoncés ci-dessus sur les écritures en base p et en base q d'un nombre réel, et il pourrait donc sembler à première vue que cette approche dynamique du problème nous a sensiblement éloignés de notre problème initial. En fait, les deux énoncés ci-dessus manifestent une forme d'indépendance entre les deux transformations $T_p = \times p$ et $T_q = \times q$. Rappelons que l'écriture en base p correspond à l'orbite $\langle T_p, x \rangle$ de x sous l'action de T_p , tandis que l'orbite $\langle T_q, x \rangle$ de x sous l'action de T_q est encodée par l'écriture en base q . La conjecture ci-dessous, dans le même esprit que le théorème 1, exprime que si x est irrationnel, et p, q multiplicativement indépendants, les écritures de x dans les bases p et q ne peuvent pas être simultanément trop simples. La situation serait donc presque à l'opposé du cas où p et q sont deux puissances d'un même entier ! Rappelons que la dimension de Hausdorff $\dim_H A$ d'une partie A dans \mathbb{R} peut prendre n'importe quelle valeur entre 0 et 1. Cette notion, dont la définition précise sera donnée au paragraphe 2.1, donne une indication de la taille des ensembles fractals, dont la mesure de Lebesgue est nulle, mais qui peuvent néanmoins contenir beaucoup de points.

conj:rat

Conjecture 2. *Soient p et q deux entiers multiplicativement indépendants. Pour tout x dans \mathbb{T} , l'inégalité $\dim_H \overline{\langle T_p, x \rangle} + \dim_H \overline{\langle T_q, x \rangle} < 1$ implique que x est rationnel.*

La dimension de Hausdorff $\alpha = \dim_H \overline{\langle T_p, x \rangle}$ mesure en quelque sorte la complexité de l'écriture de x en base p . Plus précisément, si l'on note $N_p(x, n)$ le nombre de blocs de longueur n qui apparaissent dans l'écriture de x en base p , alors

$$N_p(x, n) = p^{n(\alpha + o(1))}.$$

De plus, on peut montrer que l'égalité $\dim_H \overline{\langle T_q, x \rangle} = 1$ implique en fait que l'orbite $(q^n x)_{n \geq 0}$ est dense dans \mathbb{T} . Par conséquent, si la conjecture est vérifiée,

et si x est un irrationnel tel que le nombre $N_p(x, n)$ de blocs de longueur n dans l'écriture de x croît sous-exponentiellement, tous les blocs de chiffres doivent apparaître dans l'écriture de x en base q . Par exemple, l'écriture décimale de

$$x = \sum_{n \geq 0} 2^{-2^n} = 0,11010001\dots \quad \text{en base 2}$$

doit faire apparaître tous les chiffres de 0 à 9, et même tous les blocs de chiffres. Pour donner un deuxième exemple concret, cette conjecture implique que si x ne contient que des 0 et des 1 à la fois en base 3 et en base 10, alors x est rationnel. Une autre conséquence amusante de cette conjecture, mentionnée par Furstenberg, concerne l'écriture de 2^n en base 10. Rappelons que le critère d'équirépartition de Weyl permet de calculer la fréquence d'apparition du premier chiffre (ou bloc de chiffres) de 2^n lorsque n varie, et donc de montrer que tous les blocs de chiffres apparaissent dans l'écriture de certains 2^n , pour n arbitrairement grand. La conjecture ci-dessus impliquerait que tous les blocs apparaissent dans *tout* 2^n , pourvu que n soit suffisamment grand¹.

conj:deuxn

Conjecture 3. *Si n est suffisamment grand, tous les chiffres (ou tous les blocs de chiffres d'une longueur fixée) apparaissent dans l'écriture de 2^n en base 10.*

À l'heure actuelle, ces trois conjectures de Furstenberg sont encore ouvertes, mais une version faible de la conjecture 2 a été récemment résolue par Shmerkin [10] et Wu [11], indépendamment. Commençons par reformuler cette conjecture 2 : si A et B sont deux fermés de \mathbb{T} invariants respectivement par T_p et T_q , et vérifiant $\dim_{\mathbb{H}} A + \dim_{\mathbb{H}} B < 1$, alors $A \cap B \subset \mathbb{Q}$. Comme première étape vers cette conjecture, Furstenberg suggérerait de montrer que sous ces hypothèses, on a toujours $\dim_{\mathbb{H}}(A \cap B) = 0$. Notons que si A et B sont des sous-espaces vectoriels transverses dans \mathbb{R}^d , la dimension de l'intersection est toujours majorée par

$$\dim(A \cap B) \leq \max(0, \dim A + \dim B - d).$$

Bien sûr, cette inégalité n'est pas toujours valable pour les ensembles fractals, mais l'idée de Furstenberg est que l'hypothèse d'invariance de A et B par T_p et T_q nous assure d'une forme de transversalité. C'est le résultat qui a été démontré en 2016 par Shmerkin [10] et Wu [11], indépendamment. Une autre démonstration, plus courte, a aussi été proposée récemment par Austin [1].

th:trans

Théorème 2 (Transversalité de T_p et T_q). *Soient p, q deux entiers multiplicativement indépendants, et A, B deux fermés de \mathbb{T} invariants par T_p et T_q , respectivement. Alors, pour tous réels s, t , $t \neq 0$,*

$$\dim_{\mathbb{H}}(A \cap (s + tB)) \leq \max(\dim_{\mathbb{H}} A + \dim_{\mathbb{H}} B - 1, 0).$$

Cet article se compose de trois parties. La première partie est consacrée au théorème de Furstenberg sur les fermés invariants par $\times p$ et $\times q$; après quelques

1. On renvoie le lecteur intéressé à l'article original [4, Conjecture 2'] pour l'argument élémentaire qui permet de déduire cette conjecture de la précédente.

exemples introductifs, nous en donnerons la démonstration, suivie d’une brève discussion de son analogue conjecturel pour les mesures, la conjecture 1. La seconde partie traite de problèmes de théorie géométrique de la mesure, et a pour but d’expliquer les liens entre le problème de l’intersection d’ensembles invariants et celui des projections de mesures invariantes. Nous y esquisserons au passage une démonstration, due à Hochman et Shmerkin, du résultat de Rudolph-Johnson sur les mesures invariantes par $\times p$ et $\times q$. Enfin, la troisième partie présente succinctement deux ingrédients importants de la démonstration de Shmerkin : la notion de mesure dynamiquement auto-similaire, et les théorèmes inverses en combinatoire additive.

1 Fermés invariants

Donnons d’abord quelques exemples de fermés invariants par l’application de multiplication T_p . Bien sûr, pour commencer il existe des orbites finies, qui proviennent toutes de points rationnels. Cela n’est qu’une reformulation d’un point bien connu, que l’on découvre souvent en apprenant l’algorithme de division avec « chiffres après la virgule » : un nombre réel est rationnel si et seulement si son développement décimal est périodique à partir d’un certain rang.

Mais il existe aussi de nombreux fermés invariants infinis. Par exemple, si S est une partie de $\{0, \dots, p-1\}$, l’ensemble

$$F_S = \{x = \sum_{i \geq 1} a_i p^{-i} ; \forall i, a_i \in S\}$$

définit un fermé invariant, infini dès que S contient au moins deux éléments ; c’est l’ensemble des éléments dont une écriture en base p ne contient que des éléments de S . Ces ensembles s’appellent les *ensembles de Cantor p -adiques*, le plus célèbre est sans doute l’ensemble de Cantor triadique, invariant par T_3 , et constitué des réels dont l’écriture en base 3 ne contient pas de 1. On peut encore obtenir d’autres fermés invariants en imposant des conditions sur les différents blocs de chiffres, et il n’est pas difficile de voir à l’aide de ces constructions que l’ensemble des fermés invariants par T_p n’est pas dénombrable.

Cela montre bien que l’énoncé du théorème de Furstenberg que nous voulons démontrer est remarquable : parmi tous ces fermés invariants par T_p , les seuls qui sont invariants par multiplication par un entier q indépendant de p sont les orbites finies et le cercle \mathbb{T} tout entier !

1.1 Le théorème de Furstenberg

Nous donnons maintenant les grandes lignes de la démonstration du théorème 1 proposée par Boshernitzan [2], suivant la présentation de Malicet [8]. On renvoie d’ailleurs à cette dernière note pour les preuves détaillées des résultats intermédiaires.

Un sous-groupe additif de \mathbb{R} qui n’est pas monogène est dense. La démonstration du théorème de Furstenberg utilise une variante de cette observation

pour les semi-groupes, i.e. les parties stables par addition : un semi-groupe additif Σ_0 de $\mathbb{R}^+ = [0, +\infty[$ qui n'est pas contenu dans un semi-groupe monogène est *non-lacunaire*. Cela signifie que les points de Σ_0 sont de plus en plus denses au voisinage de l'infini. Précisément, pour tout $\varepsilon > 0$, il existe $R \geq 0$ tel que pour tout $x \geq R$, il existe s dans Σ_0 tel que $|x - s| \leq \varepsilon$.

Dans la suite, nous nous intéresserons à un semi-groupe *multiplicatif* Σ de l'ensemble \mathbb{N} des entiers naturels. La partie $\Sigma_0 = \log \Sigma$ est un semi-groupe additif de \mathbb{R}^+ , et le résultat ci-dessus montre donc que si Σ n'est pas monogène, alors Σ est non lacunaire, au sens où le quotient de deux éléments successifs de Σ converge vers 1 en l'infini : si $\Sigma = \{s_1 < s_2 < \dots\}$, alors

$$\lim_{n \rightarrow \infty} \frac{s_{n+1}}{s_n} = 1.$$

Dans toute la suite, on considère un fermé infini F invariant par multiplication par deux entiers indépendants p et q , et on cherche à montrer que $F = \mathbb{T}$. Nous noterons $\Sigma = \{s_1 < s_2 < \dots\}$ le semi-groupe de (\mathbb{N}, \times) engendré par p et q . Si l'on dispose d'un élément u dans F arbitrairement proche de 0, la propriété de non lacunarité de Σ permet d'encadrer un point quelconque x dans \mathbb{T} par des intervalles de la forme $[s_n u, s_{n+1} u]$, dont les extrémités appartiennent à F , et dont la longueur est arbitrairement petite. Cette observation élémentaire permet d'obtenir le premier lemme important en direction du théorème de Furstenberg.

Lemme 1. *Si 0 est point d'accumulation de F , alors $F = \mathbb{T}$.*

Notons que la conclusion du lemme ci-dessus est encore valable si l'on suppose seulement que F a un point d'accumulation rationnel $\frac{a}{b}$. En effet, dans ce cas, le fermé invariant $F' = bF$ admet 0 comme point d'accumulation, donc $F' = \mathbb{T}$. Cela implique $\mathbb{T} = b^{-1}(F') = \bigcup_{0 \leq k < b} F + \frac{k}{b}$, et par suite, il existe k tel que $F + \frac{k}{b}$ contient un ouvert non vide. Donc F contient un ouvert non vide, et comme F est invariant par Σ , on trouve bien que $F = \mathbb{T}$.

La suite de la démonstration consiste à construire dans F un autre fermé invariant F' qui satisfait une propriété supplémentaire d'invariance par translation. Pour $\alpha \in \mathbb{T}$, nous noterons $\tau_\alpha : \mathbb{T} \rightarrow \mathbb{T}$ l'application de translation par α , définie par $\tau_\alpha(x) = x + \alpha$. Si τ_α commute aux opérations de multiplication T_p et T_q , on procède de la façon suivante : partant de l'ensemble F_0 des points d'accumulation de F , on définit une suite de fermés invariants par la relation

$$F_n = F_{n-1} \cap \tau_\alpha(F_{n-1}), \quad \forall n \geq 1.$$

Sans perte de généralité, supposons que F_0 ne contient aucun point rationnel ; cela implique en particulier que F_0 est infini. Ensuite, si F_{n-1} est infini, le lemme précédent montre que l'ensemble $F_{n-1} - F_{n-1}$ (dont 0 est point d'accumulation) est égal à \mathbb{T} tout entier, ce qui implique que F_n est non vide, et donc infini, puisqu'il ne contient aucun point rationnel. La suite $(F_n)_{n \geq 0}$ est donc une suite décroissante de fermés non vides, et par compacité, l'intersection décroissante

$$F' = \bigcap_{n \geq 0} F_n$$

définit un fermé invariant non vide stable par τ_α . C'est exactement le contenu du second lemme dont nous aurons besoin.

Lemme 2. *Si F est un fermé invariant infini et si τ_α commute à T_p et T_q , alors F contient un fermé invariant infini F' stable par τ_α .*

Le théorème [1](#) s'obtient simplement à l'aide des deux lemmes ci-dessus. En effet, si F est un fermé infini invariant par T_p et T_q , on peut choisir un entier arbitrairement grand k puis un entier m tel que k divise à la fois $p^m - 1$ et $q^m - 1$. La translation $\tau_{1/k}$ commute alors à T_{p^m} et S_{q^m} , donc F contient un fermé F' non vide stable par $\tau_{1/k}$. Cela implique que F est $1/k$ -dense dans \mathbb{T} , et comme k peut être arbitrairement grand, on trouve bien $F = \mathbb{T}$.

Nous concluons ce paragraphe en mentionnant une version quantitative de l'énoncé de Furstenberg, due à Bourgain, Lindenstrauss, Michel et Venkatesh [\[3\]](#).

Théorème 3. *Soient p et q deux entiers multiplicativement indépendants. Si x est un point diophantien de \mathbb{T} , i.e. satisfait, pour un certain $k \geq 1$, pour tout (a, b) dans $\mathbb{Z} \times \mathbb{N}$, $|x - \frac{a}{b}| \geq b^{-k}$, alors il existe $\kappa > 0$ tel que pour tout entier N suffisamment grand, l'ensemble*

$$\{p^s q^t x ; s, t \leq N\}$$

est dense à l'échelle $(\log \log N)^{-\kappa}$ dans \mathbb{T} .

La démonstration de ce théorème utilise des versions quantitatives du résultat partiel de Rudolph-Johnson concernant la conjecture de Furstenberg sur les mesures invariantes.

1.2 Mesures invariantes

Nous présentons maintenant le théorème de Rudolph-Johnson sur les mesures invariantes. Rappelons que l'entropie pour T_p d'une mesure μ invariante par T_p est définie par

$$h_\mu(T_p) = \lim_{n \rightarrow \infty} \frac{-1}{n} \sum_{I \in \mathcal{D}_p^{(n)}} \mu(I) \log \mu(I),$$

où $\mathcal{D}_p^{(n)} = \{[\frac{i}{p^n}, \frac{i+1}{p^n}[; 0 \leq i < p^n\}$ désigne la partition de \mathbb{T} en intervalles p -adiques de niveau n . Il existe de nombreuses interprétations de l'entropie, notamment en termes d'information ; nous verrons ci-dessous que l'entropie d'une mesure est aussi étroitement reliée à sa dimension de Hausdorff.

Le théorème de Rudolph-Johnson exprime que la mesure de Lebesgue est essentiellement l'unique mesure d'entropie strictement positive invariante par T_p et T_q . Évidemment, une combinaison convexe de la mesure de Lebesgue avec une mesure invariante à support fini aura encore cette propriété, et pour s'assurer l'unicité, il faut donc interdire de telles combinaisons. On dit qu'une probabilité μ invariante par T_p est *ergodique* si μ ne peut pas s'écrire comme combinaison convexe non triviale de deux probabilités invariantes par T_p .

Théorème 4 (Rudolph-Johnson). *Soient p et q deux entiers multiplicativement indépendants, et μ une probabilité invariante sous l'action de T_p et T_q et ergodique pour T_p . Si μ est d'entropie strictement positive pour T_p , alors μ est égale à la mesure de Lebesgue sur \mathbb{T} .*

Certaines démonstrations de ce résultat ne sont pas sans lien avec celle que nous avons présentée du théorème de Furstenberg sur les fermés invariants, et relie l'invariance par le semi-groupe multiplicatif engendré par T_p et T_q à des propriétés de récurrence pour certains sous-groupes *additifs*. Une autre démonstration, due à Hochman et Shmerkin, passe par une inégalité sur la dimension des convolutions de mesures invariantes par multiplication, que nous décrivons dans la partie suivante.

2 Dimension, projection et intersection

Le but de cette partie est de ramener le théorème 2 à un énoncé plus géométrique, qui porte sur la régularité de certaines projections de mesures. Cette dualité entre intersection et projection, déjà observée par Furstenberg, est à la base de la démonstration de Shmerkin [10].

2.1 Dimension et invariance

Commençons par rappeler quelques notions élémentaires pour définir la dimension d'une partie bornée A dans \mathbb{R} . La définition la plus simple est sans doute celle de Minkowski : pour une échelle $\delta > 0$ arbitrairement petite, on note $N(A, \delta)$ le cardinal minimal d'un recouvrement de A à l'aide de boules de rayon δ , et on pose

$$\overline{\dim}_M A = \limsup_{\delta \rightarrow 0} \frac{\log N(A, \delta)}{\log \frac{1}{\delta}}.$$

Cette définition a un inconvénient majeur : elle n'est pas stable par union dénombrable. Même un ensemble discret peut avoir une dimension strictement positive, par exemple $\overline{\dim}_M \{\frac{1}{n} ; n \geq 1\} = \frac{1}{2}$. On préfère donc souvent utiliser la dimension de Hausdorff, qui met en jeu des recouvrements par des boules dont le rayon peut être arbitrairement petit :

$$\dim_H A = \inf \left\{ s > 0 \mid \forall \varepsilon > 0, \exists (x_i, \delta_i)_{i \in \mathbb{N}} : A \subset \bigcup_i B(x_i, \delta_i), \sum_i \delta_i^s \leq \varepsilon \right\}.$$

Fort heureusement, si A est un fermé invariant par multiplication par un entier $p \geq 2$, il n'est pas difficile de vérifier que ces deux notions coïncident

$$\overline{\dim}_M A = \dim_H A. \tag{1}$$

Pour une mesure μ , on définit sa dimension de Hausdorff inférieure par

$$\dim_H \mu = \inf \{ \dim_H A ; \mu(A) > 0 \}.$$

Lorsque μ est invariante et *ergodique* par multiplication par un entier $p \geq 2$, le théorème de Shannon-McMillan-Breiman permet de démontrer une formule analogue à (1). En effet, ce théorème affirme que pour presque tout x au sens de la mesure μ , le quotient $\frac{\log \mu(B(x, \delta))}{\log \delta}$ converge vers la valeur limite $\frac{h_\mu(T_p)}{\log p}$, indépendante de x . On dit que μ est de *dimension exacte* égale à

$$\dim \mu = \frac{h_\mu(T_p)}{\log p}.$$

Insistons sur le fait que cette propriété n'est pas valable en général, mais découle de l'invariance et de l'ergodicité pour T_p . Un exemple important est celui des ensembles de Cantor p -adiques, et des mesures de Cantor qui leur sont associées.

Exemple (Ensembles et mesures de Cantor). Soit S une partie de $\{0, \dots, p-1\}$, et F_S l'ensemble de Cantor p -adique associé, c'est-à-dire l'ensemble des éléments dont l'écriture en base p ne contient que des éléments de S . La dimension de Hausdorff de F_S , égale à sa dimension de Minkowski, est égale à

$$\dim_H F_S = \frac{\log |S|}{\log p}.$$

En outre, on peut définir sur F_S une mesure canonique μ_S , qui correspond à un choix uniforme parmi les éléments de S de chaque chiffre du développement en base p . Cette mesure vérifie une propriété de régularité importante : il existe une constante $C > 0$ telle que pour tout x dans F_S et tout $\delta \in]0, 1[$,

$$\frac{1}{C} \delta^{\dim_H F_S} \leq \mu_S(B(x, \delta)) \leq C \delta^{\dim_H F_S}. \quad (2)$$

ahlfors

On obtient par un calcul facile la valeur de l'entropie $h_{\mu_S}(T_p) = \log |S|$, ce qui permet de retrouver dans ce cas particulier la formule annoncée par le théorème de Shannon-McMillan-Breiman.

2.2 Projection de mesures invariantes

Comme dans le théorème 2, nous considérons maintenant deux fermés A, B dans $[0, 1]$. Pour s, t dans \mathbb{R} , l'intersection $A \cap (s + tB)$ coïncide avec la fibre au-dessus de s de l'application $\pi_t : (a, b) \mapsto a - tb$. Or, en général, entre la dimension des fibres et de l'image, on s'attend à la relation

$$\dim(A \times B) = \dim \pi_t(A \times B) + \sup_s \dim \pi_t^{-1}(\{s\}). \quad (3)$$

heur

Cette identité n'est pas toujours valable pour les ensembles fractals, mais elle a sans doute permis à Furstenberg d'entrevoir la relation entre le problème des intersections d'ensembles invariants à celui des projections d'ensembles invariants, et de formuler une conjecture étroitement reliée au théorème 2 : lorsque A et B sont respectivement invariants par multiplication par p et q , deux entiers multiplicativement indépendants, on a, pour tout $t \neq 0$,

$$\dim_H(A + tB) = \min(1, \dim_H A + \dim_H B).$$

De façon équivalente, on peut formuler cette conjecture à l'aide des projections orthogonales de $A \times B$ sur des droites, qui correspondent naturellement aux applications π_t . Cette conjecture a été résolue en 2011 par Hochman et Shmerkin, qui ont même obtenu une version plus générale, pour les projections de mesures invariantes.

th:hs

Théorème 5 (Hochman-Shmerkin). *Soient p, q deux entiers multiplicativement indépendants. Soient μ et ν deux probabilités sur $[0, 1[$ invariantes par T_p et T_q , respectivement. Pour toute projection orthogonale π sur une droite distincte des axes de coordonnées,*

$$\dim_{\mathbb{H}} \pi(\mu \otimes \nu) = \min(1, \dim_{\mathbb{H}} \mu \otimes \nu).$$

Pour retrouver le théorème de Rudolph-Johnson, supposons maintenant que μ soit une mesure invariante à la fois par T_p et T_q , ergodique pour T_p , et d'entropie $h_{\mu}(T_p)$ strictement positive. Nous avons déjà vu que μ est de dimension exacte égale à $\frac{h_{\mu}(T_p)}{\log p}$, strictement positive. Le théorème ci-dessus appliqué (plusieurs fois) à la projection $(x, y) \mapsto x + y$ montre que $\dim_{\mathbb{H}} \mu^{*k} = 1$ pour k suffisamment grand. Il n'est pas trop difficile de voir que la mesure de Lebesgue est l'unique mesure invariante par T_p de dimension exacte égale à 1, et donc $\mu^{*k} = \text{Leb}$. Mais alors, les coefficients de Fourier de μ vérifient $\hat{\mu}(n)^k = 0$ si $n \neq 0$, d'où $\hat{\mu}(n) = 0$ et μ est bien la mesure de Lebesgue.

2.3 De la projection à l'intersection

La relation heuristique (3) est fautive en général, et il n'est pas possible de déduire la dimension de $A \cap (s + tB)$ de celle de $A + tB$, donnée par le théorème 5. Cependant, l'idée générale de la démonstration de Shmerkin est tout de même de démontrer un théorème de projection suffisamment précis pour pouvoir en déduire l'inégalité souhaitée sur les intersections. On commence par remarquer qu'il suffit de démontrer le théorème lorsque les ensembles A et B sont des ensembles de Cantor p -adique et q -adique, respectivement. Cela n'est pas difficile à voir, car si A est un ensemble invariant par T_p , pour tout $\varepsilon > 0$, il existe un entier N et un ensemble de Cantor p^N -adique \tilde{A} contenant A et tel que $\dim_{\mathbb{H}} \tilde{A} \leq \dim_{\mathbb{H}} A + \varepsilon$. En appliquant alors l'inégalité du théorème à des ensembles de Cantor \tilde{A} et \tilde{B} qui approchent A et B , on obtient le résultat souhaité pour les ensembles A et B .

Le cœur du problème consiste donc à démontrer le théorème pour les ensembles de Cantor. Pour cela, nous démontrerons un analogue du théorème de projection de Hochman-Shmerkin, mais pour une autre notion, plus fine, de dimension.

Pour $r \geq 1$, on définit la *dimension L^r* d'une mesure ν en étudiant le comportement de la densité de ν à l'échelle δ , lorsque δ tend vers 0. Plus précisément, si $\phi_{\delta} = \frac{1}{\delta} \mathbb{1}_{[0, \delta]}$ désigne une unité approchée à l'échelle δ , on pose

$$\dim_r \nu = 1 - \limsup_{\delta \rightarrow 0} \frac{\log \|\nu * \phi_{\delta}\|_r^r}{(r-1) \log 1/\delta}.$$

C'est une mesure de l'étalement de la mesure ν , qui varie entre 0 (lorsque ν est concentrée autour de peu de points) et 1 (pour la mesure de Lebesgue, par exemple). Donnons maintenant la propriété importante de cette dimension qui permet de rendre rigoureuse l'intuition donnée par (3) : si A et B sont des ensembles de Cantor, η_A, η_B les mesures canoniques associées, et π une projection sur une droite, on a toujours l'inégalité

$$\forall y \in \mathbb{R}, \overline{\dim_M} \pi^{-1}(y) \leq \dim_H A + \dim_H B - (1 - \frac{1}{r}) \dim_r \pi_*(\eta_A \otimes \eta_B).$$

Si l'on dispose de l'analogue du théorème 5 pour la dimension L^r , il suffira pour démontrer le théorème 2 de faire tendre r vers l'infini dans l'inégalité ci-dessus. C'est justement ce qu'affirme le théorème ci-dessous, dû à Shmerkin.

th:shproj

Théorème 6. Soient A, B deux ensembles de Cantor associés à des entiers multiplicativement indépendants, et η_A, η_B les mesures canoniques associées. On note aussi $\mu = \eta_A \otimes \eta_B$ la mesure produit sur $A \times B$. Pour toute projection π sur une droite non parallèle aux axes de coordonnées, on a, pour tout $r > 1$,

$$\dim_r \pi_* \mu \geq \min(1, \dim_H A + \dim_H B).$$

Cette inégalité dimensionnelle provient d'une propriété remarquable d'*auto-similarité dynamique* satisfaite par la mesure $\pi_* \mu$, qui sera étudiée dans la partie suivante, où nous donnerons quelques idées de la démonstration du théorème ci-dessus.

3 Projection de mesures de Cantor

Un ensemble *auto-similaire* dans \mathbb{R} est un ensemble qui est égal à la réunion de plusieurs images de lui-même par des contractions. Tout ensemble de Cantor p -adique F_S a cette propriété, puisqu'on peut écrire

$$F_S = \bigcup_{s \in S} \frac{s}{p} + \frac{1}{p} F_S.$$

On dit de même qu'une mesure ν est auto-similaire s'il existe une famille de contractions $(\phi_s)_{s \in S}$ et des réels positifs $(p_s)_{s \in S}$ tels que $\sum_s p_s = 1$ et $\nu = \sum_{s \in S} p_s (\phi_s)_* \nu$. C'est le cas pour la mesure μ_S sur l'ensemble de Cantor F_S , si l'on prend $\phi_s(x) = \frac{s}{p} + \frac{x}{p}$ et $p_s = \frac{1}{p}$ pour chaque s . Cette équation vérifiée par μ_S peut s'écrire simplement grâce au produit de convolution :

$$\mu_S = \Delta_S * (S_{p^{-1}} \mu_S),$$

où Δ_S désigne la mesure à support fini $\frac{1}{|S|} \sum_{s \in S} \delta_{\frac{s}{p}}$, tandis que S_t est l'application de contraction par le facteur t . En itérant l'égalité ci-dessus, on obtient μ_S sous la forme d'un produit de convolution infini de mesures à support fini

$$\mu_S = *_{i=0}^{\infty} S_{p^{-i}} \Delta_S. \quad (4)$$

conv

Cette équation exprime que la géométrie de μ_S à chaque échelle p^{-i} est contrôlée par une unique mesure Δ_S , indépendante de i . La géométrie des mesures auto-similaires a été assez bien étudiée depuis les travaux fondateurs de Mandelbrot, Hutchinson et Mattila au début des années 1980. Plus récemment, en 2012, Hochman a même obtenu une formule pour la dimension de Hausdorff d'un ensemble auto-similaire général, sous une condition de séparation assez faible. La stratégie utilisée par Shmerkin pour démontrer le théorème 6 consiste à développer les idées de Hochman pour pouvoir les appliquer aux projections de mesures invariantes. Cela sera possible car la géométrie de ces projections à toutes les échelles est contrôlée par une structure simple, déjà mise en évidence par Furstenberg.

3.1 Mesures dynamiquement auto-similaires

On considère maintenant deux mesures de Cantor η_A et η_B sur des ensembles de Cantor A et B associés à des entiers p et q multiplicativement indépendants, et on s'intéresse à une projection de $\mu = \eta_A \otimes \eta_B$ sur une droite non parallèle aux axes de coordonnées. À un changement affine de coordonnées près, nous pouvons écrire cette projection sous la forme

$$\begin{aligned} \pi_x : \quad \mathbb{R}^2 &\rightarrow \mathbb{R} \\ (a, b) &\mapsto a + e^x b \end{aligned}$$

Pour décrire la structure *presque* auto-similaire de la mesure $\mu_x = (\pi_x)_* \mu$, nous commençons par reformuler l'équation (4) pour η_A en termes probabilistes.

On note $S_A \subset \{0, \dots, p-1\}$ la partie finie qui définit A et $\Delta_A = \frac{1}{|S_A|} \sum_{s \in S_A} \delta_{\frac{s}{p}}$ la probabilité uniforme associée. De même la partie $S_B \subset \{0, \dots, q-1\}$ et la mesure Δ_B sont associés à B . Si $(X_i)_{i \geq 0}$ est une suite de variables aléatoires indépendantes identiquement distribuées de loi Δ_A , alors η_A est la loi de la variable aléatoire

$$\sum_{i=0}^{\infty} p^{-i} X_i.$$

Naturellement, on dispose d'une écriture analogue pour η_B : si les variables aléatoires $(Y_i)_{i \geq 0}$ sont indépendantes et identiquement distribuées de loi Δ_B , la variable aléatoire

$$\sum_{j=0}^{\infty} q^{-j} Y_j$$

est de loi η_B . Supposons $p < q$. Pour rendre ces deux sommes plus compatibles, on peut noter que

$$\sum_{j=0}^{\infty} q^{-j} Y_j = \sum_{i=0}^{\infty} p^{-i} Y'_i$$

où

$$Y'_i = \begin{cases} q^{-j} p^i Y_j & \text{si } p^i < q^j < p^{i+1} \\ 0 & \text{sinon.} \end{cases}$$

Il apparaît que la suite des indices i tels que la variable aléatoire Y'_i n'est pas identiquement nulle est codée par le système dynamique $X = [0, \log q[$, muni de la transformation

$$\begin{aligned} T: X &\rightarrow X \\ x &\mapsto x + \log p \pmod{\log q}. \end{aligned}$$

On introduit une famille $(\Delta(x))_{x \in X}$ de mesures à support fini, définies par

$$\Delta(x) = \begin{cases} \Delta_A * S_{e^x} \Delta_B & \text{si } x \in [0, \log p[\\ \Delta_A & \text{si } x \in [\log p, \log q[\end{cases}$$

et les observations qui précèdent montrent que $\mu_x = \pi_* \mu$ est la loi d'une variable aléatoire $\sum_{i=1}^{\infty} p^{-i} Z_i$, où les Z_i sont des variables aléatoires indépendantes de loi $\Delta(T^i x)$. En d'autres termes,

$$\mu_x = *_{i=1}^{\infty} S_{p^{-i}} \Delta(T^i x).$$

Shmerkin démontre une formule générale pour la dimension de Hausdorff des mesures définies par un système dynamique comme ci-dessus. L'espace métrique X est supposé compact, et la transformation $T: X \rightarrow X$ continue. Le taux de contraction peut être un réel $\lambda \in]0, 1[$ arbitraire, non nécessairement de la forme $\frac{1}{p}$ pour p entier, mais certaines hypothèses sont nécessaires :

1. $T: X \rightarrow X$ est *uniquement* ergodique, i.e. admet une *unique* probabilité invariante, notée \mathbb{P} .
2. Les mesures μ_x sont diffuses, supportées par un intervalle compact fixé, et $x \mapsto \mu_x$ est continue (pour la topologie faible) \mathbb{P} -presque partout.
3. Pour tout x , la mesure $\Delta(x)$ est une probabilité sur \mathbb{R} à support fini de cardinal borné, et l'application $x \mapsto \Delta(x)$ est continue \mathbb{P} -presque partout.
4. Pour presque tout x , il existe $R \geq 0$ tel que, pour n arbitrairement grand, les atomes de $\mu_{x,n} \sim \sum_{i=1}^n \lambda^i Z_i$ sont distincts et λ^{Rn} -séparés.

Si ces conditions sont satisfaites — c'est bien le cas dans l'exemple qui nous intéresse — la dimension L^r de la mesure μ_x est la même pour tout x dans X , et donnée par la formule

$$\dim_r \mu_x = \min \left(1, \frac{\int_X \log \|\Delta(x)\|_r^r d\mathbb{P}(x)}{(r-1) \log \lambda} \right), \quad (5) \quad \text{sf}$$

où $\|\Delta(x)\|_r^r = \sum_{y \in \text{Supp } \Delta(x)} (\Delta(x)(\{y\}))^r$. Le lecteur [scrupuleux](#) vérifiera par lui-même que cette formule redonne bien le théorème 6. [\[th:shproj\]](#)

3.2 Combinatoire additive

La démonstration de la formule [\(5\)](#) ^{sf} est l'aboutissement de méthodes d'analyse multi-échelle des mesures développées depuis le début des années 2000 par Bourgain, puis par Hochman. Un aspect important de ces méthodes est leur

lien avec la *combinatoire additive*. Ce domaine des mathématiques, qui a connu un essor remarquable ces dernières décennies, a pour objet les liens entre la combinatoire et la structure de groupe. Étant donnée une partie A dans \mathbb{R} , on s'intéresse par exemple à l'ensemble « somme » :

$$A + A = \{a + b ; a, b \in A\}.$$

L'archétype des résultats du domaine est sans doute le théorème inverse de Freiman, qui décrit la structure des parties de \mathbb{Z} qui croissent peu sous l'effet de l'addition.

Théorème 7 (Freiman). *Étant donné un paramètre $K \geq 2$, il existe une constante $C = C(K)$ telle que l'énoncé suivant soit vérifié.*

Si $A \subset \mathbb{Z}$ est une partie finie telle que $|A + A| \leq K|A|$, alors il existe $d \leq C$, un parallélépipède $B = [L_1, M_1] \times \cdots \times [L_d, M_d]$ dans \mathbb{Z}^d et un morphisme de groupes $\phi: \mathbb{Z}^d \rightarrow \mathbb{Z}$ tel que

$$A \subset \phi(B) \quad \text{et} \quad |\phi(B)| \leq C|A|.$$

Notons que l'ensemble $\phi(B)$ vérifie $|\phi(B) + \phi(B)| \leq 2^C |\phi(B)|$; l'imprécision du théorème ne réside que dans l'expression de la constante C en fonction du paramètre K .

La démonstration de Shmerkin utilise un analogue *discrétisé* du théorème de Freiman. Ayant fixé une petite échelle $\delta > 0$, on évalue la taille d'un ensemble borné A dans \mathbb{R} par son nombre de recouvrement

$$N(A, \delta) = \min\{N ; \exists x_1, \dots, x_N : A \subset \bigcup_{i=1}^N B(x_i, \delta)\}.$$

On cherche alors à décrire les parties A qui vérifient

$$N(A + A, \delta) \leq \delta^{-\varepsilon} N(A, \delta). \tag{6}$$

smalldoubling

Exemple. Soit T un grand entier, m un entier plus grand encore, et $\delta = 2^{-mT}$. Étant donnée une partie \mathcal{I} de $\{1, \dots, m\}$, on pose

$$A = \{x = \sum_{i \in \mathcal{I}} a_i 2^{-iT} ; 0 \leq a_i < 2^T\}.$$

Alors, $N(A, \delta) = 2^{T|\mathcal{I}|}$, tandis que $N(A + A, \delta) \leq 2^{(T+1)|\mathcal{I}|} \leq \delta^{-\frac{1}{T}} N(A, \delta)$.

À toute partie bornée A dans \mathbb{R} , on peut associer un arbre qui décrit la structure multi-échelle de A . Ayant fixé un grand entier T , les sommets de l'arbre au niveau i correspondent aux intervalles de longueur 2^{-iT} qui rencontrent A . Les arêtes de l'arbre relient un intervalle de longueur 2^{-iT} à tous les sous-intervalles de longueur $2^{-(i+1)T}$ qui rencontrent A . Dans l'exemple ci-dessus, on distingue deux types de niveaux :

- si $i \in \mathcal{I}$, le branchement est maximal, égal à 2^T ;
- si $i \notin \mathcal{I}$, le branchement est minimal, égal à 1.

Cela n'est pas anodin, et un résultat de Bourgain montre que l'arbre associé à toute partie A vérifiant (6) possède une structure semblable. L'ensemble des niveaux se divise en deux parties : à certaines échelles, le branchement est essentiellement maximal, tandis qu'il est presque trivial aux autres échelles.

Cette propriété remarquable est exploitée par Shmerkin pour étudier les produits de convolutions de mesures, du point de vue de la norme L^r . Il montre ainsi un « théorème inverse » pour la norme L^r à échelle δ , qui est un analogue pour les mesures du résultat de Bourgain : si deux probabilités μ et ν sur $\delta\mathbb{Z} \cap [0, 1]$ vérifient l'inégalité

$$\|\mu * \nu\|_{L^r} \geq \delta^\varepsilon \|\mu\|_{L^r}$$

alors μ et ν admettent une structure multi-échelle voisine de celle mise en évidence ci-dessus. C'est ce théorème inverse qui permet de démontrer la formule de Shmerkin pour la dimension L^r des mesures dynamiquement auto-similaires.

Conclusion

Malgré cette avancée remarquable de Shmerkin et Wu sur le problème de Furstenberg, la conjecture 2 reste ouverte. Les implications du théorème 2 en ce qui concerne la conjecture 3 au sujet de l'écriture de 2^n en base 10 ne semblent pas non plus très claires. Il serait pourtant intéressant d'avoir au moins un résultat partiel sur la densité des entiers n tels que 2^n ne contient pas tous les chiffres en base 10. Il existe encore bien d'autres conjectures sur l'écriture de 2^n dans d'autres bases. Par exemple, Erdős a conjecturé que pour $n \geq 9$, l'écriture en base 3 de 2^n contient toujours un 2 ; et cette fois, même une résolution de la conjecture 2 ne donnerait sans doute pas d'information sur ce problème difficile.

Enfin, il faut mentionner que si le théorème de Shmerkin et Wu donne une borne supérieure optimale sur la dimension d'une intersection d'ensembles fermés invariants, on ne dispose presque d'aucune information sur la borne inférieure, même dans les cas les plus simples. À titre d'exemple, considérons l'ensemble de Cantor triadique C_3 , et l'ensemble C_4 des réels qui n'admettent ni 1 ni 2 dans leur écriture en base 4. D'après le théorème 2, on peut majorer

$$\dim_{\text{H}}(C_3 \cap C_4) \leq \frac{\log 2}{\log 3} + \frac{1}{2} - 1 \simeq 0.1309...$$

mais il semble qu'on ne sache même pas si cette intersection est infinie !

Références

austin

- [1] Tim Austin. A new dynamical proof of the Shmerkin-Wu theorem. *J. Mod. Dyn.*, 18 :1–11, 2022.

- boshernitzan [2] Michael D. Boshernitzan. Elementary proof of Furstenberg’s diophantine result. *Proc. Am. Math. Soc.*, 122(1) :67–70, 1994.
- blmv [3] Jean Bourgain, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Some effective results for $\times a \times b$. *Ergodic Theory Dyn. Syst.*, 29(6) :1705–1722, 2009.
- furst2 [4] H. Furstenberg. Intersections of Cantor sets and transversality of semi-groups. Probl. Analysis, Sympos. in Honor of Salomon Bochner, Princeton Univ. 1969, 41-59 (1970)., 1970.
- furst1 [5] Harry Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Syst. Theory*, 1 :1–49, 1967.
- hs [6] Michael Hochman and Pablo Shmerkin. Local entropy averages and projections of fractal measures. *Ann. Math. (2)*, 175(3) :1001–1059, 2012.
- johnson [7] Johnson. Measures on the circle invariant under multiplication by a non-lacunary subsemigroup of the integers. *Israel J. Math.*, 77(1-2) :211–240, 1992.
- malicet [8] Dominique Malicet. Furstenberg theorem. *notes for a talk in the workshop “groups acting on manifolds”, Teresópolis, available at <https://perso.crans.org/mdominique/>*, 2016.
- rudolph [9] Daniel J. Rudolph. $\times 2$ and $\times 3$ invariant measures and entropy. *Ergodic Theory Dyn. Syst.*, 10(2) :395–406, 1990.
- shmerkin [10] Pablo Shmerkin. On Furstenberg’s intersection conjecture, self-similar measures, and the L^q norms of convolutions. *Ann. Math. (2)*, 189(2) :319–391, 2019.
- wu [11] Meng Wu. A proof of Furstenberg’s conjecture on the intersections of $\times p$ - and $\times q$ -invariant sets. *Ann. Math. (2)*, 189(3) :707–751, 2019.