Introduction à la combinatoire additive

Pierre-Yves Bienvenu

7 novembre 2013

Table des matières

La combinatoire additive est un domaine neuf et en plein essor, pour une large part issu des conjectures et des questions de Paul Erdös (1913-1996), sur des problèmes variés touchant à la structure additive des nombres entiers. Par exemple :

- Quelle est la taille maximale d'une partie de $[n] = \{1, \cdots, n\}$ sans progression arithmétique de longueur 3 ?
- En général, quelle est la taille maximale d'une partie B sans triplets sommants $(x, y, x+y)$ d'un ensemble A de cardinal n d'entiers ?

Dans ce mémoire, il s'agira d'étudier l'existence et la fréquence de motifs additifs tels que les progressions arithmétiques ou les triplets sommants dans des parties de groupes abéliens.

1 Présence de motifs dans des ensembles d'entiers ou dans des coloriages

Nous présenterons ici essentiellement trois motifs :

1. Les triplets sommants ou de Schur : triplets (x, y, z) avec $x + y = z$.
2. Les progressions arithmétiques :

   Définition 1.1. Une progression arithmétique de longueur ℓ est un ℓ-uplet de la forme $(x, x + d, x + 2d, \cdots, x + (\ell - 1)d)$. C'est donc aussi un ℓ-uplet $(x_1, \cdots, x_\ell)$ vérifiant les $\ell - 2$ équations $x_{i-1} + x_{i+1} = 2x_i$ pour $1 < i < \ell$.

3. Les quadruplets additifs : (x, y, z, w) avec $x+y = z+w$. Les progressions de longueur 3 sont un cas particulier de quadruplet additif (cas $z = w$ ou encore $x = y$).

1.1 Triplets sommants

Issaï Schur démontra dès 1907 que les triplets sommants apparaissent spontanément dans les coloriages.

Théorème 1.1 (Schur). *Pour tout coloriage de $\mathbb{Z}$ en un nombre fini k de couleurs, il existe un triplet* monochromatique $\{x, y, z\}$ *tel que $x + y = z$.*

Ce théorème, comme beaucoup d'énoncés de cette famille, admet une reformulation « finitiste ».

Théorème 1.2. *Pour tout k, il existe $n_0 = n_0(k)$ tel que pour tout $n > n_0(k)$ et pour tout coloriage de $\{1, \cdots, n\}$ en k couleurs, il existe un triplet* monochromatique $\{x, y, z\}$ *tel que $x + y = z$.*

Ainsi, il est impossible de séparer tous les couples $(x, y, x + y)$ en partitionnant $\mathbb{Z}$ en un nombre fini de couleurs. Ce théorème a évidemment des airs de théorie de Ramsey, bien connue en théorie des graphes, dont la philosophie générale est que le désordre total est impossible, que des structures fortes survivent au chaos. Prenons le temps de développer l'analogie entre graphes et groupes abéliens, car elle est féconde. Énonçons d'abord le théorème de Ramsey adapté à notre situation.

Théorème 1.3 (Ramsey). *Pour tous entiers k et r, il existe $n_0 = n_0(k,r)$ tel que pour tout $n > n_0(k,r)$ et pour tout coloriage du graphe complet K_n en k couleurs, il existe un sous-K_r monochromatique de K_n.*

Le cas $k = 2, r = 3$ (pour lequel le n_0 minimal garantissant la propriété est 6) fait partie du folklore sous la forme suivante : dans un groupe de 6 personnes présentes à une soirée, il existe un groupe de 3 personnes qui se connaissent toutes ou un groupe de 3 personnes mutuellement étrangères.

Appliquons-le à notre problème de combinatoire additive. Soit donc k un nombre entier, $r = 3$, et prenons le $n_0(k,3)$ prescrit par le théorème de Ramsey ainsi qu'un entier $n > n_0$. Soit $c : [n] \to [k]$ un coloriage de $[n]$. Dérivons-en un coloriage de K_n de la manière suivante

$$\tilde{c}(\{x,y\}) = c(|x-y|).$$

Il existe donc un triplet $\{x,y,z\}$ tel que les trois arêtes $\{x,y\},\{x,z\}\{z,y\}$ aient la même couleur. Supposons sans perte de généralité que $x < y < z$; alors $z-y, y-x$ et $z-x$ ont la même couleur et $z-x = (z-y)+(y-x)$. Ceci est un triplet de Schur monochromatique.

1.2 Progressions arithmétiques

Un théorème parfaitement analogue au théorème de Schur existe pour les progressions arithmétiques, en version infinitiste et en version finitiste.

Théorème 1.4 (van der Waerden).
- *Pour tout $\ell \in \mathbb{N}$, pour tout coloriage de $\mathbb{Z}$ en un nombre fini k de couleurs, il existe une progression arithmétique* monochromatique *de longueur ℓ.*
- *Pour tout k et pour tout ℓ, il existe $n_0 = n_0(k,\ell)$ tel que pour tout $n > n_0$ et pour tout coloriage de $[n]$ en k couleurs, il existe une progression arithmétique monochromatique de longueur ℓ.*

Le théorème de van der Waerden est beaucoup plus difficile à démontrer. Il est remarquablement équivalent à un théorème de dynamique topologique. Comme souvent, Tao en a fait un merveilleux exposé [4].

Pour le moment, les progressions arithmétiques et les triplets de Schur exhibent un comportement analogue : dans une partition des entiers, ils apparaissent inévitablement dans l'une des parties. En fait les progressions arithmétiques sont beaucoup plus robustes. Elles apparaissent spontanément dans tout ensemble qui contient une proportion non nulle des entiers. Ainsi, pour éradiquer toute progression arithmétique dans $\mathbb{Z}$, on est contraint d'en ôter « presque tous » les éléments. Formulons ce théorème majeur, dû à Szémeredi.

Définition 1.2. La *densité supérieure* d'une partie A de $\mathbb{Z}$ est $d(A) = \limsup_{N\to+\infty} d_N(A)$ où $d_N(A) = \frac{|A\cap[-N,N]|}{2N+1}$. Une partie A de $\mathbb{Z}$ est dite dense si $d(A) > 0$.

Cette notion formalise bien l'idée d'un ensemble qui contient une « proportion non nulle » des entiers.

Remarque 1.1. Quand on ne tient pas absolument à l'existence d'un inverse additif à tout élément, on peut tout aussi bien parler de densité de $A \subset \mathbb{N}$ et poser $d_N(A) = \frac{|A \cap [1,N]|}{N}$ (on admettra qu'il n'y aura pas confusion entre densité dans $\mathbb{Z}$ et dans $\mathbb{N}$, la différence étant au pire un facteur 2, qui ne change pas la positivité stricte).

Exemples 1.1.
- Une progression arithmétique de raison r (ou encore une classe de congruence modulo r) a pour densité $1/r$.
- L'ensemble A des carrés et de leurs opposés a une densité nulle car $A \cap [-N, N] = [-\lfloor\sqrt{N}\rfloor, \lfloor\sqrt{N}\rfloor]$ qui a pour cardinal $2\lfloor\sqrt{N}\rfloor + 1$ donc $d_N(A) = O(1/\sqrt{N})$.
- La partie B de $\mathbb{N}$ définie par $A \cap [N^2+1, (N+1)^2] = [\lceil\frac{(N+1)^2-N^2}{2}\rceil, (N+1)^2]$ a densité $1/2$.

Théorème 1.5 (Széméredi). *Toute partie dense de $\mathbb{Z}$ contient des progressions arithmétiques arbitrairement longues.*

Ainsi, une simple propriété de cardinalité peut contraindre un ensemble, aussi désordonné soit-il, à contenir de grandes structures. Ce théorème fondamental n'est pas sans rappeler les idées de Ramsey.

Remarques 1.2.
- En quelque sorte, ce théorème dit que la progression arithmétique (exemple 1 ci-dessus) est l'exemple archétypal de l'ensemble dense. Bien entendu, il ne faut tout de même pas réclamer une progression infinie. Par exemple la partie B de l'exemple ci-dessus, ne saurait contenir une progression infinie d'une quelconque raison k, car à partir d'un certain rang, il n'y a aucun couple (a, b) d'éléments de B séparés d'une distance inférieure ou égale à k.
- Ce théorème implique évidemment celui de van der Waerden, car dans une partition en r parties $A_1, \cdots, A_r$, le principe des tiroirs implique que pour tout $N \in \mathbb{N}$, il existe i_N tel que $d_N(A_{i_N}) \geq 1/r$. La suite des i_N prenant un nombre fini de valeurs, il existe une valeur $i \in [r]$ qui est prise infiniment souvent. Et alors $d(A_i) \geq 1/r$, donc la partie A_i est dense.
- Un théorème analogue est impossible pour les triplets de Schur, puisque l'ensemble des nombres impairs a une densité $1/2$ mais aucun triplet de Schur. Notons toutefois que son complémentaire compense abondamment cette carence, puisque pour tout couple (x, y) de nombres pairs, leur somme $x + y$ est également paire.
- L'analogue multiplicatif de la progression arithmétique, la progression géométrique, ne jouit pas du tout de la même propriété : l'ensemble des nombres sans facteur carré, dont la densité est bien connue - elle vaut $6/\pi^2$ - ne risque pas de contenir une progression a, ar, ar^2.

Le théorème de Szemerédi a pu être exploité par Ben Green et Terence Tao pour établir la présence de progressions arithmétiques dans un célèbre ensemble de densité nulle, l'ensemble des nombres premiers.

Théorème 1.6. *L'ensemble des nombres premiers contient des progressions arithmétiques arbitrairement longues.*

Une autre généralisation du théorème de Szemerédi, qui implique également celui de Green-Tao, est la conjecture suivante.

Conjecture 1.7. *Soit $A \in \mathbb{N}^*$ un ensemble d'entiers tel que $\sum_{n\in A} \frac{1}{n} = \infty$. Alors A contient des progressions arithmétiques de toute longueur.*

La réciproque ne risque pas d'être vraie. Il suffit de prendre pour A une progression de longueur 3 et raison 1 suivie d'un vide de 8 chiffres, puis une progression de longueur 4 suivi d'un vide de 16 chiffres,..., une progression de longueur k suivi d'un vide de 2^k chiffres. Alors la somme des inverses des éléments de l'ensemble obtenu est finie.

1.3 Quadruplets additifs

Les quadruplets additifs sont encore plus ubiquitaires, et ce fait est très facile à démontrer, contrairement au théorème de Szemerédi.

Proposition 1.8. *Soit A une partie de $\mathbb{Z}$ telle que $|A \cap [-N, N]| \geq \delta N$. Alors A contient au moins $C\delta^4 N^3$ quadruplets addititfs où C est une constante positive absolue.*

Preuve. Les différences $z = x - y$ entre éléments de A s'étalent entre $-2N$ et $2N$. Notons c_z le nombre de couples (x, y) tels que $z = x - y$. Alors le nombre de couples, soit au moins $(\delta N)^2$, est donné par $\sum_{z\in[-2N,2N]} c_Z$ et le nombre de quadruplets additifs vaut $\sum_{z\in[-2N,2N]} c_z^2$. Par l'inégalité de Cauchy-Schwarz, ceci vaut au moins

$$\frac{(\sum_{z\in[-2N,2N]} c_z)^2}{4N+1} \geq \delta^4 N^3/5$$

Puisqu'il y a de l'ordre de N^3 quadruplets additifs dans $[-N, N]$, la proportion des quadruplets additifs de $[-N, N]$ qui sont dans A varie de manière polynomiale avec la densité. Nous verrons que ce n'est pas le cas du tout des progressions arithmétiques.

2 Aspects quantitatifs

Le théorème de Szemerédi est un théorème existentiel qu'on peut chercher à préciser quantitativement sur deux points.

- À partir de quel degré précis de densité un ensemble d'entiers est-il contraint de contenir des progressions arithmétiques ?
- À quel point, en fonction de la densité, les progressions arithmétiques sont-elles fréquentes ?

Nous allons aborder ces deux questions successivement, puis c'est surtout la deuxième qui retiendra notre attention.

2.1 Densité maximale d'ensemble sans progression arithmétique de longueur k

Le théorème de Szemerédi admet aussi des reformulations finitistes, à partir desquelles on peut soulever la première question évoquée ci-dessous.

Théorème 2.1. – *Pour tout $k \in \mathbb{N}$, pour tout $\delta > 0$, il existe $N = N(\delta, k)$ tel que toute partie $A \subset [N]$ de cardinal $|A| > \delta N$ contient une progression arithmétique de longueur k.*

– *Pour tout $k \in \mathbb{N}$, pour tout $N \in \mathbb{N}$, il existe $\delta = \delta(N,k)$ (pris minimal) tel que toute partie $A \subset [N]$ de cardinal $|A| > \delta N$ contient une progression arithmétique de longueur k.*

Un des grands problèmes en combinatoire additive est de fournir des bornes concernant $N(\delta, k)$ ou, de manière équivalente $\delta(N, k)$.

2.1.1 Progressions de longueur 3

Le cas particulier $k = 3$ du théorème de Szemerédi avait déjà été obtenu par Klaus Roth en 1953. Un bon exposé est donné par [3]. La borne obtenue est $N(\delta, 3) \leq \exp(\exp(C\delta^{-1}))$ soit $\delta(N, 3) \leq \frac{C}{\log\log N}$, où C est une constante absolue qui vaut en fait $132 \log 2$.

Un exemple de grand ensemble sans progression de longueur 3 a été mis au point par Behrend dès 1946 et sa construction n'a pas été grandement améliorée depuis.

Théorème 2.2. *Il existe un ensemble $A \subset [N]$ sans progression de longueur 3 dont le cardinal est $|A| > N \exp(-c\sqrt{\log N})$. Autrement dit, $\delta(N, 3) \geq \exp(-c\sqrt{\log N})$.*

Entre la borne inférieure et la borne supérieure, il y a un vrai fossé.

2.1.2 Progressions de longueur k quelconque

Le cheminement de Szemerédi ne donnait pas de borne effective sur la densité maximale, mais l'intervention de Timothy Gowers en 2001 a permis d'en savoir plus.

Théorème 2.3. *Pour tout $k \in \mathbb{N}$, il existe une constante c_k telle que $\delta(N, k) \leq \frac{C}{(\log\log N)^{c_k}}$.*

2.2 Nombre de motifs

Dans l'ensemble $[N]$, pour former une progression arithmétique de longueur k, il faut sélectionner $x \in [N]$ et d tel que $x + (k-1)d \in [N]$, donc le nombre de progressions arithmétiques de longueur k inclues dans $[N]$ est équivalent à $\frac{N^2}{k-1}$, et donc de l'ordre de grandeur de N^2. Le théorème de Szemerédi dit en fait que si $A \subset \mathbb{Z}$ est dense, une proportion positive des progressions arithmétiques possibles sont inclues dans A. Ceci s'exprime de la manière suivante.

Théorème 2.4. *Soit $A \subset [N]$ telle que $|A| = \delta N$ avec $\delta > \delta(N, k)$; alors A contient au moins $c_k(\delta)N^2$ progressions arithmétiques de longueur k, où $c_k(\delta)$ est une constante positive.*

La variation de $c_k(\delta)$ n'est absolument pas polynomiale. Avec le même genre de constructions que Behrend, on peut construire un ensemble dense particulièrement pauvre en progressions.

Proposition 2.5. *Il existe une constante positive absolue c telle que pour tout $\delta > 0$ et N entier, il existe un ensemble A de $[N]$ de densité au moins δ qui contient au plus $\delta^{c \log \frac{1}{\delta}}$ progressions de longueur 3.*

3 Motifs dans les groupes groupes abéliens

L'ensemble $\{1, \ldots, N\}$ présente le grand désavantage de ne pas être fermé sous l'addition, et $\mathbb{Z}$ celui d'être infini. Ainsi, bien que ce qui nous intéresse fondamentalement soit d'obtenir en dernière instance des résultats concernant les nombres entiers, nous n'hésiterons pas à remplacer $[N]$ par $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$, ou même par $\mathbb{F}_p^n$ (et nous noterons alors encore $N = p^n$ le cardinal du groupe). La structure de groupe permet notamment de faire de l'analyse de Fourier. Et la structure d'espace vectoriel de $\mathbb{F}_p^n$ lui confère le grand avantage d'avoir beaucoup de sous-structures, tout en introduisant des interprétations géométriques. Les preuves deviennent limpides et éclairent la situation dans $[N]$. Nous supposerons N très grand car nous visons des résultats asymptotiques.

3.1 Notations

Un *motif* dans le groupe G est un r-uplet $(x_1, \cdots, x_r)$ de solutions au système d'équations $f_j(x_1, \cdots, x_r) = 0$ pour tout $j \in [m]$, où $f_1, \cdots, f_m$ sont des fonctions $G^r \to \mathbb{C}$. Si l'on note $\mathcal{S}$ ce système d'équations et si $A \subset G$, on note $N_{\mathcal{S}}(A)$ la proportion de r-uplets appartenant à A^r parmi les r-uplets solutions, i.e. le nombre de r-uplets solutions faits d'éléments de A divisé par le nombre total de solutions. On l'appelle *le nombre normalisé de motifs* dans A.

Pour un coloriage ou une partition $A_1, \cdots, A_r$ de G, on note $M_{\mathcal{S}}(A_1, \cdots, A_r) = N_{\mathcal{S}}(A_1) + \cdots + N_{\mathcal{S}}(A_r)$ le nombre normalisé de motifs $\mathcal{S}$ monochromatiques. On note $M_{\mathcal{S}}(A) = M_{\mathcal{S}}(A, A^c)$.

On utilisera la notation $\mathbb{E}_{x \in X} = \frac{\sum_{x \in X}}{|X|}$ pour la moyenne. Le symbole $\mathbb{E}$ peut aussi désigner l'espérance d'une variable aléatoire, mais il n'y aura pas de risque de confusion. Le symbole $\mathbb{P}$ signifiera probabilité.

3.2 Notion de nombre espéré

Nous allons présenter cette notion sur le cas des progressions de longueur 3. Soit A une partie d'un groupe abélien sans 2-torsion G de cardinal N et notons $\alpha = |A|/N$. Le nombre normalisé de progressions arithmétiques de longueur 3 dans A s'écrit simplement :

$$N_{3-AP}(A) = \mathbb{E}_{x,d \in G} 1_A(x) 1_A(x+d) 1_A(x+2d)$$

Cette manière de compter inclut les progressions triviales x, x, x et compte deux fois chaque progression non-triviale $\{x, x+d, x+2d\}$ car les deux couples (x, d) et $(x + 2d, -d)$ génèrent cette progression. Déterminons l'espérance de ce nombre lorsque l'on tire au hasard un ensemble $\mathcal{A}$ en prenant chaque élément x de G avec probabilité $\alpha \in [0, 1]$, indépendamment les uns des autres. Autrement dit, pour toute partie $A \subset G$ de cardinal k, on a $\mathbb{P}(\mathcal{A} = A) = \alpha^k (1-\alpha)^{N-k}$. De manière équivalente si $G = \{x_1, \ldots, x_N\}$, cela revient à définir N variables booléennes indépendantes et identiquement distribuées $Z_1, \ldots, Z_N$ telles que $\mathbb{P}(Z_i = 1) = \alpha$ et à considérer $\mathcal{A} = \{x_i | Z_i = 1\}$. Ainsi, $\mathbb{E}(|\mathcal{A}|) = N\alpha$.

Et de même

$$\begin{aligned} N^2\mathbb{E}(N_{3-AP}(\mathcal{A}) &= \mathbb{E}(\sum_{x,d\in G} 1_{\mathcal{A}}(x)1_{\mathcal{A}}(x+d)1_{\mathcal{A}}(x+2d)) \\ &= \sum_{x,d\in G} \mathbb{E}(1_{\mathcal{A}}(x)1_{\mathcal{A}}(x+d)1_{\mathcal{A}}(x+2d)) \\ &= \sum_{x\in G} \mathbb{E}1_{\mathcal{A}}(x) + \sum_{x\in G} \mathbb{E}_{x,d\in G,d\neq 0}(1_{\mathcal{A}}(x)1_{\mathcal{A}}(x+d)1_{\mathcal{A}}(x+2d)) \end{aligned}$$

Or, $\mathbb{E}1_{\mathcal{A}}(x) = P(x \in \mathcal{A}) = \alpha$ quel que soit $x \in G$, donc la première somme fait $N\alpha$. Quant à la deuxième somme, sachant que les événements $\{x \in \mathcal{A}\}, \{x+d \in \mathcal{A}\}, \{x+2d \in \mathcal{A}\}$ sont indépendants (nous utilisons que $2d \neq 0$ quel que soit $d \in G$), on a

$$\mathbb{E}_{x,d\in G,d\neq 0}(1_{\mathcal{A}}(x)1_{\mathcal{A}}(x+d)1_{\mathcal{A}}(x+2d)) = \mathbb{P}(\{x \in \mathcal{A}\})\mathbb{P}(\{x+d \in \mathcal{A}\})\mathbb{P}(\{x+2d \in \mathcal{A}\}) = \alpha^3$$

d'où finalement

$$\mathbb{E}(N_{3-AP}(\mathcal{A})) = \alpha N^{-1} + \alpha^3 N^{-1}(N-1) \sim \alpha^3$$

On dira alors que *le nombre espéré normalisé de 3-APs* dans un ensemble de densité α de G est α^3.

Définition 3.1. On appelle nombre espéré normalisé de motifs $\mathcal{S}$ pour $\alpha \in [0,1]$ la quantité

$$N_{\mathcal{S}}(\alpha) = \lim_{N\to\infty} \mathbb{E}(N_{\mathcal{S}}(\alpha))$$

si cette limite existe, l'espérance étant prise sur l'expérience aléatoire décrite plus haut, et N étant le cardinal du groupe $\mathbb{Z}_N$ ou $\mathbb{F}_p^n$. De manière analogue, on définit $N_{\mathcal{S}}(\alpha)$ le nombre espéré normalisé de motifs $\mathcal{S}$ monochromatiques.

Par la suite, nous chercherons à quantifier le caractère « aléatoire » d'un ensemble en comparant le nombre de motifs qu'il exhibe au nombre espéré de motifs ; on appellera pseudo-aléatoire ou uniforme un ensemble qui exhibe à peu près le nombre espéré de motifs.

3.3 L'analyse de Fourier classique

L'analyse de Fourier va nous offrir un premier moyen de quantifier ce caractère aléatoire. Soit G un groupe abélien fini qui sera $\mathbb{Z}_N$ avec N premier ou $\mathbb{F}_p^n$. Soit $\omega = \exp(2i\pi/N)$ une racine N-ème (ou p-ème) de l'unité. Pour cette partie, la référence est [1].

Définition 3.2. Soit f une fonction de G dans $\mathbb{C}$. La transformée de Fourier $\widehat{f}$ est alors la fonction définie sur $\widehat{G}$, l'espace des phases, qui est en fait isomorphe à G, à valeurs dans $\mathbb{C}$, par la formule

$$\widehat{f}(t) = \mathbb{E}_{x\in G} f(x)\omega^{t\cdot x}$$

où $t \cdot x$ est tout simplement le produit dans l'anneau $\mathbb{Z}_N$ et le produit scalaire canonique dans l'espace vectoriel $\mathbb{F}_p^n$. Par la suite on omettra souvent le point du produit scalaire.

La mesure sur G est la mesure de probabilité uniforme ; la mesure correspondante sur $\widehat{G}$ est alors la mesure de comptage. Ainsi, on notera par exemple $\|f\|_2 = \mathbb{E}_x(|f(x)|^2)$ pour une fonction $f : G \to \mathbb{C}$ et $\left\|\widehat{f}\right\|_2 = \sum_t \left|\widehat{f}(t)\right|^2$ Nous serons surtout intéressés par le cas où f est la fonction indicatrice d'un ensemble.

Remarques 3.1.

1. Si $f = 1_A$ est l'indicatrice de la partie A, alors $\widehat{f}(0) = |A|/N = \alpha$ est la densité de A, et pour tout t, on a $\left|\widehat{1_A}(t)\right| \leq \alpha$ par inégalité triangulaire.
2. Si f est constamment égale à 1, alors $\widehat{f}(0) = 1$ et si $t \neq 0$, alors $\widehat{f}(t) = 0$.
3. Si $g(x) = f(x-d)$, alors $\widehat{g}(t) = \omega^{dt}\widehat{f}(t)$ et en particulier $|\widehat{g}(t)| = \left|\widehat{f}(t)\right|$.
4. Si $g(x) = f(-x)$, alors $\widehat{g} \leq \widehat{\overline{f}}$. En particulier, si $A = -A$, alors $\widehat{1_A}$ est à valeurs réelles.
5. On a l'identité suivante : $\widehat{1_{A^c}}(0) = 1 - \alpha$, et pour $t \neq 0, \widehat{1_{A^c}}(t) = -\widehat{1_A}$.
6. Si V est un hyperplan de $\mathbb{F}_p^n$, par exemple $V = t^\perp$ pour un certain t, alors $\widehat{1_V}(t) = \widehat{1_V}(0) = 1/p$.

La transformée de Fourier possède quelques propriétés classiques bien connues qui sont particulièrement faciles à démontrer dans le cas discret.

Proposition 3.1. *Soit f et g deux fonctions de G dans $\mathbb{C}$*

1. *Inversion : $f(x) = \mathbb{E}_{t\in G}\widehat{f}(t)\omega^{-x\cdot t}$.*
2. *Convolution : si $f * g(x) = \mathbb{E}_{y\in G} f(y)g(x-y)$, alors $\widehat{f * g} = \widehat{f}\widehat{g}$.*
3. *Conservation du produit scalaire : $\mathbb{E}_{x\in G} f(x)\overline{g(x)} = \sum_{t\in G} \widehat{f(t)}\overline{\widehat{g(t)}}$.*
4. *Identité de Parseval (« conservation de l'énergie ») : $\mathbb{E}_{x\in G}|f(x)|^2 = \sum_{t\in G}\left|\widehat{f}(t)\right|^2$.*

Le fait suivant nous fait soupçonner l'aptitude de la transformée de Fourier à la mesure de l'uniformité, de la proximité à l'aléatoire : un ensemble aléatoire a de très fortes chances d'avoir tous ses coefficients non-triviaux de Fourier minuscules. Au contraire un ensemble très structuré comme un hyperplan, qu'on ne s'attend pas du tout à voir surgir du hasard, a un coefficient de Fourier non-trivial important (cf remarques plus haut).

Proposition 3.2. *Si la partie A est tirée au hasard du groupe G, selon la modalité évoquée en 3.2, avec $\alpha \neq 0$, alors pour $\epsilon > 0$ fixé, avec une probabilité tendant vers 1 quand N tend vers l'infini, on a*

$$\sup_{t\neq 0}\left|\widehat{1_A}(t)\right| \leq O\left(N^{(-1+\epsilon)/2}\right).$$

Preuve. Pour $t \neq 0$, on a $N \cdot \left|\widehat{1_A}(t)\right| = N \cdot \left|\widehat{f_A}(t)\right| = N \cdot \sum_{x\in G} f_A(x)\omega^{xt}$. Notons $Z_x = f_A(x)\omega^{xt}$. C'est une variable aléatoire d'espérance nulle, de module $|Z_x| \leq 1$. Les théorèmes de concentration de la mesure, comme l'inégalité d'Azuma, fournissent l'existence de constantes positives absolues C, c, telles que pour tout $\lambda > 0$

$$\mathbb{P}(N \cdot |\widehat{1_A}(t)| \geq \lambda\sqrt{N}) \leq C\exp -c\lambda^2$$

et donc, en prenant $\lambda = N^{\epsilon/2}$ pour un petit $\epsilon > 0$, et en bornant la probabilité de l'union par la somme des probabilités

$$\mathbb{P}(\sup_{t\neq 0}|\widehat{1_A}(t)| \geq N^{(-1+\epsilon)/2}) \leq N \cdot C \exp -cN^{\epsilon}$$

La transformation de Fourier a un intérêt dans le comptage des progressions arithmétiques.

Définition 3.3. Pour trois fonctions f_1, f_2, f_3 de G dans $\mathbb{C}$, on note $T_3(f_1, f_2, f_3) = \mathbb{E}_{x,d\in G} f_1(x) f_2(x+d) f_3(x+2d)$.

Cette définition représente le nombre de progressions « le long » de f_1, f_2, f_3. En particulier, si A est une partie de G

$$N_{3-AP}(A) = T_3(1_A, 1_A, 1_A)$$

Proposition 3.3. *Pour trois fonctions f_1, f_2, f_3 de G dans $\mathbb{C}$ on a*

$$T_3(f_1, f_2, f_3) = \sum_{t\in G} \widehat{f_1}(t)\widehat{f_2}(-2t)\widehat{f_3}(t)$$

Preuve. En utilisant la propriété d'inversion, on a

$$\begin{aligned} T_3(f_1, f_2, f_3) &= \mathbb{E}_{x,d\in G} \sum_{t_1,t_2,t_3\in G} \widehat{f_1}(t)\omega^{-xt_1}\widehat{f_2}(t)\omega^{-(x+d)t_2}\widehat{f_3}(t)\omega^{-(x+2d)t_3} \\ &= \sum_{t_1,t_2,t_3\in G} \widehat{f_1}(t)\widehat{f_2}(t)\widehat{f_3}(t)\mathbb{E}_{x\in G}\omega^{-x(t_1+t_2+t_3)}\mathbb{E}_{d\in G}\omega^{-d(t_2+2t_3)} \end{aligned}$$

Or, si $t_1 + t_2 + t_3 \neq 0$, alors $\mathbb{E}_{x\in G}\omega^{-x(t_1+t_2+t_3)} = 0$ et de même, si $t_2 + 2t_3 \neq 0$, alors $\mathbb{E}_{d\in G}\omega^{-d(t_2+2t_3)} \neq 0$. Ainsi, les seuls termes de la somme qui contribuent effectivement sont ceux correspondant à des triplets (t_1, t_2, t_3) vérifiant $t_1 + t_2 + t_3 = 0$ et $t_2 + 2t_3 = 0$, autrement dit : $t_2 = -2t_1, t_3 = t_2$. Finalement, on a

$$T_3(f_1, f_2, f_3) = \sum_{t\in G} \widehat{f_1}(t)\widehat{f_2}(-2t)\widehat{f_3}(t).$$

Pour le comptage effectif de progressions arithmétiques dans un ensemble, nous avons le corollaire suivant

Corollaire 3.4. *1. Pour $A \in G$ de densité α, le nombre de progressions arithmétiques de longueur 3 vaut*

$$N_{3-AP}(A) = \sum_{t\in G} \widehat{1_A}(t)^2\widehat{1_A}(-2t) = \alpha^3 + \sum_{t\in G} \widehat{f_A}(t)^2\widehat{f_A}(-2t)$$

où $f_A = 1_A - \alpha$ est la fonction indicatrice centrée.

2. *Si*

$$\left\|\widehat{f_A}\right\|_\infty \leq \alpha^2/2$$

et si N est assez grand, alors A contient des progressions arithmétiques de longueur 3 non-triviales.

Preuve. 1. Il suffit d'appliquer la proposition précédente avec $f_1, f_2, f_3 = 1_A$, puis de remarquer $\widehat{1_A}(0) = \alpha$, et que $\widehat{1_A}(t) = \widehat{f_A}(t)$ pour $t \neq 0$, et que $\widehat{f_A}(0) = 0$.

2. Il faut remarquer que

$$\begin{aligned}\left|\sum_{t\in G} \widehat{f_A}(t)^2\widehat{f_A}(-2t)\right| &\leq \sum_{t\neq 0}\left|\widehat{1_A}(t)^2\widehat{1_A}(-2t)\right| \\ &\leq \left\|\widehat{f_A}\right\|_\infty \sum_t \left|\widehat{1_A}(t)^2\right| \\ &\leq \left\|\widehat{f_A}\right\|_\infty \sum_{t\in G} |1_A|\,(t)^2 = \left\|\widehat{f_A}\right\|_\infty \alpha\end{aligned}$$

par l'identité de Parseval. Ainsi, si $\left\|\widehat{f_A}\right\|_\infty \leq \alpha^2/2$, on a $N_{3-AP}(A) \geq \alpha^3/2$, ce qui signifie que l'ensemble contient au moins $\alpha^3/2N^2$ progressions, ce qui est bien plus (si N est assez grand) que les N progressions triviales. ■

Ainsi, si un ensemble ne contient pas de progression arithmétique, il doit avoir un grand coefficient de Fourier non-trivial. Et alors sa fonction indicatrice 1_A est assez bien corrélée (i.e. a un assez grand produit scalaire) avec une phase linéaire $x \mapsto \omega^{xt}$. C'est sur ce genre de constats que s'appuie la preuve de Roth de l'existence de progressions arithmétiques de longueur 3 dans un ensemble suffisamment dense de $[N]$.

Il y a d'autres motifs encore que la transformée de Fourier contrôle.

1. Le nombre de triplets de Schur dans A est donné par :

$$\mathbb{E}_{x,y} 1_A(x)1_A(y)1_A(x+y) = \alpha^3 + \sum_{t\neq 0} \widehat{1_A}(t)^2\widehat{1_A}(-t)$$

2. Le nombre de quadruplets additifs (solutions à $x+y=z+w$) est donné par $\left\|\widehat{1_A}\right\|_4$.

Ainsi, si la transformée de Fourier est très petite, le nombre effectif de progressions arithmétiques de longueur 3 (ou de triplets de Schur, ou de quadruplets additifs) est très proche du nombre espéré, à savoir α^3N^2 (resp. α^3N^2, α^4N^3) : l'ensemble se comporte à cet égard comme un ensemble aléatoire. Toutefois la transformée de Fourier ne contrôle pas tout : il existe des ensembles arbitrairement uniformes au sens de la transformée de Fourier qui n'ont pas du tout le nombre attendu de progressions de longueur 4.

3.4 Analyse de Fourier d'ordre supérieur

On va définir des normes successives $\|\cdot\|_{U^k}$ sur l'espace des fonctions $G \to \mathbb{C}$, de telle sorte que si la fonction indicatrice centrée f_A d'un ensemble $A \subset G$ est petite pour $\|\cdot\|_{U^k}$, alors l'ensemble a à peu près le nombre espéré de progressions arithmétiques de longueur $k+1$, et donc apparaît « aléatoire » à cet égard. Pour cette partie, la référence est toujours [1].

Définition 3.4. Pour $f : G \to \mathbb{C}$ et k un entier supérieur ou égal à 2, on pose

$$\|f\|_{U^k}^{2^k} = \mathbb{E}_{x\in G, h\in G^k} \prod_{\epsilon\in\{0,1\}^k} \mathcal{C}^\epsilon f(x + \epsilon \cdot h)$$

où $\mathcal{C}^\epsilon z = z$ si $\sum \epsilon_i$ est pair, $\overline{z}$ sinon. On appelle cette norme *norme d'uniformité de Gowers d'ordre k*.

' La norme U^2 compte le nombre de quadruplets additifs vus comme des parallélogrammes $(x, x + a, x + b, x + a + b)$, le long de f (ou encore la moyenne des valeurs de f sur les parallélogrammes, sa valeur sur un parallélogramme étant définie comme le produit de ses valeurs sur les sommets) :

$$\|f\|_{U^2}^4 = \mathbb{E}_{x,a,b} f(x)f(x + a)f(x + b)f(x + a + b)$$

Il est aisé de prouver l'identité

$$\|f\|_{U^2} = \left\|\widehat{f}\right\|_4$$

qui témoigne que les normes d'uniformité de Gowers généralisent la transformée de Fourier. Une telle relation n'existe pas concernant les normes U^k avec $k > 2$ Afin de préparer le terrain pour l'exploitation des normes U^k, reformulons de manière un peu floue, en terme de norme U^2, ce qui a été dit sur la transformée de Fourier.

Proposition 3.5. *1. Théorème de von Neumann généralisé : si A a anormalement peu ou beaucoup de progressions de longueur 3, alors $\|f_A\|_{U^2}$ est grande.*

2. Théorème inverse : si $\|f\|_{U^2}$ est grande, alors f est particulièrement bien corrélée à une fonction $x \mapsto \omega^{tx}$.

Un théorème analogue a été démontré pour la norme U^3, que l'on énonce pour $G = \mathbb{F}_p^n$.

Proposition 3.6. *1. Théorème de von Neumann généralisé : si A a anormalement peu ou beaucoup de progressions de longueur 4, alors $\|f_A\|_{U^3}$ est grande.*

2. Théorème inverse : si $\|f\|_{U^3}$ est grande, alors f est particulièrement bien corrélée à une fonction $x \mapsto \omega^{x\cdot Mx+b\cdot x}$, où M est une matrice et b un vecteur.

Le théorème inverse général a été tout récemment démontré par Green, Tao et Ziegler dans un article sensationnel [2]. Le contrôle des motifs additifs, selon leur *complexité*, par les normes d'uniformité de degré convenable, fait toujours l'objet de recherches.

4 Nombre minimal de motifs dans un coloriage d'un groupe abélien

Colorions un groupe abélien G, de cardinal N pensé très grand, en deux couleurs, ou encore partitionnons G en A et A^c. Étant donné un certain motif fixé, on peut légitimement se demander quel coloriage minimise la fréquence d'apparition de ces motifs, et quel est alors la proportion minimale, quand N tend vers l'infini, de motifs qui sont monochromatiques.

4.1 Quadruplets additifs

Les quadruplets additifs (notés QA), comme on peut s'en douter après la section 2, présentent la propriété de toujours apparaître au moins en nombre espéré dans tout ensemble.

Proposition 4.1. *Soit $A \subset G$ une partie de densité α. Alors*

$$N_{QA}(A) \geq \alpha^4.$$

Preuve. On a déjà dit que $N_{QA}(A)$ était donné par la formule

$$N_{QA}(A) = \sum_{t \in G} \left| \widehat{1_A}(t) \right|^4$$

Or, le terme pour $t = 0$ est α^4 et les autres sont positifs, d'où l'inégalité. ■

Cette proportion étant asymptotiquement égale à la proportion espérée dans un ensemble aléatoire, on peut dire que les ensembles aléatoires minimisent le nombre de quadruplets additifs.

Donc dans un coloriage (A, A^c), chaque partie exhibant au moins le nombre espéré de quadruplets additifs, le coloriage présente bien le nombre espéré de quadruplets additifs monochromatiques.

4.2 Progressions de longueur 3

Contrairement à ce qu'on pourrait penser, le nombre de progressions monochromatiques de longueur 3 dans un coloriage (A, A^c) ne dépend que de la densité α de A, et non du choix des éléments de A : il est toujours égal au nombre espéré, à savoir $\alpha^3 + (1-\alpha)^3$. En effet, $M_{3-AP}(A) = \alpha^3 + (1-\alpha)^3 + \sum_{t \neq 0} (\widehat{1_A}(t)^2 \widehat{1_A}(-2t) + \widehat{1_A^c}(t)^2 \widehat{1_A^c}(-2t)$ et chaque terme de la somme est nul car $\widehat{1_A}(t) = -\widehat{1_A^c}(t)$ pour $t \neq 0$.

4.3 Progressions de longueur 4

Ce cas est intéressant. Wolf et Peng-Lin se sont intéressés au nombre minimal de progressions arithmétiques de longueur 4 dans un coloriage monochromatique de $\mathbb{Z}_N$. Étonamment, ce n'est pas l'ensemble aléatoire qui minimise ce nombre. En effet, le nombre espéré pour un coloriage (A, A^c) est $\alpha^4 + (1-\alpha)^4 \geq 1/8$ (obtenu en $\alpha = 1/2$, par convexité) et Wolf a prouvé dans [5] que certains coloriages atteignaient une proportion légèrement inférieure.

Proposition 4.2. *La densité minimale m_{4-AP} de progressions monochromatiques de longueur 4 dans un bicoloriage de $G = \mathbb{Z}_N$ vérifie*

$$m_{4-AP} \leq \frac{1}{8} \left(1 - \frac{1}{259200} \right) + o(1).$$

La méthode de Wolf n'est pas constructive, et elle s'appuie sur le résultat de Gowers sur l'existence d'un ensemble Fourier-uniforme qui contient moins que le nombre espéré de progressions de longueur 4.

Références

[1] Ben Green. Montréal lecture notes on quadratic Fourier analysis. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 69–102, Providence, RI, 2007. Amer. Math. Soc.

[2] Ben Green, Terence Tao, and Tamar Ziegler. An inverse theorem for the Gowers $U^{s+1}[N]$-norm. *Ann. of Math. (2)*, 176(2) :1231–1372, 2012.

[3] Mustazee Rahman. Roth's theorem on 3-term arithmetic progressions.

[4] Terence Tao. The ergodic and combinatorial approaches to Szemerédi's theorem. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 145–193, Providence, RI, 2007. Amer. Math. Soc.

[5] J. Wolf. The minimal number of monochromatic 4-term progressions. *J. Comb*, 1 :53–68, 2010.