Introduction à la combinatoire additive

Pascal Millet, Corentin Henriet, Antoine Soulas
Sous la direction d'Ariane Mézard

12 septembre 2017

Table des matières

1 Introduction

1.1 Notations

La combinatoire additive est une branche de la théorie des nombres qui vise à étudier les propriétés arithmétiques des entiers vis-à-vis de l'addition. Plus généralement, elle s'intéresse en particulier au comportement des sous-ensembles finis d'un groupe abélien lorsque l'on effectue l'addition, la soustraction et éventuellement le produit des éléments de ces ensembles. Il s'agit néanmoins d'un domaine vaste, et nous évoquons dans ce mémoire des aspects très divers de la discipline : certaines sections n'ont donc pas de lien direct entre elles, puisqu'elles abordent parfois des questions très variées. Nous présenterons les premiers résultats généraux, avant de démontrer les théorèmes de Plünnecke, d'Eleke, de Roth et enfin de Balog-Szemerédi en donnant leurs améliorations possibles, leurs conséquences et leurs applications à divers problèmes, notamment la conjecture de Kakeya.

Dans tout ce qui va suivre, Z désigne toujours un groupe abélien muni d'une loi notée $+$, et A et B des sous-ensembles finis de Z. On note de plus $|E|$ le cardinal d'un ensemble fini E. On définit les opérations suivantes :

$$A + B = \{a + b \,|(a, b) \in A \times B\}$$

$$A - B = \{a - b \,|(a, b) \in A \times B\}$$

$$A \cdot B = \{ab \,|(a, b) \in A \times B\}$$

Notre but est d'étudier le comportement de quantités telles que $|A+B|$ ou $|A-B|$ selon les informations dont on dispose pour des ensembles finis non vides A et B. Par exemple, le théorème de Plünnecke indique que si le fait d'additionner B à A augmente peu la taille de A, i.e. si $|A+B|$ est comparable à $|A|$, alors il est possible de trouver un sous-ensemble $A' \subset A$ tel que $|A'+B+B|$ est comparable à $|A'|$. Le théorème de Balog-Szemerédi, quant à lui, s'intéresse aux ensembles A et B de cardinalité proche et tels qu'il existe une "grande

partie" (dans un sens qu'il nous faudra définir) $G \subset A \times B$ pour laquelle l'ensemble des différences $\{a-b\,|(a,b) \in G\}$ est petit. Dans ce cas, le théorème nous assure que G peut en fait être remplacé par un produit cartésien, puisqu'il existe A' et B' de "grandes parties" de A et B respectivement telles que $A' - B'$ est petit. En ce qui concerne le théorème d'Eleke, il montre qu'on ne peut avoir à la fois $|A+A|$ et $|A \cdot A|$ proches de $|A|$, en donnant une borne inférieure pour la quantité $\max(|A + A|, |A \cdot A|)$. Enfin, le théorème de Roth étudie le cas particulier des entiers et affirme que, étant donnée une densité $\delta \in [0, 1]$, tout sous-ensemble de $\{1, \ldots, n\}$ de densité δ admet une progression arithmétique de longueur 3 (c'est-à-dire une suite finie $(a_i)_{1 \leq i \leq 3}$ où $a_{i+1} - a_i = r$ pour une constante r appelée *raison*), pourvu que n soit suffisamment grand. Les problèmes auxquels ces théorèmes s'appliquent sont multiples ; par exemple, ils permettent des avancées à propos d'une conjecture d'Erdös et Turan qui affirme que toute partie des entiers naturels $A \subset \mathbb{N}$ telle que $\sum_{n \in A} 1/n = +\infty$ possède une infinité de progressions arithmétiques, de longueur arbitrairement grande. Nous étudierons aussi la conjecture de Kakeya mentionnée plus haut, qui stipule que tout ensemble de points $E \subset \mathbb{F}^n$, où $\mathbb{F}$ est un corps fini, qui contient au moins une droite dans chaque direction possible a en fait un cardinal très proche de celui de $\mathbb{F}^n$. Les définitions rigoureuses et les énoncés précis de ces résultats seront donnés plus loin.

1.2 Premiers résultats

Commençons par donner un premier encadrement de $|A + B|$ pour A et B des sous-ensembles finis de Z : si A et B sont quelconques, une majoration évidente est $|A+B| \leq |A||B|$. De plus, lorsque l'on travaille sur les entiers, on dispose de la minoration simple suivante :

Lemme 1.2.1. *Si A et B sont des sous-ensembles finis non vides de $\mathbb{Z}$, alors $|A + B| \geq |A| + |B| - 1$.*

Démonstration. Par translation, on se ramène au cas où $\max A = \min B = 0$ sans affecter les cardinalités. Comme $0 \in A$ et $0 \in B$ alors $A \cup B \subset A + B$. Mais A est composé d'entiers négatifs et B d'entiers positifs : seul 0 est dans $A \cap B$ et donc $|A+B| \geq |A \cup B| = |A| + |B| - 1$. □

Remarque 1.2.2. On a en fait égalité dans le Lemme 1.2.1. seulement lorsque A et B sont des progressions arithmétiques.

Lorsque Z n'est pas le groupe des entiers relatifs $\mathbb{Z}$, ni un de ses sous-groupes, on peut remarquer que tout groupe sans torsion est d'une certaine manière équivalent à $\mathbb{Z}$, au sens de la proposition 1.2.4. Pour cela, il convient d'introduire la notion d'isomorphisme de Freiman, qui est une version affaiblie de l'isomorphisme de groupe classique. En effet, un isomorphisme de Freiman d'ordre k se comporte exactement comme un isomorphisme de groupe tant que l'on ne considère jamais plus de k additions successives :

Définition 1.2.3. *Soient Z et Z' deux groupes abéliens et $A \subset Z$ et $B \subset Z'$ des sous-ensembles finis de ces groupes. Pour $k \geq 2$, on appelle isomorphisme de Freiman d'ordre*

k toute bijection $\varphi : A \to B$ telle que $\forall (x_1, \dots, x_k, y_1, \dots, y_k) \in A^{2k}$,

$$\varphi(x_1) + \cdots + \varphi(x_k) = \varphi(y_1) + \cdots + \varphi(y_k) \Leftrightarrow x_1 + \cdots + x_k = y_1 + \cdots + y_k$$

Il est à présent possible de décrire le plongement annoncé de tout $A \subset Z$ dans $\mathbb{Z}$:

Proposition 1.2.4. *Soit A un sous-ensemble fini d'un groupe abélien sans torsion Z. Alors pour tout $k \geq 2$, il existe un isomorphisme de Freiman $\varphi : A \to \varphi(A)$ d'ordre k où $\varphi(A)$ est un sous-ensemble fini de $\mathbb{Z}$.*

Pour démontrer cette proposition, nous avons besoin d'un résultat préliminaire qui permet d'étendre Z à un espace vectoriel sur $\mathbb{Q}$, ce qui va servir à se ramener au cas plus simple où $Z = \mathbb{Z}^n$:

Lemme 1.2.5. *Soit Z un groupe abélien sans torsion. Notons $Z \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ le produit tensoriel sur $\mathbb{Z}$ de Z par l'ensemble des rationnels $\mathbb{Q}$. L'application*

$$\begin{array}{rccc} \mu : & Z & \longrightarrow & Z \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \\ & x & \longmapsto & x \otimes 1 \end{array}$$

est un morphisme de groupes injectif.

Démonstration. Définissons sur $Z \times \mathbb{N}^*$ la relation d'équivalence suivante : $(x, n) \sim (y, m) \Leftrightarrow mx = ny$. Alors $\sim$ est bien réflexive et symétrique, et la transitivité provient du caractère sans torsion de Z. En effet, si $(x, n) \sim (y, m) \sim (z, p)$, alors $mpx = pny = mnz$ donc $m(px - nz) = 0$ d'où $px = nz$ puisque Z est sans torsion et $m \neq 0$.
Soit $G = (Z \times \mathbb{N}^*)/\sim$, on note $[x, n]$ la classe dans G de (x, n). L'ensemble G peut être muni d'une structure de groupe abélien par la loi associative $[x, n] + [y, m] = [mx + ny, nm]$. Cette opération est bien définie car si $[x', n'] = [x, n]$ i.e. si $nx' = n'x$, on a $[mx + ny, nm] = [mx' + n'y, n'm]$ étant donné que $nm(mx' + n'y) = n'm(mx + ny)$. En outre, si 0_Z est l'élément neutre de Z, celui de G est $[0_Z, 1]$ et on a $-[x, n] = [-x, n]$. Remarquons enfin que pour tout $m \in \mathbb{N}^*$, $m[x, n] = [x, n] + \cdots + [x, n] = [mn^{m-1}x, n^m] = [mx, n]$.

L'application ν suivante définit un morphisme de groupes :

$$\begin{array}{rccc} \nu : & Z & \longrightarrow & G \\ & x & \longmapsto & [x, 1] \end{array}$$

et ν est injective puisque $[x, 1] = [y, 1]$ implique $(x, 1) \sim (y, 1)$ soit $x = y$.
De plus l'application $\mathbb{Z}$-bilinéaire

$$\begin{array}{ccc} Z \times \mathbb{Q} & \longrightarrow & G \\ (x, \frac{n}{m}) & \longmapsto & [nx, m] \end{array}$$

induit par propriété universelle du produit tensoriel une application $\mathbb{Z}$-linéaire

$$\lambda : Z \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \longrightarrow G$$

Alors en reprenant les notations de l'énoncé, $\nu = \lambda \circ \mu$ donc μ est nécessairement injective puisque ν l'est. □

Nous pouvons à présent démontrer la proposition 1.2.4. :

Démonstration. Comme Z est sans torsion, en utilisant le lemme 1.2.5, Z peut être étendu en un $\mathbb{Q}$-espace vectoriel en remplaçant Z par $Z \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ *via* l'injection μ. L'ensemble A étant fini, $vect_{\mathbb{Q}}(\mu(A))$ est un $\mathbb{Q}$-espace vectoriel de dimension finie, autrement dit de la forme $\mathbb{Q}^n$ pour un certain $n \in \mathbb{N}$. Comme A est fini, $\mu(A)$ est contenu dans un réseau isomorphe à $\mathbb{Z}^n$, et ainsi nous pouvons supposer que $Z = \mathbb{Z}^n$ pour un certain $n \in \mathbb{N}$ quitte à se restreindre à un sous-groupe de Z contenant A. On peut alors poser $\varphi(a_1, ..., a_n) = a_1 + a_2 M + a_3 M^2 + \cdots + a_n M^{n-1}$ pour un entier naturel M, ce qui revient à voir les éléments de Z comme des décompositions d'entiers en base M. L'application $\varphi : A \to \varphi(A)$ est alors bien bijective dès que $M > \max\limits_{(a_1,...,a_n)\in A} a_i$ par unicité de la décomposition, et est même un isomorphisme de Freiman d'ordre k quitte à remplacer M par kM. □

Un concept important en combinatoire additive est la notion d'ensemble *invariant* par un autre ensemble ou *essentiellement invariant*. Pour définir cela, introduisons quelques notations commodes que nous utiliserons parfois dans la suite : lorsque A et B deux sous-ensembles finis de Z, on note $|A| \lesssim |B|$ pour signifier qu'il existe une constante $\Gamma > 0$ telle que $|A| \leq \Gamma |B|$ et que toutes les utilisations suivantes du symbole $\lesssim$ sous-entendent l'existence d'autres constantes qui peuvent s'exprimer en fonction de Γ uniquement, mais que nous n'explicitons volontairement pas pour des raisons de clarté. On trouvera également la notation $|A| \sim |B|$ si $|A| \lesssim |B|$ et $|B| \lesssim |A|$. Cependant, les théorèmes majeurs seront énoncés et démontrés sans employer ces notations allégées, mais floues.

Définition 1.2.6. *L'ensemble A est dit B-invariant si $|A + B| = |A|$. Plus généralement, A est dit essentiellement B-invariant si $|A + B| \sim |A|$. Nous dirons que A est (essentiellement) invariant si A est (essentiellement) A-invariant.*

Il se trouve que les ensembles invariants sont très bien connus, grâce au résultat suivant :

Proposition 1.2.7. *L'ensemble A est B-invariant si et seulement si A est une union de classes d'équivalence de Z/G où G est un sous groupe fini de Z tel que B soit contenu dans un translaté de G.*

Corollaire 1.2.8. *On a $|A + A| = |A|$ si et seulement si A est le translaté d'un sous-groupe G de Z.*

Démonstration. Le sens réciproque de la proposition est clair. Pour l'implication directe, on peut supposer, quitte à translater sans affecter les cardinalités, que B contient l'élément neutre de Z. Remarquons premièrement que $|A + B| = |A|$ implique $|A + B + \cdots + B| = |A|$. En effet, pour tout $(b, b') \in B^2$, on a nécessairement $A + b = A + b'$ sinon $A + B$ contiendrait plus d'éléments que A. Par conséquent, $A + B + b = A + B + b'$ qui donne ainsi $|A + B + B| = |A + B + b| = |A + B|$ puis de proche en proche, on obtient l'égalité.

On pose alors $G = \langle B \rangle$ et on considère la plus petite réunion F de classes d'équivalence de Z/G qui recouvre A. Soit $x \in F$, il existe donc $y \in A$ tel que x et y appartiennent à la même classe d'équivalence. Autrement dit $x - y \in G$ i.e. $x - y = b_1 + \cdots + b_n$ où les b_i sont dans B, puisque par définition G est une somme d'un nombre fini de B. Par conséquent, $x \in A + B + \cdots + B$ d'où $|F| \leq |A + B + \cdots + B| = |A|$. Finalement, $A = F$ d'où le résultat.
Le corollaire est obtenu en posant $A = B$ dans la proposition. □

Exemple. *Soit $n \in \mathbb{N}$. Dans le groupe $Z = (\mathbb{Z}/n\mathbb{Z})^2$, si on pose $B = \{(1,1);(2,1);(3,1)\}$ alors B est contenu dans $(0,1) + G$ où G est le sous-groupe $\{(k,0)|k \in \mathbb{Z}/n\mathbb{Z}\}$. Ainsi les sous-ensembles de Z B-invariants sont exactement ceux de la forme $A_I = \{(k,i)|k \in \mathbb{Z}/n\mathbb{Z}, i \in I\}$ pour toute partie I de $\mathbb{Z}/n\mathbb{Z}$.*

Le cas des ensembles invariants est donc bien maîtrisé : si par exemple A et A' sont B-invariants, alors A, A' et $A + A'$ sont des unions de classes d'équivalence de Z/G pour un sous-groupe G de Z commun à A, A' et $A + A'$. On dispose alors d'une majoration plus efficace que le Lemme 1.2.1., puisqu'en passant au quotient on a $|(A + A')/G| \leq |A/G||A'/G|$ soit en remaniant les termes :

$$|A + A'| \leq \frac{|A||A'|}{|G|} \leq \frac{|A||A'|}{|B|}$$

Pour tenter d'étendre ce résultat aux ensembles essentiellement B-invariants, démontrons le lemme suivant :

Lemme 1.2.9 (Ruzsa)**.** *Soient A, B et C trois sous-ensembles finis non vides de Z. Alors $|B - C| \leq \frac{|A+B||A+C|}{|A|}$.*

Démonstration. On pose la surjection évidente $\pi : B \times C \to B - C$, et soit $f : B - C \to B \times C$ une section de π. On définit aussi la diagonale $A^\Delta = \{(a,a)|a \in A\}$. Alors pour tout $x \in B - C$, $f(x) + A^\Delta \subset (A + B) \times (A + C)$ et comme $\pi(A^\Delta) = \{0\}$, $f(x) + A^\Delta$ est un ensemble de $|A|$ antécédents de x par π . Par conséquent, chaque élément de $B - C$ a au moins $|A|$ antécédents distincts, pris dans un ensemble de cardinal $|A + B||A + C|$, d'où l'inégalité. □

Une conséquence directe de ce lemme est le fait que si A et A' sont tous deux des ensembles essentiellement B-invariants, on peut généraliser l'inégalité obtenue précédemment :

$$|A - A'| \leq \frac{|A + B||A' + B|}{|B|} \lesssim \frac{|A||A'|}{|B|}$$

De même si A est simultanément B- et B'-invariant, alors on obtient des informations sur $B - B'$:

$$|B - B'| \leq \frac{|A + B||A' + B|}{|A|} \lesssim |A|$$

2 Théorème de Plünnecke

Le théorème précédent permet donc de dire que si A est essentiellemennt invariant, alors il est essentiellement $(-A)$-invariant. Cela est à rapprocher de la stabilité d'un sous-groupe par opposé. En fait, le caractère essentiellement invariant est une généralisation combinatoire de la notion de sous-groupe. Nous pouvons donc nous attendre à ce qu'un ensemble A essentiellement invariant soit essentiellemnent $(nA-mA)$-invariant pour tout $(m,n) \in \mathbb{N}$ ce qui traduirait une certaine stabilité par $+$ et $-$. Nous allons voir dans ce qui suit que cela est une conséquence du théorème de Plünnecke énoncé ci-dessous.

Théorème 2.0.10. *Soit A et B deux sous ensembles finis non vides d'un groupe Z. Supposons qu'il existe une constante $K > 0$ telle que $|A+B| \leq K|A|$. Alors, il existe $A' \subset A$ non vide tel que $|A'+B+B| \leq K^2|A'|$.*

2.1 Eléments de théorie des graphes

Pour démontrer ce théorème, nous utilisons des éléments de théorie des graphes. Introduisons d'abord deux définitions pour faire le lien entre le théorème de Plünnecke et la théorie des graphes.

Définition 2.1.1. *Considérons un graphe orienté G construit de la façon suivante : Comme ensemble de sommets, nous prenons trois sous-ensembles d'un groupe abélien Z (non nécessairement disjoints) V_0, V_1 et V_2 et pour les arêtes, nous prenons des éléments de $V_0 \times V_1 \cup V_1 \times V_2$. Notons $a \mapsto_G b$ pour "(a,b) est une arête du graphe ". Nous disons qu'un tel graphe est commutatif si $a \mapsto_G a+c$ et $a+c \mapsto_G a+c+d$ impliquent $a \mapsto_G a+d$ et $a+d \mapsto_G a+d+c$. De plus notons pour une partie A' de V_0, $G^2(A')$ (resp $G^1(A')$) pour désigner l'ensemble des sommets de V_2 (resp V_1) qui sont reliés à un sommet de A' par une suite de deux (resp une) arêtes du graphe.*

Un exemple de tel graphe est donné par la définition suivante :

Définition 2.1.2. *Pour A et B deux sous-ensembles d'un groupe abélien Z, notons $G[A,B]$ le graphe commutatif défini avec $V_0 = A$, $V_1 = A+B$, $V_2 = A+B+B$, et dont les arrêtes sont données par $x \mapsto_G x+b$ ssi $b \in B$.*

Remarque 2.1.3. Un tel graphe est commutatif car pour $a \in A$, $a \mapsto_G b$ et $a+b \mapsto_G a+b+b'$ est équivalent à $b \in B$ et $b' \in B$ et donc nous avons bien par définition des arêtes $a \mapsto_G a+b'$ et $a+b' \mapsto_G a+b'+b$.

Nous démontrons le théorème de Plünnecke en remarquant qu'il s'agit d'un corollaire de la propriété plus forte suivante :

Proposition 2.1.4. *Soit G un graphe commutatif vérifiant $|V_1| < K|V_0|$ pour une certaine constante K strictement positive. Alors il existe $A' \subset V_0$ telle que $\left|G^2(A')\right| < K^2|A'|$.*

Le plan sera le suivant : Dans un premier temps, l'énoncé d'un théorème général sur les graphes orientés : le théorème de Menger que nous ne démontrerons pas car la preuve est technique, indépendante du reste de la démonstration et sans réel lien avec la combinatoire additive. Puis nous nous en servirons pour montrer la proposition **??** dans le cas particulier $K = 1$. Enfin, en introduisant la notion de produit cartésien de graphes, nous pourrons généraliser à $K > 0$ quelconque.

2.2 Théorème de Menger

Pour énoncer le théorème de Menger, nous avons besoin de la définition suivante.

Définition 2.2.1. *On appelle séparateur de A et B un ensemble de sommet S qui déconnecte A et B c'est à dire tel que tout chemin reliant un sommet de A à un sommet de B passe par S.*

Théorème 2.2.2. *Soit G un graphe orienté et A et B deux sous-ensembles de sommets, notons $MINCUT(G)$ le cardinal minimal d'un séparateur de A et B. Notons $MAXFLOW(G)$ le cardinal d'une famille maximale de chemins disjoints (au sens des sommets) reliant un sommet de A et un sommet de B. Avec ces notations, nous avons $MICUT(G) = MAXFLOW(G)$.*

Remarque 2.2.3. Il existe des démonstrations purement combinatoires du théorème de Plünnecke qui ne nécessitent pas le théorème de Menger. Pour une preuve du théorème de Menger, voir la section 6 de *Combinatorial Problems and Exercices* (de L.Lovasz)

Ce théorème fait le lien entre la notion de séparateur et la notion de chemin. En particulier, il est crucial dans la suite car les chemins obtenus vont permettre d'établir des injections entre différents ensembles d'arêtes et ainsi d'obtenir des informations de cardinalité.

2.3 Preuve de la proposition ?? dans le cas $K = 1$

Le cas particulier $K = 1$ est fondamental car nous construisons explicitement le sous-ensemble $A' \subset V_0$ tel que $|G^2(A')| < |A'|$. Nous nous ramènerons ensuite à ce cas pour démontrer la proposition **??**. Dans un premier temps nous introduisons les notations ainsi que deux lemmes.

Soit G un graphe commutatif. Tout d'abord remarquons que l'on peut supposer sans perte de généralité que les ensembles de sommets V_0, V_1 et V_2 sont deux à deux disjoints en considérant le graphe commutatif G' associé à G où l'on a pris $V_0' = V_0 \times \{0\}$, $V_1' = V_1 \times \{1\}$ et $V_2' = V_2 \times \{2\}$.

Nous avons ensuite la propriété suivante : Soit $a \in V_0$, $i \in \{1, 2\}$ et $b \in V_i$, il existe un chemin (non vide) reliant a et b dans G si et seulement si il existe un chemin reliant $a \times \{0\}$ et $b \times \{i\}$ dans G'. Cela donne immédiatement l'équivalence entre la proposition **??** appliquée à G et celle appliquée à G'. Supposons donc désormais que V_0, V_1 et V_2 sont disjoints. Supposons également que $|V_1| < |V_0|$ (nous nous plaçons dans le cas $K = 1$).

Notons S de cardinal minimal s un ensemble de sommets qui sépare V_0 et V_2. Comme V_1 sépare V_0 et V_2, nous avons $s \leq |V_1| < |V_0|$. Ecrivons $S = S_0 \cup S_1 \cup S_2$ où $S_0 = S \cap V_0$, $S_1 = S \cap V_1$ et $S_2 = S \cap V_2$. Il est clair d'après la définition que si l'on retire des sommets de V_0 et V_2 à un graphe commutatif, il reste commutatif. Nous pouvons donc considérer G' le graphe obtenu en retirant les sommets de S_0 et de S_2.

Lemme 2.3.1. *S_1 est un séparateur minimal de $V_0 \backslash S_0$ et $V_2 \backslash S_2$ dans G'.*

Démonstration. S_1 est bien un séparateur car S est séparateur de V_0 et V_2 dans G et il est bien minimal car si S' était un séparateur d'ordre strictement inférieur, nous pourrions en prenant $S_0 \cup S' \cup S_2$ trouver un séparateur de V_0 et V_2 dans G d'ordre strictement plus petit que s ce qui est absurde. □

Donc, par définition d'un séparateur, tout chemin reliant $V_0 \backslash S_0$ et $V_2 \backslash S_2$ passe par S_1. De cette remarque, nous obtenons le fait que le graphe G'' où l'on a pris $V_0'' = V_0 \backslash S_0$, $V_1'' = S_1$ et $V_2'' = V_2 \backslash S_2$ est toujours commutatif.

Utilisons maintenant le théorème de Menger qui donne l'existence de $|S_1|$ chemins disjoints reliant V_0'' et V_1''. En particulier, ils passent chacun par un sommet de S_1 différent et nous pouvons donc écrire les chemins sous la forme $d_s \to s \to a_s$. Nous notons $W_0 = \{d_s, s \in S_1\}$ l'ensemble des points de départ de ces chemins et $W_2 = \{a_s, s \in S_1\}$ l'ensemble des points d'arrivée.

Lemme 2.3.2. *Dans le graphe G'' arêtes issues de S_0'' sont exactement les arêtes issues de W_0 et les arêtes arrivant dans V_2'' sont exactement les arêtes arrivant dans W_2.*

Démonstration. Nous considérons l'injection suivante :

$$\begin{cases} \{\text{arêtes issues de } S_1\} \to \{\text{arêtes issues de } W_0\} \\ (s \to s+b) \mapsto (d_s \to d_s + b) \end{cases}$$

Cette application est bien définie car le graphe est commutatif ! Et elle est injective car une arête $d_s \to d_s + b$ a au plus un antécédent $s \to s + b$ (si cette arête est bien une arête de G''). De même, définissons l'injection suivante :

$$\begin{cases} \{\text{arêtes arrivant en } S_1\} \to \{\text{arêtes arrivant en } W_2\} \\ (x \to s) \mapsto (d_s - (s - x) \to d_s) \end{cases}$$

Toujours bien définie par commutativité du graphe et clairement injective. Comme nous avons les égalités (dans le graphe G'') {arêtes issues de V_0''}={arêtes arrivant dans S_1} et {arêtes issues de S_1}={arêtes arrivant dans V_2''}, la première injection donne :

$$\text{Card}\{\text{issues de } S_1\} \leq \text{Card}\{\text{issues de } W_0\} \leq \text{Card}\{\text{issues de } V_0''\} = \text{Card}\{\text{arrivant dans } S_1\} \tag{1}$$

La deuxième injection donne :

$$\text{Card}\{\text{arrivant dans } S_1\} \leq \text{Card}\{\text{arrivant dans } W_2\} \leq \text{Card}\{\text{arrivant dans } V_2''\} = \text{Card}\{\text{issues de } S_1\} \tag{2}$$

Finalement, en rassemblant les deux inégalités, nous obtenons que les arêtes issues de S_0'' sont les arêtes issues de W_0 et les arêtes arrivant dans V_2'' sont les arêtes arrivant dans W_2. □

Nous avons maintenant tout ce qu'il faut pour démontrer le cas $K = 1$

Proposition 2.3.3. *Soit G un graphe commutatif vérifiant $|V_1| < |V_0|$. Alors il existe $A' \subset V_0$ tel que $|G^2(A')| < |A'|$.*

Démonstration. Nous déduisons du lemme précédent que W_0 est aussi un ensemble déconnectant V_0'' et V_2''. Et en remontant les constructions, $S_0 \cup W_0 \cup S_2$ déconnecte V_0 et V_2 dans G. Donc $G^2(V_0 \backslash (S_0 \cup W_0)) \subset S_2$. Or nous avons dit que $s = |S_0| + |W_0| + |S_2| < |V_0|$ d'où, $|S_2| < |V_0 - (S_0 \cup W_0)|$, ce qu'il fallait démontrer. □

2.4 Produit de graphes et généralisation

Pour montrer la proposition **??** dans le cas général, nous allons nous ramener au cas $K = 1$ en utilisant une astuce qui repose sur le produit cartésien de graphes.

Définition 2.4.1. *Soit G et G' deux graphes commutatifs, notons $G \times G'$ le graphe dont les sommets sont $V_0 \times V_0'$, $V_1 \times V_1'$ et $V_2 \times V_2'$ et vérifiant la propriété $(a, b) \mapsto_{G \times G'} (c, d)$ si et seulement si $a \mapsto_G c$ et $b \mapsto_{G'} d$.*

Par exemple, avec cette définition, nous avons $G[A, B] \times G[C, D] = G[A \times C, B \times D]$. Une première propriété très simple du produit cartésien de graphes commutatifs dont la preuve découle directement de la définition est la suivante :

Proposition 2.4.2. *Soit G et G' deux graphes commutatifs, $A \subset V_0$ et $A' \subset V_0'$. $G \times G'(A \times A') = G(A) \times G'(A')$ et $(G \times G')^2(A \times A') = G^2(A') \times G'^2(A')$*

Pour donner une intuition, nous dirons qu'un graphe commutatif s'étend beaucoup si quel que soit le nombre de sommets que l'on choisit dans l'ensemble V_0, ceux-ci sont reliés à un nombre bien plus grand de sommets dans V_2. Nous allons maintenant introduire une définition qui permet de caractériser la tendance d'un graphe commutatif à s'étendre.

Définition 2.4.3 (rapport de grossissement (magnification ratio))**.** *On définit pour un graphe commutatif G la quantité suivante : $D(G) = \min_{A' \subset V_0, A' \neq \emptyset} \frac{|G^2(A')|}{|A'|}$*

Proposition 2.4.4. *Pour G et G' deux graphes commutatifs, on a l'égalité suivante : $D(G \times G') = D(G)D(G')$*

Démonstration. Par la proposition **??**, on a déjà $D(G \times G') \leq D(G)D(G')$ en prenant des parties $A \subset V_0$ et $A' \subset V_0'$ qui réalisent le minimum dans la définition du magnification ratio.

Pour montrer l'inégalité inverse, prenons Ω dans $V_0 \times V_0'$ et posons $\Omega' = \{(y, x') : \exists (x, x') \in \Omega, y \in G^2(\{x\})\} = (G \times I_{V_0'})^2(\Omega)$ où on a noté $I_{V_0'} = G[V_0', \{0\}]$. Le graphe $G \times I_{V_0'}$ est donc simplement un graphe comportant $|V_0'|$ copies du graphe G. On a ainsi,

$D(G) = D(G \times I_{V_0})$. Donc le cardinal de Ω' est supérieur à $D(G)\,|\Omega|$ par définition de $D(G \times I_{V_0})$.

Il suffit alors de remarquer que par définition $(y, y') \in (G \times G')^2(\Omega)$ si et seulement si il existe $(x, x') \in \Omega$ tels que $(y, y') \in G^2(\{x\}) \times G^2(\{x'\})$. Donc $(G \times G')^2(\Omega) = \{(y, y') : \exists (y, x') \in \Omega', y' \in G'^2(x')\} = G' \times I_{V_2}$. Ainsi pour la même raison que précédemment$\left|(G \times G')^2(\Omega)\right| \geq D(G')\,|\Omega'| \geq D(G')D(G)\,|\Omega|$. Ainsi, on a donc $D(G \times G') \geq D(G)D(G')$ et la proposition est démontrée. □

Cette proposition fait le lien entre le rapport de grossissement d'un produit cartésien et celui des facteurs. En posant un produit cartésien bien choisi, nous allons donc obtenir des informations sur $D(G)$. Cela est intéressant car montrer la proposition **??** revient à majorer $D(G)$.

2.5 Généralisation de la proposition à K quelconque

Nous cherchons à nous ramener aux conditions d'application de la proposition **??** pour $K = 1$ à l'aide d'un produit cartésien bien choisi. En utilisant la relation entre les taux de grossissement, nous serons en mesure de majorer le taux de grossissement de G L'idée va donc être de diminuer le rapport $\frac{\|V_1\|}{\|V_0\|}$ de G en prenant le produit cartésien avec un certain graphe X_k^* qui a un tel rapport suffisament petit pour que celui du graphe produit soit inférieur à 1.

Pour X_k, prenons $A = \{0\} \subset Z^k$ et B la base canonique de Z^k et posons $X_k = G[A, B]$ qui vérifie clairement $D(X_k) = \frac{k(k-1)}{2}$. En prenant le graphe réfléchi X_k^* (le graphe obtenu en inversant le sens de toutes les arêtes), nous obtenons $D(X_k^*) = \frac{2}{k(k-1)}$.

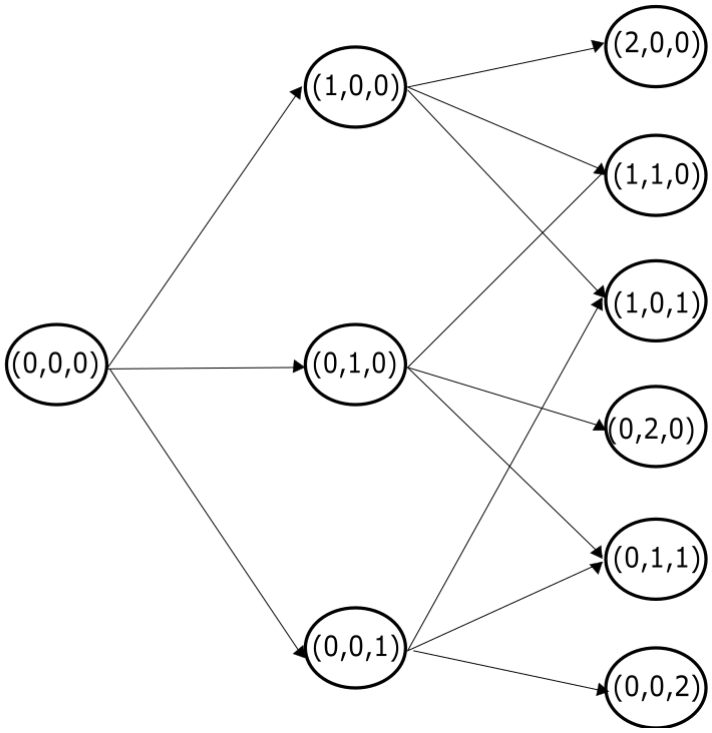

FIGURE 1 – Graphe commutatif X_3

Soit G un graphe commutatif vérifiant $V_1 < KV_0$ pour un certain $K > 0$. Prenons k entier entre $2K+1$ et $2K+2$. Posons $G' = G \times X_k^*$. Ainsi G' vérifie $V_1' < V_0'$ par définition de K. Nous pouvons donc utiliser la proposition **??** dans le cas $K = 1$. Cela donne $D(G') < 1$ et donc $D(G) < \frac{1}{D(X_k^*)} \leq 10K^2$.

Pour affiner encore le résultat, remarquons que pour un entier M, $\underbrace{G \times G \times ... \times G}_{\text{M fois}}$ est un graphe commutatif et on a $\left|(V_1)^M\right| < K^M \left|(V_0)^M\right|$ d'où par le résultat précédent, $D(G)^M = D(\underbrace{G \times G \times ... \times G}_{\text{M fois}}) < 10K^{2M}$. Ce qui donne en faisant tendre M vers l'infini : $D(G) \leq K^2$ ce qui achève la preuve du théorème de la proposition **??**. Nous avons vu que cette proposition admet le corollaire suivant (théorème de Plünnecke) :

Corollaire 2.5.1. *Soit A et B deux sous-ensembles finis non vides d'un groupe Z. Supposons qu'il existe une constante $K > 0$ telle que $|A+B| \leq K|A|$. Alors, il existe $A' \subset A$ non vide tel que $|A'+B+B| \leq K^2|A'|$.*

2.6 Analyse de l'optimalité du théorème

Nous montrons ici que l'on ne peut pas remplacer le sous-ensemble $A' \subset A$ par A tout entier dans le théorème de Plünnecke. En effet, pour une certaine constante $K > 1$,

on peut trouver A et B tels que $\frac{|A+B|}{|A|} \leq K$ mais $\frac{|A+B+B|}{|A|}$ aussi grand qu'on veut comme nous allons le voir dans la proposition suivante.

Proposition 2.6.1. *Il existe $K > 1$ telle que pour tout $M > 0$, il existe $A, B \subset \mathbb{Z}^2$ tels que $|A + B| \leq K|A|$ mais $|A + B + B| \geq M|A|$*

Remarque 2.6.2. Remarquons qu'on peut également trouver de tels ensembles dans $\mathbb{Z}$ en utilisant un isomorphisme de Freimann d'ordre 2.

Démonstration. Pour cette preuve, on va construire explicitement des ensembles A_n et B_n vérifiant :

$$\forall n \in \mathbb{N}, \begin{cases} |A_n + B_n| = O(|A_n|) \\ |A_n|^{\frac{3}{2}} = O(|A_n + B_n + B_n|) \end{cases}$$

et

$$|A_n| \underset{n\to+\infty}{\to} +\infty$$

Ce qui suffit à conclure en faisant tendre n vers $+\infty$.

Pour $n \in \mathbb{N}$, on pose $A_n = [\![0, n-1]\!]^2 \cup \{(kn, 0), k \in [\![1, n]\!]\}$. Pour B_n, il faut choisir un ensemble tel que $|B_n + B_n| >> |B_n|$. Pour cela, nous posons $|B_n| = [\![0, n-1]\!] \times \{0\} \cup \{0\} \times [\![0, n-1]\!]$. Les ensembles sont représentés pour le cas $n = 6$ sur les figures **??** et **??**. Avec ces notations, nous avons

$$n^2 \leq |A_n| \leq 2n^2$$

De plus :

$$\begin{aligned} A_n + B_n =& [\![0, n-1]\!] \times [\![0, 2n-2]\!] \cup [\![n, 2n-2]\!] \times [\![0, n-1]\!] \\ & \cup [\![0, n^2+n-1]\!] \times \{0\} \cup \bigcup_{k=1}^{n} \{kn\} \times [\![0, n-1]\!] \end{aligned}$$

ce qui donne $|A_n + B_n| \leq 5n^2 \leq 5|A_n|$. Enfin :

$$\begin{aligned} A_n + B_n + B_n =& [\![0, n-1]\!] \times [\![0, 3n-3]\!] \cup [\![n, 2n-2]\!] \times [\![0, 2n-2]\!] \\ & \cup [\![2n-1, n^2+n-1]\!] \times [\![0, n-1]\!] \\ & \cup [\![n^2+n, n^2+2n-2]\!] \times \{0\} \cup \bigcup_{k=1}^{n} \{kn\} \times [\![n, 2n-2]\!] \end{aligned}$$

Ce qui donne $|A_n + B_n + B_n| \geq n^3 \geq \frac{1}{8}|A_n|^{\frac{3}{2}}$. Nous avons donc construit les ensembles A_n et B_n mentionnés au début de la démonstration. □

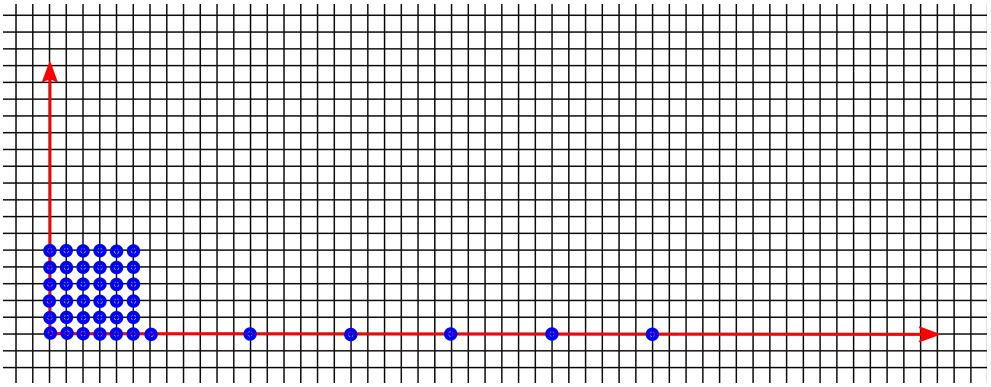

FIGURE 2 – Ensemble A_n dans le cas $n = 6$

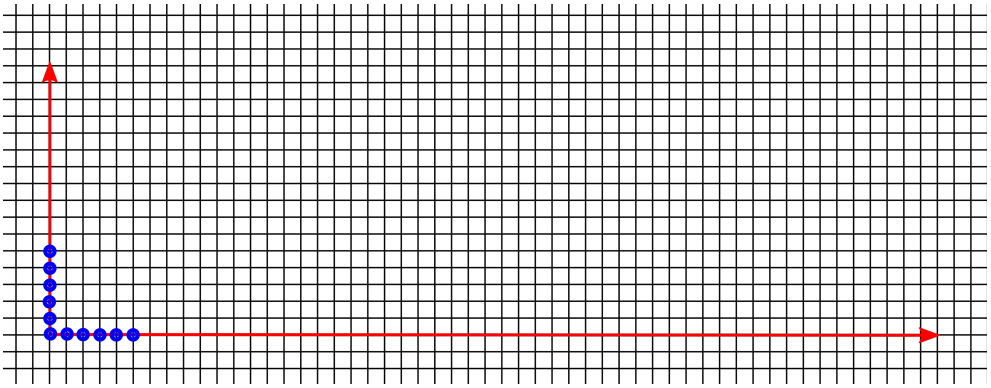

FIGURE 3 – Ensemble B_n dans le cas $n = 6$

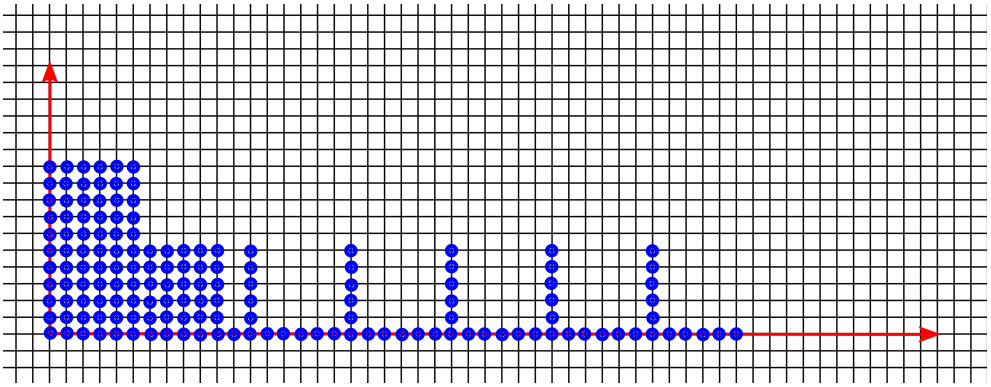

FIGURE 4 – Ensemble $A_n + B_n$ dans le cas $n = 6$

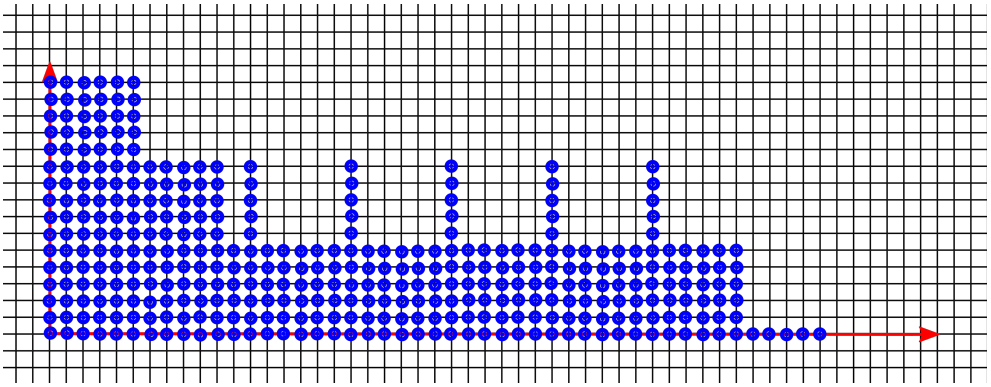

FIGURE 5 – Ensemble $A_n + B_n + B_n$ dans le cas $n = 6$

2.7 Estimation de $|nA - mA|$ (sumset estimate)

Nous allons maintenant utiliser le théorème de Plünnecke pour évaluer $|nA - mA|$. Remarquons d'abord que nous pouvons itérer le théorème :

Théorème 2.7.1. *Soit A, B deux sous-ensembles finis de Z abélien. Supposons qu'il existe $K \geq 1$ tel que $|A+B| \leq K|A|$. Alors pour tout $n \in \mathbb{N}^*$, il existe $A_n \subset A$ non vide tel que $|A_n + nB| \leq K^{C(n)}|A_n|$ pour une certaine constante $C(n)$ qui ne dépend que de n.*

Démonstration. Avec les notations précédentes, soit $n \in \mathbb{N}^*$. Il existe $k \in \mathbb{N}$ tel que $2^k - 1 < n \leq 2^k$. En itérant k fois le théorème de Plünnecke, il existe $A_n \subset A$ non vide tel que $|A_n + 2^k B| \leq 2^k |A_n|$. Soit $b \in B$, nous avons l'inclusion suivante :

$$A_n + (2^k - n)b + nB \subset A_n + 2^k B$$

ce qui donne l'inégalité sur les cardinaux : $|A_n + nB| = |A_n + (2^k - n)b + nB| \leq |A_n + 2^k B| \leq K^{2^k}|A|$ □

Théorème 2.7.2 (sumset estimate)**.** *Soit A et B deux ensembles finis non vides inclus dans un groupe abélien Z. Si $|A+B| \leq K|A|$ pour un certain $K \leq 1$, alors pour tout $m, n \in \mathbb{N}$, il existe une constante $C(n,m) \in \mathbb{N}$ telle que $|nB - mB| \leq K^{C(n,m)}|A|$.*

Démonstration. Notons $\mu = max(m,n)$. De cette façon, nous avons $nB - mB \subset \mu B - \mu B$. En utilisant le théoèreme de Plünnecke itéré, il existe $A_\mu \subset A$ non vide tel que $|A_\mu + \mu B| \leq K^{C(\mu)}|A_\mu|$. Donc, par le lemme de Rusza, l'inégalité suivante est vérifiée :

$$|\mu B - \mu B| \leq \frac{|A_\mu + \mu B|^2}{|A_\mu|} \leq K^{2C(\mu)}|A_\mu| \leq K^{2C(\mu)}|A|$$

Donc en posant $C(n,m) = 2C(\mu)$ et en tenant compte de l'inclusion mentionnée plus haut, on obtient le résultat. □

Nous avons donc bien obtenu une propriété qui précise en quel sens les ensembles essentiellement invariants sont stables par la loi + et par opposé. Cela justifie leur interprétation comme généralisation combinatoire de la notion de sous-groupe.

3 Théorème d'Eleke

Dans les sections précédentes, nous avons étudié $A + B$ où A et B sont des parties finies d'un groupe Z. Dans le cas où Z est un anneau (nous nous intéresserons ici plus particulièrement aux entiers ou aux réels), nous pouvons également étudier le comportement du produit $A \cdot B$. Une question intéressante est d'étudier l'invariance des ensembles par $+$ et $\cdot$ simultanément. En effet, un ensemble A dont la taille est de l'ordre de celle de $A + A$ ressemble à une suite arithmétique. L'analogue pour le produit est une suite géométrique. Intuitivement, les suites arithmétiques et géométriques ne se ressemblent pas, donc on s'attend à ce qu'un ensemble ne puisse pas être à la fois invariant par $+$ et invariant par $\cdot$. Dans le cas réel, c'est ce qu'affirme le théorème d'Eleke :

Théorème 3.0.3. *Soit $A \subset \mathbb{R}$, on a la borne suivante :*

$$max(|A + A|, |A \cdot A|) \geq C|A|^{\frac{5}{4}}$$

où $C > 0$ est une certaine constante.

Pour prouver ce théorème, nous allons passer par une rapide étude combinatoire de la géométrie du plan. En effet, l'étude simultanée de la somme et du produit passe par celle des droites $y = mx + b$ dont l'équation fait apparaitre à la fois l'addition et la multiplication. Nous démontrerons d'abord un résultat sur le nombre de croisements (crossing numbers) dans la représentation d'un graphe. Cela nous permettra de démontrer le théorème de Szemeredi-Trotter relatif au nombre d'incidences entre des droites et des points dans le plan. Finalement, nous déduirons le théorème d'Eleke en appliquant astucieusement ce théorème à une certaine famille de droites et de points.

3.1 Nombre de croisements

Définition 3.1.1. *On considère un graphe $G = (V, E)$ non orienté. On appelle dessin de G, un couple (φ, ψ) d'applications avec $\varphi : V \to \mathbb{R}^2$ et $\psi : E \to C^0(]0, 1[, \mathbb{R}^2)$ vérifiant aussi $\psi(e)$ est un homéomorphisme sur son image et si v_1 et v_2 sont les extrémités de e, alors (quitte à échanger v_1 et v_2) $\lim_{t\to 0} \psi(e)(t) = \varphi(v_1)$ et $\lim_{t\to 1} \psi(e)(t) = \varphi(v_2)$.*

Définition 3.1.2. *On dit qu'un dessin (φ, ψ) est propre si :*

- *φ est injective.*
- *Pour tout $e \in E$, $\psi(e)$ ne passe par aucun point de $\varphi(V)$.*
- *Pour tout $(e, e') \in E^2$ tel que $e \neq e'$, $\psi(e) \cap \psi(e')$ est fini.*
- *Si $e, e' \in E$ partagent une extrémité, alors $\psi(e) \cap \psi(e') = \emptyset$.*

Remarque 3.1.3. Tout graphe fini admet un dessin propre. Il suffit de choisir un nombre fini de points distincts du plan (un pour chaque sommet) et de prendre les segments ouverts entre ces points pour l'image des arêtes.

Définition 3.1.4. *Pour $d = (\varphi, \psi)$ un dessin propre de G, on note $Cr(d) = \sum_{\{e,e'\} \subset E : e \neq e'} |\psi(e) \cap \psi(e')|$. Puisque l'ensemble des dessins propres est non vide d'après la remarque ci-dessus, on peut également définir $Cr(G) = \inf_{d \text{ dessin propre}} Cr(d)$*

Nous cherchons maintenant à minorer le nombre de croisements d'un graphe en fonction du nombre de sommets et d'arêtes. Pour cela rappelons la formule d'Euler.

Proposition 3.1.5. *Soit G un graphe fini connexe tel que $Cr(G) = 0$. Soit $d = (\varphi, \psi)$, un dessin propre de G tel que $Cr(d) = 0$. d divise le plan en f régions ouvertes connexes appelées faces. Si $V' \neq \emptyset$, on a l'égalité suivante : $|V| - |E| + f = 2$*

Démonstration. Pour alléger les notations, dans la preuve suivante, on appellera graphe le dessin de G, les sommets sont assimilés à $\varphi(V)$ et les arêtes à $\psi(E)$.

Lemme 3.1.6. *Tout graphe connexe peut être obtenu en ajoutant des arrêtes à partir d'un graphe en arbre contenant les mêmes sommets. De plus, on peut supposer que chaque ajout ferme un cycle.*

Montrons cela par récurrence sur le nombre de faces. Si il n'y a qu'une face, alors, le graphe ne contient aucun cycle et c'est directement un arbre (graphe connexe sans cycle). Si la propriété est vraie pour un certain nombre de face f, prenons un graphe connexe à $f + 1$ faces. Alors il existe un cycle d'arêtes (bord d'une face bornée). En retirant une arête de ce cycle, le graphe reste connexe et le nombre de face diminue de 1. Appliquons l'hypothèse de récurrence, il suffit alors d'ajouter l'arête retirée pour obtenir le graphe de départ et cet ajout ferme bien un cycle.

Lemme 3.1.7. *Pour un arbre, $|V| - |E| + f = 2$.*

Il n'y a aucun cycle, donc le nombre de face est 1. De plus, dans un arbre, $|V| = |E|+1$ ce qui suffit à prouver l'égalité.

Il suffit maintenant de remarquer que si on ajoute une arête qui ferme un cycle, le nombre de face augmente de 1, le nombre d'arête augmente de 1 et le nombre de sommets reste inchangé. La quantité $|V|-|E|+f$ est donc conservée. Nous pouvons donc conclure en utilisant le premier lemme. □

En utilisant la formule d'Euler nous pouvons majorer le nombre d'arêtes d'un graphe G tel que $Cr(G) = 0$.

Proposition 3.1.8. *Si G est un graphe fini tel que $Cr(G) = 0$, alors $|E| \leq 3|V| - 6$. En particulier si $|E| > 3|V| - 6$, alors $Cr(G) > 0$.*

Démonstration. Premier cas : Si G est connexe. Toujours en considérant un dessin propre sans croisements de G. On peut appliquer la formule d'Euler : $|V|-|E|+f = 2$. De plus, chaque face étant adjacente à au moins trois arêtes et chaque arête étant adjacente à au plus deux faces, on a $3f \leq 2|E|$. En remplaçant dans la formule : $|E| \leq 3|V| - 6$.

Dans le cas général, on obtient l'inégalité sur chaque composante connexe ce qui suffit à conclure en sommant ces inégalités. □

Nous avons donc une condition suffisante pour que $Cr(G) > 0$. Dans le cas où nous avons une certaine marge dans l'inégalité, par exemple $|E|-3|V|+6 \geq k$ pour un certain entier $k > 0$, nous voudrions pouvoir dire plus. C'est l'objet du lemme suivant.

Lemme 3.1.9. *Soit G un graphe fini tel que $Cr(G) > 0$. Il existe une arête $e \in E$ telle que $Cr(G - \{e\}) < Cr(G)$. Où $G - \{e\}$ désigne le graphe $(V, E - \{e\})$.*

Démonstration. Prenons un dessin d de G qui réalise le minimum $Cr(d(G)) = Cr(G)$. Soit $e \in E$ une arrête qui réalise l'un des croisements (il en existe car $Cr(G) > 0$). Alors en notant toujours d le dessin induit sur le sous-graphe, $Cr(G-\{e\}) \leq Cr(d(G-\{e\})) \leq Cr(d(G)) - 1 = Cr(G) - 1$. □

Ainsi en itérant le lemme précédent tant que $|E| > 3|V| - 6$, nous obtenons la minoration suivante :

Proposition 3.1.10. *Si $G = (V, E)$ est un graphe fini, $Cr(G) \geq max(|E| - 3|V| + 6, 0)$*

Nous pouvons améliorer cette borne par un argument probabiliste.

Théorème 3.1.11. *Si $G = (V, E)$ est un graphe fini, $|E| \leq 4Cr(G)^{\frac{1}{3}}|V|^{\frac{2}{3}} + 5|V|$*

Soit $G = (V, E)$, un graphe fini. Considérons l'expérience aléatoire qui consiste à garder chaque sommet du graphe avec une probabilité $p \in [0, 1]$ (de manière indépendante). On conserve les arêtes dont les extrémités ont été gardées. Cela donne un sous-graphe aléatoire $G' = (V', E')$. En appliquant ce que nous avons déjà démontré à G', il vient

$$Cr(G') \geq |E'| - 3|V| + 6$$

En particulier pour d, un dessin propre de G, en notant toujours d le dessin induit sur G', $Cr(d(G')) \geq |E'| - 3|V'| + 6$ Nous pouvons passer à l'espérance et utiliser la linéarité :

$$Esp(Cr(d(G'))) \geq Esp(|E'|) - 3Esp(|V'|) + 6$$

Or nous avons $Esp(|V'|) = p|V|$. De plus, pour qu'une arête soit gardée, il faut que les deux extrémités soient gardées ce qui arrive avec une probabilité p^2 d'où $Esp(|E'|) = p^2|E|$. Enfin, pour qu'un croisement soit gardé, il faut que les deux arêtes sécantes soient gardées ce qui arrive avec une probabilité p^4 d'où $Esp(Cr(G')) = p^4 Cr(G)$. Finalement, nous obtenons

$$Cr(G) \geq \frac{p^2|E| - 3p|V| + 6}{p^4}$$

Optimisons cette inégalité en $p \in [0, 1]$. Si $|E| \geq 5|V|$, on peut poser $p = \frac{4|V|}{|E|}$ et on obtient

$$Cr(G) \geq \frac{1}{64}\frac{|E|^3}{|V|^2} + \frac{6|E|^4}{256|V|^4} \geq \frac{1}{64}\frac{|E|^3}{|V|^2}$$

En réarrangeant les termes, on obtient $|E| \leq 4Cr(G)^{\frac{1}{3}}|V|^{\frac{2}{3}}$. Pour que la majoration soit vraie même si $|E| \leq 5|V|$, on ajoute $5|V|$ au majorant. Cela donne bien la borne annoncée.

3.2 Théorème de Szemeredi-Trotter

Nous utilisons maintnenant ce que nous avons démontré sur le nombre de croisements afin de majorer le nombre d'incidences entre un ensemble de points et de droites du plan. En appliquant ce résultat à un ensemble de droites bien choisies, nous obtiendrons le théorème d'Eleke.

Définition 3.2.1. *Soit P un ensemble de points et L un ensemble de droites du plan. Nous supposons ici que ces deux ensembles sont finis. Nous appelons ensemble d'incidence entre P et L l'ensemble $Inc = \{(p, l) \in P \times L : p \in l\}$ Nous notons I son cardinal.*

Nous pouvons maintenant énoncer le théorème de Szemeredi-Trotter.

Théorème 3.2.2. *Avec les notations précédentes, $I \leq C(|L|^{\frac{2}{3}}|P|^{\frac{2}{3}} + |P| + |L|)$ où $C > 0$ est une certaine constante absolue.*

Démonstration. Considérons un graphe de sommets $V = P$ et pour lequel les arêtes sont les segments portés par une droite de L reliant deux points de P consécutifs le long de la droite. Notons que cela donne une représentation propre du graphe. Nous avons $|P| = |V|$ et (en notant $(a)_+ = max(a, 0)$) :

$$|E| = \sum_{l \in L} (|P \cap l| - 1)_+ \geq \sum_{l \in L} |P \cap l| - |L| = I - |L|$$

De plus, deux droites du plan se coupent en au plus un point, donc $Cr(G) \leq |L|^2$. En appliquant le résultat sur le nombre de croisements :

$$I - |L| \leq |E| \leq 4|L|^{\frac{2}{3}}|P|^{\frac{2}{3}} + 5|P|$$

Et finalement :

$$I \leq 4|L|^{\frac{2}{3}}|P|^{\frac{2}{3}} + 5|P| + |L|$$

Ce qui suffit à conclure (en posant $C = 5$). □

3.3 Théorème d'Eleke

Nous allons maintenant prouver le théorème en appliquant le théorème de Szemeredi à un ensemble de points et de droites bien choisis. Considérons un sous-ensemble fini $A \subset \mathbb{R}$. Prenons $P = (A + A) \times (A \cdot A)$ et $L = \{\{(x, y) : y = a(x - a')\}, a, a' \in A\}$. Nous avons alors $|P| = |A + A||A \cdot A|$ et $|L| = |A|^2$. De plus chaque ligne contient au moins $|A|$ points de P (si l est la ligne corespondant à l'équation $y = a(x - a')$, elle contient les points de l'ensemble $\{(x + a', ax), x \in A\}$). Ainsi on a la minoration $I \geq |L||A| = |A|^3$. On applique maintenant le théorème de Szemeredi-Trotter qui donne pour une certaine constante $C > 0$:

$$|A|^3 \leq C(|A|^{\frac{4}{3}}|P|^{\frac{2}{3}} + |P| + |A|^2)$$

Il existe $N_0 \in \mathbb{N}$ tel que $\forall N_0 \geq N, N^2 \leq \frac{1}{2C}N^3$. Il convient de remarquer que N_0 ne dépend que de C qui est une constante absolue. Donc N_0 est également une constante absolue.

1. Premier cas : Si $|A| \leq N_0$, alors

$$|A+A| \geq |A| \geq \frac{|A|^{\frac{5}{4}}}{N_0^{\frac{1}{4}}}$$

Donc $max(|A+A|, |A \cdot A|) \geq \frac{|A|^{\frac{5}{4}}}{N_0^{\frac{1}{4}}}$

2. Deuxième cas : si $|A| \geq N_0$. Nous avons alors par définition de N_0

$$\frac{1}{2C}|A|^3 \leq |A|^{\frac{4}{3}}|P|^{\frac{2}{3}} + |P|$$

   (a) Premier sous-cas : si $|P| \geq \frac{1}{4C}|A|^3$, alors à fortiori $|P| \geq \frac{1}{4C}|A|^{\frac{5}{2}}$

   (b) Deuxième sous-cas : si $|P| < \frac{1}{4C}|A|^3$, alors on peut réécrire l'inégalité

$$\frac{1}{4C}|A|^3 \leq |A|^{\frac{4}{3}}|P|^{\frac{2}{3}}$$

   et on obtient $|P| \geq \left(\frac{1}{4C}\right)^{3/2}|A|^{5/2}$

   Dans les deux sous-cas, on obtient $|P| \geq min\left(\left(\frac{1}{4C}\right)^{3/2}, \frac{1}{4C}\right)|A|^{5/2}$, ce qui montre (sachant que $|P| = |A+A||A \cdot A|$) :

$$max(|A+A||A \cdot A|) \geq C'|A|^{5/4}$$

   où on a posé $C' = \sqrt{min\left(\left(\frac{1}{4C}\right)^{3/2}, \frac{1}{4C}\right)}$ qui est une constante absolue strictement positive.

Finalement, dans les deux cas, $max(|A+A|, |A \cdot A|) \geq min\left(C', \frac{1}{N_0^{1/4}}\right)|A|^{5/4}$ et puisque $min\left(C', \frac{1}{N_0^{1/4}}\right)$ est une constante absolue, le théorème d'Eleke est démontré.

Ce résultat montre qu'un sous-ensemble fini de $\mathbb{R}$ ne peut pas être essentiellement invariant par $+$ et par $\cdot$. Si on considère les ensembles essentiellement invariants par $+$ comme une généralisation des sous-groupes, en poussant plus loin l'analogie un sous-ensemble invariant par $+$ et $\cdot$ serait un sous-corps généralisé. Le théorème d'Eleke affirme donc qu'il n'existe pas de tel sous-corps généralisé fini dans $\mathbb{R}$. Cependant, dans les corps finis le théorème tombe en défaut car il existe en particulier des sous-corps finis.

4 Progressions arithmétiques

4.1 Motivations

Dans cette section, nous abandonnons les questions portant sur les cardinaux d'ensembles tels que $A+A$ et $A \cdot A$, que nous venons de développer à travers les théorèmes

de Plünnecke et d'Eleke, pour aborder un autre domaine important de la combinatoire additive. Nous étudions le cas particulier des entiers i.e. $Z = \mathbb{Z}$ pour répondre au problème suivant : pour $n \in \mathbb{N}$, à quelle condition sur la taille de $A \subset \{1, \dots, n\}$ est-on sûr de trouver une progression arithmétique de longueur k dans A ? Pour rappel, on appelle progression arithmétique de longueur k toute suite finie $(a_i)_{1 \leq i \leq k}$ où $a_{i+1} - a_i = r$ pour une constante r appelée *raison*. Naturellement, nous pouvons supposer $k \geq 3$ puisque les cas $k = 1$ et $k = 2$ sont triviaux.

Le meilleur résultat actuel lorsque $k = 3$ est celui de Bourgain, qui démontre l'existence d'une progression arithmétique de longueur 3 dès que A a une densité dans $\{1, \dots, n\}$ de l'ordre de $\sqrt{\ln(\ln(n))}/\sqrt{\ln(n)}$. Nous allons ici démontrer une proposition moins forte qui date de 1953, connue sous le nom de théorème de Roth, qui demande à A d'avoir une densité de l'ordre de $1/\ln(\ln(n))$. Il est à noter qu'il n'y a pas de manière simple d'étendre un résultat de $k = 3$ à $k = 4$: ce n'est qu'en 1969 que Szemerédi est parvenu à obtenir une borne sur la densité de A lorsque $k = 4$, avant de finalement traiter le problème pour tout k en 1975.

Il semble en fait que la bonne condition soit une densité en $1/\ln(n)$: c'est ce que propose la conjecture d'Erdös et Turan, qui stipule que toute partie $A \subset \mathbb{N}$ telle que $\sum_{n \in A} 1/n = +\infty$ possède une infinité de progressions arithmétiques, et ce pour tout k. En effet, on a l'implication suivante :

Proposition 4.1.1. *Soit $\varepsilon > 0$ fixé. Supposons que nous sachions que pour tout $n \in \mathbb{N}$ et tout $A \subset \{1, \dots, n\}$ de densité au moins égale à $\frac{1}{\ln(n)^{1+\varepsilon}}$, A contienne une progression arithmétique de longueur k. Alors pour tout $A \subset \mathbb{N}$ telle que $\displaystyle\sum_{n \in A} \frac{1}{n} = +\infty$, A contient une progression arithmétique de longueur k.*

Démonstration. Soit $A \subset \mathbb{N}$ telle que $\sum_{n \in A} \frac{1}{n} = +\infty$. Si pour tout n, $A \cap \{1, \dots, n\}$ avait une densité inférieure à $\frac{1}{\ln(n)^{1+\varepsilon}}$, on aurait alors $|A \cap \{1, \dots, n\}| \leq \frac{n}{\ln(n)^{1+\varepsilon}}$. Appliqué à $n \ln(n)^{1+\varepsilon}$ au lieu de n, cette relation indique qu'il y a moins de n éléments dans $A \cap \{1, \dots, n \ln(n)^{1+\varepsilon}\}$. En écrivant $A = (a_n)_{n \in \mathbb{N}}$, cela signifie que $a_n \geq n \ln(n)^{1+\varepsilon}$ et donc :
$\sum_{n \in A} \frac{1}{n} = \sum_{n \in \mathbb{N}} \frac{1}{a_n} \leq \sum_{n \in \mathbb{N}} \frac{1}{n \ln(n)^{1+\varepsilon}} < +\infty$, ce qui est faux. Ainsi, on peut trouver un n tel que $A \cap \{1, \dots, n\}$ ait une densité supérieure à $\frac{1}{\ln(n)^{1+\varepsilon}}$, et donc A contient une progression arithmétique de longueur k. □

Par exemple, dans le cas où A est l'ensemble des nombres premiers (de densité en $1/\ln(n)$), Van der Corput a montré en 1935 qu'il existe une infinité de progressions arithmétiques de longueur 3.

4.2 Théorème de Roth

Le théorème de Roth affirme que pour une densité fixée, toute partie de $\{1, \dots, n\}$ ayant cette densité contient une progression arithmétique de longueur 3, pourvu que n soit suffisamment grand.

Théorème 4.2.1 (Roth). *Soit $\delta \in]0,1]$. Il existe un entier N_0 (dépendant de δ) tel que pour tout $N \geq N_0$, si $A \subset \{1,\dots,N\}$ vérifie $|A| \geq \delta N$, alors A contient une progression arithmétique de longueur 3.*

Notons $P(\delta)$: "Le théorème est vrai pour toutes les densités $\geq \delta$". On peut déjà remarquer que $P(1)$ est bien sûr vraie, de même que $P(\delta)$ pour $\delta > 2/3$. En effet : $|\{n \in \{1,\dots,N-2\} | n \notin A \text{ ou } n+1 \notin A \text{ ou } n+2 \notin A\}| \leq 3(1-\delta)N$ qui est strictement inférieur à $N-2$ pour N assez grand, d'où l'existence d'un n tel que $(n, n+1, n+2)$ forme une progression arithmétique dans A.

L'idée de la preuve du théorème est d'effectuer une "récurrence continue" en montrant que l'on peut progressivement abaisser δ comme suit :

Proposition 4.2.2. *Il existe une fonction continue positive $\varepsilon(\delta)$ telle que :*

$$\forall \delta \in]0,1[, P(\delta + \varepsilon(\delta)) \Rightarrow P(\delta)$$

Cette proposition implique alors le théorème de Roth, puisque si $P(\delta)$ était fausse pour un certain δ, posons $\Delta = \sup\{\delta \in]0,1] | P(\delta) \text{ est fausse}\}$. La proposition $P(\delta)$ est donc vraie pour $\delta > \Delta$ et fausse pour $\delta < \Delta$. Par continuité de ε, on peut pourtant trouver un $\delta < \Delta$ tel que $\delta + \varepsilon(\delta) > \Delta$, d'où $P(\delta)$ par la proposition : on aboutit a une contradiction.

Pour démontrer la proposition, fixons une densité δ et un ε que nous devrons déterminer. Supposons $P(\delta+\varepsilon)$: on obtient ainsi l'existence d'un M_0 associé par le théorème de Roth à $\delta + \varepsilon$. Il nous faut donc montrer qu'en choisissant correctement ε, pour N assez grand et pour toute partie $A \subset \{1,\dots,N\}$ telle que $|A| \geq \delta N$, alors A contient une progression arithmétique de longueur 3. Pour cela, on effectue la disjonction de cas suivante :

- Si A contient un "facteur compact", c'est-à-dire une progression arithmétique $P \subset \{1,\dots,N\}$ de taille au moins M_0 sur laquelle A a une densité d'au moins $\delta + \varepsilon$ i.e. $\frac{|A \cap P|}{|P|} \geq \delta + \varepsilon$. Dans ce cas on peut appliquer le théorème de Roth car $P(\delta + \varepsilon)$ est vraie : on a donc trouvé une progression arithmétique de longueur 3 dans $A \cap P$ et, a fortiori, dans A.
- Sinon, A est très homogènement réparti, puisque pour toute progression arithmétique $P \subset \{1,\dots,N\}$ de taille au moins M_0, la densité de A dans P reste inférieure à $\delta + \varepsilon$. Pour exploiter cela, nous allons plonger A dans $\mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p afin d'utiliser la théorie de Fourier discrète : nous allons voir que dans ce cas les coefficients de Fourier de la fonction indicatrice de A normalisée sont petits, ce qui indique que cette fonction agit un peu comme un "bruit aléatoire" équiréparti. L'intuition suggère qu'alors qu'on peut trouver $\sim \delta^3 N^2$ progressions arithmétiques dans A, puisqu'il y a N^2 telles progressions dans $\{1,\dots,N\}$ et que chacune devrait avoir une probabilité $\sim \delta^3$ d'être dans A.

On suppose donc dorénavant que A n'a pas de facteur compact. D'après le théorème des nombres premiers, il existe un N_0 à partir duquel on peut toujours trouver un nombre premier entre $(1-\varepsilon)N_0$ et N_0. En effet, si $\Pi(n)$ désigne le nombre de nombres premiers

inférieurs ou égaux à n, on sait que $\Pi(n) \underset{+\infty}{\sim} n\ln(n)$. ε étant toujours fixé, considérons $\eta > 0$ suffisamment petit pour que $(1-\varepsilon)(1+\eta) < 1-\eta$, et soit N tel que pour tout $n \geq N(1-\varepsilon)$ on ait :

$$(1-\eta)n\ln(n) \leq \Pi(n) \leq (1+\eta)n\ln(n)$$

Alors pour tout $n \geq N$, si l'intervalle $[\![(1-\varepsilon)n, n]\!]$ ne contenait pas de nombre premier, on aurait $\Pi((1-\varepsilon)n) = \Pi(n)$ et donc $(1-\varepsilon)n\ln((1-\varepsilon)n)(1+\eta) \geq n\ln(n)(1-\eta)$. Par conséquent,

$$(1-\varepsilon)n\ln(n)(1+\eta) \geq n\ln(n)(1-\eta) \Rightarrow (1-\varepsilon)(1+\eta) \geq 1-\eta$$

ce qui est faux par définition de η.

Soient donc un entier N et un nombre premier p donnés par l'argument précédent. On pose alors $A' = A \cap \{1, \ldots, p\}$ vu comme sous-ensemble de $\mathbb{Z}/p\mathbb{Z}$; remarquons qu'on a toujours $|A' \cap P| \leq (\delta+\varepsilon)|P|$ pour toute progression $P \subset \{1, \ldots, p\}$ de longueur supérieure à M_0. En particulier $|A'| \leq (\delta+\varepsilon)p$ puisque il est possible de choisir p plus grand que M_0. Plus précisément, on peut encadrer la densité de $|A'|$ comme suit :

$$\delta + \varepsilon \geq \frac{|A'|}{p} \geq \frac{|A \cap \{1, \ldots, N(1-\varepsilon)\}|}{p} \geq \frac{|A| - \varepsilon N}{N} \geq \delta - \varepsilon$$

Cependant, cet encadrement n'est a priori pas vrai pour toute progression de $\mathbb{Z}/p\mathbb{Z}$ de taille supérieure à M_0, qui ne sont pas forcément des progressions de $\{1, \ldots, p\}$ à cause de la structure de $\mathbb{Z}/p\mathbb{Z}$. On appelle donc *véritable progression arithmétique* toute progression de $\mathbb{Z}/p\mathbb{Z}$ telle que son image par l'application

$$\begin{array}{rccc} f: & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \{1, \ldots, p\} \\ & \overline{x} & \longmapsto & x \end{array}$$

soit une progression de $\{1, \ldots, p\}$. Ce problème peut en réalité être résolu, puisque notre majoration provenant de l'absence de facteur compact dans A s'étend en fait à toutes les progressions de $\mathbb{Z}/p\mathbb{Z}$, même si elles ne sont pas véritables.

Proposition 4.2.3. *Il existe un entier M_1 tel que $|A' \cap P| \leq (\delta+2\varepsilon)|P|$ pour toute progression arithmétique P de $\mathbb{Z}/p\mathbb{Z}$ de longueur supérieure à M_1.*

Démonstration. Soit P une progression arithmétique de $\mathbb{Z}/p\mathbb{Z}$, notons r sa raison. Dans le cas où $r \leq p/M_0$, on peut découper P en plusieurs sous-progressions en débutant une nouvelle progression dès que la précédente "reboucle" dans $\mathbb{Z}/p\mathbb{Z}$: sauf éventuellement pour la première et la dernière, elles sont alors toutes de longueur supérieure à M_0 et par conséquent de densité au plus $\delta+\varepsilon$, puisque A' n'a pas de facteur compact. D'où l'inégalité suivante :

$$|A' \cap P| \leq (\delta+\varepsilon)|P| + 2M_0$$

Si on ne suppose plus que r est suffisamment petite, on peut se ramener au cas ci-dessus en considérant les M_0 premiers termes de P dans $\mathbb{Z}/p\mathbb{Z}$: par le principe des

tiroirs, au moins deux d'entre eux sont à distance inférieure à p/M_0 i.e. $\exists k \leq M_0 : kr \mod p \leq p/M_0$. Ainsi, il suffit de diviser P en k sous-progressions disjointes de raison $kr \mod p$, auxquelles on applique séparément le résultat précédent. Il vient :

$$|A' \cap P| \leq (\delta + \varepsilon)|P| + 2kM_0 \leq (\delta + \varepsilon)|P| + 2M_0^2 \leq (\delta + 2\varepsilon)|P|$$

si $|P|$ est assez grand, ce qui donne l'existence de l'entier M_1 recherché. □

Récapitulons : nous avons supposé que la partie A était sans facteur compact, avant de la plonger dans $\mathbb{Z}/p\mathbb{Z}$ afin obtenir un nouvel ensemble A' pour lequel nous venons de montrer qu'il vérifie toujours l'hypothèse d'absence de facteur compact, et ce même pour des progressions qui ne seraient pas véritables. Désormais, il est possible d'utiliser les outils de transformation de Fourier discrète sur A', pour exploiter le fait que l'ensemble A' est très homogènement réparti dans $\mathbb{Z}/p\mathbb{Z}$.

Rappelons la définition de la transformée de Fourier dans $\mathbb{Z}/p\mathbb{Z}$: en notant $\mathrm{d}x$ la mesure de comptage normalisée et $\mathrm{d}\xi$ la mesure de comptage standard sur $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire

$$\int_{\mathbb{Z}/p\mathbb{Z}} f(x)\,\mathrm{d}x = \frac{1}{p}\sum_{x\in\mathbb{Z}/p\mathbb{Z}} f(x) \text{ et } \int_{\mathbb{Z}/p\mathbb{Z}} f(\xi)\,\mathrm{d}\xi = \sum_{\xi\in\mathbb{Z}/p\mathbb{Z}} f(\xi)$$

nous disposons du produit scalaire entre deux fonctions définies sur $\mathbb{Z}/p\mathbb{Z}$:

$$\langle f, g\rangle_{L^2(\mathbb{Z}/p\mathbb{Z},\mathrm{d}x)} = \int_{\mathbb{Z}/p\mathbb{Z}} f(x)\bar{g}(x)\,\mathrm{d}x \text{ d'où la norme } \|f\|^2_{L^2(\mathbb{Z}/p\mathbb{Z},\mathrm{d}x)} = \langle f, f\rangle_{L^2(\mathbb{Z}/p\mathbb{Z},\mathrm{d}x)}$$

ainsi que du produit scalaire dans l'espace de Fourier :

$$\langle \hat{f}, \hat{g}\rangle_{L^2(\mathbb{Z}/p\mathbb{Z},\mathrm{d}\xi)} = \int_{\mathbb{Z}/p\mathbb{Z}} \hat{f}(\xi)\overline{\hat{g}(\xi)}\,\mathrm{d}x \text{ d'où la norme } \|\hat{f}\|^2_{L^2(\mathbb{Z}/p\mathbb{Z},\mathrm{d}\xi)} = \langle \hat{f}, \hat{f}\rangle_{L^2(\mathbb{Z}/p\mathbb{Z},\mathrm{d}\xi)}$$

Dans la suite, on notera simplement $\|f\|_2$, et le produit scalaire utilisé sera implicite. La *transformée de Fourier de* f est quant à elle définie par :

$$\hat{f}(\xi) = \langle f, e^{2i\pi\xi\cdot/p}\rangle = \int_{\mathbb{Z}/p\mathbb{Z}} f(x)e^{-2i\pi x\xi/p}\,\mathrm{d}x$$

et on dispose de la formule d'inversion :

$$f(x) = \int_{\mathbb{Z}/p\mathbb{Z}} \hat{f}(\xi)e^{2i\pi x\xi/p}\,\mathrm{d}\xi = \sum_{\xi\in\mathbb{Z}/p\mathbb{Z}} \hat{f}(\xi)e^{2i\pi x\xi/p}$$

Enfin, le *produit de convolution de* f *avec* g est la fonction suivante :

$$f \star g(y) = \int_{\mathbb{Z}/p\mathbb{Z}} f(x)g(y-x)\,\mathrm{d}x = g \star f(y)$$

Pour la suite, nous aurons besoin des deux formules suivantes :

Proposition 4.2.4. *Pour toutes fonctions f et g définies sur $\mathbb{Z}/p\mathbb{Z}$ à valeurs dans $\mathbb{C}$:*

1. *(Formule de Plancherel) $\|f\|_2 = \|\hat{f}\|_2$*
2. *$\forall \xi \in \mathbb{Z}/p\mathbb{Z}, \widehat{f \star g}(\xi) = \hat{f}(\xi)\hat{g}(\xi)$*

Démonstration.

1. Un calcul direct donne :

$$\|\hat{f}\|_2^2 = \sum_{\xi \in \mathbb{Z}/p\mathbb{Z}} \hat{f}(\xi)\overline{\hat{f}(\xi)} = \frac{1}{p^2} \sum_{\xi \in \mathbb{Z}/p\mathbb{Z}} \left[\sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x) e^{-2i\pi x\xi/p} \times \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \bar{f}(y) e^{2i\pi y\xi/p} \right]$$

$$= \frac{1}{p^2} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} f(x)\bar{f}(y) \sum_{\xi \in \mathbb{Z}/p\mathbb{Z}} e^{2i\pi(y-x)\xi/p} = \frac{p}{p^2} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x)\bar{f}(x) = \|\hat{f}\|_2$$

2. De même,

$$\begin{aligned} \widehat{f \star g}(\xi) &= \frac{1}{p^2} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x) g(y-x) e^{-2i\pi y\xi/p} \\ &= \frac{1}{p^2} \sum_{(x,y') \in (\mathbb{Z}/p\mathbb{Z})^2} f(x) g(y') e^{-2i\pi(x+y')\xi/p} \\ &= \hat{f}(\xi)\hat{g}(\xi) \end{aligned}$$

□

Définissons à présent la fonction (de moyenne nulle) $\gamma(x) = \mathbb{1}_{A'}(x) - |A'|/p$ où $\mathbb{1}_{A'}$ désigne la fonction indicatrice de A'. Si P est une progression arithmétique de $\mathbb{Z}/p\mathbb{Z}$ (pas forcément véritable) de longueur supérieure à M_1, la proposition 2.2.3 donne :

$$\sum_{x \in P} \gamma(x) = |A' \cap P| - \frac{|A'||P|}{p} \leq (\delta + 2\varepsilon)|P| - (\delta - \varepsilon)|P| \leq 3\varepsilon|P|$$

ce que revient à dire que γ est en moyenne inférieure à 3ε sur toute progression P de taille supérieure à M_1, et qui se réécrit sous la forme :

$$\gamma \star \frac{\mathbb{1}_P}{|P|}(x) \leq \frac{3\varepsilon}{p}$$

Mais nous pouvons être plus précis : en remarquant que $\gamma \star \frac{\mathbb{1}_P}{|P|}$ a elle aussi une moyenne nulle, on sait que les normes 1 de sa partie positive et de sa partie négative sont égales. Et comme $\|(\gamma \star \frac{\mathbb{1}_P}{|P|})^+\|_1 \leq 3\varepsilon$, on obtient finalement $\|(\gamma \star \frac{\mathbb{1}_P}{|P|})\|_1 \leq 6\varepsilon$. C'est cette inégalité que nous allons utiliser pour déduire des informations sur la transformée de Fourier de γ.

Le lemme fondamental portant sur $\hat{\gamma}$ est le suivant :

Lemme 4.2.5. *Pour tout $\xi \in \mathbb{Z}/p\mathbb{Z}$, on a $|\hat{\gamma}(\xi)| \leq 12\varepsilon$.*

Remarque 4.2.6. De manière très informelle, on peut comprendre ce résultat ainsi : γ est d'une certaine manière presque orthogonale à toutes les fonctions phases $x \longmapsto e^{2i\pi x\xi/p}$, de la même manière que l'est une fonction aléatoire. Si γ était elle aussi une fonction phase de la forme $e^{2i\pi\varphi(x)/p}$, ce lemme signifierait que φ ne ressemble pas à une fonction linéaire du type $x \longmapsto x\xi/p + c$ pour aucun ξ et aucune constante c. On a donc bien traduit l'absence de régularité périodique de γ.

Démonstration. La fonction γ étant de moyenne nulle, on a $\hat{\gamma}(0) = 0$. Pour $\xi \neq 0$, notons $r = \xi^{-1}$ l'inverse de ξ dans $\mathbb{Z}/p\mathbb{Z}$ et $P = \{kr | 0 \leq k < M_1\}$ une progression arithmétique. D'après ce qui précède, et en utilisant la relation $\widehat{f \star g}(\xi) = \hat{f}(\xi)\hat{g}(\xi)$, on a :

$$|\hat{\gamma}(\xi)|\frac{p}{|P|}|\widehat{\mathbb{1}_P}(\xi)| = p|\widehat{\gamma \star \frac{\mathbb{1}_P}{|P|}}(\xi)| \leq \sum_{x\in\mathbb{Z}/p\mathbb{Z}} |\gamma \star \frac{\mathbb{1}_P}{|P|}(x)| \leq \|(\gamma \star \frac{\mathbb{1}_P}{|P|})\|_1 \leq 6\varepsilon$$

Par ailleurs,

$$\widehat{\mathbb{1}_P}(\xi) = \frac{1}{p}\sum_{k=0}^{M_1-1} e^{-2i\pi kr\xi/p} = \frac{1}{p}\sum_{k=0}^{M_1-1} e^{-2i\pi k/p} \underset{p\to+\infty}{\sim} \frac{|P|}{p}$$

En choisissant p assez grand par rapport à M_1 (qui ne dépend que de M_0 et de ε), on obtient $|\widehat{\mathbb{1}_P}(\xi)| \geq \frac{|P|}{2p}$, et donc $|\hat{\gamma}(\xi)| \leq 12\varepsilon$. □

Nous venons de traduire en termes de transformée de Fourier l'absence de facteur compact dans A'. Pour relier cette information aux progressions arithmétiques, introduisons l'opérateur trilinéaire suivant :

$$T(f,g,h) = \int_{\mathbb{Z}/p\mathbb{Z}}\int_{\mathbb{Z}/p\mathbb{Z}} f(x)g(x+r)h(x+2r)\mathrm{d}x\mathrm{d}r$$

Cet opérateur est crucial car le nombre de progressions arithmétiques de longueur 3 dans A' est tout simplement $p^2T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'}) - |A'|$ (le terme $-|A'|$ retranche les progressions triviales de raison 0). Il nous suffit à présent de montrer que $T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'}) > (\delta + \varepsilon)/p$ pour démontrer que la propriété $P(\delta)$ est vraie, ce qui achèvera la preuve du théorème de Roth. Le lemme de cette section qui suit permet de relier l'estimation obtenue par le lemme 2.2.5 et l'opérateur T.

Lemme 4.2.7. *Pour toutes fonctions f, g et h définies sur $\mathbb{Z}/p\mathbb{Z}$, on a : $T(f,g,h)| \leq \|f\|_2\|g\|_2\|\hat{h}\|_\infty$.*

Démonstration. D'après la formule d'inversion rappelée plus haut, on peut réécrire T comme suit :

$$T(f,g,h) = \sum_{(\xi_1,\xi_2,\xi_3)\in(\mathbb{Z}/p\mathbb{Z})^3} \hat{f}(\xi_1)\hat{f}(\xi_2)\hat{f}(\xi_3)\int_{\mathbb{Z}/p\mathbb{Z}}\int_{\mathbb{Z}/p\mathbb{Z}} e^{2i\pi[x\xi_1+(x+r)\xi_2+(x+2r)\xi_3]/p}\mathrm{d}x\mathrm{d}r$$

L'intégrale sur r est toujours nulle en tant que somme de racines de l'unité, à moins que $\xi_2 + 2\xi_3 = 0$. De même, l'intégrale sur x est éventuellement non nulle à condition que $\xi_1 + \xi_2 + \xi_3 = 0$. En ne conservant que ces termes, il reste :

$$|T(f,g,h)| = |\sum_{\xi\in\mathbb{Z}/p\mathbb{Z}} \hat{f}(\xi)\hat{g}(-2\xi)\hat{h}(\xi)| \leq \|\hat{h}\|_\infty \sum_{\xi\in\mathbb{Z}/p\mathbb{Z}} |\hat{f}(\xi)\hat{g}(-2\xi)| \leq \|\hat{f}\|_2\|\hat{g}\|_2\|\hat{h}\|_\infty = \|f\|_2\|g\|_2\|\hat{h}\|_\infty$$

en utilisant l'inégalité de Cauchy-Schwarz et la proposition 2.2.4. □

Armé de tout ce qui précède, il ne nous reste plus qu'à minorer $T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'})$, en utilisant la linéarité de l'opérateur et le fait qu'il est bien sûr possible de permuter les fonctions f, g et h dans T. Sachant de plus que $\||A'|/p\|_2 = |A'|/p \leq (\delta + \varepsilon)$, que $\|\hat{\gamma}\|_\infty \leq 12\varepsilon$ et que $\|\gamma\|_2 = \|\hat{\gamma}\|_2 \leq 12\varepsilon$, on obtient :

$$T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'}) = T(\gamma + |A'|/p, \gamma + |A'|/p, \gamma + |A'|/p)$$

$$\Rightarrow |T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'}) - T(|A'|/p, |A'|/p, |A'|/p)| \leq 1728\varepsilon^3 + 3\times 144(\delta+\varepsilon)\varepsilon^2 + 3\times 12\varepsilon(\delta+\epsilon)^2$$

Or il faut se rappeler que $\delta + \varepsilon \geq |A'|/p \geq \delta - \varepsilon$. L'expression précédente devient :

$$T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'}) \geq (\delta - \varepsilon)^3 - 1728\varepsilon^3 + 432(\delta + \varepsilon)\varepsilon^2 + 36\varepsilon(\delta + \epsilon)^2$$

Nous pouvons enfin choisir ε en fonction de δ uniquement : s'il est assez petit, l'inégalité précédente nous permet d'avoir $T(\mathbb{1}_{A'}, \mathbb{1}_{A'}, \mathbb{1}_{A'})$ aussi proche de δ^3 que voulu, soit au moins $p^2(\delta^3 - \alpha) - p(\delta - \varepsilon) > 0$ progressions arithmétiques de longueur 3 dans A', où α est un réel strictement positif qui peut être rendu arbitrairement petit. Remarquons que nous retrouvons l'estimation intuitive que nous avons proposée au début de la section.

La dernière étape consiste à s'assurer qu'au moins une des progressions ainsi obtenues est véritable. On résout facilement ce dernier problème en multipliant γ par l'indicatrice de l'intervalle $C = [\![p/3, 2p/3]\!]$ notée $\mathbb{1}_C$. La quantité $p^2T(\mathbb{1}_C\mathbb{1}_{A'}, \mathbb{1}_C\mathbb{1}_{A'}, \mathbb{1}_C\mathbb{1}_{A'}) - |A' \cap C|$ compte cette fois les progressions de longueur 3 incluses dans C, qui sont nécessairement véritables. En effet, pour qu'une progression arithmétique de longueur 3 de raison inférieure à p ne soit pas véritable, il faut que la progression "reboucle" dans $\mathbb{Z}/p\mathbb{Z}$ une et une seule fois, ce qui est impossible si tous les termes sont dans C. Il suffit donc de montrer que cette quantité est strictement positive si ε et p sont bien choisis.

La situation est similaire au cas précédent puisqu'on a toujours les majorations sur les normes 2 et infinies, bien que légèrement modifiées :

$$\|\mathbb{1}_C|A'|/p\|_2 = \sqrt{1/3}|A'|/p \leq \sqrt{1/3}(\delta + \varepsilon)$$

$$\widehat{\mathbb{1}_C\gamma} = \widehat{\widehat{\mathbb{1}_C} \star \hat{\gamma}} = \widehat{\mathbb{1}_C} \star \hat{\gamma} \text{ donc } \|\widehat{\mathbb{1}_C\gamma}\|_\infty \leq \|\widehat{\mathbb{1}_C}\|_\infty\|\hat{\gamma}\|_\infty \leq \frac{12}{3}\varepsilon$$

$$\|\mathbb{1}_C\gamma\|_2 = \|\widehat{\mathbb{1}_C\gamma}\|_2 \leq \frac{12}{3}\varepsilon$$

Et cette fois le terme non négligeable quand $\varepsilon \to 0$ s'écrit :

$$T(\mathbb{1}_C|A'|/p, \mathbb{1}_C|A'|/p, \mathbb{1}_C|A'|/p) = T(\mathbb{1}_C, \mathbb{1}_C, \mathbb{1}_C)\left(\frac{|A'|}{p}\right)^3 \geq \frac{1}{55}\left(\frac{|A'|}{p}\right)^3$$

parce que

$$\begin{aligned}
T(\mathbb{1}_C,\mathbb{1}_C,\mathbb{1}_C) &= \frac{1}{p^2}\left(\underbrace{\lfloor\frac{2p}{3}\rfloor-\lfloor\frac{p}{3}\rfloor-2}_{\text{progressions de raison 1 dans } C} + \underbrace{\lfloor\frac{2p}{3}\rfloor-\lfloor\frac{p}{3}\rfloor-4}_{\text{progressions de raison 2 dans } C} +\cdots+\lfloor\frac{2p}{3}\rfloor-\lfloor\frac{p}{3}\rfloor-2\lfloor\frac{\lfloor\frac{2p}{3}\rfloor-\lfloor\frac{p}{3}\rfloor}{3}\rfloor\right)\\
&\geq \frac{1}{p^2}\left(\frac{p}{3}-3+\frac{p}{3}-5+\cdots+\frac{p}{3}-2\lfloor\frac{p}{9}+\frac{1}{3}\rfloor-1\right)\\
&\geq \frac{1}{p^2}\left(\lfloor\frac{p}{9}+\frac{1}{3}\rfloor(\frac{p}{3}-1)-\sum_{k=1}^{\lfloor\frac{p}{9}+\frac{1}{3}\rfloor}2k\right)\\
&\geq \frac{(\frac{p}{9}-\frac{2}{3})(\frac{p}{3}-1-\frac{1}{2}(\frac{p}{3}+\frac{1}{3}+1))}{p^2}\\
&\geq \frac{1}{55}
\end{aligned}$$

dès que p est supérieur à une certaine constante absolue, indépendante de ε.

Alors pour ε assez petit devant δ uniquement, le nombre de progressions arithmétiques dans $A'\cap C$ est d'au moins $\frac{1}{55}p^2(\delta^3-\alpha)-p(\delta-\varepsilon)>0$ si p est pris suffisamment grand. Par conséquent, nous pouvons choisir $\varepsilon(\delta)$ tel que $P(\delta+\varepsilon(\delta))\Rightarrow P(\delta)$. Une inspection plus fine de l'expression qui détermine ε indique que celui-ci dépend continûment de la densité δ, ce qui achève la preuve du théorème de Roth.

4.3 Quelques considérations sur le cas k = 4

On pourrait penser que l'argument de Roth s'étend sans difficulté au cas $k=4$ et au-delà, mais il n'en est rien. Le principal problème tient au fait que la notion suffisante pour conclure n'est plus l'orthogonalité de la transformée de Fourier de l'indicatrice par rapport aux fonction à phases linéaires comme illustré par la remarque 2.2.6., mais plutôt l'orthogonalité par rapport aux fonctions à phase quadratiques $x\longmapsto e^{2i\pi\varphi(x)/p}$ où φ est un polynôme de degré inférieur à 2. Ce point a été mis en évidence par Gowers dans sa preuve du cas $k=4$, qui reprend la démonstration de Roth en étudiant les propriétés de l'uniformité quadratique, et non plus seulement linéaire.

Si nous tentons tout de même d'écrire la démonstration de Roth naïvement adaptée aux suites arithmétiques de longueur 4, elle échoue effectivement au moment de démontrer un équivalent du lemme 2.2.7. pour l'opérateur quadrilinéaire :

$$R(f,g,h,i)=\int_{\mathbb{Z}/p\mathbb{Z}}\int_{\mathbb{Z}/p\mathbb{Z}}f(x)g(x+r)h(x+2r)i(x+3r)\mathrm{d}x\mathrm{d}r$$

Les progressions de longueur 4 sont toujours au nombre de $p^2R(\mathbb{1}_{A'},\mathbb{1}_{A'},\mathbb{1}_{A'},\mathbb{1}_{A'})-|A'|$, le terme principal dans $R(\gamma+|A'|/p,\gamma+|A'|/p,\gamma+|A'|/p,\gamma+|A'|/p)$ est toujours $R(|A'|/p,|A'|/p,|A'|/p,|A'|/p)$ qui est de l'ordre de δ^3, les termes $R(|A'|/p,\cdot,\cdot,\cdot)$ et leurs permutations peuvent toujours être traités en factorisant par $|A'|/p$ et en se ramenant au lemme 2.2.7. Par contre, le terme $R(\gamma,\gamma,\gamma,\gamma)$ est plus résistant, puisque la meilleure

majoration possible est, après l'avoir reformulé via la formule d'inversion comme précédemment, et en utilisant l'inégalité de Cauchy-Schwarz sur $(\mathbb{Z}/p\mathbb{Z})^2$:

$$\begin{aligned}|R(\gamma,\gamma,\gamma,\gamma)| &= |\sum_{(\xi_1,\xi_2)\in(\mathbb{Z}/p\mathbb{Z})^2} \hat{\gamma}(\xi_1+2\xi_2)\hat{\gamma}(-2\xi_1-3\xi_2)\hat{\gamma}(\xi_1)\hat{\gamma}(\xi_2)| \\ &\leq \sqrt{\sum_{(\xi_1,\xi_2)\in(\mathbb{Z}/p\mathbb{Z})^2} |\hat{\gamma}(\xi_1+2\xi_2)\hat{\gamma}(-2\xi_1-3\xi_2)|^2}\sqrt{\sum_{(\xi_1,\xi_2)\in(\mathbb{Z}/p\mathbb{Z})^2} |\hat{\gamma}(\xi_1)\hat{\gamma}(\xi_2)|^2} \\ &\leq 144\varepsilon^2 p^2 \|\hat{\gamma}\|_2^2\end{aligned}$$

qui n'est plus indépendante de p : il devient impossible de trouver un ε assez petit qui permet de rendre négligeable ce terme, puisque $p \underset{\varepsilon\to 0}{\to} +\infty$...

5 Estimations de la densité critique

Nous avons vu avec le théorème de Roth que pour une valeur de densité $\delta > 0$, à condition de choisir N assez grand, tout sous-ensemble de densité au moins δ de $[\![1, N]\!]$ contient au moins trois termes en progression arithmétique. Si nous appelons densité critique la quantité :

$$\delta_N^{cri} = sup\left\{\frac{|A|}{N}, A \subset [\![1,N]\!] \text{ qui ne contient pas 3 termes en progression arithmétique}\right\}$$

Nous pouvons reformuler le théorème précédent en écrivant : $\delta_N^{cri} \xrightarrow[N\to\infty]{} 0$. Une solution pour affiner le résultat est donc d'estimer la vitesse de convergence. Nous nous intéresserons ici à une minoration.

5.1 Majoration par l'argument de Roth

Cherchons à reformuler le théorème de Roth : au lieu d'obtenir l'entier N après avoir fixé δ, demandons plutôt, à N fixé, la densité minimale que doit avoir une partie de $\{1, \cdots, N\}$ pour que le théorème nous assure qu'elle contienne une progression arithmétique. En analysant les contraintes imposées dans la preuve précédente entre les divers paramètres δ, ε et M_0, on trouve que l'on peut en fait prendre $\varepsilon = c\delta$ pour une constante c bien choisie, et $N_0 = CM_0^C\delta^{-C}\varepsilon^{-C}$ pour une autre constante C. On peut de plus supposer $M_0 \geq \delta^{-1}$ car si $M_0 < \delta^{-1}$, il n'existe aucun sous-ensemble de $\{1, \ldots, M_0\}$ de densité δ. Par conséquent, si l'on note $N(\delta)$ l'entier donné par le théorème de Roth associé à la densité δ, la relation suivante est vérifiée :
$N_0 = N(\delta) \leq C\left(\frac{1}{c\delta}\right)^C \leq C\left(\frac{1}{c}\right)^C M_0^C \leq DN(\delta + c\delta)^C$ pour une autre constante D.

L'argument donné plus haut pour montrer que $P(\delta)$ est vrai lorsque $\delta > 2/3$ nous apprend également que si $\delta > 3/4$, $N(\delta) \leq 9$.

Soit maintenant $\delta \in]0, 1[$. Le nombre minimal de pas de longueur $c\delta$ nécessaire pour joindre δ à un réel de [3/4,1] s'écrit $m = \lfloor \frac{3/4-\delta}{c\delta} \rfloor + 1 \leq \frac{1}{c\delta} + 2$. On peut ainsi obtenir une

majoration, en fonction de δ uniquement, de l'entier $N(\delta)$:

$$\begin{aligned} N(\delta) \leq DN(\delta + c\delta)^D &\leq DD^D N(\delta + 2c\delta)^{D^2} \\ &\leq \dots \\ &\leq DD^D \dots D^{D^{m-1}} N(\delta + mc\delta)^{D^m} \\ &\leq 9^{D^m} \exp\left[\ln(D)\frac{D^m - 1}{D-1}\right] \\ &\leq \exp\left[\left(\frac{\ln(D)}{D-1} + \ln(9)\right)\exp\left(\ln(D)(\frac{1}{c\delta} + 2)\right)\right] \\ &\leq \exp(\exp(\frac{E}{\delta})) \end{aligned}$$

pour une nouvelle constante E indépendante de δ. En notant $\delta(N)$ la densité minimale que doit avoir une partie de $\{1, \dots, N\}$ pour que le théorème de Roth certifie qu'elle contienne une progression arithmétique de longueur 3, cela se réécrit de la manière suivante :

$$\delta(N) \leq \frac{E}{\ln(\ln(N))}$$

D'où la reformulation suivante :

Théorème 5.1.1 (Roth)**.** *Soit $N \in \mathbb{N}$. Il existe une constante positive E telle que pour toute partie $A \subset \{1, \cdots, N\}$ de densité supérieure à $\frac{E}{\ln(\ln(N))}$, A contient une progression arithmétique de longueur 3.*

Ce résultat est certes puissant, mais encore très loin de la minoration supposée optimale en $\delta(N) \sim \frac{1}{\ln(N)}$. Ce problème est, nous l'avons vu, toujours ouvert...

5.2 Minoration de la densité critique

Rappelons la notation Ω.

Définition 5.2.1. *Soit f et g deux fonctions de $\mathbb{N}$ dans $\mathbb{R}_+$. Nous noterons ici :*

$$f(n) = \underset{n\to\infty}{\Omega}(g(n))$$

Si il existe $M \in \mathbb{N}$ et $C \in \mathbb{R}_+^*$ tels que :

$$\forall n \geq M, |f(n)| \geq C|g(n)|$$

5.3 Un premier exemple

Une première minoration très grossière de la densité critique peut être obtenue comme suit. Malgré le fait qu'elle est très loin de la densité critique conjecturée, elle permet assez simplement de décoller de la borne triviale en $\frac{C}{n}$ (qui revient à considérer un ensemble sans progression arithmétique de cardinal constant).

Proposition 5.3.1. *Avec les notations introduites :*

$$\delta_N^{cri} = \Omega\left(\frac{1}{n^{1-\frac{ln(2)}{ln(3)}}}\right)$$

Démonstration. Tout d'abord remarquons qu'un ensemble sans suite arithmétique de longueur 3 correspond à un ensemble dans lequel aucun point n'est le milieu du segment formé par deux autre point. Nous allons donc considérer des ensembles de la forme

$$A_n = \{k \in [\![0, 3^n - 1]\!] \text{tel que k ne comporte aucun 1 dans son écriture en base 3}\}$$

. Il s'agit d'une version discrète de l'ensemble triadique de Cantor. Montrons d'abord que le milieu de deux points de A_n n'est pas dans A_n. Soit $x, y \in A_n$ tels que $x \neq y$, on note $x = \overline{x_1 x_2 ... x_n}_{(3)}$ et $y = \overline{y_1 y_2 ... y_n}_{(3)}$ les écritures en base 3 de ces nombres (avec éventuellement des zéros au début). Notons i_0 le premier indice où les développements diffèrent. Quitte à échanger x et y, $x_{i_0} = 0$ et $y_{i_0} = 2$. La somme des chiffres d'indice inférieur à i_0 est divisible par 2 donc dans le calcul $m = \frac{x+y}{2}$, le chiffre d'indice i_0 est $\frac{0+2}{2} = 1$. Ainsi soit $m \notin \mathbb{N}$, soit m possède un 1 dans son écriture en base 3. Dans les deux cas, $m \notin A_n$.

Démontrons maintenant que les ensembles A_n permettent d'obtenir la borne annoncée. Posons $M = 3^n - 1$, $card(A_n) = 2^n$, donc la densité de A_n dans $[\![0, M]\!]$ est $(\frac{2}{3})^n$. Ce qui se réexprime en fonction de $N = M + 1$ (cardinal de $[\![0, M]\!]$) en

$$\left(\frac{2}{3}\right)^{\frac{ln(N)}{ln(3)}} = N^{\frac{ln(2)}{ln(3)}-1}$$

Pour un N quelconque, encadrons le entre deux puissances de 3 consécutives : $3^k \leq N < 3^{k+1}$ de façon à avoir $k = \lfloor log_3(N) \rfloor$. L'ensemble A_k est inclus dans $[\![0, N-1]\!]$ de densité

$$\delta_N = \frac{2^k}{N} \geq \frac{2^{\lfloor log_3(N) \rfloor}}{3^{log_3(N)}}$$

Finalement, en utilisant $log_3(N) - 1 \leq \lfloor log_3(N) \rfloor$, on aboutit à la minoration :

$$\delta_N \geq \frac{1}{2}\left(\frac{2}{3}\right)^{log_3(N)} = \frac{N^{log_3(2)-1}}{2}$$

Cela suffit pour conclure. □

5.4 L'exemple de Behrend

Nous allons ici prouver la meilleure minoration suivante.

Théorème 5.4.1. *Il existe $C > 0$ une constante telle que* $\delta_N^{cri} = \Omega\left(\exp(-C\sqrt{log(N)})\right)$

Démonstration. Soit $d \in \mathbb{N}$, on se place dans $\mathbb{R}^d$ et on considère la sphère $S_r = \{x \in \mathbb{R}^d : |x| = r\}$. D'après l'identité du parallélogramme, si $x, y \in S_r$ et sont dinstincts, on a l'égalité :

$$|x+y|^2 + |x-y|^2 = 2(|x|^2 + |y|^2)$$

d'où

$$|\frac{x+y}{2}| = \sqrt{r^2 - |\frac{x-y}{2}|^2} < r$$

Finalement, le milieu de deux points distincts sur la sphère n'est pas sur la sphère. Cette propriété reste vraie si on considère un sous-ensemble de la sphère (dans la suite on considérera des points à coordonnées entières). Considérons un rayon $r \in \mathbb{N}$, nous pouvons définir

$$S_{n,d,r} = \{(x_1, ..., x_d) \in [\![1, n]\!]^d : x_1^2 + x_2^2 + ... + x_d^2 = r^2\}$$

En tant que sous-ensemble de la sphère de rayon r, $S_{n,d,r}$ ne contient aucune progression arithmétique à trois termes. On a de plus $[\![1, n]\!]^d \subset \bigcup_{r^2=d}^{dn^2} S_{n,d,r}$. Donc par le principe des tiroirs, il existe $r \in [\![d, dn^2]\!]$ tel que $|S_{n,d,r}| \geq \frac{n^d}{dn^2-d} \geq \frac{n^d}{dn^2}$. On peut maintenant ramener cet ensemble dans Z par l'isomorphisme de Freimann d'ordre 2 suivant :

$$\varphi : \begin{cases} [\![1, n]\!]^d \to [\![\frac{(2n)^d-1}{2n-1}, n\frac{(2n)^d-1}{2n-1}]\!] \\ (x_1, ..., x_d) \mapsto \sum_{j=1}^{d} x_j (2n)^{j-1} \end{cases}$$

Par translation, on se ramène à un sous-ensemble $A = \varphi(S_{n,d,r}) - \frac{(2n)^d-1}{2n-1} + 1$ de $[\![1, (n-1)\frac{(2n)^d-1}{2n-1} + 1]\!]$. Commme la borne supérieure de l'intervalle est équivalente à $2^{d-1}n^d$ quand n tend vers l'infini, si $N \geq 2^d n^d$ pour n assez grand, alors $A \subset [\![1, N]\!]$.

Pour $N \in \mathbb{N}$, posons $d = \left\lfloor \sqrt{ln(N)} \right\rfloor$ et $n = \left\lfloor \frac{1}{2} N^{\frac{1}{d}} \right\rfloor$ (de cette façon, on a bien $N \geq 2^d n^d$). Avec ce choix, $n \xrightarrow[N\to\infty]{} \infty$. Donc en choisissant N assez grand, la construction précédente donne un ensemble $A \subset [\![1, N]\!]$. De plus on a les inégalités suivantes :

$$\begin{aligned} |A| &\geq \frac{n^d}{dn^2} \\ &\geq \left(\frac{1}{2}N^{\frac{1}{d}} - 1\right)^d \exp\left(-\frac{2}{d}\ln(N) - \ln(d)\right) \end{aligned}$$

Or

$$d\ln\left(\frac{1}{2}N^{\frac{1}{d}} - 1\right) = d\ln\left(\frac{1}{2}N^{\frac{1}{d}}\right) + d\ln\left(1 - \frac{2}{N^{\frac{1}{d}}}\right)$$

et

$$d\ln\left(1 - \frac{2}{N^{\frac{1}{d}}}\right) \sim -\frac{2\sqrt{\ln(N)}}{\exp\left(\frac{\ln(N)}{d}\right)}$$

donc tend vers 0 quand N tend vers l'infini. Finalement, nous avons donc :

$$\left(\frac{1}{2}N^{\frac{1}{d}}-1\right)^d \exp\left(-\frac{2}{d}\ln(N)-\ln(d)right)\right) \sim N\exp\left(-d\ln(2)-\frac{2}{d}\ln(N)-\ln(d)\right)$$

Fixons $\lambda > 1$, pour N assez grand, l'équivalent précédent donne :

$$|A| \geq \lambda N \exp\left(-d\ln(2)-\frac{2}{d}\ln(N)-\ln(d)\right)$$

Sachant que $\sqrt{\ln(N)}-1 \leq d \leq \sqrt{\ln(N)}$, nous obtenons :

$$|A| \geq \lambda N \exp\left(-\sqrt{\ln(N)}\ln(2)-\frac{2}{\sqrt{\ln(N)}-1}\ln(N)-\ln\ln(N)\right)$$

Or nous avons l'équivalence suivante :

$$-\sqrt{\ln(N)}\ln(2)-\frac{2}{\sqrt{\ln(N)}-1}\ln(N)-\ln\ln(N) \sim -(\ln(2)+2)\sqrt{\ln(N)}$$

Donc pour tout $\epsilon > 0$, pour N assez grand :

$$|A| \geq \lambda N \exp\left(-(\ln(2)+2+\epsilon)\sqrt{\ln(N)}\right)$$

Nous avons donc démontré :

$$\forall \lambda > 1, \forall \epsilon > 0, \exists N_{\epsilon,\lambda} : N \geq N_{\epsilon,\lambda} \Rightarrow \delta_N^{cri} \geq \lambda \exp\left(-(\ln(2)+2+\epsilon)\sqrt{\ln(N)}\right)$$

ce qui montre en particulier (version explicite de la proposition) :

$$\forall \epsilon > 0, \delta_N^{cri} = \Omega\left(\exp\left(-(\ln(2)+2+\epsilon)\sqrt{\ln(N)}\right)\right)$$

□

Pour comparaison, pour $N = 10^9$ par exemple, $\frac{1}{\ln(\ln(N))} \simeq 0,33$ tandis que la borne obtenue par Bourgain mentionnée plus haut donne $\frac{\sqrt{\ln(\ln(N))}}{\sqrt{\ln(N)}} \simeq 0,38$ et que $\frac{1}{\ln(N)} \simeq 0,05$. Pour avoir un ordre de grandeur de la borne obtenue grâce à l'exemple de Behrend, on peut calculer le nombre suivant : $\exp\left(-(\ln(2)+2)\sqrt{\ln(10^9)}\right) = 4,7 \times 10^{-6}$ ce qui est très en dessous de la borne inférieure conjecturée !
Pour $N = 10^{100}$, on a cette fois : $\frac{1}{\ln(\ln(N))} \simeq 0,18$, $\frac{\sqrt{\ln(\ln(N))}}{\sqrt{\ln(N)}} \simeq 0,15$ et $\frac{1}{\ln(N)} \simeq 0,004$. L'exemple de Behrend donne une borne de l'ordre de $1,8 \times 10^{-18}$!
Après avoir étudié la présence de progressions arithmétiques dans des parties finies de $\mathbb{N}$, nous revenons à l'estimation de la taille de parties de $A \times B$ en fonction de la structure additive que l'on peut observer dans $A \times B$.

6 Théorème de Balog-Szemerédi

6.1 Introduction

Dans cette partie, on désignera par Z un groupe additif, et A et B deux parties finies de Z.
Nous nous intéresserons au problème suivant : si l'on se donne A et B de taille semblable (de l'ordre de N) et si l'on suppose qu'une grosse partie G de $A \times B$ ($\sim N^2$) présente un ensemble de différences $\{a-b, (a,b) \in G\}$ de petite taille ($\sim N$), peut-on affirmer que $A - B$ dans son ensemble est de petite taille ($\sim N$) ? Il se trouve que la réponse est négative, car les éléments de $A \times B$ qui ne sont pas dans G peuvent créer un nombre important de différences différentes :

Exemple. Soit $A = [\![1, N]\!] \cup \{2N + 2^k, k \in [\![0, N-1]\!]\}$, $B = -A$ et $G = [\![1, N]\!] \times [\![-N, -1]\!] \subset A \times B$. Alors $|\{a-b, (a,b) \in G\}| \leq 2N$ et pourtant $|A - B| \geq \frac{N^2}{2}$.

Cependant, au lieu de chercher à étendre la propriété sur la différence de G à tout $A \times B$, on pourrait tenter de retirer les éléments gênants qui créent beaucoup de nouvelles différences (les $2N + 2^k$ dans l'exemple précédent. Ainsi, nous pourrions peut-être obtenir $A' \subsetneq A$ et $B' \subsetneq B$ ($|A'| \sim |B'| \sim N$) tels que $A' - B'$ soit de petite taille (de l'ordre de N). Cette question est intéressante car rien ne dit que G, même s'il est de grande taille dans $A \times B$, contienne un gros produit cartésien $A' \times B'$:

Exemple. Soit $N \geq 1$, $A = B = [\![1, N]\!]$. Alors il existe $G \subset A \times B$ avec $|G| \geq \frac{N^2}{2}$ et tel que si $A' \times B' \subset G$, $|A'||B'| \leq N$. De plus, comme $|A - B| = 2N - 1$, $\{a-b, (a,b) \in G\}$ est de l'ordre de N.
En effet, construisons G de manière aléatoire : chaque paire $(a,b) \in A \times B$ appartient à G avec probabilité $\frac{1}{2}$ et ce de façon indépendante.
Si l'on se donne $A' \subset A$, $B' \subset B$, alors on a :

$$\mathbb{P}(A' \times B' \subset G) = 2^{-|A'||B'|}$$

Notons $F = \{A' \times B' \subset G, |A'||B'| > N\}$.
Par linéarité de l'espérance :

$$\begin{aligned}
\mathbb{E}(|F|) = \sum_{|A'||B'|>N} \mathbb{P}(A' \times B' \subset G) = \sum_{k=1}^{N} \sum_{j=\lfloor \frac{N}{k} \rfloor + 1}^{N} 2^{-kj} &\leq \sum_{k=1}^{N} (N - \left\lfloor \frac{N}{k} \right\rfloor) 2^{-k(\lfloor \frac{N}{k} \rfloor + 1)} \\
&\leq \sum_{k=1}^{N} (N-1) 2^{-N} \\
&\leq N(N-1) 2^{-N}
\end{aligned}$$

Par conséquent, $\mathbb{P}(|F| = 0) = 1 - \mathbb{P}(|F| \geq 1) \geq 1 - N(N-1)2^{-N}$.
Montrons que $\mathbb{P}(|G| \geq \frac{N^2}{2} \cap |F| = 0) > 0$ dès que N est assez grand.

Étudions d'abord $\mathbb{P}(|G| \geq \frac{N^2}{2})$:

$$\mathbb{P}(|G| \geq \frac{N^2}{2}) = \sum_{k=\left\lceil \frac{N^2}{2} \right\rceil}^{N^2} \binom{N^2}{k} 2^{-N^2} \geq \frac{1}{2} \sum_{k=0}^{N^2} \binom{N^2}{k} 2^{-N^2} = \frac{1}{2}$$

Finalement, il vient :

$$\mathbb{P}(|G| \geq \frac{N^2}{2} \cap |F| = 0) \geq \frac{1}{2} + (1 - N(N-1)2^{-N}) - 1 = \frac{2^{N-1} - N(N-1)}{2^N} > 0 \text{ pour } N \geq 6$$

On en conclut donc l'existence du G recherché.

Cependant, même s'il n'est donc pas possible d'extraire un produit cartésien de G, on peut obtenir $A' \subsetneq A$ et $B' \subsetneq B$ avec $|A' - B'| \sim N$. C'est l'objet du théorème de Balog-Szemerédi :

Théorème 6.1.1 (Balog-Szemerédi)**.**
Soient $K, K' > 1$, A et B deux parties d'un groupe additif Z, avec $|A| \geq 32K^2$.
Supposons qu'il existe $G \subseteq A \times B$ avec $|G| \geq |A||B|/K$, tel que $|\{a - b, (a, b) \in G\}| \leq K'\sqrt{|A||B|}$.
Alors on peut trouver des sous-ensembles A' et B' de A et B respectivement tels que :
$\begin{cases} |A'| \geq \frac{|A|}{256K^3} \\ |B'| \geq \frac{|B|}{64K^2} \\ |A' - B'| \leq 2^{32} K^{13} K'^3 \sqrt{|A||B|} \end{cases}$

Remarque 6.1.2. On remarque que les constantes (par rapport à $|A|, |B|$) obtenues dans les inégalités sont polynomiales en K, K'.

6.1.1 Preuve du théorème

Fixons N, K, K', A, B et G respectant les hypothèses du théorème de Balog-Szemerédi.
Tout d'abord, il faut remarquer que A et B peuvent être supposés distincts, quitte à remplacer Z par $Z \times \mathbb{Z}/2\mathbb{Z}$, A par $A \times \{0\}$ et B par $B \times \{1\}$. On supposera donc A et B distincts par la suite.
Le lemme suivant sera utilisé à plusieurs reprises dans la preuve du théorème :

Lemme 6.1.3 (Lemme de popularité)**.**
On reprend les notations du lemme précédent et on se donne $\alpha \in]0, 1[$.
On dit qu'un élément y de Y est populaire dès lors que

$$\left|f^{-1}(\{y\})\right| = |\{x \in X, f(x) = y\}| \geq \alpha \frac{|X|}{|Y|}$$

Alors

$$|\{x \in X, f(x) \textit{est populaire}\}| \geq (1 - \alpha)|X|$$

Démonstration. On a :

$$|\{x \in X, f(x) \text{ n'est pas populaire}\}| = \sum_{y \text{ impopulaire}} \left|f^{-1}(\{y\})\right| < \alpha|Y|\frac{|X|}{|Y|} = \alpha|X|$$

Par passage au complémentaire, on obtient l'inégalité désirée. □

Même si l'on ne peut pas construire directement les ensembles A' et B' à partir des éléments de G, il paraît naturel que ceux-ci vont jouer un rôle crucial dans la construction de A' et B'. C'est pourquoi nous allons introduire quelques relations entre les éléments de A et B correspondant à leurs liaisons dans $A - B$, afin d'obtenir plus d'informations sur les liaisons que G entretient avec les autres éléments de $A \times B$:

Définition 6.1.4. *Si $a \in A$, $b \in B$, on dit que la différence $a - b$ est populaire lorsque l'on a :*

$$|\{(a', b') \in A \times B, a' - b' = a - b\}| \geq \frac{\sqrt{|A||B|}}{2KK'}.$$

On notera indifféremment $a \sim b$ ou $b \sim a$ (il n'y a pas d'ambiguïté car A et B sont distincts) et on dira que a et b sont amis lorsque la différence $a - b$ est populaire.
Soient ϵ et β deux réels de $]0, 1[$. On définit deux autres relations :

$$\begin{aligned} \text{Pour } b, b' \in B,\ b \sim\sim b' &\Leftrightarrow b' \sim\sim b &&\Leftrightarrow |\{a \in A, b \sim a \sim b'\}| \geq \epsilon|A|. \\ \text{Pour } a \in A,\ b \in B,\ a \sim\sim\sim b &\Leftrightarrow b \sim\sim\sim a &&\Leftrightarrow |\{b' \in B, a \sim b' \sim\sim b\}| \geq \beta|B|. \end{aligned}$$

On dira que b et b' se connaissent lorsque $b \sim\sim b'$ et que a et b communiquent lorsque $a \sim\sim\sim b$.

Remarque 6.1.5. • La seule relation d'amitié entre a et b est trop forte pour que l'on puisse obtenir des parties A' et B' de grande taille (comme vu dans les exemples précédents), c'est pourquoi on introduit un second degré de relation entre a et b, la communication.
• On utilise les variables ϵ et β car un choix direct de ces variables ne nous assure pas d'obtenir le résultat escompté à l'issue du raisonnement. On aurait aussi pu introduire un autre paramètre α dans la définition de la popularité ($|\{(a', b') \in A \times B, a' - b' = a - b\}| \geq \alpha N$) mais nous avons décidé de ne pas trop utiliser de paramètres afin de ne pas surcharger la preuve. Cependant, un choix optimal de tous ces paramètres (d'autres seront évoqués au cours de la preuve) permettrait de donner les constantes optimales associées au schéma de preuve suivi.

G ayant la propriété d'avoir son ensemble de différences de petite taille, il devrait donc contenir beaucoup de couples amis. En effet, en notant $\pi : (a, b) \mapsto a - b$ l'opérateur

de différence :

$$|\{(a,b) \in G, a \text{ et } b \text{ ne sont pas amis}\}| = \sum_{\substack{y \in \pi(G) \\ y \text{ impopulaire}}} \left|\pi^{-1}(\{y\})\right| < |\pi(G)| \frac{\sqrt{|A||B|}}{2KK'}$$

$$\leq K' \sqrt{|A||B|} \frac{\sqrt{|A||B|}}{2KK'}$$

$$= \frac{|A||B|}{2K}$$

On se rend alors compte que $A \times B$ contient de l'ordre de $|A||B|$ amis :

$$|\{(a,b) \in A \times B, a \text{ et } b \text{ sont amis}\}| \geq |\{(a,b) \in G, a \text{ et } b \text{ sont amis}\}|$$

$$= |G| - |\{(a,b) \in G, a \text{ et } b \text{ ne sont pas amis}\}|$$

$$\geq \frac{|A||B|}{K} - \frac{|A||B|}{2K}$$

$$= \frac{|A||B|}{2K}$$

On définit le sous-ensemble B_1 de B en ne prenant que les éléments de B qui ont beaucoup d'amis dans A :

$$b \in B_1 \Leftrightarrow |\{a \in A, a \sim b\}| \geq \frac{|A|}{4K}.$$

Là encore, on a choisi arbitrairement notre définition du fait d'avoir beaucoup d'amis, que l'on aurait également pu paramétrer.
Beaucoup d'éléments de $A \times B$ sont des couples amis, donc le nombre d'éléments de B qui sont amis avec peu d'éléments de A est faible. C'est exactement ce que dit la proposition suivante : B_1 est de la taille de B :

Proposition 6.1.6. *On a :*

$$|\{(a,b) \in A \times B_1, a \sim b\}| \geq \frac{|A||B|}{4K}$$

En particulier, $|B_1| \geq \frac{|B|}{4K}$

Démonstration. En effet :

$$|\{(a,b) \in A \times B \backslash B_1, a \sim b\}| \leq (|B| - |B_1|).\frac{|A|}{4K} \leq \frac{|A||B|}{4K}$$

Or :

$$|\{(a,b) \in A \times B, a \sim b\}| \geq \frac{|A||B|}{2K}$$

D'où le résultat. □

Soit $a \in A$, on définit $B_2 = B_2(a) = \{b \in B_1, b \sim a\}$ l'ensemble des amis de a qui sont dans B_1.
Alors, comme les éléments de B_1 ont un nombre important d'amis dans A, au moins certains $B_2(a)$ doivent être de taille importante. On peut même trouver un $B_2(a_0)$ qui contient beaucoup d'éléments qui se connaissent :

Proposition 6.1.7. *On a les inégalités suivantes :*

$$\sum_{a\in A} |B_2(a)| \geq \frac{|A||B|}{16K^2}$$

$$\sum_{a\in A} |\{(b,b') \in B_2(a)^2, b \nsim b'\}| \leq \epsilon |A||B|^2$$

Démonstration. Il suffit de modifier l'indexation des sommes :

$$\sum_{a\in A} |B_2(a)| = \sum_{a\in A} \sum_{\substack{b\in B_1 \\ b\sim a}} 1 = \sum_{b\in B_1} \sum_{\substack{a\in A \\ a\sim b}} 1 \geq |B_1| \frac{|A|}{4K} \geq \frac{|A||B|}{16K^2}$$

$$\sum_{a\in A} |\{(b,b') \in B_2(a)^2, b \nsim b'\}| = \sum_{\substack{(b,b')\in B_1 \\ b\nsim b'}} |\{a \in A, b \sim a \sim b'\}| \leq \epsilon |A|.|B_1|^2 \leq \epsilon |A||B|^2$$

□

Il est désormais possible de construire le a_0 recherché.

Corollaire 6.1.8.
Dès lors que $|A| \geq 32K^2$, *il existe* $a_0 \in A$ *tel que :*
$\begin{cases} |B_2(a_0)| \geq \frac{|B|}{32K^2} \\ |\{(b,b') \in B_2(a_0), b \nsim b'\}| \leq 32K^2 \epsilon |B|^2 \end{cases}$

Démonstration. Notons A_1 l'ensemble défini par :

$$A_1 = \{a \in A, |B_2(a)| \geq \frac{|B|}{32K^2}\}$$

Ainsi, on cherche un élément a_0 de A_1 tel que $B_2(a_0)$ contienne un nombre assez important d'éléments se connaissant.
On a l'inégalité, de manière similaire au lemme de popularité :

$$\frac{|A||B|}{16K^2} \leq \sum_{a\in A} |B_2(a)| = \sum_{a\in A_1} |B_2(a)| + \sum_{a\notin A_1} |B_2(a)| \leq |A_1||B| + |A| \frac{|B|}{32K^2}$$

On peut alors en déduire que A_1 est de taille comparable à A :

$$|A_1| \geq \frac{|A|}{16K^2} - \frac{|A|}{32K^2} = \frac{|A|}{32K^2}$$

Par ailleurs :

$$\sum_{a\in A_1} |\{(b,b')\in B_2(a)^2, b\nsim\nsim b'\}| \leq \sum_{a\in A} |\{(b,b')\in B_2(a)^2, b\nsim\nsim b'\}| \leq \epsilon|A||B|^2$$

Donc il existe $a_0 \in A_1$ tel que :

$$|\{(b,b')\in B_2(a)^2, b\nsim\nsim b'\}| \leq \frac{\epsilon|A||B|^2}{|A_1|} \leq 32K^2\epsilon|B|^2$$

□

Désormais, nous appelerons B_2 le sous-ensemble $B_2(a_0)$ construit dans le corollaire. Avec tous les objets introduits, nous sommes enfin en mesure de définir les sous-ensembles A' et B' intervenant dans le théorème de Balog-Szemerédi. Pour obtenir B', il suffit d'éliminer les éléments de B_2 qui ne connaissent que peu d'éléments dans B_2 et pour A', on ne conserve que les éléments de A qui sont amis avec une bonne partie de B_2. On pourra alors montrer que tous les éléments de A' et B' communiquent. Il suffira alors d'observer que A' et B' sont de taille équivalente à A et B et que l'ensemble des différences $\{a-b, a\sim\sim\sim b\}$ est de taille similaire à $\sqrt{|A||B|}$:

Définition 6.1.9. *Soit $\lambda \in]0,1[$ un paramètre fixé à la fin de la preuve.*
On note : $\begin{cases} A' = \{a\in A, |\{b\in B_2, a\sim b\}| \geq \frac{|B|}{256K^3}\} \\ B' = \{b\in B_2, |\{b'\in B_2, b\nsim\nsim b'\}| \leq \lambda|B|\} \end{cases}$

Montrons déjà que A' et A sont de taille comparable. Déjà :

$$\sum_{b\in B_2} |\{a\in A, a\sim b\}| \geq |B_2|\frac{|A|}{4K} \geq \frac{|A||B|}{128K^3}$$

Donc :

$$\frac{|A||B|}{128K^3} \leq \sum_{a\in A'} |\{b\in B_2, b\sim a\}| + \sum_{a\notin A'} |\{b\in B_2, b\sim a\}| \leq |A'||B| + |A|\frac{|B|}{256K^3}$$

Ainsi :

$$|A'| \geq \frac{|A|}{256K^3}$$

Pour minorer $|B'|$, on utilise le lemme de popularité :

$$|B_2\backslash B'| \leq \frac{32K^2\epsilon|B|^2}{\lambda|B|} \leq 32K^2\frac{\epsilon}{\lambda}|B|$$

D'où, en passant au complémentaire :

$$|B'| \geq |B_2| - 32K^2\frac{\epsilon}{\lambda}|B| \geq (\frac{1}{32K^2} - 32K^2\frac{\epsilon}{\lambda})|B|$$

Désormais, on montre que l'ensemble des différences des éléments qui communiquent est de taille $\sim \sqrt{|A||B|}$. Notons $D = \{a - b, a \sim b\}$, D est de petite taille par le lemme de popularité :

$$|D| \leq \frac{|A||B|}{\frac{\sqrt{|A||B|}}{2KK'}} = 2KK'\sqrt{|A||B|}$$

Soit $E = \{a - b, a \sim\sim\sim b\}$ l'ensemble des éléments qui communiquent.

Lemme 6.1.10.

$$|E| \leq \frac{8K^3K'^3}{\epsilon\beta}\sqrt{|A||B|}$$

Démonstration. Considérons $a \in A,\ b \in B$ avec $a \sim\sim\sim b$.
Par hypothèse, il existe au moins $\epsilon\beta|A||B|$ paires $(a', b') \in A \times B$ telles que $a \sim b' \sim a' \sim b$.
Or :

$$a - b = (a - b') - (a' - b') + (a' - b)$$

Chaque couple (a', b') correspond à un unique triplet $(d_1, d_2, d_3) = (a - b', a' - b', a' - b) \in D^3$.
Ainsi, il y a au moins $\epsilon\beta|A||B|$ solutions distinctes à l'équation $a - b = d_1 - d_2 + d_3$ dans D^3.
Il vient donc :

$$|E| \leq \frac{|D^3|}{\epsilon\beta|A||B|} = \frac{8K^3K'^3|A||B|^{\frac{3}{2}}}{\epsilon\beta|A||B|} = \frac{8K^3K'^3}{\epsilon\beta}\sqrt{|A||B|}$$

□

Il suffit désormais choisir les constantes ϵ, β et λ afin que $A' - B' \subseteq E$ et le théorème sera prouvé.
Fixons $a \in A'$ et $b \in B'$. Montrons que $a \sim\sim\sim b$ si l'on choisit bien les 3 paramètres précédents.
On a :

$$\begin{cases} |\{b' \in B_2, a \sim b'\}| \geq \frac{|B|}{256K^3} \\ |\{b' \in B_2, b \sim\sim b'\}| \geq |B_2| - \lambda|B| \end{cases}$$

On en déduit que :

$$|\{b' \in B_2, a \sim b' \sim\sim b\}| \geq \frac{|B|}{256K^3} + (|B_2| - \lambda|B|) - |B_2| = \frac{|B|}{256K^3} - \lambda|B|$$

Pour que $a \sim\sim\sim b$, il suffit donc que $\lambda + \beta \leq \frac{1}{256K^3}$.
En outre, il faut que $|B'|$ soit de l'ordre de $|B|$, cela impose :

$$\frac{\epsilon}{\lambda} < \frac{1}{32K^2}^2$$

Choisissons $\lambda = \beta = \frac{1}{512K^3}$ et $\epsilon = \frac{1}{2^{20}K^7}$
Finalement, $A' - B' \subseteq E$ et donc, par le lemme et les inégalités démontrées précédemment :
$\begin{cases} |A'| \geq \frac{|A|}{256K^3} \\ |B'| \geq \frac{|B|}{64K^2} \\ |A' - B'| \leq 2^{32}K^{13}K'^3\sqrt{|A||B|} \end{cases}$

6.2 Variantes du théorème

La forme précédente du théorème est peu pratique à utiliser du fait de la présence des constantes. On note donc précisément $\overset{K}{\gtrsim}$ la relation suivante :

$$x \overset{K}{\gtrsim} y \Leftrightarrow \text{ Il existe des constantes } c, c' > 0 \text{ telles que } cK^{c'}x \geq y$$

De manière symétrique, on définit aussi la relation $\overset{K}{\lesssim}$. On peut donner quelques propriétés sur ces relations d'ordre :

Proposition 6.2.1.
$\rightarrow \ \forall \alpha > 0, x \overset{K}{\lesssim} y \Leftrightarrow x \overset{K^\alpha}{\lesssim} y$
$\rightarrow \ x \overset{K}{\lesssim} y \overset{K'}{\lesssim} z \Rightarrow x \overset{KK'}{\lesssim} z$

Le théorème de Balog-Szemerédi se reformule alors comme suit :

Proposition 6.2.2. *Si $G \subseteq A \times B$ avec $|G| \overset{K}{\gtrsim} |A \times B|$, tel que $|\{a - b, (a, b) \in G\}| \overset{K'}{\lesssim} \sqrt{|A \times B|}$.*
Alors il existe des parties A' et B' de A et B respectivement telles que :
$\begin{cases} |A'| \overset{K}{\gtrsim} |A| \\ |B'| \overset{K}{\gtrsim} |B| \\ |A' - B'| \overset{KK'}{\lesssim} \sqrt{|A \times B|} \end{cases}$

Il existe également une version légèrement différente du théorème de Balog-Szemerédi, proposée par Bourgain. Sa preuve utilise des techniques assez proches de celles présentes dans la section précédente. Nous allons, en vue d'énoncer ce théorème, désigner par les notations $< x^{\alpha+}$; $> x^{\alpha-}$ les relations $< C_\epsilon x^{\alpha+\epsilon}$ pour tout $\epsilon > 0$; $> c_\epsilon x^{\alpha-\epsilon}$ pour tout $\epsilon > 0$, où les C_ϵ, c_ϵ sont des constantes dépendant exclusivement de ϵ.

Théorème 6.2.3. *Soit $N \in \mathbb{N}^*, K > 1$ et $A, B \subset Z$ avec $|A|, |B| \leq N$.*
Supposons qu'il existe $H \subseteq A \times B$ avec $|H| \geq N^2/K$, tel que $|\{a + b, (a, b) \in H\}| \leq N$.
Alors on peut trouver des sous-ensembles A' et B' de A et B tels que, pour tout :
$\begin{cases} |H \cap (A' \times B')| > K^{-9}N^{2-} \\ |A' - B'| < N^{-1+}K^{13}|H \cap (A' \times B')| \end{cases}$

Remarque 6.2.4. Les parties A' et B' du théorème précédent dépendent de ϵ, comme le montre la preuve donnée par Bourgain.

Ces théorèmes permettent d'étudier des ensembles à structure additive, on va en donner un exemple d'utilisation pour la conjecture de Kakeya pour les corps finis. Bourgain a appliqué lui-même son théorème à cette conjecture dans $\mathbb{R}^d$ dans [**?**].

6.3 Application aux ensembles de Besicovitch

On se place dans l'espace vectoriel F^n où F est le corps fini $\mathbb{Z}/p\mathbb{Z}$ (p premier) et $n \geq 2$.

Définition 6.3.1. *On appelle ligne de F^n de direction $v \in F^n \backslash \{0\}$ tout ensemble du type $l = \{x + tv, t \in F\}$, où $x \in F^n$.*
Un sous-ensemble E de F^n qui contient une ligne dans chaque direction est dit de Besicovitch. L'ensemble des des ensembles de Besicovitch de F^n sera noté $\mathfrak{B}_n(F)$.

Par exemple, F^n est un ensemble de Besicovitch.

Remarque 6.3.2. En réalité, les ensembles de Besicovitch sont plus étudiés dans des espaces euclidiens (dans $\mathbb{R}^2$, le problème de l'aiguille de Kakeya : existe-t-il des régions du plan aussi petite que l'on veut où l'on peut faire tourner continûment une aiguille de longueur 1 ?).Cette extension aux espaces vectoriels sur des corps finis a été pensée en vue de résoudre des conjectures portant sur le cas euclidien.

On s'intéresse à la taille minimale d'un ensemble de Besicovitch vis-à-vis de celle de F^n. Il semble qu'une partie de F^n doive être de grande taille pour contenir une ligne dans chaque direction, et ainsi être un ensemble de Besicovitch. Dans cette partie, nous allons donner des minorations de la taille d'un ensemble de Besicovitch en fonction de F et de n. On a déjà la minoration élémentaire suivante.

Proposition 6.3.3. *Si $|F| \geq 3$ et $E \in \mathfrak{B}_n(F)$, alors $|E| \geq \frac{|F|^{\frac{n+1}{2}}}{3}$*

Démonstration. On considère les "sections horizontales" E_t de E, pour $t \in F$:

$$E_t = E \cap (\{t\} \times F^{n-1})$$

Par l'inégalité de Markov sur les cardinaux, il vient, comme E est la réunion disjointe des E_t :

$$|\{t \in F, |E_t| \geq 3\frac{|E|}{|F|}\} \leq \frac{|F|}{3}$$

On en déduit donc qu'il y a au moins $2|F|/3 \geq 2$ valeurs de t telles que $|E_t| \leq 3|E|/|F|$que l'on note t et t'.
Par la transformation affine $x \mapsto t'^{-1}(x - t)$, on se ramène au cas $t = 0$, $t' = 1$.
Pour chaque $w \in F^{n-1}$, il existe une ligne de direction $(1, w)$ entièrement contenue dans E. Cette ligne intersecte E_0 et E_1 respectivement en les points $a(w)$ et $b(w)$, qui sont

donc tels que $a(w) - b(w) = (1, w)$.
Ainsi, la fonction $w \mapsto (a(w), b(w))$ est injective, ce qui donne l'inégalité voulue :

$$|F|^{n-1} \leq |E_0||E_1| \leq 9\frac{|E|^2}{|F|^2}$$

□

Ainsi, on a l'estimation $|E| \gtrsim \sqrt{|F|^n}$. Cependant, grâce au théorème de Balog-Szemerédi, il va être possible d'établir des inégalités plus fines.

Proposition 6.3.4. *Si $F \neq \mathbb{Z}/2\mathbb{Z}$, pour tout $\epsilon > 0$, il existe une constante $C_\epsilon > 0$telle que tout ensemble de Besicovitch E de F^n est de cardinal supérieur ou égal à $C_\epsilon |F|^{\frac{13n+12}{25}-\epsilon}$. C_ϵ ne dépend ni de F, ni de n.*

Démonstration. On considère encore les plans horizontaux de la preuve précédente. On cherche a et r tels que $|E_a|, |E_{a+r}|$ et $|E_{a+2r}|$ soient petits.
On a :

$$\sum_{\substack{a\in F\\ r\in F^*}} (|E_a| + |E_{a+r}| + |E_{a+2r}|) = 3(|F| - 1)|E|$$

Donc, par l'inégalité de Markov :

$$|\{(a, r) \in F\times F^*, |E_a|, |E_{a+r}|, |E_{a+2r}| \leq 6\frac{|E|}{|F|}\}| \geq |F|(|F|-1) - \frac{3|F|(|F| - 1)}{6} = \frac{|F|(|F| - 1)}{2} \geq 1$$

On a donc l'existence d'une progression arithmétique $a, a + r, a + 2r$ telle que $|E_a|, |E_{a+r}|, |E_{a+2r}| \leq 6\frac{|E|}{|F|}$.
On effectue la transformation affine $x \mapsto (x - a)(2r)^{-1}$ pour se ramener à $E_0, E_{\frac{1}{2}}, E_1$.
Comme dans la preuve précédente, à chaque direction $(1, w)$, pour $w \in F^{n-1}$, on associe $(a(w), b(w)) \in E_0 \times E_1$, tels que $b(w) - a(w) = (1, w)$ et la ligne passant par $a(w)$ et $b(w)$ est incluse dans E. Alors $\frac{a(w)+b(w)}{2}$ appartient à $E_{\frac{1}{2}}$.
Par conséquent, en notant $H = \{(a(w), b(w)), w \in F^{n-1}$:

$$|\{a + b, (a, b) \in H\}| = |E_{\frac{1}{2}}| \leq 6\frac{|E|}{|F|}$$

Notons $N = 6\frac{|E|}{|F|}K = \frac{N^2}{|F|^{n-1}}$ de sorte que $|H| = \frac{N^2}{K}$. On applique la version de Bourgain du théorème de Balog-Szemerédi : il existe $A' \subset E_0, B' \subset E_1$ tels que :

$$|A' - B'| < K^{13}N^{-1+}|H \cap (A' \times B')| < K^{13}N^{-1+}|A' - B'|$$

La dernière inégalité provient du fait que toutes les différences des éléments des couples de H sont distinctes. Finalement, pour tout $\epsilon > 0$, il existe une constante C_ϵ telle que :

$$|F|^{13n-13} < C_\epsilon N^{25+\epsilon} < 6^{25}C_\epsilon |E|^{25+\epsilon}|F|^{-25-\epsilon}$$

De cette inégalité se déduit le résultat. □

Remarque 6.3.5. On aurait pu montrer qu'il existe une progression arithmétique de longueur 3 $a, a+r, a+2r$ telle que $|E_a|, |E_{a+r}|, |E_{a+2r}| \leq 6|E||F|$ grâce au théorème de Roth : l'ensemble des $t \in F$ tels que $|E_t| \leq 6|E|/|F|$ est de densité au moins 5/6 grâce à l'inégalité de Markov, donc, en identifiant $F = \mathbb{Z}/p\mathbb{Z}$ à $[\![0, p-1]\!] \subset \mathbb{N}$ et en appliquant le théorème de Roth, on obtient la progression arithmétique désirée dès lors que $|F|$ est assez grand.

On a utilisé un troisième plan et le théorème de Balog-Szemerédi pour améliorer la première preuve. Pour tenter d'obtenir une meilleure borne, on pourrait également étudier un nombre de plans plus important, par exemble $E_{\frac{2}{3}}$ si $|F| > 3$, et s'inspirer des techniques employées pour prouver le théorème de Balog-Szemerédi.
Plus encore qu'une minoration en $|F|^{n-\epsilon}$ pour la taille des ensembles de Besicovitch de F^n, il semble même que l'on puisse minorer la taille de ces ensembles par une quantité de l'ordre de $|F|^n$:

Conjecture 6.3.6. *Si $n \in \mathbb{N}^*$, alors il existe une constante $c(n) > 0$ indépendante de F telle que si E est un ensemble de Besicovitch de F^n, on ait l'inégalité :*

$$|E| \geq c(n)|F|^n$$

Remarque 6.3.7. On a certes obtenu, grâce au théorème de Balog-Szemerédi, une minoration d'ordre moins bon que $|F|^n$, mais la constante obtenue par cette méthode ne dépend pas de n, contrairement à la conjecture : il se peut que la constante $c(n)$ soit prépondérante devant le terme $|F|^n$. En fait, Dvir a prouvé, par des arguments utilisant des polynômes, qu'un ensemble de Besicovitch est de taille au moins $|F|^n/n!$, et cette estimation n'est meilleure que celle obtenue dans le lemme 2.4. que lorsque n est assez petit. De récentes améliorations sur la base de la démonstration de Dvir ont permis d'obtenir la borne $(|F|/2)^n$.

7 Conclusion

Nous avons donc vu que les outils de la combinatoire additive s'appliquent à des problèmes variés tels que l'étude combinatoire des ensembles invariants et essentiellement invariants, l'étude des progressions arithmétiques et le problème de Kakeya dans les corps finis. La théorie s'appuie également sur des résultats provenant d'autres domaines tels que la théorie des graphes ou l'analyse de Fourier dans les groupes comme nous l'avons illustré ici dans les démonstrations des théorèmes de Plünnecke, Eleke, Roth et Balog-Szemeredi.

La combinatoire additive reste un domaine de recherche très actif dans lequel il reste de nombreuses questions ouvertes. Un exemple important que nous avons mentionné dans ce mémoire est la conjecture d'Erdös sur les progressions arithmétiques que l'on peut énoncer de la façon suivante.

Conjecture 7.0.8. *Soit $(x_n) \in \mathbb{N}^{\mathbb{N}}$ une suite d'entiers naturels non nuls tels que $\sum_{n=0}^{+\infty} \frac{1}{x_n} = +\infty$. Pour tout $N \in \mathbb{N}$, on peut extraire de (x_n) une suite arithmétique de longueur N.*

Nous avons vu dans la section sur l'analyse de la densité critique que même pour des suites arithmétiques de longueur 3, les résultats actuels sont encore loin de la conjecture. Cependant, le cas particulier des nombres premiers a été résolu en 2004 par Ben Green et Terence Tao.

Théorème 7.0.9 (Green-Tao)**.** *La suite des nombres premiers contient des progressions arithmétiques arbitrairement longues.*