Additive structure of integers

Petru Constantinescu
Supervisor: Martin Liebeck

Abstract

It is easy to see that if $A \subset \mathbb{Z}$, $|A| = n$, then the minimal value of $|A + A|$ is attained exactly when A is an arithmetic progression. A natural question to ask is what we can say about the structure of A if $|A + A|$ is small. We will use discrete Fourier analysis, graph theoretical methods and techniques from geometry of numbers to obtain results about subsets of integers with small sumset, of which Freiman's theorem is the jewel in the crown.

Contents

1 Introduction

We will be mostly concerned about the additive structure of sets. For this reason, it is useful to have the following definitions.

Definition An *additive group* is an abelian group Z with group operation $+$. The identity element will be 0. We can define the multiplication nx, whenever $n \in \mathbb{Z}$ and $x \in Z$ in the natural way. For instance, $2x = x + x$, $-3x = -x - x - x$.

Definition If A, B are subsets of an additive group, we define the *sum set*

$$A + B = \{a + b : a \in A, b \in B\}$$

and the *difference set*

$$A - B = \{a - b : a \in A, b \in B\} \ .$$

It is also useful to define kA, for $k \in \mathbb{Z}$ as

$$kA = \{a_1 + \cdots + a_k : a_1, a_2, \ldots, a_k \in A\} \ .$$

It is important to make the distinction between the sumset kA and $k \cdot A$:

$$k \cdot A = \{ka : a \in A\} \ .$$

It will be clear from the context with which of the above we work.

Let $A \subset \mathbb{Z}$ a finite set of integers, $|A| = n$. We have the trivial bounds

$$2n - 1 \leq |A + A| \leq n(n + 1)/2$$

which can be attained. For the upper bound, take for instance $A = \{1, 10, 10^2, \ldots, 10^{n-1}\}$. The lower bound is attained if and only if A is an arithmetic progression. If we take a large subset A' of an arithmetic progression, we can still obtain that $|A' + A'|$ is comparable to $|A'|$ (for example, if A' is a subset of at least $n/2$ elements of $\{1, 2, \ldots, n\}$, then $|A' + A'| \leq 4|A'|$).

We want to describe the structure of subsets of integers with small sumsets. That is, $|A + A| \leq C|A|$, for some constant C. As we've just seen above, subsets of arithmetic progressions satisfy this property. Freiman's deep theorem describes this kind of subsets. Before we state it, we need another definition.

Definition Given Z an additive group and $a_0, a_1, \ldots, a_d \in Z$, we define a *generalized arithmetic progression (GAP)* a subset P of Z such that

$$P = \left\{ a_0 + \sum_{j=1}^{d} \lambda_j a_j : 0 \leq \lambda_j \leq m_j - 1, \ j = 1, 2, \ldots, d \right\} \ .$$

for some $m_j \in \mathbb{Z}_{>0}$, for all $1 \leq j \leq d$.

We define $d = \dim(P)$ the *dimension* of the GAP and $|P|$ the size of it. If $|P| = m_1 m_2 \ldots m_d$, we say that P is *proper*.

A first easy remark is that if P is a GAP of dimension d, then $P + P$ and $P - P$ are also GAP's of dimension d. Moreover, if P is proper, then $|P + P| \leq 2^d |P|$.

Theorem 1.1 (Freiman) *Let $A \subset \mathbb{Z}$ a finite set of cardinality n and suppose that $|A+A| \leq C|A|$. Then A is a subset of a d-dimensional GAP P such that*

$$d \leq d(C) \tag{1}$$

and

$$|P| \leq K(C)\ n \tag{2}$$

where $d(C)$ and $K(C)$ depend only on C.

The aim of this report is to describe in full detail how we obtain the bounds

$$d(C) \leq \alpha C^2 (\log C)^2$$
$$K(C) \leq \alpha \exp(C^2 (\log C)^2)$$

where α stands for a constant. These are very close to the best bounds currently known.

The method which we will use was first described by Ruzsa [17]. It was greatly improved by Chang [4]. The method relies on results from graph theory, geometry of numbers and of course Fourier analysis. Oversimplifying everything, these are the steps of the proof:

- Under some conditions, we can work in $\mathbb{Z}_N$ instead of $\mathbb{Z}$, for a large enough N
- If $A \subset \mathbb{Z}_N$ has small sumset, then $2A-2A$ contains a large Bohr set (these will be properly described at the right time)
- A Bohr set in $\mathbb{Z}_N$ contains a large GAP as a subset
- If $2A - 2A$ contains a large GAP, then A is contained in some other GAP

Of course, in the following pages, everything will be treated carefully and we will obtain some additional important results. We will return to this proof in section 5, after all the necessary tools have been exposed.

Let $(G, \cdot)$ be a group (possibly non-commutative). Similar to the additive notation, for $A, B \subseteq G$ we can define

$$AB = \{a \cdot b : a \in A, b \in B\}\ .$$

Freiman's fundamental result described above pioneered the recent development of the rich theory of sets with small doubling constant in a general group G ($|A \cdot A|| \leq C|A|$, for some $A \subseteq G$, $|A|$ finite). In 2008, Tao [22] introduced the notion of *approximate groups*, an important topic of research in the last decade. There are several definitions for an approximate group, however the one below is the most standard.

Definition Let G a group and $A \subseteq G$ a finite subset. Then A is a *K-approximate subgroup* of G if

1. A is symmetric: $A = A^{-1} = \{a^{-1} : a \in A\}$;
2. There exists a set $X \subseteq G$ of size K such that $A \cdot A \subseteq X \cdot A$.

Note that the second condition in the definition above is similar to $|A \cdot A| \leq K|A|$. Actually, Balog-Szemerédi-Gowers theorem asserts that these two conditions are "roughly" equivalent. The precise statement and proof of the theorem can be found in [20] or [7] and are beyond the scope of this report.

It is worth to mention a result from 2012 of Breuillard, Green and Tao, which gives a structure theorem for K-approximate groups [2]. This is just an example of how influential the methods and ideas related to Freiman's theorem turned out to be.

2 Discrete Fourier analysis

Fourier analysis is a powerful tool which allows us to find many properties of subsets of finite additive group. The importance of this method is hard to be summarized in a few words. For instance, it led to a proof of Szemerédi's theorem [20] [7] or Green-Tao theorem about arbitrarily long arithmetic progressions of primes [13]. We will only develop the basic theory and adapt it to our needs.

2.1 Basic theory

For the rest of this subsection, let Z be a finite additive group. We shall be careful that Z is different from the set $\mathbb{Z}$ of integers and the notations should not be confused, as both will be used throughout the section.

Definition A *bilinear form* on an additive group Z is a map $(\xi, x) \to \xi \cdot x$ from $Z \times Z$ to $\mathbb{R}/\mathbb{Z}$ such that it is a homomorphism in each of the variables ξ and x:

$$(\xi_1 + \xi_2) \cdot x = \xi_1 \cdot x + \xi_2 \cdot x \quad \forall \xi_1, \xi_2, x \in Z$$

$$\xi \cdot (x_1 + x_2) = \xi \cdot x_1 + \xi \cdot x_2 \quad \forall \xi, x_1, x_2 \in Z$$

The form is called *non-degenerate* if for every non-zero ξ, the map $x \to \xi \cdot x$ is not identically zero, and similarly, for each non-zero x, the map $\xi \to \xi \cdot x$ is not identically zero.
The form is called it symmetric if $\xi \cdot x = x \cdot \xi$.

It can be easily seen that if 0 is the identity element in Z, then $0 \cdot x = x \cdot 0 = 0$ (we have abused notation, by calling 0 both the element in [0,1) and the identity of Z) .

Example 1. If $Z = \mathbb{Z}_N$ is a cyclic group, then

$$\xi \cdot x := \frac{x\xi \pmod N}{N} \in \left\{0, \frac{1}{N}, \ldots, \frac{N-1}{N}\right\}$$

is a symmetric, non-degenerate bilinear form.

2. If $Z = \mathbb{F}_{\mathrm{p}}^n$, p prime, then

$$(x_1, x_2, \ldots, x_n) \cdot (\xi_1, \xi_2, \ldots, \xi_n) := \frac{x_1\xi_1 + x_2\xi_2 + \cdots + x_n\xi_n \pmod p}{p}$$

is a symmetric, non-degenerate bilinear form.

In practice, we will use only the two bilinear forms from the example above. However, such a map can be defined for every finite group.

Lemma 2.1 *Every finite additive group has at least one non-degenerate symmetric bilinear form.*

Proof By the structure theorem of the finite abelian groups, we know that every finite additive group is the direct sum of cyclic groups. We have already seen in the previous example that each cyclic group has a symmetric non-degenerate bilinear form. It can be easily seen that if additve groups Z_1 and Z_2 have symmetric non-degenerate bilinear forms, then the direct sum $Z_1 \oplus Z_2$ also has a symmetric non-degenerate bilinear form, defined by $(\xi_1, \xi_2) \cdot (x_1, x_2) = \xi_1 x_1 + \xi_2 x_2$. The claim follows. ∎

Let $\mathbb{C}^Z$ denote the space of all functions $f : Z \to \mathbb{C}$. It is really convenient for computational purposes to adopt the following notation:

Definition If $f \in \mathbb{C}^Z$, the *mean* or *expectation* of f is defined to be the quantity

$$\mathbb{E}_Z(f) = \mathbb{E}_{x\in Z} f(x) := \frac{1}{|Z|}\sum_{x\in Z} f(x) \ .$$

This notation can be generalized to other finite non-empty domains than Z, for instance

$$\mathbb{E}_{x\in A, y\in B} f(x,y) := \frac{1}{|A||B|}\sum_{x\in A, y\in B} f(x,y) \ .$$

Definition If $A \subseteq Z$, we define the *density* or *probability* of A as

$$P_Z(A) = P_{x\in Z}(x \in A) := \mathbb{E}_Z(1_A) = \frac{|A|}{|Z|} \ .$$

Definition We define the exponential map $e : \mathbb{R} \to \mathbb{C}$ by $e(\theta) := e^{2\pi i\theta}$. As this function has period 1, we can naturally extend this definition to $e : \mathbb{R} \setminus \mathbb{Z} \to \mathbb{C}$.

For every $\xi \in Z$, we define the *associated character* $e_\xi : Z \to \mathbb{C}$ by $e_\xi(x) := e(\xi \cdot x)$.

Lemma 2.2 (Orthogonality properties) *For any $\xi, \xi' \in Z$, we have*

$$\mathbb{E}_{x\in Z}\left(e_\xi(x)\overline{e_{\xi'}(x)}\right) = I(\xi = \xi')$$

Proof Since $e(\xi \cdot x)\overline{e(\xi' \cdot x)} = e((\xi - \xi') \cdot x)$, it will suffice to prove tha claim in the case $\xi' = 0$. Hence we have to prove

$$\mathbb{E}_{x\in Z} e(\xi \cdot x) = I(\xi = 0) \ .$$

This is clear when $\xi = 0$. Otherwise, because the bilinear map is not degenerate, $\exists h \in Z$ such that $e(\xi \cdot h) \neq 1$. Then, by shifting by h, we have

$$\mathbb{E}_{x\in Z} e(\xi \cdot x) = \mathbb{E}_{x\in Z} e(\xi \cdot (x+h)) = e(\xi \cdot h)\mathbb{E}_{x\in Z} e(\xi \cdot x)$$

and therefore $\mathbb{E}_{x\in Z} e(\xi \cdot x) = 0$. ∎

We now look at the space of functions $f : Z \to \mathbb{C}$ (we note it by $\mathbb{C}^Z$). This is a Hilbert space over $\mathbb{C}$ of dimension $|Z|$ with respect to the inner product

$$\langle f, g\rangle := \mathbb{E}_Z f(x)\overline{g(x)} \tag{3}$$

and $\{e_\xi | \xi \in Z\}$ forms an orthonormal basis. This naturally leads to the following definition of the Fourier transform:

Definition If $f \in \mathbb{C}^Z$, the *Fourier transform* $\hat{f} \in \mathbb{C}^Z$ is defined by

$$\hat{f}(\xi) := \langle f, e_\xi\rangle = \mathbb{E}_{x\in Z}\left(f(x)\overline{e(\xi \cdot x)}\right) \ . \tag{4}$$

Since $\{e_\xi | \xi \in Z\}$ is an orthonormal basis, the following standard results can be easily derived:

- Parseval identity
$$\mathbb{E}_Z|f|^2 = \sum_{\xi\in Z} |\hat{f}(\xi)|^2 \tag{5}$$
- Plancherel identity
$$\langle f, g\rangle = \sum_{\xi\in Z} \hat{f}(\xi)\overline{\hat{g}(\xi)} \tag{6}$$

- Fourier inversion formula
$$f(x) = \sum_{\xi \in Z} \hat{f}(\xi) e_\xi(x) \tag{7}$$

With this identities, we will derive some easy results.
First, using the inversion formula and orthogonality property 2.2, we see that

$$\hat{e_\xi}(x) = I(\xi = x) \ .$$

Often it is important to know information about the *zero frequency* $\xi = 0$:

$$\hat{f}(0) = \langle f, 1 \rangle = \mathbb{E}_Z(f)$$

Therefore the zero Fourier coefficient is the same concept as the expectation.

We now introduce the concept of convolution, which is essential in the study of sum sets.

Definition If $f, g \in \mathbb{C}^Z$, we define the *convolution* $f * g$ to be

$$f * g(x) = \mathbb{E}_{y \in Z} f(x-y) g(y) = \mathbb{E}_{y \in Z} f(y) g(x-y)$$

The relevance of the convolution lies in the identity

$$\widehat{f * g} = \hat{f} \cdot \hat{g} \tag{8}$$

Proof

$$\begin{aligned}
\widehat{f * g}(\xi) &= \mathbb{E}_{x \in Z} \left(\mathbb{E}_{y \in Z} f(x-y) g(y) \right) \overline{e(\xi \cdot x)} \\
&= \mathbb{E}_{x \in Z} f(x-y) \overline{e(\xi \cdot (x-y))} \mathbb{E}_{y \in Z} f(y) \overline{e(\xi \cdot y)} \\
&= \mathbb{E}_{x \in Z} f(x) \overline{e(\xi \cdot x)} \mathbb{E}_{y \in Z} f(y) \overline{e(\xi \cdot y)} \quad \text{(just by shifting)} \\
&= \hat{f}(\xi) \hat{g}(\xi)
\end{aligned}$$

If we apply (8) for $\xi = 0$, we get

$$\mathbb{E}_Z(f * g) = (\mathbb{E}_Z f)(\mathbb{E}_Z g) \ .$$

In particular, if f or g has mean 0, then so does $f * g$.

Definition We define the support of f $\text{supp}(f)$ to be

$$\text{supp}(f) = \{x \in Z : f(x) \neq 0\} \ .$$

We identify a set $A \subseteq Z$ by its characteristic function $A : Z \to \{0, 1\}$(again, a slight abuse of notation, A can refer to the set itself or the characteristic function, it should be clear from the context). Characteristic functions are really important in the theory of sum sets. We have the easy fundamental identity

$$A + B = \text{supp}(A * B)$$

(the LHS is the sum of the sets, the RHS is the support of the convolution of the characteristic functions).

Definition If $f \in \mathbb{C}^Z$ and $0 < p < \infty$, we define $L^p(Z)$ norm of f to be

$$\|f\|_{L^p(Z)} := (\mathbb{E}_Z|f|^p)^{1/p} = (\mathbb{E}_{x\in Z}|f(x)|^p)^{1/p}$$

Similarly, we define

$$\|f\|_{l^p(Z)} := \left(\sum_{\xi\in Z}|f(\xi)|^p\right)^{1/p}$$

We also define

$$\|f\|_{L^\infty(Z)} = \|f\|_{l^\infty(Z)} = \sup_{x\in Z}|f(x)|$$

Definition If A, B are subsets of an additive group, we define the *additive energy* $E(A,B)$ as

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

For the purpose of additive combinatorics, the Fourier transform is most useful when applied to characteristic functions of sets. We begin by a relation linking additive energy to the Fourier analysis.

$$\begin{aligned}
E(A,B) &= \sum_{x\in Z}\sum_{y\in Z}|A(x-y)B(y)|^2 \\
&= |Z|^2\sum_{x\in Z}(A*B(x))^2 \\
&= |Z|^3\mathbb{E}_Z|A*B|^2 = |Z|^3\|A*B\|^2_{L^2(Z)} \\
&= |Z|^3\sum_{\xi\in Z}|\hat{A}(\xi)|^2|\hat{B}(\xi)|^2 \quad \text{(by Plancherel's identity)} \qquad (9)
\end{aligned}$$

The following lemma consists of identities of the characteristic functions.

Lemma 2.3 *Let $A \subseteq Z$. Then we have the identities:*

$$\|\hat{A}\|_{l^\infty(Z)} = \sup_{\xi\in Z}|\hat{A}(\xi)| = \hat{A}(0) = P_Z(A) \qquad (10)$$

$$\|\hat{A}\|^2_{l^2(Z)} = \sum_{\xi\in Z}|\hat{A}(\xi)|^2 = P_Z(A) \qquad (11)$$

$$\hat{A}(\xi) = \overline{\hat{A}(-\xi)} \qquad (12)$$

$$\|\hat{A}\|^4_{l^4(Z)} = \sum_{\xi\in Z}|\hat{A}(\xi)|^4 = \frac{E(A,A)}{|Z|^3} \qquad (13)$$

Proof For (10),

$$\begin{aligned}
\|\hat{A}\|_{l^\infty(Z)} = \sup_{\xi\in Z}|\hat{A}(\xi)| &= \sup_{\xi\in Z}\left|\mathbb{E}_{x\in Z}A(x)\overline{e(\xi\cdot x)}\right| \\
&= \sup_{\xi\in Z}\left|\mathbb{E}_{x\in A}\overline{e(\xi\cdot x)}\right| \\
&= \frac{|A|}{|Z|} = P_Z(A) \quad (\text{as } e(0)=1)
\end{aligned}$$

For (11),

$$\begin{aligned}
\|\hat{A}\|^2_{l^2(Z)} &= \sum_{\xi\in Z}|\hat{A}(\xi)|^2 \\
&= \mathbb{E}_{x\in Z}|A(x)|^2 \quad \text{(by Parseval identity)} \\
&= \frac{|A|}{|Z|} = P_Z(A)
\end{aligned}$$

For (12),

$$\begin{aligned}\overline{\hat{A}(-\xi)} &= \mathbb{E}_{x\in Z} A(x)e(-\xi\cdot x)\\ &= \mathbb{E}_{x\in Z} A(x)\overline{e(\xi\cdot x)}\\ &= \hat{A}(\xi)\end{aligned}$$

(13) is just an easy consequence of (9). ∎

We will prove later that the set $2A-2A$ has some useful properties. For these reason, we will prove the following identity here:

$$A*(-A)*A*(-A)(x) = \sum_{\xi\in Z} |\hat{A}(\xi)|^4 e(\xi\cdot x) \tag{14}$$

Proof

$$\begin{aligned}A*(-A)*A*(-A)(x) &= \sum_{\xi\in Z} \mathcal{F}(A*(-A)*A*(-A))(\xi)e(\xi\cdot x) \quad \text{(by Fourier inversion formula)}\\ &= \sum_{\xi\in Z} \hat{A}(\xi)\hat{A}(-\xi)\hat{A}(\xi)\hat{A}(-\xi)e(\xi\cdot x) \quad \text{by (8)}\\ &= \sum_{\xi\in Z} \hat{A}(\xi)\overline{\hat{A}(\xi)}\hat{A}(\xi)\overline{\hat{A}(\xi)}e(\xi\cdot x) \quad \text{by (12)}\\ &= \sum_{\xi\in Z} |\hat{A}(\xi)|^4 e(\xi\cdot x)\end{aligned}$$

2.2 Bohr sets

In many applications in additive combinatorics, one starts with a subset $A\subseteq Z$ with some properties and derives some conclusions about the Fourier transform $\hat{A}$. For this purpose, Bohr sets turn out to be very useful. These are in some sense highly structured subsets of Z.

Definition Let $S\subseteq Z$ and $\rho>0$. We define the *Bohr set* $B(S,\rho)$ as

$$B(S,\rho) := \left\{ x\in Z : \sup_{x\in Z} \|\xi\cdot x\| < \rho \right\} ,$$

where $\|x\|$ denotes the distance from the closest integer (in our case 0 or 1).

S is called the *frequency* of the Bohr set and ρ the *radius*. The quantity $|S|$ is called the *rank* of the Bohr set.

From now on we will work only with the additive group $Z=\mathbb{Z}_N$, where N an integer, $N\geq 2$. We will use the bilinear form

$$\xi\cdot x = \frac{\xi x}{N} .$$

So, for instance, the Bohr set $B(S,\rho)$ for $S\subseteq\mathbb{Z}_N$ is

$$B(S,\rho) := \left\{ x\in Z : \sup_{x\in Z} \left\|\frac{\xi x}{N}\right\| < \rho \right\} .$$

Set $\omega = e^{\frac{2\pi i}{N}}$. Therefore we have

$$e(\xi\cdot x) = \omega^{\xi x} .$$

In order to make the notation easier, sometimes the sum notation will be simplified:

$$\sum_x f(x) := \sum_{x \in \mathbb{Z}_N} f(x) \ .$$

The following similar 2 lemmas relate to the idea that the "large spectrum" of a set is in some sense well structured. As a motivation for the statements of these 2 lemmas, we will see later that the structure of $2A - 2A$ is closely linked to the structure of A.

Lemma 2.4 (Bogolyubov) *Let $A \subseteq \mathbb{Z}_N$ with $|A| = \delta N$. Then $2A - 2A$ contains a Bohr set $B\left(K, \frac{1}{4}\right)$ of rank $k \leq 1/\delta^2$.*

Proof Let

$$K = \left\{ r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \frac{\lambda |A|}{N} \right\}$$

the set of large Fourier coefficients, where $0 < \lambda < 1$ to be chosen later. Of course $0 \in K$, as it can be seen in (10).

Let $b \in B\left(K, \frac{1}{4}\right)$. We want to show that $b \in 2A - 2A$. As

$$\operatorname{supp}\left(A * (-A) * A * (-A)\right) \subseteq 2A - 2A$$

and using (14), it is enough to prove that

$$\left| \sum_\xi |\hat{A}(\xi)|^4 \omega^{b\xi} \right| > 0 \ .$$

But

$$\sum_\xi |\hat{A}(\xi)|^4 \omega^{b\xi} = \left(A * (-A) * A * (-A)\right)(b) \in \mathbb{R} \ ,$$

so

$$\sum_\xi |\hat{A}(\xi)|^4 \omega^{b\xi} = \Re\left(\sum_\xi |\hat{A}(\xi)|^4 \omega^{b\xi} \right) = \sum_\xi |\hat{A}(\xi)|^4 \cos\left(\frac{2\pi b\xi}{N}\right)$$

- $\xi = 0$

$$|\hat{A}(0)|^4 = \delta^4 \quad \text{by (10)}$$

- $\xi \in K \setminus \{0\}$
  As $b \in B\left(K, \frac{1}{4}\right)$, then $\left\| \frac{b\xi}{N} \right\| < \frac{1}{4}$, for all $\xi \in K \setminus \{0\}$. It follows that

$$\cos\left(\frac{2\pi b\xi}{N}\right) > \cos\left(\frac{\pi}{2}\right) = 0 \ .$$

  Therefore,

$$\sum_{\xi \in K \setminus \{0\}} |\hat{A}(\xi)|^4 \cos\left(\frac{2\pi b\xi}{N}\right)$$

  is positive.

- $\xi \notin K$

$$\begin{aligned}\left|\sum_{\xi\notin K}|\hat{A}(\xi)|^4\cos\left(\frac{2\pi b\xi}{N}\right)\right| &\leq \left|\sum_{\xi\notin K}|\hat{A}(\xi)|^4\right| \\ &\leq \left(\frac{\lambda|A|}{N}\right)^2\left|\sum_{\xi\notin K}|\hat{A}(\xi)|^2\right| \\ &\leq \frac{\lambda^2|A|^2}{N^2}\left|\sum_{\xi}|\hat{A}(\xi)|^2\right| \\ &= \frac{\lambda^2|A|^2}{N^2}\frac{|A|}{N} = \lambda^2\delta^3 \quad \text{by (11)}\end{aligned}$$

Choose $\lambda^2 = \delta$, then we get

$$\sum_{\xi}|\hat{A}(\xi)|^4\cos\left(\frac{2\pi b\xi}{N}\right) \geq \delta^4 + \sum_{\xi\in K\setminus\{0\}}|\hat{A}(\xi)|^4\cos\left(\frac{2\pi b\xi}{N}\right) - \left|\sum_{\xi\notin K}|\hat{A}(\xi)|^4\cos\left(\frac{2\pi b\xi}{N}\right)\right| > 0$$

by using the previous 3 observations. ∎

Lemma 2.5 *Let $A \subseteq \mathbb{Z}_N$ with $|A+A| \leq C|A|$. Let*

$$R = \left\{r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \frac{|A|}{2\sqrt{C}N}\right\} .$$

Then

$$B\left(R, \frac{1}{20}\right) \subseteq 2A - 2A .$$

Proof First, note $r_A(x)$ the number of pairs $(a_1, a_2) \in A^2$ with $a_1 + a_2 = x$. Then we have

$$\begin{aligned}N^3\sum_r|\hat{A}(r)|^4 &= E(A,A) \quad \text{by (13)} \\ &= \sum_{x\in A+A} r_A(x)^2 \quad \text{(by definition of additive energy)} \\ &\geq \frac{1}{|A+A|}\left(\sum_x r_A(x)\right)^2 \quad \text{(by Cauchy-Schwarz)} \\ &= \frac{|A|^4}{|A+A|} \\ &\geq \frac{|A|^3}{C}\end{aligned}$$

Hence

$$\sum_r|\hat{A}(r)|^4 \geq \frac{|A|^3}{CN^3} \tag{15}$$

If $\xi \in R$, we have

$$|1-\omega^{\xi x}| = |1-e^{2\pi i\xi x/N}| = 2\left|\sin\left(\frac{\pi\xi x}{N}\right)\right| \leq 2\left|\sin\left(\frac{\pi}{20}\right)\right| < \frac{2\pi}{20} < \frac{1}{2} \tag{16}$$

Hence, for any $x \in B\left(R, \frac{1}{20}\right)$,

$$\begin{aligned}
\left|\sum_{\xi} |\hat{A}(\xi)|^4 \omega^{\xi x}\right| &\geq \left|\sum_{\xi} |\hat{A}(\xi)|^4\right| - \left|\sum_{\xi} |\hat{A}(\xi)|^4 (1-\omega^{\xi x})\right| \\
&\geq \left|\sum_{\xi} |\hat{A}(\xi)|^4\right| - \left|\sum_{\xi \notin R} |\hat{A}(\xi)|^4 (1-\omega^{\xi x})\right| - \left|\sum_{\xi \in R} |\hat{A}(\xi)|^4 (1-\omega^{\xi x})\right| \\
&> \frac{1}{2}\left|\sum_{\xi} |\hat{A}(\xi)|^4\right| - 2\left|\sum_{\xi \notin R} |\hat{A}(\xi)|^4\right| \quad \text{(by (16) and } |1-\omega^{\xi x}| \leq 2) \\
&\geq \frac{|A|^3}{2CN^3} - 2 \sup_{\xi \notin R} |\hat{A}(\xi)|^2 \sum_{\xi} |\hat{A}(\xi)|^2 \quad \text{by (15)} \\
&\geq \frac{|A|^3}{2CN^3} - 2\frac{|A|^2}{4CN^2}\frac{|A|}{N} = 0 \quad \text{by (11) and hypothesis}
\end{aligned}$$

Therefore, if $x \in B\left(R, \frac{1}{20}\right)$,

$$\left|\sum_{\xi} |\hat{A}(\xi)|^4 \omega^{\xi x}\right| > 0 \ .$$

Hence, by (14) it follows that $x \in \operatorname{supp}(A * (-A) * A * (-A))$, which easily implies that $x \in 2A - 2A$. ∎

2.3 Chang's theorem

The purpose of this chapter is to improve the results obtained in the previous chapters. For this scope, we will work with *dissociated sets*, which are highly structured subsets of an abelian group. We will also introduce the cosine polynomials and prove some properties of those.

Definition A subset $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ of an additive group is called *dissociated* if the only solution to

$$\sum_{j=1}^{k} \epsilon_j \lambda_j = 0 \ ,$$

with $\epsilon_j \in \{-1, 0, 1\}$ is the trivial one $\epsilon_j = 0$, for all $1 \leq j \leq k$.

Definition If $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_k\} \subseteq \mathbb{Z}_N$ is a dissociated set of an additive group, we denote by $\overline{\Lambda}$ the set of all elements of the form $\sum_{j=1}^{k} \epsilon_j \lambda_j$, where $\epsilon_j \in \{-1, 0, 1\}$, for all $1 \leq j \leq k$. $\overline{\Lambda}$ is called the *cube* spanned by Λ and is said to have dimension k.

Let $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_k\} \subseteq \mathbb{Z}_N$ a dissociated set. We consider cosine polynomials of the form $f : \mathbb{Z}_N \to \mathbb{R}$

$$f(x) = \sum_{j=1}^{k} c_j \cos\left(\frac{2\pi\lambda_j x}{N} + \beta_j\right) \tag{17}$$

where $\beta_j, c_j \in \mathbb{R}$.

Lemma 2.6 *Let f a cosine polynomial of the type* (17)*. Then*

$$\sum_{x} f(x)^2 = \sum_{j=1}^{k} c_j^2 \ .$$

Proof First, we can observe that we can write

$$\begin{aligned}\cos\left(\frac{2\pi\lambda_j x}{N}+\beta_j\right) &= \cos\left(\frac{2\pi\lambda_j x}{N}\right)\cos(\beta_j)-\sin\left(\frac{2\pi\lambda_j x}{N}\right)\sin(\beta_j)\\ &= \frac{1}{2}\left(e\left(\frac{\lambda_j x}{N}\right)+e\left(-\frac{\lambda_j x}{N}\right)\right)\cos(\beta_j)+\frac{1}{2i}\left(e\left(\frac{\lambda_j x}{N}\right)-e\left(-\frac{\lambda_j x}{N}\right)\right)\sin(\beta_j)\\ &= \frac{1}{2}e\left(\frac{\lambda_j x}{N}\right)(\cos(\beta_j)-i\sin(\beta_j))+\frac{1}{2}e\left(-\frac{\lambda_j x}{N}\right)(\cos(\beta_j)+i\sin(\beta_j))\\ &= \gamma_j\ e\left(\frac{\lambda_j x}{N}\right)+\overline{\gamma_j}\ e\left(-\frac{\lambda_j x}{N}\right)\end{aligned}$$

where $|\gamma_j| = 1/2$.

Now, we see that if $i \neq j$, then

$$\begin{aligned}&\sum_x \cos\left(\frac{2\pi\lambda_i x}{N}+\beta_i\right)\cos\left(\frac{2\pi\lambda_j x}{N}+\beta_j\right)\\ &= \sum_x\left(\gamma_i\ e\left(\frac{\lambda_i x}{N}\right)+\overline{\gamma_i}\ e\left(-\frac{\lambda_i x}{N}\right)\right)\left(\gamma_j\ e\left(\frac{\lambda_j x}{N}\right)+\overline{\gamma_j}\ e\left(-\frac{\lambda_j x}{N}\right)\right)\\ &= \sum_x\left(\gamma_i\gamma_j e\left(\frac{(\lambda_i+\lambda_j)x}{N}\right)+\gamma_i\overline{\gamma_j}e\left(\frac{(\lambda_i-\lambda_j)x}{N}\right)+\overline{\gamma_i}\gamma_j e\left(\frac{(-\lambda_i+\lambda_j)x}{N}\right)+\overline{\gamma_i\gamma_j}e\left(\frac{-(\lambda_i+\lambda_j)x}{N}\right)\right)\\ &= 0\end{aligned}$$

as both $\lambda_i+\lambda_j \neq 0$ and $\lambda_i-\lambda_j \neq 0$ by the dissociativity. Therefore:

$$\begin{aligned}\sum_x f(x)^2 &= \sum_x\left(\sum_{i=1}^k\sum_{j=1}^k c_i c_j\cos\left(\frac{2\pi\lambda_i x}{N}+\beta_i\right)\cos\left(\frac{2\pi\lambda_j x}{N}+\beta_j\right)\right)\\ &= \sum_{i=1}^k\sum_{j=1}^k c_i c_j\left(\sum_x\cos\left(\frac{2\pi\lambda_i x}{N}+\beta_i\right)\cos\left(\frac{2\pi\lambda_j x}{N}+\beta_j\right)\right)\\ &= \sum_{j=1}^k c_j^2\sum_x\cos\left(\frac{2\pi\lambda_j x}{N}+\beta_j\right)^2\\ &= \sum_{j=1}^k c_j^2\sum_x\left(\gamma_j^2 e\left(\frac{2\lambda_j x}{N}\right)+2\gamma_j\overline{\gamma_j}+\overline{\gamma_j}^2 e\left(\frac{-2\lambda_j x}{N}\right)\right)\\ &= \sum_{j=1}^k 2Nc_j^2|\gamma_j|^2 \quad (\text{as } \lambda_j \neq 0)\\ &= \frac{N}{2}\sum_{j=1}^k c_j^2 \quad (\text{as } |\gamma_j| = 1/2) \quad \blacksquare\end{aligned}$$

Lemma 2.7 *Let $t \in \mathbb{R}$ and f a cosine polynomial of type* (17)*. Then*

$$N^{-1}\sum_x \exp(tf(x)) \leq \exp(N^{-1}t^2\sum_x f(x)^2)$$

Proof We first claim that, for any $t \in \mathbb{R}$, $y \in \mathbb{R}$, $|y| \leq 1$,

$$e^{ty} \leq \cosh(t) + y\sinh(t)\ . \tag{18}$$

Indeed, the function $F(x) = e^{tx}$ is convex on [-1,1], therefore

$$F(x) \leq \frac{1-x}{2}F(-1) + \frac{1+x}{2}F(1) \ .$$

The claim follows easily.

Now, by looking at what we want to prove, we see that

$$\begin{aligned} N^{-1}\sum_x \exp(tf(x)) &= N^{-1}\sum_x \exp\left(\sum_{j=1}^k tc_j \cos\left(\frac{2\pi\lambda_j x}{N} + \beta_j\right)\right) \\ &= N^{-1}\sum_x \prod_{j=1}^k \exp\left(tc_j \cos\left(\frac{2\pi\lambda_j x}{N} + \beta_j\right)\right) \\ &\leq N^{-1}\sum_x \prod_{j=1}^k \exp\left(\cosh(tc_j) + \sinh(tc_j)\cos\left(\frac{2\pi\lambda_j x}{N} + \beta_j\right)\right) \quad \text{(by (18))} \\ &= N^{-1}\sum_x \prod_{j=1}^k \left(\cosh(tc_j) + \sinh(tc_j)\gamma_j e\left(\frac{\lambda_j x}{N}\right) + \sinh(tc_j)\bar{\gamma_j} e\left(-\frac{\lambda_j x}{N}\right)\right) \end{aligned}$$

because $\cos\left(\frac{2\pi\lambda_j x}{N} + \beta_j\right) = \gamma_j e\left(\frac{\lambda_j x}{N}\right) + \bar{\gamma_j} e\left(-\frac{\lambda_j x}{N}\right)$, as we've seen in the proof of the previous lemma.

If we expand this product, we get a linear combination of terms of the form

$$e\left(\frac{2\pi(\epsilon_1\lambda_1 + \epsilon_2\lambda_2 + \ldots \epsilon_k\lambda_k)x}{N}\right)$$

where each $\epsilon_j \in \{-1, 0, 1\}$, with coefficients depending on t.

The dissociativity of Λ implies that only when $\epsilon_1 = \epsilon_2 = \cdots = \epsilon_k = 0$, the sum over all $x \in \mathbb{Z}_N$ will not vanish. Therefore,

$$N^{-1}\sum_x \exp(tf(x)) \leq N^{-1}\sum_x \prod_{j=1}^k \cosh(tc_j) = \prod_{j=1}^k \cosh(tc_j) \ .$$

Next, we note that $\cosh(y) \leq e^{y^2}/2$, for all $y \in \mathbb{R}$, a fact which can be easily verified by looking at the power series.

Returning to our problem, we see that

$$\begin{aligned} N^{-1}\sum_x \exp(tf(x)) &\leq \prod_{j=1}^k \cosh(tc_j) \\ &\leq \exp\left(\frac{1}{2}t^2\sum_{j=1}^k c_j^2\right) \quad \text{(using the previous remark)} \\ &= \exp\left(N^{-1}t^2\sum_x f(x)^2\right) \quad \text{(by previous lemma)} \quad \blacksquare \end{aligned}$$

The following theorem is essential in our approach. The proof will use our results regarding cosine polynomials.

Theorem 2.8 (Chang) *Let $A \subseteq \mathbb{Z}_N$ such that $|A| = \alpha N$. Let $R = \{r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \frac{\rho|A|}{N}\}$, $\rho \in (0,1)$. Let Λ be a dissociated subset of R. Then*

$$|\Lambda| \leq 2\rho^{-2} \log\left(\frac{1}{\alpha}\right) \ .$$

.

Proof Let $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ be a dissociated subset of R. Set $\omega = e^{\frac{2\pi i}{N}}$ and

$$g(x) = N \sum_{j=1}^{k} \hat{A}(\lambda_j) \omega^{\lambda_j x}$$

and $f(x) = \Re(g(x))$, the real part of g. Then

$$\begin{aligned} f(x) &= N \sum_{j=1}^{k} \left(\Re(\hat{A}(\lambda_j)) \cos\left(\frac{2\pi\lambda_j x}{N}\right) - \Im(\hat{A}(\lambda_j)) \sin\left(\frac{2\pi\lambda_j x}{N}\right)\right) \\ &= \sum_{j=1}^{k} N|\hat{A}(\lambda_j)| \cos\left(\frac{2\pi\lambda_j x}{N} + \beta_j\right) \qquad \text{for some } \beta_j \in \mathbb{R} \ . \end{aligned}$$

Therefore f is a cosine polynomial. Moreover,

$$f(x) = \frac{g(x) + \overline{g(x)}}{2}$$

.

$$\begin{aligned} \hat{g}(r) &= \frac{1}{N} \sum_{x} \left(N \sum_{j=1}^{k} \hat{A}(\lambda_j) \omega^{\lambda_j x} \right) \omega^{-rx} \\ &= \sum_{j=1}^{k} \hat{A}(\lambda_j) \sum_{x} \omega^{(\lambda_j - r)x} \\ &= N \sum_{j=1}^{k} \hat{A}(\lambda_j) I(\lambda_j = r) \\ &= \begin{cases} N\hat{A}(r) & r \in \Lambda \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

Similarly,

$$\begin{aligned} \hat{\bar{g}}(r) &= \frac{1}{N} \sum_{x} \left(\sum_{j=1}^{k} N\overline{\hat{A}(\lambda_j)} \omega^{-\lambda_j x} \right) \omega^{-rx} \\ &= N \sum_{j=1}^{k} \overline{\hat{A}(\lambda_j)} I(\lambda_j = -r) \end{aligned}$$

But $\overline{\hat{A}(\lambda_j)} = \hat{A}(-\lambda_j)$ (by (12)). Therefore

$$\hat{\bar{g}}(r) = \begin{cases} N\hat{A}(r) & r \in -\Lambda \\ 0 & \text{otherwise} \end{cases}$$

By dissociativity of Λ, it follows that $\Lambda \cap (-\Lambda) = \emptyset$. Therefore,

$$\hat{f}(r) = \begin{cases} \frac{N\hat{A}(r)}{2} & r \in \Lambda \cup (-\Lambda) \\ 0 & \text{otherwise} \end{cases}$$

Hence,

$$\begin{aligned} \sum_x f(x)A(x) &= N \sum_{r \in \Lambda \cup (-\Lambda)} \hat{f}(r)\overline{\hat{A}(r)} \quad \text{(by Plancherel identity)} \\ &= 2\sum_r |\hat{f}(r)|^2 \\ &= \frac{2}{N}\sum_x |f(x)|^2 \,. \end{aligned} \tag{19}$$

We have

$$\begin{aligned} \frac{1}{|A|}\exp\left(\frac{t^2\sum_x f(x)^2}{N}\right) &\geq \frac{1}{N|A|}\sum_x \exp(tf(x)) \quad \text{(by previous lemma)} \\ &\geq \frac{1}{N|A|}\sum_{x\in A} \exp(tf(x)) \\ &\geq \frac{1}{N}\exp\left(\frac{t}{|A|}\sum_{x\in A} f(x)\right) \quad \text{(by AM-GM)} \\ &= \frac{1}{N}\exp\left(\frac{t}{|A|}\sum_x f(x)A(x)\right) \\ &= \frac{1}{N}\exp\left(\frac{2t}{N|A|}\sum_x f(x)^2\right) \quad \text{(by (19))} \end{aligned}$$

Choose $t = |A|^{-1}$, we get

$$\begin{aligned} &\frac{1}{|A|}\exp\left(\frac{1}{N|A|^2}\sum_x f(x)^2\right) \geq \frac{1}{N}\exp\left(\frac{2}{N|A|^2}\sum_x f(x)^2\right) \\ \iff &\frac{1}{\alpha} \geq \exp\left(\frac{1}{N|A|^2}\sum_x f(x)^2\right) \end{aligned}$$

Observe that

$$\begin{aligned} \sum_x f(x)^2 &= \frac{N}{2}\sum_{j=1}^{k}(N|\hat{A}(\lambda_j)|)^2 \quad \text{(by Lemma 2.6)} \\ &\geq \frac{N}{2}k\rho^2|A|^2 \quad \text{(by assumption and } \Lambda \subseteq R) \end{aligned}$$

Therefore, we have that

$$\begin{aligned} &\frac{1}{\alpha} \geq \exp\left(\frac{k\rho^2}{2}\right) \\ \iff &k \leq 2\rho^{-2}\log\left(\frac{1}{\alpha}\right) \quad \blacksquare \end{aligned}$$

Corollary 2.9 *Let $\rho, \alpha \in [0,1]$, $A \subseteq \mathbb{Z}_N$, $|A| = \alpha N$ and let $R = \{r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \frac{\rho|A|}{N}\}$. Then R is contained in a "cube" of dimension at most $2\rho^{-2}\log\left(\frac{1}{\alpha}\right)$.*

Proof Let $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ a maximal dissociated subset of R. Then, by Chang's theorem, $k \leq 2\rho^{-2} \log\left(\frac{1}{\alpha}\right)$. The maximality of Λ implies that all $r \in R$ is involved in some equation of the type

$$\epsilon r + \sum_{j=1}^{k} \epsilon_i \lambda_i = 0 \ ,$$

where ϵ's are 0, ± 1. Thus R is contained in the cube spanned by Λ. ∎

Theorem 2.10 *Let $A \in \mathbb{Z}_N$, $|A| = \alpha N$, such that $|A + A| \leq C|A|$. Then there exists a Bohr neighbourhood $B(K, \delta) \subseteq 2A - 2A$ such that*

$$|K| \leq 8C \log\left(\frac{1}{\alpha}\right)$$

and

$$\delta \geq \frac{1}{160C \log\left(\frac{1}{\alpha}\right)} \ .$$

Proof Let

$$R = \left\{ r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \frac{|A|}{2\sqrt{C}N} \right\} \ .$$

Using 2.5, we know that $B\left(R, \frac{1}{20}\right) \subseteq 2A - 2A$. Now, using 2.9, we get that there exists Λ such that

$$R \subseteq \overline{\Lambda}, \quad |\Lambda| \leq 8C \log\left(\frac{1}{\alpha}\right) \ .$$

We claim that

$$B\left(\Lambda, \frac{1}{20\Lambda}\right) \subseteq B\left(R, \frac{1}{20}\right) \ . \tag{20}$$

It is easy to see that this claim implies the conclusion.

Since $R \subseteq \overline{\Lambda}$, every $r \in R$ can be written as

$$r = \sum_{j=1}^{|\Lambda|} \epsilon_j \lambda_j \ ,$$

where $\epsilon_j \in \{-1, 0, 1\}$, for all $1 \leq j \leq |\Lambda|$.

Hence, if $x \in B\left(\Lambda, \frac{1}{20\Lambda}\right)$, then

$$\left\| \frac{\lambda_j x}{N} \right\| \leq \frac{1}{20|\Lambda|} \ ,$$

so we have

$$\left\| \frac{rx}{N} \right\| = \left\| \frac{\sum_{j=1}^{|\Lambda|} \epsilon_j \lambda_j x}{N} \right\| \leq \sum_{j=1}^{|\Lambda|} \left\| \frac{\lambda_j x}{N} \right\| \leq \frac{1}{20} \ .$$

The claim follows. ∎

3 Graph theory

Graph theoretical methods play an essential role in the field of additive combinatorics. Just to mention a few important results, there is the Balog-Szemeredi-Gowers theorem or the Szemeredi's regularity lemma, which led to the first proof of the celebrated Szemeredi's theorem. Also, Ramsey theory proved to be extremely useful. However, in this section we are interested in establishing Plünnecke's inequalities, which are the sharpest inequalities currently known for sum sets.

3.1 Plünnecke graphs

In order to develop the theory, we need to introduce the definition of Plünnecke graphs.

Definition A layered graph of level n is a directed graph $G = (V(G), E(G))$ whose vertex set may be written as the disjoint union

$$V(G) = V_0 \cup V_1 \cup \cdots \cup V_n$$

and whose edges are of the form (v, v'), where $v \in V_i$, $v' \in V_{i+1}$, for some $1 \leq i \leq n-1$.

We will work with some particular layered graphs.

Definition A Plünnecke graph of level n is a layered graph of level n satifying the following 2 additional properties:

1. *Forward splitting of paths*: Suppose $0 \leq i \leq n-2$ and $u \in V_i$, $v \in V_{i+1}$, $w_1, \ldots, w_k \in V_{i+2}$ are such that (u, v) and all of (v, w_j) are edges in the graph. Then there exist distinct $v_1, \ldots, v_k \in V_{i+1}$ such that all of (u, v_j) and (v_j, w_j) are edges in the graph.

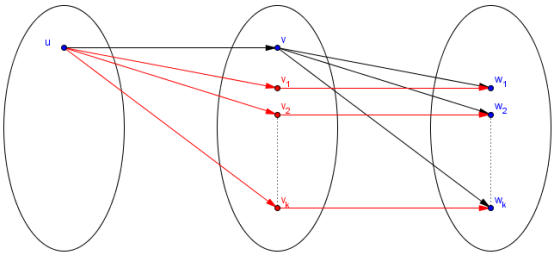


Figure 1: Forward splitting of paths

2. *Backward splitting of paths*: Suppose $0 \leq i \leq n-2$ and $u_1, \ldots, u_k \in V_i$, $v \in V_{i+1}$, $w \in V_{i+2}$ are such that all of (u_j, v) and (v, w) are edges in the graph. Then there exist distinct $v_1, \ldots, v_k \in V_{i+1}$ such that all of (u_j, v_j) and (v_j, w) are edges in the graph.

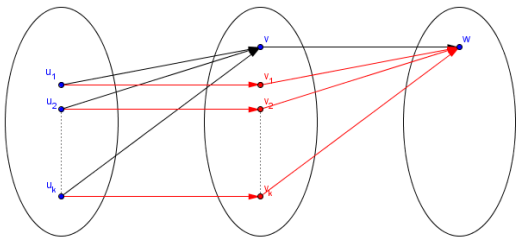


Figure 2: Backward splitting of paths

Remarks 3.1 *Let G a Plünnecke graph and $v \in V_i$. We denote by $d^+(v)$ the indegree of v, the number of edges from V_{i-1} to v. Similarly, $d^+(v)$ denotes the outdegree, the number of edges from v to V_{i+1}. We have the following two consequences of the definition of a Plünneckegraph of level n:*

1. *Forward splitting: If $(u, v) \in E(G)$ and $v \notin V_n$, then $d^+(u) \geq d^+(v)$.*
2. *Backward splitting: If $(u, v) \in E(G)$ and $u \notin V_0$, then $d^-(u) \leq d^-(v)$.*

We will need Menger's Theorem, a classical theorem in graph theory. Let G be a directed graph and $A, B \subseteq V(G)$. We define MAXFLOW$(A \to B; G)$ the maximum number of vertex disjoint paths which connect a vertex from A to a vertex in B. We define MINCUT$(A \to B; G)$ the minimum number of vertices from G which need to be removed so that A and B are disconnected.

Theorem 3.2 (Menger's theorem)

$$MAXFLOW(A \to B; G) = MINCUT(A \to B; G)$$

Proof One direction is trivial, as it is obvious that MAXFLOW $\leq$ MINCUT. The goal is to prove the other direction.

We will use induction on the number of edges in G. For the base case, if there are no edges in G, then

$$\text{MAXFLOW}(A \to B; G) = \text{MINCUT}(A \to B; G) = |A \cap B| \ .$$

Let $s = \text{MINCUT}(A \to B; G)$. Now we assume there is an edge $a \to b$ in G. We will use the induction step on $G/(a = b)$, with a and b identified as a single vertex. Let $S/(a = b)$ be a minimal subset of $G/(a = b)$ disconnecting $A/(a = b)$ from $B/(a = b)$. If $|S/(a = b)| \geq s$, we apply the induction hypothesis to $G/(a = b)$ to construct at least s disjoint paths from $A/(a = b)$ to $B/(a = b)$. This leads to at least s disjoint paths from A to B in G, as desired.

We assume $|S/(a = b)| < s$. We can see that S must disconnect A from B in G, so $|S| \geq s$. This can only happen if $|S| = s$ and $a, b \in S$.

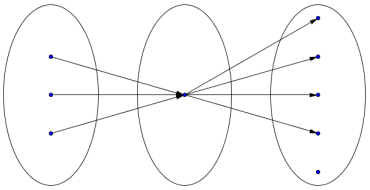
Now look at MINCUT$(A \to S; G)$. This must be at least s, because every path from A to B must pass through something in S, and if we could separate A from S using fewer than s elements, we can disconnect A from B using the same elements. As both $a, b \in S$, we see that actually MINCUT$(A \to S; G/(a = b)) \geq s$. By induction hypothesis, we find s disjoint paths from A to S. As $|S| = s$, each path has a distinct end point. Similarly, we find s distinct paths from S to B, each path having a different initial point. The paths from the first family must be disjoint of the paths in the second family except at S, since otherwise we can construct a path from A to B which avoids S. By merging the s paths from A to S with the s paths from S to B, we create s disjoint paths from A to B. ∎

Definition Given a layered graph G, we define the i-th magnification ratio by

$$D_i(G) := \inf_{X \subseteq V_0, X \neq \emptyset} \frac{|\text{Im}_i(X)|}{|X|} \ ,$$

where $\text{Im}_i(X)$ denotes the set of vertices in V_i that can be reached by a path starting from some $x \in X$.

Example • The example below is a layered graph of level 3. For this case, $D_1 = 1/3$ and $D_2 = 4/3$. It is NOT a Plünnecke graph.



- This is a key example for what will follow. Suppose A and B are subsets of an additive group and take $V_i = A + iB$. We connect a vertex v from V_i to a vertex w from V_{i+1} if and only if $w - v \in B$. It can be easily checked that this is a Plünnecke graph.
- This is a special case of the previous example, called the *independence graph*, denoted by $I_n(h)$. Let $A = \{0\}$ and B a set of h numbers such that all possible sums of n elements from B are distinct (not necessarily distinct elements of B). For instance, we can have

$$B = \{1, 2n, (2n)^2, \ldots, (2n)^{h-1}\} .$$

  In this case, we can see that $|V_i| = \binom{h+i-1}{i}$. Therefore

$$D_i = \binom{h+i-1}{i} .$$

- The *inverse independence graph*, denoted by $I_n(h)^{-1}$ is the graph obtained by reversing $I_n(h)$. So in this case,

$$D_i = \binom{h+i-1}{i}^{-1} .$$

Lemma 3.3 *Let G be a Plünnecke graph of order n and suppose $D_n \geq 1$. Then $D_i \geq 1$, for all $1 \leq i \leq n$.*

Proof Let $V(G) = V_0 \cup V_1 \cup \cdots \cup V_n$. We will prove that if $D_n \geq 1$, then there are $|V_0|$ disjoint paths from V_0 to V_n, which is statement stronger than our desired conclusion.

Let $m = \text{MINCUT}(V_0 \to V_n; G) = \text{MAXFLOW}(V_0 \to V_n; G)$. Clearly $m \leq |V_0|$. Let S a separating set for V_0 and V_n, $|S| = m$, which is as "early concentrated" as possible, in the sense that

$$\sum_{i=0}^{n} i|S \cap V_i|$$

is minimal for all separating sets.

Suppose for contradiction $m < |V_0|$. We first claim that S intersects $V_1 \cup V_2 \cup \cdots \cup V_{n-1}$. If not, suppose that $S = X \cap Y$, where $X \subseteq V_0$ and $Y \subseteq V_n$. Since S is a separating set, Y meets every path from $V_0 \setminus X$ to V_n. Therefore $\text{Im}_n(V_0 \setminus X) \subseteq Y$. On the other hand, $D_n \geq 1$ implies that $|\text{Im}_n(V_0 \setminus X)| \geq |(V_0 \setminus X|$. Therefore,

$$m = |S| = |X| + |Y| \geq |X| + |\text{Im}_n(V_0 \setminus X)| \geq |X| + |V_0 \setminus X| = |V_0|$$

a contradiction to our assumption about m.

Therefore there exists k, $1 \leq k \leq n-1$ such that $S \cap V_k \neq \emptyset$. Let $S \cap V_k = \{s_1, \ldots, s_q\}$. Let the remaining elements of S be $\{s_{q+1}, \ldots, s_m\}$. By Menger's theorem, consider m disjoint paths $\pi_1, \ldots, \pi_m$ from V_0 to V_n such that $s_i \in \pi_i$. Let $r_i \in V_{k-1}$ and $t_i \in V_{k+1}$ the

predecessor (resp. successor) of s_i along π_i. Because we assumed S is "early concentrated", $\{r_1, \ldots, r_q, s_{q+1}, \ldots, s_m\}$ is NOT a separating set. Therefore there exists $\pi*$ a path from V_0 to V_n which doesn't meet this set. Let $\{r*\} = \pi* \cap V_{k-1}$, $r* \notin \{r_1, \ldots, r_q\}$. As S is a separating set, $\pi*$ must intersect $\{s_1, \ldots, s_q\}$. Assume without losing the generality that $\pi* \cap S = \{s_1\}$.

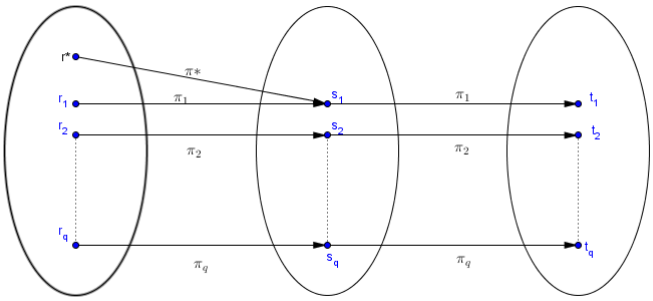


Figure 3: Induced graph G' (might contain other edges which are not shown in the figure)

We claim that the induced graph G' on vertex set $\{r*, r_1, \ldots, r_q, s_1, \ldots, s_q, t_1, \ldots, t_q\}$ is Plünnecke. Indeed, by our construction, we can see that every path in G from $\{r*, r_1, \ldots, r_q\}$ to $\{t_1, \ldots, t_q\}$ must pass through some s_i ,$1 \leq i \leq q$. So the fact that G is Plünnecke must locally imply that G' is Plünnecke, all requirements are fulfilled.

Now we study the induced graph G'. Using Remarks 3.1, since (r_i, s_i) and (s_i, t_i) are edges, for all $1 \leq i \leq q$, we obtain

$$\sum_{i=1}^{q} d^+(r_i) \geq \sum_{i=1}^{q} d^+(s_i) = \sum_{i=1}^{q} d^-(t_i)$$

and

$$d^+(r*) + \sum_{i=1}^{q} d^+(r_i) = \sum_{i=1}^{q} d^-(s_i) \leq \sum_{i=1}^{q} d^-(t_i) \ .$$

The two inequalities above imply that $d^+(r*) = 0$, which is a contradiction since $(r*, s_1)$ is an edge in G'. Hence $m = |V_0|$, which by Menger's theorem implies our conclusion. ∎

Definition If G and G' are two graphs, we define the product graph $G \times G'$ on vertex set $V(G) \times V(G')$ in which (u, u') is joined to (v, v') if and only if $(u, v) \in E(G)$ and $(u', v') \in E(G')$.

Now, if G and G' are Plünnecke graphs of level n, it is easy to see that $G \times G'$ is also a Plünnecke graph of level n. We also have the nice property below.

Proposition 3.4 *Let G, G' Plünnecke graphs of level n. Then, for $1 \leq i \leq n$, we have $D_i(G \times G') = D_i(G)D_i(G')$.*

Proof Let $V(G) = V_0 \cup V_1 \cup \cdots \cup V_n$ and $V(G') = V_0' \cup V_1' \cup \cdots \cup V_n'$.

First, suppose that $Z \subseteq V_0$ and $Z' \subseteq V_0'$ are such that

$$D_i(G) = \frac{|\mathrm{Im}_i(Z)|}{|Z|}, \quad D_i(G') = \frac{|\mathrm{Im}_i(Z')|}{|Z'|} \ .$$

Clearly, $\mathrm{Im}_i(Z \times Z') \subseteq \mathrm{Im}_i(Z) \times \mathrm{Im}_i(Z')$. Therefore we have

$$D_i(G \times G') \leq \frac{|\mathrm{Im}_i(Z \times Z')|}{|Z \times Z'|} \leq \frac{|\mathrm{Im}_i(Z)|}{|Z|} \frac{|\mathrm{Im}_i(Z')|}{|Z'|} = D_i(G)D_i(G') \ .$$

We must now show that $D_i(G \times G') \geq D_i(G)D_i(G')$. Let $X \subseteq V_0 \times V_0'$. We write X as

$$X = \bigcup_a (\{a\} \times H_a) \ ,$$

where the union is over all $a \in V_0$ such that $H_a \neq \emptyset$ (H_a denotes the set of all $b \in V_0'$ such that $(a,b) \in X$). Let $Y \subseteq V_0 \times V_i'$ be such that if $(a,b) \in X$ and there is a path from b to v in G', where $v \in V_i'$, we say that $(a,v) \in Y$. Hence

$$|Y| = \left| \bigcup_a (\{a\} \times \mathrm{Im}_i(H_a)) \right| = \sum_a |\mathrm{Im}_i(H_a)| \geq D_i(G') \sum_a |H_a| = D_i(G')|X|$$

Similarly, now write Y as

$$Y = \bigcup_w (F_w \times \{w\}) \ ,$$

where again the union is made over all $w \in V_i'$ such that $F_w \neq \emptyset$. We can be easily observe that

$$\mathrm{Im}_i(X) = \bigcup_w (\mathrm{Im}_i(F_w) \times \{w\}) \ ,$$

therefore

$$|\mathrm{Im}_i(X)| = \sum_w |\mathrm{Im}_i(F_w)| \geq D_i(G) \sum_w |F_w| = D_i(G)|Y| \geq D_i(G)D_i(G')|X| \ .$$

The last inequality gives $D_i(G \times G') \geq D_i(G)D_i(G')$. ∎

Proposition 3.5 (Plünnecke) *Let G be a Plünnecke graph of level n. Then*

$$D_1 \geq D_2^{1/2} \geq D_3^{1/3} \geq \cdots \geq D_n^{1/n} \ .$$

Proof It is enough to prove that if G is a Plünnecke graph of level n, then $D_i \geq D_n^{i/n}$, for $1 \leq i \leq n$. If $D_n = 1$, the statement follows from Lemma 3.3. So we are left with 2 cases.

Case 1: $0 < D_n < 1$.

Let r and h positive integers to be chosen later. Consider the graph $G^r \times I_n(h)$, which is a Plünnecke graph of level n. By previous proposition, we know that

$$D_n(G^r \times I_n(h)) = (D_n(G))^r \binom{h+n-1}{n} \geq (D_n(G))^r \ \frac{h^n}{n!}$$

Given r, we choose h the least integer such that $(D_n(G))^r \ \frac{h^n}{n!} \geq 1$. Therefore, we have

$$h < (n!)^{1/n} D_n(G)^{-r/n} + 1 \ .$$

We now use Lemma 3.3. As $D_n(G^r \times I_n(h)) \geq 1$, we have $D_i(G^r \times I_n(h)) \geq 1$, so

$$(D_i(G))^r \geq \frac{1}{D_i(I_n(h))} = \binom{h+n-1}{n}^{-1} \geq h^{-i} \geq \left((n!)^{1/n} D_n(G)^{-r/n} + 1 \right)^{-i} \ .$$

Therefore

$$D_i(G) \geq \left((n!)^{1/n} D_n(G)^{-r/n} + 1 \right)^{-i/r} \ .$$

Let r tend to infinity, and we obtain $D_i(G) \geq D_n(G)^{i/n}$, as desired.

Case 2: $D_n > 1$.

This will be similar to the previous case. Consider the Plünnecke graph $G^r \times I_n(h)^{-1}$. We know that

$$D_n(G^r \times I_n(h)^{-1}) = (D_n(G))^r \binom{h+n-1}{n}^{-1} \geq (D_n(G))^r h^{-n}$$

Choose h the maximal integer such that $(D_n(G))^r h^{-n} \geq 1$. Therefore, we have

$$h > D_n(G)^{r/n} - 1 \ .$$

Next, Lemma 3.3 implies that $D_i(G^r \times I_n(h)^{-1}) \geq 1$, so

$$D_i(G) \geq \binom{h+n-1}{n}^{1/r} \geq \frac{h^{i/r}}{(i!)^{1/r}} \geq \frac{(D_n(G)^{r/n} - 1)^{i/r}}{(i!)^{1/r}} \ .$$

Again, by letting $r \to \infty$, we obtain $D_i(G) \geq D_n(G)^{i/n}$. ∎

3.2 Sumset estimates

Proposition 3.6 (Plünnecke) *Let A and B subsets of an additive group, such that $|A+nB| \leq C|A|$. Then, for any $n' \geq n$, there exists $A' \subseteq A$ such that $|A' + n'B| \leq C^{n'/n}|A'|$.*

Proof As we've seen in example above, define the Plünnecke graph G by setting $V_i = A + iB$ and $(v, v') \in E(G)$ if and only if $v' - v \in B$. Then we have

$$D_n = \inf_{Z \subseteq A} \frac{\mathrm{Im}_n(Z)}{|Z|} \leq \frac{\mathrm{Im}_n(A)}{|A|} \leq \frac{|A+nB|}{|A|} \leq C \ .$$

It follows from Proposition 3.5 that $D_{n'} \leq C^{n'/n}$, for any $n' \geq n$. This implies the conclusion. ∎

An easy consequence of the previous proposition is that if $|A + A| \leq C|A|$, then $|kA| \leq C^k|A|$. Indeed, take $A = B$ and $n = 1$ to get

$$|kA| \leq |A' + kA| \leq C^k|A'| \leq C^k|A| \ .$$

We would like to provide a generalisation for the above consequence. For this purpose, we need the following simple, but essential lemma:

Lemma 3.7 (Ruzsa) *Let U, V, W subsets of an additive group. Then*

$$|U||V - W| \leq |U + V||U + W| \ .$$

Proof For each $d \in V - W$, we fix a pair $(v(d), w(d)) \in V \times W$ such that $v(d) - w(d) = d$ (there might be more such pairs, we are only interested in one of them). We now look at the map from $U \times (V - W)$ to $(U + V) \times (U + W)$ which sends (u, d) to $(u + v(d), u + w(d))$. It is easy to see that this map is injective, so the conclusion follows. ∎

We are now ready to state and prove the main result of this section.

Theorem 3.8 (Plünnecke-Ruzsa) *Let A a subset of an additive group and suppose that $|A+A| \leq C|A|$. Then $|kA - lA| \leq C^{k+l}|A|$.*

Proof Suppose without losing the generality that $l \geq k$. We apply Proposition 3.6 twice to get $A" \subseteq A' \subseteq A$ such that

$$|A' + kA| \leq C^k |A'| \tag{21}$$

and

$$|A" + lA| \leq (C^k)^{l/k} |A"| = C^l |A"| \tag{22}$$

Therefore, we have

$$\begin{aligned} |A"||kA - lA| &\leq |A" + kA||A" + lA| \quad \text{(by Ruzsa's lemma)} \\ &\leq |A' + kA||A" + lA| \quad (A" \subseteq A') \\ &\leq C^{k+l} |A'||A"| \quad \text{(by (21) and (22))} \\ &\leq C^{k+l} |A||A"| \quad (A' \subseteq A) \end{aligned}$$

Consequently, we have $|kA - lA| \leq C^{k+l}|A|$ ∎

4 Geometry of numbers

In this section we will see that some geometrical objects such as convex bodies and lattices have applications to additive combinatorics. We will see that there is a close relation between their geometrical structure (volume, rank etc.) and the behavior of GAP's or Bohr sets.

4.1 Lattices

Definition Given m linearly independent vectors $b_1, \dots, b_m \in \mathbb{R}^n$, we define the *lattice* generated by them as

$$\Lambda(b_1, \dots, b_m) := \left\{ \sum_{i=1}^{m} x_i b_i | x_i \in \mathbb{Z} \right\} .$$

$B = \{b_1, \dots, b_m\}$ is called the *basis* of the lattice. We call m the *rank* and n the *dimension*. If $m = n$, we say the lattice has *full rank*.

We can easily see that Λ is a discrete additive subgroup of $\mathbb{R}^n$.

Equivalently, if we define B as the $n \times m$ matrix with columns $b_1, \dots, b_m$, we can think of Λ as

$$\Lambda(B) = \{Bx | x \in \mathbb{Z}^m\} .$$

Note that the same lattice can be obtained from different basis. See the figures below.

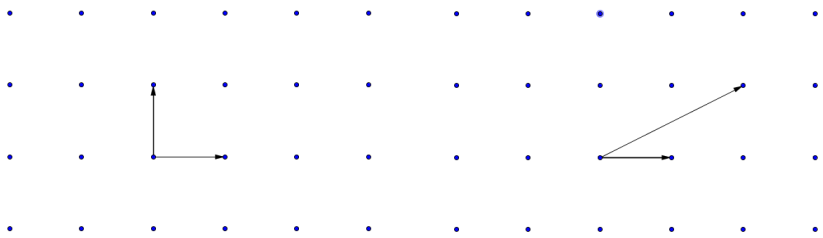


Figure 4: Two different bases for $\mathbb{Z}^2$

Definition For any lattice basis B, we define

$$P(B) := \{Bx | x \in \mathbb{R}^n, 0 \leq x_i < 1, \forall i\}$$

Note that $P(B)$ depends on the basis B. The same lattice can have different fundamental regions (see figure below). Also, we observe that we can tile $span(B)$ by translates of $P(B)$.

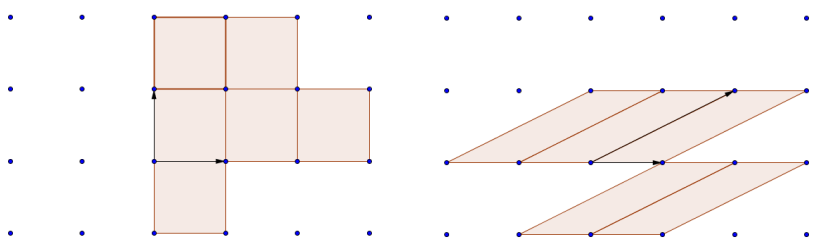


Figure 5: Two different fundamental regions for the same lattice

Next, we would like to define a quantity of the lattice which is independent of the basis.

Definition Let $\Lambda = \Lambda(B)$ a lattice of rank m. We define the determinant of Λ, denoted by $\det(\Lambda)$, as the m-dimensional volume of $P(B)$, which cand be written more explicitly as

$$\det(\Lambda) := \sqrt{\det(B^T B)}$$

If Λ is a full rank lattice, then $\det(\Lambda) = |\det(B)|$.

We will next prove that this definition makes sense. For this purpose, we have first to introduce the following lemma:

Lemma 4.1 *Two bases $B_1, B_2 \in \mathbb{R}^{n\times m}$ generate the same lattice ($\Lambda(B_1) = \Lambda(B_2)$) if and only if $B_2 = B_1 U$, for some $U \in \mathbb{Z}^{m\times m}$ such that* $\det(U) = \pm 1$.

Proof "$\Longrightarrow$" Assume $\Lambda(B_1) = \Lambda(B_2)$.
Then for each of the m columns b_i of B_2, $b_i \in \Lambda(B_1)$. Hence there exists $U \in \mathbb{Z}^{m\times m}$ such that $B_2 = B_1 U$. Similarly, there exists $V \in \mathbb{Z}^{m\times m}$ sucht that $B_1 = B_2 V$. Therefore $B_2 = B_2 VU$, so

$$B_2^T B2 = (VU)^T B_2^T B_2 (VU) \ .$$

As $B_2^T B_2 \in \mathbb{R}^{m\times m}$ is invertible, by taking determinants, we get $\det(V)\det(U) = \pm 1$. As $U \in \mathbb{Z}^{m\times m}$, the conclusion follows.

"$\Longleftarrow$" Suppose $B_2 = B_1 U$, for some $U \in \mathbb{Z}^{m\times m}$, $\det(U) = \pm 1$.
It follows that $\Lambda(B_2) \subseteq \Lambda(B_1)$. But also, $B_1 = B_2 U^{-1}$, and as $U \in \mathbb{Z}^{m\times m}$ with $\det(U) = \pm 1$, we have $U^{-1} \in \mathbb{Z}^{m\times m}$, $\det(U^{-1}) = \pm 1$. Therefore $\Lambda(B_1) \subseteq \Lambda(B_2)$. ∎

Proposition 4.2 *The determinant of a lattice is independent of the choice of basis B.*

Proof If B_1, B_2 are two bases of Λ, then by 4.1, $B_2 = B_1 U$, for some $U \in \mathbb{Z}^{m\times m}$, $\det(U) = \pm 1$. Hence

$$\sqrt{\det(B_2^T B_2)} = \sqrt{\det(U^T B_1^T B_1 U)} = \sqrt{\det(B_1^T B_1)} \quad ∎$$

From now on we will only work with full rand lattices, even if it will not be specified every time.

Definition A sublattice Λ' of a full rank lattice Λ in $\mathbb{R}^n$ is a subgroup of the addition group Λ, which is also a full rank lattice.

We have the following lemma relating the index of Λ' in Λ with the determinants of the lattices:

Lemma 4.3 *Let Λ a lattice and Λ' a sublattice of Λ. Then*

$$|\Lambda/\Lambda'| = \frac{\det(\Lambda')}{\det(\Lambda)} \ .$$

Proof Let P' be a fundamental domain for Λ'. Then $\forall x \in \mathbb{R}^n$ can be written as $x = y + z$, where $y \in \Lambda'$ and $z \in P'$. In particular, $\forall x \in \Lambda$, $x = y + z$, for some $y \in \Lambda'$ and $z \in P'$. Hence the number of cosets of Λ' in Λ is $|P' \cap \Lambda|$.

Now $|P' \cap \Lambda|$ represents the number of fundamental regions P which tile P'. Hence

$$|\Lambda/\Lambda'| = |P' \cap \Lambda| = \frac{\mathrm{vol}(P')}{\mathrm{vol}(P)} = \frac{\det(\Lambda')}{\det(\Lambda)} \quad ∎$$

4.2 Minkowski's theorems

We will denote by $\text{vol}(A)$ the n-dimensional volume of a set $A \subset \mathbb{R}^n$. We will only work with bounded open sets in order to avoid issues with measurability.

- If $A \subset \mathbb{R}^n$ and $\lambda \in \mathbb{R}$, we denote by λA the dilatiation by λ:

$$\lambda A := \{\lambda x : x \in A\}$$

  We can easily see that $\text{vol}(\lambda A) = |\lambda|^n \text{vol}(A)$.

- A set A in $\mathbb{R}^n$ is convex if $(1-\theta)x + \theta y \in A$, $\forall\ x, y \in A$, $\forall\ 0 \leq \theta \leq 1$.

- A set A in $\mathbb{R}^n$ is symmetric if $x \in A \implies -x \in A$.

- We call A a *convex body* if A is convex, open, non-empty and bounded.

Theorem 4.4 (Blichfeld) *Let Λ a (full rank) lattice and K a measurable subset of $\mathbb{R}^n$ with $vol(K) > \det(\Lambda)$. Then there exists $z_1, z_2 \in K$ two distinct points such that $z_1 - z_2 \in \Lambda$.*

Proof Let B be a basis for Λ. As x ranges over Λ, the sets $x + P(B)$ form a partition (tiling) of $\mathbb{R}^n$. Let $K_x = K \cap (x + P(B))$, for $x \in \Lambda$. As

$$K = \bigcup_{x \in \Lambda} K_x \ ,$$

it follows that $vol(K) = \sum_{x \in K_x} \text{vol}(K_x)$.

Let $B_x = K_x - x$. Then $B_x \subseteq P(B)$ and $\text{vol}(B_x) = \text{vol}(K_x)$. Therefore

$$\sum_{x \in \Lambda} \text{vol}(B_x) = \sum_{x \in \Lambda} \text{vol}(K_x) = \text{vol}(K) > \text{vol}(P(B)) \ .$$

So there exist $x, y \in \Lambda$, $x \neq y$ such that $B_x \cap B_y \neq \emptyset$. Let $z \in B_x \cap B_y$. Then $z + x \in K_x \subset K$ and $z + y \in K_y \subset K$, hence $(z + x) - (z + y) = x - y \in \Lambda$. ∎

Theorem 4.5 (Minkowski's First Theorem) *Let Λ be a full rank lattice and K a symmetric convex body such that $vol(K) > 2^n \det(\Lambda)$. Then K contains a non-zero lattice point.*

Proof We can easily see that

$$\text{vol}\left(\frac{1}{2}K\right) = \frac{1}{2^n}\text{vol}(K) > \det(\Lambda) \ .$$

By Blichfeld lemma 4.4, $\exists z_1, z_2 \in \frac{1}{2}K$ distinct points such that $z_1 - z_2 \in \Lambda$. By definition, $2z_1, 2z_2 \in K$. As K is symmetric, it follows that $-2z_2 \in K$. By convexity,

$$\frac{2z_1 - 2z_2}{2} = z_1 - z_2 \in K \ . \quad \blacksquare$$

Even if the proof is very simple, the constant in Minkowski's first theorem is the best possible. To see that 2^n cannot be improved, take $\Lambda = \mathbb{Z}^n$ and the cube $K := \{(x_1, \ldots, x_n) : -1 < x_i < 1, \forall i\}$. However, we will provide a "multiparameter" generalisation for Minkowski's first theorem by defining the successive minima.

Definition Let Λ be a full rank lattice in $\mathbb{R}^n$ and K a convex body in $\mathbb{R}^n$. We define the *successive minima* $\lambda_j = \lambda_j(K, \Lambda)$, for $1 \leq j \leq n$ as

$$\lambda_j := \inf\{\lambda > 0 : \lambda K \text{ contains } j \text{ linearly independent elements of } \Lambda\} \ .$$

Minkowski's second thoerem provides a remarkable relation between $vol(K)$ and $\det(\Lambda)$ involving successive minima.

Theorem 4.6 (Minkowski's Second Theorem) *Let $K \subset \mathbb{R}^n$ be a symmetric convex body and Λ be a full rank lattice. Let $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ be the successive minima of K with respect to Λ. Then*

$$\frac{2^n}{n!}\det(\Lambda) \leq \lambda_1\lambda_2\ldots\lambda_n vol(K) \leq 2^n \det(\Lambda) \ .$$

Before we can prove the theorem, we need the following lemma.

Lemma 4.7 (Squeezing lemma) *Let K be a symmetric convex body in $\mathbb{R}^n$ and let A be an open subset of K. If V is a k-dimensional subspace of $\mathbb{R}^n$, then for $0 \leq \theta \leq 1$, there exists an open subset A' of K such that $vol(A') = \theta^k vol(A)$ and*

$$(A' - A') \cap V \subseteq \theta(A - A) \cap V \ .$$

Proof We can assume without losing the generality that $V = \mathbb{R}^k$ and we have $\mathbb{R}^n = \mathbb{R}^k \times \mathbb{R}^{n-k}$. Any point $w \in K$ can be viewed as having the coordinates $w = (x, y)$, $x \in \mathbb{R}^k$, $y \in \mathbb{R}^{n-k}$.

Let $\pi : \mathbb{R}^n \to \mathbb{R}^{n-k}$ be the standard projection map, which restricts to $\pi : K \to \pi(K)$. We construct the map $f : \pi(K) \to K$ by mapping $y \in \pi(K)$ to the centre of mass of $\pi^{-1}(y)$.

Consider $\phi : K \to K$ which maps $w = (x, y)$ to $\theta w + (1-\theta)f(y)$. Since both $w, f(y) \in K$ and K is convex, it follows that $\phi(w) \in K$, so it is well defined. We can easily see from the definition that the second coordinate of $\phi(w)$ is y.

Let $A' = \phi(A)$, which is an open subset of K. Hence A' is the result of taking each k-dimensional "slice" of A parallel to $V = \mathbb{R}^k$ and scalling it by a factor of θ. The scalling is done centered at the centre of mass of the original slice.By Cavalieri's Principle, $\mathrm{vol}(A') = \theta^k \mathrm{vol}(A)$ (the map contracts A by a factor of θ with respect to $V = \mathbb{R}^k$).

Now, take $v = \phi(w) - \phi(v')$, where $w = (x, y)$, $w' = (x', y')$. If $v \in V$, then the second coordinate of v is zero, and using the fact that ϕ preserve the second coordinate, we get $y = y'$. Therefore $v = \theta(w - w')$. Hence, if $v \in (A' - A') \cap V$, it implies that $v \in \theta(A - A)$. ∎

Now we have all the tools required for the proof of Minkowski's second theorem.

Proof By the definition of successive minima, there exists a linear independent set $B = \{b_1, \ldots, b_n\} \subset \Lambda$ such that $b_i \in \overline{\lambda_i K} \setminus \lambda_i K$ ($\overline{\lambda_i K}$ denotes the closure). Let B_i the vector subspace of $\mathbb{R}^n$ spanned by $\{b_1, \ldots, b_i\}$, $1 \leq i \leq n$. Set $B_0 = \{0\}$.

Let $A_0 = \frac{\lambda_n}{2} K$. We apply the Squeezing lemma to get $A_n - 1 \subseteq \cdots \subseteq A_1 \subseteq A_0$ such that

$$\mathrm{vol}(A_j) = \left(\frac{\lambda_j}{\lambda_{j+1}}\right)^j \mathrm{vol}(A_{j-1}) \tag{23}$$

and

$$(A_j - A_j) \cap B_j \subseteq \frac{\lambda_j}{\lambda_{j+1}}(A_{j-1} - Aj - 1) \cap B_j \tag{24}$$

for $1 \leq j \leq n-1$.

As $\mathrm{vol}(A_0) = \left(\frac{\lambda_n}{2}\right)^n \mathrm{vol}(K)$, by multiplying all equations (23) for $1 \leq j \leq n-1$ we get

$$2^n \mathrm{vol}(A_{n-1}) = \lambda_1 \ldots \lambda_n \mathrm{vol}(K). \tag{25}$$

Moreover, using (24) and the fact that $B_1 \subset B_2 \subset \cdots \subset B_n$, we get that

$$(A_{n-1} - A_{n-1}) \cap B_j \subset \frac{\lambda_j}{\lambda_n}(A_{j-1} - A_{j-1}) \cap B_j. \tag{26}$$

As K is symmetric, $\frac{\lambda_n}{2}K - \frac{\lambda_n}{2}K = \lambda_n K$. SInce $A_{j-1} \subset A_0 = \frac{\lambda_n}{2}K$, fro the last equation we get that

$$(A_{n-1} - A_{n-1}) \cap B_j \subset (\lambda_j K) \cap B_j \tag{27}$$

for all $1 \leq j \leq n$.

By definition of successive minima, $(\lambda_j K) \cap B_j$ contains no lattice points outside B_{j-1}. Therefore $A_{n-1} - A_{n-1}$ contains no lattice points except the origin. Therefore A_{n-1} doesn't satisfy the conclusion of Blichfeld's lemma. Hence, we must have that

$$\text{vol}(A_{n-1}) \leq \det(\Lambda) \ .$$

This and (25) imply the conclusion. ∎

The following important lemma is a very good example of how the techniques above can be applied to additive combinatorics. We will also use this lemma later on in the proof of Freiman's theorem.

Proposition 4.8 *Let $R = \{r_1, \ldots, r_k\} \subseteq \mathbb{Z}_N$ and $0 < \delta < \frac{1}{2}$. Then the Bohr neighbourhood $B(R, \delta)$ contains a proper k-dimensional GAP of size at least $\left(\frac{\delta}{k}\right)^k N$.*

Proof Consider Λ the k-dimensional lattice generated by $N\mathbb{Z}^k$ and $(r_1, \ldots, r_k)$ (this is a slight abuse if notation, as r_i's are assumed to be integers). Note that this is not the proper definition of a lattice, as it is spanned by $k+1$ vectors, but it is always possible to find k vectors which span the same lattice.

For any $x \in \Lambda$, let x_N be the vector with coordinates reduced modulo N. So for each $x \in \Lambda$, $x_N = (sr_1, \ldots, sr_k)$, for some $0 \leq s \leq N-1$. Therefore $|\Lambda / N\mathbb{Z}^k| = N$. Clearly, $\det(\mathbb{Z}^k) = N^k$, so from 4.3 we obtain

$$\det(\Lambda) = N^{k-1}. \tag{28}$$

Let K be the open cube $\{x \in \mathbb{R}^k : \|x\|_\infty < \delta N\}$, which is a symmetric convex body with volume $(2\delta N)^k$. Let $\lambda_1, \ldots, \lambda_k$ the successive minima of K and $B = \{b_1, \ldots, b_k\}$ the basis for Λ generated in this way ($b_i \in \overline{\lambda_i K} \setminus \lambda_i K$). Therefore

$$\|b_i\|_\infty \leq \lambda_i \delta N, \ \forall \ 1 \leq i \leq k \ . \tag{29}$$

Since $b_i \in \Lambda$,

$$b_i = x_i(r_1, \ldots, r_k) + Nv \ , \tag{30}$$

where $v \in N\mathbb{Z}^k$ and $0 \leq x_i \leq N-1$. We may regard $x_i \in \mathbb{Z}_N$.

From (29) we get that

$$\left|\frac{x_i r}{N}\right| \leq \lambda_i \delta, \quad \forall \ 1 \leq i \leq k, \forall \ r \in R \ . \tag{31}$$

Now we study the GAP

$$Q = \left\{ \mu_1 x_1 + \cdots + \mu_k x_k : |\mu_i| \leq \left\lfloor \frac{1}{k\lambda_i} \right\rfloor \right\} \subseteq \mathbb{Z}_N \ . \tag{32}$$

The claim is that $Q \subseteq B(R, \delta)$. Indeed, if $r \in R$,

$$\begin{aligned} \left|\frac{r(\mu_1 x_1 + \cdots + \mu_k x_k)}{N}\right| &\leq \sum_{i=1}^{k} |\mu_i| \left|\frac{r x_i}{N}\right| \\ &\leq \sum_{i=1}^{k} \left\lfloor \frac{1}{k\lambda_i} \right\rfloor \lambda_i \delta \quad \text{from (31) and (32)} \\ &\leq \delta \end{aligned}$$

We'll now show that Q is proper. Suppose that

$$\mu_1 x_1 + \cdots + \mu_k x_k = \mu_1' x_1 + \cdots + \mu_k' x_k, \quad |\mu_i|, |\mu_i'| \leq \left\lfloor \frac{1}{k\lambda_i} \right\rfloor \tag{33}$$

Then consider the vector

$$b = (\mu_1 - \mu_1')b_1 + \cdots + (\mu_k - \mu_k')b_k \ .$$

Using (30) and (33), we can easily see that $b \in N\mathbb{Z}^k$. Also

$$\begin{aligned} \|b\|_\infty &\leq \sum_{i=1}^{k} 2 \left\lfloor \frac{1}{k\lambda_i} \right\rfloor \|b_i\|_\infty \\ &\leq 2\delta N \quad \text{by (29)} \end{aligned}$$

Since we assumed that $0 < \delta < \frac{1}{2}$ and we know that $b \in N\mathbb{Z}^k$, we must have $b = 0$. Hence, by the linear independence of the b_i's it follows that $\mu_i = \mu_i'$, for all i. So Q is proper. There are at least $1/k\lambda_i$ integers in the interval $[-1/k\lambda_i, 1/k\lambda_i]$. From the definition of Q (32) the the fact that it is proper, it must have size at least

$$\frac{1}{k^k \lambda_1 \dots \lambda_k} \ .$$

But

$$\begin{aligned} \frac{1}{k^k \lambda_1 \dots \lambda_k} &\geq \frac{1}{k^k} \frac{\text{vol}(K)}{2^k \text{vol}(\Lambda)} \quad \text{(by Minkowsky's second theorem)} \\ &= \frac{1}{k^k} \frac{2^k \delta^k N^k}{2^k N^{k-1}} \quad \text{by (28)} \\ &= \left(\frac{\delta}{k}\right)^k N \quad \blacksquare \end{aligned}$$

5 Freiman theorem

5.1 Freiman homomorphisms

Definition Let G and H be additive groups and $A \subseteq G$, $B \subseteq H$. A Freiman k-homomorphism from A to B is a map $\phi : A \to B$ such that

$$x_1 + x_2 + \cdots + x_k = y_1 + y_2 + \ldots y_k \implies \phi(x_1) + \cdots + \phi(x_k) = \phi(y_1) + \cdots + \phi(y_k)$$

for all $x_1, \ldots, x_k, y_1, \ldots, y_k \in A$.

In addition, if ϕ is invertible and $\phi^{-1} : B \to A$ is a k-homomorphism, then ϕ is called a k-isomorphism. We use the notation $A \cong_k B$ to express that A and B are k-isomorphic.

Remarks 5.1

1. *If $\phi : G \to G'$ is a group homomorphism (resp. isomorphism) from group G to group G', then it induces a Freiman homomorphism (resp. isomorphism) from $A \subseteq G$ to $\phi(A)$ of any order.*
2. *If $A \subseteq Z$ and $x \in Z$, Z additive group, then the translation map $\phi : A \to Z$ defined by $\phi(y) = y + x$ is a Freiman isomorphism of any order.*
3. *If $\phi : A \to B$ is a k - homomorphism (resp. isomorphism), then ϕ is a l-homomorphism (resp. isomorphism) for $1 \leq l \leq k$.*

   Proof *If $x_1 + x_2 + \cdots + x_l = y_1 + y_2 + \ldots y_l$, for some $x_1, \ldots x_l, y_1, \ldots, y_l \in A$, then*

   $$x_1 + \cdots + x_l + \underbrace{a + \cdots + a}_{k-l} = y_1 + \cdots + y_l + \underbrace{a + \cdots + a}_{k-l}$$

   for some fixed $a \in A$. As ϕ is a k-homomorphism, it follows that

   $$\phi(x_1) + \cdots + \phi(x_l) + \underbrace{\phi(a) + \cdots + \phi(a)}_{k-l} = \phi(y_1) + \cdots + \phi(y_l) + \underbrace{\phi(a) + \cdots + \phi(a)}_{k-l} .$$

   Therefore $\phi(x_1) + \cdots + \phi(x_l) = \phi(y_1) + \cdots + \phi(y_l)$, so ϕ is a l-homomorphism.

   If $A \cong_k B$, then the same argument holds for ϕ^{-1}, therefore $A \cong_l B$.
4. *If $\phi_1 : A \to B$ and $\phi_2 : B \to C$ are k-homomorphisms (resp. isomorphisms), then $\phi_2 \circ \phi_1$ gives a k-homomorphism (resp. isomorphism).*
5. *Let q a number coprime to N. Then the map $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ given by $\phi(x) = qx$ is a Freiman isomorphism of any order.*
6. *Let $A \subseteq \mathbb{Z}$ and N any positive integer. Then the reduction map (mod N) $\phi : A \to \mathbb{Z}_N$ is a Freiman homomorphism of any order.*
   However, it is not usually a Freiman isomorphism (for example, $\phi : \{0, 1\} \to \mathbb{Z}_2$, where $\{0, 1\} \in \mathbb{Z}$ is not a 2-isomorphism, because $0 + 0 \neq 1 + 1$ in $\mathbb{Z}$).
   But, if $A \subseteq \{1, 2, \ldots, m\}$ and $km < N$, then ϕ is also a k-isomorphism.
7. *Consider $\phi : \mathbb{Z}_N \to \mathbb{Z}$ by choosing a representative for a congruence class in $\{1, 2, \ldots N\}$. This is not a k-homomorphism as it stands, but if we restrict to a subset of $\mathbb{Z}_N$ of the form $\left\{ \frac{jN}{k} < x \leq \frac{(j+1)N}{k} \right\}$, this is a k-homomorphism.*

Lemma 5.2 *If $h = h'(k+l)$ and $A \cong_h B$, then $kA - lA$ and $kB - lB$ are h'-isomorphic.*

Proof Let $\phi : A \to B$ a h-isomorphism. Let $c_1, \dots c_{h'}, d_1, \dots, d_{h'} \in kA - lA$ such that

$$c_1 + \cdots + c_{h'} = d_1 + \cdots + d_{h'} \ .$$

Then, for $1 \leq i \leq h'$,

$$c_i = a_{i1} + \dots a_{ik} - b_{i1} - \dots b_{il}$$
$$d_i = \alpha_{i1} + \dots \alpha_{ik} - \beta_{i1} - \dots \beta_{il}$$

for some a's, b's, α's and β's in A. Denote

$$g(c_i) = \phi(a_{i1}) + \dots \phi(a_{ik}) - \phi(b_{i1}) - \dots \phi(b_{il} \ .)$$

By definition of h-isomorphism and Remark 3, it follows that g is well defined, whatever the choice of a's and b's. It follows that

$$a_{11} + \cdots + a_{h'k} + \beta_{11} + \dots \beta_{h'l} = \alpha_{11} + \cdots + \alpha_{h'k} + b_{11} + \dots b_{h'l}$$

and because ϕ is a h-homomorphism,

$$\phi(a_{11}) + \cdots + \phi(a_{h'k}) + \phi(\beta_{11}) + \dots \phi(\beta_{h'l}) = \phi(\alpha_{11}) + \cdots + \phi(\alpha_{h'k}) + \phi(b_{11}) + \dots \phi(b_{h'l}) \ .$$

Hence,

$$g(c_1) + \dots g(c_{h'}) = g(d_1) + \dots g(d_{h'}) \ .$$

Therefore g is a h'-isomorphism. ∎

Lemma 5.3 *Let $\phi : A \to \mathbb{Z}$ a k-homomorphism, $k \geq 2$, and P a d-dimensional GAP, $P \subseteq A$. Then $\phi(P)$ is a d-dimensional AP. Moreover, if ϕ is a k-isomorphism and P is proper, then $\phi(P)$ is proper.*

Proof Let

$$P = \{a + x_1 v_1 + \cdots + x_d v_d | 0 \leq x_i \leq l_i, i = 1, 2, \dots, d\} \ .$$

By translational invariance (as seen in the remarks), we may assume that $a = 0$ and $\phi(0) = 0$. Since in particular ϕ is a 2-homomorphism, we see that $\phi(v_i + v_i) = \phi(v_i) + \phi(v_i)$, $1 \leq i \leq d$. Iterating this we see that $\phi(l_i v_i) = l_i \phi(v_i)$. Also, we note that $\phi(v_i + v_j) = \phi(v_i) + \phi(v_j)$, for $1 \leq i < j \leq d$. Combonong these two, observations, we note that

$$\phi(x_1 v_1 + \cdots + x_d v_d) = x_1 \phi(v_1) + \cdots + x_d \phi(v_d) \ .$$

Therefore

$$\phi(P) = \{x_1 \phi(v_1) + \cdots + x_d \phi(v_d) | 0 \leq x_i \leq l_i, i = 1, 2, \dots, d\} \ .$$

Note that is ϕ is a Freiman isomorphism, then $|P| = |\phi(P)|$, so if P is proper, $\phi(P)$ must be proper. ∎

The following theorem by Ruzsa allows us to make the transition from $\mathbb{Z}$ to $\mathbb{Z}_N$:

Theorem 5.4 (Ruzsa Embedding Lemma) *Let $A \subseteq \mathbb{Z}$, $|kA - kA| \leq C|A|$, then for any prime $N > C|A|$, $\exists A' \subseteq A$, $|A'| > \frac{|A|}{k}$ such that A' is k-isomorphic to a subset of $\mathbb{Z}_N$.*

Proof Let p be a large enough prime. Then the reduction map $(\text{mod } p)$ $\phi_1 : A \to \mathbb{Z}_p$ is a k-isomorphism (as it can be seen in the remarks above). Also, for each $1 \leq q \leq p$, we define the map $\phi_2(q) : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $x \to qx$, which is also a k-isomorphism. Usually, the map $\phi_3 : \mathbb{Z}_p \to \mathbb{Z}$ which sends the corresponding residue to the interval $\{0, 1, \dots, p\}$ is not a Freiman homomorphism. However, it is a k-homomorphism when restricted to an interval of the form

$I_j = \left(\frac{(j-1)p}{k}, \frac{jp}{k}\right]$, $1 \leq j \leq k$. Finally, for any prime N, the reduction map $\phi_4 : \mathbb{Z} \to \mathbb{Z}_N$ (mod N), is a k-homomorphism.

For each $1 \leq q \leq p-1$, we find a subset A_q of A, $|A_q| \geq \frac{|A|}{k}$ such that $\forall a \in A_q$, $qa \pmod p$ lie in an interval of the type I_j, for some $1 \leq j \leq k$ (by pigeonhole principle). Therefore, we have the composition of maps

$$\mathbb{Z} \xrightarrow{\phi_1} \mathbb{Z}_p \xrightarrow{\phi_2(q)} \mathbb{Z}_p \xrightarrow{\phi_3} \mathbb{Z} \xrightarrow{\phi_4} \mathbb{Z}_N$$

which is a k-homomorphism when restricted to A_q, because the composition of k-homomorphisms gives a k-homomorphism. To conclude the proof, we need to find a q for each the map $\phi = \phi_4 \circ \phi_3 \circ \phi_2(q) \circ \phi_1$, $\phi : A_q \to \mathbb{Z}_N$ is a k-isomorphism.

If ϕ is not a k-isomorphism, then $\exists\ a_1, \ldots, a_k, b_1, \ldots, b_k \in A_q$ such that

$$\phi(a_1) + \cdots + \phi(a_k) = \phi(b_1) + \cdots + \phi(b_k) \quad \text{but} \quad \sum_{i=1}^{k} a_i \neq \sum_{i=1}^{k} b_i \ .$$

Note $s = a_1 + \cdots + a_k - b_1 - \cdots - b_k$. This means that

$$q(a_1 + \cdots + a_k) \neq q(b_1 + \cdots + b_k) \pmod p \ ,$$

so $qs \not\equiv 0 \pmod p$, but

$$(qs \pmod p) \ \equiv \ 0 \pmod N \ . \tag{34}$$

Next, we fix s. We know $s \not\equiv 0 \pmod p$. As q ranges over $\{1, 2, \ldots, p-1\}$, $qs \pmod p$ also covers $\{1, 2, \ldots, p-1\}$. Equation (34) holds if N divides $(qs \pmod p)$, which can happen for at most $\frac{p-1}{N}$ values of q. But $s \in (kA - kA) \setminus \{0\}$, so by assumption there are at most $C|A|$ values s can attain. So there are at most $C|A|(p-1)/N$ values values for q for which ϕ is not a k-isomorphism, and $C|A|(p-1)/N < p$ when $N > C|A|$. ∎

5.2 Proof of Freiman theorem

In this subsection we will put the results obtained so far together in order to obtain the desired result. We combine results from different areas, just another example how connected and surprising mathematics is.

Theorem 5.5 *Let $A \in \mathbb{Z}$, $|A| = n$ such that $|A + A| \leq Cn$. Then $2A - 2A$ contains a proper GAP of dimension d at most $2^{11} C \log C$ and size at least $C^{16} \left(\frac{1}{20d}\right)^d n$.*

Proof From Plünnecke-Ruzsa inequality, it follows that $|8A - 8A| \leq C^{16} n$. Next, we apply Ruzsa Embedding Lemma with $k = 8$. Choose a prime $N \in (C^{16}n, 2C^{16}n]$ (such a prime exists by Bertrand's postulate). Hence there exists $A' \subseteq A$, $|A'| \geq \frac{n}{8}$ such that $A' \cong_8 X$, where $X \subseteq \mathbb{Z}_N$. Now

$$|X| = |A'| \geq \frac{n}{8} \geq \frac{N}{16C^{16}} \tag{35}$$

Moreover, $A' \cong_8 X \implies A' \cong_2 X$ (by remark 3), so $|A' + A'| = |X + X|$. So

$$|X + X| = |A' + A'| \leq |A + A| \leq C|A| \leq 8C|A'| = 8C|X|$$

Now we can apply Theorem 2.10. We know from (35) that α from the statement of the Theorem 2.10 satisfies $\frac{1}{\alpha} \leq 16C^{16}$. Hence $2X - 2X$ contains a Bohr neighbourhood $B(K, \delta)$, such that

$$d = |K| \leq 2^{11} C \log C$$

and

$$\delta \geq \frac{1}{20}|K| \geq (2^{16}C\log C)^{-1} \ .$$

By Proposition 4.8 , $B(K,\delta)$ contains a proper GAP of order d and size at least

$$\left(\frac{\delta}{d}\right)^d N \geq \left(\frac{1}{20d}\right)^d N \geq C^{16}\left(\frac{1}{20d}\right)^d n \ .$$

Hence $2X-2X$ contains a proper GAP of dimension $d \leq 2^{11}C\log C$ and size at least $C^{16}\left(\frac{1}{20d}\right)^d n$.

The fact that $A' \cong_8 X$ implies that $2A'-2A' \cong_2 2X-2X$ (by 5.2). As Freiman isomorphisms preserve GAPs (by 5.3), $2A'-2A'$ contains the desired GAP. ∎

Next we provide an algorithm to find a GAP such that $\overline{P}$ such that $A \subseteq \overline{P}$ if we know that $|A+A| \leq C|A|$ and that $2A-2A$ contains a GAP.

Proposition 5.6 *Let $A \subseteq \mathbb{Z}$, $|A| = n$ such that $|A+A| \leq Cn$ and $2A-2A$ contains a proper GAP P of size dimension d and size βn. Then A is contained in a GAP of size at most $d + 20C\log\left(C^4/\beta\right)$ and dimension at most $2^d\beta\left(C^4/\beta\right)^{40C} n$.*

Proof Let $P_0 = P$. We assume there exists $R_0 \subseteq A$ such that $|R_0| = 10C$ and

$$(P_0 + x) \cap (P_0 + y) = \emptyset \quad \text{for } x, y \in R_0,\ x \neq y \ .$$

We define $P_1 = P_0 + R_0$. Therefore we have $|P_1| = 10C|P|$.

Next, we assume there exists $R_1 \subseteq A$, $|R_1| = 10C$ such that

$$(P_1 + x) \cap (P_1 + y) = \emptyset \quad \text{for } x, y \in R_1,\ x \neq y \ .$$

We define $P_2 = P_1 + R_1$. So we must have $|P_2| = |P_1||R_1| = (10C)^2|P|$. Continue in this way.

If the algorithm can be iterated t times, we obtain

$$P_t = P + R_0 + \cdots + R_{t-1} \subseteq 2A - 2A + tA \ .$$

Using Plünnecke-Ruzsa inequality 3.8 we obtaint that $|P_t| \leq C^{4+t}n$. Bu we know that

$$|P_t| = (10C)^t|P| = \beta(10C)^t n \ .$$

Therefore

$$\beta(10C)^t \leq C^{4+t} \ ,$$

which implies

$$t \leq \log\left(\frac{C^4}{\beta}\right) \ , \tag{36}$$

so the algorithm is finite.

After t steps, R_t cannot be defined, so we have $R_t' \subseteq A$, $|R_t| < 10C$ maximal subject to the translates $P_t + x$, $x \in R_t'$ being disjoint. Therefore, for any $a \in A$, there exists $x \in R_t'$ such that

$$(P_t + a) \cap (P_t + x) \neq \emptyset$$

hence

$$A \subseteq P_t - P_t + R_t' \subseteq (P-P) + (R_0 - R_0) + \cdots + (R_{t-1} - R_{t-1}) + R_t' \tag{37}$$

As we've seen earlier in the project, if $S = \{s_1, \ldots, s_k\}$ is a subset of an additive group, we define the cube $\overline{S}$ the cube spanned by S, which is the set of elements of the form $\sum_{i=1}^k \epsilon_i s_i$,

where $\epsilon_i \in \{-1, 0, 1\}$. Then we observe that $\overline{S}$ is a GAP of dimension k and size at most 3^k and in particular $S - S \subseteq \overline{S}$.

So from (37), it follows that $A \subset Q$, where Q is the GAP

$$Q = P - P + \overline{R_0} + \cdots + \overline{R_{t-1}} + \overline{R'_t}$$

We now calculate the dimension of Q:

$$\begin{aligned}\dim(Q) &\leq \dim(P) + \sum_{j=0}^{t-1} |R_j| + |R'_t| \\ &\leq d + 10C(t+1) \\ &\leq d + 20C \log\left(\frac{C^4}{\beta}\right) \quad \text{(from (36))}\end{aligned}$$

We now look at the size of Q. First, note that the fact that P is proper implies that $|P - P| = 2^d|P|$. Hence

$$\begin{aligned}|Q| &\leq |P - P| \prod_{j=0}^{t-1} 3^{|R_i|} 3^{|R'_t|} \\ &\leq 2^d 3^{10C(t+1)} |P| \\ &\leq 2^d 3^{20C \log(C^4/\beta)} C^4 n \quad \text{(using (3.8) as } P \subseteq 2A - 2A) \\ &\leq 2^d \left(\frac{C^4}{\beta}\right)^{40C} n \quad \blacksquare\end{aligned}$$

All we have left to do is to combine the previous 2 propositions to obtain our bounds. Our aim is not to obtain the sharpest constants, so the inequalities will be very crude. The order of magnitude is important in out approach. For instance, we know that $d \leq 2^{11} C \log C$, therefore

$$\begin{aligned}\log\left(C^{16}\left(\frac{1}{20d}\right)^d\right) &\geq 16 \log C - d(\log 20 + \log d) \\ &\geq 16 \log C - 2^{11} C \log C (3 + \log 2^{11} + \log C + \log(\log C)) \\ &\geq -2^{15} C (\log C)^2\end{aligned}$$

So we can guarantee $\beta \geq \exp(-2^{15} C (\log C)^2)$. Now we have

$$\begin{aligned}\dim(Q) &\leq d + 20C \log\left(\frac{C^4}{\beta}\right) \\ &\leq 2^{11} C \log C + 80C \log C + 20C 2^{15} C (\log C)^2 \\ &\leq 2^{21} C^2 (\log C)^2\end{aligned}$$

Also,

$$\begin{aligned}\log\left(2^d \left(\frac{C^4}{\beta}\right)^{40C}\right) &\leq d + 160C \log C + 40C 2^{15} C (\log C)^2 \\ &\leq 2^{21} C^2 (\log C)^2\end{aligned}$$

Using these crude approximations, we have this version of Freiman's theorem:

Theorem 5.7 (Freiman's theorem) *Let $A \subseteq \mathbb{Z}$, $|A| = n$ and suppose that $|A + A| \leq Cn$. Then A is contained in a GAP of dimension at most $\alpha_1 C^2 (\log C)^2$ and size at most $\exp(\alpha_2 C^2 (\log C)^2) n$ (where $\alpha_1, \alpha_2 \leq 2^{21}$).*

References

[1] Bollobás B. *Modern graph theory*. Graduate texts in mathematics ; 184. New York ; London: Springer, 1998.

[2] Breuillard E, Green B, Tao T. *The structure of approximate groups*. Publications mathématiques de l'IHÉS, Volume 116, Issue 1, pp 115-221, 2012.

[3] Cassels JWS. *An introduction to the geometry of numbers*. Die Grundlehren der mathematischen Wissenschaften ; Band 99. Berlin : Springer-Verlag, 1971.

[4] Chang MC. *A polynomial bound in Freiman's theorem*. Duke Math. J. Volume 113, Number 3 (2002), 399-419.

[5] Clark PL. *Geometry of Numbers with Applications to Number Theory*. University of Georgia, 2013.

[6] Freiman GA *Foundations of a structural theory of set addition* (translated from the Russian). Translations of Mathematical Monographs, Vol 37. American Mathematical Society, Providence, R. I., 1973.

[7] Gowers WT. *A new proof of Szemerédi's theorem*. Geom. Funct. Anal. 11, no. 3, 465-488, 2001.

[8] Gowers WT. *A new way of proving sumset estimates*. [Online] Available from: `https://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/` [Accessed 30 September 2015].

[9] Green B. *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak*. Current Events Bulletin of the AMS, 2010.

[10] Green B. *Structure Theory of Set Addition*. Lectures notes for the ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh March 25 – April 5 2002. [Online] Available from: `http://people.maths.ox.ac.uk/greenbj/papers/icmsnotes.pdf` [Accessed 30 September 2015].

[11] Green B. *Spectral structure of sets of integers* in Fourier analysis and convexity, 83-96. Appl. Numer. Harmon. Anal., Birkhauser Boston, 2004.

[12] Green B, Ruzsa IZ. *Sets with small sumset and rectification*. Bull. London Math. Soc. 38, no. 1, 43-52, 2006.

[13] Green B, Tao T. *The primes contain arbitrarily long arithmetic progressions*. Annals of Mathematics 167 (2): 481–547, 2008.

[14] Nathanson MB. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Graduate Texts in Mathematics, 165. Springer-Verlag, New York, 1996.

[15] Regev O. *Lecture 1 Introduction* from Lattices in Computer Science. Lecture notes from Tel Aviv University, Fall 2004. [Online] Available from: `http://www.cims.nyu.edu/ regev/teaching/lattices_fall_2004/ln/introduction.pdf` [Accessed 30 September 2015].

[16] Ruzsa I *Arithmetic progressions in sumsets*. Acta Arithmetica 60, no 2, 191-202, 1991.

[17] Ruzsa I. *Generalized arithmetic progressions and sumsets*. Acta Math. Hungar. 65, no 4, 379-388, 1994.

[18] Ruzsa I. *An analog of Freiman's theorem in groups* in Structure Theory of Set Addition. Astérisque 258, 1999.

[19] Soundararajan K. *Additive Combinatorics: Winter 2007*. [Online]. Available from: `http://math.stanford.edu/~ksound/Notes.pdf` [Accessed 30 September 2015].

[20] Tao T, Vu V. *Additive Combinatorics*. Cambridge studies in advanced mathematics; 105. Cambridge University Press, 2006.

[21] Tao T. *Lectures notes for 254A*. [Online] Available from: `http://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/Tao.pdf` [Accessed 30 September 2015].

[22] Tao T. *Product set estimates for non-commutative groups*. Combinatorica 28, 547-594, 2008.

[23] Tointon M. *A proof of Minkowski's second theorem*. [Online] Available from: `https://www.dpmms.cam.ac.uk/~mcht2/mink.pdf` [Accessed 30 September 2015].

[24] Trevisian L. *Additive Combinatorics and Theoretical Computer Science*. SIGACT News Complexity Theory Column 63, edited by Hemaspaandra LA, 2009.

[25] Verstraëte J. *Additive and Combinatorial Number Theory* Based on a course given by Gowers WT in Cambridge (1998) [Online] Available from: `http://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/notes-acnt.pdf` [Accessed 30 September 2015].

[26] Verstraëte J. *Notes on geometry of numbers*. Progressions in sumsets. [Online] Available from: `http://www.math.ucsd.edu/~jverstra/minkowski.pdf` [Accessed 30 September 2015].