Additive Combinatorics

Ben Green

Contents

Note

Lecture notes updated for Michaelmas term 2022 by Akshat Mudgal.

0.1. Overview

The aim of this course is to present classic results in additive and combinatorial number theory, showing how tools from a variety of mathematical areas may be used to solve number-theoretical problems.

We will begin by looking at classical theorems about writing natural numbers as the sums of squares and primes. For instance, we will prove Lagrange's theorem that every number is the sum of four squares, and we will show that every large integer is the sum of a bounded number of primes.

Next we will look at more general sets of integers, proving a famous theorem of Roth: every set of integers with positive density contains three distinct elements in arithmetic progression.

We will also look at the structure of finite sets A of integers which are almost closed under addition in the sense that their sumset $A+A := \{a_1+a_2 : a_1, a_2 \in A\}$ is relatively small. The highlight here is Freiman's theorem, which states that any such set has a precise combinatorial structure known as a generalised progression.

Finally, we will look at instances of the sum-product phenomenon, which says that it is impossible for a finite set of integers to be simultaneously additively- and multiplicatively structured. This section draws from a particularly rich set of other mathematical areas, including graph theory, geometry and analysis. Nonetheless, prerequisites will be minimal and we will develop what we need from scratch.

0.2. Synopsis

The classical bases. Every prime congruent to 1 modulo 4 is a sum of two squares. Every natural number is the sum of four squares. *Discussion of sums of three squares*. Schnirelman density. Application of Selberg's sieve to show that every large number is the sum of at most C primes for some fixed C.

Progressions of length 3. Basic properties of Fourier transforms. Roth's theorem that every subset of $\{1, \dots, N\}$ of size at least δN contains three elements in arithmetic progression, provided N is sufficiently large in terms of δ.

Sumsets and Freiman's theorem. Basic sumset estimates. Additive energy and its relation to sumsets: statement (but not proof) of the Balog-Szemerédi-Gowers theorem. Bohr sets and Bogolyubov's theorem. Minkowski's second theorem (statement only). Freiman's theorem on sets with small doubling constant.

Sum-product theorems. The crossing number inequality for graphs. The Szemerédi-Trotter theorem on point-line incidences, and application to prove that either $|A+A|$ or $|A \cdot A|$ has size at least $c|A|^{5/4}$. The Prékopa-Leindler inequality,

quasicubes and sumsets. Proof of Bourgain and Chang's result that either the m-fold sumset $A+A+\cdots+A$ or the m-fold product set $A\cdot A\cdot\cdots\cdot A$ has size at least $|A|^{f(m)}$, where $f(m)\to\infty$.

If time allows the course will conclude with a brief non-examinable discussion of Gowers's work on Szemerédi's theorem for progressions of length 4 and longer, which ties together several earlier strands in the course.

0.3. Further reading

M. Nathanson's two books *Additive Number Theory* have been a significant inspiriation for the choice of topics in this course. They cover quite a bit of the material. Students should bear in mind that these books were written 25 years ago, whilst this course features a number of more recent developments. The book of T. Tao and V. Vu *Additive Combinatorics* is also useful, though again this book does not cover the more recent developments.

0.4. Notation

Asymptotic notation. Throughout the course we will be using *asymptotic notation*. This is vital in handling the many inequalities and rough estimates we will encounter. Here is a summary of the notation we will see. We suggest the reader not worry too much about this now; we will gain plenty of practice with this notation. See also the first question on Sheet 0.

- $A\ll B$ means that there is an absolute constant $C>0$ such that $|A|\leqslant CB$. In this notation, A and B will typically be variable quantities, depending on some other parameter. For example, $x+1\ll x$ for $x\geqslant 1$, because $|x+1|\leqslant 2x$ in this range. It is important to note that the constant C may be different in different instances of the notation.
- $A=O(B)$ means the same thing.
- $A\ll B$ is the same as $B\gg A$.
- $O(A)$ means some quantity bounded in magnitude by CA for some absolute constant $C>0$. In particular, $O(1)$ simply means a quantity bounded by an absolute positive constant. For example, $\frac{5x}{1+x}=O(1)$ for $x\geqslant 0$.
- $A=o(B)$ means that, for all $\varepsilon>0$, $|A|\leqslant\varepsilon B$ as some other parameter becomes large enough in terms of ε. The other parameter will usually be clear from context. For example, $\frac{1}{\log x}=o(1)$ (as $x\to\infty$).
- Sometimes we write $o(1)$ by itself to be some quantity tending to zero (as some other parameter, invariably clear from context, tends to infinity).

- A standard thing to write in analytic number theory is something like

$$\tau(n) \ll_\varepsilon n^\varepsilon. \tag{0.1}$$

  This means that, for every $\varepsilon > 0$, we have $\tau(n) \ll n^\varepsilon$, but the implied constant can depend on ε. More precisely, there is some C_ε such that $\tau(n) \leqslant C_\varepsilon n^\varepsilon$ for all $n \geqslant 1$.

In these notes, $\tau(n)$ will always denote the number of divisors of n (that is, positive integers dividing n, including 1 and n). Then (0.1) is a true (and very useful) statement, called the *divisor bound*. See Lemma A.0.3 for a proof.

We shall adopt the very standard notation

$$e(t) := e^{2\pi i t}.$$

One may think of this either as a function on $\mathbf{R}$, periodic with period 1, or as a function on $\mathbf{T} = \mathbf{R}/\mathbf{Z}$; we shall not be careful in making the distinction.

For $\theta \in \mathbf{T}$ we write $\|\theta\|_{\mathbf{T}}$ for the distance of θ from 0. Thus, for example, $\|2/3\|_{\mathbf{T}} = 1/3$.

Quantities. In understanding analytic number theory, it is important to develop a robust intuitive feeling for the rough size of certain quantities. For example, one should be absolutely clear about the fact that, for X large,

$$\log^{10} X \lll e^{\sqrt{\log X}} \lll X^{0.01}.$$

CHAPTER 1

Sums of squares

In this chapter, a *square* will mean the square of an integer, which may be zero. Thus the set of squares is $\{0, 1, 4, 9, 16, \dots\}$.

1.1. Sums of two squares

THEOREM 1.1.1. *An odd prime p is the sum of two squares if and only if $p \equiv 1 (\mathrm{mod}\, 4)$.*

Proof. Since all squares are 0 or $1 (\mathrm{mod}\, 4)$, a sum of two squares can only ever be $0, 1$ or 2 modulo 4, and in particular not $3 (\mathrm{mod}\, 4)$.

Conversely, suppose $p \equiv 1 (\mathrm{mod}\, 4)$ is a prime. By basic facts about quadratic residues, -1 is a square modulo p, and so there exist integers x, y (in fact $y = 1$) with $x^2 + y^2 = mp$ for some positive integer m. Suppose that m is the minimal positive integer with this property, and assume as a hypothesis for contradiction that $m > 1$. Replacing x with $-x$ and reducing mod p if necessary, and similarly for y, we may assume that $|x|, |y| < p/2$, and therefore

$$mp < 2(\frac{p}{2})^2,$$

which certainly implies that $m < p$. In particular, at least one of x and y is not divisible by m. Indeed, if not then $m^2 | x^2 + y^2$, implying that $m | p$. Since we are assuming that $m \neq 1$, this would force $m = p$, which we know not to be the case.

Pick a, b with $|a|, |b| \leqslant m/2$ and $x \equiv a (\mathrm{mod}\, m)$, $y \equiv b (\mathrm{mod}\, m)$. Note that $a^2 + b^2 > 0$ since not both of x, y are multiples of m. Note furthermore that

$$a^2 + b^2 \equiv x^2 + y^2 \equiv 0 (\mathrm{mod}\, m);$$

let us write $a^2 + b^2 = rm$, where $r > 0$ is an integer. Note that

$$rm \leqslant 2(\frac{m}{2})^2,$$

and so $r < m$. Observing the identity

$$(x^2 + y^2)(a^2 + b^2) = (xa + yb)^2 + (xb - ya)^2,$$

we have

$$rm^2 p = (xa + yb)^2 + (xb - ya)^2.$$

Now we have

$$xa + yb \equiv x^2 + y^2 \equiv 0 (\mathrm{mod}\, m),$$

and

$$xb - ya \equiv xy - yx \equiv 0 (\mathrm{mod}\, m).$$

Therefore if we define

$$x' := \frac{xa + yb}{m}, y' := \frac{xb - ya}{m},$$

both x' and y' are integers. Furthermore

$$(x')^2 + (y')^2 = rp.$$

Since $0 < r < m$, this is contrary to the supposed minimality of m. Therefore we were wrong to assume that $m > 1$, and the proof is complete. □

**Remarks.* The "descent" argument we gave for Theorem 1.1.1 is one of the most elementary proofs of the theorem. A somewhat different proof goes via algebraic number theory in $\mathbf{Q}(i)$. It is known that the ring of integers $\mathbf{Z}[i]$ is a principal ideal domain (PID), and so if the ideal (p) splits then it must be as a product $(p) = (x + iy)(x - iy)$ of two principal ideals, both of norm p, which then implies that $x^2 + y^2 = p$. But there is a criterion (Dedekind's criterion) asserting that the factorisation of (p) in $\mathbf{Z}[i]$ can be read off from the factorisation of the polynomial $X^2 + 1$ in $\mathbf{F}_p$. In particular, (p) splits if and only if $X^2 + 1$ factors over $\mathbf{F}_p$, that is to say precisely when -1 is a quadratic residue mod p, i.e. $p \equiv 1 (\mathrm{mod}\, 4)$.

Note that, although the above argument is short modulo known results, the usual proof that $\mathbf{Z}[i]$ is a PID proceeds via showing that it is a Euclidean domain, that is to say by a descent procedure quite similar to that used in the proof of Theorem 1.1.1.

1.2. Sums of four squares

THEOREM 1.2.1. *Every natural number is the sum of four squares.*

Proof. We note the identity

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + \\ &+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ &+ (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned} \tag{1.1}$$

This means that the set of numbers which are the sum of four squares is closed under multiplication. Since $2 = 1^1 + 1^2 + 0^2 + 0^2$, it suffices to show that any odd prime p is in this set.

Now we proceed along very similar lines to the proof of Theorem 1.1.1. First, we claim that there is some $m > 0$ such that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

To see this, first observe that every element x of $\mathbf{Z}/p\mathbf{Z}$ is a sum of two squares, since the set S of squares $(\mathrm{mod}\, p)$ has size $\frac{1}{2}(p+1)$, and hence S and $x - S$ must intersect. Writing 1 and $-1(\mathrm{mod}\, p)$ as sums of two squares and then adding gives a sum of four squares, not all zero, which is a multiple of p.

Assume that m is minimal with this property, and suppose as a hypothesis for contradiction that $m > 1$.

Replacing x_i with $-x_i$ if necessary, we may assume that $|x_i| < p/2$ (note that p is odd, so the inequality is indeed strict). It follows that

$$mp < 4(\frac{p}{2})^2 = p^2,$$

and so $0 < m < p$.

If m is even, then the x_i may be grouped into two pairs in which the parities are equal, say $x_1 \equiv x_2(\mathrm{mod}\, 2)$, $x_3 \equiv x_4(\mathrm{mod}\, 2)$. But then

$$\frac{1}{2}mp = (\frac{x_1 + x_2}{2})^2 + (\frac{x_1 - x_2}{2})^2 + (\frac{x_3 + x_4}{2})^2 + (\frac{x_3 - x_4}{2})^2,$$

contrary to the minimality of m.

Suppose, then, that m is odd. Not all of the x_i are divisible by m, as this would imply $m^2 | x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ and so $m|p$. Since we are assuming $m > 1$, this forces $m = p$, but we have already proved that $m < p$. Pick y_i with $|y_i| < m/2$ and $x_i \equiv y_i(\mathrm{mod}\, m)$, $i = 1, \ldots, 4$. This is possible with *strict* inequality, as claimed, since m is odd. Then $y_1^2 + y_2^2 + y_3^2 + y_4^2$ is positive, and also a multiple of m since it is congruent to $x_1^2 + x_2^2 + x_3^2 + x_4^2$. Suppose that $y_1^2 + y_2^2 + y_3^2 + y_4^2 = rm$. Then

$$rm < 4(\frac{m}{2})^2 = m^2$$

and so $r < m$. Now from (1.1), we have

$$rm^2 p = (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 + \ldots,$$

where the $\ldots$ comprises the three other terms in (1.1). One may easily check, using $x_i \equiv y_i(\mathrm{mod}\, m)$, that all four of the bracketed terms are multiples of m. Therefore

$$rp = (\frac{x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4}{m})^2 + \ldots,$$

with all the bracketed terms integers. Since $r < m$, this contradicts the supposed minimality of m. $\square$

1.3. Sums of three squares

Theorems about sums of three squares lie a little deeper, at least partly because there is no analogue of the multiplicativity identity (1.1). However, any student of number theory should certainly be aware of the main result on the topic, due to Gauss.

THEOREM 1.3.1. *All numbers not of the form* $4^m(8k+7)$ *are the sum of three squares.*

1.4. *Further comments

Sums of squares have a rich theory. Sums of three squares are connected to class numbers. Writing $h(d)$ for the class number of the quadratic field $\mathbf{Q}(\sqrt{d})$, Gauss showed that the number of representations of $d > 3$ as a sum of 3 squares is $ch(d)$, where $c = 12$ if $d \equiv 1, 2 (\mathrm{mod}\, 4)$, $c = 24$ if $d \equiv 3 (\mathrm{mod}\, 8)$, and $c = 0$ if $d \equiv 7 (\mathrm{mod}\, 8)$.

Representations by sums of squares are intimately connected to the theory of modular forms of half integral weight. This leads to beautiful results: for example, the number of ways to write n as a sum of four squares is 8 times the sum of the divisors d of n with $4 \nmid d$.

A good source for more information is [**3**, Section 11.3], where one may find explicit formulae for the number of representations of n as a sum of s squares, $s = 4, 6, 8, 10, 12$. The formula for $s = 8$ is particularly clean, the number of representations in this case being $16 \sum_{d|n} (-1)^{n-d} d^3$.

CHAPTER 2

Sums of primes

The main theorem of this chapter is the following.

THEOREM 2.0.1. *There is some absolute constant C such that every integer greater than or equal to 2 is a sum of at most C primes.*

We will not be concerned with obtaining a particularly good value of C, or even an explicit value. It was shown by Helfgott in 2013 that every odd integer $\geqslant 3$ is a sum of at most 3 primes, and from this is follows easily that we can take $C = 4$. It is conjectured that $C = 3$ but this is an unsolved problem, more-or-less equivalent to the Goldbach conjecture. Helfgott's proof is long and it also relies on computations; we will give a much more elementary argument, which goes back to Schnirel'man.

2.1. Bases. Schnirel'man density

Let $\mathcal{A}$ be an infinite set of nonnegative integers with $0 \in \mathcal{A}$, and let $h \geqslant 1$ be an integer. Then we say that $\mathcal{A}$ is a *basis of order h* if every nonnegative integer is the sum of h elements of $\mathcal{A}$ (repetitions are allowed). We say that $\mathcal{A}$ is a *basis of finite order* if it is a basis of some order h.

If $m \geqslant 1$ is an integer then we write $m\mathcal{A}$ for the set of all sums $a_1 + \cdots + a_m$ with $a_1, \ldots, a_m \in \mathcal{A}$. Thus $\mathcal{A}$ is a basis of order h if and only if $h\mathcal{A} = \mathbf{Z}_{\geqslant 0}$, the set of all non-negative integers.

Let us quickly note some simple properties of the notion of basis, leaving the (very short) proofs to the reader:

- if $\mathcal{A}$ is a basis of order h then it is also a basis of order h' for any $h' \geqslant h$;
- if $k\mathcal{A}$ is a basis of order h then $\mathcal{A}$ is a basis of order at most kh.

As a consequence of the main result of the last chapter, the squares (together with 0) are a basis of order 4, but not a basis of order 3.

We will deduce Theorem 2.0.1 from the following statement.

PROPOSITION 2.1.1. *The set consisting of $0, 1$ and the primes is a basis of finite order.*

The deduction of Theorem 2.0.1 is quite easy, so we give it now. Let h be such that the set consisting of $0, 1$ and the primes is a basis of order h. In particular, if

n is some arbitrary integer then we may write

$$n - 2 = p_1 + \cdots + p_k + 1 + \cdots + 1,$$

where the total number of primes and ones is at most h.

If there are no 1s, we have

$$n = p_1 + \cdots + p_k + 2.$$

If there are 1s, we have

$$n = p_1 + \cdots + p_k + 1 + 1 + \cdots + 1,$$

where there are at least *three* 1s. We can replace those by 2s and 3s.

In both cases, we have written n as a sum of at most $h + 1$ primes, and so Theorem 2.0.1 is true with $C = h + 1$.

Our task, then, is to establish Proposition 2.0.1. We begin by formulating a sufficient condition for an arbitrary set $\mathcal{A}$ containing 0 and 1 to be a basis of finite order. Then we show how to apply our criterion to establish Proposition 2.1.1. The sufficient condition we will give is in terms of the concept of Schnire'lman density, which we define now.

Definition 2.1.1 (Schnirel'man density). Suppose that $\mathcal{A}$ is a set of nonnegative integers. Then the Schnirel'man density of $\mathcal{A}$, $\sigma_{\mathcal{A}}$, is defined to be the infimum of all the quantities

$$\frac{1}{N}|\mathcal{A} \cap \{1, \dots, N\}|$$

$N = 1, 2, \dots$.

It is convenient to write, as a shorthand,

$$\mathcal{A}[N] := \mathcal{A} \cap \{1, \dots, N\}.$$

Thus if $\mathcal{A}$ has Schnirel'man density $\sigma = \sigma_{\mathcal{A}}$ then $|\mathcal{A}[N]| \geqslant \sigma N$ for all N, and σ is the least constant with this property. Note that if a set has positive Schnire'lman density then $1 \in \mathcal{A}$.

Here is the key result.

Proposition 2.1.2. *Suppose that $\mathcal{A}$ is a set containing 0 which has positive Schnirel'man density. Then $\mathcal{A}$ is a basis of finite order. In fact, if the Schnirel'man density of $\mathcal{A}$ is σ then $\mathcal{A}$ is a basis of order at most $4/\sigma$.*

We will give the proof of this a little later. The key ingredient is the following key lemma, known as Schnirel'man's inequality. Here, and in what follows,

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

(This concept, the *sumset* of two sets $\mathcal{A}$ and $\mathcal{B}$, will feature heavily later in the course.)

LEMMA 2.1.1. *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are sets of nonnegative integers, both containing 0, and with Schnirel'man densities α, β respectively. Then the Schnirel'man density of $\mathcal{A}+\mathcal{B}$ is at least $\alpha+\beta-\alpha\beta$.*

Proof. Fix some positive integer N. If both α and β are zero there is nothing to prove. Suppose, then, that $\alpha > 0$. In particular, $1 \in \mathcal{A}$.

Write down the elements of $\mathcal{A}[N]$ in order,

$$1 = a_0 < a_1 < \cdots < a_k \leqslant N.$$

For each $i = 0, \dots, k-1$, the elements of $a_i + \mathcal{B}[a_{i+1} - a_i - 1]$ are all in $\mathcal{A}+\mathcal{B}$ and lie strictly between a_i and a_{i+1}. Since $0 \in \mathcal{B}$, the elements $a_0, \dots, a_k$ themselves lie in $\mathcal{A}+\mathcal{B}$, and they are distinct from the elements just listed. Finally, the elements $a_k + \mathcal{B}[N - a_k]$ again lie in $\mathcal{A}+\mathcal{B}$, and they lie in the interval $(a_k, n]$.

It follows that

$$(\mathcal{A}+\mathcal{B})[N] \geqslant k+1+\sum_{i=0}^{k-1} |\mathcal{B}[a_{i+1}-a_i-1]| + |\mathcal{B}[N-a_k]|. \tag{2.1}$$

Now by the definition of Schnirel'man density we have the inequalities

$$|\mathcal{B}[a_{i+1}-a_i-1]| \geqslant \beta(a_{i+1}-a_i-1),$$

$$|\mathcal{B}[N-a_k]| \geqslant \beta(N-a_k).$$

Substituting into (2.1) gives

$$\begin{aligned} |(\mathcal{A}+\mathcal{B})[N]| &\geqslant k+1+\beta\Big(\sum_{i=0}^{k-1}(a_{i+1}-a_i-1)+N-a_k\Big) \\ &= \beta N + (1-\beta)(k+1). \end{aligned}$$

In the last step we telescoped the sum over i.

However,

$$k+1 = |\mathcal{A}[N]| \geqslant \alpha N;$$

inserting this into the bound just obtained gives

$$|(\mathcal{A}+\mathcal{B})[N]| \geqslant \beta N + (1-\beta)\alpha N = (\alpha+\beta-\alpha\beta)N,$$

which is what we wanted to prove. □

We need to supplement this with the following, which is more effective for very large density.

LEMMA 2.1.2. *Suppose that $\mathcal{A}$ is a set containing 0 and with Schnirel'man density at least one half. Then $2\mathcal{A} = \mathcal{A} + \mathcal{A}$ contains all positive integers.*

Proof. Suppose that N does not lie in $\mathcal{A} + \mathcal{A}$. Then, for all k, $1 \leqslant k \leqslant N$, either k or $N - k$ must fail to lie in $\mathcal{A}$. It follows that $|\mathcal{A}[N]| < \frac{1}{2}N$, contrary to the assumption on Schnirel'man density. □

We turn now to the deduction of Proposition 2.1.2. For each k, write σ_k for the Schnirel'man density of $k\mathcal{A}$, and $\sigma = \sigma_1$ for short. By Schnire'lman's inequality, applied with $\mathcal{B} = k\mathcal{A}$, we have

$$\sigma_{k+1} \geqslant \sigma_k + \sigma - \sigma_k\sigma.$$

Therefore, for a given k, either $\sigma_k \geqslant \frac{1}{2}$ or else

$$\sigma_{k+1} \geqslant \sigma_k + \frac{1}{2}\sigma.$$

It follows that there must be some $k \leqslant 2/\sigma$ for which $\sigma_k > \frac{1}{2}$.

Finally, by applying Lemma 2.1.2 we see that $k\mathcal{A} + k\mathcal{A}$ contains all positive integers. This concludes the proof of Proposition 2.1.2.

To conclude this section we remark that Mann (1942) proved a stronger version of Lemma 2.1.1. Mann showed that, under the same assumptions, the Schnirel'man density of $\mathcal{A} + \mathcal{A}$ is at least $\min(1, \alpha + \beta)$.

2.2. Primes and Schnirel'man density

In this section, we let $\tilde{\mathcal{P}}$ be the set of primes augmented by 0 and 1. Our task is to prove Proposition 2.1.1, namely to show that $\tilde{\mathcal{P}}$ is a basis of finite order. It would suffice, in view of Proposition 2.1.2, to show that $\tilde{\mathcal{P}}$ has positive Schnire'lman density. Unfortunately, such a statement is false. Indeed, as $N \to \infty$ we have $|\mathcal{P}[N]|/N \to 0$. (By the prime number theorem, the left-hand side decays like $1/\log N$.)

It turns out to be true that $2\tilde{\mathcal{P}} = \tilde{\mathcal{P}} + \tilde{\mathcal{P}}$ *does* have positive Schnire'lman density, and this is enough to complete the proof of Proposition 2.1.1 by the elementary properties of bases.

PROPOSITION 2.2.1. *Let $\tilde{\mathcal{P}}$ denote the set of primes, augmented by including 0 and 1. Then $2\tilde{\mathcal{P}}$ has positive Schnire'lman density.*

To establish this result, it is enough to prove the following slightly weaker-sounding claim.

PROPOSITION 2.2.2. *There is some $c > 0$ such that, for all $N \geqslant 2$, at least cN different integers are a sum of two primes less than or equal to N.*

Proposition 2.2.2 is rather easily seen to imply Proposition 2.2.1. Indeed for $N \geqslant 2$ it implies that

$$|2\tilde{\mathcal{P}}[2N]| \geqslant cN,$$

and so for all $m \geqslant 4$ we have

$$\frac{1}{m}|2\tilde{\mathcal{P}}[m]| \geqslant \frac{c(m-1)}{2m} > \frac{c}{4}.$$

(The minus 1 here comes from the possibility that m is odd.) On the other hand if $m \leqslant 3$ then, since $1 \in 2\tilde{\mathcal{P}}$, we have the trivial bound

$$\frac{1}{m}|2\tilde{\mathcal{P}}[m]| \geqslant \frac{1}{3}.$$

These two bounds together show that the Schnirel'man density of $2\tilde{\mathcal{P}}$ is indeed positive, which is the statement of Proposition 2.2.1.

The remaining task in this chapter, then, is to prove Proposition 2.2.2. To do this, denote by $r(n)$ the number of representations of n as a sum of two primes. Write $\pi(X)$ for the number of primes less than or equal to X, and S for the set of integers expressible as a sum of two primes, both less than or equal to N. Then we have

$$\pi(N)^2 \leqslant \sum_{n \leqslant 2N} r(n) 1_S(n); \tag{2.2}$$

the LHS is the number of pairs of primes (p_1, p_2) with $p_1, p_2 \leqslant N$, whilst the RHS is the number of pairs of primes (p_1, p_2) for which $p_1 + p_2 \leqslant 2N$ and for which there exists a pair of primes $p_1', p_2' \leqslant N$ with $p_1' + p_2' = n$. The first set of pairs is contained in the second.

By the Cauchy-Schwarz inequality we have

$$\sum_{n \leqslant 2N} r(n) 1_S(n) \leqslant |S|^{1/2} \Big(\sum_{n \leqslant 2N} r(n)^2 \Big)^{1/2}. \tag{2.3}$$

We will establish the following bound.

Proposition 2.2.3. *Denote by $r(n)$ the number of representations of n as a sum of two primes. Then*

$$\sum_{n \leqslant X} r(n)^2 \ll \frac{X^3}{\log^4 X}.$$

Plugging this into (2.2), (2.3) (with $X = 2N$) and using the lower bound $\pi(N) \gg N/\log N$ (for $N \geqslant 2$) leads to $|S| \gg N$, that is to say $|S| \geqslant cN$ for some constant $c > 0$, independent of N. This is precisely the statement of Proposition 2.2.2.

It remains, of course, to prove Proposition 2.2.3. To do this, we obtain a pointwise upper bound on $r(n)$, the number of ways to write n as a sum of two primes.

Note that to obtain an asymptotic for $r(n)$, or even a lower bound of $r(n) > 0$ for even n, is a famous unsolved problem: the Goldbach Conjecture. It would be enough to show that

$$r(n) \ll \frac{n}{\log^2 n}, \tag{2.4}$$

uniformly in n. This is the bound one might naively expect: picking $x \leqslant n$ at random, x is prime with probability $\sim \frac{1}{\log n}$, and the same is true of $n-x$. However, these events are not independent, and if n is divisible by many small primes then x being prime makes $n - x$ more likely to be prime than a random integer.

In fact, (2.4) is not true uniformly. We instead establish (in the next section) the following slightly weaker bound which incorporates an arithmetic factor reflecting the dependencies hinted at in the heuristic discussion above.

PROPOSITION 2.2.4. *We have*

$$r(n) \ll \prod_{p|n}(1+\frac{1}{p}) \cdot \frac{n}{\log^2 n}.$$

It is conjectured that the right-hand side is the correct order of magnitude for $r(n)$. The factor $\prod_{p|n}(1+\frac{1}{p})$ is not bounded uniformly in n, because $1+\frac{1}{p} \sim e^{1/p}$ and the sum $\sum_p p^{-1}$ diverges. However, to deduce Proposition 2.2.3 we only need it to be bounded in square mean. We make this deduction now.

Proof. [Proof of Proposition 2.2.3, assuming Proposition 2.2.4]. We will show that

$$\sum_{n\leqslant X} \prod_{p|n}(1+\frac{1}{p})^2 \ll X. \tag{2.5}$$

This suffices to allow us to deduce Proposition 2.2.3 from Proposition 2.2.4. Indeed, $\frac{n}{\log^2 n}$ is an increasing function of n for large n and so

$$\sum_{n\leqslant X} r(n)^2 \ll \sum_{n\leqslant X} \big(\prod_{p|n}(1+\frac{1}{p}) \cdot \frac{n}{\log^2 n}\big)^2 \ll \frac{X^2}{\log^4 X} \sum_{n\leqslant X} \prod_{p|n}(1+\frac{1}{p})^2,$$

from which the required bound follows immediately from (2.5).

Now we prove (2.5). We use the fact that

$$\prod_{p|n}(1+\frac{1}{p}) \leqslant \sum_{d|n} \frac{1}{d}.$$

In fact, the LHS is just the sum of $\frac{1}{d}$ over the *squarefree* divisors of n. However,

$$\sum_{n\leqslant X} \big(\sum_{d|n} \frac{1}{d}\big)^2 = \sum_{d_1,d_2\leqslant X} \frac{1}{d_1 d_2} \sum_{\substack{n\leqslant X \\ [d_1,d_2]|n}} 1 \leqslant X \sum_{d_1,d_2\leqslant X} \frac{1}{d_1 d_2 [d_1,d_2]}.$$

Now since $[d_1, d_2] \geqslant \max(d_1, d_2) \geqslant \sqrt{d_1 d_2}$, we have

$$\sum_{d_1, d_2 \leqslant X} \frac{1}{d_1 d_2 [d_1, d_2]} \leqslant \sum_{d_1, d_2 \leqslant X} \frac{1}{d_1^{3/2} d_2^{3/2}} = (\sum_{d \leqslant X} \frac{1}{d^{3/2}})^2 \ll 1.$$

Putting these facts together gives the result. □

The remaining (and most substantial) task, then, is to establish Proposition 2.2.4. We do this using a tool known as the Selberg sieve.

2.3. Selberg's sieve

In this section we will prove an upper bound for $r(N)$, the number of representations of N as a sum of two primes (note the change from n to N; the latter seems more natural for this argument, and it means we can use n as a dummy variable). Assume throughout the section that N is even; if N is odd then clearly $r(N) \leqslant 1$ (with equality if and only if $N - 2$ is prime).

Define

$$\mathcal{A} := \{n(N-n) : n \leqslant N\}.$$

Let $z := N^{1/3}$ (any threshold of the form $z = N^c$ with $c < \frac{1}{2}$ would work for us, with sharper implied constants coming from taking c close to $\frac{1}{2}$, but let us fix on this choice for definiteness). If $n \leqslant N$ and n and $N - n$ are prime, then either (i) $n \leqslant z$; (ii) $N - n \leqslant z$ or (iii) $n(N-n)$ has no prime factors $\leqslant z$. It follows that

$$r(N) \leqslant 2z + S(\mathcal{A}, z),$$

where $S(\mathcal{A}, z)$ denotes the number of elements of $\mathcal{A}$ with no primes factors $\leqslant z$. To establish Proposition 2.2.4, it therefore sufficies to prove the upper bound

$$S(\mathcal{A}, z) \ll \prod_{p | N} (1 + \frac{1}{p}) \cdot \frac{N}{\log^2 N}. \tag{2.6}$$

The general problem of estimating $S(\mathcal{A}, z)$ (i.e., for more general sets $\mathcal{A}$, and more general parameters z) is the concern of *sieve theory*. The method we are about to describe in our particular setting can be applied to a much wider selection of problems.

For each positive integer d, write $\mathcal{A}_d$ for the set of elements of $\mathcal{A}$ which are divisible by d. The most naïve attempt at the problem would be to use inclusion-exclusion, computing

$$S(\mathcal{A}, z) = |\mathcal{A}| - \sum_{p < z} |\mathcal{A}_p| + \sum_{p < p' < z} |\mathcal{A}_{pp'}| - \cdots$$

Unfortunately, this quickly runs into difficulties due to the very large number of terms; even small errors in the estimation of the $|\mathcal{A}_d|$ blow up uncontrollably. A more subtle approach is therefore required.

One can formulate more involved versions of the inclusion-exclusion principle (the Brun sieve), but we will use an idea due to Selberg. Whilst allowing for a relatively short treatment, it does appear rather magical and unmotivated at first sight.

Before starting the details, we recall some basic concepts and notation from elementary number theory. If a, b are positive integers then we write (a, b) for the greatest common divisor of a, b, and $[a, b]$ for the lowest common multiple. We define the Möbius function $\mu : \mathbf{N} \to \{-1, 0, 1\}$ by $\mu(n) = (-1)^k$ if $n = p_1 \cdots p_k$ is a product of k distinct primes, and $\mu(n) = 0$ otherwise. A little later, we will be using some basic facts about Möbius inversion and Dirichlet convolution. For a refresher on/introduction to this topic, see Appendix **??**.

We turn now to the Selberg sieve. Let $(\lambda_d)_{d \leqslant z}$ be any real parameters subject only to $\lambda_1 = 1$. Consider then the weight

$$\nu(n) := \Big(\sum_{\substack{d | n(N-n) \\ d \leqslant z}} \lambda_d \Big)^2.$$

This weight is of course non-negative, and when $n \in S(\mathcal{A}, z)$ it equals $\lambda_1^2 = 1$, since only the term $d = 1$ appears in the sum. Therefore

$$S(\mathcal{A}, z) \leqslant \sum_{n \leqslant N} \nu(n). \tag{2.7}$$

Expanding out the definition of ν and rearranging, this gives

$$S(\mathcal{A}, z) \leqslant \sum_{d_1, d_2 \leqslant z} \lambda_{d_1} \lambda_{d_2} |\mathcal{A}_{[d_1, d_2]}|. \tag{2.8}$$

Note here that $[d_1, d_2]$ denotes the lcm of d_1, d_2 and so

$$A_{[d_1, d_2]} = \{n \leqslant N : d_1, d_2 | n(N - n)\}.$$

We will restrict the weights λ_d to be supported on squarefree d (that is, $\lambda_d = 0$ if d is divisible by the square of a prime). Let us now estimate the quantity $|\mathcal{A}_d|$ when d is squarefree. We have

$$|\mathcal{A}_d| = \omega(d) \frac{N}{d} + R_d, \tag{2.9}$$

where $\omega(d)$ is the number of solutions to $x(N - x) \equiv 0 (\mathrm{mod}\, d)$, and

$$|R_d| \leqslant \omega(d). \tag{2.10}$$

The remainder term here comes from the fact that one cannot exactly divide $\{1, \ldots, N\}$ into intervals of length d, and there can be an interval of length $< d$ left

over. Now if d is squarefree then, by the Chinese remainder theorem, we have

$$\omega(d) = \prod_{p|d} \omega(p). \tag{2.11}$$

By direct inspection, we have

$$\omega(p) = \begin{cases} 2 & p \nmid N \\ 1 & p|N. \end{cases} \tag{2.12}$$

Substituting (2.9) into (2.8) yields

$$\begin{aligned} S(\mathcal{A}, z) &\leqslant N \sum_{d_1,d_2 \leqslant z} \frac{\lambda_{d_1}\lambda_{d_2}\omega([d_1,d_2])}{[d_1,d_2]} + \sum_{d_1,d_2\leqslant z} |\lambda_{d_1}||\lambda_{d_2}|\omega([d_1,d_2]) \\ &= NQ + E, \end{aligned} \tag{2.13}$$

where

$$Q = Q((\lambda_d)_{d\leqslant z}) := \sum_{d_1,d_2\leqslant z} \frac{\lambda_{d_1}\lambda_{d_2}\omega([d_1,d_2])}{[d_1,d_2]}, \tag{2.14}$$

and

$$E = E((\lambda_d)_{d\leqslant z}) := \sum_{d_1,d_2\leqslant z} |\lambda_{d_1}||\lambda_{d_2}|\omega([d_1,d_2]). \tag{2.15}$$

Recall that, at the moment, we have not said anything about the λ_d other than that $\lambda_1 = 1$ and that they are supported on squarefree d. The strategy now is to choose the λ_d so as to minimize the quadratic form Q, and then hope that E is small, at least with z chosen appropriately.

Note that with $z = N^{1/3}$ this hope about E is not overly ambitious; we need only have the crude bounds

$$|\lambda_d|, \omega(d) \leqslant N^{1/10} \tag{2.16}$$

(say) in order to conclude that $E \ll N^{1-1/20}$ (and in particular appreciably less than the expected main term of $\sim N(\log N)^{-2}$).

Minimizing the quadratic form. We turn now to the task of choosing the λ_d so as to minimise Q. This looks like a rather scary prospect, but in fact Möbius inversion allows us to diagonalise the form, which is of course very helpful.

To begin with, we rewrite Q in the form

$$Q = \sum_{d_1,d_2\leqslant z} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} \lambda_{d_1}\lambda_{d_2} \frac{(d_1,d_2)}{\omega((d_1,d_2))}. \tag{2.17}$$

Here, we used the fact that the λ_d are supported where d is squarefree, and so we have

$$\omega(d_1)\omega(d_2) = \omega((d_1,d_2))\omega([d_1,d_2]) \tag{2.18}$$

(consider the primes dividing each argument of ω, and use (2.11)). To get a handle on this, we use a fairly standard trick. Write $g(k) = k/\omega(k)$, and observe that by Möbius inversion (see Appendix **??**) we have

$$g(k) = \sum_{\delta|k} f(\delta) \tag{2.19}$$

where

$$f(k) = \sum_{\delta|k} \mu(\frac{k}{\delta}) g(\delta).$$

In the notation of Dirichlet convolution, $g = f * 1$ and $f = g * \mu$. Note that $g(k) = k/\omega(k)$ is multiplicative, and hence so is $f = g * \mu$ (see Appendix **??**). Furthermore it is easy to check that $f(p) = \frac{p}{\omega(p)} - 1$ when p is a prime, where of course ω is as defined in (2.11), (2.12). Note that $f(p)$ is never zero (when $p = 2$, this is because we are assuming N odd), and so in fact f is strictly positive.

Substituting (2.19) into (2.17) and swapping the order of summation yields

$$Q = \sum_{\delta \leqslant z} f(\delta) \Big(\sum_{\delta|d, d \leqslant z} \frac{\omega(d)}{d} \lambda_d \Big)^2 = \sum_{\delta \leqslant z} f(\delta) u_\delta^2, \tag{2.20}$$

where

$$u_\delta := \sum_{\delta|d, d\leqslant z} \frac{\omega(d)}{d} \lambda_d.$$

(Here, d ranges over squarefrees.) With this change of variables, Q is indeed a diagonal quadratic form. To minimise Q we need to express the constraint $\lambda_1 = 1$ in terms of these new variables u_δ. This can be achieved by applying Lemma A.0.2. One obtains

$$\frac{\omega(d)}{d} \lambda_d = \sum_{d|\delta, \delta \leqslant z} \mu(\frac{\delta}{d}) u_\delta, \tag{2.21}$$

where δ ranges over squarefrees. Therefore the constraint $\lambda_1 = 1$ becomes simply

$$\sum_{\delta \leqslant z} \mu(\delta) u_\delta = 1. \tag{2.22}$$

The minimisation of Q, as given in (2.20), subject to the constraint (2.22), is a simple matter of completing the square, or more specifically looking at the inequality

$$\sum_{\delta \leqslant z} f(\delta)(u_\delta - \frac{\mu(\delta)}{D f(\delta)})^2 \geqslant 0, \tag{2.23}$$

where

$$D = D(z) := \sum_{\delta \leqslant z} \frac{\mu^2(\delta)}{f(\delta)} = \sum_{d \leqslant z, d \text{ squarefree}} \frac{1}{f(d)}. \tag{2.24}$$

This shows that the minimum value of Q (as given by (2.20)) subject to the constraint (2.22) is $1/D$, and that equality is attained when

$$u_\delta = \mu(\delta)/Df(\delta). \tag{2.25}$$

Thus we take our as yet unspecified weights λ_d to be the ones giving this choice of the u_δ. In view of (2.21), this means that we define

$$\lambda_d := \frac{d}{\omega(d)D} \sum_{d|\delta, \delta \leqslant z} \frac{\mu(\delta/d)\mu(\delta)}{f(\delta)}. \tag{2.26}$$

Let us take stock of our current position. Our aim is to prove (2.6). Taking the particular choice (2.26) of the λ_d, and $z := N^{1/3}$, substituting into (2.13) gives

$$S(\mathcal{A}, z) \leqslant \frac{N}{D} + O(N^{2/3} \max_{d \leqslant z} |\lambda_d|^2 \omega(d)^2). \tag{2.27}$$

Here, in estimating E, we have used

$$E = \sum_{d_1, d_2 \leqslant z} |\lambda_{d_1}||\lambda_{d_2}|\omega([d_1, d_2]) \leqslant \sum_{d_1, d_2 \leqslant z} |\lambda_{d_1}||\lambda_{d_2}|\omega(d_1)\omega(d_2) \leqslant z^2 \sup_d |\lambda_d|^2 \omega(d)^2,$$

where the middle step follows from (2.18).

The two terms on the right in (2.27) have the status of main term and error term respectively, though we have not yet shown anything rigorous about them.

To bound the main term, we will show that

$$D \gg \log^2 N \cdot (\prod_{p|N} (1 + \frac{1}{p}))^{-1}. \tag{2.28}$$

To bound the error term, we will show that

$$|\lambda_d|\omega(d) \ll_\varepsilon d^\varepsilon \quad \text{for all squarefree } d. \tag{2.29}$$

The desired bound (2.6) follows very quickly by substituting (2.28) and (2.29) into (2.27).

It remains, then, to establish (2.28) and (2.29). The proofs of these statements are somewhat lengthy and a little technical, though instructive to work through. They are fairly unrelated to the rest of the argument and readers may wish to skip them.

Bounding the main term. We now prove (2.28). For the purposes of this proof, extend ω to a completely multiplicative function by defining $\omega(p^j) := \omega(p)^j$. Now if d is squarefree then

$$\frac{1}{f(d)} = \prod_{p|d} \frac{1}{f(p)} = \prod_{p|d} \frac{\omega(p)/p}{1 - \frac{\omega(p)}{p}} = \prod_{p|d} \sum_{j \geqslant 1} \frac{\omega(p^j)}{p^j},$$

by the multiplicativity of f and the geometric series formula. Therefore

$$D = \sum_{d\leqslant z, d \text{ squarefree}} \prod_{p|d} \sum_{j\geqslant 1} \frac{\omega(p^j)}{p^j} = \sum_{m:\mathrm{rad}(m)\leqslant z} \frac{\omega(m)}{m} \geqslant \sum_{m\leqslant z} \frac{\omega(m)}{m}. \tag{2.30}$$

Here, the radical $\mathrm{rad}(m)$ is the product of the distinct primes dividing m, which is of course squarefree.

Let S' be the set of all positive integers coprime to N, and let S_* denote the set of all positive integers composed *only* of primes dividing N. Any integer m has a unique factorisation $m = m'm_*$, where $m' \in S'$ and $m_* \in S_*$.

We claim that

$$\omega(m) \geqslant \tau(m'). \tag{2.31}$$

Recall the definition (2.12) of $\omega(p)$. Thus if we write $m = p_1^{a_1} \cdots p_k^{a_k}$, with $p_1, \dots, p_\ell$ being those primes *not* dividing N, then $m' = p_1^{a_1} \cdots p_\ell^{a_\ell}$ and

$$\omega(m) = 2^{a_1+\cdots+a_\ell},$$

whilst

$$\tau(m') = (a_1+1)\cdots(a_\ell+1).$$

The claimed inequality (2.31) now follows from the fact that $2^a \geqslant a+1$ for all integers $a \geqslant 1$.

Substituting (2.31) into (2.30) yields

$$D \geqslant \sum_{m\leqslant z} \frac{\tau(m')}{m}. \tag{2.32}$$

Now observe that

$$\prod_{p|N} (1-\frac{1}{p})^{-1} = \sum_{t\in S_*} \frac{1}{t};$$

this follows by expanding $(1-\frac{1}{p})^{-1} = \sum_{j\geqslant 0} p^{-j}$ and multiplying up over all primes p dividing N. It follows from (2.32) that

$$D \prod_{p|N} (1-\frac{1}{p})^{-1} \geqslant \sum_{m\leqslant z} \frac{\tau(m')}{m} \sum_{t\in S_*} \frac{1}{t} = \sum_n \frac{1}{n} \sum_{\substack{m\leqslant z \\ m|n \\ n/m\in S_*}} \tau(m') \geqslant \sum_{n\leqslant z} \frac{1}{n} \sum_{\substack{m|n \\ n/m\in S_*}} \tau(m').$$

where in the middle step we substituted $n = mt$. Now in the sum over m, n/m runs exactly over the divisors of n_*, so there are $\tau(n_*)$ terms in the sum. For each of them we have $m' = n'$. It follows that

$$\sum_{\substack{m|n \\ n/m\in S_*}} \tau(m') = \tau(n_*)\tau(n') = \tau(n),$$

and so we have proven that

$$D\prod_{p|N}(1-\frac{1}{p})^{-1} \geqslant \sum_{n\leqslant z}\frac{\tau(n)}{n}. \tag{2.33}$$

We have now almost completed the proof of (2.28). To finish it, note first that

$$\sum_{n\leqslant z}\frac{\tau(n)}{n} \geqslant \Big(\sum_{x\leqslant\sqrt{z}}\frac{1}{x}\Big)^2$$

(since, by multiplying out the square, the right-hand side is $\sum_{n\leqslant z}\frac{\tilde{\tau}(n)}{n}$, where $\tilde{\tau}(n)$ denotes the number of divisors d of n with $d, n/d \leqslant \sqrt{z}$.) Recalling that $z = N^{1/3}$, it follows that

$$\sum_{n\leqslant z}\frac{\tau(n)}{n} \gg \log^2 N. \tag{2.34}$$

Finally, to deduce (2.28), we use (2.33), (2.34) and the fact that

$$\prod_{p|N}(1-\frac{1}{p}) = \prod_{p|N}(1+\frac{1}{p})^{-1}\cdot\prod_{p|N}(1-\frac{1}{p^2}) \gg \prod_{p|N}(1+\frac{1}{p})^{-1},$$

since the product $\prod_p(1-\frac{1}{p^2})$ converges to a positive real number (in fact to $1/\zeta(2) = 6/\pi^2$).

Bounding the error term. Now we prove the estimate (2.29). From the definition (2.26) of λ_d, we have

$$|\omega(d)\lambda_d| = |\frac{d}{D}\sum_{d|\delta,\delta\leqslant z}\frac{\mu(\delta/d)\mu(\delta)}{f(\delta)}| \leqslant \frac{d}{Df(d)}\sum_{\substack{\delta'\leqslant z\\ \delta' \text{ squarefree}}}\frac{1}{f(\delta')} = \frac{d}{f(d)}.$$

Now it is easy to check that $p/f(p) \leqslant 6$, the worst case being when $p = 3$ and $\omega(3) = 2$. Therefore

$$|\omega(d)\lambda_d| \leqslant \frac{d}{f(d)} = \prod_{p|d}\frac{p}{f(p)} \leqslant 6^{\#\text{ prime factors of } d} = \tau(d)^{\frac{\log 6}{\log 2}}.$$

The claim now follows from the divisor bound (Lemma A.0.3).

CHAPTER 3

Roth's theorem on progressions of length 3

In this chapter our aim is to prove the following theorem of Roth from 1953. The theorem is well-worth studying in its own right, but it also gives an opportunity to introduce a key tool: the Fourier transform.

THEOREM 3.0.1 (Roth's theorem). *There is an absolute constant C such that any subset $A \subset \{1, \dots, N\}$ with cardinality at least $CN/\log\log N$ contains a non-trivial three-term arithmetic progression (that is to say, a triple $x, x+d, x+2d$ with $d \neq 0$).*

Note, in particular, that $1/\log\log N$ is eventually smaller than any fixed positive constant.

Throughout this chapter we will assume that N is sufficiently large (meaning bigger than some absolute constant which we shall not specify precisely).

3.1. The density increment strategy

Roth's theorem proceeds via the so-called *density increment strategy,* and the key proposition which drives this is the following.

PROPOSITION 3.1.1. *Suppose that $0 < \alpha < 1$ and that $N \geqslant (8/\alpha)^{10}$. Suppose that $P \subset \mathbf{Z}$ is an arithmetic progression of length N and that $A \subset P$ is a set with cardinality at least αN. Then one of the following two alternatives holds:*

(i) *A contains a nontrivial 3-term progression;*
(ii) *There is an arithmetic progression P' of length $N' \geqslant N^{1/5}$ such that, writing $A' := A \cap P'$ and $\alpha' := |A'|/|P'|$, we have $\alpha' \geqslant \alpha + \frac{\alpha^2}{112}$.*

Theorem 3.0.1 follows by iterating this proposition. Set $P_0 := \{1, \dots, N\}$ and let us suppose that we have a set $A \subset P_0$ with $|A| = \alpha N$ and containing no nontrivial 3-term progression. Then we attempt to use Proposition 3.1.1 repeatedly to obtain a sequence $P_0, P_1, P_2, \dots$ of progressions together with sets $A_i := A \cap P_i$. The length of P_i will be $N_i \geqslant N^{(1/5)^i}$ and the densities $\alpha_i := |A_i|/|P_i|$ will satisfy $\alpha_{i+1} > \alpha_i + c\alpha_i^2$.

Now this iteration cannot last too long: after C/α steps the density has already doubled, after a further $C/2\alpha$ steps it has doubled again, and so on. Since no set

can have density greater than one, there can be no more than $2C/\alpha$ steps in total. We conclude that our applications of Proposition 3.1.1 must have been invalid, which can ony mean that the condition $N_i > C\alpha_i^{-C}$ was violated. Since

$$N_i > N^{(1/5)^i} \geqslant N^{(1/5)^{2C/\alpha}}$$

and (very crudely)

$$\alpha_i \geqslant \alpha,$$

we infer the bound

$$N^{(1/5)^{2C/\alpha}} \leqslant C\alpha^{-C}.$$

Rearranging gives

$$\log\log N \leqslant \log\log(C\alpha^{-C}) + \frac{2C}{\alpha} \leqslant \frac{C'}{\alpha},$$

which immediately gives the claimed bound.

Remark. The most important parameter by far is the number of times we performed the iteration, which was roughly $O(1/\alpha)$.

3.2. Fourier transform on Z

Let $f : \mathbf{Z} \to \mathbf{C}$ be a compactly-supported function (that is, $f(n) = 0$ outside of some finite interval). Then we define the Fourier transform $\hat{f}(\theta)$ by

$$\hat{f}(\theta) := \sum_n f(n)e(-n\theta).$$

Since f is compactly-supported, there is no issue of convergence.

A crucial fact we will need is the Parseval identity.

PROPOSITION 3.2.1. *We have*

$$\sum_n f(n)\overline{g(n)} = \int_{\mathbf{T}} \hat{f}(\theta)\overline{\hat{g}(\theta)}d\theta.$$

Proof. This is an easy check using the definitions, as well as the fact that

$$\int_{\mathbf{T}} e(m\theta)d\theta = \int_0^1 e(m\theta)d\theta = \begin{cases} 1 & m = 0 \\ 0 & m \in \mathbf{Z} \setminus \{0\}. \end{cases} \tag{3.1}$$

□

Remark. Taking $f = g$ gives

$$\sum_n |f(n)|^2 = \int_{\mathbf{T}} |\hat{f}(\theta)|^2 d\theta.$$

3.3. A large Fourier coefficient

We turn now to the details of the density increment strategy. We begin with a very simple observation, which is that we may assume without loss of generality that $P = [N] = \{1, \dots, N\}$. We may always reduce to this case by an affine rescaling.

We will first establish the following alternative version of Proposition 3.1.1, in which the conclusion of part (ii) is different, asserting the existence of a large Fourier coefficient of the function

$$f_A := 1_A - \alpha 1_{[N]},$$

the so-called *balanced function* of A. In the next section, we will show that a large Fourier coefficient implies a density increment as in the original formulation of Proposition 3.1.1.

PROPOSITION 3.3.1. *Suppose that $0 < \alpha < 1$ and that $N \geqslant 4/\alpha^2$. Suppose that $A \subset [N]$ is a set with cardinality at least αN. Then one of the following two alternatives holds:*

(i) *A contains a nontrivial 3-term progression;*
(ii) *The balanced function f_A has a large Fourier coefficient: specifically, there is some $\theta \in \mathbf{T}$ such that $|\hat{f}_A(\theta)| \geqslant \alpha^2 N/28$.*

Proof. If $f_1, f_2, f_3 : \mathbf{Z} \to \mathbf{R}$ are three finitely-supported functions then we introduce the operator

$$T(f_1, f_2, f_3) := \sum_{x,d} f_1(x) f_2(x+d) f_3(x+2d).$$

This counts the number of 3-term progressions weighted by the functions f_i. In particular,

$$T(1_A, 1_A, 1_A) = \#\{\text{number of 3-term progressions in } A\}. \tag{3.2}$$

Note carefully that this count includes "trivial" progressions with $d = 0$. However, A has precisely αN trivial progressions, so if option (i) does not hold then

$$T(1_A, 1_A, 1_A) = \alpha N \leqslant \alpha^3 N^2/4. \tag{3.3}$$

For the inequality on the right we used the assumption that $N \geqslant 4/\alpha^2$.

Note that T is a trilinear operator. Thus we may write $1_A = f_A + \alpha 1_{[N]}$ and expand $T(1_A, 1_A, 1_A)$ as a sum of eight terms,

$$T(1_A, 1_A, 1_A) = \alpha^3 T(1_{[N]}, 1_{[N]}, 1_{[N]}) + \cdots + T(f_A, f_A, f_A). \tag{3.4}$$

Each of the seven "error terms" denoted by the ellipsis $\cdots$ contains at least one copy of f_A. Let us look at the first term $\alpha^3 T(1_{[N]}, 1_{[N]}, 1_{[N]})$. It is quite simple to evaluate this exactly: the number of (x, d) with $x, x+d, x+2d \in [N]$ is precisely

the number of pairs $(n_1, n_2) \in [N] \times [N]$ with n_1, n_2 having the same parity, since we then have, uniquely, $x = n_1$ and $d = \frac{1}{2}(n_2 - n_1)$, and $x + d$ automatically lies in $[N]$. This is $N^2/2$ if N is even, and $(N^2 + 1)/2$ if N is odd, thus at least $N^2/2$ in all cases. Thus

$$\alpha^3 T(1_{[N]}, 1_{[N]}, 1_{[N]}) \geqslant \alpha^3 N^2/2.$$

It follows that if option (i) does not hold (and hence we have (3.3)) then the sum of the seven error terms in (3.4) is at least $\alpha^3 N^2/4$. Thus one of these terms is at least $\alpha^3 N^2/28$, that is to say

$$|T(f_1, f_2, f_3)| \geqslant \alpha^3 N^2/28, \tag{3.5}$$

where each f_i is either $\alpha 1_{[N]}$ or f_A, and at least one of them is f_A.

Now we come to the key idea: there is a formula for $T(f_1, f_2, f_3)$ in terms of the Fourier transform:

$$T(f_1, f_2, f_3) = \int_{\mathbf{T}} \hat{f}_1(\theta)\hat{f}_2(-2\theta)\hat{f}_3(\theta)d\theta. \tag{3.6}$$

Once written down, it is very easy to check this by substituting the definition of the Fourier transforms on the right-hand side.

Thus if (3.5) holds then

$$\Big| \int_{\mathbf{T}} \hat{f}_1(\theta)\hat{f}_2(-2\theta)\hat{f}_3(\theta)d\theta \Big| \geqslant \alpha^3 N^2/28. \tag{3.7}$$

Suppose that $f_3 = f_A$; the analysis of other possibilities is very similar. Then

$$\sup_{\theta \in \mathbf{T}} |\hat{f_A}(\theta)| \int_{\mathbf{T}} |\hat{f}_1(\theta)||\hat{f}_2(-2\theta)|d\theta \geqslant \alpha^3 N^2/28.$$

By the Cauchy-Schwarz inequality,

$$\sup_{\theta \in \mathbf{T}} |\hat{f_A}(\theta)| \Big(\int_{\mathbf{T}} |\hat{f}_1(\theta)|^2 d\theta \Big)^{1/2} \Big(\int_{\mathbf{T}} |\hat{f}_2(\theta)|d\theta \Big)^{1/2} \geqslant \alpha^3 N^2/28. \tag{3.8}$$

However, by Parseval's identity we have

$$\int_{\mathbf{T}} |f_i(\theta)|^2 d\theta = \sum_n |f_i(n)|^2.$$

One may easily check that the RHS is $\alpha^2 N$ if $f_i = \alpha 1_{[N]}$ and $\alpha(1-\alpha)N$ if $f_i = f_A$, and so certainly at most αN in either case. Thus from (3.8) we obtain

$$\sup_{\theta \in \mathbf{T}} |\hat{f_A}(\theta)| \geqslant \alpha^2 N/28,$$

which is precisely option (ii) in the proposition. □

3.4. From a large Fourier coefficient to a density increment

In this section, we show how option (ii) in Proposition 3.3.1 (the balanced function f_A has a large Fourier coefficient) may be replaced by option (ii) in Proposition 3.1.1 (a density increment on a progression). The crucial technical ingredient is the following.

Here, if $F : \mathbf{Z} \to \mathbf{C}$ is a function and $S \subset \mathbf{Z}$ a finite set, we write $\mathrm{diam}_S(F) := \sup_{x,x' \in S} |F(x) - F(x')|$.

LEMMA 3.4.1. *Suppose that $\theta \in \mathbf{T}$. Then we may partition $[N]$ into progressions P_i, each of length at least $N^{1/5}$, such that $\mathrm{diam}_{P_i}(e(\theta x)) \leqslant N^{-1/5}$ for all i.*

Proof. Throughout this argument we will assume that N is sufficiently large. Let $Q := \lfloor N^{1/2} \rfloor$. By a well-known application of the pigeonhole principle due to Dirichlet, there is some positive $d \leqslant Q$ such that $\|d\theta\| \leqslant 1/Q$. (Consider $\theta, 2\theta, \cdots, Q\theta$ as elements of $\mathbf{T}$; some two of these, say $j_1\theta$ and $j_2\theta$, lie within $1/Q$ of one another. Take $d := |j_1 - j_2|$.)

If P is any progression with common difference d and length $\leqslant 3N^{1/5}$ then, by the triangle inequality,

$$\mathrm{diam}_P(e(\theta x)) \leqslant 3N^{1/5}|e(\theta d) - 1| \leqslant 20N^{1/5}/Q < N^{-1/5},$$

where here we used the inequality

$$|e(t) - 1| = 2|\sin \pi t| \leqslant 2\pi \|t\|_{\mathbf{R}/\mathbf{Z}}.$$

Now observe that $[N]$ can be partitioned into progressions P_i with common difference d and lengths in the range $[N^{1/5}, 3N^{1/5}]$. To do this, first partition $[N]$ into progressions of common difference d, each of length $\sim N/d \gg N^{1/2}$. Then proceed along each such progression from left to right, partitioning into progressions of length $\lceil N^{1/5} \rceil$ until we have a leftover progression of length $\leqslant N^{1/5}$. Amalgamate this with the preceding one. □

The following result, together with Proposition 3.3.1, immediately implies Proposition 3.1.1, and hence completes the proof of Roth's theorem.

PROPOSITION 3.4.1. *Suppose that $|\hat{f}_A(\theta)| \geqslant \alpha^2 N/28$, that $N \geqslant (8/\alpha)^{10}$, and let $[N] = \bigcup_i P_i$ be a partition as above. Then there is some i such that $|A \cap P_i| \geqslant (\alpha + \frac{\alpha^2}{112})|P_i|$.*

Proof. Since the P_i partition $[N]$, we obviously have

$$\sum_i |\sum_{x \in P_i} f_A(x) e(-\theta x)| \geqslant \frac{\alpha^2}{28} N.$$

By the triangle inequality and the bound $|f_A(x)| \leqslant 1$, the left-hand side is at most

$$\sum_i |\sum_{x\in P_i} f_A(x)| + \sum_i |P_i| \operatorname{diam}_{P_i}(e(\theta x)) \leqslant \sum_i |\sum_{x\in P_i} f_A(x)| + N^{4/5}$$
$$\leqslant \sum_i |\sum_{x\in P_i} f_A(x)| + \frac{\alpha^2}{56}N,$$

the last step following from our assumption on N. It follows that

$$\sum_i |\sum_{x\in P_i} f_A(x)| \geqslant \frac{\alpha^2}{56}N.$$

Since $\sum_{x\in[N]} f_A(x) = 0$, we have

$$\sum_i \big(|\sum_{x\in P_i} f_A(x)| + \sum_{x\in P_i} f_A(x)\big) \geqslant \frac{\alpha^2}{56}N = \frac{\alpha^2}{56}\sum_i |P_i|,$$

so there must be some i such that

$$|\sum_{x\in P_i} f_A(x)| + \sum_{x\in P_i} f_A(x) \geqslant \frac{\alpha^2}{56}|P_i|,$$

which implies that

$$\sum_{x\in P_i} f_A(x) \geqslant \frac{\alpha^2}{112}|P_i|,$$

or in other words that

$$|A \cap P_i| \geqslant (\alpha + \frac{\alpha^2}{112})|P_i|.$$

This concludes the proof.

□

CHAPTER 4

Sumset inequalities

In this chapter we explore the notion of adding sets. There is a huge literature on this topic, from which we isolate a few key results. All of the results we shall state are valid for finite subsets of arbitrary abelian groups, and for brevity it is usual to call these "additive sets". When we are talking about more than one additive set, we assume they are all subsets of the same group. The particular abelian group in question will normally be clear from context (though often it does not matter). In fact, many of the results (but not all) remain true without the assumption of commutativity, but we shall not cover that topic in this course.

4.1. Basic notation and definitions

Let A, B be additive sets (this both A and B are finite subsets of some abelian group). Then we write

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

and

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

These definitions extend in an obvious way to more than two summands, for example

$$A_1 + \cdots + A_k := \{a_1 + \cdots + a_k : a_i \in A_i\}.$$

If $A_1 = \cdots = A_k = A$ then we usually write kA for $A_1 + \cdots + A_k$. In particular, $2A = A + A$. We also write, e.g. $2A - 2A$ for $\{a_1 + a_2 - a_3 - a_4 : a_1, \ldots, a_4 \in A\}$.

4.2. Ruzsa's triangle inequality and covering lemma

In this section we prove two elegant results of Ruzsa about the size of sumsets. They are surprisingly useful despite their apparent simplicity.

LEMMA 4.2.1 (Ruzsa triangle inequality). *Suppose that U, V, W are finite additive sets. Then*

$$|V - W||U| \leqslant |V - U||U - W|.$$

Proof. We will define a map $\phi : (V - W) \times U \to (V - U) \times (U - W)$, and prove that it is an injection, which implies the result. Given $d \in V - W$ select a pair

$v_d \in V, w_d \in W$ for which $d = v_d - w_d$ (there may be more than one such pair, but for each d we make a definite choice). Then define

$$\phi(d,u) = (v_d - u, u - w_d)$$

for each $d \in V - W$ and $u \in U$. To prove that ϕ is an injection, suppose that $(x,y) \in \mathrm{im}(\phi) \subset (V-U) \times (U-W)$. If $\phi(d,u) = (x,y)$ then $x + y = (v_d - u) + (u - w_d) = v_d - w_d = d$, and therefore we can determine d and hence v_d and w_d from (x,y). And we also determine u as $u = -x + v_d$ $(= y - w_d)$. □

Remark. If we define

$$d(U,V) := \log \frac{|U-V|}{|U|^{1/2}|V|^{1/2}}$$

then the Ruzsa triangle inequality may be written

$$d(V,W) \leqslant d(U,V) + d(U,W).$$

This explains the term "triangle inequality". Note that, although the triangle inequality is satisfied, d is not a true distance. This is because $d(U,V) = 0$ neither implies, nor is implied by, $U = V$.

LEMMA 4.2.2 (Ruzsa's covering lemma). *Suppose that A and B are finite additive sets and that $|A+B| \leqslant K|A|$. Then B may be covered by k translates of $A-A$, for some $k \leqslant K$. That is, there is a set X, $|X| \leqslant K$, such that*

$$B \subset (A-A) + X.$$

Proof. Choose $X \subset B$ maximal so that $\{A+x : x \in X\}$ are disjoint. The union of these sets contains exactly $|A||X|$ elements, and all of these elements lie in $A+B$. Therefore $|X| \leqslant K$. Now, if $b \in B$ then $A+b$ intersects $A+x$ for some $x \in X$, because of the maximality of X, and so $b \in A-A+x$. Hence, $B \subset (A-A)+X$. □

4.3. Petridis's inequality

In this section and the next we develop inequalities controlling the size of sums of three or more sets. A beautiful way to do this was discovered surprisingly recently by Petridis. His result is stated as Corollary 4.3.1 below. We give an elegant rephrasing of his proof which was given by Tao on the blog of Tim Gowers.

Let B be a set in some abelian group G. Let K be a real number, and consider the function ϕ on subsets of G defined by

$$\phi(A) := |A+B| - K|A|. \tag{4.1}$$

LEMMA 4.3.1. *ϕ is* submodular*, that is to say it satisfies*

$$\phi(A \cup A') + \phi(A \cap A') \leqslant \phi(A) + \phi(A').$$

Proof. Write $\sigma(A) := A + B$. Observe that

$$\sigma(A \cup A') = \sigma(A) \cup \sigma(A'),$$

and that

$$\sigma(A \cap A') \subseteq \sigma(A) \cap \sigma(A').$$

Therefore

$$\begin{aligned} |\sigma(A \cup A')| = |\sigma(A) \cup \sigma(A')| &= |\sigma(A)| + |\sigma(A')| - |\sigma(A) \cap \sigma(A')| \\ &\leqslant |\sigma(A)| + |\sigma(A')| - |\sigma(A \cap A')|, \end{aligned}$$

that is to say $|\sigma|$ satisfies the submodularity property

$$|\sigma(A \cup A')| + |\sigma(A \cap A')| \leqslant |\sigma(A)| + |\sigma(A')|.$$

Since the function $|A|$ satisfies

$$|A \cup A'| + |A \cap A'| = |A| + |A'|,$$

the result follows immediately, since $\phi(A) = |\sigma(A)| - K|A|$. □

LEMMA 4.3.2. *Let ϕ be any submodular function. Suppose that $A_1, \dots, A_n$ are sets with the following property: $\phi(A_i) = 0$, and $\phi(Z_i) \geqslant 0$ for every subset $Z_i \subseteq A_i$. Then $\phi\big(\bigcup_{i=1}^n A_i\big) \leqslant 0$.*

Proof. By the assumptions and submodularity, for any i and for any set S, we have

$$\phi(A_i \cup S) \leqslant \phi(A_i \cup S) + \phi(A_i \cap S) \leqslant \phi(A_i) + \phi(S) = \phi(S).$$

The result then follows immediately by induction on n. □

PROPOSITION 4.3.1 (Petridis). *Let A, B be sets in some abelian group. Suppose that $|A+B| = K|A|$ and that $|Z+B| \geqslant K|Z|$ for all $Z \subseteq A$. Then, for any further set S in the group, $|A+B+S| \leqslant K|A+S|$.*

Proof. Apply Lemma 4.3.2 with the particular function ϕ defined in (4.1) above. Take the A_i to be the translates $A + s$ of A by elements of s. It is easy to check that the hypotheses of Lemma 4.3.2 hold. Observe that $\bigcup_{i=1}^n A_i = A + S$, and so the Lemma implies that $\phi(A + S) \leqslant 0$, or in other words $|A + B + S| \leqslant K|A + S|$. □

It is convenient to apply Petridis' inequality in the following form.

COROLLARY 4.3.1. *Let A, B be sets in some abelian group. Suppose that $|A+B| \leqslant K|A|$. Let $X \subseteq A$ be a non-empty set for which the ratio $|X+B|/|X|$ is minimal. Then for any further set S we have*

$$|S+X+B| \leqslant K|S+X|.$$

Proof. Apply Proposition 4.3.1 with A replaced by X. □

4.4. The Plünnecke–Ruzsa inequality

The most widely applicable result about higher-order sumsets is the Plünnecke–Ruzsa inequality.

THEOREM 4.4.1 (Plünnecke–Ruzsa). *Suppose that A and B are additive sets with $|A+B| \leqslant K|A|$. Let $k, \ell \geqslant 0$ be integers. Then $|kB - \ell B| \leqslant K^{k+\ell}|A|$.*

The original proof was quite long and involved a fair amount of machinery from graph theory. Nowadays, it can be deduced quickly from Petridis's inequality.

LEMMA 4.4.1. *Suppose that A and B are finite additive sets for which $|A+B| \leqslant K|A|$. Then there exists $X \subset A$ for which $|X+kB| \leqslant K^k|X|$.*

Proof. Let X be the subset of A for which the ratio $|X+B|/|X|$ is minimal. By Petridis's inequality (Corollary 4.3.1) with $S = (k-1)B$, we have

$$|X+kB| = |X+(k-1)B+B| \leqslant K|X+(k-1)B|.$$

The result then follows by induction on k. □

Proof. [Proof of Theorem 4.4.1]. Suppose that A and B are finite additive sets for which $|A+B| \leqslant K|A|$. By Ruzsa's Triangle Inequality with U, V, W replaced by $X, -kB, -\ell B$, respectively, and then Lemma 4.4.1, we have

$$|kB - \ell B|\ |X| \leqslant |X+kB| \cdot |X+\ell B| \leqslant K^{k+\ell}|X|^2.$$

Thus, since $X \subset A$, $|kB - \ell B| \leqslant K^{k+\ell}|X| \leqslant K^{k+\ell}|A|$. □

CHAPTER 5

Freiman's theorem

This chapter contains one of the highlights of the course, which is a fairly complete (at least qualitatively) answer to the question of what sets with small sumset look like. Let us begin with a little context for the question.

Recall that if A is a set of integers then

$$A + A := \{a_1 + a_2 : a_1, a_2 \in A\}.$$

Suppose A has size n. How big is $A+A$? Trivially, it has size at most $\frac{1}{2}n(n+1)$, that being the number of pairs (a_1, a_2), with (a_1, a_2) and (a_2, a_1) counted the same.

On the other hand, it has size at least $2n - 1$. Writing $a_1 < \cdots < a_n$ for the elements of A, we have

$$a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_n + a_n,$$

a listing of $2n - 1$ distinct elements of A.

Equality can occur in both bounds. For example if $A = \{1, 2, \ldots, 2^{n-1}\}$ then all the sums $a_1 + a_2$ are distinct (except for the trivial relations $a_1 + a_2 = a_2 + a_1$). If $A = \{1, \ldots, n\}$ then $A + A = \{2, \ldots, 2n\}$, a set of size $2n - 1$.

We say that A has *doubling constant at most* K if

$$\frac{|A + A|}{|A|} \leqslant K.$$

Typically, we will have in mind that K is fixed (say $K = 10$) and $n = |A|$ is very large.

Here is the basic question to be considered in this chapter.

QUESTION 5.0.1. What is the structure of A if $|A + A| \leqslant K|A|$, for some small K?

5.1. Generalised progressions and Freiman's theorem

Before stating the main result, let us give some progressively more complicated motivating examples.

EXAMPLE 5.1.1 (Progression). Let A be any arithmetic progression of length n. Then $|A + A| = 2n - 1$.

EXAMPLE 5.1.2 (Subsets of progressions). Let P be a progression of length Cn, and let $A \subset P$ be an arbitrary set of size n. Then $|A+A| \leqslant 2Cn$.

EXAMPLE 5.1.3 (2-dimensional progression). Suppose that $L_1 L_2 = n$, and consider a set A of the form

$$A := \{x_0 + \ell_1 x_1 + \ell_2 x_2 : 0 \leqslant \ell_1 < L_1, 0 \leqslant \ell_2 < L_2\}.$$

If the x_i are suitably widely spaced, the elements described here are all distinct and $|A| = n$. In this case we say that A is *proper*. We have

$$A + A = \{2x_0 + \ell_1' x_1 + \ell_2' x_2 : 0 \leqslant \ell_1' < 2L_1 - 1, 0 \leqslant \ell_2' < 2L_2 - 1\},$$

and so certainly

$$|A+A| \leqslant 4|A|.$$

EXAMPLE 5.1.4 (d-dimensional progression). The same as above, but with d parameters $L_1, \dots, L_d$: thus

$$A = \{x_0 + l_1 x_1 + \cdots + l_d x_d : 0 \leqslant l_i < L_i\}. \tag{5.1}$$

Now, if A is proper, we have $|A+A| \leqslant 2^d |A|$.

EXAMPLE 5.1.5 (Subsets of multidimensional progressions). Let P be a proper d-dimensional progression of size Cn. Let $A \subset P$ be an arbitrary set of size n. Then

$$|A+A| \leqslant |P+P| \leqslant 2^d |P| = 2^d Cn.$$

The final example gives a somewhat large class of sets with doubling constant at most K (pick any parameters d, C with $2^d C \leqslant K$).

Freiman's theorem is the result that the above examples are the only ones.

THEOREM 5.1.1 (Freiman). *Suppose that $A \subset \mathbf{Z}$ is a finite set with $|A+A| \leqslant K|A|$. Then A is contained in a generalised progression P of dimension $\ll_K 1$ and size $\ll_K |A|$.*

The *size* of a generalised progression as in (5.1) is defined to be $L_1 \cdots L_d$. This is at least the cardinality of the progression, but is strictly bigger than it if the progression fails to be proper.

Freiman's theorem states that A is contained in a proper progression of dimension at most $d(K)$ and size at most $C(K)|A|$, where $d(), C()$ are functions of K only. In this course we will not be concerned with bounds, but the argument we give leads to a bound for $d(K)$ that is exponential in K, and a bound for $C(K)$ that is doubly exponential in K. This is quite far from the truth; in fact, it does not require a vast amount of further effort to remove an exponential from both of these bounds, but we will not do so here.

Many other refinements are possible, but again we will not cover them here. For example, one can insist that P be proper if desired.

5.2. Freiman homomorphisms

In his remarkably insightful 1966 book [**5**], Freiman made an attempt to treat additive number theorey by analogy with the way Klein treated geometry: as well as sets $A, B, \cdots$ of integers, one should study maps between them and, most particularly, properties invariant under natural types of map. This was doubtless regarded as somewhat eccentric at the time, but the notion of Freiman homomorphism is now quite important in additive combinatorics.

DEFINITION 5.2.1. Suppose that $s \geqslant 2$ is an integer. Suppose that A, B are additive sets. Then we say that a map $\phi : A \to B$ is a Freiman s-homomorphism if we have

$$\phi(a_1) + \cdots + \phi(a_s) = \phi(a'_1) + \cdots + \phi(a'_s)$$

whenever

$$a_1 + \cdots + a_s = a'_1 + \cdots + a'_s.$$

It is obvious that any group homomorphism restricts to a Freiman homomorphism (of arbitrary order) on any subset. However, the notion is much more general. For example, any map whatsoever from $A = \{1, 10, 100, 1000\}$ to another additive set is a Freiman 2-homomorphism, simply because A has no nontrivial relations of the form $a_1 + a_2 = a'_1 + a'_2$.

The map ϕ is said to be a Freiman s-isomorphism if it has an inverse ϕ^{-1} which is also a Freiman s-homomorphism. We caution that, contrary to what is often expected in more algebraic situations, a one-to-one Freiman homomorphism need not be a Freiman isomorphism. For example, the obvious map

$$\phi : \{0, 1\}^n \to (\mathbf{Z}/2\mathbf{Z})^n$$

is a Freiman homomorphism of all orders (it is induced from the natural group homomorphism $\mathbf{Z}^n \to (\mathbf{Z}/2\mathbf{Z})^n$). However, it is not a Freiman 2-isomorphism as $(\mathbf{Z}/2\mathbf{Z})^n$ contains a great many more additive relations than $\{0, 1\}^n$.

The following lemma records some basic facts about Freiman isomorphisms.

LEMMA 5.2.1. *Suppose that A, B, C are additive sets. Let $s \geqslant 2$ be an integer. Then we have the following.*

(i) *Suppose that $\phi : A \to B$ and $\psi : B \to C$ are Freiman s-homomorphisms. Then so is the composition $\psi \circ \phi$.*
(ii) *Suppose that $\phi : A \to B$ is a Freiman s-homomorphism. Then it is also a Freiman s'-homomorphism for every s' satisfying $2 \leqslant s' \leqslant s$.*

(iii) *Suppose that $\phi : A \to B$ is a Freiman s-homomorphism and let $k, l \geqslant 0$ be integers. Then ϕ induces a Freiman s'-homomorphism $\tilde{\phi} : kA - lA \to kB - lB$, for any integer $s' \leqslant s/(k+l)$.*

(iv) *The above three statements also hold with "homo" replaced by "iso" throughout.*

(v) *Suppose that P is a generalised progression and that $\phi : P \to B$ is a Freiman 2-homomorphism. Then $\phi(P)$ is a generalised progression of the same dimension. If ϕ is a Freiman 2-isomorphism, and if P is proper, then so is $\phi(P)$.*

(vi) *Let $\pi_m : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ be the natural map. Then π_m is a Freiman s-isomorphism when restricted to $(t, t + \frac{m}{s}] \cap \mathbf{Z}$, for any $t \in \mathbf{R}$.*

Proof. The first four parts of this are very straightforward once one has understood the definitions, and we will not go over them carefully in lectures. Perhaps (iii) requires some further comment: one should define $\tilde{\phi} : kA - lA \to kB - lB$ by

$$\tilde{\phi}(a_1 + \cdots + a_k - a'_1 - \cdots - a'_l) = \phi(a_1) + \cdots + \phi(a_k) - \phi(a'_1) - \cdots - \phi(a'_l).$$

One must then check that this is well-defined and is a Freiman homomorphism of the order claimed.

To prove (v), let $\phi : P \to \phi(P)$ be a Freiman 2-homomorphism. Suppose that $P = \{x_0 + l_1x_1 + \cdots + l_dx_d : 0 \leqslant l_i < L_i\}$. Set $y_0 = \phi(x_0)$, and define $y_1, \ldots, y_d$ by $y_0 + y_i = \phi(x_0 + x_i)$ for $i = 1, \ldots, d$; we claim that $\phi(x_0 + l_1x_1 + \cdots + l_dx_d) = y_0 + l_1y_1 + \cdots + l_dy_d$ for all $l_1, \ldots, l_d$ satisfying $0 \leqslant l_i < L_i$. This may be established by induction on $l_1 + \cdots + l_d$, noting that we have defined the y_i in such a way that it holds whenever $l_1 + \cdots + l_d = 0$ or 1. To obtain the statement for $(l_1, \ldots, l_d) = (1, 1, 0, \ldots, 0)$, for example, one may use the relation

$$x_0 + (x_0 + x_1 + x_2) = (x_0 + x_1) + (x_0 + x_2)$$

to conclude that

$$\phi(x_0) + \phi(x_0 + x_1 + x_2) = \phi(x_0 + x_1) + \phi(x_0 + x_2)$$

and hence that $\phi(x_0 + x_1 + x_2) = y_0 + y_1 + y_2$, as required.

Finally, we comment on (vi). Since π_m is a group homomorphism, it is also a Freiman homomorphism. Its restriction to any interval of length at most m is a bijection. Suppose that $x_1, \ldots, x_s, x'_1, \ldots, x'_s$ satisfy $t < x_i, x'_i \leqslant t + \frac{m}{s}$ and that $\pi_m(x_1) + \cdots + \pi_m(x_s) = \pi_m(x'_1) + \cdots + \pi_m(x'_s)$, that is to say $x_1 + \cdots + x_s = x'_1 + \cdots + x'_s (\mathrm{mod}\, m)$. Then, since $|x_1 + \cdots + x_s - x'_1 - \cdots - x'_s| < m$, we must have $x_1 + \cdots + x_s = x'_1 + \cdots + x'_s$. □

5.3. Ruzsa's model lemma

In this section we prove a remarkable lemma of Imre Ruzsa. It asserts that a subset of $\mathbf{Z}$ with small doubling has a large piece which is Freiman isomorphic to a dense subset of a cyclic group $\mathbf{Z}/m\mathbf{Z}$. In that setting the tools of harmonic analysis become much more powerful, unlike for arbitrary subsets of $\mathbf{Z}$ (even those of small doubling) which could well be highly "spread out". Here is Ruzsa's lemma.

PROPOSITION 5.3.1 (Ruzsa model lemma). *Suppose that $A \subset \mathbf{Z}$ is a finite set and that $s \geqslant 2$ is an integer. Let $m \geqslant |sA - sA|$ be an integer. Then there is a set $A' \subset A$ with $|A'| \geqslant |A|/s$ which is Freiman s-isomorphic to a subset of $\mathbf{Z}/m\mathbf{Z}$.*

Proof. By translating A if necessary, we may assume that A consists of positive integers. Let q be a very large prime number. For $\lambda \in (\mathbf{Z}/q\mathbf{Z})^\times$, consider the composition $\phi_\lambda := \gamma \circ \beta \circ \alpha_\lambda$ of maps

$$\mathbf{Z} \xrightarrow{\alpha_\lambda} \mathbf{Z}/q\mathbf{Z} \xrightarrow{\beta} \{1, \dots, q\} \xrightarrow{\gamma} \mathbf{Z}/m\mathbf{Z}$$

where

- α_λ is reduction mod q followed by multiplication by λ;
- β inverts the reduction mod q map;
- γ is the reduction mod m map.

Now α_λ and γ are Freiman homomorphisms of all orders. The map β is not, but by Proposition (5.2.1) (vi), it is a Freiman s-homomorphism on the reduction mod q of any interval $I_j := \{n \in \mathbf{Z} : \frac{jq}{s} < n \leqslant \frac{(j+1)q}{s}\}$. Since s such intervals (with $j = 0, 1, \dots, q-1$) cover $\{1, \dots, q\}$, it follows by the pigeonhole principle that for every λ there is a $j = j(\lambda)$ such that the set

$$A_\lambda := \{a \in A : \alpha_\lambda(a) \in I_{j(\lambda)} (\mathrm{mod}\, q)\}$$

has size at least $|A|/s$. By construction, ϕ_λ is a Freiman s-homomorphism when restricted to A_λ.

Everything we have said so far holds for arbitrary λ. To complete the proof, we now show that there exists some λ such that ϕ_λ is invertible, and its inverse is a Freiman s-homomorphism. If this fails for some λ then this means that there is

$$d = a_1 + \cdots + a_s - a'_1 - \cdots - a'_s \neq 0$$

such that

$$\phi_\lambda(a_1) + \cdots + \phi_\lambda(a_s) = \phi_\lambda(a'_1) + \cdots + \phi_\lambda(a'_s). \tag{5.2}$$

Here, d and the $a_i, a'_i \in A_\lambda$ depend on λ.

Write

$$x := \sum_{i=1}^{s} \beta(\alpha_\lambda(a_i)) - \sum_{i=1}^{s} \beta(\alpha_\lambda(a_i')).$$

Then if (5.2) holds we have $\gamma(x) = 0$, that is to say $x \equiv 0 (\mathrm{mod}\, m)$.

Without loss of generality (switching the a_i and the a_i' if necessary) we may assume that $x \geqslant 0$. Also, since the a_i, a_i' lie in A_λ, it follows that $x \in s(I_{j(\lambda)} - I_{j(\lambda)}) \subset (-q, q)$. Therefore $0 \leqslant x < q$.

Now by construction, x and λd are congruent modulo q. It therefore follows that

$$x = \psi(\lambda d),$$

where $\psi(n)$ is the unique integer in $\{0, 1, \dots, q-1\}$ congruent to n modulo q.

From now on we indicate the dependence of d on λ explicitly. To summarise, we have shown the following. If $\phi_\lambda|_{A_\lambda}$ is not a Freiman s-isomorphism, then there must be some $d_\lambda \in (sA - sA) \setminus \{0\}$ such that

$$\psi(\lambda d_\lambda) \equiv 0 (\mathrm{mod}\, m).$$

To get a contradiction, Let us fix $d \in (sA - sA) \setminus \{0\}$ and ask about values of λ for which $d = d_\lambda$: lacking imagination, we call them "bad for d". If the prime q is chosen big enough then it will not divide any element of $(sA - sA) \setminus \{0\}$, so d is coprime to q.

As λ ranges over $(\mathbf{Z}/q\mathbf{Z})^\times$, λd covers $(\mathbf{Z}/q\mathbf{Z})^\times$ uniformly, and hence the set $\{\psi(\lambda d) : \lambda \in (\mathbf{Z}/q\mathbf{Z})^\times\}$ coincides with $\{1, \dots, q-1\}$. The number of elements y in this interval for which $y \equiv 0 (\mathrm{mod}\, m)$ is at most $(q-1)/m$. Since each d lies in the set $(sA - sA) \setminus \{0\}$, it follows that the number of λ which are bad for *some* d is at most

$$\frac{q-1}{m}\big(|sA - sA| - 1\big) < q - 1,$$

the inequality being a consequence of the assumption that $m \geqslant |sA - sA|$.

This is a contradiction, since *every* λ is bad for some d (namely d_λ).

□

In our proof of Freiman's theorem, we will use the following corollary.

Corollary 5.3.1. *Suppose that $A \subset \mathbf{Z}$ is a finite set with doubling constant K. Then there is a prime $q \leqslant 2K^{16}|A|$ and a subset $A' \subset A$ with $|A'| \geqslant |A|/8$ such that A' is Freiman 8-isomorphic to a subset of $\mathbf{Z}/q\mathbf{Z}$.*

Proof. By the Plünnecke–Ruzsa inequality, Theorem 4.4.1, we have $|8A - 8A| \leqslant K^{16}|A|$. Now by Bertrand's postulate there is a prime q satisfying $|8A - 8A| \leqslant q \leqslant 2|8A - 8A|$. This prime of course satisfies the bound $q \leqslant 2K^{16}|A|$, and by the

Ruzsa model lemma there is a subset $A' \subset A$ with $|A'| \geqslant |A|/8$ which is Freiman 8-isomorphic to a subset of $\mathbf{Z}/q\mathbf{Z}$. □

5.4. Bogolyubov's lemma

Ruzsa's model lemma (or, more accurately, Corollary 5.3.1) allows us to switch attention from a set $A \subset \mathbf{Z}$ with small doubling to a dense subset of a cyclic group $\mathbf{Z}/q\mathbf{Z}$. We now prove a lemma about the structure of such sets.

DEFINITION 5.4.1. Suppose that $R = \{r_1, \dots, r_k\}$ is a set of nonzero elements of $\mathbf{Z}/q\mathbf{Z}$ and that $\varepsilon > 0$ is a parameter. Then we define the *Bohr set* $B(R, \varepsilon)$ with frequency set R and width ε by

$$B(R, \varepsilon) := \{x \in \mathbf{Z}/q\mathbf{Z} : \|\frac{r_i x}{q}\|_{\mathbf{T}} \leqslant \varepsilon \text{ for } i = 1, 2, \dots, k\}.$$

The parameter k is said to be the *dimension* of the Bohr set.

PROPOSITION 5.4.1 (Bogolyubov's lemma). *Let $S \subset \mathbf{Z}/q\mathbf{Z}$ be a set of size σq. Then $2S - 2S$ contains a Bohr set of dimension at most $4/\sigma^2$ and width at least $\frac{1}{10}$.*

In the proof, we will use the discrete Fourier transform, specifically the Fourier transform on $\mathbf{Z}/q\mathbf{Z}$. (The Fourier transform can in fact be developed on any locally compact abelian group, and in this way the Fourier transform on $\mathbf{Z}$ which featured in Chapter 3, and the discrete Fourier transform on $\mathbf{Z}/q\mathbf{Z}$, may be considered as special cases of the same general concept.) Here are the relevant definitions and basic properties.

DEFINITION 5.4.2. Let $f : \mathbf{Z}/q\mathbf{Z} \to \mathbf{C}$ be a function. Then for $r \in \mathbf{Z}/q\mathbf{Z}$ we define the (discrete) Fourier transform

$$\hat{f}(r) := \frac{1}{q} \sum_{x \in \mathbf{Z}/q\mathbf{Z}} f(x) e(-rx/q).$$

PROPOSITION 5.4.2. *In the following proposition, $f, g : \mathbf{Z}/q\mathbf{Z} \to \mathbf{C}$ are two functions.*

(i) *We have the inversion formula*

$$f(x) = \sum_{r \in \mathbf{Z}/q\mathbf{Z}} \hat{f}(r) e(rx/q).$$

(ii) *We have the Parseval identity*

$$\frac{1}{q} \sum_{x \in \mathbf{Z}/q\mathbf{Z}} f(x)\overline{g(x)} = \sum_{r \in \mathbf{Z}/q\mathbf{Z}} \hat{f}(r)\overline{\hat{g}(r)}.$$

(iii) *If the convolution* $f * g : \mathbf{Z}/q\mathbf{Z} \to \mathbf{C}$ *is defined by*

$$(f*g)(x) := \frac{1}{q}\sum_{y \in \mathbf{Z}/q\mathbf{Z}} f(y)g(x-y)$$

then $\widehat{f*g}(r) = \hat{f}(r)\hat{g}(r)$.

Proof. Once again, all of this is an easy check using the definitions, as well as the fact that

$$\sum_r e(rx/q) = \begin{cases} q & x = 0 \\ 0 & x \in (\mathbf{Z}/q\mathbf{Z}) \setminus \{0\}. \end{cases}$$

□

Remark. Taking $f = g$ in the Parseval identity gives

$$\frac{1}{q}\sum_{x \in \mathbf{Z}/q\mathbf{Z}} |f(x)|^2 = \sum_{r \in \mathbf{Z}/q\mathbf{Z}} |\hat{f}(r)|^2.$$

It is worth pausing to consider what convolution "does". If f and g are functions supported on sets $A, B \subseteq \mathbf{Z}/q\mathbf{Z}$ respectively (for instance, we could have $f = 1_A$ and $g = 1_B$) then $f * g$ is supported on $A + B$. Moreover, $f * g$ has a nice Fourier transform, which can be very convenient for further analysis. Note carefully that $1_A * 1_B$ is not the same thing as 1_{A+B}; the latter function puts equal weight on every element of $A + B$, whereas the former weights elements x according to the number of representations as $a + b$ with $a \in A, b \in B$.

Now we turn to the proof of Bogolyubov's lemma, Lemma 5.4.1.

Proof. [Proof of Lemma 5.4.1] Consider the function $f := 1_S * 1_S * 1_{-S} * 1_{-S}$. This is supported on $2S - 2S$, that is to say if $f(x) > 0$ then $x \in 2S - 2S$. Note also that $\hat{1}_{-S}(r) = \overline{\hat{1}_S(r)}$, and so $\hat{f}(r) = |\hat{1}_S(r)|^4$. By the Fourier inversion formula and the fact that f is real, we have

$$f(x) = \sum_r |\hat{1}_S(r)|^4 e(rx/q) = \sum_r |\hat{1}_S(r)|^4 \cos(2\pi rx/q). \tag{5.3}$$

Let R be the set of all $r \neq 0$ for which $|\hat{1}_S(r)| \geqslant \sigma^{3/2}/2$. By Parseval's identity we have

$$|R|\frac{\sigma^3}{4} \leqslant \sum_{r \in R} |\hat{1}_S(r)|^2 \leqslant \sum_r |\hat{1}_S(r)|^2 = \frac{1}{q}\sum_{x \in \mathbf{Z}/q\mathbf{Z}} 1_S(x)^2 = \sigma,$$

and so

$$|R| \leqslant 4/\sigma^2. \tag{5.4}$$

We claim that $B(R, \frac{1}{10}) \subset 2S - 2S$, to which end it suffices to show that $f(x) > 0$ for $x \in B(R, \frac{1}{10})$. To do this, we will use the formula (5.3). We split the sum over r into three pieces: the term $r = 0$, the terms with $r \in R$, and all other terms.

Clearly

$$|\hat{1}_S(0)|^4 = \sigma^4.$$

If $r \in R$ then $\cos(2\pi rx/q) \geqslant 0$, so the sum of these terms is nonnegative. Finally,

$$\sum_{r \notin R \cup \{0\}} |\hat{1}_S(r)|^4 \cos(2\pi rx/q) \geqslant -\sum_{r \notin R \cup \{0\}} |\hat{1}_S(r)|^4 \geqslant -\frac{\sigma^3}{4} \sum_r |\hat{1}_S(r)|^2 = -\frac{\sigma^4}{4},$$

the last step being a further application of Parseval's identity. Combining all of this we obtain

$$f(x) \geqslant \sigma^4 + 0 - \frac{\sigma^4}{4} > 0,$$

as required. □

5.5. Generalised progressions in Bohr sets

It is by no means obvious what has been gained in proving Proposition 5.4.1. The answer is that a Bohr set $B(R, \varepsilon)$ has a great deal of structure, in particular containing a large generalised progression. The key proposition is as follows.

PROPOSITION 5.5.1. *Let $R \subset \mathbf{Z}/q\mathbf{Z}$ be a set of size k, not containing zero. Let $0 < \varepsilon < \frac{1}{2}$. Then the Bohr set $B(R, \varepsilon)$ contains a proper generalised progression of dimension k and cardinality at least $(\varepsilon/k)^k q$.*

In the proof, we will rely on a result from the geometry of numbers, Minkowski's second theorem. This is stated as Proposition 5.5.2 below. The proof is not examinable, but it is given in Appendix B. To even state the theorem, we need some terminology.

A *lattice* $\Lambda \subset \mathbf{R}^d$ is a discrete and cocompact subgroup of $\mathbf{R}^d$. It is a theorem that every lattice is of the form $\mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \cdots \oplus \mathbf{Z}v_d$ for linearly independent $v_1, \ldots, v_d$, which are then called an *integral basis* for Λ. The set $\mathcal{F} := \{x_1v_1 + \cdots + x_dv_d : 0 \leqslant x_i < 1\}$ is then called a fundamental region for Λ; note that translates of it by Λ precisely cover $\mathbf{R}^d$. Note that the v_i (and hence $\mathcal{F}$) are not uniquely determined by Λ, but it turns out that the volume of $\mathcal{F}$ is. The determinant $\det(\Lambda)$ is the volume of a fundamental region of Λ.

The statement of Minkowski's Second Theorem also involves a centrally symmetric convex body $K \subset \mathbf{R}^d$. This means a set which is convex (meaning that if $x, y \in K$ then $\lambda x + (1-\lambda)y \in K$ for all $\lambda \in [0,1]$) and centrally symmetric, which means that if $x \in K$ then $-x \in K$.

The geometry of numbers is, to an extent, the study of how lattices Λ interact with convex bodies K.

Suppose we have a lattice Λ and a convex body K. We define the *successive minima* $\lambda_1, \ldots, \lambda_d$ of K with respect to Λ as follows: λ_j is the infimum of those

λ for which the dilate λK contains j linearly independent elements of Λ. If K is compact then $\lambda_j K$ itself contains j linearly independent elements of Λ. (For each $\varepsilon > 0$, $(\lambda_j + \varepsilon)K$ contains such elements. Since these all lie in $(\lambda_j + 1)K$, there are only finitely many choices, and in particular for some sequence of ε tending to zero we may make the same choice. Since K is compact, these elements all lie in $\lambda_j K$.)

PROPOSITION 5.5.2 (Minkowski's Second Theorem). *We have* $\lambda_1 \cdots \lambda_d \operatorname{vol}(K) \leqslant 2^d \det(\Lambda)$.

We now turn to the proof of Proposition 5.5.1.

Proof. [Proof of Proposition 5.5.1.] Let $R = \{r_1, \dots, r_k\}$ and consider the lattice

$$\Lambda = q\mathbf{Z}^k + (r_1, \dots, r_k)\mathbf{Z}.$$

Since q is prime, this may be written as a direct sum

$$q\mathbf{Z}^k \oplus \{0, 1, \dots, q-1\} \cdot (r_1, \dots, r_k).$$

Thus Λ has index q as a subgroup of $q\mathbf{Z}^k$, and from this and the fact that $\det(q\mathbf{Z}^k) = q^k$ it follows that $\det(\Lambda) = q^{k-1}$ (see Lemma B.0.1).

Take $K \subset \mathbf{R}^k$ to be the box $\{\mathbf{x} : \|\mathbf{x}\|_\infty \leqslant \varepsilon q\}$. Let $\lambda_1, \dots, \lambda_k$ be the successive minima of K with respect to Λ. Since K is closed, $\lambda_j K$ contains j linearly independent elements of Λ. We may, by choosing each element in turn, select a basis $\mathbf{b}_1, \dots, \mathbf{b}_k$ for $\mathbf{R}^k$ with $\mathbf{b}_j \in \Lambda \cap \lambda_j K$ for all j. (Such a basis is called a *directional basis*; we should caution that, whilst the $\mathbf{b}_j$ are linearly independent elements of Λ, they need not form an integral basis for Λ.) Thus $\mathbf{b}_j \in \Lambda$ and $\|\mathbf{b}_j\|_\infty \leqslant \lambda_j \varepsilon q$. Set $L_j := \lceil 1/\lambda_j k \rceil$ for $j = 1, \dots, k$. Then if $0 \leqslant l_j < L_j$ we have $\|l_j \mathbf{b}_j\|_\infty \leqslant \varepsilon q/k$ and therefore

$$\|l_1 \mathbf{b}_1 + \cdots + l_k \mathbf{b}_k\|_\infty \leqslant \varepsilon q.$$

Now each $\mathbf{b}_i$ lies in Λ and hence is congruent to $x_i(r_1, \dots, r_k) (\mathrm{mod}\, q)$ for some x_i, $0 \leqslant x_i < q$. Abusing notation slightly, we think of these x_i as lying in $\mathbf{Z}/q\mathbf{Z}$. The preceding observation implies that

$$\|\frac{(l_1 x_1 + \cdots + l_k x_k) r_i}{q}\|_{\mathbf{T}} \leqslant \varepsilon$$

for each i, or in other words the generalised progression $\{l_1 x_1 + \cdots + l_k x_k : 0 \leqslant l_i < L_i\}$ is contained in the Bohr set $B(R, \varepsilon)$.

It remains to prove a lower bound on the size of this progression and also to establish its properness. The lower bound on the size is easy: it is at least $k^{-k}(\lambda_1 \cdots \lambda_k)^{-1}$ which, by Minkowski's Second Theorem and the fact that $\det(\Lambda) = q^{k-1}$ and $\operatorname{vol}(K) = (2\varepsilon q)^k$, is at least $(\varepsilon/k)^k q$.

To establish the properness, suppose that

$$l_1 x_1 + \cdots + l_k x_k = l_1' x_1 + \cdots + l_k' x_k (\mathrm{mod}\, q),$$

where $|l_i|, |l_i'| < \lceil 1/k\lambda_i \rceil$. Then the vector

$$\mathbf{b} = (l_1 - l_1')\mathbf{b}_1 + \cdots + (l_k - l_k')\mathbf{b}_k$$

lies in $q\mathbf{Z}^k$ and furthermore

$$\|\mathbf{b}\|_\infty \leqslant \sum_{i=1}^{k} 2\lfloor \frac{1}{\lambda_i k} \rfloor \|\mathbf{b}_i\|_\infty \leqslant 2\varepsilon q.$$

Since we are assuming that $\varepsilon < 1/2$ it follows that $\mathbf{b} = 0$ and hence, due to the linear independence of the $\mathbf{b}_i$, that $l_i = l_i'$ for all i. Therefore the progression is indeed proper. □

5.6. Freiman's theorem: conclusion of the proof

In this section, we conclude the proof of Freiman's theorem.

Proof. [Proof of Theorem 5.1.1] By Corollary 5.3.1, the corollary of Ruzsa's model lemma, there is a prime $q \leqslant 2K^{16}|A|$ and a subset $A' \subset A$ with $|A'| \geqslant |A|/8$ such that A' is Freiman 8-isomorphic to a subset $S \subset \mathbf{Z}/q\mathbf{Z}$. If $\sigma := |S|/q$ then we have $\sigma \geqslant \frac{1}{16}K^{-16}$.

By Bogolyubov's lemma, Proposition 5.4.1, $2S - 2S$ contains a Bohr set of dimension at most $2^{10}K^{32}$ and width at least $\frac{1}{10}$.

By Proposition 5.5.1, that Bohr set (and hence $2S - 2S$) contains a proper generalised progression P of dimension at most $K^{O(1)}$ and cardinality at least $\exp(-K^{O(1)})q$. (We could keep track of exact constants, but this becomes a little tedious).

Now A' is Freiman 8-isomorphic to S, and so by Lemma 5.2.1 (iii), $2A' - 2A'$ is Freiman 2-isomorphic to $2S - 2S$. The inverse of this Freiman isomorphism restricts to a Freiman isomorphism $\phi : P \to \phi(P) \subset 2A' - 2A'$. By Lemma 5.2.1 (v), $Q = \phi(P)$ is also a proper generalised progression, of the same dimension and size as P. Therefore we have shown that $2A - 2A$ contains a proper generalised progression Q of dimension $K^{O(1)}$ and

$$|Q| \geqslant \exp(-K^{O(1)})|A|. \tag{5.5}$$

To finish the argument, we apply the covering lemma, Lemma 4.2.2, to the sets Q and A. Since

$$Q + A \subset (2A - 2A) + A = 3A - 2A,$$

the Plünnecke–Ruzsa inequality and (5.5) imply that

$$|Q + A| \leqslant K^5|A| \leqslant \exp(K^{O(1)})|Q|.$$

By Lemma 4.2.2, there is some set $Y = \{y_1, \dots, y_m\}$,

$$m \leqslant \exp(K^{O(1)}), \tag{5.6}$$

such that

$$A \subset (Q - Q) + Y.$$

Suppose that

$$Q = \{x_0 + l_1 x_1 + \cdots + l_d x_d : 0 \leqslant l_i < L_i\}$$

and that

$$Y = \{y_1, \dots, y_m\}.$$

Then

$$\begin{aligned}(Q - Q) + Y &\subset \{\tilde{x}_0 + l_1 x_1 + \cdots + l_d x_d + l'_1 y_1 + \cdots + l'_m y_m, 0 \leqslant l_i < 2L_i, 0 \leqslant l'_j < 2\} \\ &= \tilde{Q}\end{aligned}$$

where

$$\tilde{x}_0 = -(L_1 x_1 + \cdots + L_d x_d).$$

Note that $\tilde{Q}$ is a generalised progression of dimension $d + m$ and that

$$\text{size}(\tilde{Q}) = 2^{d+m} L_1 \cdots L_d = 2^{d+m}|Q| \leqslant 2^{d+m}|2A - 2A| \ll_K |A|,$$

the penultimate step following since $Q \subset 2A - 2A$.

The dominant term in the bound is 2^m, which is double exponential in K. $\square$

CHAPTER 6

Additive energy and Balog–Szemerédi-Gowers

In this chapter we introduce the concept of additive energy, which is closely related to the notion of sumset and arises naturally in applications (such as in Chapter 9).

6.1. Introduction

We have already seen the notion of an additive set having small doubling. The next definition introduces some notation for this, and also introduces a kind of bipartite variant of the concept which applies to pairs of sets.

Definition 6.1.1. Let A be an additive set. Then we define the *doubling constant*

$$\sigma[A] := \frac{|A+A|}{|A|}.$$

If A, B are two additive sets, we write

$$\sigma[A,B] := \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}.$$

Remark. This notation should not be confused with the notion of Schnirel'man density, which is of course something quite different.

Note that $\sigma[A] = \sigma[A,A]$, so one may think of the former as a shorthand for the latter.

The notion of a set having small doubling is somehow "combinatorial" in that it refers to the *size* of $|A+A|$ and does not take account, for example, of the number of representations. The notion has some serious shortcomings, for example being highly sensitive to small changes to A.

In this chapter we explore the related notion of additive energy, which is more "analytic", more robust to small perturbations, and often arises in nature.

Definition 6.1.2. Let A be an additive set. Then we define the *additive energy* $E(A)$ to be the number of *additive quadruples* in A, that is to say quadruples $(a_1,a_2,a_3,a_4) \in A^4$ such that $a_1+a_2 = a_3+a_4$. We define the normalised additive energy $\omega[A]$ to be $E(A)/|A|^3$. More generally if A, B are two additive sets, we write

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

and

$$\omega[A,B] := |A|^{-3/2}|B|^{-3/2}E(A,B).$$

Note that $0 \leqslant \omega(A) \leqslant 1$: the upper bound here follows from the fact that three elements of an additive quadruple uniquely determine the fourth. More generally, $0 \leqslant \omega[A,B] \leqslant 1$. This follows from the fact that $E(A,B) \geqslant \max(|A|^2|B|, |A||B|^2)$, since any three elements of a quadruple (a,b,a',b') satisfying $a+b = a'+b'$ determine the fourth. However, $\max(|A|^2|B|, |A||B|^2) \geqslant |A|^{3/2}|B|^{3/2}$.

6.2. Basic properties. Statement of Balog-Szemerédi-Gowers

PROPOSITION 6.2.1. *We have $\sigma[A,B]\omega[A,B] \geqslant 1$. In particular, if the doubling constant of a pair A, B of additive sets is at most K, their normalised additive energy is at least $1/K$. In particular, specialising to the case $A = B$, we have $\sigma[A]\omega[A] \geqslant 1$.*

Proof. For $x \in A+B$ write $r(x)$ for the number of pairs $(a,b) \in A \times B$ with $a+b = x$. Then

$$\sum r(x) = |A||B|,$$

whilst

$$\sum r(x)^2 = E(A,B).$$

Moreover, $r(x)$ is supported (that is, is nonzero) on $A+B$. Thus by Cauchy-Schwartz

$$|A|^2|B|^2 = \big(\sum_x r(x)\big)^2 \leqslant |A+B| \sum_x r(x)^2 = |A+B|E(A,B),$$

which rearranges to give the stated inequality. □

The converse to this kind of statement fails dramatically, as the following shows.

Example. Let n be a large even number. Let $A_1 = \{1, \dots, n/2\}$ and let A_2 be some arbitrary set of $n/2$ integers having no additive relation with A_1, for instance $A_2 = \{10^n, 10^{2n}, \dots, 10^{n^2/2}\}$. Set $A = A_1 \cup A_2$, a set of size n. Then

$$E(A) \geqslant E(A_1) \geqslant \frac{1}{10}n^3,$$

but

$$|A+A| \geqslant |A_2+A_2| \geqslant \frac{1}{8}n^2,$$

since the sums of pairs in A_2 are distinct apart from the relations $x+y = y+x$. Thus $\omega[A] \geqslant \frac{1}{10}$, but $\sigma[A]$ grows linearly in n.

The Balog-Szemerédi-Gowers theorem is a remarkable result which nonetheless salvages a kind of partial converse to Lemma 6.2.1. We state a bipartitie and a

single set version of the result. Recall that by convention C is an absolute constant which can change from line to line (but could be written in explicitly wherever it occurs, if desired, with a bit of work).

THEOREM 6.2.1 (Balog-Szemerédi-Gowers). *We have the following statements.*

(i) *Suppose that A, B are additive sets and that $\omega[A,B] \geqslant 1/K$. Then there are sets $A' \subseteq A$, $B' \subseteq B$ with $|A'| \geqslant K^{-C}|A|$, $|B'| \geqslant K^{-C}|B|$ such that $\sigma[A',B'] \ll K^C$.*

(ii) *Suppose that A is an additive set and that $\omega[A] \geqslant 1/K$. Then there is a set $A' \subset A$ with $|A'| \gg K^{-C}|A|$ such that $\sigma[A'] \ll K^C$.*

The value of C we obtain is quite reasonable in principle, but we will not be too concerned with computing an exact value.

The remainder of the chapter is devoted to the proof of Theorem 6.2.1.

6.3. *Paths of length 2

The proof of the Balog-Szemerédi-Gowers theorem proceeds via the language of graph theory, establishing two lemmas of interest in their own right. The first, concerning paths of length 2, has the cleverer proof.

LEMMA 6.3.1. *Suppose that G is a bipartite graph on vertex set $V \cup W$, where $|V| = |W| = n$, and with αn^2 edges all of which join a vertex in V to one in W. Let $\eta > 0$ be a further parameter. Then there is a subset $V' \subseteq V$ with $|V'| \geqslant \alpha n/2$ such that between $(1-\eta)|V'|^2$ of the ordered pairs of points $(v_1, v_2) \in V' \times V'$ there are at least $\eta\alpha^2 n/2$ paths of length 2.*

Proof. If $x \in G$, write $N(x)$ for the neighbourhood of x in G, or in other words the set of vertices in G which are joined to x by an edge. Note that, since G is bipartite, $N(v) \subseteq W$ whenever $v \in V$ and $N(w) \subseteq V$ whenever $w \in W$.

Now by a double-counting argument, we have

$$\sum_{w \in W} \sum_{v \in V} 1_{vw \in E(G)} = \alpha n^2,$$

where $E(G)$ is of course the set of edges of G. Applying Cauchy-Schwarz to this gives

$$\sum_{w \in W} \sum_{v,v' \in V} 1_{vw \in E(G)} 1_{v'w \in E(G)} \geqslant \alpha^2 n^3,$$

or in other words

$$\mathbb{E}_{v,v' \in V} |N(v) \cap N(v')| \geqslant \alpha^2 n. \tag{6.1}$$

This constitutes the rather basic observation that, on average, pairs (v, v') have many common neighbours. Now say that two vertices v and v' are *extremely unfriendly* if $|N(v) \cap N(v')| < \eta\alpha^2 n/2$, or in other words if there are fewer than $\eta\alpha^2 n/2$

paths of length two between v and v'. Write $S \subseteq V \times V$ for the set of extremely unfriendly pairs. Manifestly, from (6.1), we have

$$\mathbb{E}_{v,v' \in V}(\eta - 1_{(v,v') \in S})|N(v) \cap N(v')| \geqslant \eta\alpha^2 n/2.$$

This may be rewritten as

$$\mathbb{E}_{v,v' \in V}(\eta - 1_{(v,v') \in S}) \sum_{w \in W} 1_{vw \in E(G)} 1_{v'w \in E(G)} \geqslant \eta\alpha^2 n/2.$$

Turning the sum over W into an expectation (by dividing by $|W| = n$) and swapping the order of summation, this implies that

$$\mathbb{E}_{w \in W}\mathbb{E}_{v,v' \in V}(\eta - 1_{(v,v') \in S}) 1_{v,v' \in N(w)} \geqslant \eta\alpha^2/2.$$

In particular there is a choice of w such that

$$\mathbb{E}_{v,v' \in V}(\eta - 1_{(v,v') \in S}) 1_{v,v' \in N(w)} \geqslant \eta\alpha^2/2.$$

Simply the fact that this expectation is greater than zero tells us that at most a proportion η of the pairs $v, v' \in N(w)$ are extremely unfriendly. Furthermore (ignoring the term involving S completely) we have

$$\mathbb{E}_{v,v' \in V} 1_{v,v' \in N(w)} \geqslant \alpha^2/2,$$

which implies that $|N(w)| \geqslant \alpha/\sqrt{2}$. Taking $V' := N(w)$, this proves the result. □

Remarks. This proof looks extremely slick at first sight. However when faced with the task of proving Lemma 6.3.1 it is not hard to develop the feeling that one must somehow select a very "connected" subset of V. The way we have done this is essentially by picking a random vertex $w \in W$, and taking V' to be the neighbourhood $N(w)$ of w in V, though this was easier to manage by using expectations rather than starting with "pick $w \in W$ uniformly at random and consider $N(w)$". This kind of technique seems to have been pioneered in this context by Gowers, and it is called "dependent random selection": one chooses something random (w in this case), then makes a deterministic choice based on it ($N(w)$).

6.4. *Paths of length 3

LEMMA 6.4.1. *Suppose that G is a bipartite graph on vertex set $V \cup W$, where $|V| = |W| = n$, and with αn^2 edges all of which join a vertex in V to one in W. Then there are subsets $V' \subseteq V$ and $W' \subseteq W$ with $|V'|, |W'| \geqslant c\alpha^C n$ such that between every pair $v' \in V'$ and $w' \in W'$ there are at least $c\alpha^C n^2$ paths of length 3 in G.*

Proof. Delete all edges emanating from vertices in V with degree less than $\alpha n/2$; this causes the deletion of at most $\alpha n^2/2$ edges in total, so at least $\alpha n^2/2$ remain.

From now on if we speak of an *edge* we mean one of these edges. Let $\eta > 0$ be a parameter to be chosen later. Using the preceding lemma, we may select a set $V' \subseteq V$ with $|V'| \geqslant \alpha n/4$ such that a proportion $1-\eta$ of the pairs of vertices in V' have at least $\eta\alpha^2 n/8$ common neighbours in W.

All vertices in V' have degree 0 or else degree at least $\alpha n/2$, but it is conceivably the case that some do have degree 0. However if $\eta < 1/4$ then clearly no more than half of them do. Thus we may pass to a set $V'' \subseteq V'$, $|V''| \geqslant \alpha n/8$, such that every vertex in V'' has degree at least $\alpha n/2$ and still such that a proportion $1-\eta$ of the pairs of vertices in V'' have at least $\eta\alpha^2 n/8$ common neighbours in W.

Now let us focus on W. Look at all the edges from V'' into W: since each vertex in V'' has degree at least $\alpha n/2$, and $|V''| \geqslant \alpha n/8$, there are at least $\alpha^2 n^2/16$ of these. It follows that there is some set $W' \subseteq W$, $|W'| \geqslant \alpha^2 n/32$, such that each $w \in W'$ has at least $\alpha^2 n/32$ neighbours in V''.

Before concluding, let us jump back over to the other side and effect one final refinement of V''. Say that a vertex $v \in V''$ is *sociable* if there is a proportion at least $1-2\eta$ of the other vertices $v' \in V''$ are such that v and v' have at least $\eta\alpha^2 n/8$ common neighbours. Then at least half the vertices of V'' are sociable: call this set V''', so that $|V'''| \geqslant \alpha n/16$.

We now claim that for any $x \in V'''$ and $y \in W'$ there are many paths of length three between x and y (in the original graph G). Indeed by the choice of W' there must be at least $\alpha^2 n/32$ elements of V'' adjacent to y. There must also be at least $(1-2\eta)|V''|$ vertices of V'' which have at least $\eta\alpha^2 n/8$ common neighbours with x. Provided that $\alpha^2 n/32 \geqslant 3\eta|V''|$, which will be the case if $\eta \leqslant \alpha^2/96$, these two sets intersect in a set $\tilde{V} \subseteq V''$ of size at least $\eta|V''|$. Thus each element z of $\tilde{V}$ is adjacent to y, and has $\eta\alpha^2 n/8$ common neighbours with x. This clearly leads to at least $\eta^2\alpha^2|V''|n/8$ paths of length three between x and y.

The only constraints on η were that $\eta \leqslant 1/4$ and that $\eta \leqslant \alpha^2/96$. The latter is clearly the more severe constraint, so set $\eta := \alpha^2/96$. The lemma is proven. □

6.5. Proof of Balog-Szemerédi-Gowers

In this section we deduce Theorem 6.2.1 from the paths of length 3 lemma, Lemma 6.4.1. It is particularly important to remember during this proof that the constant C may change from line to line.

Proof. [Proof of Theorem 6.2.1] For the majority of the proof we handle the two-sets case (i) and the one-set case (ii) at the same time, taking $A = B$ in the latter case.

Suppose then that A, B are two sets in some abelian group G and that $\omega[A,B] \geqslant 1/K$. This means that there are at least $|A|^{3/2}|B|^{3/2}/K$ solutions to $a_1 - b_1 =$

$a_2 - b_2$. Note that the number of solutions to this equation is at most $|A|^2|B|$, since once a_1, b_1 and a_2 are specified b_2 is uniquely determined. Therefore $|B| \leqslant K^2|A|$, and similarly $|A| \leqslant K^2|B|$.

Write $s(x)$ for the number of pairs $(a, b) \in A \times B$ with $a - b = x$. Thus we have

$$\sum_x s(x)^2 \geqslant |A|^{3/2}|B|^{3/2}/K,$$

whilst by double-counting pairs $(a, b) \in A \times B$ we have

$$\sum_x s(x) = |A||B|.$$

We claim there are at least $|A|^{1/2}|B|^{1/2}/2K$ "popular" values of x for which $s(x) \geqslant |A|^{1/2}|B|^{1/2}/2K$. To see this, let Δ denote the set of these popular x. Then

$$\sum_{x \notin \Delta} s(x)^2 \leqslant \frac{1}{2K}|A|^{1/2}|B|^{1/2} \sum_x s(x) = |A|^{3/2}|B|^{3/2}/2K,$$

so

$$\sum_{x \in \Delta} s(x)^2 \geqslant |A|^{3/2}|B|^{3/2}/2K.$$

However, since $s(x) \leqslant \min(|A|, |B|) \leqslant |A|^{1/2}|B|^{1/2}$ for every x,

$$\sum_{x \in \Delta} s(x)^2 \leqslant |\Delta||A||B|.$$

The claim follows.

Note also, for use below, that

$$|\Delta| \leqslant 2K|A|^{1/2}|B|^{1/2}, \tag{6.2}$$

a bound which follows straightforwardly by double-counting pairs $(a, b) \in A \times B$.

Define a bipartite graph G on vertex set $A \cup B$ by joining $a \in A$ to $b \in B$ by an edge if $a - b$ is a popular difference in the above sense, that is to say if and only if $a - b \in \Delta$. Then G has at least $|A||B|/4K^2$ edges. Let $n = \max(|A|, |B|)$, and "pad out" the smaller vertex class of G to obtain a new graph having n vertices in each class. Recalling that $K^{-2} \leqslant |A|/|B| \leqslant K^2$, this graph has at least $n^2/4K^4$ edges.

Applying Lemma 6.4.1, we may locate sets $A' \subseteq A$ and $B' \subseteq B$ with $|A'| \gg K^{-C}|A|$, $|B'| \gg K^{-C}|B|$ and such that for every $a' \in A'$ and $b' \in B'$ there are $\gg K^{-C}n^2$ paths of length 3 in G between a' and b'. This, of course, means that there $\gg K^{-C}n^2$ choices of $a'' \in A$ and $b'' \in B$ such that all three of $a' - b''$, $a'' - b''$ and $a'' - b'$ lie in Δ.

Noting that $a' - b' = (a' - b'') - (a'' - b'') + (a'' - b')$, it follows that for all $a' \in A'$ and $b' \in B'$ the difference $a' - b'$ can be written in $\gg K^{-C}n^2$ ways as $x - y + z$, where $x, y, z \in \Delta$. These are genuinely distinct representations, since it is easy to recover a'' and b'' from knowledge of a', b', x, y and z. However, by (6.2),

the number of popular differences is bounded *above* by $2K|A|^{1/2}|B|^{1/2} \ll Kn$. It follows that

$$|A' - B'| \cdot K^{-C}n^2 \ll (Kn)^3,$$

which of course implies that

$$|A' - B'| \ll K^C n. \tag{6.3}$$

To finish the argument, we consider parts (i) and (ii) of Theorem 6.2.1 separately.

In case (i), applying (**??**) together with the lower bounds $|A'|, |B'| \geqslant K^{-2}n$ gives the desired upper bound $|A' + B'| \ll K^C n \ll K^C |A'|^{1/2}|B'|^{1/2}$.

In case (ii), we first apply the Ruzsa triangle inequality with $U = B'$, $V = W = A'$ to conclude from (6.3) that $|A' - A'| \ll K^C n$. From this, it follows that $|A' + A'| \ll K^C n$, using (**??**) again.

□

CHAPTER 7

Combinatorial geometry and sum-product

Let A be a set of n integers. We have already discussed the sumset $A + A$ at some length. We may also introduce the product set $A \cdot A := \{aa' : a, a' \in A\}$. A famous conjecture of Erdős and Szemerédi is that

$$|A + A| + |A \cdot A| \geqslant n^{2-o(1)}.$$

This is far from being proven, but the final result of this chapter is the non-trivial result

$$|A + A| + |A \cdot A| \gg n^{5/4},$$

which is due to Elekes. The main input in establishing this is the so-called Szemerédi-Trotter theorem, a result in combinatorial geometry of substantial independent interest.

THEOREM 7.0.1 (Szemerédi-Trotter). *Let $r \geqslant 2$. Let L be a set of m lines. Then the number of points which lie on at least r lines in L is $O(\frac{m}{r} + \frac{m^2}{r^3})$.*

There are various slightly different ways to state this theorem, a matter we discuss on the example sheets. The proof we shall give of this uses a lemma about crossing numbers which is also of independent interest.

7.1. Crossing number inequality

This section assumes that you are familiar with the basic language of graph theory; if not, it should be easy to read up on the relevant definitions.

DEFINITION 7.1.1. A *drawing* of a graph G is a representation of G in the plane $\mathbf{R}^2$ where the vertices of G are points and the edges are "nice" simple curves between pairs of vertices, not passing through any other vertex of the graph. A *crossing* is an intersection of two edge-curves, other than at a vertex. The *crossing number* $\mathrm{cr}(G)$ of a graph G is the least number of crossings in any drawing of G in the plane. A graph is said to be *planar* if $\mathrm{cr}(G) = 0$.

Remark. We will not bother to set up what "nice" means rigorously, and it does not really matter; for example, we could take the curves to be polygonal. Note also that crossings are counted as pairs of edge-curves which intersect, not as the actual

points of intersection. Thus, for example, three edge-curves all intersecting at the same point counts as three crossings.

We begin by recalling *Euler's formula*. If G is a connected planar graph then

$$V - E + F = 2, \tag{7.1}$$

where V, E, F denote the numbers of vertices, edges and faces respectively. Now if $V \geqslant 3$ then every face has at least three edges, and no edge belongs to more than two faces. Therefore, double counting edges,

$$3F \leqslant 2E.$$

Substituting into Euler's formula (7.1) gives $E - 3V \leqslant -6$. Considering the cases where $V = 1$ or 2, one sees that certainly

$$E \leqslant 3V \tag{7.2}$$

in all cases. By splitting into connected components, we see that (7.2) holds for all planar graphs, connected or not.

Remark. Formalising the details here (even defining exactly what is meant by a face, especially in degenerate cases such as when G is a tree) is slightly subtle and not the domain of this course. For a much fuller discussion, see the graph theory course.

If we have a graph G then consider a drawing of G with $\mathrm{cr}(G)$ crossings. For each such crossing, remove one of the edges in it. Continuing in this fashion gives a planar graph G' with the same vertex set as G and with $E' \geqslant E - \mathrm{cr}(G)$ edges. It follows from (7.2) that $E' \leqslant 3V$ and so

$$\mathrm{cr}(G) \geqslant E - 3V. \tag{7.3}$$

It turns out that by a random sampling trick we can bootstrap this to the following inequality, which is much stronger when E is relatively large in terms of V.

PROPOSITION 7.1.1. *Suppose that $E \geqslant 4V$. Then $\mathrm{cr}(G) \geqslant \frac{E^3}{64V^2}$.*

Proof. Take a drawing of G with the minimal number $\mathrm{cr}(G)$ of crossings. Then all crossings involve four distinct vertices: if there is some crossing involving edges vx, vy then there is an easy procedure to reduce the number of crossings, best described by a picture (see Figure 7.1).

Let p, $0 \leqslant p \leqslant 1$, be a parameter to be specified later. Consider a random subgraph $\mathbf{G}'$ of G, formed by picking a random set $\mathbf{S}$ of vertices by selecting each v in the vertex set of G to lie in $\mathbf{S}$ independently at random with probability p,

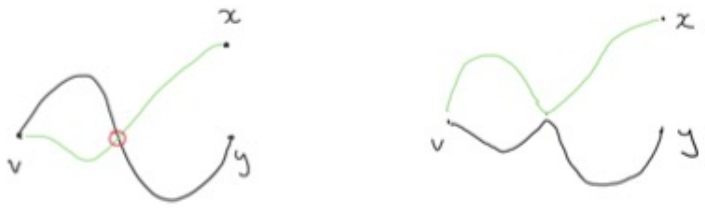

FIGURE 1. Removing a crossing

and then taking $\mathbf{G}'$ to be the subgraph of G induced by $\mathbf{S}$: that is, include all the edges in G between two vertices in $\mathbf{S}$. Let the number of vertices and edges in $\mathbf{G}'$ be $\mathbf{V}'$, $\mathbf{E}'$ respectively; these are of course random variables. Also, let $\tilde{\mathrm{cr}}(\mathbf{G}')$ be the number of crossings in $\mathbf{G}'$ in the drawing we have, that is to say in the drawing induced from that on G. Note that $\tilde{\mathrm{cr}}(\mathbf{G}') \geqslant \mathrm{cr}(\mathbf{G}')$, but we do not necessarily have equality since there might be a different drawing of $\mathbf{G}'$ with fewer crossings.

For each instance of this random selection we have the inequality (7.3), that is to say

$$\mathrm{cr}(\mathbf{G}') \geqslant \mathbf{E}' - 3\mathbf{V}'.$$

Certainly, then

$$\tilde{\mathrm{cr}}(\mathbf{G}') \geqslant \mathbf{E}' - 3\mathbf{V}'.$$

We may take expectations of the three random variables appearing here and deduce, using linearity of expectation, that

$$\mathbb{E}\tilde{\mathrm{cr}}(\mathbf{G}') \geqslant \mathbb{E}\mathbf{E}' - 3\mathbb{E}\mathbf{V}'. \tag{7.4}$$

However, it is easy to see that

$$\mathbb{E}\mathbf{V}' = pV \qquad \text{and} \qquad \mathbb{E}\mathbf{E}' = p^2 E$$

(since, for each edge in G, both endpoint vertices must be selected in order for it to be an edge in $\mathbf{G}'$), and

$$\mathbb{E}\tilde{\mathrm{cr}}(\mathbf{G}') = p^4\,\mathrm{cr}(G)$$

(since, for each crossing in G, all four endpoint vertices of the two edges involved must be selected in order for it to be a crossing in $\mathbf{G}'$).

Substituting into (7.4) gives

$$p^4 \operatorname{cr}(G) \geqslant p^2 E - 3pV.$$

We are free to choose any parameter $p \in [0,1]$ that we like. Choosing $p = 4V/E$ (noting that, by the hypothesis, $p \leqslant 1$) gives the desired bound after rearranging the terms. □

7.2. The Szemerédi-Trotter theorem

In this section we prove Theorem 7.0.1.

Proof. [Proof of Theorem 7.0.1] First of all, note that Theorem 7.0.1 is trivial if $r \leqslant 7$ (say) since there are at most $\binom{m}{2}$ points lying on two or more lines.

Suppose henceforth that $r \geqslant 8$. Draw a graph G as follows. The vertices of G are the points P lying on at least r lines in L. Two vertices x, y are joined by an edge if and only if x, y are *consecutive* points *of* P on the same line in L. Denote by $n = |P|$ the number of vertices in this graph; this is the quantity we wish to bound.

Now observe that G comes with a natural drawing, that is to say the one induced by the lines in L; in this drawing, every edge is in fact represented by a straight line segment. Since two lines intersect in at most one point, the number of crossings in this drawing is at most $\binom{m}{2}$. Therefore

$$\operatorname{cr}(G) \leqslant \binom{m}{2} < m^2. \tag{7.5}$$

The number of edges E is at least $rn - m$. To see why, count the number of edges starting at v. Usually, v is adjacent to at least $2r$ other vertices. The exception is when v is one of the two endmost points (in either direction) on one of the lines in L, in which case we lose one adjacency. Summing over v gives at least $2rn - 2m$ pairs (v, w) with vw an edge, which of course double-counts the number of edges.

Now consider Proposition 7.1.1. Either we are in a position to apply this proposition, or we are not. If not, then $E < 4n$, so $rn - m < 4n$. Since $r \geqslant 8$, this implies that $rn/2 \leqslant m$, and so Theorem 7.0.1 holds in this case. Otherwise, $E \geqslant 4n$ and we may apply Proposition 7.1.1. This gives

$$m^2 \geqslant \frac{(rn-m)^3}{64n^2}. \tag{7.6}$$

If $n \leqslant 2m/r$ then again Theorem 7.0.1 holds. Otherwise, $rn - m \geqslant rn/2$ and so (7.6) becomes

$$m^2 \geqslant \frac{(rn/2)^3}{64n^2},$$

which immediately rearranges to $n \ll m^2/r^3$, and once again Theorem 7.0.1 holds. This concludes the proof. □

7.3. Sum-product

In this section we give Elekes's bound for the sum-product problem.

THEOREM 7.3.1. *Suppose that $A \subset \mathbf{R}$ is a finite set of size n. Then $|A+A||A \cdot A| \gg n^{5/2}$. In particular, at least one of $A+A, A \cdot A$ has cardinality $\gg n^{5/4}$.*

Proof. It clearly suffices to handle the case $0 \notin A$ (otherwise remove 0 and apply the bound to the resulting set). Consider the set of points

$$P := \{(\frac{1}{a'}, -\frac{1}{aa'}) : a, a' \in A\},$$

and the set of lines

$$L := \{\{(x,y) \in \mathbf{R}^2 : ux + vy = 1\} : u \in A+A, v \in A \cdot A\}.$$

Observe that $|P| = n^2$, whilst the number $m = |L|$ of lines is $|A+A||A \cdot A|$.

The crucial observation is now that every point of P lies on at least n of these lines. Indeed, the point $(\frac{1}{a'}, -\frac{1}{aa'})$ lies on the line $ux + vy = 1$ when $u = a' + t$ and $v = at$, for every $t \in A$.

It follows from Szemerédi-Trotter that

$$n^2 \ll \frac{m}{n} + \frac{m^2}{n^3},$$

which implies that $m \gg n^{5/2}$. This is the desired result. □

CHAPTER 8

Some further results about set addition

In this chapter we gather together some further inequalities about sumsets and set addition. Several of these are interesting in their own right, but the overriding aim of the chapter is to assemble ingredients for the proof of a sum-product theorem of Bourgain and Chang in the next chapter.

8.1. The Prékopa-Leindler inequality on the line

We begin with a simple sumset inequality for measurable subsets of $\mathbf{R}$, a kind of continuous analogue of the observation at the start of Chapter 5. Throughout this section, μ denotes Lebesgue measure.

LEMMA 8.1.1. *Suppose that $X, Y, Z \subset \mathbf{R}$ are non-empty measurable sets with $X + Y \subset Z$. Then $\mu(Z) \geqslant \mu(X) + \mu(Y)$.*

Proof. For any $\varepsilon > 0$, there are compact subsets $X' \subset X$ and $Y \subset Y'$ such that $\mu(X') \geqslant \mu(X) - \varepsilon$ and $\mu(Y') \geqslant \mu(Y) - \varepsilon$. (This property is the fact that Lebesgue measure is *inner regular*; however, for our discrete applications we will only apply Lemma 8.1.1 in cases where this is clear by inspection.)

Let $x := \inf X'$ and $y := \sup Y'$. Since X', Y' are compact, $x \in X'$ and $y \in Y'$, and therefore the two sets $x + Y'$ and $X' + y$ both lie in Z. Note that every element of $x + Y'$ is at most $x + y$, whilst every element of $X' + y$ is at least $x + y$. Therefore $(x + Y') \cap (X' + y)$ is the singleton $\{x + y\}$, which of course has measure zero, so

$$\begin{aligned} \mu(Z) \geqslant \mu((X' + y) \cup (x + Y')) &= \mu(X' + y) + \mu(x + Y') \\ &= \mu(X') + \mu(Y') \\ &\geqslant \mu(X) + \mu(Y) - 2\varepsilon. \end{aligned}$$

Letting $\varepsilon \to 0$, the result follows. □

Now we turn to the main topic of this section. Suppose that $f, g : \mathbf{R} \to [0, \infty)$ are compactly supported, piecewise continuous functions. Define the *max-convolution* by

$$f \overline{*} g(x) := \sup_{y \in \mathbf{R}} f(x - y) g(y).$$

The following is a special case of a 1-dimensional version of a special case of the so-called Prékopa-Leindler inequality

PROPOSITION 8.1.1. *Let $f, g : \mathbf{R} \to [0, \infty)$ be compactly supported, piecewise continuous functions. Then we have the inequality*

$$\int f \overline{*} g \geqslant 2\|f\|_2 \|g\|_2, \tag{8.1}$$

where the norms are the usual Lebesgue norms

$$\|f\|_2 := \big(\int_{\mathbf{R}} f^2\big)^{1/2}, \quad \|g\|_2 := \big(\int_{\mathbf{R}} g^2\big)^{1/2}.$$

Proof. Let $\lambda \geqslant 0$. Then if $f(x-y), g(y) \geqslant \sqrt{\lambda}$ then we have $f \overline{*} g(x) \geqslant \lambda$, or in other words

$$\{t : f(t) \geqslant \sqrt{\lambda}\} + \{t : g(t) \geqslant \sqrt{\lambda}\} \subseteq \{t : f \overline{*} g(t) \geqslant \lambda\},$$

or equivalently

$$\{t : f(t)^2 \geqslant \lambda\} + \{t : g(t)^2 \geqslant \lambda\} \subseteq \{t : f \overline{*} g(t) \geqslant \lambda\}.$$

By Lemma 8.1.1 it follows that

$$\mu(\{t : f(t)^2 \geqslant \lambda\}) + \mu(\{t : g(t)^2 \geqslant \lambda\}) \leqslant \mu(\{t : f \overline{*} g(t) \geqslant \lambda\}), \tag{8.2}$$

where μ is Lebesgue measure.

Now by Fubini's theorem, for any measurable $F : \mathbf{R} \to [0, \infty)$ we have the "layer-cake" decomposition

$$\int_0^\infty \mu(\{x : F(x) \geqslant \lambda\}) d\lambda = \int_{\mathbf{R}} F(x) dx.$$

Applying this to (8.2) gives

$$\|f\|_2^2 + \|g\|_2^2 \leqslant \int_{\mathbf{R}} f \overline{*} g. \tag{8.3}$$

The desired inequality (8.1) follows immediately from this and the elementary inequality $a^2 + b^2 \geqslant 2ab$, applied of course with $a = \|f\|_2$ and $b = \|g\|_2$. □

Remark. The last step appears wastful, and one might wonder why we did not simply state the stronger inequality (8.3). The answer is that the form stated in (8.1) is much more useful for applications.

8.2. A weighted discrete Prékopa–Leindler inequality

We now turn to discrete results. The main aim of this section is to establish Proposition 8.2.1 below, which is a weighted discrete Prékopa–Leindler inequality. The statement has clear analogies with that of Proposition 8.1.1.

Let $a, b : \mathbf{Z} \to [0, \infty)$ be compactly supported functions. We define the *max-convolution*

$$a \overline{*} b(n) := \sup_{m \in \mathbf{Z}} a(n-m)b(m).$$

PROPOSITION 8.2.1. *Let $a, b : \mathbf{Z} \to [0, \infty)$ be compactly supported functions and let $p \in [0, 1]$. Then we have*

$$\sum_n \max(pa\overline{*}b(n), (1-p)a\overline{*}b(n-1)) \geqslant \|a\|_2 \|b\|_2.$$

Now, the norms are the discrete ℓ^2 norms given by

$$\|a\|_2 := \big(\sum_n a(n)^2\big)^{1/2}, \quad \|b\|_2 := \big(\sum_n b(n)^2\big)^{1/2}.$$

Proof. In this proof, we will use the notations $\overline{*}$ and $\|\cdot\|_2$ on both $\mathbf{R}$ (with definitions as in the previous section) and on $\mathbf{Z}$ (with definitions as above). It should hopefully be clear what the domain of definition of the functions we are working with at any given point are.

By continuity we may assume that $p \in (0, 1)$. Set $\lambda := \log(\frac{1}{p} - 1)$. Apply Proposition 8.1 with functions f, g defined by

$$f(x) := e^{\lambda\{x\}} a(\lfloor x \rfloor), \quad g(y) := e^{\lambda\{y\}} b(\lfloor y \rfloor).$$

Let $n \in \mathbf{Z}$ and $0 \leqslant t < 1$. Suppose that $x+y = n+t$. Then, since $x-1 < \lfloor x \rfloor \leqslant x$, we have $n - 2 < \lfloor x \rfloor + \lfloor y \rfloor < n + 1$, or in other words $\lfloor x \rfloor + \lfloor y \rfloor = n - 1$ or n. If $\lfloor x \rfloor + \lfloor y \rfloor = n - 1$ then

$$f(x)g(y) \leqslant e^{\lambda(t+1)} a\overline{*}b(n-1),$$

whilst if $\lfloor x \rfloor + \lfloor y \rfloor = n$ then

$$f(x)g(y) \leqslant e^{\lambda t} a\overline{*}b(n).$$

Therefore

$$f\overline{*}g(n+t) \leqslant e^{\lambda t} \max(a\overline{*}b(n), e^{\lambda} a\overline{*}b(n-1)).$$

Integrating over $t \in [0, 1)$ and then summing over $n \in \mathbf{Z}$ yields

$$\int_{\mathbf{R}} f\overline{*}g \leqslant \frac{e^{\lambda} - 1}{\lambda} \sum_n \max(a\overline{*}b(n), e^{\lambda} a\overline{*}b(n-1)). \tag{8.4}$$

On the other hand,

$$\|f\|_2^2 = \frac{e^{2\lambda} - 1}{2\lambda} \|a\|_2^2, \quad \|g\|_2^2 = \frac{e^{2\lambda} - 1}{2\lambda} \|b\|_2^2.$$

Substituting into Proposition 8.1 gives

$$\sum_n \max(a\overline{*}b(n), e^{\lambda} a\overline{*}b(n-1)) \geqslant (e^{\lambda} + 1)\|a\|_2 \|b\|_2.$$

Recalling the choice of λ (thus $p = \frac{1}{e^\lambda+1}$), the proposition follows. □

8.3. Quasicubes, binary sets and sumsets

Quasicubes. The notion of a quasicube $\Sigma \subseteq \mathbf{Z}^d$ is defined inductively. When $d = 1$, a quasicube is simply a set of size two. For larger d, Σ is a quasicube if

(i) $\pi(\Sigma) = \{x_0, x_1\}$ is a set of size two, where $\pi : \mathbf{Z}^d \to \mathbf{Z}$ is the coordinate projection onto the final coordinate, and
(ii) The fibre $\Sigma_i := \Sigma \cap \pi^{-1}(x_i)$ (considered as a subset of $\mathbf{Z}^{d-1}$) is a quasicube.

Thus, for instance, the usual cube $\{0,1\}^d$ is a quasicube. Another example of a quasicube with $d = 2$ is the set $\Sigma = \{(0,0),(1,0),(0,1),(1,2)\}$.

Binary sets. A subset of a quasicube is called a *binary set* (we caution that this is not a standard term in the literature).

THEOREM 8.3.1. *Let $A, B \subseteq \mathbf{Z}^d$ be finite sets and suppose that $U \subseteq \mathbf{Z}^d$ is a binary set. Then $|A+B+U| \geqslant |A|^{1/2}|B|^{1/2}|U|$.*

Proof. We proceed by induction on d. The proof of the inductive step also proves the base case $d = 1$.

Suppose that U is contained in a quasicube $\Sigma \subset \mathbf{Z}^d$. Suppose that $\pi(\Sigma) = \{x_0, x_1\}$, where $\pi : \mathbf{Z}^d \to \mathbf{Z}$ is projection onto the last coordinate. Since the inequality is translation-invariant, we may assume that $x_0 = 0$ and $x_1 = q > 0$. Suppose first that $q = 1$.

Let $A_i := A \cap \pi^{-1}(n)$ be the fibre of A above n, and similarly for B. The set U has just two fibres U_0, U_1 and, by the definition of quasicubes, they are both contained in quasicubes of dimension $d-1$.

Observe that the fibre of $A+B+U$ above n contains $A_x + B_y + U_0$ whenever $x+y = n$, and $A_x + B_y + U_1$ whenever $x + y = n-1$. By induction,

$$|A_x + B_y + U_0| \geqslant |A_x|^{1/2}|B_y|^{1/2}|U_0|,$$

$$|A_x + B_y + U_1| \geqslant |A_x|^{1/2}|B_y|^{1/2}|U_1|,$$

and so the fibre $(A+B+U)_n$ of $A+B+U$ above n has size at least

$$\max\big(|U_0| \max_{x+y=n} |A_x|^{1/2}|B_y|^{1/2}, |U_1| \max_{x+y=n-1} |A_x|^{1/2}|B_y|^{1/2}\big).$$

This is equal to

$$|U| \max\big(pa\bar{*}b(n) + (1-p)a\bar{*}b(n-1)\big),$$

where $p := |U_0|/|U|$, $a(x) := |A_x|^{1/2}$ and $b(y) := |B_y|^{1/2}$. Summing over n and applying Proposition 8.2.1 we obtain

$$\begin{aligned}|A+B+U| &= \sum_n |(A+B+U)_n| \\ &\geqslant |U| \sum_n \max\big(pa\overline{*}b(n) + (1-p)a\overline{*}b(n-1)\big) \\ &\geqslant |U|\|a\|_2\|b\|_2 = |U||A|^{1/2}|B|^{1/2}.\end{aligned}$$

This proves the result when $q = 1$. Suppose now that q is arbitrary, and foliate $A = \bigcup_{r\in\mathbf{Z}/q\mathbf{Z}} A_r$, $B = \bigcup_{s\in\mathbf{Z}/q\mathbf{Z}} B_s$, where $A_r := \{a \in A : \pi(a) \equiv r (\mathrm{mod}\, q)\}$ and similarly for B_s. Let r_* be such that $|A_r| \leqslant |A_{r_*}|$ for all r, and s_* be such that $|B_s| \leqslant |B_{s_*}|$ for all s.

The sets $A_{r_*} + B_s + U$ are disjoint as s varies, and so by the case $q = 1$ (rescaled) we have

$$|A+B+U| \geqslant \sum_s |A_{r_*} + B_s + U| \geqslant |U||A_{r_*}|^{1/2} \sum_s |B_s|^{1/2}. \tag{8.5}$$

Similarly,

$$|A+B+U| \geqslant |U||B_{s_*}|^{1/2} \sum_r |A_r|^{1/2}. \tag{8.6}$$

Taking products of (8.5), (8.6) and using

$$|A_{r_*}|^{1/2} \sum_r |A_r|^{1/2} \geqslant \sum_r |A_r| = |A|,$$

$$|B_{s_*}|^{1/2} \sum_s |B_s|^{1/2} \geqslant \sum_s |B_s| = |B|,$$

the result follows. □

8.4. Skew-dimension and the Pálvölgyi–Zhelezov Theorem

For the purposes of this section, an *affine space* is a subspace of $\mathbf{Z}^d$ (for some d) obtained by fixing the values of some possibly empty set of coordinates. Thus, for example, $\{(2,-1,x_3) : x_3 \in \mathbf{Z}\} \subset \mathbf{Z}^3$ is an affine space. If π is one of the d standard coordinate maps on $\mathbf{Z}^d$, and if it restricts to a nontrivial map on V (that is, if its image is $\mathbf{Z}$ rather than a singleton) then we say that π is a coordinate map on V. In the example, there is just one coordinate map, the map $\pi((2,-1,x_3)) = x_3$.

Let A be a finite subset of some affine space. As usual, the doubling constant $\sigma[A]$ is defined to be $\frac{|A+A|}{|A|}$. The *weak*[1] *Polynomial Freiman-Ruzsa conjecture* is the following statement.

CONJECTURE 8.4.1. *Suppose that A is a finite subset of an affine space and that $\sigma[A] \leqslant K$. Then there is a subset $A' \subset A$, $|A'| \geqslant K^{-C}|A|$, with $\dim A' \ll \log K$.*

We will give an argument of Pálvölgyi and Zhelezov which establishes a weak variant of Conjecture 8.4.1, in which the notion of dimension is replaced by a notion which we call the *skew-dimension* $\dim_*$. We define it in the following inductive manner.

DEFINITION 8.4.1 (Skew dimension). Let A be a finite set in some affine space V. If A is a singleton, define $\dim_*(A) = 0$. Otherwise, there is some coordinate map $\pi : V \to \mathbf{Z}$ such that $|\pi(A)| > 1$; for definiteness, take π to correspond to the coordinate with biggest index for which this is so. Then we define $\dim_*(A) := 1 + \max_x \dim_*(\pi^{-1}(x) \cap A)$.

Example. Consider the set $A = \{(1,0,0),(2,0,0),(0,1,1),(0,2,1)\} \subset \mathbf{Z}^3$. The coordinate map π_3 is such that $\pi_3(A) = \{0,1\}$ has size greater than 1. The fibres are then

$$A_0 = \pi_3^{-1}(0) \cap A = \{(1,0,0),(2,0,0)\} \subset V_0 := \{(x,y,0) : x,y \in \mathbf{Z}\}$$

and

$$A_1 = \pi_3^{-1}(1) \cap A = \{(0,1,1),(0,2,1)\} \subset V_1 := \{(x,y,1) : x,y \in \mathbf{Z}\}.$$

We have $\pi_2(A_0) = \{0\}$, which has size 1. However, $\pi_1(A_0) = \{1,2\}$. The fibres are both singletons and so $\dim_*(A_0) = 1$. We have $\pi_2(A_1) = \{1,2\}$, and again the fibres are both singletons. Therefore $\dim_*(A_1) = 1$. We conclude that $\dim_*(A) = 2$.

This example, which has 1-dimensional fibres over a 1-dimensional base (but the fibres are "skew" to one another), should be thought of a typical example of a set of skew-dimension 2. Note that its *true* (vector space) dimension is 3.

Here is the main result.

THEOREM 8.4.1 (Pálvölgyi–Zhelezov). *Let A be a set in some affine space, and that $\sigma[A] \leqslant K$. Then there is $A' \subset A$, $|A'| \geqslant K^{-3}|A|$, with $\dim_*(A') \leqslant 3\log_2 K$.*

Recall, from the last section, the definition of *binary set*. Let $\mathrm{bin}[A]$ denote the size of the largest binary set in A. This invariant is connected to the doubling

[1]The term "weak" comes from the fact that no attempt is made to place any portion of A efficiently inside a progression. There is a stronger version of the conjecture in which such an attempt is made.

constant of A, as the following result of Matolcsi, Ruzsa, Shakan and Zhelezov shows.

PROPOSITION 8.4.1. *We have* $\mathrm{bin}[A] \leqslant \sigma[A]^3$.

Proof. Let U be a binary set. It follows from Theorem 8.3.1 that $|A+A+U| \geqslant |U||A|$. If $U \subseteq A$, $|A+A+U| \leqslant |A+A+A| = |3A|$. It follows that $\mathrm{bin}[A] \leqslant \frac{|3A|}{|A|}$. By the Plünnecke Ruzsa inequality, Theorem 4.4.1, we have $\frac{|3A|}{|A|} \leqslant \sigma[A]^3$. The proposition follows. □

Theorem 8.4.1 is an immediate consequence of Proposition 8.4.1 and the following proposition, which provides a link between binary sets and skew dimension.

PROPOSITION 8.4.2. *Suppose that A is a finite set in some affine space, and that* $\mathrm{bin}[A] = m$. *Then there is a subset $A' \subset A$ with $|A'| \geqslant \frac{1}{m}|A|$ and* $\dim_*(A') \leqslant \log_2 m$.

Proof. We induct on this dimension of the affine space containing A. Let $\pi : V \to \mathbf{Z}$ be the coordinate map corresponding to largest index. If $|\pi(A)| = 1$, say $\pi(A) = \{x\}$, then A lives in the affine space $V' := \pi^{-1}(x) \cap V$, which has $\dim V' < \dim V$. In this case the inductive step is trivial. Suppose, then, that $|\pi(A)| \geqslant 2$. For each $x \in \pi(A)$ write $A_x := \pi^{-1}(x) \cap A$ for the fibre of A above x. Thus $A = \bigcup_x A_x$. Write m_x for the size of the largest binary set in A_x. By the inductive hypothesis, there is $A'_x \subset A_x$, $|A'_x| \geqslant \frac{1}{m_x}|A_x|$, with $\dim_*(A'_x) \leqslant \log_2 m_x$.

We may assume that

$$\frac{1}{m_x}|A_x| \leqslant \frac{1}{m}|A| \tag{8.7}$$

for all x, or else we may simply take $A' = A'_x$ for any x violating this bound.

Note also that for distinct $x, y \in \pi(A)$ the set $A_x \cup A_y$ (and hence A) contains a binary set of size $m_x + m_y$, and so

$$m_x + m_y \leqslant m. \tag{8.8}$$

Now let y be such that m_y is maximal, and set $A' := \bigcup_{x \neq y} A'_x$. By (8.8), we see that if $x \neq y$ then $m_x \leqslant m/2$. Therefore

$$\dim_*(A') = 1 + \max_{x \neq y} \dim_*(A'_x) \leqslant 1 + \max_{x \neq y} \log_2 m_x \leqslant \log_2 m.$$

Moreover,

$$|A'| = \sum_{x \neq y} |A'_x| \geqslant \sum_{x \neq y} \frac{1}{m_x}|A_x| \geqslant \frac{1}{m - m_y} \sum_{x \neq y} |A_x| = \frac{|A| - |A_y|}{m - m_y} \geqslant \frac{|A|}{m}.$$

Here, we used $m_x \leqslant m - m_y$ and, in the last step, (8.7) with $x = y$. □

CHAPTER 9

Higher sum-product theorems

In this chapter, we will be considering higher-order sumsets and product sets of sets of integers. If $A \subset \mathbf{Z}$ is finite, and if $m \geqslant 1$ is an integer, we have already defined

$$mA := \{a_1 + \cdots + a_m : a_i \in A\}.$$

We now further define

$$A^{(m)} := \{a_1 \cdots a_m : a_i \in A\}.$$

Note that $2A = A + A$ and $A^{(2)} = A \cdot A$.

We showed in Theorem 7.3.1 that if $A \subset \mathbf{R}$ then either $2A$ or $A^{(2)}$ has size appreciably bigger than that of A, in fact size at least roughly $|A|^{5/4}$. In this section we will prove a more difficult result due to Bourgain and Chang, which asserts that if $A \subset \mathbf{Z}$ then either mA or $A^{(m)}$ is *much* bigger than A, for large values of m. Here is the result we will prove.

THEOREM 9.0.1. *Let $A \subset \mathbf{Z}$. Then for any m either the m-fold sumset $|mA|$ or the m-fold product set $A^{(m)}$ has cardinality at least $|A|^{b(m)}$, where $b(m) \geqslant c \log m / \log\log m$.*

Note that it is important that $A \subset \mathbf{Z}$; no corresponding result is currently known for sets $A \subset \mathbf{R}$, and this is a very interesting open question.

In the form stated in Theorem 9.0.1, the result is due to Pálvölgyi and Zhelezov; their proof (which is the one we will give) is much easier than the original argument of Bourgain and Chang, and leads to a stronger bound. *Remark.* The original bound of Bourgain and Chang is on the order $b(m) \gg \log^{1/4} m$. The main point of these results is that $b(m) \to \infty$, which is a highly-nontrivial fact.

9.1. Higher-order additive energies

We begin by generalising the notion of additive energy, which we introduced in Chapter 6.

DEFINITION 9.1.1. Let $k \geqslant 2$ be an integer. Given an additive set X, its additive $(2k)$-energy $E_{2k}(X)$ is the number of $(2k)$-tuples $(x_1, \ldots, x_{2k}) \in X^{2k}$ such that $x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}$. More generally, if $X_1, \ldots, X_{2k}$ are additive

sets then we define $E(X_1,\dots,X_{2k})$ to be the number of solutions to $x_1+\cdots+x_k = x_{k+1}+\cdots+x_{2k}$ with $x_i \in X_i$ for all i.

Thus $E_4(X)$ is the number of quadruples (x_1,x_2,x_3,x_4) such that $x_1+x_2 = x_3+x_4$, which is what we called simply the *additive energy* in Chapter 6, where we denoted it by $E(X)$.

We will need the following inequality.

LEMMA 9.1.1. *Let $X_1,\dots,X_{2k} \subset \mathbf{Z}$ be finite sets. Then we have*

$$E(X_1,\dots,X_{2k}) \leqslant \prod_{i=1}^{2k} E_{2k}(X_i)^{1/2k}.$$

Proof. A quick proof of this may be given using the Fourier transform and Hölder's inequality. For this, observe that

$$E(X_1,\dots,X_{2k}) = \int_0^1 \hat{1}_{X_1}(\theta)\cdots\hat{1}_{X_k}(\theta)\overline{\hat{1}_{X_{k+1}}(\theta)}\cdots\overline{\hat{1}_{X_{2k}}(\theta)}d\theta,$$

where for any set

$$\hat{1}_X(\theta) := \sum_n 1_X(n)e(-n\theta),$$

as in Chapter 3. The proof involves simply substituting the definition of the Fourier transform and using orthogonality, exactly as for the proof of (3.6).

Similarly (in fact, consequently) we have

$$E_{2k}(X_i) = \int_0^1 |\hat{1}_{X_i}(\theta)|^{2k}d\theta.$$

The stated inequality is now a consequence of Hölder's inequality on the Fourier side, that is to say the inequality

$$\int_0^1 f_1\cdots f_{2k} \leqslant \prod_{i=1}^{2k}(\int_0^1 |f_i|^{2k})^{1/2k}.$$

This concludes the proof. □

We will also need the following, which is essentially the higher-order version of Proposition 6.2.1, proved in the same way.

LEMMA 9.1.2. *Let X be an additive set, and let $k \geqslant 2$ be an integer. Then*

$$|kX| \geqslant \frac{|X|^{2k}}{E_{2k}(X)}.$$

Proof. Write $r_k(n)$ for the number of tuples $(x_1,\dots,x_k) \in X^k$ with $x_1+\cdots+x_k = n$. Then we have, by the Cauchy-Schwarz inequality,

$$|X|^{2k} = \big(\sum_{n\in kX} r_k(n)\big)^2 \leqslant |kX|\sum_n r_k(n)^2 = |kX|E_{2k}(X).$$

This concludes the proof. □

9.2. A lemma of Chang

If p is a prime and $m \in \mathbf{N}$, write $v_p(m)$ for the p-adic valuation of m, that is to say the exponent of the largest power of p dividing m. We have the following lemma of Mei-Chu Chang.

LEMMA 9.2.1. *Let p be a prime, and suppose that $A \subset \mathbf{Z}$ is a finite set. Let $A_i := \{n \in A : v_p(n) = i\}$. Then*

$$E_{2k}(A)^{1/k} \leqslant \binom{2k}{2} \sum_i E_{2k}(A_i)^{1/k}.$$

Proof. Since A is the disjoint union of the A_i, we have

$$E_{2k}(A) = \sum_{j_1,\dots,j_{2k}} E(A_{j_1}, \dots, A_{j_{2k}}).$$

However, not all of the terms here make any contribution. For a nonzero contribution we must have

$$p^{j_1} n_1 + \cdots + p^{j_k} n_k = p^{j_{k+1}} n_{k+1} + \cdots + p^{j_{2k}} n_{2k}$$

for some n_i coprime to p. Let $j = \min(j_1, \dots, j_{2k})$. Dividing through by p^j and considering congruences mod p, we see that there must be two i, i' with $j_i = j_{i'} = j$. Let us estimate the contribution in the case $\{i, i'\} = \{1, 2\}$; the other cases are essentially identical. This contribution is

$$\begin{aligned}\sum_{j, j_3, j_4, \dots, j_{2k}} E(A_j, A_j, A_{j_3}, \dots, A_{j_{2k}}) &= \sum_j E(A_j, A_j, A, \dots, A) \\ &\leqslant \sum_j E_{2k}(A_j)^{1/k} E_{2k}(A)^{(k-1)/k},\end{aligned}$$

where in the last step we used Lemma 9.1.1. Summing over the $\binom{2k}{2}$ choices of the pair $\{i, i'\}$ now gives

$$E_{2k}(A) \leqslant \binom{2k}{2} E_{2k}(A)^{(k-1)/k} \sum_j E_{2k}(A_j)^{1/k},$$

from which the lemma follows immediately. □

9.3. The Bourgain-Chang theorem

Suppose that $A \subset \mathbf{N}$ is a finite set. By the *multiplicative skew-dimension* of A, we mean the skew-dimension of the image of A under the map $v := (v_p)_{p \text{ prime}} : \mathbf{N} \to \prod_p \mathbf{Z}$. Note that since A is a finite set, only finitely many primes are relevant here,

so we can assume the image of v is finite-dimensional. We denote the multiplicative skew-dimension by $\dim_*^\times(A)$.

PROPOSITION 9.3.1. *Suppose that $A \subset \mathbf{N}$ is a set with multiplicative skew-dimension at most D. Then*

$$E_{2k}(A)^{1/k} \leqslant \binom{2k}{2}^D |A|.$$

Proof. The result is almost immediate using Lemma 9.2.1 and induction on D, the result being trivial when $D = 0$ (in which case A is a singleton and $E_{2k}(A) = 1$). To see this, let us consider the definition of multiplicative skew-dimension. If it is at most D, there is (by definition) some prime p such that the fibres of the "coordinate map" $v_p : A \to \mathbf{Z}$ have multiplicative skew dimension at most $D-1$. These fibres, however, are precisely the A_i in the statement of Lemma 9.2.1. □

Now we turn to the main result, Theorem 9.0.1.

Proof. [Proof of Theorem 9.0.1] At the expense of reducing c slightly, it suffices to handle the case when $m = 2^t$ is a sufficiently large power of two. Set $k := \lfloor \frac{t}{\log t} \rfloor$ and $b := \frac{t}{100 \log t}$.

Suppose that

$$|A^{(2^t)}| \leqslant |A|^b. \tag{9.1}$$

Our aim is to show that

$$|2^t A| \geqslant |A|^b, \tag{9.2}$$

which will conclude the proof. The assumption (9.1) implies that

$$\prod_{i=0}^{t-1} \frac{|A^{(2^{i+1})}|}{|A^{(2^i)}|} \leqslant |A|^b,$$

so there is some $i \leqslant t-1$ such that

$$|A^{(2^{i+1})}| \leqslant K|A^{(2^i)}| \tag{9.3}$$

where $K = |A|^{b/t}$.

By Theorem 8.4.1, there is a set $S \subset A^{(2^i)}$, $|S| \geqslant K^{-3}|A^{(2^i)}|$, with $\dim_*^\times(S) \leqslant 3 \log_2 K$. Here $\dim_*^\times$ denotes the multiplicative skew-dimension.

In the following argument, we will use the fact that if $X \subset \mathbf{N}$ has $|X \cdot X| \leqslant K|X|$ then $|X \cdot X^{-1}| \leqslant K^2|X|$, where $X^{-1} := \{x^{-1} : x \in X\}$. This is nothing more than the Plünnecke-Ruzsa inequality, Theorem 4.4.1, in the case $k = \ell = 1$, but stated multiplicatively; note that $\mathbf{N}$ (with multiplication) is contained in the abelian group $\mathbf{Q}^\times$.

Now we have $\sum_x |A \cap xS| = |A||S|$, and the sum is supported on $x \in AS^{-1}$. By the multiplicative Plünnecke-Ruzsa inequality just stated, the containment $S \subset A^{(2^i)}$ and (9.3), we have

$$|AS^{-1}| \leqslant |A^{(2^i)}(A^{(2^i)})^{-1}| \leqslant K^2|A^{(2^i)}|.$$

Therefore there is some x such that

$$|A \cap xS| \geqslant \frac{|A||S|}{|AS^{-1}|} \geqslant K^{-5}|A|.$$

Setting $A' := A \cap xS$, we therefore have

$$|A'| \geqslant K^{-5}|A| \tag{9.4}$$

and

$$\dim_*^\times(A') \leqslant \dim_*^\times(xS) = \dim_*^\times(S) \leqslant 3\log_2 K < 5\log K,$$

since multiplicative skew dimension is invariant under (multiplicative) translation.

By Proposition 9.3.1, $E_{2k}(A') \leqslant \binom{2k}{2}^{5k\log K}|A|^k$. Using the crude bound $\binom{2k}{2} \leqslant 2k^2$, we may put this in the tidier form

$$E_{2k}(A') \leqslant K^{15k\log k}|A|^k, \tag{9.5}$$

Finally, applying Lemma 9.1.2 and using (9.4), (9.5) gives

$$|2^tA| \geqslant |kA| \geqslant |kA'| \geqslant K^{-25k\log k}|A|^k = |A|^{k-\frac{25bk\log k}{t}} \geqslant |A|^{k/2} > |A|^b$$

by the choice of b and k. This is (9.2), the bound we aimed to prove, so the proof is finished. □

APPENDIX A

Arithmetical functions

In this section, relevant mostly to the material in Chapter 2, we give a brief refresher on the basic arithmetic functions.

An *arithmetical function* is simply a function $f : \mathbf{N} \to \mathbf{C}$. The ones we shall consider will be real-valued. The ones which come up in Chapter 2 are the following:

- The Möbius function μ, defined by $\mu(1) = 1$, $\mu(n) = (-1)^k$ if $n = p_1 \cdots p_k$ for distinct primes p_i, and $\mu(n) = 0$ if n is divisible by the square of some prime;
- The divisor function $\tau(n)$, defined to be the number of positive integer divisors of n (including n itself).

Other important arithmetic functions include the Euler totient function $\phi(n)$, the number of positive integers less than n and coprime to it.

The Möbius function μ. The first important fact we need about the Möbius function is Möbius inversion. If $f_1, f_2 : \mathbf{N} \to \mathbf{C}$ are two arithmetic functions then we write $f_1 \star f_2$ for their *Dirichlet convolution*

$$f_1 \star f_2(n) := \sum_{d|n} f_1(d) f_2(\frac{n}{d}).$$

One may easily check that this is a symmetric, associative operation.

LEMMA A.0.1 (Möbius inversion). *Suppose that $f, g : \mathbf{N} \to \mathbf{C}$ are arithmetic functions. Then*

$$g(n) = \sum_{d|n} f(d)$$

for all n if and only if

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$$

for all n.

Proof. In the notation of Dirichlet convolution, this states that $g = f \star 1$ if and only if $f = g \star \mu$. To prove this, the key observation to make is that

$$\mu \star 1 = \delta, \tag{A.1}$$

where $\delta : \mathbf{N} \to \mathbf{C}$ is the arithmetic function defined by $\delta(1) = 1$ and $\delta(n) = 0$ for $n > 1$. In other words,

$$\sum_{d|n} \mu(d) = 0$$

unless $n = 1$, in which case it equals 1. This may be easily checked by considering the prime factorisation of n.

One may also observe that δ acts like an identity for Dirichlet convolution: $f = f \star \delta$.

Therefore if $g = f \star 1$ then we have $g \star \mu = (f \star 1) \star \mu = f \star (1 \star \mu) = f \star \delta = f$, whilst in the other direction, if $g \star \mu = f$ then $f \star 1 = (g \star \mu) \star 1 = g \star (\mu \star 1) = g \star \delta = g$. This completes the proof. □

We also need the following variant of Möbius inversion.

LEMMA A.0.2. *Let $z \geqslant 1$ be a parameter. Suppose we have two arithmetical functions $f, g : \mathbf{N} \to \mathbf{C}$ related by*

$$g(\delta) = \sum_{\substack{d \leqslant z \\ \delta | d}} f(d). \tag{A.2}$$

Then

$$f(d) = \sum_{\substack{\delta \leqslant z \\ d | \delta}} \mu(\frac{\delta}{d}) g(\delta). \tag{A.3}$$

Proof. Substitute (A.2) into the right hand side of (A.3). This gives

$$\sum_{d' \leqslant z} f(d') \sum_{d | \delta | d'} \mu(\frac{\delta}{d}).$$

(Note the condition $\delta \leqslant z$ has disappeared since it is automatically implied by $d' \leqslant z$ and $\delta | d'$). Substituting $\delta = kd$ in the inner sum, we see that

$$\sum_{d | \delta | d'} \mu(\frac{\delta}{d}) = \sum_{k | \frac{d'}{d}} \mu(k) = 1_{d'/d=1}.$$

This completes the proof. □

Remark. All that was used about the set $\mathcal{D} := \{d : d \leqslant z\}$ is that it is *divisor-closed*, that is to say if $d \in \mathcal{D}$ and $d' | d$, then $d' \in \mathcal{D}$. Therefore, a similar statement holds for other divisor-closed sets.

The divisor function τ. Recall that $\tau(n)$ is the number of (positive integer) divisors of n. If $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorisation of n, then

$$\tau(n) = (a_1 + 1) \cdots (a_k + 1);$$

the divisors of n are precisely the numbers $p_1^{a_1'} \cdots p_k^{a_k'}$ with $0 \leqslant a_i' \leqslant a_i$ for all i.

A very important fact about the divisor function – used throughout analytic number theory – is the *divisor bound*, which asserts that $\tau(n)$ grows slower than any fixed power of n.

LEMMA A.0.3 (Divisor bound). *For any $\varepsilon > 0$ there is a constant C_ε such that $\tau(n) \leqslant C_\varepsilon n^\varepsilon$ for all n.*

Proof. Let the prime factorisation of n be $p_1^{a_1} \cdots p_k^{a_k}$. For each fixed prime p we have $\lim_{a\to\infty} \frac{a+1}{p^{\varepsilon a}} = 0$, so there is some $C = C(p,\varepsilon)$ such that $a + 1 \leqslant C(p,\varepsilon)p^{a\varepsilon}$ for all natural numbers a. Moreover, since $a + 1 \leqslant 2^a$, we can take $C(p,\varepsilon) = 1$ for $p \geqslant 2^{1/\varepsilon}$. It follows that

$$\tau(n) = \prod_{i=1}^{k}(a_i + 1) \leqslant \prod_i C(p_i,\varepsilon)p_i^{a_i\varepsilon} \leqslant C(\varepsilon)n^\varepsilon,$$

where

$$C(\varepsilon) := \prod_p C(p,\varepsilon).$$

Note this is a finite constant because of the fact that $C(p,\varepsilon) = 1$ for $p \geqslant 2^{1/\varepsilon}$. □

Multiplicative functions. An arithmetical function $f : \mathbf{N} \to \mathbf{C}$ is multiplicative if $f(ab) = f(a)f(b)$ whenever a and b are coprime. Note carefully that the condition is *not* that $f(ab) = f(a)f(b)$ for *all* a, b; that is a stronger condition, known as complete multiplicativity.

Both the Möbius function μ and the divisor function τ are multiplicative, but neither is completely multiplicative.

One may check that if $f, g : \mathbf{N} \to \mathbf{C}$ are two multiplicative functions, then their Dirichlet convolution $f \star g$ is also multiplicative. Indeed, if a and b are coprime then

$$\begin{aligned} f \star g(ab) &= \sum_{d|ab} f(\frac{ab}{d})g(d) = \sum_{d_1|a,d_2|b} f(\frac{a}{d_1}\frac{b}{d_2})g(d_1d_2) \\ &= \sum_{d_1|a} f(\frac{a}{d_1})g(d_1)\sum_{d_2|b} f(\frac{b}{d_2})g(d_2) = (f\star g)(a)(f\star g)(b). \end{aligned}$$

APPENDIX B

Geometry of numbers

The main goal of this section is to prove Minkowski's second theorem. First we briefly go over some standard properties of the determinant of a lattice.

LEMMA B.0.1. *If $q \in \mathbf{N}$ then $\det(q\mathbf{Z}^d) = q^d$. If Λ, Λ' are two lattices with $\Lambda' \subset \Lambda$, then $\det(\Lambda')/\det(\Lambda) = [\Lambda : \Lambda']$, where the latter quantity is the index of Λ' as a subgroup of Λ, that is to say the number of cosets of Λ' needed to cover Λ.*

Now let us recall the statement of Minkowski's Second theorem, and let us also state Minkowski's *first* theorem. In both of these results, $K \subset \mathbf{R}^d$ is a centrally symmetric convex body, and $\Lambda \subset \mathbf{R}^d$ a lattice. The successive minima of K with respect to Λ are $\lambda_1, \dots, \lambda_d$.

THEOREM B.0.1 (Minkowski I). *Suppose that $\mathrm{vol}(K) > 2^d \det(\Lambda)$. Then K contains a nonzero point of Λ.*

THEOREM B.0.2 (Minkowski II). *We have $\lambda_1 \cdots \lambda_d \mathrm{vol}(K) \leqslant 2^d \det(\Lambda)$.*

Let us remark that Minkwoski I is a consequence of Minkowski II. To see this, note that if $\mathrm{vol}(K) > 2^d \det(\Lambda)$ then Minkowski II implies that $\lambda_1 \cdots \lambda_d < 1$. Since $\lambda_1 \leqslant \cdots \lambda_d$, this implies that $\lambda_1 < 1$. By the definition of λ_1, it follows that K contains at least one nonzero point of Λ.

Minkowski I is a very straightforward consequence of the following result, *Blichfeldt's lemma*, which is also an ingredient in the proof of Minkowski II.

LEMMA B.0.2 (Blichfeldt's lemma). *Suppose that $K \subset \mathbf{R}^d$, and suppose that $\mathrm{vol}(K) > \det(\Lambda)$. Then there are two distinct points $\mathbf{x}, \mathbf{y} \in K$ with $\mathbf{x} - \mathbf{y} \in \Lambda$.*

Remark. Note that here K is not required to be either centrally symmetric or convex.

Proof. By considering the sets $K \cap B(0, R)$, as $R \to \infty$, whose volumes tend to that of K, we may assume that K lies inside some ball $B(0, R)$. Now let us suppose that the conclusion is false: then no translate of K contains two points of Λ, or in other words

$$\sum_{\mathbf{x}} 1_K(\mathbf{x} - \mathbf{t}) 1_\Lambda(\mathbf{x}) \leqslant 1$$

for all $\mathbf{t} \in \mathbf{R}^d$. Let R' be much bigger than R, and average this last inequality over $\mathbf{t}$ lying in the ball $B(0, R')$ to obtain

$$\sum_x 1_\Lambda(\mathbf{x})\big(\frac{1}{\mathrm{vol}(B(0,R'))}\int_{B(0,R')} 1_K(\mathbf{x}-\mathbf{t})d\mathbf{t}\big) \leqslant 1.$$

Since $K \subset B(0,R)$, the inner integral equals $\mathrm{vol}(K)$ if $\|x\| \leqslant R' - R$, and therefore

$$\sum_{\mathbf{x}} 1_\Lambda(\mathbf{x}) 1_{B(0,R'-R)}(\mathbf{x})d\mathbf{x} \leqslant \frac{\mathrm{vol}(B(0,R')}{\mathrm{vol}(K)},$$

and hence

$$\frac{1}{\mathrm{vol}(B(0,R'-R))}\sum_{\mathbf{x}} 1_\Lambda(\mathbf{x}) 1_{B(0,R'-R)}(\mathbf{x})d\mathbf{x} \leqslant \frac{\mathrm{vol}(B(0,R')}{\mathrm{vol}(B(0,R'-R))}\cdot\frac{1}{\mathrm{vol}(K)}. \tag{B.1}$$

However it is "clear" by tiling with fundamental parallelepipeds that

$$\lim_{r\to\infty}\frac{1}{\mathrm{vol}(B(0,r))}\sum_{\mathbf{x}} 1_\Lambda(\mathbf{x}) 1_{B(0,r)}(\mathbf{x}) = \frac{1}{\det(\Lambda)},$$

and moreover

$$\lim_{R'\to\infty}\frac{\mathrm{vol}(B(0,R')}{\mathrm{vol}(B(0,R'-R))} = 1.$$

Comparing with (B.1) immediately leads to

$$\frac{1}{\det(\Lambda)} \leqslant \frac{1}{\mathrm{vol}(K)},$$

contrary to assumption. □

Although we will not formally need it in what follows, let us pause to give the simple deduction of Minkowski I.

Proof. [Proof of Minkowski I] By Blichfeldt's lemma, the set $\frac{1}{2}K = \{\frac{1}{2}\mathbf{x} : \mathbf{x} \in \mathbf{R}^d\}$ contains two distinct points of Λ; thus there are $\mathbf{x}, \mathbf{y} \in K$ with $\frac{1}{2}(\mathbf{x}-\mathbf{y}) \in \Lambda$. However, since K is convex and centrally symmetric we have $\frac{1}{2}(\mathbf{x}-\mathbf{y}) \in K$. □

Now we turn to the proof of Minkowski II.

Proof. [Proof of Minkowski II] It is technically convenient to assume that K is *open*; this we may do by passing from K to the interior K°. Take a directional basis $\mathbf{b}_1, \ldots, \mathbf{b}_d$ for Λ with respect to K. Since K is open, $\lambda_k K \cap \Lambda$ is spanned (over $\mathbf{R}$) by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$. Indeed if it were not then we could choose some further linearly independent vector $\mathbf{b} \in \lambda_k K \cap \Lambda$, and by the openness of K this would in fact lie in $(\lambda_k - \varepsilon)K \cap \Lambda$ for some $\varepsilon > 0$, contrary to the definition of λ_k.

Write each given $\mathbf{x}$ in coordinates relative to the basis vectors $\mathbf{b}_i$ as $x_1\mathbf{b}_1 + \cdots + x_d\mathbf{b}_d$. We now define some rather unusual maps $\phi_j : K \to K$, by mapping $\mathbf{x} \in K$ to the centre of gravity of the slice of K which contains $\mathbf{x}$ and is parallel to the

subspace spanned by $\mathbf{b}_1, \cdots, \mathbf{b}_{j-1}$ (for $j = 1$, $\phi_1(\mathbf{x}) = \mathbf{x}$). Next, we define a map $\phi : K \to \mathbf{R}^d$ by

$$\phi(\mathbf{x}) := \sum_{j=1}^{d} (\lambda_j - \lambda_{j-1})\phi_j(\mathbf{x}),$$

where we are operating with the convention that $\lambda_0 = 0$. Let us make a few further observations concerning the ϕ_j and ϕ. In coordinates we have $\phi_j(\mathbf{x}) = \sum_i c_{ij}(\mathbf{x})\mathbf{b}_i$, where $c_{ij}(\mathbf{x}) = x_i$ for $i \geqslant j$, and $c_{ij}(\mathbf{x})$ depends only on $x_j, \cdots, x_d$ for $i < j$. It follows that

$$\phi(\mathbf{x}) = \sum_{i=1}^{d} \mathbf{b}_i(\lambda_i x_i + \psi_j(x_{i+1}, \cdots, x_d))$$

for certain continuous functions ψ_j. It follows easily that

$$\mathrm{vol}(\phi(K)) = \lambda_1 \cdots \lambda_d \,\mathrm{vol}(K), \tag{B.2}$$

the Jacobian of the transformation $x_i' = \lambda_i x_i + \psi_i(x_{i+1}, \ldots, x_d)$ being $\lambda_1 \cdots \lambda_d$.

Suppose, as a hypothesis for contradiction, that $\lambda_1 \cdots \lambda_d \,\mathrm{vol}(K) > 2^d \det(\Lambda)$. By Blichfeldt's lemma and (B.2), this means that $\phi(K)$ contains two elements $\phi(\mathbf{x})$ and $\phi(\mathbf{y})$ which differ by an element of $2 \cdot \Lambda = \{2\lambda : \lambda \in \Lambda\}$, and this means that $\frac{1}{2}(\phi(\mathbf{x}) - \phi(\mathbf{y})) \in \Lambda$. Write $\mathbf{x} = \sum_i x_i \mathbf{b}_i$ and $\mathbf{y} = \sum_i y_i \mathbf{b}_i$, and suppose that k is the largest index such that $x_k \neq y_k$. Then we have $\phi_i(\mathbf{x}) = \phi_i(\mathbf{y})$ for $i > k$, so that

$$\begin{aligned}\frac{\phi(\mathbf{x}) - \phi(\mathbf{y})}{2} &= \sum_{j=1}^{d} (\lambda_j - \lambda_{j-1})\Big(\frac{\phi_j(\mathbf{x}) - \phi_j(\mathbf{y})}{2}\Big) \\ &= \sum_{j=1}^{k} (\lambda_j - \lambda_{j-1})\Big(\frac{\phi_j(\mathbf{x}) - \phi_j(\mathbf{y})}{2}\Big).\end{aligned}$$

This has two consequences. First of all the convexity of K implies that $\frac{1}{2}(\phi_j(\mathbf{x}) - \phi_j(\mathbf{y})) \in K$ for all j, and hence (again by convexity) $\frac{1}{2}(\phi(\mathbf{x}) - \phi(\mathbf{y})) \in \lambda_k K$. Secondly we may easily evaluate the coefficient of $\mathbf{b}_k$ when $\frac{1}{2}(\phi(\mathbf{x}) - \phi(\mathbf{y}))$ is written in terms of our directional basis: it is exactly $\lambda_k(x_k - y_k)/2$. In particular this is nonzero, which means that $\frac{1}{2}(\phi(\mathbf{x}) - \phi(\mathbf{y}))$ lies in Λ and $\lambda_k K$, but not in the span of $\mathbf{b}_1, \cdots, \mathbf{b}_{k-1}$. This is contrary to the observation made at the start of the proof. □

Bibliography

[1] H. Davenport, *Analytic methods for diophantine equations and diophantine inequalities* Second edition. With a foreword by R. C. Vaughan, D. R. Heath-Brown and D. E. Freeman. Edited and prepared for publication by T. D. Browning. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2005. xx+140 pp

[2] B. J. Green, *Course notes for C3.8*, available at
`http://people.maths.ox.ac.uk/greenbj/papersprimenumbers.pdf`

[3] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Math. **17**, Springer.

[4] T. D. Wooley, *Large improvements in Waring's problem,* Ann. of Math. (2) **135** (1992), no. 1, 131–164.

[5] G. A. Freiman, *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. vii+108 pp.