Some Results in Set Addition



Przemysław Mazur
Magdalen College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy

Trinity 2016

This thesis is dedicated to
my wife Sylwia
and my children Adam and Maja
for being an inexhaustible source of motivation and inspiration.

Acknowledgements

First and foremost, I would like to thank my advisor, Professor Ben J. Green for his guidance and support during my time as a D.Phil. student.

I also thank Professor Tomasz Schoen for the opportunity to pay academic visits to my home country.

Many thanks go to the University of Cambridge, where I started my doctoral studies and was funded for my first year, as well as to the University of Oxford for recognizing my previous achievements and letting me contitnue my studies here.

I thank my colleagues: Rudi Mrazović, Jakub Konieczny, Freddie Manners, Sean Eberhard, Sofia Lindqvist and Aled Walker for all the discussions that helped me to pursue my research.

Abstract

This thesis is concerned with some problems regarding set addition.

One of them is trying to find the correct dependence of parameters in the Balog-Szemerédi-Gowers Theorem. Although we do not resolve this issue completely, we provide a nontrivial lower bound.

In the main part of the thesis we develop the structure theory of sets with small popular doubling. We prove various results for subsets of integers, groups of prime order or arbitrary abelian groups; all of them are direct analogues of the results about sets of small doubling.

In addition, we provide an estimate of the number of subsets of an interval with certain size and bounded doubling constant; this extends a theorem of Green and Morris. Roughly speaking, we prove that it is enough to count sets that, except a few points, form a dense subset of a (one-dimensional) arithmetic progression. As a tool we prove a result about approximating sets, which might be considered interesting on its own right.

Finally, we apply results from previous chapters to strengthen another theorem of Green and Morris. We prove that if a sumset of a random subset of the set of natural numbers misses at least k elements of $\mathbb{N}$, with positive probability it means that in fact among those elements we can find all of $1, 2, \ldots, k$.

Contents

1 Introduction **1**

1.1 Historical background 1
1.2 Notation and conventions 2
1.3 The concept of set addition 4
1.4 Sets of small doubling 5
1.5 Additive energy and the Balog-Szemerédi-Gowers Theorem 11
1.6 Popular sums 13
1.7 The Green-Morris Theorem on counting sets 17
1.8 Probability of holes in the sumset 18

2 Preliminary results **20**

2.1 Analytic tools and the Fourier transform 20
2.2 Gowers uniformity norms 21
2.3 Green's regularity lemma 22
2.4 The Green-Morris regularity lemma 23
2.5 The Green-Tao regularity lemma 24
2.6 Freĭman's Theorem, homomorphisms and dimension 37
2.7 Results about $\mathbb{F}_2^n$ 40

3 A lower bound in the Balog-Szemerédi-Gowers Theorem **43**

3.1 Additive energy of the Euclidean ball 44
3.2 Discrete approximation 45
3.3 Doubling constants of d-dimensional sets 47
3.4 Conclusion 49
3.5 Further comments 50

4 Sets with small popular doubling **51**
4.1 Subsets of abelian groups 51
4.2 Sets of integers 58
4.3 Sets of residues modulo a prime 63

5 Counting subsets with small doubling **68**
5.1 Examples 68
5.2 Splitting into cases 70
5.3 The regularity lemma and approximating sets 71
5.4 Counting sets 73
5.5 Subsets of $\mathbb{F}_2^n$ 75
5.6 Further discussion 78

6 Probability of holes in a sumset **80**
6.1 The Green-Morris Theorem, revisited 80
6.2 Completing the proof 85

A Estimates of binomial coefficients **88**

Bibliography **90**

Chapter 1

Introduction

1.1 Historical background

Additive combinatorics is an area of mathematics which aims to describe various kinds of approximate structure. Although its rapid development was initiated about 50 years ago by Gregory Freĭman, one of the oldest results that can be called additive combinatorial was published in 1813 by Cauchy [7] (known nowadays as the Cauchy-Davenport Theorem). He proved that whenever p is a prime and A and B are nonempty subsets of the cyclic group $\mathbb{Z}/p\mathbb{Z}$, the number of elements that can be written as a sum $a+b$ with $a \in A$ and $b \in B$ is at least $\min(|A|+|B|-1, p)$. The lower bound is attained for sets $A = \{1, \ldots, |A|\}$ and $B = \{1, \ldots, |B|\}$. This theorem was reproved in 1935 by Davenport [8, 9]. Later, in 1956, it was complemented by Vosper [40], who showed that this is essentially the only nontrivial example for which equality occurs.

A more rapid development of additive combinatorics began with Gregory Freĭman. Most of his work was devoted to describing structure of sets with small doubling, i.e. those sets A whose number of pairwise sums $a+a'$ with $a, a' \in A$ is not much larger than the size of A itself. He proved many different results; the deepest of all is relating such sets with small doubling to generalized arithmetic progressions, i.e. (images of) intersections of boxes in $\mathbb{R}^d$ with $\mathbb{Z}^d$. Freĭman gathered his results in his book [17] published in 1966.

One of the important concepts in additive combinatorics is called additive energy, i.e. the number of solutions to the equation $a+d = b+c$, where a, b, c, d are restricted to belong to a given set. Although the name "additive enrgy" first appears in [39], the concept itself was studied long before. Balog and Szemerédi [1] proved that sets with large additive energy must necessarily contain a dense structured part. Their theorem was later reproved with much better quantitative dependencies, crucial for

applications, by Gowers [19]. In Chapter 3 we discuss the dependency of one constant on another in the statement of the theorem.

Some of the results of additive combinatorics concern what are called popular sums. Specifically, Pollard extended the Cauchy-Davenport Theorem in the following way. For p prime and $A, B \subset \mathbb{Z}/p\mathbb{Z}$, he called N_k the number of elements of $\mathbb{Z}/p\mathbb{Z}$ that can be written as a sum $a+b$ with $a \in A, b \in B$ in at least k different ways. Now the Cauchy-Davenport Theorem can be expressed in the form $N_1 \geq \min(|A|+|B|-1, p)$; Pollard's Theorem states that $N_1 + \ldots + N_t \geq t \cdot \min(|A| + |B| - t, p)$ as long as $\min(|A|, |B|) \geq t$ — again the lower bound we get for arithmetic progressions [31]. This theorem was complemented as well — Nazarewicz et al. [30] showed that for most values of $|A|$ and $|B|$, two arithmetic progressions is the only possibility for equality (the actual restrictions being $\min(|A|, |B|) \geq t+1$, $\max(|A|, |B|) \geq t+2$ and $|A|+|B| < p+t$). These results are important to us; in Chapter 4 we develop a structure theory of sets based on popular sums count.

The paper that we will most often refer to is the one published by Green and Morris [23]. Their main result provides an estimate for the number of sets with small doubling (in an appropriate sense). They also find several applications of it, one of which is estimating how many natural numbers x cannot be expressed as $x = a + a'$, where a and a' are constrained to belong to some randomly chosen subset of $\mathbb{N}$. We spend Chapters 5 and 6 improving the asymptotics in both of the aforementioned results.

This thesis is organized as follows. In the remainder of this chapter we set up the notation, present all the pre-existing results that motivate our research, and introduce the results to be proven. In Chapter 2 we present the results that we use, but do not serve us as motivation. In the next chapters we present the proofs of our results. Specifically, in Chapter 3 we discuss the Balog-Szemerédi-Gowers Theorem. Chapter 4 is devoted to studying sets of small popular doubling. In Chapter 5 we count the number of sets with small doubling in two different settings. Finally, in Chapter 6 we apply previous results to estimating the probability that a sumset of a random subset of the natural numbers misses some number of elements.

1.2 Notation and conventions

We use the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ in a standard way to denote the sets of all positive integers, integers, real and complex numbers respectively. The symbol $\mathbb{T}$ might be

less standard and denotes the additive group $\mathbb{R}/\mathbb{Z}$. By $\mathbb{F}_2$ we mean the field with two elements.

If A is a finite set, then the symbol $\mathbb{E}_{x\in A}$ is a shorthand for $\frac{1}{|A|}\sum_{x\in A}$.

For two positive functions f, g defined on the same domain, we use the following notation:

- $f(x) = O(g(x))$ or $f(x) \ll g(x)$ to mean $\sup_x \frac{f(x)}{g(x)} < \infty$,
- $f(x) = \Omega(g(x))$ or $f(x) \gg g(x)$ to mean $\inf_x \frac{f(x)}{g(x)} > 0$,
- $f(x) = \Theta(g(x))$ to mean $f(x) = O(g(x))$ and $f(x) = \Omega(g(x))$ simultaneously.

If in addition the common domain of f and g is a neighbourhood of a point x_0, then we write:

- $f(x) = o(g(x))$ as $x \to x_0$ to mean $\lim_{x\to x_0} \frac{f(x)}{g(x)} = 0$,
- $f(x) = \omega(g(x))$ as $x \to x_0$ to mean $\lim_{x\to x_0} \frac{f(x)}{g(x)} = \infty$.

Note that with the above notation the symbol ω is an inverse of o, Ω is an inverse of O and Θ is its own inverse. By inverse we mean $f(x) = o(g(x)) \Leftrightarrow g(x) = \omega(f(x))$ etc. We can relax the condition of positivity; for complex-valued functions f, g writing $f(x) = o(g(x))$ means $|f(x)| = o(|g(x)|)$ etc. For example we have $\log(x) = o(x)$ as $x \to \infty$, $x^4 + 1 = \Omega(x^2)$ and $x^2 + 1 = \Theta(8x^2 + 13)$. These symbols might appear in the equations in a nested way, e.g. by $3^n + 2^n + 1 = 3^{n+o(1)}$ as $n \to \infty$ we mean that $\log_3(3^n + 2^n + 1) - n = o(1)$.

The symbols above might also come with subscripts. For example, $f(x, y) = O_y(g(x, y))$ means that for every fixed y we have $f(x, y) = O(g(x, y))$. It means that for every y the function $\frac{f(x,y)}{g(x,y)}$ is bounded, but it might become unbounded if we let y vary, as in $xy = O_y(x)$. Another example: we have $\frac{m}{m+n} = o_m(1)$ as $n \to \infty$ and at the same time $\frac{m}{m+n} = 1 - o_n(1)$ as $m \to \infty$, but neither of $\frac{m}{m+n} = o(1)$, $\frac{m}{m+n} = 1 - o(1)$ is true as $m, n \to \infty$.

Each abelian group G mentioned in the text comes naturally equipped with a measure μ. For compact groups, such as $G = \mathbb{T}^d$, μ usually denotes the Haar probability measure. Discrete groups, such as $G = \mathbb{Z}^d$ are usually equipped with the counting measure, satisfying $\mu(A) = |A|$ for all sets $A \subset G$. This creates an ambiguity: for finite groups, i.e. simultaneously compact and discrete ones, we will each time specify the measure μ.

If μ is counting measure, then integration turns into summation: $\int_G f(x)d\mu(x) = \sum_{x\in G} f(x)$. If μ is Haar measure, then we occasionally write $\mathbb{E}_x f(x) = \mathbb{E}_{x\in G} f(x) \coloneqq \int_G f(x)d\mu(x)$, or just $\int_G f(x)dx \coloneqq \int_G f(x)d\mu(x)$. In general, the symbol $\mathbb{E}$ is used to denote averaging with respect to some pre-specified probability measure. If we are doing this over a finite set A, our measure is always the normalized counting measure ($\mathbb{E}_{x\in A} f(x) \coloneqq \frac{1}{|A|}\sum_{x\in A} f(x)$).

1.3 The concept of set addition

Although we have talked about set addition for a bit, we have not defined it accurately yet. Let us do this now.

Definition 1.3.1. Let G be an abelian group and let $A, B \subset G$ be sets. Then the *sumset* $A + B$ is defined as follows:

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

Similarly we define the *difference set* $A - B \coloneqq \{a - b \ : \ a \in A, \ b \in B\}$. If one of the sets has only one element, we use obvious shorthands, e.g. $A - b = A - \{b\}$, $a + B = \{a\} + B$, $-B = \{0\} - B$.

We can now ask the question how large (or small) the set $A + B$ can be, in terms of sizes of the sets A, B. The answer is captured by the following proposition.

Proposition 1.3.2. *Let G be an abelian group and let $A, B \subset G$ be nonempty finite sets. Then*

$$\max(|A|, |B|) \leq |A + B| \leq |A| \cdot |B|$$

and both bounds are optimal. In the case of one set ($A = B$), the optimal upper bound is $|A + A| \leq \binom{|A|+1}{2}$.

Proof. For $a \in A$ we have $a + B \subset A + B$ and consequently $|B| = |a + B| \leq |A + B|$. Similarly $|A| \leq |A + B|$ and therefore $\max(|A|, |B|) \leq |A + B|$. We get the equality if $B = G$ is a group and A is any subset of G.

For the upper bound note that $A + B$ is the image of $A \times B$ under the addition map $(a, b) \mapsto a + b$. Therefore $|A + B| \leq |A \times B| = |A| \cdot |B|$. To get the equality, let $A', B' \subset \mathbb{Z}$ be any sets and let $A = A' \times \{0\}, B = \{0\} \times B' \subset \mathbb{Z}^2$.

For a single set A note that since $a + a' = a' + a$ for any $a, a' \in A$, we can have at most $\binom{|A|}{2}$ sums for a, a' distinct and $|A|$ sums for $a = a'$. Altogether it gives $|A + A| \leq \binom{|A|+1}{2}$. To get equality, let $A = \{e_1, \ldots, e_d\} \subset \mathbb{Z}^d$ be a standard basis. $\square$

To get started, we need one more piece of notation.

Definition 1.3.3. Let G be an abelian group and let $A \subset G$ be a nonempty finite set. The *doubling constant* of A is defined as

$$\sigma(A) := \frac{|A+A|}{|A|}.$$

1.4 Sets of small doubling

In this section we present what happens in various settings when $|A+B|$ is close to its lower bound. We state the results that give some structural information about the sets A and B. Let us start from the simplest case, i.e. when $|A+B|$ is minimal.

Proposition 1.4.1. *Let G be an abelian group and let $A, B \subset G$ be nonempty finite sets. Then $|A+B| = |B|$ if and only if B is a union of cosets of the group generated by $A-A$.*

Proof. If B is a union of cosets, then a translate $x+A-A$ can be either contained in B, or disjoint from B (depending on which coset it is contained in). Specifically, we have $x+A-A \subset B \Leftrightarrow x \in B$ and consequently $A-A+B=B$. Now we can write the sequence of inequalities $|B| = |a+B| \leq |A+B| = |A-a+B| \leq |A-A+B| = |B|$ valid for all $a \in A$; it follows that $|A+B| = |B|$. Conversely, pick any $a \in A$. Since $a+B \subset A+B$, we have $|B| = |a+B| \leq |A+B| = |B|$ and hence $a+B = A+B$. It means that for any $a' \in A$, $b \in B$ we have $a'+b \in a+B$ or in other words $a'-a+b \in B$. Since a, a', b were arbitrary, we have $A-A+B \subset B$. It follows that for any $h \in A-A$ we have $h+B \subset B$; comparing the sizes gives $h+B=B$. Now if $h_1+B=B$ and $h_2+B=B$, then $(h_1-h_2)+B = (h_1-h_2)+(h_2+B) = h_1+B = B$, so the set $H = \{h \in G \ : \ h+B=B\}$ is a subgroup of G containing $A-A$. In the end, if $b \in B$, then $b+h \in B$ for any $h \in H$, so $b+H \subset B$ and B is a union of cosets of H. □

What happens if we move a little bit from the minimal value? The following argument is based on [18] and [39, Exercise 2.6.5].

Proposition 1.4.2. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Suppose that $|A+B| < \frac{3}{2}N$. Then the set $H = A-A = B-B$ is a subgroup with $|H| = |A+B|$. Consequently, A and B are contained in single cosets of H.*

Proof. For any $a_1, a_2 \in A$ the sets $a_1 + B$ and $a_2 + B$ both have size $|B| = N$ and are contained in the set $A + B$ of size less than $\frac{3}{2}N$. Therefore their intersection has size $|(a_1 + B) \cap (a_2 + B)| \geq |B| + |B| - |A + B| > \frac{1}{2}N$, or in other words $|(a_1 - a_2 + B) \cap B| > \frac{1}{2}N$. Since a_1, a_2 were arbitrary, it follows that $|(h+B) \cap B| > \frac{1}{2}N$ for any $h \in H_A \coloneqq A - A$. Now for any two $h_1, h_2 \in H_A$, the sets $(h_1 + B) \cap B$ and $(h_2 + B) \cap B$ both have size greater than $\frac{1}{2}N$ and are contained in the set B of size N. Therefore their intersection is nonempty. If we pick $x \in (h_1 + B) \cap (h_2 + B)$, then $h_1 - h_2 = (x - h_2) - (x - h_1) \in H_B \coloneqq B - B$. Since h_1, h_2 were arbitrary, we have proved that $H_A - H_A \subset H_B$. Similarly $H_B - H_B \subset H_A$. Those two imply that $H = H_A = H_B$ is a subgroup.

Now picking any $a \in A$ we get $A - a \subset A - A = H$, in other words $A \subset a + H$. Similarly $B \subset b + H$ for any $b \in B$. Those are the desired cosets.

For the size of H recall that each $h \in H$ has $|(h + B) \cap B| > \frac{1}{2}N$, or in other words can be written as $h = b_1 - b_2$ with $b_1, b_2 \in B$ in more than $\frac{1}{2}N$ ways. Since there are only N^2 pairs $(b_1, b_2) \in B^2$, it follows that $|H| < \frac{N^2}{N/2} = 2N$. Now we know that $A + B \subset (a + H) + (b + H) \subset a + b + H$. Conversely, if $x \in a + b + H$, then the sets A and $x - B$ have both size N and are subsets of $a + H$ of size less than $2N$ (as $x - B \subset (a + b + H) - (b + H) \subset a + H$). Therefore their intersection is nonempty. Picking $y \in A \cap (x - B)$ we have $x = y + (x - y) \in A + B$. Since x was arbitrary, it follows that $a + b + H \subset A + B$. In the end $A + B = a + b + H$ and so $|H| = |A + B|$. □

The assumptions of the statement above ($|A| = |B|$, but not necessarily $A = B$) may seem a bit artificial. One should think of $A = B$ and $A = -B$ as two main applications. We phrased it that way to avoid giving two separate proofs.

Example 1.4.3. Let $A = B = \{0, 1\} \subset \mathbb{Z}$. Then $|A + B| = \frac{3}{2}|A| = \frac{3}{2}|B|$, yet there is no coset of a finite subgroup of $\mathbb{Z}$ containing either A or B. This shows that the constant $\frac{3}{2}$ in the above statement is optimal.

For sets of different sizes we need to invoke Kneser's Theorem[28]. For a short proof, see [10].

Theorem 1.4.4 (Kneser)**.** *Let G be an abelian group and let $A, B \subset G$ be nonempty finite sets. Let $H = \{h \in G \ : \ A + B + h = A + B\}$ be the stabilizer of $A + B$. Then*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

An immediate corollary is that $|A+B| \geq |A|+|B|-|H|$, or in other words, there are at least $|A|+|B|-|A+B|$ elements $h \in G$ with $h+A+B = A+B$. This is a nontrivial result for $|A+B| < |A|+|B|-1$ (as we always have $0+A+B = A+B$).

Let us now turn our attention to the integers. There are no nontrivial finite subgroups and so the most structured sets are arithmetic progressions. For completeness we give the following definition.

Definition 1.4.5 (arithmetic progression)**.** Let G be an abelian group. An *arithmetic progression* is a set of the form

$$P = \{x + jd \ : \ j \in \{0, \dots, k-1\}\},$$

where $x, d \in G$ and k is a positive integer. The element d is the *common difference* (or *difference* for short) and the number k is the *length* of P.

Since in the integers there are no nontrivial finite subgroups, Kneser's Theorem tells us that $|A+B| \geq |A|+|B|-1$. Actually the proof of this statement is much simpler and may be regarded as folklore.

Proposition 1.4.6. *Let $A, B \subset \mathbb{Z}$ be finite sets with $\min(|A|, |B|) \geq 2$. Then $|A+B| \geq |A|+|B|-1$ with the equality if and only if or A and B are arithmetic progressions of the same common difference.*

Proof. Let $a_1 < \ldots < a_k$ be all the elements of A and $b_1 < \ldots < b_l$ be all the elements of B, so that $|A| = k$ and $|B| = l$. Then the numbers

$$a_1 + b_1 < \ldots < a_k + b_1 < \ldots < a_k + b_l$$

are $k+l-1$ distinct elements of $A+B$.

If A and B are progressions of common difference d, then

$$A + B = \{a_1 + b_1 + jd \ : \ j \in \{0, 1, \ldots k+l-2\}\}$$

and consequently $|A+B| = k+l-1$.

Suppose that $|A+B| = k+l-1$. We have another way to write out $k+l-1$ elements of $A+B$, namely

$$a_1 + b_1 < a_1 + b_2 < \ldots < a_k + b_2 < \ldots a_k + b_l.$$

Since $|A+B| = k+l-1$, these two sequences are actually the same and consequently $a_{i+1} + b_1 = a_i + b_2$ for $i = 1, \ldots, k-1$. In other words $a_{i+1} - a_i = b_2 - b_1 =: d$ and A is an arithmetic progression. Similarly we prove that B is an arithmetic progression of difference d. $\square$

The above statement applied with $A = B$ gives us a structural information about sets with $|A+A| = 2|A|-1$. Freĭman was the first one to extend this result to larger values of $|A + A|$.

Theorem 1.4.7 (Freĭman [15]). *Let $A \subset \mathbb{Z}$ be a finite set satisfying $|A+A| < 3|A|-3$. Then there exists an arithmetic progression $P \supset A$ with $|P| \leq |A + A| - |A| + 1$.*

The above statement is traditionally called the Freĭman $(3k-3)$ Theorem, since for $k = |A|$ we can write the assumption as $|A + A| < 3k - 3$. The value $3|A| - 3$ cannot be improved, as seen in the following example.

Example 1.4.8. Let $A = \{0, 1, \ldots, |A| - 2\} \cup \{M\} \subset \mathbb{Z}$ for some number $M \geq 2|A| - 3$. Then

$$A + A = \{0, \ldots, 2|A| - 4\} \cup \{M \ldots, M + |A| - 2\} \cup \{2M\}.$$

Therefore $|A + A| = (2|A| - 3) + (|A| - 1) + 1 = 3|A| - 3$, yet $|A|$ cannot be covered with an arithmetic progression of length at most M.

Theorem 1.4.7 was generalized by Lev and Smeliansky to two different sets.

Theorem 1.4.9 (Lev, Smeliansky [29]). *Let $A, B \subset \mathbb{Z}$ be finite sets. Suppose that the number $\mu = |A + B| - |A| - |B|$ satisfies the inequalities*

$$\mu \leq \min(|A|, |B|) - 3 \qquad \textit{and} \qquad \mu \leq \max(|A|, |B|) - 4.$$

Then there are arithmetic progressions $P \supset A$ and $Q \supset B$ with $|P| \leq |A| + \mu + 1$ and $|Q| \leq |B| + \mu + 1$.

We can provide a similar example in the case $|A| \neq |B|$ to prove sharpness.

Example 1.4.10. Let $A = \{0, 1, \ldots, |A| - 1\} \subset \mathbb{Z}$ and $B = \{0, 1, \ldots |B| - 2\} \cup \{M\}$ with $|A| < |B|$ and $M \geq |A| + |B| - 2$. Then

$$A + B = \{0, \ldots, |A| + |B| - 3\} \cup \{M, \ldots, M + |A| - 1\}.$$

Therefore $|A+B| = (|A|+|B|-2)+|A| = |A|+|B|+\min(|A|, |B|)-2$, yet B cannot be covered with an arithmetic progression of length at most M.

The above theorems show that all sets of doubling slightly less than 3 are in some sense related to arithmetic progressions. One can ask if that is still the case for larger doubling constant. The next example shows that things may get more complicated.

Example 1.4.11 (sets of doubling at most 4)**.** Let P be an arithmetic progression of length $2k$ and let $A \subset P$ be a set of size k. Then $|A+A| \leq |P+P| < 4k$.

Let P be an arithmetic progression of length $\lfloor \frac{3}{2}k \rfloor$ and let A be a set of size k with $|A \setminus P| = 1$. Then

$$|A+A| \leq |(A\cap P)+(A\cap P)| + |(A\setminus P)+A| \leq |P+P| + |A\setminus P|\cdot|A| < 3k+k = 4k.$$

Let P be an arithmetic progression of size k and let A be a set of size k with $|A \setminus P| = 2$. Then

$$|A+A| \leq |(A\cap P)+(A\cap P)| + |(A\setminus P)+A| \leq |P+P| + |A\setminus P|\cdot|A| < 2k+2k = 4k.$$

Let P and Q be arithmetic progressions and let $A = P \times Q$. Then

$$|A+A| = |(P+P)\times(Q+Q)| = |P+P|\cdot|Q+Q| < \\ < 2|P|\cdot 2|Q| = 4|P||Q| = 4|P\times Q| = 4|A|.$$

The last of the above examples is significantly different from the others. Here, the largest part of A that can be covered by an arithmetic progression has size $\max(|P|,|Q|)$, which can be as small fraction of A as we want. That means that this kind of multidimensional progressions (mentioned in the introductory section) must be also taken into account.

Definition 1.4.12 (Generalized arithmetic progression)**.** Let G be an abelian group. A *generalized arithmetic progression* is a set of the form

$$P = \left\{ x_0 + \sum_{j=1}^{d} a_j x_j \ : \ a_j \in \{0,\dots L_j - 1\} \right\},$$

where d is a positive integer, $L_1,\dots L_d \geq 2$ are integers and $x_0,\dots x_d \in G$. The *dimension* of P is defined as $\dim P := d$ and the *size* of P is $\mathrm{size}(P) = \prod_{j=1}^{d} L_j$.

In general we have $|P| \leq \mathrm{size}(P)$. In the case of equality we say that P is *proper*.

It might happen that for a set P the values of $\dim P$ and $\mathrm{size}(P)$ are ambiguous, so we always assume that a set P comes with the description as above.

With the above definition we are ready to state Freĭman's Theorem on sets of small doubling, referred to as simply Freĭman's Theorem.

Theorem 1.4.13 (Freĭman, [17])**.** *Let $K \geq 1$ be a real number and let $A \subset \mathbb{Z}$ be a finite set with $|A+A| \leq K|A|$. Then there exists a d-dimensional arithmetic progression $P \supset A$ with $d \leq F_1(K)$, satisfying $\mathrm{size}(P) \leq F_2(K)|A|$. The quantities $F_1(K)$ and $F_2(K)$ depend only on K.*

Freĭman's original argument turned out to be difficult to understand. A more accessible version, leading to useful quantitative bounds, was found subsequently by Ruzsa [33]. For that reason the above result is often called the Freĭman-Ruzsa Theorem. Also a nontrivial contribution was done by Bilu ([4]).

For completeness, we note also here the results about subsets of finite groups of prime order. Those also do not have any nontrivial subgroups, so we already know that $|A+B| \geq |A|+|B|-1$ unless $A+B$ is the entire group.

Theorem 1.4.14 (Cauchy-Davenport [7, 8]). *Let p be a prime and let $A, B \subset \mathbb{Z}/p\mathbb{Z}$ be nonempty sets. Then*

$$|A+B| \geq \min(|A|+|B|-1, p).$$

Theorem 1.4.15 (Vosper [40]). *Let p be a prime number and let $A, B \subset \mathbb{Z}/p\mathbb{Z}$ be nonempty sets. Then $|A+B| = |A|+|B|-1$ if and only if one of the following conditions holds:*

(a) $\min(|A|, |B|) = 1$,

(b) $|A+B| = p$,

(c) $B = (\mathbb{Z}/p\mathbb{Z}) \setminus (c-A)$ *for some* $c \in \mathbb{Z}/p\mathbb{Z}$,

(d) A and B are arithmetic progressions of the same common difference.

Theorem 1.4.16 (Freĭman [16]). *Let p be a prime number and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a nonempty set of size $|A| \leq \frac{p}{35}$. Suppose that $|A+A| \leq 2.4|A|-3$. Then there is an arithmetic progression $P \supset A$ with $|P| \leq |A+A|-|A|+1$.*

The last theorem is not optimal, both in terms of the density of A and its doubling constant. The following two results increase one of them at the cost of decreasing the other.

Theorem 1.4.17 (Green-Ruzsa [24]). *Let p be a prime number and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a nonempty set of size $|A| \leq 2^{-2^{10}}p$. Suppose that $|A+A| < 3|A|-3$. Then there is an arithmetic progression $P \supset A$ with $|P| \leq |A+A|-|A|+1$.*

Theorem 1.4.18 (Serra-Zémor [36]). *Let $p > 2^{94}$ be a prime number and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a nonempty set with $|A| \leq |A+A|-|A|+1 \leq \frac{p-1}{2}$. Suppose that $|A+A| \leq \min(3|A|-4, (2+10^{-4})|A|)$. Then there is an arithmetic progression $P \supset A$ with $|P| \leq |A+A|-|A|+1$.*

Actually Theorem 1.4.17 is a consequence of [24, Theorem 1.3] and the Freĭman $(3k-3)$ Theorem.

Freĭman's 2.4 Theorem can be also improved using similar methods that he used (see [32])

Notice that most of the resuls from this section followed the pattern: find the minimal possible popular sums count, find the sets that achieve this minimum and also find those that are close to minimum. This was done for abelian groups in general as well as for integers and finite groups of prime order. We can summarize the results in the following table:

Small doubling

	inequality	extremizers	near-extremizers
in any abelian group	folklore	folklore	folklore/Kneser
in $\mathbb{Z}$	folklore	folklore	Freĭman/Lev-Smeliansky
in $\mathbb{Z}/p\mathbb{Z}$	Cauchy-Davenport	Vosper	Freĭman/Green-Ruzsa/Serra-Zémor

1.5 Additive energy and the Balog-Szemerédi-Gowers Theorem

We have already explained the importance of the concept of doubling constant. Another important quantity related to a set is the additive energy.

Definition 1.5.1. Let G be an abelian group and let $A \subset G$ be a nonempty finite set. The *addititve energy* of A is the following quantity:

$$E(A) = |\{(a,b,c,d) \in A^4 \ : \ a+d = b+c\}|$$

A quadruple (a,b,c,d) with $a+d=b+c$ is called an *additive quadruple*. Thus the additive energy of A is just the number of additive quadruples.

Proposition 1.5.2. *Let G be an abelian group and let $A \subset G$ be a nonempty finite set. Then $E(A) \leq |A|^3$. Moreover $E(A) = |A|^3$ if and only if A is a coset of a subgroup.*

Proof. For every $(a,b,c) \in A^3$ the equation $a+d=b+c$ has exactly one solution in $d \in G$ and therefore at most one solution in $d \in A$. Therefore the number of additive quadruples of elements of A is bounded by $|A^3| = |A|^3$.

By the above analysis $E(A) = |A|^3$ if and only if $b+c-a \in A$ for every $a,b,c \in A$, or equivalently $(b-c)-(a-c) \in A-c$. By a well known criterion $A-c$ is then a subgroup, which makes A its coset. □

The additive energy is connected with the doubling constant in the following way.

Proposition 1.5.3. *Let G be an abelian group and let $A \subset G$ be a nonempty finite set. Suppose that $|A+A| \leq K|A|$ for some real number $K \geq 1$. Then $E(A) \geq \frac{|A|^3}{K}$.*

Proof. Rewrite the fromula for additive energy as follows:

$$E(A) = \sum_{r \in G} |\{(a,b,c,d) \in A^4 \ : \ a+d = b+c = r\}| = \\ = \sum_{r \in G} |\{(x,y) \in A^2 \ : \ x+y = r\}|^2 = \sum_{r \in G} |A \cap (r-A)|^2.$$

Note that $A \cap (r-A) \neq \emptyset$ if and only if $r - x \in A$ for some $x \in A$ or in other words $r \in A+A$. Therefore we can restrict the above summation to $r \in A+A$. This allows us to use the Cauchy-Schwarz inequality:

$$|A|^4 = \left(\sum_{r \in A+A} |\{(x,y) \in A^2 \ : \ x+y = r\}| \right)^2 = \left(\sum_{r \in A+A} |A \cap (r-A)| \right)^2 \leq \\ \leq \left(\sum_{r \in A+A} |A \cap (r-A)|^2 \right) \left(\sum_{r \in A+A} 1 \right) = E(A)|A+A|.$$

In the end $E(A) \geq \frac{|A|^4}{|A+A|} \geq \frac{|A|^3}{K}$. □

One might wonder if the converse is true, i.e. if large additive energy implies small doubling. This is false, as shown in the following example.

Example 1.5.4. Let G be a finite abelian group and let m be a positive integer to be chosen later. Define $A = \{0\} \times G \cup \{1, \ldots, m\} \times \{0\} \subset \mathbb{Z} \times G$. Then

$$|A+A| \geq |\{0, \ldots, m\} \times G| = (m+1)|G|$$

and so $\frac{|A+A|}{|A|} \geq \frac{(m+1)|G|}{m+|G|} = \frac{m+1}{1+\frac{m}{|G|}}$. On the other hand

$$\frac{E(A)}{|A|^3} \geq \frac{|\{(a,b,c,d) \in \{0\} \times G \ : \ a+d = b+c\}|}{|A|^3} = \left(\frac{|G|}{|A|} \right)^3 = \left(\frac{1}{1+\frac{m}{|G|}} \right)^3.$$

Therefore if m and $\frac{|G|}{m}$ are sufficiently large, then $\frac{E(A)}{|A|^3}$ is as close to 1 as we like, yet $\frac{|A+A|}{|A|}$ is as large as we like.

Note that in the above example large portion of the set A has small doubling, specifically $|A'+A'| = |A'|$ for $A' = \{0\} \times G$. Balog and Szemerédi [1] proved that this is always the case.

Theorem 1.5.5 (Balog-Szemerédi-Gowers)**.** *Let A be a finite subset of an abelian group G. Suppose that $E(A) \geq \frac{|A|^3}{K}$ for some positive real number K. Then there exists a subset $A' \subset A$ with $|A'| \gg_K |A|$ satisfying $|A' + A'| \ll_K |A'|$.*

Gowers [19] was the first to prove the above result with polynomial bounds and that is why the theorem is named after him as well. Currently the best bounds in the theorem are the ones obtained by Schoen [35].

Theorem 1.5.6 (Schoen)**.** *Let A be a finite subset of an abelian group G. Suppose that $E(A) \geq \frac{|A|^3}{K}$ for some positive real number K. Then there exists a subset $A' \subset A$ with $|A'| \gg \frac{|A|}{K}$ satisfying $|A' - A'| \ll K^4|A'|$.*

The above statement is different to the previous one in the sense that $A' + A'$ is replaced with $A' - A'$. However, this difference is of very little significance to us.

Our aim is to check if the exponent 4 in $|A' - A'| \ll K^4|A'|$ can be replaced by anything smaller. Although we do not provide a complete solution, we give a lower bound of $\frac{\log 2}{\log \frac{3\sqrt{3}}{4}} = 2.6494\ldots$. Specifically, we prove the following statement.

Proposition 1.5.7. *Let $C < \frac{\log 2}{\log \frac{3\sqrt{3}}{4}}$, $M > 0$ be real numbers and let $f : [1, \infty) \to [1, \infty)$ be an increasing function. Then there exists an abelian group G and a finite set $A \subset G$ for which the following statement is true. Let $K = \frac{|A|^3}{E(A)}$. Every set $A' \subset A$ with $|A'| \geq \frac{|A|}{f(K)}$ satisfies $|A' \pm A'| > M \cdot K^C|A'|$.*

The base of the construction of the set A will be the Euclidean ball in a high dimensional real vector space. In Chapter 3 we give the details of the construction. Following Shao [37], we also explain why the Euclidean ball is the optimal shape amongst all subsets of $\mathbb{R}^d$.

1.6 Popular sums

We start this section with the definition of popular sums.

Definition 1.6.1. Let G be an abelian group, let $A, B \subset G$ be sets and let $t > 0$ be a real number. An element $x \in G$ is said to be *t-popular sum* of the pair (A, B) if it can be written as a sum $x = a + b$ with $a \in A$, $b \in B$ in at least t different ways. More formally, we need $|\{(a, b) \in A \times B \ : \ a + b = x\}| = |A \cap (x - B)| = |B \cap (x - A)| \geq t$. Similarly, we define *$t$-popular differences* of (A, B) as those $x \in G$ for which $|\{(a, b) \in A \times B \ : \ a - b = x\}| = |A \cap (x + B)| \geq t$. For a single set A, a t-popular sum or difference of A is just that of the pair (A, A).

We can now ask the following question: to what extent can we develop similar results to those in the previous section, with sums replaced with popular sums? In other words, can it be proven that having close to minimal number of popular sums imposes some rigid algebraic structure? The following example shows that this approach fails at the very beginning.

Example 1.6.2. Let $A = \{e_1, \ldots, e_d\} \subset \mathbb{Z}^d$ be the standard basis. Then A has no t-popular sums for any $t > 2$, yet elements of A satisfy no nontrivial algebraic relations whatsoever.

One can wonder, in the light of the above example, why we bother dealing with popular sums. To explain, let us cite the following results.

Theorem 1.6.3 (Pollard [31])**.** *Let t be a positive integer, p be a prime and let $A, B \subset \mathbb{Z}/p\mathbb{Z}$ be sets of size at least t. Let N_k be the number of k-popular sums of (A, B) for $k = 1, \ldots t$. Then*

$$\sum_{k=1}^{t} N_k \geq t(|A| + |B| - t).$$

Theorem 1.6.4 (Nazarewicz, O'Brien, O'Neill, Staples [30])**.** *Let t be a positive integer, p be a prime and let $A, B \subset \mathbb{Z}/p\mathbb{Z}$ be sets of size at least t. Let N_k be the number of k-popular sums of (A, B) for $k = 1, \ldots t$. Then*

$$\sum_{k=1}^{t} N_k = t(|A| + |B| - t).$$

if and only if at least one of the following conditions holds:

(a) $\min(|A|, |B|) = t$,

(b) $|A| + |B| \geq p + t$,

(c) $|A| = |B| = t + 1$ *and* $B = c - A$ *for some* $c \in \mathbb{Z}$,

(d) A and B are arithmetic progressions of the same common difference.

In light of the above results, it turns out that the correct quantity to consider was not the number of t-popular sums, but the *average* number of k popular sums for $k = 1, \ldots, t$. We can try to construct a similar table as at the end of the preceding section. At the moment it would look like this.

Small popular doubling

	inequality	extremizers	near-extremizers
in any abelian group	?	?	?
in $\mathbb{Z}$	(Pollard)	(Nazarewicz et al.)	?
in $\mathbb{Z}/p\mathbb{Z}$	Pollard	Nazarewicz et al.	?

The names in brackets mean that the results in $\mathbb{Z}$ can be deduced from the corresponding results for $\mathbb{Z}/p\mathbb{Z}$. Indeed, it does not matter for popular sums which underlying group we choose as long as $A, B \subset \{0, 1, \ldots, \frac{p-1}{2}\}$.

In Chapter 4 we provide the results to fill in the remainder of the above table completely, including separate proofs of the results in brackets, not relying on their analogues in finite groups. The actual statements of the results go as follows:

Proposition 1.6.5. *Let $t > 0$, G be an abelian group and let $A, B \subset G$ be finite sets of size at least t. Then*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) \geq t \cdot \max(|A|, |B|).$$

Proposition 1.6.6. *Let $t > 0$, G be an abelian group and let $A, B \subset G$ be finite sets of size at least t. Suppose that $|A| \leq |B|$. Then*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) = t|B|$$

if and only if one at least of the following conditions holds:

(a) $|A| = t$,

(b) B *is a union of cosets of the subgroup generated by* $A - A$.

Theorem 1.6.7. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Let $t, \delta > 0$ be two real numbers satisfying the inequality $\delta + \frac{t}{N} \leq \frac{1}{2}$. Moreover suppose that the following inequality holds:*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) \leq (1 + \delta)Nt.$$

Then there exists a subgroup $H \leq G$ and cosets C_A and C_B of H satisfying the following conditions:

- $|H| \leq (1 + \delta)N$,

- $|A \setminus C_A| + |B \setminus C_B| \leq t$.

Proposition 1.6.8. *Let t be a positive integer and $A, B \subset \mathbb{Z}$ be finite sets of size at least t. Then*

$$\sum_{x \in \mathbb{Z}} \min(1_A * 1_B(x), t) \geq t(|A| + |B| - t).$$

Proposition 1.6.9. *Let t be a positive integer and $A, B \subset \mathbb{Z}$ be finite sets of size at least t. Then*

$$\sum_{x \in \mathbb{Z}} \min(1_A * 1_B(x), t) = t(|A| + |B| - t)$$

if and only if at least one of the following conditions holds:

(a) $\min(|A|, |B|) = t$,

(b) $|A| = |B| = t + 1$ *and* $B = c - A$ *for some* $c \in \mathbb{Z}$,

(c) A and B are arithmetic progressions of the same common difference.

Theorem 1.6.10. *Let $A \subset \mathbb{Z}$ be a nonempty finite set and let t be a positive integer. Suppose that*

$$\sum_{x \in \mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2 + \delta)t|A|,$$

for some $\delta > 0$. Then there is an arithmetic progression $P \subset \mathbb{Z}$ with $|P| \leq (1 + 2\delta)|A| + 6t$ and $|A \setminus P| \leq \frac{5t}{2}$, provided that $\delta + \frac{5t}{|A|} \leq \frac{1}{4}$.

Theorem 1.6.11. *Let $0 < \alpha_1 < \alpha_2$ and $\delta_0, \eta > 0$ be real numbers. Suppose that one of the following conditions holds:*

- $\delta_0 < 0.4$ *and* $\alpha_2 = \frac{1}{35}$,
- $\delta_0 < 1$ *and* $\alpha_2 = 2^{-2^{10}}$,
- $\delta_0 < 10^{-4}$ *and* $\alpha_2 = \frac{1}{2(1+\delta_0)}$.

Then there exists a number $t_0 = t_0(\alpha_1, \eta, \delta_0)$ with the following property. Let $p > p_0(\alpha_1, \eta, \delta_0)$ be a sufficiently large prime, $A \subset \mathbb{Z}/p\mathbb{Z}$ be a set satisfying $\alpha_1 p \leq |A| \leq \alpha_2 p$ and let $t \in (0, t_0)$ be a real number. Suppose that for some $\delta \in (0, \delta_0)$ the following inequality holds:

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2 + \delta)|A|t.$$

Then there exists an arithmetic progression $P \subset \mathbb{Z}/p\mathbb{Z}$ with $|P| \leq (1 + \delta + \eta)|A| + 1$ and $|A \setminus P| \leq \eta|A|$.

1.7 The Green-Morris Theorem on counting sets

We start this section with citing the Green-Morris theorem.

Theorem 1.7.1 (Green, Morris [23]). *Fix $\delta > 0$ and $K > 0$. Then the following holds for all integers $k \geq k_0(\delta, K)$. For any $N \in \mathbb{N}$ there are at most*

$$2^{\delta k}\binom{\frac{1}{2}Kk}{k}N^{\lfloor K+\delta \rfloor}$$

sets $A \subset \{1, \ldots, N\}$ with $|A| = k$ and $|A + A| \leq K|A|$.

In their paper the authors provide two families of sets $A \subset \{1, \ldots, N\}$ with $|A| = k$ and $|A + A| \leq K|A|$. There are $\binom{\frac{1}{2}Kk}{k}$ subsets of size k of an arithmetic progression of length $\frac{1}{2}Kk$ and roughly $N^{\lfloor K \rfloor}$ that consist of an arithmetic progression and $\lfloor K \rfloor - 2$ arbitrarily chosen points (as long as $\frac{k}{N} \to 0$). The existence of those two families of sets shows that in most ranges of parameters N, k their number is estimated accurately up to an exponent of $1 + o(1)$. This happens when either of the factors N^K and $\binom{\frac{1}{2}Kk}{k}$ dominates over the other. For fixed $K > 2$, we have $\binom{\frac{1}{2}Kk}{k} = 2^{\Phi(K/2)k - o(k)}$ (see Corollary A.0.8), so this term is dominating if $\frac{\log N}{k} \to 0$. Conversely N^K is dominating if $\frac{\log N}{k} \to \infty$.

In Chapter 5 we fill this gap providing an accurate estimate for the number of sets $A \subset \{1, \ldots, N\}$ with $|A| = k$ and $|A + A| \leq K|A|$ in the remaining range $k = \Theta(\log N)$. Specifically, we prove the following result.

Theorem 1.7.2. *Let $\delta > 0$ and $K \geq 2$ be real numbers. Then there exists a number $k_0 = k_0(\delta, K)$ such that for all integers $k > k_0$ and N with $2N \geq Kk$ we have*

$$\max_{0 \leq t \leq \lfloor K \rfloor - 2} \binom{\lfloor \frac{1}{2}(K - t - \delta)k \rfloor}{k} N^{t+2} \leq$$
$$\#\{A \subset [N] \ : \ |A| = k, |A + A| \leq K|A|\} \leq$$
$$\leq \max_{0 \leq t \leq \lfloor K+\delta \rfloor - 2} \binom{\lfloor \frac{1}{2}(K - t + \delta)k \rfloor}{k} N^{t+2}.$$

We might want to evaluate the above maximum depending on the value of $\alpha = \lim \frac{\log_2 N}{k}$. This is done in the statement below.

Corollary 1.7.3. Let N, k be integers $K \geq 2$ be a real number. Suppose that $N, k \to \infty$ with $\frac{\log_2 N}{k} \to \alpha \in (0, \infty)$. Then

$$\#\{A \subset [N] \ : \ |A| = k, \ |A + A| \leq Kk\} = N^{f(\alpha, K) + o(1)},$$

where f is a function defined in the following way:

$$f(\alpha, K) = \begin{cases} 2 + \frac{1}{\alpha}\Phi(\frac{K}{2}), & \alpha \leq \Phi(\frac{K}{2}) - \Phi(\frac{K-1}{2}), \\ t + 2 + \frac{1}{\alpha}\Phi(\frac{K-t}{2}), & \alpha \in [\Phi(\frac{K-t+1}{2}) - \Phi(\frac{K-t}{2}), \Phi(\frac{K-t}{2}) - \Phi(\frac{K-t-1}{2})], \\ \lfloor K \rfloor + \frac{1}{\alpha}\Phi(1 + \frac{\{K\}}{2}), & \alpha \geq \Phi(\frac{3+\{K\}}{2}) - \Phi(1 + \frac{\{K\}}{2}). \end{cases}$$

Here $\Phi(x) = x \log_2 x - (x-1)\log_2(x-1)$ (see Definition A.0.7) and t represents an integer in the interval $(0, \lfloor K \rfloor - 2)$. To make t explicit, we can set

$$\begin{aligned} \Psi(x) &= \Phi(x) - \Phi(x - \tfrac{1}{2}) = \\ &= x \log_2 x - (x - \tfrac{1}{2}) \log_2(x - \tfrac{1}{2}) - (x-1)\log_2(x-1) + (x - \tfrac{3}{2}) \log_2(x - \tfrac{3}{2}); \end{aligned}$$

then we have $t = \min(\max(\lceil K - \Psi^{-1}(\alpha) \rceil, 0), \lfloor K \rfloor - 2)$.

Note that this is consistent with Green-Morris Theorem. Indeed, if $\alpha \to 0$, then we fall into the first case and the result is $N^2 2^{\Phi(K/2)k}$. If $\alpha \to \infty$, then we are in the last case and the answer is $N^{\lfloor K \rfloor} 2^{\Phi(1+\{K\}/2)k}$. In any case, the dominating term agrees with what is given by the Green-Morris Theorem.

In Chapter 5 we also count sets with small doubling inside vector spaces over the two-element field $\mathbb{F}_2$. Using similar methods, we prove an analogue of the Green-Morris theorem.

Theorem 1.7.4. *Fix $\delta > 0$ and $K > 0$. Then the following holds for all integers $k \geq k_0(\delta, K)$. For any $n \in \mathbb{N}$ there are at most*

$$2^{\delta k} \binom{2^{\lfloor \log_2 Kk + \delta \rfloor}}{k} k^{n(1+\delta)}$$

sets $A \subset \mathbb{F}_2^n$ with $|A| = k$ and $|A + A| \leq K|A|$.

We also explain why this bound is *always* accurate, for all ranges of parameters.

1.8 Probability of holes in the sumset

Green and Morris in their paper proved also the following statement ([23, Theorem 1.3]).

Theorem 1.8.1. *Let $A \subset \mathbb{N}$ be chosen by selecting each positive integer to lie in A with probability $\frac{1}{2}$, these choices being made independently. Then the probability that $A + A$ omits exactly s elements of $\mathbb{N}$ is equal to $(2 + o(1))^{-s/2}$ as $s \to \infty$.*

In Chapter 5 we strengthen the above result, replacing $(2+o(1))^{-s/2}$ with $\Theta(2^{-s/2})$. We do it in two different ways. Firstly, we modify the original proof of Green and Morris using structural information about sets of small popular doubling. Secondly, we use the techniques developed in Chapter 4 so that popular sums are no longer introduced; instead we are able to use Freĭman $(3k-3)$ to get the structural information.

The exact statement of the result is the following.

Theorem 1.8.2. *Let $A \subset \mathbb{N}$ be a set chosen randomly by picking each element of $\mathbb{N}$ independently with probability $\frac{1}{2}$. Define a sequence $\{p_k\}$ via*

$$p_k = 2^{k/2} \cdot \mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k).$$

Then the subsequences $\{p_{2k}\}$ and $\{p_{2k+1}\}$ are both increasing and bounded and therefore convergent. In particular $\mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k) = \Theta(2^{-k/2})$ and the implied constants can only oscillate between c and $c\sqrt{2}$ for some $c > 0$ as $k \to \infty$.

Chapter 2

Preliminary results

In this chapter we gather all the statements needed to develop the main results.

In general, we assume that all quantities we write are well defined. For example, writing $\int_G f(x)dx$ means that the integral exists, most often when either $f(x) \geq 0$ for all $x \in G$ or $\int_G |f(x)|dx < \infty$.

2.1 Analytic tools and the Fourier transform

Along with the measure defined on an abelian group G we get the notion of inner product and L^p norms. Recall those:

$$\begin{aligned}
\langle f, g\rangle &= \int_G f(x)\overline{g(x)}dx, \\
\|f\|_p &= \left(\int_G |f(x)|^p dx\right)^{\frac{1}{p}}, \\
\|f\|_\infty &= \inf\{t \geq 0 \ : \ \mu(\{x \in G \ : \ |f(x)| > t\}) = 0\}.
\end{aligned}$$

Recall also $L^p(G) \coloneqq \{f : G \to \mathbb{C} \ : \ \|f\|_p < \infty\}$. The quantities above satisfy Hölder's inequality: if $p, q \geq 1$ with $\frac{1}{p} + \frac{1}{q} = 1$ (using the convention $\frac{1}{\infty} = 0$), then $|\langle f, g\rangle| \leq \|f\|_p \|g\|_q$. In the special case $p = q = 2$ we call it the Cauchy-Schwarz inequality. Applying Hölder's inequality to functions $|f|^r$ and $|g|^r$ we get the following statement: if $p, q, r \geq 1$ with $\frac{1}{p} + \frac{1}{q} = \frac{1}{r}$, then $\|fg\|_r \leq \|f\|_p \|g\|_q$.

The measure gives also rise to the notion of convolution. If $f, g : G \to \mathbb{C}$ are functions, then we put

$$f * g(x) = \int_G f(y)g(x - y)dy.$$

For different measures the above equation may take alternate forms, i.e.

$$f * g(x) = \sum_{y \in G} f(y)g(x - y) \qquad \text{or} \qquad f * g(x) = \mathbb{E}_{y \in G} f(y)g(x - y).$$

The convolutions obey Young's inequality: if $p, q, r \geq 1$ with $\frac{1}{p} + \frac{1}{q} = 1 + \frac{1}{r}$, then $\|f * g\|_r \leq \|f\|_p \|g\|_q$.

We can also define the Fourier transform; in that case we insist that G is compact and equipped with Haar probability measure. We denote by $\widehat{G}$ the space of all continuous multliplicative characters (i.e. functions satisfying $|\chi(x)| = 1$ and $\chi(x + y) = \chi(x)\chi(y)$ for all $x, y \in G$). It is an abelian group under pointwise multiplication. It is also discrete, so we can endow it with the counting measure. For $f \in L^1(G)$, define the function $\widehat{f} : \widehat{G} \to \mathbb{C}$ via the formula:

$$\widehat{f}(\chi) = \langle f, \chi \rangle = \mathbb{E}_x f(x)\chi(-x).$$

The following statements are true for all functions $f, g \in L^2(G)$:

$$\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)} =: \langle \widehat{f}, \widehat{g} \rangle = \langle f, g \rangle \coloneqq \mathbb{E}_x f(x)\overline{g(x)},$$

$$\left(\sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2 \right)^{\frac{1}{2}} =: \|\widehat{f}\|_2 = \|f\|_2 \coloneqq \left(\mathbb{E}_x |f(x)|^2 \right)^{\frac{1}{2}},$$

$$f(x) = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(x).$$

The last equation holds for all x when f is a continuous function (e.g. when G is discrete), but might fail at a set of measure zero if merely $f \in L^2(G)$. The first two equations are called Placharel's and Parseval's identity respectively.

The Fourier transform maps convolution to multiplication and vice versa:

$$\widehat{f * g}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi),$$
$$\widehat{f \cdot g}(\chi) = \widehat{f} * \widehat{g}(\chi).$$

2.2 Gowers uniformity norms

In this section we introduce uniformity norms. They were first defined by Gowers in his paper on Szemerédi's Theorem [19]. We will focus on the U^2 norm, as it is the most important to us. For a group G and a bounded function $f : G \to \mathbb{C}$ the U^2-norm of f is defined as follows:

$$\|f\|_{U^2} = \left(\mathbb{E}_{x,h_1,h_2 \in G} f(x)\overline{f(x + h_1)f(x + h_2)}f(x + h_1 + h_2) \right)^{\frac{1}{4}},$$

The sum inside the brackets is always real and nonnegative, so it makes sense to take a rational power. It can be checked that this expression defines a norm. In fact, it obeys the following equation:

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

All the above results can be found in Chapter 11 of [39].

For completeness, we give the definition of the U^k norm for an integer $k \geq 2$:

$$\|f\|_{U^k} \coloneqq \left(\mathbb{E}_{x \in G, h \in G^k} \left(\prod_{\omega \in \{0,1\}^k} \mathcal{C}^{|\omega|}(f(x + \omega \cdot h)) \right) \right)^{2^{-k}}.$$

Here $|\omega| = \sum_{j=1}^{k} \omega_j$, $\omega \cdot h = \sum_{j=1}^{k} \omega_j h_j$ and $\mathcal{C}$ is the complex conjugation operator.

2.3 Green's regularity lemma

In the following sections we gather some statements about the concept of regularity. The general idea originates in Szemerédi's regularity lemma [38], which decomposes a graph into pieces with most of the pairs being mutually regular (in a certain sense), the number of pieces being bounded in terms of the accuracy we want to achieve. In other words, every graph can be well approximated with a graph-like object of bounded complexity. This idea was extended to complex-valued functions defined on groups. I turns out that in many cases we can approximate every function (in a certain sense) with a function of bounded complexity.

We present a couple of results of this kind. Our list is by no means complete, but contains all the results that are useful in our applications. Chronologically the first of this family of results was the one proven by Green [22, Theorem 2.1]. It is about subsets of vector spaces over a two-element field $\mathbb{F}_2$. To state it we need the following definition.

Definition 2.3.1. Let $\epsilon > 0$, let V be a finite-dimensional vector space over $\mathbb{F}_2$ and let $A \subset V$ be a set. We say that A is *ϵ-uniform in V*, if the inequality $|\widehat{1_A}(\chi)| \leq \epsilon$ holds for every nontrivial multiplicative character χ.

Theorem 2.3.2. *For every $\epsilon > 0$ there exists a number $M = M(\epsilon)$ such that the following statement is true. Let $n > 0$ be an integer and let $A \subset \mathbb{F}_2^n$ be a set. Then there exists a subspace $V \leq \mathbb{F}_2^n$ with $\operatorname{codim} V \leq M$ such that*

$$\#\{x \in \mathbb{F}_2^n \ : \ (A + x) \cap V \text{ is } \epsilon\text{-uniform in } V\} \geq (1 - \epsilon)2^n.$$

To make use of the above statement, we need an associated counting lemma, also due to Green.

Lemma 2.3.3. *Let $\epsilon > 0$, let V be a finite-dimensional vector space over $\mathbb{F}_2$ and let $A, B \subset V$ be sets. Suppose that $\min(|A|, |B|) \geq \epsilon|V|$ and A is ϵ^2-uniform. Then $|A + B| \geq (1 - \epsilon)|V|$.*

Proof. Let $C = V \setminus (A + B)$. By Fourier analytic identities we have

$$0 = 1_A * 1_B * 1_C(0) = \sum_{\chi \in \widehat{V}} \widehat{1_A}(\chi)\widehat{1_B}(\chi)\widehat{1_C}(\chi)\chi(0) = \frac{|A||B||C|}{|V|^3} + \sum_{\chi \neq 1} \widehat{1_A}(\chi)\widehat{1_B}(\chi)\widehat{1_C}(\chi).$$

Rearranging gives

$$\frac{|A||B||C|}{|V|^3} = \left| \sum_{\chi \neq 1} \widehat{1_A}(\chi)\widehat{1_B}(\chi)\widehat{1_C}(\chi) \right| \leq$$

$$\leq \epsilon^2 \left(\sum_{\chi \neq 1} |\widehat{1_B}(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \neq 1} |\widehat{1_C}(\chi)|^2 \right)^{1/2} \leq \frac{\epsilon^2 \sqrt{|B||C|}}{|V|}.$$

Squaring and rearranging again we get $|A|^2|B||C| \leq (\epsilon|V|)^4$. Since $|A|, |B| \geq \epsilon|V|$, it follows that $|C| \leq \epsilon|V|$, as claimed. □

Those two statements combined tell us that every set $A \subset \mathbb{F}_2^n$ is very close to a random-looking subset of a set of bounded complexity. For more datailed statement of this kind, see Proposition 5.5.1.

2.4 The Green-Morris regularity lemma

We turn now to a slightly different type of statement, proven by Green and Morris. We do not present it in full, as the full discussion would take longer than desirable. We restrict ourselves to citing [23, Theorem 2.1]. A full discussion can be found in [23].

Theorem 2.4.1. *For every $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that the following is true. Let $p > p_0(\epsilon)$ be a sufficiently large prime and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a set. There is a dilate $A^* = \lambda A$ and a prime q, $\frac{1}{\epsilon^{10}} \leq q \leq p^{1-\delta}$, such that the following holds. If $A_i^* = A^* \cap I_i(q)$ for each $i \in \mathbb{Z}/q\mathbb{Z}$ then, for at least $(1 - \epsilon)q^2$ pairs $(i, j) \in (\mathbb{Z}/q\mathbb{Z})^2$*

$$\min(|A_i^*|, |A_j^*|) \leq \epsilon p/q \qquad \text{or} \qquad |A_i^* + A_j^*| \geq (2 - \epsilon)p/q.$$

Here $I_i(q) = \{x \in \mathbb{Z}/p\mathbb{Z} \ : \ x/p \in [i/q, (i+1)/q)\}$.

Roughly speaking, this statement says that every set, possibly after a dilation, can be expressed as a union of random-looking subsets of intervals of (almost) equal length. Note that $|I_i(q) + I_j(q)| \leq \lceil 2p/q \rceil$ for all $i, j \in \mathbb{Z}/q\mathbb{Z}$, so the condidion $|A_i^* + A_j^*| \geq (2-\epsilon)p/q$ means that $A_i^* + A_j^*$ is almost as large as it could possibly be. The disadvantage of this result is that we can only expect this inequality for almost all *pairs*, as opposed to all pairs that can be formed from almost all possible *sets* (like in the previous section). Among the advantages there is a pretty simple description of the cells of the decomposition (random-looking subsets of intervals) and a reasonable dependence of parameters (see [23] for more details).

One could also ask why we needed a dilate and we could not achieve the same result with the set A itself. The counterexample would be $A = \{2x \ : \ x \in \{0, \dots, \lfloor \frac{p}{4} \rfloor\}\}$. Here A is an arithmetic progression (as regular as it could possibly be), but the sumset $A + A$ fills only half of any interval. However replacing A with $A/2$ resolves this issue completely.

2.5 The Green-Tao regularity lemma

In this section we give a self-contained proof of the arithmetic regularity lemma for the U^2-norm. First instance of this lemma was proven by Green [22, Theorem 5.2]. In the modern language we would say it was a variant of what we know now as the U^2 case. Subsequently, the lemma was proven in full generality (i.e. for the U^k-norm for arbitrary k) by Green and Tao in [25]. There is also an exposition by Eberhard of the U^2 case [11]. Unfortunately none of these statements is exactly compatible with our purposes. The first one is phrased very differently and it would be difficult to translate it into what we need. The last two have a feature that is a disadvantage for us, namely they deal with functions defined on $\{1, \dots, N\}$ rather than $\mathbb{Z}/p\mathbb{Z}$. As a result the "structured part" obtained there comes from a Lipschitz function defined on $[0,1] \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{T}^d$ (in the U^2 case). However, as we work over a cyclic group of prime order, in our setting everything is periodic $\pmod p$ and there is no room either for non-periodic behaviour (such as $[0,1]$), or periodic behaviour modulo other numbers. Therefore we are aiming for a slightly different statement of the regularity lemma, but the methods of proof remain the same. The proof itself becomes easier as some of the issues are not present in the world of finite groups.

By a *pre-character* on a group G we mean a homomorphism $\phi : G \to \mathbb{T}$ and by a *character* a homomorphism $\chi : G \to \{z \in \mathbb{C} \ : \ |z| = 1\}$. Of course there is

a one-to-one correspondence between these, given by the equation $\chi = e^{2\pi i\phi}$. This terminology is by no means standard and is used only for the purpose of this section.

Before we start, let us fix some notation. For any set Γ of pre-characters on $\mathbb{Z}/p\mathbb{Z}$ and any positive integer n, we define a partition $\mathcal{B} = \mathcal{B}(\Gamma, n)$ of $\mathbb{Z}/p\mathbb{Z}$ into cells. Intuitively, $\mathcal{B}$ corresponds to the partition of the torus $\mathbb{T}^\Gamma$ into $n^{|\Gamma|}$ cubes of side length $\frac{1}{n}$. More formally, two points $x, y \in \mathbb{Z}/p\mathbb{Z}$ belong to the same cell if $\phi(x), \phi(y) \in [\frac{k_\phi}{n}, \frac{k_\phi+1}{n}) \subset \mathbb{T}$ for some $k_\phi \in \mathbb{Z}$ for all $\phi \in \Gamma$. Note that if $\Gamma \subset \Gamma'$ and $n|n'$, then $\mathcal{B}(\Gamma', n')$ is a refinement of $\mathcal{B}(\Gamma, n)$, i.e. each cell of the latter is a union of cells of the former.

For any function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ and any partition $\mathcal{B} = \mathcal{B}(\Gamma, n)$ define the conditional expectation $\mathbb{E}(f|\mathcal{B})$ in the standard way, i.e. $\mathbb{E}(f|\mathcal{B})(x)$ is the average of f on the cell of $\mathcal{B}$ containing x. In other words, $\mathbb{E}(f|\mathcal{B})$ is just the orthogonal projection of f onto the space of all $\mathcal{B}$-measurable functions (constant on every cell of $\mathcal{B}$). Note that if $\mathcal{B}'$ is a refinement of $\mathcal{B}$ then $\mathbb{E}(\mathbb{E}(f|\mathcal{B}')|\mathcal{B}) = \mathbb{E}(f|\mathcal{B})$, since the inner expectation does not change the average over any cell of $\mathcal{B}$. Also $\mathbb{E}(f \cdot \mathbb{E}(g|\mathcal{B})|\mathcal{B}') = \mathbb{E}(f|\mathcal{B}')\mathbb{E}(g|\mathcal{B})$ since $\mathbb{E}(g|\mathcal{B})$ is constant on every cell of $\mathcal{B}'$ and hence can be pulled out by the linearity of conditional expectation.

Lemma 2.5.1. *Let $n > 0$ and let $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}$ be a pre-character and let $\chi = e^{2\pi i\phi}$. Let Γ be a set of pre-characters containing ϕ and let $\mathcal{B} = \mathcal{B}(\Gamma, n)$. Suppose that $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a function with $\|f\|_\infty \leq 1$. Then*

$$|\langle f - \mathbb{E}(f|\mathcal{B}), \chi\rangle| \leq \frac{2\pi}{n}.$$

Proof. The key idea is that χ is almost constant on each cell of $\mathcal{B}$. More precisely, by properties of $\mathbb{E}(\cdot|\mathcal{B})$ we have

$$\langle f - \mathbb{E}(f|\mathcal{B}), \chi\rangle = \langle f, \chi\rangle - \langle \mathbb{E}(f|\mathcal{B}), \chi\rangle = \langle f, \chi\rangle - \langle \mathbb{E}(f|\mathcal{B}), \mathbb{E}(\chi|\mathcal{B})\rangle = \\ = \langle f, \chi\rangle - \langle f, \mathbb{E}(\chi|\mathcal{B})\rangle = \langle f, \chi - \mathbb{E}(\chi|\mathcal{B})\rangle.$$

But since $\phi \in \Gamma$, the function $\chi - \mathbb{E}(\chi|\mathcal{B})$ is bounded pointwise by $|1 - e^{2\pi i/n}| \leq \frac{2\pi}{n}$ and the claim follows. □

Corollary 2.5.2. Let $\delta > 0$ and let $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ with $\|f\|_\infty \leq 1$. Let Γ be a set of pre-characters and let n be a positive integer. Then there exists a set $\Gamma' \supset \Gamma$ of pre-characters of size $|\Gamma'| \leq \frac{4}{\delta^2} + |\Gamma|$ and $n' \leq \frac{16}{\delta}$ such that for $\mathcal{B}' = \mathcal{B}(\Gamma', nn')$ and any character χ we have

$$|\langle f - \mathbb{E}(f|\mathcal{B}'), \chi\rangle| \leq \delta. \tag{2.1}$$

Proof. Define $n' = \lceil \frac{4\pi}{\delta} \rceil$ and build the set Γ' iteratively, initialising the process with $\Gamma' = \Gamma$. At each stage we ask if the inequality (2.1) is satisfied for every character. If so, we finish our procedure, otherwise we take a character χ for which the inequality fails and add the corresponding pre-character ϕ to Γ. Let $\mathcal{B}' = \mathcal{B}(\Gamma', nn')$ and $\mathcal{B}'' = \mathcal{B}(\Gamma \cup \{\phi\}, nn')$. By the previous lemma we know that

$$|\langle f - \mathbb{E}(f|\mathcal{B}''), \chi \rangle| \leq \frac{2\pi}{nn'} \leq \frac{\delta}{2}.$$

Combining this with the initial assumption on χ and triangle inequality gives

$$|\langle \mathbb{E}(f|\mathcal{B}'') - \mathbb{E}(f|\mathcal{B}'), \chi \rangle| \geq \frac{\delta}{2}.$$

Now we use Cauchy-Schwarz and the fact that $\mathbb{E}(f|\mathcal{B}')$ is an orthogonal projection of $\mathbb{E}(f|\mathcal{B}'')$ (as $\mathcal{B}''$ is a refinement of $\mathcal{B}'$ and we have $\mathbb{E}(f|\mathcal{B}') = \mathbb{E}(\mathbb{E}(f|\mathcal{B}'')|\mathcal{B}')$):

$$\|\mathbb{E}(f|\mathcal{B}'')\|_2^2 - \|\mathbb{E}(f|\mathcal{B}')\|_2^2 = \|\mathbb{E}(f|\mathcal{B}'') - \mathbb{E}(f|\mathcal{B}')\|_2^2 \geq |\langle \mathbb{E}(f|\mathcal{B}'') - \mathbb{E}(f|\mathcal{B}'), \chi \rangle|^2 \geq \frac{\delta^2}{4}.$$

In other words, it means that adding to Γ' the pre-character corresponding to χ increases the value of $\|\mathbb{E}(f|\mathcal{B}')\|_2^2$ by at least $\frac{\delta^2}{4}$. Since this quantity can only take values between 0 and 1, this procedure must terminate in at most $\frac{4}{\delta^2}$ steps. In the end we get a set Γ of size at most $\frac{4}{\delta^2}$ satisfying the inequality (2.1) for each character χ.

It remains to check that the bound on n' is correct. For that we can freely assume $\delta \leq 1$, which implies $\frac{4\pi}{\delta} \geq 4\pi > \frac{25}{2}$. However, for any $x > \frac{25}{2}$ we have the bound $\lceil x \rceil \leq \frac{14}{13}x \leq \frac{16}{4\pi}x$. □

The corollary above says that we extract all the large Fourier coefficients using only projections of bounded complexity. The heart of the arithmetic regularity lemma is to iterate this argument. Before we do that, let us explain what a growth function is. A *growth function* is simply an increasing function $\mathcal{F} : (0, +\infty) \to (0, +\infty)$, typically describing how large we need one parameter to be in terms of another parameter. In most applications one can think of $\mathcal{F}$ as of an exponential function $x \mapsto C_1 e^{C_2 x}$.

Let us note the following fact. For a function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ with $\|f\|_\infty \leq 1$ we have

$$\|f\|_{U^2}^2 = \|\widehat{f}\|_4^2 \leq \|\widehat{f}\|_\infty \|\widehat{f}\|_2 = \|\widehat{f}\|_\infty \|f\|_2 \leq \|\widehat{f}\|_\infty \|f\|_\infty \leq \|\widehat{f}\|_\infty \leq \|\widehat{f}\|_4 = \|f\|_{U^2}.$$

To make it short, $\|f\|_{U^2}^2 \leq \|\widehat{f}\|_\infty \leq \|f\|_{U^2}$. That allows us state the regularity lemma in terms of the l_∞ norm of the Fourier transform, which is convenient for us.

Proposition 2.5.3 (arithmetic regularity lemma: baby version)**.** *Let $\epsilon > 0$ and let $\mathcal{F}$ be a growth function. Then there exists a real number $M_0 = M_0(\epsilon, \mathcal{F}) > 0$ for which the following statement is true. Let p be a prime and $f : \mathbb{Z}/p\mathbb{Z} \to [0,1]$ be a function. Then there exists a number $0 < M \leq M_0$ and a decomposition*

$$f = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$$

satisfying the following properties:

- *$f_{\text{str}} = \mathbb{E}(f|\mathcal{B})$, where $\mathcal{B} = \mathcal{B}(\Gamma, n)$ for some set Γ of pre-characters and some positive integer n with $|\Gamma|, n \leq M$ (f_{str} is structured),*
- *$\|f_{\text{sml}}\|_2 \leq \epsilon$ (f_{sml} is small),*
- *$|\langle f_{\text{unf}}, \chi\rangle| \leq \frac{1}{\mathcal{F}(M)}$ for every character χ (f_{unf} is U^2-uniform).*
- *f_{str} and $f_{\text{str}} + f_{\text{sml}}$ both take values in $[0,1]$.*

Proof. We will again use an iterative procedure. At the beginning, let $\mathcal{B}$ be the trivial partition, corresponding to $\Gamma = \emptyset$ and $n = 1$. At each stage, we set $M = \max(|\Gamma|, n)$ and then apply Corollary 2.5.2 with parameter $\delta = \frac{1}{\mathcal{F}(M)}$ to the function f. This way we get a set Γ' and an integer n', both bounded in terms of M and $\mathcal{F}$. After applying this procedure we wish to set $f_{\text{str}} = \mathbb{E}(f|\mathcal{B})$, $f_{\text{sml}} = \mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B})$ and $f_{\text{unf}} = f - \mathbb{E}(f|\mathcal{B}')$, where $\mathcal{B}' = \mathcal{B}(\Gamma', nn')$. All the required conditions are clearly satisfied except one: it might happen that $\|f_{\text{sml}}\|_2 > \epsilon$. To take care of it, we use iteration: if this actually happened, set $\Gamma := \Gamma'$ and $n := nn'$ and start over. Again, we can argue that since $\mathcal{B}'$ is a refinement of $\mathcal{B}$, we have

$$\|\mathbb{E}(f|\mathcal{B}')\|_2^2 - \|\mathbb{E}(f|\mathcal{B})\|_2^2 = \|\mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B})\|_2^2 = \|f_{\text{sml}}\|_2^2 > \epsilon^2$$

and therefore each iteration increases the value of $\|\mathbb{E}(f|\mathcal{B})\|_2^2$ by at least ϵ^2, so we cannot have more than $\frac{1}{\epsilon^2}$ iterations in total. It means that in the end the result is true with $M_0 = \underbrace{\mathcal{F}'(\dots(\mathcal{F}'(1))\dots)}_{\lfloor \frac{1}{\epsilon^2} \rfloor \text{ iterations}}$. □

The above version of the arithmetic regularity lemma is not quite satisfactory, as we expect to have a slightly different kind of structure for f_{str}. Before we explain how to fix that, let us exploit some properties of the Fejér kernel.

Lemma 2.5.4. *Let d and K be positive integers, let $\chi_j : \mathbb{T}^d \to \mathbb{C}$ $(j = 1, \dots, d)$ be the basic characters defined as $\chi_j(t) = e^{2\pi i t_j}$ and let $\Phi_K : \mathbb{T} \to [0, +\infty)$ be the Fejér kernel of order K:*

$$\Phi_K(t) = \frac{1}{K^d} \prod_{j=1}^{d} \left| \sum_{k=0}^{K-1} \chi_j^k(t) \right|^2 .$$

Then $\int_{\mathbb{T}^d} \Phi_K(t)dt = 1$ and moreover

$$\int_{[-\lambda,\lambda]^d} \Phi_K(t)dt \geq 1 - \frac{d}{4K\lambda^2}.$$

Proof. The first assertion is standard; to prove it one only needs to expand Φ_K as the linear combination of characters and observe that the trivial character comes with coefficient 1. To prove the inequality, let us first note that

$$\left| \sum_{k=0}^{K-1} \chi_j^k(t) \right| = \left| \frac{1 - \chi_j^K(t)}{1 - \chi_j(t)} \right| \leq \frac{2}{|1 - e^{2\pi i t_j}|} \leq \frac{1}{2\|t_j\|}.$$

Therefore if $d = 1$, we have

$$\int_{[-\lambda,\lambda]} \Phi_K(t)dt = 1 - \int_{\|t\| \geq \lambda} \Phi_K(t)dt \geq 1 - \sup_{\|t\| \geq \lambda} \Phi_K(t) = 1 - \frac{1}{4K\lambda^2}.$$

Now for $d > 1$, the d-dimensional Fejér kernel is just a product of d copies of a 1-dimensional one, which gives the bound

$$\int_{[-\lambda,\lambda]^d} \Phi_K(t)dt \geq \left(1 - \frac{1}{4K\lambda^2}\right)^d \geq 1 - \frac{d}{4K\lambda^2}.$$

□

Before stating let us make the maximum norm a default norm on $\mathbb{T}^d$. Then we can write $\|t\| = \max_{1 \leq j \leq d} \|t_j\|$. Consequently, we call a function $F : \mathbb{T}^d \to \mathbb{C}$ M-Lipschitz, if $|F(t_1) - F(t_2)| \leq M\|t_1 - t_2\|$ holds for all $t_1, t_2 \in \mathbb{T}$.

Proposition 2.5.5 (arithmetic regularity lemma: intermediate version)**.** *Let $\epsilon > 0$ and let $\mathcal{F}$ be a growth function. Then there exists a real number $M_0 = M_0(\epsilon, \mathcal{F}) > 0$ for which the following statement is true. Let $p > p_0(\epsilon, \mathcal{F})$ be a prime and $f : \mathbb{Z}/p\mathbb{Z} \to [0, 1]$ be a function. Then there exists a number $0 < M \leq M_0$ and a decomposition*

$$f = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$$

satisfying the following properties:

- $f_{\mathrm{str}} = F \circ \phi$, *where* $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^d$ *is a homomorphism with* $d \leq M$ *and* $F : \mathbb{T}^d \to [0,1]$ *is an* M*-Lipschitz function* (f_{str} *is structured),*
- $\|f_{\mathrm{sml}}\|_2 \leq \epsilon$ (f_{sml} *is small),*
- $|\langle f_{\mathrm{unf}}, \chi\rangle| \leq \frac{1}{\mathcal{F}(M)}$ *for every character* χ (f_{unf} *is* U^2*-uniform).*
- f_{str} *and* $f_{\mathrm{str}} + f_{\mathrm{sml}}$ *both take values in* $[0,1]$.

The only difference between this version and the previous one is the presence of the Lipschitz function F. We will need this fact later on, more precisely for us a Lipschitz function is one that is locally almost constant, in a way we can quantify.

Proof. First we apply to f the baby version with some different parameters ϵ' and $\mathcal{F}'$ to be specified later. We get a decomposition $f = f'_{\mathrm{str}} + f'_{\mathrm{sml}} + f'_{\mathrm{unf}}$; now we set $f_{\mathrm{unf}} = f'_{\mathrm{unf}}$ and try to find f_{str} of the new type so that $\|f_{\mathrm{str}} - f'_{\mathrm{str}}\|_2$ is small and in the end set $f_{\mathrm{sml}} = f'_{\mathrm{sml}} + f'_{\mathrm{str}} - f_{\mathrm{str}}$. We know the structure of f'_{str}; it can be alternatively said that $f'_{\mathrm{str}} = F' \circ \phi$, where $\phi = (\phi_1, \dots, \phi_d) : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^d$ is just a product of all pre-characters forming Γ and $F' : \mathbb{T}^d \to [0,1]$ is a function that is constant on cubes of the form $[\frac{k_1}{n}, \frac{k_1+1}{n}] \times \ldots \times [\frac{k_d}{n}, \frac{k_d+1}{n}]$ for $k_1, \dots, k_d \in \mathbb{Z}$. The function F' does not need to be unique, we can pick any that fits into the formula. Also, it does not need to be Lipschitz and we have to fix that. To do this, put $F = F' * \Phi_K$ for some K to be specified. To see that F is Lipschitz, let us calculate

$$|F(t_1) - F(t_2)| = \left| \int_{\mathbb{T}^d} F'(s)(\Phi_K(t_1 - s) - \Phi_K(t_2 - s)) \right| \leq \\ \leq \sup_s |\Phi_K(t_1 - s) - \Phi_K(t_2 - s)|.$$

The above calculation shows that the Lipschitz constant of F is bounded by that of Φ_K. To estimate it, let us note that Φ_K is a linear combination of characters of the form $\prod_{j=1}^d \chi_j^{k_j}$ with $|k_j| < K$, and a character of this particular form comes with coefficient $\prod_{j=1}^d (1 - \frac{|k_j|}{K})$ and is itself a $(2\pi \sum_{j=1}^d |k_j|)$-Lipschitz function. Therefore the Lipschitz constant of Φ_K is at most

$$L_d = 2\pi \sum_{k_1,\dots,k_d} \left(\left(\sum_{j=1}^d |k_j| \right) \cdot \prod_{j=1}^d \left(1 - \frac{|k_j|}{K} \right) \right).$$

To calculate this, let us set $L'_d = \sum_{k_1,\dots,k_d} \prod_{j=1}^d \left(1 - \frac{|k_j|}{K}\right)$. Then one can check that these sequences satisfy the recurrence $L_{d_1+d_2} = L_{d_1} L'_{d_2} + L_{d_2} L'_{d_1}$ and $L'_{d_1+d_2} =$

$L'_{d_1} + L'_{d_2}$, which together with the boundary conditions $L_1 = \frac{2\pi}{3}(K^2 - 1)$, $L'_1 = K$ gives $L_d = \frac{2\pi}{3} dK^{d-1}(K^2 - 1) \leq 4dK^{d+1}$.

Set $f_{\text{str}} = F \circ \phi$. We would like to bound the expression

$$\|f'_{\text{str}} - f_{\text{str}}\|_2^2 = \mathbb{E}_x |F'(\phi(x)) - F' * \Phi_K(\phi(x))|^2.$$

Let $\lambda > 0$ be a quantity to be chosen later; divide all the elements of $\mathbb{Z}/p\mathbb{Z}$ into two categories. One of them consitis of all the elements x for which $\phi(x)$ lies no further than λ from the boundary of one of the cubes of the partition. Let us estimate the number of such elements: the set of all $t_j \in \mathbb{T}$ with $\|t_j - \frac{k_j}{n}\| \leq \lambda$ has measure 2λ; since p is sufficiently large we can assume that the set of all x with $\|\phi_j(x) - \frac{k_j}{n}\| \leq \lambda$ has size at most $4\lambda p$. Taking into account all possible values of j and k_j we see that in fact all but at most $4\lambda dnp$ elements are separated from the boundary of their cubes by at least λ. For those elements x in the other category let us estimate

$$|F'(\phi(x)) - F' * \Phi_K(\phi(x))| \leq \int_{\mathbb{T}} \Phi_K(t) |F'(\phi(x)) - F'(\phi(x) - t)| dt.$$

By the description of x the latter factor is zero on the cube $[-\lambda, \lambda]^d$; on the remaining set it is bounded by 1, so by the previous lemma the value of the integral is bounded by $\frac{d}{4K\lambda^2}$. In the end, taking into account all elements x (and the trivial bound $|F'(\phi(x)) - F' * \Phi_K(\phi(x))| \leq 1$), we have an estimate

$$\|f'_{\text{str}} - f_{\text{str}}\|_2^2 = \mathbb{E}_x |F'(\phi(x)) - F' * \Phi_K(\phi(x))|^2 \leq 4\lambda dn + \left(\frac{d}{4K\lambda^2}\right)^2.$$

We wish the last quantity to be at most $\frac{\epsilon}{2}$; to achieve this set $\lambda = \frac{\epsilon}{16dn}$ and $K = \lceil \frac{d}{2\lambda^2\sqrt{\epsilon}} \rceil$.

Now we return to the beginning, where we had to specify ϵ' and $\mathcal{F}'$. We can take $\epsilon' = \frac{\epsilon}{2}$, then $\|f_{\text{sml}}\|_2 \leq \|f'_{\text{sml}}\|_2 + \|f'_{\text{str}} - f_{\text{str}}\|_2 \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$. To choose $\mathcal{F}'$, let us first note that

$$K \leq \frac{d}{\lambda^2\sqrt{\epsilon}} = \frac{2^8 d^3 n^2}{\epsilon^{5/2}} \leq \frac{2^8 M^5}{\epsilon^{5/2}}.$$

The Lipschitz constant of F is then bounded by

$$4dK^{d+1} \leq 4M \left(\frac{2^8 M^5}{\epsilon^{5/2}}\right)^{M+1} =: a(M, \epsilon).$$

It is now enough to take $\mathcal{F}'(M) = \mathcal{F}(a(M, \epsilon))$ and $M_0 = M_0(\epsilon', \mathcal{F}')$ given by the previous version of the lemma. $\square$

Note that the assumption $p > p_0$ may be omitted, as for smaller p we can take $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}$ to be $\phi(x) = \frac{x}{p}$ and $F : \mathbb{T} \to [0,1]$ to be the piecewise linear extension of $f \circ \phi$:

$$F(t) = (\lfloor tp \rfloor + 1 - tp) f(\lfloor tp \rfloor) + (tp - \lfloor tp \rfloor) f(\lfloor tp \rfloor + 1).$$

This way $f_{\text{sml}} = f_{\text{unf}} = 0$ and F is p_0-Lipschitz.

Now the structure of f_{str} appears to be more natural, although we are still missing some information. We would like to know that the image of the homomorphism ϕ is well equidisributed in $\mathbb{T}^d$ so that we could expect that f_{str} has roughly the same global structure as F. To achieve this, let us set a notion of K-independence. The homomorphism $\phi = (\phi_1, \ldots, \phi_d)$ will be called K-independent if the only solution to the equation $k_1\phi_1 + \ldots + k_d\phi_d = 0$ with $|k_j| < K$ is $k_1 = \ldots = k_d = 0$. We will show how we can require independence, in particular what to do if ϕ turns out not to be independent.

Lemma 2.5.6. *Let $(a_1, \ldots a_d)$ be a vector with integer coordinates. There exists a matrix $A = [a_{ij}] \in \mathcal{M}_d(\mathbb{Z})$ with $a_{1j} = a_j$ (for $j = 1, \ldots, d$) and satisfying the following properties:*

$$\sum_{j=1}^{d} a_j a_{ij} = 0 \qquad \text{for } i = 2, \ldots, d,$$

$$\det A = \frac{\sum_{j=1}^{d} a_j^2}{\gcd(a_1, \ldots, a_d)}.$$

Moreover, if $\max\limits_{1 \le j \le d} |a_j| \le K$, then we can choose the entries of the matrix A to be bounded by K.

Proof. Let us prove the claim by induction on d. For $d = 1$ the statement is trivial. Suppose $d > 1$ and we have already proved it for $d - 1$. We would like to extend the matrix found for the vector $(a_1, \ldots, a_{d-1})$ to make it work for $(a_1, \ldots, a_d)$. Setting $a_{id} = 0$ for $i = 2, \ldots, d-1$ makes the first property satisfied for those values of i. Also, it makes the determinant quite easy to calculate by expanding it with respect to the last column. Since

$$\frac{\sum_{j=1}^{d} a_j^2}{\gcd(a_1, \ldots, a_d)} = \frac{\sum_{j=1}^{d-1} a_j^2}{\gcd(a_1, \ldots, a_{d-1})} \cdot \frac{\gcd(a_1, \ldots, a_{d-1})}{\gcd(a_1, \ldots, a_d)} + \frac{a_d^2}{\gcd(a_1, \ldots, a_d)},$$

it looks reasonable to set $a_{dd} = \frac{\gcd(a_1, \ldots, a_{d-1})}{\gcd(a_1, \ldots, a_d)} \in \mathbb{Z}$ and try to complete the last row so that the submatrix B obtained by deleting the first row and the last column has

determinant $\frac{(-1)^{d-1}a_d}{\gcd(a_1,\ldots,a_d)} \in \mathbb{Z}$. Note that the formula

$$\det B = \frac{(-1)^d \sum_{j=1}^{d-1} a_j a_{dj}}{\gcd(a_1, \ldots, a_{d-1})}$$

is true if we set $a_{dj} = a_{ij}$ for some $1 \leq i \leq d-1$ and all $j = 1, \ldots d-1$. Since the vectors $(a_{ij})_{j=1}^{d-1}$ span all of $\mathbb{R}^{d-1}$ (as the determinant of the matrix they form is non-zero by the inductive hypothesis), the formula above is in fact true for any choice of $a_{d,1}, \ldots, a_{d,d-1}$. This plays in our favour — if we insist that

$$0 = \sum_{j=1}^{d} a_j a_{dj} = \sum_{j=1}^{d-1} a_j a_{dj} + \frac{a_d \gcd(a_1, \ldots, a_{d-1})}{\gcd(a_1, \ldots, a_d)},$$

then automatically we have

$$\det A = a_{dd} \cdot \frac{\sum_{j=1}^{d-1} a_j^2}{\gcd(a_1, \ldots, a_{d-1})} + (-1)^{d-1} a_d \cdot \det B = \\ \frac{\sum_{j=1}^{d-1} a_j^2}{\gcd(a_1, \ldots, a_d)} - \frac{a_d \sum_{j=1}^{d-1} a_j a_{dj}}{\gcd(a_1, \ldots, a_{d-1})} = \frac{\sum_{j=1}^{d} a_j^2}{\gcd(a_1, \ldots, a_d)}.$$

So the only condition remaining is $\sum_{j=1}^{d-1} a_j a_{dj} = \frac{-a_d}{\gcd(a_1,\ldots,a_d)} \cdot \gcd(a_1, \ldots, a_{d-1})$. This can be satisifed by the Euclidean algorithm since $\frac{-a_d}{\gcd(a_1,\ldots,a_d)} \in \mathbb{Z}$, and thus we have proved the existence of the matrix A.

Now let us consider the bounds for the entries. Obviously if $|a_j| \leq K$, then $|a_{dd}| = \left|\frac{\gcd(a_1,\ldots,a_{d-1})}{\gcd(a_1,\ldots,a_d)}\right| \leq K$. Choosing the vector $(a_{d,1}, \ldots, a_{d,d-1})$ carefully might be a little bit more complicated. But if we write the equation in the form

$$\sum_{j=1}^{d-1} a_{dj} \cdot \frac{a_j}{\gcd(a_1, \ldots, a_{d-1})} = -\frac{a_d}{\gcd(a_1, \ldots, a_d)},$$

we can see that the claim boils down to the lemma below. □

Lemma 2.5.7. *Let $m, K > 0$ be integers and let $b_1, \ldots, b_m$ be coprime integers not exceeding K in absolute value. Let b be an integer with $|b| \leq K$. Then there exist integers $c_1, \ldots, c_m$ not exceeding K in absolutee value and satisfying*

$$b_1 c_1 + \ldots + b_m c_m = b.$$

This lemma is of well-known type, but for convenience we include the proof.

Proof. If $m = 1$, then $b_1 = \pm 1$ and the statement is trivial. For $m = 2$, if either of b_1, b_2 is equal to ± 1, the statement is trivial as well. If it is not the case, then without loss of generality we can assume $b_1 > b_2 > 0$. But then the numbers $b - kb_2$ for $|k| \leq K$ are at most Kb_1 in absolute value and at least one of them is a multiple of b_1, so the claim follows. Suppose now that $m > 2$ and we have already proven the claim for all smaller values of m. Let $g = \gcd(b_1, \ldots, b_{m-1})$. Then b_m and g are coprime and have absolute value at most K, so we can use the claim for $m = 2$ to get $gb' + b_m c_m = b$ with $|b'|, |c_m| \leq K$. Also the numbers $\frac{b_1}{g}, \ldots, \frac{b_{m-1}}{g}$ are coprime integers bounded by K in absolute value, which gives us $\frac{b_1}{g}c_1 + \ldots + \frac{b_{m-1}}{g}c_{m-1} = b'$ with $|c_1|, \ldots, |c_{m-1}| \leq K$. Combining those two identities we get the claim. □

Lemma 2.5.6 gives us the following corollary.

Corollary 2.5.8. Let $d > 1$ be an integer, let $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^d$ be a homomorphism and let $F : \mathbb{T}^d \to \mathbb{C}$ be an M-Lipschitz function. Then at least one of the following holds:

- ϕ is K-independent,
- there exits a homomorphism $\phi' : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^{d-1}$ and a dKM-Lipschitz function $F' : \mathbb{T}^{d-1} \to \mathbb{C}$ with $F' \circ \phi' = F \circ \phi$.

Proof. Suppose ϕ is not K-independent, i.e. there exist integers $a_1, \ldots, a_d$ satisfying $\sum_{j=1}^{d} a_j \phi_j = 0$ and $|a_j| < K$. It is not hard to see that the second part is true for $p \leq K$ as long as $d - 1 \geq 1$; suppose then $p > K$. In that case we are allowed to divide all of a_j by their greatest common divisor and without loss of generality assume $\gcd(a_1, \ldots, a_d) = 1$. By Lemma 2.5.6 we can find $d - 1$ integer vectors orthogonal to $a = (a_1, \ldots, a_d)$ such that the matrix A consisting of all of them has determinant $\sum_{j=1}^{d} a_j^2$. We claim that the $\mathbb{Z}$-span of these $d - 1$ vectors coincides with the intersection of their $\mathbb{R}$-span and $\mathbb{Z}^d$. Indeed, we know that the $\mathbb{Z}$-span of all d vectors is a subgroup of $\mathbb{Z}^d$ of index $\det A = \sum_{j=1}^{d} a_j^2$. On the other hand, the map $x \mapsto \langle a, x \rangle \pmod{\det A}$ gives rise to a surjective homomorphism from the quotient group to a group of size $\det A$. Therefore this homomorphism is in fact an isomorphism and its kernel is precisely the $\mathbb{Z}$-span of all d vectors. Intersecting it with the $\mathbb{R}$-span of the last $d - 1$ vectors obviously gives us their $\mathbb{Z}$-span. But this intersection can be easily seen as $\{x \in \mathbb{Z}^d : \langle a, x \rangle = 0\}$ or in other words the intersection of the $\mathbb{R}$-span and all of $\mathbb{Z}^d$.

Since $\gcd(a_1, \ldots, a_d) = 1$, it follows that the set $\{t \in \mathbb{T}^d : \langle a, t \rangle = 0 \in \mathbb{T}\}$ is in fact the image of the subspace $\{x \in \mathbb{R}^d : \langle a, x \rangle = 0 \in \mathbb{R}\}$ under the projection $\pmod{\mathbb{Z}^d}$.

Therefore it can be parametrized as $A'(\mathbb{T}^{d-1})$, where A' is $(d-1)\times d$ matrix obtained from A by deleting its first row $(a_1,\dots,a_n)$. Let $F':\mathbb{T}^{d-1}\to\mathbb{C}$ and $\phi':\mathbb{Z}/p\mathbb{Z}\to\mathbb{T}^{d-1}$ be functions satisfying $F'=F\circ A'$ and $\phi=A'\circ\phi'$. Note that ϕ' is well defined and is a homomorphism. Then

$$F'\circ\phi'=F\circ A'\circ\phi'=F\circ\phi.$$

The only thing left is to estimate the Lipschitz constant of F'. Since A' has entries bounded by K, it can be viewed as a dK-Lipschitz function. Composing it with an M-Lipschitz function F gives us a function of Lipschitz constant at most dKM. □

Now we are ready to give a proof of the full version of the regularity lemma (in the U^2 case).

Theorem 2.5.9 (arithmetic regularity lemma: final version)**.** *Let $\epsilon>0$ and let $\mathcal{F}$ be a growth function. Then there exists a real number $M_0=M_0(\epsilon,\mathcal{F})>0$ for which the following statement is true. Let p be a prime and $f:\mathbb{Z}/p\mathbb{Z}\to[0,1]$ be a function. Then there exists a number $0<M\le M_0$ and a decomposition*

$$f=f_{\mathrm{str}}+f_{\mathrm{sml}}+f_{\mathrm{unf}}$$

satisfying the following properties:

- *$f_{\mathrm{str}}=F\circ\phi$, where $\phi:\mathbb{Z}/p\mathbb{Z}\to\mathbb{T}^d$ is a $\mathcal{F}(M)$-independent homomorphism with $d\le M$ and $F:\mathbb{T}^d\to[0,1]$ is an M-Lipschitz function (f_{str} is structured),*
- *$\|f_{\mathrm{sml}}\|_2\le\epsilon$ (f_{sml} is small),*
- *$|\langle f_{\mathrm{unf}},\chi\rangle|\le\frac{1}{\mathcal{F}(M)}$ for every character χ (f_{unf} is U^2-uniform).*
- *f_{str} and $f_{\mathrm{str}}+f_{\mathrm{sml}}$ both take values in $[0,1]$.*

Proof. Let us start with applying the previous version of the regularity lemma with the same parameter ϵ and a different growth function $\mathcal{F}'$ to be specified. We stick to the obtained decomposition $f=f_{\mathrm{str}}+f_{\mathrm{sml}}+f_{\mathrm{unf}}$ but we would like to exploit more properties of F and ϕ. If ϕ is $\mathcal{F}$-independent, we are done. Otherwise we use Lemma 2.5.8 to decrease the dimension d by 1 at the cost of potentially increasing the Lipschitz constant up to $dM\mathcal{F}(M)\le M^2\mathcal{F}(M)$. Put $\mathcal{F}_1(M)=M^2\mathcal{F}(M)$; since this procedure can be applied at most $d\le M$ times, so the correct choice of $\mathcal{F}'$ is $\mathcal{F}'(M)=\mathcal{F}(\underbrace{\mathcal{F}_1(\dots(\mathcal{F}_1(M))\dots)}_{\lfloor M\rfloor\text{ times}})$. □

To make a proper use of the above result, we often need to relate the behaviours of f_{str} and F. Below we prove a statement of this kind. It is sometimes called a baby counting lemma.

Lemma 2.5.10. *Let d be a positive integer, p be a prime, let $\phi_1, \dots, \phi_d : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}$ be pre-characters and let $\phi = (\phi_1, \dots, \phi_d) : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^d$. Suppose that the set $\{\phi_j\}_{j=1}^d$ is K-independent. Let $F : \mathbb{T}^d \to \mathbb{C}$ be an M-Lipschitz function. Then*

$$\left| \mathbb{E}_x F(\phi(x)) - \int_{\mathbb{T}^d} F(t)dt \right| \leq \frac{M\sqrt{d}}{\sqrt{K}}.$$

One may wonder how we can manage to prove the above lemma without assuming that p is large. In fact, the K-independence of a set of d homomorphisms carries a hidden assumption $p \geq K^d$.

Proof. Let $\chi_j : \mathbb{T}^d \to \mathbb{C}$ defined via $\chi(t_1 \dots, t_d) = e^{2\pi i t_j}$ be the basic characters and let $\Phi_K : \mathbb{T}^d \to \mathbb{C}$ be the Fejér kernel defined via the formula

$$\Phi_K(t) = \frac{1}{K^d} \prod_{j=1}^{d} \left| \sum_{k=0}^{K-1} \chi_j^k(t) \right|^2.$$

Recall that $\int_{\mathbb{T}^d} \Phi_K(t)dt = 1$ and $\int_{[-\lambda,\lambda]^d} \Phi_K(t)dt \geq 1 - \frac{d}{4K\lambda^2}$ for any $\lambda \in (0, \frac{1}{2}]$. Having these inequalities we would like to show that $F(t)$ and $F * \Phi_K(t)$ are close together for any $t \in \mathbb{T}^d$. Let us estimate their difference:

$$|F(t) - F * \Phi_K(t)| = \left| \int_{\mathbb{T}^d} (F(t) - F(t-s))\Phi_K(s)ds \right| \leq M \int_{\mathbb{T}^d} \|s\|\Phi_K(s)ds.$$

This is already independent of t; now we would like to estimate the last quantity:

$$\int_{\mathbb{T}^d} \|s\|\Phi_K(s)ds = \int_{\mathbb{T}^d} \int_0^{1/2} 1_{\{\lambda \leq \|s\|\}} \Phi_K(s)d\lambda ds =$$
$$= \int_0^{1/2} \int_{\mathbb{T}^d} 1_{\{\lambda \leq \|s\|\}} \Phi_K(s)ds d\lambda \leq \int_0^{1/2} \min\left(1, \frac{d}{4K\lambda^2}\right) d\lambda \leq \sqrt{\frac{d}{K}},$$

and consequently $|F(t) - F * \Phi_K(t)| \leq \frac{M\sqrt{d}}{\sqrt{K}}$ for any $t \in \mathbb{T}^d$. In particular, the triangle inequality yields $|\mathbb{E}_x F(\phi(x)) - \mathbb{E}_x F * \Phi_K(\phi(x))| \leq \frac{M}{\sqrt{K}}$. Let us now expand the last expression:

$$\mathbb{E}_x F * \Phi_K(\phi(x)) = \mathbb{E}_x \left(\int_{\mathbb{T}^d} F(t)\Phi_K(\phi(x) - t)dt \right) =$$
$$= \int_{\mathbb{T}^d} F(t) \left(\mathbb{E}_x \Phi_K(\phi(x) - t) \right) dt.$$

Expanding out the formula for Φ_K, we can see that the average $\mathbb{E}_x\Phi_K(\phi(x)-t)$ is a sum of the averages of the form $c\cdot\mathbb{E}_x\chi(\phi(x)-t)$, where $\chi(t)=\prod_{j=1}^d\chi_j^{\alpha_j}$ for some $\alpha_1,\dots\alpha_j\in\{1-K,\dots,-1,0,1,\dots,K-1\}$. But from the K-independence of ϕ we can see that $\chi(\phi(x)-t)$ is never a constant function in x and therefore has average 0, unless χ is a trivial character with $\alpha_1=\ldots=\alpha_j=0$, in which case $c=1$. In the end, $\mathbb{E}_x\Phi_K(\phi(x)-t)=1$ for all $t\in\mathbb{T}^d$, which leads to $\mathbb{E}_xF*\Phi_K(\phi(x))=\int_{\mathbb{T}^d}F(t)dt$. Plugging this formula into the previous inequality, we get the desired result. □

The lemma above means that in fact independence of characters implies equidistribution of the image of ϕ inside the torus. One can make further use of this fact, here we will not do this.

We also need to know that the structured part does not correlate too much with the uniform part.

Lemma 2.5.11. *Let p be a prime and let d be a positive integer. Let $\phi:\mathbb{Z}/p\mathbb{Z}\to\mathbb{T}^d$ be a homomorphism and let $F:\mathbb{T}^d\to[0,1]$ be an M-Lipschitz function. Let $f=F\circ\phi$. Then for any function $g:\mathbb{Z}/p\mathbb{Z}\to[-1,1]$ we have*

$$|\langle f,g\rangle|\leq(M+d+1)\|\widehat{g}\|_\infty^{1/(3d+1)}.$$

Proof. Let K be a parameter and let $\Phi_K:\mathbb{T}^d\to[0,\infty)$ be the Fejér kernel defined as

$$\Phi_K(t)=\frac{1}{K^d}\prod_{j=1}^d\left|\sum_{k=0}^{K-1}\chi_j^k(t)\right|^2,$$

where $\chi_j:\mathbb{T}^d\to\mathbb{C}$ are the basic characters ($\chi_j(t)=e^{2\pi it_j}$). From Lemma 2.5.4 we know that $\int_{\mathbb{T}^d}\Phi_K(t)dt=1$ and $\int_{[-\lambda,\lambda]^d}\Phi_K(t)dt\geq1-\frac{d}{4K\lambda^2}$ for any $\lambda\in(0,\frac{1}{2}]$. Thererore for every $t\in\mathbb{T}^d$ we have

$$|F(t)-F*\Phi_K(t)|=\left|\int_{\mathbb{T}^d}(F(t)-F(t-t'))\Phi(t')dt'\right|\leq$$
$$\leq\int_{[-\lambda,\lambda]^d}\Phi(t')|(F(t)-F(t-t'))|dt'+\int_{\mathbb{T}^d\setminus[-\lambda,\lambda]^d}\Phi(t')|(F(t)-F(t-t'))|dt'\leq$$
$$\leq M\lambda+\frac{d}{4K\lambda^2}.$$

Now we can write $f=(F-F*\Phi_K)\circ\phi+(F*\Phi_K)\circ\phi$. The contribution from the first summand is bounded by

$$|\langle(F-F*\Phi_K)\circ\phi,g\rangle|\leq\|(F-F*\Phi_K)\circ\phi\|_2\|g\|_2\leq$$
$$\leq\|(F-F*\Phi_K)\circ\phi\|_\infty\|g\|_\infty\leq M\lambda+\frac{d}{4K\lambda^2}.$$

The second summand can be handled as follows:

$$|\langle (F * \Phi_K) \circ \phi, g\rangle| = |\langle \widehat{(F * \Phi_K)} \circ \phi, \widehat{g}\rangle| \leq \|\widehat{(F * \Phi_K)} \circ \phi\|_1 \|\widehat{g}\|_\infty.$$

Writing out $F * \Phi_K = \sum_i c_i \chi_i$ as the linear combination of characters, we see that $\chi_i \circ \phi$ are characters on $\mathbb{Z}/p\mathbb{Z}$. Therefore the ℓ^1 norm of $\widehat{(F * \Phi_K)} \circ \phi$ is bounded by that of $\widehat{(F * \Phi_K)}$ (might not be equal since composing with ϕ might make different characters the same). But $\|\widehat{(F * \Phi_K)}\|_1 = \|\widehat{F} \cdot \widehat{\Phi_K}\|_1 \leq \|\widehat{F}\|_\infty \|\widehat{\Phi_K}\|_1 \leq \|\widehat{\Phi_K}\|_1$. The last quantity can be easily calculated and is equal to K^d. In the end, $|\langle (F * \Phi_K) \circ \phi, g\rangle| \leq K^d \|\widehat{g}\|_\infty$. Putting two bounds together we get

$$|\langle f, g\rangle| \leq M\lambda + \frac{d}{4K\lambda^2} + K^d \|\widehat{g}\|_\infty.$$

Setting $K = \lfloor \|\widehat{g}\|_\infty^{-3/(3d+1)} \rfloor \geq \frac{1}{2}\|\widehat{g}\|_\infty^{-3/(3d+1)}$ and $\lambda = \|\widehat{g}\|_\infty^{1/(3d+1)}$ gives the desided bound. □

In this thesis we do not need the full version of the regularity lemma (the intermediate version is enough) or its consequences (such as Lemma 2.5.10). However, for completeness of presentation, we decided to include them here.

In this section we include one more result ([39, Lemma 4.20]), not directly related to the regularity lemma, but useful in dealing with the situation that the lemma produces.

Lemma 2.5.12. *Let G be an abelian group, let $d > 0$ be an integer and let $\phi : G \to \mathbb{T}^d$ be a homomorphism. Let $\beta \in (0, \frac{1}{2})$ and let $B = \{x \in G \ : \ \phi(x) \in [-\beta, \beta]^d\}$. Then $|B| \geq \beta^d |G|$.*

2.6 Freĭman's Theorem, homomorphisms and dimension

This section is devoted to elements of the theory of set addition developed by Freĭman in [16]. We follow [39, Section 5.5]; all the omitted proofs can be found there. We start with the following definitions.

Definition 2.6.1 (Freĭman homomorphism)**.** Let G, H be abelian groups, let $A \subset G, B \subset H$ be sets and let k be a positive integer. A map $\phi : A \to B$ is said to be a *Freĭman homomorphism of order k* if for every $a_1, \ldots, a_{2k} \in A$ with $\sum_{i=1}^k a_i = \sum_{j=k+1}^{2k} a_j$ we have $\sum_{i=1}^k \phi(a_i) = \sum_{j=k+1}^{2k} \phi(a_j)$. A *Freĭman homomorphism* is a shorthand for a Freĭman homomorphism of order 2. We call ϕ a *Freĭman isomorphism* if it has an inverse and both ϕ and ϕ^{-1} are Freĭman homomorphisms.

Definition 2.6.2 (universal ambient group)**.** Let G be an abelian group and let $A \subset G$ be a set. We call G a *universal ambient group* for A if for every abelian group H any Freĭman homomorphism $\phi : A \to H$ can be uniquely extended to a group homomorphism $\widetilde{\phi} : G \to H$. More generally, we call an abelian group G' a *universal ambient group* for A if there exists a set $A' \subset G'$ Freĭman isomorphic to A such that G' is its universal ambient group.

Observation 2.6.3. Every two universal ambient groups of a set A are isomorphic in a canonical way (i.e. this isomorphism restricts to a Freĭman isomorphism between the Freĭman isomorphic copies of A). Therefore we can talk about *the* universal ambient group of A.

Definition 2.6.4 (Freĭman dimension)**.** Let G be an abelian group and let $A \subset G$ be a finite set. The *Freĭman dimension* of A, denoted by $\dim_F A$, is the largest positive integer d such that $\mathbb{Z}^{d+1}$ is a quotient of the universal ambient group of A.

Example 2.6.5. Let $A = \{1, 2, 3, 4, 10\} \in \mathbb{Z}$, $B = \{0, 1, 2, 4, 8, 16, 32\} \in \mathbb{Z}$ and $C = \{0, 1, 2, 3\} \in \mathbb{Z}/5\mathbb{Z}$. Then the universal ambient group of A is $\mathbb{Z}^3$ and hence A is 2-dimensional. One of the embeddings verifying this fact is $x \mapsto (1, 0, x)$ for $x \in A \setminus 10\}$ and $10 \mapsto (1, 1, 0)$. The embedding of B into its universal ambient group is $B \hookrightarrow \{1\} \times B \subset \mathbb{Z}^2$, which makes B 1-dimensional. Similaly the embedding of C is $C \hookrightarrow \{1\} \times C \subset \mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})$ and so C is 0-dimensional.

Observation 2.6.6. Let G be an abelian group and let $A \subset G$ be a finite set. The space of Freĭman homomorphisms from A to $\mathbb{Z}$ is a group under pointwise addition and is isomorphic to $\mathbb{Z}^{\dim_F A+1}$.

Observation 2.6.7. Let $A \subset \mathbb{Z}$ be a finite set of Freĭman dimension d. There exists a Freĭman isomorphic copy $A' \subset \mathbb{Z}^d$ not contained in any coset of a proper subgroup.

Lemma 2.6.8 (Freĭman dimension lemma)**.** *Let $d > 0$ and let $A \subset \mathbb{Z}^d$ be a nonempty finite set. Suppose that A is not contained in any $d-1$ dimensional sublattice. Then*

$$|A + A| \geq (d + 1)|A| - \binom{d+1}{2}.$$

We will also need the following statement.

Theorem 2.6.9. *Let d be a positive integer and let $A \subset \mathbb{Z}^d$ be a set. Suppose that $\dim_F A = d$ and A affinely generates $\mathbb{Z}^d$. Suppose that $K \geq \frac{|A+A|}{|A|}$ is a real number. Then there exists a d-dimensional progression $P \subset \mathbb{Z}^d$ with $A \subset P$ and $\mathrm{size}(P) = |P| \leq F(K)|A|$ for some quantity $F(K)$ depending only on K.*

The above statement does not appear in the literature in this form, but its proof is very similar to the proof of [21, Theorem 3.2].

Before giving a proof, we extract all the necessary ingredients from [21].

Definition 2.6.10 (convex progression)**.** Suppose that $B \subset \mathbb{R}^d$ is a closed, centrally symmetric, convex body. If $B \cap \mathbb{Z}^d$ spans $\mathbb{R}^d$ as a vector space then we say that B is *full*. Suppose that B is full, and that $\phi : \mathbb{Z}^d \to \mathbb{Z}^m$ is a homomorphism. Then we refer to the image

$$X \coloneqq \phi(B \cap \mathbb{Z}^d)$$

as a *convex progression*. If $s > 1$ is some integer and if the restriction $\phi|_{sB\mathbb{Z}^d}$ is one-to-one, then we say that X is s-proper. The *size* of X is simply $\mathrm{size}(X) := |B \cap \mathbb{Z}^d|$, and the *volume* is $\mathrm{vol}(X) := \mathrm{vol}_d(B)$.

Lemma 2.6.11. *Suppose that $X \subset \mathbb{Z}^m$ is a convex progression of dimension d. Then there is an s-proper convex progression $X' \supset X$ of dimension $d' \leq d$, for which*

$$\mathrm{vol}(X') \leq s^d d! \,\mathrm{vol}(X).$$

Lemma 2.6.12 (Sections of round convex bodies)**.** *Suppose that $B \subset \mathbb{R}^m$ is a centrally symmetric convex body and that $B(0,\rho) \subset B$. Suppose that $H \subset \mathbb{R}^m$ is a subspace of dimension mr. Write $B' = B \cap H$. Then we have*

$$\mathrm{vol}_{mr}(B') \leq \frac{m!}{(mr)!\rho^r} \mathrm{vol}_m(B).$$

Theorem 2.6.13. *Suppose that $X = \phi(B \cap \mathbb{R}^d)$ is a convex progression. Let $t > 1$ be an integer. Then there is some $d' \leq d$ and a t-proper centred progression $P' \supset X$ of dimension d' which satisfies the estimate*

$$\mathrm{size}(P') \leq (2t)^d d^{6d^2} \mathrm{vol}(X).$$

We need one additional ingredient ([26, Theorem 2]; see [27] for the primary source).

Theorem 2.6.14 (John ellipsoid Theorem)**.** *Let K be a convex body in $\mathbb{R}^n$ which is symmetric about the origin. Then there is an ellipsoid E, also symmetric about the origin, so that $E \subset K \subset \sqrt{n}E$.*

Proof of Theorem 2.6.9. Let A be a set satisfying all the assumptions. By [33, Theorem 1.1] the conclusion is almost satisfied with the exception that instead of $\dim P = d$ we only know that $\dim P = O_K(1)$.

To fix that, note that for any $a \in A$ we have $A - a \subset P - P$ and $P - P$ is a convex progression of dimension $\dim P \leq O_K(1)$. By Lemma 2.6.11 there exists a 2-proper convex progression $X \subset P$ with $\mathrm{vol}(X) = O_K(\mathrm{vol}(P-P)) \leq O_K(\mathrm{size}(P)) \leq O_K(|A|)$. Write $X = \phi(B \subset \mathbb{Z}^{d'})$, where $\phi|_{2B \subset \mathbb{Z}^{d'}}$ is one-to-one. Then $\phi|_{2 \subset \mathbb{Z}^{d'}}$ is a Freĭman isomorphism and consequently $Y = \phi^{-1}(A - a)$ has Freĭman dimension $d = \dim_F A$. Therefore the linear dimension of Y is at most d. On the other hand, the linear dimension of Y is at least that of A — its homomorphic image. In the end we conclude that $\dim_F Y = \dim Y = d$, where by $\dim Y$ we understand the linear image of Y.

Let H be linear subspace generated by Y and let $B' = B \cap H$. We see that $\dim H = d$ and so $A - a \subset \phi(B')$ is covered by a convex progression of dimension d. We would like to estimate the volume of B'. To do this apply John's Theorem to the set B to conclude that there is an ellipsoid $E \subset B$ of volume $\mathrm{vol}_{d'}(E) = \Omega_K(\mathrm{vol}_{d'}(B))$. We can then apply a volume-preserving linear transformation so that E becomes a ball of radius $\rho = \Omega_K(\mathrm{vol}_{d'}(B)^{1/d'})$. Now apply Lemma 2.6.12 to get $\mathrm{vol}_d(B') = O_K(\mathrm{vol}_{d'}(B))$.

In the end apply Theorem 2.6.13 to get a generalized progression $P' \supset (B' \cap \mathbb{Z}^{d'})$ with $\mathrm{size}(P) = O_K(\mathrm{vol}_d(B')) \leq O_K(\mathrm{vol}_{d'}(B)) = O_K(\mathrm{vol}(X)) \leq O_K(A)$. We have $A - a \subset \phi(P')$ and also $\dim_P \leq d$. But $A - a$ is itself d-dimensional so in fact we have $\dim'_P = d$. In the end $a + \phi(P')$ is our desired progression. □

2.7 Results about $\mathbb{F}_2^n$

In this section we gather results about $\mathbb{F}_2^n$. We start with a finite field version of Freĭman's Theorem, proved by Ruzsa [34]. It is about subsets of groups with bounded torsion. We only need the case of $\mathbb{F}_2^n$, which goes as follows:

Theorem 2.7.1 (Ruzsa)**.** *Let $n > 0$ be an integer and let $K \geq 1$ be a real number. Suppose that $A \subset \mathbb{F}_2^n$ is a set with $|A + A| \leq K|A|$. Then A generates a subgroup of size at most $K^2 2^{K^4}|A|$.*

A version of the above theorem has recently been proven with tight bounds, see [12, 13].

Proposition 2.7.2. *Let $n \geq 0$ be an integer and let $S \subset \mathbb{F}_2^n$ be anonempty set. Then $|S| \leq 2^{\lfloor \log_2 |S+S| \rfloor}$.*

Proof. By Kneser's Theorem (Theorem 1.4.4) we know that $|S+S| \geq 2|S+H|-|H|$, where H is the subgroup of periods of $S+S$. Since H is a subgroup, we know that $|H| = 2^t$ for some integer $t \geq 0$. Let $k = \log_2 |S+S| \rfloor$. Then $|S+S| < 2^{k+1}$ and since it is a union of cosets of H, we have in fact $|S+S| \leq 2^{k+1} - 2^t$. Therefore we conclude that $|S| \leq |S+H| \leq \frac{1}{2}((2^{k+1}-2^t)+2^t) = 2^k$. □

Definition 2.7.3 (Gaussian binomial coefficients)**.** Let $n \geq 0$ be an integer. We define

$$n!_2 = \prod_{j=1}^{n}(2^j - 1).$$

If $0 \leq k \leq n$ are integers, write

$$\binom{n}{k}_2 = \frac{n!_2}{k!_2(n-k)!_2}.$$

The lemma below is quite standard; we include the proof for convenience.

Lemma 2.7.4. *Let $0 \leq k \leq n$ be integers. Then there are exactly $\binom{n}{k}_2$ k-dimensional subspaces of $\mathbb{F}_2^n$.*

Proof. First of all, let us count in how many ways we can write a sequence of k independent vectors. Having chosen j of them, the next one can be anything outside the subspace generated by the previous vectors, leaving us $2^n - 2^j$ choices. Altogether, the number of k-term sequences is $\prod_{j=0}^{k-1}(2^n - 2^j)$. Now let us count how many sequences generate a given subspace. This just corresponds to choosing a sequance of k independent vectors from a k-dimensional subspace; we can plug $n = k$ into the previous formula getting $\prod_{j=0}^{k-1}(2^k - 2^j)$. In the end, the numer of subspaces of dimension k is equal to

$$\frac{\prod_{j=0}^{k-1}(2^n - 2^j)}{\prod_{j=0}^{k-1}(2^k - 2^j)}.$$

Reducing j-th factors by 2^j gives

$$\frac{\prod_{j=0}^{k-1}(2^{n-j} - 1)}{\prod_{j=0}^{k-1}(2^{k-j} - 1)} = \frac{\prod_{j=n-k+1}^{n}(2^j - 1)}{\prod_{j=1}^{k}(2^j - 1)}.$$

The numerator of the last expression is just $\frac{n!_2}{(n-k)!_2}$ while the denominator is equal to $k!_2$. □

Observation 2.7.5. Let $0 \leq k \leq n$ be integers. We have the following inequalities:

$$1 \leq 2^{-k(n-k)}\binom{n}{k}_2 \leq \prod_{j=1}^{\infty}\frac{2^j}{2^j - 1} \leq 4.$$

The last inequality comes from the following calculation:

$$\prod_{j=1}^{\infty}(1-2^{-j}) \geq \frac{1}{2}\cdot\frac{3}{4}\cdot\left(1-\sum_{j=3}^{\infty}2^{-j}\right) = \frac{3}{8}\cdot\frac{3}{4} = \frac{9}{32} \geq \frac{1}{4}.$$

Chapter 3

A lower bound in the Balog-Szemerédi-Gowers Theorem

We start this chapter with a generalization of the additive energy to all sets of finite measure. For us, it will be convenient to abuse notation and denote $E(A) \coloneqq \frac{1}{|A|^3}|\{(a,b,c,d) \in A^4 \ : \ a+d=b+c\}|$. This way we always have $0 \leq E(A) \leq 1$. The formula we derived in the introduction becomes

$$E(A) = \frac{1}{|A|^3} \sum_{r \in G} |A \cap (r-A)|^2.$$

The equation above has the advantage of being easily generalizable to all compact subsets of locally compact abelian groups.

Definition 3.0.1. Let A be a compact subset of a locally compact abelian group G equipped with a Haar measure μ. The *additive energy* of the set A is the following quantity:

$$E(A) = \frac{1}{\mu(A)^3} \int_G (\mu(A \cap (x-A)))^2 d\mu(x).$$

Note that the above definition is invariant under multiplying the measure μ by any positive constant.

Now we would like to construca a set with large additive energy with no large subset of small doubling. As we mentioned, the base of our construction will be a high dimensional Euclidean ball. We use the above formula to estimate its additive energy. Then we prove that any dense subset of (a discrete approximation of) a ball is (in a certain sense) d-dimensional and therefore has doubling at least (close to) 2^d.

3.1 Additive energy of the Euclidean ball

This section is devoted to estimate the energy of the d-dimensional Euclidean ball. Specifically, if we denote this quantity by E_d, our aim is to show that $\lim_{d\to\infty} E_d^{1/d} = \frac{4}{3\sqrt{3}}$.

For the purpose of this chapter, let B^d be a d-dimensional ball and denote by V_d its (d-dimensional) volume and by S_{d-1} its ($(d-1)$-dimensional) surface area.

To use Definition 3.0.1, we need to examine the set $B^d \cap (x - B^d)$ for various choices of x. It is obviously empty if $\|x\| > 2$, otherwise it is just an intersection of two congruent balls, which is in other words a union of two "ball caps", symmetric with respect to the hyperplane containing their common base. Denote its volume by $V_d(\|x\|)$ (as it depends only on the distance from x to the origin). Although this shape is quite easy to visualize, it is much harder to compute precisely its volume. However we are interested only in limit of d-th root of the final answer, so we can allow ourselves to compute it up to a constant that would be sub-exponential (e.g. polynomial) in d. Let us extend this idea by thinking about shapes whose volumes are easier to compute. Namely, each "ball cap" contains a cone with the same base and top vertex and is itself contained in a cylinder with the same base and height. Recalling that the common base of those sets is a $(d-1)$-dimensional ball of radius $\sqrt{1-(\frac{s}{2})^2}$ (where $s = \|x\|$) and the height is equal to $1 - \frac{s}{2}$, we have the following inequalities:

$$\frac{2}{d}\left(1-\frac{s}{2}\right)\left(1-\left(\frac{s}{2}\right)\right)^{\frac{d-1}{2}} V_{d-1} \le V_d(s) \le 2\left(1-\frac{s}{2}\right)\left(1-\left(\frac{s}{2}\right)\right)^{\frac{d-1}{2}} V_{d-1},$$

where the factor $\frac{1}{d}$ on the left hand side comes from the integral $\int_0^1 t^{d-1}dt$ in the formula for the volume of the cone. We would like to get rid of V_{d-1} in the estimates; let us set $s = 0$ for a moment:

$$\frac{2V_{d-1}}{d} \le V_d \le 2V_{d-1},$$

or in other words $\frac{V_d}{2} \le V_{d-1} \le \frac{dV_d}{2}$. Combining these two inequalities we get

$$\frac{1}{d}\left(1-\frac{s}{2}\right)\left(1-\left(\frac{s}{2}\right)\right)^{\frac{d-1}{2}} V_d \le V_d(s) \le d\left(1-\frac{s}{2}\right)\left(1-\left(\frac{s}{2}\right)\right)^{\frac{d-1}{2}} V_d.$$

Note that the ratio of the bounds above is equal to d^2, which is negligible (having in mind that at the end we are taking the d-th root). Hence we can plug into the formula of additive energy any quantity that is between the bounds above, e.g. $\frac{1}{\sqrt{d}}\left(1-\frac{s}{2}\right)\left(1-\left(\frac{s}{2}\right)\right)^{\frac{d-1}{2}} V_d$. Note that this function is constant on any sphere centred

in the origin, so to calculate the final formula we need to multiply this one by the surface area of the sphere and integrate it with respect to the radius. So the final quantity we are interested in is the d-th root of

$$\frac{1}{V_d^3}\int_0^2 s^{d-1}S_{d-1}\left(\frac{1}{\sqrt{d}}\left(1-\frac{s}{2}\right)\left(1-\left(\frac{s}{2}\right)\right)^{\frac{d-1}{2}}V_d\right)^2 ds.$$

To estimate this, let us first put all the constants in front of the integral. We get $\frac{S_{d-1}V_d^2}{dV_d^3}=1$, since the volume of the ball can be calculated as the integral of the surface of the sphere: $V_d=\int_0^1 t^{d-1}S_{d-1}=\frac{S_{d-1}}{d}$. The remaining part is the following integral:

$$\int_0^2 s^{d-1}\left(1-\frac{s}{2}\right)^2\left(1-\frac{s^2}{4}\right)^{d-1}ds.$$

We will show that the d-th root of this expression tends to the maximum of the function $f(s)=s(1-\frac{s^2}{4})$ on the interval $[0,2]$, which happens to be equal to $\frac{4}{3\sqrt{3}}$ (for $s=\frac{2}{\sqrt{3}}$). We basically prove that the (weighted) L^d norm of f tends to its L^∞ norm. The upper bound can be easily obtained by estimating the integrand with $(\frac{4}{3\sqrt{3}})^{d-1}$ To get the lower bound, choose $\epsilon>0$ to be a small quantity. There is a neighbourhood U_ϵ of $\frac{2}{\sqrt{3}}$ such that $f\geq\frac{4}{3\sqrt{3}}-\epsilon$ on U_ϵ. Let $c_\epsilon=\int_{U_\epsilon}(1-\frac{s}{2})^2ds>0$. Then we can estimate

$$\int_0^2 s^{d-1}\left(1-\frac{s}{2}\right)^2\left(1-\frac{s^2}{4}\right)^{d-1}ds\geq$$
$$\geq\int_{U_\epsilon}\left(\frac{4}{3\sqrt{3}}-\epsilon\right)^{d-1}\left(1-\frac{s}{2}\right)^2=c_\epsilon\left(\frac{4}{3\sqrt{3}}-\epsilon\right)^{d-1}.$$

Taking the d-th root of this expression we get a lower bound of $\frac{4}{3\sqrt{3}}-\epsilon$. Since $\epsilon>0$ was arbitrary, we have finished the proof of the fact that $E_d^{1/d}\to\frac{4}{3\sqrt{3}}$ as $d\to\infty$.

3.2 Discrete approximation

In fact, to prove Proposition 1.5.7 we need a finite set, not a d-dimensional object. To deal with this, let us set

$$B_R^d=\{(x_1,\ldots,x_d)\in\mathbb{Z}^d\ :\ x_1^2+\ldots+x_d^2\leq R^2\}.$$

Our goal is to convince ourselves that $\lim_{R\to\infty}E(B_R^d)=E_d$ for any fixed d. To do this, we will first show that E_d is close to $E(B_R^d+[-\frac{1}{2},\frac{1}{2}]^d)$ (viewed in $\mathbb{R}^d$), which is on the other hand close to $E(B_R^d)$. To estimate the first quantity, let us note that

since every point of the cube $[-\frac{1}{2},\frac{1}{2}]$ has distance at most $\frac{\sqrt{d}}{2}$ from the origin, we have the relations

$$\left(R-\tfrac{\sqrt{d}}{2}\right)B^d \subset B_R^d + \left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d \subset \left(R+\tfrac{\sqrt{d}}{2}\right)B^d.$$

The inclusions above are preserved both by translations and taking intersections, so plugging the corresponding inequalities of measure into the definition of additive energy we get

$$\left(\frac{R-\frac{\sqrt{d}}{2}}{R+\frac{\sqrt{d}}{2}}\right)^3 \leq \frac{E(B_R^d+[-\frac{1}{2},\frac{1}{2}]^d)}{E_d} \leq \left(\frac{R+\frac{\sqrt{d}}{2}}{R-\frac{\sqrt{d}}{2}}\right)^3.$$

The bounds above both go to 1 as $R\to\infty$.

Now we focus on the distance between $E(B_R^d+[-\frac{1}{2},\frac{1}{2}]^d)$ and $E(B_R^d)$. Note that the cube $[-\frac{1}{2},\frac{1}{2}]^d$ was chosen so that

$$|B_R^d \cap (x-B_R^d)| = \mu\left(\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\cap\left(x-\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\right)\right)$$

whenever $x\in\mathbb{Z}^n$ (here and onwards, μ denotes the d-dimensional Haar measure). On the other hand, since the projection of $B_R^d+[-\frac{1}{2},\frac{1}{2}]^d$ along each axis is contained in the cube $[-R-\frac{1}{2},R+\frac{1}{2}]^{d-1}$, we have

$$\mu\left(\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\triangle\left(y+\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\right)\right)\leq 2t(2R+1)^{d-1},$$

where $y=(t,0,\ldots,0)\in\mathbb{R}^d$. Now if $y\in[-\frac{1}{2},\frac{1}{2}]^d$, this estimate together with triangle inequality gives us

$$\mu\left(\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\triangle\left(y+\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\right)\right)\leq d(2R+1)^{d-1}.$$

Taking a suitable translation and intersection leads us to the conclusion that replacing an arbitrary point x in the expression

$$\mu\left(\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\cap\left(x-\left(B_R^d+\left[-\tfrac{1}{2},\tfrac{1}{2}\right]^d\right)\right)\right)$$

with the nearest point in $\mathbb{Z}^d$ can lead to an error of at most $d(2R+1)^{d-1}$. Also, the above expression is trivially bounded by $(2R+1)^d$. Now by the inequality $|a^2-b^2|\leq(|a|+|b|)|a-b|$, replacing x in the *square* of the above expression with the nearest point in $\mathbb{Z}^d$ gives an error of at most $2d(2R+1)^{2d-1}$. Integrating this over the set $2(B_R^d+[-\frac{1}{2},\frac{1}{2}]^d)$ leads to an error of at most $2^{d+1}d(2R+1)^{3d-1}$, which is negligible (for large R) when compared $|B_R^d|^3=\mu(B_R^d+[-\frac{1}{2},\frac{1}{2}]^d)^3$, which is at least $V_d^3(R-\frac{\sqrt{d}}{2})^{3d}$. Thus we have proven that $\lim_{R\to\infty}E(B_R^d)=E_d$ for any fixed d.

3.3 Doubling constants of d-dimensional sets

In this section we examine the possible values of the doubling constant of a subset of $\mathbb{Z}^d$ that looks somewhat "d-dimensional" in an appropriate sense. Note that for any genuinely d-dimensional set $A \subset \mathbb{R}^d$ the set $A + A$ contains the dilation $2 \cdot A$, which has volume 2^d times as large as this of A. We would like to have something along those lines for discrete sets. Unfortunately, in this case $|2 \cdot A| = |A|$, so we need to be a little bit more subtle. Note that not all the subsets of $\mathbb{Z}^d$ of positive measure "look" d-dimensional, e.g. we have the "line segment" $\{(k, 0, \ldots, 0) \ : 0 \leq k \leq n\}$. For us, a set will be d-dimensional, if the projections along all the axes are significantly smaller than the set itself. We will not state the precise definition, as matters should be clear from the next lemma. Before we state it, let us write $\pi_i : \mathbb{Z}^d \to \mathbb{Z}^{d-1}$ for the projection along the i-th axis.

Lemma 3.3.1. *For any finite set $A \subset \mathbb{Z}^d$ the following inequality holds:*

$$|A \pm A| \geq 2^d \left(|A| - \sum_{i=1}^{d} |\pi_i(A)| \right).$$

The idea of the proof is to compress the set A on one hand to reduce its doubling constant and on the other hand to make it easier to calculate it. Define a compression along the i-th axis or an i-compression in the following way:

$$C_i(A) = \{x \in \mathbb{Z}^d \ : \ 0 \leq x_i < |\pi_i^{-1}(\pi_i(x)) \cap A|\}$$

In other words, we compress each fibre of A with respect to π_i to make it a segment starting at 0. Compressions in combinatorics were known as early as 1991 (see [5]). A paper definitely worth looking is [20]. Both the statement and the proof of Lemma 3.3.1 are very similar to those of [20, Lemma 2.8]

We call a set i-compressed if it is equal to its i-compression. Before we start proving the lemma above, we need the following properties of compressions.

Lemma 3.3.2. *Compressions, defined as above, satisfy the following properties (for any finite sets $A, B \subset \mathbb{Z}^d$ and any $i, j \in \{1, \ldots, d\}$):*

- $|A| = |C_i(A)|$,
- $|A + B| \geq |C_i(A) + C_i(B)|$,
- *the j-compression of an i-compressed set is again i-compressed,*

- $|\pi_j(A)| \geq |\pi_j(C_i(A))|$.

Proof. The first property follows from the fact that each fibre of A with respect to π_i has the same size as that of $C_i(A)$.

For the second statement, a fibre $(C_i(A)+C_i(B))\cap\pi_i^{-1}(u)$ is the union of the sets $(C_i(A)\cap\pi_i^{-1}(v))+(C_i(B)\cap\pi_i^{-1}(u-v))$ for various $v\in\mathbb{Z}^{d-1}$, each of which being a sum of two segments starting at 0, which is again a segment starting at 0. There is some $v\in\mathbb{Z}^{d-1}$ for which this segment is maximal and therefore equal to the entire union, in other words $(C_i(A)+C_i(B))\cap\pi_i^{-1}(u) = (C_i(A)\cap\pi_i^{-1}(v))+(C_i(B)\cap\pi_i^{-1}(u-v))$ for some v. This allows us to write

$$\begin{aligned}|(A+B)\cap\pi_i^{-1}(u)| &\geq |(A\cap\pi_i^{-1}(v))+(B\cap\pi_i^{-1}(v-u))| \geq \\ &\geq |A\cap\pi_i^{-1}(v)|+|B\cap\pi_i^{-1}(v-u)|-1 = \\ &= |C_i(A)\cap\pi_i^{-1}(v)|+|C_i(B)\cap\pi_i^{-1}(u-v)|-1 = |(C_i(A)+C_i(B))\cap\pi_i^{-1}(u)|.\end{aligned}$$

Here we used the fact that $|S_1+S_2|\geq|S_1|+|S_2|-1$ for any two finite sets $S_1,S_2\subset\mathbb{Z}$. Summing the above for all $u\in\mathbb{Z}^{d-1}$ we get the claim.

The third statement can be proven by examining the sets on which all coordinates except i-th and j-th are fixed. Therefore wihout loss of generality we can assume $d=2$, $i=1$, $j=2$. In this case the notion of being 1-compressed is precisely the condition that $(x_1,x_2)\in A$ implies $x_1\geq 0$ and $(x_1',x_2)\in A$ for any $0\leq x_1'\leq x_1$. This means that there are at least as many points with first coordinate x_1' as x_1. Since $(x_1,x_2)\in C_2(A)$ holds precisely when $x_2\geq 0$ and there are at least x_2+1 points with first coordinate x_1 in A, the above condition translates into $(x_1,x_2)\in C_2(A)\Rightarrow(x_1',x_2)\in C_2(A)$ which means exactly that $C_2(A)$ is 1-compressed.

For the last statement we can also assume $d=2$, $i=1$, $j=2$. Then π_2 by definition is a projection onto the first coordinate and by construction $\pi_2(C_1(A)) = \{0,\ldots,n-1\}$ for some n. It follows that $(n-1,x_2)\in C_1(A)$ for some x_2 and so A contains n points with the second coordinate x_2. All of them have distinct images and hence $|\pi_2(A)|\geq n = |\pi_2(C_1(A))|$. □

We are ready to deal with the case of $A+A$; to handle $A-A$ we need the following lemma.

Lemma 3.3.3. *Let $A\subset\mathbb{Z}^d$ be a finite set. Then*

$$C_1(\ldots(C_d(A))\ldots) = C_1(\ldots(C_d(-A))\ldots).$$

Proof. We prove by induction that $(x_1, \ldots, x_d) \in C_{j+1}(\ldots(C_d(A))\ldots)$ if and only if $(-x_1, \ldots, -x_j, x_{j+1}, \ldots, x_d) \in C_{j+1}(\ldots(C_d(-A))\ldots)$. The claim is obviously true for $j = d$. To go from j to $j-1$, denote $B = C_{j+1}(\ldots(C_d(A))\ldots)$ and let $P_j : \mathbb{Z}^d \to \mathbb{Z}^d$ be the reflection about the origin in the first j coordinates. The compression C_j applied to the sets B and $P_j(B)$ acts separately on each fibre of π_j. The corresponding fibres $B \cap \pi_j^{-1}(\pi_j(u))$ and $P_j(B) \cap \pi_j^{-1}(\pi_j(P_j(u)))$ are negatives of each other (viewed as subsets of $\mathbb{Z}$), after applying C_j they become the same. It follows that $P_{j-1}(C_j(B)) = C_j(P_j(B))$, as claimed.

Applying the claim to $j = 0$ proves the lemma. □

Proof of Lemma 3.3.1. By the properties of compressions the inequality for an arbitrary set A follows from the inequality for a set $C = C_1(\ldots(C_d(A))\ldots)$, which is an i-compressed set for each i. But for the set C observe that each $x \in C$ with all non-zero coordinates gives rise to 2^d elements of $C + C$, namely $2x - v$ for $v \in \{0, 1\}^d$ (since $x - v$ is also in C). Therefore $|C + C| \geq 2^d |C'|$, where C' is a set of points of C with all non-zero coordinates, with size bounded below by $|C| - \sum_{i=1}^d |\pi_i(C)|$, as $|\pi_i(C)|$ is precisely the number of points of C with i-th coordinate 0. Putting everything together we get

$$|A \pm A| \geq |C + C| \geq 2^d \left(|C| - \sum_{i=1}^d |\pi_i(C)| \right) \geq 2^d \left(|A| - \sum_{i=1}^d |\pi_i(A)| \right).$$

□

3.4 Conclusion

Now we are ready to prove the main result of this chapter.

Proof of Proposition 1.5.7. Fix $C < \frac{\log 2}{\log \frac{3\sqrt{3}}{4}}$ as above. By the inequality we can find $\alpha > \frac{3\sqrt{3}}{4}$ and $\beta < 2$ with $\beta > \alpha^C$. For d large enough we have $\beta^d > M \cdot \alpha^{Cd}$ and $E_d > \alpha^{-d}$. Fix d for which both inequalities hold. We know that for R large enough we have $E(B_R^d) > \alpha^{-d}$. Set $K = \alpha^d$ and let $A = B_R^d$ for R sufficiently large depending on $f(K)$. Any subset $A' \subset A$ with $|A'| \geq \frac{|A|}{f(K)}$ is d-dimensional in the sense that we need; indeed, $\sum_{i=1}^d |\pi_i(A')| \leq d(2R+1)^{d-1}$ while $|A'| \geq \frac{1}{f(K)} V_d(R - \frac{\sqrt{d}}{2})^d$. Therefore for R large enough $|A' + A'| \geq \beta^d |A'| > M \cdot \alpha^{Cd} |A'| = M \cdot K^C |A'|$ for any subset $A' \subset A$ satisfying $|A'| \geq \frac{|A|}{f(K)}$. □

3.5 Further comments

One may wonder why we chose to work with the Euclidean ball rather than any other shape. The reason is that it has the largest additive energy among all the subsets of $\mathbb{R}^d$ (see [37, Proposition 2.3]). Indeed, for any subset of $\mathbb{R}^d$ satisfying some mild regularity conditions we could apply Lemma 3.3.1, and for a fixed doubling constant large additive energy gives large exponent in Proposition 1.5.7.

The constant $\frac{3\sqrt{3}}{4}$ appears also in the Young's inequality for convolution over real vector spaces (see [2, 3, 6, 14]).

We suspect that the exponent $\frac{\log 2}{\log \frac{3\sqrt{3}}{4}}$ is the best possible. In fact, in the light of the Green-Tao regularity lemma, one could hope to transform an arbitrary set into a set in (or more precisely: a function on) $\mathbb{T}^{d'}$ for some possibly very large d'. This already looks more geometric than additive combinatorial; the downside is that the geometry takes place in a torus rather than a real vector space. A hope would be, given a set $A \subset \mathbb{T}^{d'}$ with no dense subset of doubling less than 2^d, to be able to compress it into a set Freĭman isomorphic to a subset of $\mathbb{R}^d \times \mathbb{T}^{d'-d}$ and then apply methods from this chapter. Let us illustrate it with an example.

Example 3.5.1. Let $A \subset \mathbb{T}$ be a set satisfying $\mu(A+A) > 2\mu(A)$. Let $C(A) = \{t \in \mathbb{T} \ : \ |t| \leq \frac{1}{2}\mu(A)\}$ be the compression of A. Then $2\mu(A) < \mu(A+A) \leq 1$, which implies $C(A) \subset [-\frac{1}{4}, \frac{1}{4}]$ and therefore $C(A)$ is Freĭman isomorphic to a subset of $\mathbb{R}$. It can be also checked that the compression can only increase the additive energy, which leads to $E(A) \leq E(C(A)) \leq \frac{2}{3}$.

Unfortunately this strategy in general looks somewhat similar to the isoperimetric problem on the torus, at the moment considered very hard. We were unable to push it much further than the example above.

Chapter 4

Sets with small popular doubling

In this chapter we develop the theory of sets with small popular doubling. As explained in section 1.6, the quantity we are interested in is the average size of the set of k-popular sums for $k = 1, \dots, t$. Note that by definition of convolution, if G is an abelian group and $A, B \subset G$ are finite sets, then the element $x \in G$ can be expressed in exactly $1_A * 1_B(x)$ ways as a sum $x = a + b$ with $a \in A$, $b \in B$. The sum $\sum_{k=1}^{t} N_k$ that appears in the statements of Theorems 1.6.3 and 1.6.4 can be then rearranged as

$$\begin{aligned}\sum_{k=1}^{t} N_k = \sum_{k=1}^{t} |\{x \in G \ : \ 1_A * 1_B(x) \geq k\}| = \\ = |\{(x,k) \in G \times \{1,\dots,t\} \ : \ 1_A * 1_B(x) \geq k\}| = \\ = \sum_{x \in G} |\{k \in \{1,\dots,t\} \ : \ k \leq 1_A * 1_B(x)\}| = \sum_{x \in G} \min(1_A * 1_B(x), t).\end{aligned}$$

From now on we are interested only in the expression above. We shall show that this being small is strongly connected with the algebraic structure of A and B.

4.1 Subsets of abelian groups

In this section we deal with subsets of any abelian group. We also drop the assumption that $t \in \mathbb{Z}$, allowing t to be any positive real number instead. We first have two easy results to prove; let us start with some observations.

Observation 4.1.1. Let G be an abelian group and let $A, B \subset G$ be finite sets. The function $(0, +\infty) \ni t \mapsto \sum_{x \in G} \min(1_A * 1_B(x), t) \in [0, +\infty)$ is concave.

Proof. The function $t \mapsto \min(1_A * 1_B(x), t)$ is concave for each individual $x \in G$, so their sum also is. □

Observation 4.1.2. Let $t \in (0,1]$, G be an abelian group and let $A, B \subset G$ be finite sets. Then

$$\sum_{x \in G} \min(1_A * 1_B(x), t) = t|A+B|.$$

Proof. For $x \in A+B$ we have $1_A * 1_B(x) \geq 1 \geq t$ and so $\min(1_A * 1_B(x), t) = t$; otherwise $1_A * 1_B(x) = 0$ and $\min(1_A * 1_B(x), t) = 0$. □

Proposition 1.6.5. *Let $t > 0$, G be an abelian group and let $A, B \subset G$ be finite sets of size at least t. Then*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) \geq t \cdot \max(|A|, |B|).$$

Proof. For $t' = \min(|A|, |B|)$ and any $x \in G$ we have $1_A * 1_B(x) = |A \cap (x - B)| \leq t'$ and consequently $\sum_{x \in G} \min(1_A * 1_B(x), t') = \sum_{x \in G} 1_A * 1_B(x) = |A| \cdot |B| = t' \cdot \max(|A|, |B|)$. Therefore by concavity

$$\sum_{x \in G} \min(1_A * 1_B(x), t) \geq$$
$$\geq \frac{t}{t'} \sum_{x \in G} \min(1_A * 1_B(x), t') + \frac{t' - t}{t'} \sum_{x \in G} \min(1_A * 1_B(x), 0) =$$
$$= t \cdot \max(|A|, |B|).$$

□

Proposition 1.6.6. *Let $t > 0$, G be an abelian group and let $A, B \subset G$ be finite sets of size at least t. Suppose that $|A| \leq |B|$. Then*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) = t|B|$$

if and only if one at least of the following conditions holds:

(a) $|A| = t$,

(b) B is a union of cosets of the subgroup generated by $A - A$.

Proof. For the "if" part, if $|A| = t$, then $1_A * 1_B \leq t$ and consequently

$$\sum_{x \in G} \min(1_A * 1_B(x), t) = \sum_{x \in G} 1_A * 1_B(x) = |A| \cdot |B| = t|B|.$$

If the second condition holds, then the equation $\sum_{x \in G} \min(1_A * 1_B(x), t) = t|B|$ is satisfied for $t = 1$ by Proposition 1.4.1. It also holds for $t = 0$ and $t = |A|$, so by

concavity it is satisfied for *all* values $t \in [0, |A|]$, in particular for our desired value of t.

Conversely, if $t < |A|$, then the equation $\sum_{x \in G} \min(1_A * 1_B(x), t) = t|B|$ is satisfied for $t = 0$, $t = |A|$ and at least one intermediate value of t. Again, by concavity it is satisfied for all values $t \in [0, |A|]$, in particular for $t = 1$. It means that $|A + B| = |B|$ and we can use Proposition 1.4.1. □

We know about the minimum of $\sum_{x \in G} \min(1_A * 1_B(x), t)$ and which sets achieve it. The only task left in this section is to find all sets for which it is near-minimal. Ideally, we would like to cover such a set with a coset of a subgroup whose size only slightly exceeds the size of the original set. However, this example shows that this is impossible.

Example 4.1.3. Let G be an abelian group and let $A = \{0\} \times G \cup \{(1, 0)\} \subset \mathbb{Z} \times G$. Then

$$1_A * 1_A(x, y) = \begin{cases} |G|, & x = 0, \\ 2, & x = 1, \\ 1, & x = 2 \text{ and } y = 0, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if $2 \leq t \leq |G|$, then $\sum_{x \in G} \min(1_A * 1_B(x), t) = |G|(t + 2) + 1 = (1 + \frac{2|G| - t + 1}{(|G|+1)t})|A|t \leq (1 + \frac{2}{t})|A|t$. Note that $\frac{2}{t}$ can be made arbitrarily small, yet A cannot be covered by a coset of a finite subgroup.

The above example shows that we have to allow a small number of points, like $(1, 0)$ to lie outside our coset. Therefore we prove the following statement, based on Proposition 1.4.2. Again, we prove a version for two sets of the same size to deal with the pairs of sets (A, A) and $(A, -A)$ at the same time.

Theorem 1.6.7. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Let $t, \delta > 0$ be two real numbers satisfying the inequality $\delta + \frac{t}{N} \leq \frac{1}{2}$. Moreover suppose that the following inequality holds:*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) \leq (1 + \delta)Nt.$$

Then there exists a subgroup $H \leq G$ and cosets C_A and C_B of H satisfying the following conditions:

- $|H| \leq (1 + \delta)N$,
- $|A \setminus C_A| + |B \setminus C_B| \leq t$.

For convenience we split the proof of the above result into several lemmas. First of all we want to find the subgroup H. Although the statement of the following lemma appears to be new in the literature, the methods that go into the proof were already used in [14].

Lemma 4.1.4. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Let $t, \delta > 0$ be two real numbers satisfying the inequality $\delta + \frac{t}{N} \leq \frac{1}{2}$. Moreover suppose that the following inequality holds:*

$$\sum_{x \in G} \min(1_A * 1_B(x), t) \leq (1+\delta)Nt.$$

Then there exists a subgroup $H \leq G$ satisfying the following conditions:

- $1_A * 1_{-A}(x) \geq (1-\delta)N$ *and* $1_B * 1_{-B}(x) \geq (1-\delta)N$ *for all* $x \in H$,
- $1_A * 1_{-A}(x) < 2t$ *and* $1_B * 1_{-B}(x) < 2t$ *for all* $x \in G \setminus H$.

Before we proceed, observe that the triangle inequality for symmetric difference of sets $|V \triangle W| \leq |U \triangle V| + |U \triangle W|$ can be rearranged as $|U \cap V| + |U \cap W| \leq |U| + |V \cap W|$. We will frequently use a variant of this inequality, namely the assertion that $|U \cap (V - v)| + |U \cap (W - w)| \leq |U| + |V \cap (W - w + v)|$ for arbitrary elements v, w. We will refer to all statements of this kind as the triangle inequality.

Proof. Let us start with the set of popular sums $D = \{x \in G : 1_A * 1_B(x) \geq t\}$. Note that D contains most of the sums $a + b$; more precisely we have

$$\begin{aligned}\#\{(a,b) \in A \times B : a+b \in D\} &= \sum_{x \in D} 1_A * 1_B(x) = \\ &= \sum_{x \in D} t + \sum_{x \in G} \max(1_A * 1_B(x) - t, 0) = \\ &= t|D| + \sum_{x \in G} 1_A * 1_B(x) - \sum_{x \in G} \min(1_A * 1_B(x), t) \geq t|D| + N^2 - (1+\delta)Nt.\end{aligned}$$

Now let $H = \{x \in G : 1_A * 1_{-A}(x) \geq 2t\}$. We would like to show that for any $h \in H$ we have $1_B * 1_{-B}(h) \geq (1-\delta)N$. Let us start by noticing that for any $a \in G$ we have

$$|B \cap (B+h)| \geq |(B+a) \cap D| + |(B+a+h) \cap D| - |D|$$

by triangle inequality. Now let $w : G \to [0,1]$ be a weight function supported on $A \cap (A+h)$ and satisfying the condition $\sum_{x \in G} w(x) = 2t$ (there exists one by the choice of h). Multiplying the above inequality by $w(a)$ and summing over a we get

$$2t|B \cap (B+h)| \geq \sum_{a \in A} (w(a) + w(a-h))|(B+a) \cap D| - 2t|D|.$$

Now we combine the inequalities

$$\sum_{a\in A} 2|(B+a)\cap D| \geq 2t|D| + 2N^2 - 2(1+\delta)Nt,$$

$$\sum_{a\in A}(2-w(a)-w(a-h))|(B+a)\cap D| \leq |B|\sum_{a\in A}(2-w(a)-w(a-h)) =$$
$$= N(2N-4t)$$

to get

$$|B\cap(B+h)| \geq \frac{2t|D| + 2N^2 - 2(1+\delta)Nt - (2N^2-4Nt) - 2t|D|}{2t} = (1-\delta)N.$$

In similar way we can prove that the inequality $1_B * 1_{-B}(x) \geq 2t$ implies $1_A * 1_{-A}(x) \geq (1-\delta)N$ for any $x \in G$. Since $(1-\delta)N \geq 2t$, we have just constructed the set H satisfying all the postulated inequalities. The only thing remaining is to show that H is a subgroup. This follows from triangle inequality: if $h_1, h_2 \in H$, then

$$|A\cap(A+h_1-h_2)| \geq |A\cap(A+h_1)| + |A\cap(A+h_2)| - |A| \geq$$
$$\geq 2(1-\delta)N - N = (1-2\delta)N \geq 2t$$

and consequently $h_1 - h_2 \in H$. Also $0 \in H$ because $1_A * 1_{-A}(0) = N \geq 2t$. □

We have already constructed a set D containing most of the sums $a+b$ and the subgroup H satisfying certain inequalities. Now it is time to construct a *coset* C of H containing most of the sums $a+b$. We will do it in two steps: first we show that C contains just enough sums to perform calculations quite accurately, which in turn will give us the cosets C_A and C_B with desired properties.

Lemma 4.1.5. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Let $t, \delta > 0$ be two real numbers satisfying the inequality $\delta + \frac{t}{N} \leq \frac{1}{2}$. Moreover suppose that the following inequality holds:*

$$\sum_{x\in G} \min(1_A * 1_B(x), t) \leq (1+\delta)Nt.$$

Then there exists a coset C of a subgroup H satisfying $|C| \leq (1+\delta)N$ and

$$\#\{(a,b)\in A\times B : a+b\in C\} > \frac{(1+\delta)N^2}{2}.$$

Proof. Let H be the subgroup constructed in Lemma 4.1.4. We want to translate H to make it contain most of the sums $a+b$, so a reasonable choice is to take $x_0 \in G$

for which $1_A * 1_B(x_0)$ is maximal and set $C = H + x_0$. Let $k = N - 1_A * 1_B(x_0)$. Note that by concavity for any $t' \in [t, \frac{N}{1+\delta})$ we have $\sum_{x\in G} \min(1_A * 1_B(x), t') \leq \frac{t'}{t} \min(1_A * 1_B(x), t) < N^2 = \sum_{x\in G} 1_A * 1_B(x)$, which implies $1_A * 1_B(x_0) \geq \frac{N}{1+\delta}$ or in other words $k \leq \frac{\delta N}{1+\delta}$. Moreover, by triangle inequality we have $|1_A * 1_B(x + x_0) - 1_A * 1_{-A}(x)| \leq k$; in particular C contains the set $C' = \{x \in G \ : 1_A * 1_B(x) \geq 2t + k\}$. Therefore we are interested in the size of the set $\#\{(a, b) \in A \times B : a + b \in C'\}$. By the same calculations as for the set D in the proof of the Lemma 4.1.4 we know that

$$\#\{(a, b) \in A \times B : a + b \in C'\} \geq N^2 - (1 + \delta)N(2t + k) + (2t + k)|C'|.$$

Here we have also used here the previous corollary with $t' = 2t + k$. Let us bound the size of C' from below. We know that

$$\begin{aligned} N^2 = \sum_{x\in G} 1_A * 1_B(x) = \\ = \sum_{x\in G} \min(1_A * 1_B(x), 2t + k) + \sum_{x\in C'} (1_A * 1_B(x) - (2t + k)) \leq \\ \leq (1 + \delta)N(2t + k) + |C'|(N - 2t - 2k), \end{aligned}$$

which rearranges to $|C'| \geq \frac{N(N-(1+\delta)(2t+k))}{N-2t-2k}$. Substituting this into the previous bound we get

$$\#\{(a, b) \in A \times B : a + b \in C'\} \geq N^2 - \frac{N(2t + k)(\delta N - (1 + \delta)k)}{N - 2t - 2k}.$$

It is easy to check that the expression on the right hand side is a decreasing function in t, so we can substitute $t = (\frac{1}{2} - \delta)N$ to get

$$\#\{(a, b) \in A \times B : a + b \in C'\} \geq N^2 - \frac{N((1 - 2\delta)N + k)(\delta N - (1 + \delta)k)}{2(\delta N - k)}.$$

Now it is also easy to check that this being greater than $\frac{1+\delta}{2}N^2$ is equivalent to the inequality $(\delta N - k)^2 + (1 - 2\delta)\delta Nk + \delta k^2 > 0$, which is true because we assumed $\delta > 0$.

Now we only need to bound the size of C; because of triangle inequality it is contained in the set $C'' = \{x \in G : 1_A * 1_B(x) \geq (1 - \delta)N - k\}$, so using the corollary with $t' = (1 - \delta)N - k > t$ we get

$$\begin{aligned} t'|C| \leq t'|C''| = \sum_{x\in C''} \min(1_A * 1_B(x), t') \leq \\ \leq \sum_{x\in G} \min(1_A * 1_B(x), t') \leq (1 + \delta)Nt'. \end{aligned}$$

Thus we have proved both desired inequalities. □

Now we are ready to prove Theorem 1.6.7.

Proof of Theorem 1.6.7. Let H and C be as in previous considerations. By an averaging argument, there exist $a \in A$, $b \in B$ with $|(A+b) \cap C| > \frac{1+\delta}{2}N$ and $|(B+a) \cap C| > \frac{1+\delta}{2}$. Define $C_A = C - a$ and $C_B = C - b$. Now let us estimate the sum of the expressions $\min(1_A * 1_B(x), t)$ separately on and outside $C_A + C_B$. To do this, let $f, g, h : G \to [0,1]$ be auxiliary functions supported on C_B, $G \setminus C_B$ and $G \setminus C_A$ respectively, satisfying $f, g \leq 1_B$, $h \leq 1_A$ and the conditions

$$\sum_{x \in G} f(x) = t,$$
$$\sum_{x \in G} g(x) = \min(|B \setminus C_B|, t),$$
$$\sum_{x \in G} h(x) = \min\left(|A \setminus C_A|, t - \sum_{x \in G} g(x)\right).$$

Now we have the following estimates:

$$\sum_{x \in C_A + C_B} \min(1_A * 1_B(x), t) \geq \sum_{x \in C_A + C_B} 1_{A \cap C_A} * f(x) > \frac{(1+\delta)Nt}{2},$$
$$\sum_{x \notin C_A + C_B} \min(1_A * 1_B(x), t) \geq \sum_{x \notin C_A + C_B} (1_{A \cap C_A} * g(x) + 1_{B \cap C_B} * h(x)) >$$
$$> \frac{(1+\delta)N}{2} \sum_{x \in G} (g(x) + h(x)).$$

Comparing that to the initial estimate $\sum_{x \in G} \min(1_A * 1_B(x), t) \leq (1+\delta)Nt$ we see that $\sum_{x \in G}(g(x) + h(x)) < t$, which is only possible if $\sum_{x \in G} g(x) = |B \setminus C_B|$ and $\sum_{x \in G} h(x) = |A \setminus C_A|$. Therefore $|A \setminus C_A| + |B \setminus C_B| < t$.

To finish the proof, notice that $|H| = |C| \leq (1+\delta)N$. □

Before proceeding, let us make the remark that in fact the larger the subgroup H is, the fewer points of A and B are allowed to lie outside C_A and C_B respectively. One can try to perform even more precise calculations, using the fact that now we know that actually for all $x \in C = C_A + C_B$ we have $1_A * 1_B(x) \geq t$. However this would make the statement of the result much less clear and give no additional benefit, so instead we leave it as it is.

4.2 Sets of integers

In this section we deal with sets of integers with small popular doubling. We start with establishing the minimum and sets achieving it, independently of corresponding results for finite groups.

The proposition below is of well-known type; we present the proof for completeness.

Proposition 1.6.8. *Let t be a positive integer and $A, B \subset \mathbb{Z}$ be finite sets of size at least t. Then*

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) \geq t(|A| + |B| - t).$$

Proof. Let $a_1 < \ldots < a_k$ be all the elements of A and $b_1 < \ldots < b_l$ be all the elements of B. Define sets $S_j = \{(a_1, b_j), \ldots (a_{k-j+1}, b_j), \ldots, (a_{k-j+1}, b_l)\} \subset A \times B$ for $1 \leq j \leq t$. Those are well defined (and disjoint) since $k, l \geq t$; note that the pairs in each S_j are listed in strictly increasing order of their sum. Therefore we have a pointwise bound $\sum_{(a,b)\in S_j} 1_{\{a+b\}} \leq 1$. Summing it over all j gives $\sum_{(a,b)\in S} 1_{\{a+b\}} \leq t$, where $S = \bigcup_{j=1}^{t} S_j$. Since $S \subset A \times B$, we also have $\sum_{(a,b)\in S} 1_{\{a+b\}} \leq 1_A * 1_B$. In the end we have

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) \geq \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S} 1_{\{a+b\}}(x) = \sum_{(a,b)\in S} \sum_{x\in\mathbb{Z}} 1_{\{a+b\}}(x) =$$

$$= \sum_{(a,b)\in S} 1 = |S| = \left|\bigcup_{j=1}^{t} S_j\right| = \sum_{j=1}^{t} |S_j| = \sum_{j=1}^{t} (k + l + 1 - 2j) = t(k + l - t).$$

□

Proposition 1.6.9. *Let t be a positive integer and $A, B \subset \mathbb{Z}$ be finite sets of size at least t. Then*

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) = t(|A| + |B| - t)$$

if and only if at least one of the following conditions holds:

(a) $\min(|A|, |B|) = t$,

(b) $|A| = |B| = t + 1$ *and* $B = c - A$ *for some* $c \in \mathbb{Z}$,

(c) A and B are arithmetic progressions of the same common difference.

Proof. Let us start with the "if" part. If $\min(|A|,|B|) = t$, then $1_A * 1_B \le t$ pointwise and $\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) = \sum_{x\in\mathbb{Z}} 1_A * 1_B(x) = |A| \cdot |B| = t(|A| + |B| - t)$.

For part (b), note that $1_A * 1_B(c) = |A \cap (c - B)| = t + 1$ and so

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) = \sum_{x\in\mathbb{Z}} 1_A * 1_B(x) - \sum_{x\in\mathbb{Z}} \max(1_A * 1_B(x) - t, 0) \le$$
$$\le |A| \cdot |B| + \sum_{x\in\mathbb{Z}} 1_{\{c\}}(x) = (t+1)^2 - 1 = t(t+2) = t(|A| + |B| - t).$$

The reverse inequality has already been proven, so in fact we have an equality.

For the last part, let $A = \{a, a+d, \dots a+(k-1)d\}$ and $B = \{b, b+d, \dots b+(l-1)d\}$. Then

$$\min(1_A * 1_B(x), t) =$$
$$= \begin{cases} \frac{x-a-b}{d}, & x \in \{a+b, a+b+d \dots, a+b+(t-2)d\}, \\ t, & x \in \{a+b+(t-1)d, \dots a+b+(k+l-t-1)d\}, \\ \frac{a+b+(k+l-1)d-x}{d}, & x \in \{a+b+(k+l-t)d, \dots, a+b+(k+l-2)d\}, \\ 0 & \text{otherwise.} \end{cases}$$

Summing all the above values we get

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) = t(k+l-t) = t(|A| + |B| - t).$$

Let us now deal with the "only if" part. First, if $|A| = |B| = t+1$, then we cannot have $1_A * 1_B \le t$, as this would imply

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) = \sum_{x\in\mathbb{Z}} 1_A * 1_B(x) = |A| \cdot |B| = (t+1)^2 > t(t+2) = t(|A| + |B| - t).$$

Therefore for some $c \in \mathbb{Z}$ we must have $t < 1_A * 1_B(c) = |A \cap (c - B)|$. The sets A and $c - B$ both have $t + 1$ elements, so the only possibility is $A = c - B$.

Now the case that remains is $\min(|A|,|B|) > t$ excluding $|A| = |B| = t + 1$; by symmetry assume $|A| \ge t + 2$ and $|B| \ge t + 1$. Let $a_1 < \dots < a_k$ be all the elements of A and $b_1 < \dots < b_l$ be all the elements of B. Define $S^i_j = \{(a_1, b_j), \dots, (a_{t-j+1}, b_j), \dots, (a_{t-j+1}, b_{j+i}), \dots, (a_{k-j+1}, b_{j+i}), \dots, (a_{k-j+1}, b_l)\}$ for $0 \le i \le l - t$ and $1 \le j \le t$. Now for any $u = 1, \dots, l - t$ and $v = 0, \dots, t$ the sets in the collection $S^{u-1}_1, \dots, S^{u-1}_v, S^u_{v+1}, \dots S^u_t$ are all disjoint. As previously, the pairs in each set are sorted with respect to their sum and $|S^i_j| = k + l + 1 - 2j$. Therefore we can repeat the inequality:

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) \ge \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S^{(u)}_{(v)}} 1_{\{a+b\}}(x) = t(k+l-t),$$

where $S^{(u)}_{(v)} = \left(\bigcup_{j=1}^{v} S_j^{u-1}\right) \cup \left(\bigcup_{j=v+1}^{t} S_j^u\right)$. By our hypothesis the above inequality is in fact an equality and so $\sum_{x\in\mathbb{Z}} \min(1_A * 1_B(x), t) = \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S^{(u)}_{(v)}} 1_{\{a+b\}}(x)$ for each $v = 0, \dots, t$. Comparing this for $v = j$ and $v = j-1$ we get

$$0 = \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S^{(u)}_{(j)}} 1_{\{a+b\}}(x) - \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S^{(u)}_{(j-1)}} 1_{\{a+b\}}(x) =$$
$$= \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S_j^{u-1}} 1_{\{a+b\}}(x) - \sum_{x\in\mathbb{Z}} \sum_{(a,b)\in S_j^{u}} 1_{\{a+b\}}(x).$$

But the pairs in both S_j^{u-1} and S_j^u are sorted in increasing order of their sum, so we know the exact correspondence between them. Omitting the trivial ones, we can write $a_s + b_{j+u-1} = a_{s-1} + b_{j+u}$ for $s = t-j+2, \dots, k-j+1$, in other words $a_s - a_{s-1} = b_{j+u} - b_{j+u-1}$. Since $k \geq t+2$, for every $s = 2 \dots, k-1$ we can find $j \in \{1, \dots, t\}$ with $t - j + 2 \leq s \leq k - j$; that leads to $a_s - a_{s-1} = b_{j+u} - b_{j+u-1} = a_{s+1} - a_s$. Therefore A is an arithmetic progression. Denoting by d its common difference, we get $b_{j+u} - b_{j+u-1} = d$ for all $u = 1, \dots, l-t$ and $j = 1, \dots, t$. Since $l \geq t+1$, B also is an arithmetic progression with common dofference d. □

Now the only remaining thing is to establish the result about near-extremizers. We prove the following analogue of Freĭman $3k-3$ Theorem.

Theorem 1.6.10. *Let $A \subset \mathbb{Z}$ be a nonempty finite set and let t be a positive integer. Suppose that*

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2+\delta)t|A|,$$

for some $\delta > 0$. Then there is an arithmetic progression $P \subset \mathbb{Z}$ with $|P| \leq (1 + 2\delta)|A| + 6t$ and $|A \setminus P| \leq \frac{5t}{2}$, provided that $\delta + \frac{5t}{|A|} \leq \frac{1}{4}$.

We use similar methods to those used by Lev and Smeliansky in [29] to prove (a generalisation of) Freĭman's $3k-3$ Theorem. Their first step was to wrap the set A modulo $q := (\max A - \min A)$ and consider a subset of a finite group instead. Note that since the sets $(A + \min A)$ and $(A + \max A)$ share only one element, this wrapping procedure results in a huge decrement of the doubling constant. In our situation taking just two endpoints would not lead to such decrement; however we can still find two points near the ends such that wrapping modulo their difference gives us exactly what we need.

Proposition 4.2.1. *Let $A \subset \mathbb{Z}$ be a nonempty finite set and t be a positive integer satisfying*

$$\sum_{x\in\mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2+\delta)|A|t$$

for some $\delta \geq -\frac{t}{|A|}$. Then there exist a positive integer n and an integer m and such that the set $A' = (A \cap [m, m+n)) \pmod n$ (the image of the set $A \cap [m+n)$ under the projection $\pmod n$) satisfies the following conditions:

- $|A'| \geq |A| - 2t$,
- $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \min(1_{A'} * 1_{A'}(x), t) \leq \left(1 + 2\delta + \frac{6t}{|A|}\right)|A|t$.

Proof. Set $N = |A|$. The claim is vacuously true for $t \geq \frac{N}{2}$, so we may assume otherwise. Divide A into three subsets U, V, W with $|U| = |W| = t$, $|V| = N - 2t$, $\max U < \min V$, $\max V < \min W$ (intuitively they are the left, middle and right part respectively). We can write the convolution as

$$1_A * 1_A = (1_U + 1_V + 1_W) * (1_U + 1_V + 1_W) \geq 2(1_U * 1_V + 1_V * 1_W),$$

where the inequality comes from discarding some of the positive summands. Note that since $\max(U+V) < \min(V+W)$, the functions $1_U * 1_V$ and $1_V * 1_W$ are supported on disjoint sets and therefore the above implies the following:

$$\sum_{x\in\mathbb{Z}} \min(2 \cdot 1_U * 1_V(x), t) + \sum_{x\in\mathbb{Z}} \min(2 \cdot 1_V * 1_W(x), t) \leq \\ \leq \sum_{x\in\mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2+\delta)Nt.$$

Now we use an easy to check inequality $s^2 \geq t(2s - \min(2s, t))$, valid for all real numbers s. Specifically, we substitute $s = 1_U * 1_V(x)$ and $s = 1_V * 1_W(x)$ and sum over $x \in \mathbb{Z}$ to get

$$\sum_{x\in\mathbb{Z}} ((1_U * 1_V)(x))^2 + \sum_{x\in\mathbb{Z}} ((1_V * 1_W)(x))^2 \geq t(4t(N-2t) - (2+\delta)Nt) = (2-\delta)Nt^2 - 8t^3.$$

Here we also used the previous estimate and the formula for the sum $\sum_{x\in\mathbb{Z}} 1_U * 1_V(x) = \sum_{x\in\mathbb{Z}} 1_V * 1_W(x) = t(N-2t)$. Note that since each $x \in \mathbb{Z}$ can be written in exactly $1_U * 1_V(x)$ ways as a sum $x = u + v$ for $u \in U$, $v \in V$ (and similarly for $1_V * 1_W$), the above expression is in fact equal to

$$\sum_{x\in\mathbb{Z}} ((1_U * 1_V)(x))^2 + \sum_{x\in\mathbb{Z}} ((1_V * 1_W)(x))^2 = \sum_{u\in U}\sum_{v\in V} 1_U * 1_V(u+v) + \sum_{w\in W}\sum_{v\in V} 1_V * 1_W(v+w).$$

By choosing elements $u \in U$ and $w \in W$ for which the inner sums are above average, we can see that

$$\sum_{v \in V} 1_U * 1_V(u+v) + \sum_{v \in V} 1_V * 1_W(v+w) \geq (2-\delta)Nt - 8t^2$$

for some u and w (as $|U| = |W| = t$). Since $1_U * 1_V$ and $1_V * 1_W$ are bounded by both $1_A * 1_A$ and t, we actually proved that

$$\sum_{x \in (u+V) \cup (w+V)} \min(1_A * 1_A(x), t) \geq (2-\delta)Nt - 8t^2.$$

This is just enough for us do define the wrapping procedure. Indeed, projection modulo $(w-u)$ merges the sets $u+V$ and $w+V$ into a single copy of V, on which sum of the values of $\min(1_A * 1_A(x), t)$ cannot exceed $t|V| = t(N-2t)$. Also, we have just calculated that the sum outside of this copy is bounded by $(2+\delta)Nt - ((2-\delta)Nt - 8t^2)$. After a short calculation $(2+\delta)Nt - ((2-\delta)Nt - 8t^2) + t(N-2t) = (1+2\delta)Nt + 6t^2$ we see that the set A' for $m = u$ and $n = w - u$ satisfies the inequality

$$\sum_{x \in \mathbb{Z}} \min(1_{A'} * 1_{A'}(x), t) \leq (1+2\delta)Nt + 6t^2.$$

□

Now we can use results from the previous section to prove Theorem 1.6.10.

Proof of Theorem 1.6.10. Suppose that we have a set A for which the inequality $\sum_{x \in \mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2+\delta)|A|t$ holds. Let $N = |A|$. We use Lemma 4.2.1 to obtain a set $A' \subset \mathbb{Z}/n\mathbb{Z}$ of size at least $N - 2t$ satisfying the inequality $\sum_{x \in \mathbb{Z}} \min(1_{A'} * 1_{A'}(x), t) \leq (1+2\delta)Nt + 6t^2$. We see that the assumptions of Proposition 1.6.7 are satisfied with $A = B = A'$ as long as

$$\frac{1}{2} \geq \frac{(1+2\delta)N + 6t - |A'|}{|A'|} + \frac{t}{|A'|} = \frac{(1+2\delta)N + 7t - |A'|}{|A'|},$$

in other words $3|A'| \geq (2+4\delta)N + 14t$, which is certainly true if $\delta + \frac{5t}{N} \leq \frac{1}{4}$. Proposition 1.6.7 then tells us that the set A' is essentially contained in a coset of a subgroup of size at most $(1+2\delta)N + 6t$, with the exception of at most $\frac{t}{2}$ points. Unwrapping the situation back again, we see that the set A has all but at most $\frac{5t}{2}$ elements contained in an arithmetic progression of length at most $(1+2\delta)N + 6t$. □

4.3 Sets of residues modulo a prime

Following the pattern, we want to have three results about subsets of $\mathbb{Z}/p\mathbb{Z}$. Two of them are theorems of Pollard and Nazarewicz et al., which we have already cited. The remaining task in this section is to prove an analogue of Freĭman 2.4 Theorem. Let us first recall the result to be proven.

Theorem 1.6.11. *Let $0 < \alpha_1 < \alpha_2$ and $\delta_0, \eta > 0$ be real numbers. Suppose that one of the following conditions holds:*

- $\delta_0 < 0.4$ *and* $\alpha_2 = \frac{1}{35}$,
- $\delta_0 < 1$ *and* $\alpha_2 = 2^{-2^{10}}$,
- $\delta_0 < 10^{-4}$ *and* $\alpha_2 = \frac{1}{2(1+\delta_0)}$.

Then there exists a number $t_0 = t_0(\alpha_1, \eta, \delta_0)$ with the following property. Let $p > p_0(\alpha_1, \eta, \delta_0)$ be a sufficiently large prime, $A \subset \mathbb{Z}/p\mathbb{Z}$ be a set satisfying $\alpha_1 p \leq |A| \leq \alpha_2 p$ and let $t \in (0, t_0)$ be a real number. Suppose that for some $\delta \in (0, \delta_0)$ the following inequality holds:

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_A(x), t) \leq (2+\delta)|A|t.$$

Then there exists an arithmetic progression $P \subset \mathbb{Z}/p\mathbb{Z}$ with $|P| \leq (1+\delta+\eta)|A| + 1$ and $|A \setminus P| \leq \eta|A|$.

One of our tools will be a corresponding result for sets of small doubling. At the moment we have three such statements available, namely theorems of Freĭman, Green-Ruzsa and Serra-Zémor. For this reason we are able to prove the above theorem in three different ranges of parameters. In fact Freĭman 2.4 Theorem has a more general form (see [16]), which allows us to make the above statement valid in even wider range. However we are not going to do so, as it would make it less clean and our proof methods remain the same.

The general idea is to use the Green-Tao regularity lemma (Proposition 2.5.5). Let $\epsilon > 0$ and $\mathcal{F}$ be a growth function to be specified later. Given a prime p and a set $A \subset \mathbb{Z}/p\mathbb{Z}$, apply the regularity lemma to get $1_A = f_{\mathrm{str}} + f_{\mathrm{sml}} + f_{\mathrm{unf}}$. First of all, if $f, g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ are functions, we can bound

$$\|f * g\|_2 = \|\widehat{f} \cdot \widehat{g}\|_2 \leq \|\widehat{f}\|_2 \|\widehat{g}\|_\infty = \|f\|_2 \|\widehat{g}\|_\infty \leq \|f\|_\infty \|\widehat{g}\|_\infty.$$

Setting $f = f_{\text{unf}}$ and $g = 1_A + (f_{\text{str}} + f_{\text{sml}})$ we get

$$\|1_A * 1_A - (f_{\text{str}} + f_{\text{sml}}) * (f_{\text{str}} + f_{\text{sml}})\|_2 \leq \frac{2}{\mathcal{F}(M)}. \tag{4.1}$$

We will need the statement of the regularity lemma; recall it now.

Proposition 2.5.5 (arithmetic regularity lemma: intermediate version)**.** *Let $\epsilon > 0$ and let $\mathcal{F}$ be a growth function. Then there exists a real number $M_0 = M_0(\epsilon, \mathcal{F}) > 0$ for which the following statement is true. Let $p > p_0(\epsilon, \mathcal{F})$ be a prime and $f : \mathbb{Z}/p\mathbb{Z} \to [0, 1]$ be a function. Then there exists a number $0 < M \leq M_0$ and a decomposition*

$$f = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$$

satisfying the following properties:

- *$f_{\text{str}} = F \circ \phi$, where $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^d$ is a homomorphism with $d \leq M$ and $F : \mathbb{T}^d \to [0, 1]$ is an M-Lipschitz function (f_{str} is structured),*
- *$\|f_{\text{sml}}\|_2 \leq \epsilon$ (f_{sml} is small),*
- *$|\langle f_{\text{unf}}, \chi\rangle| \leq \frac{1}{\mathcal{F}(M)}$ for every character χ (f_{unf} is U^2-uniform).*
- *f_{str} and $f_{\text{str}} + f_{\text{sml}}$ both take values in $[0, 1]$.*

Now we wish to exploit the decomposition $1_A = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$. The key idea is captured by the following lemma.

Lemma 4.3.1. *Let $1_A = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$ as in the statement of Proposition 2.5.5 and let $\lambda, \eta, \beta \in (0, 1)$ be parameters. Define a Bohr set $B = B(\beta) = \{x \in \mathbb{Z}/p\mathbb{Z} : \|\phi(x)\| \leq \beta\}$ and a set*

$$S = S(\lambda, \eta, \beta) = \{x \in \mathbb{Z}/p\mathbb{Z} : f_{\text{str}}(x) \geq \lambda \quad \text{and} \quad \mathbb{E}_{y \in B}|f_{\text{sml}}(x + y)|^2 \leq \eta\}.$$

Then for every $x \in S + S$ we have the following inequality:

$$(f_{\text{str}} + f_{\text{sml}}) * (f_{\text{str}} + f_{\text{sml}})(x) \geq ((\lambda - M\beta)^2 - 2\sqrt{\eta})\beta^M.$$

Moreover,

$$|A \setminus S| \leq p\left(\lambda + \epsilon + \frac{\epsilon^2}{\eta} + \frac{3M}{\lambda \mathcal{F}(M)^{1/(3M+1)}}\right).$$

The above statement is slightly more general than needed, as we want to avoid reproving a similar lemma in the next chapter.

Proof. We start with proving the first inequality. Suppose that $x = x_1 + x_2$ with $x_1, x_2 \in S$. Unwrapping the definition of convolution we get

$$\begin{aligned}(f_{\text{str}} + f_{\text{sml}}) * (f_{\text{str}} + f_{\text{sml}})(x_1 + x_2) = \\ = p^{-1} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} (f_{\text{str}} + f_{\text{sml}})(x_1 + y)(f_{\text{str}} + f_{\text{sml}})(x_2 - y) \geq \\ \geq p^{-1} \sum_{y \in B} (f_{\text{str}} + f_{\text{sml}})(x_1 + y)(f_{\text{str}} + f_{\text{sml}})(x_2 - y).\end{aligned}$$

By definition of B and the Lipschitz nature of F we have $|f_{\text{str}}(x) - f_{\text{str}}(x+y)| \leq \beta M$ for $x \in \mathbb{Z}/p\mathbb{Z}$ and $y \in B$ (recall that $f_{\text{str}} = F \circ \phi$). Therefore, by definition of S, $f_{\text{str}}(x_i \pm y) \geq \lambda - \beta M$ for $x_i \in S$ and $y \in B$. Substituting this into the formula for convolution, we get

$$p^{-1} \sum_{y \in B} f_{\text{str}}(x_1 + y) f_{\text{str}}(x_2 - y) \geq (\lambda - \beta M)^2 \frac{|B|}{p}.$$

On the other hand, by Cauchy-Schwarz inequality

$$\begin{aligned}\left| \sum_{y \in B} f_{\text{str}}(x_1 + y) f_{\text{sml}}(x_2 - y) \right| \leq \\ \leq \left(\sum_{y \in B} |f_{\text{str}}(x_1 + y)|^2 \right)^{\frac{1}{2}} \left(\sum_{y \in B} |f_{\text{sml}}(x_2 - y)|^2 \right)^{\frac{1}{2}} \leq \sqrt{|B|} \cdot \sqrt{\eta |B|} = |B| \sqrt{\eta}.\end{aligned}$$

Similarly $\left| \sum_{y \in B} f_{\text{sml}}(x_1 + y)(f_{\text{str}} + f_{\text{sml}})(x_2 - y) \right| \leq |B| \sqrt{\eta}$. Plugging these inequalities into the formula for convolution, we get $(f_{\text{str}} + f_{\text{sml}}) * (f_{\text{str}} + f_{\text{sml}})(x_1 + x_2) \geq ((\lambda - M\beta)^2 - 2\sqrt{\eta}) \frac{|B|}{p}$. From Lemma 2.5.12 we know that $|B| \geq \beta^d p \geq \beta^M p$; this gives us the desired bound.

To prove the bound on $|A \setminus S|$, we need to count points of A that for which one of two conditions fails. The first one is $\sum_{y \in B} |f_{\text{sml}}(x + y)|^2 \leq \eta |B|$; comparing it to $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \sum_{y \in B} |f_{\text{sml}}(x + y)|^2 = |B| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |f_{\text{sml}}(x)|^2 = |B| \cdot \|f_{\text{sml}}\|_2^2 \cdot p \leq |B| \epsilon^2 p$, we see that the number of points not satisfying this is at most $\frac{\epsilon^2 p}{\eta}$.

Now we want to count the number of points $x \in A$ with $f_{\text{str}}(x) < \lambda$. To do this, define the function $\widetilde{f} : \mathbb{Z}/p\mathbb{Z} \to [0, 1]$ via the formula

$$\widetilde{f}(x) = \begin{cases} 1, & f_{\text{str}}(x) \leq \lambda, \\ 2 - \frac{f_{\text{str}}(x)}{\lambda}, & \lambda < f_{\text{str}}(x) < 2\lambda, \\ 0, & f_{\text{str}}(x) \geq 2\lambda. \end{cases}$$

The number of points interesting to us is bounded by $p\langle 1_A, \widetilde{f} \rangle$. Writing $1_A = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$, we see that

- $|\langle f_{\text{str}}, \widetilde{f}\rangle| \le \max(\lambda, \max_t((2-t)t\lambda), 0) = \lambda$,
- $|\langle f_{\text{sml}}, \widetilde{f}\rangle| \le \|f_{\text{sml}}\|_2 \|\widetilde{f}\|_2 \le \|f_{\text{sml}}\|_2 \|\widetilde{f}\|_\infty \le \epsilon$,
- $|\langle f_{\text{unf}}, \widetilde{f}\rangle| \le (\frac{M}{\lambda} + d + 1)\|\widehat{f_{\text{unf}}}\|_\infty^{1/(3d+1)} \le \frac{3M}{\lambda \mathcal{F}(M)^{1/(3M+1)}}$.

The last inequality follows from Lemma 2.5.11 and the fact that $\widetilde{f} = \widetilde{F} \circ \phi$, where

$$\widetilde{F}(t) = \begin{cases} 1, & F(x) \le \lambda, \\ 2 - \frac{F(t)}{\lambda}, & \lambda < F(t) < 2\lambda, \\ 0, & F(t) \ge 2\lambda \end{cases}$$

is a $\frac{M}{\lambda}$-Lipschitz function. Putting all the bounds together, we get the desired estimate of $|A \setminus S|$. □

In this chapter we only need the following corollary.

Corollary 4.3.2. Let $\delta > 0$ be a real number. Then there exists a real number $t = t(\delta) > 0$ such that the following statement is true. Let p be a prime and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a set. Then there exists a set $S \subset \mathbb{Z}/p\mathbb{Z}$ satisfying the inequalities:

$$|A \setminus S| \le \delta p,$$
$$\sum_{x \in S+S} \min(1_A * 1_A(x), t) \ge t(|S+S| - \delta p).$$

Proof. Apply the Green-Tao regularity lemma with parameter $\epsilon = 2^{-9}\delta^3$ and a function $\mathcal{F}(M) = (\frac{48M}{\delta^2})^{3M+1}$ to the function 1_A; we get a number M and a decomposition $1_A = f_{\text{str}} + f_{\text{sml}} + f_{\text{unf}}$. Then apply Lemma 4.3.1 with parameters $\lambda = \frac{\delta}{4}$, $\eta = 2^{-16}\delta^2$ and $\beta = \frac{\delta}{8M}$ to get a set S. Since

$$\lambda = \frac{\delta}{4}, \qquad \frac{\epsilon^2}{\eta} = \frac{\delta^6}{2^{16}} \cdot \frac{2^{16}}{\delta^4} = \frac{\delta^2}{4} \le \frac{\delta}{4},$$
$$\epsilon = \frac{\delta^3}{2^9} \le \frac{\delta}{4}, \qquad \frac{3M}{\lambda \mathcal{F}(M)^{1/(3M+1)}} = \frac{12M}{\delta} \cdot \frac{\delta^2}{48M} = \frac{\delta}{4},$$

it follows that $|A \setminus S| \le \delta p$. Moreover, we calculate

$$((\lambda - M\beta)^2 - 2\sqrt{\eta})\beta^M = ((\tfrac{\delta}{4} - M\tfrac{\delta}{8M}) - 2\sqrt{2^{-16}\delta^4})(\tfrac{\delta}{8M})^M =$$
$$= ((\tfrac{\delta}{8})^2 - 2\tfrac{\delta^2}{2^8})(\tfrac{\delta}{8M})^M = 2^{-7}\delta^2(\tfrac{\delta}{8M})^M.$$

It means that for $t = 2^{-7}\delta^2(\frac{\delta}{8M})^M$ and any $x \in S+S$ we have $(f_{\text{str}} + f_{\text{sml}}) * (f_{\text{str}} + f_{\text{sml}})(x) \ge t$.

Denote $u = 1_A * 1_A$ and $v = (f_{\text{str}} + f_{\text{sml}}) * (f_{\text{str}} + f_{\text{sml}})$. Since $|\min(u,t) - \min(v,t)| \leq |u - v|$, we have

$$\left| \sum_{x \in S+S} (\min(u(x),t) - \min(v(x),t)) \right| \leq \sum_{x \in S+S} |u(x) - v(x)| \leq$$
$$\leq p \cdot \|u - v\|_1 \leq p \cdot \|u - v\|_2 \leq \frac{2p}{\mathcal{F}(M)}.$$

Since we have $\sum_{x \in S+S} \min(v(x),t) = t|S+S|$, it follows that $\sum_{x \in S+S} \min(u(x),t) \geq t|S+S| - \frac{2p}{\mathcal{F}(M)}$. The bound we need follows from the fact that $\frac{2}{\mathcal{F}(M)} \leq 2(\frac{\delta}{8M})^{M+3} \leq 2^{-7}\delta^3(\frac{\delta}{8M})^M = \delta t$.

The number t we have found depends on the parameter M. However for fixed sets A, S the function $t \mapsto \sum_{x \in S+S} \min(1_A * 1_A(x), t)$ is concave in t and $t \mapsto t(|S+S| - \delta p)$ is linear. Since both are 0 at $t = 0$, it follows that the inequality is still valid if we replace t with any number from the interval $(0,t)$. We can then replace t with its lower bound $2^{-7}\delta^2(\frac{\delta}{8M_0})^{M_0}$, where $M_0 = M_0(\epsilon, \mathcal{F})$ is the bound given by the Green-Tao regularity lemma. □

The above result applied to a set A of small popular doubling, assigns to it a set S of small doubling. Therefore we can use it and one of the Theorems of Freĭman, Green-Ruzsa and Serra-Zémor (1.4.16, 1.4.17 and 1.4.18 respectively) to prove a structure theorem for sets of small popular doubling.

Proof of Theorem 1.6.11. Denote by m_δ the bound on δ_0 from the statement (so that $m_\delta \in \{0.4, 1, 10^{-4}\}$). Apply Corollary 4.3.2 with parameter $\min(\frac{\eta\alpha_1}{2}, \frac{\alpha_1(m_\delta - \delta_0)}{8})$ to get a number t_0 and a set S. We know that $|A \setminus S| \leq \frac{\alpha_1(m_\delta - \delta_0)p}{8}$, in which case $|S| \geq |A| - \frac{\alpha_1(m_\delta - \delta_0)p}{8} \geq (1 - \frac{m_\delta - \delta_0}{8})|A|$. We also have $|S+S| \leq \frac{1}{t_0}\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_A(x), t_0) + \frac{\alpha_1(m_\delta - \delta_0)p}{8} \leq \frac{1}{t}\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_A(x), t) + \frac{m_\delta - \delta_0}{8}|A| \leq (2 + \delta + \frac{m_\delta - \delta_0}{8})|A|$ (here we used concavity of the function $t \mapsto \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_A(x), t)$). Since

$$\frac{2 + \delta + \frac{m_\delta - \delta_0}{8}}{1 - \frac{m_\delta - \delta_0}{8}} - 2 = \frac{\delta + \frac{3(m_\delta - \delta_0)}{8}}{1 - \frac{m_\delta - \delta_0}{8}} < \frac{\delta_0 + \frac{3(m_\delta - \delta_0)}{8}}{1 - \frac{m_\delta - \delta_0}{4(m_\delta + \delta_0)}} = \frac{m_\delta + \delta_0}{2},$$

we can use one of the Theorems 1.4.16, 1.4.17, 1.4.18 to conclude that there exists an arithmetic progression $P \subset \mathbb{Z}/p\mathbb{Z}$ containing S with $|P| \leq |S+S| - |S| + 1 \leq (1 + \delta + \eta)|A| + 1$. We also have $|A \setminus P| \leq |A \setminus S| \leq \frac{\eta\alpha_1 p}{2} \leq \frac{\eta}{2}|A|$. □

Chapter 5

Counting subsets with small doubling

In this chapter we estimate the number of subsets of an interval $\{1,\dots,N\}$ with size k and doubling at most K. Note that for every $A \subset \{1,\dots,N\}$ we have $A+A \subset \{2,\dots 2N\}$ and consequently $|A+A| \leq 2N-1$. The task is then trivial if $Kk \geq 2N$; let us focus on the case $Kk \leq 2N$. Green and Morris gave the answer under the additional constraint $k = o(\log N)$ or $k = \omega(\log N)$. In this chapter we prove an extension of the Green-Morris Theorem (Theorem 1.7.2) that removes this constraint. Recall the statement of the result:

Theorem 1.7.2. *Let $\delta > 0$ and $K \geq 2$ be real numbers. Then there exists a number $k_0 = k_0(\delta, K)$ such that for all integers $k > k_0$ and N with $2N \geq Kk$ we have*

$$\max_{0\leq t\leq \lfloor K\rfloor -2} \binom{\lfloor \frac{1}{2}(K-t-\delta)k\rfloor}{k} N^{t+2} \leq \#\{A\subset [N] \ : \ |A|=k, |A+A|\leq K|A|\} \leq \max_{0\leq t\leq \lfloor K+\delta\rfloor -2} \binom{\lfloor \frac{1}{2}(K-t+\delta)k\rfloor}{k} N^{t+2}.$$

5.1 Examples

In this section we aim to justify the lower bound in Theorem 1.7.2. To do this, we provide a collection of examples.

Example 5.1.1. Let N, k be natural numbers and let $K \geq 2$ be a real number. For an integer $0 \leq t \leq K-2$ we define the family of sets $\mathcal{S}_t$ in the following way. A set A belongs to $\mathcal{S}_t$ if $|A| = k$ and there exists a progression $P \subset [N]$ with $|P| \leq \frac{(K-t)k}{2}$

and $|A \setminus P| \le t$. For any $A \in \mathcal{S}_t$ we have

$$|A+A| = |((A\cap P)+(A\cap P)) \cup (A+(A\setminus P))| \le$$
$$\le |P+P| + |A|\cdot|A\setminus P| \le (K-t)k + tk = Kk.$$

We would like to estimate the size $|\mathcal{S}_t|$ as $N, k \to \infty$ with $Kk \le 2N$. To avoid counting the same set $A \in \mathcal{S}_t$ multiple times, we need a couple of technical constraints. For $Kk \le 2N$, there are at least $\frac{4N^2}{K^3k^3}$ progressions $P \subset [N]$ with $|P| = m := \lfloor \frac{(K-t)k}{2} \rfloor$. Indeed, there are $N-(m-1)d$ progressions with common difference d; summing over d gives

$$\sum_{d=1}^{\infty} \max(N-(m-1)d, 0) \ge \int_1^{\infty} \max(N-(m-1)x, 0)dx =$$
$$= \frac{(N-(m-1))^2}{2(m-1)} \ge \frac{1}{2(m-1)}\left(\frac{N}{m}\right)^2 \ge \frac{4N^2}{K^3k^3}.$$

For each such progression, denote by Q a progression of the same difference and length $t+1$. We count the sets A that contain

- $2t+2$ initial and $2t+2$ final elements of P,
- t elements outside of $P+Q-Q$,
- $k-5t-4$ of the remaining elements of P.

This way each progression P corresponds to at least $\binom{N-\lfloor \frac{1}{2}(K-t)k \rfloor - 2t}{t}\binom{\lfloor \frac{1}{2}(K-t)k \rfloor - 4t - 4}{k-5t-4}$ sets. Also, each set A can be counted only once. Indeed, the first condition ensures that we can recover the common difference of P and position of P up to translation by at most t elements. Then the second condition allows us to recover the t points outside of P. Having those points, the first condition allows us to recover P exactly. In the end we have shown that

$$|\mathcal{S}_t| \ge \frac{4N^2}{K^3k^3}\binom{N-\lfloor \frac{1}{2}(K-t)k \rfloor - 2t}{t}\binom{\lfloor \frac{1}{2}(K-t)k \rfloor - 4t - 4}{k-5t-4}.$$

Let us make some rearrangements to see how large this bound really is. We have

$$\binom{N-\lfloor \frac{1}{2}(K-t)k \rfloor - 2t}{t} \ge \left(\frac{N-\frac{1}{2}(K-t)k-3t}{t}\right)^t \ge$$
$$\ge \left(\frac{N-(K-t)\frac{N}{K}-3t}{t}\right)^t = \left(\frac{N-3}{K}\right)^t \ge \frac{N^t}{(2K)^t}$$

for N sufficiently large. The above calculations are valid for $t \geq 1$ but the final bound holds also for $t = 0$.

The last term can be estimated as

$$\binom{\lfloor \frac{1}{2}(K-t)k \rfloor - 4t - 4}{k - 5t - 4} \geq \binom{\lfloor \frac{1}{2}(K-t)k \rfloor - 5t - 4}{k - 5t - 4} \geq$$
$$\geq \left(\frac{k-5t-4}{\frac{1}{2}(K-t)k - 5t - 4} \right)^{5t+4} \binom{\lfloor \frac{1}{2}(K-t)k \rfloor}{k} \geq K^{-5t-4} \binom{\lfloor \frac{1}{2}(K-t)k \rfloor}{k}$$

if k is large enough.

In the end we have

$$|\mathcal{S}_t| \geq N^{t+2} \binom{\lfloor \frac{1}{2}(K-t)k \rfloor}{k} \cdot \frac{4}{2^t K^{6t+7} k^3}.$$

We can pull the last factor into the binomial coefficient, as follows:

$$\binom{\lfloor \frac{1}{2}(K-t)k \rfloor}{k} \geq \binom{\lfloor \frac{1}{2}(K-t-\delta)k \rfloor}{k} \left(\frac{\lfloor \frac{1}{2}(K-t)k \rfloor}{\lfloor \frac{1}{2}(K-t-\delta)k \rfloor} \right)^k \geq$$
$$\geq \binom{\lfloor \frac{1}{2}(K-t-\delta)k \rfloor}{k} \left(\frac{K-t}{K-t-\frac{\delta}{2}} \right)^k$$

for k large enough. Since K is fixed and $t \leq K-1$ and $k \to \infty$, the last term grows exponentially for any fixed δ; therefore it exceeds $2^{t-2} K^{6t+7} k^3$ for $k > k_0(\delta)$. This way we have proved the lower bound in Theorem 1.7.2.

5.2 Splitting into cases

To get the upper bound, we need to understand where the maximum in the statement comes from and why it is achieved for different t at different times. In other words, we wish to divide all the subsets $A \subset [N]$ with $|A| = k$ and $|A+A| \leq Kk$ into classes such that each class has size bounded by $|\mathcal{S}_t|^{1+o(1)}$. It turns out that the parameter that drives this division is Freĭman dimension (see Definition 2.6.4). We use it as follows.

Proposition 5.2.1. *Let $\delta > 0$ and $K \geq 2$ be real numbers and let $0 \leq t \leq \lfloor K + \delta \rfloor - 2$ be an integer. Then there exists $k_0 = k_0(\delta, K)$ such that for all integers $k > k_0$ and N with $2N \geq Kk$ we have*

$$\#\{A \subset [N] \ : \ |A| = k, \ |A+A| \leq K|A|, \ \dim_F A = t+1\} \leq$$
$$\leq 2^{\delta k} \binom{\lfloor \frac{1}{2}(K-t)k \rfloor}{k} N^{t+2}.$$

Proposition 5.2.1 implies Theorem 1.7.2 as long as we know that $t \leq K + \delta - 2$, or in other words $\dim_F A \leq K + \delta - 1$. This is guaranteed by the Freĭman dimension lemma (Lemma 2.6.8).

In the sequel we will focus on proving Proposition 5.2.1.

5.3 The regularity lemma and approximating sets

In this section we prove a result on approximating sets. In fact we prove that any subset of $\mathbb{Z}/p\mathbb{Z}$ is essentially a random-looking subset of a set of a set that is not too complex. Although the precise definition of a "not too complex" set could be extracted from the result below, for applications we only need a bound for the number of these. For this reason we state the result as follows.

Proposition 5.3.1. *For any $\delta > 0$ there exists a constant $M = M(\delta) > 0$ such that the following statement is true. For every prime p there exists a family $\mathcal{S}$ of subsets of $\mathbb{Z}/p\mathbb{Z}$ with $|\mathcal{S}| \leq p^M$ such that for any $A \subset \mathbb{Z}/p\mathbb{Z}$, there exists $S \in \mathcal{S}$ with $\max(|A \setminus S|, |(S+S) \setminus (A+A)|) \leq \delta p$.*

Proof. We will prove that the following family $\mathcal{S}$ satisfies postulated conditions. A set S belongs to $\mathcal{S}$ if there exist integers $d, K = O_\delta(1)$ and a homomorphism $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}^d$ such that for any $i \in (\mathbb{Z}/K\mathbb{Z})^d$ the set

$$S_{(i)} = \{x \in \mathbb{Z}/p\mathbb{Z} \ : \ \phi_j(x) \in [\tfrac{i_j}{K}, \tfrac{i_j+1}{K}) \text{ for } j = 1, \dots d\}$$

is either contained in S or disjoint from S. The numbers K and d can take at most $O_\delta(1)$ values and the homomorphism ϕ can be chosen in $p^{O_\delta(1)}$ ways. Given ϕ, there are at most $O_\delta(1)$ possible sets S. In the end, the number of possible sets S is $p^{O_\delta(1)}$. Let us now prove that for any $A \subset \mathbb{Z}/p\mathbb{Z}$ among such sets S there is always one with $\max(|A \setminus S|, |(S+S) \setminus (A+A)|) \leq \delta p$.

Fix $\epsilon = \frac{\delta^3}{2^{14}}$ and a growth function $\mathcal{F}(M) = (\frac{2^6 M}{\delta^2})^{3(M+1)}$. We intend to use Lemma 4.3.1, which would produce a set $S = S(\lambda, \eta, \beta)$ for a given set A. However, we have no information about the structure of S. To get around this, note that the inequality $|A \setminus S| \leq p\left(\lambda + \epsilon + \frac{\epsilon^2}{\eta} + \frac{3M}{\lambda \mathcal{F}(M)^{1/(3M+1)}}\right)$ is valid for all sets $S \supset S(\lambda, \eta, \beta)$, while the inequality $(f_{\mathrm{str}} + f_{\mathrm{sml}}) * (f_{\mathrm{str}} + f_{\mathrm{sml}})(x) \geq ((\lambda - M\beta)^2 - 2\sqrt{\eta})\beta^M$ holds for all $x \in S+S$ with $S \subset S(\lambda, \eta, \beta)$. Therefore we define two sets of parameters:

$$\lambda_1 = \frac{\delta}{4}, \qquad \eta_1 = \frac{\delta^5}{2^{25}} \qquad \beta_1 = \frac{(s+1)\delta}{32M^3}$$
$$\lambda_2 = \frac{\delta}{8} \qquad \eta_2 = \frac{\delta^4}{2^{20}} \qquad \beta_2 = \frac{s\delta}{32M^3}$$

for some positive integer $s \le 2M^2$ to be specified later, and let $B_1 = B(\beta_1)$, $B_2 = B(\beta_2)$, $S_1 = S(\lambda_1, \eta_1, \beta_1)$, $S_2 = S(\lambda_2, \eta_2, \beta_2)$. Let also $\beta = \frac{\delta}{32M^3}$ and $B = B(\beta)$. Note that by the description of f_{str}, we have $|f_{\mathrm{str}}(x) - f_{\mathrm{str}}(x+y)| \le M\beta \le \frac{\delta}{8}$ for every $s \in \mathbb{Z}/p\mathbb{Z}$ and $y \in B$. Therefore $f_{\mathrm{str}}(x) \ge \lambda_1$ implies $f_{\mathrm{str}}(x+y) \ge \lambda_1 - \frac{\delta}{8} = \lambda_2$. Also, since $B_2 + B \subset B_1$, we know that $\mathbb{E}_{y \in B_2} |f_{\mathrm{sml}}(x + x' + y)|^2 \le \eta_2$ implies $\mathbb{E}_{y \in B_1} |f_{\mathrm{sml}}(x+y)|^2 \le \eta_1$ as long as $x' \in B$ and $\eta_1 |B_1| \le \eta_2 |B_2|$. To make sure that this is satisfied, define the sequence $b_s = p^{-1}|B(\frac{s\delta}{32M^3})|$ for $s = 1, \dots, \lceil M^2 \rceil + 1$. We know that $b_1 \ge (\frac{\delta}{32M^3})^M$ (Lemma 2.5.12) and $b_{\lceil M^2 \rceil + 1} \le 1$, therefore there exists $s \in \{1, \dots, M\}$ with $\frac{b_s}{b_{s+1}} \ge (\frac{\delta}{32M^3})^{1/M} \ge \frac{\delta}{32} = \frac{\eta_1}{\eta_2}$.

In the end, we have proved that $S_1 \subset S_1 + B \subset S_2$. By the choice of parameters we have

$$\lambda_1 = \frac{\delta}{4}, \qquad \frac{\epsilon^2}{\eta_1} = \frac{\delta^6}{2^{28}} \cdot \frac{2^{25}}{\delta^5} = \frac{\delta}{8} \le \frac{\delta}{4},$$
$$\epsilon = \frac{\delta^3}{2^{14}} \le \frac{\delta}{4}, \qquad \frac{3M}{\lambda_1 \mathcal{F}(M)^{1/(3M+1)}} \le \frac{12M}{\delta} \cdot \frac{\delta^2}{2^6 M} \le \frac{\delta}{4},$$

so $|A \setminus S_1| \le \delta p$. To estimate $|(S_2 + S_2) \setminus (A + A)|$, note that for each $x \in S_2 + S_2$ we have

$$(f_{\mathrm{str}} + f_{\mathrm{sml}}) * (f_{\mathrm{str}} + f_{\mathrm{sml}})(x) \ge ((\lambda_2 - M\beta_2)^2 - 2\sqrt{\eta_2})\beta_2^M \ge$$
$$\ge \left(\left(\frac{\delta}{8} - M \frac{2M^2 \delta}{32M^3} \right)^2 - 2\sqrt{2^{-20}\delta^4} \right) \left(\frac{\delta}{32M^3} \right)^M = \frac{\delta^2}{2^9} \left(\frac{\delta}{32M^3} \right)^M.$$

Since $1_A * 1_A(x) = 0$ for each $x \notin A + A$, it follows that

$$\|1_A * 1_A - (f_{\mathrm{str}} + f_{\mathrm{sml}}) * (f_{\mathrm{str}} + f_{\mathrm{sml}})\|_2^2 \ge p^{-1} |(S_2 + S_2) \setminus (A + A)| \left(\frac{\delta^2}{2^9} \left(\frac{\delta}{32M^3} \right)^M \right)^2.$$

We already know that the left hand side is bounded by $(\frac{2}{\mathcal{F}(M)})^2$; using this bound we get

$$p^{-1} |(S_2 + S_2) \setminus (A + A)| \le \left(\frac{\frac{2^{10}}{\delta^2} (\frac{32M^3}{\delta})^M}{\mathcal{F}(M)} \right)^2 \le \left(\frac{(\frac{2^{10} M^3}{\delta^2})^{M+1}}{\mathcal{F}(M)} \right)^2 = \left(\frac{\delta^4}{2^8} \right)^{2(M+1)} \le \delta.$$

Now let $K = \lceil \frac{1}{\beta} \rceil$; observe that $S_{(i)} - S_{(i)} \subset B$ for $i \in (\mathbb{Z}/K\mathbb{Z})^d$. Let S be the union of all those $S_{(i)}$ that intersect S_1; obviously $S_1 \subset S$. Also for any $x \in S$, if we denote by y a common point of the corresponding $S_{(i)}$ with S_1, we can write $x = y - y + x \in S_1 - S_{(i)} + S_{(i)} \subset S_1 + B \subset S_2$. In the end $S_1 \subset S \subset S_2$ and consequently $|A \setminus S|, |(S + S) \setminus (A + A)| \le \delta p$. $\square$

5.4 Counting sets

We are now ready to return to the counting sets problem. Our strategy is to first count the Freĭman isomorphism classes of sets in $\mathbb{Z}^d$ and then count the number of embeddings of each set into $[N]$. First of all, we need the following result.

Proposition 5.4.1. *Let $\delta > 0$ and $K \geq 2$ be real numbers and let d be a positive integer. Then there exists $k_0 = k_0(\delta, K)$ such that the following statement is true. Let $k > k_0$ be an integer and let $\mathcal{A}$ be a family of subsets of $\mathbb{Z}^d$ with the following properties:*

- *every set $A \subset \mathcal{A}$ satisfies $|A| = k$, $|A + A| \leq Kk$, $\dim_F A = d$.*
- *no two distinct elements of $\mathcal{A}$ are Freĭman isomorphic.*

Then

$$|\mathcal{A}| \leq 2^{\delta k} \binom{\lfloor \frac{1}{2}(K - d + 1)k \rfloor}{k}.$$

Proof. First of all, if $d > K - 1 + \frac{\delta}{4}$, then by Freĭman dimension lemma we can take $k_0 \geq \frac{4K^2}{\delta}$ so that every set with $\dim_F = d$ has $|A + A| > K|A|$ and consequently $|\mathcal{A}| = 0$. We can then assume $d \leq K - 1 + \frac{\delta}{4}$. Pick any set $A \in \mathcal{A}$. Without loss of generality assume that A is contained in no coset of a proper subgroup. By Theorem 2.6.9 there exists a generalized arithmetic progression $P \supset A$ with $\dim P = d$ and $|P| \leq F(K)k$. From these inequalities we know that $|P + P| \leq 2^d F(K)k \leq 2^{K+\delta} F(K)k =: F'(K)k$. Pick any prime $p \in [F'(K)k, 2F'(K)k]$. There exists an injective Freĭman homomorphism $\phi : P + P \hookrightarrow \mathbb{Z}/p\mathbb{Z}$. Let $A' = \phi(A)$. Note that ϕ is a Freĭman isomorphism when restricted to any subset of P, so given the set A' we can identify A uniquely. It suffices then to estimate the number of possible sets A'. Let us apply Proposition 5.3.1 with δ replaced with $\epsilon = \left(\frac{\delta}{32(K+\delta)F'(K)}\right)^2$. It gives us a set $S \subset \mathbb{Z}/p\mathbb{Z}$ with $\max(|A' \setminus S|, |(S + S) \setminus (A' + A')| \leq \epsilon p$; the number of possible sets S is $p^{O_{\delta,K}(1)}$. Rename $S := S \cap \phi(P)$; since $A' \subset \phi(P)$, the inequality is still satisfied. The number of possible sets $\phi(P)$ is at most $p^{1+\dim P}|P|^{\dim P} \leq p^{2K+1+\delta} = p^{O_{\delta,K}(1)}$, so the bound on the number of possible sets S is still valid after renaming. Now given a set S we can bound the number of corresponding sets A'. To get the set A', we first need to pick $0 \leq l \leq \epsilon p$, then pick $k - l$ points from $|S|$ and the remaining l points from $\mathbb{Z}/p\mathbb{Z}$. In the end, the number of sets corresponding to S is at most

$$\sum_{l=0}^{\lfloor \epsilon p \rfloor} \binom{p}{l} \binom{|S|}{k-l} \leq \binom{|S|}{k} \sum_{l=0}^{\lfloor \epsilon p \rfloor} \binom{p}{l} \binom{|S|}{l}.$$

The last sum can be estimated as

$$\sum_{l=0}^{\lfloor \epsilon p \rfloor} \binom{p}{l}\binom{|S|}{l} \leq \sum_{l=0}^{\lfloor \epsilon p \rfloor} \binom{p}{l}^2 \leq \left(\sum_{l=0}^{\lfloor \epsilon p \rfloor} \binom{p}{l}\right)^2 \leq 2^{2pH(\epsilon)} \leq 2^{4p\sqrt{\epsilon}},$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ (see Definition A.0.5). For all the inequalities used, see the appendix. The total number of sets A' is then bounded by $p^{O_{\delta,K}(1)}2^{4p\sqrt{\epsilon}}\binom{\max|S|}{k}$ and the only task remaining is to estimate the size of S. Pick a set $S \subset \phi(P) \subset \mathbb{Z}/p\mathbb{Z}$ and let $S' = \phi^{-1}(S) \subset P \subset \mathbb{Z}^d$. Let d' be the affine dimension of S'. By Freĭman dimension lemma we have $|S'+S'| \geq (d'+1)|S'| - \binom{d'+1}{2}$. Let $A'' = A \cap S'$; since the dimension of A is d, there are elements $a_{d'+1}, \ldots, a_d \in A$ such that the sets $S'+S', a_{d'+1}+A'', \ldots a_d + A''$ are pairwise disjoint. All of them except the first one are contained in $A+A$; the remaining one satisfies $|(S'+S') \setminus (A+A)| = |(S+S) \setminus (A'+A')| \leq \epsilon p$ since ϕ is a Freĭman isomorphism on P. Also, we have $|A''| = |A \cap S'| = |A' \cap S| \geq k - \epsilon p$. Those inequalities combined give

$$|S'+S'| \leq |A+A| + \epsilon p - (d-d')|A''| \leq (K-(d-d'))k + (d-d'+1)\epsilon p.$$

This in turn gives $|S'| \leq \frac{(K-(d-d'))k+(d-d'+1)\epsilon p + \binom{d'+1}{2}}{d'+1} \leq \frac{(K-(d-d'))k+(d-d'+2)\epsilon p}{d'+1}$. By definition of ϵ we have $(d-d'+2)\epsilon p \leq (d+1)\frac{\delta}{32F'(K)(K+\delta)}p \leq \frac{\delta k}{16}$. Now either it follows that

$$|S'| \leq \frac{(K-d+1+\frac{\delta}{2})k}{2},$$

or there exists d' with $(K-(d-d')+\frac{\delta}{8})k > \frac{d'+1}{2}\left(K-d+1+\frac{\delta}{2}\right)k$. Rearranging gives $\frac{\delta}{8} > \frac{d'-1}{2}(K-d-1) + \frac{(d'+1)\delta}{4}$. Since $d' \geq 1$ and $K-d-1 \geq -\frac{\delta}{4}$, the right hand side is at least $\frac{(d'+1)\delta}{4} - \frac{(d'-1)\delta}{8} = \frac{(d'+3)\delta}{8} \geq \frac{\delta}{2}$, which contradicts the previous inequality. It follows that the bound on $|S'|$ is always valid and consequently

$$|\mathcal{A}| \leq p^{O_{\delta,K}(1)}2^{4p\sqrt{\epsilon}}\binom{\lfloor \frac{1}{2}(K-d+1+\frac{\delta}{2})k \rfloor}{k}.$$

We would like the last quantity to be bounded by $\binom{\lfloor \frac{1}{2}(K-d+1+\delta)k \rfloor}{k}$. Let us make some rearrangements to see that this is true:

$$\binom{\lfloor \frac{1}{2}(K-d+1+\delta)k \rfloor}{k} \geq \binom{\lfloor \frac{1}{2}(K-d+1+\frac{\delta}{2})k \rfloor}{k}\left(\frac{\lfloor \frac{1}{2}(K-d+1+\delta)k \rfloor}{\lfloor \frac{1}{2}(K-d+1+\frac{\delta}{2})k \rfloor}\right)^k$$

by Lemma A.0.3. The last ratio is at least $1 + \frac{\delta}{4(K+\delta)} \geq 2^{\delta/4(K+\delta)}$ for k large enough. On the other hand, we have $4p\sqrt{\epsilon} \leq \frac{\delta k}{8(K+\delta)}$. Also, $p^{O_{\delta,K}(1)} \leq 2^{\delta k/8(K+\delta)}$ for k large enough. Combining the bounds, we have shown that

$$|\mathcal{A}| \leq \binom{\lfloor \frac{1}{2}(K-d+1+\delta)k \rfloor}{k}.$$

□

Now we are ready to prove Proposition 5.2.1.

Proof of Proposition 5.2.1. Divide all sets $A \subset [N]$ with $|A| = k$, $|A + A| \leq K|A|$ and $\dim_F A = d$ into Freĭman isomorphism classes and for each class choose its representative in $\mathbb{Z}^d$, not contained in a coset of a proper subgroup. If k is large enough, the number of isomorphism classes is bounded by $\binom{\lfloor \frac{1}{2}(K-d+1+\delta)k \rfloor}{k}$. We need to know how many sets isomorphic to a fixed set $A' \subset \mathbb{Z}^d$ there are in $[N]$. Since A' is not contained in any coset, $\mathbb{Z}^d$ is generated by $a_1 - a_0, \ldots, a_d - a_0$ for some $a_0, \ldots, a_d \in A'$. But then any Freĭman homomorphism $\phi : A' \to [N]$ is uniquely defined by the values $\phi(a_0), \ldots, \phi(a_d)$. This means that there are no more than N^{d+1} sets $A \subset [N]$ isomorphic to A'. In the end, taking $t = d - 1$ we have

$$\#\{A \subset [N] \ : \ |A| = k, \ |A + A| \leq K|A|, \ \dim_F A = t + 1\} \leq \\ \leq N^{t+2} \binom{\lfloor \frac{1}{2}(K - t + \delta)k \rfloor}{k}.$$

□

5.5 Subsets of $\mathbb{F}_2^n$

In this section we consider a counting sets problem in vector spaces over $\mathbb{F}_2$. We use similar methods (which are easier in this setting), but we get a slightly different answer. For a full discussion, see the next secion. Here we prove similar statements as before.

Proposition 5.5.1. *For any $\delta > 0$ there exists a constant $M = M(\delta) > 0$ such that the following statement is true. For every $n > 0$ there exists a family $\mathcal{S}$ of subsets of $\mathbb{F}_2^n$ with $|\mathcal{S}| \leq (2^n)^M$ such that for any $A \subset \mathbb{F}_2^n$, there exists $S \in \mathcal{S}$ with $\max(|A \setminus S|, |(S + S) \setminus (A + A)|) \leq \delta 2^n$.*

Proof. Let $n > 0$ and take any $A \subset \mathbb{F}_2^n$. Apply the regularity lemma (Theorem 2.3.2) with parameter $\epsilon = \frac{\delta^2}{4}$. We get a subspace $V \leq \mathbb{F}_2^n$ of bounded codimension with at least $(1 - \epsilon)2^n$ points ϵ-regular. Now let

$$S = \{x \in \mathbb{F}_2^n \ : \ |(x + A) \cap V| \geq \frac{\delta}{2}|V| \text{ and } (x + A) \cap V \text{ is } \epsilon\text{-uniform}\}.$$

Then S is a union of cosets of V. Since $\operatorname{codim} V$ is bounded, the number of possible subspaces V is polynomial in 2^n by Lemma 2.7.4. Also, if $x, y \in S$, then $|(x + y +$

$A+A)\cap V| \geq |((x+A)\cap V)+((y+A)\cap V)| \geq (1-\frac{\delta}{2})|V|$ by Lemma 2.3.3. Taking into account all cosets of V, we have $|(S+S)\setminus(A+A)| \leq \frac{\delta}{2}|V||[\mathbb{F}_2^n : V]| \leq \delta 2^n$. Also, the points of $A \setminus S$ can be ϵ-regular, and their number is at most $\frac{\delta}{2}2^n$, or irregular, and their number is at most $\frac{\delta^2}{4}2^n \leq \frac{\delta}{2}2^n$. □

Proposition 5.5.2. *Fix $\delta > 0$ and $K \geq 1$. Then the following holds for all integers $k \geq k_0(\delta, K)$. For any $n \in \mathbb{N}$ there are at most*

$$2^{\delta k}\binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{k}$$

affinely generating sets (i.e. not contained in any coset of a proper subgroup) $A \subset \mathbb{F}_2^n$ with $|A| = k$ and $|A+A| \leq K|A|$.

Proof. If we want $|\mathcal{A}| > 0$, there must exist an affinely generating set $A \subset \mathbb{F}_2^n$ with $|A| = k$ and $|A+A| \leq K|A|$. This implies $k \leq 2^n$ and also $2^n \leq F(K)k$ by Theorem 2.7.1.

Let then $n \in [\log_2 k, \log_2 F(K)k]$ be an integer. Apply Proposition 5.5.1 with parameter $\epsilon = (\frac{\delta}{4F(K)})^2$ to get a bounded number of sets S. For each such set we have $|S+S| \leq |A+A| + \epsilon 2^n \leq (K+\epsilon F(K))k \leq 2^\delta Kk$. By Corollary 2.7.2 we get $|S| \leq 2^{\lfloor \log_2 Kk+\delta \rfloor}$. Now to find a set A corresponding to a given set S, we need first to pick an integer $0 \leq l \leq \epsilon 2^n$, then pick $k-l$ elements from S and remaining l elements from $\mathbb{F}_2^n$. Their number is then bounded by

$$\sum_{l=0}^{\lfloor \epsilon 2^n \rfloor}\binom{2^n}{l}\binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{k-l} \leq \binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{k}\sum_{l=0}^{\lfloor \epsilon 2^n \rfloor}\binom{2^n}{l}\binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{l}$$

We can bound the last sum as follows:

$$\sum_{l=0}^{\lfloor \epsilon 2^n \rfloor}\binom{2^n}{l}\binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{l} \leq \sum_{l=0}^{\lfloor \epsilon 2^n \rfloor}\binom{\lfloor F(K)k \rfloor}{l}^2 \leq$$

$$\leq \left(\sum_{l=0}^{\lfloor \epsilon F(K)k \rfloor}\binom{\lfloor F(K)k \rfloor}{l}\right)^2 \leq 2^{2F(K)kH(\epsilon)} \leq 2^{2F(K)k\sqrt{\epsilon}} \leq 2^{\delta k/2}.$$

Here we used inequalities from the appendix. In the end, for k large enough there are at most $2^{\delta k/2}$ possible sets S, which proves the desired bound. □

Theorem 5.5.3. *Fix $\delta > 0$ and $K \geq 1$. Then the following holds for all integers $k \geq k_0(\delta, K)$. For any $n \in \mathbb{N}$ there are at most*

$$2^{\delta k}\binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{k}k^{(1+\delta)n}$$

sets $A \subset \mathbb{F}_2^n$ with $|A| = k$ and $|A+A| \leq K|A|$.

Proof. For a set A let m be its affine dimension over $\mathbb{F}_2$. For a given m, there are at most $4 \cdot 2^{(m+1)(n-m)}$ cosets of m-dimensional subspaces of $\mathbb{F}_2^m$. Inside each of them there are at most $2^{\delta k}\binom{2^{\lfloor \log_2 Kk+\delta \rfloor}}{k}$ generating sets. To find a total number, we need to count the contribution for $m \in [\log_2 k, \log_2 F(K)k]$ for some $F(K)$. The number of such cosets is bounded by

$$\sum_{m=\lceil \log_2 k \rceil}^{\lfloor \log_2 F(K)k \rfloor} 4 \cdot 2^{(m+1)(n-m)} \leq 4\lceil \log_2 F(K) \rceil (2F(K)k)^n.$$

Since k is large enough, we have $4\lceil \log_2 F(K) \rceil (2F(K))^n \leq k^{\delta n}$. Now it is enough to put all the bounds together. □

Now we will show that the above result is always tight up to the occurences of the parameter δ.

Proposition 5.5.4. *Fix $\delta > 0$ and $K \geq 1$. Then the following holds for all integers $k \geq k_0(\delta, K)$. For any $n \in \mathbb{N}$ with $n \geq Kk$ there are at least*

$$2^{-\delta k}\binom{2^{\lfloor \log_2 Kk \rfloor}}{k} k^n$$

sets $A \subset \mathbb{F}_2^n$ with $|A| = k$ and $|A + A| \leq K|A|$.

Proof. Let $m = \lfloor \log_2 Kk \rfloor$. If A is contained in a coset of an m-dimensional subspace V, then $A + A \subset V$ and consequently $|A + A| \leq 2^m \leq Kk$. Therefore we wish to count all the subsets of $\mathbb{F}_2^n$ whose affine span is m-dimensional.

There are at least $2^{(m+1)(n-m)}$ cosets of an m-dimensional subspace in $\mathbb{F}_2^n$. For each coset, choose an affine basis of cardinality $m+1$; there are $\binom{2^m-m-1}{k-m-1}$ k-element sets containing this basis. This way we avoided overcounting and we have at least $2^{(m+1)(n-m)}\binom{2^m-m-1}{k-m-1} \geq 2^{(m+1)(n-2m)}\binom{2^m}{k}$ sets. Further, we can use the following estimate: $2^{(m+1)(n-2m)} \geq (2^n(Kk)^{-2})^{m+1} \geq (Kk)^{n-2m-2}$. Now we have $K^n \geq 1$ and $(Kk)^{2\log_2 Kk+2} \leq 2^{\delta k}$ for k sufficiently large. Combining all the inequalities we get the desired bound. □

To complete the analysis, we need to check that $2^{\delta k}$ is indeed an error term. The number $2^{\lfloor \log_2 Kk \rfloor} \geq \frac{Kk}{2}$ is linear in k. Therefore the term $\binom{2^{\lfloor \log_2 Kk \rfloor}}{k}$ grows exponentially in k (as long as $K > 2$; see Appendix for details). In the end $2^{\delta k}$ is an error term since δ can be arbitrarily small.

5.6 Further discussion

In this section we discuss the relation between the results in the integers and $\mathbb{F}_2^n$. There is a natural correspondence between the bounds in Theorems 1.7.1 and 5.5.3. The term $\frac{1}{2}Kk$ is the size of the largest set $S \subset \mathbb{Z}$ of the integers with $|S+S| \leq Kk$ — an arithmetic progression. In $\mathbb{F}_2^n$ the set S becomes a subspace with $|S| = 2^{\lfloor \log_2 Kk \rfloor}$. The exponent K of N^K is the largest (linear) dimension of a set A with $|A| = k$ and $|A + A| \leq Kk$. This can be far from 2 — the dimension of an arithmetic progression. That is why in general we cannot compare the number of progressions (of dimension 2 and size $\frac{1}{2}Kk$) and sets of dimsnsion K and size k — each of them can be significantly greater than the other. On the other hand in $\mathbb{F}_2^n$ the largest dimension and the dimension of the largest set are both $\log_2 k + O_K(1)$, which can be written as $(1 + o(1)) \log_2 k$. This way the spread of the dimension becomes just an error term, unlike over the integers. The number of all sets with small doubling is then always bounded by the number of subsets of subspaces of size $2^{\lfloor \log_2 Kk \rfloor}$ (up to $(1 + o(1))$ factor in the exponent).

We would also like to note that Propositions 5.3.1 and 5.5.1 look very similar. In fact, one can mimic the proof of Proposition 5.3.1 to get the following statement.

Proposition 5.6.1. *For any $\delta > 0$ there exists a constant $M = M(\delta) > 0$ such that the following statement is true. For every finite abelian group G there exists a family $\mathcal{S}$ of subsets of G with $|\mathcal{S}| \leq |G|^M$ such that for any $A \subset G$, there exists $S \in \mathcal{S}$ with $\max(|A \setminus S|, |(S + S) \setminus (A + A)|) \leq \delta |G|$.*

To get the proof one should run the proof of Proposition 5.3.1 (all the way from Lemma 2.5.1) and replace every instance of $\mathbb{Z}/p\mathbb{Z}$ with G. The only problem appears in the proof of Proposition 2.5.5, where we require some kind of equidistribution of a homomorphism $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{T}$ to argue that for any "nice" partition of $\mathbb{T}$, most of the image lies far from the edges of the partition. This might not be true in general (even if G is large), as seen from the following example.

Example 5.6.2. Let $G = \mathbb{F}_2^n$ and let $\phi : G \to \mathbb{T}$ be a homomorphism. Let $I_j = [\frac{j}{2}, \frac{j+1}{2}) \subset \mathbb{T}$ for $j = 0, 1$ be a partition of $\mathbb{T}$ into two equal parts. Then the entire image of ϕ lies on the edges of the partition.

The above example can be easily fixed though. If we let $I'_j = [\frac{2j-1}{4}, \frac{2j+1}{4})$ for $j = 0, 1$, then $\phi^{-1}(I_j) = \phi^{-1}(I'_j)$ and the distance of each point of $\phi(G)$ to the nearest edge is $\frac{1}{4}$. This construction can be extended to the general case, as seen from the following lemma.

Lemma 5.6.3. *Let G be a finite abelian group and let $\phi : G \to \mathbb{T}$ be a homomorphism. Suppose that $\mathbb{T} = \bigcup_{j=1}^{k} I_j$ is a partition into half-closed intervals. Then there exists a partition $\mathbb{T} = \bigcup_{j=1}^{k} I'_j$ into half closed intervals with the following properties:*

- *$\phi^{-1}(I_j) = \phi^{-1}(I'_j)$ for $j = 1, \ldots, k$,*
- *for any $\lambda > 0$ there are at most $4k\lambda|G|$ elements of G the distance of whose image to the nearest edge of the partition does not exceed λ.*

Proof. Let I'_j be the set of all the points of $\mathbb{T}$ whose distance to $\phi(\phi^{-1}(I_j))$ is smaller than to any other set of this type (in the case of equality, join the point with the interval to the right). This is clearly a partition into half-closed intervals satisfying the first property.

To check the second property, note that the image of G is a finite subgroup of $\mathbb{T}$, the only ones are of the form $\{\frac{x}{n} \ : \ x \in \mathbb{Z}/n\mathbb{Z}\}$ for $n \in \mathbb{N}$. Moreover, the preimages of all the points in the image are all cosets of $\ker \phi$. Since we care only about the proportion of points whose image lies in a certain set, we can replace G with $G/\ker \phi$ and assume that $G = \mathbb{Z}/n\mathbb{Z}$ and $\phi(x) = \frac{x}{n}$.

There are k endpoits of the partition; each of them generates an interval of length 2λ of all the points that lie no further than λ from it. Inside the interval, there are at most $4\lambda n + 1$ points of the form $\frac{y}{2n}$ for $y \in \mathbb{Z}/2n\mathbb{Z}$. By construction, each endpoint is of that form for y odd. It does not belong to $\phi(G)$ though; therefore the number of points of $\phi(G)$ in the interval is at most $4\lambda n$. Since we have k such intervals, the total number of points is bounded by $4k\lambda n$, as claimed. □

Now using the lemma above we can fill the gap in the proof of the analogue of Proposition 2.5.5. Therefore Proposition 5.6.1 has now been verified.

Chapter 6

Probability of holes in a sumset

In this chapter we prove Theorem 1.8.2.

6.1 The Green-Morris Theorem, revisited

Our first step is to prove a variant of the Green-Morris Theorem on counting sets. We will need the fact that a vast majority of sets with small sumset have a certain structure. The actual statement is the following:

Proposition 6.1.1. *For any $\delta \in (0, \frac{1}{2})$ there exists $N_0 = N_0(\delta)$ such that the following statement is true. For every $N > N_0$ and $k, m \geq \delta N$ and all but at most $2^{\frac{m}{2} H(\frac{2k}{m}) - \frac{\delta^2 N}{256}}$ sets $A \subset \{1, \ldots, N\}$ with $|A| = k$ and $|A + A| = m$ there exists an arithmetic progression $P \subset \{1, \ldots, N\}$ with $|P| \leq \frac{(1+\delta)m}{2}$ and $|(A + A) \setminus (P + P)| \leq \delta m$.*

Recall that $H(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$ (see Definition A.0.5).

We will present two proofs of this result. The first one comes the time when Theorem 1.6.11 was not available to us. It still has the advantage of not using the Green-Tao regularity lemma. As a result the constant hidden in the statement of Theorem 1.8.2 ($\mathbb{P}(|\mathbb{N} \setminus (A + A)| \geq k) = \Theta(2^{-k/2})$) is not that huge.

On the contrary, the second proof uses the result about approximating sets from the previous section. It it conceptually simpler, given all our prior knowledge, at the cost of using the Green-Tao regularity lemma. Following this proof, the constants that we obtain are practically ineffective.

For the first proof we need to jump between finite groups and the integers several times. For this reason we prove the following lemma.

Lemma 6.1.2. *Let p be a prime and let $P, Q \subset \mathbb{Z}/p\mathbb{Z}$ be arithmetic progresssions satisfying $|P| \leq \frac{p}{4}$ and $|P \cap Q| \geq \frac{|Q|}{2} + 1$. Then the set $P \cap Q$ is an arithmetic progression with the same common difference as Q.*

Proof. By dilating if necessary, we can assume that P is an interval (i.e. the common difference of P is 1). Since $|P \cap Q| \geq \frac{|Q|}{2} + 1$, we know that there are two consecutive elements of Q that belong to P. That means that the common difference of Q is less than the size of P; let us denote it by d. Suppose for the sake of contradiction, that the intersection $P \cap Q$ is not a progression of common difference d. In other words, if we look at the elements of Q in order, we see at least two separate groups of elements of $P \cap Q$ with at least one element of $Q \setminus P$ in between. Since the common difference of Q is d, each group of elements of $P \cap Q$ has cardinality at most $\left\lceil \frac{|P|}{d} \right\rceil$ and each group of elements of $Q \setminus P$ (maybe except those containing the endpoints) has cardinality at least $\left\lfloor \frac{p-|P|}{d} \right\rfloor$. Also, if we dentote $l = \left\lceil \frac{|P|}{d} \right\rceil$, then

$$\left\lfloor \frac{p-|P|}{d} \right\rfloor > \frac{p-|P|}{d} - 1 \geq \frac{3|P|}{d} - 1 > 3\left\lceil \frac{|P|}{d} \right\rceil - 4 = 3l - 4,$$

so in fact $\left\lfloor \frac{p-|P|}{d} \right\rfloor \geq 3l - 3$. By $d < |P|$ we know that $l \geq 2$. Now denote by $k \geq 2$ the number of groups of elements of $P \cap Q$, we see that the number of groups of $Q \setminus P$ not containing the endpoints is $k - 1$. By assumption $Q \setminus P$ has at least 2 elements less than $P \cap Q$, which leads to the inequality

$$kl \geq |P \cap Q| \geq |Q \setminus P| + 2 \geq (k-1)(3l-3) + 2.$$

Rearranging gives $(2k-3)(2l-3) \leq -1$, which is impossible since both of the factors are positive. □

As we mentioned before, we give two proofs of Proposition 6.1.1. Each is based on a different structural information about subsets of finite cyclic groups.

First proof. First, pick a prime $8N < p < 16N$ and embed $A \subset \{1, \ldots, N\} \hookrightarrow \mathbb{Z}/p\mathbb{Z}$. Then use [23, Theorem 2.1] with parameter $\epsilon = 2^{-27}\delta^4$ to find a prime q, a dilate $A^* = \lambda A$ and a corresponding partition $\mathbb{Z}/p\mathbb{Z} = \bigcup_{i \in \mathbb{Z}/q\mathbb{Z}} I_i$. We may assume that p is so large that the bound on q implies $q \leq \frac{\delta^p}{256} \leq \frac{\delta p}{64}$. We know that at least $(1-\epsilon)q^2$ pairs (i,j) of indices are ϵ-regular, meaning that either $\min(|A_i^*|, |A_j^*|) \leq \epsilon p/q$ or $|A_i^* + A_j^*| \geq (2-\epsilon)p/q$.

Let $S = \{i \in \mathbb{Z}/q\mathbb{Z} \ : \ |A_i^*| \geq \epsilon p/q\}$ and $T = \{i + j \in \mathbb{Z}/q\mathbb{Z} \ : \ |A_i^* + A_j^*| \geq (2-\epsilon)p/q\}$. By ϵ-regularity there at most ϵq^2 pairs $(i,j) \in S^2$ with $i + j \notin T$; in other words, T resembles $S + S$ to some extent.

Suppose that $|S| \geq \frac{(\frac{1}{2} - \frac{\delta}{128})mq}{p}$. We prove that in that case S is contained in an arithmetic progression of length at most $\frac{q+1}{2}$. Indeed, since $(\frac{(1-\epsilon)m}{p})^2 > \epsilon$, there exists at least one regular pair $(i,j) \in S^2$. It follows that $|A_i^* + A_j^*| \geq (2-\epsilon)p/q \geq \frac{p}{q} + \frac{3}{2} \geq$

$\frac{1}{2}|I_{i+j} \cup I_{i+j+1}| + 1$. But $A_i^* + A_j^* \subset (\lambda A) + (\lambda A) \subset \{2\lambda, \dots 2N\lambda\}$ and $A_i^* + A_j^* \subset I_{i+j} \cup I_{i+j+1}$. Since $2N < \frac{p}{4}$, those two progressions satisfy the assumptions of Lemma 6.1.2 and therefore $(I_{i+j} \cup I_{i+j+1}) \cap \{2\lambda, \dots 2N\lambda\}$ is an interval of length at least $(2-\epsilon)p/q \geq \frac{p}{q}+1$. Let $\lambda' \subset \{\frac{1-p}{2}, \dots, \frac{p-1}{2}\} \subset \mathbb{Z}$ with $\lambda\lambda' \equiv 1 \pmod{p}$; it follows that $(\lambda' I_{i+j}) \cup (\lambda' I_{i+j+1})$ is an arithmetic progression of common difference $|\lambda'|$, intersecting an interval $\{2, \dots, 2N\}$ in at least $\frac{p}{q}+1$ points. Therefore $|\lambda'| \leq \frac{2N-2}{\frac{p}{q}} \leq \frac{\frac{p}{4}}{\frac{p}{q}} = \frac{q}{4}$. Now for any $i \in S$ we have $0 < \epsilon p/q \leq |A_i^*| \leq |I_i \cap \{\lambda, \dots, \lambda N\}| = |\lambda' I_i \cap \{1, \dots N\}|$. But every $x \in I_i$ satisfies $\lambda' \frac{x}{p} \in [\frac{\lambda' i}{q}, \frac{\lambda'(i+1)}{q}) \subset \mathbb{R}/\mathbb{Z}$. So this must have a nonempty intersection with $\{\frac{1}{p}, \dots, \frac{N}{p}\} \subset [0, \frac{1}{8}] \subset \mathbb{R}/\mathbb{Z}$. It follows that $\frac{\lambda' i}{q}$ is allowed to be in an interval $[0, \frac{1}{8}] + (-\frac{\lambda'}{q}, 0]$ of length $\frac{|\lambda'|}{q} + \frac{1}{8} \leq \frac{3}{8} < \frac{1}{2}$, as claimed.

We also need some structure of S. To get this, note that for every positive integer t we have

$$\sum_{y \in \mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) \leq \epsilon q^2 + t|T|$$

as there are at most ϵq^2 irregular pairs and the sum of each regular pair belongs to T. Let $t = \lfloor 2^{-13}\delta^2 q \rfloor$; since $m \geq \delta N \geq \frac{\delta p}{16}$ it follows that $\frac{\delta m q}{512p} \geq t \geq 2^{-14}\delta^2 q$ and consequently $\frac{\epsilon q^2}{t} \leq 2^{-13}\delta^2 q \leq \frac{\delta m q}{512p}$. Now by definition of T we have $|(A^* + A^*) \cap (I_y \cup I_{y+1})| \geq (2-\epsilon)p/q$ for each $y \in T$ and consequently

$$\begin{aligned}\frac{(2-\epsilon)p|T|}{q} &\leq \sum_{y \in T} |(A^* + A^*) \cap (I_y \cup I_{y+1})| = \\ &= \sum_{y \in T \cup (T+1)} |(A^* + A^*) \cap I_y| + \sum_{y \in T \cap (T+1)} |(A^* + A^*) \cap I_y| \leq \\ &\leq |A^* + A^*| + \sum_{y \in T \cap (T+1)} |I_y| \leq m + |T \cap (T+1)| \left(\frac{p}{q} + 1\right)\end{aligned}$$

or in other words $m \geq \frac{p}{q}((2-\epsilon)|T| - (1+\frac{\delta}{64})|T \cap (T+1)|)$. It follows that $m \geq (1 - \epsilon - \frac{\delta}{64})|T|\frac{p}{q} \geq (1 - \frac{\delta}{32})|T|\frac{p}{q}$ and consequently $|T| \leq (1 + \frac{\delta}{16})\frac{mq}{p}$. We can plug this bound into the estimate for $1_S * 1_S$ to get

$$\sum_{y \in \mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) \leq \epsilon q^2 + (1 + \frac{\delta}{32})t\frac{mq}{p} \leq (1 + \frac{\delta}{16})t\frac{mq}{p}.$$

We aim to use Theorem 1.6.10. We already know that S is Freĭman isomorphic to a set of integers. What we also need is

$$\frac{1}{t|S|} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) + \frac{5t}{|S|} \leq \frac{1 + \frac{\delta}{16}}{\frac{1}{2} - \frac{\delta}{64}} + \frac{16tp}{mq} \leq \left(2 + \frac{\delta}{4}\right) + \frac{\delta}{4} \leq \frac{9}{4}.$$

Therefore by Theorem 1.6.10 there is a progression $Q \subset \mathbb{Z}/q\mathbb{Z}$ such that $|Q| \leq \frac{2}{t}\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) - 3|S| + 6t \leq (\frac{1}{2}+\frac{\delta}{4})\frac{mq}{p}$ and $|S \setminus Q| \leq \frac{5t}{2}$.

Let us now go back to the inequality $m \geq \frac{p}{q}((2-\epsilon)|T| - (1+\frac{\delta}{64})|T\cap(T+1)|)$; rewrite it as $|T\cap(T+1)| \geq (2-\frac{\delta}{32})|T| - \frac{mq}{p}$ or $2|T| - |T\cap(T+1)| \leq \frac{mq}{p} + \frac{\delta}{32}|T| \leq (1+\frac{\delta}{16})\frac{mq}{p}$. We also know that

$$\sum_{y\in Q+Q} \min(1_S * 1_S(y), t) \geq \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \min(1_{Q\cap S} * 1_{Q\cap S}(y), t) \geq t(2|Q\cap S| - t) \geq t(2|S| - 6t).$$

The contribution of the elements outside T to the above sum is at most ϵq^2, it follows that $\sum_{y\in(Q+Q)\cap T} \min(1_S * 1_S(y), t) \geq t(2|S| - 6t) - \epsilon q^2$ and consequently $|(Q+Q)\cap T| \geq 2|S| - 6t - \frac{\epsilon q^2}{t} \geq (1-\frac{\delta}{32})\frac{mq}{p}$. Now by triangle inequality for set sizes we have

$$\begin{aligned}|(Q+Q)\cap(Q+Q+1)| \geq \\ \geq |(Q+Q)\cap T| - |T| + |T\cap(T+1)| - |T+1| + |(T+1)\cap(Q+Q+1)| = \\ = 2|(Q+Q)\cap T| - (2|T| - |T\cap(T+1)|) \geq \frac{(1-\frac{\delta}{8})mq}{p}.\end{aligned}$$

Let $\lambda^* \in \{\frac{1-q}{2}, \ldots, \frac{q-1}{2}\}$ such that $\lambda^*(Q+Q)$ is an interval. Then $|\lambda^*| = |\lambda^*(Q+Q)| - |\lambda^*(Q+Q+1)| = |Q+Q| - |Q+Q+1| \leq \frac{\delta mq}{4p}$.

Consider now the set $P' = \bigcup_{y\in Q} \lambda^* I_y \subset \mathbb{Z}/p\mathbb{Z}$. Since $\lambda^* I_y \subset \{x \in \mathbb{Z}/p\mathbb{Z} \ : \ \frac{x}{p} \in [\frac{\lambda^* y}{q}, \frac{(\lambda^*+1)y}{q})\}$, the entire P' is contained in $P = \{x \in \mathbb{Z}/p\mathbb{Z} \ : \ \frac{x}{p} \in Q/q + [0, \frac{\lambda^*}{q})\}$. The set $Q/q + [0, \frac{\lambda^*}{q}) \subset \mathbb{R}/\mathbb{Z}$ is an interval of length $\frac{|Q|-1+\lambda^*}{q} \leq \frac{(1+\delta)m-2}{2p}$ and so P is a progression of length at most $\frac{(1+\delta)m}{2}$.

To estimate the size $(A+A)\setminus(P+P)$, note that

$$|(A+A)\cap(P+P)| \geq |(A+A)\cap(P'+P')| = \sum_{y\in(Q+Q)} |(A+A)\cap I_y| \geq$$

$$\geq \sum_{y\in(Q+Q)\cap T} |(A+A)\cap I_y| \geq |(Q+Q)\cap T|(1-2\epsilon)\frac{p}{q} \geq (1-2\epsilon-\frac{\delta}{32})m \geq (1-\delta)m.$$

This was all true when $|S| \geq \frac{(\frac{1}{2}-\frac{\delta}{128})mq}{p}$. Suppose now that $|S| \leq \frac{(\frac{1}{2}-\frac{\delta}{128})mq}{p}$. Then to construct a dilate λA, we first pick an integer $0 \leq l \leq \epsilon p$, then pick $k-l$ points form S and l remaining points from $[N]$. Therefore for a given set S there are at most

$$\sum_{l=0}^{\lfloor 4\epsilon N\rfloor} \binom{|S|}{k-l}\binom{N}{l} \leq \binom{|S|}{k}\sum_{l=0}^{\lfloor 4\epsilon N\rfloor}\binom{|S|}{l}\binom{N}{l}.$$

The last sum can be estimated as $\sum_{l=0}^{\lfloor 4\epsilon N\rfloor}\binom{|S|}{l}\binom{N}{l} \leq \sum_{l=0}^{\lfloor 4\epsilon N\rfloor}\binom{N}{l}^2 \leq (\sum_{l=0}^{\lfloor 4\epsilon N\rfloor}\binom{N}{l})^2 \leq 2^{2NH(4\epsilon)} \leq 2^{8N\sqrt{\epsilon}}$. We also have $\binom{|S|}{k} \leq 2^{k\Phi(\frac{|S|}{k})} \leq 2^{k\Phi((1-\frac{\delta}{64})\frac{m}{2k})} \leq 2^{k(\Phi(\frac{m}{2k})-\frac{\delta}{64})} \leq 2^{k\Phi(\frac{m}{2k})-\frac{\delta^2}{64}N}$. For the definition of Φ and the inequalities used, see the appendix.

The number of possible sets S is $2^q \le 2^{\frac{\delta^2 p}{256}} \le 2^{\frac{\delta^2 N}{256}}$ and the number of dilates is $p < 16N \le 2^{\frac{\delta^2 N}{256}}$. Taking all this into account, the number of possible sets A with $|S| \le (\frac{1}{2} - \frac{\delta}{8})m$ is bounded by

$$2^{N(8\sqrt{\epsilon} - \frac{\delta^2}{64} + \frac{\delta^2}{128})} 2^{k\Phi(\frac{m}{2k})} \le 2^{\frac{m}{2}H(\frac{2k}{m}) - \frac{\delta^2 N}{256}}.$$

□

Second proof. First, pick a prime $2N < p < 4N$ and embed $A \subset \{1, \dots, N\} \hookrightarrow \mathbb{Z}/p\mathbb{Z}$. Then use Proposition 5.3.1 with parameter $\epsilon = \frac{\delta^4}{16}$ to get a set $S \subset \mathbb{Z}/p\mathbb{Z}$ with $\max(|A \setminus S|, |(S+S) \setminus (A+A)|) \le \epsilon p \le 4\epsilon N$. Intersecting S with $\{1, \dots, N\}$ does not change this inequality, and we also have $|\{S \cap \{1, \dots, N\} \ : \ S \in \mathcal{S}\}| \le |\mathcal{S}|$, so we may assume that $S \subset \{1, \dots, N\}$.

Suppose that $|S| \ge (\frac{1}{2} - \frac{\delta}{4})m + 1$. Then $|S+S| \ge (1 - \frac{\delta}{2})m + 1$ and consequently $|(A+A) \setminus (S+S)| = |A+A| - |S+S| + |(S+S) \setminus (A+A)| \le \frac{\delta m}{2} - 1 + 4\epsilon N \le \delta m$. We also have $|S+S| \le |A+A| + |(S+S) \setminus (A+A)| \le |A+A| + 4\epsilon N \le (1 + \frac{\delta}{4})m$. Since $3(\frac{1}{2} - \frac{\delta}{4}) > 1 + \frac{\delta}{4}$, we can use Freĭman $(3k-3)$ Theorem. It gives us a progression $P \subset \{1, \dots, N\}$ containing S with $|P| \le |S+S| - |S| + 1 \le \frac{(1+\delta)m}{2}$. Also, we have $|(A+A) \setminus (P+P)| \le |(A+A) \setminus (S+S)| \le \delta m$.

Now the only thing to prove is that there are at most $2^{-\delta k}\binom{m/2}{k}$ sets A with $|S| \le (\frac{1}{2} - \frac{\delta}{4})m + 1 \le (\frac{1}{2} - \frac{\delta}{8})m$. For each $S \in \mathcal{S}$ satisfying this inequality, the set A can be constructed in the following way: pick a number $0 \le l \le 4\epsilon N$, then pick $k - l$ points from S and l remaining points from $\{1, \dots, N\}$. The total number of such sets A is then bounded by

$$\sum_{l=0}^{\lfloor 4\epsilon N \rfloor} \binom{|S|}{k-l}\binom{N}{l} \le \binom{|S|}{k} \sum_{l=0}^{\lfloor 4\epsilon N \rfloor} \binom{|S|}{l}\binom{N}{l}.$$

The last sum can be estimated as $\sum_{l=0}^{\lfloor 4\epsilon N \rfloor} \binom{|S|}{l}\binom{N}{l} \le \sum_{l=0}^{\lfloor 4\epsilon N \rfloor} \binom{N}{l}^2 \le (\sum_{l=0}^{\lfloor 4\epsilon N \rfloor} \binom{N}{l})^2 \le 2^{2NH(4\epsilon)} \le 2^{8N\sqrt{\epsilon}}$. We also have $\binom{|S|}{k} \le 2^{k\Phi(\frac{|S|}{k})} \le 2^{k\Phi((1-\frac{\delta}{4})\frac{m}{2k})} \le 2^{k(\Phi(\frac{m}{2k}) - \frac{\delta}{4})} \le 2^{k\Phi(\frac{m}{2k}) - \frac{\delta^2}{4}N}$. For the definition of Φ and the inequalities used, see the appendix.

The number of possible sets S is polynomial in $p \le 4N$; for N large enough it is less than $2^{\frac{\delta^2 N}{16}}$. Taking it into account, the number of possible set A with $|S| \le (\frac{1}{2} - \frac{\delta}{8})m$ is bounded by

$$2^{N(8\sqrt{\epsilon} - \frac{\delta^2}{4} + \frac{\delta^2}{16})} 2^{k\Phi(\frac{m}{2k})} \le 2^{\frac{m}{2}H(\frac{2k}{m}) - \frac{\delta^2 N}{16}} \le 2^{\frac{m}{2}H(\frac{2k}{m}) - \frac{\delta^2 N}{256}}.$$

□

As we see, we finished the second proof with a better constant in the exponent. This came at the cost of the size if $N_0(\delta)$ (which we were not bothered to trace).

6.2 Completing the proof

In this section we use the previous results to get Theorem 1.8.2; first let us note that it can be easily reduced to the following statement.

Proposition 6.2.1. *Suppose that $A \subset \mathbb{N}$ is a set chosen randomly by picking each element of $\mathbb{N}$ independently with probability $\frac{1}{2}$. Then the inequality*

$$\mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k \text{ and } 1 \in A) \leq 2^{-(1/2+2^{-25})k}$$

holds for every sufficiently large integer k.

Comparing this to what we are trying to prove in the end, this statement says that for a set A satisfying $|\mathbb{N} \setminus (A+A)| \geq k$ it is exponentially (in k) unlikely to contain 1.

Proof of Theorem 1.8.2 assuming Proposition 6.2.1. Let $A \subset \mathbb{N}$ be a random subset. Note that the conditional distribution of A on the event $1 \notin A$ is exactly the same as the initial distribution of $A+1$. This, and the fact that $\mathbb{P}(1 \in A) = \frac{1}{2}$, allows us to write (for each $k \geq 2$):

$$\begin{aligned} p_k - p_{k-2} &= 2^{k/2} \cdot \mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k) - 2^{(k-2)/2} \cdot \mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k-2) \\ &= 2^{k/2}(\mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k) - \tfrac{1}{2}\mathbb{P}(|\mathbb{N} \setminus ((A+1)+(A+1))| \geq k) = \\ &= 2^{k/2}(\mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k) - \mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k \text{ and } 1 \notin A)) = \\ &= 2^{k/2} \cdot \mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k \text{ and } 1 \in A). \end{aligned}$$

The above quantity is obviously nonnegative, which makes both sequences $\{p_{2k}\}$ and $\{p_{2k+1}\}$ increasing. Proposition 6.2.1 allows us to say they are bounded. Indeed, for k sufficiently large we get

$$p_k - p_{k-2} = 2^{k/2} \cdot \mathbb{P}(|\mathbb{N} \setminus (A+A)| \geq k \text{ and } 1 \in A) \leq 2^{-2^{-25}k}.$$

Summing the above inequalities over numbers of the same parity gives

$$p_k - p_{k_0} \leq \sum_{s=k_0/2}^{\infty} 2^{-2^{-24}s} = \frac{2^{-2^{-25}k_0}}{1-2^{-2^{-24}}} < \infty$$

for an appropriate value of k_0.

We have proved that the sequences $\{p_{2k}\}$ and $\{p_{2k+1}\}$ are increasing and bounded, which makes them convergent. This, and the fact that $p_k > 0$, implies $\mathbb{P}(|\mathbb{N}\setminus(A+A)| \geq k) = \Theta(2^{-k/2})$. □

For the rest of this section we will focus on proving Proposition 6.2.1.

Proof of Proposition 6.2.1. First, let us estimate the probability that $A+A$ does not contain some element $m > 4k$. For any such m, there are at least $\frac{m-1}{2}$ pairs of (not necessarily distinct) natural numbers u, v with $u + v = m$. The probability that $m \notin A + A$ is then bounded by $(\frac{3}{4})^{(m-1)/2}$. All in all,

$$\mathbb{P}(4k + \mathbb{N} \not\subset A + A) \leq \sum_{m=4k+1}^{\infty} (\frac{3}{4})^{(m-1)/2} = \frac{(\frac{3}{4})^{2k}}{1 - \sqrt{\frac{3}{4}}} \leq 8 \cdot \left(\frac{3}{4}\right)^{2k}.$$

Next, let $A' = A \cap [4k]$. Now A' is uniformly distributed over all subsets of $[4k]$. We can then estimate the probability that $|A'| \leq k$:

$$\mathbb{P}(|A'| \leq k) \leq 2^{-3k} \sum_{l=0}^{k} \binom{4k}{k} \leq 2^{4k(H(\frac{1}{4})-1)} = \left(\frac{16}{27}\right)^{2k}.$$

Now assume that $4k + \mathbb{N} \subset A + A$ and $|A'| \geq k$. By definition of A' we have $k \geq |\mathbb{N} \setminus (A + A)| = |[4k] \setminus (A' + A')|$. This together with $A' + A' \subset [8k]$ gives $|A' + A'| \leq 7k$. Now if $|A' + A'| \leq (7 - \frac{1}{128})k$, then we can apply [23, Proposition 3.1] with parameter $\delta = 2^{-11}$ to get that for k large enough the number of such sets is bounded by $2^{4k/2048+(7k/2-k/256)} = 2^{7k/2-k/512}$. The probability of choosing such set is then bounded by $2^{7k/2-k/512-4k} = 2^{-k/2-k/512}$.

Assume then that $(7 - \frac{1}{128})k < |A' + A'| \leq 7k$. Apply Proposition 6.1.1 with parameter $\delta = 2^{-10}$. The number of sets that do not fit the description is bounded by $2^{(7/2-2^{-24})k}$, so the probability of choosing such a set is at most $2^{-(1/2+2^{-24})k}$.

Now suppose that A' fits the description, so that there exists a progression $P \subset [4k]$ with $|P| \leq (\frac{7}{2} + \frac{1}{128})k$ and $|(A' + A') \setminus (P + P)| \leq \frac{k}{128}$. It means that $|P + P| \geq (7 - \frac{1}{128})k - \frac{k}{128} \geq (7 - \frac{1}{64})k$ and so $|P| \geq (\frac{7}{2} - \frac{1}{128})k$. It follows that the common difference of P is 1. Also, $k \leq |[4k]\setminus(A'+A')| \leq |[4k]\setminus(P+P)|+|(P+P)\setminus(A'+A')| = |[4k]\setminus(P+P)|+|P+P|-|A'+A'|+|(A'+A')\setminus(P+P)| \leq |[4k]\setminus(P+P)|+(7+\frac{1}{64})k-(7-\frac{1}{128})k+\frac{k}{128} = |[4k]\setminus(P+P)|+\frac{k}{32}$ and therefore $|[4k]\setminus(P+P)| \geq \frac{31}{32}k$. It means that the least element of $P + P$ is at least $\frac{31}{32}k$. If we now denote $P' = \{\lceil \frac{k}{2} \rceil + 1, \ldots, 4k\}$, we have that $|(P + P) \setminus (P' + P')| \leq \frac{k}{32}$ and hence $|(A' + A') \cap [k + 1]| \leq |(A' + A') \setminus (P' + P')| \leq |(A' + A') \setminus (P + P)| + |(P + P) \setminus (P' + P')| \leq \frac{k}{16}$. Since $1 \in A'$, we have $|A' \cap [k]| = |(1 + A') \cap [k + 1]| \leq |(A' + A') \cap [k + 1]| \leq \frac{k}{16}$. But $A' \cap [k]$ is uniformly distributed among all the subsets of $[k]$ and therefore probability of choosing such set is at most

$$2^{-k} \sum_{l=0}^{\lfloor \frac{k}{16} \rfloor} \binom{k}{l} \leq 2^{k(H(\frac{1}{16})-1)} = \left(\frac{8}{15^{15/16}}\right)^{k} < \left(\frac{2}{3}\right)^{k}$$

In the end the probability that $1 \in A$ and $|\mathbb{N} \setminus (A + A)| \geq k$ is bounded by

$$8 \cdot \left(\frac{3}{4}\right)^{2k} + \left(\frac{16}{27}\right)^{2k} + 2^{-k/2-k/512} + 2^{-(1/2+2^{-24})k} + \left(\frac{2}{3}\right)^{k} \leq 2^{-(1/2+2^{-25})k}$$

for k sufficiently large. □

Appendix A

Estimates of binomial coefficients

In the appendix we state and prove inequalities between various expressions involving binomial coefficients. They are heavily used in Chapters 5 and 6. Although many of them are standard, we keep them here for completeness.

Lemma A.0.1. *Let $m, n, k \geq 0$ be integers with $m \leq n$. Then $\binom{m}{k} \leq \binom{n}{k}$.*

Proof. Each subset of $\{1, \ldots, m\}$ of size k is also a subset of $\{1, \ldots, n\}$. □

Lemma A.0.2. *Let $n, k, l \geq 0$ be integers. Then*

$$\max\left(\binom{n}{k+l}, \binom{n}{k-l}\right) \leq \binom{n}{k}\binom{n}{l}.$$

Proof. We have an identity $\binom{n}{k+l}\binom{k+l}{k} = \frac{n!}{k!l!(n-k-l)!} = \binom{n}{k}\binom{n-k}{l}$. Therefore $\binom{n}{k+l} \leq \binom{n}{k}\binom{n-k}{l} \leq \binom{n}{k}\binom{n}{l}$. To get the second inequality apply the first one to $n, n-k, l$. □

Lemma A.0.3. *Let $m, n, k \geq 0$ be integers with $m \leq n$. Then $\binom{n}{k} \leq \binom{m}{k}\left(\frac{n-k}{m-k}\right)^k$.*

Proof. Note that $\binom{n}{k}\binom{m}{k}^{-1} = \prod_{j=0}^{k-1} \frac{n-j}{m-j}$ and for each j we have $\frac{n-j}{m-j} \leq \frac{n-k}{m-k}$. □

Lemma A.0.4. *Let $0 \leq k \leq n$ be integers. Then the following inequalities hold.*

$$\frac{1}{n+1} \leq \frac{k^k(n-k)^{n-k}}{n^n}\binom{n}{k} \leq 1.$$

Proof. Expand out the equation $1 = (\frac{k}{n} + \frac{n-k}{n})^n$. The number $\frac{k^k(n-k)^{n-k}}{n^n}\binom{n}{k}$ is one of the positive summands, which confirms the latter inequality. To prove the former, note that it is the largest among $n+1$ summands, as the sequance $\frac{k^l(n-k)^{n-l}}{n^n}\binom{n}{l}$ is increasing for $l \leq k$ and decreasing for $l \geq k$. □

Definition A.0.5. The function $H : [0,1] \to \mathbb{R}$ is defined via the formulae

$$H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$$

for $x \in (0,1)$ and $H(x) = 0$ otherwise.

Lemma A.0.6. *Let n be a nonnegative integer and let $\delta \in [0, \frac{1}{2}]$. Then the following inequality holds.*

$$\sum_{k=0}^{\lfloor \delta n \rfloor} \binom{n}{k} \leq 2^{nH(\delta)}$$

Moreover for every $k \in \{0, \ldots, n\}$ we have $\binom{n}{k} = 2^{n(H(\frac{k}{n}) - o(1))}$ as $n \to \infty$.

Proof. For the first part, denote $\lambda = 1 - \delta$. Since $\delta \leq \lambda$, we can write

$$1 = (\delta + \lambda)^n \geq \sum_{k=0}^{\lfloor \delta n \rfloor} \binom{n}{k} \delta^k \lambda^{n-k} \geq \delta^{\delta n} \lambda^{\lambda n} \sum_{k=0}^{\lfloor \delta n \rfloor} \binom{n}{k}.$$

Now by definition of H we have $2^{H(\delta)} = \delta^{-\delta} \lambda^{-\lambda}$ and the first claim follows.

To get the second one, note that $\frac{1}{n+1} = 2^{-o(n)}$ and $\frac{n^n}{k^{l+1}(n-k)^{n-l-1}} = 2^{nH(\frac{k}{n})}$. Therefore it follows from Lemma A.0.4. □

Definition A.0.7. The function $\Phi : [1, \infty) \to \mathbb{R}$ is defined as

$$\Phi(x) = x \log_2 x - (x-1) \log_2 (x-1)$$

for $x > 1$ and $\Phi(1) = 0$. In other words, $\Phi(x) = xH(\frac{1}{x})$.

Corollary A.0.8. Let $k \geq 0$ be an integer and $K \geq 1$ be a real number. Then $\binom{\lfloor Kk \rfloor}{k} = 2^{k(\Phi(K) - o(1))}$ as $k \to \infty$.

Lemma A.0.9. *For any number $x \in [0.1]$, the following inequality holds:*

$$H(x) \leq 2\sqrt{x}.$$

Proof. We will prove a stronger statement, namely $H(x) \leq 2\sqrt{x(1-x)}$. For $x \in \{0,1\}$ it takes the form $0 \leq 0$, so we can focus on $x \in (0,1)$. Let us examine the function $f(x) = \frac{H(x)}{\sqrt{x(1-x)}} = -\sqrt{\frac{x}{1-x}} \log_2 x - \sqrt{\frac{1-x}{x}} \log_2 (1-x)$. We have

$$f'(x) = \frac{-x \log_2 x + (1-x) \log_2 (1-x)}{2\sqrt{x^3 (1-x)^3}}$$

and so the sign of $f'(x)$ is equal to the sign of $g(x) = -x \log x + (1-x) \log (1-x)$. It is easy to check that $\lim_{x \to 0} g(x) = \lim_{x \to 1} g(x) = g(\frac{1}{2}) = 0$ and $g''(x) = \frac{2x-1}{x(1-x)}$. Therefore g is concave and positive on $(0, \frac{1}{2})$ and convex and negative on $(\frac{1}{2}, 1)$. It follows that f has a maximum at $\frac{1}{2}$ with $f(\frac{1}{2}) = 2$. □

Bibliography

[1] Antal Balog and Endre Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, 1994.

[2] Franck Barthe. Optimal young's inequality and its converse: a simple proof. Available at https://arxiv.org/pdf/math/9704210.pdf.

[3] William Beckner. Inequalities in Fourier analysis. *Ann. of Math. (2)*, 102(1):159–182, 1975.

[4] Yuri Bilu. Structure of sets with small sumset. *Astérisque*, (258):xi, 77–108, 1999. Structure theory of set addition.

[5] Béla Bollobás and Imre Leader. Compressions and isoperimetric inequalities. *J. Combin. Theory Ser. A*, 56(1):47–62, 1991.

[6] Herm Jan Brascamp and Elliott H. Lieb. Best constants in Young's inequality, its converse, and its generalization to more than three functions. *Advances in Math.*, 20(2):151–173, 1976.

[7] Augustin Cauchy. Recherches sur les nombres. *J. École Polytechnique*, 9:99–116, 1813.

[8] Henry Davenport. On the addition of residue classes. *J. London Math. Soc.*, 10:30–32, 1935.

[9] Henry Davenport. A historical note. *J. London Math. Soc.*, 22:100–101, 1947.

[10] Matt DeVos. A short proof of Kneser's addition theorem for Abelian groups. In *Combinatorial and additive number theory—CANT 2011 and 2012*, volume 101 of *Springer Proc. Math. Stat.*, pages 39–41. Springer, New York, 2014.

[11] Sean Eberhard. The abelian arithmetic regularity lemma. Available at https://arxiv.org/abs/1606.09303, 2016.

[12] Chaim Even-Zohar. On sums of generating sets in $\mathbb{Z}_2^n$. *Combin. Probab. Comput.*, 21(6):916–941, 2012.

[13] Chaim Even-Zohar and Shachar Lovett. The Freiman-Ruzsa theorem over finite fields. *J. Combin. Theory Ser. A*, 125:333–341, 2014.

[14] John J. F. Fournier. Sharpness in Young's inequality for convolution. *Pacific J. Math.*, 72(2):383–397, 1977.

[15] Gregory A. Freĭman. The addition of finite sets. I. *Izv. Vysš. Učebn. Zaved. Matematika*, 6(13):202–213, 1959.

[16] Gregory A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[17] Gregory A. Freĭman. *Nachala strukturnoi teorii slozheniya mnozhestv*. Kazan. Gosudarstv. Ped. Inst; Elabuž. Gosudarstv. Ped. Inst., Kazan, 1966.

[18] Gregory A. Freĭman. On finite subsets of nonabelian groups with small doubling. *Proc. Amer. Math. Soc.*, 140(9):2997–3002, 2012.

[19] William Timothy Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

[20] B. Green and T. Tao. Compressions, convex geometry and the Freĭman-Bilu theorem. *Q. J. Math.*, 57(4):495–504, 2006.

[21] Ben Green. Notes on progressions and convex geometry. Available at http://people.maths.ox.ac.uk/greenbj/papers/convexnotes.pdf, 2005.

[22] Ben Green. A Szemerédi-type regularity lemma in abelian groups, with applications. *Geom. Funct. Anal.*, 15(2):340–376, 2005.

[23] Ben Green and Robert Morris. Counting sets with small sumset and applications. *Combinatorica*, pages 1–31, 2015.

[24] Ben Green and Imre Z. Ruzsa. Sets with small sumset and rectification. *Bull. London Math. Soc.*, 38(1):43–52, 2006.

[25] Ben Green and Terence Tao. An arithmetic regularity lemma, an associated counting lemma, and applications. In *An irregular mind*, volume 21 of *Bolyai Soc. Math. Stud.*, pages 261–334. János Bolyai Math. Soc., Budapest, 2010.

[26] Ralph Howard. The john ellipsoid theorem. Available at http://people.math.sc.edu/howard/Notes/john.pdf.

[27] Fritz John. Extremum problems with inequalities as subsidiary conditions. In *Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948*, pages 187–204. Interscience Publishers, Inc., New York, N. Y., 1948.

[28] Martin Kneser. Abschätzung der asymptotischen Dichte von Summenmengen. *Math. Z.*, 58:459–484, 1953.

[29] Vsevolod F. Lev and Pavel Y. Smeliansky. On addition of two distinct sets of integers. *Acta Arith.*, 70(1):85–91, 1995.

[30] E. Nazarewicz, M. O'Brien, M. O'Neill, and C. Staples. Equality in Pollard's theorem on set addition of congruence classes. *Acta Arith.*, 127(1):1–15, 2007.

[31] John M. Pollard. A generalisation of the theorem of Cauchy and Davenport. *J. London Math. Soc. (2)*, 8:460–462, 1974.

[32] Øystein J. Rødseth. On Freiman's 2.4-Theorem. *Skr. K. Nor. Vidensk. Selsk.*, (4):11–18, 2006.

[33] Imre Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.*, 65(4):379–388, 1994.

[34] Imre Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, (258):xv, 323–326, 1999. Structure theory of set addition.

[35] Tomasz Schoen. New bounds in Balog-Szemerédi-Gowers theorem. *Combinatorica*, 35(6):695–701, 2015.

[36] Oriol Serra and Gilles Zémor. Large sets with small doubling modulo p are well covered by an arithmetic progression. *Ann. Inst. Fourier (Grenoble)*, 59(5):2043–2060, 2009.

[37] Xuancheng Shao. Large values of the additive energy in $\mathbb{R}^d$ and $\mathbb{Z}^d$. *Math. Proc. Cambridge Philos. Soc.*, 156(2):327–341, 2014.

[38] Endre Szemerédi. Regular partitions of graphs. In *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*, volume 260 of *Colloq. Internat. CNRS*, pages 399–401. CNRS, Paris, 1978.

[39] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[40] A. G. Vosper. The critical pairs of subsets of a group of prime order. *J. London Math. Soc.*, 31:200–205, 1956.