Notes on additive combinatorics

by

Marcel K. Goh

5 May 2023

Note. I am compiling this set of expository notes primarily to solidify these fundamental results of additive combinatorics in my own mind. Sources that are far more comprehensive exist on the web, so I'm not sure how useful this will be to anyone else. Currently, the bulk of these notes come from a series of YouTube lectures of Timothy Gowers (given in early 2022), though I intend in future to add more relevant topics as I learn about them.

1. Plünnecke's theorem

Let A and B be finite subsets of an abelian group. We define the *sumset* $A+B = \{a+b : a \in A,\, b \in B\}$ as well as the *difference set* $A-B = \{a-b : a \in A,\, b \in B\}$. For a nonnegative integer r, the *r-fold iterated sumset* rA is defined recursively by $0A = \{0\}$ and $rA = A+(r-1)A$. The goal of this first section is to show that if the cardinality of a sumset $|A+B|$ is small compared to the size of the set A, then the difference $rB - sB$ of two iterated sumsets must also be small relative to the size of A, in some sense. This result is called Plünnecke's theorem as it follows from a statement given by H. Plünnecke in 1969, though this particular formulation of it was stated and proved by I. Z. Ruzsa in 1989.

Theorem 1 (*Plünnecke,* 1969; *Ruzsa,* 1989). *Let A_0 and B be finite subsets of an abelian group and suppose that $|A_0 + B| \leq K_0|A_0|$ for some constant K_0. Then there exist $A \subseteq A_0$ and $K \leq K_0$ such that for any nonnegative integers r and s, not both zero, we have $|rB - sB| \leq K^{r+s}|A|$. In particular, this means that $|rB - sB| \leq {K_0}^{r+s}|A_0|$.*

Ruzsa used Menger's theorem from graph theory to prove this theorem, but we will use a shorter argument from a 2012 paper by G. Petridis. It hinges on the following lemma. In this proof (and the rest of these notes), we will write $A + x$ instead of $A + \{x\}$ for convenience.

Lemma 2 (*Petridis,* 2012). *Let A and B be subsets of an abelian group and let K be such that $|A_0 + B| = K_0|A_0|$. Then there exist $A \subseteq A_0$ and $K \leq K_0$ such that $|A + B + C| = K|A + C|$ for every finite subset C of the group.*

Proof. We pick $A \subseteq A_0$ nonempty such that the ratio $|A + B|/|A|$, which we shall set as K, is minimised. So $|A + B| = K|A|$ and $|A' + B| \geq K|A'|$ for all $A' \subseteq A_0$. Now we shall show by induction on C that $|A + B + C| \leq K|A + C|$

for all C. If C is empty we are done, of course. Now assume the result holds for C and let $x \notin C$ be arbitrary. We have

$$\big|A + (C \cup \{x\})\big| = |A + C| + |A + x| - |A' + x|$$

where $A' = \{a \in A : a + x \in A + C\}$. But adding x to everything in a set does not change its cardinality, so we have

$$|A + C| + |A + x| - |A' + x| = |A + C| + |A| + |A'|.$$

Also, any element of $A' + B + x$ is an element of $A + B + C$, since $a' + x \in A + C$ for all $a' \in A'$. Applying the induction hypothesis now gives

$$\begin{aligned}\big|A + B + (C \cup \{x\})\big| &\le |A + B + C| + |A + B + x| - |A' + B + x| \\ &\le K|A + B| + K|A| = K|A'| \\ &= K\big|A + (C \cup \{x\})\big|,\end{aligned}$$

which completes the proof. ∎

This lemma has an immediate corollary that already has some resemblance to the version of Plünnecke's theorem that we eventually want to prove.

Corollary 3. *If $|A_0 + B| \le K_0|A_0|$, then there is $A \subseteq A_0$ nonempty and $K \le K_0$ such that $|A + rB| \le K^r|A|$ for all nonnegative integers r.*

Proof. The previous lemma gives A and K such that $|A + B + C| \le K|A + C|$ for all C. We now induce on r. The case $r = 0$ is obvious. Now for $r > 0$ applying the lemma again with $C = (r - 1)B$ and then invoking the induction hypothesis gives

$$|A + rB| = |A + B + (r - 1)B| \le K|A + (r - 1)B| \le K^r|A|. \quad ∎$$

To get from this corollary to the full theorem, we will use a certain inequality of Rusza (1996), which is often called the Ruzsa triangle inequality due to its similarity to the triangle inequality in metric spaces.

Lemma 4 (*Ruzsa triangle inequality*). *Let U, V, and W be finite subsets of an abelian group. Then*

$$|U| \cdot |V - W| \le |U - V| \cdot |U - W|.$$

Proof. For each $x \in V - W$, pick $v(x) \in V$ and $w(x) \in W$ such that $v(x) - w(x) = x$ (there may be multiple choices for each of $v(x)$ and $w(x)$, but we arbitrarily pick one). Define $\phi : U \times (V - W) \to (U - V) \times (U - W)$ by $\phi(u, x) = \big(u - v(x), u - w(x)\big)$. If $\big(u_1 - v(x_1), u_1 - w(x_2)\big) = \big(u_2 - v(x_2), u_2 - w(x_2)\big)$, then subtracting the second coordinate of each pair from the first, we find that

$$x_1 = v(x_1) - w(x_1) = v(x_2) - w(x_2) = x_2,$$

and this also implies that $u_1 = u_2$. So ϕ gives an injection from $U \times (V - 1)$ to $(U - V) \times (U - W)$. ∎

If we define $d(U, V) = |U - V|/\big(|U|^{1/2}|V|^{1/2}\big)$, then this lemma states that $d(U, W) \leq d(V, U)d(U, W)$. Taking logarithms gives a genuine additive triangle inequality, but the space of finite subsets of an abelian group does not form a metric space, since $|U - U|/|U|$ does not equal 1 in general. In any case, we are now able to prove Ruzsa's version of Plünnecke's inequality.

Proof of Theorem 1. Let A and K be given by Lemma 2. By the corollary to that lemma, we have $|A + rB| \leq K^r|A|$ and $|A + sB| \leq K^r|A|$. Cardinalities are not changed by taking additive inverses of everything, so $|-A - rB| \leq K^r|A|$ and $|-A - sB| \leq K^r|A|$. Now an application of Ruzsa's triangle inequality with $U = -A$, $V = rB$ and $W = sB$ yields

$$|A| \cdot |rB - sB| = |-A| \cdot |rB - sB| \leq |-A - rB| \cdot |-A - sB| \leq K^{r+s}|A|^2,$$

and dividing both sides by $|A|$ proves the theorem. ∎

2. Khovanskii's theorem

The goal of this section is to prove the following wonderful theorem of A. Khovanskii.

Theorem 5 (*Khovanskii,* 1992). *Let A be a finite subset of an abelian group and let $f_A(n) = |nA|$ for each $n \in \mathbf{N}$. Then there exists n_A and a polynomial p_A such that $f_A(n) = p_A(n)$ for all $n \geq n_A$.*

Consider the example when $A = \{0, 1, b - 1, b\} \subseteq \mathbf{Z}$. Then letting $[a, b] = \{x \in \mathbf{Z} : a \leq x \leq b\}$, we have

$$nA = [0, n] \cup [b - 1, \ldots, b + n - 1] \cup [2b - 2, 2b + n - 2] \cup \cdots \cup [n(b - 1), nb].$$

This has size $(n + 1)^2$ as long as $n < b - 1$, but when $n \geq b - 1$, nA is simply the set of integers in the range $[0, bn]$, which has size $bn + 1$.

We shall present a combinatorial proof of Khovanskii's theorem, given by M. B. Nathanson and I. Z. Ruzsa in 2002. Let $A = \{a_1, \ldots, a_r\}$ and for $x = (x_1, \ldots, x_r) \in {\mathbf{N}_0}^r$, write

$$\sigma(x) = \sum_{i=1}^{r} x_i \qquad \text{and} \qquad \alpha(x) = \sum_{i=1}^{r} a_i x_i.$$

Then

$$nA = \{\alpha(x) : x \in {\mathbf{N}_0}^r,\ \sigma(x) = n\}.$$

Let $\prec$ be the lexicographic order on ${\mathbf{N}_0}^r$; that is, $(x_1, \ldots, x_r) \prec (y_1, \ldots, y_r)$ if there is some $i \in [r]$ such that $x_i < y_i$ and $x_j = y_j$ for all $1 \leq j < i$. Say that x is *useless* if there is $x' \prec x$ such that $\sigma(x') = \sigma(x)$ and $\alpha(x') = \alpha(x)$; otherwise, say that x is *useful*. It is easy to see that $|nA|$ is exactly the number of useful x with $\sigma(x) = n$. Now let $\leq$ denote the usual partial order on ${\mathbf{N}_0}^r$, where $(x_1, \ldots, x_r) \leq (y_1, \ldots, y_r)$ if $x_i \leq y_i$ for all $1 \leq i \leq r$.

Lemma 6. *If $x \leq y$ and x is useless, then y is useless.*

Proof. Since x is useless, we can find $x' \prec x$ with $\sigma(x') = \sigma(x)$ and $\alpha(x') = \alpha(x)$. Let $y' = y + x' - x$. Since $x \leq y$, $y - x$ is in ${\mathbf{N}_0}^r$ and therefore so is y'. Then since $x'_i < x_i$ for the first i at which the two tuples differ, the first coordinate at which y' and y differ is also i and we have $y'_i < y_i$. Hence $y' \prec y$. Lastly,

$$\sigma(y') = \sigma(y + x' - x) = \sigma(y) + \sigma(x') - \sigma(x) = \sigma(y)$$

and the same is true with σ replaced by α, so y is useless. ∎

For each useless x we can find a useless x', minimal in the $\leq$ order, such that $x' \leq x$. This lemma gives a converse; it says that if x' is a minimal useless element and $x' \leq x$, then x is also useless.

Lemma 7. *For any nonempty $U \subseteq {\mathbf{N}_0}^r$, the set of minimal elements of U (with respect to the $\leq$ order) is finite.*

Proof. We perform induction on r. If $r = 1$, then it is clear that U has exactly one minimal element. Now let $r > 1$ and let u be a minimal element of u. Then for every $v \in U$ with $u \not\leq v$, there exists some i and $t < u_i$ such that $v_i = t$. Let

$$V(i,t) = \{v \in U : v_i = t\}$$

for all $1 \leq i \leq r$ and $0 \leq t < u_i$. Each set $V(i,t)$ is order-isomorphic to a subset of ${\mathbf{N}_0}^{r-1}$, so by induction it has finitely many minimal elements. The number of $V(i,t)$ is $r \prod_{i=1}^{r} u_i$, and every minimal element of u is either u or a minimal element of some $V(i,t)$, so there are finitely many minimal elements in U. ∎

We will need just one more lemma before we are able to prove Khovanskii's theorem. It shows that for any fixed r-tuple x', the number of x with $x' \leq x$ and $\sigma(x) = n$ is given by a polynomial in the variable n, with coefficients depending on x' and r.

Lemma 8. *Let $x' \in {\mathbf{N}_0}^r$ and for $n \geq \sigma(x')$, let*

$$C(x', n) = \{n \in {\mathbf{N}_0}^r : \sigma(x) = n,\, x' \leq x\}.$$

Then

$$\left|C(x', n)\right| = \binom{n - \sigma(x') + r - 1}{r - 1}.$$

Proof. Given $x \in C(x', n)$, map it to $x - x'$. This is a bijection from $C(x', n)$ to $C(0, n - \sigma(x')$. Now let $m = n - \sigma(x')$. The map $(x_1, \ldots, x_r) \mapsto (x_1, +1, \ldots, x_r + 1)$ is a bijection from $C(0, m)$ to the set of $y \in \mathbf{N}^r$ such that $y_1 + \cdots + y_r = m + r$. Now the map

$$(y_1, \ldots, y_r) \mapsto \{y_1, y_1 + y_2, \ldots, y_1 + \cdots + y_r\}$$

is a bijection from the previous set to the set of subsets of $[m+r]$ that contain $m+r$. (It is inverted by the map $\{a_1,\dots,a_r\} \mapsto (a_1, a_2-a_1,\dots,a_r-a_{r-1})$.) But this final set has size $\binom{m+r-1}{r-1}$, so we are done. ∎

Without further ado, let us now prove Khovanskii's theorem.

Proof of Theorem 5. Let U be the set of all useless r-tuples. By Lemma 7, the set $X \subseteq U$ of all minimal useless r-tuples is finite. Recall that $|nA|$ is the number of useful x such that $\sigma(x) = n$, so using the notation of the previous lemma, we have

$$|nA| = \big|C(0,n)\big| - \Big|\bigcup_{x'\in X} C(x',n)\Big| = \big|C(0,n)\big| - \sum_{Y\subseteq X}(-1)^{|Y|}\Big|\bigcap_{x'\in Y} C(x',n)\Big|$$

But for any $Y \subseteq X$, $\bigcap_{x'\in Y} C(x',n) = C(x_Y,n)$, where x_Y has for its ith coordinate the integer $\max_{y\in Y} y_i$. Hence every term in the inclusion-exclusion formula depends polynomially on n once

$$n \geq \sum_{1\leq i\leq r} \max_{x\in X} x_i. \quad ∎$$

3. The Balog–Szemerédi–Gowers theorem

Let A be a finite nonempty subset of an abelian group. An *additive quadruple* in A is a quadruple $(x,y,z,w) \in A^4$ such that $x+y = z+w$. The *additive energy* $E(A)$ of A is the number of additive quadruples in A. If (x,y,z,w) is an additive quadruple, then $w = x+y-z$, so $E(A) \leq |A|^3$. The following lemma roughly states that if a set has a small sumset, then it has large additive energy.

Lemma 9. *Let A be a finite subset of an abelian group and let C be such that $|A+A| \leq C|A|$. Then $E(A) \geq |A|^3/C$.*

Proof. Define $f : A+A \to \mathbf{N}$ by letting $f(d)$ equal the number of pairs $(a,b) \in A^2$ such that $a+b = d$. Then

$$\sum_{d\in A+A} f(d) = |A|^2 \qquad \text{and} \qquad \sum_{d\in A+A} f(d)^2 = E(A).$$

By the Cauchy–Schwarz inequality,

$$|A|^2 = \sum_{d\geq 1} 1\cdot f(d) \leq \Big(\sum_{d\geq 1} 1\Big)^{1/2}\Big(\sum_{d\geq 1} f(d)^2\Big)^{1/2} \leq C^{1/2}|A|^{1/2}E(A)^{1/2}.$$

From here, squaring the whole inequality and then dividing through by $C|A|$ gives the statement we want to prove. ∎

The converse of this lemma does not hold. For example, we could take the disjoint union of an arithmetic progression with a geometric progression of the

same length. This set has a large additive energy, because of the arithmetic progression, but it also has a large sumset, because of the geometric progression. However, we can pass to a large subset that has a small sumset (namely, the arithmetic progression), and this is essentially the statement of the Balog–Szemerédi–Gowers theorem. We shall state it later on in the section, after we have given the graph-theoretic definitions and lemmas needed in its proof.

Let G be a bipartite graph with finite vertex sets X and Y. For a vertex $v \in X \cup Y$, let $d(v) = \deg(v)$ denote the *degree* of x, that is, the number of vertices adjacent to v. For $x_1, x_2 \in X$, let $d(x_1, x_2)$ denote the number of paths of length 2 from x_1 to x_2. This is called the *codegree* of x_1 and x_2. The *density* of G is the number of edges of G divided by the maximum number of vertices it could have, namely $|X| \cdot |Y|$.

Lemma 10. *Let G be a bipartite graph with bipartition $X \cup Y$ and let the density of G be δ. Then for every $c > 0$ there is a subset $X' \subseteq X$ with $|X'| \geq \delta|X|/\sqrt{2}$ such that the number of pairs $(x_1, x_2) \in (X')^2$ with $d(x_1, x_2) < c|Y|$ is at most $2c|X|^2/\delta^2$.*

Proof. Let $y \in Y$ be chosen uniformly at random. Letting $X' = N(y)$, we have

$$\mathbf{E}\big\{|X'|\big\} = \mathbf{E}_{y \in Y}\big\{d(y)\big\} = \frac{1}{|Y|}\sum_{y \in Y} d(y) = \frac{|E(G)|}{|Y|} = \delta|X|.$$

By convexity of the map $x \mapsto x^2$, we then find that $\mathbf{E}\big\{|X'|^2\big\} \geq \delta^2|X|^2$. Let

$$B = \big\{(x_1, x_2) \in X^2 : d(x_1, x_2) < c|Y|\big\}.$$

The probability that any $(x_1, x_2) \in B$ is also in $(X')^2$ is the same as the probability that y is connected to both x_1 and x_2; this is less than $c|Y|$ by the construction of B. So by linearity of expectation, $\mathbf{E}\big\{|B \cap (X')^2|\big\} < c|X|^2$ and in particular, we have

$$\left\{|X'|^2 - \frac{\delta^2}{2c}|B \cap (X')^2|\right\} > \left(\delta^2 - \frac{\delta^2}{2c} \cdot c\right)|X|^2 = \frac{\delta^2}{2}|X|^2.$$

So there is X' such that $|X'| - \big(\delta^2/(2c)\big)|B \cap (X')^2| \geq \delta^2|X|^2/2$. This set X' has cardinality at least $\delta|X|/\sqrt{2}$ and $|B \cap (X')^2| \leq 2c|X'|^2/\delta^2$. ∎

This lemma says that we can find a fairly large subset of X such that almost every pair in this subset is joined by at least $c|Y|$ paths of length 2. We would really like to remove the "almost" in this statement, but to do so, we will have to pass to paths of length 3. First, we need a little lemma about sums of real numbers between 0 and 1.

Lemma 11. *Let $a_1, \dots, a_n \in [0, 1]$. If $\sum_{i=1}^n a_i \geq an$, then the number of i such that $a_i \geq b$ is at least*

$$\left(\frac{a-b}{1-b}\right)n.$$

Proof. Let I be the set of i such that $a_i \geq b$. Then we may write

$$an \leq \sum_{i=1}^{n} a_i = \sum_{i \in I} a_i + \sum_{i \notin I} a_i \leq |I| + (n - |I|)b.$$

It remains to isolate for $|I|$. ∎

For example, if $b = a/2$, then the number of i with $a_i \geq b$ must be at least $an/2$, and more generally, if $a = 1 - \theta$ and $b = 1 - \eta$, then the number of such i is at least $(1 - \theta/\eta)n$. If $\eta = 2\theta$, then $a_i \geq 1 - 2\theta$ at least half the time. Next we prove the lemma alluded to earlier, concerning paths of length 3.

Lemma 12. *Let G be a bipartite graph with vertex sets X and Y and density δ. Then there are subsets $X' \subseteq X$ and $Y' \subseteq Y$ such that*

$$|X'| \geq \frac{\delta^2}{8\sqrt{2}}|X| \qquad \text{and} \qquad |Y'| \geq \frac{\delta}{4}|Y|$$

and every $x \in X'$ and $y \in Y'$ are joined by at least $(\delta^6/2^{13})|X| \cdot |Y|$ paths of length 3 in G.

Proof. By letting $n = |X|$ and setting the a_i equal to the degrees of the vertices in X, we have $a = \delta|Y|$ and we can choose $b = a/2$ in the previous lemma to deduce that X has a subset X_1 such that every vertex in X_1 has degree at least $\delta|Y|/2$ and $|X_1| \geq \delta|X|/2$. Note that the density of the bipartite subgraph with vertex set $X_1 \cup Y$ is $\geq \delta/2$, so we may invoke the lemma about paths of length 2 with δ set to $\delta/2$. It tells us that for any $c > 0$, X_1 has a subset X_2 of size $\delta|X_1|/2^{3/2}$ such that for all but at most $8c|X_2|^2/\delta^2$ pairs $(x_1, x_2) \in {X_2}^2$, we have $d(x_1, x_2) \geq c|Y|$.

Now let Γ be a graph with vertex set X_2 and an edge between x_1 and x_2 if and only if $\delta(x_1, x_2) \geq c|Y|$. Note that by this definition, there may be loops in Γ. In any case, the average degree in Γ is at least $(1 - 8c/\delta^2)|X_2|$. Invoking the previous lemma again, at least half the vertices in X_2 have degree at least $(1 - 16c/\delta^2)|X_2|$. Let X' be the set of all such vertices. Then

$$|X'| \geq \frac{|X_2|}{2} \geq \frac{\delta|X_1|}{4\sqrt{2}} \geq \frac{\delta^2|X|}{8\sqrt{2}}.$$

Every vertex in X_2 has degree at least $\delta|Y|/2$, so the bipartite subgraph on $X_2 \cup Y$ has density at least $\delta/2$ and the average degree of $y \in Y$ is at least $\delta|X_2|/2$. The previous lemma comes in handy once again, telling us that at least $\delta|Y|/4$ vertices in Y has degree at least $\delta|X_2|/4$. Let Y' be the set of these vertices.

For any $x \in X'$ and $y \in Y'$, we know that x has at least $(1 - 16c/\delta^2)|X_2|$ neighbours in Γ and y has at least $\delta|X_2|/4$ neighbours in X_2. There must be at least $(\delta/4 - 16c/\delta^2)|X_2|$ neighbours in commmon. Letting $c = \delta^3/128$, the

number of neighbours in common becomes $\delta|X_2|/8$, and the number of paths of length 3 from x to y is at least

$$\frac{\delta|X_2|}{8}|X_2| \cdot c|Y| = \frac{\delta}{8} \cdot \frac{\delta^3}{128} \cdot \frac{\delta^2}{4\sqrt{2}}|X| \cdot |Y| \geq \frac{\delta^6}{2^{13}}|X| \cdot |Y|,$$

as foretold. ∎

Let A be a finite subset of an abelian group. We say that an element $d \in A - A$ is *θ-popular* if $\big|\{(a,b) \in A^2 : b - a = d\}\big| \geq \theta|A|$.

Lemma 13. *Let A be a finite subset of an abelian group and let $E(A)$ denote the additive energy of A. If $E(A) \geq c|A|^3$, then there are at least $c|A|/2$ elements of $A - A$ that are $(c/2)$-popular.*

Proof. Define $f : A - A \to \mathbf{N}$ by $f(d) = \big|\{(a,b) \in A^2 : b - a = d\}\big|$. Note that

$$\sum_{d \in A-A} f(d) = |A|^2 \qquad \text{and} \qquad \sum_{d \in A-A} f(d)^2 = E(A).$$

Let P be the set of $(c/2)$-popular differences and let $U = (A - A) \setminus P$. Then

$$\begin{aligned} c|A|^3 &\leq E(A) \\ &= \sum_{d \in A-A} f(d)^2 \\ &= \sum_{d \in P} f(d)^2 + \sum_{d \in U} f(d)^2 \\ &\leq |P| \cdot |A|^2 + \frac{c|A|}{2} \sum_{d \in U} f(d) \\ &= |P| \cdot |A|^2 + \frac{c|A|^3}{2}, \end{aligned}$$

which implies that $|A| \geq c|A|/2$. ∎

We are, at long last, ready to state and prove the Balog–Szemerédi–Gowers theorem. It is named for A. Balog and E. Szemerédi, who first proved it in 1994, as well as for W. T. Gowers, who gave an alternative proof in 1998 that yielded power-type bounds, a vast improvement to the tower-type bounds in Balog and Szemerédi's proof.

Theorem 14 (*Balog–Szemerédi,* 1994; *Gowers,* 1998). *Let A be a finite subset of an abelian group with $E(A) \geq c|A|^3$. Then A has a subset A' of size at least $c'|A|$ such that $|A' - A'| \leq C|A'|$, where c' and C have a power-type dependence on c. In particular, we may take*

$$c' = \frac{c^4}{2^8} \qquad \text{and} \qquad C = \frac{2^{68}}{c^{36}}.$$

Proof. Define a bipartite graph G with both vertex sets being copies of A (though we'll call one of these copies B to avoid any confusion). Join $a \in A$ to $b \in B$ if and only if $b-a$ is $(c/2)$-popular. Each $(c/2)$-popular difference leads to at least $c|A|/2$ edges, so by the lemma, there are at least $c^2|A|^2/4$ edges. Let $\delta = c^2/4$. By the lemma concerning paths of length 3, there exist $A' \subseteq A$ and $B' \subseteq B$ with

$$|A'| \geq \frac{\delta^2}{8\sqrt{2}}|A| \qquad \text{and} \qquad |B'| \geq \frac{\delta}{4}|A|$$

such that every $a \in A$ and $b \in B$ are joined by at least $\delta^6|A|^2/2^{13}$ paths of length 3 in G.

Given a path (a, u, v, b) of length 3, we have $b-a = u-a-(u-v)+b-v$, where $u-a$, $u-v$, and $b-v$ are all $(c/2)$-popular. Hence the number of ways of writing $b-a$ as $r_1 - s_1 - (r_2 - s_2) + r_3 - s_3$ is at least

$$\frac{\delta^6}{2^{13}}|A|^2\left(\frac{c}{2}|A|\right)^3 = \frac{c^{15}}{2^{28}}|A|^5.$$

But the number of possible $(r_1, s_1, r_2, s_2, r_3, s_3)$ is $|A|^6$. So

$$|B'-A'| \cdot \frac{c^{15}}{2^{28}}|A|^5 \leq |A|^6$$

and $\frac{|B'-A'| \leq 2^{28}|A|}{c^{15}}$. Now the Ruzsa triangle inequality with $U = B'$ and $V = W = A'$ tells us that $|B'| \cdot |A'-A'| \leq |B'-A'|^2$, so

$$|A'-A'| \leq \frac{|B'-A'|^2}{|B'|} \leq \frac{2^{56}|A|^2}{c^{30}} \cdot \frac{2^4}{c^2|A|} = \frac{2^{60}}{c^{32}}|A|.$$

But recall that

$$|A'| \geq \frac{\delta^2}{8\sqrt{2}}|A| \geq \frac{c^4}{2^8}|A|,$$

so $|A'-A'| \leq 2^{68}|A'|/c^{36}$. ∎

4. Freiman homomorphisms and Ruzsa embedding lemmas

We have been talking a lot about finite subsets of abelian groups, so it's about time we gave a special name for these sets. An *additive set* is a pair (A, Z) where Z is an abelian group and A is a finite subset of Z. In almost all cases we shall suppress mention of Z and speak simply of an additive set A.

Let A and B be additive sets (not necessarily in the same group). A function $\phi : A \to B$ is a *Freiman homomorphism of order k* if for any $2k$ elements $a_1, \ldots, a_k, b_1, \ldots, b_k \in A$ satisfying $a_1 + \cdots + a_k = b_1 + \cdots + b_k$, we also have $\phi(a_1) + \cdots + \phi(a_k) = \phi(b_1) + \cdots + \phi(b_k)$. The existence of such a ϕ tells us that the additive relationships among the elements of A are approximately the

same as the additive relationships in B. Note that a Freiman homomorphism of order k is also a Freiman homomorphism of order k' for all $k' > k$. If we write simply "Freiman homomorphism", then we mean a Freiman homomorphism of order 2, and we will sometimes write "k-homomorphism" instead of "Freiman homomorphism of order k".

A k-homomorphism $\phi : A \to B$ induces a map from kA to kB. Indeed, if we define $\psi : kA \to kB$ by

$$\psi(a_1 + \cdots + a_k) = \phi(a_1) + \cdots + \phi(a_k),$$

then the definition of k-homomorphism ensures that ϕ is well-defined. More generally, if ϕ is a $k(r+s)$-homomorphism, then defining $\psi : rA - sA \to rB - sB$ by

$$\phi(a_1 + \cdots + a_r - a'_1 - \cdots - a'_s) = \phi(a_1) + \cdots + \phi(a_r) - \phi(a'_1) - \cdots - \phi(a'_s),$$

it is easy to see that ψ is a k-homomorphism. It is also clear that if ϕ is the restriction of a group homomorphism to A, then ϕ is a k-homomorphism for every k, and if $\phi : A \to B$ and $\psi : B \to C$ are k-homomorphisms, then $\psi \circ \phi : A \to C$ is a k-homomorphism as well.

If $\phi : A \to B$ is a k-homomorphism with an inverse that is also a k-homomorphism, then we say that ϕ is a *Freiman isomorphism of order k* or, more briefly, a *k-isomorphism*. These maps preserve a lot of the properties that are of interest in additive combinatorics. Suppose that A is k-isomorphic to B. Then

i) $|kA| = |kB|$;
ii) $|rA - sA| = |rB - sB|$ for all r and s with $r + s \leq k$;
iii) $E(A) = E(B)$ if $k = 2$; and
iv) if $k = 2$ and A contains an arithmetic progression of length r, then so does B.

Of these statements, the only slightly nontrivial one is (iv). It follows from the fact that an arithmetic progression is a sequence $(a_1, \ldots, a_r)$ with $a_i + a_i = a_{i-1} + a_{i+1}$ for all $1 < i < r$. Taking ϕ of both sides gives

$$\phi(a_i) + \phi(a_i) = \phi(a_i + a_i) = \phi(a_{i-1} + a_{i+1}) = \phi(a_{i-1}) + \phi(a_{i+1}).$$

Let us now state and prove two important "embedding lemmas". These lemmas tell us that if $kA - kA$ is not too large, then the additive set A is k-isomorphic to a subset of a group that is simpler, in some sense.

Lemma 15 (*Ruzsa embedding lemma in $\mathbf{F}_p^N$*). *Let $k \geq 1$ and $C > 0$. Let $A \subseteq \mathbf{F}_p^N$ be such that $|kA - kA| \leq C|A|$. Then A is isomorphic to a subset of $\mathbf{F}_p^n$, where $p^{n-1} < C|A|$.*

Proof. Let X be a subspace of $\mathbf{F}_p^N$ chosen uniformly at random from all subspaces of codimension n, where n will be specified later. Let $q : \mathbf{F}_p^N \to \mathbf{F}_p^N/X$ be the

quotient map taking v to $v+X$. Since q is a group homomorphism, its restriction to A is a Freiman homomorphism of order k. The only way that the restriction of q to A can fail to be a *k-isomorphism* is if there exist $a_1, \dots, a_k, b_1, \dots, b_k \in A$ such that $a_1 + \cdots + a_k \neq b_1 + \cdots + b_k$ but $q(a_1) + \cdots + q(a_k) = q(b_1) + \cdots + q(b_k)$. This is equivalent to $a_1 + \cdots + a_k - b_1 - \cdots - b_k$ being in X. For any nonzero $y \in \mathbf{F}_p^N$, we have

$$\mathbf{P}\{y \in X\} = \frac{p^{N-n} - 1}{p^N - 1} < \frac{1}{p^n},$$

and since $|kA - kA| \leq C|A|$,

$$\mathbf{P}\left\{ \bigcup_{y \in (kA-kA)\setminus\{0\}} \{y \in X\} \right\} \leq \sum_{y \in (kA-kA)\setminus 0} \mathbf{P}\{y \in X\} < \frac{C|A|}{p^n},$$

the probability that q is a k-isomorphism is nonzero so long as $p^n \geq C|A|$. Taking the minimal such n, we have $p^{n-1} < C|A|$ and can conclude there is a subspace X of dimension n that contains a set k-isomorphic to A. ∎

Next, we will prove an embedding lemma for subsets of $\mathbf{Z}$. In this setting the "simpler" group that we pass to is a cyclic group, but first we need a lemma that essentially says that passing to a cyclic group preserves the additive structure.

Lemma 16. *Let k and n be positive integers and let $A \subseteq \mathbf{Z}$ be a set of diameter less than n/k; i.e., $\max A - \min A < n/k$. Then the map $\phi : A \to \mathbf{Z}_n$ that sends $a \mapsto a \bmod n$ is a Freiman isomorphism of order k.*

Proof. The function ϕ is the restriction of a group homomorphism to A, so it is a Freiman homomorphism of every order. Now suppose that $\min A = r$ and $\max A = s$, so that $s - r < n/k$. Then if $a_1, \dots, a_k, b_1, \dots, b_k$ are such that $\phi(a_1) + \cdots + \phi(a_k) = \phi(b_1) + \cdots + \phi(b_k)$, then $a_1 + \cdots + a_k - b_1 - \cdots - b_k$ is at most $k(s-r) < n$ but also a multiple of n. Hence this difference is zero and $a_1 + \cdots + a_k = b_1 + \cdots + b_k$. ∎

As promised, here is the embedding lemma for subsets $A \subseteq \mathbf{Z}$. This time, we cannot simply say anything about the whole set A, but we can about a large subset of it.

Lemma 17 (*Ruzsa embedding lemma in* $\mathbf{Z}$). *Let $k \in \mathbf{N}$ and $C \in \mathbf{R}$. If $A \subseteq \mathbf{Z}$ with $|kA - kA| \leq C|A|$, then there exists $A' \subseteq A$ with $|A'| \geq |A|/k$ such that A' is k-isomorphic to a subset of $\mathbf{Z}/N\mathbf{Z}$, where N is a prime between $2C|A|$ and $4C|A|$.* ∎

Proof. It is easily checked that translation is a Freiman isomorphism of every order, so we may assume that $A \subseteq \mathbf{N}_0$. Let p be a prime bigger than $k \max A$ and consider the sequence of functions

$$\mathbf{Z} \xrightarrow{q_1} \mathbf{Z}_p \xrightarrow{\mu_r} \mathbf{Z}_p \xrightarrow{\iota} \mathbf{Z} \xrightarrow{q_2} \mathbf{Z}_N,$$

where q_1 is reduction modulo p, μ_r is multiplication by a random nonzero element $r \in \mathbf{Z}_p$, ι takes an element of $\mathbf{Z}_p$ to its representative in $[0,p)$, and q_2 is reduction mod N. The only map here that is not a group homomorphism is ι, so to show that the composition $\phi = q_2 \circ \iota \circ \mu_r \circ q_1$ restricted to A is a k-homomorphism, it suffices to worry about ι. Split the interval $\{0, 1, \dots, p-1\}$ into k subintervals $J_1, \dots, J_k$, each of diameter less than p/k and let $I_j = \iota^{-1}(J_j)$ for each $1 \le j \le k$. By the previous lemma, the map ι^{-1} restricted to any J_j is a k-isomorphism, so ι restricted to I_j is a k-isomorphism as well. Now let

$$A_{j,r} = \big\{a \in A : \mu_r\big(q_1(a)\big) \in I_j\big\}$$

and note that $\mu_r\big(q_1(a)\big) = ra \bmod p$. Thus the composition ϕ is a k-homomorphism when restricted to any $A_{j,r}$.

We shall now show that with positive probability, the restriction of ϕ to every $A_{j,r}$ is a k-isomorphism. For fixed r, the restriction to $A_{j,r}$ is not a k-isomorphism if there exist j and $a_1, \dots, a_k, b_1, \dots, b_k \in A_{j,r}$ such that $a_1 + \cdots + a_k \ne b_1 + \cdots + b_k$ but $\phi(a_1) + \cdots + \phi(a_k) = \phi(b_1) + \cdots + \phi(b_k)$.

5. Basics of discrete Fourier analysis

Let Z be a finite abelian group. A *character* on Z is a homomorphism from Z to the multiplicative group $\mathbf{C} \setminus \{0\}$. If χ is such a homomorphism, then $\big|\chi(x)\big| = 1$ for every $x \in Z$, so we can actually regard χ as being a function from Z to the unit circle $\mathbf{T} = \{z \in \mathbf{C} : |z| = 1\}$. The pointwise product of two characters gives another character, and the function χ_0 that sends every $x \in Z$ to 1 has the property that if χ is any character, then $\chi\chi_0 = \chi = \chi_0\chi$. Lastly, we note that multiplication is commutative and for any character χ, the product of χ with $\overline{\chi}$ gives χ_0, so the set of characters on Z is an abelian group. This is called the *dual group* (or sometimes the *Pontryagin dual*) of Z and is denoted $\widehat{Z}$.

We define an inner product on the space $\mathbf{C}^Z$ of functions from Z to $\mathbf{C}$ by setting

$$\langle f, g\rangle = \mathbf{E}_x\, f(x)\overline{g(x)},$$

where $\mathbf{E}_{x\in Z}\, F(x) = |Z|^{-1} \sum_{x\in Z} F(x)$. We can also make $\widehat{Z}$ into an inner product space by letting

$$\langle \widehat{f}, \widehat{g}\rangle = \sum_{\chi\in\widehat{Z}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)};$$

note that this time we do not normalise by dividing by $|Z|$. Two functions f and g in an inner product space are said to be *orthogonal* if $\langle f, g\rangle = 0$. The first lemma we'll prove concerns certain orthogonality relations.

Lemma 18 (*Orthogonality relations*). *Let Z be a finite abelian group.*

a) If χ_1 and χ_2 are characters on Z, then

$$\langle \chi_1, \chi_2\rangle = \mathbf{E}_{x\in Z}\, \chi_1(x)\overline{\chi_2(x)} = \begin{cases} 1, & \text{if } \chi_1 = \chi_2; \\ 0, & \text{if } \chi_1 \ne \chi_2. \end{cases}.$$

b) For $x, y \in Z$, we have

$$\sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)} = \begin{cases} |\widehat{Z}|, & \text{if } x = y; \\ 0, & \text{if } x \neq y, \end{cases}$$

Proof. Let χ_0 denote the trivial character. We have

$$\mathbf{E}_{x \in Z}\, \chi_0(x) = \mathbf{E}_{x \in Z}\, 1 = 1.$$

On the other hand, let χ be a nontrivial character and let $u \in Z$ be such that $\chi(u) \neq 1$. Then from

$$\mathbf{E}_{x \in Z}\, \chi(x) = \mathbf{E}_{x \in Z}\, \chi(u + x) = \mathbf{E}_{x \in Z}\, \chi(u)\chi(x) = \chi(u)\, \mathbf{E}_{x \in Z}\, \chi(x),$$

it follows that $\mathbf{E}_{x \in Z}\, \chi(x) = 0$. Now consider $\chi_1\overline{\chi_2}$. If $\chi_1 = \chi_2$, then this is the trivial character and from our first observation, $\langle \chi_1, \chi_2 \rangle = 0$. Otherwise, we are in the second case and the inner product is zero. This proves part (a).

Part (b) is proven similarly. Note that $\chi(x)\overline{\chi(y)} = \chi(x - y)$. If $x = y$, then we have

$$\sum_{\chi \in \widehat{Z}} \chi(x - y) = \sum_{\chi \in \widehat{Z}} \chi(0) = |\widehat{Z}|.$$

If $x \neq y$, then there is some $\psi \in \widehat{Z}$ such that $\psi(x - y) \neq 1$, and then writing

$$\sum_{\chi \in \widehat{Z}} \chi(x - y) = \sum_{\chi \in \widehat{Z}} \psi(x - y)\chi(x - y) = \psi(x - y) \sum_{\chi \in \widehat{Z}} \chi(x - y),$$

we see that $\sum_{\chi \in \widehat{Z}} \chi(x - y)$ must be zero. ∎

Since the space of functions from $Z \to \mathbf{C}$ has dimension $|Z|$, there are at most $|Z|$ characters. Every finite abelian group can be written as a direct product of cyclic groups, and we shall use this fact to show that there are exactly $|Z|$ characters; i.e., $|\widehat{Z}| = |Z|$. For brevity, let $\mathbf{Z}_n$ stand for $\mathbf{Z}/n\mathbf{Z}$ for all $n \in \mathbf{N}$, and for $\alpha \in \mathbf{R}$, let $e(\alpha) = e^{2\pi i \alpha}$.

Lemma 19. *The set of characters on a finite abelian group Z spans the space of functions from Z to $\mathbf{C}$.*

Proof. Write $Z \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_r}$. For every $u = (u_1, \ldots, u_r) \in Z$, the function $\chi_u : Z \to \mathbf{C}$ that maps

$$(x_1, \ldots, x_r) \mapsto \prod_{i=1}^{r} e\left(\frac{u_i x_i}{n_i}\right)$$

is a character (this is easy to show, since $e(x_i + x_i') = e(x_i)e(x_i')$). If $u \neq u'$, then $\chi_u \neq \chi_{u'}$ and $\langle \chi_u, \chi_{u'} \rangle = 0$ by the previous lemma. Hence the set $\{\chi_u : u \in Z\}$

comprises $|Z|$ linearly independent elements in a space of dimension $|Z|$, which must be spanning. ∎

Note that the map $u \mapsto \chi_u$ gives an isomorphism from Z to $\widehat{Z}$. The two main examples we shall consider are when $Z = \mathbf{Z}_n$ and when $Z = \mathbf{F}_p^n$. In the first case, χ_u maps $x \mapsto e(ux/N)$ and in the second case χ_u maps $x \mapsto e(u \cdot x/p)$. (Recall that if $u = (u_1, \dots, u_n)$ and $x = (x_1, \dots, x_n)$ then the dot product $u \cdot x$ is the sum $\sum_{i=1}^n u_i x_i$.)

For a finite set X, we shall denote by $L_p(X)$ the normed vector space of all functions $f : X \to \mathbf{C}$ under the norm

$$\|f\|_p = \big(\mathbf{E}_{x \in X} \big|f(x)\big|^p\big)^{1/p}.$$

The notation $l_p(X)$ denotes the same set, but with the norm

$$\|f\|_p = \Big(\sum_{x \in X} \big|f(x)\big|^p\Big)^{1/p}$$

instead. Note that $\|f\|_2^2 = \langle f, f\rangle$ and $\|f\|_\infty = \max_{x \in X} \big|f(x)\big|$.

The Fourier transform. If $f : Z \to \mathbf{C}$, the *Fourier transform* of f is the function $\widehat{f} : \widehat{Z} \to \mathbf{C}$ given by

$$\widehat{f}(\chi) = \langle f, \chi\rangle = \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(x)}.$$

We shall now state and prove an identity which is extremely useful in Fourier analysis.

Lemma 20 (*Parseval's identity*). *Let Z be a finite abelian group and let f and g be functions from Z to $\mathbf{C}$. If $\widehat{f}$ and $\widehat{g}$ are the Fourier transforms of f and g respectively, then $\langle f, g\rangle = \langle \widehat{f}, \widehat{g}\rangle$.*

Proof. First, we expand all the definitions and rearrange sums to obtain

$$\begin{aligned}
\langle \widehat{f}, \widehat{g}\rangle &= \sum_{\chi \in \widehat{Z}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)} \\
&= \sum_{\chi \in \widehat{Z}} \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(x)}\overline{\mathbf{E}_{y \in Z}\, g(y)\overline{\chi(y)}} \\
&= \mathbf{E}_{x \in Z}\, f(x)\overline{\mathbf{E}_{y \in Z}\, \overline{g(y)} \sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)}}.
\end{aligned}$$

By the second orthogonality relation and the fact that $|\widehat{Z}| = |Z|$, the inner sum equals $|Z|$ when $y = x$ and 0 otherwise. Thus for any given x, we have

$$\mathbf{E}_{y \in Z}\, \overline{g(y)} \sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)} = \overline{g(x)},$$

which is exactly what we need for the whole thing to equal $\langle f, g\rangle$. ∎

We also have the following inversion formula that recovers the original function f from $\widehat{f}$.

Lemma 21 (*Fourier inversion formula*). *Let Z be a finite abelian group and let $f : Z \to \mathbf{C}$. We have*

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

Proof. We expand

$$\sum_{\chi \in \widehat{Z}} \widehat{f}(\chi)\chi(x) = \sum_{\chi \in \widehat{Z}} \mathbf{E}_{y \in Z}\, f(y)\overline{\chi(y)}\chi(x) = \mathbf{E}_{y \in Z}\, f(y) \sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)},$$

and we noted in the proof of Parseval's theorem that the right-hand side is exactly $f(x)$. ∎

The inversion formula tells us that two functions from $Z \to \mathbf{C}$ are equal if and only if their Fourier transforms are equal. For the next lemma, which concerns dilates of a function $f : Z \to \mathbf{C}$, we will establish some notation. If $x \in Z$, we define nx recursively for all integers $n \geq 0$ by $0x = 0$ and $nx = x + (n-1)x$. We then set $nz = -(-n)x$ for all negative integers. Since the group operation on characters is multiplication, we will not write $n\chi$ but instead χ^n for χ multiplied with itself n times.

Lemma 22 (*Dilation rule*). *Let Z be a finite abelian group and let $a \in \mathbf{Z}$ be an integer that is coprime to $|Z|$. Denote the multiplicative inverse of a modulo $|Z|$ by a^{-1}. Letting $f_a : Z \to \mathbf{C}$ be the function given by $f_a(x) = f(a^{-1}x)$, we have $\widehat{f_a}(\chi) = \widehat{f}(\chi^a)$.*

Proof. We have

$$\widehat{f_a}(\chi) = \mathbf{E}_{x \in Z}\, f_a(x)\overline{\chi(x)} = \mathbf{E}_{x \in Z}\, f(a^{-1}x)\overline{\chi(x)}.$$

Since $x \mapsto ax$ is a bijection from Z to itself, we can replace x formally by ax in the above to get

$$\widehat{f_a}(\chi) = \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(ax)} = \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(ax)}^a = \widehat{f}(\chi^a). \quad ∎$$

Convolutions. For functions f and g from a finite abelian group Z to $\mathbf{C}$, the *convolution* $f * g$ is defined by

$$(f * g)(x) = \mathbf{E}_{y+z=x}\, f(y)g(z).$$

If instead $\widehat{f}$ and $\widehat{g}$ are functions from $\widehat{Z}$ to $\mathbf{C}$, then

$$(\widehat{f} * \widehat{g})(\chi) = \sum_{\chi_1\chi_2 = \chi} \widehat{f}(\chi_1)\widehat{g}(\chi_2).$$

Lemma 23 (*Convolution law*). *Let Z is a finite abelian group and $f, g : \mathbf{Z} \to \mathbf{C}$. For all $\chi \in \widehat{Z}$, we have $\widehat{f * g}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi)$.*

Proof. We start by expanding

$$\widehat{f * g}(\chi) = \mathbf{E}_{x \in Z}(f * g)(x)\overline{\chi(x)} = \mathbf{E}_{x \in Z}\, \mathbf{E}_{y+z=x}\, f(y)g(z)\overline{\chi(y)\chi(z)}.$$

But note that x does not appear in the summand anymore, meaning that we can simply rewrite this as an expectation over *all* y and z (their sum will equal x for some $x \in Z$). Thus we can conclude that

$$\widehat{f * g}(\chi) = \mathbf{E}_{y \in Z}\, \mathbf{E}_{z \in Z}\, f(y)g(z)\overline{\chi(y)\chi(z)} = \widehat{f}(\chi)\widehat{g}(\chi),$$

which is what we wanted to show. ∎

If A is a subset of a finite abelian group Z, we associate to A the *characteristic function* $\mathbf{1}_A : Z \to \mathbf{C}$ given by

$$\mathbf{1}_A(x) = \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{otherwise.} \end{cases}$$

When it will not cause confusion, we will abuse notation and write $A(x)$ instead of $\mathbf{1}_A(x)$. With the definitions and results stated above, we are now in a position to translate properties of A to Fourier-analytic statements about the function $\mathbf{1}_A$. First off, note that

$$\left\|\widehat{\mathbf{1}_A}\right\|_2^2 = \|\,\mathbf{1}_A\,\|_2^2 = \mathbf{E}_{x \in Z}\, A(x)^2 = \mathbf{E}_{x \in Z}\, A(x) = \frac{|A|}{|Z|}.$$

If $|A|/|Z| = \delta$, then we will say that A has *density* δ. Another way of expressing δ in terms of $\mathbf{1}_A$ is

$$\widehat{\mathbf{1}_A}(\chi_0) = \mathbf{E}_{x \in Z}\, A(x)\chi_0(x) = \mathbf{E}_{x \in Z}\, A(x) = \delta,$$

where χ_0 is the trivial character.

The fact that $\|\,\mathbf{1}_A\,\|_2^2 = \delta$ means that if we sample x and y from Z and condition that $x = y$, the probability that x (or y) is in A is δ. The reason for stating this obvious fact in such a stilted fashion is that it generalises by way of the convolution operation we defined earlier; that is, what if we are interested in the probability that a 4-tuple (x, y, z, w) satisfying $x + y = z + w$ is a member of A^4? Well, the convolution law gives

$$\begin{aligned}
\mathbf{E}_{x+y=z+w}\, A(x)A(y)A(z)A(w) &= \mathbf{E}_{u \in Z}\, \mathbf{E}_{x+y=u}\, \mathbf{E}_{z+w=u}\, A(x)A(y)A(z)A(w) \\
&= \mathbf{E}_{u \in Z}(\mathbf{1}_A * \mathbf{1}_A)(u)^2 \\
&= \|\,\mathbf{1}_A * \mathbf{1}_A\,\|_2^2 \\
&= \left\|\widehat{\mathbf{1}_A * \mathbf{1}_A}\right\|_2^2 \\
&= \left\|\left(\widehat{\mathbf{1}_A}\right)^2\right\|_2^2 \\
&= \sum_{\chi \in \widehat{Z}} \left|\widehat{\mathbf{1}_A}(\chi)\right|^4 \\
&= \|\,\mathbf{1}_A\,\|_4^4,
\end{aligned}$$

and more generally, the probability that a tuple $(a_1, \dots, a_k, b_1, \dots, b_k) \in Z^{2k}$ with $a_1 + \cdots + a_k = b_1 + \cdots + b_k$ is a member of A^{2k} is $\| \mathbf{1}_A \|_{2k}^{2k}$. Recall that the number of $(x, y, z, w) \in A^4$ with $x + y = z + w$ is the additive energy $E(A)$ of A; we just showed above that $E(A) = |Z|^3 \| \mathbf{1}_A \|_4^4$.

6. Bohr sets and Bogolyubov's lemma

Let Z be a finite abelian group, let $\chi_1, \dots, \chi_k$ be characters on Z, and let $\delta > 0$. The *Bohr set* $B(\chi_1, \dots, \chi_k; \delta)$ is the set

$$\big\{x \in Z : \chi_i(x) \in e\big([-\delta, \delta]\big) \text{ for all } 1 \le i \le k\big\}.$$

(As before, we write $e(\alpha)$ for $e^{2\pi i \alpha}$.) We say that such a Bohr set has *dimension* k and *width* δ.

If $Z = \mathbf{F}_p^n$, we can write $\chi_i = \chi_{u_i}$ where $\chi_{u_i}(x) = e(u_i \cdot x/p)$. If $\delta < 1/p$, then $\chi_{u_i}(x) \in e\big([-\delta, \delta]\big)$ if and only if $(u_i \cdot x)/p \bmod 1 \in [-\delta, \delta]$. But $u_i \cdot x$ is an integer, so this is true if and only if $u_i \cdot x = 0$, so consequently

$$B(\chi_1, \dots, \chi_k; \delta) = \{x \in \mathbf{F}_p^n : u_i \cdot x = 0 \text{ for all } 1 \le i \le k\},$$

which is a subspace cut out by k linear conditions, i.e., of codimension at most k.

Lemma 24 (*Bogolyubov*). *Let Z be a finite abelian group. Let $A \subseteq Z$ be a subset of density α. Then $2A - 2A$ contains a Bohr set of dimension at most $1/\alpha^2$ and width $1/4$.*

Proof. For $x \in Z$, let

$$\begin{aligned} f(x) &= \big(\mathbf{1}_A * \mathbf{1}_A * (-\mathbf{1}_A) * (-\mathbf{1}_A)\big)(x) \\ &= \mathbf{E}_{p+q-r-s=x} \, \mathbf{1}_A(p) \, \mathbf{1}_A(q) \, \mathbf{1}_A(r) \, \mathbf{1}_A(s). \end{aligned}$$

Then $x \in 2A - 2A$ if and only if $f(x) \neq 0$. We want to find a Bohr set on which f does not vanish.

Note first that for any character χ,

$$\widehat{-\mathbf{1}_A}(\chi) = \mathbf{E}_x \, \mathbf{1}_A(-x)\overline{\chi(x)} = \mathbf{E}_x \, \mathbf{1}_A(x)\overline{\chi(-x)} = \mathbf{E}_x \, \mathbf{1}_A(x)\chi(x) = \overline{\widehat{\mathbf{1}_A}(\chi)}.$$

(The last identity relies on the fact that $\mathbf{1}_A(x)$ is real.) This implies that $\widehat{\mathbf{1}_A}(\widehat{-\mathbf{1}_A}) = |\, \mathbf{1}_A \,|^2$. Now we apply the Fourier inversion formula and the convolution law to expand

$$\begin{aligned} f(x) &= \sum_\chi \mathbf{1}_A * \mathbf{1}_A * (\widehat{-\mathbf{1}_A}) * (-\mathbf{1}_A)(\chi)(\chi)(x) \\ &= \sum_\chi \widehat{\mathbf{1}_A}(\chi)^2 \widehat{-\mathbf{1}_A}(\chi)^2 \chi(x) \\ &= \sum_\chi \big|\widehat{\mathbf{1}_A}(\chi)\big|^4 \chi(x). \end{aligned}$$

Let

$$K = \{\chi \in \widehat{Z} : |\widehat{\mathbf{1}_A}(\chi)| \geq \alpha^{3/2}\}$$

and let B be the Bohr set $B(K; 1/4)$. Then the expression above for $f(x)$ can be split into

$$f(x) = |\widehat{\mathbf{1}_A}(\chi_0)|^4 + \sum_{\chi \in K} |\widehat{\mathbf{1}_A}(\chi)|^4 \chi(x) + \sum_{\chi \notin K \cup \{\chi_0\}} |\widehat{\mathbf{1}_A}(\chi)|^4 \chi(x).$$

We shall assume that $x \in B$ and deal with each of the three terms separately.

The first term is easy; since A has density α, $\widehat{\mathbf{1}_A}(\chi_0) = \alpha$, and thus the first time is α^4. For the second term, note that if $\chi \in K$ and $x \in B$, then $\chi(x) \in e\big([-1/4, 1/4]\big)$. This means that $\chi(x)$ has argument between $-\pi/2$ and $\pi/2$, and *a fortiori* has nonnegative real part. Now, if $\chi \notin K$ and $\chi \neq \chi_0$, then $|\widehat{\mathbf{1}_A}| < \alpha^{3/2}$, so we take the absolute value of the third term and apply the triangle inequality and Parseval's identity to obtain

$$\Big| \sum_{\chi \notin K \cup \{\chi_0\}} |\widehat{\mathbf{1}_A}(\chi)|^4 \chi(x) \Big| \leq \sum_{\chi \notin K \cup \{\chi_0\}} |\widehat{\mathbf{1}_A}(\chi)|^4 < \sum_{\chi \in \widehat{Z}} \alpha^3 |\widehat{\mathbf{1}_A}(\chi)|^2 = \alpha^3 \langle \widehat{\mathbf{1}_A}, \widehat{\mathbf{1}_A} \rangle.$$

But by Parseval's identity, the right-hand side equals $\alpha^3 \langle \mathbf{1}_A, \mathbf{1}_A \rangle = \alpha^4$, so we find that the real part of the third term is more than $-\alpha^4$. This means that $\Re f(x) > 0$, so $f(x) \neq 0$ for all $x \in B$; that is, $B \subseteq 2A - 2A$.

It remains to give an upper bound on the size of K. We have

$$\alpha = \sum_{\chi \in \widehat{Z}} |\mathbf{1}_A(\chi)|^2 \geq \sum_{\chi \in K} |\widehat{\mathbf{1}_A(\chi)}|^2 \geq |K| \alpha^3,$$

meaning that $|K| \leq 1/\alpha^2$. ∎

When A is a subset of density α in $Z = \mathbf{F}_p^n$, Bogolyubov's lemma tells us that $2A - 2A$ contains a subspace of codimension at most $1/\alpha^2$.

7. Freiman's theorem in vector spaces over fields of prime order

Let Z be an additive group and let A be a finite subset of Z. It is possible that $|A + A| = |A|$, but this happens if and only if A is a coset of a subgroup of Z (which means that Z must be finite). If A is a finite subset of integers, then without loss of generality we can shift A so that $\min A = 0$. if A only contains 0 then $|A + A|$ is $1 = 2|A| - 1$, and if $|A| > 1$, then let $m = \max A$ and note that $A + A$ contains A and $m + A$, and $A \cap (m + A) = \{m\}$, so in this case we also have $|A + A| \geq 2|A| - 1$.

It is not hard to see that if A is an arithmetic progression in the integers, then $A + A$ is exactly $2|A| - 1$, but for instance $A = \{1, \ldots, n\} \subseteq \mathbf{Z}$ is not contained in any nontrivial subgroup of $\mathbf{Z}$ and it also has $|A + A| = 2|A| - 1$. So

next we might amend our conjecture to say that if $|A+A|$ is small, then A is a large subset of an arithmetic progression. But this is also false. Consider the set

$$\{0,1,2, \quad 10,11,12, \quad 20,21,22, \quad 30,31,32\}.$$

In some sense this is a "progression of progressions," or a 2-dimensional arithmetic progression. Such a set is the projection of some rectangle in $\mathbf{Z}^2$, and from this observation it is not hard to see that $|A+A| \leq 4|A|$. If we increase d, we can still say that $|A+A| \leq 2^d|A|$.

Once we add these d-dimensional arithmetic progressions into consideration, it turns out that we can have an inverse statement. Concretely, if $|A+A| \leq C|A|$, then there exists a d-dimensional arithmetic progression P such that $|P| \leq K|A|$ and $A \subseteq P$, where d and K depend only on C (otherwise we could simply embed A into $[\min A, \max A]$).

This statement is called Freiman's theorem, as it was first proved by Freiman over the integers. In these notes we will prove an analogue of it for subsets of $\mathbf{F}_p^N$, in which "d-dimensional arithmetic progression" is replaced by "subspace". First we need a lemma.

Lemma 25 (*Ruzsa covering lemma*). *Let Z be an abelian group and let A and B be finite subsets of Z. Then there is a set $K \subseteq A$ of size at most $|A+B|/|B|$ such that $A \subseteq K+B-B$.*

Proof. Let $K = \{a_1, \ldots, a_k\}$ be a maximal subset of A with the property that the sets $a_i + B$ are disjoint. For all $a \in A$ there is i such that $(a+B) \cap (a_i+B) \neq \emptyset$, otherwise we could add a to K and contradict maximality. Equivalently, we can find b and b' such that $a+b = a_i+b'$ so $a \in a_i + B - B$. Hence $A \subseteq K+B-B$. Lastly, $|K| \cdot |B| = |K+B| \leq |A+B|$. ∎

Next, we prove two simple lemmas about Freiman isomorphisms, the second concerning how they behave on subspaces of $\mathbf{F}_p^n$.

Lemma 26. *A Freiman isomorphism of order $k(r+s)$ from A to B induces a Freiman isomorphism of order k from $rA-sA$ to $rB-sB$.*

Proof. This proof is conceptually very easy but notationally a total nightmare. Let ϕ be a $k(r+s)$ isomorphism from A to B. Then

$$x_1 + \cdots x_{k(r+s)} = y_1 + \cdots + y_{k(r+s)}$$

if and only if

$$\phi(x_1) + \cdots \phi(x_{k(r+s)}) = \phi(y_1) + \cdots + \phi(y_{k(r+s)})$$

Now let $g_1, \ldots, g_k, h_1, \ldots, h_k$ be $2k$ elements in $rA-sA$. Then the expression

$$g_1 + \cdots g_k = h_1 + \cdots + h_k$$

has a sum of kr elements of A and ks elements of $-A$ on each side. We can subtract off the elements of $-A$ on each side to get $k(r+s)$ elements of A on either side, and the equality holds if and only if it holds with ϕ applied to every term. So letting

$$g_i = g'_{i,1} + \cdots + g'_{i,r} - g''_{i,1} - \cdots - g''_{i,s}$$

and

$$h_i = h'_{i,1} + \cdots + h'_{i,r} - h''_{i,1} - \cdots - h''_{i,s}$$

for all i, we find that $g_1 + \cdots g_k = h_1 + \cdots + h_k$ holds if and only if

$$\begin{aligned}\phi(g'_{1,1}) + \cdots + \phi(g'_{k,r}) + \phi(h''_{1,1}) + \cdots + \phi(h''_{k,s}) \\ = \phi(h'_{1,1}) + \cdots + \phi(h'_{k,r}) + \phi(g''_{1,1}) + \cdots + \phi(g''_{k,s}).\end{aligned}$$

Subtracting all the double-prime terms from both sides yields

$$\begin{aligned}\phi(g'_{1,1}) + \cdots + \phi(g'_{k,r}) - \phi(g''_{1,1}) - \cdots - \phi(g''_{k,s}) \\ = \phi(h'_{1,1}) + \cdots + \phi(h'_{k,r}) - \phi(h''_{1,1}) - \cdots - \phi(h''_{k,s}),\end{aligned}$$

and letting

$$\psi(g_i) = \phi(g'_{i,1}) + \cdots + \phi(g'_{i,r}) - \phi(g''_{i,1}) - \cdots - \phi(g''_{i,s})$$

and

$$\psi(h_i) = \phi(h'_{i,1}) + \cdots + \phi(h'_{i,r}) - \phi(h''_{i,1}) - \cdots - \phi(h''_{i,s})$$

for all i, we see that $g_1 + \cdots g_k = h_1 + \cdots + h_k$ holds if and only if

$$\psi(g_1) + \cdots \psi(g_k) = \psi(h_1) + \cdots + \psi(h_k).$$

It is invertible, since we can just apply ϕ^{-1} termwise to an element of $rB - sB$, so this is the k-isomorphism we need between $rA - sA$ and $rB - sB$. ∎

Lemma 27. *Let X be a linear subspace of $\mathbf{F}_p^n$ and let ϕ be a 2-isomorphism from X to a set $A \subseteq \mathbf{F}_p^n$. Then A is an affine subspace of $\mathbf{F}_p^n$ of dimension $\dim X$.*

Proof. We shall show that $Y = A - \phi(0)$ is a linear subspace of $\mathbf{F}_p^n$. Clearly it contains 0, since A contains $\phi(0)$. Now let $y_1, y_2 \in Y$ so that $y_1 + \phi(0)$ and $y_2 + \phi(0)$ are both in A. Let $x_1 = \phi^{-1}\big(y_1 + \phi(0)\big)$, $x_2 = \phi^{-1}\big(y_1 + \phi(0)\big)$, and let x denote their sum in X. Then since $x_1 + x_2 = x + 0$, we have

$$y_1 + \phi(0) + y_2 + \phi(0) = \phi(x) + \phi(0).$$

Subtracting $\phi(0)$ from both sides, we find that $y_1 + y_2 + \phi(0) = \phi(x)$, meaning that $y_1 + y_2 \in A - \phi(0) = Y$. This proves that Y is closed under finite sums, and since scalar multiplication over a finite field can always be reëxpressed as a finite sum, we find that A is an affine subspace of $\mathbf{F}_p^n$ in bijection with X, that is, of dimension $\dim X$. ∎

We are now able to prove Freiman's theorem for $\mathbf{F}_p^n$, whose proof amounts to little more than a concatenation of several previous results.

Theorem 28 (*Freiman's theorem in* $\mathbf{F}_p^n$). *Let* $A \subseteq \mathbf{F}_p^n$ *and suppose that* $|A+A| \leq C|A|$. *Then there is a subspace* X *of* $\mathbf{F}_p^n$ *such that* $A \subseteq X$ *and* $|X| \leq C'|A|$, *where* C' *depends only on* C *and* p.

Proof. By Plünnecke's theorem, $|8A-8A| \leq C^{16}|A|$, hence by Ruzsa's embedding lemma, A is 8-isomorphic to a subset $A_1 \subseteq \mathbf{F}_p^m$ where $p^m \leq pC^{16}|A|$. By Bogolyubov's lemma with $\alpha = p^{-1}C^{-16}$, $2A_1 - 2A_1$ contains a Bohr set $B(K; 1/4)$ of dimension at most p^2C^{32}. But letting $\delta < 1/(2p) \leq 1/4$, and $X = B(K;\delta)$, we have $X \subseteq B(K;1/4)$ and X is a linear subspace of $\mathbf{F}_p^m$ of codimension at most p^2C^{32}.

Now since A is 8-isomorphic to A_1, we can apply Lemma 26 to deduce that $2A-2A$ is 2-isomorphic to $2A_1 - 2A_1$. It follows that $2A-2A$ contains a set Y that is 2-isomorphic to the linear subspace X. By Lemma 27, this set Y is an affine subspace, of dimension at least $m - p^2C^{32}$, and thus of cardinality at least $p^{m-p^2C^{32}} \geq p^{p^2C^{32}}|A|$ (here we used the fact that $A_1 \subseteq \mathbf{F}_p^m$ and A_1 is Freiman isomorphic to A).

Ruzsa's covering lemma tells us that there exists L of size at most $|A+Y|/|Y|$ such that $A \subseteq L + Y - Y$. But since Y is an affine subspace, $Y - Y$ is a linear subspace; setting $V = Y - Y$, we have

$$|V| = |Y| \leq |2A - 2A| \leq C^4|A|,$$

which follows from another application of Plünnecke's theorem. Then by possibly adding $|L|$ basis vectors, $L + V$ is contained in a linear subspace of size at most $p^{|L|}|V| \leq p^{|L|}C^4|A|$. On the other hand, L has size at most

$$\frac{|A+2A-2A|}{|V|} \leq \frac{C^5|A|}{p^{-p^2C^{32}}|A|} = C^5 p^{p^2C^{32}},$$

where yet again we have used Plünnecke's theorem. Hence we conclude that A is contained in a linear subspace of size at most

$$p^{C^5 p^{p^2 C^{32}}} C^4|A|. \quad \blacksquare$$

8. Roth's theorem

In the previous section we showed that any set A with $A + A$ small must be a dense subset of a structured set. We didn't prove this over $\mathbf{Z}$, but we saw briefly that the notion of "structured set" in that case was a d-dimensional arithmetic progression. Now we switch gears and try to find arithmetic progressions in subsets of $\mathbf{Z}$. The first major theorem in this vein was proved by B. L. van der Waerden in 1927.

Theorem W (*van der Waerden,* 1927). *For all* k *and* r, *there is* n *such that if we partition* $[n]$ *into disjoint sets* $C_1 \cup \cdots \cup C_r$ *then some* C_i *contains an arithmetic progression of length* k. $\blacksquare$

A stronger statement is given by the celebrated 1975 theorem of E. Szemerédi.

Theorem S (*Szemerédi,* 1975). *For every $\delta > 0$ and $k \in \mathbf{N}$ there exists n such that if $A \subseteq [n]$ and $|A| \geq \delta n$, then A contains an arithmetic progression of length k.* ∎

By setting $\delta = 1/r$ and invoking the pigeonhole principle, we see that Szemerédi's theorem implies van der Waerden's theorem. We will not prove either of these statements in these notes. The first has a relatively elementary proof, but not one that is very additive-combinatorial in nature, while the second is far too complex to prove in full generality here. We will, however, prove Szemerédi's theorem in the case $k = 3$. This special case is called Roth's theorem as it was proved by K. Roth in 1953. Before we get there we first establish three lemmas. In their proofs we will write, e.g., A instead of $\mathbf{1}_A$, and identify r with its corresponding element $\chi_r \in \widehat{\mathbf{Z}_N}$, writing $\widehat{f}(r)$ instead of $\widehat{f}(\chi_r)$.

Lemma 29. *Let N be odd and let A, B, and C be subsets of $\mathbf{Z}_N$ with densities α, β, and γ respectively. Suppose that $N > 2/(\alpha\beta\gamma)$. Then either there exists x and $d \neq 0$ such that $(x, x+d, x+2d) \in A \times B \times C$, or there exists $r \neq 0$ such that $|\widehat{A}(r)| \geq \alpha\beta^{1/2}\gamma^{1/2}/2$.*

Proof. Consider the quantity

$$\begin{aligned}\mathbf{E}_{x,d}\, A(x)B(x+d)C(x+2d) &= \mathbf{E}_{x+z=2y}\, A(x)C(z)B(y) \\ &= \mathbf{E}_u\big(\mathbf{E}_{x+z=u}\, A(x)C(z)\big)B(u/2).\end{aligned}$$

Using the notation $f_a(x) = f(x/a)$ for a dilation, we see that this expectation is actually the inner product $\langle A * C, B_2\rangle$, which by Parseval's identity is equal to $\langle \widehat{A * C}, \widehat{B_2}\rangle$. Recall that the characters of $\mathbf{Z}_N$ are given by $\chi_a(x) = e(ax/N)$. Applying the dilation rule gives

$$\widehat{B_2}(r) = \widehat{B_2}(\chi_r) = \widehat{B}(\chi_r{}^2) = \widehat{B}(\chi_{2r}) = \widehat{B}(2r) = (\widehat{B})_{2^{-1}}(r)$$

where 2^{-1} denotes the inverse of 2 modulo N. This, combined with the convolution law, gives $\langle \widehat{A * C}, \widehat{B_2}\rangle = \big\langle \widehat{A}\widehat{C}, (\widehat{B})_{2^{-1}}\big\rangle$. But since B is real-valued,

$$\widehat{B}(-r) = \mathbf{E}_x\, B(x)\overline{\chi_{-r}(x)} = \mathbf{E}_x\, B(x)\chi_r(x) = \overline{\mathbf{E}_x\, B(x)\overline{\chi_r(x)}} = \overline{\widehat{B}(r)},$$

so putting everything together yields

$$\begin{aligned}\mathbf{E}_{x,d}\, A(x)B(x+d)C(x+2d) &= \big\langle \widehat{A}\widehat{C}, (\widehat{B})_{2^{-1}}\big\rangle \\ &= \sum_r \widehat{A}(r)\widehat{C}(r)\overline{\widehat{B}(2r)} \\ &= \sum_r \widehat{A}(r)\widehat{C}(r)\widehat{B}(-2r) \\ &= \alpha\beta\gamma + \sum_{r\neq 0} \widehat{A}(r)\widehat{C}(r)\widehat{B}(-2r).\end{aligned}$$

Note that by the triangle and Cauchy–Schwarz inequalities,

$$\begin{aligned}\Big|\sum_{r\neq 0}\widehat{A}(r)\widehat{C}(r)\widehat{B}(-2r)\Big| &\leq \max_{r\neq 0}\big|\widehat{A}(r)\big|\sum_{r\in\mathbf{Z}_N}\big|\widehat{B}(-2r)\big|\cdot\big|\widehat{C}(r)\big| \\ &\leq \max_{r\neq 0}\big|\widehat{A}(r)\big|\Big(\sum_{r\in\mathbf{Z}_N}\big|\widehat{B}(-2r)\big|^2\Big)^{1/2}\Big(\sum_{r\in\mathbf{Z}_N}\big|\widehat{C}(r)\big|^2\Big)^{1/2} \\ &= \big\|\widehat{B}\big\|_2\big\|\widehat{C}\big\|_2\max_{r\neq 0}\big|\widehat{A}(r)\big| \\ &= \beta^{1/2}\gamma^{1/2}\max_{r\neq 0}\big|\widehat{A}(r)\big|.\end{aligned}$$

(We used the fact that N is odd in the third line above.) So

$$\mathbf{E}_{x,d}\,A(x)B(x+d)C(x+2d) \geq \alpha\beta\gamma - \beta^{1/2}\gamma^{1/2}\max_{r\neq 0}\big|\widehat{A}(r)\big|,$$

meaning that if $\max_{r\geq 0}\big|\widehat{A}(r)\big| < \alpha\beta^{1/2}\gamma^{1/2}/2$, then $\mathbf{E}_{x,d}\,A(x)B(x+d)C(x+2d) > \alpha\beta\gamma/2$. The further assumption that $\alpha\beta\gamma/2 > 1/N$ allows us to conclude that there is some x for which $\mathbf{E}_d\,A(x)B(x+d)C(x+2d) > 1$, and thus some $d \geq 0$ such that $(x, x+d, x+2d) \in A\times B\times C$. ∎

References

Antal Balog and Endre Szemerédi, "A statistical theorem of set addition," *Combinatorica* **14** (1994), 263–268.

William Timothy Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four," *Geometric and Functional Analysis* **8** (1998), 529–551.

Askold Khovanskii, "Newton polyhedron, Hilbert polynomial, and sums of finite sets," *Functional Analysis and its Applications* **26** (1992), 276–281.

Melvyn Bernard Nathanson and Imre Zoltán Ruzsa, "Polynomial growth of sumsets in abelian semigroups," *Journal de Théorie des Nombres de Bordeaux* **14** (2002), 553–560.

Giorgis Petridis, "New proofs of Plünnecke-type estimates for product sets in groups.," *Combinatorica* **32** (2012), 721–733.

Helmut Plünnecke, *Eigenschaften und Abschätzungen von Wirkungsfunktionen* (Bonn: Berichte der Gesellschaft für Mathematik und Datenverarbeitung, 1969).

Klaus Friedrich Roth, "On certain sets of integers," *Journal of the London Mathematical Society* **28** (1953), 104–109.

Imre Zoltán Ruzsa, "An application of graph theory to additive number theory," *Scientia, Series A* **3** (1989), 97–109.

Imre Zoltán Ruzsa, "Sums of finite sets," *Number Theory: New York Seminar 1991–1995* (1996).

Endre Szemerédi, "On sets of integers containing no k elements in arithmetic progression," *Acta Arithmetica* **27** (1975), 199–245.

Terence Tao and Van Ha Vu, *Additive Combinatorics* (Cambridge: Cambridge University Press, 2006).

Bartel Leendert van der Waerden, "Beweis einer Baudetschen Vermutung," *Nieuw Archief voor Wiskunde* **15** (1927), 212–216.