ADDITIVE COMBINATORICS (WINTER 2010)

Andrew Granville

Introduction

For A, B subsets of an additive group Z, we define $A+B$ to be the sumset $\{a+b : a \in A, b \in B\}$, and kA to be the k-fold sum $A+A+\cdots+A$ of A. We also let $A-B = \{a-b : a \in A, b \in B\}$ and $b+A = \{b\}+A$ for a single element set $\{b\}$, a *translate* of A. Note that $A-A$ is *not* 0 unless $|A| = 1$. We let $k \diamond A = \{ka : a \in A\}$, a *dilate* of A. There are many obvious properties of "+" that can be checked like commutativity, associativity and the distributive law $A+(B \cup C) = (A+B) \cup (A+C)$.

Prove that $k \diamond A \subseteq kA$ and classify when they are equal. Prove that $|b+A| = |A|$. Show that $|A| \le |A+B| \le |A||B|$. Describe the situations when we get equality. Improve this last upper bound for $|A+A|$ and for $|A-A|$.

We shall be most interested in understanding the size and structure of sumsets which are subsets of the integers $\mathbb{Z}$, often working with $\mathbb{Z}_{\ge m}$ (where $A_{\ge m}$ denotes the integers in A that are $\ge m$), or of $\mathbb{Z}/N\mathbb{Z}$ for some positive integer N. That every integer is the sum of four squares of integers can be written down as $4\mathbb{Z}^2 = \mathbb{Z}_{\ge 0}$ (where here $\mathbb{Z}^2$ denotes the squares of the integers); if $h(A \cup \{0\}) \supseteq \mathbb{Z}_{\ge m}$ for some m then we say that A is a *basis of order* h for the integers, and thus $\mathbb{Z}^2$ is a basis of order 4. The Goldbach conjecture can be written as $2\mathbb{P} = 2 \diamond \mathbb{Z}_{\ge 2}$ where $\mathbb{P}$ is the set of primes, or even $3(\mathbb{P} \cup \{0\}) = \mathbb{Z}_{\ge 2} \cup \{0\}$ (verify this is indeed equivalent). The twin primes conjecture states that for every even integer k there are infinitely many pairs of primes $p, p+2k$: verify that this can be rewritten as $\mathbb{P}_{\ge m} - \mathbb{P}_{\ge m} = 2 \diamond \mathbb{Z}$ for all m.

In this course we will be primarily studying what it means that $A+A$ is small; that is, if this is so then what it implies about A. We shall find that this implies that A has a readily describable structure which can then be applied to various problems. There are many open problems in this field that invite investigation; for example to fully understand the structure of $A+B$ when this sumset is "small", in the case that B is significantly smaller than A.

It is easy to see that if $A \subset \mathbb{Z}$ then $|2A| \le |A|(|A|+1)/2$, since the distinct elements of $2A$ are a subset of $\{a_i + a_j : 1 \le i \le j \le |A|\}$; moreover $2A$ can be this large, for example with $A = \{1, 2, 2^2, 2^3, \dots, 2^{n-1}\}$. Prove that this is so, and give an infinite class of such examples described simply by the growth of the elements of A. Moreover show that if we select a set A of

These notes borrow from those of Tim Gowers and Jacques Verstraete, Terry Tao and Van Vu, Ben Green, and various published books

n integers "at random" from $\{1,\dots x\}$ with $x \ge n^{4+\epsilon}$ then $|2A|$ will equal $|A|(|A|+1)/2$ with probability $\to 1$ as $n \to \infty$.

So we have proved that "typically" $|2A|$ is large and that it is only very special circumstances that it is small. A key, but easy, result for getting a feel for our subject is the following:

Lemma 1. *If A and B are finite subsets of $\mathbb{Z}$ then $|A+B| \ge |A|+|B|-1$. Equality holds if and only if A and B are each complete finite segments of an arithmetic progression to the same modulus.*

Proof. Write the elements of A as $a_1 < a_2 < \dots a_r$, and those of B as $b_1 < b_2 < \dots b_s$. Then $A+B$ contains the $r+s-1$ distinct elements

$$a_1+b_1 < a_1+b_2 < a_1+b_3 < \cdots < a_1+b_s < a_2+b_s < a_3+b_s < \cdots < a_r+b_s.$$

If it contains exactly $r+s-1$ elements then these must be the same, in the same order, as $a_1+b_1 < a_2+b_1 < a_2+b_2 < a_2+b_3 < \cdots < a_2+b_s < a_3+b_s < \cdots < a_r+b_s$. Comparing terms, we have $a_1+b_{i+1} = a_2+b_i$ for $1 \le i \le s-1$; that is $b_j = b_1+(j-1)d$ where $d = a_2-a_1$. A similar argument with the roles of a and b swapped, reveals our result.

If $A+B$ is small, not as small as $|A|+|B|-1$ but not much bigger, then we might expect to be able to use a similar proof to prove a similar structure theorem. Try! After a little play one quickly finds that $A+B$ is small if A and B are both large subsets of complete finite segments of an arithmetic progression to the same modulus. A further interesting example is given by $A = B = \{1,2,\dots,10,101,102,\dots 110,201,202,\dots 210\}$, or its large subsets. One observes that this can be written as $1+\{0,1,2,\dots,9\}+\{0,100,200\}$, a translate of the sum of complete finite segments of two arithmetic progressions. More generally, define a *generalized arithmetic progression* $C = C(a_0,a_1,\dots a_k; N_1,N_2,\dots,N_k)$ as

$$C := \{a_0+a_1n_1+a_2n_2+\cdots+a_kn_k : \ 0 \le n_j \le N_j-1 \text{ for } 1 \le j \le k\}$$

where $a_0,a_1,\dots a_k$ are given integers, and $N_1,N_2,\dots N_k$ are given positive integers. Note that $C(a_0,a_1,\dots a_k;N_1,N_2,\dots,N_k) = a_0+\sum_{i=1}^k a_i \diamond \{0,1,\dots,N_i-1\}$. This generalized arithmetic progression is said to have *dimension* k and *volume* $N_1N_2\dots,N_k$. Notice that

$$2C(a_0,a_1,\dots a_k;N_1,N_2,\dots,N_k) = C(2a_0,a_1,\dots a_k;2N_1-1,2N_2-1,\dots,2N_k-1).$$

so that $|2C| < 2^k|C|$. In fact this inequality generalizes to an C which is the "image" in $\mathbb{Z}$ of that part of a lattice that is inside a convex, compact region of $\mathbb{R}^k$.

If you try to find other sets A and B with $A+B$ small then it seems you will be out of luck. In the case that $A=B$ this is the extraordinary insight of Freiman [5]: he showed that $2A$ can be "small" if and only if it is a "large" subset of a "low" dimensional generalized arithmetic progression of "not too big" volume[1]. This is the central result of this course. Freiman's 1962 proof is both long and difficult to understand. I believe that it is fair to say that the subject did not progress as much as it might have done since people

[1]The terms inside quotation marks all need quantifying and this is not easy.

had difficulty appreciating what Freiman had done. It was not until Ruzsa's 1994 proof of Freiman's result, which is extraordinarily elegant and insightful, that the subject exploded with new ideas and results. As we will see in this course, much of our development of the subject stems from the wealth of ideas in Ruzsa'a treatment, and it is for this reason that we call this main result "the Freiman-Ruzsa theorem".

Densities

For a given set of integers $A = \{a_1 < a_2 < \dots\}$, define $A(n) = \#\{a \in A : \ 1 \le a \le n\}$. As usual, the *upper* and *lower densities* are given by

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{A(n)}{n} \quad \text{and} \quad \overline{d}(A) = \limsup_{n\to\infty} \frac{A(n)}{n},$$

with the *density* $d(A) = \underline{d}(A) = \overline{d}(A)$ if they are equal.

The *Schnirelmann density* of A is defined by

$$\sigma(A) := \inf_{n\ge 1} \frac{A(n)}{n}.$$

Note that $A(n) \ge n\sigma(A)$ for all $n \ge 1$.

Show that (i) $\sigma(A) = 1$ if and only if $A \supseteq \mathbb{Z}_{\ge 1}$; (ii) If $1 \notin A$ then $\sigma(A) = 0$; (iii) If $\sigma(A) = 0$ then $1 \notin A$ or $\underline{d}(A) = 0$; (iv) $\underline{d}(A) \ge \sigma(A)$.

The Schnirelmann density is more combinatorially accessible than the regular notions of density. However the two are easily related: Define $\sigma_{>m}(A) := \inf_{n>m} \frac{A(n)-A(m)}{n-m}$, so that $\sigma(A) = \sigma_{>0}(A)$.

Lemma. *We have* $\underline{d}(A) = \limsup_{m\to\infty} \sigma_{>m}(A)$.

Proof. Fix $\epsilon > 0$. There are infinitely many n for which $A(n) \le (\underline{d}(A) + \frac{\epsilon}{2})n$. Given $m \ge 2 + \frac{2}{\epsilon}$ take such an $n > e^m$ so that

$$\sigma_{>m}(A) \le \frac{A(n) - A(m)}{n - m} \le \frac{(\underline{d}(A) + \frac{\epsilon}{2})n}{n - \log n} \le \underline{d}(A) + \epsilon.$$

Hence $\limsup_{m\to\infty} \sigma_{>m}(A) \le \underline{d}(A)$.

On the other hand suppose that $\sigma_{>m}(A) \le \underline{d}(A) - 2\epsilon$ for all $m \ge m_0$. Define $m_0 < m_1 < m_2 < \dots$ as follows: Select $m_{j+1} > m_j$ so that $\frac{A(m_{j+1})-A(m_j)}{m_{j+1}-m_j} = \sigma_{>m_j}(A) \le \underline{d}(A) - 2\epsilon$. Therefore

$$\begin{aligned} A(m_k) &= A(m_0) + \sum_{j=0}^{k-1} A(m_{j+1}) - A(m_j) \le A(m_0) + \sum_{j=0}^{k-1} (\underline{d}(A) - 2\epsilon)(m_{j+1} - m_j) \\ &= A(m_0) + (\underline{d}(A) - 2\epsilon)(m_k - m_0) \le (\underline{d}(A) - \epsilon)m_k, \end{aligned}$$

if $m_k > m_0/\epsilon$; and so $\underline{d}(A) \le \lim_{k\to\infty} \frac{A(m_k)}{m_k} \le \underline{d}(A) - \epsilon$, a contradiction.

We are interested in adding sets and obtaining a large sum. We will usually assume that $0 \in A \cap B$ for this implies that $A \cup B \subseteq A + B$. In the next result we prove a simple consequence of the pigeohole principle but rephrased here in our terminology.

Lemma 2.1. *If $0 \in A \cap B$ and $\sigma(A) + \sigma(B) \geq 1$ then $A + B \supseteq \mathbb{Z}_{\geq 0}$.*

Proof. Suppose not and let n be the smallest positive integer for which $n \notin A + B$: then $n \notin A \cup B$, and A and $n - B$ are disjoint. Let $C = A \cup (n - B)$ so that $n - 1 \geq C(n-1) = A(n-1) + (n-B)(n-1) = A(n-1) + B(n-1) = A(n) + B(n) \geq \sigma(A)n + \sigma(B)n \geq n$, a contradiction to the supposition.

Schnirelmann's theorem. *If $1 \in A$ and $0 \in B$ then $\sigma(A+B) \geq \sigma(A)+\sigma(B)-\sigma(A)\sigma(B)$.*

A greedy proof. Given $a \in A_{\geq 1}$ we count the number of elements in $a + B \subseteq A + B$ just a little larger than a. That is, if $x > a$ then $(A + B)(x) - (A + B)(a - 1) \geq (a + B)(x) - (a + B)(a - 1) = B(x - a) + 1 \geq \sigma(B)(x - a) + 1$. Therefore if $1 = a_1 < a_2 < \cdots < a_k \leq n$ are the elements of $A \cap [1, n]$ then

$$\begin{aligned}(A+B)(n) &= \sum_{i=1}^{k-1}((A+B)(a_{i+1}-1) - (A+B)(a_i-1)) + ((A+B)(n) - (A+B)(a_k-1)) \\ &\geq \sum_{i=1}^{k-1}(\sigma(B)(a_{i+1}-a_i-1)+1) + (\sigma(B)(n-a_k)+1) \\ &= \sigma(B)(n-k) + k = \sigma(B)n + (1-\sigma(B))A(n) \geq (\sigma(A)+\sigma(B)-\sigma(A)\sigma(B))n.\end{aligned}$$

We can deduce that any set of positive density is a basis for the integers:

Corollary 2.2. *If $0 \in A$ and $\sigma(A) > 0$ then there exists h such that $hA \supseteq \mathbb{Z}_{\geq 0}$. We may take $h \leq 2\lceil(\log 2)/(-\log(1-\sigma(A))\rceil$.*

Proof. As $\sigma(A) > 0$ we know that $1 \in A \subset kA$ for all $k \geq 1$; and we deduce, by induction, from Schnirelmann's theorem, that if $0, 1 \in A$ then $1 - \sigma(kA) \leq (1 - \sigma(A))^k$ for all $k \geq 1$. Now let k be the smallest integer for which $(1 - \sigma(A))^k \leq 1/2$ so that $\sigma(kA) \geq 1/2$, and then $kA + kA \supseteq \mathbb{Z}_{\geq 0}$ by Lemma 2.1.

The most famous consequence of this is Schnirelmann's result that the primes form an additive basis, a first step along the road to Goldbach's conjecture. To prove this will require a little sieve theory to prove that $\underline{d}(2\mathbb{P}_{\geq 3}) \geq 2/3$[11]. Use this to show that the primes form an additive basis of order $\leq 2^{17}$.

A similar method can be used to prove Hilbert's theorem on Waring's problem, that for every integer k, there exists h such that every the kth powers of integers form an additive basis.

Before the sieve theory, we will make an analogous first step along the road to the twin prime conjecture, rather than Goldbach.

Given $S \subset G$ we define *the cube* $\overline{S} := \{\sum_{s\in S} \epsilon_s s : \ \epsilon_s \in \{-1, 0, 1\} \text{ for each } s \in S\}$, to have *dimension* $|S|$. Notice that $|\overline{S}| \leq 3^{|S|}$. If we have equality here then we call this a *proper cube*. Notice that a cube is a special case of a generalized arithmetic progression; and that our definition works for any additive group G.

Proposition 2.3. *If $A \subseteq \mathbb{Z}_{\geq 1}$ with $\overline{d}(A) > 0$, then there exists a finite cube $\overline{S}$ for which $A - A + \overline{S} = \mathbb{Z}$. In fact there exists such a cube of dimension $\lfloor \log(1/\overline{d}(A))/\log 2 \rfloor$.*

Proof. If $A-A\neq\mathbb{Z}$ then there exists an integer m such that $m\notin A-A$, and so A and $m+A$ are disjoint. Let $A_1=A\cup(m+A)=A+\{0,m\}$ so that $\overline{d}(A_1)=2\overline{d}(A)$ and $A_1-A_1=A-A+\overline{\{m\}}$. If this is not $\mathbb{Z}$, we then define $A_2,A_3,\dots$ and so on. However this construction cannot continue if $\overline{d}(A_k)>1/2$ (since we cannot have $\overline{d}(A_{k+1})>1$), and therefore $A_k-A_k=\mathbb{Z}$. This gives our result with k chosen so that $2^k\overline{d}(A)>1/2$.

From this and the result that $\underline{d}(2\mathbb{P}_{\geq 3})\geq 2/3^{11}$ we deduce that there exists a cube $\overline{S}$ of dimension ≤ 16 for which $2\diamond\mathbb{Z}=2\mathbb{P}_{\geq 3}-2\mathbb{P}_{\geq 3}+\overline{S}$.

One can continue this line of thinking in the well-known example that $4\mathbb{Z}^2=\mathbb{Z}_{\geq 0}$; in this case it is known that every positive integer is represented many times as the sum of four squares and that there are infinitely which are not the sum of three squares (in fact, precisely the integers $\{4^k(8m-1):k\geq 0,m\geq 1\}$). One might ask whether one can find a "thin" subset A of $\mathbb{Z}^2$, perhaps finite, such that $3\mathbb{Z}^2+A=\mathbb{Z}_{\geq 0}$. From the classification of integers that do not belong to $3\mathbb{Z}^2$ it is easy to show that $3\mathbb{Z}^2+\{0,1,4\}=\mathbb{Z}_{\geq 0}$. It is a challenge to find a "thin" set A for which $2\mathbb{Z}^2+A=\mathbb{Z}_{\geq 0}$ – show that such a set A cannot be finite.

The prime k-tuplets conjecture

The prime number theorem tells us that there are $\sim x/\log x$ primes $\le x$; or, put another way, if we randomly chose an integer near x then it is prime with probability $1/\log x$.

If we were to ask how often n and $n+d$ are prime when $n \le x$ then we might guess that one can assume that the events that they are each prime are "independent" of one another, and so this happens for about $1/\log^2 x$ of the integers n around x. However, in the case that $d = 1$ this heuristic fails to account for the fact that one of n and $n+1$ is always even, and thus n and $n+1$ cannot be simultaneously prime when $n > 2$. To take the divisibility of prime numbers into account, we note that the probability that neither of two randomly chosen numbers are divisible by p is $(1-1/p)^2$, whereas the probability that neither of n and $n+d$ are divisible by p if n is chosen randomly is $1-\omega(p)/p$ where $\omega(p) = 2$ unless p divides d, in which case $\omega(p) = 1$. Thus we have a "correction factor"

$$\text{Correction}_{t,t+d}(p) := \frac{\#\{n \pmod p : \ (n(n+d),p) = 1\}/p}{(\#\{m \pmod p : \ (m,p)=1\}/p)^2} = \frac{1-\omega(p)/p}{(1-1/p)^2},$$

and so expect there to be

$$\{\text{Twin}(d) + o(1)\} \ \frac{x}{\log^2 x} \ \text{ where } \text{Twin}(d) := \prod_{p \text{ prime}} \text{Correction}_{t,t+d}(p)$$

prime pairs $n, n+d$ with $n \le x$, and this claim is well supported by computational evidence. Note that if d is odd then $\text{Correction}_{t,t+d}(2) = 0$ so $\text{Twin}(d) = 0$. If d is even then we can rewrite our constant, $\text{Twin}(d)$, as

$$C\ \kappa_d \ \text{ where } \ \kappa_d := \prod_{\substack{p|n \\ p \text{ odd}}} \frac{p-1}{p-2} \ \text{ and } \ C := 2\prod_{p\ge 3} \frac{1-2/p}{(1-1/p)^2}.$$

It is not obvious that the infinite product defining C converges to a constant:

Exercise: (i) We define $\zeta(s) := \sum_{n\ge 1} \frac{1}{n^s}$ when $s = \sigma + it$ and $\sigma > 1$. Justify each of the inequalities $|\zeta(s)| \le \zeta(\sigma) \le 1 + \int_1^\infty \frac{dt}{t^\sigma} = \frac{\sigma}{\sigma-1}$, which proves that the sum is absolutely convergent.

(ii) Use the Fundamental Theorem of Arithmetic to show that $\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$ if $\text{Re}(s) > 1$.

(iii) Prove that $1 \le \frac{1-2/p}{(1-1/p)^2} \le \frac{1}{(1-1/p^2)}$ for each prime p. Deduce that $2 \le C \le \frac{3}{2}\zeta(2) \le 3$.

Given a set of irreducible polynomials $f_1(t), f_2(t), \dots, f_k(t)$ we analogously expect that the number of integers $n \le x$ for which $|f_1(n)|, |f_2(n)|, \dots$ and $|f_k(n)|$ are all prime is

$$\left\{ \prod_{p \text{ prime}} \text{Correction}_{|f_1(t)|,|f_2(t)|,\dots,|f_k(t)|}(p) + o(1) \right\} \ \frac{x}{\prod_{j=1}^k \log|f_j(x)|},$$

where

$$\text{Correction}_{|f_1(t)|,\dots,|f_k(t)|}(p) := \frac{\#\{n \pmod p : \ (f_1(n)\dots f_k(n),p) = 1\}/p}{(\#\{m \pmod p : \ (m,p)=1\}/p)^k}.$$

Define $r(n) = \#\{p, q \text{ primes} : p + q = n\}$. Evidently $r(n) \le 2$ if n is odd, and the above heuristic suggests that if n is even then

$$r(n) \sim C\ \kappa_d\ \cdot \frac{n}{\log^2 n}\ ,$$

the quantitative form of the *Goldbach conjecture*. The fundamental lemma of the sieve gives an upper bound for $r(n)$ that is slightly weaker than this: From Theorem 3.11 in [HR] we have that $r(n)$ is no more than $4 + o(1)$ times the prediction above. Now

$$\left(\frac{x}{2\log x}\right)^2 \sim \left(\sum_{p\le x/2} 1\right)^2 \le \sum_{\substack{p,q \text{ prime}\\ p+q\le x}} 1 = \sum_{n\le x} r(n),$$

whereas, by the Cauchy-Schwarz inequality,

$$\left(\sum_{n\le x} r(n)\right)^2 \le |(2\mathbb{P})(x)|\ \sum_{n\le x} r(n)^2 \lesssim |(2\mathbb{P})(x)| \sum_{\substack{n\le x\\ n \text{ odd}}} \left(4C \prod_{\substack{p\mid n\\ p \text{ odd}}} \frac{p-1}{p-2}\cdot\frac{n}{\log^2 n}\right)^2 .$$

Next we average this constant in a complicated exercise:

Exercise: (i) Prove that $\left(\frac{p-1}{p-2}\right)^2 \le 1 + \frac{9}{p}$ for each prime $p \ge 3$.

(ii) Let $\omega(d) = \sum_{p\mid d} 1$. Prove that $\prod_{p\mid n,\ p \text{ odd}} \left(\frac{p-1}{p-2}\right)^2 \le \sum_{d\mid n,\ d \text{ odd}} \frac{\mu^2(d)9^{\omega(d)}}{d}$.

(iii) Show that

$$\sum_{\substack{n\le x\\ n \text{ odd}}} \left(\prod_{\substack{p\mid n\\ p \text{ odd}}} \tfrac{p-1}{p-2}\right)^2 \le \sum_{\substack{d\le x\\ d \text{ odd}}} \tfrac{\mu^2(d)9^{\omega(d)}}{d}\cdot\tfrac{x}{d} \le x\prod_{p>2}\left(1+\tfrac{9}{p^2}\right) \le \left(\tfrac{3\zeta(2)}{4}\right)^9 x \le \left(\tfrac{3}{2}\right)^9 x.$$

Since $\frac{n}{\log^2 n} \le \frac{x}{\log^2 x}$, combining the last few equations yields that

$$|(2\mathbb{P})(x)| \gtrsim \frac{2x}{3^{11}}, \text{ so that } \underline{d}(2\mathbb{P}_{\ge 3}) \ge \frac{2}{3^{11}}.$$

Modify the above argument to show that if Q is any subset of the primes of positive density (that is, there exists a constant $c > 0$ such that $Q(x) \ge c\pi(x)$ if x is sufficiently large) then $\underline{d}(2Q) > 0$. Deduce that Q is an additive basis for the integers.

The Dyson transformation and its consequences

Freeman Dyson defined a transformation $A, B \to \delta_e(A), \delta_e(B)$ on a pair sets, which is useful in the context of adding sets: For any $e \in A$ we let $B_e := \{b \in B : \ b + e \notin A\}$ and then

$$\delta_e(A) := A \cup (e + B) = A \cup (e + B_e) \quad \text{and} \quad \delta_e(B) := B \setminus B_e.$$

Notice that $B_e \subseteq B$ and $A \cap (e + B_e) = \emptyset$, so that $|\delta_e(A) + |\delta_e(B)| = |A| + |B|$. We also have that $e + \delta_e(B) \subseteq A \subseteq \delta_e(A)$. It is useful in the context of adding sets for two reasons:

- We have $A \cap (e + B) = \delta_e(A) \cap (e + \delta_e(B))$ and $A \cup (e + B) = \delta_e(A) \cup (e + \delta_e(B))$;
- Also $\delta_e(A) + \delta_e(B) \subseteq A + B$.

To see this last assertion note that if $a \in \delta_e(A), b \in \delta_e(B) \subseteq B$ then either $a \in A$ (in which case $a + b \in A + B$ trivially) or $a \in e + B_e$, that is $a = e + b'$ with $b' \in B_e$: however we then have $e + b \in A$ (as $b \in \delta_e(B)$), say $e + b = a' \in A$, and so $a + b = (e + b') + b = (e + b) + b' = a' + b' \in A + B$.

With this tool we can prove Mann's improvement of Schnirelmann's theorem and other central results in this subject.

Mann's theorem. *If $0 \in A \cap B$ then $\sigma(A + B) \geq \min\{1, \sigma(A) + \sigma(B)\}$.*

This follows immediately from the stronger

Proposition 2.4. *If $0 \in A \cap B$ then $\frac{(A+B)(n)}{n} \geq \min\left\{1, \min_{1 \leq m \leq n} \frac{A(m)+B(m)}{m}\right\}$.*

Proof. Let $\eta := \min_{1 \leq m \leq n}(A(m)+B(m))/m$. The result follows from the proof of Lemma 2.1 if $\eta \geq 1$, so we may assume that $\eta < 1$. It will be convenient in this proof to suppose that $A, B \subseteq [0, n]$, wlog. There is nothing to prove if $n = 0$ or $B(n) = 0$ or $A(n) = 0$. So we will proceed by induction on n and then on $B(n)$, and we may now assume that $n, B(n) \geq 1$. We select e minimal so that $e + B$ is not a subset of A (evidently e exists, for we may simply take consider e and b to be the largest elements of A and B respectively, so that $e+b \notin A$). Note that $B_e(n) \geq 1$, so that $\delta_e(B)(n) < B(n)$ and thus we may proceed by the induction hypothesis as $(A+B)(n) \geq (\delta_e(A)+\delta_e(B))(n)$ (since $\delta_e(A)+\delta_e(B) \subseteq A+B$), once we prove that $\delta_e(A)(m) + \delta_e(B)(m) \geq \eta m$ for all $1 \leq m \leq n$.

Now $\{b \in B_e : \ m - e < b \leq m\} \subseteq \{b \in B : \ m - e < b \leq m\}$ so we have

$$\begin{aligned}\delta_e(A)(m) + \delta_e(B)(m) &= (A(m) + B_e(m - e)) + (B(m) - B_e(m)) \\ &= A(m) + B(m) - (B_e(m) - B_e(m - e)) \\ &\geq A(m) + B(m) - (B(m) - B(m - e)) = A(m) + B(m - e).\end{aligned}$$

If $B(m) = B(m - e)$ then we are done, for example in the case $e = 0$. Otherwise let b_1 be the smallest element of B which is $> m-e$, so that $b_1 \leq m$, and let $0 \leq r := m-b_1 \leq e-1$ $(\leq n-1)$. Then $A(m)+B(m-e) = A(m)+B(b_1-1) = (A(b_1+r)-A(b_1-1))+(A(b_1-1)+B(b_1-1))$. Now $A(b_1-1)+B(b_1-1) \geq \eta(b_1-1)$ by hypothesis. Now if $a \in A$ with $a \leq r < e$ then $a + B \subset A$ so that $b_1 + a \in A$: therefore $A(b_1 + r) - A(b_1 - 1) \geq A(r) + 1$, and $A(r) = (A+B)(r)$ since every element of $A+B$ which is $< e$ must belong to A (by the definition of e). Putting this altogether, and using the induction hypothesis on n to note that $(A+B)(r) \geq \eta r$, we have $A(m)+B(m-e) \geq \eta r+1+\eta(b_1-1) = \eta m+(1-\eta) \geq \eta m$.

Dyson generalization. *If* $0 \in A_1 \cap A_2 \cap \cdots \cap A_k$ *then*

$$\frac{(A_1 + A_2 + \cdots + A_k)(n)}{n} \geq \min\left\{1, \min_{1 \leq m \leq n} \frac{A_1(m) + A_2(m) + \cdots + A_k(m)}{m}\right\}.$$

A key question is how these results generalize to $\underline{d}$: one might guess that $\underline{d}(A+B) \geq \min\{1, \underline{d}(A)+\underline{d}(B)\}$, but this is wrong: The example $A = B = A+B = \{n \equiv 0 \pmod m\}$ shows that subgroups must be taken into consideration. The example $A = B = \{n \equiv 0 \text{ or } 1 \pmod m\}$ and $A+B = \{n \equiv 0, 1 \text{ or } 2 \pmod m\}$ shows that cosets of subgroups must also be taken into consideration. Evidently we first need to study addition of sets $\pmod m$, before going on to $\underline{d}$.

The Cauchy-Davenport theorem. *If* A *and* B *are non-empty subsets of* $\mathbb{Z}/N\mathbb{Z}$ *with* $0 \in B$*, and where* $(b, N) = 1$ *for all* $b \in B \setminus \{0\}$ *then* $|A + B| \geq \min\{N, |A| + |B| - 1\}$.

Proof. We need only prove this when $|A| + |B| - 1 \leq N$, for if $|A| + |B| - 1$ is larger then we simply take subsets $A' \subseteq A$ and $B' \subseteq B$ with $|A'| + |B'| - 1 = N$ and then $\mathbb{Z}/N\mathbb{Z} \supseteq A + B \supseteq A' + B' \supseteq \mathbb{Z}/N\mathbb{Z}$.

Proof by induction on $|B|$: if $|B| = 1$ then $B = \{0\}$ so $A+B = A$ and the result follows. For $|B| \geq 2$ select $b \in B \setminus \{0\}$. We claim that there exists $e \in A$ such that $e + B \not\subset A$ else $A + B = A$ and then summing the solutions of $a + b = a'$ over all $a \in A$ (and thus a' runs through the elements of A), we obtain $|A|b \equiv 0 \pmod N$. Now $(b, N) = 1$ by hypothesis and so $N||A|$ which is impossible since $1 \leq |A| \leq N - 1$.

The result holds for the pair $\delta_e(A), \delta_e(B)$ by the induction hypothesis (as $|\delta_e(B)| < |B|$), and then the result holds for the pair A, B by the properties of the Dyson-transform (verify this).

At first sight it would seem we could significantly weaken the hypothesis on B in the proof above to something like $(N, b_1, \ldots, b_r) = 1$ where $B = \{0, b_1, \ldots, b_r\}$. Explain why the proof fails in this situation.

Corollary 2.5. *If* A *and* B *are non-empty subsets of* $\mathbb{Z}/p\mathbb{Z}$ *where* p *is prime, then* $|A + B| \geq \min\{p, |A| + |B| - 1\}$.

Proof. Determine how to satisfy the hypotheses of the Cauchy-Davenport theorem in this case.

In fact one can prove that $|A + B| = |A| + |B| - 1 < p$ if and only if either
(i) A or B has just one element; or
(ii) $A = a_0 + d \diamond \{0, 1, \ldots, r-1\}, B = b_0 + d \diamond \{0, 1, \ldots, s-1\}$ for some $r + s \leq p - 1$; or
(iii) $A \cup (d - B)$ is a partition of $\mathbb{Z}/p\mathbb{Z}$ for some integer d.

In the proof above we see that if $|\delta_e(A) + \delta_e(B)| \geq |\delta_e(A)| + |\delta_e(B)|$ then $|A + B| \geq |A| + |B|$. Now if $|B| = 1$ then, trivially

Summing sets to get all of the integers

Proposition 2.6. *If A is an additive basis of order h then $A(n) \gg hn^{1/h}$. On the other hand there exists an additive basis A of order h with $A(n) \ll hn^{1/h}$.*

Proof. Suppose that $hA \supseteq \mathbb{Z}_{\geq m}$. Then $n + O(1) \leq (hA)(n) \leq \binom{A(n)+h-1}{h} = A(n)^h/h! + O(A(n)^{h-1})$, and the first result follows from Stirling's formula. On the other hand one can show that

$$A = \bigcup_{j=0}^{h-1} (2^j \diamond B) \text{ where } B = \left\{ \sum_{i=1}^{\ell} 2^{e_i h} : 0 \leq e_1 < e_2 < \cdots < e_\ell, \ell \geq 0 \right\}$$

is a basis of order h (Fill in the details here as an exercise. Hint: Consider representing $2^h - 1$ as a sum of elements of A). Now if $2^{(k-1)h} \leq n \leq 2^{kh} - 1$ then $B(n) \leq B(2^{kh} - 1) = 2^k \leq 2n^{1/h}$ and so $A(n) \leq \sum_{j=0}^{h-1} 2(2^{-j}n)^{1/h} \leq 2(1 - 2^{-1/h})^{-1} n^{1/h} \ll hn^{1/h}$. Determine an asymptotic formula for the value of $B(n)$ and then of $A(n)$.

Evidently $(h-1)A$ in this example is nowhere close to being all of $\mathbb{Z}$. One might guess that bases are, in some sense, "complementary"; in that of you added enough together you would obtain $\mathbb{Z}$. Nothing could be further from the truth, as the following generalization of the above construction shows.

Cute example: For given integers $h \geq 2$ and k, we now construct additive bases $B_1, \dots B_k$ of order h such that if $T = (h-1)(B_1 + B_2 + \cdots + B_k)$ then $T(n) \ll_{h,k} n^{1-1/(2h^k)}$:

Fix integer $g \geq (k(h-1))^2$and for any $S \subset \mathbb{Z}_{\geq 0}$ define $G(S) = \{\sum_{j \in S} e_j g^j : 0 \leq e_j \leq g-1\}$. Note that if $A \cap B = \emptyset$ then $G(A \cup B) = G(A) + G(B)$.

If $n = \sum_i n_i h^i$ in base n then let $N_{i,j}$ be the set of non-negative integers n with $n_i = j$, and note that $\cup_{j=0}^{h-1} N_{i,j}$ is a partition of $\mathbb{Z}_{\geq 0}$. Then define

$$B_i = \bigcup_{j=0}^{h-1} G(N_{i,j}), \text{ so that } (h-1)B_i = \bigcup_{j_i=0}^{h-1} (h-1)W(j_i) \text{ where } W(j_i) := \bigcup_{\substack{j=0 \\ j \neq j_i}}^{h-1} G(N_{i,j});$$

and therefore $T = \cup(h-1)(W(j_0) + W(j_1) + \cdots + W(j_{k-1}))$ where the union is taken over $0 \leq j_0, \dots, j_{k-1} \leq h-1$. Fix $j_0, \dots, j_{k-1}$ and write $U = (h-1)(W(j_0) + W(j_1) + \cdots + W(j_{k-1}))$, Now if $e \equiv j_0 + j_1 h + \cdots + j_{k-1}h^{k-1} \pmod{h^k}$ then $e \notin \cup_{j \neq j_i} N_{i,j}$ for any i, and so the least residue $\pmod{g^{e+1}}$ of an element of $W(j_1)$ is $\leq g^e - 1$. Therefore the least residue $\pmod{g^{e+1}}$ of an element of U is $\leq k(h-1)(g^e - 1)$, and so the coefficient of g^e in the base g expansion is $\leq k(h-1) - 1$. Therefore if $g^{(m-1)h^k} < n \leq g^{mh^k}$ for some integer $m \geq 1$ then

$$U(n) \leq U(g^{mh^k}) \leq (k(h-1)g^{h^k - 1})^m \leq g^{m(h^k - 1/2)} \leq g^{h^k - 1/2} n^{1-1/(2h^k)};$$

and then $T(n) \leq h^k g^{h^k - 1/2} n^{1-1/(2h^k)}$, as required.

It is often difficult, for given sets A and B, to determine whether $A+B=\mathbb{Z}$? (for example if $A=\{0\}\cup\{(p-1)/2:\ p\in\mathbb{P}_{\ge 3}\}$). Or, for a given set A one might wish to find "thin" sets B for which $A+B=\mathbb{Z}$ (for example where $A=\{0\}\cup\mathbb{P}$).

An *essential component* is a set B such that if $1>\sigma(A)>0$ then $\sigma(A+B)>\sigma(A)$. Khintchin showed in 1933 that $\mathbb{Z}^2$ is an essential component, and Erdős and Landau showed that they do turn out to be more common than one might expect.

We shall consider how small a set B one can add to A to guarantee that $A+B\supseteq\mathbb{Z}_{\ge m}$.

Lemma 2.7. *Let $a_0\ge 0$ be the smallest element of A, and suppose that $n+1\ge m+a_0$. Then there exists a subset S of $[m,2n-1]$ such that $\{n+1,n+2,\dots,2n\}\subseteq A+S$ with $|S|\ll n\log(2A(n-m+1))/A(n-m+1)$.*

With this key lemma we deduce Lorentz's theorem:

Theorem 2.8. *If $0\in A$ then there exists $B\subset\mathbb{Z}_{\ge 0}$ for which $A+B=\mathbb{Z}_{\ge 0}$ and $B(n)\ll a_1+\sum_{n>m\ge 1}\log(A(m))/A(m)$, where a_1 is the smallest element of $A_{\ge 1}$.*

Deduce that there exists B with $B+\mathbb{P}=\mathbb{Z}_{\ge 2}$ and $B(n)\ll\log^3 n$. Also that there exists C with $C+\mathbb{Z}^2=\mathbb{Z}_{\ge 0}$ with $C(n)\ll\sqrt{n}\log n$.

We can also deduce a "mod n version:

Theorem 2.9. *For any subset A of $\mathbb{Z}/N\mathbb{Z}$ there exists $B\subseteq\mathbb{Z}/N\mathbb{Z}$ for which $A+B=\mathbb{Z}/N\mathbb{Z}$ and $|B|\ll N\log(2|A|)/|A|$.*

Note that $|A||B|\ll N\log N$ (obviously one needs $|A||B|\ge N$; I have no idea whether one can improve on this log factor).

Proof of Theorem 2.9. Represent A as a subset of $\{1,\dots,n\}$ and then apply Lemma 2.7 with $m=1$ and $B=S$.

Proof of Theorem 2.8. For any $j\ge 2$, we can take $n=2^j$ and $m=2^{j-1}+1$ in Lemma 2.7 to obtain $B_j\subseteq(2^{j-1},2^{j+1})$ such that $\{2^j+1,2^j+2,\dots,2^{j+1}\}\subseteq A+B_j$ and $|B_j|\ll 2^j\log(2A(2^{j-1}))/A(2^{j-1})\ll\sum_{i=2^{j-2}}^{2^{j-1}}\log(A(i))/A(i)$ as $\log(A(i))/A(i)$ is a decreasing function for $A(i)\ge 3$. We take $B=\{0,1,\dots,a_1\}$ together with the B_j for all j with $2^{j+1}\ge a_1$.

Proof of Lemma 2.7. (Greedy) Let $I_0=\{n+1,n+2,\dots,2n\}$. Given $I_j\subset I_0$ we select integer $s_j\in[m,2n-1]$ so that $J_j:=(A+s_j)\cap I_j$ is maximal, and then let $I_{j+1}=I_j\setminus J_j$. Note that if $i\in I_0$ and $s\in[m,2n-1]$ then $i-s\ge n+1-m$ and so

$$(2n-m)|J_j|\ge\sum_{s=m}^{2n-1}|(A+s)\cap I_j|=\sum_{i\in I_j}|A\cap\{i-m,\dots,i-(2n-1)\}|$$
$$=\sum_{i\in I_j}A(i-m)\ge|I_j|A(n+1-m).$$

This implies that $|I_{j+1}|=|I_j|-|J_j|\le|I_j|(1-A(n+1-m)/(2n-m))$. Select k to be the smallest integer $>(2n-m)\log(2A(n+1-m))/A(n+1-m)$, so that $|I_k|\ll n/A(n+1-m)$. We let $S=\{s_1,s_2,\dots,s_k\}\cup(I_k-a_0)$, and the result follows.

Constructions by probabilistic methods!?

Tilings: Discuss

Covering congruences. One can sometimes show that $A+B \neq \mathbb{Z}$ in spectacular fashion by showing that $A+B$ misses a complete arithmetic progression; that is $(A+B) \cap (c + N \diamond \mathbb{Z}_{\geq m}) = \emptyset$. In the case that $A = \mathbb{P}$ we may be able to write $B = B_1 \cup B_2 \cup \dots B_k$ such that $B_j \subset c_j + p_j \diamond \mathbb{Z}$, for certain distinct primes $p_1, \dots, p_k$. In this case $(A+B) \cap (c + p_1 \dots p_k \diamond \mathbb{Z}) \subset \{p_1, \dots, p_k\}$ where c is chosen so that $c \equiv c_j \pmod{p_j}$ for each j by the Chinese Remainder theorem, for if $a + b \in c + p_1 \dots p_k \diamond \mathbb{Z}$ with $b \in b_j$, say, then $p_j | a$ so that $a = p_j$ since $A = \mathbb{P}$.

Erdős invented this idea to show that a certain congruence class of odd integers cannot be written in the form $p + 2^k$ with $p \in \mathbb{P}$. To develop this proof yourself consider writing the set $B = \{2^k : k \geq 1\}$ as $B_2 \cup B_3 \cup B_4 \cup B_8 \cup B_{12} \cup B_{24}$ where $B_m = \{2^k : k \equiv c_m \pmod{m}\}$ with $c_2 = 0, c_3 = 0, c_4 = 1, c_8 = 3, c_{12} = 7, c_{24} = 23$, and go from there.

Kneser's Theorem. *If A and B are finite subsets of additive group Z with $|A|, |B| > 1$ for which $|A+B| < |A|+|B|$ then let H be the largest subgroup of Z for which $A+B$ is a union of cosets of H (note that such a subgroup always exists, namely $H = \{0\}$; and also that H can possibly be all of Z). Let $A_0 \subset A$ and $B_0 \subset B$ be minimal so that $A \subset A_0 + H$ and $B \subset B_0 + H$ (and therefore $A + B = A_0 + B_0 + H$). Then $|A_0 + B_0| = |A_0| + |B_0| - 1$ in Z/H, and if $A^* = (A_0 + H) \setminus A$ and $B^* = (B_0 + H) \setminus B$ then $|A^*| + |B^*| \le |H| - 1$.*

It is worth noting that if we have $|A^*| + |B^*| \le |H| - 1$ as above then we must have $A + B = A + B + H$ (that is, $A + B$ is a union of cosets of H), for if $a + b \in A + B$ then $|A \cap (a + H)| + |B \cap (b + H)| \ge 2|H| - |A^*| - |B^*| \ge |H| + 1$ and so for any $c \in a + b + H$ we obtain $c \in A + B$ by the pigeonhole principle (as in the proof of Lemma 2.1).

Let $r(n) = r_{A+B}(n)$ be the number of representations of n in the form $a+b, a \in A, b \in B$. By another application of the pigeonhole principle one can show that for each $n \in A + B$,

$$r_{A+B}(n) \ge |A| + |B| - |A + B|.$$

To prove Kneser's theorem we will need to develop the theory of Dyson transformations: We saw above that the transformation $A, B \to \delta_e(A), \delta_e(B)$ has the properties that $\delta_e(B) \subset B$, $A \subset \delta_e(A)$ with $|\delta_e(A)| + |\delta_e(B)| = |A| + |B|$ and $\delta_e(A) + \delta_e(B) \subseteq A + B$. We may assume, wlog, that $0 \in B$ (after a translation), and then $0 \in \delta_e(B)$. A non-trivial transformation exists unless $A+B \subset A$ (so that all $B_e = \emptyset$), in which case $A+H \subset A$ where $H =< B >$ is the semigroup generated by B (and if Z is finite then H is a subgroup of Z). If we start with any pair of sets A, B we can go through a "derived" sequence of Dyson transformations $A, B \to^{e_1} A_1, B_1 \to^{e_2} \cdots \to^{e_r} A_r, B_r$, and from the above properties we have that $0 \in B_r \subset B$ and $A_r \supset A$ with $|A_r| + |B_r| = |A| + |B|$ and $A_r + B_r \subseteq A + B$. If B is finite then this can continue for only finitely many steps (since $|B_r| \le |B| - r$), and then we must have that $A_r + H \subset A_r$ where $H =< B_r >$. If A is also finite then $A_r + H = A_r$.

We also need a little technical lemma, for which we give a frustratingly long proof at the end of these notes. A keen student is invited to supply me with a short proof!

Lemma 2.10. *Let H_1, H_2 be finite subgroups of Z with $H_1 \cap H_2 = \{0\}$. Let C_j be a non-empty finite set of coset representatives for H_j, for $j = 1, 2$, and let $S_j = C_j + H_j$. Then either $S_1 \cup S_2 = S_1$ or S_2, or $|S_1 \cup S_2| \ge \min_{j=1,2} |S_j| + |H_j| - 1$.*

Proof of Kneser's Theorem. We will prove, by induction on $|T| \ge 1$, that for any non-empty subset $T \subset A + B$ there exists C, a finite set of coset representatives for some subgroup H, such that $T \subset C + H \subset A + B$, where $|A| + |B| \le (|C| + 1)|H|$. Once this is proved then we take $T = A + B$ so that $A + B = C + H'$, and therefore $|A + B| \ge |A| + |B| - |H'|$ (since $|A + B| = |C||H'|$). Now select H to be the largest subgroup of Z for which $A + B$ takes the form $C' + H$, and note that $|A + B| \ge |A| + |B| - |H'| \ge |A| + |B| - |H|$. Now $(A + H) + (B + H) = A + B$, so we get the same largest subgroup, H, when we add $A + H$ and $B + H$, and then the inequality above is $|A + B| \ge |A + H| + |B + H| - |H|$. Writing $A + H = A_0 + H, B + H = B_0 + H, A + B = C_0 + H$ where A_0, B_0, C_0 are minimal such sets, then we see that $|C_0||H| = |A + B| \ge |A + H| + |B + H| - |H| = (|A_0| + |B_0| - 1)|H|$. Therefore $|C_0| \ge |A_0| + |B_0| - 1$: we may assume that $|C_0| = |A_0| + |B_0| - 1$, for if $|C_0| \ge |A_0| + |B_0|$ then $|A + B| = |C_0||H| \ge (|A_0| + |B_0|)|H| \ge |A + H| + |B + H| \ge |A| + |B|$. Thus $|A_0 + B_0| = |A_0| + |B_0| - 1$ in Z/H as claimed, and finally note that

$|A+B| = |H|(|A_0|+|B_0|-1) = |A|+|B|+|A^*|+|B^*|-|H|$ and so $|A^*|+|B^*| < |H|$, when $|A+B| < |A|+|B|$. Now to prove our claim:

For $T = \{a_0+b_0\}$ take $A, B \to A-a_0, B-b_0$ so, wlog, $T = \{0+0\}$ and $0 \in A \cap B$. We now go through a derived sequence of Dyson transformations on the pair A, B to end up with a pair of sets A', B' for which $0 \in B' \subset B$ and $|A'|+|B'| = |A|+|B|$ with $0 \in A \subset A' = A'+B' = A'+H \subseteq A+B$ where $H =< B' >$. The result follows by taking C minimal so that $C+H = A'+H = A'$, giving that $|A|+|B| = |A'|+|B'| \leq |C+H|+|H| = (|C|+1)|H|$, with equality if and only if $B' = H$.

For $|T| \geq 2$ we partition $T = T_1 \cup T_2$ with $|T_1|, |T_2| \geq 1$ and apply the induction hypothesis to each part, obtaining $T_j \subset C_j + G_j \subset A+B$, where $|A|+|B| \leq (|C_j|+1)|G_j|$ for $j = 1, 2$. If $C_1+G_1 \subset C_2+G_2$ then we simply take $C = C_2$ and $H = G_2$ (and similarly if $C_2+G_2 \subset C_1+G_1$). Otherwise let $H = G_1 \cap G_2$ and $H_j = G_j/H$ for $j = 1, 2$. Put $C = (C_1+H_1) \cup (C_2+H_2)$ so that $C+H = (C_1+G_1) \cup (C_2+G_2) \supset T_1 \cup T_2 = T$. By Lemma 2.10 we have that $|C| \geq \min_{j=1,2} |C_j+H_j| + |H_j| - 1$; and so for that value of j we have $|A|+|B| \leq (|C_j|+1)|G_j| = (|C_j+H_j|+|H_j|)|H| \leq (|C|+1)|H|$ as required.

Remarks: It would be good to have a result pertaining to the structure of A_0 and B_0. In particular if $\{0\}$ is the largest subgroup H of Z for which $A+B = A+B+H$ and $|A+B| = |A|+|B|-1$ then we should be able to classify the possible structures for A and B. Perhaps the classification is analagous to what one finds for $\mathbb{Z}/p\mathbb{Z}$, as in just after Corollary 2.5 above.

It would be good to have a direct proof of Kneser's theorem, using little more than induction and Dyson transformations, but I have not yet found out how to do this (but seem to be close).

Counting representations

We define $r_{A+B}(n)$ to be the number of representations of n in the form $a+b, a \in A, b \in B$; and we analogously define $r_{A-B}(n)$, $r_{AB}(n)$, $r_{2A-2B}(n)$, etc. It is more natural, analytically, to work with $r_{A+B}(n)$ than $A+B$, because

$$\hat{A}(m)\hat{B}(m) = \sum_n r_{A+B}(n) e\left(\frac{nm}{p}\right) \quad \text{for every } m.$$

Proof. Exercise.

However, applications in additive combinatorics need estimates on $A+B$, which are often developed from an in-depth understanding of $r_{A+B}(n)$. The key link between the two is seen by using the Cauchy-Schwarz inequality. First note that, and justify as an exercise, that

$$|A||B| = \sum_n r_{A+B}(n) = \sum_{n \in A+B} r_{A+B}(n) = \sum_j r_{A-B}(j) = \sum_k r_{AB}(k).$$

Squaring this and then using Cauchy-Schwarz, yields

$$(|A||B|)^2 = \left(\sum_{n \in A+B} r_{A+B}(n)\right)^2 \le \sum_{n \in A+B} 1 \cdot \sum_{n \in A+B} r_{A+B}(n)^2. \tag{6.2}$$

The first term here is $|A+B|$; we need to better understand the second. Indeed (exercise) justify that

$$E(A,B) := \#\{a+b = a'+b' : \ a, a' \in A, \ b, b' \in B\} = \sum_{n \in A+B} r_{A+B}(n)^2.$$

We call $E(A,B)$ the *additive energy* between two sets A and B. Any quadruple counted in $E(A,B)$ also gives rise to solutions to $a - b' = a' - b$, so that $E(A,B) = E(B,A) = E(A+x, B+y) = E(A,-B)$. Such a quadruple also implies that $a - a' = b' - b$, and so

$$E(A,B) = \sum_x r_{A+B}(x)^2 = \sum_y r_{A-B}(y)^2 = \sum_z r_{A-A}(z) r_{B-B}(z). \tag{6.1}$$

We can re-write (6.2) as

$$(|A||B|)^2 \le |A \pm B| \ E(A,B). \tag{6.2'}$$

We deduce that if $A+B$ or $A-B$ is "small", say $\le C \max\{|A|,|B|\}$ then $E(A,B)$ is "large", that is $|E(A,B)| \ge \frac{1}{C}|A||B| \min\{|A|,|B|\}$.

Exercise: Prove that $|A||B| \le E(A,B) \le |A||B| \min\{|A|,|B|\}$.

We would like a converse theorem. That is, if $E(A,B)$ is "large" then $A+B$ and $A-B$ are "small", or something of this nature. We will return to this later, eventually proving the Balog-Szemerédi-Gowers Theorem which states that if $E(A,A)$ is large then there is a large subset A' of A, such that $A'+A'$ is small.

(6.2') also leads to a lower bound on the largest $r_{A+B}(x)$:

Lemma 6.3. $\max_x r_{A+B}(x) \geq \frac{|A||B|}{\min\{|A+B|,|A-B|\}}$.

Proof. $|A||B| \max_x r_{A+B}(x) = \max_x r_{A+B}(x) \sum_n r_{A+B}(n) \geq \sum_n r_{A+B}(n)^2 = E(A,B)$ and the result follows from (6.2').

We note that we can separate the variables:

(6.3)
$$E(A,B)^2 = \left(\sum_z r_{A-A}(z) r_{B-B}(z)\right)^2 \leq \sum_z r_{A-A}(z)^2 \sum_z r_{B-B}(z)^2 = E(A,A)E(B,B).$$

Now $E(A,B) \geq |A||B|$ with equality if and only if the $a+b$ are all distinct. We shall explore this in the next subsection. Evidently $E(A,A) \geq \binom{|A|+1}{2}$, and we obtain equality if all the $a_i + a_j,\ i \leq j$ are distinct; such a set is called a *Sidon set*.

Exercise: Show that if $A' \subset A$ then $E(A',B) \leq E(A,B)$. Show that for any set C we have $E(A,B) \leq E(A+C,B)$. In particular $E(mA,nB) \geq E(A,B)$ for all $m,n \geq 1$.

Adding finite sets

One has $\max\{|A|,|B|\} \le |A+B| \le |A||B|$ for any two sets A, B in a commutative, additive group G. We are interested in when these bounds can be attained.

(i) Prove that $|A+B| = |A|$ if and only if $|A-B| = |A|$.
(ii) Prove that $|A+B| = |A||B|$ if and only if $|A-B| = |A||B|$. Show that this is also equivalent to $(A-A)\cap(B-B) = \emptyset$.
(iii) Show that if $|A|+|B| > |G|$ then $A+B = A-B = G$. Give an example where $A+B \ne G$ with $|A|+|B| = |G|$.

The *Cartesian product* of two sets $A \times B$ is simply the set of ordered pairs (a,b) with $a \in A,\ b \in B$. We define $(A\times B)+(C\times D) = (A+C)\times(B+D)$; that is the sum of two Cartesian products is taken componentwise. Also define $A^{(k)} := A\times A\times\ldots\times A$ (k times).

(iv) Prove that $|A\times B| = |A||B|$.

In general $A+B$ and $A-B$ do not have the same size: For $A=\{0,1,3\}$ we have $A+A = \{0,1,2,3,4,6\}$ and $A-A = \{-3,-2,-1,0,1,2,3\}$, so $|A+A| = 6 < |A-A| = 7$. Hence $|B+B| = 6^k < |B-B| = 7^k$ for $B = A^{(k)} = \{0,1,3\}^k$. For random sets A (where the sums are all distinct) we have $|A+A| = \frac{|A|(|A|+1)}{2}$ whereas $|A-A| = |A|^2 - |A| + 1$, so it is not surprising that we can find an example with $|A+A| < |A-A|$. More interesting would be examples with $|A+A| > |A-A|$; indeed examples with $A+A$ a lot bigger than $A-A$. For $A = \{0,2,3,4,7,11,12,14\}$ we have $|A-A| = 25 < |A+A| = 26$. Hence $|B-B| = 25^k < |B+B| = 26^k$ for $B = A^{(k)}$.

In the Freiman-Ruzsa theorem we are interested in the size of $A+A$ compared to A, so we define the *doubling constant* $D(A) := |2A|/|A|$. Note that $1 \le D(A) \le (|A|+1)/2$. The upper bound is attained exactly for Sidon sets.

Show that if A is a subset of an abelian group G. Let $H(A) := \{h \in Z :\ h+A = A\}$. Prove that $A+H(A) = A$, and that $H(A)$ must be a subgroup of G. Deduce that there exist $a_1,\ldots,a_k \in G$, each belonging to different cosets of H, such that $A = \bigcup_{i=1}^k (a_i+H)$

Define the *Ruzsa distance* between two sets A, B in an abelian group G as $d(A,B) = \log\left(\frac{|A-B|}{\sqrt{|A||B|}}\right)$. Prove each of the following:
(i) $d(A,B) = d(-A,-B) = d(B,A) = d(A+x, B+y)$.
(ii) $d(A\times A', B\times B') \le d(A,B) + d(A',B')$.
(iii) Prove that the positivity and symmetry properties hold.
(iv) Prove that $d(A,B) \ge 0$. Moreover $d(A,B) = 0$ if and only if $B \subset b + H(A)$ for some $b \in G$. Deduce that the Ruzsa distance is not truly a distance function.

However the Ruzsa distance does satisfy the triangle inequality, $d(A,C) \le d(A,B) + d(B,C)$, as we will deduce from the next lemma.

The Plünnecke-Ruzsa theorem. Fix constant $C > 0$. The (as yet unproved) Freiman-Ruzsa Theorem tells us that if $|2A| \le C|A|$ then A is a large subset of a low dimensional generalized arithmetic progression P. Let us suppose that $|P| \le v(C)|A|$ and has dimension $\le d = d(C)$, where $d(C)$ and $v(C)$ depend only on C. Then $|mP| \le m^{d(C)}v(C)|A|$. Can we directly obtain a result of this type? In other words if $|2A| \le C|A|$ is it true that $|mA| \le C_m|A|$ where C_m is a constant that depends only on C and m? What about $|mA - nA|$? There is a remarkably complete answer to this problem:

Plünnecke-Ruzsa theorem. *We have* $\frac{|mA-nA|}{|A|} \le \left(\frac{|2A|}{|A|}\right)^{m+n}$ *for* $m, n \ge 1$.

Plünnecke's proof is a delightful excursion in graph theory, molded into a beautiful proof in work of Ruzsa. We will not give their proof here,[2] preferring to obtain a weaker result, which is good enough for our purposes, obtained strictly through combinatorial means, and more in the spirit of what is to come later in this course. We will now prove:

Corollary 6.10. *We have* $\frac{|mA-nA|}{|A|} \le \left(\frac{|2A|}{|A|}\right)^{6m+6n-10}$, *for any* $m, n \ge 1$.

Lemma. (Ruzsa) *For any sets* A, B, C *we have*

$$|A-C||B| \le |A-B||B-C|. \tag{6.0}$$

Exercise: Deduce the triangle inequality for the Ruzsa distance.

Proof. We will define a map $\phi : (A-C)\times B \to (A-B)\times(B-C)$, and prove that it is an injection, which implies the result. Given $d \in A-C$ select a unique pair $a_d \in A, c_d \in C$ for which $d = a_d - c_d$. Then $\phi(d,b) = (a_d - b, b - c_d)$ for each $d \in A-C,\ b \in B$. To prove that it is an injection, suppose that $(u,v) \in \text{Image}(\phi) \subset (A-B)\times(B-C)$. If $\phi(d,b) = (u,v)$ then $u+v = (a_d-b)+(b-c_d) = a_d - c_d = d$, and therefore we can determine d and hence a_d and c_d from (u,v). And we also determine b as $b = a_d - u$.

Our first goal in this section is to show that $A+A$ is "not much larger than" A (that is, $|A+A|$ is no more than some constant times $|A|$) if and only if $A-A$ is not much larger than A. We do this by combining Ruzsa's lemma with the following lemma due to Lev.

Lemma. (Lev) *For any sets* A, B *and* $x \in G$ *we have* $r_{A+B}(x)|A+B| \le |A-B|^2$.

Proof. We will define a map $\phi : \{(a,b,c) \in A\times B\times(A+B) : a+b = x\} \to (A-B)\times(A-B)$, and prove that it is an injection, which implies the result. Give $c = A+B$ select a unique pair $a_c \in A, b_c \in B$ for which $c = a_c + b_c$. Then $\phi(a,b,c) = (a-b_c, b-a_c)$ for each $a \in A,\ b \in B$ with $a+b = x$ and $c \in A+B$. Suppose that $(u,v) \in \text{Image}(\phi)$. If $\phi(a,b,c) = (u,v)$ then $x-u-v = x-(a-b_c)-(b-a_c) = (x-a-b)+(a_c+b_c) = c$, so that we can determine c and hence a_c and b_c from (u,v). Finally we can determine $a = u+b_c$ and $b = v+a_c$.

Corollary. *For any set* A *we have*

$$\left(\frac{|A+A|}{|A|}\right)^{1/3} \le \frac{|A-A|}{|A|} \le \left(\frac{|A+A|}{|A|}\right)^{2}.$$

Proof. We get the second inequality by taking $B = -A$ and $C = A$ in Ruzsa's lemma.

Combining (6.2) (with B replaced by $-B$) and (6.1) we have

$$\begin{aligned}(|A||B|)^2 &\le |A-B| \cdot \sum_{n\in A-B} r_{A-B}(n)^2 \le |A-B| \cdot \sum_{m\in A+B} r_{A+B}(m)^2 \\ &\le |A-B|\ \max_x r_{A+B}(x) \cdot \sum_{m\in A+B} r_{A+B}(m) = |A-B|\ |A|\ |B|\ \max_x r_{A+B}(x).\end{aligned}$$

[2]The reader should consult [.] for Ruzsa's proof.

We divide through by $|A||B|$, multiply through by $|A+B|$, and use Lev's lemma to obtain

$$|A||B||A+B| \le |A-B|\ |A+B|\ \max_x r_{A+B}(x) \le |A-B|^3.$$

The first inequality follows by taking $B = A$.

Exercise: Use the last displayed equation to obtain $d(A,-B) \le 3d(A,B)$.

Corollary. *For any set A and any integers $m, n \ge 0$ with $m+n \ge 1$ we have*

$$\frac{|mA-nA|}{|A|} \le \left(\frac{|2A|}{|A|}\cdot\frac{|3A|}{|A|}\right)^{m+n-1}$$

Proof. Suppose that $r, s \ge 0$ are given integers. Writing $(r+s)A = rA-(-sA)$ we have $|(r+s)A||-A| \le |(r+1)A||sA-A|$, as well as $|rA-sA||-A| \le |(r+1)A||(s+1)A|$ from (6.0). Exercise: Deduce that

$$\frac{|(r+s)A|}{|A|} \le \frac{|(r+1)A|}{|A|}\ \frac{|(s+1)A|}{|A|}\ \frac{|2A|}{|A|};$$

and then, from a simple induction hypothesis, that

$$\frac{|nA|}{|A|} \le \left(\frac{|3A|}{|A|}\right)^{n-2}\left(\frac{|2A|}{|A|}\right)^{n-3} \quad \text{for all } n \ge 3.$$

Deduce similar bounds for $|rA-sA|/|A|$ when $r, s \ge 2$, and then prove our result for all $m, n \ge 0$.

Since $|2A| \le |3A|$ we deduce that if $3A$ is not much larger than A, then any given difference of multiples of A is not much larger than A. This hints at the structure given by the Freiman-Ruzsa Theorem. It would be preferable to prove this result in terms of the ratio $\frac{|2A|}{|A|}$ only. To do this we move onto the next type of technique, which is to not only look at the set of all sums $A+B$ but also at a well-chosen subset.

Covering Lemmas. The idea will be to cover B by translates of $A-A$, for any given sets A, B. The size of X will be bounded by the growth when we add B to A.

Lemma. (Ruzsa) *$B \subset A-A+X$ for some $X \subset B$ with $|X| \le |A+B|/|A|$.*

Proof. Choose $X \subset B$ maximal so that $\{A+x : x \in X\}$ are disjoint. Their union contains exactly $|A||X|$ elements, all inside $A+B$, and thus the bound on $|X|$. Now, if $b \in B$ then $A+b$ intersects $A+x$ for some $x \in X$, and so $b \in A-A+x$.

Corollary. *There exists $X \subset 2A-A$ of size $\le |2A-2A|/|A|$ such that*

$$mA-nA \subset A-A+(m-1)X-(n-1)X \quad \textit{for all } m, n \ge 1.$$

Let $\langle A\rangle$ be the subgroup generated by A. Then $\langle A\rangle \subset A-A+\langle X\rangle$.

Proof. Let $B = A-2A$ in Ruzsa's covering lemma to get $2A-A \subset A-A+X$ for $X \subset 2A-A$ with $|X| \le |2A-2A|/|A|$. But then, adding A to both sides we obtain $3A-A \subset 2A-A+X \subset A-A+2X$. Exercise: Show that the first result now follows by induction on $m, n \ge 1$. To obtain the second result simply take the union of both sides over all $m, n \ge 1$, and note that $kA \subset (k+1)A-A$ for all $k \ge 1$.

This allows us to prove another version of Corollary *:

Corollary 6.7. *We have* $\frac{|mA-nA|}{|A|} \le \frac{|A-A|}{|A|}\left(\frac{|2A-2A|}{|A|}\right)^{m+n-2}$, *for any* $m, n \ge 1$.

Proof. We have $|mA - nA| \le |A - A||(m-1)X||(n-1)X| \le |A - A||X|^{m+n-2}$ from the previous Corollary, and the result follows.

Exercise: Show that $|mX| = \binom{|X|+m-1}{m} \le (m+1)^{|X|-1}$. Deduce that if $|2A - 2A| \le \kappa|A|$ then there exists a constant C_κ such that $\frac{|mA-nA|}{|A|} \le C_\kappa(mn)^{\kappa-1}$, for any $m, n \ge 1$.
Now be a little more precise. Show that if $y \in mX - mX$ there exists a partition of $X = U \cup V$ such that $y \in rU - rV$ where $m \ge r \ge 0$. Show that the number of such y is $|rU||rV| \le (r+1)^{|X|-2}$. Deduce that $|mX - mX| \le 2(2m+2)^{|X|-1}$. Conclude that if $|2A - 2A| \le \kappa|A|$ then there exists a constant C_κ such that $\frac{|mA-nA|}{|A|} \le C_\kappa(m+n)^{\kappa-1}$, for any $m, n \ge 0$.

Lemma. (Green's variation) *There exists* $X \subset B$ *with* $|X| \le 2|A+B|/|A| - 1$, *such that for all* $b \in B$ *there are* $> |A|/2$ *values of* $a \in A$ *for which* $a + b \in A + X$. *Hence* $B \subset A - A + X$ *and* $B - B \subset A - A + X - X$.

Proof. Let $X_0 = \emptyset$. We create $X_1, X_2, \dots$ by the following greedy algorithm: Given X_j, if there exists $b \in B$ for which $b + A$ has $\ge |A|/2$ elements that are not already in $A + X_j$, that is if $|(b + A) \cap (X_j + A)| \le |A|/2$, then let $X_{j+1} = X_j \cup \{b\}$ and $b_{j+1} = b$; otherwise let $X = X_j$ and stop the algorithm.

For each $b \in X$ we have $a + b \in A + X$ for all $a \in A$, that is for $|A|$ values of $a \in A$.

If $b \notin X$ then $b + A$ has $< |A|/2$ elements that are not in $A + X$, else we could have expanded X. In other words $> |A|/2$ elements of $b + A$ also belong to $A + X$, as required.

Now $X_{j+1} + A = (X_j + A) \cup ((b_j + A) \setminus (X_j + A))$ so that

$$|X_{j+1} + A| = |X_j + A| + |b_j + A| - |(b_j + A) \cap (X_j + A)| \ge |X_j + A| + |A| - |A|/2.$$

Exercise: Deduce, by an appropriate induction hypothesis, that $|X_j + A| \ge \frac{j+1}{2}\,|A|$, and so $|B + A| \ge |X + A| \ge |A|(|X| + 1)/2$ as $X + A \subset B + A$. We have now established the first part of the Lemma.

That $B \subset A - A + X$ follows immediately. For each of $b, b' \in B$ there are $> |A|/2$ values of $a, a' \in A$ for which $a + b, a' + b' \in A + X$. By the pigeonhole principle, there exists some $a' = a$, and therefore $b - b' = (a + b) - (a + b') \in (A + X) - (A + X)$.

Theorem 6.9. $|2B - 2B| \le |A + B|^4|A - A|/|A|^4$.

Proof. Let $z \in B - B$ so that $z = b_1 - b_2$ for some $b_1, b_2 \in B$. We first show that $\#\{(x, c, a_1) \in X \times (A + B) \times A : \ z = c - a_1 - x\} > |A|/2$. To prove this simply take the $> |A|/2$ solutions to $b_2 = a_1 - a_2 + x$ from the previous lemma and write $z = (a_2 + b_1) - a_1 - x$.

Now let $y \in 2B - 2B$ so that $y = z - z'$ for some $z, z' \in B - B$. We have $\#\{(x, x', c, c', d) \in X^2 \times (A + B)^2 \times (A - A) : \ y = c - c' - d - x + x'\} > (|A|/2)^2$. To see this simply take the solutions to $z = c - a_1 - x,\ z' = c' - a_1' - x'$ from the previous paragraph and then $d = a_1 - a_1'$. These give distinct solutions, since we recover z, z', c, c', x, x' from the solutions, and then $a_1 = c - x - z,\ a_1' = c' - x' - z'$. Summing over each $y \in 2B - 2B$ we obtain

$$|2B - 2B|\ |A|^2 < 4|X|^2|A + B|^2|A - A| < \frac{16\ |A + B|^4|A - A|}{|A|^2}.$$

To complete the proof we use the Cartesian product. Thus, from this last inequality we deduce that, for any $k \ge 1$, we have

$$|2B-2B|^k = |2B^{(k)}-2B^{(k)}| < \frac{16|A^{(k)}+B^{(k)}|^4|A^{(k)}-A^{(k)}|}{|A^{(k)}|^4} = 16\left(\frac{|A+B|^4|A-A|}{|A|^4}\right)^k.$$

Taking kth roots and letting $k \to \infty$ we get the result (since A and B are fixed and finite).

Proof of Corollary 6.10. Ruzsa' lemma with $C = A$ and $B = -A$ gives that $\frac{|A-A|}{|A|} \le \left(\frac{|2A|}{|A|}\right)^2$. Theorem 6.9 with $B = A$ gives $\frac{|2A-2A|}{|A|} \le \left(\frac{|2A|}{|A|}\right)^4 \frac{|A-A|}{|A|}$. Inserting these into Corollary 6.7 yields our result.

Lemma 6.6. *There exists $S \subset A+B$ such that $\#\{a \in A, b \in B : \ a+b \in S\} \ge |A||B|/2$ with $|S| \ge \max\{|A|,|B|\}/2$ and for which $|A+B+nS| \le 2^n|A+B|^{2n+1}/|A|^n|B|^n$ for all $n \ge 0$.*

Proof. Let $S = \{s : r_{A+B}(s) \ge |A||B|/2|A+B|\}$ and prove the first two assertions. For any $c \in A+B+nS$ there exists $a_0 \in A, b_{n+1} \in B$ and $s_1, \dots, s_n \in S$ such that $c = a_0+b_{n+1}+s_1+\cdots+s_n$. Now for any given s_j there exists at least $|A||B|/2|A+B|$ solutions to $a_j + b_j = s_j$ and thus at least $(|A||B|/2|A+B|)^n$ sets $a_1, \dots, a_n \in A,\ b_1, \dots, b_n \in B$ with $a_1+b_1 = s_1, \dots, a_n+b_n = s_n$. Each such solution leads to an element $(t_1, \dots, t_{n+1}) \in (A+B)^{n+1}$ defined by $t_i = a_{i-1} + b_i$: we claim that these are distinct since we can recover $a_1, \dots, a_n,\ b_1, \dots, b_n$ given $a_0, b_{n+1}, s_1, \dots, s_n, t_1, \dots, t_{n+1}$. Therefore $(|A||B|/2|A+B|)^n|A+B+nS| \le |A+B|^{n+1}$ and the result follows.

A discussion of Plünnecke's Theorem. Let A and B be sets of elements. Plünnecke considered a class of graphs modeled on the graph with ith vertex set $V_i := A+iB,\ i = 0, 1, 2, \dots$, where the only edges are directed edges between V_i and V_{i+1} for some $i \ge 0$, and there is an edge from $u \in V_i$ to $v \in V_{i+1}$ if and only if there exists $b \in B$ for which $u+b = v$. We define the ith magnification ratio to be

$$D_i := \min_{\substack{X \subset A \\ X \ne \emptyset}} \frac{|\Gamma_i(X)|}{|X|},$$

where $\Gamma_i(X)$ is the set of vertices in V_i that are at the end of a directed path starting in X; in our case $\Gamma_i(X) = X+iB$. Plünnecke proved the remarkable result that

$$D_1 \ge D_2^{1/2} \ge D_3^{1/3} \ge \dots \ge D_n^{1/n} \ge \dots$$

We deduce

Proposition. (Plünnecke) *If $|A+hB| \le C^h|A|$ then, for any given $k \ge h$, there exists a non-empty $X \subset A$ such that $|X+kB| \le C^k|X|$.*

Proof. By the above we know there exists a non-empty $X \subset A$ such that

$$\frac{|X+kB|}{|X|} = D_k \le D_h^{k/h} \le \left(\frac{|A+hB|}{|A|}\right)^{k/h} \le C^k.$$

Corollary. *If* $|A+B| \leq C|A|$ *then* $|kB - \ell B| \leq C^{k+\ell}|A|$ *for all* $k, \ell \geq 0$.

Proof. When $\ell = 0$ take $h = 1$ in the Proposition, so that $|kB| \leq |X + kB| \leq C^k|X| \leq C^k|A|$.

Otherwise suppose $k \geq \ell \geq 1$. Apply the Proposition with $h = 1, k = \ell$ to obtain that there exists a non-empty $X \subset A$ such that $|X + \ell B| \leq C^\ell |X|$. Now apply the Proposition with $h = \ell$ to obtain that there exists a non-empty $Y \subset X$ such that $|Y + kB| \leq C^k|Y|$. Finally we apply Ruzsa's lemma to obtain $|kB - \ell B||-Y| \leq |Y + kB||Y + \ell B| \leq C^{k+\ell}|Y|^2$, and the result follows as $Y \subset A$.

The Hales-Jewett Theorem

In 1927 van der Waerden [20] answered a conjecture of Schur, by showing that if the natural numbers are partitioned into two sets then one set must contain arbitrarily long arithmetic progressions. One can ask to generalize this to r sets, and ask for explicit bounds: That is, for given positive integers k, r determine the least integer $W = W(k, r)$ such that no matter how the integers in $\{1, 2, \dots, W\}$ are partitioned (or "coloured"), there is always a partition containing a k-term arithmetic progression (that is, there is always "a monochromatic k-term arithmetic progression").

`Examples and Discussion needed`

The Hales-Jewett Theorem [8] provides a beautiful, highly combinatorial, way to prove this result; it can be thought of as a generalization of van der Waerden's problem. For given positive integers k, r we wish to find the least integer $d = d(k, r)$ such that if the elements of $\{1, 2, \dots, k\}^d$ are r-colored then it contains a *monochromatic line*: For a given nonempty $S \subset \{1, 2, \dots, k\}$ a *line* is a set of points of the form $L = \{\mathbf{x}_0 + t\mathbf{y}_S : \ t = 1, 2, \dots k\}$ where $(\mathbf{y}_S)_i = 1$ if $i \in S$ and $(\mathbf{y}_S)_i = 0$ if $i \notin S$, and $(\mathbf{x}_0)_i = 0$ if $i \in S$. The Hales-Jewett Theorem asserts that $d(k, r)$ exists for all $k, r \geq 1$.

Show that $W(k, r) \leq k^{d(k,r)}$ by representing the integers up to $k^{d(k,r)}$ in base k, and then representing each such number by points in $\{1, 2, \dots, k\}^{d(k,r)}$.

Shelah [14] recently gave a delightfully ingenious proof that $d(k, r)$ exists: We prove the result by induction on k. It is clear that $d(1, r) = 1$ for all r, so now suppose that $k \geq 2$ and we have a value for $d(k-1, s)$ for all $s \geq 1$. Take $M = d(k-1, r)$ and define $N_1 = r^{(k-1)^{M-1}}$ and $N_i = r^{(k-1)^{M-i} k^{N_1 + \cdots + N_{i-1}}}$ for $i = 2, 3, \dots, r$. We will prove that $d(k, r) \leq N := N_1 + N_2 + \cdots + N_M$.

An r-colouring κ of $\{1, 2, \dots, k\}^N$ is a function $\kappa : \{1, 2, \dots, k\}^N \to \{1, \dots, r\}$. Our plan is to construct lines $L_1, \dots, L_M$ with each L_j $(= \mathbf{x}_j + t_j \mathbf{y}_j) \subset \{1, 2, \dots, k\}^{N_j}$, so that $\kappa(\mathbf{x}_1 + t_1\mathbf{y}_1, \mathbf{x}_2 + t_2\mathbf{y}_2, \dots, \mathbf{x}_M + t_M\mathbf{y}_M)$ does not change value for any given set of values $t_1, t_2, \dots, t_{i-1}, t_{i+1}, \dots, t_M$ as t_i changes from $k-1$ to k. Now define a colouring of $\{1, \dots, k-1\}^M$, so that the colour of $\kappa^*(t_1, \dots, t_M) = \kappa(\mathbf{x}_1 + t_1\mathbf{y}_1, \dots, \mathbf{x}_M + t_M\mathbf{y}_M)$; we know that there exists a monochromatic line $\{\mathbf{z}_0 + t\mathbf{w}_U : \ t = 1, 2, \dots k-1\} \subset \{1, \dots, k-1\}^M$ corresponding to some $U \subset \{1, \dots, k-1\}$ by the definition of M. Define $S \subset \{1, \dots, N\}$ to be the union of the subsets S_j, corresponding to the 1s in the vector $\mathbf{y}_j$, for each $j \in U$, yielding a monochromatic line $\{\mathbf{x}_0 + t\mathbf{y}_S : \ t = 1, 2, \dots k-1\} \subset (L_1, \dots, L_M) \subset \{1, \dots, k-1\}^N$. By the construction of our lines $L_1, \dots, L_M$, this implies the result.

We need to construct the lines $L_M, L_{M-1}, \dots, L_1$ which we do in this order. In fact for, $J = M, M-1, \dots, 1$ we assume that $L_i = \{\mathbf{x}_i + t_i\mathbf{y}_i : t_i = 1, 2, \dots, k\}$ is given for each $J < i \leq M$ with the property that $\kappa(x, \mathbf{x}_{J+1} + t_{J+1}\mathbf{y}_{J+1}, \dots, \mathbf{x}_M + t_M\mathbf{y}_M)$ is fixed as any t_j changes from $k-1$ to k, for any given $x \in \{1, 2, \dots, k\}^{N_1 + N_2 + \cdots + N_J}$ and $j, J < j \leq M$.

For each $x_J \in \{1, 2, \dots, k\}^{N_J}$ we define a colouring κ_{x_J} on $\{1, 2, \dots, k\}^{N_1 + N_2 + \cdots + N_{J-1}} \times L_{J+1} \times \cdots \times L_M$ by $\kappa_{x_J}(y, l_{J+1}, \dots, l_M) = \kappa(y, x_J, l_{J+1}, \dots, l_M)$. Given that the value of κ does not change as the t_j change from $k-1$ to k, the number of vectors $(y, l_{J+1}, \dots, l_M)$ with possibly independently chosen colourings is $\leq k^{N_1 + N_2 + \cdots + N_{J-1}} (k-1)^{M-J}$ and so the number of possibly different r-colourings is $\leq N_J$. There are $N_J + 1$ elements in $\{1, 2, \dots, k\}^{N_J}$ consisting of $(k-1)$s followed by ks and so, by the pigeonhole principle, two must have the same colouring. Let us suppose that these have exactly g and h $(k-1)$s,

respectively, where $g < h$. Then we define the line $L_J = \{\mathbf{x}_J + t_J\mathbf{y}_J : t_J = 1, 2, \dots, k\}$, by taking $S_J = \{g+1, g+2, \dots, h\}$ with $(x_J)_i = k-1$ for $1 \leq i \leq g$ and $(x_J)_i = k$ for $h+1 \leq i \leq k$. From this construction it is clear that L_J has the required properties and the result follows.

This proof was a breakthrough in that it was the first to give primitive recursive bounds on the van der Waerden numbers, $W(k, r)$. The reader should deduce bounds, themselves, from the above proof; the necessary information is in the first paragraph of the proof.

Define $n_k(N)$ to be the smallest integer n such that every subset of $\{1, \dots, N\}$ of size n contains a k-term arithmetic progression. If one can get a good enough bound on $n_k(N)$ then this would obviously imply good bounds on $W(k, r)$.

Discrete Fourier transforms, I

Let $n \in \mathbb{N}$ and $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$. The *(discrete) Fourier transform* $\hat{f}$ of f is defined by

$$\hat{f}(r) = \sum_{s=0}^{N-1} f(s) e\left(\frac{rs}{N}\right),$$

where $e(t) = \exp(2i\pi t)$. This has inverse

$$f(s) = \frac{1}{N} \sum_{r=0}^{N-1} \hat{f}(r) e\left(\frac{-rs}{N}\right)$$

(Verify). The reader should verify that

$$\sum_r \hat{f}(r)\overline{\hat{g}}(r) = N \sum_r f(r)\overline{g}(r)$$

which in the special case $f = g$ gives Parseval's identity: $\sum_r |\hat{f}(r)|^2 = N \sum_r |f(r)|^2$.

The *convolution $f * g$ of f and g* is defined by

$$(f * g)(r) = \sum_{t-u=r} f(t)\overline{g(u)},$$

and the reader should verify that $\widehat{(f * g)} = \hat{f}\overline{\hat{g}}$ as well as

$$N \sum_r |(f * g)(r)|^2 = \sum_r |\hat{f}(r)|^2 |\hat{g}(r)|^2.$$

Taking $g = f$ we obtain $\sum_r |\hat{f}(r)|^4 = N \sum_{a+b=c+d} f(a)f(b)\overline{f(c)f(d)}$.

In an abuse of notation we let $A(.)$ be the characteristic function of the set A, that is $A(n) = 1$ if $n \in A$, and $A(n) = 1$ otherwise. We have used $A(x)$ to mean $\#\{a \in A : 1 \le a \le x\}$ above – we can only hope the reader does not get confused but reckons which definition we are using depending on context. Note that $\hat{A}(m) = \sum_{a \in A} e(am/N)$. When considering sumsets, like $A + B$, we define $r_{A+B}(n) = \#\{a \in A, b \in B : a + b = n\}$. Discrete Fourier transforms fit naturally in this context, for example $(A * B)(n) = r_{A-B}(n)$ so that, as one can verify,

$$\frac{1}{N} \sum_n |\hat{A}(n)|^2 |\hat{B}(n)|^2 = \sum_n |(A * B)(n)|^2 = E(A, B)$$

(see (6.1)). One also has that $\hat{A}(m)\hat{B}(m) = \sum_n r_{A+B}(n)e(mn/N)$ and this can be inverted to give $r_{A+B}(n) = (1/N) \sum_m \hat{A}(m)\hat{B}(m)e(-mn/N)$. A particular case of this is $r_{A-A}(n) = (1/N) \sum_m |\hat{A}(m)|^2 e(-mn/N)$, as well as $r_{kA-kA}(n) = (1/N) \sum_m |\hat{A}(m)|^{2k} e(-mn/N)$. In fact $r_{A-A}(n) = (1/N) \sum_m |\hat{A}(m)|^2 \cos(2\pi mn/N)$ since $\hat{A}(-m) = \overline{\hat{A}(m)}$.

Discrete Fourier transforms have traditionally appeared in understanding how well sets are distributed: Let $(t)_N$ denote the least non-negative residue of $t \pmod N$. We say that a set A is *uniformly distributed* $\pmod N$ if $\#\{a \in A : \alpha N < (ma)_N \le \beta N\} \sim (\beta - \alpha)|A|$ for any $m \not\equiv 0 \pmod N$. This definition involves an asymptotic estimate "$\sim$", something we will see a lot more of. This "$\sim$" could be replaced by $\{1 + g(N)\}$ where $g(.)$ is some function for which $g(N) \to 0$ as $N \to \infty$.

This natural notion of uniform distribution fits in well with Fourier transforms:

The equidistribution theorem. *A is uniformly distributed* $\pmod N$ *if and only if* $\hat{A}(m) = o(|A|)$ *for all* $m \not\equiv 0 \pmod N$.

Our equidistribution theorem is the natural analogy to Weyl's famous equidistribution theorem for sequences of reals: Let $\{t\}$ be the fractional part of t (so, for example, $\{ma/N\} = (ma)_N/N$), and suppose that $a_1, a_2, \dots$ is a given (and ordered) sequence of real numbers. Then Weyl showed that the a_j are *uniformly distributed mod one*, that is $\#\{n \le N : \alpha < \{a_n\} \le \beta\} \sim (\alpha - \beta)N$ as $N \to \infty$, if and only if for each integer m, we have $\sum_{n \le N} e(ma_n) = o(N)$ as $N \to \infty$.

Show that if $a_1, a_2, \dots$ is uniformly distributed mod one, then so is $ka_1, ka_2, \dots$ for any integer $k \ge 1$.

The notion of uniform distribution surprisingly is related to the question: Do there exist solutions to $a + b = c$ with $a \in A, b \in B, c \in C$, three sets of residues $\pmod N$?

Proposition 3.1. *If A is uniformly distributed* $\pmod N$ *with $|A| \gg N$, and B, C are any other two sets mod N of size $\gg N$, then for any integers i, j, k coprime with N, and for any integer m we have that*

$$\#\{a \in A, b \in B, c \in C : ia + jb + kc \equiv m \pmod N\} \sim |A||B||C|/N.$$

Proof. We count the above set as

$$\sum_{\substack{a \in A, b \in B \\ c \in C}} \frac{1}{N} \sum_r e\left(\frac{r(ia + jb + kc - m)}{N}\right) = \frac{1}{N} \sum_r e\left(\frac{-rm}{N}\right) \hat{A}(ir)\hat{B}(jr)\hat{C}(kr).$$

The $r = 0$ term gives $|A||B||C|/N$. We regard the remaining terms as error terms, and bound them by their absolute values, giving a contribution

$$\le \frac{1}{N} \max_{s \ne 0} |\hat{A}(s)| \sum_r |\hat{B}(jr)||\hat{C}(kr)| \le \frac{1}{N} \max_{s \ne 0} |\hat{A}(s)| \left(\sum_t |\hat{B}(t)|^2\right)^{1/2} \left(\sum_u |\hat{C}(u)|^2\right)^{1/2}$$
$$= \frac{1}{N} \max_{s \ne 0} |\hat{A}(s)| (N|B|N|C|)^{1/2} = (|B||C|)^{1/2} \max_{s \ne 0} |\hat{A}(s)| \le N \max_{s \ne 0} |\hat{A}(s)|$$

using the Cauchy-Schwarz inequality. The result follows from the fact that $\hat{A}(m) = o(|A|)$ for all $m \not\equiv 0 \pmod N$ since this implies that $N \max_{s \ne 0} |\hat{A}(s)| = o(|A||B||C|/N)$.

We are interested in whether there are necessarily three elements of A in arithmetic progression; in fact we will examine solutions to $a + b = 2b'$ with $a \in A,\ b, b' \in B \subset A$ other than $a = b = b'$. In other words we want $\#\{a \in A,\ b, b' \in B : a + b \equiv 2b' \pmod N\} > |B|$. The above proof gives that $\#\{a \in A,\ b, b' \in B : a + b \equiv 2b' \pmod N\} \ge |A||B|^2/N - |B| \max_{s \ne 0} |\hat{A}(s)|$ which is $> |B|$ provided $\max_{s \ne 0} |\hat{A}(s)| < |A||B|/N - 1$.

Proof of the equidistribution theorem. Suppose that $\#\{a \in A :\ \alpha N < (ma)_N \le \beta N\} \sim (\beta - \alpha)|A|$ for any $m \not\equiv 0 \pmod N$, for any $0 \le \alpha < \beta \le 1$. In particular if $\alpha N <$

$(ma)_N \le \beta N$ then $e(ma/N) = e(\alpha) + O(|\beta - \alpha|)$, so subdividing $(0, N]$ into intervals $I_j := (jN/k, (j+1)N/k]$ for fixed large k, we find that

$$\hat{A}(m) = \sum_{j=0}^{k-1} \sum_{\substack{a\in A\\ (ma)_N\in I_j}} e(ma/N) = \sum_{j=0}^{k-1} \{1+o(1)\}(|A|/k)(e(jN/k)+O(1/k)) \ll |A|/k.$$

Letting $k \to \infty$ we have that $\hat{A}(m) = o(|A|)$.

On the other hand for $J = [\delta N]$

$$\sum_{\substack{a\in A\\ 1\le (ma)_N\le J}} 1 = \sum_{j=1}^{J} \sum_{a\in A} \frac{1}{N} \sum_r e\left(r\left(\frac{ma-j}{N}\right)\right) = \frac{J}{N}|A| + \frac{1}{N}\sum_{r\neq 0} \hat{A}(rm) \sum_{j=1}^{J} e\left(\frac{-rj}{N}\right).$$

If r runs through the non-zero integers in $(-N/2, N/2]$ then $|\sum_{j=1}^{J} e\left(\frac{-rj}{N}\right)| \ll N/|r|$. Thus the second term here is

$$\begin{aligned} &\ll \sum_{r\neq 0} \frac{|\hat{A}(rm)|}{r} \le \sum_{0\le |r|\le R} \frac{|\hat{A}(rm)|}{r} + \sum_{R<|r|\le N/2} \frac{|\hat{A}(rm)|}{r} \\ &\le (\log R) \max_{s\neq 0} |\hat{A}(s)| + \left(\sum_r |\hat{A}(rm)|^2\right)^{1/2} \left(\sum_{R<|r|} 1/r^2\right)^{1/2} \\ &\le (\log R) \max_{s\neq 0} |\hat{A}(s)| + (|A|N/R)^{1/2} = o(N) \end{aligned}$$

if we let $R \to \infty$ slowly enough. The result follows.

Try to develop an analogous proof of Weyl's theorem; or a proof of Weyl's theorem as a corollary to our equidistribution theorem.

In what follows we will be interested in determining how big $\#\{a \in A : \ \alpha N < (ma)_N \le \beta N\}$ can get when $|\hat{A}(r)| > cN$.

We have seen direct connections between how well a set is distributed and the size of its Fourier transforms. In the context of set addition we are interested in when $A + B$ is small, and/or perhaps when $r_{A+B}(n)$ is large for some n. We now see that $r_{A-A}(n)$ is very large if and only if the weight of the Fourier transform is concentrated on the $\hat{A}(m)$ with $(mn)_N$ small:

Proposition 3.2a. *Let $\eta > 0$ be small. Suppose that $A \subset \mathbb{Z}/N\mathbb{Z}$. If $r_{A-A}(n) > (1-\eta)|A|$ then*

$$\sum_{m:|(mn)_N/N|\le \eta^{1/3}} |\hat{A}(m)|^2 \ge (1 - O(\eta^{1/3})) \sum_m |\hat{A}(m)|^2.$$

On the other hand if

$$\sum_{m:|(mn)_N/N|\le \epsilon} |\hat{A}(m)|^2 \ge (1-\delta) \sum_m |\hat{A}(m)|^2$$

then $r_{A-A}(n) \geq (1-\delta-O(\epsilon^2))|A|$.

Proof. We remark that $\sum_m |\hat{A}(m)|^2 = N|A|$. Since $\cos t$ is decreasing for $0 \leq |t| \leq \pi$ we know that $\cos(2\pi mn/N) < \cos(2\pi\theta)$ if $|(mn)_N/N| > \theta$ and so, using the formula above, $(1-\eta)|A|N < Nr_{A-A}(n)$ which is

$$= \sum_m |\hat{A}(m)|^2 \cos(2\pi mn/N) \leq \sum_{m:|(mn)_N/N|>\theta} |\hat{A}(m)|^2 \cos(2\pi\theta) + \sum_{m:|(mn)_N/N|\leq\theta} |\hat{A}(m)|^2$$
$$= |A|N - (1-\cos(2\pi\theta)) \sum_{m:|(mn)_N/N|>\theta} |\hat{A}(m)|^2.$$

Now selecting $\theta = \eta^{1/3}$, we deduce that $\sum_{m:|(mn)_N/N|>\eta^{1/3}} |\hat{A}(m)|^2 \ll \eta^{1/3}N|A|$.

In the other direction

$$Nr_{A-A}(n) = \sum_m |\hat{A}(m)|^2 \cos(2\pi mn/N) \geq \sum_{m:|(mn)_N/N|\leq\epsilon} |\hat{A}(m)|^2 \cos(2\pi\epsilon)$$
$$\geq \cos(2\pi\epsilon)(1-\delta) \sum_m |\hat{A}(m)|^2 = \cos(2\pi\epsilon)(1-\delta)|A|N.$$

As a counterpart to this theorem we have the uncertainty principle, which tells us that a function's support and the support of its Fourier transform cannot both be small. More precisely we now show that if A has no elements in a long segment then $\hat{A}$ is concentrated near to 0.

Proposition 3.2b. *Suppose that $A \subset \mathbb{Z}/N\mathbb{Z}$ has no elements in the interval $(x-L, x+L)$. Then there exists $m, 0 < m < (N/L)^2$ such that $|\hat{A}(m)| \geq (L/2N)|A|$.*

Proof. We can assume wlog that $x = 0$ since $\hat{A-x}(m) = e(mx/N)\hat{A}(m)$. Let I be the interval $[0, L)$ and note that $(I-I) \cap A = \emptyset$, so $\sum_r |\hat{I}(r)|^2 \hat{A}(r) = 0$. Therefore

$$L^2|A| = |\hat{I}(0)|^2\hat{A}(0) \leq \sum_{r\neq 0} |\hat{I}(r)|^2|\hat{A}(r)|$$
$$\leq \max_{0\leq|r|\leq R} |\hat{A}(r)| \sum_r |\hat{I}(r)|^2 + |A| \sum_{R<|r|\leq N/2} |\hat{I}(r)|^2$$
$$\leq NL \max_{0\leq|r|\leq R} |\hat{A}(r)| + |A|N^2/2R$$

since $\hat{I}(r) \leq 1/|\sin(\pi r/N)| \leq N/2|r|$ for $|r| \leq N/2$. Taking $R = (N/L)^2$ the result follows.

The equidistribution theorem gives that if $|\hat{A}(m)| > c|A|$ then A is not uniformly distributed mod N. We seek a more explicit result than this:

Proposition 3.3. *Suppose $A \subset \{1, \dots, N\}$. For any $m \neq 0$ there exists $\ell > |\hat{A}(m)|/6\pi$ and a value x such that $\#\{a \in A : x < (am)_N \leq x+\ell\} \geq (1+|\hat{A}(m)|/4|A|)\ (|A|/N)\ \ell$. If $(m, N) = 1$ and $|\hat{A}(m)| > CN/\log N$ for a large constant $C > 0$ then there exist integers*

b and r and length $J \gg \sqrt{N}/\log N$ *such that* $\#\{a \in A : \ a = b + jr, \ 0 \le j < J\} \ge (1 + |\hat{A}(m)|/4|A|)\ (|A|/N)\ J$.

Proof. Define $\delta = |A|/N$. Let

$$\Delta(n) := A(n) - \delta = \begin{cases} 1-\delta & \text{if } n \in A \\ -\delta & \text{otherwise} \end{cases}$$

so that $\hat{\Delta}(r) - \hat{A}(r) = -\delta \sum_n e(-rn/N) = 0$ if $r \ne 0$. Fix J large and let $I_j := \{n : (j-1)N/J < (mn)_N < jN/J\}$ for $j = 1, 2, \dots, J$. We observe that

$$\left| \sum_{n \in I_j} \Delta(n) e(mn/N) - e(j/J) \sum_{n \in I_j} \Delta(n) \right| \le \sum_{n \in I_j} |\Delta(n)||1 - e(1/J)| \le 2|I_J| \sin(\pi/J),$$

so that

$$\left| \hat{\Delta}(m) - \sum_{j=1}^{J} e(jN/J) \sum_{n \in I_j} \Delta(n) \right| \le 2N \sin(\pi/J);$$

and, of course, $\sum_{j=1}^{J} \sum_{n \in I_j} \Delta(n) = 0$. An easy consequence is that

$$\begin{aligned} |\hat{A}(m)| = |\hat{\Delta}(m)| &\le \sum_{j=1}^{J} \left\{ \sum_{n \in I_j} \Delta(n) + \left| \sum_{n \in I_j} \Delta(n) \right| \right\} + 2N \sin(\pi/J) \\ &\le 2J \max_j \sum_{n \in I_j} \Delta(n) + 2N \sin(\pi/J). \end{aligned}$$

Taking $J = [5\pi N/|\hat{A}(m)|]$ we deduce that $\max_j \sum_{n \in I_j} \Delta(n) \ge |\hat{A}(m)|/4J$, and the first part of the result follows.

There exist integers $r \ne 0, s$ with $0 \le |r|, s < \sqrt{N}$ such that $mr \equiv s \pmod N$ (hint: consider the values $i + jm \pmod N$, $0 \le i, j \le \sqrt{N}$). Select $1 \le a_i \le N$ so that $(ma_i)_N = x + i$ for $i = 1, 2, \dots, s$, so that $m(a_i + jr) \equiv x + i + js \pmod N$. Therefore if $0 \le x < x + ks < N$ then

$$\#\{a \in A : x < (am)_N \le x + ks\} = \bigcup_{i=1}^{s} S_i \text{ where } S_i := \{a \in A : \ a = (a_i + jr)_N, \ 0 \le j \le k-1\};$$

and so, selecting $k = [N/Js]$, we deduce from the above that there exists i for which $|S_i| \ge \delta k(1 + \eta|\hat{A}(m)|/|A|)$ for some fixed $\eta > 1/4$. We may assume $r > 0$ for, if not, rewrite S_i as $\{a \in A : \ a = (a_i' + j|r|)_N, \ 0 \le j \le k-1\}$ where $a_i' \equiv a_i + (k-1)r \pmod N$ with $1 \le a_i' \le N$.

Now define $j_0 = 0 < j_1 < \dots < j_w = k$ with j_ℓ chosen minimal so that $[(a_i + j_\ell r)/N] = \ell$ for $1 \le \ell \le w - 1 = [(a_i + (k-1)r)/N]$. Note that for $b_\ell = (a_i + j_\ell r)_N$ we have

$$\{a \in A : \ a = (a_i + jr)_N, \ j_\ell \le j < j_{\ell+1}\} = \{a \in A : \ a = b_\ell + jr, \ 0 \le j < j_{\ell+1} - j_\ell\},$$

and that $j_{\ell+1} - j_\ell = N/r + O(1)$ for $1 \le \ell \le w-2$. If $w > 1$ then let $u = 0$ unless $j_1 < \min\{N/r, k\}/\log N$ in which case we let $u = 1$, and let $v = w$ unless $j_w - j_{w-1} < \min\{N/r, k\}/\log N$ in which case we let $v = w-1$. Therefore

$$\sum_{\ell=u}^{v-1} \#\{a \in A : \ a = (a_i + jr)_N, \ j_\ell \le j < j_{\ell+1}\} \ge \delta k \left(1 + \eta \frac{|\hat{A}(m)|}{|A|}\right) - 2\frac{\min\{N/r, k\}}{\log N}$$
$$\ge \delta(j_v - j_u)\left(1 + \frac{|\hat{A}(m)|}{4|A|}\right).$$

Therefore there exists an integer b and $z \ge \min\{N/r, k\}/\log N \gg \sqrt{N}/\log N$ such that $\#\{a \in A : \ a = b + jr, \ 0 \le j < z\} \ge \delta z(1 + |\hat{A}(m)|/4|A|)$

Lemma 3.3b. *Given an arithmetic progression P in $\mathbb{F}_p$ of length m, there exist arithmetic progressions $P_1, P_2, \dots, P_k \subset [1, p-1]$, each of length ℓ where $\ell \ll \sqrt{m}$, such that $P_1, P_2, \dots, P_k \pmod p$ is a partition of P less $O(\ell\sqrt{m})$ elements of $\mathbb{F}_p$.*

Proof. Suppose that $P = \{a + id : \ 1 \le i \le m\}$. By Lemma * we know that there exist integers $|r| \le p/\sqrt{m}$ and $1 \le s \le \sqrt{m}$ such that $d \equiv r/s \pmod p$. Fix h, $1 \le h \le s$. If $i = h + js$ then $a + id \equiv a + hd + jr$, so the $Q_h := \{a_h + jr : \ 0 \le j \le (m-h)/s\}$, where $a_h \equiv a + hd \pmod p$, partition P.

Next we partition the Q_h into subprogressions of length ℓ, containing consecutive elements of Q_h, and that lie between consecutive multiples of p. Between two consecutive multiples of p we can include all but at most $\ell - 1$ elements of Q_h in our subprogressions; and so in total we include all but $\ll \ell(mr/sp + 1)$ elements of Q_h in our subprogressions, and all but $\ll \ell s(mr/sp + 1) \ll \ell\sqrt{m}$ elements of P in our subprogressions. The result follows by letting the P_i by the reductions of these subprogressions.

3b. Roth's Theorem.

Roth [11] showed that any set of integers of positive upper density contains arithmetic progressions of length three. This was generalized by Szemerédi [17] who showed that any set of integers of positive upper density contains arbitrarily long arithmetic progressions. His proof used ingenious combinatorial techniques, and a later proof given by Fürstenburg [6] surprisingly used methods from ergodic theory.

Szemerédi actually proved more than this: Let $n_k(N)$ denote the smallest integer such that any subset of $n_k(N)$ integers from $\{1,\dots,N\}$ contains an arithmetic progression of length k. Szemerédi established that $n_k(N) = o(N)$ for each k, proving a conjecture of Erdős and Turán [4]. His proof used van der Waerden's Theorem and Szemerédi's Regularity Lemma, and so the upper bound on the order of $n_k(N)$ obtained can be no better than the bounds given by these theorems. However Roth's remarkable analytic proof that $n_3(N) = o(N)$ can be used to get an explicit upper bound, namely $n_3(N) \le cN/\log\log N$ for some constant $c > 0$, and offers the possibility of generalization.

Roth's Theorem. *There exists a constant $c > 0$ such that any set of $cN/\log\log N$ integers from $\{1,\dots,N\}$ contains an arithmetic progression of length three.*

Proof. Suppose that $A \subset \{1,\dots,N\}$ does not contain an arithmetic progression of length three. We will show that there exists a subset A' of A which is a subset of an arithmetic progression, and denser than A. Then we create a Freiman homomorphism of order 2 between $A_1 \subset \{1,\dots,N_1\}$ and A' in each case, so that A_1 does not contain an arithmetic progression of length three. In fact we will show that $\sqrt{N}/\log N \ll N_1 \le N$ and if $|A| = \delta N$ then $|A_1| \ge (1+\delta/20)\ \delta\ N_1$. Iterating this enough times we create a set A^* of density $> 2/3$ in the integers up to some point, so that it contains three consecutive integers. Do this explicitly and deduce the result.

To prove our claim, fix $1/5 > \eta > 0$ and let P be the smallest prime $> N$: by the prime number theorem $P = N + O(N/\log^2 N)$. If $\#\{a \in A:\ 0 < a \le P/3\} \ge (1+\eta)|A|/3$ then let $A_1 = A' = \{a \in A:\ 0 < a \le P/3\}$, or if $\#\{a \in A:\ 2P/3 < a \le P\} \ge (1+\eta)|A|/3$ then let $A' = \{a \in A:\ 2P/3 < a < P\} = P - A_1$. Otherwise we must have $|B| \ge (1-2\eta)|A|/3$ where $B = \{a \in A:\ P/3 < a \le 2P/3\}$. Notice that if $b, c \in B$ then $0 < 2c - b < N$. In this case let $i = j = 1, k = -2$ and $C = B$ in the remarks following Proposition 3.1, so that there exists $m \not\equiv 0 \pmod P$ such that $|\hat{A}(m)| \ge |A||B|/P - 1$, Thus, by Proposition 3.3, if we take $A_1 = \{j : 0 \le j < J\}$ and $A' = \{a \in A:\ a = b + jr,\ j \in A_1\}$ then $|A_1| = |A'| \ge (1 + |\hat{A}(m)|/4|A|)\ (|A|/N)\ J$ where $J \gg \sqrt{N}/\log N$.

Heath-Brown [9] and Szemerédi [18] have recently improved this to $n_3(N) \ll N/(\log N)^c$, for some constant $c > 0$. It is unclear what is the correct order of $n_3(N)$. There is a beautiful lower bound due to Behrend:

Behrend's Theorem. *There exists a set of* $\geq N/\exp(c\sqrt{\log N})$ *integers from* $\{1,\dots,N\}$ *which does not contain an arithmetic progression of length three.*

Proof. The set $\{(x_0,\dots,x_{n-1}) \in \mathbb{Z}^n : \ 0 \leq x_i \leq d-1\}$ contains $(d-1)^n$ elements. Moreover if $\mathbf{x}$ belongs to this set then $|\mathbf{x}|^2$ is a positive integer $\leq n(d-1)^2$. Thus there exists an integer k such that the set $S = \{\mathbf{x} : \ |\mathbf{x}|^2 = k, \ 0 \leq x_i \leq d-1\}$ has $\geq d^{n-2}/n$ elements.

Let $A = \{x_0+x_1(2d-1)+x_2(2d-1)^2+\cdots+x_{n-1}(2d-1)^{n-1} : \ \mathbf{x} \in S\}$. If $a_1+a_2 = 2a_3$ where each $a_i = a_i(\mathbf{x}_i) = \sum_j x_{i,j}(2d-1)^j$ then prove by induction that $x_{1,j}+x_{2,j} = 2x_{3,j}$ for each $j \geq 0$ (hint: consider $a_1+a_2 \equiv 2a_3 \pmod{2d-1}$, etc.). Therefore $\mathbf{x}_1+\mathbf{x}_2 = 2\mathbf{x}_3$, which implies that these three points of S lie on the same line: however this is impossible since a line intersects the surface of a sphere in at most two points. Thus A contains no three term arithmetic progressions.

Now every element of A is $\leq (d-1)\sum_{j=0}^{n-1}(2d-1)^j < N := (2d-1)^n/2$ and $|A| = |S| \geq d^{n-2}/n \geq N/(2^n d^2)$. Choosing n to be an even integer and $d = 2^{n/2-1}$ we obtain $N < 2^{n^2-1}$ and $|A| \geq 4N/2^{2n}$ which implies the result for arbitrarily large N. Prove the result for all sufficiently large N using this construction.

3c. How often can $|\hat{A}(m)|$ be large?. For fixed $\rho > 0$ let $R := \{r \pmod N : \ |\hat{A}(r)| > \rho|A|\}$. Then

$$|A|N = \sum_m |\hat{A}(m)|^2 \geq \sum_{m\in R} \rho^2|A|^2,$$

so that $|R| \leq \rho^{-2}\alpha^{-1}$, where $\alpha := |A|/N$; that is, it is bounded as a function of ρ and α. One can determine some structure in the set R:

Theorem 3.4. *Suppose that* $A \subset \mathbb{Z}/N\mathbb{Z}$. *The set* $R := \{r \pmod N : \ |\hat{A}(r)| > \rho|A|\}$ *is contained in a cube of dimension* $\leq 2\rho^{-2}\log(N/|A|)$.

Remember that a cube of dimension k is a set $\overline{\Lambda}$ of the form $\{\epsilon_1\lambda_1+\cdots+\epsilon_k\lambda_k :$ each $\epsilon_i \in \{-1,0,1\}\}$, for given $\Lambda = \{\lambda_1,\lambda_2,\dots,\lambda_k\}$. We say that Λ is *dissociated* if $\epsilon_1\lambda_1+\cdots+\epsilon_k\lambda_k = 0$ with each $\epsilon_i \in \{-1,0,1\}$ only for $\epsilon_1 = \cdots = \epsilon_k = 0$.

The proof of Theorem 3.4 involves some seemingly ad hoc analysis, which we state in the next lemma. For now write the "general" finite trigonometric polynomial as $f(x) = \sum_j c_j\cos(2\pi(\lambda_j x/N+\beta_j))$ where each $c_j \in \mathbb{R}$ and $0 \leq \beta_j < 1$. Show:

Lemma 3.5.
(i) We have $e^{ty} \leq \cosh(t)+y\sinh(t)$ *for all* $t \in \mathbb{R}$ *and* $|y| \leq 1$.
(ii) $\cosh(u) \leq e^{u^2/2}$ *for any* $u \in \mathbb{R}$.
(iii) With $f(x)$ *as above,* $\sum_{x \pmod N} f(x)^2 = (N/2)\sum_j c_j^2$.

We deduce

Proposition 3.6. *If* Λ *is dissociated then*

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

Proof. Using (i) (of Lemma 3.5) the left side above is

$$\le \frac{1}{N}\sum_x \prod_j (\cosh(tc_j) + \cos(2\pi(\lambda_j x/N + \beta_j))\sinh(tc_j)).$$

Writing each $\cos\theta$ as $(e^{i\theta}+e^{-i\theta})/2$ the jth term in the product takes the form $\sum_{\epsilon_j\in\{-1,0,1\}} c(j,\epsilon_j)\exp(\epsilon_j\lambda_j x/N)$ for certain constants $c(j,\epsilon_j)$. Multiplying this out over the j, then summing over $x \pmod N$, we see that the only terms that can have a non-zero sum are those for which $\sum_j \epsilon_j\lambda_j = 0$: and thus $\epsilon_1 = \cdots = \epsilon_k = 0$ as Λ is dissociated. This term is easily obtained from the above product as

$$\frac{1}{N}\sum_x \prod_j \cosh(tc_j) = \prod_j \cosh(tc_j) \le \exp\left(\frac{t^2}{2}\sum_j c_j^2\right) = \exp\left(\frac{t^2}{N}\sum_x f(x)^2\right)$$

using Lemma 3.5 (ii) and (iii).

With this preparation we can prove

Proposition 3.7. *Suppose that $A \subset \mathbb{Z}/N\mathbb{Z}$. Any dissociated subset of $R := \{r \pmod N : |\hat{A}(r)| > \rho|A|\}$ has size $\le 2\rho^{-2}\log(N/|A|)$.*

Deduction of Theorem 3.4. Let Λ be a maximal dissociated subset of R. Then any $r \in R$ can be written in the form $r = \sum_i \epsilon_i\lambda_i$ so that $R \subset \Lambda$.

Proof of Proposition 3.7. If $\Lambda = \{\lambda_1, \lambda_2, \dots, \lambda_k\}$ is a dissociated subset of R, let $f(x) = \mathrm{Re}\left(\sum_j \hat{A}(\lambda_j)e(\lambda_j x/N)\right)$, which we can rewrite as $f(x) = \sum_j c_j\cos(2\pi(\lambda_j x/N + \beta_j))$ where $c_j = |\hat{A}(\lambda_j)|$ and β_j is chosen appropriately. Note also that $\hat{f}(r) = N\hat{A}(r)/2$ if $r \in \Lambda \cup -\Lambda$, and $\hat{f}(r) = 0$ otherwise, so that

$$\sum_x f(x)A(x) = \frac{1}{N}\sum_r \hat{f}(r)\overline{\hat{A}(r)} = \frac{2}{N^2}\sum_r |\hat{f}(r)|^2 = \frac{2}{N}\sum_x |f(x)|^2.$$

Therefore, for any t we have, using the arithmetic-geometric mean inequality and then Proposition 3.6,

$$\exp\left(\frac{2t}{N|A|}\sum_x |f(x)|^2\right) = \exp\left(\frac{t}{|A|}\sum_{x\in A} f(x)\right)$$
$$\le \frac{1}{|A|}\sum_{x\in A}\exp(tf(x)) \le \frac{N}{|A|}\exp\left(\frac{t^2}{N}\sum_x f(x)^2\right).$$

Taking $t = 1/|A|$ we deduce that $\sum_x f(x)^2 \le N|A|^2\log(N/|A|)$. On the other hand, by Lemma 3.5(iii), $(2/N)\sum_x f(x)^2 = \sum_j c_j^2 = \sum_j |\hat{A}(\lambda_j)|^2 \ge |\Lambda|(\rho|A|)^2$, and the result follows from combining these last two inequalities.

Exponential sums, I

Suppose that $\alpha, \beta \in \mathbb{R}$. As each term has absolute value ≤ 1, and by summing the geometric series, we obtain

$$\left|\sum_{n=0}^{N-1} e(\alpha n+\beta)\right| \le \min\{N, 1/2\|\alpha\|\}. \tag{4.1}$$

It is also useful to note that for any given $y_1, y_2, \dots, y_k$ we have

$$\sum_i \min\{N, 1/\|y_i\|\} \ll N + \frac{\log(2N)}{\min_{i\neq j}\|y_i - y_j\|}. \tag{4.2}$$

Now suppose that $|\alpha - a/q| \le 1/q^2$ where $(a,q)=1$. We use this to show that

$$\sum_{n=0}^{N} \min\left\{Q, \frac{1}{\|\alpha n+\beta\|}\right\} \ll (Q + q\log 2Q)(1+N/q). \tag{4.3}$$

The implicit constant here does not depend on α. First we prove it for $N < q/2$, since if $0 \le m < n \le N$ then $\|(\alpha n+\beta) - (\alpha m+\beta) = \|\alpha(m-n)\| \ge \|(m-n)a/q\| - |m-n|/q^2 \ge 1/q - (q/2)/q^2 = 1/(2q)$ and we apply (4.2). The result follows for general but cutting the sum up into intervals of length $< q/2$.

All this preparation leads to a remarkable lemma:

Lemma 4.1. *For any $\alpha \in \mathbb{R}$ and any quadratic polynomial $f(x) \in \mathbb{R}[x]$ with leading coefficient α we have*

$$\left|\sum_{n=0}^{N-1} e(f(n))\right| \ll \frac{N}{q^{1/2}} + ((q+N)\log 2N)^{1/2}$$

where $|\alpha - a/q| \le 1/q^2$ with $(a,q)=1$.

Proof. If $f(x) = \alpha x^2 + bx + c$ then $f(x+h) - f(x) = h(2\alpha x + b + \alpha h)$ so that, writing $m = n+h$ we obtain

$$\begin{aligned}\left|\sum_{n=0}^{N-1} e(f(n))\right|^2 &= \sum_{m,n=0}^{N-1} e(f(m)-f(n)) \\ &= \sum_{h=-(N-1)}^{N-1} e(\alpha h^2 + bh) \sum_{n=\max\{0,-h\}}^{\min\{N-1, N-1-h\}} e(2h\alpha n) \\ &\le \sum_{h=-(N-1)}^{N-1} \min\{N, 1/\|2\alpha h\|\}\end{aligned}$$

using (4.1), and the result follows from (4.3).

A little further down we will generalize Lemma 4.1 to arbitrary degree polynomials, but the proof is quite technical, and to get the general idea it is easier to prove the analogous result in finite fields:

Lemma 4.1*. *For any polynomial $f(x) \in \mathbb{F}_p[x]$ of degree k with $p > k \geq 1$, we have*

$$\left|\sum_{n=0}^{p-1} e\left(\frac{f(n)}{p}\right)\right| \leq 2p^{1-1/2^{k-1}}.$$

Proof. We proceed by induction on degree $k \geq 1$. If f has degree 1, then the sum is over a geometric progression and the value is 0. For $k = 2$ we have

$$\left|\sum_{n=0}^{p-1} e\left(\frac{an^2+bn+c}{p}\right)\right|^2 = \sum_{h=0}^{p-1}\sum_{n=0}^{p-1} e\left(\frac{a(h^2+2hn)+bh}{p}\right)$$
$$= p + \sum_{h=1}^{p-1} e\left(\frac{ah^2+bh}{p}\right)\sum_{n=0}^{p-1} e\left(\frac{2ahn}{p}\right) = p$$

expanding the sum with variables $n + h$ and n. Hence the sum has size exactly $\sqrt{p}$; in fact it is known as a *Gauss sum*. For larger k we have note that if $f(n) = an^k + \dots$ then $f_h(n) := f(n+h) - f(n) = ahkn^{k-1} + \dots$ where the "$\dots$" signify a polynomial of lower degree in n. Note that $p|ahk$ if and only if $p|h$; and that $f_0(n) = 0$. Hence modifying the above argument we obtain

$$\left|\sum_{n=0}^{p-1} e\left(\frac{f(n)}{p}\right)\right|^2 = \sum_{h=0}^{p-1}\sum_{n=0}^{p-1} e\left(\frac{f_h(n)}{p}\right) \leq p + \sum_{h=1}^{p-1} 2p^{1-1/2^{k-2}} \leq 4p^{2-1/2^{k-2}},$$

and the result follows.

The generalization of Lemma 4.1 proceeds along similar lines. However because we are now not dealing with "complete" exponential sums (that is a sum over all the values in the group) we do not get the same convenient cancelations, so have to work a little harder:

Lemma 4.1$^+$. *For any $\alpha \in \mathbb{R}$ and any polynomial $f(x) \in \mathbb{R}[x]$ of degree k with leading coefficient α we have*

$$\left|\sum_{n=0}^{N-1} e(f(n))\right| \ll \frac{N}{q^{1/2^k}}\ (\log N)^{5/8}$$

where $|\alpha - a/q| \leq 1/q^2$ with $(a,q) = 1$, and $q \leq N$.

Proof. We prove, by induction on $k \geq 2$, that

$$\left|\frac{1}{2N}\sum_{n=0}^{M-1} e(f(n))\right|^{2^{k-1}} \leq \frac{1}{(2N)^{k-1}} \sum_{-N<h_1,h_2,\dots,h_{k-1}<N} \min\left\{1, \frac{1}{N\|k!\alpha h_1 \dots h_{k-1}\|}\right\}.$$

Note that if we multiply the right side through by N^k we get an increasing function of N, and that $2^{k-1} \geq k$ for all $k \geq 1$. The inequality appears in the proof of Lemma 4.1 for $k = 2$.

Now if f has degree k then we square, and note that $f(n+h)-f(n) = k\alpha h n^{k-1}+\ldots = g_h(n)$ say, to obtain the upper bound

$$\left|\frac{1}{2N}\sum_{n=0}^{M-1} e(f(n))\right|^2 \leq \frac{1}{2N}\sum_{-N<h<N}\left|\frac{1}{2N}\sum_{n=\max\{0,-h\}}^{\min\{N-1,N-1-h\}} e(g_h(n))\right|.$$

We Cauchy this $k-2$ times and then apply the induction hypothesis to get the claim.

Note that the summand does not change if we replace h by $-h$. Moreover the contribution from $h_i = 0$ is $\leq kN^{k-2}/(2N)^{k-1} \leq 1/N$. So we may rewrite our inequality as

$$\left|\frac{1}{2N}\sum_{n=0}^{M-1} e(f(n))\right|^{2^{k-1}} \leq \frac{1}{N^{k-1}}\sum_{1\leq h_1,h_2,\ldots,h_{k-1}<N} \min\left\{1, \frac{1}{N\|k!\alpha h_1\ldots h_{k-1}\|}\right\} + \frac{1}{N}.$$

Let $\tau_k(n)$ be the number of ways of writing $n = h_1 h_2 \ldots h_k$ with each $1 \leq h_i \leq N$, so our big sum is

$$\frac{1}{N^{k-1}}\sum_{n\leq N^{k-1}} \tau_{k-1}(n)\min\left\{1, \frac{1}{N\|k!\alpha n\|}\right\}$$

We now Cauchy this, so the square is

$$\leq \frac{1}{N^{k-1}}\sum_{n\leq N^{k-1}} \tau_{k-1}(n)^2 \cdot \frac{1}{N^{k-1}}\sum_{n\leq N^{k-1}} \min\left\{1, \frac{1}{N\|\alpha k!n\|}\right\}^2.$$

Since the summand in the second sum is always ≤ 1, that sum is

$$\leq \frac{1}{N^{k-1}}\sum_{m\leq k!N^{k-1}} \min\left\{1, \frac{1}{N\|\alpha m\|}\right\} \ll (1+\frac{q\log 2N}{N})(\frac{1}{N^{k-1}}+\frac{k!}{q})$$

by (4.3). Moreover

$$\frac{1}{N^k}\sum_{n\leq N^k}\tau_k(n)^2 \leq \sum_{n\leq N^k}\frac{\tau_k(n)^2}{n} \leq \prod_{p\leq N}\left(1+\frac{\tau_k(p)^2}{p}+\frac{\tau_k(p^2)^2}{p^2}+\ldots\right).$$

Since $\tau_k(p^e)$ depends only on k and e, the Euler product can be bounded using just the first term. Now $\tau_k(p) = k$, and so the above is

$$\ll_k \left(1+\frac{1}{p}\right)^{k^2} \ll (\log N)^{k^2}.$$

Collecting up the estimates above we obtain

$$\left|\sum_{n=0}^{N-1} e(f(n))\right| \ll \frac{N}{q^{1/2^k}}\ (\log N)^{5/8}\left(\left(1+\frac{q}{N}\right)\left(1+\frac{q}{N^{k-1}}\right)\right)^{1/2^k} + N^{1-1/2^{k-1}},$$

and the result follows.

Theorem 4.2. *Fix $k \ge 2$. For any $\alpha \in \mathbb{R}$ and any M, there exists $m \le M$ such that $\|\alpha m^k\| \ll (\log M)/M^{1/K(k)}$, where $K(2) = 5$ and $K(k) := (k-1)2^k + 2k - 1$ for $k \ge 3$.*

Proof. Select prime $N > M^{k+1}$, and b with $|\alpha - b/N| \le 1/(2N)$. Let $A = \{bm^k \pmod N : 1 \le m \le M\} \subset \mathbb{Z}/N\mathbb{Z}$ and let $L = N(\log M)^{5/8}/M^{1/K}$. We see that A contains exactly M distinct elements. If A contains an element in $(-L, L)$ then $\|\alpha m^k\| \le \|bm^k/N\| + M^k/2N \le 2L/N$, and the result follows. Otherwise there exists $r, 0 < r < (N/L)^2$ such that $|\hat{A}(r)| \ge (L/2N)|A| = LM/2N$ by Proposition 3.2b. Select $q \le M$ for which $|\alpha r - a/q| < 1/qM$ for some $(a, q) = 1$, so that

$$|\hat{A}(r)| = \left|\sum_{m \le M} e\left(\frac{brm^k}{N}\right)\right| \le \left|\sum_{m \le M} e\left(r\alpha m^k\right)\right| + \left(\sum_{m \le M} \frac{rm^k}{N}\right)$$
$$\ll \frac{M}{q^{1/2^k}} \cdot (\log M)^{5/8} + \frac{NM^{k+1}}{L^2},$$

by Lemma 4.1^+ (with exponent $1/2^2$ replaced by $1/2$ when $k = 2$ by Lemma 4.1). Combining the last two inequalities gives that $q \ll M^{2^k/K}$ (and $q \ll M^{2/5}$ when $k = 2$), and so

$$\|\alpha(qr)^k\| \le q^k r^{k-1}|r\alpha - a/q| \ll \frac{(qr)^{k-1}}{M} \ll \frac{1}{M^{1/K}(\log M)^{5(k-1)/4}} \ll \frac{L}{N}.$$

The Geometry of Numbers

A *lattice* in $\mathbb{R}^n$ is a subgroup generated by n linearly independent vectors, with basis $x_1, x_2, \dots, x_n$ say. The *fundamental parallellopiped* of Λ with respect to $x_1, x_2, \dots, x_n$ is the set $P = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : 0 \le a_i < 1\}$. The sets $x + P$, $x \in \Lambda$ are disjoint and their union is $\mathbb{R}^n$. The *determinant* $det(\Lambda)$ of Λ is the volume of P; in fact $det(\Lambda) = |det(A)|$, where $A = (x_1, x_2, \dots, x_n)$ and the x_i are column vectors with respect to the canonical basis for $\mathbb{R}^n$. A *convex body* K is a bounded convex open subset of $\mathbb{R}^n$. Show that $vol(K) = \lim_{t\to\infty} |\Lambda \cap tK| det(\Lambda)/t^n$. A key result is:

Blichfeldt's Lemma. *Let $K \subset \mathbb{R}^n$ be a measurable set, Λ a lattice and suppose $vol(K) > det(\Lambda)$. Then $K - K$ contains a non-zero lattice point.*

The proof is a challenge problem. This immediately gives

Minkowski's First Theorem. *If K is a centrally symmetric convex body with $vol(K) > 2^n det(\Lambda)$ then K contains a non-zero point of Λ.*

Proof. As K is convex and centrally symmetric, $K = \frac{1}{2}K - \frac{1}{2}K$. However, $vol(\frac{1}{2}K) > det(\Lambda)$, so the result follows by Blichfeldt's Lemma.

For a centrally symmetric convex body K define λ_k to be the infimum of those λ for which λK contains k linearly independent vectors of Λ. We call $\lambda_1, \lambda_2, \dots, \lambda_n$ the successive minima of K with respect to Λ. Let $b_1, b_2, \dots, b_n \in \mathbb{R}^n$ be linearly independent vectors with $b_k \in \lambda_k \overline{K} \cap \Lambda$ for each k. The proof of the next result, and much more, can be found in [15].

Minkowski's Second Theorem. *If $0 < \lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$ are the successive minima of convex body K with respect to Λ then $\lambda_1\lambda_2 \dots \lambda_n vol(K) \le 2^n det(\Lambda)$.*

Let $r_1, r_2, \dots, r_k \in \mathbb{Z}/N\mathbb{Z}$ and $\delta > 0$ be given. We define the *Bohr neighbourhood*

$$B(r_1, r_2, \dots, r_k; \delta) := \{s \in \mathbb{Z}/N\mathbb{Z} : \|r_i s/N\| \le \delta \text{ for } i = 1, 2, \dots, k\};$$

that is, the least residue, in absolute value, of each $r_i s \pmod N$ is $< \delta N$ in absolute value.

A generalized arithmetic progression is called *proper* if its elements are distinct are all distinct (that is $|C(a_0, a_1, \dots, a_k; N_1, N_2, \dots, N_k)| = N_1N_2 \dots N_k$).

It will be seen, in §6, that Bohr neighbourhoods can be used as a step in finding arithmetic progressions, using Fourier transforms.

Theorem 5.7. *If $0 < \delta < 1/2$ then the Bohr neighbourhood $B(r_1, \dots, r_k, \delta)$ contains a proper k-dimensional arithmetic progression of cardinality at least $(2\delta/k)^k N$.*

Proof. We have $s \in B(r_1, r_2, \dots, r_k; \delta)$ if and only if $(r_1s, r_2s, \dots, r_ks) + N\mathbb{Z}^k$ contains a point x with $\|x\|_\infty \le \delta N$. Let Λ be the lattice generated by $N\mathbb{Z}^k$ and $(r_1, r_2, \dots, r_k)$: It can be shown that $det(\Lambda) = N^{k-1}$.

Let $K = \{(a_1, a_2, \dots, a_k) : -1 < a_i < 1\}$ and, as described above, obtain a basis $b_1, b_2, \dots, b_k$ of $\mathbb{R}^k$ with each $b_i \in \Lambda$ satisfying $\|b_i\|_\infty = \lambda_i$. Define s_i so that $b_i \in (r_1s_i, r_2s_i, \dots, r_ks_i) + N\mathbb{Z}^k$. By Minkowski's Second Theorem, $\lambda_1\lambda_2 \dots \lambda_k vol(K) \le det(\Lambda) \cdot 2^k$ so that $\lambda_1\lambda_2 \dots \lambda_k \le N^{k-1}$.

Let P be the k-dimensional arithmetic progression $\{\sum_{i=1}^k a_i s_i : |a_i| \le \delta N/k\lambda_i\}$. If $s \in P$ then, for each j,

$$\left\| \frac{r_j s}{N} \right\| \le \sum_{i=1}^k |a_i| \left\| \frac{r_j s_i}{N} \right\| \le \sum_{i=1}^k \frac{\delta N}{k\lambda_i} \left\| \frac{(b_i)_j}{N} \right\| \le \sum_{i=1}^k \frac{\delta N}{k\lambda_i} \frac{\|b_i\|_\infty}{N} = \delta.$$

Moreover since $\delta < 1/2$ we have that P is proper. Finally note that $|P| \ge \prod 2\delta N/k\lambda_i = (2\delta N/k)^k \cdot (\lambda_1\lambda_2 \dots \lambda_k)^{-1} \ge (2\delta/k)^k N$.

SUBCHAPTER: SUM-PRODUCT FORMULAS, I. PROOFS FROM "THE BOOK"

All true mathematicians are motivated by elegant proofs, none more so than the great Paul Erdős. Erdős used to say that "the supreme being" kept a book which contained all of the most beautiful proofs of each theorem and just occasionally we mortals are allowed to glimpse this book, as we discover an extraordinary proof. In this section we shall see three such proofs from "The Book", all by Hungarians.

One of Paul Erdős's proofs from the book, comes in his "multiplication table theorem": Let $A = \{1, 2, \dots, N\}$; how big is $A \cdot A = \{ab : a, b \in A\}$? That is, how many distinct integers appear in the N-by-N multiplication table? It is trivial that $|A \cdot A| \leq N(N+1)/2$ (using the symmetry that $ab = ba$) but is it the case that $|A \cdot A|/N^2 \to$a limit as $N \to \infty$, and if so, what is that limit? Erdős proved that the limit exists and is 0, that is $|A \cdot A| = o(N^2)$. His proof rests on the beautiful result of Hardy and Ramanujan that all but $o(N)$ of the integers $n \leq N$ have $\{1+o(1)\} \log\log N$ prime factors (counting multiplicity[3]). But then all but $o(N^2)$ of the products ab with $a, b \leq N$ have $\{2+o(1)\} \log\log N$ prime factors, whereas almost all integers up to N^2 have $\{1 + o(1)\} \log\log(N^2) = \{1 + o(1)\} \log\log N$ prime factors, and the result follows!

In the other direction, consider integers of the form $n = pm \leq N^2$ where $p \in (N^{2/3}, N]$ is prime and $m \leq N$. There are $\geq \{1+o(1)\}N^2/\log N$ such product by the prime number theorem, and any n can be represented in at most two ways as such a product, so that $|A \cdot A| \geq \{1/2+o(1)\}N^2/\log N$. In the case that A is an arithmetic progression $\{a+ib : 1 \leq i \leq N\}$ then we may assume without loss of generality that $(a, b) = 1$ (else we divide through by the common factor). If $b > 2N$ then $|A \cdot A| = N(N+1)/2$; for if $(a+ib)(a+jb) = (a+Ib)(a+Jb)$ then $a(i+j)+bij = a(I+J)+bIJ$ so that $a(i+j) \equiv a(I+J) \pmod b$ implying $i+j \equiv I+J \pmod b$ and thus $i+j = I+J$ since $2 \leq i+j, I+J \leq 2N < b$, and so $ij = IJ$ and therefore $\{i, j\} = \{I, J\}$. Similarly if $a > N^2$ then $|A \cdot A| = N(N+1)/2$. Finally if $b \leq 2N$ and $a \leq N^2$ then all elements of A are $\leq N^2+N(2N) = 3N^2$. Let B be the subset of A consisting of all integers in A with a prime factor in $(N/2, N]$. Note that all primes in $(N/2, N]$ that do not divide b, divide either one or two elements of A so that $|B| \geq \{1/2+o(1)\}N/\log N$. Any element of $A \cdot B$ is $\leq 9N^4$ so contains no more than 4 prime factors $> N/2$ and so cannot be written in more than eight ways as $ab, a \in A, b \in B$. Therefore $|A \cdot A| \geq |A \cdot B| \geq \{1/8 + o(1)\}N^2/\log N$.

One might expect to generalize this so that if $A + A$ is small then A has a lot of additive structure, that is it is a subset of a generalized arithmetic progression, and so $A \cdot A$ is large. In fact there should be some "play off" between the two in that if one is much smaller than the expected size then the other should not be; that is one might guess, as did Erdős and Szemerédi, that

$$|A + A| + |A \cdot A| \gg_\epsilon |A|^{2-\epsilon}$$

for any $\epsilon > 0$; or, more daringly like Solymosi, that

$$|A + B| + |A \cdot C| \gg_\epsilon |A|^{2-\epsilon} \text{ whenever } |A| = |B| = |C|.$$

There are several results of this type, for various values of ϵ, in the literature, but none more elegantly proved than the result of Elekes. This rests on a (generalization of a) result in combinatorial geometry of Szemerédi and Trotter, which in turn has recently been given a gorgeous proof via geometric and random graph theory by Székely:

[3]So that, for instance, 12 has 3 prime factors.

The Szemerédi-Trotter theorem. *We are given a set Υ of m curves in the complex plane such that*

- *Each pair of (distinct) curves in Υ meet in at most B_1 points;*
- *No more than B_2 curves in Υ contain any given pair of (distinct) points.*

For a given set, Π, of m points, define $X = X(\Upsilon, \Pi)$ to be the number of pairs (P, C) with $P \in \Pi, C \in \Upsilon$ where P lies on C. Then $X(\Upsilon, \Pi) \le m + 4B_2n + 4B_2B_1^{1/3}(mn)^{2/3}$.

Proof. (Székely) The key idea is to determine how far away our set of curves and points are from being embeddable on the plane in the sense of graph theory, that is that the curves of Υ should only cross at points in Π. To convert this directly into a graph theory problem we replace each point of Π by a vertex of our graph G, and we join two vertices of G if and only if the corresponding points lie on the same curve $C \in \Upsilon$ with no other point of Π in-between (we call such pairs of points "neighbours on C"). In this definition G is a simple graph, even if two points are neighbours on several curves of Υ. We will also define a hypergraph G^* with the same vertex set as G, but as many edges between two vertices as the number of curves of Υ on which they are neighbours. Note that $X = e(G^*) + m \le B_2e(G) + m$ (where $e(H)$ and $v(H)$ are the number of edges and vertices, respectively, in H; note that $v(G) = n$). Therefore we will assume that $e(G) \ge 4n$ for otherwise we already have $X < 4B_2n + m$ as desired.

We now define $Y = Y(G)$ to be the minimum, over all drawings of G in the complex plane, of the number of crossings of edges of G that occur at some point not in the vertex set of G; so $Y(G) = 0$ if G is planar. Note that if we remove these $Y(G)$ edges from G and as well as any isolated vertices, then the resulting new graph H is planar, with $e(H) = e(G) - Y(G)$ and $v(H) \le v(G)$. Note also that $Y(G)$ can be no bigger than the sum over all pairs of curves in Υ, of the number of ways that those two curves can cross; that is $Y(G) \le B_1\binom{m}{2}$.

Now for any simple planar graph H one has the Euler characteristic formula that $f(H) - e(H) + v(H) = 2$ where $f(H)$ is the number of faces of H, and that any edge separates at most two faces whereas any face is surrounded by at least three edges so that $3f(H) \le 2e(H)$. Therefore $6 + 3e - 3v = 3f \le 2e$ so that $e(H) \le 3v(H) - 6$. Combining this with the previous paragraph we deduce that $Y(G) \ge e(G) - 3v(G) + 6$.

Székely's extraordinary trick is to apply the result of the previous paragraph to randomly chosen subgraphs of G, resulting in an improvement of the above inequality! The random process involves deciding at random whether to select each vertex, independently, where the probability of each vertex being chosen is $p = 4v(G)/e(G)$ (which is ≤ 1 by the above assumption); and then retaining the edges from G that go between chosen vertices. If we call the resulting subgraph K then we see that the expected numbers of vertices in K is $pv(G)$, written $\mathbb{E}(v(K)) = pv(G)$ and also that $\mathbb{E}(e(K)) = p^2e(G)$ and $\mathbb{E}(Y(K)) = p^4Y(G)$. Substituting this into the bound attained above we have $p^4Y(G) = \mathbb{E}(Y(K)) \ge E(e(K)) - 3\mathbb{E}(v(K)) + 6 = p^2e(G) - 3pv(G) + 6$. With our choice of p, and the above bound for Y, this implies that $B_1m^2/2 > Y(G) > e(G)^3/64v(G)^2$, so that $X \le B_2(32B_1)^{1/3}(mn)^{2/3} + m$.

Prove that each term in the upper bound here is necessary by giving appropriate examples. For example for the third term let Υ be the set of lines $y = ax + b$ with $0 \le a \le A$ and $0 \le b \le AC$, and let Π be the

set of points in the rectangle $\{0,1,\dots,C\}\times\{0,1,\dots 2AC\}$. A big subset of the points counted by X are given by the points on the lines with $0\le x\le C$.

Corollary (Elekes)**.** *If* $|B||C|\ge|A|$ *then* $|A+B|+|A\cdot C|\ge(64|B||C|/(|A|-1))^{1/4}(|A|-1)$.

Proof. Consider the set of points $\Pi=(A+B)\times(A\cdot C)$, and the set Υ of lines $y=c(x-b)$ for each $b\in B, c\in C$. Note that $B_1=B_2=1$. Each such line contains $|A|$ points, namely $\{(a+b,ac):a\in A\}$ and so $X\ge|A|m$ where $m=|B||C|$ and $n=|A+B||A\cdot C|$. Substituting this into the proof of the Szemerédi-Trotter theorem we obtain $(|A|-1)m\le n/4+(mn)^{2/3}/32^{1/3}$, from which we deduce that $|A+B||A\cdot C|\ge 2(|B||C|(|A|-1)^3)^{1/2}$ if $|B||C|\ge|A|$, and the result follows.

In the particular case that $|A|=|B|=|C|$ this gives $|A+B|+|A\cdot C|\ge|A|^{5/4}$, a first step to the above conjectures.

Proposition. (Solymosi, 2009) *Suppose that* $A,B\subset\mathbb{R}^+$ *with* $|A|\ge|B|>1$. *Then*

$$|AB||A+A||B+B|\gg\frac{(|A||B|)^2}{\log|B|}.$$

Proof. In this proof we will use the *multiplicative energy* $E_\times(A,B)$ which counts the number of solutions $a,a'\in B,\ b,b'\in B$ to $ab=a'b'$.

Define $C_m:=\{(a,b)\in A\times B: b=ma\}$. If $m<n$ and $(x,y)=(a,b)+(a',b')\in C_m+C_n\subset(A+A)\times(B+B)$ then $a+a'=x$ and $ma+na'=b+b'=y$, so that a and a' are determined, and hence $|C_m+C_n|=|C_m||C_n|$. Note that $m<\frac{y}{x}=\frac{b+b'}{a+a'}<n$.

Therefore if $m_1<m_2<\ldots<m_k$ then the elements of $C_{m_i}+C_{m_{i+1}}$, $i=1,2,\dots,k-1$ are all distinct (since if $(x_i,y_i)\in C_{m_i}+C_{m_{i+1}}$, then $m_1<\ldots<m_{j-1}<\frac{y_{j-1}}{x_{j-1}}<m_j<\frac{y_j}{x_j}<m_{j+1}<\ldots<m_k$). We deduce that

$$\sum_{i=1}^{k-1}|C_{m_i}||C_{m_{i+1}}|\le|A+A||B+B|. \tag{1}$$

Let $\mathcal{L}_j$ be the set of m for which $2^j\le|C_m|<2^{j+1}$. Applying (1) to the m's in $\mathcal{L}_j$ we obtain

$$(|\mathcal{L}_j|-1)2^{2j}\le\sum_{i=1}^{k-1}|C_{m_i}||C_{m_{i+1}}|\le|A+A||B+B|.$$

Now if $2^J>|B|$ then

$$\begin{aligned}E_\times(A,B)&=\sum_m|C_m|^2\le\sum_{j=0}^{J-1}2^{2(j+1)}|\mathcal{L}_j|\\ &\le 4\sum_{j=0}^{J-1}(|A+A||B+B|+2^{2j})\le 4J|A+A||B+B|+4^{J+1}/3. \qquad (2)\end{aligned}$$

Now the multiplicative analogy to (6.2') is $(|A||B|)^2\le|AB|E_\times(A,B)$, and we can assume $2^J\le 2|B|$ so combining the above yields the result.

Corollary. *Suppose that $A \subset \mathbb{R}^+$ with $|A| > 1$. Then*

$$|AA| + |A + A| \gg \frac{|A|^{4/3}}{(\log |A|)^{1/3}}.$$

Proof. We partition our set A into $A_+ \subset \mathbb{R}^+$ and $A_- \subset \mathbb{R}^-$. Taking $A = B = A_+$ and then $A = B = -A_-$ in the Proposition then yields the result.

The Freiman-Ruzsa Theorem

Freiman's Theorem [5] describes the structure of a set A under the condition that $A + A$ has size close to that of A. We define a *generalised arithmetic progression* to be a sum P of ordinary arithmetic progressions (see Theorem 5.7). If P is a subset of a small generalised arithmetic progression then $|P + P|$ is close to $|P|$. Freiman's Theorem states the converse: if $|P + P|$ is close to P then P must be contained in a small generalized arithmetic progression.

We now proceed to the proof of Freiman's Theorem, using a remarkable and ingenious approach due to Ruzsa [12].

Let $A \subset \mathbb{Z}/s\mathbb{Z}$ or $A \subset \mathbb{Z}$ and $B \subset \mathbb{Z}/t\mathbb{Z}$.

Then $\phi : A \to B$ is called a *(Freiman) k-homomorphism* if whenever $x_1+x_2+\cdots+x_k = y_1 + y_2 + \cdots + y_k$, with $x_i, y_i \in A$, we have $\sum \phi(x_i) = \sum \phi(y_i)$. In addition, ϕ is called a *k-isomorphism* if ϕ is invertible and ϕ and ϕ^{-1} are k-homomorphisms.

Note that ϕ is a k-homomorphism if the map $\psi : (x_1, \ldots, x_k) \mapsto \sum \phi(x_i)$ induced by ϕ is a well defined map $kA \to kB$, and a k-isomorphism if ψ is a bijection. Our interest will be in 2-isomorphisms, as these preserve arithmetic progressions – a set 2-isomorphic to an arithmetic progression is clearly an arithmetic progression. We use the following notation:

If $\phi : A \to B$ and $A' \subset A$, then $\phi|_{A'}$ denotes the restriction of ϕ to A'.

Lemma 6.1. *Let $A \subset \mathbb{Z}$ and suppose $|kA - kA| \leq C|A|$. Then, for any prime $N > C|A|$, there exists $A' \subset A$ with $|A'| \geq |A|/k$ that is k-isomorphic to a subset of $\mathbb{Z}/N\mathbb{Z}$.*

Proof. We may suppose $A \subset \mathbb{N}$ and select a prime $p > k \max A$. Then the quotient map $\phi_1 : \mathbb{Z} \to \mathbb{Z}_p$ is a homomorphism of all orders, and $\phi_1|_A$ is a k-isomorphism. Now let q be a random element of $[p-1]$ and define $\phi_2 : \mathbb{Z}_p \to \mathbb{Z}_p$ by $\phi_2(x) = qx$. Then ϕ_2 is an isomorphism of all orders, and hence a k-isomorphism. Let $\phi_3(x) = x$ where $\phi_3 : \mathbb{Z}_p \to \mathbb{Z}$. Then for any j, $\phi_3|_{I_j}$ is a k-isomorphism where

$$I_j = \{x \in \mathbb{Z}_p : \frac{j-1}{k}p \leq x < \frac{j}{k}p - 1\}.$$

For, if $\sum_{i=1}^k x_i = \sum_{i=1}^k y_i \pmod p$ with $x_i, y_i \in I_j$, then $\sum_{i=1}^k x_i = \sum_{i=1}^k y_i$ in $\mathbb{Z}$. By the pigeonhole principle, there exist $A' \subset A$ with $|A'| \geq |A|/k$ (depending on q) and $\phi_2\phi_1[A'] \subset I_j$ for some j. Restricted to A', $\phi_3\phi_2\phi_1$ is a k-homomorphism. Finally, let ϕ_4 be the quotient map (a k-homomorphism) $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$. Then with $\phi = \phi_4\phi_3\phi_2\phi_1$, $\phi(x) = qx \pmod p \pmod N$ and $\phi|_{A'}$ is a k-homomorphism, as it is the composition of k-homomorphisms.

The only way $\phi|_{A'}$ is not a k-isomorphism is if there are $a_1, a_2, \ldots, a_k, a'_1, a'_2, \ldots, a'_k \in A'$ such that $\sum_{i=1}^k \phi(a_i) = \sum_{i=1}^k \phi(a'_i)$ but $\sum_{i=1}^k \phi(a_i) \neq \sum_{i=1}^k \phi(a'_i)$.

Now $\sum_i a_i \neq \sum_i a'_i$ implies $\sum_i a_i \neq \sum_i a'_i \pmod p$ so we have $q(\sum_i a_i - \sum_i a'_i) \pmod p$ is a multiple of N. The probability of this event is at most $|kA - kA|/N < 1$ since $|kA - kA| \leq C|A|$ and $N > C|A|$. So for some q, $\phi|_{A'}$ is a k-isomorphism.

The next theorem, due to Bogolyubov [3], shows that we may find long arithmetic progressions with small dimension in $2A - 2A$. The proof is surprisingly simple.

Theorem 6.2. *Let $A \subset \mathbb{Z}/N\mathbb{Z}$ with $|A| \ge \alpha N$. Then $2A-2A$ contains an arithmetic progression of length at least $(\alpha^2/4)^{\alpha^{-2}}N$ and dimension at most α^{-2}.*

Proof. Let $g(x)$ be the number of ways of writing $x = (a-b)-(c-d)$ with $a,b,c,d \in A$. That is, $g = (A*A)*(A*A)$ and $x \in 2A-2A$ if and only if $g(x) \ne 0$. Now $g(x) = N^{-1}\sum_r |\hat{A}(r)|^4\omega^{rx}$,

by Lemma 2.2 (3). Let $K = \{r \ne 0 : \hat{A}(r) \ge \alpha^{3/2}N\}$. Then

$$\sum_{\substack{r\ne 0\\ r\notin K}} |\hat{A}(r)|^4 \le \max_{\substack{r\ne 0\\ r\notin K}} |\hat{A}(r)|^2 \sum_r |\hat{A}(r)|^2 < \alpha^3N^2\cdot \alpha N^2 = \alpha^4N^4.$$

Therefore, if x is such that $Re(\omega^{rx}) \ge 0$ for all $r \in K$, then

$$Re\Big(\sum_r |\hat{A}(r)|^4\omega^{rx}\Big) > |\hat{A}(0)|^4 - \alpha^4N^4 = 0.$$

Therefore $g(x) \ne 0$ and $2A-2A$ contains the Bohr neighbourhood $B(K;1/4)$ – $Re(\omega^{rs}) \ge 0$ if and only if $-N/4 \le rs \le N/4$. Now $\sum_{r\in K}|\hat{A}(r)|^2 \ge k\alpha^3N^2$ and $\sum_{r\in K}|\hat{A}(r)|^2 \le \alpha N^2$. By Theorem 5.7, $2A-2A$ contains the required arithmetic progression.

We now present Ruzsa's proof of Freiman's Theorem.

Freiman's Theorem. *Let $A \subset \mathbb{Z}/N\mathbb{Z}$ be a set such that $|A+A| \le C|A|$. Then A is contained in a d-dimensional arithmetic progression P of cardinality at most $k|A|$ where d and k depend on C only.*

Proof. By Theorem 5.15, $|8A-8A| \le C^{16}|A|$. By Lemma 6.1, A contains a subset A' of cardinality at least $|A|/8$ which is 8-isomorphic to a a set $B \subset \mathbb{Z}/N\mathbb{Z}$ with $C^{16}|A| < N \le 2C^{16}|A|$, where N is prime and $C|A| < N \le 2C|A|$, using Bertrand's Postulate. So $|B| = \alpha N$ with $\alpha \ge (16C^{16})^{-1}$. By Theorem 6.2, $2B-2B$ contains an arithmetic progression of dimension at most α^{-2} and cardinality at least $(\alpha^2/4)^{\alpha^{-2}}N \ge (\alpha^2/4)^{\alpha^{-2}}|A|$. Since B is 8-isomorphic to A', $2B-2B$ is 2-isomorphic to $2A'-2A'$. Any set 2-isomorphic to a d-dimensional arithmetic progression is a d-dimensional arithmetic progression. Therefore $2A'-2A'$, and hence $2A-2A$, contains an arithmetic progression Q of dimension at most α^{-2} and cardinality $\gamma|A|$, where $\gamma \ge (\alpha^2/4)^{\alpha^{-2}}$. Now let $X = \{x_1, x_2, \dots, x_k\} \subset A$ be maximal such that $x,y \in X$, $x \ne y$ imply $x-y \in Q-Q$. Equivalently, all the sets $x+Q$ are disjoint, so $X+Q = |X||Q|$. Since X is maximal, $A \subset X+(Q-Q)$ and X is contained in the k-dimensional arithmetic progression $R = \Big\{\sum_{i=1}^k a_ix_i : 0 \le a_i \le 1\Big\}$. Clearly $|R| \le 2^k$. Therefore A is contained in the arithmetic progression $R+(Q-Q)$, of dimension at most $\alpha^{-2}+k$. We know that $X+(Q-Q) \subset A+(4A-4A) = A+2A-2A+2A-2A$, and that $X+Q \subset A+2A-2A = 3A-2A$.

So $|X+Q| \le |3A-2A| \le C^5|A|$, by Theorem 5.15. So $k \le C^5|A|/|Q| \le C^5\gamma^{-1}$. Finally, $|Q-Q| \le 2^{\alpha^{-2}}|Q|$, by d-dimensionality. So A is contained in an arithmetic progression of dimension at most $\alpha^{-2}C^5\gamma^{-1}$, and cardinality at most $2^k2^{\alpha^{-2}}|Q| \le 2^k2^{\alpha^{-2}}|2A-2A|$ $\le kC^4 2^{\alpha^{-2}}|A|$.

The constants from this theorem can be chosen to be $d = exp(C^\alpha)$ and $k = expexp(C^\beta)$, where $\alpha, \beta > 0$ are absolute constants.

The Balog-Szemerédi-Gowers theorem

Lemma 6.5. *Let $A_1, A_2, \dots, A_m$ be subsets of an N element set S, let $\gamma > 0$ and suppose that $\sum_{i=1}^m |A_i| \geq \gamma mN$. Then there exists $B \subset \{1, \dots, m\}$, of cardinality at least $\gamma^5 m/2$, such that for at least ninety-five percent of pairs $(i,j) \in B \times B$, $|A_i \cap A_j| \geq \gamma^2 N/2$.*

Proof. The idea is to show that this is true of a randomly chosen subset B, and thus there exist such B. So, let $x_1, x_2, \dots, x_5$ be chosen randomly and independently from S and define $B = \{i : \{x_1, x_2, \dots, x_5\} \subset A_i\}$. Then $\mathrm{Prob}[i \in B] = (|A_i|/N)^5$ and thus the expected size of B is $\sum_{i=1}^m (|A_i|/N)^5 \geq m(\sum |A_i|/mN)^5 \geq \gamma^5 m$ (Exercise: Justify this inequality). Then, by the Cauchy-Schwartz inequality, $\mathbb{E}[|B|^2] \geq \mathbb{E}[|B|]^2 \geq \gamma^{10} m^2$.

If $|A_i \cap A_j| \leq \gamma^2 N/2$, then

$$\mathrm{Prob}[i,j \in B] = \mathrm{Prob}\{\{x_1, x_2, \dots, x_5\} \subset A_i \cap A_j\} < (\gamma^2/2)^5 = \gamma^{10}/32.$$

Define $C = \{i,j \in B \times B : |A_i \cap A_j| < \gamma^2 N/2\}$ so that $\mathbb{E}[|C|] < \gamma^{10} m^2/32$. Therefore $\mathbb{E}[|B|^2 - 24|C|] > \gamma^{10} m^2/4$, so that there exist $x_1, \dots, x_5$ such that $|B|^2 > 24|C| + \gamma^{10} m^2/4$, that is $|B| > \gamma^5 m/2$ and $|C| \leq \frac{1}{24}|B|^2 \leq \frac{1}{20}|B|^2$.

The following result is due to Balog and Szemerédi [1]. However the constants they gave were at least exponential in α; and it was Gowers who gave polynomial growth:

Theorem 6.6. (Balog-Szemerédi-Gowers) *Let A be a subset of an abelian group, and $\alpha > 0$. If $E(A,A) \geq \alpha |A|^3$ then A contains a subset A' such that $|A'| \geq c|A|$ and $|A' - A'| \leq C|A'|$ where c and C depend on α only (we can take $c = 2^{-12}\alpha^{10}$ and $C = 2^{38}\alpha^{-32}$).*

Proof. Let $n = |A|$ and note that $r_{A-A}(x) = r_{A-A}(-x) \leq r_{A-A}(0) = n$. By hypothesis $\sum_x r_{A-A}(x)^2 = E(A,A) \geq \alpha n^3$. Let $X = \{x \neq 0 : \ r_{A-A}(x) \geq \frac{\alpha}{2} n\}$. Now if $x \in X \cup \{0\}$ then $r_{A-A}(x)^2 \leq \frac{\alpha}{2} n r_{A-A}(x) + (1 - \frac{\alpha}{2})n^2$, and so

$$\alpha n^3 \leq \sum_x r_{A-A}(x)^2 \leq \frac{\alpha}{2} n \sum_x r_{A-A}(x) + (1 - \frac{\alpha}{2})n^2(|X|+1) = \frac{\alpha}{2} n^3 + (1 - \frac{\alpha}{2})n^2(|X|+1),$$

and therefore $|X| \geq \frac{\alpha}{2} n$ (as $\alpha \geq 2/\sqrt{n}$).

We now construct a graph G with vertices corresponding to the elements of A, and

$$a \sim_G b \text{ if and only if } a - b \in X.$$

Define $\Gamma_G(a) := \{b \in G : a \sim_G b\}$ to be the set of neighbours of a in G. Then

$$\sum_{a \in A} |\Gamma_G(a)| = \#\{a \neq b \in A : a \sim_G b\} = \sum_{x \in X} r(x) \geq |X| \frac{\alpha}{2} n \geq \frac{\alpha^2}{4} n^2.$$

Applying Lemma 6.5 with $S = A$ and the A_i equal to the $\Gamma_G(a)$, so that $m = N = n$ and $\gamma = \alpha^2/4$, we deduce that there exists $B \subset A$ with $|B| \geq \alpha^{10} n/2^{11}$ such that $|\Gamma_G(a) \cap \Gamma_G(b)| \geq \alpha^4 n/32$ for at least ninety-five percent of pairs $(a,b) \in B \times B$.

Now define a new graph H with vertex set B and edges defined so that

$$a \sim_H b \text{ if and only if } |\Gamma_G(a) \cap \Gamma_G(b)| \geq \alpha^4 n/32.$$

Let A' be the set of vertices of H with degree $\geq 3|B|/4$.

Exercise: Since the average degree in H is at least $(19/20)|B|$, deduce that $|A'| \ge 4|B|/5$.

Therefore $|A'| \ge \alpha^{10}n/(5\cdot 2^9)$. We will show that if $x \in A'-A'$ then $r_{4A-4A}(x) \ge \kappa n^7$ for a certain constant $\kappa > 0$ depending only on α. But then

$$\kappa n^7|A'-A'| \le \sum_{x\in A'-A'} r_{4A-4A}(x) \le \sum_x r_{4A-4A}(x) = n^8,$$

and so $|A'-A'| \le n/\kappa \le (5\cdot 2^9)\alpha^{-10}|A'|/\kappa$, as desired.

Now for each $x \in A'-A'$ select $a, a' \in A'$ for which $x = a-a'$. If $a \sim_H b$ then there are at least $\alpha^4 n/32$ values of $c \in A$ for which $a-c, c-b \in X$. If $a-c \in X$ then there exists $\ge \alpha n/2$ pairs $x_1, y_1 \in A$ for which $a-c = x_1-y_1$, and similarly there are $\ge \alpha n/2$ pairs $x_2, y_2 \in A$ for which $c-b = x_2-y_2$. Taking all these representations for all such c we have $\ge (\alpha^4 n/32)(\alpha n/2)^2 = \alpha^6 n^3/2^7$ quadruples $x_1, y_1, x_2, y_2 \in A$ for which $a-b = x_1-y_1+x_2-y_2$: To verify that these representations are distinct note that if we are given a, x_1, y_1 we can recover c as $a-x_1+y_1$. If $a' \sim_H b$ then we can similarly find such representations for $b-a'$, and adding these together we find representations for $a-a'$ as desired which are all distinct as we can recover b in each case. Therefore $R(x) \ge |\Gamma_H(a) \cap \Gamma_H(a')|(\alpha^6 n^3/2^7)^2$; and we have $|\Gamma_H(a)\cap\Gamma_H(a')| \ge |\Gamma_H(a)| + |\Gamma_H(a')| - |H| \ge 3|B|/4 + 3|B|/4 - |B| = |B|/2$, and the result follows with $\kappa = \alpha^{22}/2^{26}$.

We recall that (6.2') implies that if $|A \pm A| < C|A|$, then $E(A,A) \ge |A|^3/C$. The Balog-Szemerédi-Gowers Theorem is a partial converse, stating in this context that if $E(A,A) > |A|^3/C$ then there exists a large subset A' of A, such that $|A'| \ge c|A|$ and $|A'+A'| \le \kappa|A|$ is small. where c and κ depend only on C.

We do need involve a subset of A in the conclusion of Theorem 6.6, for consider the example $A = \{1, 2, \dots, N\} \cup \{2^N, 2^{N+1}, \dots, 2^{2N-1}\}$. Then $|A| = 2N$, $|A+A| = N^2/2 + O(N)$ and $E(A,A) \ge 2N^3/3 + O(N^2)$; that is $E(A,A) \gtrsim |A|^3/12$, as in the hypothesis of Theorem 6.6, yet $A+A$ is large, so to obtain the desired conclusion we need the subset $A' = \{1, 2, \dots, N\}$.

It is worth noting that this can be converted into an "if and only if" Theorem:

Corollary 6.6B. *Let A be a subset of an abelian group. Then $E(A,A) \gg |A|^3$ if and only if there exists $A' \subset A$ such that $|A'| \gg |A|$ and $|A'+A'| \ll |A'|$.*

Proof. One direction is Theorem 6.6 together with the Corollary to Lev's lemma. In the other direction we have, by (6.2'),

$$E(A,A) \ge E(A',A') \ge |A'|^4/|A'+A'| \gg |A'|^3 \gg |A|^3.$$

An alternate but useful version of Theorem 6.6 is as follows:

Theorem 6.6A. *If $S \subset A\times A$ with $|S| \ge \beta|A|^2$ and $\#\{a+b : (a,b) \in S\} \le (1/\beta)|A|$ for some given $\beta > 0$ then A contains a subset A' such that $|A'| \ge c|A|$ and $|2A'| \le C|A'|$ where c and C depend on β only (we can take $c = 2^{-12}\beta^{30}$ and $C = 2^{38}\beta^{-96}$).*

Proof. Let $X = \{a+b : (a,b) \in S\}$ and $r_S(x) = \#\{(a,b) \in S : \ a+b = x\}$. Therefore

$$|S|^2 = \left(\sum_{x\in X} r_S(x)\right)^2 \le |X| \sum_{x\in X} r_S(x)^2 \le |X|E(A,A).$$

Hence $E(A,A) \geq |S|^2/|X| \geq \beta^3|A|^3$, and the result follows from Theorem 6.6 with $\alpha = \beta^3$.

Corollary 6.7. *If $A \subset \mathbb{Z}^k$ with $|A| = m$ and $E(A,A) \geq \alpha m^3$ then there exists a generalized arithmetic progression Q of cardinality at most $V(\alpha)m$ and dimension at most $d(\alpha)$ such that $|A \cap Q| \geq c(\alpha)m$, where $V(\alpha), d(\alpha)$ and $c(\alpha)$ depend only on α.*

Proof. By Theorem 6.6 there exists $A' \subset A$ for which $|A'| \geq c(\alpha)|A|$ and $|A' - A'| \leq C(\alpha)|A'|$. By the Freiman-Ruzsa Theorem there exists a generalized arithmetic progression Q which contains A', with $\dim(Q) \leq d(\alpha)$ and cardinality $\leq V(\alpha)|A'|$. The result follows as $A' \subset A \cap Q$.

The following result will be very useful in studying four-term arithmetic progressions in the next chapter.

Corollary 6.8. *Let $B \subset \mathbb{Z}/p\mathbb{Z}$ be a set with $|B| = \beta p$, and let $\phi : B \to \mathbb{Z}/p\mathbb{Z}$ be such that*
$$\#\{a,b,c,d \in B : a-b = c-d \text{ and } \phi(a) - \phi(b) = \phi(c) - \phi(d)\} \geq \alpha p^3.$$
Then there exist constants γ and η, depending only on α and β, a $\mathbb{Z}/p\mathbb{Z}$-arithmetic progression P of cardinality at least N^γ and integers λ and μ for which $\phi(s) = e(2\lambda s + \mu)$ for at least $\eta|P|$ values of $s \in B \cap P$. The constants can be taken to be polynomial in α.

Proof. If $A = \{(a, \phi(a)) \in (\mathbb{Z}/p\mathbb{Z})^2 : a \in B\}$ then $E(A,A) \geq \alpha p^3 \geq \alpha m^3$ where $m = |A| = |B| \in [\beta p, p]$. We then proceed as in Corollary 6.7 except we can now use the Freiman-Ruzsa theorem in a finite group (see ***), so that the relevant constants are all polynomial in α.

Write $Q = \{b + a_1 n_1 + \ldots + a_d n_d : \ 0 \leq n_i \leq N_i - 1\}$ where $1 \leq N_1 \leq N_2 \leq \ldots \leq N_d$ and $p \geq N_1 N_2 \ldots N_d \geq c(\alpha)p$. (Note that the $a_j \in (\mathbb{Z}/p\mathbb{Z})^2$.) Therefore $N_d \geq (c(\alpha)p)^{1/d}$. We can partition of Q as the union of the arithmetic progressions $Q_{\mathbf{n}} := \{b_{\mathbf{n}} + a_d n_d : \ 0 \leq n_i \leq N_d - 1\}$ over each fixed $\mathbf{n} := (n_1, \ldots, n_{d-1})$ with $0 \leq n_i \leq N_i - 1$ for $1 \leq i \leq d-1$. Hence there exists $\mathbf{m}$ such that

$$|A \cap Q_{\mathbf{m}}| \geq \frac{1}{N_1 N_2 \ldots N_{d-1}} \sum_{\mathbf{n}} |A \cap Q_{\mathbf{n}}| = \frac{|A \cap Q| N_d}{|Q|} \geq \frac{c(\alpha) m |Q_{\mathbf{m}}|}{V(\alpha) m}.$$

Now write $Q_{\mathbf{m}} = \{(b,c) + n(u,v) : \ 0 \leq n \leq N_d\}$ and then take $P = \{b + nu : \ 0 \leq n \leq N_d\}$, so that $|P \cap B| = |A \cap Q_{\mathbf{m}}| \geq \eta |P|$, where $\eta = c(\alpha)/V(\alpha)$. Note that for each $h = b + nu \in P \cap B$ we have $\phi(b) = c + nv = \mu + 2\lambda h$ for some $\lambda, \mu \in \mathbb{F}_p$, as long as $u \neq 0$. But it is clear that $u \neq 0$ else $P = \{b\}$, so that $|A \cap Q_{\mathbf{m}}| = |P \cap B| = 1$, which is a contradiction.

Szemerédi's Theorem

We will develop a strategy to prove, by analytic methods,

Szemerédi's Theorem. *For any $\delta > 0$ and integer $k \ge 3$, there exists an integer $N_{k,\delta}$ such that if $N \ge N_{k,\delta}$ and $A \subset \{1, 2, \dots, N\}$ with $|A| \ge \delta N$ then A contains an arithmetic progression of length k.*

This strategy is based on Roth's proof for $k = 3$, given in section *. We will give a complete proof for $k = 4$, and give a complete proof for general k assuming one particularly difficult conjecture, that has recently been proved.

Three term arithmetic progresions and Parallellograms. We return to the proof of Roth's Theorem, and look to re-interpret it. Let $A, B, C \in \mathbb{F}_p$ The number of three term arithmetic progressions a, b, c with $a \in A,\ b \in B,\ c \in C$, minus the expected amount, namely $|A||B||C|/p$, is $\frac{1}{p}\sum_{m=1}^{p-1} \hat{A}(m)\hat{B}(-2m)\hat{C}(m)$. The square of the absolute value of this error term is, by Cauchying,

$$\le \frac{1}{p}\sum_{m=1}^{p-1} |\hat{B}(-2m)|^2 \cdot \frac{1}{p}\sum_{m=1}^{p-1} |\hat{A}(m)\hat{C}(m)|^2 \le |B| \left(\sum_{\substack{a,a' \in A,\ c,c' \in C \\ a+c=a'+c'}} 1 - \frac{|A|^2|C|^2}{p} \right).$$

One can re-parametrize solutions to $a + c = a' + c'$ as $a' = a + h_1,\ c' = a + h_2$ so that $c = a + h_1 + h_2$, in other words, these are the four vertices of a parallelogram projected onto the real axis. So, if $A = B = C$ has δp elements then

$$\left| \frac{1}{p^2} \sum_{a,d \in \mathbb{F}_p} A(a)A(a+d)A(a+2d) - \delta^3 \right|^2$$

$$\le \delta \left(\frac{1}{p^3} \sum_{a,h_1,h_2 \in \mathbb{F}_p} A(a)A(a+h_1)A(a+h_2)A(a+h_1+h_2) - \delta^4 \right). \tag{8.1}$$

In other words the error term in the number of 3-term arithmetic progressions in A is bounded by the error term in the count of the number of parallelograms in A. (Note that an arithmetic progression is the special case $h_1 = h_2 = d$.) Rather surprisingly it is this observation that generalizes to 4-term arithmetic progressions and beyond.

One complication in these calculations is that we always have to subtract the "main term". This can be dealt with by replacing $A(x)$ by

$$f_A(x) = A(x) - \delta = \begin{cases} 1 - \delta & \text{if } x \in A \\ -\delta & \text{otherwise} \end{cases}.$$

This also has the advantage of simplifying the Fourier transforms, since now $\hat{f}(m) = \hat{A}(m)$ if $m \ne 0$, and $\hat{f}(0) = 0$.

Write $A(a)A(a+d)A(a+2d) = (f(a)+\delta)(f(a+d)+\delta)(f(a+2d)+\delta)$ and expand. We get the "main term" δ^3 and the key term which is $A(a)A(a+d)A(a+2d)$. In all of the other terms we have a sum over at least as many variables as functions, so the sum is zero; for example

$$\sum_{a,d\in\mathbb{F}_p} f(a)f(a+2d) = \sum_{a,b\in\mathbb{F}_p} f(a)f(b) = 0$$

writing $b = a+2d$. Hence $\sum_{a,d} A(a)A(a+d)A(a+2d) - \delta^3 = \sum_{a,d} f(a)f(a+d)f(a+2d)$. Similar remarks can be made about the sum over the parallellograms. Hence the above inequality becomes

$$\left|\frac{1}{p^2}\sum_{a,d\in\mathbb{F}_p} f(a)f(a+d)f(a+2d)\right|^2$$

$$\le \delta\left(\frac{1}{p^3}\sum_{a,h_1,h_2\in\mathbb{F}_p} f(a)f(a+h_1)f(a+h_2)f(a+h_1+h_2)\right). \tag{8.2}$$

Moreover this type of result is true if we replace $f_A(a)f_A(a+d)f_A(a+2d)$ by $f_A(a)f_B(a+\beta d)f_C(a+\gamma d)$. We also observe that for any function f we have

$$\frac{1}{p^3}\sum_{a,h_1,h_2\in\mathbb{F}_p} f(a)\overline{f(a+h_1)}\ \overline{f(a+h_2)}f(a+h_1+h_2) = \frac{1}{p^4}\sum_{m\in\mathbb{F}_p}|\hat{f}(m)|^4. \tag{8.3}$$

Do we need anything more than Fourier transforms?. In our proof of Roth's Theorem, and above, we saw that if $|A| = \delta p$ and each $|\hat{f}_A(m)| = o(p)$ then A contains $\sim \delta^3 p^2$ 3-term arithmetic progressions, the number that one gets in a randomly chosen set of δp elements. In analogy we want an analytic condition that implies that A contains $\sim \delta^4 p^3$ 4-term arithmetic progressions (which is what holds for a randomly chosen set of δp elements). We now give an example to show that $|\hat{f}_A(m)| = o(p)$ cannot be that condition.

Let $(t)_p$ be the least residue of $t \pmod p$ in absolute value; in other words $(t)_p \equiv t \pmod p$ and $|(t)_p| < p/2$. Note that $|(t)_p| = p\|t/p\|$. Let $A = A_\delta := \{a \le p : |(a^2)_p| \le D\}$, where $D = [\delta p/2]$. The characteristic function for A can be written as:

$$A(a) = \sum_{d=-D}^{D}\frac{1}{p}\sum_{j=0}^{p-1} e\left(\frac{j(d-a^2)}{p}\right) = \begin{cases} 1 & \text{if } a\in A \\ 0 & \text{otherwise}\end{cases}.$$

Hence, for $m \ne 0$,

$$\hat{A}(m) = \sum_{a=0}^{p-1} A(a)e\left(\frac{am}{p}\right) = \frac{1}{p}\sum_{j=0}^{p-1}\sum_{d=-D}^{D} e\left(\frac{jd}{p}\right)\sum_{a=0}^{p-1} e\left(\frac{am-ja^2}{p}\right).$$

Now if $j \ne 0$ then the sum over a has size $\le 2\sqrt{p}$ by Lemma 4.1*; if $j = 0$ then the sum is 0 since $m \ne 0$ and we are this summing up a geometric progression. Therefore

$$|\hat{A}(m)| \le \frac{2}{\sqrt{p}}\sum_{j=1}^{p-1}\left|\sum_{d=-D}^{D} e\left(\frac{jd}{p}\right)\right| \le \frac{2}{\sqrt{p}}\sum_{j=1}^{p-1}\min\left\{2D+1, \frac{1}{2\,\|j/p\|}\right\} \ll \sqrt{p}\log p. \tag{8.3b}$$

Exercise: Prove the last inequality. Hence each Fourier coefficient is small, and so by the previous subsection[4] we know that A contains $\sim |A|^3/p$ arithmetic progressions. For $m = 0$ the term with $j = 0$ is exactly $2D + 1$, and otherwise the argument is the same, hence $|A| = \hat{A}(0) = 2D + O(\sqrt{p}\log p) = \delta p + O(\sqrt{p}\log p)$, and the hence the number of three term arithmetic progressions in A_δ is $\sim \delta^3 p^2$.

Now suppose that we have a three term arithmetic progression $a, a+d, a+2d \in A_{\delta/7}$. Now $(a+3d)^2 - 3(a+2d)^2 + 3(a+d)^2 - a^2 = 0$ and hence $|((a+3d)^2)_p| \le 3|((a+2d)^2)_p| + 3|((a+d)^2)_p| + |(a^2)_p| \le \delta$; and so $a, a+d, a+2d, a+3d$ is a 4-term arithmetic progression in A_δ. But then the number of 4-term arithmetic progressions in A_δ is $\gtrsim (\delta/7)^3 p^2$ which is significantly larger than the "expected" $\delta^4 p^2$ when $\delta < 1/7^3$. So we have seen, in this example, a case where all of the Fourier coefficients are small, yet there are not the expected number of four term arithmetic progressions.

Exercise: Prove that there are $\gtrsim (2\delta/(k^2 - 2k - 1))^3 p^2$ k-term arithmetic progressions. (Hint: Find identities for $(a + jd)^2$ as a linear combination of $a^2, (a + d)^2$ and $(a + 2d)^2$ for all integers j.)

Parallellopipeds. We work with the *discrete derivatives*, $\delta_h(g)(x) := g(x) - g(x+h)$, and in the multiplicative form $\Delta_h(f)(x) := f(x)\overline{f(x+h)}$. We see the connection between the two notions: $\Delta_h(e^g) = e^{\delta_h(g)}$ We define higher derivatives such as $\delta_{h_1,h_2}(g) = \delta_{h_2}(\delta_{h_1}(g))$ (notice that the order of the h_i does not effect the value), and in general

$$\Delta_{h_1,h_2,\dots,h_k}(f) = \Delta_{h_k}(\Delta_{h_1,h_2,\dots,h_{k-1}}(f)) = \prod_{\omega\in\{0,1\}^k} f^{(\omega)}(x + \omega\cdot h)$$

where $\omega = (\omega_1, \dots, \omega_k)$ and $h = (h_1, \dots, h_k)$, and $f^{(\omega)} = f$ if $\sum_i \omega_i$ is even, and $f^{(\omega)} = \overline{f}$ if $\sum_i \omega_i$ is odd.

Like continuous derivatives $\delta_h(P)$ has the property that it reduces the degree of a polynomial P by one; in particular if P is a constant then $\delta_h(P) = 0$. More generally if P is a polynomial of degree $k-1$ then $\delta_{h_1,h_2,\dots,h_k}(P) = 0$ for any choice of the $h_i's$, and so $\Delta_{h_1,h_2,\dots,h_k}(e^{iP(x)}) = 1$. If P has degree k and leading coefficient P_0 then $\Delta_{h_1,h_2,\dots,h_k}(e^{ig(x)}) = e^{i(-1)^k k! P_0 h_1 \dots h_k}$.

Exercise: Prove that if $f(x) = e^{iP(x)}g(x)$ where P is a polynomial of degree $< k$ then
$$\Delta_{h_1,h_2,\dots,h_k}(f(x)) = \Delta_{h_1,h_2,\dots,h_k}(g(x)).$$

We now define the *Gowers' U^k-norms*. To do so it is convenient to borrow notation from probability theory, even though we are working with determined sums: Instead of writing $\frac{1}{p}\sum_{x\in\mathbb{F}_p}$ we will write $\mathbb{E}_{x\in\mathbb{F}_p}$; this is convenient since the notation keeps track of much of the re-normalization that takes place in the proofs. The *Gowers' U^k-norms* is a measure of the size of the kth discrete derivatives of a a given function f, as we average all possible derivatives. So suppose that G is a given finite abelian group. Then $\|f\|_{U^k(G)}$ is the non-negative real number given by

$$\|f\|_{U^k(G)}^{2^k} := \mathbb{E}_{x,h_1,\dots,h_k\in G}\left(\Delta_{h_1,h_2,\dots,h_k} f(x)\right).$$

[4]Or by Proposition 3.1 together with the Equidistribution Theorem.

Note that $\|f\|_{U^0} = \|f\|_{U^1} = \mathbb{E}_{x\in G} f(x)$ and $\|f\|_{U^1} = |\mathbb{E}_{x\in G} f(x)|$. One deduces from the definition that

$$\|f\|_{U^k(G)}^{2^k} = \|\mathbb{E}_{h\in\mathbb{F}_p}(\Delta_h f)\|_{U^{k-1}(G)}^{2^{k-1}} = \mathbb{E}_{h\in\mathbb{F}_p}\|(\Delta_h f)\|_{U^{k-1}(G)}^{2^{k-1}}. \tag{8.4}$$

What does the Gowers' norm measure? We can determine when it equals 1:

Exercise: Show that if $\|f\|_{U^k(G)} = 1$ then $f(x) = e^{iP(x)}$ where P is a polynomial of degree $< k$. (Hint: First show that if $\|f\|_{U^k(G)} = 1$ then $\Delta_{h_1,h_2,\dots,h_k}(f(x)) = 1$ for all h_i, x, and then use induction on k.)

The key question is to understand when the Gowers' U^k-norm is "large", that is $\|f\|_{U^k(G)} > \delta$ for some fixed $\delta > 0$. We begin our study of the Gowers' U^2-norm by noting that the last equation of the previous section yields

$$\|f\|_{U^2}^4 = \frac{1}{p^4}\sum_{m\in\mathbb{F}_p} |\hat{f}(m)|^4 = \|\hat{f}\|_4^4, \tag{8.5}$$

so that $\|f\|_{U^2} = \|\hat{f}\|_4$. We can deduce a Cauchy-Schwarz type result:

Lemma 7.1. *For any $f, g : \mathbb{F}_p \to \mathbb{U} = \{z : |z| \le 1\}$, we have*

$$\mathbb{E}_{n\in\mathbb{F}_p}\big|E_{m\in\mathbb{F}_p} f(m)\overline{g(n-m)}\big|^2 \le \|f\|_{U^2}^2\|g\|_{U^2}^2.$$

Proof. First observe that

$$\frac{1}{p}\sum_r |\hat{f}(r)\hat{g}(r)|^2 = \sum_{\substack{a,b,c,d\\ a+b=c+d}} f(a)g(b)\overline{f}(c)\overline{g}(d) = \sum_n \big|\sum_m f(m)\overline{g(n-m)}\big|^2$$

The square of the left side is, by the Cauchy-Schwartz inequality and (8.5),

$$\le \frac{1}{p}\sum_r |\hat{f}(r)|^4 \cdot \frac{1}{p}\sum_r |\hat{g}(r)|^4 = p^6\|f\|_{U^2}^4\|g\|_{U^2}^4.$$

We have a good understanding of when the Gowers' U^2-norm is "large".

Lemma 8.1. (The Inverse Theorem for the Gowers' U^2-norm) *Let m be chosen to maximize $|\hat{f}(m)|$. Then $|\hat{f}(m)/p| \le \|f\|_{U^2}$; and, if each $|f(x)| \le 1$ then $\|f\|_{U^2} \le |\hat{f}(m)/p|^{1/2}$.*

Proof. Now $|\hat{f}(m)|^4 \le \sum_r |\hat{f}(r)|^4 = \|f\|_{U^2}^4 p^4$, implying the first inequality. On the other hand, we have $\sum_r |\hat{f}(r)|^2 = p\sum_x |f(x)|^2 \le p^2$ by Parseval's identity, and so

$$\|f\|_{U^2}^4 p^4 = \sum_r |\hat{f}(r)|^4 \le |\hat{f}(m)|^2 \sum_r |\hat{f}(r)|^2 \le p^2|\hat{f}(m)|^2,$$

and the second inequality follows.

The reason this is called an *Inverse Theorem* is that it gives us precise "if and only if" conditions for when $\|f\|_{U^2}$ is large; that is, $\|f\|_{U^2} \gg 1$ if and only if there exists some m such that $\frac{1}{p}\sum_{n \pmod p} f(n)e(-\frac{mn}{p}) \gg 1$, that is $f(x)$ "correlates" with some $e(\frac{mx}{p})$, the exponential of a linear polynomial in x. Perhaps this is not so surprising since $\|e(\frac{mx}{p})\|_{U^2} = 1$.

More generally we know that $\|e^{iP(x)}\|_{U^k} = 1$ when P is a polynomial of degree $< k$. So perhaps $\|f\|_{U^k} \gg 1$ if and only if $f(x)$ "correlates" with $e^{iP(x)}$ for some polynomial P of degree $< k$? Keep this thought in mind as we begin our study of higher Gowers' norms with a technical Cauchy-Schwarz type lemma:

What if for each ω we had a different function f_ω? How would this affect things?

Proposition 8.4. (Gowers-Cauchy-Schwarz inequality) *We have*

$$\left|\mathbb{E}_{x,h_1,\dots,h_k\in\mathbb{F}_p}\left(\prod_{\omega\in\{0,1\}^k} f_\omega^{(\omega)}(x+\omega\cdot h)\right)\right| \le \prod_{\omega\in\{0,1\}^k}\|f_\omega\|_{U^k(G)}.$$

Proof. By induction on k. For $k = 0$ this is trivial, so suppose that $k \ge 1$. For given $\nu \in \{0,1\}^{k-1}$ define $g_{\nu,h_k}(x) = f_{\nu\cup\{0\}}(x)\overline{f}_{\nu\cup\{1\}}(x+h_k)$, so that

$$\prod_{\omega\in\{0,1\}^k} f_\omega^{(\omega)}(x+\omega\cdot h) = \prod_{\nu\in\{0,1\}^{k-1}} f_{\nu\cup\{0\}}^{(\nu)}(x+\nu\cdot h')\overline{f}_{\nu\cup\{1\}}^{(\nu)}(x+h_k+\nu\cdot h')$$

where $h' = (h_1,\dots,h_{k-1})$; and so our expectation is

$$\mathbb{E}_{h_1,\dots,h_{k-1}\in\mathbb{F}_p}\left(\mathbb{E}_{x\in\mathbb{F}_p}\prod_{\nu\in\{0,1\}^{k-1}} f_{\nu\cup\{0\}}^{(\nu)}(x+\nu\cdot h')\cdot\mathbb{E}_{y\in\mathbb{F}_p}\prod_{\nu\in\{0,1\}^{k-1}}\overline{f}_{\nu\cup\{1\}}^{(\nu)}(y+\nu\cdot h')\right)$$

replacing the variable h_k by $y = x + h_k$. The square of this is, by Cauchy-Schwarz,

$$\le \prod_{j=0}^{1}\mathbb{E}_{h_1,\dots,h_{k-1}\in\mathbb{F}_p}\left|\mathbb{E}_{x\in\mathbb{F}_p}\prod_{\nu\in\{0,1\}^{k-1}} f_{\nu\cup\{j\}}^{(\nu)}(x+\nu\cdot h')\right|^2$$

$$\le \prod_{j=0}^{1}\mathbb{E}_{x,h_1,\dots,h_k\in\mathbb{F}_p}\prod_{\nu\in\{0,1\}^{k-1}} f_{\nu\cup\{j\}}^{(\nu)}(x+\nu\cdot h')\overline{f}_{\nu\cup\{j\}}^{(\nu)}(x+\nu\cdot h'+h_k)$$

by letting the second variable be $x+h_k$ when we expand the square out. The result follows from the induction hypothesis.

Corollary 8.3. $\|f\|_{U^1(G)} \le \|f\|_{U^2(G)} \le \|f\|_{U^3(G)} \le \dots$.

Proof. If $f_{\nu\cup\{0\}} = f$ and $f_{\nu\cup\{1\}} = 1$ then Proposition 8.4 gives that $\|f\|_{U^{k-1}(G)} \le \|f\|_{U^k(G)}$.

The connection between arithmetic progressions and Gowers' norms, that we saw for the U^2-norm in the previous section, will be proved in some generality. The key result is to show that we can express the count for the number of k-term arithmetic progressions in certain sets in terms of all of the vertices of a $(k-1)$-dimensional parallelipiped being in one of the sets.

The Generalized Von Neumann Theorem. *Suppose that each* $|g_j(x)| \le 1$. *For any distinct* $c_1, c_2, \dots, c_k$ *we have*

$$\left| \mathbb{E}_{a,d\in\mathbb{F}_p} \prod_{j=1}^{k} g_j(a + c_j d) \right| \le \|g_k\|_{U^{k-1}(G)}.$$

Proof. By induction on $k \ge 2$. For $k = 2$ the left side is just the product of two independent sums, that is it equals $\prod_{j=1}^{2} |\mathbb{E}_{m\in\mathbb{F}_p} g_j(m)|$. Now, by Cauchying we have

$$|\mathbb{E}_{m\in\mathbb{F}_p} g(m)|^2 = \mathbb{E}_{m,n\in\mathbb{F}_p} g(m)\overline{g}(n) = \mathbb{E}_{m,h\in\mathbb{F}_p} g(m)\overline{g}(m+h) = \|g\|^2_{U^1(G)},$$

writing $n = m + h$. The result follows since each $\|g_j\|_{U^1(G)} \le 1$.

For $k \ge 3$ the proof is more interesting. The left side is $\le \mathbb{E}_{a\in\mathbb{F}_p} |\mathbb{E}_{d\in\mathbb{F}_p} \prod_{j=2}^{k} g_j(a+c_j d)|$ since each $|g_1(a)| \le 1$. Cauchying we see that the square is

$$\le \mathbb{E}_{a\in\mathbb{F}_p} \mathbb{E}_{d,D\in\mathbb{F}_p} \prod_{j=2}^{k} g_j(a + c_j d)\overline{g}_j(a + c_j D).$$

We now change variables: Let $x = a + c_k d$ and $h = c_k(D - d)$. Then let $\gamma_j = c_j - c_k$ and $\rho_j = c_j/c_k$, so that $g_j(a+c_j d)\overline{g}_j(a+c_j D) = g_j(x+\gamma_j d)\overline{g}_j(x+\gamma_j d+\rho_j h) = \Delta_{\rho_j h} g_j(x+\gamma_j d)$. Therefore the above is

$$\mathbb{E}_{h\in\mathbb{F}_p} \mathbb{E}_{x,d\in\mathbb{F}_p} \prod_{j=2}^{k} \Delta_{\rho_j h} g_j(x + \gamma_j d).$$

We now use the induction hypothesis, for each h, since we now have the product of $k - 1$ functions, to obtain an upper bound of

$$\mathbb{E}_{h\in\mathbb{F}_p} \|\Delta_h g_k\|_{U^{k-2}(G)},$$

since $\rho_k = 1$. We now Cauchy this $k - 2$ times to obtain

$$\left| \mathbb{E}_{a,d\in\mathbb{F}_p} \prod_{j=1}^{k} g_j(a + c_j d) \right|^{2^{k-1}} \le \mathbb{E}_{h\in\mathbb{F}_p} \|\Delta_h g_k\|^{2^{k-2}}_{U^{k-2}(G)} = \|g_k\|^{2^{k-1}}_{U^{k-1}(G)}$$

by (8.4), which is the result.

The U^{k-1} Gowers' norm and k-term arithmetic progressions.

At the end of §8.1 we saw that when considering arithmetic progressions it is typographically easier to consider "balanced functions"; that is f for which $\hat{f}(0) = 0$. Let us see how this works in this more general context:

Theorem 8.5. *Let $A_j, 1 \le j \le k$ be given subsets of $\mathbb{F}_p$ of size $\delta_j p$, and define $f_j(x) = A_j(x) - \delta_j$. Then*

$$\left|\mathbb{E}_{a,d\in\mathbb{F}_p} A_1(a+d)A_2(a+2d)\dots A_k(a+kd) - \delta_1\dots\delta_k\right| < \prod_j(1+\delta_j)\ \max_j \|f_j\|_{U^{k-1}(\mathbb{F}_p)}.$$

There is a particular case of interest: If $A_j = A$ for all but at most two values of j then the upper bound can be taken to be $< \prod_j(1+\delta_j)\ \|f_A\|_{U^{k-1}(\mathbb{F}_p)}$.

Proof. We have that

$$\mathbb{E}_{a,d\in\mathbb{F}_p}\left(\prod_j A_j(a+jd)\right) - \delta_1\dots\delta_k = \sum_{\substack{J\subset\{1,\dots,k\}\\ J\neq\emptyset}}\left(\prod_{i\notin J}\delta_i\right) E_{a,d\in\mathbb{F}_p}\left(\prod_{j\in J} f_j(a+jd)\right).$$

By the Generalized Von Neumann Theorem this is, in absolute value

$$\le \sum_{\substack{J\subset\{1,\dots,k\}\\ J\neq\emptyset}}\left(\prod_{i\notin J}\delta_i\right)\ \min_{j\in J}\|f_j\|_{U^{|J|-1}(G)}.$$

Now each $\delta_j \le 1$, so the result follows from Corollary 8.3.

For the second part of the result, we note that by definition $\|f_j\|_{U^0} = \|f_j\|_{U^1} = 0$, since $\mathbb{E}_{x\in\mathbb{F}_p} f_j(x) = 0$. Now if J has more than two elements then one of the $A_j, j \in J$ must be A. The result follows.

The reason for the sequence of Gowers' norms.

The idea is that if $\|f_A\|_{U^k}$ is small then A has the expected number of $(k+1)$-term arithmetic progressions. We now construct an example of A such that $\|f_A\|_{U^k}$ is small and A has the expected number of j-term arithmetic progressions for each $j,\ 3 \le j \le k+1$, but that A has significantly more $(k+2)$-term arithmetic progressions than expected.

First though we prove the following result on exponential sums:

Lemma 4.1.** *For any polynomial $f(x_1,\dots,x_m) \in \mathbb{F}_p[x_1,\dots,x_m]$ of degree d with $p > d \ge 1$, there are $\le dp^{m-1}$ solutions of $f(x_1,\dots,x_m) = 0$. Moreover*

$$\left|\sum_{x_1,\dots,x_m\in\mathbb{F}_p} e\left(\frac{f(x_1,\dots,x_m)}{p}\right)\right| \ll_{d,k} p^{m(1-1/2^{d-1})}.$$

Proof. Throughout we shall let x_1^k be the highest power of any variable in f, for some $k \ge 1$, and suppose that this appears in f as $x_1^k g(x_2,\dots,x_m)$ for some polynomial g of degree $\le d-k$.

We begin by proving the first result by induction. For $m = 1$ the result is the fundamental theorem of algebra. For more variables let $S := \{(x_2,\dots,x_m) :\ g(x_2,\dots,x_m) =$

0}. If $(x_2,\dots,x_m)\notin S$ then there are $\le k$ values of x_1 for which $f(x_1,\dots,x_m)=0$. There are $\le p|S|$ solutions of $f(x_1,\dots,x_m)=0$ with $(x_2,\dots,x_m)\in S$. Hence the total number of solutions is $\le kp^{m-1}+p|S|\le kp^{m-1}+p(d-k)p^{m-2}$, and the result follows.

Now for the second part of the lemma, note that there are $\le (d-k)p^{m-1}$ choices of $(x_1,\dots,x_m)$ for which $g(x_2,\dots,x_m)=0$; each of these terms we bound by 1. Otherwise we apply Lemma 4.1* to bound the sum over x_1, so that in total our bound is $\le (d-k)p^{m-1}+2p^{m-1/2^{k-1}}$, and the result follows.

Example. *Let $A=A_\delta:=\{a\le p:\ |(a^k)_p|\le D\}$, where $D=[\delta p/2]$. We will prove that $\|f_A\|_{U^d}\ll 1/p^{d/2^{d+k}}$ if $d\le k$, and $\|f_A\|_{U^{k+1}}\ge\delta$ if $\delta\le 1/2$ and p is sufficiently large.*

Proof. Let $c_0=0$ and $c_j:=\sum_{d=-D}^{D} e\left(\frac{-jd}{p}\right)$ if $j\ne 0$ so that

$$f_A(x)=\mathbb{E}_{j\in\mathbb{F}_p}c_j\ e\left(\frac{jx^k}{p}\right).$$

Let $\sigma(\omega)=1$ if $\sum_i\omega_i$ is even, and $\sigma(\omega)=-1$ if $\sum_i\omega_i$ is odd, so that

$$\|f_A\|_{U^d}^{2^d}:=\mathbb{E}_{j_\omega\in\mathbb{F}_p,\omega\in\{0,1\}^d}\prod_{\omega\in\{0,1\}^d}c_{j_\omega}^{(\omega)}\ \mathbb{E}_{x,h_1,\dots,h_d\in\mathbb{F}_p}e\left(\frac{\sum_{\omega\in\{0,1\}^d}j_\omega\sigma(\omega)(x+\omega\cdot h)^k}{p}\right)$$

By Lemma 4.1**, if the polynomial $\sum_{\omega\in\{0,1\}^d}j_\omega\sigma(\omega)(x+\omega\cdot h)^k$ is not identically zero then the last expectation is $\ll p^{-(d+1)/2^{k-1}}$. Taking absolute values, the sum over all such terms, is bounded by this multiplied by $\le|\mathbb{E}_{j\in\mathbb{F}_p}|c_j||^{2^d}$, and

$$\mathbb{E}_{j\in\mathbb{F}_p}|c_j|\ll E_{j\in\mathbb{F}_p}\min\left\{D,\frac{1}{\|j/p\|}\right\}\ll\log p$$

as in (8.3b). Hence the contribution is $\ll(C\log p)^{2^d}/p^{(d+1)/2^{k-1}}\ll 1/p^{d/2^k}$.

We will now prove that if $\sum_{\omega\in\{0,1\}^d}j_\omega\sigma(\omega)(x+\omega\cdot h)^k\equiv 0$, where $d\le k$ then each $j_\omega=0$, and these terms do not contribute to our exponential sum (since $c_0=0$), so we deduce our claim for $d\le k$. Now, the coefficient of $h_1\dots h_d^{k+1-d}$ is $\frac{k!}{(k+1-d)!}j_{(1,\dots,1)}\sigma((1,\dots,1))$ since this is the only term which contains all the h_i. But then $j_{(1,\dots,1)}=0$. The coefficient of a monomial where all the h_is appear, except h_d, is a linear combination of $j_{(1,\dots,1,1)}$ and $j_{(1,\dots,1,0)}$, each with non-zero coefficients, and so $j_{(1,\dots,1,0)}=0$ (since $j_{(1,\dots,1,1)}=0$). Similarly each $j_\omega=0$ if exactly one coordinate of ω equals 0. We now consider the coefficients of monomials containing all but two of our variables, and deduce that $j_\omega=0$ if exactly two coordinates of ω equals 0. Continuing by induction on the number of zero co-ordinates of ω we deduce that each $j_\omega=0$, as claimed.

Now if $d=k+1$ then the above argument does not start in the same way. Indeed the coefficient of $xh_1\dots h_k$ is $(-1)^{d+1}d!(j_{(1,\dots,1,1)}-j_{(1,\dots,1,0)})$, and hence $j_{(1,\dots,1,0)}=j_{(1,\dots,1,1)}$.

If we write $j = j_{(1,\dots,1,1)}$ then the above induction hypothesis yields that $j_\omega = j$ for all ω. Hence we get scalar multiples of the identity

$$\sum_{\omega\in\{0,1\}^{k+1}} \sigma(\omega)(x+\omega\cdot h)^k = 0.$$

The contribution of these terms is

$$\sum_{j\in\mathbb{F}_p} \left(\frac{|c_j|}{p}\right)^{2^d} \ge 2\sum_{1\le j\le p/6D} (D/p)^{2^d} = \frac{1}{3}(\delta/2)^{2^d-1}$$

if $\delta < 1/2$, since $c_j = \sum_{d=-D}^{D} \cos\left(\frac{2\pi jd}{p}\right) \ge D$ when $1 \le |j| \le p/6D$, and the result follows.

Exercise: Be a little more precise. First show that $c_j = \sin(\frac{\pi j(2D+1)}{p})/\sin(\frac{\pi j}{p})$. Then, for bounded j, approximate the denominator, and give a lower bound on the resulting sum.

Why are k-term arithmetic progressions controlled by $(k-1)$-dimensional parallellipipeds?. This is not an easy question to answer. One viewpoint is that, parallellipipeds are a generalization of arithmetic progressions with more variables added (which usually makes something easier to estimate). Thus for 3-term arithmetic progressions we are looking for solutions to $a + c = b + b$ with $a, b, c \in A$, whereas for the U^2-norm we want solutions to $a + c = b_1 + b_2$ with $a, b_1, b_2, c \in A$; the arithmetic progression is the special case $b_1 = b_2$. This viewpoint generalizes easily: The $(k-1)$-dimensional parallellipiped one requires $a + \omega\cdot h \in A$ for all $\omega \in \{0,1\}^{k-1}$, where $h = (h_1, \dots, h_{k-1})$. The k-term arithmetic progression $a + jd$, $j = 0, 1, \dots k-1$ is simply the special case $h_1 = h_2 = \dots = h_k = h$.

The plan for k-term arithmetic progressions.

Corollary 8.6. *Suppose $A \subset [1, p-1]$ has δp elements, and does not contain any non-trivial k-term arithmetic progressions. Then either there exists j for which $S_j := \{a \in A : \frac{j-1}{2k-1}\ p < a < \frac{j}{2k-1}\ p\}$ contains $\ge (1 + \frac{1}{4k-4})\delta\frac{p}{2k-1}$ elements, or $\|f_A\|_{U^{k-1}(\mathbb{F}_p)} > \delta^k/2^{k+2}$.*

Proof. Let $A_j = A$ for $1 \le j \le k-2$, with $A_{k-1} = S_{2k-2}$ and $A_k = S_{2k-1}$. We may assume that $\delta_{k-1}, \delta_k \ge \frac{\delta}{2}$, else $|S_j| \ge (1 + \frac{1}{4k-4})\delta\frac{p}{2k-1}$ for some j. We will show that there are no k-term arithmetic progressions, mod p, with the jth term in $\overline{A}_j := \{a \pmod p : a \in A_j\}$ for each j. For if the progression is $a + jd, 1 \le j \le k$ then $d = (a+kd) - (a+(k-1)d) \in (0, \frac{2}{2k-1}p)$. But then $a + jd = (a+kd) - (k-j)\cdot d$ so that $p - 0 > a + jd > \frac{2k-2}{2k-1}\ p - (k-j)\cdot\frac{2}{2k-1}p = \frac{2(j-1)}{2k-1}\ p > 0$, for $1 \le j \le k-2$. Hence the arithmetic progression mod p, is also an arithmetic progression in A, contradicting the hypothesis. We now apply the second part of Theorem 8.5 to the sets $\overline{A}_j$ to obtain the result.

Strategy for proving Szemerédi's Theorem:. We wish to show that for given $\delta > 0$ and integer $k \ge 3$, there exists a constant $N_{k,\delta}$ such that if $N \ge N_{k,\delta}$ then any subset A of $[1, N]$ with δN elements, contains a non-trivial k-term arithmetic progression. We prove

this for fixed k first for δ close to 1, and then for smaller and smaller δ. If A is a subset of the integers in $[1, N]$ with $\geq (1 - 1/k)N + 1$ elements then A contains k consecutive elements, and hence a k-term arithmetic progression. So now assume $0 < \delta \leq 1 - 1/k$, and that the result is proved for $\delta + \epsilon$.

Let us suppose that A is a subset of the integers in $[1, N]$ with δN elements, which does not contain a non-trivial k term arithmetic progression. Let p be the smallest prime $> N$; we know that $p \leq N + O((N/\log N)$ by the prime number theorem, so that $A \subset [1, p-1]$ with $\{\delta + o(1)\}p$ elements, and does not contain any non-trivial k-term arithmetic progression. We need to prove the following steps:
I) Either there exists j for which $S_j := \{a \in A : \frac{j-1}{2k-1}\ p < a < \frac{j}{2k-1}\ p\}$ contains $\geq (1+\frac{1}{4k-4})\delta M$ elements where $M := [p/(2k-1)]$, or $\|f_A\|_{U^{k-1}(\mathbb{F}_p)} > \delta^k/2^{k+2}$. (Corollary 8.6).

Under our hypothesis the first case cannot hold since $B = \{1 \leq n \leq M : [\frac{j-1}{2k-1}\ p]+n \in A\}$ has $\geq (1 + \frac{1}{4k-4})\delta M$ elements, so contains a k term arithmetic progression. But this implies that A contains a k term arithmetic progression, which is a contradiction. Hence using (I) we can assume that $\|f_A\|_{U^{k-1}(\mathbb{F}_p)} \gg 1$.

II) If $\|f_A\|_{U^{k-1}(\mathbb{F}_p)} \gg 1$ then there exists a polynomial $\phi(x)$ of degree $\leq k-2$ such that $f_A(x)$ "correlates" with $e^{i\phi(x)}$. (The Inverse Gowers' U^k-norm conjecture.)

III) For each integer $d \geq 0$ there exist constants $\gamma, \eta > 0$ that depend only on d, such that if there exists a polynomial $\phi(x)$ of degree d for which $f_A(x)$ "correlates" with $e^{i\phi(x)}$ then there exists an arithmetic progression $Q \subset [1, p-1]$ of size $> p^\gamma$ such that $Q \cap A$ has $> (\delta + \eta)|Q|$ elements.

If $Q = \{u + nv : 1 \leq n \leq N\}$ then $B := \{n \leq N : \ u + nv \in A\} \subset [1, N]$ has $> (\delta + \eta)N$ elements and so contains a non-trivial k-term arithmetic progression. But this implies that A contains a k term arithmetic progression, which is a contradiction.

We will next prove (III), indeed a generalization of (III), which is a fairly simple application of Weyl's Theorem (Theorem 4.2). It is step (II) that is difficult, and has only recently been established, and even then in a rather more complicated form.

Translating correlations into higher density on subprogressions

The main result in this section is the following:

Theorem 7*. *Suppose that $A \subset \mathbb{F}_p$, and that there is a partition of $\mathbb{F}_p$ into arithmetic progressions $P_1, P_2, \dots, P_q$ of P, each of length $\gg p^\gamma$, and polynomials $\phi_1, \phi_2, \dots, \phi_q$ of degree $< k$ such that*

$$\sum_{j=1}^{q} \left| \sum_{x \in P_j} f_A(x) e\left(\frac{\phi_j(x)}{p}\right) \right| \geq \eta p.$$

Then there exists an arithmetic progression $Q \subset [1, p-1]$ of length $\geq p^\theta$ such that $|A \cap Q| \geq \{\delta + \frac{\eta}{4}\}|Q|$. Here $\theta > 0$ depends only on γ and k.

For any set $S \subset \mathbb{F}_p$ define $\mathrm{diam}(S) = \max\{p\|\frac{x-y}{p}\| : x, y \in S\}$.

Lemma 7.11. *Suppose that positive integers $\ell, m, r \le p$ are given for which $\ell \le (m/r)^{1/3}$. If P is a $\mathbb{F}_p$-arithmetic progression of length m and $\phi : \mathbb{F}_p \to \mathbb{F}_p$ is a linear function then P can be partitioned into subprogressions $P_i, i \ge 1$ of lengths ℓ or $\ell - 1$, such that* $\operatorname{diam}(\phi(P_i)) \le p/r$ *for each i.*

Proof. Suppose that $P = \{a + id : \ 0 \le i \le m-1\}$. By the pigeonhole principle, there exists $0 \le i < j \le r\ell$ such that $|\phi(a+jd)-\phi(a+id)| \le p/r\ell$. As ϕ is linear we deduce that for $k = j-i \le r\ell$ such that $|\phi(kd)-\phi(0)| = |\phi(a+jd)-\phi(a+id)| \le p/r\ell$. We will partition P up into congruence classes mod k, each of which contains at least $m/k \ge m/r\ell \ge \ell^2$ elements, and so can be partitioned into subprogressions, each of length ℓ or $\ell - 1$. If $Q \subset \{a + bd, a + bd + dk, \dots, a + bd + (\ell-1)dk\}$ is such a subprogression then there exists $0 \le u < v \le \ell - 1$ such that

$$\operatorname{diam}(\phi(Q)) = |\phi(a + bd + vdk) - \phi(a + bd + udk)| \le |v - u||\phi(dk) - \phi(0)| < p/r.$$

The result follows.

Lemma 7.12$^+$. *Let $\phi : \mathbb{F}_p \to \mathbb{F}_p$ be a polynomial of degree k, and let P be a $\mathbb{F}_p$-arithmetic progression of length m. Then for any $\ell \le m^{\epsilon_k}$, P can be partitioned into subprogressions, P_i, $i \ge 1$, of length $\ell + O(1)$, with* $\operatorname{diam}(\phi(P_i)) \ll p/m^{\epsilon_k}$.
We can take $\epsilon_k = 1/(3^{k-1}2^{\frac{k^2+k}{2}+1}k!^2)$

Proof. We proceed by induction on k. Lemma 7.11 gives our result for $k = 1$ with $\epsilon_1 = 1/4$. Now suppose $k \ge 2$, and that $P = \{u + iv : \ 0 \le i \le m-1\}$, with $\phi(u + iv) = ai^k + \dots$. Select $D = m^{1/2}$ and $n = m^{1/3kK}$ where $K = k2^k$ $(> K(k) := (k-1)2^k + 2k - 1)$.

Taking $\alpha = a/p$ in Weyl's Theorem (Theorem 4.2), we know that there exists $d \le D$ such that $\|ad^k/p\| \ll p/D^{1/K}$. We partition P into subprogressions $P_h = \{u + (h + jd)v : 0 \le j < m/d\}$, for $0 \le h \le d-1$. We split these into progressions of length n: that is

$$P_{h,r} := \{u + (h + (rn + i)d)v : \ 0 \le i \le n-1\} \text{ for } 0 \le r < m/dn\}.$$

Now $\phi(u + (h + (rn + i)d)v) = ad^k i^k + g_{h,r}(u + (h + (rn + i)d)v)$ where $g_{h,r}$ is some polynomial of degree $k-1$. By the induction hypothesis each $P_{h,r}$ may be partitioned into subprogressions $P_{h,r,j}$ of length $\ell + O(1)$, for any given $\ell \le n^{\epsilon_{k-1}} = m^{\epsilon_k}$, such that $\operatorname{diam}(g_{h,r}(P_{h,r,j})) \ll p/n^{\epsilon_{k-1}}$. Therefore

$$\operatorname{diam}(\phi(P_{h,r,j})) \le \left\| \frac{ad^k n^k}{p} \right\| + \operatorname{diam}(g_{h,r}(P_{h,r,j})) \ll \frac{pn^k}{D^{1/K}} + \frac{p}{n^{\epsilon_{k-1}}} = \frac{p}{m^{1/6K}} + \frac{p}{m^{\epsilon_k}} \ll \frac{p}{m^{\epsilon_k}}.$$

Lemma 7.13. *Let $\phi : \mathbb{F}_p \to \mathbb{F}_p$ be a polynomial of degree k, and let P be a $\mathbb{F}_p$-arithmetic progression of length m. For any $\ell \le m^{\epsilon_k}$, we can partition P into subprogressions P_j, $1 \le j \le J$, of lengths $\ell + O(1)$, such that if $|f(x)| \le 1$ for all x then*

$$\sum_{j=1}^{J} \Big| \sum_{x \in P_j} f(x) \Big| \ge \left| \sum_{x \in P} f(x) e\left(\frac{\phi(x)}{p}\right) \right| + O(m^{1-\epsilon_k}).$$

Proof. By Lemma 7.12, we have $\operatorname{diam}(\phi(P_j)) \ll p/m^{\epsilon_k}$. Now if $x, y \in P_j$ then

$$\left|e\left(\frac{\phi(x)}{p}\right) - e\left(\frac{\phi(y)}{p}\right)\right| = \left|e\left(\frac{\phi(x)-\phi(y)}{p}\right) - 1\right| \le \left|e\left(\frac{\operatorname{diam}(\phi(P_j))}{p}\right) - 1\right| \ll \frac{\operatorname{diam}(\phi(P_j))}{p} \ll \frac{1}{m^{\epsilon_k}}.$$

Therefore $|\sum_{x\in P_j} f(x)| = |\sum_{x\in P_j} f(x)e(\phi(x)/p)| + O(\ell/m^{\epsilon_k})$; and so, by the triangle inequality,

$$\left|\sum_{x\in P} f(x)e\left(\frac{\phi(x)}{p}\right)\right| \le \sum_{j=1}^{J}\left|\sum_{x\in P_j} f(x)e\left(\frac{\phi(x)}{p}\right)\right| \le \sum_{j=1}^{J}\left|\sum_{x\in P_j} f(x)\right| + O(m^{1-\epsilon_k}).$$

Proof of Theorem 7.* Let $\theta = \gamma\epsilon_{k-1}/5$ and $\ell = 20p^{4\theta}$. We begin by assuming the hypothesis for any f for which $|f(x)| \le 1$ for all x, and $\hat{f}(0) = 0$. By Lemma 7.13 we can partition each P_j into subprogressions $P_{j,i}$, $1 \le i \le I$, of lengths $\ell + O(1)$, such that

$$\sum_{i=1}^{I}\Big|\sum_{x\in P_{j,i}} f(x)\Big| \ge \left|\sum_{x\in P_j} f(x)e\left(\frac{\phi_j(x)}{p}\right)\right| + O(|P_j|/p^{4\theta}).$$

If we now sum up over all j, we get a partition of $\mathbb{F}_p$ into subprogressions $P_{j,i}$ of lengths $\ell + O(1)$, such that

$$\sum_{\substack{1\le j\le J\\ 1\le i\le I}}\Big|\sum_{x\in P_{j,i}} f(x)\Big| \ge \eta p + O(p^{1-4\theta}).$$

Now $\sum_{j,i}\sum_{x\in P_{j,i}} f(x) = \sum_{x\in\mathbb{F}_p} f(x) = \hat{f}(0) = 0$, so adding these two equations yields

$$\sum_{\substack{1\le j\le J\\ 1\le i\le I}} \max\left\{\sum_{x\in P_{j,i}} f(x), 0\right\} \ge \frac{\eta}{2}p + O(p^{1-4\theta}) \ge \frac{\eta}{3}p.$$

Therefore there exists i, j such that

$$\sum_{x\in P_{j,i}} f(x) \ge \frac{\eta}{3}\,|P_{j,i}|.$$

Now if $f = f_A$ then this tells us that $|P_{j,i} \cap A| \ge \{\delta + \frac{\eta}{3}\}|P_{j,i}|$. Finally by Lemma 3.3b there are arithmetic progressions $Q_1, Q_2, \dots, Q_k \subset [1, p-1]$, of length $> p^\theta$, such that $Q_1, Q_2, \dots, Q_k \pmod p$ is a partition of $P_{j,i}$ less no more than $|P_{j,i}|^{3/4}$ elements. Hence the result follows for at least one of the Q_i.

Sets with large Gowers' U^3-norm

In this section we develop the theory of sets A, of density δ, for which f_A has a large Gowers' $U^3(\mathbb{F}_p)$-norm. Our goal is to show that A intersects a $\mathbb{Z}$-arithmetic progression $P \subset \{1, 2, \dots, N\}$ of size at least N^d and such that $|A \cap P| \ge (\delta + \varepsilon)|P|$ where ε and d depend only on α and δ.

We begin with a technical lemma that hints at how quadratic phases enter the picture:

Lemma 7.10.1. *If each $|f(x)|, |g(x)| \le 1$, and $A \subset \mathbb{F}_p$ then*

$$\sum_{a\in A}\Big|\sum_x f(x)\overline{g(x+a)}\ e\left(\frac{(2\lambda a+\mu)x}{p}\right)\Big|^2 \le p\sum_x \max_{r\in\mathbb{F}_p}\left|\sum_{w\in x-A} g(w)e\left(\frac{rw-\lambda w^2}{p}\right)\right|.$$

Proof. Taking $F(x) = f(x)e(-\frac{\lambda x^2-\mu x}{p})$ and $G(x) = g(x)e(-\frac{\lambda x^2}{p})$ the left-hand side is

$$\begin{aligned}\sum_{a\in A}\Big|\sum_x F(x)\overline{G(x+a)}\Big|^2 &= \sum_{a\in A}\sum_{x,y}\overline{F(x)}G(x+a)F(y)\overline{G(y+a)}\\ &= \sum_x \overline{F(x)}\sum_{a\in A}\sum_b G(x+a)F(x+b)\overline{G(x+a+b)}\\ &= \frac{1}{p}\sum_x \overline{F(x)}\sum_m e\left(\frac{-xm}{p}\right)\sum_{a\in A} G(x+a)e\left(\frac{(x+a)m}{p}\right)\hat{F}(m)\hat{\overline{G}}(m)\end{aligned}$$

replacing y by $x+b$, and then taking the Fourier transforms. Taking absolute values, this is

$$\le \frac{1}{p}\sum_x \max_{r\in\mathbb{F}_p}\left|\sum_{a\in A} G(x+a)e\left(\frac{(x+a)r}{p}\right)\right|\ \sum_m |\hat{F}(m)\hat{G}(m)|$$

as each $|F(x)| \le 1$, and the result follows from Cauchying and using Parseval.

Before this is used we see how a large U^3-norm implies that there is an arithmetic progression with an extraordinary property. It is in the proof of this proposition that we see the key tools of additive combinatorics, the Balog-Szemerédi-Gowers lemma in conjunction with the Freiman-Ruzsa theorem

Proposition 7.7. *Let $\alpha = \|f\|^8_{U^3(G)}$. There exist $\eta, \gamma > 0$, depending only on α, and an $\mathbb{F}_p$-arithmetic progression P of length at least p^γ, and integers λ and μ for which*

$$\sum_{h\in P} |\widehat{\Delta_h f}(2\lambda h+\mu)|^2 \ge \eta\ p^2\ |P|.$$

Proof. Let B be the set of $h \in \mathbb{F}_p$ for which $\|\Delta_h f\|^4_{U^2} \ge \alpha/2$, so that $|B|\cdot 1 + p\cdot\alpha/2 \ge \sum_h \|\Delta_h f\|^4_{U^2} = \alpha p$, and hence $|B| \ge \alpha p/2$. If $\phi(h)$ is chosen so that $|\widehat{\Delta_h f}(\phi(h))|$ is maximized, then $|\widehat{\Delta_h f}(\phi(h))|^2 \ge \|\Delta_h f\|^4_{U^2}\ p^2$ by Lemma 8.1, and therefore

$$\sum_{h\in B} |\widehat{\Delta_h f}(\phi(h))|^2 \ge |B|\cdot(\alpha/2)\cdot p^2 \ge \alpha^2 p^3/4.$$

Now

$$\sum_{h\in B}|\widehat{\Delta_h f}(\phi(h))|^2 = \sum_{h\in B}\sum_{r,x}\Delta_h f(r)\overline{\Delta_h f(x)}e\left(\frac{r-x}{p}\phi(h)\right)$$
$$= \sum_{h\in B}\sum_{k,r}\Delta_{h,k}f(r)e\left(-\frac{k}{p}\phi(h)\right)$$
$$\leq \sum_{k,r}\Big|\sum_{h\in B}\overline{\Delta_k f(r+h)}e\left(-\frac{k}{p}\phi(h)\right)\Big|,$$

writing $x = r+k$, since $|\Delta_k f(r)| \leq 1$. The square of this is, by Cauchy-Schwarz,

$$\leq p^2\sum_{k,r}\Big|\sum_{h\in B}e\left(\frac{k}{p}\phi(h)\right)\ \Delta_k f(r+h)\Big|^2 \leq p^5\sum_k \|\Delta_k f\|_{U^2}^2\|\beta^k\|_{U^2}^2$$

by applying Lemma 7.1 to this last sum with $f(-m) = \beta(m)^k$ where $\beta(m) = e\left(\frac{\phi(m)}{p}\right)$ if $m \in B$ and 0 otherwise, and $\overline{g(n)} = \Delta_k f(n)$. The square of this is, by Cauchy-Schwarz,

$$\leq p^{10}\sum_k \|\Delta_k f\|_{U^2}^4\sum_k\|\beta^k\|_{U^2}^4 = p^7\|f\|_{U^3}^8\sum_k\sum_{r\in\mathbb{F}_p}|\widehat{\beta^k}(r)|^4.$$

Now $\widehat{\beta^k}(r) = \sum_{n\in B}e\left(\frac{k\phi(n)+rn}{p}\right)$, so expanding the last sum yields

$$\sum_{k,r}\sum_{a,b,c,d\in B}e\left(\frac{k(\phi(a)+\phi(b)-\phi(c)-\phi(d))+r(a+b-c-d)}{p}\right)$$

which is p^2 times the number of solutions of $a+b=c+d$ and $\phi(a)+\phi(b) = \phi(c)+\phi(d)$ with $a,b,c,d \in B$.

Collecting up the estimates above, we find that we have proved that there are at least $\alpha^7p^3/2^8$ quadruples $(a,b,c,d) \in B^4$ for which $a+b=c+d$ and $\phi(a)+\phi(b) = \phi(c)+\phi(d)$. Then, by Corollary 6.8, there exist $\eta,\gamma > 0$, depending only on α, and an $\mathbb{F}_p$-arithmetic progression P of length at least p^γ, and integers λ and μ for which $\phi(h) = e(2\lambda h+\mu)$ for at least $\eta|P|$ values of $h \in B\cap P$. Therefore

$$\sum_{h\in P}|\widehat{\Delta_h f}(2\lambda h+\mu)|^2 \geq \sum_{h\in B\cap P}|\widehat{\Delta_h f}(\phi(h))|^2 \geq |B\cap P|\ (\alpha/2)\ p^2,$$

and the result follows (replacing η in Corollary 6.8 by $\eta/(\alpha/2)$).

In the next result we see how we use Lemma 7.10.1 allows us to make the transition from an arithmetic progression with an extraordinary property, to a partition of $\mathbb{F}_p$ into arithmetic progressions each of which correlates with the exponential of a quadratic polynomial.

Lemma 7.10.2. *Suppose that P is an arithmetic progression in $\mathbb{F}_p$ for which*

$$\sum_{h\in P} |\widehat{\Delta_h f}(2\lambda h+\mu)|^2 \ge \eta p^2|P|$$

Then there exists a partition of $\mathbb{F}_p$ into translates $P_1, P_2, \dots, P_{q-1}$ of P or P with an endpoint removed, such that for each i we can find $r_i \in \mathbb{F}_p$ so that

$$\sum_{i=0}^{q-1} \left| \sum_{x\in P_i} f(x) e\left(\frac{r_i x - \lambda x^2}{N}\right)\right| \ge q(\eta|P|-1).$$

Proof. We take $g=f$ and $A=P$ in Lemma 7.10.1 to deduce that for each x there exists r_x for which

$$\eta p|P| \le \frac{1}{p}\sum_{h\in P} |\widehat{\Delta_h f}(2\lambda h+\mu)|^2 \le \sum_x \left| \sum_{w\in x-P} f(w) e\left(\frac{r_x w - \lambda w^2}{p}\right)\right|.$$

Suppose that $P=\{a+id : 0\le i\le m\}$ where $p=qm+s$ with $0\le s\le m-1$. Let $v_j=(m+1)j$ for $0\le j\le s$, and $v_j = mj+s$ for $s\le j\le q$. Define $Q_j = [v_j, v_{j+1})$, so that $y+Q_0 d, y+Q_1 d, \dots, y+Q_{q-1}d$ is a partition of $\mathbb{F}_p$ for any y. Moreover $\bigcup_y \{y+Q_0 d, y+Q_1 d, \dots, y+Q_{q-1}d\}$ yields every translate of P exactly s times, and every translate minus its last point $q-s$ times. Therefore

$$\sum_y \sum_{j=0}^{q-1} \left| \sum_{w\in y-Q_j d} f(w) e\left(\frac{r_{y+a-dv_j} w - \lambda w^2}{N}\right)\right| \ge \sum_x q \left| \sum_{w\in x-P} f(w) e\left(\frac{r_x w - \lambda w^2}{p}\right)\right| - (q-s)$$

which is $\ge q\eta p|P| - p(q-s)$. We select y for the summand on the left side is maximal, and then let $P_j = y - Q_j d$ and $r_j = r_{y+a-dv_j}$, to obtain the result.

Pointing the pieces together.

Suppose $A \subset [1, p-1]$ has δp elements, and does not contain any non-trivial 4-term arithmetic progressions. By Corollary 8.6 there either exists j for which $S_j := \{a \in A : \frac{j-1}{7}\ p < a < \frac{j}{7}\ p\}$ contains $\geq (1 + \frac{1}{12})\delta\frac{p}{7}$ elements, or the reduction of A mod p satisfies $\|f_A\|_{U^3(\mathbb{F}_p)} > \tau$ where $\tau := \delta^4/64$.

By Corollary 7.9 there exist $\eta, \gamma > 0$, depending only on δ, an $\mathbb{F}_p$-arithmetic progression P of length at least p^γ, and integers λ and μ for which

$$\sum_{h\in P} |\widehat{\Delta_h f}(2\lambda h + \mu)|^2 \geq \eta p^2 |P|.$$

By Lemma 7.10.2 there exists a partition of $\mathbb{F}_p$ into translates $P_1, P_2, \dots, P_{q-1}$ of P or P with an endpoint removed, such that for each i we can find $r_i \in \mathbb{F}_p$ so that

$$\frac{1}{q}\sum_{i=0}^{q-1} \left| \frac{1}{|P_i|} \sum_{x\in P_i} f(x) e\left(\frac{r_i x - \lambda x^2}{N}\right)\right| \geq \frac{2\eta}{3}\ .$$

Let S be the set of P_i for which

$$\left| \frac{1}{|P_i|} \sum_{x\in P_i} f(x) e\left(\frac{r_i x - \lambda x^2}{N}\right)\right| \geq \frac{\eta}{3}\ .$$

Note that $|S| \cdot 1 + q \cdot \frac{\eta}{3} \geq q \cdot \frac{2\eta}{3}$, so that $|S| \geq \frac{\eta}{3}\ q$ By Lemma 7.13 we can partition the $P_i \in S$ into subprogressions $P_{i,j}$, $1 \leq j \leq k$, of lengths ℓ or $\ell - 1$, where $\ell \asymp \eta^{16/33} p^{\gamma/33}$, such that

$$\sum_{j=1}^{k} \Big| \sum_{x\in P_{i,j}} f(x)\Big| \geq \frac{\eta m}{2}.$$

Equally partitioning the $P_i \notin S$ into subprogressions $P_{i,j}$, $1 \leq i \leq k$, of lengths ℓ or $\ell - 1$, we obtain a partition of $\mathbb{F}_p$ into arithmetic progressions $P_{i,j}$, $1 \leq i \leq q$, $1 \leq j \leq k$, of lengths ℓ or $\ell - 1$, such that

$$\sum_{i=0}^{q-1}\sum_{j=1}^{k} \Big| \sum_{x\in P_{i,j}} f(x)\Big| \geq |S| \cdot \frac{\eta m}{2} \geq \frac{\eta^2}{6}\ p.$$

Now $\sum_x f(x) = 0$ and so, adding this above, there exists i, j such that

$$\sum_{x\in P_{i,j}} f(x) \geq |S| \cdot \frac{\eta m}{2} \geq \frac{\eta^2}{12kq}\ p > \frac{\eta^2}{13}|P_{i,j}|,$$

and so $|P_{i,j} \cap A| \geq \{\delta + \frac{\eta^2}{13}\}|P_{i,j}|$. This is not quite what we want since $P_{i,j}$ is an $\mathbb{F}_p$-arithmetic progression, and we need an arithmetic progression in the integers. However by Lemma 3.3b there exists an arithmetic progression in the integers of length $\asymp \ell^{1/4}$

Boring, technical Proofs

Proof of Lemma 2.10. Assume that the result in false and consider the counterexample with $|C_1|$ minimal.

We begin by supposing that there exists $c_1 \in C_1$ such that $c_1 + H_1 \subset S_2$. Note that the elements of $c_1 + H_1$ must belong to different cosets of H_2 else $c_1 + h_1 = c_2 + h_2$ and $c_1 + h_1' = c_2 + h_2'$ and so $h_1' - h_1 = h_2' - h_2 \in H_1 \cap H_2 = \{0\}$. Therefore we may write $S_2 = ((c_1 + H_1) \cup C_2') + H_2$. Now if for each $h_1 \in H_1$ there exists $h_2 \in H_2$ such that $(c_1 + h_1 + h_2) \notin S_1$ then $|S_2 \setminus S_1| \geq |H_1|$, and thus $|S_1 \cup S_2| \geq |S_1| + |H_1|$. Hence we may assume that there exists $h_1 \in H_1$ such that $(c_1 + h_1 + H_2) \subset S_1$. But S_1 is closed under addition by elements of H_1 and so $(c_1 + H_1 + H_2) \subset S_1$, and therefore we may write $S_1 = ((c_1 + H_2) \cup C_1') + H_1$. But now $S_j = (c_1 + H_1 + H_2) \cup S_j'$ where $S_j' = C_j' + H_j$, and the result follows from the induction hypothesis.

Now, since the elements of $c_2 + H_2$ must belong to different cosets of H_1 we deduce that $|(c_2 + H_2) \cap S_1| \leq |C_1|$ and so $|S_1 \cap S_2| \leq |C_1||C_2|$. Therefore $|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2| \geq |S_1| + |S_2| - |C_1||C_2|$.

We may now assume that for every $c_1 \in C_1$ there exists $h_1 \in H_1$ such that $c_1 + h_1 \notin S_2$; and therefore $|S_1 \cup S_2| \geq |S_2| + |C_1|$. Since all of the above arguments may be made with the roles of S_1 and S_2 exchanged, we also have $|S_1 \cup S_2| \geq |S_1| + |C_2|$.

Let us suppose that $|S_j| + |H_j| - 1 \geq |S_1 \cup S_2|$ for $j = 1, 2$. The equations of the last two paragraphs imply that $|H_1| - 1 \geq |C_2|(|H_2| - |C_1|)$ and $|H_2| - 1 \geq |C_1|(|H_1| - |C_2|)$, and then $|C_1| \leq |H_2| - 1$ and $|C_2| \leq |H_1| - 1$, respectively. Since all these terms are positive these can be combined: $|H_1| - 1 \geq |C_2|(|H_2| - 1) - |C_2|(|C_1| - 1) \geq |C_2||C_1|(|H_1| - |C_2|) - |C_2|(|C_1| - 1)$, so that $(|C_1||C_2| - 1)(|C_2| + 1 - |H_1|) \geq 0$. Therefore either $|C_1| = |C_2| = 1$, or $|C_2| = |H_1| - 1$ (and $|C_1| = |H_2| - 1$ by symmetry). In the first case $|S_1 \cup S_2| = |S_j| + |H_j| - |S_1 \cap S_2|$ for each j, so we get the result, with equality if and only if $S_1 \cap S_2 \neq \emptyset$. In the second case $|S_1 \cup S_2| \geq |S_1| + |S_2| - |C_1||C_2| = |S_j| + |H_j| - 1$ for each j, so we get the result, with equality if and only if $|S_1 \cap S_2| = |C_1||C_2|$. In this situation one has that $C_1 - C_2 \subset H_2 - H_1$; and that for every $c_1 \in C_1$ there exists a unique $h_1 \in H_1$ such that $c_1 + h_1 \notin S_2$. (Go on to fully classify when one gets equality in the lemma).

References

[BC] P.T. Bateman and S. Chowla, *Averages of character sums*, Proc. Amer. Math. Soc **1** (1950), 781-787.

[D] H. Davenport, *Multiplicative number theory*, Springer Verlag, New York, 1980.

[AK] N. Alon and R. Kleitman, *Sum free Sets of Integers*, A Tribute to Paul Erdős, (eds. Baker, Bollobás, Hajnal), Cam. Univ. Press, 1990, pp. 13–26.

[1] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, Combinatorica **14** (1994), 263–268.

[BE] S. J. Benkoski and P. Erdos, Math. Comp **28** (1974), 617–623.

[2] Y. Bilu, *Structure of sets with small sumset, Structure Theory of Set Addition*, Astérisque **258** (1999), 77–108.

[3] N. N. Bogolyubov, Zap. Kafedry Mat. Fizi **4** (1939), 185.

[**] J. P. Bourgain, A Tribute to Paul Erdős, Cambridge Univ. Press, Cambridge, 1990, pp. 105–109.

[**] P. Erdős and A. Sárközy, *Arithmetic progressions in subset sums*, Disc. Math. **102** (1992), 249–264.

[4] P. Erdős and P. Turán, *On some sequences of integers*, J. London Math. Soc **11** (1936), 261–264.

[**] P. E. Fraenkel, *Integer sets with distinct subset sums*, Proc. Amer. Math. Soc **126** (1998), 3199–3200.

[**] G. A. Freiman, *New analytical results in subset sum problems*, Disc. Math. **114** (1993), 205–217.

[5] G. R. Freiman, *Foundations of a Structural Theory of Set Addition, Translations of Mathematical Monographs*, vol. 37, Amer. Math. Soc, Providence, R. I., USA.

[6] H. Fürstenburg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256.

[7] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), 529–551.

[**] R. L. Graham, B. L. Rothschild, J. H. Spencer, *Ramsey Theory*, Wiley,, 1980.

[HR] H. Halberstam, H.-E. Richert, *Sieve methods*, Academic Press.

[8] A. W. Hales, R. I. Jewett, *Regularity and positional games*, Trans. Amer. Math. Soc. **106** (1963), 222–229.

[**] Y. O. Hamidoune and J. A. D. da Silva, *Cyclic spaces for Grassman derivatives and additive theory*, Bull. London Math. Soc **26** (1994), 140–146.

[**] F. Hanson, J. M. Steele, F. Stenger, Proc. Amer. Math. Soc 66 (1977), 179–180.

[9] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc **35** (1987), 385–394.

[**] J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math **103** (1960), 63–88.

[10] N. M. Korobov, *Exponential Sums and their Applications, Mathematics and its Applications* **80** (1992), Kluwer.

[**] V. Lev, *The structure of multisets with a small number of subset sums, Structure Theory of Set Addition*, Astérisque **258** (1999), 317–321..

[**] V. Lev, *On small sumsets in abelian groups, Structure Theory of Set Addition*, Astérisque **258** (1999), 317–321.

[**] E. Lipkin, *Subset sums of sets of residues, Structure Theory of Set Addition*, Astérisque **258** (1999), 187–193.

[11] K. F. Roth, *On certain sets of integers*, J. London Math. Soc **28** (1953), 245–252.

[**] I. Ruzsa, *Arithmetic progressions in sumsets*, Acta Arith. **60** (1991), 191–202.

[12] I. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. **65** (1994), , 379–388.

[13] I. Ruzsa, *An analog of Freiman's Theorem for abelian groups, Structure Theory of Set Addition*, Astérisque **258** (1999), 323–326.

[14] S. Shelah, *Primitive recursive bounds for van der Waerden Numbers*, J. Amer. Math. Soc **1** (1988), 683–697.

[**] C. F. Siegel, *Lectures on Geometric Number Theory.*

[**] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hungar **20** (1969), , 89–104.

[**] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. Hungar **27** (1975), 299–345.

[**] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar **56** (1990), 155–158.
[**] G. Tenenbaum, *Introduction to analytic and probabilistic number theory, Cam. Studies in Advanced Math.*, vol. 46, Cam. Univ. Press, 1995.
[**] B. L. van der Waerden, *Beweis einer Baudetschen vermutung*, Nieuw Arch. Wisk **15** (1927), 212–216..
[**] R. C. Vaughan, *The Hardy-Littlewood Method, 2nd Ed. Cam. Tracts in Math.*, vol. 125, Cam. Univ. Press, 1997.
[**] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Trav. Inst. Math. Steklof **23** (1947).
[**] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Annalen **77** (1913), 313–352..