A proof of Freiman's Theorem, continued

Brad Hannigan-Daley
University of Waterloo

Freiman's Theorem

Recall that a d-dimensional *generalized arithmetic progression* (*GAP*) in an abelian group G is a subset of the form

$$Q = \{a_0 + \sum_{i=1}^{d} x_i a_i : 0 \leq x_i < n_i\}$$

for some elements $a_0, \ldots, a_k$ of G. Such a GAP is *proper* if each of those sums is distinct; equivalently, the size of the GAP is $\prod_{i=1}^{d} n_i$. Given a finite set of integers A, recall that $|A + A| \geq 2|A| - 1$ and that A is an arithmetic progression (that is, a 1-dimensional GAP) if and only if this bound is sharp. Freiman's Theorem similarly asserts that if A has a small sumset $A + A$, then A is contained in a GAP that isn't "too big" in the following sense:

Freiman's Theorem. *Let A be a finite subset of $\mathbb{Z}$ with $|A + A| \leq C|A|$. Then there exist constants d and S depending only on C such that A is contained in a GAP of dimension at most d and size at most $S|A|$.*

Using some graph theory, particularly Menger's Theorem on counting vertex-disjoint paths, we have previously proved the following result which will be used several times in the following exposition:

Plünnecke's Theorem A. *If A and B are finite sets of integers for which $|A + B| \leq C|B|$, then $|kA - \ell A| \leq C^{k+\ell}|B|$ for all integers k and ℓ.*

The particular case of this theorem that we find most useful is that if $|A + A| \leq C|A|$, we have $|kA - \ell A| \leq C^{k+\ell}|A|$ for all k and ℓ.

An analogue of Freiman's Theorem in a bounded torsion group

Given a finite subset A of $\mathbb{Z}$ with small sumset $A + A$, Freiman's Theorem is about finding upper bounds for the smallest size and dimension of a GAP containing A. A naturally analogous problem to consider is, given a finite subset A of a bounded torsion group with small $A + A$, to find an upper bound for the size of the subgroup $\langle A \rangle$ that it generates (*i.e.* the smallest subgroup containing A). Suppose that G is an abelian group, written additively, such that each element of G has order at most r, and let A be a finite subset of G. Where $\langle A \rangle$ denotes the subgroup generated by A, we have $\langle A \rangle = \{\sum_{a \in A} n_a a : 0 \leq n_a < r\}$ and hence $|\langle A \rangle| \leq r^{|A|}$. This bound is not especially clever, though it is tight for general A.[1] However, if $A + A$ is small, we can use one of Plünnecke's results to give what may be a much nicer bound:

Ruzsa's version of Freiman's Theorem in a bounded torsion group. *Let G be an abelian group in which every element has order at most r. Let A be a finite subset of G such that $|A + A| \leq C|A|$ for some $C > 0$. Then $|\langle A \rangle| \leq C^2 r^{C^4}|A|$.*

[1] For example, suppose $G = (\mathbb{Z}/2\mathbb{Z})^N$ and $A = \{e_1, \ldots, e_n\}$ for some $n \leq N$, where $\{e_1, \ldots, e_N\}$ is the usual basis for G. In this situation, we can take $r = 2$ and we have $\langle A \rangle = 2^n$.

Proof. Suppose we had some $X \subseteq G$ such that $\langle A\rangle \subseteq A - A + \langle X\rangle$. We could then conclude that $|\langle A\rangle| \leq |A-A| \cdot |\langle X\rangle| \leq C^2|A|r^{|X|}$ where this final equality follows from Plünnecke's Theorem A (with $k = l = 1$). We proceed by looking for a small X which satisfies this condition. Since G is a torsion group, we have $\langle A\rangle = \cup_{j=1}^{\infty} jA$ and similarly for each $X \subseteq G$. We therefore want a subset X such that $jA \subseteq A - A + \langle X\rangle$ for every $j \geq 1$. Take X to be a maximal subset of $2A - A$ such that the translates $\{A + x : x \in X\}$ are disjoint. (There exists such a set since any singleton {x} trivially satisfies this condition.) As each translate $x + A$ is contained in $3A - A$, we then have

$$|X| = \frac{1}{|A|}\left|\bigcup_{x\in X}(x+A)\right| \leq \frac{1}{|A|}|3A-A| \leq \frac{1}{|A|}C^4|A| = C^4$$

where we have again used Plünnecke's Theorem A, with $k = 3, l = 1$.
Let $t \in 2A - A$. By maximality of X, there is some $x \in X$ such that $(A + t) \cap (A + x) \neq \emptyset$, so $t \in A - A + X$ and thus $2A - A \subseteq A - A + X$. It follows that $3A - A \subseteq 2A - A + X \subseteq A - A + 2X$, and similarly we obtain $(j + 1)A - A \subseteq A - A + jX \subseteq A - A + \langle X\rangle$ for each $j \geq 1$. But observe that $jA \subseteq (j + 1)A - A$, since each element of jA is of the form $a_1 + \ldots + a_j = (a_1 + \ldots + a_j + a_j) - a_j \in (j + 1)A - A$. We have therefore shown $jA \subseteq A - A + \langle X\rangle$ for each $j \geq 1$, and thus $\langle A\rangle \subseteq A - A + \langle X\rangle$. Then from previous remarks, $|\langle A\rangle| \leq C^2|A|r^{|X|} \leq C^2 r^{C^4}|A|$. □

Freiman homomorphisms and Ruzsa's embedding lemma

As we are interested in finding GAPs in abelian groups ($\mathbb{Z}$, in particular), it would be useful to have an understanding of functions which preserve this structure. It is clear that any group homomorphism from G to another abelian group H preserves GAPs, but this is a severer restriction than we require. As a simple case, suppose $\phi : G \to H$ is a function which preserves 1-dimensional GAPs, *i.e.* arithmetic progressions. We must then require that if $a, b, c \in G$ with $b - a = c - b$, we have $\phi(b) - \phi(a) = \phi(c) - \phi(b)$ or, equivalently, $a + c = b + b$ implies $\phi(a) + \phi(c) = \phi(b) + \phi(b)$. We can consider this as motivating the following definition:

Definition. *Let A and B be subsets of abelian groups G and H respectively, written additively. A* ***(Freiman) k-homomorphism*** *from A to B is a map $\phi : A \to B$ such that whenever $x_1 + \ldots + x_k = y_1 + \ldots + y_k$ holds for elements $x_i, y_i \in A$, we have $\phi(x_1) + \ldots + \phi(x_k) = \phi(y_1) + \ldots + \phi(y_k)$. If such a ϕ is a bijection whose inverse is also a k-homomorphism, then ϕ is called a* ***k-isomorphism*** *and we shall say that A and B are* ***k-isomorphic****.*

A few simple remarks about Freiman homomorphisms:

- The restriction of a homomorphism of abelian groups to a subset of its domain is clearly a k-homomorphism for each k.
- If ϕ is a k-homomorphism then it is also a j-homomorphism for all $1 \leq j \leq k$: choose any $c \in A$, and suppose $x_1 + \ldots + x_j = y_1 + \ldots + y_j$. Adding $(k - j)c$ to each side of this equation, we then have $\phi(x_1) + \ldots + \phi(x_j) + (k - j)\phi(c) = \phi(y_1) + \ldots + \phi(y_j) + (k - j)\phi(c)$ and the result follows.
- The composition of two k-homomorphisms is again a k-homomorphism, and if they are both k-isomorphisms then so is their composition.
- If $\phi : A \to B$ is a k-homomorphism, then it induces a map from kA to kB by taking $a_1 + \ldots + a_k$ to $\phi(a_1) + \ldots + \phi(a_k)$. Hence if A and B are k-isomorphic then $|kA| = |kB|$.

- Given coprime integers q and N, the map from $\mathbb{Z}/N$ to itself which takes $\overline{a}$ to $\overline{qa}$ is a k-isomorphism for all k since it is a group automorphism.

From previous discussion, we see that 2-homomorphisms preserve arithmetic progressions. Even more strongly, they preserve GAPs of *all* dimensions:

Proposition. *Let $\phi : A \to B$ be a 2-homomorphism, and suppose Q is a d-dimensional GAP in A. Then $\phi(Q)$ is a d-dimensional GAP in B.*

Proof. Write $Q = \{a_0 + \sum_{i=1}^{d} x_i a_i : 0 \leq x_i < n_i\}$. We show that

$$\phi\left(a_0 + \sum_{i=1}^{d} x_i a_i\right) = \phi(a_0) + \sum_{i=1}^{d} x_i(\phi(a_0 + a_i) - \phi(a_0))$$

for all elements $a_0 + \sum_{i=1}^{d} x_i a_i$ of Q, from which the result follows immediately. We proceed by induction on $m = \sum_{i=1}^{d} x_i$. If $m = 0$ then each side of the equation is $\phi(a_0)$. If $m = 1$, then there is some j with $x_j = 1$ and $x_i = 0$ for all other i, in which case both sides of the equation are equal to $\phi(a_0 + a_j)$.
Now, take any $r = a_0 + \sum_{i=1}^{d} x_i a_i$ with $\sum_{i=1}^{d} x_i > 1$. Choose an index j with $x_j \geq 1$. By induction, we then have

$$\phi\left(r - a_j\right) = \phi(a_0) + \left(\sum_{i \neq j} x_i\left(\phi(a_0 + a_i) - \phi(a_0)\right)\right) + (x_j - 1)\left(\phi(a_0 + a_j) - \phi(a_0)\right).$$

Since ϕ is a 2-homomorphism and $r + a_0 = (r - a_j) + (a_0 + a_j)$ with each of these four terms lying in Q, we have

$$\phi(r) + \phi(a_0) = \phi(r - a_j) + \phi(a_0 + a_j)$$

from which we recover

$$\phi(r) = \phi(a_0) + \sum_{i=1}^{d} x_i(\phi(a_0 + a_i) - \phi(a_0))$$

as desired. □

Suppose we have $A \subseteq \mathbb{Z}$ and N a natural number. The map $\pi : A \to \mathbb{Z}/N$ given by reduction $\pmod N$ is the restriction of a group homomorphism, and therefore it is a k-homomorphism for all k. It is injective if A lies in an interval of length less than N, but in general its inverse may not be a k-homomorphism: as a simple example, suppose $A = \{1, 2\}$ and we take $\pi : A \to \mathbb{Z}/2$. This map is an injective k-homomorphism for all k, but its inverse is not a k-homomorphism for any $k \geq 2$ since $\overline{1} + \overline{1} = \overline{2} + \overline{2}$ but $1 + 1 \neq 2 + 2$.
On the other hand, suppose we have defined $\psi : \mathbb{Z}/N \to \mathbb{Z}$ by mapping each residue class to its unique representative in $[1, N]$. In general this is not a k-homomorphism, but suppose we restrict ψ to a subset B of $\mathbb{Z}/N$ such that $\psi(B) \subseteq \left(\frac{jN}{k}, \frac{(j+1)N}{k}\right]$ for some j. Using bars to denote residue classes, let $\overline{a_1}, \ldots, \overline{a_k}, \overline{b_1}, \ldots, \overline{b_k} \in B$ with $\sum_{i=1}^{k} \overline{a_i} = \sum_{i=1}^{k} \overline{b_i}$. Then $\sum_{i=1}^{k} \psi(\overline{a_i}) - \sum_{i=1}^{k} \psi(\overline{b_i})$ is a multiple of N, but from the way we have restricted ψ we must have $\left|\sum_{i=1}^{k} \psi(\overline{a_i}) - \sum_{i=1}^{k} \psi(\overline{b_i})\right| < N$ and so we really have $\sum_{i=1}^{k} \psi(\overline{a_i}) = \sum_{i=1}^{k} \psi(\overline{b_i})$, thus ψ is a k-homomorphism.

Given a finite subset A of $\mathbb{Z}$, we outline our strategy for finding a GAP containing A as follows:

- (Ruzsa's Embedding Lemma) Find sufficiently large N such that A has a large subset A' which is k-isomorphic to a subset A'' of $\mathbb{Z}/N$.
- (Bogolyubov's Lemma) Using a Fourier argument, find a highly structured *Bohr set* in $2A'' - 2A''$.
- Using Minkowski's theorems from the geometry of numbers, show that such a Bohr set contains a large GAP Q.
- From Q, construct a GAP containing A as a large subset.

Ruzsa's Embedding Lemma. *Let A be a set of integers with $|kA - kA| \leq C|A|$. Then for any prime $N > 2C|A|$ we may find a subset A' of A with $|A'| \geq |A|/k$ such that A' is k-isomorphic to a subset of $\mathbb{Z}/N$.*

Proof. Let p be a very large prime, and let $1 \leq q \leq p-1$. Define the map $\phi_q : A \to \mathbb{Z}$ which takes each a to the reduction of qa (mod p) in $[1,p] \subseteq \mathbb{Z}$. We clearly have

$$A = \bigcup_{j=0}^{k-1} \phi_q^{-1}\left(\left(\frac{jp}{k}, \frac{(j+1)p}{k}\right]\right).$$

Then, by the pigeonhole principle, we can choose some j such that the size of the preimage $\phi_q^{-1}\left(\left(\frac{jp}{k}, \frac{(j+1)p}{k}\right]\right)$ is at least $|A|/k$. Denote this preimage by A_q. Restrict ϕ_q to A_q; from previous remarks, we see that ϕ_q is then a k-isomorphism from A_q to its image. Let $N > 0$ be a parameter, and define $\overline{\phi_q} : A_q \to \mathbb{Z}/N$ by taking each a to the residue class of $\phi_q(a)$ (mod N). As a composition of two k-homomorphisms, $\overline{\phi_q}$ is a k-homomorphism. Our goal is to show that for large enough N, there is some q for which $\overline{\phi_q}$ is, in fact, a k-isomorphism.

Suppose that $\overline{\phi_q}$ is not a k-isomorphism. Then there are a_i, b_i in A_q with $\sum_{i=1}^k a_i \neq \sum_{i=1}^k b_i$ but $\sum_{i=1}^k \overline{\phi_q}(a_i) = \sum_{i=1}^k \overline{\phi_q}(b_i)$. We will count the number of ("bad") values of q for which this is possible, given fixed N. Since ϕ_q is a k-isomorphism, $\sum_{i=1}^k \phi_q(a_i) \neq \sum_{i=1}^k \phi_q(b_i)$, but these two quantities are congruent (mod N) from the previous inequation. That is, there is some nonzero integer ℓ such that

$$\ell N = \sum_{i=1}^k \phi_q(a_i) - \sum_{i=1}^k \phi_q(b_i).$$

Note that since the image of ϕ_q is contained in an interval of size p/k, we have $|\ell N| \leq k(p/k) = p$ and hence $0 < |\ell| \leq p/N$. From the definition of ϕ_q, it follows that

$$\ell N \equiv q\left(\sum_{i=1}^k a_i - \sum_{i=1}^k b_i\right) \pmod{p}.$$

Suppose we fix such nonzero $\sum_{i=1}^k a_i - \sum_{i=1}^k b_i$ and l. Assuming without loss of generality that $p > \max_{x,y \in kA} |x-y| \geq \sum_{i=1}^k a_i - \sum_{i=1}^k b_i$, it follows that $\sum_{i=1}^k a_i - \sum_{i=1}^k b_i$ is not congruent to 0 (mod p) and hence there is exactly one q which satisfies the above congruence. As there are at most $|kA - kA| \leq C|A|$ choices of $\sum_{i=1}^k a_i - \sum_{i=1}^k b_i$ and at most $2p/N - 1$ choices of ℓ, there are at most $C|A|(2p/N - 1)$ "bad" values of q. To guarantee the existence of a "good" q, it therefore suffices to have

$$C|A|\left(\frac{2p}{N} - 1\right) < p - 1$$

or, rearranged,

$$N > \frac{2C|A|}{1+\frac{C|A|-1}{p}}$$

from which the result follows. $\square$

Bohr sets and the geometry of numbers

Definition. *Let N be a large prime, let $K = \{r_1, \ldots, r_k\}$ be a set of distinct residue classes (mod N), and let $\delta \in [0, 1)$. The **Bohr set** $\mathcal{B}(K;\delta)$ is the set of all residue classes s such that $\left\|\frac{sr_j}{N}\right\| \leq \delta$ for each $1 \leq j \leq k$. We refer to k as the **dimension** of this Bohr set.*

Bogolyubov's Lemma. *Let X be a subset of $\mathbb{Z}/N$ with $|X| \geq \delta N$. Then $2X - 2X$ contains a Bohr set $\mathcal{B}(K; 1/4)$ of dimension $k \leq 1/\delta^2$.*

Proof. Assume without loss of generality that $|X| = \delta N$. Recall that, by Parseval's formula, we have

$$\sum_{r (\bmod N)} \left|\hat{1}_X(r)\right|^2 = N|X| = \delta N^2.$$

It follows that there are at most $1/\delta^2$ elements r of $\mathbb{Z}/N$ with $\left|\hat{1}_X(r)\right| \geq \sqrt{\delta}|X|$, since otherwise we would have

$$\sum_{r (\bmod N)} \left|\hat{1}_X(r)\right|^2 > \frac{1}{\delta^2}(\sqrt{\delta}|X|)^2 = \delta N^2,$$

a contradiction. One of these elements is 0, since $\hat{1}_X(0) = |X| > \sqrt{\delta}|X|$. Let $K = \{r_1, \ldots, r_k\}$ be the set of all nonzero r with $\left|\hat{1}_X(r)\right| \geq \sqrt{\delta}|X|$. We show that $\mathcal{B}(K; 1/4) \subseteq 2X - 2X$.
Let b be an element of that Bohr set. Consider the exponential sum

$$\begin{aligned} S &:= \sum_{r (\bmod N)} \left|\hat{1}_X(r)\right|^4 e\left(\frac{br}{N}\right) \\ &= \sum_{r (\bmod N)} \sum_{x_1,x_2,x_3,x_4 \in X} e\left(\frac{(x_3 + x_4 - x_1 - x_2 + b)r}{N}\right) \\ &= N\#\left\{(x_1, x_2, x_3, x_4) \in X^4 : x_1 + x_2 - x_3 - x_4 \equiv b (\bmod N)\right\}. \end{aligned}$$

To show that $b \in 2X - 2X$, then, it suffices to show that S is positive. Since S is real, we may rewrite it as $\sum_{r(\bmod N)} \left|\hat{1}_X(r)\right|^4 \cos\left(\frac{2\pi br}{N}\right)$. Clearly, the contribution from the term $r = 0$ is $|X|^4$. Suppose $r \in K$; then since $b \in \mathcal{B}(K; 1/4)$ we have $\left\|\frac{br}{N}\right\| \leq 1/4$ and so $\left|\hat{1}_X(r)\right|^4 \cos\left(\frac{2\pi br}{N}\right) \geq \left|\hat{1}_X(r)\right|^4 \cos(\pi/2) = 0$. It therefore suffices to show that the contribution to S from the nonzero $r \notin K$ — that is, those r for which $|\hat{1}_X(r)| < \sqrt{\delta}|X|$ — is less than $|X|^4$ in absolute value. Let R be the set of such r, so

$$\begin{aligned} \left|\sum_{r \in R} \left|\hat{1}_X(r)\right|^4 \cos\left(\frac{2\pi br}{N}\right)\right| &\leq (\sqrt{\delta}|X|)^2 \sum_{r \in R} \left|\hat{1}_X(r)\right|^2 \\ &< \delta|X|^2 \sum_{r (\bmod N)} \left|\hat{1}_X(r)\right|^2 \\ &= \delta|X|^2(N|X|) = |X|^4, \end{aligned}$$

and the result follows. $\square$

We shall need some results from the geometry of numbers. In particular, recall Minkowski's Second Theorem:

Minkowski's Second Theorem. *Let K be a symmetric convex body and Λ a lattice in $\mathbb{R}^k$. Let $\lambda_1 \leq \cdots \leq \lambda_k$ be the successive minima of C with respect to Λ. Then $\lambda_1 \cdots \lambda_k \leq 2^k \det(\Lambda)/\mathrm{vol}(K)$.*

Recall also the Volume Packing Lemma:

Lemma (Volume Packing Lemma)**.** *Let Λ, Λ' be lattices with $\Lambda \subseteq \Lambda' \subseteq \mathbb{R}^n$. Then*

$$\det(\Lambda) = \det(\Lambda')[\Lambda' : \Lambda].$$

We are now ready to prove that Bohr sets contain large GAPs.

Proposition. *Let N be a large prime, let $r_1, \ldots, r_k$ be distinct residue classes (mod N) with $k \geq 2$, and let $\delta \in (0,1)$. Then the Bohr set $\mathcal{B}(r_1, \ldots, r_k; \delta)$ in $\mathbb{Z}/N$ contains a proper GAP of dimension k and size at least $(\delta/k)^k N$.*

Proof. Let $\mathbf{r} = (r_1, \ldots, r_k)$, identifying each r_j with its representative in $[1, N]$, and define Λ to be the lattice generated by $N\mathbb{Z}^k$ and $\mathbf{r}$, *i.e.*

$$\Lambda = \bigcup_{\ell=0}^{N-1} (\ell \mathbf{r} + (N\mathbb{Z})^k).$$

As N is prime and the r_j are distinct, at least one of the r_j is coprime to N. Assume without loss of generality that r_1 is coprime to N. It follows that the cosets $\ell\mathbf{r} + (N\mathbb{Z})^k$ are disjoint for $0 \leq \ell \leq N-1$, since the values ℓr_1 are distinct (mod N), and hence $[\Lambda : (N\mathbb{Z})^k] = N$. We therefore have $\det(\Lambda) = \det((N\mathbb{Z})^k)/N = N^{k-1}$. Now, let $C = \{\mathbf{x} \in \mathbb{R}^k : |x_i| < 1, 1 \leq i \leq k\}$. Then clearly C is a convex symmetric body with $\mathrm{vol}(C) = 2^k$. Taking $\lambda_1 \leq \ldots \leq \lambda_k$ to be the successive minima of C with respect to Λ, choose linearly independent lattice points $\mathbf{b}_1, \ldots, \mathbf{b}_k$ such that $\mathbf{b}_j \in \overline{\lambda_j C}$.
For $1 \leq j \leq k$, write $\mathbf{b}_j = (b_j r_1 + q_{1,j}N, \ldots, b_j r_k + q_{k,j}N)$ for $b_j \in \{0, \ldots, N-1\}$ and $q_{i,j} \in \mathbb{Z}$. Consider linear combinations of the form

$$\sum_{j=1}^{k} n_j \mathbf{b}_j = \left(\sum_{j=1}^{k} n_j (b_j r_1 + q_{1,j}N), \ldots, \sum_{j=1}^{k} n_j (b_j r_k + q_{k,j}N) \right)$$

where the n_j are integers with $|n_j| \leq \delta N/(k\lambda_j)$. Since each $\mathbf{b}_j \in \overline{\lambda_j C}$, each coordinate $\sum_{j=1}^{k} n_j (b_j r_i + q_{i,j}N)$ of this linear combination is bounded in absolute value by $\sum_{j=1}^{k} |n_j| \lambda_j \leq \sum_{j=1}^{k} \left(\frac{\delta N}{k\lambda_j}\right) \lambda_j = \delta N$. Then for each $1 \leq i \leq k$,

$$\begin{aligned} \left\| \frac{r_i \sum_{j=1}^{k} n_j b_j}{N} \right\| &= \left\| \frac{\sum_{j=1}^{k} n_j (b_j r_i + q_{i,j}N)}{N} \right\| \\ &\leq \left| \frac{\sum_{j=1}^{k} n_j (b_j r_i + q_{i,j}N)}{N} \right| \\ &\leq \frac{\delta N}{N} = \delta \end{aligned}$$

and so $\sum_{j=1}^{k} n_j b_j \in \mathcal{B}(r_1, \ldots, r_k; \delta)$. This is the k-dimensional GAP that we seek. To see that it is a proper GAP, consider that if $\sum_{j=1}^{k} n_j b_j = \sum_{j=1}^{k} n'_j b_j$, we then have $\sum_{j=1}^{k} n_j \mathbf{b}_j \equiv \sum_{j=1}^{k} n'_j \mathbf{b}_j \pmod{N}$

coordinatewise, but we have seen that the coordinates of these vectors are bounded in absolute value by $\delta N < N$ and so the two vectors must actually be equal. Then $n_j = n'_j$ for all j since the vectors $\mathbf{b}_j$ are linearly independent, so the GAP is proper. Since our n_j run over $|n_j| \leq \frac{\delta N}{k\lambda_j}$, the size of the GAP is

$$\begin{aligned} \prod_{j=1}^{k}\left(1+2\left\lfloor\frac{\delta N}{k\lambda_j}\right\rfloor\right) &\geq \prod_{j=1}^{k}\frac{\delta N}{k\lambda_j} \\ &\geq \left(\frac{\delta}{k}\right)^k N^k(\lambda_1\cdots\lambda_k)^{-1}. \end{aligned}$$

From Minkowski's Second Theorem, we have $\lambda_1\cdots\lambda_k \leq 2^k\frac{\det(\Lambda)}{\mathrm{vol}(C)} = 2^k\frac{N^{k-1}}{2^k} = N^{k-1}$, and thus the size of the GAP is at least $\left(\frac{\delta}{k}\right)^k N$ as desired. $\square$

Now we put everything together to prove Freiman's Theorem.

The proof of Freiman's Theorem

Freiman's Theorem. *Let A be a finite subset of $\mathbb{Z}$ with $|A+A| \leq C|A|$. Then there exist constants d' and S depending only on C such that A is contained in a GAP of dimension at most d' and size at most $S|A|$.*

Proof. By Plünnecke's inequality, $|8A-8A| \leq C^{16}|A|$. Let N be any prime with $2C^{16}|A| < N < 4C^{16}|A|$; such N exists by Bertrand's postulate. Then by Ruzsa's Embedding Lemma, there exists some $A_1 \subseteq A$ which is 8-isomorphic to a subset A_2 of $\mathbb{Z}/N$, with $|A_1| \geq |A|/8$. Thus $|A_2| \geq |A|/8 \geq N/(32C^{16})$. Taking $\delta = 1/(32C^{16})$, Bogolyubov's Lemma implies that $2A_2 - 2A_2$ contains a Bohr set $\mathcal{B}(K;1/4)$ of dimension $k \leq 1/\delta^2 \leq 1024C^{32}$. From the geometry of numbers, we conclude that $2A_2-2A_2$ contains a proper GAP Q of dimension d about $1024C^{32}$, and size about $e^{-C^{33}}|A|$.
Let X be a maximal subset of A such that the translates $\{Q+x : x\in X\}$ are all disjoint. Then $Q+X \subseteq 3A-2A$, so from Plünnecke's inequality we have $|Q+X| \leq C^5|A|$. Clearly $|X| = \frac{|Q+X|}{|Q|} \ll \frac{C^5|A|}{e^{-C^{33}}|A|} = C^5e^{C^{33}}$. Now, by maximality of X, for any $a\in A$ we must have $(Q+a)\cap(Q+X) \neq \emptyset$, and hence $a \in X+Q-Q$. Then $A \subseteq X+Q-Q$. If we write $Q = \{a_0 + \sum_{j=1}^d y_ja_j : 1 \leq x_j \leq n_j\}$, we see that $Q-Q$ is the GAP $Q-Q = \{\sum_{j=1}^d y_ja_j : |y_j| \leq n_j - 1\}$ of dimension d about $1024C^{32}$ and size at most

$$\begin{aligned} \prod_{j=1}^{d}(2n_j-1) &\leq 2^d\prod_{j=1}^{d}n_j \\ &= 2^d|Q| \\ &\ll 2^{1024C^{32}}e^{-C^{33}}|A| \\ &\ll |A|. \end{aligned}$$

Clearly $X+Q-Q$ is contained in the GAP $Z = \{\sum_{x\in X}\delta_x x + \sum_{j=1}^d y_ja_j : \delta_x \in \{0,1\}, |y_j| \leq n_j - 1\}$ of dimension

$$d + |X| \ll 2^{10}C^{32} + C^5e^{C^{33}}$$

and size

$$|Z| \leq 2^{|X|}|Q-Q| \ll 2^{|X|}|A| \ll 2^{C^5e^{C^{33}}}|A|.$$

This Z is the GAP we seek, and both its dimension and the density of A in Z are bounded by functions of C as desired. $\square$

We note finally that [2] by using some results of Chang [3], the bounds on d' and S may be improved to $d' \ll C^2(\log C)^2$ and $S \le e^{2^{20}C^2(\log C)^2}$.

References

[1] M. B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets.* Springer-Verlag, GTM 165, 1996.

[2] K. Soundararajan, *Additive Combinatorics: Winter 2007*. Stanford University, 2007.

[3] M.-C. Chang, A polynomial bound in Freiman's theorem. *Duke Mathematical Journal* 113 (2002), no. 3, 399–419.