C3.10 Additive and Combinatorial NT
Lecture 12: Freiman's theorem

Joni Teräväinen

Mathematical Institute

Freiman's theorem

In this lecture we will prove

Theorem (Freiman)

Let $A \subset \mathbb{Z}$ satisfy $|A+A| \leq K|A|$. Then there exists a generalized arithmetic progression P of dimension $\ll_K 1$ and of size $|P| \ll_K |A|$ such that $A \subset P$.

Bogolyubov's lemma

Definition

Let $R = \{r_1, \ldots, r_k\} \subset \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$, and let $\varepsilon > 0$. We define the *Bohr set* $B(R, \varepsilon)$ with *frequency set* R and *width* ε by

$$B(R, \varepsilon) := \{x \in \mathbb{Z}/q\mathbb{Z} : \|\frac{r_i x}{q}\| \leq \varepsilon \text{ for } i = 1, 2, \ldots, k\}.$$

The parameter k is called the *dimension* of the Bohr set.

Proposition (Bogulyobov)

Let $S \subset \mathbb{Z}/q\mathbb{Z}$, $|S| = \sigma q$. Then $2S - 2S$ contains a Bohr set of dimension at most $4/\sigma^2$ and width at least $\frac{1}{10}$.

Proof of Bogolyubov's lemma

Proof. We use Fourier analysis. Consider $f := 1_S * 1_S * \overline{1_{-S} * 1_{-S}}$. This is supported on $2S - 2S$. Note also that $\hat{1}_{-S}(r) = \overline{\hat{1}_S(r)}$, and so $\hat{f}(r) = |\hat{1}_S(r)|^4$.
By the Fourier inversion formula and the real-valuedness of f, we have

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

Let $R = \{r \neq 0 : |\hat{1}_S(r)| \geq \sigma^{3/2}/2\}$. By Parseval's identity,

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

and so

$$|R| \leq 4/\sigma^2. \qquad (2)$$

We claim that $B(R, \frac{1}{10}) \subset 2S - 2S$. For this it suffices to show that $f(x) > 0$ for $x \in B(R, \frac{1}{10})$.

Proof of Bogolyubov's lemma

To show that $f(x) > 0$ for $x \in B(R, \frac{1}{10})$, we will use the formula (1). We split the sum over r into three pieces: the term $r = 0$, the terms with $r \in R$, and all other terms. Clearly

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

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

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

the last step coming from Parseval. Putting this together, we get

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

as required. □

GAPs inside Bohr sets

Proposition (Proposition 12.2.1)

Let $R \subset \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$, $|R| = k$. Let $0 < \varepsilon < \frac{1}{2}$. Then the Bohr set $B(R, \varepsilon)$ contains a proper GAP of dimension d and size $\geq (\varepsilon/k)^k q$.

Proof. We shall use Minokwski's second theorem (Appendix A). Let $K \subset \mathbb{R}^d$ be a centrally symmetric (that is, $x \in K$ implies $-x \in K$) convex body , and let $\Lambda \subset \mathbb{R}^d$ be a lattice. It can be shown that $\Lambda = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_d$ for linearly independent $v_1, \ldots, v_d$, which are then called an *integral basis* for Λ. The set $\mathcal{F} := \{x_1 v_1 + \cdots + x_d v_d : 0 \leq x_i < 1\}$ is then called a fundamental region for Λ. The determinant $\det(\Lambda)$ is the volume of a fundamental region of Λ. We define the *successive minima* $\lambda_1, \ldots, \lambda_d$ of K wrt. Λ as follows: λ_j is the infimum of those λ for which the dilate λK contains j linearly independent elements of Λ.

Proposition (Minkowski's second theorem)

We have $\lambda_1 \cdots \lambda_d \mathrm{vol}(K) \leq 2^d \det(\Lambda)$.

GAPs inside Bohr sets

Returning to the proof of Prop. 12.2.1, let $R = \{r_1, \ldots, r_k\}$ and consider the lattice

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

Since q is prime, this may be written as a direct sum $q\mathbb{Z}^k \oplus \{0, 1, \ldots, q-1\} \cdot (r_1, \ldots, r_k)$. Thus Λ has index q as a subgroup of $q\mathbb{Z}^k$, and from this and $\det(q\mathbb{Z}^k) = q^k$ it follows that $\det(\Lambda) = q^{k-1}$.

GAPS in Bohr sets

Take $K \subset \mathbb{R}^k$ to be the box $\{x : \|x\|_\infty \leq \varepsilon q\}$. Let $\lambda_1, \ldots, \lambda_k$ be the successive minima of K wrt. Λ. Since K is closed, $\lambda_j K$ contains j linearly independent elements of Λ. We may, by choosing each element in turn, select a basis $b_1, \ldots, b_k$ for $\mathbb{R}^k$ with $b_j \in \Lambda \cap \lambda_j K$ for all j. Thus $b_j \in \Lambda$ and $\|b_j\|_\infty \leq \lambda_j \varepsilon q$. Set $L_j := \lceil 1/\lambda_j k \rceil$ for $j = 1, \ldots, k$. Then if $0 \leq l_j < L_j$ we have $\|l_j b_j\|_\infty \leq \varepsilon q/k$ and therefore

$$\|l_1 b_1 + \cdots + l_k b_k\|_\infty \leq \varepsilon q.$$

Each b_i lies in Λ and hence is congruent to $x_i(r_1, \ldots, r_k) \pmod q$ for some x_i, $0 \leq x_i < q$. We think of these x_i as lying in $\mathbb{Z}/q\mathbb{Z}$. The preceding observation implies that

$$\left\| \frac{(l_1 x_1 + \cdots + l_k x_k) r_i}{q} \right\| \leq \varepsilon$$

for each i, i.e. the GAP $\{l_1 x_1 + \cdots + l_k x_k : 0 \leq l_i < L_i\}$ is contained in the Bohr set $B(R, \varepsilon)$.

Proof of Freiman's theorem

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

To prove the properness, suppose that

$$l_1 x_1 + \cdots + l_k x_k = l_1' x_1 + \cdots + l_k' x_k \pmod q,$$

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

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

lies in $q\mathbb{Z}^k$ and

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

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

Proof of Freiman's theorem

Proof.

Step 1: embedding to a cyclic group. By the corollary of Ruzsa's model lemma, there is a prime $q \leq 2K^{16}|A|$ and $A' \subset A$ with $|A'| \geq |A|/8$ such that A' is Freiman 8-isomorphic to a set $S \subset \mathbb{Z}/q\mathbb{Z}$. If $\sigma := |S|/q$ then $\sigma \geq \frac{1}{16}K^{-16}$.

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

Step 3: Finding a GAP inside a Bohr set. By Proposition 12.2.1, that Bohr set (and hence $2S - 2S$) contains a proper GAP P of dimension at most $K^{O(1)}$ and size at least $\exp(-K^{O(1)})q$.

Step 4: Undoing the embedding Now A' is Freiman 8-isomorphic to S, and so by basic property (iii) of Freiman isomorphisms, $2A' - 2A'$ is Freiman 2-isomorphic to $2S - 2S$. The inverse of this restricts to a Freiman isomorphism $\phi : P \to \phi(P) \subset 2A' - 2A'$. By basic property (v) of Freiman isomorphisms, $Q = \phi(P)$ is also a proper generalised progression, of the same dimension and size as P.

Proof of Freiman's theorem

Now we have shown that $2A - 2A$ contains a proper GAP Q of dimension $K^{O(1)}$ and

$$|Q| \geq \exp(-K^{O(1)})|A|. \tag{3}$$

Step 5: Covering lemma. We apply Ruzsa's covering lemma to the sets Q and A. Since

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

the Plünnecke–Ruzsa inequality and (3) give

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

By the covering lemma, there is some set $Y = \{y_1, \ldots, y_m\}$,

$$m \leq \exp(K^{O(1)}), \tag{4}$$

such that

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

Proof of Freiman's theorem

Step 6: Finishing the proof. Suppose that

$$Q = \{x_0 + l_1x_1 + \cdots + l_dx_d : 0 \le l_i < L_i\}$$

and

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

Then

$$\begin{aligned}(Q - Q) + Y &\subset \{\tilde{x}_0 + \sum_{i \le d} \ell_i x_i + \sum_{i \le m} l'_i y_i, 0 \le l_i < 2L_i, 0 \le l'_j < 2\} \\ &= \tilde{Q},\end{aligned}$$

where

$$\tilde{x}_0 = -(L_1x_1 + \cdots + L_dx_d).$$

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

$$|\tilde{Q}| = 2^{d+m}L_1 \cdots L_d = 2^{d+m}|Q| \le 2^{d+m}|2A - 2A| \ll_K |A|.$$