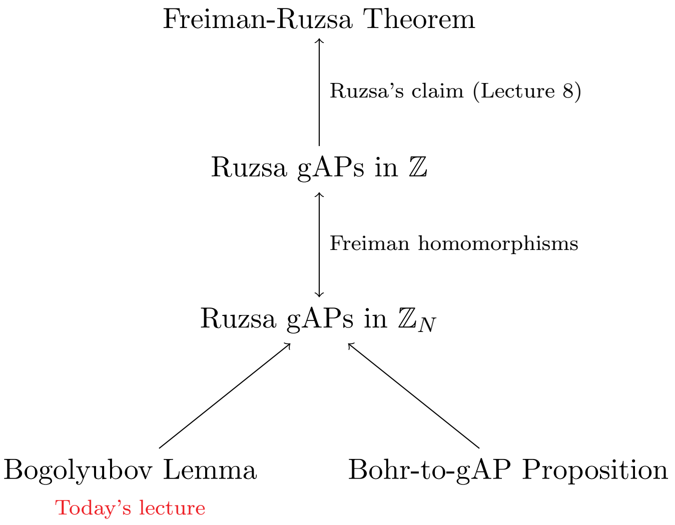
Additive Combinatorics Lecture 10

Leo Goldmakher

Scribe: Gal Gross

March 21st, 2014

Recall that the Freiman-Ruzsa theorem asserts that if $A \subseteq \mathbb{Z}$ has small doubling, then A is contained in a low-dimensional gAP which isn't much larger than A. In Lecture 8 we proved that it suffices to find some positive integers m and n such that $mA - nA$ contains a large proper gAP of small dimension (which we shall call a "Ruzsa gAP"). Over the next two lectures we will solve this problem for $A \subseteq \mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$. To do so, first we follow an idea of Bogolyubov and use Fourier analysis to construct certain number theoretic sets called *Bohr sets* inside $2A - 2A$ for any $A \subseteq \mathbb{Z}_N$. Next, we use Minkowski's second theorem from the geometry of numbers to show that any Bohr set contains a large proper gAP whose dimension is controlled by the Bohr set. However, what we're really interested in is finding Ruzsa gAPs in $\mathbb{Z}$, not in $\mathbb{Z}_N$! The final step of the proof will be to develop the theory of Freiman homomorphisms (in particular Ruzsa's 'modelling lemma') to build a bridge between gAPs in $\mathbb{Z}$ and gAPs in $\mathbb{Z}_N$.



Lemma (N. Bogolyubov[1])**.** Let $A \subseteq \mathbb{Z}_N$ with $|A| = \delta N$. Then $2A - 2A$ contains a Bohr set $B(R, \frac{1}{4})$ of dimension $|R| \le \delta^{-2}$.

As things stand, this is not an impressive result, because we haven't yet defined what a Bohr set is! The precise definition is somewhat technical, and in order to motivate it I will postpone stating it until after the proof. For now, let me just say that given a set $R \subseteq \mathbb{Z}_N$, the associated Bohr set $B(R, \alpha) \subseteq \mathbb{Z}_N$ is the set of all solutions to a certain system of inequalities defined in terms of α and the elements of R. Next lecture we will show that $B(R, \alpha)$ contains a large proper gAP of dimension $|R|$; this motivates defining the *dimension* of a Bohr set $B(R, \alpha)$ to be $|R|$.

Before proving Bogolyubov's Lemma, we review our previous discussion of Fourier analysis. First is the following simple but useful formula:

$$\frac{1}{N} \sum_{n \in \mathbb{Z}_N} e\Big(\frac{an}{N}\Big) = \begin{cases} 1 & \text{if } a \equiv 0 \pmod{N} \\ 0 & \text{else.} \end{cases}$$

[1] Nikolay Bogolyubov (1909–1992) was a Soviet mathematician and physicist who defended his PhD at age 19 and went on to discover fundamental results in quantum field theory, statistical mechanics, several complex variables, and dynamical systems.

Next, we recall two results from last lecture.

Theorem (Fourier Inversion)**.** Given any function $f : \mathbb{Z}_N \to \mathbb{C}$, there exists a function $\hat{f} : \mathbb{Z}_N \to \mathbb{C}$ such that for all $k \in \mathbb{Z}_N$ we have

$$f(n) = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \hat{f}(k) e\Big(\frac{nk}{N}\Big).$$

In fact, we have the following formula for $\hat{f}$:

$$\hat{f}(k) = \sum_{a \in \mathbb{Z}_N} f(a) e\Big(-\frac{ak}{N}\Big).$$

Theorem (Parseval's formula)**.** Given any $f : \mathbb{Z}_N \to \mathbb{C}$, we have

$$\sum_{n \in \mathbb{Z}_N} |f(n)|^2 = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} |\hat{f}(k)|^2$$

Given $A \subseteq \mathbb{Z}_N$, define $A(n)$ as its characteristic function

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

This allows us to perform Fourier analysis. Consider the Fourier coefficients of this characteristic function:

$$\hat{A}(k) = \sum_{n \in A} e\Big(-\frac{kn}{N}\Big).$$

Note that $e(\alpha)$ is some point on the complex unit circle, so $\hat{A}(k)$ is a sum of points on the unit circle. Heuristically, the only way for $\hat{A}(k)$ to be large is for $e(\frac{-kn}{N})$ to point in the same direction for many values of $n \in A$; in other words, the set A displays some bias, in that the dilated set $\{ka : a \in A\}$ has many values which are roughly the same (mod N). The worst such bias is evident in $\hat{A}(0)$, in which the elements of the dilated set are all the same: $\hat{A}(0) = |A|$. For other values of k, however, we typically do not have such easy formulas. Instead of studying these individually, we use an idea we've seen before (Lecture 2) and compute the average value of the Fourier coefficients.

$$\frac{1}{N} \sum_{k \in \mathbb{Z}_N} \hat{A}(k) = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \sum_{n \in \mathbb{Z}_N} A(n) e\Big(\frac{-kn}{N}\Big) = \sum_{n \in A} \frac{1}{N} \sum_{k \in \mathbb{Z}_N} e\Big(\frac{-kn}{N}\Big)$$

$$= \sum_{\substack{n \in A \\ n \equiv 0 \pmod{N}}} 1 = \#\{n \in A : n \equiv 0 \pmod{N}\} = A(0).$$

Thus we can pick out whether or not $0 \in A$ by using the Fourier coefficients of A. More generally, one can determine whether or not $a \in A$ in terms of the Fourier coefficients:

$$A(a) = \#\{n \in A : n \equiv a \pmod{N}\} = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \hat{A}(k) e\Big(\frac{ak}{N}\Big). \tag{1}$$

What happens if we look at the second moment instead of the average?

$$\frac{1}{N} \sum_{k \in \mathbb{Z}_N} \hat{A}(k)^2 = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \left(\sum_{n \in \mathbb{Z}_N} A(n) e\Big(\frac{-kn}{N}\Big) \right)^2 = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \sum_{m,n \in \mathbb{Z}_N} A(m)A(n) e\Big(\frac{-km}{N}\Big) e\Big(\frac{-kn}{N}\Big)$$

$$= \sum_{m,n \in A} \frac{1}{N} \sum_{k \in \mathbb{Z}_N} e\Big(\frac{-k(m+n)}{N}\Big) = \#\{m, n \in A : m + n \equiv 0 \pmod{N}\}.$$

As with (1), one may generalize this to

$$\#\{m,n\in A\,:\,m+n\equiv a \pmod N\}=\frac{1}{N}\sum_{k\in\mathbb{Z}_N}\hat{A}(k)^2 e\Big(\frac{ak}{N}\Big). \tag{2}$$

Therefore, we conclude that $a\in A+A$ iff the RHS in (2) (henceforth $\clubsuit(a)$) is positive:

$$a\in A+A \iff \clubsuit(a)>0 \tag{3}$$

Exercise 1. Recall that the modulus $|\cdot|$ of a complex number is defined by $|z|^2=z\cdot\overline{z}$, where $\overline{z}$ denotes the complex conjugate of z. Prove that

$$\#\{m,n\in A\,:\,m-n\equiv a \pmod N\}=\frac{1}{N}\sum_{k \pmod N}\left|\hat{A}(k)\right|^2 e\Big(\frac{ak}{N}\Big).$$

Exercise 2. Prove that

$$\#\{m,n,p,q\in A\,:\,(m+n)-(p+q)\equiv a \pmod N\}=\frac{1}{N}\sum_{k \pmod N}\left|\hat{A}(k)\right|^4 e\Big(\frac{ak}{N}\Big). \tag{4}$$

Denoting the RHS of (4) by $\heartsuit(a)$, we conclude that

$$a\in 2A-2A \iff \heartsuit(a)>0.$$

Armed with this observation, we are ready to prove Bogolyubov's Lemma.

Proof of Bogolyubov's Lemma. One conclusion to draw from (4) is that $\heartsuit(a)$ is always a real number (in fact, an integer). It follows that the imaginary part is zero, whence we have

$$\heartsuit(a)=\frac{1}{N}\sum_{k\in\mathbb{Z}_N}\left|\hat{A}(k)\right|^4\cos\left(\frac{ak}{N}\right).$$

Recall that $a\in 2A-2A$ iff $\heartsuit(a)>0$. We now try to identify a large set of a for which $\heartsuit(a)>0$; the set of such a will be our Bohr set. Our approach is to study which $k\in\mathbb{Z}_N$ contribute the most to the sum $\heartsuit(a)$.

- $\underline{k=0.}$ This contribution is easy to calculate: it is

$$\frac{1}{N}|A|^4=\delta^4N^3.$$

- $\underline{\hat{A}(k)\text{ small.}}$ Observe that $|\hat{A}(k)|$ is trivially bounded above by $|A|$. Fix some constant $\lambda<1$ (to be chosen optimally below), and say $\hat{A}(k)$ is *small* if $|\hat{A}(k)|<\lambda|A|$. Let S denote the set of all k for which $\hat{A}(k)$ is small. What's the total contribution to the sum $\heartsuit(a)$ above? We immediately see

$$\left|\frac{1}{N}\sum_{k\in S}\left|\hat{A}(k)\right|^4\cos\left(\frac{ak}{N}\right)\right|<\frac{1}{N}\sum_{k\in S}\lambda^4|A|^4=\frac{\lambda^4|A|^4|S|}{N}\le\lambda^4|A|^4$$

However, a clever use of Parseval leads to a much better bound:

$$\begin{aligned}\left|\frac{1}{N}\sum_{k\in S}\left|\hat{A}(k)\right|^4\cos\left(\frac{ak}{N}\right)\right|&<\frac{\lambda^2|A|^2}{N}\sum_{k\in S}\left|\hat{A}(k)\right|^2\le\frac{\lambda^2|A|^2}{N}\sum_{k\in\mathbb{Z}_N}\left|\hat{A}(k)\right|^2\\&=\lambda^2|A|^2\sum_{n\in\mathbb{Z}_N}|A(n)|^2=\lambda^2|A|^3\end{aligned}$$

Now observe that if we choose $\lambda=\sqrt{\delta}$, then the total contribution from $k=0$ and $k\in S$ is

$$\frac{1}{N}\left|\hat{A}(0)\right|^4+\frac{1}{N}\sum_{k\in S}\left|\hat{A}(k)\right|^4\cos\left(\frac{ak}{N}\right)>0.$$

- $\hat{A}(k)$ large. The remaining k's are exactly those occupying the set

  $$R := \{k \in \mathbb{Z}_N \,:\, k \neq 0 \text{ and } |\hat{A}(k)| \geq \sqrt{\delta}\,|A|\}.$$

  Let us engage in some wishful thinking and suppose that there exists an $a \in \mathbb{Z}_N$ such that $\cos\left(\frac{2\pi ak}{N}\right) \geq 0$ for *all* $k \in R$. Then by our above analysis, we deduce that $\heartsuit(a) > 0$ and so $a \in 2A - 2A$. Geometrically, $\cos x \geq 0$ precisely on the "right" half-circle $[-\frac{\pi}{2}, \frac{\pi}{2}]$, i.e. the inequality $\cos\left(\frac{2\pi ak}{N}\right) \geq 0$ holds whenever $-\frac{1}{4} \leq \frac{ak}{N} \leq \frac{1}{4}$. Actually, it holds in other intervals as well, for example $\frac{3}{4} \leq \frac{ak}{N} \leq \frac{5}{4}$. More generally, the inequality $\cos\left(\frac{2\pi ak}{N}\right) \geq 0$ holds iff $\left\|\frac{ak}{N}\right\| \leq \frac{1}{4}$, where $\|\cdot\|$ denotes the distance to the nearest integer (e.g. $\|1.2\| = \|1.8\| = 0.2$).

  Putting all this together, we see that if $\left\|\frac{ak}{N}\right\| \leq \frac{1}{4}$ for every $k \in R$, then $a \in 2A - 2A$. Thus, if we set

  $$B\Big(R, \frac{1}{4}\Big) := \{x \in \mathbb{Z}_N \,:\, \left\|\frac{kx}{N}\right\| \leq \frac{1}{4} \text{ for all } k \in R\},$$

  we have that $B(R, 1/4) \subseteq 2A - 2A$. This set $B(R, 1/4)$ is an example of a *Bohr set*; we will give a general definition immediately following the conclusion of the proof. (We will also show that $B(R, 1/4)$ is decently large, which isn't obvious *a priori.*)

  To complete the proof it remains to evaluate the dimension of $B(R, \frac{1}{4})$; recall that this is defined to be $|R|$. Since $|\hat{A}(k)| \geq \sqrt{\delta}|A|$ for every $k \in R$, we have

  $$\frac{1}{N}\sum_{k \in R}\left|\hat{A}(k)\right|^2 \geq \frac{1}{N}\sum_{k \in R}\delta\,|A|^2 = \frac{1}{N}\,|R| \cdot \delta\,|A|^2 = |R|\,N\delta^3.$$

  On the other hand, by Parseval we have

  $$\frac{1}{N}\sum_{k \in R}\left|\hat{A}(k)\right|^2 \leq \frac{1}{N}\sum_{k \in \mathbb{Z}_N}\left|\hat{A}(k)\right|^2 = \sum_{n \in \mathbb{Z}_N}|A(n)|^2 = |A| = \delta N.$$

  We conclude that $|R| \leq \delta^{-2}$, which completes the proof of Bogolyubov's Lemma. □

In the above proof, we needed to consider the set $B(R, 1/4) \subseteq \mathbb{Z}_N$ of all nonzero solutions $x \in \mathbb{Z}_N$ to the system of inequalities

$$\left\|\frac{rx}{N}\right\| \leq \frac{1}{4} \text{ for all } r \in R.$$

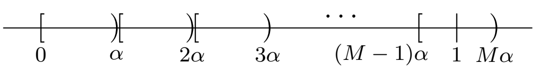
More generally, given $R \subseteq \mathbb{Z}_N$ and $\alpha \in [0, 1/2]$, let

$$B(R, \alpha) := \{x \in \mathbb{Z}_N \,:\, \left\|\frac{rx}{N}\right\| \leq \alpha \text{ for all } r \in R\}.$$

This is a Bohr set. As discussed above, the *dimension* of the Bohr set $B(R, \alpha)$ is the size of the set R.

Having proved the existence of a Bohr set inside $2A - 2A$, our next goal is to find a large proper gAP of small dimension inside that Bohr set. Before we do this, it would be nice to know that the Bohr set itself is large. To build up our intuition, we first consider the situation of a 1-dimensional Bohr set $B(k, \alpha) := B(\{k\}, \alpha)$.

Consider the sequence of points $\{\frac{nk}{N} \pmod 1 \,:\, n \in \mathbb{Z}_N\}$. They are all distributed somewhere on the interval $[0, 1)$. Let us cover $[0, 1)$ by the smaller intervals $[m\alpha, (m+1)\alpha)$ for $0 \leq m \leq M - 1$, where M is the smallest natural number such that $M\alpha \geq 1$. Thus, $M \approx \frac{1}{\alpha}$.



Therefore, we are distributing N points (counted with multiplicity, as they are not necessarily distinct) among $\approx \frac{1}{\alpha}$ boxes. By the pigeonhole principle, some interval I among the $[m\alpha, (m+1)\alpha)$ contains $\gg \alpha N$ points. Observe that for any $x, y \in I$ we have $\|x - y\| \leq \alpha$; it follows that $I - I \subseteq B(k, \alpha)$. We therefore have

$$|B(k, \alpha)| \geq |I - I| \geq |I| \gg \alpha N.$$

Thus, as long as α isn't too small, $B(k, \alpha)$ occupies a decent proportion of the group $\mathbb{Z}_N$.

Exercise 3. Suppose $R \subseteq \mathbb{Z}_N$, and set $d = |R|$. Prove that

$$B(R, \alpha) \gg \alpha^d N.$$

It follows that if α isn't too small and the dimension of the Bohr set isn't too large, the Bohr set occupies a decent proportion of $\mathbb{Z}_N$.

*   *   *
   *   *

It turns out that to prove the existence of large proper gAPs in a Bohr set, we need to know something about the Geometry of Numbers. This field was pioneered by Minkowski[2], and makes unexpected appearances in numerous areas of mathematics. A precursor to the sorts of questions which come up in this area was first studied by Gauss.

Gauss' Circle Problem. How many $\mathbb{Z} \times \mathbb{Z}$ lattice points are there in a circle of radius r centered at the origin?

Exercise 4. Let $G(r)$ denote the number of lattice points in a circle of radius r centred at the origin. Give a heuristic argument to justify the approximation $G(r) \approx \pi r^2$.

Gauss showed that $G(r) = \pi r^2 + O(r)$; it is a long-standing conjecture that the error term can be improved to $O_\epsilon(r^{1/2+\epsilon})$ for any $\epsilon > 0$. The strongest result known towards this is due to M. Huxley, who in 2003 proved the approximation $G(r) = \pi r^2 + O(r^{0.63})$. From the other side, G. H. Hardy and E. Landau independently proved that $G(r) \neq \pi r^2 + O(r^{1/2})$, in the sense that

$$\limsup_{r \to \infty} \frac{|G(r) - \pi r^2|}{\sqrt{r}} = \infty.$$

[2] Hermann Minkowski (1864–1909) was a mathematician who applied geometry to solve numerous important problems in mathematics and physics, notably introducing the idea of four-dimensional space-time into Einstein's theory of special relativity.