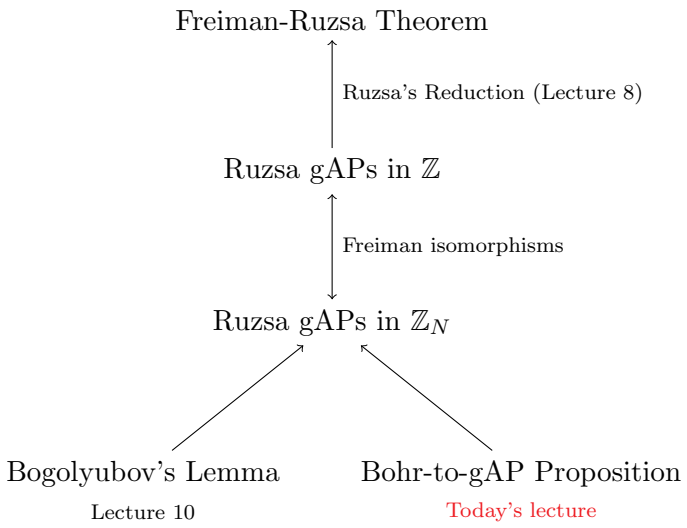
Additive Combinatorics Lecture 11

Leo Goldmakher
Scribe: Gal Gross

March 28th, 2014

Last time we proved Bogolyubov's Lemma, which asserts that given any decently large subset $A \subseteq \mathbb{Z}_N$, the set $2A-2A$ contains a low-dimensional Bohr set. We also showed that low-dimensional Bohr sets are pretty big. The purpose of today's lecture is to demonstrate that any low-dimensional Bohr set contains a large low-dimensional proper gAP. Before launching into this, let's zoom out and recall where we are in the proof of Freiman-Ruzsa.



How do we find a gAP inside a Bohr set? We warm up with a toy case. Recall that a 1-dimensional Bohr set has the form

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

where $\|\cdot\|$ denotes the distance to the nearest integer. I claim that $B(\{r\},\alpha)$ contains a long AP.

Exercise 1.

(a) Prove that $\|t\| \leq |t|$ for all $t \in \mathbb{R}$.

(b) Prove that $\|a/N\| = \|b/N\|$ whenever $a \equiv b \pmod N$.

The above exercise implies that for any $x \in \mathbb{Z}$,

$$\left\|\frac{rx}{N}\right\| \leq \left|\frac{rx \pmod N}{N}\right|.$$

If we're lucky, we can find some x_0 for which $\left|\frac{rx_0 \pmod N}{N}\right|$ is very small, so that x_0 and its multiples form an arithmetic progression inside $B(\{r\},\alpha)$. So our problem becomes: how do we minimize $rx \pmod N$?

Consider the group $\langle r, N\rangle := r\mathbb{Z} + N\mathbb{Z}$. A classical result (often attributed to Bézout) asserts that $\langle r, N\rangle = \langle g\rangle$, where $g = \gcd(r, N)$. It follows that there exist $x_0, y_0 \in \mathbb{Z}$ such that $rx_0 + Ny_0 = g$, whence

$$rx_0 \equiv g \pmod{N}. \tag{1}$$

Applying Exercise 1, we see that

$$\left\| \frac{krx_0}{N} \right\| \leq \left| \frac{kg}{N} \right|,$$

so $kx_0 \in B(\{r\}, \alpha)$ whenever $|k| \leq \frac{N\alpha}{g}$. We have thus found an arithmetic progression inside our Bohr set:

$$Q := \left\{ kx_0 \pmod{N} : |k| \leq \frac{N\alpha}{g} \right\}.$$

How big is Q? This isn't a silly question: it's possible that not all of its elements are distinct (mod N). We will show that, so long as $\alpha < 1/2$, Q is a proper AP.

Suppose two elements of Q are indistinguishable, say

$$kx_0 \equiv k'x_0 \pmod{N}.$$

We can't cancel x_0, since it might not be coprime to N. Instead we multiply both sides by r; (1) implies

$$kg \equiv k'g \pmod{N},$$

whence $N \mid (k - k')g$. Now by definition, $|k|, |k'| \leq \frac{\alpha N}{g}$. Assuming $\alpha < 1/2$, we have that $|(k - k')g| < N$, and hence that $(k - k')g = 0$. We conclude that $k = k'$, which shows that Q is a proper AP.

To summarize, given any Bohr set $B(\{r\}, \alpha) \subseteq \mathbb{Z}_N$ with $\alpha < 1/2$, it must contain a proper arithmetic progression Q of size $2\left\lfloor \frac{N\alpha}{g} \right\rfloor + 1$.

Exercise 2. Prove that $2\lfloor x \rfloor + 1 \geq x$ for all $x \geq 0$.

Thus, $|Q| \geq \frac{N\alpha}{g}$. In particular, if N is prime and $r \neq 0$ then $g = 1$, in which case $B(\{r\}, \alpha)$ contains a proper AP of size at least αN. This motivates the following generalization.

Proposition (Bohr-to-gAP)**.** Let N be a prime, $\alpha < 1/2$, and $R \subseteq \mathbb{Z}_N$ with $d := |R| \geq 2$. Then the Bohr set $B(R, \alpha)$ contains a proper generalized arithmetic progression Q of dimension d and size $|Q| \gg_d \alpha^d N$.

The proof is similar to the 1-dimensional case. Recall that, inspired by Exercise 1, we first found an $x \in \mathbb{Z}_N$ which minimizes rx (mod N); we then used x to generate an arithmetic progression inside our Bohr set. Similarly, in the d-dimensional case, we look for $x \in \mathbb{Z}_N$ which makes rx (mod N) small, but now we need this to hold for every $r \in R$ simultaneously. We can no longer ask for the x which minimizes, since there are multiple r's. Instead, we assemble all d elements of R into a single vector $\vec{r} \in \mathbb{Z}^d$. We then search for $x \in \mathbb{Z}_N$ which minimizes the magnitude of $x\vec{r}$ (mod N). In fact, we will be able to find multiple scalars $x_1, x_2, \ldots, x_d$ which make $x\vec{r}$ (mod N) small. Finally, we will use these to generate a proper gAP inside our Bohr set.

An analysis of the 1-dimensional proof shows that, beyond the initial set-up, the only tricky step was obtaining a lower bound on the size of the AP. The same applies to the general case: to get a bound on the size we use a deep theorem of Minkowski's from the Geometry of Numbers. We will apply his theorem in a 'soft' way in our proof; a more judicious application of Minkowski's theorem would yield the precise lower bound

$$|Q| \geq \left(\frac{\alpha}{d}\right)^d N.$$

For our application we can get away with the less precise bound stated in the Proposition, because Bogolyubov's Lemma allows us to get a strong upper bound on the dimension d of the Bohr set.

Proof of Bohr-to-gAP Proposition. Given a Bohr set $B(R,\alpha)$, enumerate $R = \{r_1, r_2, \ldots, r_d\}$ and set

$$\vec{r} := (r_1, r_2, \ldots, r_d).$$

Consider the subgroup of $\mathbb{Z}^d$ generated by $N\mathbb{Z}^d$ and $\vec{r}$, namely

$$\Lambda := \langle \vec{r}, N\vec{e}_1, N\vec{e}_2, \ldots, N\vec{e}_d \rangle = \mathbb{Z}\vec{r} + N\mathbb{Z}\vec{e}_1 + N\mathbb{Z}\vec{e}_2 + \cdots + N\mathbb{Z}\vec{e}_d$$

where $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_d\}$ denotes the standard basis for $\mathbb{Z}^d$. Let $\vec{g}_1$ be the shortest[1] nonzero vector in Λ. Let $\vec{g}_2$ be the shortest nonzero vector in Λ which is linearly independent of $\vec{g}_1$ (over $\mathbb{R}^d$). In general, for $j \le d$, let $\vec{g}_j$ be the shortest nonzero vector in Λ which is linearly independent of $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_{j-1}$. In this way we find d linearly independent vectors $\vec{g}_j \in \Lambda$.

Exercise 3. Is $\Lambda = \langle \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_d \rangle$? Either prove that it is, or show by example that it might not be.

Since $\vec{g}_i \in \Lambda$, by the definition of Λ there must exist $x_i \in \mathbb{Z}$ such that

$$\vec{g}_i \equiv x_i \vec{r} \pmod{N}. \tag{2}$$

(This is the analogue of (1) from the one-dimensional case.) Since the vectors $\vec{g}_i$ are short, linear combinations of them with small coefficients will also be fairly short. We consider this more carefully. Let

$$\overline{Q} := \{k_1\vec{g}_1 + k_2\vec{g}_2 + \cdots + k_d\vec{g}_d : |k_i| \le K_i\},$$

where the bounds K_i will be chosen later. For any $\vec{q} = (q_1, q_2, \ldots, q_d) \in \overline{Q}$, (2) implies

$$\vec{q} \equiv (k_1x_1 + k_2x_2 + \cdots + k_dx_d)\vec{r} \pmod{N},$$

whence (looking at the j^{th} coefficient on both sides) we obtain

$$\left\| \frac{(k_1x_1 + k_2x_2 + \cdots + k_dx_d)r_j}{N} \right\| = \left\| \frac{q_j}{N} \right\| \le \frac{|\vec{q}|}{N} \le \frac{1}{N} \sum_i |k_i|\,|\vec{g}_i| \le \frac{1}{N} \sum_i K_i\,|\vec{g}_i|\,. \tag{3}$$

We can make the right hand side small by choosing K_i appropriately, e.g.

$$K_i := \frac{\alpha N}{d\,|\vec{g}_i|}.$$

This bounds the right hand side of (3) by α, and thus produces a gAP inside of our Bohr set:

$$Q := \left\{ k_1x_1 + k_2x_2 + \cdots + k_dx_d \pmod{N} : |k_i| \le \frac{\alpha N}{d\,|\vec{g}_i|} \right\} \subseteq B(R,\alpha).$$

It remains only to show that Q is proper, and then estimate its size.

Suppose two elements of Q are indistinguishable (mod N), say,

$$\sum_i k_ix_i \equiv \sum_i k_i'x_i \pmod{N}.$$

As in the 1-dimensional case, we multiply both sides by $\vec{r}$ and apply (2) to obtain

$$\sum_i k_i\vec{g}_i \equiv \sum_i k_i'\vec{g}_i \pmod{N}.$$

I claim that the two sides of this congruence are actually equal, not just congruent modulo N. For brevity, set $\vec{v} := \sum k_i\vec{g}_i$ and $\vec{w} := \sum k_i'\vec{g}_i$, and write $\vec{v} = (v_1, v_2, \ldots, v_d)$ and $\vec{w} = (w_1, w_2, \ldots, w_d)$.

Exercise 4. Prove that $|v_j|, |w_j| \le \alpha N$.

[1] If there are several such vectors, pick any one of them.

Since $\alpha < 1/2$ by assumption and $v_j \equiv w_j \pmod N$ for all j, the exercise implies that $v_j = w_j$ for all j. It follows that $\vec{v} = \vec{w}$, or in other words,

$$\sum_i k_i \vec{g}_i = \sum_i k_i' \vec{g}_i.$$

Since the vectors $\vec{g}_i$ are linearly independent, we conclude that $k_i = k_i'$ for every i. We have thus proved that Q is a proper gAP. This also implies that $\dim Q = d$.

The final step is to estimate the size of Q. By properness of Q and Exercise 2, we see

$$|Q| = \prod_{j=1}^{d} \left(2 \left\lfloor \frac{\alpha N}{d\,|\vec{g}_j|} \right\rfloor + 1 \right) \geq \prod_{j=1}^{d} \frac{\alpha N}{d\,|\vec{g}_j|} = \left(\frac{\alpha N}{d} \right)^d \left(\prod_{j=1}^{d} |\vec{g}_j| \right)^{-1}.$$

A consequence of Minkowski's second theorem from the Geometry of Numbers is that

$$\prod_{j=1}^{d} |\vec{g}_j| \ll_d N^{d-1}.$$

(We will explain this step next lecture.) This concludes the proof of the Bohr-to-gAP proposition. □