Part III Topics in Additive Combinatorics

Based on lectures by Prof W.T. Gowers

Michaelmas 2016
University of Cambridge

Contents

1 Discrete Fourier Analysis and Roth's Theorem

Let $N \in \mathbb{N}$, $\omega = e^{\frac{2\pi i}{N}}$. Write $\mathbb{Z}_N$ for the cyclic group of integers mod N. Use the notation $\mathbb{E}_x f(x)$ to stand for the average $N^{-1} \sum_{x \in \mathbb{Z}_N} f(x)$.

Definition (Discrete Fourier Transform)**.** *Given a function $f : \mathbb{Z}_N \to \mathbb{C}$, define its* ***discrete Fourier transform*** *$\hat{f}$ by the formula*

$$\hat{f}(r) = \mathbb{E}_x f(x) \omega^{-rx}$$

Definition (Convolution)**.** *We define the* ***convolution*** *$f * g$ of f and g by*

$$f * g(x) = \mathbb{E}_{y+z=x} f(y) g(z)$$

$$\hat{f} * \hat{g}(r) = \sum_{s+t=r} \hat{f}(s) \hat{g}(t)$$

We also define two inner products

$$\langle f, g\rangle = \mathbb{E}_x f(x)\overline{g(x)}$$

$$\langle \hat{f}, \hat{g}\rangle = \sum_r \hat{f}(r)\overline{\hat{g}(r)}$$

Have the following basic properties:

1. Parseval's Identity:
$$\langle \hat{f}, \hat{g}\rangle = \langle f, g\rangle$$
for any $f, g : \mathbb{Z}_N \to \mathbb{C}$.

2. Convolution Law: for any $f, g : \mathbb{Z}_N \to \mathbb{C}$, $r \in \mathbb{Z}_N$
$$\widehat{f * g}(r) = \hat{f}(r)\hat{g}(r)$$

3. Inversion Formula: let $f : \mathbb{Z}_N \to \mathbb{C}$. Then
$$f(x) = \sum_r \hat{f}(r)\omega^{rx}$$

4. Dilation Rule: let a be invertible mod N and define $f_a(x)$ to be $f(a^{-1}x)$. Then
$$f_a\hat{(}r) = \hat{f}(ar)$$

If $A \subset \mathbb{Z}_N$, we shall write $A(x)$ for $\begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$. If $|A| = \alpha N$, then $\hat{A}(0) = \mathbb{E}_x A(x) = \alpha$.

We shall define $||f||_p$ to be $(\mathbb{E}_x |f(x)|^p)^{\frac{1}{p}}$ and $\left|\left|\hat{f}\right|\right|_p$ to be $\left(\sum_r \left|\hat{f}(x)\right|^p\right)^{\frac{1}{p}}$.

Then if $A \subset \mathbb{Z}_N$, $||A||_2^2 = \langle A, A\rangle = \alpha$. By Parseval, we get

$$\sum_r \left|\hat{A}(r)\right|^2 = \alpha \ \left(= \left|\left|\hat{A}\right|\right|_2^2\right)$$

Theorem 1 (Roth)**.** *For every $\delta > 0$ $\exists N$ s.t. every subset $A \subset [N]$ of size at least δN contains an arithmetic progression of length 3.*

Broad strategy: a density increment argument.

The idea is to show that if A has density α and contains no 3-AP then there is a reasonably long AP P s.t. $\frac{|A \cap P|}{|P|}$ is significantly larger than α. There we are either done or can pass to P and start again with a larger density. Then repeat, and eventually, since α can't exceed 1, we must get a 3-AP.

In order to use Fourier analysis, we want to think of A as a subset of $\mathbb{Z}_n$. For this purpose, define sets $B = C = A \cap \left[\frac{N}{3}, \frac{2N}{3}\right]$, and observe that if (x, y, z) is an AP in $A \times B \times C$ in $\mathbb{Z}_N$, then it also is in $[N]$.

Let α be the density of A. Assume that N is odd. If $|B| < \frac{\alpha N}{5}$ then one of $\left|A \cap \left[1, \frac{N}{3}\right]\right|$ and $\left|A \cap \left[\frac{2N}{3}, N\right]\right|$ is at least $\frac{2\alpha N}{5}$, so we get an interval in which A has density at least $\frac{6\alpha}{5}$, which is a very healthy density increment.

Otherwise, $|B| = |C| > \frac{\alpha N}{5}$, so let's assume that.

Define the **3-AP-density** of (A, B, C) to be $\mathbb{E}_{x+z=2y} A(x)B(y)C(z)$. This is the probability that a random (x, y, z) with $x + z = 2y$ lies in $A \times B \times C$.

$$\begin{aligned}
\mathbb{E}_{x+z=2y} A(x)B(y)C(z) &= \mathbb{E}_u \left(\mathbb{E}_{x+z=u} A(x)C(z)\right) B(u/2) \\
&= \mathbb{E}_u A * C(u) B_2(u) \\
&= \langle A * C, B_2 \rangle \\
&= \langle \widehat{A * C}, \hat{B}_2 \rangle \\
&= \langle \hat{A}\hat{C}, \hat{B}_2 \rangle \\
&= \sum_r \hat{A}(r)\hat{C}(r)\overline{\hat{B}_2(r)} \\
&= \sum_r \hat{A}(r)\hat{C}(r)\hat{B}(-2r) \\
&= \alpha\beta\gamma + \sum_{r \neq 0} \hat{A}(r)\hat{C}(r)\hat{B}(-2r)
\end{aligned}$$

where $\beta = \gamma =$ density of B (or C). Now

$$\begin{aligned}
\left|\sum_{r \neq 0} \hat{A}(r)\hat{B}(-2r)\hat{C}(r)\right| &\leq \max_{r \neq 0} \left|\hat{A}(r)\right| \sum_r \hat{B}(-2r)\hat{C}(r) \\
&\leq \max_{r \neq 0} \left|\hat{A}(r)\right| \left|\left|\hat{B}\right|\right|_2 \left|\left|\hat{C}\right|\right|_2 \quad \text{(Cauchy-Schwarz)} \\
&= \beta^{\frac{1}{2}}\gamma^{\frac{1}{2}} \max_{r \neq 0} \left|\hat{A}(r)\right|
\end{aligned}$$

Therefore, if $\max_{r \neq 0} \left|\hat{A}(r)\right| \beta^{\frac{1}{2}}\gamma^{\frac{1}{2}} \leq \frac{\alpha\beta\gamma}{2}$, i.e. $\max_{r \neq 0} \left|\hat{A}(r)\right| \leq \frac{1}{2}\alpha(\beta\gamma)^{\frac{1}{2}}$ then the 3-AP-density of (A, B, C) is at least $\frac{\alpha\beta\gamma}{2}$. Since $\beta\gamma \geq \frac{\alpha^2}{25}$, this tells us that we get 3-APs provided $\max_{r \neq 0} \left|\hat{A}(r)\right| \leq \frac{\alpha^2}{10}$ and $\frac{\alpha^3}{50} > \frac{1}{N}$ (ensures that the progression is non-trivial). So we may assume that $\exists r$ s.t. $\left|\hat{A}(r)\right| \geq \frac{\alpha^2}{10}$.

Lemma 2. *Let $\epsilon > 0$ and let $r \in \mathbb{Z}_N$. Then the set $[N]$ can be partitioned into arithmetic progressions of length at least $\frac{\epsilon}{8\pi}N^{\frac{1}{2}}$ on each of which the function $x \mapsto \omega^{rx}$ varies by at most ϵ.*

Proof. Let $m = \lfloor N^{\frac{1}{2}} \rfloor$. Of the numbers $1, \omega^r, \dots, \omega^{mr}$ there must be two, say ω^{ur} and ω^{vr} with $u < v$, that differ by at most $\frac{2\pi}{m}$.

Let $t = v - u$ and note that $|\omega^{ur} - \omega^{vr}| = |1 - \omega^{tr}|$, so $|1 - \omega^{tr}| \leq \frac{2\pi}{m}$.

Note also that if $a < b$, then

$$\begin{aligned} \left|\omega^{btr} - \omega^{atr}\right| &\leq \sum_{j=1}^{b-a} \left|\omega^{(a+j)tr} - \omega^{(a+j-1)tr}\right| \\ &\leq (b-a)\frac{2\pi}{m} \end{aligned}$$

by the triangle inquality.

Now partition $[N]$ into congruence classes mod t, and partition each congruence class into 'intervals' of length at most $\frac{\epsilon m}{2\pi}$ and at least $\frac{\epsilon m}{4\pi}$. This is possible, since $t \leq m \leq \sqrt{N}$ (exercise). These progressions do the job, since $\frac{\epsilon m}{4\pi} \geq \frac{\epsilon N^{\frac{1}{2}}}{8\pi}$. □

The **balanced function** f of A is defined by $f(x) = A(x) - \alpha$. Note that $\mathbb{E}_x f(x) = 0$ and $\hat{f}(r) = \hat{A}(r)$ when $r \neq 0$.

Let $r \neq 0$ be such that $\left|\hat{f}(r)\right| \geq \frac{\alpha^2}{10}$. Then

$$\begin{aligned} \frac{a^2}{10} &\leq \left|\hat{f}(r)\right| \\ &= \left|\mathbb{E}_x f(x)\omega^{-rx}\right| \\ &= N^{-1}\left|\sum_x f(x)\omega^{-rx}\right| \end{aligned}$$

Now let $\epsilon = \frac{\alpha^2}{20}$ and let $P_1, \dots, P_m$ be given by Lemma 2.

$$\begin{aligned}
N^{-1}\left|\sum_x f(x)\omega^{-rx}\right| &\le N^{-1}\sum_i\left|\sum_{x\in P_i} f(x)\omega^{-rx}\right| \\
&\le N^{-1}\sum_i\left|\sum_{x\in P_i} f(x)(\omega^{-rx}-\omega^{-rx_i})\right| + N^{-1}\sum_i\left|\sum_{x\in P_i} f(x)\omega^{-rx_i}\right| \\
&\quad \text{where } x_i \in P_i \text{ is arbitrary} \\
&\le \frac{\alpha^2}{20} + N^{-1}\sum_i\left|\sum_{x\in P_i} f(x)\right|
\end{aligned}$$

So we may conclude that $\sum_i \left|\sum_{x\in P_i} f(x)\right| \ge \frac{\alpha^2}{20}N$. Also, $\sum_i\sum_{x\in P_i} f(x) = 0$. Therefore, $\sum_i \left(\left|\sum_{x\in P_i} f(x)\right| + \sum_{x\in P_i} f(x)\right) \ge \frac{\alpha^2}{20}N$.

So $\exists i$ s.t. $\left|\sum_{x\in P_i} f(x)\right| + \sum_{x\in P_i} f(x) \ge \frac{\alpha^2|P_i|}{20}$, which implies that

$$\sum_{x\in P_i} f(x) \ge \frac{\alpha^2}{40}|P_i|$$

Or equivalently, $|A\cap P_i| \ge \left(\alpha + \frac{\alpha^2}{40}\right)|P_i|$.

Back of envelope calculation: each time we iterate, α goes to at least $\alpha + \frac{\alpha^2}{40}$, so after $\frac{40}{\alpha}$ iterations, the density at least doubles. So the total number of iterations (before we get a 3-AP) is at most $\frac{40}{\alpha} + \frac{40}{2\alpha} + \frac{40}{4\alpha} + \dots = \frac{80}{\alpha}$.

Each time we iterate, N goes to $\frac{\alpha^2}{20}\frac{N^{\frac{1}{2}}}{8\pi}$, so as long as $N \ge ??$ this is at least $N^{\frac{1}{3}}$. So all the iterative processes have that the new N is at least $N^{\left(\frac{1}{3}\right)^{\frac{80}{\alpha}}}$, which we need to be greater than $\frac{50}{\alpha^3}$.

To solve $N^{\left(\frac{1}{3}\right)^{\frac{80}{\alpha}}} > \frac{50}{\alpha^3}$ take logs twice.

$$\begin{aligned}
\left(\frac{1}{3}\right)^{\frac{80}{\alpha}} \log N &> \log 50 + \log(\alpha^{-3}) \\
\implies \frac{80}{\alpha}\log\left(\frac{1}{3}\right) + \log\log N &> \log(\log 50 + \log(\alpha^{-3}))
\end{aligned}$$

So for an appropriate constant C, we are done if

$$\log\log N \ge \frac{C}{\alpha}, \text{ or } \alpha \ge \frac{C}{\log\log N}$$

Theorem 3 (Behrend, 1947)**.** *For every N there exists a subset $A \subset [N]$ of size $\frac{N}{e^{c\sqrt{\log N}}}$ that contains no 3-AP.*

Proof. For this proof let $[N]$ mean $\{0, 1, \ldots, N-1\}$.

Let m, d be positive integers and consider the grid $[m]^d$. Note that in $\mathbb{R}^d$, no sphere $\{x : x_1^2 + \cdots + x_d^2 = t\}$ contains three distinct points x, y, z with $x + z = 2y$.

But on $[m]^d$, $x_1^2 + \cdots + x_d^2$ takes at most dm^2 different values. Therefore, we can find a sphere that intersects $[m]^d$ in at least $\frac{m^d}{m^2 d}$ points.

Let $\phi : [m]^d \to [(2m)^d]$ be defined by

$$\phi(x) = x_1 + 2mx_2 + (2m)^2 x_3 + \cdots + (2m)^{d-1} x_d$$

So ϕ sends $(x_1, \ldots, x_d)$ to the integer with base-$2m$ representation $x_d x_{d-1} \ldots x_1$.

If we add $\phi(x)$ and $\phi(y)$ then no carrying takes place base-$2m$ since all digits are $< m$. So if $\phi(x) + \phi(z) = 2\phi(y)$ it follows that $x + z = 2y$, i.e. no new 3-APs are created.

So (ignoring divisibility etc.) we can find a subset of $[(2m)^d]$ of size $\frac{m^d}{m^2 d}$ that contains no 3-AP. If we let $N = (2m)^d$, then $m = \frac{N^{\frac{1}{d}}}{2}$ and $\frac{m^d}{m^2 d} = \frac{4N}{2^d N^{\frac{2}{d}} d}$. So we'd like to minimise $2^d N^{\frac{2}{d}} d$.

Take logs: $d \log 2 + \frac{2}{d} \log N + \log d$, so $d = \sqrt{\log N}$ is a pretty good choice. So we get

$$\frac{N}{2^{\sqrt{\log N}} e^{2\sqrt{\log N}} \sqrt{\log N}} \geq \frac{N}{e^{c\sqrt{\log N}}}$$

□

2 Bohr Sets and Boglyubov's Method

Definition (Bohr set)**.** *Let $K \subset \mathbb{Z}_N$ and let $\epsilon > 0$. The* ***Bohr set*** *$B(K, \epsilon)$ is defined to be*

$$\{x \in \mathbb{Z}_N \mid |1 - \omega^{rx}| \leq \epsilon \ \forall r \in K\}$$

Definition (Sumset)**.** *Let A be a subset of an abelian group G. The* ***sumset*** *$A + A$ is $\{x + y \mid x, y \in A\}$. The* ***difference set*** *$A - A$ is $\{x - y \mid x, y \in A\}$. More generally, $\pm A_1 \pm A_2 \pm \cdots \pm A_k = \{\pm x_1 \pm \cdots \pm x_k \mid x_i \in A_i\}$. We write rA for $A + A + \cdots + A$ (r times).*

Lemma 1 (Boglyubov's method)**.** *Let $A \in \mathbb{Z}_N$ be a subset of density α. Then $2A - 2A$ contains a Bohr set $B(K, \sqrt{2})$ with $|K| \leq \alpha^{-2}$.*

Proof. Let $K = \left\{ r : \left| \hat{A}(r) \right| \geq \alpha^{\frac{3}{2}} \right\}$. Observe that $x \in 2A - 2A \iff A * A * (-A) * (-A)(x) \neq 0$ (i.e. $\mathbb{E}_{a+b-c-d=x} A(a)A(b)A(c)A(d) \neq 0$).

But

$$\begin{aligned} A * A * (-A) * (-A)(x) &= \sum_r \widehat{A * A * (-A) * (-A)}(r)\omega^{rx} \text{ (inversion)} \\ &= \sum_r \left| \hat{A}(r) \right|^4 \omega^{rx} \text{ (convolution)} \\ &= \alpha^4 + \sum_{r \in K, r \neq 0} \left| \hat{A}(r) \right|^4 \omega^{rx} + \sum_{r \notin K} \left| \hat{A}(r) \right|^4 \omega^{rx} \end{aligned}$$

for each $x \in B(K, \sqrt{2})$ and each $r \in K$, $\Re(\omega^{rx}) \geq 0$. So if $x \in B(K, \sqrt{2})$, then the second term has real part ≥ 0.

Also,

$$\begin{aligned} \left| \sum_{r \notin K} \left| \hat{A}(r) \right|^4 \omega^{rx} \right| &\leq \sum_{r \notin K} \left| \hat{A}(r) \right|^4 \\ &\leq \max_{r \notin K} \left| \hat{A}(r) \right|^2 \sum_{r \notin K} \left| \hat{A}(r) \right|^2 \\ &< \alpha^3 \cdot \alpha = \alpha^4 \end{aligned}$$

It follows that the sum is not 0. So $B(Km\sqrt{2})$ does the job. Note also that $\alpha^3 |K| \leq \sum_r \left| \hat{A}(r) \right|^2 = \alpha$, so $|K| \leq \alpha^{-2}$, as claimed. □

Lemma 2. *Writing $B[K, \delta]$ for $\{x \in \mathbb{Z}_N \mid \forall r \in K, rx \in [-\delta N, \delta N] \mod N\}$, we have that $B[K, \delta]$ has density at least δ^k, where $k = |K|$.*

Proof. Let $K = \{r_1, \ldots, r_k\}$ and assume (wlog) that $0 \notin K$. Define $\phi : \mathbb{Z}_N \to \mathbb{Z}_N^k$ by $\phi : x \mapsto (r_1 x, \ldots, r_k x)$.

Pick a random translate $\boldsymbol{u} + [\delta N]^k$ of $[\delta N]^k$. On average, this contains at least $\delta^k N$ points of $\operatorname{Im} \phi$.

It follows that there is some translate $\boldsymbol{u} + [\delta N]^k$ that contains at least $\delta^k N$ points of $\operatorname{Im} \phi$. But if $\phi(x), \phi(y) \in \boldsymbol{u} + [\delta N]^k$, then $\phi(x - y) = \phi(x) - \phi(y) \in [-\delta N, \delta N]^k$.

$\implies x - y \in B[K, \delta]$. There are at least $\delta^k N$ distinct such $x - y$. □

Corollary 3. *The Bohr set $B[K, \delta]$ contains an AP (mod N) of length at least $\delta N^{\frac{1}{|K|}}$*

Proof. By Lemma 2, $|B[K, \theta]| \geq \theta^{|K|} N$, so if $\theta > N^{-\frac{1}{|K|}}$ then $|B[K, \theta]| > 1$. By compactness there is some non-zero $x \in B[K, N^{-\frac{1}{|K|}}]$. Then for any m we have that $mx \in B[K, |m| N^{-\frac{1}{|K|}}]$, so $mx \in B[K, \delta]$ whenever $|m| \leq \delta N^{\frac{1}{|K|}}$, which proves the result. $\square$

Definition. *Let A and B be subsets of abelian groups. A map $\phi : A \to B$ is a **Freiman homomorphism of order k** if*

$$\begin{aligned} a_1 + a_2 + \cdots + a_k = a_{k+1} + \cdots + a_{2k} \ \textit{(all } a_i \in A\textit{)} \\ \implies \phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a_{k+1}) + \cdots + \phi(a_{2k}) \end{aligned}$$

*It is a **Freiman isomorphism of order k** if it is a bijection and its inverse is also a Freiman homomorphism of order k (that is, the implication can be reversed).*

The case $k = 2$ is particularly important. It says

$$x + y = z + w \implies \phi(x) + \phi(y) = \phi(z) = \phi(w)$$

or equivalently

$$x - y = z - w \implies \phi(x) - \phi(y) = \phi(z) - \phi(w)$$

Freiman homomorphisms preserve 'additive structure'. Note in particular that Freiman isomorphisms preserve arithmetic progressions.

Definition. *A **lattice of dimension k** is a discrete subgroup of $\mathbb{R}^k$ that spans $\mathbb{R}^k$ in the vector space sense. Equivalently, it is the subgroup generated by some basis $u_1, \ldots, u_k$ of $\mathbb{R}^k$.*

Proposition 4. *Let N be an odd prime, and let $\delta \leq \frac{1}{4}$. Then for every $K \subset \mathbb{Z}_N$, $0 \notin K$, the Bohr set $B[K, \delta]$ is Freiman isomorphic of order 2 to a lattice convex body, that is, the intersection of a convex body with a lattice, of dimension $|K|$*

3 Phïnecke's Theorem and Related Results

If A is a set of integers and $|A + A| \leq C |A|$, how big can $|rA - sA|$ be?

Lemma 1. *Let A_0 and B be subsets of an abelian group G and suppose that $|A_0 + B| = K_0 |A_0|$. Then there exists $A \subset A_0$ and $K \leq K_0$ s.t. $|A + B + C| \leq K |A + C|$ for every $C \subset G$.*

Proof. Let $A \subset A_0$ be a non-empty subset that minimises the ratio $K := \frac{|A+B|}{|A|}$. Then $|A' + B| \geq K |A'|$ for every $A' \subset A$.

We now prove that $|A + B + C| \leq K |A + C|$ by induction on $|C|$. When $C = \emptyset$ we're done by hypothesis. So suppose we have the result for C. We would like to show that if $x \notin C$, then

$$|A + B + (C \cup x)| \leq K |A + (C \cup x)|$$

but

$$\begin{aligned} A + (C \cup x) &= (A + C) \cup (A + x) \\ &= (A + C) \cup (A' + x) \end{aligned}$$

where $A' = \{a \in A \,|\, a + x \notin A + C\}$.

Since this is a disjoint union, $|A + (C \cup x)| = |A + C| + |A'|$

Also, $A + B + (C \cup x) = (A + B + C) \cup (A + B + x)$. So

$$\begin{aligned} |A + B + (C \cup x)| &= |A + B + C| + |A + B + x| - |(A + B + C) \cap (A + B + x)| \\ &\leq |A + B + C| + |A + B| - |(A')^c + B + x| \\ &\leq K |A + C| + K |A| - K |(A')^c| \\ &= K |A + C| + K |A'| \\ &= K |A + (C \cup x)| \end{aligned}$$

□