Part III – Introduction to Discrete Analysis (Ongoing course, rough)

Based on lectures by Professor W. T. Gowers
Notes taken by Bhavik Mehta

Michaelmas 2018

Contents

1 The discrete Fourier transform

Let N be some fixed positive integer. Write ω for $e^{\frac{2\pi i}{N}}$, and $\mathbb{Z}_N$ for $\mathbb{Z}/N\mathbb{Z}$.

Definition (Discrete Fourier transform)**.** Let $f : \mathbb{Z}_N \to \mathbb{C}$. Given $r \in \mathbb{Z}_N$, define $\hat{f}(r)$ to be

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x)\omega^{-rx}.$$

Notation. From now on, we shall use notation $\mathbb{E}_{x\in\mathbb{Z}_N}$ for $\frac{1}{N}\sum_{x\in\mathbb{Z}_N}$, where the subscript is omitted when it is clear from context.

Notice we can write

$$\hat{f}(r) = \mathop{\mathbb{E}}_x f(x)e^{-\frac{2\pi i r x}{N}},$$

highlighting the similarity with the usual Fourier transform.

If we write ω_r for the function $x \mapsto \omega^{rx}$, and $\langle f, g\rangle$ for $\mathbb{E}_x f(x)\overline{g(x)}$, then $\hat{f}(r) = \langle f, \omega_r\rangle$. Let us write $\|f\|_p$ for $(\mathbb{E}_x |f(x)|^p)^{\frac{1}{p}}$ and call the resulting space $L_p(\mathbb{Z}_N)$.

Important convention. We use *averages* for the 'original functions' in 'physical space' and *sums* for their Fourier transforms in 'frequency space'.

Lemma 1.1 (Parseval's identity)**.** If $f, g : \mathbb{Z}_N \to \mathbb{C}$, then $\langle \hat{f}, \hat{g}\rangle = \langle f, g\rangle$.

Proof.

$$\begin{aligned}
\langle \hat{f}, \hat{g}\rangle &= \sum_r \hat{f}(r)\overline{\hat{g}(r)} \\
&= \sum_r (\mathop{\mathbb{E}}_x f(x)\omega^{-rx})\overline{(\mathop{\mathbb{E}}_y g(y)\omega^{-ry})} \\
&= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_y f(x)\overline{g(y)}\sum_r \omega^{-r(x-y)} \\
&= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_y f(x)\overline{g(y)}\Delta_{xy} \\
&= \mathop{\mathbb{E}}_x f(x)\mathop{\mathbb{E}}_y \overline{g(y)}\Delta_{xy} \\
&= \mathop{\mathbb{E}}_x f(x)\overline{g(x)} = \langle f, g\rangle
\end{aligned}$$

where

$$\Delta_{xy} = \begin{cases} N & x = y \\ 0 & x \neq y. \end{cases}$$

□

Definition (Convolution)**.** The convolution $\widehat{f * g}(x)$ is defined to be

$$\mathop{\mathbb{E}}_{y+z=x} f(y)g(z) = \mathop{\mathbb{E}}_y f(y)g(x-y).$$

Lemma 1.2 (Convolution identity)**.**

$$\widehat{f * g}(r) = \hat{f}(r)\hat{g}(r).$$

Proof.

$$\begin{aligned}
\widehat{f * g}(r) &= \mathop{\mathbb{E}}_{x} f * g(x)\omega^{-rx} \\
&= \mathop{\mathbb{E}}_{x} \mathop{\mathbb{E}}_{y+z=x} f(y)g(z)\omega^{-rx} \\
&= \mathop{\mathbb{E}}_{x} \mathop{\mathbb{E}}_{y+z=x} f(y)g(z)\omega^{-ry}\omega^{-rz} \\
&= \mathop{\mathbb{E}}_{y} f(y)\omega^{-ry} \mathop{\mathbb{E}}_{z} g(z)\omega^{-rz} = \hat{f}(r)\hat{g}(r).
\end{aligned}$$

□

Lemma 1.3 (Inversion formula)**.**

$$f(x) = \sum_r \hat{f}(r)\omega^{rx}$$

Proof.

$$\begin{aligned}
\sum_r \hat{f}(r)\omega^{rx} &= \sum_r \mathop{\mathbb{E}}_{y} f(y)\omega^{r(x-y)} \\
&= \mathop{\mathbb{E}}_{y} f(y) \sum_r \omega^{r(x-y)} \\
&= \mathop{\mathbb{E}}_{y} f(y)\Delta_{xy} = f(x).
\end{aligned}$$

□

Further observations:

- If f is real-valued, then $\hat{f}(-r) = \mathbb{E}_x f(x)\omega^{rx} = \overline{\mathbb{E}_x f(x)\omega^{-rx}} = \overline{\hat{f}(r)}$.
- If $A \subset \mathbb{Z}_n$, write A (instead of $\mathbb{1}_A$ or χ_A) for the characteristic function of A. Then $\hat{A}(0) = \mathbb{E}_x A(x) = \frac{|A|}{N}$, the density of A.
- Also, $\|\hat{A}\|_2^2 = \langle \hat{A}, \hat{A} \rangle = \langle A, A \rangle = \mathbb{E}_x A(x)^2 = \mathbb{E}_x A(x) = \frac{A}{N}$.

Let $f : \mathbb{Z}_N \to \mathbb{C}$. Given $\mu \in \mathbb{Z}_N$ with $(\mu, N) = 1$, define $f_\mu(x)$ to be $f(\mu^{-1}x)$. Then

$$\begin{aligned}
\hat{f}_\mu(r) &= \mathop{\mathbb{E}}_{x} f_\mu(x)\omega^{-rx} \\
&= \mathop{\mathbb{E}}_{x} f(x/\mu)\omega^{-rx} \\
&= \mathop{\mathbb{E}}_{x} f(x)\omega^{-r\mu x} \\
&= \hat{f}(\mu r).
\end{aligned}$$

1.1 Roth's Theorem

Theorem 1.4. For every $\delta > 0$, there exists N such that if $A \subseteq \{1, \ldots, N\}$ is a set of size at least δN then A must contain an arithmetic progression of length 3.

This is the $k = 3$ case of Szemerédi's theorem.

Basic strategy: show that if A has density $\geq \delta$ and no arithmetic progression of length 3, then there is a long arithmetic progression $P \subseteq \{1, \ldots, N\}$ such that

$$|A \cap P| \geq (\delta + c(\delta))|P|.$$

In particular, we have that $|P| \to \infty$ as $N \to \infty$.

The proof we give will produce a bound $\delta \geq \frac{C}{\log \log N}$, but this is not the best known. If the bound was reduced to $\frac{1}{\log N}$, this produces a combinatorial proof of the fact that there are arbitrarily long arithmetic progressions in the primes. The best known bound is $\frac{(\log \log N)^4}{\log N}$ by Thomas Bloom. In the other direction, we know $e^{-\sqrt{\log N}}$ does not work.

Lemma 1.5. Let $A, B, C \subset \mathbb{Z}_N$ have densities α, β, γ, for N odd. If $\max_{r \neq 0} |\hat{A}(r)| \leq \frac{\alpha(\beta\gamma)^{\frac{1}{2}}}{2}$ and $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$ then there exists $x, d \in \mathbb{Z}_N$ with $d \neq 0$ such that $(x, x+d, x+2d) \in A \times B \times C$.

Proof.

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

We have a lower bound on the left term, so focus on the right.

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

The contribution to $\mathbb{E}_{x,d}\, A(x)B(x+d)C(x+2d)$ from $d=0$ is at most $\frac{1}{N}$, so if $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$, we are done. $\square$

Now let A be a subset of $\{1,\dots,N\}$ of density $\geq \delta$ and let $B = C = A \cap (\frac{N}{3}, \frac{2N}{3}]$. If B has density $< \frac{\delta}{5}$, then either $A \cap [1, \frac{N}{3}]$ or $A \cap [\frac{2N}{3}, N]$ has density at least $\frac{2\delta}{5}$. So in that case we find an AP P of length about $\frac{N}{3}$ such that $\frac{|A\cap P|}{|P|} \geq \frac{6\delta}{5}$.

Otherwise, we find that if $\max_{r\neq 0} |\hat{A}(r)| \leq \frac{\delta^2}{10}$ and $\frac{\delta^3}{50} > \frac{1}{N}$ then $A \times B \times C$ contains a 3AP $\implies$ A contains a 3AP. So if A does not contain a 3AP, then either we find P of length about $\frac{N}{3}$ with $\frac{|A\cap P|}{|P|} \geq \frac{6\delta}{5}$ or $\exists r \neq 0$ such that $|\hat{A}(r)| \geq \frac{\delta^2}{10}$.

Definition. If X is a finite set and $f : X \to \mathbb{C}$, $Y \subseteq X$, write $\operatorname{osc}(f|_Y)$ to mean $\max_{y_1,y_2\in Y} |f(y_1) - f(y_2)|$.

Lemma 1.6. Let $r \in \hat{\mathbb{Z}}_n$ and let $\epsilon > 0$. Then there is a partition of $\{1,2,\dots,N\}$ into arithmetic progressions P_i of length at least $c(\epsilon)\sqrt{N}$ such that $\operatorname{osc}(\omega_r|_{P_i}) \leq \epsilon$ for each i.

Proof. Let $t = \lfloor \sqrt{N} \rfloor$. Of the numbers $1, \omega^r, \omega^{2r}, \dots, \omega^{tr}$ there must be two that differ by at most $\frac{2\pi}{t}$. If $|\omega^{ar} - \omega^{br}| \leq \frac{2\pi}{t}$ with $a < b$, then $|1 - \omega^{dr}| \leq \frac{2\pi}{t}$ where $d = b-a$. Now, by the triangle inequality, if $u < v$, then

$$|\omega^{urd} - \omega^{vrd}| \leq |\omega^{urd} - \omega^{(u+1)rd}| + |\omega^{urd} - \omega^{(u+1)rd}| + \cdots + |\omega^{urd} - \omega^{(u+1)rd}| \leq \frac{2\pi}{t}(v-u).$$

So if P is a progression with common difference d and length l, then $\operatorname{osc}(\omega_r|_P) \leq \frac{2\pi l}{t}$. So divide up $\{1,\dots,N\}$ into residue classes mod d and partition each residue class into parts of length between $\frac{\epsilon t}{4\pi}$ and $\frac{\epsilon t}{2\pi}$ (possible, since $d \leq t \leq \sqrt{N}$). We are done, with $c(\epsilon) = \frac{\epsilon}{16}$. $\square$

Now let us use the information that $r \neq 0$ and $|\hat{A}(r)| \geq \frac{\delta^2}{10}$. Define the balanced function f of A by $f(x) = A(x) - \frac{|A|}{N}$ for each x.

Note that $\hat{f}(0) = 0$ and $\hat{f}(r) = \hat{A}(r)$ for all $r \neq 0$. Now let $P_1, \dots, P_m$ be given by Lemma 1.6 with $\epsilon = \frac{\delta^2}{20}$. Then

$$\begin{aligned} \frac{\delta^2}{10} \leq \frac{1}{N}\left|\sum_x f(x)\omega^{-rx}\right| &\leq \frac{1}{N}\sum_{i=1}^m \left|\sum_{x\in P_i} f(x)\omega^{-rx}\right| \\ &\leq \frac{1}{N}\sum_{i=1}^m \left[\left|\sum_{x\in P_i} f(x)\omega^{-rx_i}\right| + \left|\sum_{x\in P_i} f(x)(\omega^{-rx} - \omega^{-rx_i})\right|\right] \end{aligned}$$

where $x_i \in P_i$ is arbitrary

$$\leq \frac{1}{N}\sum_{i=1}^m \left|\sum_{x\in P_i} f(x)\right| + \frac{\delta^2}{20}$$

So

$$\sum_{i=1}^N \left|\sum_{x\in P_i} f(x)\right| \geq \frac{\delta^2 N}{20}.$$

Also,

$$\sum_{i=1}^{m} \sum_{x \in P_i} f(x) = 0.$$

So

$$\sum_{i=1} \left(\left| \sum_{x \in P_i} f(x) \right| + \sum_{x \in P_i} f(x) \right) \geq \frac{\delta^2}{20} \sum_{i=1}^{m} |P_i|$$

Therefore, $\exists i$ such that

$$\left| \sum_{x \in P_i} f(x) \right| + \sum_{x \in P_i} f(x) \geq \frac{\delta^2}{20} |P_i|$$
$$\implies \sum_{x \in P_i} f(x) \geq \frac{\delta}{40} |P_i|$$
$$\implies |A \cap P_i| \geq \left(\delta + \frac{\delta^2}{40} \right) |P_i|$$

So now, either

1. A contains a $3AP$
2. N is even
3. $\exists P \subset \{1, \dots, N\}$, $|P| \geq \frac{N}{3}$ such that $|A \cap P| \geq \frac{6\delta}{5} |P|$
4. $\exists P \subset \{1, \dots, N\}$, $|P| \geq \frac{\delta^2}{320} \sqrt{N}$ such that $|A \cap P| \geq \left(\delta + \frac{\delta^2}{40} \right) |P|$

If 2 holds, write $N = N_1 + N_2$ with N_1, N_2 odd, $N_1 + N_2 \approx \frac{N}{2}$. Then A has density at least δ in one of $\{1, \dots, N_1\}$ or $\{N_1 + 1, \dots, N_1 + N_2\}$.

If 4 holds (note $3 \Rightarrow 4$) then we pass to P and start again. After $\frac{40}{\delta}$ iterations, the density at least doubles. So the total number of iterations we can have is $\leq \frac{40}{\delta} + \frac{40}{2\delta} + \frac{40}{4\delta} + \dots \leq \frac{80}{\delta}$.

If $\frac{\delta^2}{320} \sqrt{N} \geq N^{\frac{1}{3}}$ at each iteration, and $\frac{\delta^3}{25} > N^{-1}$ (which follows from the first condition) then after $\frac{80}{\delta}$ iterations we have $N \geq N^{\left(\frac{1}{3}\right)^{\frac{80}{\delta}}}$. So the argument works provided

$$\begin{aligned} N^{\left(\frac{1}{3}\right)^{\frac{80}{\delta}}} \geq \left(\frac{320}{\delta^2} \right)^6 &\impliedby \left(\frac{1}{3} \right)^{\frac{80}{\delta}} \log N \geq 6 \left(\log 320 + 2 \log \frac{1}{\delta} \right) \\ &\impliedby -\frac{80}{\delta} \log 3 + \log\log N \geq \log 6 + \log \left(\log 320 + 2 \log \frac{1}{\delta} \right) \\ &\impliedby \log\log N \geq \frac{160}{\delta} \impliedby \delta \geq \frac{160}{\log\log N}. \end{aligned}$$

1.2 Bogolyubov's method

Let $K \subset \hat{\mathbb{Z}}_N$ and let $\delta > 0$.

Definition (Bohr set)**.** The **Bohr set** $B(K, \delta)$ has two definitions.

1. $B(K, \delta) = \{ x \in \mathbb{Z}_N \mid rx \in [-\delta N, \delta N] \ \forall r \in K \}$ (arc-length definition)
2. $B(K, \delta) = \{ x \in \mathbb{Z}_N \mid |1 - \omega^{rx}| < \delta \ \forall r \in K \}$ (chord-length definition)

Definition. Let G be an abelian group and let A, B be subsets of G. Then

$$\begin{aligned} A + B &= \{ a + b \mid a \in A, b \in B \} \\ A - B &= \{ a - b \mid a \in A, b \in B \} \\ rA &= \{ a_1 + \cdots + a_r \mid a_1, \ldots, a_r \in A \} \end{aligned}$$

Lemma 1.7. Let $A \subset \mathbb{Z}_N$ be a set of density α. Then $2A - 2A$ contains a Bohr set (arc) with $|K| \geq \alpha^{-2}$.

Proof. Observe that $x \in 2A - 2A$ iff $A * A * (-A) * (-A)(x) \neq 0$. But

$$\begin{aligned} A * A * (-A) * (-A)(x) &= \sum_r \widehat{A * A * (-A) * (-A)}(r)\omega^{rx} \\ &= \sum_r |\hat{A}(r)|^4 \omega^{rx}. \end{aligned}$$

Let $K = \{ r \mid |\hat{A}(r)| \geq \alpha^{\frac{3}{2}} \}$. Then $\alpha = \|\hat{A}\|_2^2 = \sum_r |\hat{A}(r)|^2 \geq \alpha^3 |K|$ So $|K| \leq \alpha^{-2}$.

Now suppose that $x \in B(K, \frac{1}{4})$. Then

$$\sum_r |\hat{A}(r)|^4 \omega^{rx} = \alpha^4 + \sum_{r \in K \setminus \{0\}} |\hat{A}(r)|^4 \omega^{rx} + \sum_{r \notin K} |\hat{A}(r)|^4 \omega^{rx}.$$

The real part of the second term is non-negative, since $rx \in \left[-\frac{N}{4}, \frac{N}{4}\right]$ when $r \in K$. Also

$$\left| \sum_{r \notin K} |\hat{A}(r)|^4 \omega^{rx} \right| \leq \sum_{r \notin K} |\hat{A}(r)|^4 < \alpha^3 \sum_{r \notin K} |\hat{A}(r)|^2 \leq \alpha^4.$$

It follows that $\mathrm{Re}\left(\sum_r |\hat{A}(r)|^4 \omega^{rx}\right) > 0$, so $x \in 2A - 2A$. □

Lemma 1.8. Let $K \subset \mathbb{Z}_N$ and let $\delta > 0$. Then

(i) $B(K, \delta)$ (arc) has density at least $\delta^{|K|}$

(ii) $B(K, \delta)$ contains a mod-N arithmetic progression of length $\geq \delta N^{\frac{1}{|K|}}$

Proof.

(i) Let $K = \{r_1, \ldots, r_k\}$. Consider the N k-tuples $(r_1 x, r_2 x, \ldots, r_k x) \in \mathbb{Z}_N^k$. If we intersect this set of k-tuples with a random 'box' $[t_1, t_1 + \delta N] \times \cdots \times [t_k, t_k + \delta N]$ then the expected number of the k-tuples in the box is $\delta^k N$ (since each one has a probability δ^k). But if $(r_1 x, \ldots, r_k x)$ and $(r_1 y, \ldots, r_k y)$ belong to this box, then $x - y \in B(K, \delta)$.

(ii) If we take $\eta > N^{\frac{1}{2}}$, then by (i) we get that $|B(K,\eta) > 1$, so $\exists x \in B(K,\eta)$ such that $x \neq 0$. But then $dx \in B(K, d\eta)$ for every d. So if $d\eta \leq \delta$ then $dx \in B(K,\delta)$. That gives us an AP of length at least $\frac{\delta}{\eta}$. So we get one of length at least $\delta N^{\frac{1}{k}}$. $\square$

Definition (Freiman homomorphism)**.** Let A, B be subsets of Abelian groups and let $\phi : A \to B$. Then ϕ is a **Freiman homomorphism of order** k if

$$a_1 + \cdots + a_k = a_{k+1} + \ldots + a_{2k} \implies \phi(a_1) + \cdots + \phi(a_k) = \phi(a_{k+1}) + \cdots + \phi(a_{2k}).$$

If $k = 2$, we call this a **Freiman homomorphism**. In that case, the condition is equivalent to $a - b = c - d \implies \phi(a) - \phi(b) = \phi(c) - \phi(d)$.

If ϕ has an inverse which is also a Freiman homomorphism of order k, then ϕ is a Freiman isomorphism of order k.

Lemma 1.9. Assume $0 \notin K$ and N prime. If $\delta < \frac{1}{4}$, then $B(K,\delta)$ (arc) is Freiman isomorphic to the intersection in $\mathbb{R}^K$ of $[-\delta N, \delta N]^{|K|}$ with some lattice Δ.

Proof. Let $K = \{r_1, \ldots, r_k\}$ and let $\Lambda = N\mathbb{Z}^k + \{\, (r_1 x, \ldots, r_k x) \mid x \in \mathbb{Z}\,\}$. Write $\mathbf{r}$ for $(r_1, \ldots, r_k)$. Claim that $B(K,\delta) \cong \Lambda \cap [-\delta N, \delta N]^k$. Define a map $\phi : B(K,\delta) \to \Lambda \cap [-\delta N, \delta N]^k$ by sending x to $(\langle r_1 x\rangle, \ldots, \langle r_k x\rangle)$ where $\langle u\rangle$ means the least-modulus residue of u mod N.

If $x + y = z + w$, then $\mathbf{r}x + \mathbf{r}y = \mathbf{r}z + \mathbf{r}w$ in $\mathbb{Z}_N^k$. But for each i, $\langle r_i x\rangle + \langle r_i y\rangle - \langle r_i z\rangle - \langle r_i w\rangle \in [-4\delta N, 4\delta N]$. Since $\delta < \frac{1}{4}$, that implies that $\langle r_i x\rangle + \langle r_i y\rangle - \langle r_i z\rangle - \langle r_i w\rangle = 0$. So $\langle \mathbf{r}x\rangle + \langle \mathbf{r}y\rangle = \langle \mathbf{r}z\rangle + \langle \mathbf{r}w\rangle$.

That already implies that ϕ is an injection. If $\mathbf{r}x + \mathbf{a}N \in [-\delta N, \delta N]^k$ then $r_i x \in [-\delta N, \delta N]$ mod N for each i, so $x \in B(K,\delta)$ and $\phi(x) = \mathbf{r}x + \mathbf{a}N$. So ϕ is a surjection.

If $\mathbf{r}x + \mathbf{a}N + \mathbf{r}y + \mathbf{b}N = \mathbf{r}z + \mathbf{c}N + \mathbf{r}w + \mathbf{d}N$, then $r_1(x+y) = r_1(z+w)$ mod N, so $x + y = z + w$ mod N. So the inverse of ϕ is also a Freiman homomorphism. $\square$

Lemma 1.10. Let Λ be a lattice and let C be a symmetric convex body, both in $\mathbb{R}^k$. Then $\Lambda \cap C \leq 5^k |\Lambda \cap \frac{C}{2}|$.

Proof. Let $x_1, \ldots, x_n$ be a maximal subset of $\Lambda \cap C$ such that for all $i \neq j$, $x_j \notin x_i + \frac{C}{2}$. Then by maximality, the sets $x_i + \frac{C}{2}$ cover all of $\Lambda \cap C$. Also, the sets $x_i + \frac{C}{4}$ are disjoint subsets of $\mathbb{R}^k$, and they are all contained in $C + \frac{C}{4} = \frac{5}{4}C$. So

$$m \leq \frac{\mathrm{vol}(\frac{5}{4}C)}{\mathrm{vol}(\frac{1}{4}C)} = 5^k.$$

$\square$

Corollary 1.11. If N is prime, $0 \notin K$, $|K| = k$, $\delta < \frac{1}{4}$, then $|B(K,\delta)| \leq 5^k |B(K, \frac{\delta}{2})$.

2 Sumsets and their structure

The idea is to show that for $A \subset \mathbb{Z}$, if $|A+A| \le K|A|$ then $|rA - sA| \le K^{r+s}|A|$.

Lemma 2.1 (Petridis)**.** Let A_0, B be finite subsets of an abelian group such that $|A_0 + B| \le K_0|A_0|$. Then there exists a non-empty subset $A \subset A_0$ and $K \le K_0$ such that $|A+B+C| \le K|A+C|$ for every finite subset C of the group.

Proof. Let A minimise the ratio $\frac{|A+B|}{|A|}$ and let the minimal ratio be K. Claim: this works. We prove this by induction on C.

If $C = \varnothing$, then the result holds. Now assume it for C and let $x \notin C$. Then

$$A + (C \cup \{x\}) = (A+C) \cup (A + \{x\}) = (A+C) \cup [(A+x) \setminus (A'+x)]$$

where $A' = \{ a \in A \mid a + x \in A + C \}$. This is a disjoint union, so

$$|A + (C \cup \{x\})| = |A+C| + |A| - |A'|.$$

Similarly,

$$A + B + (C \cup \{x\}) = (A+B+C) \cup ((A+B+x) \setminus (A'+B+x))$$

(since if $a + x \in A + C$ then $a + B + x \subset A + B + C$)

$$\begin{aligned} \implies |A+B+(C\cup\{x\})| &\le |A+B+C| + |A+B| - |A'+B| \\ &\le K|A+C| + K|A| - K|A'| \end{aligned}$$

by induction and minimality property of A. □

Corollary 2.2. If A, B are finite subsets of an Abelian group and $|A+B| \le K|A|$, then there exists $A' \subseteq A$, $A' \ne \varnothing$ such that $|A' + rB| \le K^r|A'|$ for every positive integer r.

Proof. Choose A' as we chose A in the proof of Lemma 2.1. Then

$$|A' + rB| = |A' + B + (r-1)B| \le K|A' + (r-1)B|$$

and $|A'+B| \le K|A'|$ so we are done by induction. □

Corollary 2.3. If $|A+A| \le K|A|$ or $|A-A| \le K|A|$, then $|rA| \le K^r|A|$.

Proof. Set $B = A$ or $-A$ in Corollary 2.2 □

Lemma 2.4 (Rusza inequality)**.** Let A, B, C be finite subsets of an abelian group. Then $|A||B-C| \le |A-B||A-C|$.

Proof. Define a map $\phi : A \times (B-C) \to (A-B) \times (A-C)$ as follows. Given (a,x) with $a \in A, x \in B - C$, choose, somehow, $b(x) \in B$ and $c(x) \in C$ such that $b(x) - c(x) = x$ and set $\phi(a,x) = (a - b(x), a - c(x))$.

Note that $(a - c(x)) - (a - b(x)) = b(x) - c(x) = x$. Having worked out x, we know $b(x)$ and $a = a - b(x) + b(x)$, so a is determined too. So ϕ is an injection. □

Why is it called a triangle inequality? We can write it as

$$\frac{|B-C|}{|B|^{\frac{1}{2}}|C|^{\frac{1}{2}}} \le \frac{|A-B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}} + \frac{|A-C|}{|A|^{\frac{1}{2}}|C|^{\frac{1}{2}}}$$

so if we define the Rusza distance $d(A,B)$ to be

$$\frac{|A-B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}},$$

then the inequality says $d(B,C) \le d(A,B)d(A,C)$.

Corollary 2.5. If $|A-B| \le K|A|$, then $|rB - sB| \le K^{r+s}|A|$ for all r, s.

Proof. Pick A' as before. Then by Corollary 2.2 with B replaced by $-B$, $|A' - rB| \le K'|A'|$ and $|A' - sB| \le K^s|A'|$. Therefore, by Rusza inequality,

$$|A'||rB - sB| \le K^{r+s}|A'|^2 \implies |rB - sB| \le K^{r+s}|A|. \qquad \square$$

Corollary 2.6 (Plünnecke's theorem)**.** If $|A+A| \le K|A|$ or $|A-A| \le K|A|$, then $|rA-sA| \le K^{r+s}|A|$.

Proof. Apply Corollary 2.5 with $B = -A$ or $B = A$. $\square$

Lemma 2.7 (Ruzsa's embedding theorem)**.** Let $A \subseteq \mathbb{Z}$ be finite and suppose that $|kA - kA| \le C|A|$. Then there exists a prime $p \le 4C|A|$ and a subset $A' \subseteq A$ of size at least $|A|/k$ such that A' is Freiman isomorphic of order k to a subset of $\mathbb{Z}_p$.

Proof. Consider the following composition of maps

$$\mathbb{Z} \xrightarrow{\text{reduce mod } q} \mathbb{Z}_q \xrightarrow[\text{non-zero } r]{\times \text{ by some}} \mathbb{Z}_q \xrightarrow[\text{residue}]{\text{least non-negative}} \mathbb{Z} \xrightarrow{\text{reduce mod } p} \mathbb{Z}_p$$

where q is a prime bigger than $\operatorname{diam} A$ and p is a prime $\in (2C|A|, 4C|A|]$.

Let ϕ be the composition. The first, second and fourth parts are group homomorphisms, and thus Freiman homomorphisms of all orders. Also, the third map is a Freiman homomorphism of order k if you restrict to a subinterval of $[0, q-1]$ of length $\le \frac{q}{k}$. To see this, write $\langle u \rangle$ for the least non-negative residue. Then if I has length $\le \frac{q}{k}$ (and therefore $< \frac{q}{k}$) and $u_1, \dots, u_{2k} \in I$, then if $u_1 + \dots + u_k - u_{k+1} - \dots - u_{2k} = 0$, then

$$\langle u_1 \rangle + \dots + \langle u_k \rangle - \langle u_{k+1} \rangle - \dots - \langle u_{2k} \rangle \equiv 0 \pmod q$$

and also has modulus less than q. So it is zero.

By the pigeonhole principe, for any r we can find I of length $\le \frac{q}{k}$ such that

$$A' = \{\, a \in A \mid ra \in I \,\}$$

has size at least $|A|/k$.

Remains to prove that ϕ is an isomorphism to its image. That is, we must show that if

$$a_1 + \dots + a_k - a_{k+1} - \dots a_{2k} \equiv 0 \quad (a_i \in A)$$

then

$$\langle ra_1 \rangle + \cdots + \langle ra_k \rangle - \langle ra_{k+1} \rangle - \langle ra_{2k} \rangle \neq 0 \pmod p$$

But if the a_i are chosen such that the ra_i all belong to the same interval of length $\frac{q}{k}$,

$$|\langle ra_1 \rangle + \cdots \langle ra_k \rangle - \langle ra_{k+1} \rangle - \cdots - \langle ra_{2k} \rangle| < q$$

and

$$\langle ra_1 \rangle + \cdots + \langle ra_k \rangle - \langle ra_{k+1} \rangle - \cdots - \langle ra_{2k} \rangle \equiv r(a_1 + \cdots + a_k - a_{k+1} - \cdots - a_{2k}) \bmod q$$

So all that can go wrong is if $r(a_1 + \cdots + a_k - a_{k+1} - \cdots - a_{2k})$ is xp for some $x \neq 0$ with $|x| < \frac{q}{p}$. The number of values to avoid is at most $\frac{2q}{p}$, so for each $a_1 + \cdots + a_k - a_{k+1} - \ldots - a_{2k}$ the probability of going wrong if r is chosen randomly is at most $\frac{2}{p}$. So since $|kA - kA| \leq C|A|$, the probability of going wrong is at most $\frac{2}{p}C|A|$. Since $p > 2C|A|$, there exists r such that we get a Freiman isomorphism of order k. □