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 (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 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 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 4. For every $\delta > 0$, there exists N such that if $A \subseteq \{1, \dots, N\}$ 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 $P \subseteq \{1, \dots, N\}$ 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 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 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 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
$$\begin{aligned}\left|\sum_{x\in P_i} f(x)\right| + \sum_{x\in P_i} f(x) &\geq \frac{\delta^2}{20}|P_i| \\ \implies \sum_{x\in P_i} f(x) &\geq \frac{\delta}{40}|P_i| \\ \implies |A\cap P_i| &\geq \left(\delta + \frac{\delta^2}{40}\right)|P_i|\end{aligned}$$

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 $\leq \frac{40}{\delta} + \frac{40}{2\delta} + \frac{40}{4\delta} + \ldots \leq \frac{80}{\delta}$.

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

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

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 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 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 $\delta N^{\frac{1}{k}}$.

$\square$