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 $A \subseteq \{1, \ldots, N\}$ 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 $\frac{C}{\log\log N}$, 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, **add the bound**.