

Introduction to Discrete Analysis

proof) dddddd

=====

(4th October 2018, Thursday)

Chapter 1. The discrete Fourier transform

Let N be some fixed positive integer. Write ω for $e^{2\pi i/N}$. and \mathbb{Z}_N for $\mathbb{Z}/N\mathbb{Z}$. Let $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Given $r \in \mathbb{Z}_N$ define $\widehat{f}(r)$ to be $\frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) \omega^{-rx}$. From now on, we shall use the notation $\mathbb{E}_{x \in \mathbb{Z}_N}$ for $\frac{1}{N} \sum_{x \in \mathbb{Z}_N}$ (so that $\widehat{f}(r) = \mathbb{E}_x f(x) e^{-2\pi i r x / N}$). 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 $\widehat{f}(r) = \langle f, \omega_r \rangle$.

Let us write $\|f\|_p$ for $(\mathbb{E}_x |f(x)|^p)^{1/p}$ 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 spaces".

Lemma 1) (Parseval's identity) If $f, g : \mathbb{Z}_N \rightarrow \mathbb{C}$, then $\langle \widehat{f}, \widehat{g} \rangle = \langle f, g \rangle$.

proof)

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

where $\Delta_{xy} = N$ if $x = y$ and 0 if $x \neq y$ (in analogy with δ -distribution).

(End of proof) \square

Lemma 2) (Convolution identity) $\widehat{f * g}(r) = \widehat{f}(r) \widehat{g}(r)$

proof) The convolution $f * g(x)$ is defined to be $\mathbb{E}_{y+z=x} f(y) g(z) = \mathbb{E}_y f(y) g(x-y)$. Then,

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

(End of proof) \square

Lemma 3) (Inversion formula) $f(x) = \sum_r \widehat{f}(r) \omega^{rx}$.

proof)

$$\sum_r \widehat{f}(r) \omega^{rx} = \sum_r \mathbb{E}_y f(y) \omega^{r(x-y)} = \mathbb{E}_y f(y) \sum_r \omega^{r(x-y)} = \mathbb{E}_y f(y) \Delta_{xy} = f(x)$$

(End of proof) \square

Further Observations :

- If f is real-valued, then $\widehat{f}(-r) = \mathbb{E}_x f(x) \omega^{rx} = \overline{\mathbb{E}_x f(x) \omega^{-rx}} = \overline{\widehat{f}(r)}$.
- If $A \subset \mathbb{Z}_N$, write A (instead of 1_A or χ_A) for the characteristic function of A . Then $\widehat{A}(0) = \mathbb{E}_x A(x) = \frac{|A|}{N}$, the **density** of A . Also, $\|\widehat{A}\|_2^2 = \langle \widehat{A}, \widehat{A} \rangle = \langle A, A \rangle = \mathbb{E}_x A(x)^2 = |A|/N$.
- Let $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Given $\mu \in \mathbb{Z}_N$ with $(\mu, N) = 1$, define $f_\mu(x)$ to be $f(\mu^{-1}x)$. Then $\widehat{f}_\mu(r) = \mathbb{E}_x f_\mu(x) \omega^{-rx} = \mathbb{E}_x f(x/\mu) \omega^{-rx} = \mathbb{E}_x f(x) \omega^{-r\mu x} = \widehat{f}(\mu r)$.

Roth's Theorem

Theorem 4 (Szemerédi's theorem for $k = 3$) For every $\delta > 0$, there exists N such that if $A \subset \{1, \dots, N\}$ is a set of size at least δN , then A must contain an arithmetic progression of length 3.

Basic strategy : show that if A has density $\geq \delta$ and no 3AP, then there is a long arithmetic progression $P \subset \{1, \dots, n\}$ such that

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

=====

(9th October, Tuesday)

Theorem 4 (Roth's theorem, or Szemerédi's theorem for $k = 3$) For every $\delta > 0$, there exists N such that if $A \subset \{1, \dots, N\}$ is a set of size at least δN , then A must contain an arithmetic progression of length 3.

Lemma 5 Let $A, B, C \subset \mathbb{Z}_N$ have densities α, β, γ . If $\max_{r \neq 0} |\widehat{A}(r)| \leq \frac{\alpha(\beta\gamma)^{1/2}}{2}$ and $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$ then there exist $x, d \in \mathbb{Z}_N$ with $d \neq 0$ s.t. $(x, x+d, x+2d) \in A \times B \times C$.

proof Assume N is odd.

Consider the function $A(x)B(x+d)C(x+2d)$, which is non-zero if and only if there is a arithmetic progression of length 3. So $\mathbb{E}_{x,d} A(x)B(x+d)C(x+2d)$ counts the density of x, d satisfying such condition.

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

(Recall, $B_\mu(x)$ is defined to be $B(\mu^{-1}x)$ whenever $(\mu, N) = 1$. We can generalize this to write $B_\mu(x) = \mathbb{E}_{\mu u = x} B(u)$)

The first term $\alpha\beta\gamma$ gives a rough estimate of the value just in terms of the densities and the second term gives an estimate for how random the sets A, B, C behave.

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

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.

(End of proof) \square

Now let A be a subset of \mathbb{Z}_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(arithmetic progression), P (one of $\mathbb{Z}_N \cap [1, N/3]$ and $\mathbb{Z}_N \cap [2N/3, N]$), of length about $N/3$ such that $|A \cap P|/|P| \geq 6\delta/5$.
- Otherwise, if $\max_{r \neq 0} |\widehat{A}(r)| \leq \frac{\delta^2}{10}$. We may pick N large so that $\frac{\delta^3}{50} > \frac{1}{N}$. Then $A \times B \times C$ contains a 3AP by the **Lemma 5** and therefore A contains a 3AP.
- So if A does not contain a 3AP, then either we find P of length about $N/3$ with $|A \cap P|/|P| \geq 6\delta/5$ or we find $r \neq 0$ such that $|\widehat{A}(r)| \geq \delta^2/10$. (This is sometimes called the *dichotomy of order and chaos*)

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

Lemma 6) Let $r \in \widehat{\mathbb{Z}}_N$ (or just \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 $\text{osc}(\omega_r|_{P_i}) \leq \epsilon$ for each i .

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

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

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

(End of proof) \square

Now let us use the information that $r \neq 0$ and $|\widehat{A}(r)| \geq \delta^2/10$.

Define the **balanced function** f of A by $f(x) = A(x) - |A|/N$ for each x . Note that $\widehat{f}(0) = 0$ and $\widehat{f}(r) = \widehat{A}(r)$ for all $r \neq 0$.

Now let P_1, \dots, P_m be given by **Lemma 6** with $\epsilon = \delta^2/20$. Then

$$\begin{aligned} \frac{\delta^2}{10} &\leq |\widehat{f}(r)| = \frac{1}{N} \left| \sum_x f(x) \omega^{-rx} \right| \leq \frac{1}{N} \sum_i \left| \sum_{x \in P_i} f(x) \omega^{-rx} \right| \\ &\leq \frac{1}{N} \sum_{i=1}^m \left[\left| \sum_{x \in P_i} f(x) \omega^{-rx_i} \right| + \left| \sum_{x \in P_i} f(x) (\omega^{-rx} - \omega^{-rx_i}) \right| \right] \quad \text{where } x_i \text{ arbitrary } \in P_i \\ &\leq \frac{1}{N} \sum_{i=1}^m \left| \sum_{x \in P_i} f(x) \right| + \frac{\delta^2}{20} \end{aligned}$$

So $\sum_{i=1}^m \left| \sum_{x \in P_i} f(x) \right| \geq \delta^2 N/20$. Also, $\sum_{i=1}^m \sum_{x \in P_i} f(x) = 0$. So

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

Therefore, $\exists i$ s.t. $\left| \sum_{x \in P_i} f(x) \right| + \sum_{x \in P_i} f(x) \geq \frac{\delta^2}{20} |P_i|$ by pigeon hole principle and hence $\sum_{x \in P_i} f(x) \geq \frac{\delta^2}{40} |P_i|$. This implies $|A \cap P_i| = \left| \sum_{x \in P_i} f(x) + \frac{|A|}{N} \right| \geq (\delta + \delta^2/40) |P_i|$

=====

(11th October, 2018)

(Example sheets handed out - do not try to use particular theorem, but to apply the idea of using Fourier analysis in combinatorics.

Why does Fourier analysis have anything to do with combinatorics? Because we can formulate various problems in terms of Fourier transformation, e.g. by convolution and Parseval's law.)

•What we have showed : Let $A \subset \mathbb{Z}_N$, $|A| \geq \delta N$. Then,

(1) A contains a 3AP or

(2) N is even or

(3) $\exists P \subset \{1, \dots, N\}$, $|P| \geq N/3$ s.t. $|A \cap P| \geq \frac{6\delta}{5}|P|$ or

(4) $\exists P \subset \{1, \dots, N\}$, $|P| \geq \frac{\delta^2}{320}\sqrt{N}$ s.t. $|A \cap P| \geq (\delta + \delta^2/40)|P|$

If (2) holds, write $N = N_1 + N_2$ with N_1, N_2 odd, $N_1, N_2 \simeq N/2$. 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 (NB (3) \Rightarrow (4)) then we pass to P and start again (that is, replace \mathbb{Z}_N with P and A with $A \cap P$). After $40/\delta$ iterations, the density at least doubles. So the total number of iterations we can have is at most $\leq \frac{40}{\delta} + \frac{40}{2\delta} + \frac{40}{4\delta} + \dots \leq \frac{80}{\delta}$.

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

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

(just the follow the idea of calculation,, do not try to learn a particular thing from this calculation)
(In fact 320 above should be corrected to 640 because of (2))

Bogolyubov's Method

Definition) Let $K \subset \widehat{\mathbb{Z}}_N$ and let $\delta > 0$. The **Bohr set** $B(K, \delta)$ has two definitions.

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

It turns out that Bohr set has a lot of structure.

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

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

Lemma 7) Let $A \subset \mathbb{Z}_N$ be a set of density α . Then $2A - 2A$ contains a Bohr set $B(K, 1/4)$ (arc) with $|K| \leq \alpha^{-2}$.

proof) Observe that $x \in 2A - 2A$ if and only if $A * A * (-A) * (-A)(x) \neq 0$ (think for a second). But

$$\begin{aligned} A * A * (-A) * (-A)(x) &= \sum_r \overline{A * A * (-A) * (-A)(r)} \omega^{rx} \quad (\text{inversion formula}) \\ &= \sum_r |\widehat{A}(r)|^4 \omega^{rx} \end{aligned}$$

Let $K = \{r : |\widehat{A}(r)| \geq \alpha^{3/2}\}$. Then

$$\alpha = \|\widehat{A}\|_2^2 = \sum_r |\widehat{A}^2(r)|^2 \geq \alpha^3 |K|$$

so $|K| \leq \alpha^{-2}$. Now suppose that $x \in B(K, 1/4)$. Then

$$\sum_r |\widehat{A}(r)|^4 \omega^{rx} = \alpha^4 + \sum_{r \in K, r \neq 0} |\widehat{A}(r)|^4 \omega^{rx} + \sum_{r \notin K} |\widehat{A}(r)|^4 \omega^{rx}$$

The real part of the second term is non-negative, since $rx \in [-N/4, N/4]$ when $r \in K$. Also the final term can be bounded by

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

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

(End of proof) \square

Lemma 8) Let $K \subset \mathbb{Z}_N$ and let $\delta > 0$. Then

- (i) $B(K, \delta)$ has density at least $\delta^{|K|}$.
- (ii) $B(K, \delta)$ contains a mod- N arithmetic progression of length $\geq \delta N^{1/|K|}$.

proof)

- (i) Let $K = \{r_1, \dots, r_k\}$. Consider the N number of k -tuples $(r_1x, \dots, r_kx) \in \mathbb{Z}_N^k$ (for $x \in \mathbb{Z}_N$). If we intersect this set of k -tuples with a random "box" $Q = [t_1, t_1 + \delta N] \times \dots \times [t_k, t_k + \delta N]$. Then the expected number of k -tuples in the box is $\delta^k N$ (since each intersection has probability δ^k .)

But if (r_1x, \dots, r_kx) and (r_1y, \dots, r_ky) belong to this box, then $x - y \in B(K, \delta)$, so the expected number of in (r_1y, \dots, r_ky) is smaller or equal to the expected number of y in $B(K, \delta)$. i.e. if we let q be a random point in $Q \cap \mathbb{Z}_N^k$, then

$$\mathbb{E}\left(\sum_y 1_{y \in B(K, \delta)}\right) \geq \mathbb{E}\left(\sum_y 1_{q \in Q} 1_{q+y \in Q}\right) = \sum_y \mathbb{P}(y \in Q) = N|\delta|^K$$

(there must be an easy argument... in fact, in the lecture, it was concluded before so the expected number of, so there must be more intuitive way of understanding this)

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

(End of proof) \square