

Introduction to Discrete Analysis

October 11, 2018

<i>CONTENTS</i>	2
-----------------	---

Contents

0	Introduction	3
1	The discrete Fourier transform	4
1.1	Roth's theorem	5
1.2	Bogolyubov's method	8

0 Introduction

asdasd

1 The discrete Fourier transform

Let N be a 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 $\hat{f}(r)$ to be

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

From now on we use the notation $\mathbb{E}_{x \in \mathbb{Z}_N}$ for $\frac{1}{N} \sum_{x \in \mathbb{Z}_N}$, so $\hat{f}(r) = \mathbb{E}_x f(x) e^{-\frac{2\pi i r x}{N}}$.

If we write ω_r for the function $x \rightarrow \omega^{rx}$, and $\langle f, g \rangle$ for $\mathbb{E}_x f(x) \overline{g(x)}$, then $\hat{f}(r) = \langle f, \omega_r \rangle$. So the discrete fourier transform is basically expanding the function f in the set of orthonormal basis ω_r .

Let us write $\|f\|_p$ for $\mathbb{E}_x |f(x)|^p$ ^{1/p} (the L_p -norm), and call the resulting space $L_p(\mathbb{Z}_n)$.

Important convention: we use *averages* for the 'original functions' in 'physical spaces', and *sums* for their Fourier transforms in 'frequency space' (referring to \mathbb{E} : \langle, \rangle is average in the original space but just \sum in frequency space, i.e. for \hat{f}, \hat{g} etc.)

Lemma. (1, Parseval's identity)

If $f, g : \mathbb{Z}_n \rightarrow \mathbb{C}$, then $\langle \hat{f}, \hat{g} \rangle = \langle f, g \rangle$.

Proof.

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

□

Lemma. (2, Convolution identity)

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

where

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

Proof.

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

□

Lemma. (3, Inversion formula)

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

(note the sign of ω^{rx}).

Proof.

$$\begin{aligned}
\sum_r \hat{f}(r) \omega^{rx} &= \sum_r \mathbb{E}_y f(y) \omega^{r(x-y)} \\
&= \mathbb{E}_y f(y) \sum_r \omega^{r(x-y)} \\
&= \mathbb{E}_y f(y) n \delta_{xy} \\
&= f(x)
\end{aligned}$$

This is really just the statement that we get the original vector back when we sum up its components. □

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 $1_A, \chi_A$) for the characteristic function of A . Then $\hat{A}(0) = \mathbb{E}_x A(x) = \frac{|A|}{N}$, the *density* of A .

Also, $\|\hat{A}\|_2^2 = \langle \hat{A}, \hat{A} \rangle = \langle A, A \rangle = \mathbb{E}_x A(x)^2 = \mathbb{E}_x A(x) = \frac{|A|}{N}$, again the density.

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

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

1.1 Roth's theorem

Theorem. (4) For every $\delta > 0$, $\exists N$ s.t. if $A \subset \{1, \dots, N\}$ is a set of size at least δN , then A must contain an arithmetic progression of length 3.

This is also true for 4, 5, ..., but the proof is much harder – Szemerédi's theorem. Basic strategy of proof: show that if A has density δ and no AP of length 3 (3AP), then there's a long AP in $P \subset \{1, 2, \dots, n\}$ s.t.

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

where $c(\delta)$ is some positive number. But then we can continue this argument to expand $A \cap P$ to infinity (note that $|A \cap P|$ is an integer, so each time increase by 1 at least).

The best known relationship between δ and the N required is around $\delta \sim \frac{c}{\log \log N}$ for some constant c .

—Lecture 2—

Lemma. (5)

Let N be odd, $A, B, C \subset \mathbb{Z}_N$ have densities α, β, γ .

If $\max_{r \neq 0} |\hat{A}(r)| \leq \frac{\alpha(\beta\gamma)^{1/2}}{2}$ and $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$, then there exists $x, d \in \mathbb{Z}_N$ with $d \neq 0$ s.t. $(x, x+d, x+2d) \in A \times B \times C$.

Proof.

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

Recall here the notation is $B_2(u) = B(u/2)$. now

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

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 $\{1, \dots, N\}$ with 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 $\frac{2\delta}{5}$. In that case we find an AP P of length about $N/3$ such that $|A \cap P|/|P| \geq \frac{6\delta}{5}$.

Otherwise, we find that if $\max_{r \neq 0} |\hat{A}(r)| \leq \frac{\delta}{10}$ and $\frac{\delta^3}{50} > \frac{1}{N}$, then $A \times B \times C$ contains a 3AP, so A contains a 3AP.

So if A does not contain a 3AP, then either we find P of length about $N/3$ with $|A \cap P|/|P| \geq \frac{6\delta}{5}$, or there exists $r \neq 0$ s.t. $|\hat{A}(r)| \geq \frac{\delta}{10}$.

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

Lemma. (6)

Let $r \in \mathbb{Z}_n$ and let $\varepsilon > 0$. Then there is a partition of $\{1, 2, \dots, N\}$ into arithmetic progressions P_i of length at least $c(\varepsilon)\sqrt{N}$ such that

$$\text{osc}(\omega_r|_{P_i}) \leq \varepsilon$$

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 $\frac{2\pi}{t}$.

If $|\omega^{ar} - \omega^{br}| \leq \frac{2\pi}{t}$ with $a < b$, then $|1 - \omega^{dr}| \leq \frac{2\pi}{t}$ where $d = b - a$. 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 mod d , and partition each residue class into parts of length between $\frac{\varepsilon t}{4\pi}$ and $\frac{\varepsilon t}{2\pi}$ (possible, since $d \leq t \leq \sqrt{N}$).

We are done, with $c(\varepsilon) = \frac{\varepsilon}{16}$ (a casual choice). \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 $\varepsilon = \delta^2/20$. Then

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

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

We also have $\sum_{i=1}^m \sum_{x \in P_i} f(x) = 0$, 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,

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

—Lecture 3—

Now let $A \subset \mathbb{Z}_N$, $|A| \geq \delta N$. Then:

- either A contains a $3AP$,
- or N is even,
- or $\exists P \subset \{1, \dots, N\}$, $|P| \geq N/3$ s.t. $|A \cap P| \geq \frac{6\delta}{5} |P|$,
- or $\exists P \subset \{1, \dots, N\}$, $|P| \geq \frac{\delta^2}{640} \sqrt{N}$ (casual) s.t. $|A \cap P| \geq \left(\delta + \frac{\delta^2}{40} \right) |P|$.

Note that the third case is strictly worse than the fourth.

Well if the first is true then we're done. Suppose now the second 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) \implies (4)), then we pass to P and start to again. After $\frac{40}{\delta}$ iterations, the density at least doubles. Therefore the total number of iterations we can have is at most $\frac{40}{\delta} + \frac{40}{2\delta} + \dots \leq \frac{80}{\delta}$.

If $\frac{\delta^2}{640} \sqrt{N} \geq N^{1/3}$ (to account for the above, and also for the possible use of (2)) at each iteration, and $\frac{\delta^3}{25} \geq N^{-1}$ (which follows from the first condition), then after $\frac{80}{\delta}$ iterations we have $N \geq N^{(1/3)^{80/\delta}}$, so the argument works provided

$$N^{(1/3)^{80/\delta}} \geq \left(\frac{640}{\delta^2} \right)^6$$

taking logs and simplify a bit, we need

$$\begin{aligned} -\frac{80}{\delta} \log 3 + \log \log N &\geq \log 6 + \log(\log 640 + 2 \log \frac{1}{\delta}) \\ \Leftrightarrow \log \log N &\geq \frac{160}{\delta} \\ \Leftrightarrow \delta &\geq \frac{160}{\log \log N} \end{aligned}$$

1.2 Bogolyubov's method

Let $K \subset \hat{\mathbb{Z}}_N$ and let $\delta > 0$. The *Bohr set* $B(K, \delta)$ has two definitions (not exactly equivalent, but quite equivalent):

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

Definition. Let G be an abelian group and let A, B be subsets of G . Then write $A + B = \{a + b : a \in A, b \in B\}$ and the obvious definition for $A - B$. We also write $rA = \{a_1 + \dots + a_r : a_1, \dots, a_r \in A\}$ (note this might be different than what you think this notation should mean).

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 $x \in 2A - 2A$ iff $A * A * (-A) * (-A)(x) \neq 0$ (this makes more sense if we write it as $\mathbb{E}_{a+b-c-d=x} A(a)A(b)A(c)A(d) \neq 0$, i.e. we are basically just counting the number of ways x can be written as $a + b - c - d$ where $a, b, c, d \in A$.)

But

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

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

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

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

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

Also

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

So it follows that the real part of $\sum_r |\hat{A}(r)|^4 \omega^{rx} > 0$, i.e. it is non-zero. So $x \in 2A - 2A$. \square

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 at least $\delta N^{1/|K|}$.

Proof. (i) Let $K = \{r_1, \dots, r_k\}$. Consider the N k -tuples $(r_1 x, \dots, r_k x) \in \mathbb{Z}_N^k$. If we intersect this set of k -tuples with a random 'box' $[t_1, t_1 + \delta N] \times \dots \times [t_k, t_k + \delta N]$

(here we are thinking t_i as real numbers), 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_1x, \dots, r_kx) and (r_1y, \dots, r_ky) belong to this box, then $x - y \in B(K, \delta)$.

(ii) If we take $\eta > N^{-1/k}$, then by (i) we get that $|B(K, \eta)| > 1$, therefore at least 2. 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 $dx \in B(K, \delta)$. That gives us an AP of length at least $\frac{\delta}{\eta}$. So we get one of length at least $\delta N^{1/k}$. \square