FOURIER ANALYSIS AND ITS APPLICATION TO ROTH'S THEOREM

A REPORT

submitted in partial fulfillment of the requirements

for the award of the dual degree of

Bachelor of Science-Master of Science

in

MATHEMATICS

by

AMAN KUMAR

(17025)

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH BHOPAL
BHOPAL - 462066

April 2022

भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान भोपाल
Indian Institute of Science Education and Research
Bhopal
(Estb. By MHRD, Govt. of India)

CERTIFICATE

This is to certify that **AMAN KUMAR**, BS-MS (Mathematics), has worked on the project entitled **'Fourier Analysis and its Application to Roth's theorem'** under my supervision and guidance. The content of this report has not been submitted elsewhere for the award of any academic or professional degree.

April 2022
IISER Bhopal

Dr. Saurabh Shrivastava

Committee Member	Signature	Date
Dr. Saurabh Shrivastava	_____	_____
Dr. Jyoti Prakash Saha	_____	_____
Dr. Rahul Garg	_____	_____

ACADEMIC INTEGRITY AND COPYRIGHT DISCLAIMER

I hereby declare that this project is my own work and, to the best of my knowledge, it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at IISER Bhopal or any other educational institution, except where due acknowledgement is made in the document.

I certify that all copyrighted material incorporated into this document is in compliance with the Indian Copyright Act (1957) and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless IISER Bhopal from any and all claims that may be asserted or that may arise from any copyright violation.

April 2022 **AMAN KUMAR**

IISER Bhopal

ACKNOWLEDGEMENT

First and foremost, I would like to express my heartfelt thanks to my thesis advisor Dr. Saurabh Shrivastava for allowing me to work on such an interesting topic and for his patient guidance and constant motivation throughout the thesis work. The training that I received during this period was astonishing and it will always help me in my future career. Along with being my mentor, his personality has been a source of inspiration for me which not only helped me in my academic field but also supported me in the tough times of my life.

I would like to thank and express my sincere gratitude to my thesis evaluation committee: Dr. Jyoti Prakash Saha, Dr. Rahul Garg for attending my presentations and for providing me with valuable suggestions. I would also like to thank my seniors Riju Basak, Ranveer Kumar Singh for always being available for me to discuss mathematics from the beginning of the IISER-B journey.

I thank Heena, my dearest friend, who has been there for me through thick and thin, my IISER Journey would have been incomplete without her. Additionally, I thank Nitish, Pranav, Gurleen, and Sabhrant, who have been extremely helpful in my academic endeavors. I'd also like to say thank you to Rajiv, Shenky, Aditya, and Govind from my squad members, who assisted me in numerous ways and made my college journey memorable.

Lastly, I would like to thank my parents and my lovely sister for their support in every decision that I made in my career. This thesis is dedicated to them.

AMAN KUMAR

ABSTRACT

In this thesis, we study Fourier analysis and some of its applications. We begin with an introduction to the notion of Fourier series and its discrete analogue the discrete Fourier transform. First, we discuss the Weyl's equidistribution criteria and the fast Fourier transform as applications.

Next, we study the main part of the thesis- the Roth's theorem. Roth's theorem asserts that under certain size constraints, every subset of integers has 3-term arithmetic progressions. This is a fundamental result in additive combinatorics and has laid the foundation for many important developments. We approach the proof of Roth's theorem in the finite field setting and then extend the ideas to prove Roth's theorem for integers.

Finally, we briefly discuss some recent progress around this theorem in the finite field setting and the recent breakthrough concerning upper bounds for the cap set problem using the polynomial method due to Ellenberg and Gijswijt in 2017.

CONTENTS

1. FOURIER SERIES

1.1 Basic Theory

We now begin our study of Fourier analysis with the precise definition of the Fourier series of a function. Given an integrable function $f : [0, L] \to \mathbb{C}$, we define the n-th Fourier coefficient of f for $n \in \mathbb{N}$

$$\hat{f}(n) = \frac{1}{L} \int_a^b f(x) e^{-2\pi i n x/L} dx$$

The Fourier series of f is given formally by

$$f(x) \sim \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{2\pi i n x/L}$$

General assumption: f is at least Riemann integrable.

Remark. There is, a priori, no guarantee that the Fourier series will converge at all; even if it does converge, it may not converge to f.

The N^{th} partial sum of the Fourier series of f, for N a positive integer is given by

$$S_N(f)(x) = \sum_{n=-N}^{N} \hat{f}(n) e^{2\pi i n x/L}.$$

Note: "Convergence of the Fourier series to f" will always mean "convergence of the above partial sums to f".

Theorem 1.1. ***(Uniqueness)*** *Suppose that f is an integrable function on the circle with $\hat{f}(n) = 0$ for all $n \in \mathbb{Z}$. Then $f(\theta_0) = 0$ whenever f is continuous at the point θ_0.*

Corollary 1.2. Suppose that f is a continuous function on the circle and that the Fourier

series of f is absolutely convergent, $\sum_{n=-\infty}^{\infty} |\hat{f}(n)| < \infty$. Then, the Fourier series converges uniformly to f, that is,

$$\lim_{N\to\infty} S_N(f)(\theta) = f(\theta) \quad \text{uniformly in } \theta.$$

Definition 1.3 (Big O notation). We say $f(x) = O(g(x))$ as $x \to a$ if there exists a $C > 0$ such that

$$\lim_{x\to a} \frac{f(x)}{g(x)} \leq C$$

Corollary 1.4. Suppose that f is a twice continuously differentiable function on the circle. Then

$$\hat{f}(n) = O\left(1/|n|^2\right) \quad \text{as } |n| \to \infty$$

so that the Fourier series of f converges absolutely and uniformly to f.

Definition 1.5 (Convolution). Let $f, g : \mathbb{R} \to \mathbb{C}$ be 2π-periodic functions. The convolution $f * g$ of f and g is the function defined on $[-\pi, \pi]$ by

$$(f * g)(x) := \frac{1}{2\pi} \int_{-\pi}^{\pi} f(y)g(x-y)dy$$

Proposition 1.6. (Basic properties). Let f, g, h be 2π-periodic integrable functions, and $c \in \mathbb{C}$. Then

1. (Linearity I) $f * (g + h) = (f * g) + (f * h)$
2. (Linearity II) $(cf) * g = c(f * g) = f * (cg)$
3. (Commutative) $f * g = g * f$
4. (Associative) $(f * g) * h = f * (g * h)$
5. (Continuity) $f * g$ is continuous.
6. (Interaction with Fourier transform) $\widehat{f * g}(n) = \hat{f}(n)\hat{g}(n)$

Lemma 1.7. Suppose f is integrable on the circle and bounded by B. Then there exists a sequence $\{f_k\}_{k=1}^{\infty}$ of continuous functions on the circle so that

$$\sup_{x\in[-\pi,\pi]} |f_k(x)| \leq B \quad \text{for all } k = 1, 2, \ldots$$

and

$$\int_{-\pi}^{\pi} |f(x) - f_k(x)|\, dx \to 0 \quad \text{as } k \to \infty$$

1.2 Good kernels

We built a sequence of trigonometric polynomials p_k with the property that the functions p_k peaked at the origin in order to prove Uniqueness theorem 1.1. As a result, we were able to isolate the behavior of f at the origin. We'll return to such families of functions in this section, but this time in a more general setting. We begin by defining the term "good kernel" and discussing the characteristics of such functions. Then, using convolutions, we show how to recover a given function using these kernels.

Definition 1.8. A family of kernels $\{K_n(x)\}_{n=1}^{\infty}$ on the circle is said to be a family of good kernels if it satisfies the following properties:

1. For all $n \geq 1$,
$$\frac{1}{2\pi} \int_{-\pi}^{\pi} K_n(x) dx = 1$$

2. There exists $M > 0$ such that for all $n \geq 1$,
$$\int_{-\pi}^{\pi} |K_n(x)|\, dx \leq M$$

3. For every $\delta > 0$,
$$\int_{\delta \leq |x| \leq \pi} |K_n(x)|\, dx \to 0, \quad \text{as } n \to \infty$$

Theorem 1.9. *Let $\{K_n\}_{n=1}^{\infty}$ be a family of good kernels, and f an integrable function on the circle. Then*

$$\lim_{n \to \infty} (f * K_n)(x) = f(x)$$

whenever f is continuous at x. If f is continuous everywhere, then the above limit is uniform.

Definition 1.10. Dirichlet kernel is the trigonometric polynomial defined for $x \in [-\pi, \pi]$ by

$$D_N(x) = \sum_{n=-N}^{N} e^{inx}$$

or closed form

$$D_N(x) = \frac{\sin\left(\left(N + \frac{1}{2}\right)x\right)}{\sin(x/2)}$$

Note: Its Fourier coefficient are

$$a_n = \begin{cases} 1 & \text{if } |n| \leq N \\ 0 & \text{Else} \end{cases}$$

Calculation part: Closed form formula of Dirichlet kernel using geometric series.

$$\begin{aligned} \sum_{n=-N}^{N} \omega^n &= \sum_{n=-N}^{-1} \omega^n + \sum_{n=0}^{N} \omega^n \\ &= \frac{\omega^{-N} - 1}{1 - w} + \frac{1 - w^{N+1}}{1 - w} \\ &= \frac{\omega^{-N} - \omega^{N+1}}{1 - w} \\ &= \frac{\omega^{-N-1/2} - w^{N+1/2}}{w^{-1/2} - w^{1/2}} \\ &= \frac{\sin\left(\left(N + \frac{1}{2}\right)x\right)}{\sin(x/2)} \end{aligned}$$

Proposition 1.11. $S_N(f)(x) = (f * D_N)(x)$

Proof.

$$\begin{aligned} S_N(f)(x) &= \sum_{n=-N}^{N} \hat{f}(n) e^{inx} \\ &= \sum_{n=-N}^{N} \left(\frac{1}{2\pi} \int_{-\pi}^{\pi} f(y) e^{-iny} dy \right) e^{inx} \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} f(y) \left(\sum_{n=-N}^{N} e^{in(x-y)} \right) dy \\ &= (f * D_N)(x) \qquad [D_N \text{ is the } N^{th} \text{ Dirichlet kernel}] \end{aligned}$$

□

Remark :Now, the understanding of $S_N(f)$ boils down to understanding the convolution $f * D_N$.

The important question is whether DN is a good kernel, because if it is, Theorem 1.9 implies that the Fourier series of f converges to $f(x)$ whenever f is continuous at x.

Lemma 1.12. (D_N **is NOT a good kernel)** Let D_N denote the Dirichlet kernel

$$D_N(\theta) = \sum_{n=N}^{N} e^{ik\theta} = \frac{\sin(N + 1/2)\theta}{\sin(\theta/2)}$$

and define

$$L_N = \frac{1}{2\pi} \int_{-\pi}^{\pi} |D_N(\theta)| \, d\theta$$

Then

$$L_N \geq c \log N$$

for some constant $c > 0$. A more careful estimate gives

$$L_N = \frac{4}{\pi^2} \log N + O(1)$$

Proof. Claim : D_N violates the second property of good kernel.

$$D_N(\theta) = \sum_{n=N}^{N} e^{ik\theta} = \frac{\sin(N + 1/2)\theta}{\sin(\theta/2)}$$

and define

$$L_N = \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_N(\theta)|\, d\theta$$

Then

$$L_N = \frac{1}{2\pi}\int_{-\pi}^{\pi} \frac{|sin((N+1/2)\theta)|}{|sin(\theta/2)|} d\theta$$

We know that $|D_N(\theta)|$ is an even function and $\forall\ \ x \in \mathbb{R}$, $|sinx| \leq |x|$. So,

$$L_N \geq \frac{1}{\pi}\int_{0}^{\pi} \frac{|sin((N+1/2)\theta)|}{|\theta/2|} d\theta$$

Now, we use the substitution $x = (N+1/2)\theta$. Then by change of variables,

We have:

$$L_N \geq \frac{2}{\pi}\int_{0}^{(N+1/2)\pi} \frac{|sin(x)|}{|x|} dx =$$

$$= \frac{2}{\pi}\sum_{k=0}^{N-1}\int_{k\pi}^{(k+1)\pi} \frac{|sin(x)|}{|x|} dx + \frac{2}{\pi}\int_{N\pi}^{(N+1/2)\pi} \frac{|sin(x)|}{|x|}$$

Let

$$c_N = \frac{2}{\pi}\int_{N\pi}^{(N+1/2)\pi} \frac{|\sin(x)|}{x}$$

.

Now, make the change of variable $z = xk\pi$ in each of the summand above to get :

$$L_N \geq \frac{2}{\pi}\sum_{k=0}^{N-1}\int_{0}^{\pi} \frac{\sin(z)}{z+k\pi} dz + c_N$$

Interchanging the summation and integral, we get:

$$L_N \geq \frac{2}{\pi}\int_{0}^{\pi} \sin(z)\left(\sum_{k=0}^{N-1}\frac{1}{z+k\pi}\right) dz + c_N$$

Since $z \leq \pi$, $\frac{1}{z+k\pi} \geq \frac{1}{(k+1)\pi}$.

So we have:

$$\sum_{k=0}^{N-1}\frac{1}{z+k\pi} \geq \sum_{k=0}^{N-1}\frac{1}{(1+k)\pi} = \frac{1}{\pi}\sum_{k=1}^{N}\frac{1}{k}$$

Substituting this back in the integral

$$L_N \geq \frac{2}{\pi^2} \sum_{k=1}^{N} \frac{1}{k} \int_0^{\pi} \sin(z) dz + c_N = \frac{4}{\pi^2} \sum_{k=1}^{N} \frac{1}{k} + c_N$$

Now, we know that

$$\sum_{k=1}^{N} \frac{1}{k} \geq \int_1^{N+1} \frac{1}{x} dx = \log(N+1) > \log(N)$$

Finally we get:

$$L_N = \frac{4}{\pi^2} \log(N) + O(1)$$

□

Definition 1.13. Poisson kernel is defined for $\theta \in [-\pi, \pi]$ and $\gamma \in [0, 1]$ by the absolutely and uniformly convergent series.

$$P_\gamma(\theta) = \sum_{n=-\infty}^{\infty} \gamma^{|n|} e^{in\theta}$$

or **closed form formula**

$$P_\gamma(\theta) = \frac{1 - \gamma^2}{1 - 2\gamma \cos\theta + \gamma^2}$$

Fourier coefficient

$$\hat{P}_\gamma(n) = \gamma^{|n|}$$

Note: In calculation of fourier coefficient of $P_\gamma(\theta)$ we can interchange the order of integration and summation since the sum converges uniformly in θ for each fixed γ

Calculation part: For closed form formula of Poisson kernel using geometric se-

ries.

$$\begin{aligned}\mathrm{P}_\gamma(\theta) &= \sum_{n=0}^{\infty} \omega^n + \sum_{n=1}^{\infty} \bar{\omega}^n; \quad \omega = \gamma e^{i\theta} \\ &= \frac{1}{1-\omega} + \frac{\bar{\omega}}{1-\bar{\omega}} \\ &= \frac{1-\bar{\omega}+(1-\omega)\bar{\omega}}{(1-\omega)(1-\bar{\omega})} \\ &= \frac{1-\gamma^2}{1-2\gamma\cos\theta+\gamma^2}\end{aligned}$$

1.3 Cesaro and Abel summability

Even if the function is continuous, as we can see, the Fourier series may not be able to reconstruct it. On the other hand, the Fourier coefficients should contain enough information to reconstruct the function, especially for continuous functions: after all, the uniqueness theorem exists.

To recover the function, we'll show two distinct approaches of averaging the Fourier series.

Definition 1.14. Given a sequence $\{c_n\}$, let $s_n := -\sum_{k=0}^{n} c_k$ be the sequence of partial sums. We define the N^{th} Cesaro mean σ_N of the sequence $\{s_k\}$ (also known as the N^{th} Cesaro sum of the series $\sum_{k=0}^{\infty} c_k$) by

$$\sigma_N := \frac{s_0 + s_1 + \cdots + s_{N-1}}{N}$$

Remark. Convergence implies Cesaro summability.
i.e, $\lim_{N\to\infty} \sigma_N = \sigma$, then the series $\sum C_n$ is cesario summable to σ.

Definition 1.15. (**Fejer kernel**) Let $F_N(x)$ denote the N^{th} Cesaro mean of the sequence $\{D_k(x)\}$; i.e.,

$$F_N(x) := \frac{1}{N} \sum_{k=0}^{N-1} D_k(x)$$

Remark. Then consider:

$$\begin{aligned} f * F_N(x) &:= \frac{1}{N} \sum_{k=0}^{N-1} f * D_k(x) \\ &= \frac{1}{N} \sum_{k=0}^{N-1} S_k(f)(x) \end{aligned}$$

the average of the first N partial sums of the Fourier series of f.

Lemma 1.16. Fejer kernel is a good kernel

$$F_N(x) = \frac{1}{N} \frac{\sin^2(Nx/2)}{\sin^2(x/2)}$$

Theorem 1.17. *Let f be an integrable function on the circle. If f is continuous at θ_0, then the Fourier series of f is Cesaro summable to f at θ_0. Further, if f is continuous on the entire circle, then the convergence of the Cesaro sums is uniform.*

Corollary 1.18. Any continuous function on the circle can be uniformly approximated by trigonometric polynomials.

Definition 1.19. Let $\sum_{k=0}^{\infty}$ be a series of complex numbers.

i We define the Abel means $A(r)$ of the series $\sum c_k$ by

$$A(r) := \sum_{k=0}^{\infty} c_k r^k$$

ii If, for every $0 \leq r < 1$, the Abel means $A(r)$ converges, and

$$\lim_{r \to 1} A(r) = s$$

then we say the series $\sum c_k$ is Abel summable to s.

Definition 1.20. Suppose we know the Fourier series of a function f :

$$f(\theta) \sim \sum_{n=-\infty}^{\infty} a_n e^{in\theta}$$

We define the **Abel means** $A_r(f)(\theta)$ **of the Fourier series** of the function f by

$$\Lambda_r(f)(\theta) = \sum_{n=-\infty}^{\infty} r^{|n|} a_n e^{in\theta}$$

Lemma 1.21 (**Abel means as a convolution**).

$$A_r(f)(\theta) = (f * P_r)(\theta)$$

Lemma 1.22. The Poisson kernel is a good kernel.

Corollary 1.23. Let f be an integrable function on the circle. Then the Abel means of the (Fourier series of) f converges point wise to f at every point of continuity. If, further, f is continuous on the circle, then the convergence is uniform.

Example 1.24. (Abel summability is stronger than the standard or Cesáro methods of summation)

i Show that if the series $\sum_{n=1}^{\infty} c_n$ of complex numbers converges to a finite limit s, then the series is Abel summable to s.

ii However, show that there exist series which are Abel summable, but that do not converge.

iii Argue similarly to prove that if a series $\sum_{n=1}^{\infty} c_n$ is Cesáro summable to σ, then it is Abel summable to σ.

iv Give an example of a series that is Abel summable but not Cesáro summable.

Remark: **convergent** $\Longrightarrow$ **Ceráro summable** $\Longrightarrow$ **Abel summable**
Note : None of the arrows can be reversed.

Proof. i Without loss of generality, we assume that $s = 0$. In fact, if $\sum_{n=1}^{\infty} c_n = s \neq 0$, we can simply define $d_n = c_n - \frac{s}{2^n}$ and $\sum_{n=1}^{\infty} d_n = 0$ Letting $s_1 = c_1, s_N =$

$c_1 + c_2 + \cdots + c_N$, we have

$$\begin{aligned}\sum_{n=1}^{N} c_n r^n &= \sum_{n=1}^{N-1} (s_{n+1} - s_n)\, r^{n+1} + c_1 r \\ &= \sum_{n=1}^{N} s_n r^n - \sum_{n=1}^{N-1} s_n r^{n+1} \\ &= (1-r) \sum_{n=1}^{N} s_n r^n + s_N r^{N+1}\end{aligned}$$

With the assumption that $s = 0$, we will obtain that
$\sum_{n=1}^{\infty} c_n r^n = (1-r)\sum_{n=1}^{\infty} s_n r^n$ as $N \to \infty$ in the previous equation. For any $\epsilon > 0$, we may choose N large enough such that $|s_n| < \epsilon$ when $n > N$. Also, there exists an $M > 0$ such that $\sup_{n\in\mathbb{N}} |s_n| \le M$. Then we have

$$\begin{aligned}\left|\sum_{n=1}^{\infty} c_n r^n\right| &= \left|(1-r)\sum_{n=1}^{\infty} s_n r^n\right| \\ &\le \left|(1-r)\sum_{n=1}^{N} s_n r^n\right| + \left|(1-r)\sum_{n=N+1}^{\infty} s_n r^n\right| \\ &< (1-r)\sum_{n=1}^{N} M r^n + (1-r)\frac{\epsilon r^N}{1-r} \\ &\le Mr\left(1 - r^N\right) + \epsilon\end{aligned}$$

Thus, $\lim_{r\to 1^-} \sup |\sum_{n=1}^{\infty} c_n r^n| \le \epsilon$. Since ϵ is arbitrary,
we have $\lim_{r\to 1^-} \sum_{n=1}^{\infty} c_n r^n = 0$.

ii Consider $c_n = (-1)^n$. The partial sum $s_N = \sum_{n=1}^{N} c_n$ is -1 when N is odd and 0 when N is even. Thus it does not converge. However, its Abel limit is $\lim_{r\to 1^-} \sum_{n=1}^{\infty} (-r)^n = \lim_{r\to 1^-} \frac{-r}{1+r} = -\frac{1}{2}$.

iii First we let $\sigma_N = \frac{s_1 + s_2 + \cdots + s_N}{N}$ and obtain that

$$s_1 = \sigma_1, s_N = N\sigma_N - (N-1)\sigma_{N-1}.$$

Then assuming $\sigma = 0$ and by (a), we obtain that

$$\begin{aligned}\sum_{n=1}^{N} c_n r^n &= (1-r)\sum_{n=1}^{N} s_n r^n + s_N r^{N+1} \\ &= (1-r)\sum_{n=1}^{N} \left[n\sigma_n - (n-1)\sigma_{n-1}\right] r^n + \left[N\sigma_N - (N-1)\sigma_{N-1}\right] r^{N+1} \\ &= (1-r)\sum_{n=1}^{N} n\sigma_n r^n - (1-r)\sum_{n=1}^{N-1} n\sigma_n r^n + \left[N\sigma_N - (N-1)\sigma_{N-1}\right] r^{N+1}\end{aligned}$$

$$(1-r)^2 \sum_{n=1}^{N} n\sigma_n r^n + (2-r)N\sigma_N r^{N+1} - (N-1)\sigma_{N-1} r^{N+1}$$

Since $\{\sigma_n\}$ is bounded and the series $\sum_{n=1}^{\infty} r^n$ converges for any $0 < r < 1$,

the derivative of $\sum_{n=1}^{\infty} r^n$ with respect to r also converge, then,

$$Nr^{N-1} \quad \text{and} \quad (N-1)r^{N-2} \quad \text{tend to} \quad 0 \quad \text{as} \quad N \to \infty$$

Letting $N \to \infty$ in the previous equation,

we have

$$\sum_{n=1}^{\infty} c_n r^n = (1-r)^2 \sum_{n=1}^{\infty} n\sigma_n r^n.$$

With the assumption $\sigma = 0$, we can choose N large enough such that $|\sigma_n| < \epsilon$ when $n > N$ for any $\epsilon > 0$. Meanwhile, there exists a $B > 0$ such that $|\sigma_n| \leq B$

for all $n \in \mathbb{N}$. Therefore,

$$\begin{aligned}\left|\sum_{n=1}^{\infty} c_n r^n\right| &= \left|(1-r)^2 \sum_{n=1}^{\infty} n\sigma_n r^n\right| \\ &\leq (1-r)^2 \sum_{n=1}^{N} Bnr^n + (1-r)^2 \sum_{n=N+1}^{\infty} \epsilon n r^n \\ &= (1-r)^2 B \frac{r-(N+1)r^{N+1}+Nr^{N+2}}{(1-r)^2} \\ &+ (1-r)^2 \epsilon \frac{(N+2)r^{N+1}-(1+N)r^{N+2}}{(1-r)^2} \\ &= B\left[r-(N+1)r^{N+1}+Nr^{N+2}\right] + \epsilon\left[(N+2)r^{N+1}-(1+N)r^{N+2}\right]\end{aligned}$$

As $r \to 1^-$, we have $\lim_{r\to 1^-} \sup|\sum_{n=1}^{\infty} c_n r^n| \leq \epsilon$, i.e., $\lim_{r\to 1^-} \sum_{n=1}^{\infty} c_n r^n = 0$ by the arbitrariness of ϵ.

In the case when $\sigma \neq 0$, we let $d_1 = c_1 - \sigma, d_n = c_n$ for $n > 1$.

Then $\lim_{r\to 1^-} \sum_{n=1}^{\infty} d_n r^n = 0 = \lim_{r\to 1^-} \sum_{n=1}^{\infty} c_n r^n - \sigma$

iv Consider

$$c_n = (-1)^{n-1} n.$$

Then

$$\sum_{n=1}^{\infty} (-1)^{n-1} n r^n = -\left[\sum_{n=1}^{\infty} (n+1)(-r)^n - \sum_{n=1}^{\infty} (-r)^n\right] = \frac{r}{(1+r)^2}.$$

Thus its Abel limit is

$$\lim_{r\to 1^-} \sum_{n=1}^{\infty} (-1)^{n-1} r^n = \lim_{r\to 1^-} \frac{r}{(1+r)^2} = \frac{1}{4}.$$

Note that the Cesáro sum has the property $\sigma_n - \left(\frac{n-1}{n}\right)\sigma_{n-1} = \frac{a_n}{n}$. Hence for a Cesáro summable series $\sum_{n=1}^{\infty} a_n$, $\lim_{n\to\infty} \frac{a_n}{n}$ must be 0 . Therefore, $\sum_{n=1}^{\infty} (-1)^{n-1} n$ is not Cesáro summable.

□

1.4 Convergence of Fourier Series

1.4.1 Mean-square convergence

Theorem 1.25. *Let f be an integrable function on the circle with $f \sim \sum_{n=-\infty}^{\infty} a_n e^{in\theta}$. Then we have:*

i ***Mean-square convergence*** *of the Fourier series*

$$\frac{1}{2\pi}\int_0^{2\pi} |f(\theta) - S_N(f)(\theta)|^2 \, d\theta \to 0 \quad \text{as } N \to \infty$$

ii ***Parseval's identity***

$$\sum_{n=-\infty}^{\infty} |a_n|^2 = \frac{1}{2\pi}\int_0^{2\pi} |f(\theta)|^2 d\theta = \|f\|^2.$$

Theorem 1.26 (**Riemann-Lebesgue lemma**)**.** *If f is integrable on the circle, then $\hat{f}(n) \to 0$ as $|n| \to \infty$*

1.4.2 Pointwise convergence

Theorem 1.27. *Let f be an integrable function on the circle. Suppose f is differentiable at θ_0. Then* $\lim_{N\to\infty} S_N(f)(\theta_0) = f(\theta_0)$

Corollary 1.28 (Localization principle of Riemann)**.** Let f and g be integrable on the circle. Suppose $f \equiv g$ in some neighborhood of a point θ_0. Then

$$\lim_{N\to\infty} S_N(f)(\theta_0) - S_N(g)(\theta_0) = 0$$

Remark. Note that neither f nor g need to be differentiable at θ_0, and that this does not imply that the Fourier series of either converges at θ_0, only that their convergence or divergence is connected (and, if they converge, they converge to the same limit).

1.5 Continuous function with Fourier series diverging at a point

Theorem 1.18 fails, if the differentiability assumption is replaced by the **weaker assumption of continuity**. Construction is based on **"Breaking of symmetry"** in the partial sum. When we break the symmetry, that is, when we split the Fourier series $\sum_{n=-\infty}^{\infty} a_n e^{in\theta}$ into the two pieces

$$\sum_{n\geq 0} a_n e^{in\theta} \quad \text{and} \quad \sum_{n<0} a_n e^{in\theta}.$$

Consider **Sawtooth function** after re-scaling

$$f(\theta) = \begin{cases} -i(\pi+\theta) & \text{if } -\pi < \theta < 0 \\ i(\pi-\theta) & \text{if } 0 < \theta < \pi \end{cases}.$$

The fourier series of sawtooth function is given by $f(\theta) \sim \sum_{n\neq 0} \frac{e^{in\theta}}{n}$. Consider the series

$$\sum_{n=-\infty}^{-1} \frac{e^{in\theta}}{n}.$$

Note: above is not fourier series of Riemann integrable function.

Proof. Suppose to the contrary that $\exists$ a riemann integrable function $\tilde{f}$ such that

$$\hat{\tilde{f}}(n) = \begin{cases} \frac{1}{n} & \text{for } -n \in \{1, 2, \cdots\} \\ 0 & \text{for } n \in \{0, 1, 2, \cdots\} \end{cases}$$

Using the Abel means of $\tilde{f}$, we then have

$$\left| A_r(\tilde{f})(0) \right| = \sum_{n=1}^{\infty} \frac{r^n}{n}$$

which tends to infinity as r tends to 1 , because $\sum 1/n$ diverges. This gives the desired

contradiction since

$$\left|A_r(\tilde{f})(0)\right| \leq \frac{1}{2\pi}\int_{-\pi}^{\pi} |\tilde{f}(\theta)|P_r(\theta)d\theta \leq \sup_{\theta} |\tilde{f}(\theta)|$$

where $P_r(\theta)$ denotes the Poisson kernel.

□

Now,
For each $N \geq 1$ we define the following two functions on $[-\pi, \pi]$,

$$f_N(\theta) = \sum_{1\leq|n|\leq N} \frac{e^{in\theta}}{n} \quad \text{and} \quad \tilde{f}_N(\theta) = \sum_{-N\leq n\leq -1} \frac{e^{in\theta}}{n}.$$

Lemma 1.29. Suppose that the Abel means $A_r = \sum_{n=1}^{\infty} r^n c_n$ of the series $\sum_{n=1}^{\infty} c_n$ are bounded as r tends to 1 (with $r < 1$). If $c_n = O(1/n)$, then the partial sums $S_N = \sum_{n=1}^{N} c_n$ are bounded.

Claim:

1. $\left|\tilde{f}_N(0)\right| \geq c \log N$,
2. $f_N(\theta)$ is uniformly bounded in N and θ.

Proof. 1. $\left|\tilde{f}_N(0)\right| = \sum_{n=1}^{N} \frac{1}{n} \geq c \log N$, since,

$$\sum_{n=1}^{N} \frac{1}{n} \geq \sum_{n=1}^{N-1} \int_n^{n+1} \frac{dx}{x} = \int_1^N \frac{dx}{x} = \log N$$

2. We look at the series $\sum_{n\neq 0} \frac{e^{in\theta}}{n}$. Now, for $n \geqslant 1$, if $n \geqslant 1$

$$C_n = \frac{1}{n}e^{in\theta} + \frac{1}{(-n)}e^{-in\theta}$$

then $|C_n| \leqslant \frac{2}{n}$, i.e $C_n = O\left(\frac{1}{n}\right)$. Also, $A_r f(\theta) = f * P_r(\theta)$, and

$$\begin{aligned} \text{therefore } \left|A_r f(\theta)\right| &\leqslant \frac{1}{2\pi}\int_{-\pi}^{\pi}\left|f(\theta-t)\right| p_r(t)dt \\ &\leqslant \sup|f(s)|\frac{1}{2\pi}\int_{-\pi}^{\pi} p_r(t)dt \\ &= \sup_s |f(s)|. \end{aligned}$$

So, we are in a position to apply the proof of Lemma 1.30 to conclude that $\left|\sum_{\substack{n\neq 0 \\ m|\leq N}} \frac{1}{n}e^{in\theta}\right|$ is bounded uniformly in $N\&\theta$.

□

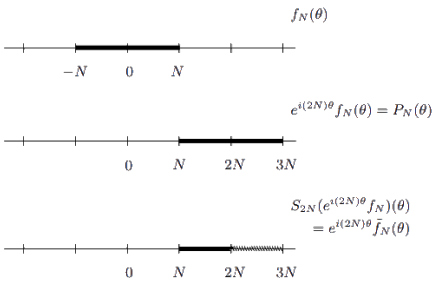
Now, we define the following two function by **shifting frequency of f_N and $\tilde{f}_N$ by $2N$ units**, we define

$$P_N(\theta) = e^{i(2N)\theta} f_N(\theta) \quad \text{and} \quad \tilde{P}_N(\theta) = e^{i(2N)\theta}\tilde{f}_N(\theta).$$

Now the coefficients of P_N are non-vanishing for $N \leq n \leq 3N$, $n \neq 2N$. Whereas coefficients of $\tilde{P}_N$ are non-vanishing for only when $N \leq n \leq 2N-1$.
$\left|\tilde{P}_N(\theta)\right| = \left|\tilde{f}_N(\theta)\right| \Rightarrow \left|\tilde{P}_N(0)\right|$ is **badly behaved** (by claim 1).

Lemma 1.30.

$$S_M(P_N) = \begin{cases} P_N & \text{if } M \geq 3N \\ \tilde{P}_N & \text{if } M = 2N \\ 0 & \text{if } M < N \end{cases}$$



Breaking symmetry in Lemma

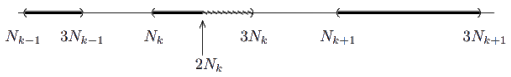
Finally, we **need to find a convergent series** of positive terms $\sum \alpha_k$ and a sequence of integers $\{N_k\}$ which increases rapidly enough so that:

1. $N_{k+1} > 3N_k$,
2. $\alpha_k \log N_k \to \infty$ as $k \to \infty$.

We choose $\alpha_k = 1/k^2$ and $N_k = 3^{2^k}$ which are easily seen to satisfy the above criteria. Finally, our desired function is

$$g(\theta) = \sum_{k=1}^{\infty} \alpha_k P_{N_k}(\theta).$$

Continuity of g follows from absolute convergence of $\sum_{k=1}^{\infty} \alpha_k P_{N_k}(\theta)$, the series above converges uniformly to a continuous periodic function.



Symmetry broken in the middle interval $(N_k, 3N_k)$

With the choice of $N_k's$,one can verity that

$$|S_{2N_m} P_{N_k}(0)| = \begin{cases} 0 & k > m \\ O(1) & k < m \end{cases}$$

However, by our lemma we get

$$|S_{2N_m}(g)(0)| \geq c\alpha_m \log N_m + O(1) \to \infty \quad \text{as } m \to \infty.$$

So the partial sums of the Fourier series of g at 0 are not bounded. Hence we proved the divergence of the Fourier series of g at $\theta = 0$.

1.6 Weyl's equidistribution criteria

1.6.1 Equidistribution

Definition 1.31. Let x be a real number. Then

1. Let $[x]$, the integer part of x, denote the greatest integer less than or equal to x.
2. Let $\langle x\rangle := x - [x]$ denote the fractional part of x.
3. Given $x, y \in \mathbb{R}$, if $x - y \in \mathbb{Z}$ we say $x \equiv y \bmod \mathbb{Z}$ or $x \equiv y \bmod 1$. Of course $x \equiv y \bmod \mathbb{Z}$ iff $\langle x\rangle = \langle y\rangle$.

We can easily see that $\{\langle n\gamma\rangle : n \in \mathbb{Z} \text{ and } \gamma = rational\}$ is finite. Also, $\{\langle n\gamma\rangle : n \in \mathbb{Z} \text{ and } \gamma = irrational\}$ is not finite.

Theorem 1.32 (Kronecker's theorem). *The sequence $\{\langle n\gamma\rangle : n \in \mathbb{Z}$ and $\gamma = irrational\}$ is dense in [0,1).*

Definition 1.33 (Definition of equidistributed sequence). A sequence of numbers $\xi_1, \xi_2, \ldots, \xi_n, \ldots$ in $[0, 1)$ is said to be **equidistributed** if for every interval $(a, b) \subset [0, 1)$,

$$\lim_{N\to\infty} \frac{\#\{1 \le n \le N : \xi_n \in (a, b)\}}{N} = b - a$$

Example 1.34. $0, \frac{1}{2}, 0, \frac{1}{3}, \frac{2}{3}, 0, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, 0, \frac{1}{5}, \frac{2}{5}, \cdots$ is equidistributed in $[0, 1]$

Example 1.35. Let $\{r_n\}_{n=1}^{\infty}$ be any enumeration of the rationals in $[0, 1)$. Then the sequence defined by

$$\xi_n = \begin{cases} r_{n/2} & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

is **NOT** equidistributed.

Now, More general version of Kronecker's theorem is as follows,

Theorem 1.36. *The sequence $\{\langle n\gamma\rangle : n \in \mathbb{Z}$ and $\gamma = irrational\}$ is equidistributed in [0,1).*

Proof. Fix $(a, b) \subset [0, 1)$ Define characteristic function on (a, b) by

$$\chi_{(a,b)}(x) = \begin{cases} 1 & \text{if } x \in (a, b) \\ 0 & \text{if } x \in [0, 1) \setminus (a, b) \end{cases}$$

Now, We may extend this function to $\mathbb{R}$ by periodicity (period 1).

Then, by applying definitions of equidistribution , we find that

$$\#\{1 \leq n \leq N : \langle n\gamma \rangle \in (a,b)\} = \sum_{n=1}^{N} \chi_{(a,b)}(n\gamma)$$

and the theorem can be reformulated as the statement of analysis that

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{(a,b)}(n\gamma) \to \int_0^1 \chi_{(a,b)}(x)dx, \quad \text{as } N \to \infty \tag{1.1}$$

Translation from number theory to analysis

This step removes the difficulty of working with fractional parts and reduces the number theory to analysis.
In order to prove 1.1 , we first established the relation 1.1 for continuous function on $\mathbb{R}$ which are periodic of period 1.

Lemma 1.37. If f is continuous and periodic of period 1, and γ is irrational, then

$$\frac{1}{N}\sum_{n=1}^{N} f(n\gamma) \to \int_0^1 f(x)dx \quad \text{as } N \to \infty$$

Assume above lemma 1.37 is true. Now,

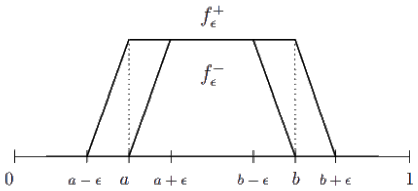
Choose two continuous periodic functions $f_\epsilon^+$and $f_\epsilon^-$of period 1 which approximate $\chi_{(a,b)}(x)$ on $[0,1)$ from above and below. In particular, $f_\epsilon^-(x) \leq \chi_{(a,b)}(x) \leq f_\epsilon^+(x)$, So, by Lemma 1.37,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f_\epsilon^-(n\gamma) = \int_0^1 f_\epsilon^-(x)dx$$
$$\& \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f_\epsilon^+(n\gamma) = \int_0^1 f_\epsilon^+(x)dx$$

Then notice that,

$$b - a - 2\epsilon = \int_{a+\epsilon}^{b=\epsilon} f_\epsilon^-(x)dx \leq \int_0^1 f_\epsilon^-(x)dx \quad \text{and}$$

$$\int_0^1 f_\epsilon^+(x)dx = \int_{a-\epsilon}^{b+\epsilon} f_\epsilon^+(x)dx \leq \int_{a-\epsilon}^{b+\epsilon} dx = b - a + 2\epsilon$$



Approximations of $\chi_{(a,b)}(x)$

If $S_N = \frac{1}{N}\sum_{n=1}^N \chi_{(a,b)}(n\gamma)$, then we get

$$\frac{1}{N}\sum_{n=1}^N f_\epsilon^-(n\gamma) \leq S_N \leq \frac{1}{N}\sum_{n=1}^N f_\epsilon^+(n\gamma)$$

$$b - a - 2\epsilon \leq \liminf_{N\to\infty} S_N \quad \text{and} \quad \limsup_{N\to\infty} S_N \leq b - a + 2\epsilon.$$

Since this is true for every $\epsilon > 0$, the limit $\lim_{N\to\infty} S_N$ exists and must equal $b - a$.

□

Theorem 1.38 (Weyl's criterion). *A sequence of real numbers $\xi_1, \xi_2 \ldots$ in $[0, 1)$ is equidistributed **if and only if** for all integers $k \neq 0$ one has*

$$\frac{1}{N}\sum_{n=1}^N e^{2\pi i k \xi_n} \to 0, \quad \text{as } N \to \infty$$

2. DISCRETE FOURIER TRANSFORM

2.1 Basic Theory

Define N-dimensional vector space over $\mathbb{C}$ with the usual notion of addition and scalar multiplication

$\ell^2(\mathbb{Z}_N) = \{z = (z(0), z(1), \ldots, z(N-1)) : z(j) \in \mathbb{C}, 0 \leq j \leq N-1\}$

With one standard basis for $\ell^2(\mathbb{Z}_N)$ is the Euclidean basis $E = \{e_0, e_1, \ldots, e_{N-1}\}$, where $e_j(n) = 1$ if $n = j$ and $e_j(n) = 0$ if $n \neq j$.

The complex inner product on $\ell^2(\mathbb{Z}_N)$ is

$$\langle z, w \rangle = \sum_{k=0}^{N-1} z(k)\overline{w(k)}$$

with the norm associated to it

$$\|z\| = \left(\sum_{k=0}^{N-1} |z(k)|^2 \right)^{1/2}. \qquad (\ell^2 \text{ norm})$$

Definition 2.1. Define $E_0, E_1, \ldots, E_{N-1} \in \ell^2(\mathbb{Z}_N)$ by

$$E_m(n) = \frac{1}{\sqrt{N}} e^{2\pi imn/N} \quad \text{for} \quad 0 \leq m, n \leq N-1$$

Lemma 2.2. The set $\{E_0, \ldots, E_{N-1}\}$ is an orthonormal basis for $\ell^2(\mathbb{Z}_N)$

Definition 2.3 (Discrete Fourier Transform)**.** Suppose $z = (z(0), \ldots, z(N-1)) \in \ell^2(\mathbb{Z}_N)$. For $m = 0, 1, \ldots, N-1$, define

$$\hat{z}(m) = \sum_{n=0}^{N-1} z(n) e^{-2\pi imn/N}$$

Let

$$\hat{z} = (\hat{z}(0), \hat{z}(1), \ldots, \hat{z}(N-1))$$

Then $\hat{z} \in \ell^2(\mathbb{Z}_N)$. The map $\hat{}: \ell^2(\mathbb{Z}_N) \to \ell^2(\mathbb{Z}_N)$, which takes z to $\hat{z}$, is called the **discrete Fourier transform**.

Remark:

1. The above formula use to define $\hat{z}(m)$ for all $m \in \mathbb{Z}$, is periodic with period N :

$$\begin{aligned}\hat{z}(m+N) &= \sum_{n=0}^{N-1} z(n) e^{-2\pi i(m+N)n/N} \\ &= \sum_{n=0}^{N-1} z(n) e^{-2\pi imn/N} e^{-2\pi iNn/N} = \hat{z}(m)\end{aligned}$$

$$\text{since } e^{-2\pi iNn/N} = e^{-2\pi in} = 1 \text{ for every } n \in \mathbb{Z}$$

2. The DFT can be represented by a matrix,because the map taking z to $\hat{z}$ is a linear transformation.

Definition 2.4 (DFT in matrix form)**.**

$$\hat{z} = W_N z$$

where, W_N be the matrix $[w_{mn}]_{0 \le m,n \le N-1}$ such that $\omega_N^{mn} = e^{2\pi imn/N}$ and

$$W_N = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdot & \cdot & 1 \\ 1 & \omega_N & \omega_N^2 & \omega_N^3 & \cdot & \cdot & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \omega_N^6 & \cdot & \cdot & \omega_N^{2(N-1)} \\ 1 & \omega_N^3 & \omega_N^6 & \omega_N^9 & \cdot & \cdot & \omega_N^{3(N-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \omega_N^{3(N-1)} & \cdot & \cdot & \omega_N^{(N-1)(N-1)} \end{bmatrix}.$$

Example 2.5. Let $z = (1, 0, -3, 4) \in \ell^2(\mathbb{Z}_4)$. Find $\hat{z}$.

Solution

$$\hat{z} = W_4 z = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ -3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 4+4i \\ -6 \\ 4-4i \end{bmatrix}$$

How Many Complex Multiplications Are Required?

- Each inner product requires N complex multiplications.
  - There are N inner products.
- Hence we require N^2 multiplications.
- However, the first row and first column are all 1 s, and should not be counted as multiplications.
  - There are $2N-1$ such instances.
- Hence, the number of complex multiplications is $N^2 - 2N + 1$ i.e., $(N-1)^2$.

Theorem 2.6. *Let* $z = (z(0), z(1), \ldots, z(N-1)), w = (w(0)w(1), \ldots, w(N-1)) \in \ell^2(\mathbb{Z}_N)$. *Then*

i ***(Fourier inversion formula)***

$$z(n) = \frac{1}{N} \sum_{m=0}^{N-1} \hat{z}(m) e^{2\pi i m n/N} \text{ for } n = 0, 1, \ldots, N-1$$

ii ***(Parseval's relation)***

$$\langle z, w \rangle = \frac{1}{N} \sum_{m=0}^{N-1} \hat{z}(m) \overline{\hat{w}(m)} = \frac{1}{N} \langle \hat{z}, \hat{w} \rangle$$

iii ***(Plancherel's formula)***

$$\|z\|^2 = \frac{1}{N} \sum_{m=0}^{N-1} |\hat{z}(m)|^2 = \frac{1}{N} \|\hat{z}\|^2$$

Proof. i

$$\begin{aligned} z(n) &= \sum_{m=0}^{N-1} \langle z, E_m \rangle \, E_m(n) \\ &= \sum_{m=0}^{N-1} \frac{1}{\sqrt{N}} \hat{z}(m) \frac{1}{\sqrt{N}} e^{\frac{2\pi i m n}{N}} \\ &= \frac{1}{N} \sum_{m=0}^{N-1} \hat{z}(m) e^{\frac{2\hbar i m n}{N}} \qquad \text{for } n = 0, 1, -N-1 \end{aligned}$$

ii

$$\begin{aligned} \langle z, \omega \rangle &= \sum_{m=0}^{N-1} \langle z, E_m \rangle \left\langle \overline{\omega, E_m} \right\rangle \\ &= \sum_{m=0}^{N-1} \frac{1}{\sqrt{N}} \hat{z}(m) \frac{1}{\sqrt{N}} \hat{\omega}(m) \\ &= \frac{1}{n} \langle \hat{z}, \hat{\omega} \rangle \end{aligned}$$

iii for $\omega = z, \quad \langle \hat{z}, \hat{z} \rangle = \|\hat{z}\|^2$

□

Definition 2.7 (Fourier basis for $\ell^2(\mathbb{Z}_N)$)**.** For $m = 0, 1, \ldots, N-1$, define $F_m \in \ell^2(\mathbb{Z}_N)$ by

$$F_m(n) = \frac{1}{N} e^{2\pi i m n / N}, \quad \text{for} \quad n = 0, 1, \ldots, N-1$$

Definition 2.8. The map : $\ell^2(\mathbb{Z}_N) \to \ell^2(\mathbb{Z}_N)$ is the **inverse discrete Fourier transform**, or **IDFT**. For $w = (w(0), \ldots, w(N-1)) \in \ell^2(\mathbb{Z}_N)$, define

$$\check{w}(n) = \frac{1}{N} \sum_{m=0}^{N-1} w(m) e^{2\pi i m n / N}, \text{ for } n = 0, 1, \ldots, N-1$$

Important points

1. $(\check{w})^{\wedge} = w$
2. Since the DFT is an invertible linear transformation, the matrix W_N is invertible, Then we have

$$\check{w} = W_N^{-1} w$$

where, $w_N^{-1} = \frac{\overline{\omega_N}}{N}$

Proof. We have colomns ol a matrix forms orthonormal basis for $\ell^2(\mathbb{Z}_N)$ So, $\frac{1}{\sqrt{N}}\omega_N$ is unilary matrix Now,

$$\left(\frac{1}{\sqrt{N}}\omega_N\right)\left(\frac{1}{\sqrt{N}}\omega_N\right)^H = I$$
$$\frac{1}{N}\omega_N\overline{\omega_N} = 1$$
$$\Rightarrow \omega_{N^{-1}} = \frac{1}{N}\overline{\omega_N}$$

□

3. $\check{w}$ has period $N : \check{w}(n+N) = \check{w}(n)$ for all n.

4. easy to see by definition of DFT and IDFT

$$\check{w}(n) = \frac{1}{N}\hat{w}(-n)$$

Since $\check{w}$ has period N, we can write this as

$$\check{w}(n) = \frac{1}{N}\hat{w}(N-n)$$

which is more convenient since $n \in \{1,\ldots,N-1\}$ if and only if $N-n \in \{1,\ldots,N-1\}$; the exceptional case is $n=0$, for which $N-n=N$

2.1.1 Translation-Invariant Linear Transformations

Definition 2.9. Suppose $z \in \ell^2(\mathbb{Z}_N)$ and $k \in \mathbb{Z}$. Define

$$(R_k z)(n) = z(n-k) \quad \text{for} \quad n \in \mathbb{Z}$$

We call $R_k z$ **the translate of** z **by** k**.**

Lemma 2.10. Suppose $z \in \ell^2(\mathbb{Z}_N)$ and $k \in \mathbb{Z}$. Then for any $m \in \mathbb{Z}$,

$$(R_k z)^\wedge(m) = e^{-2\pi imk/N}\hat{z}(m)$$

Proof. By definition,

$$(R_k z)^\wedge(m) = \sum_{n=0}^{N-1} (R_k z)(n) e^{-2\pi i m n/N} = \sum_{n=0}^{N-1} z(n-k) e^{-2\pi i m n/N}$$

In this last sum, we change variables by letting $\ell = n - k$ (recall k is fixed, and n is the summation variable). If $n = 0$, then $\ell = -k$, whereas for $n = N - 1$, we have $\ell = N - k - 1$. Since $n = \ell + k$, we obtain

$$(R_k z)^\wedge(m) = \sum_{\ell=-k}^{N-k-1} z(\ell) e^{-2\pi i m(\ell+k)/N} = e^{-2\pi i m k/N} \sum_{\ell=-k}^{N-k-1} z(\ell) e^{-2\pi i m \ell/N}$$

However, we claim that

$$\sum_{\ell=-k}^{N-k-1} z(\ell) e^{-2\pi i m \ell/N} = \sum_{n=0}^{N-1} z(n) e^{-2\pi i m n/N} = \hat{z}(m)$$

If so, substituting this gives the final result. To see above equation , note that both $z(\ell)$ and $e^{-2\pi i m \ell/N}$ are periodic functions in the variable

ℓ with period N. If $k = 0$, there is nothing to prove, so suppose $0 < k \leq N - 1$. Then

$$\sum_{\ell=-k}^{N-k-1} z(\ell) e^{-2\pi i m \ell/N} = \sum_{\ell=-k}^{-1} z(\ell + N) e^{-2\pi i m(\ell+N)/N} + \sum_{\ell=0}^{N-k-1} z(\ell) e^{-2\pi i m \ell/N}$$

In the first of these last two sums, we let $n = \ell + N$, whereas in the second we just let $n = \ell$. This gives us

$$\begin{aligned}\sum_{\ell=-k}^{N-k-1} z(\ell) e^{-2\pi i m \ell/N} &= \sum_{n=N-k}^{N-1} z(n) e^{-2\pi i m n/N} + \sum_{n=0}^{N-k-1} z(n) e^{-2\pi i m n/N} \\ &= \sum_{n=0}^{N-1} z(n) e^{-2\pi i m n/N}\end{aligned}$$

as desired. Now let $k \in \mathbb{Z}$ be arbitrary. Then there is some integer r such that $k' = k + rN \in \{0, 1, 2, \ldots, N-1\}$. Then, by changing the summation variable by setting

$\ell' = \ell - rN$ we get

$$\sum_{\ell=-k}^{N-k-1} z(\ell) e^{-2\pi i m \ell/N} = \sum_{\ell'=-k-rN}^{N-k-rN-1} z\left(\ell' + rN\right) e^{-2\pi i m(\ell'+rN)/N}$$
$$= \sum_{\ell'=-k'}^{N-k'-1} z\left(\ell'\right) e^{-2\pi i m \ell'/N}$$

by the N-periodicity of both z and the exponential. So by the case $k' \in \{0, 1, 2, \ldots, N-1\}$ considered above, the last sum is $\hat{z}(m)$. □

Definition 2.11. Let $T : \ell^2\left(\mathbb{Z}_N\right) \to \ell^2\left(\mathbb{Z}_N\right)$ be a linear transformation. T is **translation invariant** if

$$T\left(R_k z\right) = R_k T(z)$$

for all $z \in \ell^2\left(\mathbb{Z}_N\right)$ and all $k \in \mathbb{Z}$.

Definition 2.12 (Periodicity of matrix). For $[a_{mn}]_{0 \le m,n \le N-1}$ given, we define, a_{mn} for all $m, n \in \mathbb{Z}$ by assuming periodicity with period N in each index:

$$a_{m+N,n} = a_{mn} \quad \text{and} \quad a_{m,n+N} = a_{mn}$$

for all m and n

Definition 2.13 (Circulant). A matrix $A = [a_{mn}]_{0 \le m,n \le N-1}$, periodized as above, is **circulant** if

$$a_{m+k,n+k} = a_{m,n}$$

for all $m, n, k \in \mathbb{Z}$.

Example 2.14. The matrix is circulant

$$\begin{bmatrix} 3 & 2+i & -1 & 4i \\ 4i & 3 & 2+i & -1 \\ -1 & 4i & 3 & 2+i \\ 2+i & -1 & 4i & 3 \end{bmatrix}$$

Definition 2.15 (Convolution). For $z, w \in \ell^2\left(\mathbb{Z}_N\right)$, the convolution $z * w \in \ell^2\left(\mathbb{Z}_N\right)$ is

the vector with components

$$z * w(m) = \sum_{n=0}^{N-1} z(m-n)w(n)$$

for all m.

Definition 2.16 (Convolution operator). Definition 2.25 Suppose $b \in \ell^2(\mathbb{Z}_N)$. Define $T_b : \ell^2(\mathbb{Z}_N) \to \ell^2(\mathbb{Z}_N)$ *by*

$$T_b(z) = b * z$$

for all $z \in \ell^2(\mathbb{Z}_N)$. Any transformation T of the form $T = T_b$, for some $b \in \ell^2(\mathbb{Z}_N)$, is called a convolution operator.

Lemma 2.17. Let A be an $N \times N$ matrix, $A = [a_{mn}]_{0 \le m,n \le N-1}$. Suppose A is circulant. Define $b \in \ell^2(\mathbb{Z}_N)$ by

$$b(n) = a_{n,0}$$

for all n. Then for all $z \in \ell^2(\mathbb{Z}_N)$,

$$Az = b * z = T_b(z)$$

Proof. Since A is circulant, we have

$$a_{mn} = a_{m-n,0} = b(m-n)$$

for any $m, n \in \mathbb{Z}$. Hence, by the definition of matrix multiplication,

$$(Az)(m) = \sum_{n=0}^{N-1} a_{mn} z(n) = \sum_{n=0}^{N-1} b(m-n)z(n) = b * z(m)$$

□

Definition 2.18 (Dirac delta function). Define $\delta \in \ell^2(\mathbb{Z}_N)$ by

$$\delta(n) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n = 1, 2, \ldots, N-1 \end{cases}$$

Lemma 2.19. Suppose $z, w \in \ell^2(\mathbb{Z}_N)$. Then for each m,

$$(z * w)^\wedge(m) = \hat{z}(m)\hat{w}(m)$$

Definition 2.20 (Fourier multiplier operator). Definition 2.32 Let $m \in \ell^2(\mathbb{Z}_N)$. Define $T_{(m)} : \ell^2(\mathbb{Z}_N) \to \ell^2(\mathbb{Z}_N)$ by

$$T_{(m)}(z) = (m\hat{z})^\vee$$

where $m\hat{z}$ is the vector obtained from multiplying m and $\hat{z}$ component-wise; that is, $(m\hat{z})(n) = m(n)\hat{z}(n)$ for each n.

Theorem 2.21. *Let $T : \ell^2(\mathbb{Z}_N) \to \ell^2(\mathbb{Z}_N)$ be a linear transformation. Then the following statements are equivalent:*

1. *T is translation invariant.*
2. *The matrix $A_{T,E}$ representing T in the standard basis E is circulant.*
3. *T is a convolution operator.*
4. *T is a Fourier multiplier operator.*
5. *The matrix $A_{T,F}$ representing T in the Fourier basis F is diagonal.*

Example 2.22. Define $T : \ell^2(\mathbb{Z}_4) \to \ell^2(\mathbb{Z}_4)$ by

$$T(z)(n) = z(n) + 2z(n+1) + z(n+3)$$

Find the eigenvalues and eigenvectors of T, and diagonalize the matrix A representing T in the standard basis, if possible.
Solution One can check that T is translation invariant:

$$\begin{aligned} T(R_k z) &= (R_k z)(n) + 2(R_k z)(n+1) + (R_k z)(n+3) \\ &= z(n-k) + 2z(n+1-k) + z(n+3-k) \\ &= R_k(z(n) + 2z(n+1) + z(n+3)) = R_k T(z) \end{aligned}$$

Alternatively, one can write the matrix A that represents T in the standard basis (i.e., satisfying $T(z) = Az$) by considering $T(z)(0), T(z)(1), T(z)(2)$, and $T(z)(3)$, obtaining

$$A = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 \\ 2 & 0 & 1 & 1 \end{bmatrix}$$

which is circulant. Then $b = (1, 1, 0, 2)$. we can easily calculated $\hat{b}$, where we obtained $m = \hat{b} = (4, 1 + i, -2, 1 - i)$. These components are the eigenvalues of A, and the eigenvectors are the Fourier basis vectors in F. In particular,

$$D = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1-i \end{bmatrix}$$

satisfies $W_4 A W_4^{-1} = D$.

2.2 Fast Fourier Transform

Theorem 2.23 (Danielson and Lanczos Lemma (FFT)). *Suppose $M \in \mathbb{N}$, and $N = 2M$. Let $z \in \ell^2(\mathbb{Z}_N)$. Define $u, v \in \ell^2(\mathbb{Z}_M)$ by*

$$u(k) = z(2k) \quad \textit{for} \quad k = 0, 1, \ldots, M-1$$

and

$$v(k) = z(2k+1) \textit{ for} \quad k = 0, 1, \ldots, M-1$$

Then for $m = 0, 1, \ldots, M-1$

$$\hat{z}(m) = \hat{u}(m) + e^{-2\pi i m/N} \hat{v}(m) \tag{2.1}$$

Also, for $m = M, M+1, M+2, \ldots, N-1$, let $\ell = m - M$. Note that the corresponding values of ℓ are $\ell = 0, 1, \ldots, M-1$. Then

$$\hat{z}(m) = \hat{z}(\ell + M) = \hat{u}(\ell) - e^{-2\pi i \ell/N}\hat{v}(\ell). \tag{2.2}$$

Proof. For any $m = 0, 1, \ldots, N-1$,

$$\hat{z}(m) = \sum_{n=0}^{N-1} z(n) e^{-2\pi i m n/N}$$

Then for $m = 0, 1, \ldots, M-1$

$$\begin{aligned}
\hat{z}(m) &= \sum_{k=0}^{M-1} z(2k) e^{-2\pi i 2km/N} + \sum_{k=0}^{M-1} z(2k+1) e^{-2\pi i (2k+1)m/N} \\
&= \sum_{k=0}^{M-1} u(k) e^{-2\pi i km/(N/2)} + e^{-2\pi i m/N} \sum_{k=0}^{M-1} v(k) e^{-2\pi i km/(N/2)} \\
&= \sum_{k=0}^{M-1} u(k) e^{-2\pi i km/M} + e^{-2\pi i m/N} \sum_{k=0}^{M-1} v(k) e^{-2\pi i km/M} \\
&= \hat{u}(m) + e^{-2\pi i m/N}\hat{v}(m).
\end{aligned}$$

For $m = M, M+1, \ldots, N-1$. By writing $m = \ell + M$ for $\ell = 0, 1, \ldots, M-1$, we get

$$\begin{aligned}
\hat{z}(m) &= \sum_{k=0}^{M-1} z(2k) e^{-2\pi i 2km/N} + \sum_{k=0}^{M-1} z(2k+1) e^{-2\pi i (2k+1)m/N} \\
&= \sum_{k=0}^{M-1} u(k) e^{-2\pi i k(\ell+M)/M} + e^{-2\pi i (\ell+M)/N} \sum_{k=0}^{M-1} v(k) e^{-2\pi i k(\ell+M)/M} \\
&= \sum_{k=0}^{M-1} u(k) e^{-2\pi i k\ell/M} - e^{-2\pi i \ell/N} \sum_{k=0}^{M-1} v(k) e^{-2\pi i k\ell/M} \\
&= \hat{u}(\ell) - e^{-2\pi i \ell/N}\hat{v}(\ell) = \hat{z}(\ell + m)
\end{aligned}$$

Since the exponential $e^{-2\pi i k l/M}$ are periodic with period M, and $e^{-2\pi i M/N} = e^{-\pi i} = -1$ for $N = 2M$. □

Example 2.24. Let $z = (1, 1, 1, i, 1, -1, 1, -i)$. Find $\hat{z}$.

Solution Following theorem, we obtain

$$u = (1, 1, 1, 1) \quad \text{and} \quad v = (1, i, -1, -i)$$

Note that $u = 4F_0$ and $v = 4F_1$ by direct computation,

$$\hat{u} = (4, 0, 0, 0) \quad \text{and} \quad \hat{v} = (0, 4, 0, 0)$$

Hence by equation 2.1,

$$\begin{aligned}
\hat{z}(0) &= \hat{u}(0) + 1\hat{v}(0) = 4 + 0 = 4 \\
\hat{z}(1) &= \hat{u}(1) + e^{-2\pi i 1/8}\hat{v}(1) = 0 + 4e^{-\pi i/4} = 2\sqrt{2} - 2\sqrt{2}i \\
\hat{z}(2) &= \hat{u}(2) + e^{-2\pi i 2/8}\hat{v}(2) = 0 + 0 = 0
\end{aligned}$$

and

$$\hat{z}(3) = \hat{u}(3) + e^{-2\pi i 3/8}\hat{v}(3) = 0 + 0 = 0$$

Then by equation 2.2,

$$\begin{aligned}
\hat{z}(4) &= \hat{u}(0) - 1\hat{v}(0) = 4 - 0 = 4 \\
\hat{z}(5) &= \hat{u}(1) - e^{-2\pi i 1/8}\hat{v}(1) = 0 - 4e^{-\pi i/4} = -2\sqrt{2} + 2\sqrt{2}i \\
\hat{z}(6) &= \hat{u}(2) - e^{-2\pi i 2/8}\hat{v}(2) = 0 - 0 = 0
\end{aligned}$$

and

$$\hat{z}(7) = \hat{u}(3) - e^{-2\pi i 3/8}\hat{v}(3) = 0 - 0 = 0$$

Hence

$$\hat{z} = (4, 2\sqrt{2} - 2\sqrt{2}i, 0, 0, 4, -2\sqrt{2} + 2\sqrt{2}i, 0, 0)$$

Complexity

- $$\#_N \leq 2\#_M + M \tag{2.3}$$

  where, $\#_N$, for any positive integer N, to be the least number of complex multiplications required to compute the DFT of a vector of length N.

- The most favorable case is when $N = 2^n$.

- *Note :* If $N \neq 2^n$, then it is harmless to pad it with some extra zeros at the end until it has length $N = 2^n$.

Lemma 2.25. Suppose $N = 2^n$ for some $n \in \mathbb{N}$. Then

$$\#_N \leq \frac{1}{2} N \log_2 N.$$

Proof. proof is by induction on n

- When $n = 1$, a vector of length 2^1 is of the form $z = (a, b)$. Then from the definition

  $$\hat{z} = (a + b, a - b)$$

  Note that this computation does not require any complex multiplications, so $\#_2 = 0 < 1 = (2 \log_2 2)/2$. So the result holds.

- By induction, suppose it holds for $n = k - 1$.

  $$\#_{2^{k-1}} \leq \frac{1}{2}(k-1)2^{k-1}$$

- Then for $n = k$, by equation 2.3 and the induction hypothesis that

  $$\begin{aligned} \#_{2^k} \leq 2\#_{2^{k-1}} + 2^{k-1} &\leq 2\frac{1}{2}2^{k-1}(k-1) + 2^{k-1} \\ &= k2^{k-1} = \frac{1}{2}k2^k = \frac{1}{2}N \log_2 N \end{aligned}$$

  This completes the induction step, and hence establishes the result.

□

2.2.1 Generalised version of FFT

Theorem 2.26. *Suppose* $p, q \in \mathbb{N}$ *and* $N = pq$. *Let* $z \in \ell^2(\mathbb{Z}_N)$. *Define* $w_0, w_1, \ldots, w_{p-1} \in \ell^2(\mathbb{Z}_q)$ *by*

$$w_\ell(k) = z(kp + \ell) \quad \textit{for} \quad k = 0, 1, \ldots, q-1$$

For $b = 0, 1, \ldots, q-1$, define $v_h \in \ell^2(\mathbb{Z}_p)$ by

$$v_b(\ell) = e^{-2\pi i b\ell/N}\hat{w}_\ell(b) \quad \textit{for} \quad \ell = 0, 1, \ldots, p-1$$

Then for $a = 0, 1, \ldots, p-1$ and $b = 0, 1, \ldots, q-1$,

$$\hat{z}(aq+b) = \hat{v}_b(a)$$

Note that by the division algorithm, every $m = 0, 1, \ldots, N-1$ is of the form $aq+b$ for some $a \in \{0, 1, \ldots, p-1\}$ and $b \in \{0, 1, \ldots, q-1\}$, so above equation gives the full DFT of z.

Proof. We can write each $n = 0, 1, \ldots, N-1$ uniquely in the form $kp + \ell$ for some $k \in \{0, 1, \ldots, q-1\}$ and $\ell \in \{0, 1, \ldots, p-1\}$. Hence

$$\hat{z}(aq+b) = \sum_{n=0}^{N-1} z(n)e^{-2\pi i(aq+b)n/N} = \sum_{\ell=0}^{p-1}\sum_{k=0}^{q-1} z(kp+\ell)e^{-2\pi i(aq+b)(kp+\ell)/(pq)}.$$

Note that

$$e^{-2\pi i(aq+b)(kp+\ell)/(pq)} = e^{-2\pi iak}e^{-2\pi ia\ell/p}e^{-2\pi ibk/q}e^{-2\pi ib\ell/(pq)}$$

Since $e^{-2\pi iak} = 1$ and $pq = N$, using the definition of $w_\ell(k)$ we obtain

$$\begin{aligned}\hat{z}(aq+b) &= \sum_{\ell=0}^{p-1} e^{-2\pi ia\ell/p}e^{-2\pi ib\ell/N}\sum_{k=0}^{q-1} w_\ell(k)e^{-2\pi ibk/q} \\ &= \sum_{\ell=0}^{p-1} e^{-2\pi ia\ell/p}e^{-2\pi ib\ell/N}\hat{w}_\ell(b) = \sum_{\ell=0}^{p-1} e^{-2\pi ia\ell/p}v_b(\ell) = \hat{v}_b(a)\end{aligned}$$

□

2.2.2 Iterative FFT

For simplicity, we restrict ourselves here to the case where N is a power of 2 , say $N = 2^n$. Then we can expand any $m \in \{0, 1, \ldots, N-1\}$ in base 2 in the form

$$m = m_0 + 2m_1 + 2^2m_2 + \cdots + 2^{n-1}m_{n-1}$$

where $m_0, m_1, \ldots, m_{n-1} \in \{0, 1\}$. For $z \in \ell^2(\mathbb{Z}_N)$, denote

$$z(m) = z(m_{n-1}, m_{n-2}, \ldots, m_1, m_0).$$

For any $k = k_0 + 2k_1 + 2^2k_2 + \cdots + 2^{n-1}k_{n-1}$ with $k_0, k_1, \ldots, k_{n-1} \in \{0, 1\}$,

Then,

$$\begin{aligned}
\hat{z}(k) &= \sum_{m=0}^{N-1} z(m) e^{-2\pi i k m/N} \\
&= \sum_{m_0=0}^{1} \sum_{m_1=0}^{1} \cdots \sum_{m_{n-1}=0}^{1} z(m_{n-1}, m_{n-2}, \ldots, m_1, m_0) \\
&\times \exp\left(\frac{-2\pi i (k_0 + 2k_1 + \cdots + 2^{n-1}k_{n-1})(m_0 + 2m_1 + \cdots + 2^{n-1}m_{n-1})}{2^n} \right),
\end{aligned}$$

where $\exp(t)$ denotes e^t. Now

$$\begin{aligned}
&\exp\Big(\frac{-2\pi i (k_0 + 2k_1 + \cdots + 2^{n-1}k_{n-1})(m_0 + 2m_1 + \cdots + 2^{n-1}m_{n-1})}{2^n} \Big) \\
&= \exp\left(\frac{-2\pi i (k_0 + 2k_1 + \cdots + 2^{n-1}k_{n-1}) 2^{n-1} m_{n-1}}{2^n} \right) \cdots \\
&\times \exp\left(\frac{-2\pi i (k_0 + 2k_1 + \cdots + 2^{n-1}k_{n-1}) 2m_1}{2^n} \right) \\
&\times \exp\left(\frac{-2\pi i (k_0 + 2k_1 + \cdots + 2^{n-1}k_{n-1}) m_0}{2^n} \right)
\end{aligned}$$

Remark: In each exponent we can delete all products that give an integer multiple of $2\pi i 2^n$ in the numerator because after division by 2^n, the argument is an integer multiple of 2π.

Thus,

$$\begin{aligned}
&\exp\left(\frac{-2\pi i\left(k_0+2k_1+\cdots+2^{n-1}k_{n-1}\right)\left(m_0+2m_1+\cdots+2^{n-1}m_{n-1}\right)}{2^n}\right)\\
&=\exp\left(\frac{-2\pi i k_0 2^{n-1}m_{n-1}}{2^n}\right)\exp\left(\frac{-2\pi i\left(k_0+2k_1\right)2^{n-2}m_{n-2}}{2^n}\right)\\
&\quad\times\exp\left(\frac{-2\pi i\left(k_0+2k_1+2^2k_2\right)2^{n-3}m_{n-3}}{2^n}\right)\cdots\\
&\quad\times\exp\left(\frac{-2\pi i\left(k_0+2k_1+2^2k_2+\cdots+2^{n-1}k_{n-1}\right)m_0}{2^n}\right).
\end{aligned}$$

Note: Now, Substituting this into the preceding equation gives

$$\begin{aligned}
\hat{z}(k)=&\sum_{m_0=0}^{1}\sum_{m_1=0}^{1}\cdots\sum_{m_{n-1}=0}^{1}z\left(m_{n-1},\ldots,m_1,m_0\right)\exp\left(\frac{-2\pi i k_0 2^{n-1}m_{n-1}}{2^n}\right)\\
&\times\exp\left(\frac{-2\pi i\left(k_0+2k_1\right)2^{n-2}m_{n-2}}{2^n}\right)\cdots\\
&\times\exp\left(\frac{-2\pi i\left(k_0+2k_1+\cdots+2^{n-1}k_{n-1}\right)m_0}{2^n}\right).
\end{aligned}$$

Remark: Notice that the inside sum depends on the outside summation variables $m_0, m_1, \ldots, m_{n-2}$ and on k_0 but not on $k_1, \ldots, k_{n-1}$.

So define

$$\begin{aligned}
&y_1\left(k_0, m_{n-2}, m_{n-3}, \ldots, m_0\right)\\
=&\sum_{m_{n-1}=0}^{1}z\left(m_{n-1}, m_{n-2}, \ldots, m_1, m_0\right)\exp\left(-2\pi i k_0 2^{n-1}m_{n-1}/2^n\right)\\
=&z\left(0, m_{n-2}, \ldots, m_1, m_0\right)\cdot 1\\
&+z\left(1, m_{n-2}, \ldots, m_1, m_0\right)\exp\left(\frac{-2\pi i k_0 2^{n-1}}{2^n}\right).
\end{aligned}$$

Note: Computing $y_1\left(k_0, m_{n-2}, m_{n-3}, \ldots, m_0\right)$ requires only one complex multiplication for each of the 2^n choices of $k_0, m_{n-2}, m_{n-3}, \ldots, m_0 \in \{0,1\}$, for a total of 2^n complex multiplications to compute all 2^n possible values of y_1.

At the next step, define

$$\begin{aligned} & y_2\left(k_0,\ k_1, m_{n-3}, \ldots, m_0\right) \\ & \quad = \sum_{m_{n-2}=0}^{1} y_1\left(k_0, m_{n-2}, m_{n-3}, \ldots, m_0\right) \\ & \qquad \times \exp\left(\frac{-2\pi i\left(k_0+2k_1\right) 2^{n-2} m_{n-2}}{2^n}\right). \end{aligned}$$

Remark: It takes just one complex multiplication to compute each one of these, hence 2^n total to compute all possible values of y_2. We continue in this way, each time replacing the highest remaining m index by the next k index.

Thus the scheme is to make the sequence of transformations

$$\begin{gathered} z\left(m_{n-1}, m_{n-2}, \ldots, m_1, m_0\right) \rightarrow y_1\left(k_0, m_{n-2}, m_{n-3}, \ldots, m_0\right), \\ y_1\left(k_0, m_{n-2}, m_{n-3}, \ldots, m_0\right) \rightarrow y_2\left(k_0, k_1, m_{n-3}, \ldots, m_0\right), \\ \vdots \\ y_{n-1}\left(k_0, k_1, k_2, \ldots, k_{n-2}, m_0\right) \rightarrow y_n\left(k_0, k_1, k_2, \ldots, k_{n-2}, k_{n-1}\right). \end{gathered}$$

Complexity

- Each step we required at most 2^n computation.
- There are n steps.
- Total $= n2^n = N \log_2 N$ computations.
- *Note:* Onces y_i has been computed y_{i-1} is no longer needed.

More application of FFT

1. **Inverse Discrete Fourier Transform** We know simple relation between IDFT and DFT which is $\check{w}(n) = \frac{1}{N}\hat{w}(N-n)$. Hence, FFT algorithm can be used to compute the IDFT quickly also, in at most $(N/2)\log_2 N$ steps if $N = 2^n$.
2. **Convolution** We know formula for convolution in terms of DFT and IDFT is $z * w = (\hat{z}\hat{w})\check{}$. If $z, w \in \ell^2\left(\mathbb{Z}_N\right)$, for $N = 2^n$, it takes at most $N \log_2 N$ multiplications to compute $\hat{z}$ and $\hat{w}$ and there are N multiplications to compute $\hat{z}\hat{w}$,

and at most $(N/2)\log_2 N$ multiplications to take the IDFT of $\hat{z}\hat{w}$. Thus overall, $N + (3N/2)\log_2 N$ multiplications to compute $z * w$.

Comparative graph

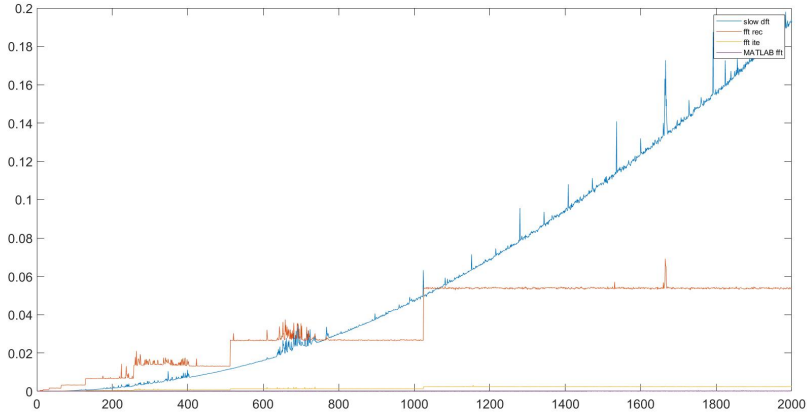


Fig. 2.1: Comparison of the runtimes of four DFT/FFT algorithms, for arrays of lengths from 100 to 2000

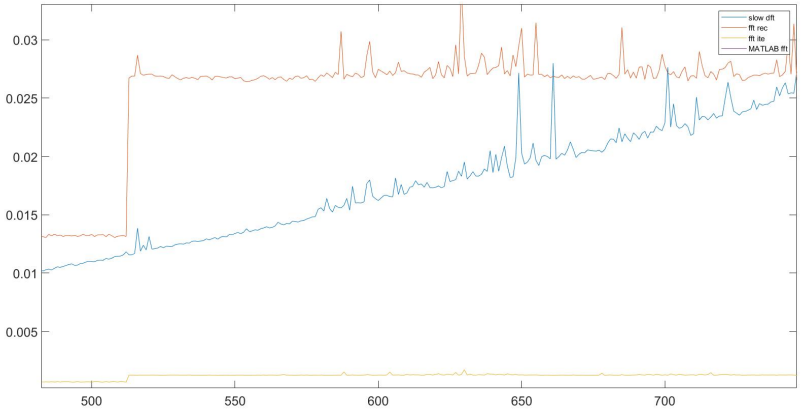


Fig. 2.2: Smaller upper bound on the runtime axis in order to show the difference in speed between the iterative FFT and MATLAB's in-built FFT

3. ROTH'S THEOREM ON 3-TERM ARITHMETIC PROGRESSIONS

In this chapter, we study at Roth's theorem, which states that given certain size constraints, every subset of integers has 3-term arithmetic progressions. Roth's theorem is a foundational result in additive combinatorics and has laid foundation for many important developments.

3.1 Roth's Theorem in the Finite Field Model

In this section, we use Fourier analysis to prove the finite field analogue of Roth's theorem (Meshulam 1995). Later in the chapter, we will convert this proof to the integer setting.

In an abelian group, a set A is said to be **3-AP-free** if A does not have three distinct elements of the form $x, x+y, x+2y$. A 3-AP-free subset of $\mathbb{F}_3^n$ is also called a **cap set**. The **cap set problem** is to determine the size of the largest cap set in $\mathbb{F}_3^n$.

Theorem 3.1. *(**Roth's theorem in** $\mathbb{F}_3^n$) Every 3 -AP-free subset of* $\mathbb{F}_3^n$ *has size* $O\left(3^n/n\right)$.

3.1.1 Fourier Analysis in Finite Field Vector Spaces

We will see some basic facts about Fourier analysis in $\mathbb{F}_p^n$ for a prime p. Everything here can be extended to arbitrary abelian groups.

Definition 3.2. (**Fourier transform in** $\mathbb{F}_p^n$) The Fourier transform of $f : \mathbb{F}_p^n \to \mathbb{C}$ is a function $\widehat{f} : \mathbb{F}_p^n \to \mathbb{C}$ defined by setting, for each $r \in \mathbb{F}_p^n$,

$$\widehat{f}(r) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{-r \cdot x} = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} f(x)\omega^{-r \cdot x}$$

where

- $\omega = \exp(2\pi i/p)$
- $r \cdot x = r_1 x_1 + \cdots + r_n x_n$.

Note: $\widehat{f}(0) = \mathbb{E}f$

The next result allows us to write f in terms of $\widehat{f}$.

Theorem 3.3. ***(Fourier inversion formula)*** *Let $f : \mathbb{F}_p^n \to \mathbb{C}$. For every $x \in \mathbb{F}_p^n$,*

$$f(x) = \sum_{r \in \mathbb{F}_p^n} \widehat{f}(r)\omega^{r \cdot x}$$

The next result tells us that the Fourier transform preserves inner products.

Theorem 3.4. ***(Parseval's identity)*** *Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, we have*

$$\mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\overline{g(x)} = \sum_{r \in \mathbb{F}_p^n} \widehat{f}(r)\overline{\widehat{g}(r)}$$

In particular, as a special case ($f = g$),

$$\mathbb{E}_{x \in \mathbb{F}_p^n} |f(x)|^2 = \sum_{r \in \mathbb{F}_p^n} |\widehat{f}(r)|^2$$

Definition 3.5. **(Character of the group $\mathbb{F}_p^n$)** $\gamma_r : \mathbb{F}_p^n \to \mathbb{C}$ for the function defined by

$$\gamma_r(x) := \omega^{r \cdot x}$$

Definition 3.6. **(Convolution)** Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, define $f * g : \mathbb{F}_p^n \to \mathbb{C}$ by

$$(f * g)(x) := \mathbb{E}_{y \in \mathbb{F}_p^n} f(y)g(x - y).$$

Theorem 3.7. ***(Convolution identity)*** *For any $f, g : \mathbb{R}_p^n \to \mathbb{C}$ and any $r \in \mathbb{F}_p^n$,*

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

3.1.2 Proof of Roth's Theorem in the Finite Field Model

In $\mathbb{F}_3^n$, there are several equivalent interpretations of $x, y, z \in \mathbb{F}_3^n$ forming a 3-AP (allowing the possibility for a trivial 3-AP with $x = y = z$):

- $(x, y, z) = (x, x + d, x + 2d)$ for some d;
- $x - 2y + z = 0$;
- $x + y + z = 0$;
- x, y, z are three distinct points of a line in $\mathbb{F}_3^n$ or are all equal;

The strategy for Roth's theorem is the **density increment argument**. Given $A \subset \mathbb{F}_3^n$, we use the following strategy:

1. If A is pseudo-random or Fourier uniform, which means that all its Fourier coefficients are small, then there is a counting lemma which shows that A has lots of 3-AP.
2. If A is not pseudo-random, then A has a large Fourier coefficient. Then we can find hyperplane where density of A will increase. Now we consider A restricted to this hyperplane, and repeat the previous steps.
3. Each time we repeat, we obtain a density increment, which helps us to obtain an upper bound on A.

Definition 3.8. (**3-AP density**)(counting total numbers of 3-AP) Given $f, g, h : \mathbb{F}_p^n \to \mathbb{C}$, we write

$$\Lambda(f, g, h) := \mathbb{E}_{x,y} f(x)g(x + y)h(x + 2y)$$

and

$$\Lambda_3(f) := \Lambda(f, f, f)$$

Definition 3.9. (**Indicator function**) The indicator function of a subset A of a set X is a function

$$\mathbf{1}_A : X \to \{0, 1\}$$

defined as

$$\mathbf{1}_A(x) := \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Remark 3.10. (**3 AP Density of A**)

$$\begin{aligned}\wedge(1_A) &= \wedge(1_A, 1_A, 1_A)\\ &= \mathbb{E}_{x,y} 1_A(x)1_A(x+y)1_A(x+2y)\\ &= \frac{1}{p^{2n}}\sum 1_A(x)1_A(x+y)1_A(x+2y)\\ &= P^{-2n}\left|\{(x,y) : x, x+y, x+2y \in A\}\right|\end{aligned}$$

Note: Here we includes trivial 3-AP

The following identity, relating the Fourier transform and 3-APs, plays a central role in the Fourier analytic proof of Roth's theorem.

Proposition 3.11. (**Fourier and 3-AP**) Let p be an odd prime. If $f, g, h : \mathbb{F}_p^n \to \mathbb{C}$, then

$$\Lambda(f,g,h) = \sum_r \widehat{f}(r)\widehat{g}(-2r)\widehat{h}(r).$$

Proof. We expand the left-hand side using the formula for Fourier inversion.

$$\begin{aligned}\mathbb{E}_{x,y}\quad & f(x)g(x+y)h(x+2y)\\ &= \mathbb{E}_{x,y}\left(\sum_{r_1}\widehat{f}\left(r_1\right)\omega^{r_1\cdot x}\right)\left(\sum_{r_2}\widehat{g}\left(r_2\right)\omega^{r_2\cdot(x+y)}\right)\left(\sum_{r_3}\widehat{h}\left(r_3\right)\omega^{r_3\cdot(x+2y)}\right)\\ &= \sum_{r_1,r_2,r_3}\widehat{f}\left(r_1\right)\widehat{g}\left(r_2\right)\widehat{h}\left(r_3\right)\mathbb{E}_x\omega^{x\cdot(r_1+r_2+r_3)}\mathbb{E}_y\omega^{y\cdot(r_2+2r_3)}\\ &= \sum_{r_1,r_2,r_3}\widehat{f}\left(r_1\right)\widehat{g}\left(r_2\right)\widehat{h}\left(r_3\right)1_{r_1+r_2+r_3=0}1_{r_2+2r_3=0}\\ &= \sum_r \widehat{f}(r)\widehat{g}(-2r)\widehat{h}(r).\end{aligned}$$

In the last step, we use that $r_1+r_2+r_3=0$ and $r_2+2r_3=0$ together imply $r_1=r_3=r, r_2=-2r_3=-2r$.

□

Lemma 3.12. (**3-AP counting lemma**) Let $f : \mathbb{F}_3^n \to [0,1]$. Then

$$\left|\Lambda_3(f) - (\mathbb{E}f)^3\right| \le \max_{r\neq 0}|\widehat{f}(r)|\|f\|_2^2.$$

Proof. Using Fourier 3-AP Proposition 3.11

$$\Lambda_3(f) = \sum_r \widehat{f}(r)^3 = \widehat{f}(0)^3 + \sum_{r\neq 0}\widehat{f}(r)^3$$

Since $\mathbb{E}f = \widehat{f}(0)$, we have

$$\left|\Lambda_3(f) - (\mathbb{E}f)^3\right| \leq \sum_{r\neq 0} |\widehat{f}(r)|^3 \leq \max_{r\neq 0} |\widehat{f}(r)| \cdot \sum_r |\widehat{f}(r)|^2 = \max_{r\neq 0} |\widehat{f}(r)| \|f\|_2^2.$$

last step is by Plancherel theorem 3.4. □

Step 1. ***A 3-AP-free set has a large Fourier coefficient***

Lemma 3.13. (**3-AP-free implies large Fourier coefficient**) Let $A \subset \mathbb{F}^n$ and $\alpha = |A|/3^n$. If A is 3 -AP-free and $3^n \geq 2\alpha^{-2}$, then there is $r \neq 0$ such that $\left|\widehat{1_A}(r)\right| \geq \alpha^2/2$.

Proof. Using the fact

$$\Lambda_3(1_A) = 3^{-2n}\left|\{(x,y,z) \in A^3 : x+y+z = 0\}\right|$$

Also,

$\mathbb{E}1_A = |A|/3^n = \alpha$ and $\|1_A\|_2^2 = \mathbb{E}1_{A^2} = \alpha$ by Plancherel theorem 3.4

Since A is 3-AP-free, $\Lambda_3(A) = |A|/3^{2n} = \alpha/3^n$, as all 3-APs are trivial. By the 3-AP counting lemma 3.12,

$$\alpha^3 - \frac{\alpha}{3^n} = \alpha^3 - \Lambda_3(1_A) \leq \max_{r\neq 0}\left|\widehat{1}_A(r)\right| \|1_A\|_2^2 = \max_{r\neq 0}\left|\widehat{1}_A(r)\right| \alpha.$$

By the hypothesis $3^n \geq 2\alpha^{-2}$, the left-hand side above is $\geq \alpha^3/2$. So there is some $r \neq 0$ with $\left|\widehat{1_A}(r)\right| \geq \alpha^2/2$. □

Step 2. ***A large Fourier coefficient implies density increment on some hyperplane***

Lemma 3.14. (**Large Fourier coefficient implies density increment**) Let $A \subset \mathbb{F}_3^n$ with $\alpha = |A|/3^n$. Suppose $\left|\widehat{1_A}(r)\right| \geq \delta > 0$ for some $r \neq 0$. Then A has density at least $\alpha + \delta/2$ when restricted to some hyperplane.

Proof. We have

$$\widehat{1_A}(r) = \mathbb{E}_x 1_A(x)\omega^{-r\cdot x} = \frac{\alpha_0 + \alpha_1\omega + \alpha_2\omega^2}{3}$$

where $\alpha_0, \alpha_1, \alpha_2$ are densities of A on the cosets of $r^\perp$.

Claim: To show that one of $\alpha_0, \alpha_1, \alpha_2$ is significantly larger than α.

We have

$$\alpha = (\alpha_0 + \alpha_1 + \alpha_2)/3 \tag{3.1}$$

By the triangle inequality,

$$\begin{aligned} 3\delta &\leq \left|\alpha_0 + \alpha_1\omega + \alpha_2\omega^2\right| \\ &= \left|(\alpha_0 - \alpha) + (\alpha_1 - \alpha)\,\omega + (\alpha_2 - \alpha)\,\omega^2\right| \\ &\leq |\alpha_0 - \alpha| + |\alpha_1 - \alpha| + |\alpha_2 - \alpha| \\ &= \sum_{j=0}^{2} (|\alpha_j - \alpha| + (\alpha_j - \alpha)) \quad \text{[by equation 3.1]}. \end{aligned}$$

By pigeonhole principle, there exists j such that $|\alpha_j - \alpha| + (\alpha_j - \alpha) \geq \delta$.

Note

$$|t| + t = \begin{cases} 2t & t > 0 \\ 0 & t \leq 0 \end{cases}$$

So we get $\alpha_j - \alpha \geq \delta/2$. □

Combining the previous two lemmas, here is what we have proved as above.

Lemma 3.15. (**3-AP-free implies density increment**) Let $A \subset \mathbb{F}_3^n$ and $\alpha = |A|/3^n$. If A is 3 -AP-free and $3^n \geq 2\alpha^{-2}$, then A has density at least $\alpha + \alpha^2/4$ when restricted to some hyperplane.

Step 3. ***Iterate the density increment***

- We start with a 3-AP-free $A \subset \mathbb{F}_3^n$.
- Let $V_0 := \mathbb{F}_3^n$ with density $\alpha_0 := \alpha = |A|/3^n$.
- Repeatedly apply density increment lemma 3.15.
- After i rounds,
  - We restrict A to a co-dimension i affine subspace V_i (with $V_0 \supset V_1 \supset \cdots$).
  - Let $\alpha_i = |A \cap V_i| \,/\, |V_i|$ be the density of A in V_i.

- As long as $2\alpha_i^{-2} \leq |V_i| = 3^{n-i}$, we can apply density increment lemma 3.15 to obtain a V_{i+1} with density increment

$$\alpha_{i+1} \geq \alpha_i + \alpha_i^2/4$$

Claim:

$$\alpha_i \geq \alpha + \frac{i\alpha^2}{4} \tag{3.2}$$

Above claim can be proved using simple observation.

- Since $\alpha = \alpha_0 \leq \alpha_1 \leq \cdots \leq 1$, the process terminates after $m \leq 4/\alpha^2$ rounds.
  - By equation 3.2, $\alpha_i \geqslant \alpha + \left(\frac{4}{\alpha^2}\right)\frac{\alpha^2}{4} = \alpha + 1 \quad (\text{at } i = m)$
- Then, we must have $3^{n-m} < 2\alpha_m^{-2} \leq 2\alpha^{-2}$ (else continue to apply lemma 3.15).
- So $n < m + \log_3\left(2\alpha^{-2}\right) = O\left(1/\alpha^2\right)$, i.e., $\alpha \leq 1/\sqrt{n}$.
- Now, let us **re-do the density increment analysis** more carefully to analyze how quickly α_i grows.
  - Each round, α_i increases by at least $\alpha^2/4$.
  - So it takes $\leq \lceil 4/\alpha \rceil$ initial rounds for α_i to double (by equation 3.2).
  - Once $\alpha_i \geq 2\alpha$, it then increases by at least $\alpha_i^2/4$ each round afterwards (by equation 3.2).
  - so it takes $\leq \lceil 1/\alpha_i \rceil \leq \lceil 1/\alpha \rceil$ additional round for the density to double again.
  - And so on: the k-th doubling time is at most $\left\lceil 4^{2-k}/\alpha \right\rceil$.
  - Since the density is always at most 1.
  - The density can double at most $\log_2(1/\alpha)$ times.
  - So the total number of rounds is at most

$$\sum_{j \leq \log_2(1/\alpha)} \left\lceil \frac{4^{2-j}}{\alpha} \right\rceil = O\left(\frac{1}{\alpha}\right)$$

- Suppose the process terminates after m steps with density α_m.

- Then, we check the hypothesis of Density increment lemma, $3^{n-m} < 2\alpha_m^{-2} \leq 2\alpha^{-2}$
- So $n \leq m + \log_3(2/\alpha^2) \leq O(1/\alpha)$.
- Thus $\alpha = |A|/N = O(1/n)$.
- Equivalently, $|A| = \alpha N = O\left(\frac{3^n}{n}\right)$.

Hence, this completes the proof of Roth's theorem 3.1 in $\mathbb{F}_3^n$.

3.2 Roth's Theorem in the Integers

In previous section we saw a Fourier analytic proof of Roth's theorem in $\mathbb{F}_3^n$. In this section, we adapt the proof to the integers and obtain the following result. This is Roth's original proof (1953).

Theorem 3.16. ***(Roth's theorem)*** *Every 3-AP-free subset of* $[N] = \{1, \ldots, N\}$ *has size* $O(N/\log\log N)$.

The proof of Roth's theorem in $\mathbb{F}_3^n$ proceeded by density increment when restricting to subspaces. An important difference between $\mathbb{F}_3^n$ and $\mathbb{Z}$ is that $\mathbb{Z}$ has no subspaces . Instead, we will proceed in $\mathbb{Z}$ by restricting to subprogressions.

Analog of Fourier and 3-AP 3.11 and 3-AP counting lemma 3.12

Proposition 3.17. (**Fourier and 3-AP**) Given finitely supported $f, g, h : \mathbb{Z} \to \mathbb{C}$,

$$\Lambda(f, g, h) = \int_0^1 \widehat{f}(\theta)\widehat{g}(-2\theta)\widehat{h}(\theta)d\theta$$

Proposition 3.18. (**3-AP counting lemma**) Let $f, g : \mathbb{Z} \to \mathbb{C}$ be finitely supported functions. Then

$$|\Lambda_3(f) - \Lambda_3(g)| \leq 3\|\widehat{f - g}\|_\infty \max\left\{\|f\|_{\ell^2}^2, \|g\|_{\ell^2}^2\right\}$$

Proof. We have

$$\begin{aligned}\Lambda_3(f) - \Lambda_3(g) &= \Lambda(f,f,f) - \Lambda(g,g,g)\\ &= \mathbb{E}_{x,y} f(x)f(x+y)f(x+2y) - \mathbb{E}_{x,y} g(x)g(x+y)g(x+2y)\\ &= \mathbb{E}_{x,y}[f-g](x)f(x+y)f(x+2y) + \mathbb{E}_{x,y} g(x)[f-g](x+y)f(x+2y) +\\ &\mathbb{E}_{x,y} g(x)g(x+y)[f-g](x+2y) + \mathbb{E}_{x,y} g(x)g(x+y)g(x+2y)\\ &- \mathbb{E}_{x,y} g(x)g(x+y)g(x+2y)\\ &= \Lambda(f-g,f,f) + \Lambda(g,f-g,f) + \Lambda(g,g,f-g).\end{aligned}$$

Let us bound the first term on the right-hand side. We have

$$\begin{aligned}&|\ \Lambda(f-g,f,f)\ |\\ &\quad= \left|\int_0^1 \widehat{(f-g)}(\theta)\widehat{f}(-2\theta)\widehat{f}(\theta)d\theta\right| && \text{[Proposition 3.17]}\\ &\quad\le \|\widehat{f-g}\|_\infty \left|\int_0^1 \widehat{f}(-2\theta)\widehat{f}(\theta)d\theta\right|\\ &\quad\le \|\widehat{f-g}\|_\infty \left(\int_0^1 |\widehat{f}(-2\theta)|^2 d\theta\right)^{1/2}\left(\int_0^1 |\widehat{f}(\theta)|^2 d\theta\right)^{1/2} && \text{[Cauchy Schwarz]}\\ &\quad\le \|\widehat{f-g}\|_\infty \|f\|_{\ell^2}^2 && \text{[Parseval identity 2.6].}\end{aligned}$$

By similar arguments, we have

$$|\Lambda(g,f-g,f)| \le \|\widehat{f-g}\|_\infty \|f\|_{\ell^2}\|g\|_{\ell^2}$$

and

$$|\Lambda(g,g,f-g)| \le \|\widehat{f-g}\|_\infty \|g\|_{\ell^2}^2$$

Combining all three result, we get

$$|\Lambda_3(f) - \Lambda_3(g)| \le 3\|\widehat{f-g}\|_\infty \max\left\{\|f\|_{\ell^2}^2, \|g\|_{\ell^2}^2\right\}$$

□

Step 1. ***A 3-AP-free set has a large Fourier coefficient***

Lemma 3.19. (**3-AP-free implies large Fourier**) Let $A \subset [N]$ be a 3 -AP free set with $|A| = \alpha N$. If $N \geq 5\alpha^{-2}$, then there exists $\theta \in \mathbb{R}/\mathbb{Z}$ satisfying

$$\left| \sum_{x=1}^{N} (1_A - \alpha)(x) e(\theta x) \right| \geq \frac{\alpha^2}{10} N$$

Proof. Since A is 3-AP-free, the quantity $1_A(x)1_A(x+y)1_A(x+2y)$ is nonzero only for trivial APs. Thus

$$\Lambda_3(1_A) = |A| = \alpha N.$$

Also, a 3-AP in $[N]$ can be counted by counting pairs of integers with the same parity to form the first and third element of the 3-AP,

$$\Lambda_3\left(1_{[N]}\right) = \lfloor N/2 \rfloor^2 + \lceil N/2 \rceil^2 \geq N^2/2.$$

Now apply the counting lemma (Proposition 3.18) to $f = 1_A$ and $g = \alpha 1_{[N]}$.

We have $\|1_A\|_{\ell^2}^2 = |A| = \alpha N$ and $\left\|\alpha 1_{[N]}\right\|_{\ell^2}^2 = \alpha^2 N$.

So

$$\frac{\alpha^3 N^2}{2} - \alpha N \leq \alpha^3 \Lambda_3\left(1_{[N]}\right) - \Lambda_3(1_A) \leq 3\alpha N \left\| \left(1_A - \alpha 1_{[N]}\right)^\wedge \right\|_\infty.$$

Thus, using $N \geq 5/\alpha^2$, we have

$$\left\| \left(1_A - \alpha 1_{[N]}\right)^\wedge \right\|_\infty \geq \frac{\frac{1}{2}\alpha^3 N^2 - \alpha N}{3\alpha N} = \frac{1}{6}\alpha^2 N - \frac{1}{3} \geq \frac{1}{10}\alpha^2 N$$

Therefore there exists some $\theta \in \mathbb{R}$ with

$$\left| \sum_{x=1}^{N} (1_A - \alpha)(x) e(\theta x) \right| = \left(1_A - \alpha 1_{[N]}\right)^\wedge (\theta) \geq \frac{1}{10}\alpha^2 N$$

□

In the finite field model, if $\widehat{1_A}(r)$ is large for some $r \in \mathbb{F}_3^n \backslash \{0\}$, then we obtained a density increment by restricting A to some coset of the hyperplane $r^\perp$.

Now we adapt this argument in the integers.

In the finite field model, we used that the Fourier character $\gamma_r(x) = \omega^{r \cdot x}$ is constant

on each coset of the hyperplane $r^\perp \subset \mathbb{F}_3^n$. In the integer setting, we want to partition $[N]$ into subprogressions such that the character $\mathbb{Z} \to \mathbb{C} : x \mapsto e(x\theta)$ is roughly constant on each subprogression.

Remark 3.20. We write

$$\|\theta\|_{\mathbb{R}/Z} := \text{ distance from } \theta \text{ to the nearest integer.}$$

Lemma 3.21. (**Dirichlet's lemma**) Let $\theta \in \mathbb{R}$ and $0 < \delta < 1$. Then there exists a positive integer $d \leq 1/\delta$ such that $\|d\theta\|_{\mathbb{R}/Z} \leq \delta$.

Proof. Let $m = \lfloor 1/\delta \rfloor$.

By the pigeonhole principle, among the $m+1$ numbers $0, \theta, \cdots, m\theta$, we can find $0 \leq i < j \leq m$ such that the fractional parts of $i\theta$ and $j\theta$ differ by at most δ.

Set $d = |i - j|$.

Then $\|d\theta\|_{\mathbb{R}/Z} \leq \delta$. □

Given θ, we now partition $[N]$ into subprogressions with roughly constant $e(x\theta)$ inside each progression.

Lemma 3.22. (**Partition into progression level sets**) Let $0 < \eta < 1$ and $\theta \in \mathbb{R}$. Suppose $N \geq (4\pi/\eta)^6$. Then one can partition $[N]$ into subprogressions P_i, each with length

$$N^{1/3} \leq |P_i| \leq 2N^{1/3}$$

such that

$$\sup_{x,y \in P_i} |e(x\theta) - e(y\theta)| < \eta, \qquad \text{for each } i.$$

Proof. By Dirichlet's lemma 3.21, there is a positive integer $d < \sqrt{N}$ such that $\|d\theta\|_{\mathbb{R}/\mathbb{Z}} \leq 1/\sqrt{N}$.

Partition $[N]$ greedily into progressions with common difference d of lengths between $N^{1/3}$ and $2N^{1/3}$.

Then, for two elements x, y within the same progression P_i, we have

$$|e(x\theta) - e(y\theta)| \leq |P_i|\,|e(d\theta) - 1| \leq 2N^{1/3} \cdot 2\pi \cdot N^{-1/2} \leq \eta$$

Remark: $|e(d\theta) - 1| \leq 2\pi \|d\theta\|_{\mathbb{R}/Z}$ from the fact that the length of a chord on a circle is at most the length of the corresponding arc. □

We can now apply this lemma to obtain a density increment.

Lemma 3.23. (**3-AP-free implies density increment**) Let $A \subset [N]$ be 3-AP-free, with $|A| = \alpha N$ and $N \geq (16/\alpha)^{12}$. Then there exists a subprogression $P \subset [N]$ with $|P| \geq N^{1/3}$ and $|A \cap P| \geq (\alpha + \alpha^2/40)\,|P|$.

Proof. By Lemma 3.19, there exists θ satisfying

$$\left| \sum_{x=1}^{N} (1_A - \alpha)(x) e(x\theta) \right| \geq \frac{\alpha^2}{10} N$$

Next, apply Lemma 3.22 with $\eta = \alpha^2/20$ (the hypothesis $N \geq (4\pi/\eta)^6$ is satisfied since $(16/\alpha)^{12} \geq (80\pi/\alpha^2)^6 = (4\pi/\eta)^6$) to obtain a partition $P_1, \ldots, P_k$ of $[N]$ satisfying $N^{1/3} \leq |P_i| \leq 2N^{1/3}$ and $|e(x\theta) - e(y\theta)| \leq \frac{\alpha^2}{20}$ for all i and $x, y \in P_i$.

So on each P_i,

$$\left| \sum_{x \in P_i} (1_A - \alpha)(x) e(x\theta) \right| \leq \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right| + \frac{\alpha^2}{20} |P_i| .$$

Thus

$$\begin{aligned} \frac{\alpha^2}{10} N &\leq \left| \sum_{x=1}^{N} (1_A - \alpha)(x) e(x\theta) \right| \\ &\leq \sum_{i=1}^{k} \left| \sum_{x \in P_i} (1_A - \alpha)(x) e(x\theta) \right| \\ &\leq \sum_{i=1}^{k} \left(\left| \sum_{x \in P_i} (1_A - \alpha)(x) \right| + \frac{\alpha^2}{20} |P_i| \right) \\ &= \sum_{i=1}^{k} \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right| + \frac{\alpha^2}{20} N \end{aligned}$$

Thus

$$\frac{\alpha^2}{20} N \leq \sum_{i=1}^{k} \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right|$$

and hence

$$\frac{\alpha^2}{20}\sum_{i=1}^{k}|P_i| \leq \sum_{i=1}^{k}||A\cap P_i| - \alpha|P_i||$$

We want to show that there exists some P_i such that A has a density increment when restricted to P_i.

$$\begin{aligned}\frac{\alpha^2}{20}\sum_{i=1}^{k}|P_i| &\leq \sum_{i=1}^{k}||A\cap P_i| - \alpha|P_i|| \\ &= \sum_{i=1}^{k}\left(||A\cap P_i| - \alpha|P_i|| + (|A\cap P_i| - \alpha\,|P_i|)\right)\end{aligned}$$

as the newly added terms in the final step sum to zero. Thus there exists an i such that

$$\frac{\alpha^2}{20}|P_i| \leq ||A\cap P_i| - \alpha|P_i|| + (|A\cap P_i| - \alpha\,|P_i|)$$

Since

$$|t| + t = \begin{cases} 2t & t > 0 \\ 0 & t \leq 0 \end{cases}$$

So we get

$$\frac{\alpha^2}{20}|P_i| \leq 2\,(|A\cap P_i| - \alpha\,|P_i|)$$

Hence

$$|A\cap P_i| \geq \left(\alpha + \frac{\alpha^2}{40}\right)|P_i|$$

□

Step 3. ***Iterate the density increment***

This step is nearly identical to the proof in the finite field model.

- Start with $\alpha_0 = \alpha$ and $N_0 = N$.
- After i iterations, we arrive at a subprogression of length N_i where A has density α_i.
- As long as $N_i \geq (16/\alpha_i)^{12}$, we can apply apply density increment lemma 3.23 to

pass down to a subprogression with

$$N_{i+1} \geq N_i^{1/3} \quad \text{and} \quad \alpha_{i+1} \geq \alpha_i + \alpha_i^2/40.$$

We double α_i from α_0 after $\leq \lceil 40/\alpha \rceil$ iterations. Once the density reaches at least 2α, the next doubling takes $\leq \lceil 20/\alpha \rceil$ iterations, and so on. In general, the k-th doubling requires $\leq \left\lceil 40 \cdot 2^{-k}/\alpha \right\rceil$ iterations. There are at most $\log_2(1/\alpha)$ doublings since the density is always at most 1 . Summing up, the total number of iterations is

$$m \leq \sum_{i=1}^{\log_2(1/\alpha)} \left\lceil 40 \cdot 2^{-k}/\alpha \right\rceil = O(1/\alpha)$$

When the process terminates, we must have $N^{1/2^m} \leq N_m$ by density increment lemma 3.23. So

$$N^{1/2^m} \leq N_m < (16/\alpha_i)^{12} \leq (16/\alpha)^{12}.$$

So

$$N \leq (16/\alpha)^{12 \cdot 2^m} \leq (16/\alpha)^{2^{O(1/\alpha)}}$$

Therefore

$$\frac{|A|}{N} = \alpha = O\left(\frac{1}{\log \log N}\right).$$

Hence, this completes the proof of Roth's theorem 3.16.

3.3 Roth's theorem in $\mathbb{F}_3^n$ using the polynomial method

We'll examine a whole new demonstration of Roth's theorem in $\mathbb{F}_3^n$ using the polynomial technique in this section, which offers substantially stronger quantitative bounds. This polynomial method technique, however, only applies to the finite field situation, and it is uncertain how to apply it to integers.

Croot, Lev, and Pach (2017) made a significant breakthrough by demonstrating how to use the polynomial approach to solve Roth-type issues in the finite field model. Their approach immediately found a wide range of uses. Ellenberg and Gijswijt (2017) adopted Croot, Lev, and Pach's reasoning to show the following bound on the cap set

problem less than a week after it was published. The community was taken aback by the discovery, especially because the proof is so brief.

Theorem 3.24. *(**Cap set upper bound**) Every 3-AP-free subset of* $\mathbb{F}_3^n$ *has size* $O\left(2.76^n\right)$.

Definition 3.25. (**Slice rank 1 function**) A function $F : A \times A \times A \to \mathbb{F}$ is said to have **slice rank 1** if it can be written as

$$u(x)v(y,z), \quad u(y)v(x,z), \quad \text{or} \quad u(z)v(x,y)$$

for some nonzero functions $u : A \to \mathbb{F}$ and $v : A \times A \to \mathbb{F}$.

Definition 3.26. (**Slice rank of a function**)

The **slice rank of a function** $F : A \times A \times A \to \mathbb{F}$ is the minimum r so that F can be written as a sum of r slice rank 1 functions, i.e

$$F(x,y,z) = \sum_{i=1}^{r_1} u_i(x)v_i(y,z) + \sum_{i=r_1+1}^{r_2} u_i(y)v_i(x,z) + \sum_{i=r_2+1}^{r} u_i(z)v_i(x,y).$$

Here is an easy fact about the slice rank.

Lemma 3.27. (**Trivial upper bound for slice rank**)[1] Every function $F : A\times A\times A \to \mathbb{F}$ has slice rank at most $|A|$.

Proof. Let F_a be the restriction of F to the "slice" $\{(x,y,z) \in A \times A \times A : x = a\}$, i.e.,

$$F_a(x,y,z) = \begin{cases} F(x,y,z) & \text{if } x = a, \\ 0 & \text{if } x \neq a \end{cases}$$

Then F_a has slice rank ≤ 1 since $F_a(x,y,z) = \delta_a(x)F(a,y,z)$, where,

$$\delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$$

Thus $F = \sum_{a\in A} F_a$ has slice rank at most $|A|$. □

We will use a formulation that appear on Tao's blog [2]

Let $A \subseteq \mathbb{F}_3^n$ be 3 -AP- free. Then we have idenity

$$\delta_{0^n}(x+y+z) = \sum_{a \in A} \delta_a(x)\delta_a(y)\delta_a(z)$$

Note:

- Above hold $x+y+z=0$ iff $z-y=y-x$ in $\mathbb{F}_3^n \implies x,y,z$ in A.P.
- This possible only when $x=y=z=a$ (trivial A.P) for some a $\in \mathbb{F}_3^n$..

Lemma 3.28. (**Slice rank of a diagonal**) [3, 1] Suppose $F : A \times A \times A \to \mathbb{F}$ satisfies $F(x,y,z) \neq 0$ if and only if $x=y=z$. Then F has slice rank $|A|$.

Proof. We can write,

$$F(x,y,z) = \sum_{a \in A} F(a,a,a)\delta_a(x)\delta_a(y)\delta_a(z)$$

where,

$$\delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$$

for every $(x,y,z) \in A \times A \times A$, which implies that F **has slice rank** $\leq |A|$ (since a product of two one-variable functions is a two-variable function by definition 3.26).

Claim: F has slice rank $\geq |A|$

Now, decomposition by definition 3.26

$$F(x,y,z) = \sum_{i=1}^{r_1} u_i(x)v_i(y,z) + \sum_{i=r_1+1}^{r_2} u_i(y)v_i(x,z) + \sum_{i=r_2+1}^{r} u_i(z)v_i(x,y).$$

WLOG, $r_1 > 0$ [For non-empty first term]

Sub-claim: There is a function $h : A \to \mathbb{F}$ such that $\sum_{x \in A} h(x)u_i(x) = 0$ for $i = 1,2,\ldots,r_1$ and such that h is non-zero outside a set of size r_1.

Proof of sub-claim

- Form an $r_1 \times |A|$ matrix M with the functions u_i as its rows ($M(i,x) = u_i(x)$).

- Then we are trying to find a solution to the equation $Mh = 0$ such that h does not have many zeros.
- We can put M into reduced row-echelon form.
- Then it has $s \leq r_1$ non-zero rows, which implies non zero identity matrix.
- Let $S \subset A$ be the subset corresponding to the set of columns. Then we may choose arbitrary values $h(x)$ for every $x \notin S$.
- Then the values of h inside S are uniquely determined by the equations.

Now consider the function $G : A \times A \to \mathbb{F}$ given by the formula

$$G(y, z) = \sum_x h(x)F(x, y, z).$$

Then $G(y, z) = 0$ if $y \neq z$ or if $y = z \notin A$. If $y = z \in A$, then it takes the value $h(a)F(a, a, a)$. Since h is non-zero outside a set of size at most r_1, $h(a)F(a, a, a)$ is non-zero on a set of size at least $|A| - r_1$. From this it follows that G **has rank at least** $|A| - r_1$.

However, we also know that $G(y, z)$ is given by the formula

$$\sum_{i=r_1+1}^{r_2} u_i(y) \sum_x h(x)v_i(x, z) + \sum_{i=r_2+1}^{r} u_i(z) \sum_{x \in X} h(x)v_i(x, y)$$

which is a sum of $r - r_1$ products of two one-variable functions.

This proves that G **has rank at most** $r - r_1$**.**

It follows that

$$|A| - r_1 \leq \text{ rank } G \leq r - r_1$$

Hence, $|A| \leq r$, so the F has slice rank $\geq |A|$.

□

The connection between slice rank and the cap-set problem comes with the following key observation. Suppose that A is a subset of $\mathbb{F}_3^n$ that does not contain distinct elements x, y, z with $x + y + z = 0$. Then if x, y, z belong to A and are not all the same,

we must have that $x+y+z \neq 0$ and hence that there exists i such that $x_i+y_i+z_i \neq 0$. And this last assertion can be written in a polynomial form as

$$1-(x_i+y_i+z_i)^2=0.$$

Now let $F: A^3 \to \mathbb{F}_3$ be defined by setting $F(x,y,z)=1$ if $x=y=z \in A$ and 0 otherwise. Then

$$F(x,y,z)=\prod_{i=1}^{n}\left(1-(x_i+y_i+z_i)^2\right) \tag{3.3}$$

for every $(x,y,z) \in |A|^3$. By the above lemma 3.28, the slice rank of f is $|A|$, so any upper bound we can obtain for the slice rank will translate directly into an upper bound for the size of A.

Lemma 3.29. (**Upper bound on the slice rank of** $1_{x+y+z=0}$) Define $F: A\times A\times A \to \mathbb{F}_3$ by

$$F(x,y,z)=\begin{cases}1 & \text{if } x+y+z=0\\ 0 & \text{otherwise}\end{cases}$$

Then the slice rank of F is at most

$$3\sum_{\substack{a,b,c\geq 0\\ a+b+c=n\\ b+2c\leq 2n/3}}\frac{n!}{a!b!c!}$$

Proof. In $\mathbb{F}_3$, one has

$$1-x^2=\begin{cases}1 & \text{if } x=0\\ 0 & \text{if } x\neq 0\end{cases}$$

So, writing $x=(x_1,\ldots,x_n), y=(y_1,\ldots,y_n)$, and $z=(z_1,\ldots,z_n)$, we have by equation 3.3

$$F(x,y,z)=\prod_{i=1}^{n}\left(1-(x_i+y_i+z_i)^2\right)$$

If we expand the right-hand side, we obtain a polynomial in $3n$ variables with degree $2n$. This is a sum of monomials, each of the form

$$x_1^{i_1}\cdots x_n^{i_n}y_1^{j_1}\cdots y_n^{j_n}z_1^{k_1}\cdots z_n^{k_n},$$

where $i_1, i_2, \ldots, i_n, j_1, \ldots, j_n, k_1, \ldots, k_n \in \{0, 1, 2\}$.

For each term, by the pigeonhole principle, at least one of $i_1 + \cdots + i_n, j_1 + \cdots + j_n, k_1 + \cdots + k_n$ is at most $2n/3$. So we can split these summands into three sets:

$$\begin{aligned}\prod_{i=1}^{n}\left(1-(x_i+y_i+z_i)^2\right) = &\sum_{i_1+\cdots+i_n\leq\frac{2n}{3}} x_1^{i_1}\cdots x_n^{i_n} f_{i_1,\ldots,i_n}(y,z)\\ &+\sum_{j_1+\cdots+j_n\leq\frac{2n}{3}} y_1^{j_1}\cdots y_n^{j_n} g_{j_1,\ldots,j_n}(x,z)\\ &+\sum_{k_1+\cdots+k_n\leq\frac{2n}{3}} z_1^{k_1}\cdots z_n^{k_n} h_{k_1,\ldots,k_n}(x,y)\end{aligned}$$

Each summand has slice rank at most 1. The number of summands in the first sum is precisely the number of triples of nonnegative integers a, b, c with $a + b + c = n$ and $b + 2c \leq 2n/3$ (a, b, c correspond to the numbers of i_* 's that are equal to $0, 1, 2$ respectively).

Hence, the slice rank of F is at most

$$3\sum_{\substack{a,b,c\geq 0\\ a+b+c=n\\ b+2c\leq 2n/3}}\frac{n!}{a!b!c!}$$

□

Lemma 3.30. (**A trinomial coefficient estimate**) For every positive integer n,

$$\sum_{\substack{a,b,c\geq 0\\ a+b+c=n\\ b+2c\leq 2n/3}}\frac{n!}{a!b!c!}\leq 2.76^n$$

Proof. Let $x \in [0, 1]$.

$$\begin{aligned}\frac{(1+x+x^2)^n}{x^{\frac{2n}{3}}} &= \sum_{i=0}^{2n}\left(\sum_{\substack{a+b+c=n\\ b+2c=i}}\frac{n!}{a!b!c!}\right)x^{i-\frac{2n}{3}}\\ &\geq \sum_{i=0}^{2n/3}\sum_{\substack{a+b+c=n\\ b+2c=i}}\frac{n!}{a!b!c!}\end{aligned} \tag{3.4}$$

The sum equals to the coefficients of all the monomials x^i with $i \leq 2n/3$ in the expansion of $(1+x+x^2)^n$. By deleting contributions x^i with $i > 2n/3$ and using $1 \leq x^{i-2n/3}$ whenever $i \leq 2n/3$, we have

$$\sum_{\substack{a,b,c\geq 0\\ a+b+c=n\\ b+2c\leq 2n/3}}\frac{n!}{a!b!c!} \leq \frac{(1+x+x^2)^n}{x^{2n/3}}$$

Setting $x = 0.6$ shows that the left-hand side sum is $\leq (2.76)^n$.

To verify above we can see following calculations,

$$f(x) = \left(x^{-2/3}+x^{1/3}+x^{4/3}\right)^n \text{ for } x \in [0,1]$$

.

then $f'(x) = 0$

$$\begin{aligned}f'(x) &= -\frac{2}{3}x^{-5/3}+\frac{1}{3}x^{-2/3}+\frac{4}{3}x^{1/3} = 0\\ &= \frac{x^{-5/3}}{3}\left(-2+x+4x^2\right) = 0\end{aligned}$$

it follows, $x = \frac{-1\pm\sqrt{33}}{8}$ and $x > 0$

So $x = \frac{\sqrt{33}-1}{8} = 0.59307$

Hence, we obtain $\leq (2.7550\ldots)^n$ □

It is straightforward to extend the above proof from $\mathbb{F}_3$ to any other fixed $\mathbb{F}_p$, resulting:

Theorem 3.31. ***(Roth's theorem in the finite field model)*** *For every odd prime p, there is some $c_p < p$ so that every 3-AP-free subset of $\mathbb{F}_p^n$ has size at most $3c_p^n$.*

BIBLIOGRAPHY

[1] Yufei Zhao. *Graph Theory and Additive Combinatorics*. Lecture notes available at yufeizhao.com/gtacbook, 2021.

[2] Terence Tao. *A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound*. Available at terrytao.wordpress.com, 2016.

[3] Timothy Gowers. *Topics in combinatorics*. Lecture notes available online, 2020.

[4] E.M. Stein and R. Shakarchi. *Fourier Analysis: An Introduction*. Princeton University Press, 2003.

[5] Michael W Frazier. *An introduction to wavelets through linear algebra*. Springer Science & Business Media, 2006.

[6] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. *Numerical Recipes 3rd Edition: The Art of Scientific Computing*. Cambridge University Press, USA, 3 edition, 2007.