

Magic of Frequencies

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

September, 2025

VII

1 Introduction

The laws governing some physical phenomena were expressed by two different partial differential equations, namely the wave equation and the heat equation. To solve these problems Fourier series was developed. Fourier analysis later became an active field of study, as it is applicable for various domains, and we will discuss one such application in Cryptography.

We will keep in mind that the functions we will be dealing with will have nice properties such as convergence, differentiability, etc., for our applications. Throughout the discussion we would often call these functions **NICE FUNCTIONS**. We would start by defining the Fourier Transform in one dimension and generalize it for the n -dimensional case.

2 Fourier Transform

Fourier Transform is an integral transform between two spaces. The input space is often called the time domain, and the output space is often called the frequency domain. So any given function is treated as a function of time(t) and the consequent function after applying the Fourier transform is treated as a function of frequency(ω). We will define the $L^1(\mathbb{R})$ space and then take the function from that space and define the Fourier transform. We will use the variable x instead of t as a matter of convention.

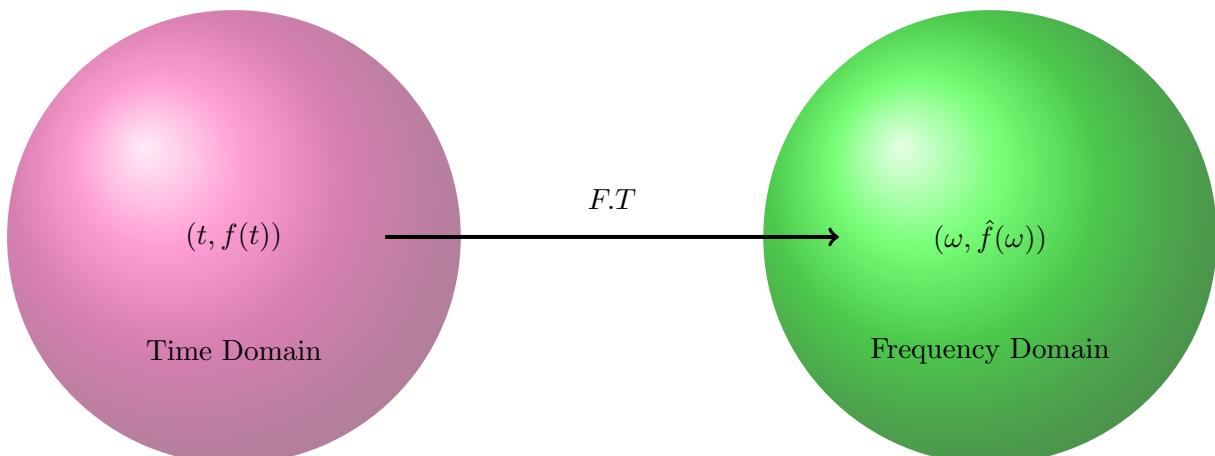


Figure 1: Fourier Transform

3 Fourier in One Dimension

Definition 3.1. ($L^1(\mathbb{R})$ Function) The function class $L^1(\mathbb{R})$ is the set of all functions $f : \mathbb{R} \rightarrow \mathbb{C}$ for which

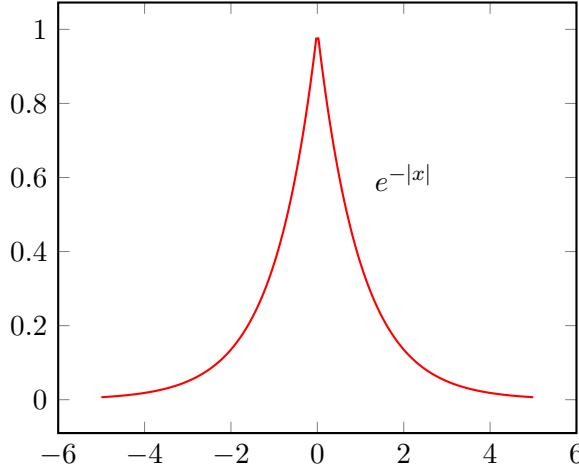
$$\int_{\mathbb{R}} |f(x)| dx < \infty$$

$$L^1(\mathbb{R}) = \left\{ f : \mathbb{R} \rightarrow \mathbb{C} \mid \int_{\mathbb{R}} |f(x)| dx < \infty \right\}$$

Example 3.2. $f(x) = e^{-|x|} \in L^1(\mathbb{R})$

Even function like $|e^{-|x|}|$ satisfies the property $\int_{-a}^a f(x) dx = 2 \int_0^a f(x) dx$ which we will use here.

$$I = \int_{\mathbb{R}} |f(x)| dx = \int_{\mathbb{R}} |e^{-|x|}| dx = 2 \int_0^{\infty} e^{-x} dx = 2 \times [-e^{-x}]_0^{\infty} = 2 \times (0 + 1) = 2 < \infty$$



Definition 3.3. (Fourier Transform) Given $f \in L^1(\mathbb{R})$, its Fourier Transform $\hat{f} : \mathbb{R} \rightarrow \mathbb{C}$ is defined as

$$\hat{f}(\omega) := \int_{\mathbb{R}} f(x) e^{-2\pi i \omega x} dx$$

Note: $\hat{f}(\omega)$ of any function in $L^1(\mathbb{R})$ is bounded for all $\omega \in \mathbb{R}$

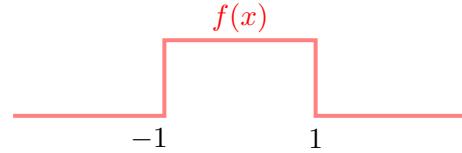
$$|\hat{f}(\omega)| = \left| \int_{\mathbb{R}} f(x) e^{-2\pi i \omega x} dx \right| \leq \int_{\mathbb{R}} |f(x)| |e^{-2\pi i \omega x}| dx \leq \int_{\mathbb{R}} |f(x)| \cdot 1 \cdot dx \leq \int_{\mathbb{R}} |f(x)| dx < \infty$$

We also have to prove $|e^{-2\pi i \omega x}| = 1$

$$|e^{-2\pi i \omega x}| = \left| e^{i(-2\pi \omega x)} \right| = |\cos(-2\pi \omega x) + i \sin(-2\pi \omega x)| = \cos^2(-2\pi \omega x) + \sin^2(-2\pi \omega x) = 1$$

□

Example 3.4. Define $f(x) = \begin{cases} 1; & -1 \leq x \leq 1 \\ 0; & \text{otherwise} \end{cases}$



Clearly, $f(x) \in L^1(\mathbb{R})$ and its Fourier transform would be

$$\begin{aligned}\hat{f}(\omega) &= \int_{-\infty}^{\infty} f(x) e^{-2\pi i \omega x} dx = \int_{-1}^{1} e^{-2\pi i \omega x} dx = \frac{e^{-2\pi i \omega} - e^{2\pi i \omega}}{-2\pi i \omega} \\ &= \frac{\cos(2\pi\omega) - i \sin(2\pi\omega) - \cos(-2\pi\omega) - i \sin(-2\pi\omega)}{-2\pi i \omega} = \frac{-2i \sin(2\pi\omega)}{-2\pi i \omega} = \frac{\sin(2\pi\omega)}{\pi\omega}\end{aligned}$$

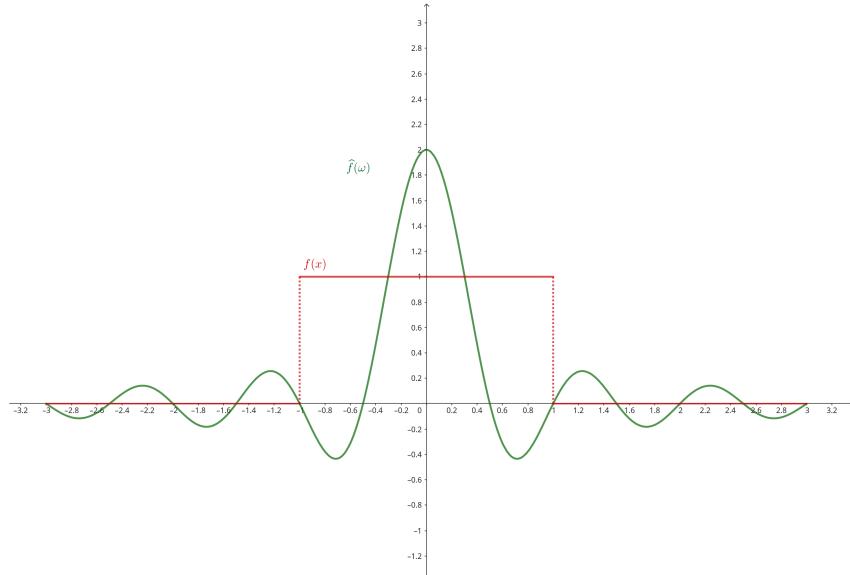
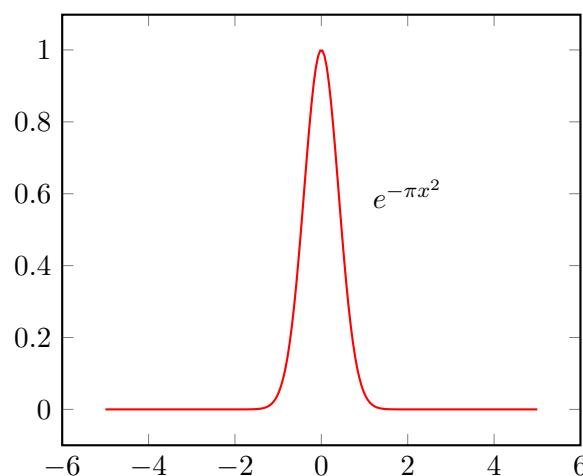


Figure 2: $f(x)$ and its Fourier Transform $\hat{f}(\omega)$

The figure above shows the function $f(x)$ and its Fourier transform $\hat{f}(\omega)$

Example 3.5. *The Gaussian function*

$$f(x) = e^{-\pi x^2}$$



Clearly, $f(x) \in L^1(\mathbb{R})$ as $\int_{\mathbb{R}} |e^{-\pi x^2}| dx = 1$

$$\begin{aligned}
\hat{f}(\omega) &= \int_{\mathbb{R}} e^{-\pi x^2} e^{-2\pi i \omega x} dx = \int_{\mathbb{R}} e^{-\pi x^2 - 2\pi i \omega x} dx \\
&= \int_{\mathbb{R}} e^{-\pi(x^2 + 2i\omega x)} dx \\
&= \int_{\mathbb{R}} e^{-\pi(x^2 + 2i\omega x + i^2\omega^2 - i^2\omega^2)} dx \\
&= \int_{\mathbb{R}} e^{-\pi((x+i\omega)^2 + \omega^2)} dx \\
&= e^{-\pi\omega^2} \int_{\mathbb{R}} e^{-\pi(x+i\omega)^2} dx \\
&= e^{-\pi\omega^2} \times 1 = e^{-\pi\omega^2} = f(\omega)
\end{aligned}$$

Result 3.6.

$$I(\omega) = \int_{-\infty}^{\infty} e^{-\pi(x+i\omega)^2} dx = 1, \quad \omega \in \mathbb{R}$$

Proof needs a little understanding of Complex Analysis, we include this as a result, however for detailing, one can always read the proof part. An attempt to make it simple has been made. one can skip the part of proving this result.

Proof. Define $g(z) = e^{-\pi z^2}$, $z \in \mathbb{C}$, then g is entire.

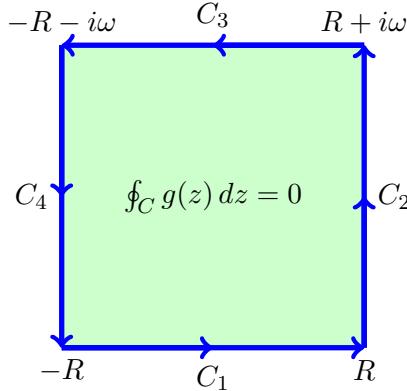
Along the horizontal line $\text{Im}(z) = \omega$ we have

$$g(x + i\omega) = e^{-\pi(x+i\omega)^2}$$

So $I(\omega)$ is the integral of g along that horizontal line.

Fix $R > 0$ and consider the rectangle Γ_R with vertices oriented counterclockwise.

$$-R \xrightarrow{C_1} R \xrightarrow{C_2} R + i\omega \xrightarrow{C_3} -R + i\omega \xrightarrow{C_4} -R$$



By Cauchy's theorem,

$$\oint_C g(z) dz = \int_{C_1} g + \int_{C_2} g + \int_{C_3} g + \int_{C_4} g = 0$$

where C_1, \dots, C_4 denote the four sides.

On the bottom edge C_1 : $z = x$, $x \in [-R, R]$,

$$\int_{C_1} g(z) dz = \int_{-R}^R e^{-\pi x^2} dx$$

On the top edge C_3 : $z = x + i\omega$, x runs from R to $-R$,

$$\int_{C_3} g(z) dz = \int_R^{-R} e^{-\pi(x+i\omega)^2} dx = - \int_{-R}^R e^{-\pi(x+i\omega)^2} dx$$

Thus

$$\int_{-R}^R e^{-\pi(x+i\omega)^2} dx = \int_{-R}^R e^{-\pi x^2} dx + \int_{C_2} g + \int_{C_4} g$$

Vertical sides vanish as there is no change in x

$$\int_{-R}^R e^{-\pi(x+i\omega)^2} dx = \int_{-R}^R e^{-\pi x^2} dx + 0 + 0 = \int_{-R}^R e^{-\pi x^2} dx$$

$$\int_{-R}^R e^{-\pi(x+i\omega)^2} dx = \int_{-R}^R e^{-\pi x^2} dx = 1 \quad [\text{As } R \rightarrow \infty]$$

It is well known that

$$\int_{-\infty}^{\infty} e^{-\pi x^2} dx = 1$$

Finally, for all real ω ,

$$\int_{-\infty}^{\infty} e^{-\pi(x+i\omega)^2} dx = 1.$$

□

3.1 Properties of Fourier Transform

1. Linearity

For all $f, g \in L^1(\mathbb{R})$ and $a \in \mathbb{R}$

a. $\hat{f} + \hat{g} = \hat{f} + \hat{g}$

Proof.

$$\begin{aligned} \hat{f} + \hat{g}(x) &= \int_{\mathbb{R}} (\hat{f} + \hat{g})(x) e^{-2\pi i \omega x} dx \\ &= \int_{\mathbb{R}} \hat{f}(x) e^{-2\pi i \omega x} dx + \int_{\mathbb{R}} \hat{g}(x) e^{-2\pi i \omega x} dx \\ &= \hat{f}(\omega) + \hat{g}(\omega) \end{aligned}$$

□

b. $\hat{af} = a\hat{f}$

Proof.

$$\begin{aligned} \hat{af}(x) &= \int_{\mathbb{R}} (af)(x) e^{-2\pi i \omega x} dx \\ &= a \int_{\mathbb{R}} f(x) e^{-2\pi i \omega x} dx \\ &= a\hat{f}(\omega) \end{aligned}$$

□

2. Time Shift

Let $f \in L^1(\mathbb{R})$ and $h(x) = f(x - c)$ for some $c \in \mathbb{R}$, then

$$\hat{h}(\omega) = e^{-2\pi i \omega c} \hat{f}(\omega)$$

Proof.

$$\begin{aligned}\hat{h}(\omega) &= \int_{\mathbb{R}} f(x - c) e^{-2\pi i \omega x} dx \\ &= \int_{\mathbb{R}} f(u) e^{-2\pi i \omega (u+c)} du \\ &= \int_{\mathbb{R}} f(u) e^{-2\pi i \omega u} e^{-2\pi i \omega c} du \\ &= e^{-2\pi i \omega c} \int_{\mathbb{R}} f(u) e^{-2\pi i \omega u} du \\ &= e^{-2\pi i \omega c} \hat{f}(\omega)\end{aligned}$$

□

3. Time Scale

Let $f \in L^1(\mathbb{R})$ and $h(x) = f(cx)$ for some $c \in \mathbb{R}^*$, then

$$\hat{h}(\omega) = \frac{1}{c} \hat{f}\left(\frac{\omega}{c}\right)$$

Proof.

$$\begin{aligned}\hat{h}(\omega) &= \int_{\mathbb{R}} f(cx) e^{-2\pi i \omega x} dx \\ &= \int_{\mathbb{R}} f(u) e^{-2\pi i \omega (u/c)} \frac{1}{c} du \\ &= \frac{1}{c} \int_{\mathbb{R}} f(u) e^{-2\pi i (\omega/c) u} du \\ &= \frac{1}{c} \hat{f}\left(\frac{\omega}{c}\right)\end{aligned}$$

□

4. Transform Inversion

For any $f \in L^1(\mathbb{R})$

$$f(x) = \int_{\mathbb{R}} \hat{f}(\omega) e^{2\pi i x \omega} d\omega$$

Given a Fourier transform, we can always recover the original function.

Note: For the Dirac delta function defined as $\delta(x) = \begin{cases} 0 & x \neq 0 \\ \infty & x = 0 \end{cases}$

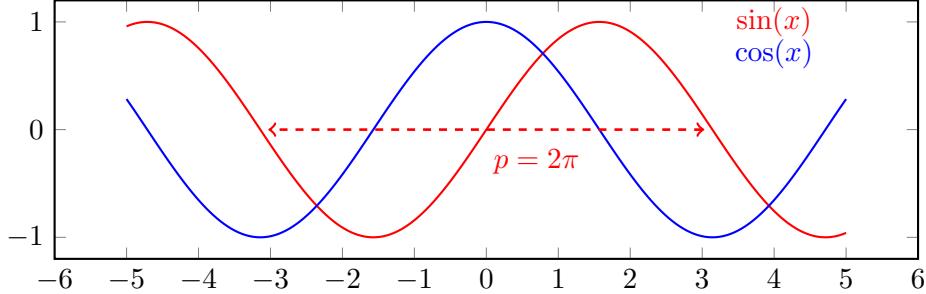
$$\hat{\delta}(x) = \int_{\mathbb{R}} \delta(x) e^{-2\pi i \omega x} dx = 1$$

3.2 Fourier Series for Periodic Function

Definition 3.7. (Periodic Function)

A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is periodic with period $p \in \mathbb{R} - \{0\}$ if $f(x + p) = f(x)$ for all values of x .

For example, $\sin(x), \cos(x)$ are functions with period 2π .



Definition 3.8. Let $g : \mathbb{R} \rightarrow \mathbb{C}$, not necessarily in $L^1(\mathbb{R})$ with unit period (we call it \mathbb{Z} periodic), i.e.

$$g(x) = g(x + z) \quad \forall z \in \mathbb{Z}$$

These are basically function whose period is 1, i.e given an interval $[\lambda, \lambda + 1]$ for $\lambda \in \mathbb{R}$ if $f(x)$ is known for all $x \in [\lambda, \lambda + 1]$ then the function's complete behavior is known in \mathbb{R} .

Definition 3.9. (Periodization)

Let $S \subset \mathbb{R}$ be a countable set then for a function f defined on \mathbb{R} we define

$$f(S) := \sum_{s \in S} f(s)$$

Now define $g : \mathbb{R} \rightarrow \mathbb{C}$ as

$$g(x) = \sum_{z \in \mathbb{Z}} f(x + z)$$

or,

$$g(x) = f(x + \mathbb{Z}) = \sum_{z \in \mathbb{Z}} f(x + z)$$

Such a construction of $g(x)$ is \mathbb{Z} -periodic.

$$g(x) = g(x \pm 1) = g(x \pm 2) = \dots$$

Definition 3.10. (Fourier Series) For a \mathbb{Z} -periodic function $g : \mathbb{R} \rightarrow \mathbb{C}$ its Fourier series is defined as

$$g(x) = \sum_{k=-\infty}^{\infty} \hat{g}(k) e^{2\pi i k x}$$

where $\hat{g} : \mathbb{Z} \rightarrow \mathbb{C}$ is computed as

$$\hat{g}(k) = \int_0^1 g(x) e^{-2\pi i k x} dx$$

is called the k -th Fourier coefficient in the Fourier series of $g(x)$.

$$\begin{aligned}
\hat{g}(\omega) &= \int_{-\infty}^{\infty} g(x) e^{-2\pi i \omega x} dx \\
&= \cdots + \int_{-2}^{-1} g(x) e^{-2\pi i \omega x} dx + \int_{-1}^0 g(x) e^{-2\pi i \omega x} dx + \int_0^1 g(x) e^{-2\pi i \omega x} dx + \int_1^2 g(x) e^{-2\pi i \omega x} dx + \cdots \\
&= \sum_{k \in \mathbb{Z}} \left(\int_k^{k+1} g(x) e^{-2\pi i \omega x} dx \right) = \sum_{k \in \mathbb{Z}} I_k = \sum_{k \in \mathbb{Z}} \hat{g}(k) e^{2\pi i k x}
\end{aligned}$$

$$\begin{aligned}
I_k &= \int_k^{k+1} g(x) e^{-2\pi i \omega x} dx \\
&= \int_0^1 g(y+k) e^{-2\pi i \omega(y+k)} dy \quad [\text{Substitute } x = y+k] \\
&= e^{-2\pi i \omega k} \int_0^1 g(y+k) e^{-2\pi i \omega y} dy \\
&= e^{2\pi i \omega k} \int_0^1 g(y) e^{-2\pi i \omega y} dy \\
&= e^{2\pi i \omega k} \hat{g}(\omega)
\end{aligned}$$

Example 3.11. Let $g(x) = e^{2\pi i x k}$ where $k \in \mathbb{Z}$. Clearly, g is \mathbb{Z} periodic, and

$$\hat{g}(\omega) = \int_0^1 e^{2\pi i x k} e^{-2\pi i x \omega} dx = \int_0^1 e^{2\pi i x(k-\omega)} dx = \delta_{k,\omega} = \begin{cases} 0 & k \neq \omega \\ 1 & k = \omega \end{cases}$$

3.3 Poission Summasion Formula

We already have build the background of Fourier transform of a function in $L^1(\mathbb{R})$ and the Fourier series of a \mathbb{Z} -periodic function, moreover we have known the way of periodization a function. We would use these ingredients to prepare a nice looking formula called the Poission summation formula, named after the very wellknown French mathematician and Physicist Baron Siméon Denis Poisson. It is an equation that relates the Fourier series and the Fourier transformation of a function.

We will quickly prove one theorem that will support us to achieve a proof for the Poission Summasion Formula.

Theorem 3.12. Let g be the \mathbb{Z} -periodization of f then then the Fourier series of g is

$$\hat{g}(\omega) = \hat{f}(\omega)$$

Proof. Let $f \in L^1(\mathbb{R})$ then define the \mathbb{Z} -periodization of $f(x)$ as

$$g(x) = \sum_{z \in \mathbb{Z}} f(x+z)$$

Now for any $k \in \mathbb{Z}$

$$\begin{aligned}
\hat{g}(k) &= \int_0^1 g(x) e^{-2\pi i k x} dx = \int_0^1 \sum_{z \in \mathbb{Z}} f(x+z) e^{-2\pi i k x} dx = \int_0^1 \sum_{z \in \mathbb{Z}} f(x+z) e^{-2\pi i k(x+z)} dx \\
&= \int_{\mathbb{R}} f(y) e^{-2\pi i k y} dy = \hat{f}(k)
\end{aligned}$$

□

We have the following ingredients ready

- ✓ $g(x) = \sum_{k \in \mathbb{Z}} f(x + k)$ is how we have defined g to periodize f .
Putting $x = 0$ we get

$$g(0) = \sum_{k \in \mathbb{Z}} f(0 + k) = \sum_{k \in \mathbb{Z}} f(k)$$

- ✓ $g(x) = \sum_{w \in \mathbb{Z}} \hat{g}(\omega) e^{2\pi i x \omega}$ is the Fourier series for $g(x)$.
- ✓ Fourier coefficient of g is $\hat{g}(\omega) = \hat{f}(\omega)$

Theorem 3.13. (Poisson Summation Formula)

For any $f \in L^1(\mathbb{R})$ we have $f(\mathbb{Z}) = \hat{f}(\mathbb{Z})$ or equivalently,

$$\sum_{k=-\infty}^{\infty} f(k) = \sum_{k=-\infty}^{\infty} \hat{f}(k)$$

Proof. Let $f \in L^1(\mathbb{R})$ then define the \mathbb{Z} -periodization of $f(x)$ as

$$g(x) = \sum_{k \in \mathbb{Z}} f(x + k)$$

We already proved that the Fourier series of g is $\hat{g}(\omega) = \hat{f}(\omega)$ and equality still holds for a sum over \mathbb{Z} ,

$$\sum_{z \in \mathbb{Z}} \hat{g}(\omega) = \sum_{z \in \mathbb{Z}} \hat{f}(\omega)$$

Finally, we put them all together to deduce,

$$\sum_{z \in \mathbb{Z}} f(z) = g(0) = \sum_{w \in \mathbb{Z}} \hat{g}(\omega) e^{2\pi i 0 \omega} = \sum_{z \in \mathbb{Z}} \hat{g}(\omega) = \sum_{z \in \mathbb{Z}} \hat{f}(\omega)$$

□

Result 3.14. For a lattice in one dimension $\mathcal{L}(b)$ (say $b \in \mathbb{R}$), we can apply Poission formula .

Let $h(z) = f(bz)$ for $z \in \mathbb{Z}$ then, we already know, $\hat{h}(z) = b^{-1} \hat{f}(bz)$

Now running sum over \mathbb{Z} we get

$$\sum_{z \in \mathbb{Z}} h(z) = \sum_{z \in \mathbb{Z}} f(bz) \quad \text{and} \quad \sum_{z \in \mathbb{Z}} \hat{h}(z) = \sum_{z \in \mathbb{Z}} b^{-1} \hat{f}(bz)$$

Finally, applying the Poission Summasion Formula for h we obtain

$$\sum_{z \in \mathbb{Z}} h(z) = \sum_{z \in \mathbb{Z}} \hat{h}(z)$$

which is same as,

$$\sum_{z \in \mathbb{Z}} f(bz) = \sum_{z \in \mathbb{Z}} b^{-1} \hat{f}(bz)$$

Example 3.15. $f(x) = e^{-\pi x^2}$ and $f_s(x) := f(x/s) = e^{-\pi(x/s)^2}$

we will approximate $f_s(\mathbb{Z})$ for somewhat large s ,

$$\begin{aligned} f_s(\mathbb{Z}) &= f(s^{-1}\mathbb{Z}) = s\hat{f}(s\mathbb{Z}) = sf(s\mathbb{Z}) \\ &= sf(0) \quad \left[f(sz) = e^{-\pi(sz)^2} \approx 0 \text{ for } z \in \mathbb{Z}^* \right] \\ &= s \end{aligned}$$

4 Fourier in n -Dimension

Now we shift our attention towards the n -dimensional case. Here we fix our variables to be members in the n -dimensional space, $\mathbf{x}, \mathbf{w} \in \mathbb{R}^n$

Definition 4.1. ($L^1(\mathbb{R}^n)$ Function) *The function class $L^1(\mathbb{R}^n)$ is the set of all functions $f : \mathbb{R}^n \rightarrow \mathbb{C}$ for which*

$$\begin{aligned} \int_{\mathbb{R}^n} |f(\mathbf{x})| d\mathbf{x} &< \infty \\ L^1(\mathbb{R}^n) &= \left\{ f : \mathbb{R}^n \rightarrow \mathbb{C} \mid \int_{\mathbb{R}^n} |f(\mathbf{x})| d\mathbf{x} < \infty \right\} \end{aligned}$$

Definition 4.2. (Fourier Transform) *Given $f \in L^1(\mathbb{R}^n)$, its Fourier Transform $\hat{f} : \mathbb{R}^n \rightarrow \mathbb{C}$ is defined as*

$$\hat{f}(\mathbf{w}) := \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{w} \rangle} d\mathbf{x}$$

4.0.1 Properties of Fourier Transform in n -dimension

1. Linearity

For all $f, g \in L^1(\mathbb{R}^n)$ and $a \in \mathbb{R}$

- a. $\widehat{f+g} = \hat{f} + \hat{g}$
- b. $\widehat{af} = a\hat{f}$

2. Time Shift

Let $f \in L^1(\mathbb{R}^n)$ and $h(\mathbf{x}) = f(\mathbf{x} - \mathbf{c})$ for some $\mathbf{c} \in \mathbb{R}^n$, then

$$\hat{h}(\mathbf{w}) = e^{-2\pi i \langle \mathbf{w}, \mathbf{c} \rangle} \hat{f}(\mathbf{w})$$

3. Time Scale

Let $f \in L^1(\mathbb{R}^n)$ and $h(\mathbf{x}) = f(c\mathbf{x})$ for some $0 \neq c \in \mathbb{R}$, then

$$\hat{h}(\mathbf{w}) = \frac{1}{c} \hat{f}\left(\frac{\mathbf{w}}{c}\right)$$

4. Linear Transform Property

For any non-singular matrix $B \in \mathbb{R}^{n \times n}$, let $h(\mathbf{x}) = f(B\mathbf{x})$ then,

$$\hat{h}(\mathbf{x}) = \frac{1}{\det(B)} \hat{f}(B^{-T}\mathbf{w})$$

Proof.

$$\begin{aligned}
\hat{h}(\mathbf{w}) &= \int_{\mathbb{R}^n} f(B\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{w} \rangle} d\mathbf{x} \\
&= \int_{\mathbb{R}^n} f(\mathbf{u}) e^{-2\pi i \langle B^{-1}\mathbf{u}, \mathbf{w} \rangle} d(B^{-1}\mathbf{u}) && [\text{Substituting } B\mathbf{x} = \mathbf{u} \text{ gives } \mathbf{x} = B^{-1}\mathbf{u}] \\
&= \int_{\mathbb{R}^n} f(\mathbf{u}) e^{-2\pi i \langle \mathbf{u}, B^{-T}\mathbf{w} \rangle} d(B^{-1}\mathbf{u}) && [\text{Using the fact that } \langle B^{-1}\mathbf{u}, \mathbf{w} \rangle = \langle \mathbf{u}, B^{-T}\mathbf{w} \rangle] \\
&= \int_{\mathbb{R}^n} f(\mathbf{u}) e^{-2\pi i \langle \mathbf{u}, B^{-T}\mathbf{w} \rangle} \frac{1}{\det(B)} d\mathbf{u} && [\text{Using the fact that } d(Ax) = \det(A) dx] \\
&= \frac{1}{\det(B)} \int_{\mathbb{R}^n} f(\mathbf{u}) e^{-2\pi i \langle \mathbf{u}, B^{-T}\mathbf{w} \rangle} d\mathbf{u} \\
&= \frac{1}{\det(B)} \hat{f}(B^{-T}\mathbf{w})
\end{aligned}$$

□

Definition 4.3. (Fourier Series) For a \mathbb{Z}^n -periodic function $g : \mathbb{R}^n \rightarrow \mathbb{C}$ its Fourier series is defined as

$$g(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbb{Z}^n} \hat{g}(\mathbf{k}) e^{2\pi i \langle \mathbf{x}, \mathbf{k} \rangle}$$

where $\hat{g} : \mathbb{Z}^n \rightarrow \mathbb{C}$ is

$$\hat{g}(\mathbf{k}) = \int_0^1 g(\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{k} \rangle} d\mathbf{x}$$

is called the k -th Fourier coefficient.

$$\begin{aligned}
\hat{g}(\mathbf{w}) &= \int_{\mathbb{R}^n} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \\
&= \cdots + \int_{\mathcal{P}+\mathbf{z}_{-1}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} + \int_{\mathcal{P}+\mathbf{z}_0} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} + \int_{\mathcal{P}+\mathbf{z}_1} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} + \cdots \\
&= \sum_{\mathbf{z} \in \mathbb{Z}^n} \left(\int_{\mathcal{P}+\mathbf{z}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \right) = \sum_{\mathbf{z} \in \mathbb{Z}^n} I_{\mathbf{z}} = \sum_{\mathbf{z} \in \mathbb{Z}} \hat{g}(\mathbf{z}) e^{2\pi i \langle \mathbf{w}, \mathbf{z} \rangle}
\end{aligned}$$

$$\begin{aligned}
I_{\mathbf{z}} &= \int_{\mathcal{P}+\mathbf{z}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} = \int_{\mathcal{P}} g(\mathbf{x} - \mathbf{z}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} - \mathbf{z} \rangle} d\mathbf{x} \\
&= e^{2\pi i \langle \mathbf{w}, \mathbf{z} \rangle} \int_{\mathcal{P}} g(\mathbf{x} - \mathbf{z}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \\
&= e^{2\pi i \langle \mathbf{w}, \mathbf{z} \rangle} \int_{\mathcal{P}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \\
&= e^{2\pi i \langle \mathbf{w}, \mathbf{z} \rangle} \hat{g}(\mathbf{w})
\end{aligned}$$

Theorem 4.4. (Poisson Summation Formula)

For any $f \in L^1(\mathbb{R}^n)$ we have $f(\mathbb{Z}^n) = \hat{f}(\mathbb{Z}^n)$ or equivalently,

$$\sum_{\mathbf{z} \in \mathbb{Z}^n} f(\mathbf{z}) = \sum_{\mathbf{z} \in \mathbb{Z}^n} \hat{f}(\mathbf{z})$$

Proof. Let $f \in L^1(\mathbb{R})$ then define the \mathbb{Z}^n -periodization of $f(\mathbf{x})$ as

$$g(\mathbf{x}) = \sum_{\mathbf{z} \in \mathbb{Z}^n} f(\mathbf{x} + \mathbf{z})$$

Now we have,

$$\sum_{\mathbf{z} \in \mathbb{Z}^n} f(\mathbf{z}) = g(\mathbf{0}) = \sum_{\mathbf{w} \in \mathbb{Z}^n} \hat{g}(\mathbf{w}) e^{2\pi i \langle \mathbf{0}, \mathbf{w} \rangle} = \sum_{\mathbf{z} \in \mathbb{Z}^n} \hat{g}(\mathbf{w}) = \sum_{\mathbf{z} \in \mathbb{Z}^n} \hat{f}(\mathbf{w})$$

□

5 Fourier in Lattice

Our definition of lattice points is

$$\mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\}$$

and since it is discrete and repeats in a periodic fashion, we will try to see behaviour of functions in \mathcal{L} similar as the way it behaves for \mathbb{Z}^n . Mostly we will associate \mathcal{L} in the places where we used \mathbb{Z}^n .

Definition 5.1. (Dual Lattice) Let $L \subset \mathbb{R}^n$ then the dual lattice $\mathcal{L}^* \subset \mathbb{R}^*$ is defined as

$$\mathcal{L}^* = \{\mathbf{w} \in \mathbb{R}^n \mid \langle \mathbf{x}, \mathbf{w} \rangle \in \mathbb{Z}, \forall \mathbf{x} \in \mathcal{L}\}$$

equivalently,

$$\mathcal{L}^* = \{\mathbf{w} \in \mathbb{R}^n \mid \langle \mathcal{L}, \mathbf{w} \subseteq \mathbb{Z} \rangle\}$$

Result 5.2. If \mathcal{L} is a lattice (full rank) generated by B then its dual \mathcal{L}^* is generated by B^{-T} .

It is evident from the **Linear Transform Property** that for any non-singular matrix $B \in \mathbb{R}^{n \times n}$, let $h(\mathbf{x}) = f(B\mathbf{x})$ then,

$$\hat{h}(\mathbf{x}) = \frac{1}{\det(B)} \hat{f}(B^{-T} \mathbf{w})$$

$$B\mathbf{x} \subseteq \mathcal{L}$$

$$B^{-T} \mathbf{w} \subseteq \mathcal{L}^*$$

Definition 5.3. (Fourier Series) For a \mathcal{L} -periodic function $g : \mathbb{R}^n \rightarrow \mathbb{C}$ its Fourier series is defined as

$$g(\mathbf{x}) = \sum_{\mathbf{w} \in \mathcal{L}^*} \hat{g}(\mathbf{w}) e^{2\pi i \langle \mathbf{x}, \mathbf{w} \rangle}$$

where $\hat{g} : \mathcal{L}^* \rightarrow \mathbb{C}$ is

$$\hat{g}(\mathbf{w}) = \int_0^1 g(\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{w} \rangle} d\mathbf{x}$$

$$\begin{aligned} \hat{g}(\mathbf{w}) &= \int_{\mathbb{R}^n} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \\ &= \cdots + \int_{\mathcal{P} + \mathbf{w}_{-1}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} + \int_{\mathcal{P} + \mathbf{w}_0} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} + \int_{\mathcal{P} + \mathbf{w}_1} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} + \cdots \\ &= \sum_{\mathbf{w} \in \mathcal{L}^*} \left(\int_{\mathcal{P} + \mathbf{w}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \right) = \sum_{\mathbf{w} \in \mathcal{L}^*} I_{\mathbf{w}} = \sum_{\mathbf{w} \in \mathcal{L}^*} \hat{g}(\mathbf{w}) e^{2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} \end{aligned}$$

$$\begin{aligned}
I_{\mathbf{v}} &= \int_{\mathcal{P}+\mathbf{v}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} = \int_{\mathcal{P}} g(\mathbf{x} - \mathbf{v}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} - \mathbf{v} \rangle} d\mathbf{x} \\
&= e^{2\pi i \langle \mathbf{w}, \mathbf{v} \rangle} \int_{\mathcal{P}} g(\mathbf{x} - \mathbf{v}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \\
&= e^{2\pi i \langle \mathbf{w}, \mathbf{v} \rangle} \int_{\mathcal{P}} g(\mathbf{x}) e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} d\mathbf{x} \\
&= e^{2\pi i \langle \mathbf{w}, \mathbf{v} \rangle} \hat{g}(\mathbf{w})
\end{aligned}$$

Definition 5.4. (Fourier Series) For a \mathcal{L} -periodic function $g : \mathbb{R}^n \rightarrow \mathbb{C}$ its Fourier series $\hat{g} : \mathcal{L} \rightarrow \mathbb{C}$ is defined as

$$g(x) = \sum_{\omega \in \mathcal{L}^*} \hat{g}(\omega) e^{2\pi i \langle x, \omega \rangle}$$

where the Fourier coefficients are computed as,

$$\hat{g}(\omega) = \frac{1}{\det \mathcal{L}} \int_{\mathcal{P}} g(x) e^{-2\pi i \langle x, \omega \rangle} dx$$

over the fundamental parallelepiped of the lattice \mathcal{L} .

Result 5.5. (Poisson Summation Formula)

$$\sum_{\mathbf{z} \in \mathcal{L}} f(\mathbf{z}) = \sum_{\mathbf{z} \in \mathcal{L}} \hat{f}(\mathbf{z})$$

Our discussion on Fourier analysis will be used in the subsequent articles where we will be discussing about duals and more. We will see some snippets of Fourier over there.

References

- [Kre10] Erwin Kreyszig. *Advanced Engineering Mathematics 10E*. Chichester, England: John Wiley & Sons, Dec. 2010.
- [Pei13] Chris Peikert. “Lecture Notes on Lattices in Cryptography”. Georgia Tech, Fall 2013. 2013. URL: <https://github.com/cpeikert/LatticesInCryptography>.
- [Reg09] Regev. *Lecture Notes on Lattices in Computer Science*. Tel Aviv University, 2009.
- [Sha11] Rami Shakarchi. *Fourier Analysis*. Princeton, NJ: Princeton University Press, Feb. 2011.