1 Fourier transform and Fourier series in n-dimension

Recall from last lecture that in the one dimensional case, the Fourier transform of a function $f\colon \mathbb{R} \to \mathbb{C}$ is the function $\hat{f}\colon \mathbb{R} \to \mathbb{C}$ defined as

$$\hat{f}(w) = \int_{x\in\mathbb{R}} f(x)\exp(-2\pi i x w)\,dx.$$

The inversion formula is

$$f(x) = \int_{w\in\mathbb{R}} \hat{f}(w)\exp(2\pi i x w)\,dx.$$

For a $\mathbb{Z}$-periodic function $g\colon (\mathbb{R}/\mathbb{Z}) \to \mathbb{C}$, its Fourier series is the function $\hat{g}\colon \mathbb{Z} \to \mathbb{C}$ defined as

$$\hat{g}(w) = \int_{x\in\mathbb{R}/\mathbb{Z}} g(x)\exp(-2\pi i x w)\,dx.$$

The inversion formula is

$$g(x+\mathbb{Z}) = \sum_{w\in\mathbb{Z}} \hat{g}(w)\exp(2\pi i x w).$$

We now extend the Fourier transform and Fourier series to n dimensions. Similarly to before, define $L^1(\mathbb{R}^n)$ to be the set of functions $f\colon \mathbb{R}^n \to \mathbb{C}$ for which $\int_{\mathbb{R}^n} |f(\mathbf{x})|\,d\mathbf{x} < \infty$.

Definition 1.1. For $f \in L^1(\mathbb{R}^n)$, the Fourier transform of f is the function $\hat{f}\colon \mathbb{R}^n \to \mathbb{C}$ defined as

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

Definition 1.2. For a $\mathbb{Z}^n$-periodic function $g\colon \mathbb{R}^n/\mathbb{Z}^n \to \mathbb{C}$, its Fourier series $\hat{g}\colon \mathbb{Z}^n \to \mathbb{C}$ is defined as

$$\hat{f}(\mathbf{w}) = \int_{\mathbf{x}\in\mathbb{R}^n/\mathbb{Z}^n} f(\mathbf{x})\exp(-2\pi i\langle \mathbf{x}, \mathbf{w}\rangle)\,d\mathbf{x}.$$

We now mention some easy properties of the n-dimensional Fourier transform and Fourier series (where applicable); their proofs naturally generalize from the one-dimensional case.

1. *Linearity:* $\widehat{f+g} = \hat{f} + \hat{g}$ and $\widehat{c\cdot f} = c\cdot\hat{f}$ for any $c \in \mathbb{R}$.
2. *Shift property:* if $h(\mathbf{x}) = f(\mathbf{x}-\mathbf{c})$ for some $\mathbf{c}\in\mathbb{R}^n$ then $\hat{h}(\mathbf{w}) = \exp(-2\pi i\langle \mathbf{c}, \mathbf{w}\rangle)\cdot\hat{f}(\mathbf{w})$.
3. *Linear transform property:* if $h(\mathbf{x}) = f(\mathbf{B}\mathbf{x})$ for some nonsingular $\mathbf{B}\in\mathbb{R}^{n\times n}$, then $\hat{h}(\mathbf{w}) = \frac{1}{\det(\mathbf{B})}\hat{f}(\mathbf{B}^{-t}\mathbf{w})$. Here $\mathbf{B}^{-t} = (\mathbf{B}^{-1})^t = (\mathbf{B}^t)^{-1}$.

   Proof. From the definition of Fourier transform, we have

   $$\hat{h}(\mathbf{w}) = \int_{\mathbf{x}\in\mathbb{R}^n} f(\mathbf{B}\mathbf{x})\exp(-2\pi i\langle \mathbf{x}, \mathbf{w}\rangle)\,d\mathbf{x}.$$

   Letting $\mathbf{u} = \mathbf{B}\mathbf{x}$, we have $d\mathbf{u} = \det(\mathbf{B})\,d\mathbf{x}$, and $\langle \mathbf{x}, \mathbf{w}\rangle = \mathbf{x}^t\cdot\mathbf{w} = (\mathbf{x}^t\mathbf{B}^t)\cdot(\mathbf{B}^{-t}\mathbf{w}) = \langle \mathbf{B}\mathbf{x}, \mathbf{B}^{-t}\mathbf{w}\rangle$. So

   $$\begin{aligned}\hat{h}(\mathbf{w}) &= \int_{\mathbf{u}\in\mathbb{R}^n} f(\mathbf{u})\exp(-2\pi i\langle \mathbf{u}, \mathbf{B}^{-t}\mathbf{w}\rangle)\frac{1}{\det(\mathbf{B})}\,d\mathbf{u} \\ &= \frac{1}{\det(\mathbf{B})}\hat{f}(\mathbf{B}^{-t}\mathbf{w}).\end{aligned}$$ □

4. *Poisson summation formula:* $f(\mathbb{Z}^n) = \hat{f}(\mathbb{Z}^n)$.

2 Dual Lattices and $\mathcal{L}$-Periodic Functions

2.1 Definitions

So far, the periodic functions we have considered have only been $\mathbb{Z}^n$-periodic. We now extend the notion of Fourier series to functions that are periodic over a lattice $\mathcal{L}$, namely functions $g \colon \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$. One approach is to transform g to a $\mathbb{Z}^n$-periodic function h. Letting $\mathbf{B}$ be a basis of $\mathcal{L}$, we can write $\mathcal{L} = \mathbf{B}\mathbb{Z}^n$. Since g is $\mathcal{L}$-periodic, $h(\mathbf{x}) := g(\mathbf{B}\mathbf{x})$ is $\mathbb{Z}^n$-periodic. We can find the Fourier series for h and then use the scaling property to obtain the Fourier series for g. However, this approach requires switching back and forth between a $\mathcal{L}$-periodic function and a $\mathbb{Z}^n$-periodic function, which can be cumbersome. Therefore, we show another approach, which is to define the Fourier series for g directly. For this we need the notion of the *dual lattice*.

Definition 2.1 (Dual lattice). For a lattice $\mathcal{L} \subset \mathbb{R}^n$, its dual lattice $\mathcal{L}^* \subset \mathbb{R}^n$ is defined as

$$\begin{aligned} \mathcal{L}^* &= \{\mathbf{w} : \langle \mathbf{v}, \mathbf{w} \rangle \in \mathbb{Z} \; \forall \; \mathbf{v} \in \mathcal{L}\} \\ &= \{\mathbf{w} : \langle \mathcal{L}, \mathbf{w} \rangle \subseteq \mathbb{Z}\}. \end{aligned}$$

Definition 2.2. For a lattice $\mathcal{L} \subset \mathbb{R}^n$ and a function $g \colon \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$, its Fourier series $g \colon \mathcal{L}^* \to \mathbb{C}$ is defined as

$$\hat{g}(\mathbf{w}) = \frac{1}{\det(\mathcal{L})} \int_{\mathbf{x} \in \mathbb{R}^n/\mathcal{L}} g(\mathbf{x}) \exp(-2\pi i \langle \mathbf{x}, \mathbf{w} \rangle) \, d\mathbf{x}.$$

Notice that $\mathbf{x}$ is a *coset* $\mathbf{c} + \mathcal{L}$ for some $\mathbf{c} \in \mathbb{R}^n$; because $\langle \mathbf{x}, \mathbf{w} \rangle = \langle \mathbf{c} + \mathcal{L}, \mathbf{w} \rangle \subseteq \langle \mathbf{c}, \mathbf{w} \rangle + \mathbb{Z}$, the phase term $\exp(-2\pi i \langle \mathbf{x}, \mathbf{w} \rangle) = \exp(-2\pi i \langle \mathbf{c}, \mathbf{w} \rangle)$ is well defined, and invariant under the choice of $\mathbf{c}$ from the coset.

2.2 Properties of the Dual Lattice

We show some basic properties of the dual lattice. Definition 2.1 defines the dual of $\mathcal{L}$ as the set of points whose inner product with any point in $\mathcal{L}$ is an integer. The following claim establishes that $\mathcal{L}^*$ actually is a lattice.

Claim 2.3. *If $\mathbf{B}$ is a basis of $\mathcal{L}$, then $\mathbf{B}^{-t}$ is a basis of $\mathcal{L}^*$.*

Proof. We show that $\mathcal{L}^* = \mathcal{L}(\mathbf{B}^{-t})$ by proving inclusions in both directions. For any $\mathbf{w} = \mathbf{B}^{-t}\mathbf{z}$ where $\mathbf{z} \in \mathbb{Z}^n$,

$$\langle \mathbf{B} \cdot \mathbb{Z}^n, \mathbf{w} \rangle = \langle \mathbf{B} \cdot \mathbb{Z}^n, \mathbf{B}^{-t}\mathbf{z} \rangle = \langle \mathbb{Z}^n, \mathbf{z} \rangle \subseteq \mathbb{Z}.$$

So $\mathcal{L}(\mathbf{B}^{-t}) \subseteq \mathcal{L}^*$. In the other direction, for any $\mathbf{w} \in \mathcal{L}^*$, we have $\mathbf{z} := \mathbf{B}^t\mathbf{w} \in \mathbb{Z}^n$ (because the columns of $\mathbf{B}$ are vectors in $\mathcal{L}$), so $\mathbf{w} = \mathbf{B}^{-t}\mathbf{z} \in \mathcal{L}(\mathbf{B}^{-t})$, hence $\mathcal{L}^* \subseteq \mathcal{L}(\mathbf{B}^{-t})$. □

Claim 2.4. *For any lattice $\mathcal{L}$, we have $(\mathcal{L}^*)^* = \mathcal{L}$.*

Proof. By Claim 2.3, a basis of $(\mathcal{L}^*)^*$ is $(\mathbf{B}^{-t})^{-t} = \mathbf{B}$. Therefore, $(\mathcal{L}^*)^* = \mathcal{L}$, since they are generated by the same basis. □

Claim 2.5. *For any lattice $\mathcal{L}$, we have $\det(\mathcal{L}^*) = 1/\det(\mathcal{L})$.*

Proof. Since $\mathbf{B}$ is a basis of $\mathcal{L}$, and $\mathbf{B}^{-t}$ is a basis of $\mathcal{L}^*$,

$$\det(\mathcal{L}^*) = |\det(\mathbf{B}^{-t})| = \frac{1}{|\det(\mathbf{B})|} = \frac{1}{\det \mathcal{L}}.$$ □

Claim 2.6. *For any n-dimensional lattice $\mathcal{L}$, we have $\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \leq n$.*

Proof. By Minkowski's inequality we have $\lambda_1(\mathcal{L}) \leq \sqrt{n}\det(\mathcal{L}^{1/n})$ and $\lambda_1(\mathcal{L}^*) \leq \sqrt{n}\det(\mathcal{L}^*)^{1/n}$, so by Claim 2.5,

$$\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \leq n \cdot \det(\mathcal{L})^{1/n} \cdot \det(\mathcal{L}^*)^{1/n} \leq n. \qquad \square$$

2.3 Properties of the Fourier Series

We mention two important properties of the Fourier series of $\mathcal{L}$-periodic functions.

Inversion formula. For any $\mathcal{L}$-periodic function $g \colon \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$, we have

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

Periodization. Generalizing the one-dimensional case, we can "periodize" a function by a lattice, and then establish a link between the Fourier transform and Fourier series, respectively. Let $f \in L^1(\mathbb{R}^n)$, and for a countable set S, define $f(S) := \sum_{x\in S} f(x)$. For a lattice $\mathcal{L} \subset \mathbb{R}^n$, periodize f by summing all its $\mathcal{L}$-translates, i.e., define $g \colon \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$ as

$$g(\mathbf{x} + \mathcal{L}) := f(\mathbf{x} + \mathcal{L}) = \sum_{\mathbf{v}\in\mathcal{L}} f(\mathbf{x} + \mathbf{v}). \tag{2.1}$$

Lemma 2.7. *The Fourier series of g is $\hat{g}(\mathbf{w}) = \hat{f}(\mathbf{w})/\det(\mathcal{L}) = \det(\mathcal{L}^*)\hat{f}(\mathbf{w})$.*

Proof. Let $\mathcal{F}$ be any fundamental region of $\mathcal{L}$. Then for any $\mathbf{w} \in \mathcal{L}^*$, we have

$$\begin{aligned}
\hat{g}(\mathbf{w}) &= \frac{1}{\det(\mathcal{L})} \int_{\mathbf{x}\in\mathbb{R}^n/\mathcal{L}} g(\mathbf{x}) \exp(-2\pi i\langle \mathbf{x}, \mathbf{w}\rangle) d\mathbf{x} \\
&= \frac{1}{\det(\mathcal{L})} \int_{\mathbf{c}\in\mathcal{F}} g(\mathbf{c} + \mathcal{L}) \exp(-2\pi i\langle \mathbf{c}, \mathbf{w}\rangle) d\mathbf{x} \\
&= \frac{1}{\det(\mathcal{L})} \int_{\mathbf{c}\in\mathcal{F}} \sum_{\mathbf{v}\in\mathcal{L}} f(\mathbf{c} + \mathbf{v}) \exp(-2\pi i\langle \mathbf{c} + \mathbf{v}, \mathbf{w}\rangle) d\mathbf{x} \\
&= \frac{1}{\det(\mathcal{L})} \int_{\mathbf{u}\in\mathbb{R}^n} f(\mathbf{u}) \exp(-2\pi i\langle \mathbf{u}, \mathbf{w}\rangle) d\mathbf{u} \\
&= \frac{1}{\det(\mathcal{L})} \hat{f}(\mathbf{w}).
\end{aligned} \qquad \square$$

Lemma 2.8 (Poisson Summation Formula). *For any "nice enough" (differentiable, continuous, ...) function $f \colon \mathbb{R}^n \to \mathbb{C}$ and any lattice $\mathcal{L} \subset \mathbb{R}^n$, we have*

$$f(\mathcal{L}) = \hat{f}(\mathcal{L}^*)/\det(\mathcal{L}) = \det(\mathcal{L}^*) \cdot \hat{f}(\mathcal{L}^*).$$

Proof. Let g be the $\mathcal{L}$-periodization of f. By the inversion formula and Lemma 2.7,

$$f(\mathcal{L}) = g(\mathbf{0}) = \sum_{\mathbf{w}\in\mathcal{L}^*} \hat{g}(\mathbf{w}) \exp(2\pi i\langle \mathbf{0}, \mathbf{w}\rangle) = \sum_{\mathbf{w}\in\mathcal{L}^*} \hat{g}(\mathbf{w}) = \sum_{\mathbf{w}\in\mathcal{L}^*} \hat{f}(\mathbf{w})/\det(\mathcal{L}) = \hat{f}(\mathcal{L}^*)/\det(\mathcal{L}). \qquad \square$$

3 Application

In this section, we discuss an application of high dimensional Fourier transform, which provides a way of distinguishing "close" points from "far" points away from a lattice $\mathcal{L}$, using a "hint."

Problem definition. Given $\mathcal{L}$, we preprocess it to a hint W, which allows us to later answer queries: "Given a point $\mathbf{x}$, is $\mathrm{dist}(\mathbf{x}, \mathcal{L}) \leq 1$ or $\mathrm{dist}(\mathbf{x}, \mathcal{L}) \geq \sqrt{n}$?"

Strategy. Our strategy is to find a $\mathcal{L}$-periodic function f such that:

1. $f(x) \geq 1/1000$ for $d(\mathbf{x}, \mathcal{L}) \leq 1$.
2. $f(x) \leq 2^{-n}$ for $d(\mathbf{x}, \mathcal{L}) \geq \sqrt{n}$.
3. f can be succinctly represented, and there exists a good approximation to compute f.

Our main tool to create a function f is high dimensional Fourier transform and series. However, we need another tool, namely, the Gaussian function.

Definition 3.1. Define the Gaussian function $\rho(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2) = \exp(-\pi\langle \mathbf{x}, \mathbf{x}\rangle)$.

Definition 3.2.

Define
$$f(\mathbf{x}) = \frac{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{x}-\mathbf{v})}{\rho(\mathcal{L})} = \frac{\rho(\mathbf{x}+\mathcal{L})}{\rho(\mathcal{L})}.$$

Note that f is $\mathcal{L}$-periodic. The expression $\rho(\mathbf{x}+\mathcal{L})$ can be thought of as sum of the weights at $\mathbf{0}$ of the Gaussian functions centered at points in the coset $\mathbf{x}+\mathcal{L}$. Intuitively, when $\mathbf{x}$ is not close to any lattice point, $\mathbf{0}$ is not close to any point in the coset $\mathbf{x}+\mathcal{L}$, and the tail weights at $\mathbf{0}$ are all small. When $\mathbf{x}$ is close to a lattice point, $\mathbf{0}$ is close to a point in the coset $\mathbf{x}+\mathcal{L}$, and the weight of the Gaussian function centered at that point is large. In the next part of the lecture, we will show that f actually satisfies our above three requirements. First, we have the following easy claims:

Claim 3.3. *$\rho(\mathbf{x}+\mathcal{L}) \leq \rho(\mathcal{L})$ for any $\mathbf{x} \in \mathbb{R}^n$.*

Proof.

$$\begin{aligned}
\rho(\mathbf{x}+\mathcal{L}) &= \det(\mathcal{L}^*) \sum_{\mathbf{w}\in\mathcal{L}^*} \hat{\rho}(\mathbf{w}) \exp(2\pi\langle \mathbf{x}, \mathbf{w}\rangle) \\
&\leq \det(\mathcal{L}^*) \sum_{\mathbf{w}\in\mathcal{L}^*} \rho(\mathbf{w}) \\
&= \rho(\mathcal{L}).
\end{aligned}$$

Note that we used Poisson Summation Formula and the fact that $\hat{\rho}(\mathbf{w}) = \rho(\mathbf{w})$ for Gaussian function. ☐

Claim 3.4. *For any $s \geq 1$, $\rho_s(\mathcal{L}) \leq s^n \rho(\mathcal{L})$, where $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.*

Proof. From Poisson Summation Formula:

$$\rho_s(\mathcal{L}) = \det(\mathcal{L}^*)\hat{\rho}_s(\mathcal{L}^*).$$

Since $\hat{\rho}_s = s^n \rho_{1_s}$, we can write:

$$\rho_s(\mathcal{L}) = \det(\mathcal{L}^*) s^n \rho_{1/s}(\mathcal{L}^*).$$

Notice that $\rho_{1/s} \leq \rho_1$ for $s \geq 1$, therefore:

$$\rho_s(\mathcal{L}) \leq \det(\mathcal{L}^*) s^n \rho(\mathcal{L}^*).$$

Now apply the Poisson Summation Formula again, $\rho(\mathcal{L}) = \det(\mathcal{L}^*)\hat{\rho}(\mathcal{L}^*) = \det(\mathcal{L}^*)\rho(\mathcal{L}^*)$, we have $\rho(\mathcal{L}^*) = \rho(\mathcal{L})/\det(\mathcal{L}^*)$. Therefore:

$$\rho_s(\mathcal{L}) \leq s^n \rho(\mathcal{L}).$$

□

Next, we state three lemmas whose results directly show that function f that we defined meets our requirements.

Lemma 3.5. $f(\mathbf{x}) \geq \exp(-\pi \operatorname{dist}(\mathbf{x}, \mathcal{L})^2)\ \forall \mathbf{x}$

Proof. Since $\rho(\mathbf{x} + \mathcal{L}) = \rho(\mathbf{x} - \mathcal{L})$:

$$\rho(\mathbf{x} + \mathcal{L}) = 1/2(\rho(\mathbf{x} + \mathcal{L}) + \rho(\mathbf{x} - \mathcal{L})).$$

By the definition of Gaussian function:

$$\begin{aligned} \rho(\mathbf{x} + \mathcal{L}) &= 1/2 \sum_{\mathbf{v} \in \mathcal{L}} (\exp(-\pi\|\mathbf{x} + \mathbf{v}\|^2) + \exp(-\pi\|\mathbf{x} - \mathbf{v}\|^2)) \\ &= 1/2 \exp(-\pi\|\mathbf{x}\|^2) \sum_{\mathbf{v} \in \mathcal{L}} \exp(-\pi\|\mathbf{v}\|^2)(\exp(-2\pi\langle \mathbf{x}, \mathbf{v}\rangle) + \exp(2\pi\langle \mathbf{x}, \mathbf{v}\rangle)). \end{aligned}$$

By the Cauchy-Schwarz inequality $\exp(-2\pi\langle \mathbf{x}, \mathbf{v}\rangle) + \exp(2\pi\langle \mathbf{x}, \mathbf{v}\rangle) \geq 2$. We have:

$$\rho(\mathbf{x} + \mathcal{L}) \geq \exp(-\pi\|\mathbf{x}\|^2) \sum_{\mathbf{v} \in \mathcal{L}} \exp(-\pi\|\mathbf{v}\|^2) = \exp(-\pi\|\mathbf{x}\|^2)\rho(\mathcal{L}).$$

Therefore,

$$f(\mathbf{x}) = \rho(\mathbf{x} + \mathcal{L})/\rho(\mathcal{L}) \geq \exp(-\pi\|\mathbf{x}\|^2).$$

Now for all points in the coset $\mathbf{x} + \mathcal{L}$, there is a point $\mathbf{x}_0$ such that $\|\mathbf{x}_0\| = d(\mathbf{x}_0, \mathcal{L}) = d(\mathbf{x}, \mathcal{L})$. Represent $\mathbf{x} + \mathcal{L}$ as $\mathbf{x}_0 + \mathcal{L}$ and we have:

$$f(\mathbf{x}) = \rho(\mathbf{x}_0 + \mathcal{L})/\rho(\mathcal{L}) \geq \exp(-\pi\|\mathbf{x}_0\|^2) = \exp(-\pi d(\mathbf{x}_0, \mathcal{L})^2) = \exp(-\pi d(\mathbf{x}, \mathcal{L})^2).$$

□

From the above lemma, we see that if $d(\mathbf{x}, \mathcal{L}) = \mathcal{O}(1)$, then $f(\mathbf{x}) = \Omega(1)$, so f satisfies our first requirement.

Lemma 3.6. *For any coset* $\mathbf{x} + \mathcal{L}$, $\rho((\mathbf{x} + \mathcal{L}) \backslash \sqrt{n}\mathcal{B}) \leq 2^{-n}\rho(\mathcal{L})$, *where* $\mathcal{B}$ *represents the unit ball.*

Proof. From the Claim 3.4 above, $2^n\rho(\mathcal{L}) \geq \rho_2(\mathbf{x}+\mathcal{L})$, therefore:

$$\begin{aligned}
2^n\rho(\mathcal{L}) &\geq \rho_2(\mathbf{x}+\mathcal{L}) \\
&\geq \rho_2((\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}) \\
&= \sum_{\mathbf{v}\in(\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}} \exp(-\pi\|\mathbf{v}\|^2/4) \\
&= \sum_{\mathbf{v}\in(\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}} \exp(3\pi\|\mathbf{v}\|^2/4)\exp(-\pi\|\mathbf{v}\|^2) \\
&\geq \exp(3\pi n/4) \sum_{\mathbf{v}\in(\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}} \exp(-\pi\|\mathbf{v}\|^2) \\
&\geq 4^n\rho_1((\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}).
\end{aligned}$$

Therefore, $\rho((\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}) \leq 2^{-n}\rho(\mathcal{L})$ as desired. □

Corollary 3.7. *If $d(\mathbf{x},\mathcal{L}) \geq \sqrt{n}$ then $f(\mathbf{x}) \leq 2^{-n}$.*

Proof. If $d(\mathbf{x},\mathcal{L}) \geq \sqrt{n}$, $\mathbf{x}+\mathcal{L} = (\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}$, since there is no point of coset $\mathbf{x}+\mathcal{L}$ in the ball radius $\sqrt{n}$ centered at the origin. Therefore,

$$\rho(\mathbf{x}+\mathcal{L}) = \rho((\mathbf{x}+\mathcal{L})\backslash\sqrt{n}\mathcal{B}) \leq 2^{-n}\rho(\mathcal{L}),$$

And $f(\mathbf{x}) \leq 2^{-n}$ as desired. □

Next we need to show that f can be approximately computed.

Lemma 3.8. *f can be approximated efficiently.*

Proof. The idea is we can represent f by its Fourier series $\hat{f}(\mathbf{w})$, with $\mathbf{w} \in \mathcal{L}^*$. We know that:

$$\hat{f}(\mathbf{w}) = \hat{\rho}(\mathbf{w})\det(\mathcal{L}^*)/\rho(\mathcal{L}) = \hat{\rho}(\mathbf{w})/\rho(\mathcal{L}^*).$$

Therefore, $\sum_{\mathbf{w}\in\mathcal{L}^*}\hat{f}(\mathbf{w}) = 1$, and we can view $\hat{f}$ as a probability distribution. Then the expectation:

$$\mathop{\mathbb{E}}_{\mathbf{w}\leftarrow\hat{f}}(\exp(2\pi i\langle\mathbf{x},\mathbf{w}\rangle)) = \sum_{\mathbf{w}\in\mathcal{L}^*}\hat{f}(\mathbf{w})\exp(2\pi i\langle\mathbf{x},\mathbf{w}\rangle) = f(\mathbf{x}).$$

The first equality is just the definition of expectation, and the second one follows from the Poisson Summation Formula. Therefore, to approximate f, we can estimate the expectation above. We preprocess the lattice by output many values of $\mathbf{w}$ from the probability distribution $\hat{f}$, and store them. Then, given a query point $\mathbf{x}$, we can just compute average value of $\exp(2\pi i\langle\mathbf{x},\mathbf{w}\rangle)$ to be an estimator of $f(\mathbf{x})$. □

References