1 Fourier Transform and Series

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

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

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. Also notice the $1/\det(\mathcal{L})$ normalization factor, which is present because we are integrating over a set of volume $\det(\mathcal{L})$, and to make the definition invariant under nonzero scaling (or other invertible linear transform) of $\mathcal{L}$ and the input to g (with the dual transform applied to $\mathcal{L}^*$).

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 $\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \le n$.*

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

$$\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \le n \cdot \det(\mathcal{L})^{1/n} \cdot \det(\mathcal{L}^*)^{1/n} = n.$$ □

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 (Periodization lemma). *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

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

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,

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

□

3 Application: Closest Vector Problem with Preprocessing

In this section, we give an application of Fourier series over lattices, due to Aharonov and Regev [AR04] and building on foundational work by Banaszczyk [Ban93]. It provides a way of distinguishing points that are "close" to a lattice $\mathcal{L}$ from those that are "far" from the lattice, using some polynomial-sized (but typically inefficient-to-compute) "advice." More generally, the techniques developed here will prove extremely useful in other complexity-theoretic and cryptographic contexts.

Problem statement. For a given n-dimensional lattice $\mathcal{L}$, we wish to preprocess it to some advice W, which will allow us to later efficiently answer queries of the form: "Given a point $\mathbf{x}$, is $\operatorname{dist}(\mathbf{x}, \mathcal{L}) \le 1$ or $\operatorname{dist}(\mathbf{x}, \mathcal{L}) \ge \sqrt{n}$?" (The advice will not necessarily be useful for distances between these two thresholds.) That is, the advice lets us efficiently solve $\mathsf{GapCVP}_{\sqrt{n}}$ on the preprocessed lattice.

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

1. $g(\mathbf{x}) \ge 1/1000$ (say) whenever $\operatorname{dist}(\mathbf{x}, \mathcal{L}) = \lambda(\mathbf{x} + \mathcal{L}) \le 1$,
2. $g(\mathbf{x}) \le 2^{-n}$ whenever $\operatorname{dist}(\mathbf{x}, \mathcal{L}) = \lambda(\mathbf{x} + \mathcal{L}) \ge \sqrt{n}$, and
3. there is a succinct (polynomial-sized) advice that allows us to efficiently estimate g (to within, say, $1/\operatorname{poly}(n)$ additive error).

Then, to determine if a given point $\mathbf{x}$ is "close" to or "far" from the lattice, we simply estimate $g(\mathbf{x} + \mathcal{L})$ using the advice. We construct such g by periodizing the Gaussian function.

Definition 3.1. The Gaussian function $\rho\colon \mathbb{R}^n \to \mathbb{R}^+$ is defined as $\rho(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2) = \exp(-\pi\langle \mathbf{x}, \mathbf{x}\rangle)$. For an n-dimensional lattice $\mathcal{L}$, define the (scaled) $\mathcal{L}$-periodized Gaussian $g\colon \mathbb{R}^n/\mathcal{L} \to \mathbb{R}^+$ as

$$g(\mathbf{x} + \mathcal{L}) = \frac{\rho(\mathbf{x} + \mathcal{L})}{\rho(\mathcal{L})} = \frac{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{x} - \mathbf{v})}{\rho(\mathcal{L})}. \tag{3.1}$$

The denominator is simply a normalizing factor that makes $g(\mathcal{L}) = 1$. The expression $\rho(\mathbf{x} + \mathcal{L})$ in the numerator is the sum of the Gaussian function over all elements of the coset $\mathbf{x} + \mathcal{L}$. This can equivalently be seen as the sum of Gaussian functions centered at every lattice point, evaluated at $\mathbf{x}$. When $\mathbf{x}$ is fairly close to a lattice point, the Gaussian centered at that point contributes significantly to the sum. (Equivalently, the Gaussian mass of the shortest vector in $\mathbf{x} + \mathcal{L}$ is fairly large.) Whereas when $\mathbf{x}$ is far from every lattice point, none of the lattice-centered Gaussians contribute much. In what follows, we will show that g does indeed satisfy our above three requirements. We start with two fairly simple claims.

Claim 3.2. *We have $\rho(\mathbf{x}+\mathcal{L}) \le \rho(\mathcal{L})$ for any $\mathbf{x} \in \mathbb{R}^n$, i.e., $g(\mathbf{x}) \in [0,1]$.*

Proof. By the Poisson Summation Formula (twice), the shift property, and the fact that $\hat{\rho} = \rho$ is real-valued and positive, we have

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

□

Claim 3.3. *For any $s \ge 1$, we have $\rho_s(\mathcal{L}) \le s^n \cdot \rho(\mathcal{L})$, where $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.*

Proof. By the Poisson Summation Formula (twice) and the fact that $\widehat{\rho_s} = s^n \cdot \rho_{1/s} \le s^n \cdot \rho_1$ for $s \ge 1$,

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

□

Next, we establish three lemmas which show that the function g meets our requirements.

Lemma 3.4. *For all $\mathbf{x} \in \mathbb{R}^n$, we have $g(\mathbf{x}) \ge \exp(-\pi \operatorname{dist}(\mathbf{x}, \mathcal{L})^2)$.*

It is tempting to think that this claim is trivial: letting $\mathbf{v} \in \mathcal{L}$ be a closest lattice vector to $\mathbf{x}$, the Gaussian centered at $\mathbf{v}$ contributes $\rho(\mathbf{x}-\mathbf{v}) = \exp(-\pi \operatorname{dist}(\mathbf{x}, \mathcal{L})^2)$ to the sum of Gaussians centered at all lattice points. The issue is that this sum is merely the *numerator* of $g(\mathbf{x}+\mathcal{L})$, and it is normalized by $\rho(\mathcal{L}) > \rho(\mathbf{0}) = 1$. So, the contribution of the $\mathbf{v}$-centered Gaussian alone is definitely not enough to prove the claim. Instead, we use a clever symmetrization argument that pairs up the contributions from the centers $\pm\mathbf{v}$, over all $\mathbf{v} \in \mathcal{L}$.

Proof. Since $\mathbf{x}+\mathcal{L} = \mathbf{x}-\mathcal{L}$, we have

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

Now, by definition of the Gaussian function and the fact that $\exp(t) + \exp(-t) \ge 2$ for all t, we have

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

The claim follows by noticing that there is a point $\mathbf{x}_0 \in \mathbf{x}+\mathcal{L}$ for which $\|\mathbf{x}_0\| = \operatorname{dist}(\mathbf{x}_0, \mathcal{L}) = \operatorname{dist}(\mathbf{x}, \mathcal{L})$.□

By Lemma 3.4, we see that $g(\mathbf{x}+\mathcal{L}) \ge \exp(-\pi) > \frac{1}{24}$ whenever $\operatorname{dist}(\mathbf{x}, \mathcal{L}) \le 1$, so g satisfies our first requirement.

Lemma 3.5 ([Ban93]). *For any coset $\mathbf{x}+\mathcal{L}$, we have $\rho((\mathbf{x}+\mathcal{L}) \setminus \sqrt{n}\mathcal{B}) \le 2^{-n} \cdot \rho(\mathcal{L})$, where $\mathcal{B}$ is the (open) unit ball.*

Let us consider what Lemma 3.5 says, and give some intuition for the proof. It is a "tail bound," which says that the total Gaussian mass of the points in $\mathbf{x} + \mathcal{L}$ having norm at least $\sqrt{n}$ is a tiny fraction of the total Gaussian mass of $\mathcal{L}$ itself. To prove this, we will go through the scaled Gaussian ρ_2. For simplicity, consider the coset $\mathbf{x} + \mathcal{L} = \mathcal{L}$. By Claim 3.3, we know that $\rho_2(\mathcal{L}) \leq 2^n \cdot \rho_1(\mathcal{L})$, i.e., $\mathcal{L}$'s total mass under ρ_2 is no more than 2^n times larger than its mass under ρ_1. On the other hand, every vector that is sufficiently far from the origin has *much larger* mass under ρ_2 than it has under ρ_1, by a multiplicative factor of at least (say) 2^{2n}. The only way both statements can be true is if, under ρ_1, the "far" vectors account for at most a $2^n/2^{2n} = 2^{-n}$ fraction of the total mass.

Proof. By Claims 3.2 and 3.3 above, $2^n \cdot \rho(\mathcal{L}) \geq \rho_2(\mathbf{x} + \mathcal{L})$, so

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

The claim follows by dividing. □

Corollary 3.6. *If* $\operatorname{dist}(\mathbf{x}, \mathcal{L}) \geq \sqrt{n}$ *then* $g(\mathbf{x}) \leq 2^{-n}$.

Proof. If $\operatorname{dist}(\mathbf{x}, \mathcal{L}) \geq \sqrt{n}$, then $\mathbf{x} + \mathcal{L} = (\mathbf{x} + \mathcal{L}) \setminus \sqrt{n}\mathcal{B}$, since $\mathbf{x} + \mathcal{L}$ does not have any point of length less than $\sqrt{n}$. Therefore, by Lemma 3.5 we have

$$g(\mathbf{x} + \mathcal{L}) = \frac{\rho(\mathbf{x} + \mathcal{L})}{\rho(\mathcal{L})} = \frac{\rho((\mathbf{x} + \mathcal{L}) \setminus \sqrt{n}\mathcal{B})}{\rho(\mathcal{L})} \leq 2^{-n}.$$

□

Lemma 3.7. *Given appropriate polynomial-sized advice about* $\mathcal{L}$*, the function* g *can be efficiently approximated to within additive* $1/\operatorname{poly}(n)$ *error.*

Proof sketch. The first key idea is that by the inversion formula, g can be evaluated using its Fourier series coefficients $\hat{g}(\mathbf{w})$, over all $\mathbf{w} \in \mathcal{L}^*$. Of course, there are an infinite number of these coefficients, which we cannot represent (much less sum over) efficiently.

The second key idea is that the Fourier series can be thought of as a *probability distribution*, and the inversion formula as an *expectation* taken over this distribution. Observe that by definition of g (Equation (3.1)), the periodization lemma (Lemma 2.7), and the Poisson Summation Formula (Lemma 2.8), the Fourier coefficients are

$$\hat{g}(\mathbf{w}) = \frac{\hat{\rho}(\mathbf{w})/\det(\mathcal{L})}{\rho(\mathcal{L})} = \frac{\rho(\mathbf{w})/\det(\mathcal{L})}{\rho(\mathcal{L}^*)/\det(\mathcal{L})} = \rho(\mathbf{w})/\rho(\mathcal{L}^*) \in [0, 1].$$

Therefore, $\hat{g}(\mathcal{L}^*) = \sum_{\mathbf{w} \in \mathcal{L}^*} \hat{g}(\mathbf{w}) = 1$, and we can think of the Fourier coefficient $\hat{g}(\mathbf{w})$ as the probability assigned to $\mathbf{w}$ by distribution $\hat{g}$. The inversion formula can then be expressed (using the symmetry of $\mathcal{L}^*$) as

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

Therefore, to approximate g, we can estimate the above expectation by random sampling. That is, we sample many values of $\mathbf{w}$ from the probability distribution $\hat{g}$. Then, given a query point $\mathbf{x}$, we estimate $g(\mathbf{x} + \mathcal{L})$ simply by computing the average value of $\cos(2\pi\langle \mathbf{x}, \mathbf{w}\rangle)$. By standard Chernoff-style bounds, this estimate will be with $1/\operatorname{poly}(n)$ of the true value, with high probability. By the probabilistic method, this implies that there *exists* preprocessing advice that gives a good enough estimate of $g(\mathbf{x} + \mathcal{L})$.

The above shows that a suitable random sampling of dual lattice vectors $\mathbf{w} \in \mathcal{L}^*$ lets us approximate $g(\mathbf{x} + \mathcal{L})$ for a *single* coset $\mathbf{x} + \mathcal{L}$. But what we really want is that the *same collection* of samples is likely to work for *all cosets* simultaneously. This can be shown via a (somewhat grungy) union-bound argument. First, we fix a huge (but finite), exponential-size "dense net" S of points that contains a good enough approximation to any $\mathbf{x} + \mathcal{L}$. Then, we can take enough samples so that, by Chernoff-like bounds, the probability that our estimator is inaccurate for any *fixed* point in the net is $\ll 1/|S|$. By the union bound, with positive probability, the estimator is accurate on all net points simultaneously. So, there exists some good advice that works for all query points. □

References

[AR04] D. Aharonov and O. Regev. Lattice problems in NP ∩ coNP. *J. ACM*, 52(5):749–765, 2005. Preliminary version in FOCS 2004. Page 4.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993. Pages 4 and 5.