Lecture 6

Lecturers: D. Dadush, L. Ducas
Scribe: S. Huiberts

Introduction to transference

1 Introduction

In this lecture, we study transference theorems. These are theorems relating properties of a lattice $\mathcal{L}$ and its dual lattice $\mathcal{L}^*$. In the first half of this lecture we will prove transference theorems using basis reduction techniques achieving (suboptimal) polynomial bounds, which are much better than the guarantees from LLL reduced bases. In the second half, we will introduce important concepts in Fourier analysis, which will be used in the following two lectures to prove optimal transference results.

2 Transference

The first elementary transference principle we have already seen in earlier lectures.

PROPOSITION 1 *For a lattice $\mathcal{L} \subseteq \mathbb{R}^n$ of rank at least 1, we have*

$$\det(\mathcal{L}) = \frac{1}{\det(\mathcal{L}^*)}.$$

In this lecture we will see bounds relating the successive minima and the covering radius of a lattice and its dual lattice.

THEOREM 2 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ we have $\lambda_i(\mathcal{L}) \cdot \lambda_{n-i+1}(\mathcal{L}^*) \geq 1$.*

PROOF: Let $\mathbf{v}_1, \ldots, \mathbf{v}_{n-i+1} \in \mathcal{L}^*$ be linearly independent vectors achieving the successive minima, i.e., $\|\mathbf{v}_1\| = \lambda_1(\mathcal{L}^*), \ldots, \|\mathbf{v}_{n-i+1}\| = \lambda_{n-i+1}(\mathcal{L}^*)$, and let $\mathbf{y}_1, \ldots, \mathbf{y}_i \in \mathcal{L}$ be such that $\|\mathbf{y}_1\| = \lambda_1(\mathcal{L}), \ldots, \|\mathbf{y}_i\| = \lambda_i(\mathcal{L})$. By dimension counting the sets $\mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_{n-i+1})$ and $\mathrm{span}(\mathbf{y}_1, \ldots, \mathbf{y}_i)$ have a non-trivial intersection, hence there exist indices j_1, j_2 such that $|\langle \mathbf{v}_{j_1}, \mathbf{y}_{j_2} \rangle| > 0$. As the inner product must be integer, this means $|\langle \mathbf{v}_{j_1}, \mathbf{y}_{j_2} \rangle| \geq 1$. From the Cauchy-Schwarz inequality we know $\|\mathbf{v}_{j_1}\| \cdot \|\mathbf{y}_{j_2}\| \geq 1$. From our choice of $\mathbf{v}_{j_1}$ and $\mathbf{y}_{j_2}$ we get $\lambda_{j_1}(\mathcal{L}^*) \cdot \lambda_{j_2}(\mathcal{L}) \geq 1$. Since $\lambda_{j_1}(\mathcal{L}^*) \leq \lambda_{n-i+1}(\mathcal{L}^*)$ and $\lambda_{j_2}(\mathcal{L}) \leq \lambda_i(\mathcal{L})$, the result follows. □

In lecture 2, we saw that $\mu(\mathcal{L}) \leq \frac{1}{2} \sum_{i=1} \lambda_i(\mathcal{L})$. The next theorem will be a reverse inequality. First we need to prove a claim.

CLAIM 3 *For a linear subspace $W \subsetneq \mathbb{R}^n$ and full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, there exists $\mathbf{v} \notin W, \mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq 2\mu(\mathcal{L})$.*

PROOF: Pick $\mathbf{z} \in \mathbb{R}^n$ orthogonal to W such that $\|\mathbf{z}\| = \mu(\mathcal{L})$. If $\mathbf{z} + \mu(\mathcal{L})\mathcal{B}_2^n$ contains a non-zero lattice point, we are done. The triangle inequality implies that such a point has norm at most $2\mu(\mathcal{L})$, and $\mathbf{0}$ is the unique closest point to $\mathbf{z}$ in W at distance $\mu(\mathcal{L})$, meaning that our point is not in W. Now suppose that $(\mathbf{z} + \mu(\mathcal{L})\mathcal{B}_2^n) \cap \mathcal{L} = \{\mathbf{0}\}$, then there exists some $\varepsilon > 0$ such that $(1+\varepsilon)\mathbf{z} + \mu(\mathcal{L})\mathcal{B}_2^n$ contains no lattice points. But that means that $(1+\varepsilon)\mathbf{z}$ has distance more than $\mu(\mathcal{L})$ to the lattice $\mathcal{L}$, contradicting the definition of $\mu(\mathcal{L})$. Hence the claim is true. □

THEOREM 4 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, $\mu(\mathcal{L}) \geq \lambda_n(\mathcal{L})/2$.*

PROOF: We will use Claim 3 to inductively build a chain of subspaces $W_1 \subset \cdots \subset W_n$, such that W_i is the span of i linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_i \in \mathcal{L}$ of length at most $2\mu(\mathcal{L})$. Let $W_0 = \{\mathbf{0}\}$. For each $i \in [n]$, let $\mathbf{v}_i \in \mathcal{L}$ be such that $\mathbf{v}_i \notin W_{i-1}$ and $\|\mathbf{v}_i\| \le 2\mu(\mathcal{L})$, which exists by claim 3, and let $W_i = \mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_i)$. The linear subspace W_n is full-dimensional and $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$, so $\lambda_n(\mathcal{L}) \le \max_{i \le n} \|\mathbf{v}_i\| \le 2\mu(\mathcal{L})$. □

THEOREM 5 *For a lattice $\mathcal{L} \subset \mathbb{R}^n$ of rank at least 1, $\mu(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \ge 1/2$.*

PROOF: Pick $\mathbf{y} \in \mathcal{L}^*$ with $\|\mathbf{y}\| = \lambda_1(\mathcal{L}^*)$. All vectors in $\mathcal{L}$ have integer inner product with $\mathbf{y}$ because $\mathbf{y} \in \mathcal{L}^*$, so $\mathcal{L} \subset \bigcup_{i \in \mathbb{Z}} \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{y}, \mathbf{x} \rangle = i\}$. For $\mathbf{z} = \frac{\mathbf{y}}{2\|\mathbf{y}\|^2}$, we have

$$\mathrm{d}(\mathcal{L}, \mathbf{z}) \ge \frac{\min_{\mathbf{x} \in \mathcal{L}} |\langle \mathbf{z} - \mathbf{x}, \mathbf{y} \rangle|}{\|\mathbf{y}\|} = \min_{z \in \mathbb{Z}} \frac{|\frac{1}{2} - z|}{\|\mathbf{y}\|} = \frac{1}{2\|\mathbf{y}\|} = \frac{1}{2\lambda_1(\mathcal{L}^*)}.$$

□

PROPOSITION 6 *For a rank k lattice $\mathcal{L} \subset \mathbb{R}^n$, $k \ge 1$, we have $\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \le k$.*

PROOF: By Minkowski's first theorem we have

$$\lambda_1(\mathcal{L}) \le \sqrt{k} \det(\mathcal{L})^{1/k}$$

and

$$\lambda_1(\mathcal{L}^*) \le \sqrt{k} \det(\mathcal{L}^*)^{1/k}.$$

Recall that $\det(\mathcal{L}) = \frac{1}{\det(\mathcal{L}^*)}$. We multiply the two inequalities to find the desired result. □

For the next two results, we use the existence of bases satisfying certain nice properties. The bounds we will achieve in this lecture are sub-optimal, and in later lectures we will prove better bounds using Fourier-analytic techniques.

DEFINITION 7 *A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ is Hermite-Korkine-Zolotareff-reduced (HKZ) if*

- *$\mathbf{B}$ is size-reduced, and*
- *for all $i \in [n]$, $\|\widetilde{\mathbf{b}}_i\| = \lambda_1(\pi_i(\mathcal{L}))$, where π_i is the orthogonal projection onto* $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$.

We can size-reduce a basis $\mathbf{B}$ while preserving the second property, and we can produce a basis satisfying the second property by setting $\mathcal{L}_1 = \mathcal{L}$ and iteratively picking $\mathbf{b}_i$ as a shortest vector of $\mathcal{L}_i$ and setting $\mathcal{L}_{i+1} = \pi_{\mathbf{b}_i^\perp}(\mathcal{L}_i)$. In particular, this means that every lattice has an HKZ-reduced basis.

FACT 8 *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ and linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathcal{L}$,*

$$\pi_{\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_k)^\perp}(\mathcal{L})^* = \mathcal{L}^* \cap \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_k)^\perp.$$

THEOREM 9 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, we have that $\frac{1}{2} \le \mu(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \le \frac{1}{2} n^{3/2}$.*

Proof: Let $\mathbf{B}$ be an HKZ-reduced basis of $\mathcal{L}$. For $i \in [n]$, let $W_i := \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$. The correctness of Babai's algorithm tells us that

$$\begin{aligned}
\mu(\mathcal{L})^2 &\leq \frac{1}{4}\sum_{i=1}^{n} \|\widetilde{\mathbf{b}}_i\|^2 && \text{(Babai)} \\
&= \frac{1}{4}\sum_{i=1}^{n} \lambda_1(\pi_{W_i}(\mathcal{L}))^2 && \text{(HKZ-reducedness)} \\
&\leq \frac{1}{4}\sum_{i=1}^{n} \frac{n^2}{\lambda_1(\mathcal{L}^* \cap W_i)^2} && \text{(Proposition 6 + Fact 8)} \\
&\leq \frac{1}{4}\sum_{i=1}^{n} \frac{n^2}{\lambda_1(\mathcal{L}^*)^2} && \text{(By inclusion)} \\
&= \frac{1}{4}\frac{n^3}{\lambda_1(\mathcal{L}^*)^2}.
\end{aligned}$$

□

Theorem 10 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, we have $1 \leq \lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^*) \leq n^2$.*

Proof: Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be an HKZ-reduced basis, and for $i \in [n]$, let $W_i = \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$. From here, we have that

$$\begin{aligned}
\lambda_i(\mathcal{L})^2 &\leq \max_{j \leq i} \|\mathbf{b}_j\|^2 \\
&\leq \max_{j \leq i} \sum_{k=1}^{j} \|\widetilde{\mathbf{b}}_k\|^2 \quad \text{(By size-reduction of the basis)} \\
&\leq \sum_{k=1}^{i} \|\widetilde{\mathbf{b}}_k\|^2 \\
&= \sum_{k=1}^{i} \lambda_i(\pi_k(\mathcal{L}))^2 \quad \text{(By HKZ property)}\,.
\end{aligned} \tag{1}$$

Since $\pi_k(\mathcal{L})$ is an $n-k+1 \geq n-i+1$ dimensional lattice and $\pi_k(\mathcal{L})^* = \mathcal{L}^* \cap W_k$, we have

$$\lambda_i(\pi_k(\mathcal{L}))^2 \lambda_{n-i+1}(\mathcal{L}^* \cap W_k)^2 \underbrace{\leq}_{\text{Theorem 4}} 4\lambda_i(\pi_k(\mathcal{L}))^2 \mu(\mathcal{L}^* \cap W_k)^2 \underbrace{\leq}_{\text{Theorem 9}} n^3.$$

From the above, we may continue (1) as follows,

$$\begin{aligned}
\sum_{k=1}^{i} \lambda_i(\pi_k(\mathcal{L}))^2 &\leq \sum_{k=1}^{i} \frac{n^3}{\lambda_{n-i+1}(\mathcal{L}^* \cap W_k)^2} \\
&\leq \sum_{k=1}^{i} \frac{n^3}{\lambda_{n-i+1}(\mathcal{L}^*)^2} \quad \text{(By inclusion)} \\
&= \frac{n^4}{\lambda_{n-i+1}(\mathcal{L}^*)^2}.
\end{aligned} \tag{2}$$

The statement now follows by combining (1), (2). □

3 Fourier analysis

For the last two theorems we will be able to prove a stronger bound of $O(n)$ using Fourier-analytic techniques. The rest of this lecture, plus the next two lectures, are devoted to developing the tools to prove this. In this part of the lecture we talked about a few basic notions in Fourier analysis, which will give us a more principled way of proving transference results.

Definition 11 *For $f, g : \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$, we define their inner product by*

$$\langle f, g \rangle = \frac{1}{\det(\mathcal{L})} \int_D f(\mathbf{x} + \mathcal{L})\overline{g(\mathbf{x} + \mathcal{L})} \mathrm{d}\mathbf{x},$$

where $\overline{g(\mathbf{x} + \mathcal{L})}$ is the complex conjugate of $g(\mathbf{x} + \mathcal{L})$ and D is any fundamental domain of $\mathcal{L}$. We note that the inner product is well-defined: one can check that it is independent of the choice of fundamental domain.

Definition 12 *For $\mathbf{y} \in \mathcal{L}^*$, we define $\chi_{\mathbf{y}} : \mathbb{R}^n/\mathcal{L} \to \mathbb{C}^*$, where $\mathbb{C}^* = \{z \in \mathbb{Z} : |z| = 1\}$ is the complex unit circle, by $\chi_y(\mathbf{t}) = e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle}$ for $\mathbf{t} \in \mathbb{R}^n/\mathcal{L}$. Note that this function is well-defined, since for any $\mathbf{a}, \mathbf{b} \in \mathbf{t} + \mathcal{L}$, we have that*

$$\mathbf{a} - \mathbf{b} \in \mathcal{L} \Rightarrow \langle \mathbf{y}, \mathbf{a} - \mathbf{b} \rangle \in \mathbb{Z} \Rightarrow e^{2\pi i \langle \mathbf{y}, \mathbf{a} - \mathbf{b} \rangle} = 1 \Rightarrow \chi_{\mathbf{y}}(\mathbf{a}) = \chi_{\mathbf{y}}(\mathbf{b}).$$

$\chi_{\mathbf{y}}$ is in fact a character of the group $\mathbb{R}^n/\mathcal{L}$, that is, it is a homomorphism from $\mathbb{R}^n/\mathcal{L}$ to the complex unit circle, i.e. $\chi_{\mathbf{y}}(\mathbf{a} + \mathbf{b}) = \chi_{\mathbf{y}}(\mathbf{a})\chi_{\mathbf{y}}(\mathbf{b})$, $\forall \mathbf{a}, \mathbf{b} \in \mathbb{R}^n/\mathcal{L}$.

It is an interesting exercise to check that the functions $\{\chi_{\mathbf{y}} : \mathbf{y} \in \mathcal{L}^*\}$ correspond exactly to set of continuous homomorphisms from $\mathbb{R}^n/\mathcal{L}$ to $\mathbb{C}^*$. We now show that they form an orthonormal set of functions under the inner product defined above.

Proposition 13 *The characters are orthonormal: for $\mathbf{x}, \mathbf{y} \in \mathcal{L}^*, \mathbf{x} \neq \mathbf{y}$ we have $\langle \chi_{\mathbf{x}}, \chi_{\mathbf{x}} \rangle = 1$ and $\langle \chi_{\mathbf{x}}, \chi_{\mathbf{y}} \rangle = 0$.*

Proof:

$$\begin{aligned}\langle \chi_{\mathbf{x}}, \chi_{\mathbf{x}} \rangle &= \frac{1}{\det(\mathcal{L})} \int_D e^{2\pi i \langle \mathbf{x}, \mathbf{t} \rangle} \overline{e^{2\pi i \langle \mathbf{x}, \mathbf{t} \rangle}} \mathrm{d}\mathbf{t} \\ &= \frac{1}{\det(\mathcal{L})} \int_D 1 \, \mathrm{d}\mathbf{t} \\ &= 1.\end{aligned}$$

Let $\mathbf{b}_1^* = \mathbf{x} - \mathbf{y}$ and extend this to a basis $\mathbf{B}^*$ of $\mathcal{L}^*$. Now let $\mathbf{B}$ be the dual basis to $\mathbf{B}^*$. Choose

$D = \mathbf{B}[0,1)^n$ as fundamental domain of $\mathcal{L}$.

$$\begin{aligned}
\langle \chi_{\mathbf{x}}, \chi_{\mathbf{y}} \rangle &= \frac{1}{\det(\mathcal{L})} \int_{\mathbf{B}[0,1)^n} e^{2\pi i \langle \mathbf{x}-\mathbf{y}, \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \\
&= \frac{1}{\det(\mathcal{L})} \int_{\mathbf{B}[0,1)^n} e^{2\pi i \langle \mathbf{b}_1^*, \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \\
&= \frac{|\det(\mathbf{B})|}{\det(\mathcal{L})} \int_{[0,1)^n} e^{2\pi i \langle \mathbf{B}\mathbf{e}_1, \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \\
&= \frac{|\det(\mathbf{B})|}{\det(\mathcal{L})} \int_{[0,1)} e^{2\pi i \cdot s} \mathrm{d}s \\
&= 0.
\end{aligned}$$

□

For a complex valued function f on $\mathbb{R}^n/\mathcal{L}$ and a character $\chi_{\mathbf{y}}$ of $\mathbb{R}^n/\mathcal{L}$, we define the Fourier coefficients of f with respect to $\mathbf{y}$ as $\widehat{f}(\mathbf{y}) := \langle f, \chi_{\mathbf{y}} \rangle$. Given the above orthonormality, it is natural to hope that as long as f is reasonable then it can be expressed as a (possibly infinite) linear combinations of the characters $\{\chi_{\mathbf{y}} : \mathbf{y} \in \mathcal{L}^*\}$, known as the Fourier basis. In particular, one would likely expect that

$$f = \sum_{\mathbf{y} \in \mathcal{L}^*} \langle f, \chi_{\mathbf{y}} \rangle \chi_{\mathbf{y}} := \sum_{\mathbf{y} \in \mathcal{L}^*} \widehat{f}(\mathbf{y}) \chi_{\mathbf{y}} \, .$$

While the above type equality holds without restriction on f when the domain is a finite abelian group, for a continuous group the situation is somewhat more delicate. In particular, it is not even clear when the series on the right hand side is well-defined. The following useful theorem in Fourier analysis, which we state without proof, will give sufficient conditions for this equality to hold.

Theorem 14 *For continuous* $f : \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$ *satisfying* $\sum_{\mathbf{y} \in \mathcal{L}^*} |\widehat{f}(\mathbf{y})| < \infty$, *we have that*

$$f(\mathbf{t}) = \sum_{\mathbf{y} \in \mathcal{L}^*} \widehat{f}(\mathbf{y}) e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle}.$$

We note that the second condition in the above theorem in essence addresses the concern that series $\sum_{\mathbf{y} \in \mathcal{L}^*} \widehat{f}(\mathbf{y}) e^{2\pi i \langle \mathbf{y}, \mathbf{x} \rangle}$ is well-defined, since the above makes the series absolutely convergent. Furthermore, given the continuity of the terms, it is not hard to check that any such series must indeed yield a continuous function, and hence the continuity condition on f is necessary for achieving equality. Interestingly, the range of situations where convergence can be understood is much wider than the above theorem suggests. However, in the non-absolutely convergent setting one must carefully specify the order in which we sum the terms of the series. Fortunately, we will not require such delicate considerations here.

Periodizing Functions on $\mathbb{R}^n$. As can be seen above, Fourier analysis allows us to make an explicit link between the geometry of the torus, via the behavior of functions on it, and the dual lattice, via Fourier series. One may for example, attempt to study the behavior of the function $d(\mathcal{L}, \mathbf{t})$ for $\mathbf{t} \in \mathbb{R}^n/\mathcal{L}$, i.e. the distance from $\mathbf{t} + \mathcal{L}$ to $\mathcal{L}$, where the maximum is $\mu(\mathcal{L})$. Then, to prove transference, one might hope to extract an upper bound on $\mu(\mathcal{L})$ as a function of $\lambda_1(\mathcal{L}^*)$, by examining the Fourier series for $d(\mathcal{L}, \mathbf{t})$. While this is a natural approach, it is unclear how one could actually compute the Fourier coefficients of such a complex function, and thus derive the appropriate relations with $\lambda_1(\mathcal{L}^*)$ (we suspect such a proof can be made to work however and we encourage the reader to try).

Our approach will in fact be somewhat different. Instead of picking a very taylored or difficult to compute function of the torus, we will instead start with a class of "easy to compute with" functions on $\mathbb{R}^n$ that we will be able to analyze on any torus via periodization. More specifically, given any function $f : \mathbb{R}^n \to \mathbb{C}$ and full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, we may examine the periodic function

$$f(\mathcal{L} + \mathbf{t}) := \sum_{\mathbf{x} \in \mathcal{L}} f(\mathbf{x} + \mathbf{t}).$$

For the moment, it is unclear why such a periodization should be useful, in the sense that its corresponding Fourier coefficients on $\mathbb{R}^n/\mathcal{L}$ may still be very difficult to compute. Fortunately, it will turn out that if we know Fourier transform of f on $\mathbb{R}^n$, then we directly know the Fourier coefficients of a periodization of f on with respect to any lattice.

For a function $f : \mathbb{R}^n \to \mathbb{C}$, we define the n-dimensional Fourier transform $\widehat{f} : \mathbb{R}^n \to \mathbb{C}$ by

$$\widehat{f}(\mathbf{y}) = \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i \langle \mathbf{y}, \mathbf{x} \rangle} \mathrm{d}\mathbf{x}, \text{ for } \mathbf{y} \in \mathbb{R}^n \ . \tag{3}$$

As before, we can view evaluations of the Fourier transform as the inner product with characters.

Definition 15 *For $f, g : \mathbb{R}^n \to \mathbb{C}$, we define their inner product by $\langle f, g \rangle := \int_{\mathbb{R}^n} f(\mathbf{x}) \overline{g(\mathbf{x})} \mathrm{d}\mathbf{x}$. For $\mathbf{y} \in \mathbb{R}^n$ we define $\chi_{\mathbf{y}}(\mathbf{x}) := e^{2\pi i \langle \mathbf{y}, \mathbf{x} \rangle}$ to be the corresponding character. With these definitions, we note the identity $\widehat{f}(\mathbf{y}) = \langle f, \chi_{\mathbf{y}} \rangle$.*

The crucial relation for us in this setting, is that the Fourier coefficients of a perodization of f w.r.t. $\mathcal{L}$ and the Fourier transform of f restricted to $\mathcal{L}^*$, in fact coincide up to scaling. This is proven in the following lemma, under appropriate decay conditions on f.

Lemma 16 *Let $f : \mathbb{R}^n \to \mathbb{C}$ be a measurable function satisfying $|f(\mathbf{x})| \leq \frac{C}{(1+\|\mathbf{x}\|)^{n+\delta}}$, $\mathbf{x} \in \mathbb{R}^n$, for some $C, \delta > 0$. Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice and define $g(\mathbf{t}) := f(\mathcal{L} + \mathbf{t}) : \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$. Then for $\mathbf{y} \in \mathcal{L}^*$, we have that*

$$\widehat{g}(\mathbf{y}) = \frac{1}{\det(\mathcal{L})} \widehat{f}(\mathbf{y}) \ .$$

Proof: To begin, we leave as an exercise to show that the decay conditions on f imply that the sums $\sum_{\mathbf{x} \in \mathcal{L}} |f(\mathbf{x} + \mathbf{t})|$ are uniformly bounded $\forall \mathbf{t} \in \mathbb{R}^n$. This will allow us to arbitrarily rearrange such series as well as swap integrals and sums by applying the dominated convergence theorem.

From here, the statement is derived from the following computation:

$$\begin{aligned}
\widehat{g}(\mathbf{y}) &= \frac{1}{\det(\mathcal{L})} \int_D g(\mathbf{t}) e^{-2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \\
&= \frac{1}{\det(\mathcal{L})} \int_D \sum_{\mathbf{x} \in \mathcal{L}} f(\mathbf{x} + \mathbf{t}) e^{-2\pi i \langle \mathbf{y}, \mathbf{x} + \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \\
&= \frac{1}{\det(\mathcal{L})} \sum_{\mathbf{x} \in \mathcal{L}} \int_D f(\mathbf{x} + \mathbf{t}) e^{-2\pi i \langle \mathbf{y}, \mathbf{x} + \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \quad (\text{ by dominated convergence}) \\
&= \frac{1}{\det(\mathcal{L})} \sum_{\mathbf{x} \in \mathcal{L}} \int_{\mathbf{x} + D} f(\mathbf{t}) e^{-2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \\
&= \frac{1}{\det(\mathcal{L})} \int_{\mathbb{R}^n} f(\mathbf{t}) e^{-2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} \mathrm{d}\mathbf{t} \quad (\text{ by dominated convergence}) \\
&= \frac{1}{\det(\mathcal{L})} \widehat{f}(\mathbf{y}).
\end{aligned}$$

□

Now we are ready to prove the Poisson summation formula, which will be one of our main Fourier-analytic tools for studying lattices.

Theorem 17 *Let $f : \mathbb{R}^n \to \mathbb{C}$ be a continuous function satisfying for some $C, \delta > 0$, $\max(|\widehat{f}(\mathbf{x})|, |f(\mathbf{x})|) \leq \frac{C}{(1+\|\mathbf{x}\|)^{n+\delta}}$, $\forall \mathbf{x} \in \mathbb{R}^n$. Then, for a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, we have*

$$f(\mathcal{L} + \mathbf{t}) = \frac{1}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} \widehat{f}(\mathbf{y}) e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle}.$$

In particular,

$$f(\mathcal{L}) = \frac{1}{\det(\mathcal{L})} \widehat{f}(\mathcal{L}^*).$$

Proof: To begin, we leave it as an exercise to show that the continuity and decay assumptions on f imply that the periodization $g(\mathbf{t}) := f(\mathcal{L} + \mathbf{t})$, $\mathbf{t} \in \mathbb{R}^n / \mathcal{L}$, is continuous. As a second exercise, one can show that the decay conditions on $\widehat{f}$ imply that $\sum_{\mathbf{y} \in \mathcal{L}^*} |\widehat{f}(\mathbf{y})| < \infty$. Note that by Lemma 16, we have that $\widehat{g}(\mathbf{y}) = \frac{1}{\det(\mathcal{L})} \widehat{f}(\mathbf{y})$, $\forall \mathbf{y} \in \mathcal{L}^*$, and hence $\sum_{\mathbf{y} \in \mathcal{L}^*} |\widehat{g}(\mathbf{y})| < \infty$ also clearly holds. Since g now satisfies the conditions of Theorem 14, we get that

$$\begin{aligned}
f(\mathcal{L} + \mathbf{t}) &= g(\mathbf{t}) \\
&= \sum_{\mathbf{y} \in \mathcal{L}^*} \widehat{g}(\mathbf{y}) e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} \\
&= \frac{1}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} \widehat{f}(\mathbf{y}) e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle},
\end{aligned}$$

as needed. □

In the next class, we will use the Poisson summation formula on Gaussian density functions to recover optimal transference bounds.