Rise of the Duals and Transference

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

September, 2025

$VIII$

---

1 Introduction

The concept of dual is visible in many fields. For example in optimization we consider two problems one the maximization of profit and the second minimization of cost. One problem is called the primal problem and the other is called dual. In physics the dual nature of light is discussed i.e light has both particle and wave nature. Keeping this motivation in mind we will now jump into duals as some mathematical structures.

2 Dual Space and Dual Basis

2.1 Dual Space

For a given vector space V over a field $\mathbb{F}$, let V^* is the set of all linear transformations that take elements from V to some element of the field $\mathbb{F}$. Such linear transformations are called **functionals**. The set V^* forms a vector space over the same field $\mathbb{F}$ and we give it the name dual space.

Definition 2.1. **(Dual Space)** *Let V be a finite dimensional vector space over $\mathbb{R}$, then the dual space of V is defined as*

$$V^* = \{f | f : V \to \mathbb{R}, \textit{Linear Maps}\}$$

Example 2.2. *Let $V = \mathbb{R}^3$ and $\varphi : \mathbb{R}^3 \to \mathbb{R}$ then $\varphi(x, y, z) = 2x + 3y + 5z$ is a member of V^*.*

Example 2.3. *Let $V = P_n$ which is the set of all polynomials over $\mathbb{R}$ with degree n and $\varphi : P_n \to \mathbb{R}$ then $\varphi(p) = p(1)$ is a member of V^*.*
For instance, $\varphi(x^2 + 2x + 5) = 1^2 + 2 \cdot 1 + 5 = 8$

Example 2.4. *Let $V = M_{n\times n}$ which is the set of all $n \times n$ matrices over $\mathbb{R}$ and $\varphi : M_{n\times n} \to \mathbb{R}$ then $\varphi(A) = trace(A)$ is a member of V^*.*
For instance,

$$\varphi\left(\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}\right) = 1 + 5 = 6$$

Example 2.5. *Let $V = C([0, 1])$ be the set of all continuous functions on the interval $[0, 1]$ and $\varphi : C[0, 1] \to \mathbb{R}$ then $\varphi(f) = \int_0^1 f(x)\, dx$ is a member of V^*.*
For instance,

$$\varphi\left(\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}\right) = 1 + 5 = 6$$

2.2 Dual Basis

Let $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ is a basis for vector space V, then the basis of its dual space V^* is $B^* = \{\mathbf{d_1}, \mathbf{d_2}, \cdots, \mathbf{d_n}\}$ if we identify them as

$$f_{d_i}(\underbrace{c_1\mathbf{b_1} + c_2\mathbf{b_2} + \cdots + c_n\mathbf{b_n}}_{c_i \in \mathbb{R}}) = c_i, \qquad i = 1, 2, \cdots, n$$

Another way to write the above relation is $f_{d_i}(b_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$
Then any functional can be written as a linear combination of the the dual basis

$$f = \alpha_1 f_{d_1} + \alpha_2 f_{d_2} + \cdots + \alpha_n f_{d_n}$$

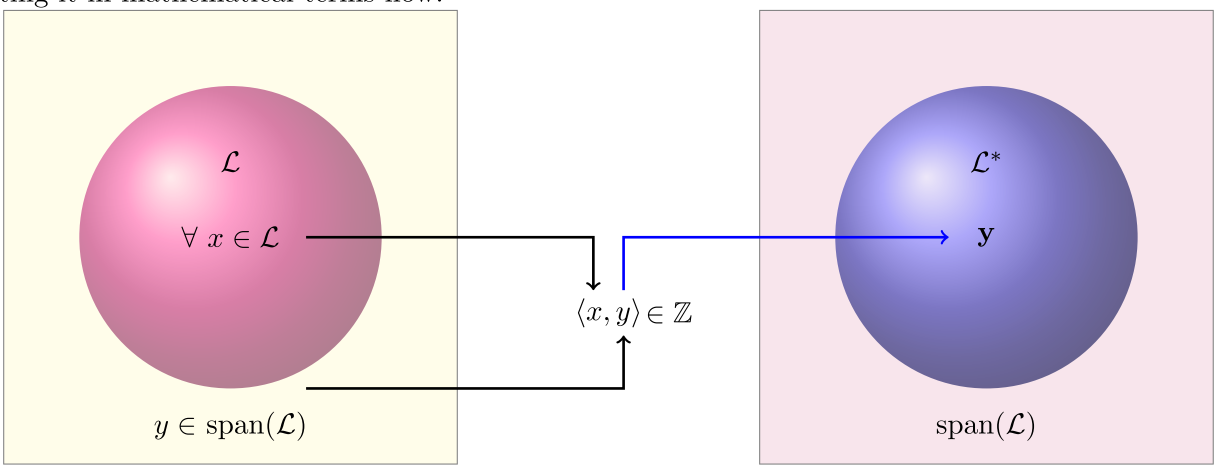
A homomorphism between V and V^* is

$$\phi : V \to V^*, \quad \mathbf{v} \mapsto \langle \cdot, \mathbf{v} \rangle$$

Note: V^* is a vector space where vectors are linear maps.

3 Dual Lattice

The dual lattice which is sometimes also refered as reciprocal lattice is thet set of points in the span of $\mathcal{L}$ such that its inner product with any lattice vector is always an integer. We will be writing it in mathematical terms now.



Definition 3.1. **(Dual Lattice)** *Let $\mathcal{L}$ be a lattice, then the dual lattice $\mathcal{L}^*$ is defined as*

$$\mathcal{L}^* = \{f | f : \mathcal{L} \to \mathbb{Z}, \textit{Linear Maps } (\ \mathbb{R}\text{−}\textit{linear}\ )\}$$

Definition 3.2. *Let $\mathcal{L} = \mathcal{L}(B)$ then the dual lattice $\mathcal{L}^*$ is defined as*

$$\mathcal{L}^* = \{\mathbf{y} \in \textit{span}(\mathcal{L}) |\ \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{x} \in \mathcal{L}\}$$

equivalently,

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

Definition 3.3. *Let $\mathcal{L} \subseteq \mathbb{R}^n$ we define $\mathcal{L}^* \subseteq (\mathbb{R}^n)^*$ as lattice of all linear maps $f : \mathbb{R}^n \to \mathbb{R}$ such that $f(\mathcal{L}) \subseteq \mathbb{Z}$*

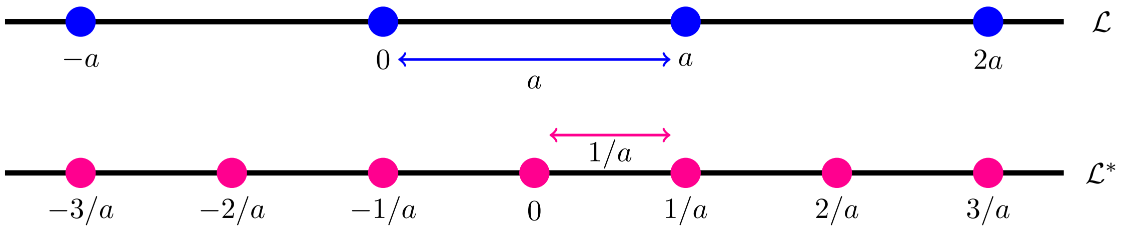


Figure 1: Lattice and its dual

Definition 3.4. *Let $\mathcal{L} \subseteq \mathbb{R}^n$ then the dual lattice $\mathcal{L}^* \subseteq (\mathbb{R}^n)^*$ is defined as*

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

equivalently,

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

Example 3.5. *Lattice and their duals*

$\mathcal{L}$	$\mathcal{L}^*$
$\mathbb{Z}$	$\mathbb{Z}$
$2\mathbb{Z}$	$\frac{1}{2}\mathbb{Z}$
$\mathbb{Z}^n$	$\mathbb{Z}^n$
$2\mathbb{Z}^n$	$\frac{1}{2}\mathbb{Z}^n$
Stretch	Compress
Rotate	Rotate
Dense	Sparse
Short Vector	Long Direction

4 Lattice Dual Basis

Let $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ is a basis for lattice $\mathcal{L}$, then the basis of its dual $\mathcal{L}^*$ is $D = \{\mathbf{d_1}, \mathbf{d_2}, \cdots, \mathbf{d_n}\}$ if we identify them as

$$f_{d_i}(\underbrace{c_1\mathbf{b_1} + c_2\mathbf{b_2} + \cdots + c_n\mathbf{b_n}}_{c_i \in \mathbb{Z}}) = c_i, \qquad i = 1, 2, \cdots, n$$

Another way to write the above relation is $f_{d_i}(b_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$
Then any dual lattice element can be written as an integer linear combination of the dual basis elements

$$\begin{aligned} f &= \alpha_1 f_{d_1} + \alpha_2 f_{d_2} + \cdots + \alpha_n f_{d_n} \\ &= \begin{bmatrix} f_{d_1} & f_{d_2} & \cdots & f_{d_n} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \end{aligned}$$

and now the dual lattice $\mathcal{L}^*$ can be represented as

$$\mathcal{L}^* = \{Dx | x \in \mathbb{Z}^n\}$$

Definition 4.1. *Let $B = [\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}]$ be basis of lattice $\mathcal{L}$ and $D = [\mathbf{d_1}, \mathbf{d_2}, \cdots, \mathbf{d_n}]$ be unique dual basis that satisfies*

- $\text{span}(D) = \text{span}(B)$
- $B^T D = I$

The second condition can also be written as $\langle \mathbf{b_i}, \mathbf{d_j} \rangle = \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$

Also since we have $B^T D = I$ so we have $D = B^{-T}$
With this definition the number of basis elements in $\mathcal{L}$, i.e rank of $\mathcal{L}$ is always same as that of $\mathcal{L}^*$.

Result 4.2. *Let B be a non square matrix that serves as a the basis of a lattice $\mathcal{L}$, then the basis of the dual $\mathcal{L}^*$ is $D = B(B^T B)^{-1}$*

5 Some Dual Theorems

Theorems that relate lattice to its duals are known as transference theorems, we will quickly prove some of them.

Theorem 5.1. *If D is the dual basis of B then $(\mathcal{L}(B))^* = \mathcal{L}(D)$*

Proof. Let $x \in \mathcal{L}(B)$ so we can express it as $\mathbf{x} = a_1\mathbf{b_1} + a_2\mathbf{b_2} + \cdots a_n\mathbf{b_n}$ for some $a_i \in \mathbb{Z}$. Therefore for any $1 \leq j \leq n$ we have the following

$$\begin{aligned}
\langle \mathbf{x}, \mathbf{d_j} \rangle &= \langle a_1\mathbf{b_1} + a_2\mathbf{b_2} + \cdots + a_n\mathbf{b_n}, \mathbf{d_j} \rangle \\
&= \langle a_1\mathbf{b_1}, \mathbf{d_j} \rangle + \langle a_2\mathbf{b_2}, \mathbf{d_j} \rangle + \cdots + \langle a_j\mathbf{b_j}, \mathbf{d_j} \rangle + \cdots + \langle a_n\mathbf{b_n}, \mathbf{d_j} \rangle \\
&= a_1 \langle \mathbf{b_1}, \mathbf{d_j} \rangle + a_2 \langle \mathbf{b_2}, \mathbf{d_j} \rangle + \cdots + a_j \langle \mathbf{b_j}, \mathbf{d_j} \rangle + \cdots + a_n \langle \mathbf{b_n}, \mathbf{d_j} \rangle \\
&= a_1\delta_{1j} + a_2\delta_{2j} + \cdots + a_j\delta_{jj} + a_n\delta_{nj} \\
&= a_1 0 + a_2 0 + \cdots + a_j 1 + a_n 0 \\
&= a_j
\end{aligned}$$

and we get $D \subseteq (\mathcal{L}(B))^*$. It is also true that $(\mathcal{L}(B))^*$ is closed under addition so we get $\mathcal{L}(D) \subseteq (\mathcal{L}(B))^*$
Now we just have to show that $\mathcal{L}(D) \subseteq (\mathcal{L}(B))^*$
Consider $y \in (\mathcal{L}(B))^*$. Since we have $y \in \text{span}(B)$ =span(D)
$\mathbf{y} = \alpha_1\mathbf{d_1} + \alpha_2\mathbf{d_2} + \cdots \alpha_n\mathbf{d_n}$ for some $\alpha_i \in \mathbb{R}$.
Now for all $1 \leq j \leq n$

$$\begin{aligned}
\mathbb{Z} \ni \langle \mathbf{y}, \mathbf{b_j} \rangle &= \langle \alpha_1\mathbf{d_1} + \alpha_2\mathbf{d_2} + \cdots \alpha_n\mathbf{d_n}, \mathbf{b_j} \rangle \\
&= \langle \alpha_1\mathbf{b_1}, \mathbf{d_j} \rangle + \langle \alpha_2\mathbf{b_2}, \mathbf{d_j} \rangle + \cdots + \langle \alpha_j\mathbf{b_j}, \mathbf{d_j} \rangle + \langle \alpha_n\mathbf{b_n}, \mathbf{d_j} \rangle \\
&= \alpha_1 \langle \mathbf{b_1}, \mathbf{d_j} \rangle + \alpha_2 \langle \mathbf{b_2}, \mathbf{d_j} \rangle + \cdots + a_j \langle \mathbf{b_j}, \mathbf{d_j} \rangle + \alpha_n \langle \mathbf{b_n}, \mathbf{d_j} \rangle \\
&= \alpha_1\delta_{1j} + \alpha_2\delta_{2j} + \cdots + \alpha_j\delta_{jj} + \alpha_n\delta_{nj} \\
&= \alpha_1 0 + \alpha_2 0 + \cdots + \alpha_j 1 + \alpha_n 0 \\
&= \alpha_j
\end{aligned}$$

Hence, $y \in \mathcal{L}(D)$ and this completes the proof. □

Theorem 5.2. *For any lattice $\mathcal{L}$ let $\mathcal{L}^*$ be its dual, then $(\mathcal{L}^*)^* = \mathcal{L}$. In words, the dual of the dual is the primal itself.*

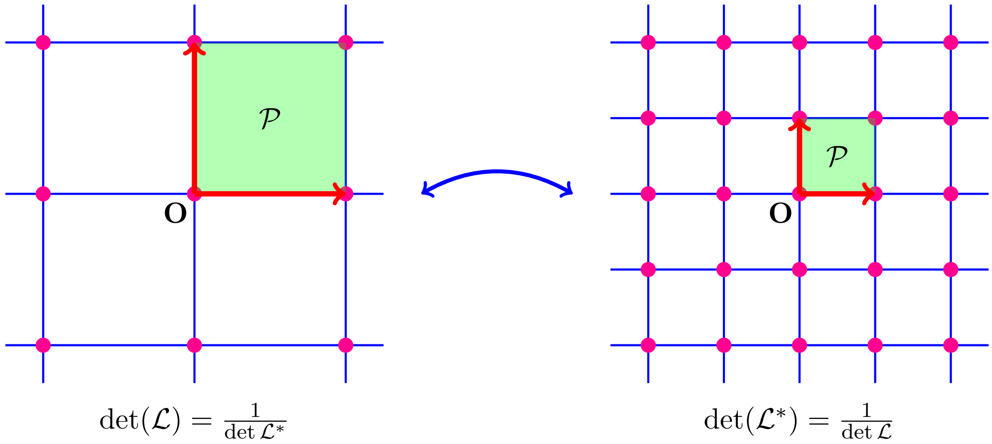


Figure 2: Illustration taht shows relationship between volume of dual lattice and primal lattice

Proof. We have the following result that for a lattice $\mathcal{L} = \mathcal{L}(B)$ the dual lattice can be written as $\mathcal{L}^* = (\mathcal{L}(B))^* = \mathcal{L}(B^{-T})$
Applying the same to $((\mathcal{L}(B))^*)^*$ we get $((\mathcal{L}(B))^*)^* = (\mathcal{L}(B^{-T}))^* = \mathcal{L}((B^{-T})^{-T}) = \mathcal{L}(B)$ □

Theorem 5.3. *For any lattice $\mathcal{L}$ let $\mathcal{L}^*$ be its dual, then*

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

Proof.

$$\det(\mathcal{L}^*) = |\det(B^{-T})| = \left|\frac{1}{\det(B^T)}\right| = \left|\frac{1}{\det(B)}\right| = \frac{1}{\det(\mathcal{L})}$$

□

The above theorem says that the volume of parallelepiped of dual is reciprocal of the volume of parallelepiped of the primal. Thus, the name reciprocal lattice for dual lattice is justified.

6 Transference Theorems

A property of lattice and its dual connected together is called a transference and the theorems of such kinds are called transference theorems. A transference theorem gives some relationship between primal and dual lattices. For example $\det(\mathcal{L}) \times \det(\mathcal{L}^*) = 1$ is a transference theorem.

Theorem 6.1. *For any full rank lattice of rank n we have*

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

Proof. We will use Minkowski's first theorem that we established earlier.

Minkowski's First Theorem
For any full rank lattice $\mathcal{L}$ of rank n we have $\lambda_1(\mathcal{L}) \leq \sqrt{n}(\det(\mathcal{L}))^{1/n}$

Minkowski's first theorem on $\mathcal{L}$ gives $\lambda_1(\mathcal{L}) \leq \sqrt{n}(\det(\mathcal{L}))^{1/n}$
Minkowski's first theorem on $\mathcal{L}^*$ gives $\lambda_1(\mathcal{L}^*) \leq \sqrt{n}(\det(\mathcal{L}^*))^{1/n}$
Now we have

$$\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \leq \sqrt{n}(\det(\mathcal{L}))^{1/n} \times \sqrt{n}(\det(\mathcal{L}^*))^{1/n} \leq n$$

□

Theorem 6.2. *For any full rank lattice of rank n we have*

$$1 \le \lambda_1(\mathcal{L}) \cdot \lambda_n(\mathcal{L}^*) \le n$$

Proof. We will prove one part $1 \le \lambda_1(\mathcal{L}) \cdot \lambda_n(\mathcal{L}^*)$
Let $\mathbf{v}$ be a short vector in $\mathcal{L}$, then we have $\lambda_1(\mathcal{L}) = \|\mathbf{v}\|$.
Now consider $\mathbf{y_1}, \mathbf{y_2}, \cdots, \mathbf{y_n}$ be n linearly independent vectors in $\mathcal{L}^*$ and not all of them are orthogonal to $\mathbf{v}$.
Thus, we must get some i for which $\langle \mathbf{y_i}, \mathbf{v} \rangle \neq 0$.
Also since $\langle \mathbf{y_i}, \mathbf{v} \rangle \in \mathbb{Z}$, we can apply Cauchy Schwarx inequality as follows

$$1 \le |\langle \mathbf{y_i}, \mathbf{v} \rangle|^2 \le \|\mathbf{y_i}\|^2 \|\mathbf{v}\|^2 \le \lambda_n(\mathcal{L}^*)^2 \lambda_1(\mathcal{L})^2$$

and finally we get, $\lambda_1(\mathcal{L}) \cdot \lambda_n(\mathcal{L}^*) \ge 1$ □

Theorem 6.3. *For a lattice $\mathcal{L} \subset \mathbb{R}^n$ we have, $\lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^*) \ge 1$*

Proof. Let $\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_{n-i+1}} \in \mathcal{L}^*$ be linearly independent vectors such that

$$\begin{gathered} \lambda_1(\mathcal{L}^*) = \|v_1\| \\ \lambda_2(\mathcal{L}^*) = \|v_2\| \\ \vdots \\ \lambda_{n-i+1}(\mathcal{L}^*) = \|v_{n-i+1}\| \end{gathered}$$

and for any value $1 \le k_1 \le n - i + 1$ we will have $\|v_{k_1}\| \le \|v_{n-i+1}\|$

Let $\mathbf{y_1}, \mathbf{y_2}, \cdots, \mathbf{y_i} \in \mathcal{L}$ be linearly independent vectors such that

$$\begin{gathered} \lambda_1(\mathcal{L}) = \|y_1\| \\ \lambda_2(\mathcal{L}) = \|y_2\| \\ \vdots \\ \lambda_i(\mathcal{L}) = \|y_i\| \end{gathered}$$

and for any value $1 \le k_2 \le i$ we will have $\|y_{k_2}\| \le \|v_i\|$
By counting we argue that the span of $\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_{n-i+1}}$ and span of $\mathbf{y_1}, \mathbf{y_2}, \cdots, \mathbf{y_i}$ has a nontrivial intersection. Hence, we will end up getting two indices k_1 and k_2 such that $|\langle v_{k_1}, y_{k_2} \rangle| > 0$.
For integer lattices we will have $|\langle v_{k_1}, y_{k_2} \rangle| \ge 1$ By Cauchy Schwartz inequality we get

$$1 \le |\langle v_{k_1}, y_{k_2} \rangle| \le \|v_{k_1}\| \|y_{k_2}\| \le \|v_{n-i+1}\| \|v_i\| \le \lambda_{n-i+1}(\mathcal{L}^*)\lambda_i(\mathcal{L})$$

This completes the proof that $\lambda_{n-i+1}(\mathcal{L}^*)\lambda_i(\mathcal{L}) \ge 1$ □

Definition 6.4. (Covering Radius) *For a full rank lattice $\mathcal{L}$ the covering radius of $\mathcal{L}$ is defined as*

$$\mu(\mathcal{L}) = \max_{x \in \mathbb{R}^n} dist(x, \mathcal{L})$$

In other words, the covering radius of a lattice is the minimum value of r such that any point is within distance at most r from lattice.

Moreover we can also think of it as a sphere packing, i.e. the minimum radius of sphere applicable so that any each sphere centred at lattice points such that they are disjoint.
The covering radius of $\mathbb{Z}^n$ is $\mu(\mathbb{Z}^n) = \sqrt{n}/2$.

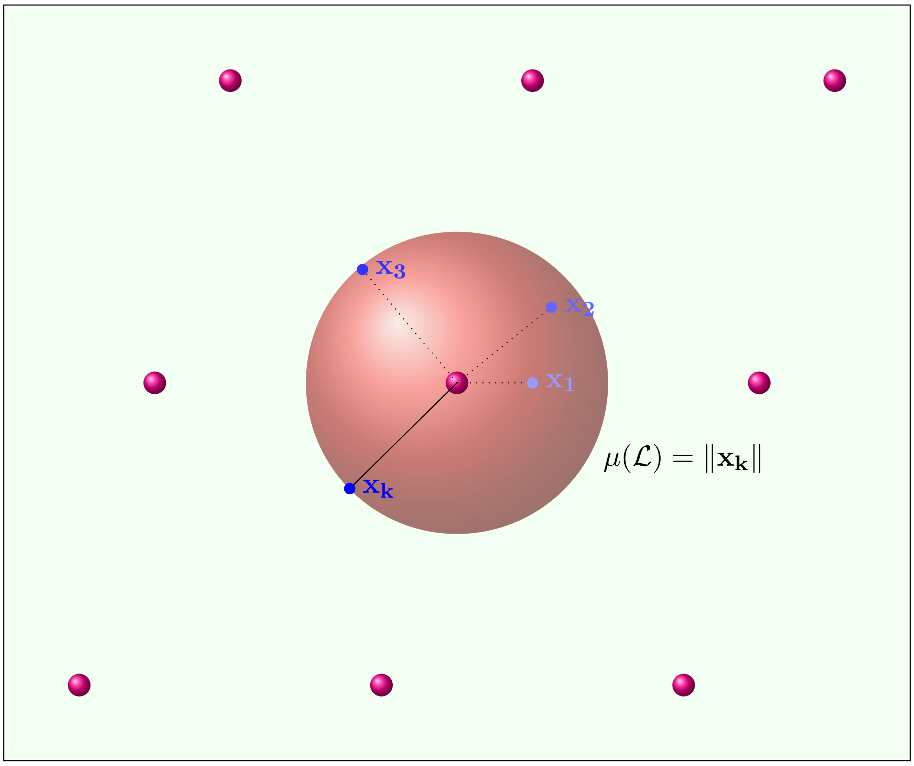


Figure 3: The Covering Radius

Theorem 6.5. *For a full rank lattice* $\mu(\mathcal{L}) \geq \frac{\lambda_n(\mathcal{L})}{2}$

Proof.

$$\lambda_i = \inf\{r > 0 : B(0, r) \cap \mathcal{L} \text{ contains at least } i \text{ linearly independent short vectors}\}$$

We have $B(0, \lambda_n)$ which contains all lattice points in a hyperplane of dimension $(n - 1)$.
Now choose a point $\mathbf{x}$ at a distance $\lambda_n/2$ from the origin taken in the orthogonal direction from the hyperplane.
In the best case is $\mathbf{x}$ must be at a distance $\lambda/2$ from any lattice point inside this ball and it can even be farther.
So we finally conclude

$$\|\mathbf{x}\| \geq \frac{\lambda_n}{2}$$

or,

$$\mu(\mathcal{L}) \geq \frac{\lambda_n}{2}$$

□

Result 6.6. *For a linear subspace* $W \subsetneq \mathbb{R}^n$ *and full rank lattice* $\mathcal{L} \subset \mathbb{R}^n$*, there exists* $v \notin W$ *and* $v \in \mathcal{L}$ *such that* $\|v\| \leq 2\mu(\mathcal{L})$

Result 6.7. *(theorem 4 in oded) For a full rank lattice* $\lambda_1(\mathcal{L}) \cdot \mu(\mathcal{L}^*) \leq n$

Theorem 6.8. *For a lattice* $\mathcal{L}$ *of rank at least* 1 $\mu(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \geq 1/2$

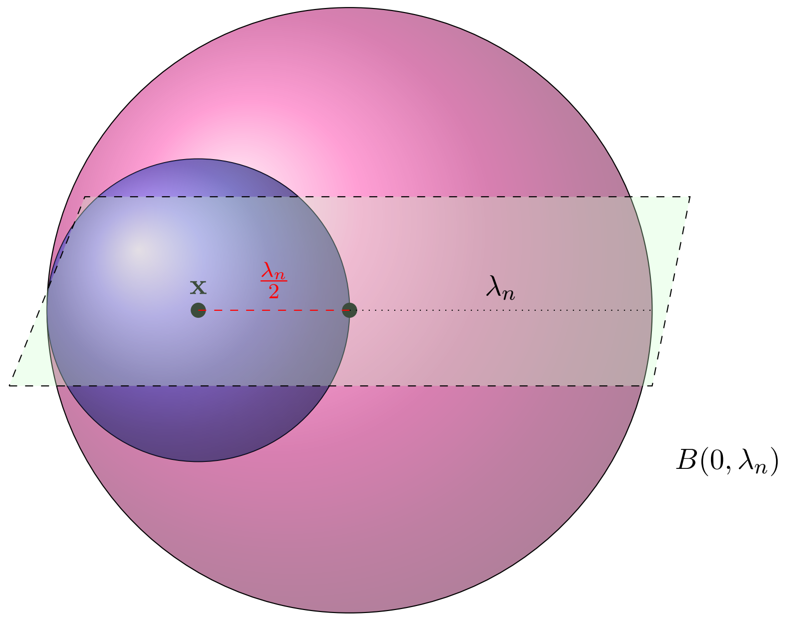


Figure 4: $\mu(\mathcal{L}) \geq \frac{\lambda_n}{2}$

Proof. Let $\mathbf{y} \in \mathcal{L}^*$ be a short vector in lattice, so $\|\mathbf{y}\| = \lambda_1(\mathcal{L}^*)$
Now for any $\mathbf{x} \in \mathcal{L}$ it must satisfy $\langle \mathbf{y}, \mathbf{x} \rangle \in \mathbb{Z}$.
Now we have a set of hyperplanes

$$H_i = \{x \in \mathbb{R}^n \mid \langle \mathbf{y}, \mathbf{x} \rangle = i\}$$

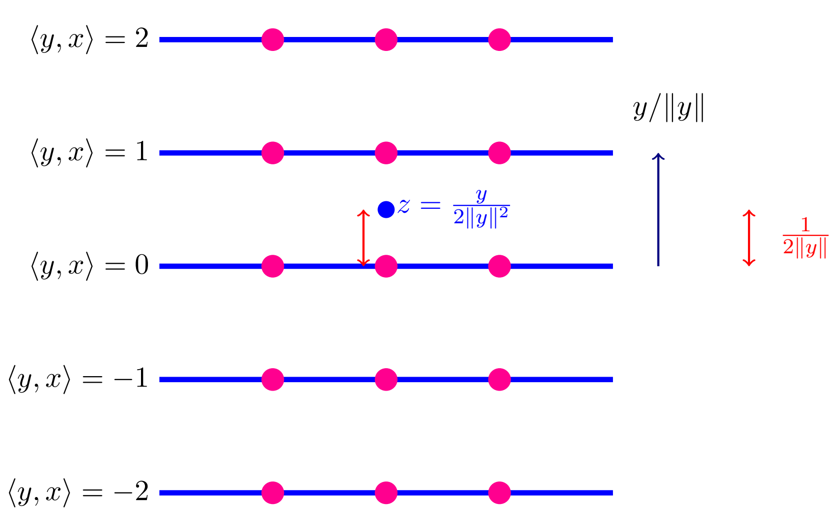
and

$$\mathcal{L} \subset \cup_{i \in \mathbb{Z}} H_i$$

Each H_i and H_{i+1} is separated by a distance $1/\|y\|$ because moving in the direction of $y/\|y\|$ by $1/\|y\|$ increases the inner product $\langle y, x \rangle$ by 1.
Choose a point $\mathbf{z}$ halfway along this direction $\mathbf{z} = \frac{\mathbf{y}}{2\|\mathbf{y}\|^2}$

$$\operatorname{dist}(\mathcal{L}, \mathbf{z}) \geq \frac{\min_{\mathbf{x} \in \mathcal{L}} |\langle \mathbf{z} - \mathbf{x}, \mathbf{y} \rangle|}{\|\mathbf{y}\|} = \min_{\mathbf{z} \in \mathbb{Z}} \frac{\left|\frac{1}{2} - \mathbf{z}\right|}{\|\mathbf{y}\|} = \frac{1}{2\|\mathbf{y}\|} = \frac{1}{2\lambda_1(\mathcal{L}^*)}$$

□



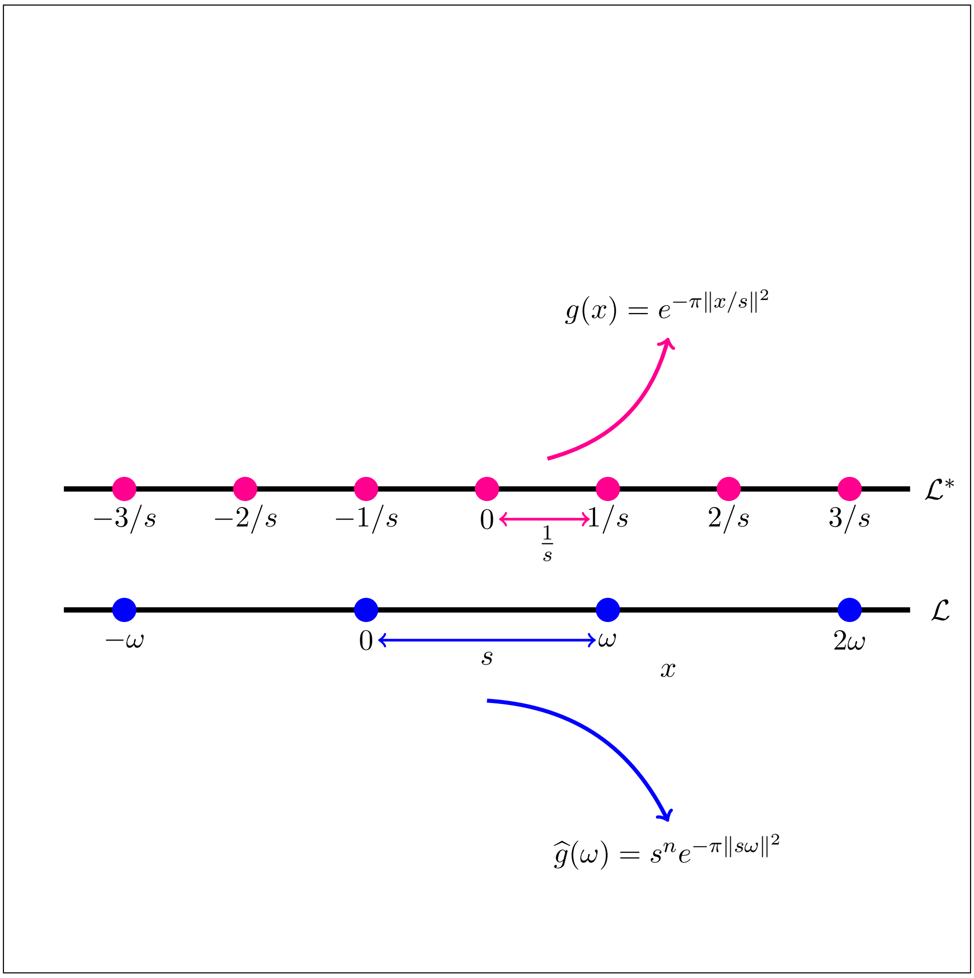


Figure 5: Realizing $\hat{g}$ and g are similar to dual and primal lattice

7 Fourier in Lattice

A lattice $\mathcal{L} \subset \mathbb{R}^n$ is a countable set, using this fact we can use the periodization technique to make any function periodic. Such periodic function we will call $\mathcal{L}-$periodic. After achieving this periodicity in lattices we can go ahead with computing the Fourier series. A function that we would use very often is $f(x) = e^{-\pi\|x\|^2}$. We already know that the Fourier transform of this function is $\hat{f}(\omega) = e^{-\pi\|\omega\|^2}$. Keeping all these things into account we go ahead towards utilizing Fourier analysis in $\mathcal{L}$.

Definition 7.1. **($\mathcal{L}-$Periodic Function)** *Let $g : \mathbb{R} \to \mathbb{C}$ we call it $\mathcal{L}$ periodic if*

$$g(x) = g(x + \mathbf{v}) \quad \forall\ \mathbf{v} \in \mathcal{L}$$

Definition 7.2. **(Fourier Series)** *For a $\mathcal{L}-$periodic function $g : \mathbb{R} \to \mathbb{C}$ its Fourier series is defined as*

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

Where,

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

Definition 7.3. **(Fourier Transform)**

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

For $g(x) = e^{-\pi \|x/s\|^2}$ we will have $\widehat{g}(\omega) = s^n e^{-\pi \|s\omega\|^2}$ by the time scaling property.

Theorem 7.4. **(Poisson Summation Formula)**
For any $f \in L^1(\mathbb{R}^n)$ *we have* $f(\mathcal{L}) = \det(\mathcal{L}^*) \widehat{f}(\mathcal{L}^*)$ *or equivalently,*

$$\boxed{\sum_{k \in \mathcal{L}} f(k) = \det(\mathcal{L}^*) \sum_{\omega \in \mathcal{L}^*} \widehat{f}(\omega)}$$

or,

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

Result 7.5. *For any* $f \in L^1(\mathbb{R}^n)$ *we have,*

$$\boxed{\sum_{k \in \mathcal{L}} f(\mathbf{x} + \mathbf{k}) = \det(\mathcal{L}^*) \sum_{\omega \in \mathcal{L}^*} \widehat{f}(\omega) e^{2\pi i \langle \mathbf{x}, \mathbf{w} \rangle}}$$

References

[Mic14] Daniel Micciancio. *Lecture Notes on Lattices Algorithms and Applications*. 2014. URL: https://cseweb.ucsd.edu/classes/sp14/cse206A-a/.

[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.