

Basic Definitions:

A lattice $\mathcal{L} \subset \mathbb{R}^n$ is a discrete additive subgroup of \mathbb{R}^n .

For linearly independent $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$, $\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_k) = \{\sum_{i=1}^k a_i \mathbf{b}_i : a_i \in \mathbb{Z}, i \in [k]\}$.

B_2^n is the unit Euclidean ball in \mathbb{R}^n .

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{y} \in \mathcal{L} \setminus \{0\}} \|\mathbf{y}\|.$$

Exercise 1 Let $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$ be linearly independent vectors. The dual basis $\mathbf{b}_1^*, \dots, \mathbf{b}_k^*$ is the unique set of vectors satisfying $\mathbf{b}_1^*, \dots, \mathbf{b}_k^* \in \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_k)$, $\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = 1$ if $i = j$ and 0 otherwise. Give an explicit matrix theoretic formula for computing the dual basis and prove its correctness (note that this is trivial when $k = n$).

Exercise 2 (Packing Bounds) Show that $|\mathcal{L} \cap rB_2^n| \leq (\frac{2r}{\lambda_1} + 1)^n$ for any $r > 0$.

(Hint: show that balls of radius $\lambda_1(\mathcal{L})/2$ placed around points of \mathcal{L} are interior disjoint)

Exercise 3 If $\mathcal{L} \subset \mathbb{R}^n$ is a lattice show that $\mathcal{L}^* = \{\mathbf{x} \in \text{span}(\mathcal{L}) : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{y} \in \mathcal{L}\}$ is a lattice and that $\mathcal{L}^{**} = \mathcal{L}$.

Exercise 4 Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and let $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$ denote a basis of a sublattice $M := \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_k)$ of Λ satisfying $M = \Lambda \cap \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_k)$. Show that $\mathbf{b}_1, \dots, \mathbf{b}_k$ can be extended to a basis of Λ .