

**Definitions:**

For a non-singular matrix  $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_k) \in \mathbb{R}^{n \times k}$  define the parallelepiped

$$\mathcal{P}(\mathbf{b}_1, \dots, \mathbf{b}_k) := \mathcal{P}(B) = B[0, 1)^k.$$

For a lattice  $\mathcal{L} \subset \mathbb{R}^n$  define its (closed) Voronoi cell as

$$\mathcal{V}(\mathcal{L}) := \{\mathbf{x} \in \text{span}(\mathcal{L}) : \|\mathbf{x}\| \leq \|\mathbf{x} - \mathbf{y}\|, \forall \mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}\}.$$

**Exercise 1** Let  $\mathcal{L} \subset \mathbb{R}^n$  denote a full rank lattice. Let  $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathcal{L}$  be linearly independent vectors. Show  $\mathbf{b}_1, \dots, \mathbf{b}_n$  are a basis of  $\mathcal{L}$  if and only if  $\mathcal{P}(\mathbf{b}_1, \dots, \mathbf{b}_n) \cap \mathcal{L} = \{\mathbf{0}\}$ .

**Exercise 2** Let  $\mathcal{L}_1 \subset \mathbb{R}^n$  be full rank lattice and let  $\mathcal{L}_2 \subset \mathcal{L}_1$  denote a full rank sublattice. Show that the index  $[\mathcal{L}_1 : \mathcal{L}_2] = \frac{\det(\mathcal{L}_2)}{\det(\mathcal{L}_1)}$  (recall that  $[\mathcal{L}_1 : \mathcal{L}_2] = |\mathcal{L}_1 / \mathcal{L}_2|$ ).  
(Hint: Take a fundamental domains  $D_1, D_2$  of  $\mathcal{L}_1, \mathcal{L}_2$  respectively, and write the volume of  $D_2$  as an integral over lattice point counts over  $D_1$ .)

**Exercise 3** Let  $\mathcal{L} \subset \mathbb{R}^n$  be a full rank lattice with basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$ . Let  $U \sim \text{uniform}(\mathcal{P}(\mathbf{b}_1, \dots, \mathbf{b}_n))$  be uniformly distributed over the fundamental parallelepiped. Let  $Z = U - \text{CVP}(\mathcal{L}, U)$ , where  $\text{CVP}(\mathcal{L}, U)$  denotes the closest vector to  $U$  in  $\mathcal{L}$  (note that this is well-defined w.p. 1). Show that  $Z$  is uniformly distributed over the Voronoi cell  $\mathcal{V}(\mathcal{L})$ .

**Exercise 4** Let  $\mathcal{L} \subset \mathbb{R}^n$  denote a full rank lattice. Define

$$\lambda_1(B_1^n, \mathcal{L}) := \min_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|_1,$$

where  $\|\mathbf{y}\|_1 = \sum_{i=1}^n |y_i|$  is the  $\ell_1$  norm and  $B_1^n = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|_1 \leq 1\}$  is the  $\ell_1$  ball. Show that  $\lambda_1(B_1^n, \mathcal{L}) \leq n \cdot \det(\mathcal{L})^{1/n}$ .

(Hint: Minkowski's Convex Body Theorem)