Lattices I – Introduction

Tomáš Kobrle

My task to this presentation is introduce you to the theory of lattices in $\mathbb{R}^n$. After definition of the term and important parameters of lattice we focus on equivalency of bases of lattices and upper bound of parameter known as first succesive minimum in Minkowski Theorem. Finally I will mention some computational problems of lattice like the shortest vector problem or the closest vector problem.

Definition 1. Let $v_1, \ldots, v_m$ be linearly independent vectors in $\mathbb{R}^n$ and B be a matrix whose columns are $v_1, \ldots, v_m$ then a set of points

$$L(B) = \{Bx \,|\, x \in \mathbb{Z}^m\}$$

is called **lattice** generated by the vectors $v_1, \ldots, v_m$, the matrix B is called basis matrix of lattice. If $m = n$, the lattice is called full-rank.

Definition 2. *Fundamental Parallelepiped* of a lattice $L(B)$ is

$$P(B) = \{By \,|\, y \in [0,1)^n\}$$

Definition 3. For a lattice $L(B)$ we define *determinant* of L as $\det L(B) = |\det B|$.

Definition 4. For a lattice $L(B)$ we define *k-th succesive minimum* $\lambda_k(L)$ as the smallest radius of a closed ball containing k linearly independent vectors in L.

Lemma 5. *Lattices $L(B_1)$ and $L(B_2)$ are the same if and only if*

$$\det L(B_1) = \det L(B_2).$$

Theorem 6 (Blichfeld)**.** *For lattice L and set $S \subseteq \mathbb{R}^n$ with $\mathrm{vol}(S) > \det L$ there exist nonequal points z_1, z_2 in S such that $z_1 - z_2 \in L$.*

Theorem 7 (Minkowski Theorem)**.** *Let L be full-rank lattice of rank n, then*

$$\lambda_1(L) \leq \sqrt{n}\,(\det L)^{1/n}.$$

Hard computational problems with variants:

- Find the shortest nonzero vector in lattice—SVP Given a basis B of lattice L find vector $v \in L(B)$ such that $\|v\| = \lambda_1(L(B))$.
- Find n shortest independant vectors in lattice—SIVP Given a basis B find n linearly independant vectors in $L(B)$ of lenght $\leq \lambda_n(L(B))$.
- Find the lattice point which is the closest to given point—CVP
  Search: Given a basis and vector z, find $v \in L(B)$