Integer Optimization
Problem Set 9

Presentations: May 15

i) Let $B \in \mathbb{R}^{n\times n}$ be a non-singular lattice. The *orthogonality defect* of B is $\gamma = \prod_{i-1}^{n} \|b_i\| / |\det(B)|$, where b_i is the i-th column of B.

   Show that the orthogonality defect of an LLL-reduced lattice basis B is bounded by $2^{n^2/2}$.

ii) Show how to retrieve a shortest nonzero vector of a lattice $\Lambda(B) \subseteq \mathbb{R}^n$ in time $(2\gamma+1)^n$, where γ is the orthogonality defect of B. Conclude that the shortest vector problem for a lattice Λ spanned by $B \in \mathbb{Z}^{n\times n}$ can be solved in time $2^{O(n^3)}$ times a polynomial in the size of B.

iii) Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. The *Voronoi cell* of Λ is the set of points

$$\mathscr{V}(\Lambda) = \{x \in \mathbb{R}^n \colon \forall v \in \Lambda \colon \|x\| \leqslant \|x - v\|\}.$$

   Show that $\mathscr{V}(\Lambda)$ is a polytope.

iv) Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Show that the number of lattice points of euclidean norm bounded by R is at most

$$\left(\frac{R+\rho(\Lambda)}{\rho(\Lambda)}\right)^n.$$

v) Show that $\mathscr{V}(\Lambda)$ can be described by $2^{O(n)}$ inequalities.

   Hint: Consider parities (mod 2).

vi) Use Minkowski's theorem to show the following result of Dirichlet:

   Let $Q \geqslant 1$ be a real number and let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$. There exists an integer q and integers $p_1, \dots, p_n$ with

   a) $1 \leqslant q \leqslant Q^n$ and
   b) $|q \cdot \alpha_i - p_i| \leqslant 1/Q$ for $i = 1, \dots, n$.