# Integer Optimization
# Problem Set 10

Presentations: May 22

i) For a lattice $\Lambda$ let us write $SVP(\Lambda)$ and $CVP(\Lambda, t)$ as the values of the shortest vector and closest vector problems. We have seen in an earlier exercise that for any lattice $\Lambda$, the number of lattice vectors of length, say $2 \cdot SVP(\Lambda)$ is bounded by $2^{O(n)}$. Here we want to show that this is not true anymore for CVP. To be precise, for any function $f(n)$, construct a lattice in $n$ dimensions and a point $t$ so that

$$|\{x \in \Lambda | \|x - t\|_2 \leqslant 2 \cdot CVP(\Lambda, t)\}| \geqslant f(n)$$

ii) Let $t \in \mathbb{R}^n$ and $L \subseteq \mathbb{R}^n$ a lattice. The goal of the closest vector problem (CVP) is to find a closest lattice vector to $t$, e.g. finding $c \in L$ such that $\|t - c\|_2 = \min_{w \in L} \|t - w\|_2$. Assume that you are given a vector $u \in L^*$ (the dual of L) such that $\|u\|_2 > 2 \cdot \|t\|_2$. Find a lattice $L' \subseteq \mathbb{R}^{n-1}$ such that finding the closest vector to $t$ on $L$ is equivalent to solving a closest vector problem on $L'$ and prove why this is so.

iii) Given a lattice $\Lambda$, we denote by $\lambda_k(\Lambda) \in \mathbb{R}_{>0}$ the minimal number so that $B(0, \lambda_k)$ contains $k$ linearly independent lattice vectors. Show that for any lattice $\Lambda \subseteq \mathbb{R}^n, \lambda_1(\Lambda) \cdot \lambda_n(\Lambda*) \geqslant 1$.

iv) In this exercise, we want to show that SVP is not harder than CVP in the sense that we can use an oracle for CVP to solve the SVP problem. We denote $CVP(B', t) := argmin\{\|x - t\|_2 : x \in \Lambda(B')\}$. Suppose that $B = (b_1, ..., b_n)$ is the input basis for our SVP problem. Consider the following algorithm:

   (a) FOR i = 1 TO n DO

   (b) Set $v_i := CVP((b_1, ..., b_{i-1}, 2b_i, b_{i+1}, ..., b_n), b_i)$

   (c) Return the shortest vector in $\{v_i - b_i | i = 1, ..., n\}$

   Note that the algorithm calls the CVP oracle only n times on a lattice of dimension n. Prove that the algorithm returns the shortest vector in $\Lambda(B)$.

v) The convex hull $P = conv\{v_1, ..., v_n\}$ of integer points $v_i \in \mathbb{Z}^2$, $i = 1, ..., n$ is a convex lattice polygon. Let $A, I$ and $B$ be the area, number of integer points in the interior and boundary of P respectively. Prove Picks formula

$$A = I + \frac{B}{2} - 1$$

*Hint: consider the matrix* $(v_2 - v_1, v_3 - v_2)$