Integer Optimization
Problem Set 6

Working session: April 17, Presentations: April 24

Let $\Lambda \subseteq \mathbb{R}^2$ be a lattice and $b_1, b_2 \in \Lambda \setminus \{0\}$ be a basis of Λ, ordered such that $\|b_1\|_2 \leqslant \|b_2\|_2$.

i) Show that $b_1, b_2 - xb_1$, $x \in \mathbb{Z}$ is also a basis of Λ.

ii) Let $b_2^* = b_2 - \mu b_1$ with $\mu = \langle b_2, b_1\rangle / \langle b_1, b_1\rangle$ be the *projection* of b_2 into the *orthogonal complement of* b_1.

   Prove that, if $|\mu| > 1/2$, then $b_2 - \lfloor\mu\rceil \cdot b_1$ is strictly shorter than b_2, w.r.t. $\|\cdot\|_2$. Here $\lfloor\mu\rceil$ is the closest integer to μ.

iii) If $b_2 - \lfloor\mu\rceil \cdot b_1$ is still longer than b_1, then the enclosed angle between these vectors is between 60° and 120°.

iv) Show that the following algorithm terminates in $O(\log(\|b_2\|)$ many steps: While $\|b_2^*\| \leqslant \frac{1}{4}\|b_1\|$: Replace b_2 by $b_2 - \lfloor\mu\rceil \cdot b_1$. Swap b_1 and b_2.

   Hint: $b_2 - \lfloor\mu\rceil \cdot b_1$ is much shorter than b_2.

v) We call b_1, b_2 *partially reduced* if $\|b_2\| \geqslant \|b_2\|$ and $\|b_2^*\| \geqslant \frac{1}{4}\|b_1\|$ holds. Show how to compute a shortest nonzero lattice vector in constant time, given a partially reduced basis.

   Hint: The length of $xb_1 + yb_2$ is at least $|y|\,\|b_2^*\| \geqslant |y|\|b_2\|/4$.

For a lattice $\Lambda \subseteq \mathbb{R}^n$ and $i \in \{1,\dots,n\}$ the number $\lambda_i(\Lambda)$ is defined as the minimum $R \geqslant 0$ such that the ball or radius R around 0, $B(0,R) = \{x \in \mathbb{R}^n : \|x\| \leqslant R\}$ contains i *linearly independent* lattice points.

vi) Show that each lattice $\Lambda \subseteq \mathbb{R}^2$ has a basis v_1, v_2 such that $\|v_i\| = \lambda_i(\Lambda)$, $i = 1,2$ holds.

   Hint: Use the first problems above. This answers the question of Samuel asked in class.

vii) Consider the lattice $\Lambda = \{Ax : x \in \mathbb{Z}^5\}$ with A being the matrix

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

   Show that the vectors $2 \cdot e_i$ $i = 1,\dots,5$ are attaining the successive minima but do not form a basis of Λ.

viii) Provide an example of a 2-dimensional lattice $\Lambda(b_1, b_2) \subseteq \mathbb{R}^2$ with $b_1, b_2 \in \mathbb{R}^2$ linearly independent, such that the projection of Λ onto the line generated by b_1 is not a (one-dimensional) lattice. Recall that the projection of v onto the line generated by b_1 is the vector

$$\frac{\langle v, b_1 \rangle}{\langle b_1, b_1 \rangle} b_1$$

Finally we repeat some basics from Linear Algebra 2. Recall that an integer matrix $U \in \mathbb{Z}^{n\times n}$ is called *unimodular* if $\det(U) = \pm 1$ holds.

ix) Let $B \in \mathbb{R}^{n\times n}$ be non-singular and linearly independent and $C \in \mathbb{R}^{n\times n}$. One has $\Lambda(B) = \Lambda(C)$ if and only if there exists a unimodular matrix $U \in \mathbb{Z}^{n\times n}$ with $B \cdot U = C$.

Consequently, the absolute value of the determinant of any basis of a lattice Λ is an invariant of the lattice, called the *lattice determinant*, $\det(\Lambda)$.