Topics: Lattice reduction and applications.

12.1. Find a Lagrange–Gauss reduced basis for the lattice L given by

$$\left\{\begin{bmatrix}-5\\-4\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}\right\}$$

and use it to solve SVP in L. If you have a calculator handy, keep track of the Hadamard ratio as you apply the algorithm.

Solution. We apply Lagrange–Gauss reduction:

step	v_1	v_2	$\|v_1\|^2$	$\|v_2\|^2$	$\langle v_1, v_2\rangle$	$\lfloor t \rceil$	Hadamard ratio $\mathcal{H}$
1	$\left[\begin{smallmatrix}2\\3\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-5\\-4\end{smallmatrix}\right]$	13	41	-22	2	0.551
2	$\left[\begin{smallmatrix}-1\\2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}2\\3\end{smallmatrix}\right]$	5	13	4	-1	0.932
3	$\left[\begin{smallmatrix}-1\\2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]$	5	10	-1	0	0.995

We conclude that $\begin{bmatrix}-1\\2\end{bmatrix}$ is a shortest vector in L, of length $\sqrt{5}$. □

12.2. Let $L \subset \mathbf{R}^2$ be the lattice with basis matrix

$$M = \begin{bmatrix}2 & 1\\-1 & 1\end{bmatrix}.$$

Let $L^\vee \subset \mathbf{R}^2$ be the lattice with basis matrix $M^\vee = (M^\mathsf{T})^{-1}$.

(a) Show that

$$L^\vee = \{y \in \mathbf{R}^2 : \ \langle x, y\rangle \in \mathbf{Z} \text{ for all } x \in L\}.$$

We call $L^\vee$ the *dual lattice to* L.

(b) Let B be the $\mathbf{Z}$-basis of L consisting of the columns of M, and $B^\vee$ the $\mathbf{Z}$-basis of $L^\vee$ consisting of the columns of $M^\vee$. Compare the Hadamard ratios $\mathcal{H}(B)$ and $\mathcal{H}(B^\vee)$.

Solution.

(a) We have

$$(M^\mathsf{T})^{-1} = \frac{1}{3}\begin{bmatrix}1 & 1\\-1 & 2\end{bmatrix} = \begin{bmatrix}1/3 & 1/3\\-1/3 & 2/3\end{bmatrix}.$$

Let $v_1^\vee, v_2^\vee$ denote the columns of $M^\vee$ and v_1, v_2 the columns of M. We have

$$\begin{aligned}\langle v_1, v_1^\vee\rangle &= \frac{2}{3} + \frac{1}{3} = 1,\\ \langle v_1, v_2^\vee\rangle &= \frac{2}{3} - \frac{2}{3} = 0,\\ \langle v_2, v_1^\vee\rangle &= \frac{1}{3} - \frac{1}{3} = 0,\\ \langle v_2, v_2^\vee\rangle &= \frac{1}{3} + \frac{2}{3} = 1.\end{aligned}$$

Since every vector in L is a $\mathbf{Z}$-linear combination of v_1 and v_2, and every vector in $L^\vee$ is a $\mathbf{Z}$-linear combination of $v_1^\vee$ and $v_2^\vee$, we conclude that

$$L^\vee \subseteq \{y \in \mathbf{R}^2 : \ \langle x, y\rangle \in \mathbf{Z} \text{ for all } x \in L\}.$$

For the opposite inclusion, let $y = \begin{bmatrix} a \\ b \end{bmatrix}$ be any vector in the set on the RHS, then

$$2a - b = \langle v_1, y \rangle \in \mathbf{Z} \quad \text{and} \quad a + b = \langle v_2, y \rangle \in \mathbf{Z}.$$

We observe then that

$$y = \begin{bmatrix} a \\ b \end{bmatrix} = (2a - b)v_1^\vee + (a + b)v_2^\vee \in L^\vee.$$

(b) We have

$$\det L = |\det M| = 3, \qquad \det L^\vee = |\det (M^{\mathsf{T}})^{-1}| = \frac{1}{3},$$

so that

$$\mathcal{H}(B) = \left(\frac{3}{\sqrt{5}\sqrt{2}} \right)^{1/2},$$
$$\mathcal{H}(B^\vee) = \left(\frac{1/3}{\sqrt{2}/3\,\sqrt{5}/3} \right)^{1/2}$$

and $\mathcal{H}(B) = \mathcal{H}(B^\vee)$. □

12.3. Given $n \in \mathbf{Z}_{\geqslant 1}$, a real number x is said to be *algebraic of degree n* if there exist integers $a_0, \ldots, a_n$ with $a_n \neq 0$ such that

$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$

(a) Describe a lattice-based procedure for investigating whether a given real number is algebraic of degree n.

(b) You are given a real number α such that

$$\alpha \approx -1.764, \quad \alpha^2 \approx 3.112, \quad \alpha^3 \approx -5.489, \quad \alpha^4 \approx 9.683.$$

You form the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1000 & -1764 & 3112 & -5489 & 9683 \end{bmatrix}$$

and find out that the LLL reduction of the lattice with basis matrix M has basis matrix

$$\begin{bmatrix} 1 & -4 & 5 & -2 & 2 \\ -1 & -3 & -4 & 6 & -2 \\ -4 & 0 & 1 & 0 & 3 \\ 0 & 2 & 1 & 3 & 8 \\ 1 & 1 & -1 & 3 & 3 \\ -1 & -3 & -4 & -2 & 1 \end{bmatrix}$$

What do you guess about the number α? How could you build more confidence in your guess?

Solution.

(a) This is a problem of finding an integer relation linking the real numbers $1, x, x^2, \dots, x^n$. We therefore proceed by choosing a large parameter A and applying LLL reduction to the $(n+2) \times (n+1)$ matrix

$$M = \begin{bmatrix} & & I_{n+1} & & \\ A & \lfloor Ax \rceil & \lfloor Ax^2 \rceil & \dots & \lfloor Ax^n \rceil \end{bmatrix}$$

The first column of the resulting matrix gives a candidate for the integer relation.

(b) The guess is that there is an integer relation

$$1 - \alpha - 4\alpha^2 + \alpha^4 = 0.$$

In particular, α is algebraic of degree 4.

A good way to see if this is likely to be true is to compute more decimals for α, say

$$\alpha \approx -1.764015, \quad \alpha^2 \approx 3.111749, \quad \alpha^3 \approx -5.489171, \quad \alpha^4 \approx 9.682980,$$

and try again. The matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1000000 & -1764015 & 3111749 & -5489171 & 9682980 \end{bmatrix}$$

turns after LLL reduction into

$$\begin{bmatrix} 1 & 17 & 2 & 31 & 12 \\ -1 & -2 & 12 & 12 & -45 \\ -4 & 7 & -7 & -1 & 3 \\ 0 & 13 & 19 & -27 & 6 \\ 1 & 3 & 15 & -16 & -7 \\ -1 & -10 & 28 & 8 & 36 \end{bmatrix}$$

The fact that the first column is exactly the same as before is strong evidence (but not proof!) in favour of the integer relation. □

12.4. Let (w_1, w_2) be an ordered $\mathbf{Z}$-basis of a lattice $L \subset \mathbf{R}^2$. Prove that (w_1, w_2) is Lagrange–Gauss reduced if and only if

$$\|w_1\| \leqslant \|w_2\| \qquad \text{and} \qquad |\langle w_1, w_2 \rangle| \leqslant \frac{1}{2}\|w_1\|^2.$$

Solution. The forward direction was proved in Lemma 4.13.

We prove the converse. Suppose $\|w_1\| \leqslant \|w_2\|$ and $|\langle w_1, w_2 \rangle| \leqslant \|w_1\|^2/2$, then

$$-\frac{1}{2}\|w_1\|^2 \leqslant \pm\langle w_1, w_2 \rangle \leqslant \frac{1}{2}\|w_1\|^2,$$

therefore

$$\|w_2 \pm w_1\|^2 = \|w_2\|^2 \pm 2\langle w_1, w_2 \rangle + \|w_1\|^2 \geqslant \|w_2\|^2 - \|w_1\|^2 + \|w_1\|^2 = \|w_2\|^2,$$

so we can conclude by Proposition 4.14. □

12.5. (*) Let (w_1, w_2) be a $\mathbf{Z}$-basis of a lattice $L \subset \mathbf{R}^2$.

(a) Prove that if (w_1, w_2) is Lagrange–Gauss reduced then it is LLL-reduced.

(b) Give an example to show that the converse is not true in general.

Solution.

(a) Gram–Schmidt orthogonalisation for (w_1, w_2) gives $w_1^* = w_1$, $\mu_{21} = \dfrac{\langle w_1, w_2\rangle}{\|w_1\|^2}$, and $w_2^* = w_2 - \mu_{21} w_1^*$. Therefore (w_1, w_2) is LLL-reduced if and only if

$$|\langle w_1, w_2\rangle| \leqslant \frac{\|w_1\|^2}{2} \qquad \text{and} \qquad \|w_2\|^2 = \|w_2^* + \mu_{21} w_1^*\| \geqslant \frac{3}{4}\|w_1\|^2.$$

But if (w_1, w_2) is Lagrange–Gauss reduced then we have already seen that the inequality for $|\langle w_1, w_2\rangle|$ holds, and also $\|w_2\|^2 \geqslant \|w_1\|^2 \geqslant \dfrac{3}{4}\|w_1\|^2$.

(b) Take

$$w_1 = \begin{bmatrix} 4 \\ 0 \end{bmatrix}, \qquad w_2 = \begin{bmatrix} 2 \\ 3 \end{bmatrix},$$

then $\|w_1\|^2 = 16$, $\|w_2\|^2 = 13$, $\langle w_1, w_2\rangle = 8$. So $\mu_{21} = 1/2$ and

$$\|w_2\|^2 = 13 \geqslant 12 = \frac{3}{4}\|w_1\|^2,$$

hence (w_1, w_2) is LLL-reduced.

However, it is not Lagrange–Gauss reduced, since $\|w_2\| < \|w_1\|$. □

12.6. We explore the Closest Vector Problem (CVP) in full rank 2. Let $L \subset \mathbf{R}^2$ be a full lattice and let $\mathcal{F}$ be the fundamental domain with respect to a $\mathbf{Z}$-basis of L.

(a) Convince yourself that it suffices to know how to solve the CVP for $v \in \mathcal{F}$.

(b) Let $L = \mathbf{Z}^2 \subset \mathbf{R}^2$ be the square lattice with the standard basis $\{e_1, e_2\}$. For a vector $v \in \mathcal{F}$, show that the closest vector to v is the closest corner of the closure of $\mathcal{F}$.

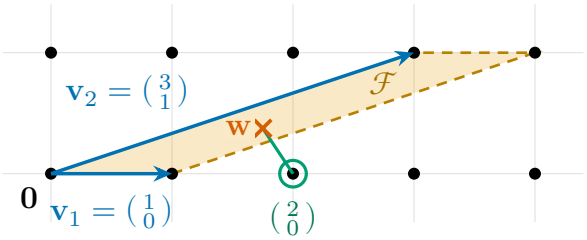
(c) Give an example showing that the statement in (b) does not hold for all $\mathbf{Z}$-bases of $\mathbf{Z}^2$.

Solution.

(a) By Tutorial Question 11.1, we can translate an arbitrary v to a point in $\mathcal{F}$, solve the CVP there and translate the solution back.

(b) This is basically Tutorial Question 11.2, the CVP for orthogonal bases question from last week.

(c) Take the basis $v_1 = e_1$, $v_2 = 3e_1 + e_2$. Visually it is clear that there are vectors in $\mathcal{F}$ whose closest lattice vector is not a corner of the closure of $\mathcal{F}$. For instance, you can take $w = \dfrac{7}{4}e_1 + \dfrac{3}{8}e_2$, with closest lattice vector $2e_1$.



□