Chapter 17

Lattice Basis Reduction

The goal of lattice basis reduction is to transform a given lattice basis into a "nice" lattice basis consisting of vectors that are short and close to orthogonal. To achieve this one needs both a suitable mathematical definition of "nice basis" and an efficient algorithm to compute a basis satisfying this definition.

Reduction of lattice bases of rank 2 in $\mathbb{R}^2$ was given by Lagrange[1] and Gauss. The algorithm is closely related to Euclid's algorithm and we briefly present it in Section 17.1. The main goal of this section is to present the lattice basis reduction algorithm of Lenstra, Lenstra and Lovász, known as the LLL or L^3 algorithm.[2] This is a very important algorithm for practical applications. Some basic references for the LLL algorithm are Section 14.3 of Smart [571], Section 2.6 of Cohen [135] and Chapter 17 of Trappe and Washington [608]. More detailed treatments are given in von zur Gathen and Gerhard [237], Grötschel, Lovász and Schrijver [268], Section 1.2 of Lovász [394], and Nguyen and Vallée [463]. I also highly recommend the original paper [372].

The LLL algorithm generalises the Lagrange-Gauss algorithm and exploits the Gram-Schmidt orthogonalisation. Note that the Gram-Schmidt process is not useful, in general, for lattices since the coefficients $\mu_{i,j}$ do not usually lie in $\mathbb{Z}$ and so the resulting vectors are not usually elements of the lattice. The LLL algorithm uses the Gram-Schmidt vectors to determine the quality of the lattice basis, but ensures that the linear combinations used to update the lattice vectors are all over $\mathbb{Z}$.

[1] The algorithm was first written down by Lagrange and later by Gauss, but is usually called the "Gauss algorithm". We refer to [454] or Chapter 2 of [463] for the original references.

[2] Chapter 1 of [463] gives an excellent survey of the historical development of the algorithm.

17.1 Lattice Basis Reduction in Two Dimensions

Let $\underline{b}_1, \underline{b}_2 \in \mathbb{R}^2$ be linear independent vectors and denote by L the lattice for which they are a basis. The goal is to output a basis for the lattice such that the lengths of the basis vectors are as short as possible (in this case, successive minima). Lagrange and Gauss gave the following criteria for a basis to be reduced and then developed Algorithm 23 to compute such a basis.

Definition 17.1.1. An ordered basis $\underline{b}_1, \underline{b}_2$ for $\mathbb{R}^2$ is **Lagrange-Gauss reduced** if $\|\underline{b}_1\| \leq \|\underline{b}_2\| \leq \|\underline{b}_2 + q\underline{b}_1\|$ for all $q \in \mathbb{Z}$.

The following theorem shows that the vectors in a Lagrange-Gauss reduced basis are as short as possible. This result holds for any norm, though the algorithm presented below is only for the Euclidean norm.

Theorem 17.1.2. *Let λ_1, λ_2 be the successive minima of L. If L has an ordered basis $\{\underline{b}_1, \underline{b}_2\}$ that is Lagrange-Gauss reduced then $\|\underline{b}_i\| = \lambda_i$ for $i = 1, 2$.*

Proof: By definition we have

$$\|\underline{b}_2 + q\underline{b}_1\| \geq \|\underline{b}_2\| \geq \|\underline{b}_1\|$$

for all $q \in \mathbb{Z}$.

Let $\underline{v} = l_1\underline{b}_1 + l_2\underline{b}_2$ be any non-zero point in L. If $l_2 = 0$ then $\|\underline{v}\| \geq \|\underline{b}_1\|$. If $l_2 \neq 0$ then write $l_1 = ql_2 + r$ with $q, r \in \mathbb{Z}$ such that $0 \leq r < |l_2|$. Then $\underline{v} = r\underline{b}_1 + l_2(\underline{b}_2 + q\underline{b}_1)$ and, by the triangle inequality

$$\begin{aligned} \|\underline{v}\| &\geq |l_2|\,\|\underline{b}_2 + q\underline{b}_1\| - r\|\underline{b}_1\| \\ &= (|l_2| - r)\|\underline{b}_2 + q\underline{b}_1\| + r(\|\underline{b}_2 + q\underline{b}_1\| - \|\underline{b}_1\|) \\ &\geq \|\underline{b}_2 + q\underline{b}_1\| \geq \|\underline{b}_2\| \geq \|\underline{b}_1\|. \end{aligned}$$

This completes the proof. □

Definition 17.1.3. Let $\underline{b}_1, \ldots, \underline{b}_n$ be a list of vectors in $\mathbb{R}^n$. We write[3] $B_i = \|\underline{b}_i\|^2 = \langle \underline{b}_i, \underline{b}_i \rangle$.

A crucial ingredient for the Lagrange-Gauss algorithm is that

$$\|\underline{b}_2 - \mu\underline{b}_1\|^2 = B_2 - 2\mu\langle \underline{b}_1, \underline{b}_2 \rangle + \mu^2 B_1 \tag{17.1}$$

is minimised at $\mu = \langle \underline{b}_1, \underline{b}_2 \rangle / B_1$ (to see this, note that the graph as a function of μ is a parabola and that the minimum can be found by differentiating with respect to μ). Since we are working in a lattice we therefore replace $\underline{b}_2$ by $\underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$ where $\lfloor \mu \rceil$ is the nearest integer to μ. Hence lines 3 and 9 of Algorithm 23 reduce the size of $\underline{b}_2$ as much as possible using $\underline{b}_1$. In the one-dimensional case the formula $\underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$ is the familiar operation $r_{i+1} = r_{i-1} - \lfloor r_{i-1}/r_i \rceil r_i$ from Euclid's algorithm.

Lemma 17.1.4. *An ordered basis $\{\underline{b}_1, \underline{b}_2\}$ is Lagrange-Gauss reduced if and only if*

$$\|\underline{b}_1\| \leq \|\underline{b}_2\| \leq \|\underline{b}_2 \pm \underline{b}_1\|.$$

Proof: The forward implication is trivial. For the converse, suppose $\|\underline{b}_2\| \leq \|\underline{b}_2 \pm \underline{b}_1\|$. We use the fact that the graph of $F(\mu) = \|\underline{b}_2 + \mu\underline{b}_1\|^2$ is a parabola. It follows that the

Algorithm 23 Lagrange-Gauss lattice basis reduction

INPUT: Basis $\underline{b}_1, \underline{b}_2 \in \mathbb{Z}^2$ for a lattice L
OUTPUT: Basis $(\underline{b}_1, \underline{b}_2)$ for L such that $\|\underline{b}_i\| = \lambda_i$

```
B_1 = ||b_1||^2
μ = ⟨b_1, b_2⟩/B_1
b_2 = b_2 − ⌊μ⌉ b_1
B_2 = ||b_2||^2
while B_2 < B_1 do
    Swap b_1 and b_2
    B_1 = B_2
    μ = ⟨b_1, b_2⟩/B_1
    b_2 = b_2 − ⌊μ⌉ b_1
    B_2 = ||b_2||^2
end while
return (b_1, b_2)
```

miniumum of $F(\mu)$ is taken for $-1 < \mu < 1$. Hence $\|\underline{b}_2\| \leq \|\underline{b}_2 + q\underline{b}_1\|$ for $q \in \mathbb{Z}$ such that $|q| > 1$. □

Algorithm 23 gives the Lagrange-Gauss algorithm for lattices in $\mathbb{Z}^2$. Note that the computation of μ is as an exact value in $\mathbb{Q}$. All other arithmetic is exact integer arithmetic.

Lemma 17.1.5. *Algorithm 23 terminates and outputs a Lagrange-Gauss reduced basis for the lattice L.*

Exercise 17.1.6. Prove Lemma 17.1.5.

Example 17.1.7. We run the Lagrange-Gauss algorithm on $\underline{b}_1 = (1, 5)$ and $\underline{b}_2 = (6, 21)$. In the first step, $\mu = 111/26 \approx 4.27$ and so we update $\underline{b}_2 = \underline{b}_2 - 4\underline{b}_1 = (2, 1)$. We then swap $\underline{b}_1$ and $\underline{b}_2$ so that the values in the loop are now $\underline{b}_1 = (2, 1)$ and $\underline{b}_2 = (1, 5)$. This time, $\mu = 7/5 = 1.4$ and so we set $\underline{b}_2 = \underline{b}_2 - \underline{b}_1 = (-1, 4)$. Since $\|\underline{b}_2\| > \|\underline{b}_1\|$ the algorithm halts and outputs $\{(2, 1), (-1, 4)\}$.

Exercise 17.1.8. Run the Lagrange-Gauss reduction algorithm on the basis $\{(3, 8), (5, 14)\}$.

Lemma 17.1.9. *Let $\underline{b}_1, \underline{b}_2$ be the initial vectors in an iteration of the Lagrange-Gauss algorithm and suppose $\underline{b}'_1 = \underline{b}_2 - m\underline{b}_1$ and $\underline{b}'_2 = \underline{b}_1$ are the vectors that will be considered in the next step of the algorithm. Then $\|\underline{b}'_1\|^2 < \|\underline{b}_1\|^2/3$, except perhaps for the last two iterations.*

Proof: Note that $m = \lfloor \mu \rceil = \lfloor \langle \underline{b}_1, \underline{b}_2 \rangle / \langle \underline{b}_1, \underline{b}_1 \rangle \rceil = \langle \underline{b}_1, \underline{b}_2 \rangle / \langle \underline{b}_1, \underline{b}_1 \rangle + \epsilon$ where $|\epsilon| \leq 1/2$. Hence,

$$\langle \underline{b}_1, \underline{b}'_1 \rangle = \langle \underline{b}_1, \underline{b}_2 - (\langle \underline{b}_1, \underline{b}_2 \rangle / \langle \underline{b}_1, \underline{b}_1 \rangle + \epsilon)\, \underline{b}_1 \rangle = -\epsilon \langle \underline{b}_1, \underline{b}_1 \rangle = -\epsilon \|\underline{b}_1\|^2.$$

We show that $\|\underline{b}'_1\|^2 < \|\underline{b}_1\|^2/3$ unless we are in the last two iterations of the algorithm. To do this, suppose that $\|\underline{b}'_1\|^2 \geq \|\underline{b}_1\|^2/3$. Then

$$|\langle \underline{b}'_1, \underline{b}'_2 \rangle| = |\langle \underline{b}'_1, \underline{b}_1 \rangle| = |\epsilon| \|\underline{b}_1\|^2 \leq \tfrac{1}{2} \|\underline{b}_1\|^2 \leq \tfrac{3}{2} \|\underline{b}'_1\|^2.$$

It follows that, in the next iteration of the algorithm, we will be taking $m = \lfloor \mu \rceil \in \{-1, 0, 1\}$ and so the next iteration would, at most, replace $\underline{b}'_1$ with $\underline{b}'_2 \pm \underline{b}'_1 = \underline{b}_1 \pm (\underline{b}_2 - m\underline{b}_1)$. But, if this were smaller than $\underline{b}'_1$ then we would have already computed $\underline{b}'_1$ differently in the current iteration. Hence, the next step is the final iteration. □

[3] The reader is warned that the notation B_i will have a different meaning when we are discussing the LLL algorithm.