Euclidean lattices

Anna Somoza

1 Definitions

A *lattice* Λ is a free $\mathbb{Z}$-module of finite rank. Given a linearly-independent basis $(b_i)_{1\leq i\leq n}$ of $\mathbb{R}^d$ with $n \leq d$, we have

$$\Lambda = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

In general, we will consider the case $n = d$.

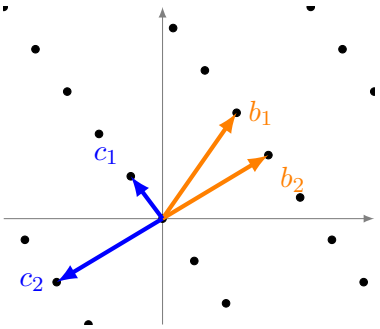

Figure 1: A lattice in $\mathbb{R}^2$, which is generated both by $\{b_1, b_2\}$, and by $\{c_1, c_2\}$.

In general, they are the result of applying a nonsingular transformation to the integer lattice $\mathbb{Z}^n$, that is,

$$\Lambda = \{Bx : x \in \mathbb{Z}^n\}$$

for $B \in \mathbb{R}^{d\times n}$ the matrix that has $b_1, \ldots, b_n$ as columns.

Note that the same lattice can be represented by several different bases, see Figure 1.

Definition 1.1. A *unimodular matrix* is a square integer matrix with determinant ± 1.

Equivalently, it is a matrix $U \in \mathbb{Z}^{n\times n}$ such that there exists a matrix $V \in \mathbb{Z}^{n\times n}$ that satisfies

$$UV = VU = I_n.$$

Proposition 1.2. *Two bases with matrices B and C respectively generate the same lattice if and only if there exists a unimodular matrix $M \in \mathbb{Z}^{n\times n}$ such that $B = CM$.*

Proof. Start by assuming $B = CM$ for some unimodular matrix M, so we also have $C = BM^{-1}$. Then, since both M and M^{-1} are integer matrices, it follows that $\Lambda(B) \subseteq \Lambda(C)$ and $\Lambda(C) \subseteq \Lambda(B)$,

Now assume that B and C are two bases for the same lattice Λ. Then, by definition, there exist integer matrices $M, N \in \mathbb{Z}^{n\times n}$ such that $B = CM$ and $C = BN$. It follows that $B = BNM$ or, equivalently, $B(I_n - NM) = 0$. Since B is nonsingular, we obtain $I_n - NM = 0$. Analogously one gets $I_n - MN = 0$, so we conclude that M is unimodular. □

2 Gram-Schmidt orthogonalization (GSO)

Definition 2.1. A basis $(b_i)_{1\leq i\leq n}$ is called *orthogonal* (with respect to a scalar product $\langle\cdot,\cdot\rangle$) if we have $\langle b_i, b_j\rangle = 0$ for all $i \neq j$.

We define the *orthogonalization* of a basis $(b_i)_{1\leq i\leq n}$ of $\mathbb{R}^n$ as a basis $(b_i^*)_{1\leq i\leq n}$ such that b_i^* is the component of b_i that is orthogonal to the space generated by $b_1, \ldots, b_{i-1}$.

We compute it iteratively with the following formula:

$$b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*, \tag{GSO}$$

where $\mu_{ij} = \langle b_i, b_j^*\rangle / \langle b_j^*, b_j^*\rangle$.

Proposition 2.2. *The basis obtained with* (GSO) *is orthogonal.*

Proof. We prove it by induction.

- By definition, b_1^* is orthogonal.
- Assume that for a fixed i, the family $(b_i^*)_{1\leq i\leq i-1}$ is orthogonal, that is,

$$\langle b_r^*, b_s^*\rangle = \begin{cases} 0 & \text{if } r \neq s, \\ \langle b_r^*, b_r^*\rangle & \text{if } r = s; \end{cases}$$

  and define b_i^* as in (GSO). Then, for r in $1, \ldots, i-1$, we have

$$\langle b_i^*, b_r^*\rangle = \langle b_i - \sum_{j<i} \mu_{ij} b_j^*, b_r^*\rangle = \langle b_i, b_r^*\rangle - \sum_{j<i} \mu_{ij} \langle b_j^*, b_r^*\rangle = \langle b_i, b_r^*\rangle - \mu_{ir} \langle b_r^*, b_r^*\rangle = 0,$$

  hence we conclude that the family $(b_i^*)_{1\leq i\leq i}$ is also orthogonal. □

Let B, B^* be respectively the matrices for the bases $(b_i)_{1\leq i\leq n}$, $(b_i^*)_{1\leq i\leq n}$. Then, the matrix

$$A = \begin{pmatrix} 1 & \mu_{2,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mu_{n,n-1} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \tag{1}$$

satisfies $B = B^* A$.

Remark 2.3. Given a lattice basis, the basis obtained with (GSO) is not necessarily a lattice basis. See Figure 2.

Remark 2.4. We do not consider the orthonormalization, that is, scaling the generators to have norm 1, to avoid taking square roots. Therefore, if the original basis is defined over $\mathbb{Q}$, then its GSO is also defined over $\mathbb{Q}$.

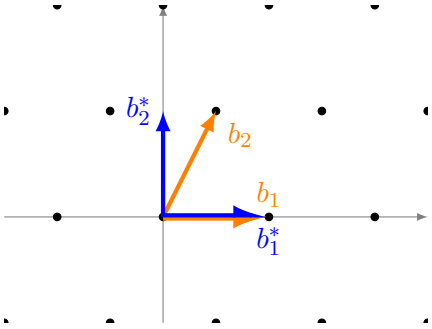

Figure 2: The GSO of the basis $\{b_1, b_2\}$ is not a basis of the original lattice because b_2^* is not an element of the original lattice.

3 Determinant of a lattice

We define the *Gram matrix* of the basis $(b_i)_{1\leq i\leq n}$ as the matrix

$$\mathrm{Gram}(b_1, \ldots, b_n) \;=\; (\langle b_i, b_j\rangle)_{1\leq i,j\leq n}\,.$$

Equivalently, one writes

$$\mathrm{Gram}(b_1, \ldots, b_n) = {}^T BB.$$

The Gram matrix is symmetric and positive definite. We write

$$\det \Lambda = \sqrt{\det \mathrm{Gram}(b_1, \ldots, b_n)}.$$

Remark 3.1. Recall that B is a $(d \times n)$-matrix, hence not necessarily square. When $d = n$, then we have

$$\det \Lambda = |\det B|.$$

Proposition 3.2. *The value* $\det \Lambda$ *does not depend on the basis* $(b_i)_i$*, and it is equal to the product of the norms of the elements* b_i^* *of the GSO of* $(b_i)_i$*.*

Proof. To prove that the determinant of the lattice is independent on the basis, let B, C be the matrices of two bases of a lattice Λ. By Proposition 1.2 there exists a unimodular matrix $M \in \mathbb{Z}^{n\times n}$ that satisfies $C = BM$. Since by definition $\det M = \pm 1$, the claim follows from

$$\det \mathrm{Gram}(c_1, \ldots, c_n) = \det({}^T CC) = \det({}^T M^T BBM) = (\det M)^2 \det \mathrm{Gram}(b_1, \ldots, b_n).$$

To prove the second claim, recall that by Proposition 2.2, we have $B = B^* A$ for A as defined in (1). Since A has determinant 1, by an equivalent argument we get

$$\det \Lambda = \sqrt{\det \mathrm{Gram}(b_1^*, \ldots, b_n^*)} = \sqrt{\det \begin{pmatrix} \langle b_1^*, b_1^*\rangle & & \\ & \ddots & \\ & & \langle b_n^*, b_n^*\rangle \end{pmatrix}}.$$

The result follows. □

We define the *fundamental domain* of a lattice $\Lambda(B)$ as the set

$$\mathcal{F}(\Lambda) = \left\{ \sum_{i=1}^{n} \lambda_i b_i : 0 \leq \lambda_i < 1 \right\},$$

and define $\mathrm{vol}\,\mathcal{F}(\Lambda) = \det \Lambda$.

The following result is obtained immediately from the inequality $||b_i^*|| \leq ||b_i||$.

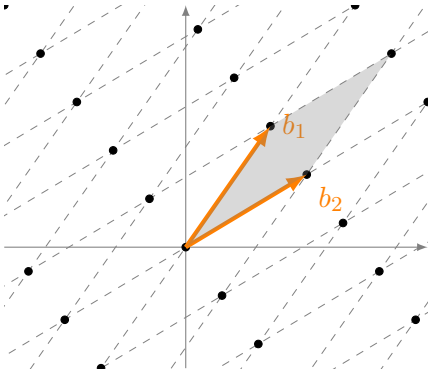

Figure 3: The fundamental domain of the lattice Λ generated by b_1, b_2.

Corollary 3.3 (Hadamard's inequality)**.** *For any lattice $\Lambda(B)$, we have*

$$\det \Lambda \leq \prod_{i=1}^{n} ||b_i||.$$

4 Minimum of a lattice

We define the *minimum of a lattice* Λ, denoted $\lambda(\Lambda)$, as the minimal length of a nonzero vector of Λ.

Finding an element $x \in \Lambda(B)$ such that $||x|| = \lambda(\Lambda)$ is an NP-complete problem.

Proposition 4.1. *Let Λ be a lattice with basis $(b_i)_{1\leq i\leq n}$ and let $(b_i^*)_{1\leq i\leq n}$ be its Gram-Schmidt orthogonalization. We have*

$$\lambda(\Lambda) \geq \min_{1\leq i\leq n} ||b_i^*|| > 0.$$

Proof. Let $x \in \mathbb{Z}^n$ be a nonzero integer vector, let B be the matrix associated to $(b_i)_i$, and consider the element of Λ given by Bx. We will show that $||Bx|| \geq \min_{1\leq i\leq n} ||b_i^*||$.

To that end, let j be the largest index with $x_j \neq 0$. Using that b_j^* is orthogonal to all b_i with $i < j$, we obtain

$$|\langle Bx, b_j^*\rangle| = |\langle \sum_{i=1}^{n} x_i b_i, b_j^*\rangle| = |x_j||\langle b_j^*, b_j^*\rangle| = |x_j|\,||b_j^*||^2.$$

We also have that $\langle Bx, b_j^*\rangle \leq ||Bx||\,||b_j^*||$, hence we conclude

$$||Bx|| \geq |x_j|\,||b_j^*|| \geq \min_{1\leq i\leq n} ||b_i^*|| > 0. \qquad \square$$

Given $x, y \in \mathbb{R}^n$, we write $x \equiv y \mod \Lambda$ if and only if $x - y$ is an element of Λ.

Lemma 4.2. *Let S be a measurable set in $\mathbb{R}^n$ such that $\operatorname{vol} S > \det \Lambda$. Then there exist $x, y \in S$ such that $x \equiv y \mod \Lambda$.*

Proof. For every $x \in \Lambda$ consider the set $S_x = X \cap (x + \mathcal{F}(\Lambda))$, which define a partition of the set S. In particular, we have

$$\operatorname{vol} S = \sum_{x\in\Lambda} \operatorname{vol} S_x.$$

If we now consider the translations $S'_x = S_x - x = (S - x) \cap \mathcal{F}(\Lambda)$, then all the sets S'_x are contained in the fundamental domain of the lattice, and it is clear that $\operatorname{vol} S_x = \operatorname{vol} S'_x$.

Therefore, since we have $S'_x \subseteq \mathcal{F}(\Lambda)$ and also $\det \Lambda = \operatorname{vol} \mathcal{F}(\Lambda) < \operatorname{vol} S = \sum_{x \in \Lambda} \operatorname{vol} S'_x$, we conclude that the sets S'_x cannot be disjoint, that is, there exist $x, y \in \Lambda$ and $z \in \mathcal{F}(\Lambda)$ such that $z \in S'_x \cap S'_y$.

If we consider the opposite translation, we obtain two points $z_1 = z + x \in S_x, z_2 = z + y \in S_y$ such that their difference $z_1 - z_2 = x - y$ is an element of the lattice. □

Theorem 4.3 (Minkowski)**.** *Let C be a centrally-symmetric convex set in $\mathbb{R}^n$ such that $\operatorname{vol} C > 2^n \det \Lambda$. Then there exists a nonzero element of Λ in C.*

Proof. Start by considering the set $\dfrac{C}{2} = \{x : 2x \in C\}$. We have

$$\operatorname{vol} \frac{C}{2} = \frac{\operatorname{vol}(C)}{2^n} > \det \Lambda,$$

hence by Lemma 4.2 there exist $z_1, z_2 \in \frac{C}{2}$ such that $l = z_1 - z_2 \in \Lambda$ or, equivalently, that there exist $c_1, c_2 \in C$ such that

$$l = \frac{1}{2}(c_1 - c_2).$$

That l is an element of C follows from it being centrally-symmetric and convex. □

Theorem 4.4. *Let Λ be a full-rank lattice in $\mathbb{R}^n$. Then we have*

$$\lambda(\Lambda) \leq \sqrt{n} (\det \Lambda)^{1/n}.$$

Proof. Consider the open ball $B = B(0, \lambda(\Lambda))$, which by definition contains no nonzero lattice points. Then, by Theorem 4.3, we have $\operatorname{vol} B \leq 2^n \det \Lambda$.

Consider also a cube C of side length $\frac{2\lambda(\Lambda)}{\sqrt{n}}$ centered at the origin, and note that it is contained in B. Altogether we obtain

$$\left(\frac{2\lambda(\Lambda)}{\sqrt{n}}\right)^n \leq \operatorname{vol} B \leq 2^n \det \Lambda,$$

and rearranging the inequality above we obtain the desired result. □

This result motivates the study of the so-called *Hermite constant*,

$$\gamma_n = \sup_{\Lambda, \dim \Lambda = n} \frac{\lambda(\Lambda)^2}{(\det \Lambda)^{2/n}}.$$

To this day, this is only known for some values of n, as shown on the following table:

n	1	2	3	4	5	6	7	8	24
γ_n^n	1	4/3	2	4	8	64/3	64	256	4^{24}

5 Reduced bases

The goal for the following sections is to present algorithms to obtain reduced bases for a given lattice.

Definition 5.1. We will say that a basis $(b_i)_{1 \leq i \leq n}$ of Λ is *proper* if the coefficients of the matrix A obtained with the (GSO) satisfy $|\mu_{ij}| \leq \frac{1}{2}$ for $i > j$.

Algorithm 1: Proprification algorithm

input : A basis $(b_i)_{1\leq i\leq n}$ of Λ
output: A *proper* basis $(c_i)_{1\leq i\leq n}$ of Λ such that $c_i = b_i + \sum_{j<i} x_j b_j$.
Compute the GSO of (b_i) and note the coefficients μ_{ij}.
for $i = 1$ **to** n **do**
  for $j = i-1$ **to** 1 **do**
    $x_j = \lfloor \mu_{ij} \rceil$
    $b_i = b_i - x_j b_j$
    $\mu_{ij} = \mu_{ij} - x_j$
    for $k = 1$ **to** $j-1$ **do**
      $\mu_{ik} = \mu_{ik} - x_j \mu_{jk}$
return $(b_i)_{1\leq i\leq n}$

Proof. Observe that the changes made at each step do not change the final GSO basis. The goal is to prove that the output base is proper. We proceed by induction.

- The base case is true by definition.
- Assume that for a fixed pair (i, j), the family $c_1, \ldots, c_{i-1}$ is proper, that is, for every $k < l \leq i-1$ we have $|\mu_{lk}| \leq \frac{1}{2}$, and for every $j+1 \leq k \leq i-1$ we also have $|\mu_{ik}| \leq \frac{1}{2}$. We will now prove $|\mu_{ij}| \leq \frac{1}{2}$. Since we have

$$b_i = b_i^* + \sum_{k<i} \mu_{ik} b_k^*$$

we write

$$\begin{aligned} b_i - \lfloor \mu_{ij} \rceil b_j &= \left(b_i^* + \sum_{k<i} \mu_{ik} b_k^* \right) - \lfloor \mu_{ij} \rceil \left(b_j^* + \sum_{k<j} \mu_{jk} b_k^* \right) \\ &= b_i^* + \sum_{k<i} \mu_{ik} b_k^* - \lfloor \mu_{ij} \rceil b_j^* - \lfloor \mu_{ij} \rceil \sum_{k<j} \mu_{jk} b_k^* \\ &= b_i^* + \sum_{k=j+1}^{i-1} \mu_{ik} b_k^* + (\mu_{ij} - \lfloor \mu_{ij} \rceil)\, b_j^* + \sum_{k<j} (\mu_{ik} - \lfloor \mu_{ij} \rceil \mu_{jk})\, b_k^*. \end{aligned}$$

  The new value of μ_{ij} is then $\mu_{ij} - \lfloor \mu_{ij} \rceil$, so we obtain $|\mu_{ij}| \leq \frac{1}{2}$. □

Definition 5.2. We will say that a basis $(b_i)_{1\leq i\leq n}$ of Λ is *Siegel-reduced* if it satisfies

$$\|b_i^*\|^2 \;\leq\; 2\|b_{i+1}^*\|^2$$

for every $i < n$.

In the definition of LLL-reduced basis there is a more general condition, known as the Lovász condition, in terms of a parameter $\delta \in]\frac{1}{4}, 1[$:

$$\delta \|b_{i-1}^*\|^2 \;\leq\; \|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2.$$

The condition in the definition of Siegel-reduced is equivalent to the Lovász condition when $\delta = \frac{3}{4}$, and we will always consider this case for the current course.

Remark 5.3. For a Siegel-reduced basis, we have

$$\|b_1\|^2 = \|b_1^*\|^2 \leq 2\|b_2^*\|^2 \leq \cdots \leq 2^{n-1}\|b_n^*\|^2,$$

from where we obtain

$$\|b_1\|^n \;\leq\; \left(\prod_{i=1}^{n} \|b_i^*\|\right) (\sqrt{2})^{\frac{n(n-1)}{2}} \;=\; 2^{\frac{n(n-1)}{4}} \det \Lambda.$$

Definition 5.4. We will say that a basis $(b_i)_{1\leq i\leq n}$ of Λ is *reduced* if it is both Siegel-reduced and proper.

Lemma 5.5. *Let $(b_i)_{1\leq i\leq n}$ be a reduced basis. Then it satisfies*

$$1 \;\leq\; \frac{\|b_i\|^2}{\|b_i^*\|^2} \;\leq\; 2^{i-1}.$$

Proof. Since we have $b_i = b_i^* + \sum_{j<i} \mu_{ij} b_j^*$, we can write

$$\frac{\|b_i\|^2}{\|b_i^*\|^2} \;=\; 1 + \sum_{j<i} \mu_{ij}^2 \frac{\|b_j^*\|^2}{\|b_i^*\|^2}.$$

From the fact that the basis is Siegel-reduced we obtain $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$. On the other hand, since the basis is proper we also have $|\mu_{ij}| \leq \frac{1}{2}$. We conclude

$$\frac{\|b_i\|^2}{\|b_i^*\|^2} \leq 1 + \sum_{j=1}^{i-1} \frac{1}{4} 2^{i-j} = \frac{1}{2} + 2^{i-2} \leq 2^{i-2} + 2^{i-2} = 2^{i-1}. \qquad \square$$

Theorem 5.6. *Let $x \in \Lambda\backslash\{0\}$, and let $(b_i)_{1\leq i\leq n}$ be a reduced basis of Λ. Then we have:*

(i) $\|b_1\| \leq 2^{(n-1)/2}\|x\|$, *and*

(ii) if $x_1, x_2, \cdots, x_t$ are linearly-independent elements of Λ, then $\|b_t\| \leq 2^{(n-1)/2} \max_{i\leq t} \|x_i\|$.

Proof. (i) Let b_k^* be the vector of the GSO that attains the minimum norm. Given that the basis (b_i) is Siegel-reduced, we have $\|b_1\|^2 = \|b_1^*\|^2 \leq 2^{k-1}\|b_k^*\|^2$, and it follows from Proposition 4.1 that we have $\|b_k^*\|^2 \leq \lambda(\Lambda)^2 \leq \|x\|^2$. Altogether we obtain

$$\|b_1\|^2 \leq 2^{k-1}\|b_k^*\|^2 \leq 2^{k-1}\|x\|^2 \leq 2^{n-1}\|x\|^2.$$

(ii) Once again, since the basis $(b_i)_i$ is Siegel-reduced, we have

$$\|b_j^*\|^2 \leq 2\|b_{j+1}^*\|^2 \leq \cdots \leq 2^{i-j}\|b_i^*\|^2.$$

Moreover, for every j let us write $x_j = \sum_{i=1}^{n} r_{ij} b_j$, with $r_{ij} \in \mathbb{Z}$, and let $I(j)$ denote the biggest i such that $r_{ij} \neq 0$. By a reasoning analogous to the one in the proof of Proposition 4.1 we have

$$\|x_j\|^2 \geq \|b_{I(j)}^*\|^2. \tag{2}$$

Changing the order of the elements x_j if necessary, we can always assume $I(1) \leq \cdots \leq I(t)$.

Next we prove by induction that $j \leq I(j)$.

- For the base case, the claim is vacuously true: $1 \leq I(1)$.

- Assume that for a given j the condition $j-1 \leq I(j-1)$ is satisfied, and recall that we have $I(j-1) \leq I(j)$. So we write $j-1 \leq I(j)$. If $I(j) = j-1$, then we have

$$\langle x_1, \cdots, x_j \rangle \subseteq \langle b_1, \cdots, b_{j-1} \rangle,$$

what contradicts the independence of the elements (x_i). So we conclude that $j \leq I(j)$.

Next, by Lemma 5.5 we have $\|b_j\|^2 \leq 2^{j-1}\|b_j^*\|^2$, so we write

$$\|b_j\|^2 \leq 2^{j-1}2^{I(j)-j}\|b_{I(j)}^*\|^2 = 2^{I(j)-1}\|b_{I(j)}^*\|^2,$$

and together with (2) we obtain

$$\|b_j\|^2 \leq 2^{n-1}\|x_j\|^2 \leq 2^{n-1}\max_{i \leq t}\|x_i\|.$$

Since the previous equation holds for all $j \leq t$, the claim follows. □

Corollary 5.7. *Let $x \in \Lambda \backslash \{0\}$ and let $(b_i)_{1 \leq i \leq n}$ be a reduced basis. Then we have*

$$\|b_1\| \leq 2^{(n-1)/2}\lambda(\Lambda).$$

6 The LLL algorithm and some applications

Named after Arjen *Lenstra*, Hendrik *Lenstra* and László *Lovász*, the LLL algorithm computes a reduced lattice base in polynomial time.

Algorithm 2: The LLL algorithm (1982)

input : A basis $(b_i)_{1 \leq i \leq n}$ of a lattice $\Lambda \subseteq \mathbb{R}^n$.
output: A reduced basis of Λ.

$k = 2$
compute the GSO of $(b_i)_{1 \leq i \leq n}$, $(b_i^*)_{1 \leq i \leq n}$
while $k \leq n$ **do**
  for $j = k-1$ **to** 1 **do** `// Corresponds to` j`-loop of Algorithm 1, for` $i = k$`.`
    $x_j = \lfloor \mu_{kj} \rceil$
    $b_k = b_k - x_j b_j$
    $\mu_{kj} = \mu_{kj} - x_j$
    for $l = 1$ **to** $j-1$ **do**
      $\mu_{kl} = \mu_{kl} - x_j \mu_{jl}$
  if $k > 1$ **and** $\|b_{k-1}^*\|^2 > 2\|b_k^*\|^2$ **then**
    swap(b_{k-1}, b_k)
    update $(b_i^*)_{1 \leq i \leq n}$
    $k = k-1$
  else
    $k = k+1$
return $(b_i)_{1 \leq i \leq n}$

6.1 Complexity of the algorithm

In order to simplify the computation of the complexity we make the benign assumption that the coefficients of the vectors $(b_i)_{1 \leq i \leq n}$ in the base are integers.

The algorithm alternates two phases: the *proprification* phase (the j-loop) and the *swap* phase (the if-else clause). The first phase changes the vectors $(b_i)_i$ to guarantee that the basis $(b_1, \dots, b_k)$ is proper, and the second phase swaps the elements b_{k-1}, b_k in the base if they do not satisfy the Siegel condition in Defintion 5.2, changing the GSO basis.

If the algorithm terminates, then the output is correct by construction. We want to prove that it terminates in polynomial time.

To do so we first bound the number of iterations and then bound the size of the data.

Notation For this section, we will use the following notation:

- $A = \max_{1 \le i \le n} \|b_i\|^2$,
- $\Lambda_i = \langle b_1, \dots, b_i \rangle_{\mathbb{Z}}$,
- $D_i = (\det \Lambda_i)^2 = \prod_{j=1}^{i} \|b_j^*\|^2$,
- $D = \prod_{i=1}^{n} D_i$

and using Corollary 3.3 for every Λ_i we obtain

$$D \le \prod_{i=1}^{n} \prod_{j=1}^{i} \|b_i\|^2 = \|b_1\|^{2n} \|b_2\|^{2(n-1)} \dots \|b_n\|^2 \le A^{n(n+1)/2}.$$

Number of iterations

We show how a swap changes the values of $(D_i)_{1 \le i \le n}$ and D, and use it to bound the number of times that it can happen.

Lemma 6.1. *The value of D decreases by a factor $\frac{3}{4}$ at each iteration.*

Proof. As we discussed in the proof of Algorithm 1, the proprification phase does no change the GSO basis, hence it does not affect D_i or D.

Therefore, all the changes happen at the swap phase. Note that for a given k, the swap of b_{k-1} and b_k happens if and only if

$$\|b_{k-1}^*\|^2 > 2\|b_k^*\|^2.$$

In that case, the lattices Λ_i remain unchanged for all $i \neq k-1$, hence the only D_i that changes is $D_{k-1} = (\det \Lambda_{k-1})^2$. Let us denote as D', D_i', b_i' the values of D, D_i, b_i after the swap. Then we have

$$\frac{D'}{D} = \frac{D_{k-1}'}{D_{k-1}} = \frac{\|b_{k-1}'^*\|^2}{\|b_{k-1}^*\|^2}. \tag{3}$$

We write $b_{k-1}'^*$ in terms of $(b_i)_{1 \le i \le n}$.

$$b_{k-1}'^* = b_{k-1}' - \sum_{j<k-1} \mu_{k-1,j}' b_j'^* = b_k - \sum_{j<k-1} \mu_{kj} b_j^* = b_k + \mu_{k,k-1} b_{k-1}^*.$$

Going back to (3) we conclude

$$\frac{D'}{D} = \frac{\|b_{k-1}'^*\|^2}{\|b_{k-1}^*\|^2} = \frac{\|b_k^*\|^2}{\|b_{k-1}^8 8\|^2} + \mu_{k,k-1}^2 \le \frac{1}{2} + \frac{1}{4} = \frac{3}{4}. \tag{4}$$

□

Let $D^{(k)}$ denote the value of D after k iterations, and note that it is a positive integer. By the previous lemma we have

$$1 \leq D^{(k)} \leq \left(\frac{3}{4}\right)^k D \leq \left(\frac{3}{4}\right)^k A^{n(n+1)/2}$$

hence by taking logarithms we obtain

$$0 \leq k \log \frac{3}{4} + \frac{n(n+1)}{2} \log A,$$

so we conclude $k = O(n^2 \log A)$.

We also observe that an iteration has $O(n^2)$ operations over $\mathbb{Z}$, and conclude that there are $O(n^4 \log A)$ operations in total.

Next we focus on bounding the size of the integers in use.

Lemma 6.2. *For every $l < k \leq n$ we have*

$$D_{k-1} b_k^* \in \mathbb{Z}^n \text{ and } D_k \mu_{kl} \in \mathbb{Z}.$$

Proof. Consider the relation

$$b_k^* = b_k - \sum_{l<k} \nu_{kl} b_l,\ \nu_{kl} \in \mathbb{Q},$$

and consider the scalar products

$$0 = \langle b_t, b_k^* \rangle = \langle b_t, b_k \rangle - \sum_{l<k} \nu_{kl} \langle b_t, b_l \rangle \text{ for } 1 \leq t < k.$$

We write this set of equations as a linear system with matrices

$${}^T B_{k-1} B_{k-1} (\nu_{kl})_l = {}^T B_{k-1} b_k = v \in \mathbb{Z}^{k-1}$$

where $G = {}^T B_{k-1} B_{k-1}$ is the Gram matrix of the basis $(b_i)_{1 \leq i \leq k-1}$, and $\det G = D_{k-1}$. We obtain

$$D_{k-1} (\nu_{kl})_l = \det G \cdot (\nu_{kl})_l = \det G \cdot G^{-1} v = \mathrm{adj}(G) v \in \mathbb{Z}^{k-1},$$

where we use $b_i \in \mathbb{Z}$.

It follows that for all $l < k$ we have $D_{k-1} \nu_{kl} \in \mathbb{Z}$, hence we conclude

$$D_{k-1} b_k^* = D_{k-1} b_k - \sum_{l<k} (D_{k-1} \nu_{kl}) b_l \in \mathbb{Z}^n.$$

For the second claim we write

$$D_l \mu_{kl} = D_{l-1} \|b_l^*\|^2 \frac{\langle b_k, b_l^* \rangle}{\langle b_l^*, b_l^* \rangle} = \langle b_k, D_{l-1} b_l^* \rangle \in \mathbb{Z}. \qquad \square$$

Lemma 6.3. *Throughout the LLL algorithm, the value $M = \max_{1 \leq i \leq n} \|b_i^*\|$ does not increase.*

Proof. It is once again true that the proprification phase does not affect the vectors in $(b_i^*)_{1 \leq i \leq n}$. As for the swap phase, it follows from Equation (4) that

$$\|b_{k-1}'^*\|^2 = \|b_k^*\|^2 + \mu_{k,k-1}^2 \|b_{k-1}^*\|^2 \leq \frac{3}{4} \|b_{k-1}^*\|^2 \leq M^2.$$

Next we focus on $b_k'^*$. Recall that the value

$$(\det \Lambda')^2 = \prod_{i=1}^{n} \|b_i'^*\|^2$$

is invariant, so we have

$$\|b_{k-1}^*\|^2 \|b_k^*\|^2 = \|b_{k-1}'^*\|^2 \|b_k'^*\|^2 \geq \|b_k^*\|^2 \|b_k'^*\|^2,$$

hence

$$\|b_k'^*\|^2 \leq \|b_{k-1}^*\|^2 \leq M^2.$$

□

It follows from the lemmas above that the denominators in b_k^* and μ_{kl} are bounded by $D_n \leq A^n$.

Next we bound $\|b_k\|$ and $|\mu_{ij}|$. On the one hand we have

$$|\mu_{ij}|^2 = \left(\frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2} \right)^2 \leq \frac{\|b_i\|^2}{\|b_j^*\|^2},$$

and

$$\|b_j^*\|^2 = \frac{D_j}{D_{j-1}} \geq \frac{1}{D_{j-1}},$$

so we conclude

$$|\mu_{ij}|^2 \leq D_{j-1} \|b_i\|^2. \tag{5}$$

Lemma 6.4. *During the proprification phase we have*

$$\|b_i\|^2 \leq n^2 (4A)^{n+1},$$

and elsewhere we have

$$\|b_i\|^2 \leq nA$$

.

Proof. At the start of the algorithm we have, by definition of A, that

$$\|b_i\| \leq A \leq nA.$$

Recall the definition of b_i in terms of $(b_i^*)_{1 \leq i \leq n}$,

$$b_i = b_i^* + \sum_{j<i} \mu_{ij} b_j^*$$

and define $\mu_{ii} = 1$ so that we can write b_i^* inside the summation. Let $m_i = \max_{1 \leq j \leq i} |\mu_{ij}|$ and consider

$$\|b_i\| = \sum_{j=1}^{i} |\mu_{ij}|^2 \|b_j^*\|^2 \leq n m_i^2 A$$

Whenever we are outside of the proprification phase we have $m_i = |\mu_{ii}| = 1$ since for $j < i$ we have $|\mu_{ij}| \leq 1/2$.

Now for the proprification phase, at the beginning of an iteration we have

$$m_i^2 = \max_{1\le j\le n} \mu_{ij}^2 \le \max_{1\le j\le n} D_{j-1}\|b_i\|^2 \le A^{n-1}\cdot nA,$$

where we are using that the vectors $(b_i)_i$ are unchanged since the end of the previous proprification phase, and hence they satisfy the bound $\|b_i\|^2 \le nA$.

Now let $j < i$, and assume that the basis is already proper for $l > j$, that is, $|\mu_{il}| \le 1/2$. We want to see how the value of m_i changes when we update the values μ_{il} with respect to x_j for $l \le j$.

$$|\mu_{il} - x_j\mu_{jl}| \le |\mu_{il}| + |x_j|\cdot|\mu_{kl}| \le m_i + (m_i + \frac{1}{2})\cdot\frac{1}{2} \le \frac{3}{2}m_i + \frac{1}{4} \le 2m_i.$$

It follows that on a proprification phase, the value of m_i may increase by a factor of up to $2^{i-1} \le 2^n$, so we conclude

$$m_i^2 \le 2^{2n}A^n n \le n(4A)^n$$

hence we obtain the bound on the claim. □

If we summarize all the bonds that we have found, we obtain

$$\|b_k\| \le n(4A)^{(n+1)/2}, \quad \|D_{k-1}b_k^*\| \le A^{(2n+1)/2}, \quad |D_l\mu_{kl}| \le A^n D_{l-1}^{1/2}\|b_k\| \le A^n A^{n/2} n(4A)^{(n+1)/2}.$$

All in all, the integers in question are of the order $\tilde{O}(n\log A)$.

Theorem 6.5. *Let $A = \max_{1\le i\le n}\|b_i\|^2$. Then, the LLL algorithm*

- *finishes in $O(n^4\log A)$ operations over the integers of size $\tilde{O}(n\log A)$,*
- *requires $\tilde{O}(n^5\log^2 A)$ binary operations, and*
- *requires $\tilde{O}(n^3\log A)$ bits of space.*

6.2 An application: The minimal polynomial

Theorem 6.6. *Let $z \in \mathbb{C}$ and assume that there exists an irreducible polynomial $P = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$ that satisfies $P(z) = 0$ and $\|P\|_\infty = \max_{1\le k\le n}|a_k| < a$, and that we can compute $\tilde{z}(\epsilon) \in \mathbb{Q}(i)$ sich that $|z - \tilde{z}| < \varepsilon$ for all $\varepsilon > 0$ with*

$$\log\left(\frac{1}{\varepsilon}\right) = O(n^2\log A).$$

Then, we can find P in polynomial time, $O(n\log A)$.

Corollary 6.7. *We can factor in $\mathbb{Q}[x]$ in polynomial time.*

Proof. Consider $\tilde{z}$ an approximation of a root z of P, and compute its minimal polynomial D. (We can bound $\|D\|_\infty$ in terms of P with Mignotte's bound). Then, either P is irreducible, that is, we have $D = P$, or D is a factor of P and we can repeat the process with P/D. □

Idea of the proof of Theorem 6.6. We consider the lattice Λ generated by the columns of

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \\ C\,\mathrm{Re}(\tilde{z}^n) & \cdots & C\,\mathrm{Re}(\tilde{z}) & C \\ C\,\mathrm{Im}(\tilde{z}^n) & \cdots & C\,\mathrm{Im}(\tilde{z}) & 0 \end{pmatrix}$$

where C is a very big number.

Now let

$$v = \left(\lambda_n, \ldots, \lambda_0, C \operatorname{Re}\left(\sum_{k=0}^{n} \lambda_k \tilde{z}^k\right), C \operatorname{Im}\left(\sum_{k=0}^{n} \lambda_k \tilde{z}^k\right)\right)$$

be the first vector of a reduced basis of Λ.

For it to be short, we need

$$|C| \cdot \left|\operatorname{Re}\left(\sum_{k=0}^{n} \lambda_k \tilde{z}^k\right)\right|, |C| \cdot \left|\operatorname{Im}\left(\sum_{k=0}^{n} \lambda_k \tilde{z}^k\right)\right|$$

to be small, so if C is big enough, then they are zero, and we conclude that

$$Q(x) = \sum_{k=0}^{n} \lambda_k x^k$$

is the minimal polynomial of z. □