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 $n \leq d$, then we have

$$\Lambda = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$
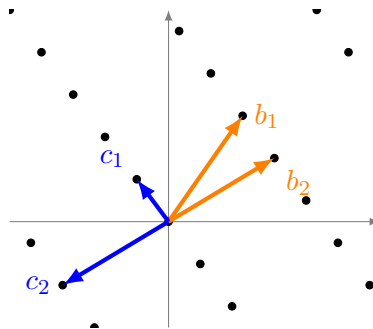
In general, we will consider the case $n = d$.

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 having $b_1, \ldots, b_n$ 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, $B(I_n - NM) = O$. Since B is nonsingular, we obtain $I_n - NM = 0$. Analogously one gets $I_n - MN = 0$, so we conclude that M is unimodular. $\qquad\square$

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,

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

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. $\square$

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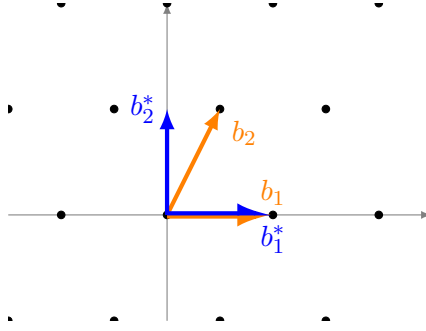
Figure 2: The GSO of the basis $\{b_1, b_2\}$ is not a basis of the original lattice because b_2^* is not an element of the original lattice.

3   Determinant of a lattice

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

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

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. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

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

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

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

The following result is obtained immediately from the inequality $||b_i^*|| \le ||b_i||$.
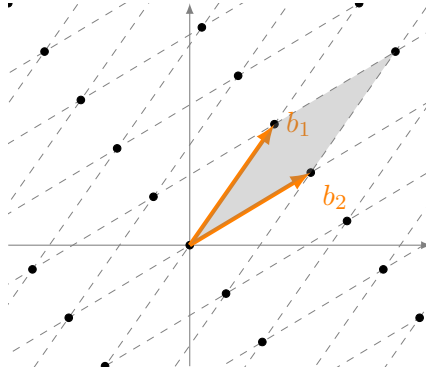
Figure 3: A lattice in $\mathbb{R}^2$, which is generated both by $\{b_1, b_2\}$, and by $\{c_1, c_2\}$.

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 $\lambda(\Lambda)$, the minimal length of a nonzero vector of Λ.

Given a basis (b_i), finding an element x such that $||x|| = \lambda(\Lambda)$ is an NP-complete problem.

Proposition 4.1. *Let B be the matrix representing a basis of a lattice Λ of rank n, and let B^* be its Gram-Schmidt orthogonalization. Then 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, 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 $\mathrm{vol}\, S > \det \Lambda$. 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

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

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:

---

   input : A basis $(b_i)_{1 \le i \le n}$ of Λ

   output: A *proper* basis $(c_i)_{1 \le i \le n}$ 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 $(b_i)_{1 \le i \le n}$

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 $c_1, \dots, c_{i-1}$ is proper, that is, for every $k < l \le i - 1$ we have $|\mu_{lk}| \le \frac{1}{2}$, and for every $j + 1 \le k \le i - 1$ we also have $|\mu_{ik}| \le \frac{1}{2}$. We will now prove $|\mu_{ij}| \le \frac{1}{2}$. Since we have

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

we write

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

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

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

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

for every $i < n$

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

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

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

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

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

from where we obtain

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

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

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

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

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

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

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

   (i) $\|x\| \ge \min\|b_i^*\|$,

   (ii) $\|b_1\| \le 2^{(n-1)/2}\|x\|$, and

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

Proof.   (i) It follows from Proposition 4.1.

  (ii) 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 $\|b_1\|^2 = \|b_1^*\|^2 \le 2^{k-1}\|b_k^*\|^2$, and by (i) we have $\|b_k^*\|^2 \le \|x\|^2$. Altogether we obtain

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

  (iii) Once again, since the basis (b_i) is Siegel-reduced, we have

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

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 $r_{ij} \ne 0$. By a reasoning analogous to the one in the proof of Proposition 4.1 we have

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

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

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

- 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.

$\square$

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

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