6.876 Advanced Topics in Cryptography: Lattices September 9, 2015

Lecture 1

Lecturer: Vinod Vaikuntanathan *Scribe: Vinod Vaikuntanathan*

Lattices are amazing mathematical objects with applications all over mathematics and theoretical computer science. Examples include

- **Sphere Packing:** A classical problem called the "Sphere Packing Problem" asks for a way to pack the largest number of spheres of equal volume in 3-dimensional space (in an asymptotic sense, as the volume of the available space goes to infinity). The so-called *Kepler's Conjecture*, recently turned into a theorem by Hales, states that the face-centered cubic lattice offers the optimal packing of spheres in 3 dimensions.

  The optimal sphere packing in 2 and 3 dimensions are lattice packings – could this be the case in higher dimensions as well? This remains a mystery.

- **Error Correcting Codes:** Generalizing to n dimensions, the sphere packing problem and friends have applications to constructing *error-correcting codes* with the optimal rate.

- **Number Theory:** In mathematics, the study of lattices is called the "Geometry of Numbers", a term coined by Hermann Minkowski. Minkowski's Theorem and subsequent developments have had an enormous impact on Number Theory, Functional Analysis and Convex Geometry. Lattices have been used to test various number theoretic conjectures, the most famous being a disproof of Merten's Conjecture by Odlyzko and te Riele in 1985.

Lattices have also been quite influential in Theoretical Computer Science:

- In **Algorithms:** The famed Lenstra-Lenstra-Lovász algorithm for the shortest vector problem has generated a treasure-trove of algorithmic applications. Lattices have been used to construct an Integer Linear Programming algorithm in constant dimensions, in factoring polynomials over the rationals, and algorithms to find small solutions to systems of polynomial equations.

- In **Complexity Theory:** Lattices provide one of the most striking sources of problems with a worst-case to average-case connection. NP-hard problems are widely believed to be hard in the worst case, but are they hard on typical or average instances? For many problems and many average-case distributions, we know that this is not the case. In contrast, for the (approximate) shortest vector problem, we can show that finding a solution in a "random lattice" chosen from a certain easily sampleable distribution is as hard as finding a solution in the worst case, namely for arbitrary lattices.

- In **Cryptography:** The first applications of lattices in Cryptography have been in breaking cryptosystems, for example, variants of the knapsack cryptosystem, the NTRU cryptosystem and special cases of the RSA function. More recently, however, lattices have been used quite successfully in constructing secure cryptographic algorithms that achieve highly expressive functionalities such as fully homomorphic encryption.

In this course, we will study lattices from the point of view of theoretical computer science, first the mathematics of lattices, then the algorithms and complexity theory and finally lattice-based cryptography.

Notation. We will denote the natural numbers by $\mathbb{N}$, integers by $\mathbb{Z}$, rationals by $\mathbb{Q}$ and the reals by $\mathbb{R}$.

1 Lattices

Definition 1 (Lattices)**.** *Given* n linearly independent *vectors* $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$*, the lattice generated by them is defined as*

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}$$

We call $\mathbf{b}_1, \ldots, \mathbf{b}_n$ a *basis* of the lattice. Note that the definition requires $\mathbf{b}_1, \ldots, \mathbf{b}_n$ to be linearly independent over $\mathbb{R}$ (and not over $\mathbb{Z}$).

We call n the *rank* of the lattice, and m the *dimension* of the lattice. In general, $n \leq m$. When $n = m$, we call the lattice a *full-rank* lattice. Throughout this course, we will focus on full-rank lattices – most results we prove can be generalized to the non full-rank case.

We will use a notational short-hand when dealing with bases, denoting them by a matrix $\mathbf{B}$ whose columns are the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. That is, we will write

$$\mathbf{B} = \begin{pmatrix} | & & | \\ \mathbf{b}_1 & \ldots & \mathbf{b}_n \\ | & & | \end{pmatrix}$$

and thus, in this notation,

$$\mathcal{L}(\mathbf{B}) \stackrel{\text{def}}{=} \{\mathbf{B}\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$$

In general, we treat all vectors as column vectors unless otherwise specified. For a matrix $\mathbf{B}$ (resp. row vector $\mathbf{v}$), $\mathbf{B}^T$ (resp. $\mathbf{v}^T$) denotes the transpose of $\mathbf{B}$ (resp. $\mathbf{v}$).

Examples of Lattices.

1. Figure 1(a) shows the lattice in 2 dimensions generated by the vectors $(1, 0)^T$ and $(0, 1)^T$. This lattice is the set of all points in $\mathbb{R}^2$ with integer coordinates.

   This can be generalized to n dimensions, where the lattice $\mathbb{Z}^n$ is called the *integer lattice*.

2. Figure 1(b) shows a different basis for the same lattice, namely the basis consisting of the vectors $(1, 2)^T$ and $(2, 3)^T$.

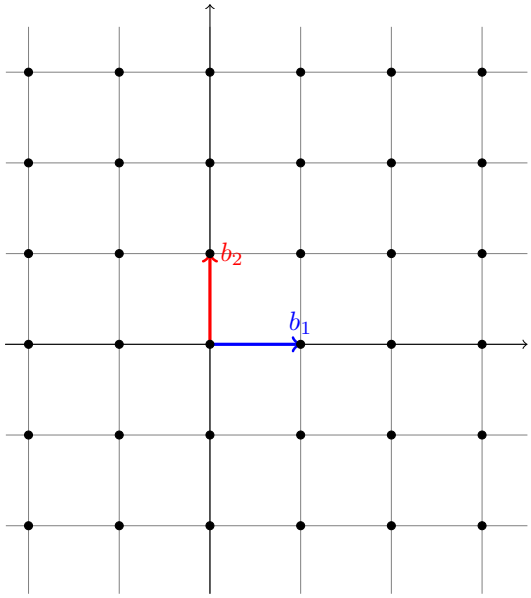
3. Figure 1(c) shows a different lattice in 2 dimensions, generated by the basis vectors $(2, 0)^T$ and $(1, 1)^T$. Note that this is a sub-lattice of $\mathbb{Z}^2$, namely a subset of $\mathbb{Z}^2$ which is also a lattice. (We will formally define sublattices later in the course).

4. In one dimension, all lattices are multiples of a single number. For example, the lattice generated by (2) is the set of all even numbers.

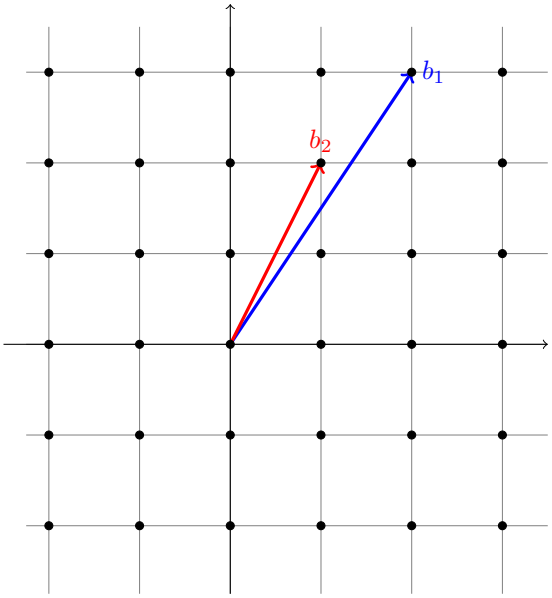
5. All the examples we saw so far are full-rank lattices. Figure 1(d) shows a lattice in 2 dimensions generated by the vector $(1, 1)^T$ – this lattice has rank 1. We will not deal with non full-rank lattices in this course.

6. The set of points generated by (1) and $(\sqrt{2})$ in one dimension is not a lattice. First, this example does not conform to Definition 1 since 1 and $\sqrt{2}$ are *linearly dependent* over $\mathbb{R}$. Secondly, any n-dimensional lattice is a discrete subset of $\mathbb{Z}^n$ (see Lecture 2 for why this is the case). However, the set generated by (1) and $(\sqrt{2})$ is not a discrete subset of $\mathbb{Z}$ since one can generate arbitrarily small numbers as linear combinations of 1 and $\sqrt{2}$.

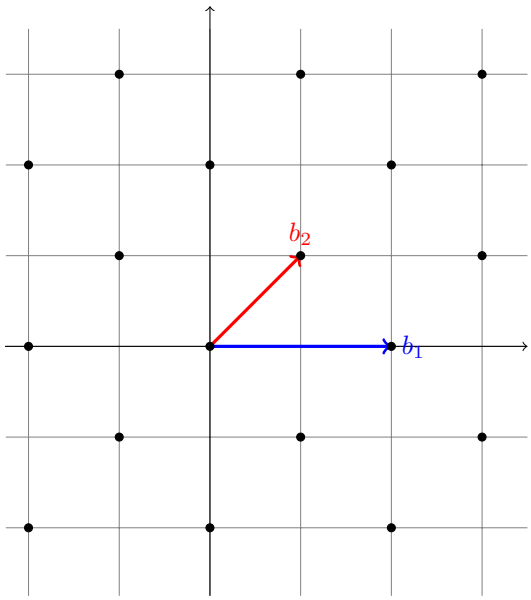
It is instructive to compare the definition of a lattice generated by n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ to the definition of the span of these vectors.



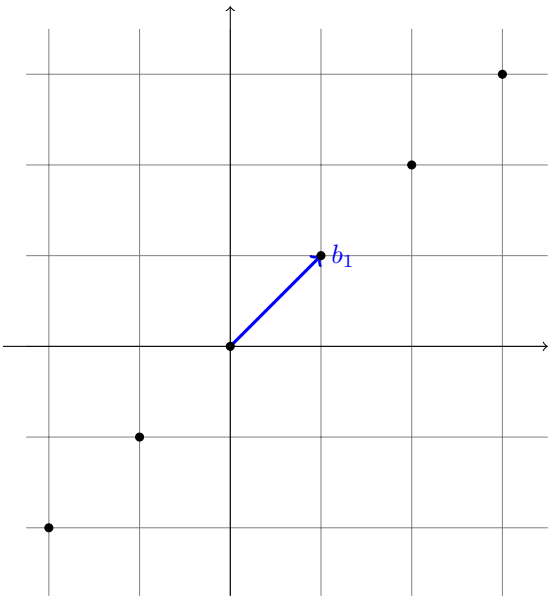
(a) The lattice $\mathbb{Z}^2$ with basis vectors $(0, 1)$ and $(1, 0)$.



(b) The lattice $\mathbb{Z}^2$ with a different basis consisting of vectors $(1, 2)$ and $(2, 3)$. In fact, any lattice has infinitely many bases.



(c) A full-rank lattice generated by the basis vectors $(1, 1)$ and $(2, 0)$. Note that this is a sub-lattice of $\mathbb{Z}^2$.



(d) A *non full-rank* lattice with basis vector $(1, 1)$

Figure 1: Various lattices and their bases.

Definition 2 (Span)**.** *Given* n linearly independent *vectors* $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$*, their* span *is defined as*

$$\mathsf{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \stackrel{\mathsf{def}}{=} \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{R} \right\}$$

Note the difference between Definition 1 of a lattice generated by a set of vectors – which consists of all of its *integer* linear combinations – and the above definition of the span of a set of vectors – which consists of all of its linear combinations with *real* coefficients. The crucial power of lattices comes from the fact that it is a discrete set (which the span is not).

Clearly, $\mathsf{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \supset \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

2 Same Lattice, Many Bases

We already saw from the examples above (Figure 1(a) and Figure 1(b)) that the same lattice can have many different bases. For example, it turns out that all the bases given below generate the same lattice, namely $\mathbb{Z}^2$:

$$\mathbf{B}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B}_2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B}_3 = \begin{pmatrix} 647 & 64 \\ 91 & 9 \end{pmatrix}$$

but the following basis *does not* generate $\mathbb{Z}^2$, but only a proper *sub-lattice* of $\mathbb{Z}^2$.

$$\mathbf{B}_4 = \begin{pmatrix} 42 & 41 \\ 9 & 8 \end{pmatrix}$$

In fact, any lattice has infinitely many bases. In particular, the bases can have arbitrarily large coefficients.

A natural question to ask is: *how can we efficiently tell if two given bases* $\mathbf{B}$ *and* $\mathbf{B}'$ *generate the same lattice?* We will give two answers to this question – an algebraic answer and a geometric answer.

2.1 An Algebraic Characterization using Unimodular Matrices

Our first characterization provides an efficient algorithm to determine if two bases generate the same lattice. In order to present the characterization, we first need to define the notion of a *unimodular matrix*.

Notation. For any $x \in \mathbb{R}$, we will let $|x|$ represent the absolute value of x.

Definition 3. *A matrix* $\mathbf{U} \in \mathbb{Z}^{n \times n}$ *is unimodular if* $|\det(\mathbf{U})| = 1$.

Here, $\det(\mathbf{U})$ denotes the determinant of the (square) matrix $\mathbf{U}$, and $|\cdot|$ denotes the absolute value. For example, the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ is unimodular, and so is $\left(\begin{smallmatrix} 647 & 64 \\ 91 & 9 \end{smallmatrix}\right)$, but not $\left(\begin{smallmatrix} 42 & 41 \\ 9 & 8 \end{smallmatrix}\right)$.

Proposition 4. *If* $\mathbf{U}$ *is unimodular, so is* $\mathbf{U}^{-1}$.

Proof. This follows from the way inverses are computed. In particular,

- Each entry in $\mathbf{U}^{-1}$ is the ratio of the determinant of a *minor* of $\mathbf{U}$ to the determinant of $\mathbf{U}$ itself. Since the determinant of any minor of $\mathbf{U}$ is an integer, and the determinant of $\mathbf{U}$ is ± 1, each entry of $\mathbf{U}^{-1}$ is an integer. Thus, $\mathbf{U}^{-1} \in \mathbb{Z}^{n \times n}$.
- $\det(\mathbf{U}^{-1}) = 1/\det(\mathbf{U}) = \pm 1$. Thus, $|\det(\mathbf{U}^{-1})| = 1$.

Together, these two observations mean that $\mathbf{U}$ is unimodular. □

We can now state the characterization of equivalent bases.

Theorem 5. *Given two full-rank bases* $\mathbf{B} \in \mathbb{R}^{n \times n}$ *and* $\mathbf{B}' \in \mathbb{R}^{n \times n}$*, the following two conditions are equivalent:*

- $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$
- *There exists a unimodular matrix* $\mathbf{U}$ *such that* $\mathbf{B}' = \mathbf{BU}$.

Proof. ("⇒") First, assume that $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$. Then, there are integer matrices $\mathbf{V}$ and $\mathbf{V}'$ such that

$$\mathbf{B}' = \mathbf{BV} \qquad \text{and} \qquad \mathbf{B} = \mathbf{B}'\mathbf{V}'$$

It suffices to show that $|\det(\mathbf{V})| = |\det(\mathbf{V}')| = 1$.

Putting these two equations together, we have $\mathbf{B}' = \mathbf{BV} = \mathbf{B}'(\mathbf{V}'\mathbf{V})$. Since $\mathbf{B}'$ is non-singular (remember: $\mathbf{B}$ is a full-rank matrix, and so is $\mathbf{B}'$) we can multiply both sides of the equation by $(\mathbf{B}')^{-1}$ and we get

$$\mathbf{V}'\mathbf{V} = \mathbf{1}_n \tag{1}$$

were $\mathbf{1}_n$ denotes the n-by-n identity matrix.

Since determinant is multiplicative, we get $\det(\mathbf{V}')\det(\mathbf{V}) = 1$. Since $\mathbf{V}$ and $\mathbf{V}'$ are integer matrices, their determinant is also an integer.

Putting these two facts together, we see that the only two choices are:

- $\det(\mathbf{V}) = \det(\mathbf{V}') = 1$, or
- $\det(\mathbf{V}) = \det(\mathbf{V}') = -1$

In either case, $|\det(\mathbf{V})| = |\det(\mathbf{V}')| = 1$, and we are done.

("⇐") For the other direction, assume that there is a unimodular matrix $\mathbf{U}$ such that $\mathbf{B}' = \mathbf{BU}$. Then, since $\mathbf{U}$ is an integer matrix,

$$\mathcal{L}(\mathbf{B}') \subseteq \mathcal{L}(\mathbf{B})$$

This is because each vector (column) of $\mathbf{B}'$ can be written as a linear combination of vectors in $\mathbf{B}$. Thus, the set of all integer linear combinations of vectors in $\mathbf{B}'$ is contained in the set of all integer linear combinations of vectors in $\mathbf{B}$.

Now, $\mathbf{B} = \mathbf{B}'(\mathbf{U}^{-1})$ where $\mathbf{U}^{-1}$ is also unimodular by Proposition 4. This shows that

$$\mathcal{L}(\mathbf{B}) \subseteq \mathcal{L}(\mathbf{B}')$$

by the same argument as above. Together, we have $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$. □

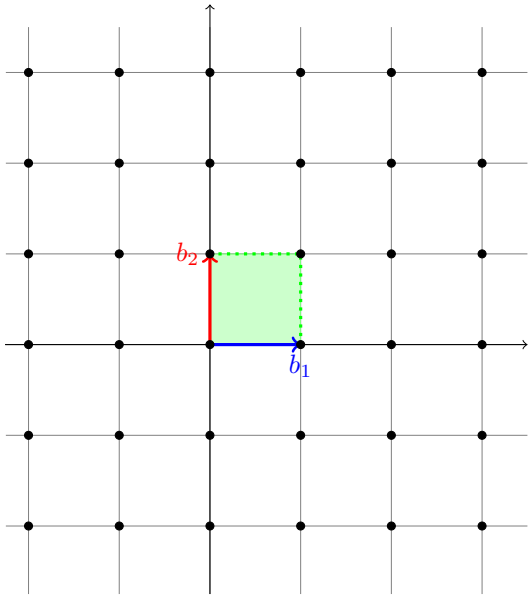
2.2 A Geometric Characterization using the Fundamental Parallelepiped

We need the notion of a fundamental parallelepiped of a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

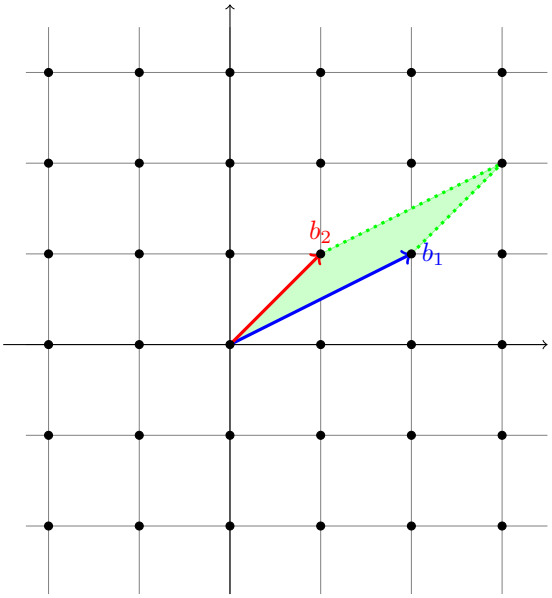
Definition 6 (Fundamental Parallelepiped)**.** *Given* n linearly independent *vectors* $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$*, their* fundamental parallelepiped *is defined as*

$$\mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{R}, 0 \leq x_i < 1 \right\}$$

Thus, pictorially, a fundamental parallelepiped is the (half-open) region enclosed by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Clearly, different bases of the same lattice generate different fundamental paralellepipeds. See Figure 2(a) and 2(b).



(a) The lattice $\mathbb{Z}^2$ with basis vectors $(0,1)$ and $(1,0)$ and the associated fundamental parallelepiped.



(b) The lattice $\mathbb{Z}^2$ with a different basis consisting of vectors $(1,1)$ and $(2,1)$, and the associated fundamental parallelepiped.

Figure 2: Parallelepipeds for various bases of the lattice $\mathbb{Z}^2$. Note that the parallelepipeds in either case do not contain any non-zero lattice point.

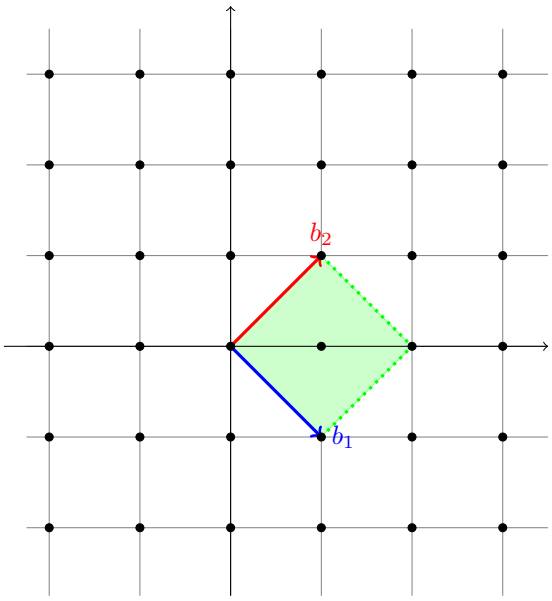


Figure 3: $\mathbf{b}_1$ and $\mathbf{b}_2$ do not form a basis of $\mathbb{Z}^2$. Note that the parallelepiped of $\mathbf{b}_1$ and $\mathbf{b}_2$ contains a non-zero lattice point, namely $(1,0)$.

Note that in Figures 2(a) and 2(b), the vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ form a basis of the lattice, and the parallelepiped associated to the basis does not contain any lattice point other than $\mathbf{0}$. On the other hand, in Figure 3, the vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ do not form a basis of the lattice, and the parallelepiped associated to the basis contains a non-zero lattice point. In fact, this is not a coincidence as our next theorem shows.

Theorem 7. *Let $\mathcal{L}$ be a full-rank n-dimensional lattice, and let $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$ denote* linearly independent *vectors in $\mathcal{L}$. Then, $\mathbf{b}_1, \ldots, \mathbf{b}_n$ form a basis of $\mathcal{L}$* if and only if $\mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \cap \mathcal{L} = \{\mathbf{0}\}$.

Proof. ("⇒") Suppose that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a basis of $\mathcal{L}$. Let

$$\mathbf{a} = \sum_{i=1}^{n} x_i \mathbf{b}_i \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \cap \mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$$

We will show that $\mathbf{a} = \mathbf{0}$.

Since $\mathbf{a} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, $x_i \in \mathbb{Z}$ for all i. Since $\mathbf{a} \in \mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, $x_i \in [0, 1)$ for all i. Together, this means that $x_i = 0$ for all i, and thus, $\mathbf{a} = \mathbf{0}$.

("⇐") Suppose that $\mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \cap \mathcal{L} = \{\mathbf{0}\}$. We would like to show that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ form a basis of $\mathcal{L}$.

The vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are linearly independent. Since they belong to $\mathcal{L}$, $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \subseteq \mathcal{L}$. What remains is to show that $\mathcal{L} \subseteq \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Pick any vector $\mathbf{a} \in \mathcal{L}$ and write it as

$$\mathbf{a} = \sum_{i=1}^{n} x_i \mathbf{b}_i \qquad \text{where } x_i \in \mathbb{R}$$

Consider now the vector

$$\mathbf{a}' = \sum_{i=1}^{n} \lfloor x_i \rfloor \, \mathbf{b}_i \qquad \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$$

which is clearly in the lattice $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ since the coefficients $\lfloor x_i \rfloor$ are integers. Therefore, the vector $\mathbf{a} - \mathbf{a}'$ is in $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ as well. Now,

$$\mathbf{a} - \mathbf{a}' = \sum_{i=1}^{n} (x_i - \lfloor x_i \rfloor) \mathbf{b}_i \qquad \in \mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$$

is in the parallelepiped of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ since $0 \leq x_i - \lfloor x_i \rfloor < 1$ for all i.

Since $\mathbf{a} - \mathbf{a}' \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \cap \mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, it must be the case that $\mathbf{a} - \mathbf{a}' = 0$ by assumption. Since the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are linearly independent, this means that $x_i - \lfloor x_i \rfloor = 0$ for all i which in turn means that $x_i \in \mathbb{Z}$ for all i.

Thus, $\mathbf{a} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, showing us that $\mathcal{L} \subseteq \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. □

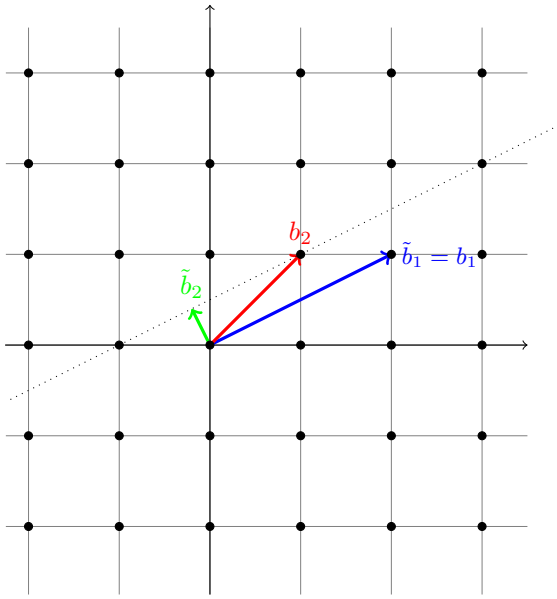
2.3 Determinant of a Lattice

Another quantity associated to a lattice is its determinant, denoted $\det(\mathcal{L})$. The determinant of a lattice is the n-dimensional volume of its fundamental parallelepiped, computed as the absolute value of the determinant of its basis matrix $\mathbf{B}$. A couple of facts about the determinant of a lattice are worth noting:

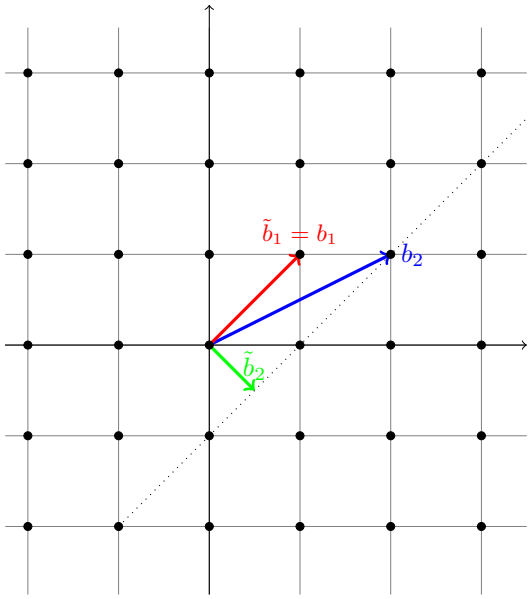
1. The parallelepipeds associated with different bases of a lattice have the same volume. Thus, *the determinant is a lattice invariant.* This is easy to see using our characterization of equivalent bases from Theorem 5.

   Let $\mathbf{B}$ and $\mathbf{B}'$ be any two lattice bases. By Theorem 5, there is a unimodular matrix $\mathbf{U}$ such that $\mathbf{B}' = \mathbf{B}\mathbf{U}$. Thus, $|\det(\mathbf{B}')| = |\det(\mathbf{B})| \cdot |\det(\mathbf{U})| = |\det(\mathbf{B})|$ since $|\det(\mathbf{U})| = 1$.

2. Intuitively, the determinant of a lattice is inversely proportional to its "density". The larger the determinant, the sparser the lattice.



(a) Gram-Schmidt orthogonalization of the vectors b_1 and b_2 in that order.



(b) Gram-Schmidt orthogonalization of the same vectors, but in the opposite order.

Figure 4: Gram-Schmidt Orthogonalization.

3 Gram-Schmidt Orthogonalization

Gram-Schmidt orthogonalization is a procedure in linear algebra that transforms a set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ into a set of orthogonal vectors $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n$. In two dimensions, this proceeds as follows:

- The first Gram-Schmidt vector $\tilde{\mathbf{b}}_1$ is $\mathbf{b}_1$ itself.
- The second Gram-Schmidt vector $\tilde{\mathbf{b}}_2$ is the component of $\mathbf{b}_2$ that is orthogonal to $\mathsf{Span}(\tilde{\mathbf{b}}_1)$. This can be computed as

$$\tilde{\mathbf{b}}_2 = \mathbf{b}_2 - \left(\frac{\langle \mathbf{b}_2, \tilde{\mathbf{b}}_1 \rangle}{\langle \tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_1 \rangle}\right) \tilde{\mathbf{b}}_1$$

  See Figure 4 for an illustration of this process.

In general, the Gram-Schmidt vectors are obtained by projecting each vector successively on the space orthogonal to the span of all the previous vectors.

Definition 8 (Gram-Schmidt Orthogonalization)**.** *For a sequence of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$, we define their* Gram-Schmidt orthogonalization *as the sequence of vectors $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n$ defined as follows:*

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\mathbf{b}}_j \qquad \text{where } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle}$$

Thus, $\tilde{\mathbf{b}}_j$ is the component of $\mathbf{b}_i$ that is orthogonal to $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_{i-1}$. The coefficients $\mu_{i,j}$ are called the Gram-Schmidt coefficients.

Remarks.

1. True to its name, the different Gram-Schmidt vectors $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n$ are orthogonal to each other. That is, for each $i \neq j$, $\langle \tilde{\mathbf{b}}_i, \tilde{\mathbf{b}}_j \rangle = 0$. This is an easy consequence of Definition 8.
2. The span of $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_i$ is the same as the span of $\mathbf{b}_1, \ldots, \mathbf{b}_i$ for all $1 \leq i \leq n$.
3. The vectors $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n$ do not form a lattice basis. In fact, the Gram-Schmidt vectors are not necessarily in the lattice. See Figure 4 for example.
4. The (Euclidean) length of the Gram-Schmidt vector $\tilde{\mathbf{b}}_i$ is at most the length of the basis vector $\mathbf{b}_i$. Namely, $\|\tilde{\mathbf{b}}_i\| \leq \|\mathbf{b}_i\|$.
5. Clearly, as seen in Figure 4, the Gram-Schmidt vectors depend on the order in which the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are processed.

Let $\tilde{\mathbf{b}}_1/\|\tilde{\mathbf{b}}_1\|, \ldots, \tilde{\mathbf{b}}_n/\|\tilde{\mathbf{b}}_n\|$ denote the unit vectors in the direction of the Gram-Schmidt vectors. Then, the Gram-Schmidt orthogonalization process can be written in matrix form as

$$\begin{pmatrix} | & & | \\ \mathbf{b}_1 & \cdots & \mathbf{b}_n \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ \tilde{\mathbf{b}}_1 & \cdots & \tilde{\mathbf{b}}_n \\ | & & | \end{pmatrix} \cdot \begin{pmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & \cdots & \mu_{n,2} \\ 0 & 0 & 1 & \cdots & \mu_{n,3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} | & & | \\ \frac{\tilde{\mathbf{b}}_1}{\|\tilde{\mathbf{b}}_1\|} & \cdots & \frac{\tilde{\mathbf{b}}_n}{\|\tilde{\mathbf{b}}_n\|} \\ | & & | \end{pmatrix} \cdot \begin{pmatrix} \|\tilde{\mathbf{b}}_1\| & \mu_{2,1}\|\tilde{\mathbf{b}}_1\| & \mu_{3,1}\|\tilde{\mathbf{b}}_1\| & \cdots & \mu_{n,1}\|\tilde{\mathbf{b}}_1\| \\ 0 & \|\tilde{\mathbf{b}}_2\| & \mu_{3,2}\|\tilde{\mathbf{b}}_2\| & \cdots & \mu_{n,2}\|\tilde{\mathbf{b}}_2\| \\ 0 & 0 & \|\tilde{\mathbf{b}}_3\| & \cdots & \mu_{n,3}\|\tilde{\mathbf{b}}_3\| \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \|\tilde{\mathbf{b}}_n\| \end{pmatrix}$$

Since the vectors $\frac{\tilde{\mathbf{b}}_i}{\|\tilde{\mathbf{b}}_i\|}$ are orthonormal, the determinant of the matrix with columns $\frac{\tilde{\mathbf{b}}_i}{\|\tilde{\mathbf{b}}_i\|}$ is 1.

Thus, we have

$$\det(\mathcal{L}(\mathbf{B})) = \prod_{i=1}^{n} \|\tilde{\mathbf{b}}_i\|$$

In other words, the Gram-Schmidt orthogonalization process is a volume-preserving transformation that results in a set of orthogonal vectors $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n$, whose enclosing parallelepiped is rectangular and generates a volume of $\prod_{i=1}^{n} \|\tilde{\mathbf{b}}_i\|$.

4 Successive Minima of a Lattice

A basic parameter of the lattice is the length of the shortest non-zero vector in the lattice (since any lattice contains the zero vector which has norm zero, we have to ask for a non-zero vector). This parameter is also called the *first successive minimum* of the lattice, and is denoted $\lambda_1(\mathcal{L})$. When we speak of length, we mean the Euclidean norm defined as follows: for a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, the Euclidean norm of $\mathbf{x}$, denoted $\|\mathbf{x}\|_2$ (or simply as $\|\mathbf{x}\|$ is defined as

$$\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2}$$

The Euclidean norm is also frequently referred to as the ℓ_2 norm. We can speak of other norms such as the ℓ_1 norm – $\|\mathbf{x}\|_1 = \sum_{i=1}^{n} |x_i|$ – and the ℓ_∞ norm – $\|\mathbf{x}\|_\infty = \max_{i=1}^{n} |x_i|$, but we will stick to the Euclidean norm for most of this course.

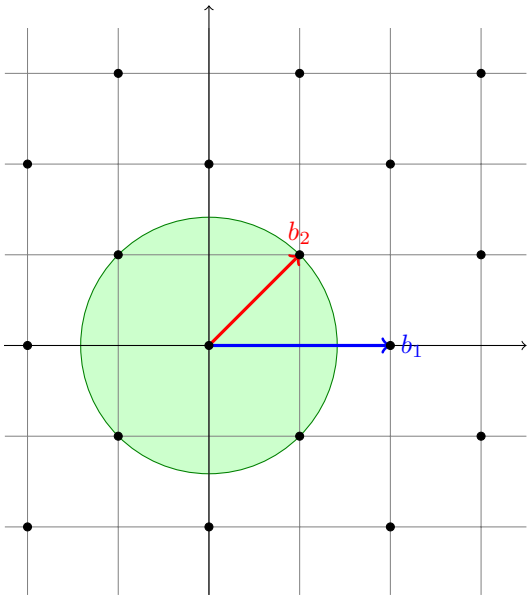


Figure 5: The shortest vector in the lattice generated by $(1,1)$ and $(2,0)$. $\lambda_1(\mathcal{L}) = \sqrt{2}$.

Figure 5 shows a shortest vector in the lattice generated by $(1,1)$ and $(2,0)$. The shortest vector is not unique in general. There could be many, even exponentially many, shortest vectors. Clearly, there are at least two – if $\mathbf{v}$ is a shortest vector in a lattice, then so is $-\mathbf{v}$.

We will be interested in lower and upper bounds on λ_1. We first show a lower bound on λ_1 using Gram-Schmidt orthogonalization. In the next lecture, we will prove Minkowski's theorem which provides an upper bound on λ_1 in terms of the determinant of the lattice.

Lower Bound on λ_1. We show the following theorem. Roughly speaking, the theorem says that the shortest non-zero vector in a lattice is at least as long as the shortest Gram-Schmidt vector of a basis of the lattice. To see why, observe that a lattice can be partitioned into many hyperplanes perpendicular to its Gram-Schmidt vector $\tilde{\mathbf{b}}_n$. See Figure 6 for an illustration in two dimensions.

Now, there are two possibilities:

- There is a shortest non-zero vector in one of the hyper-planes not passing through the origin. In that case, the vector has to have length at least $\|\tilde{\mathbf{b}}_n\| \geq \min_j \|\tilde{\mathbf{b}}_j\|$ since the i^{th} such hyper-plane is at a distance of $i \cdot \|\tilde{\mathbf{b}}_n\|$ from the origin.
- The shortest non-zero vector lives in the hyper-plane that passes through the origin, in which case, repeat the same argument in dimension $n-1$ with the $(n-1)$-dimensional sublattice partitioned into hyper-planes perpendicular to $\tilde{\mathbf{b}}_{n-1}$.

Eventually, if the argument reaches dimension 1, the shortest non-zero vector has to have length at least $\|\mathbf{b}_1\| = \|\tilde{\mathbf{b}}_1\| \geq \min_j \|\tilde{\mathbf{b}}_j\|$.

The formal statement and proof of the theorem follows.

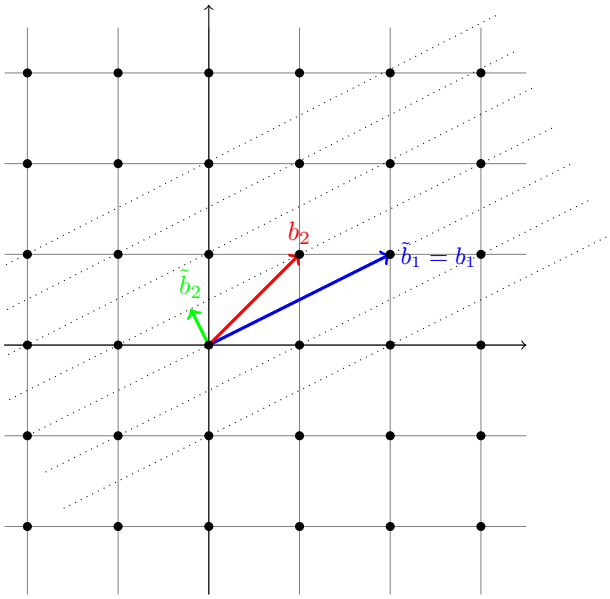


Figure 6: The lattice is partitioned into many parallel hyperplanes perpendicular to $\tilde{\mathbf{b}}_2$. Either the shortest vector lives in a hyperplane that does not pass through the origin, in which case its length is at least $\|\tilde{\mathbf{b}}_2\|$ or it lives in the hyperplane that passes through the origin, in which case its length is at least $\tilde{\mathbf{b}}_1 = \|\tilde{\mathbf{b}}_1\|$. In general, in two dimensions, $\lambda_1(\mathcal{L}) \geq \min\{\|\tilde{\mathbf{b}}_1\|, \|\tilde{\mathbf{b}}_2\|\}$. This argument can be generalized to n dimensions.

Theorem 9. *Let* $\mathbf{B}$ *be a rank-*n *lattice basis, and* $\tilde{\mathbf{B}}$ *be its Gram-Schmidt orthogonalization. Then,*

$$\lambda_1(\mathcal{L}(\mathbf{B})) \geq \min_{i=1,\ldots,n} \|\tilde{\mathbf{b}}_i\| > 0$$

Proof. Let $\mathbf{x} \in \mathbb{Z}^n$ be *any* non-zero integer vector. We would like to show that the lattice vector $\mathbf{Bx} \in \mathcal{L}(\mathbf{B})$ has length at least $\min_i \|\tilde{\mathbf{b}}_i\|$.

The proof follows by calculating the quantity $|\langle \mathbf{Bx}, \tilde{\mathbf{b}}_j \rangle|$ in two different ways.

1. Let $j \in \{1, \ldots, n\}$ be the largest index such that $x_j \neq 0$. Then,

$$|\langle \mathbf{Bx}, \tilde{\mathbf{b}}_j \rangle| = |\langle \sum_{i=1}^{n} x_i \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle| = |\sum_{i=1}^{n} x_i \langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle| = |x_j| \langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle = |x_j| \cdot \|\tilde{\mathbf{b}}_j\|^2 \tag{2}$$

where the first equality follows by rewriting $\mathbf{Bx}$ as $\sum_{i=1}^{n} x_i \mathbf{b}_i$, the second follows by the linearity of the inner product, and the third because

- for $j < i$, $\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle = 0$
- for $j > i$, $x_j = 0$ by the definition of j.

The fourth equality follows by the definition of $\|\tilde{\mathbf{b}}_j\|^2 = \langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle$.

2. On the other hand,

$$|\langle \mathbf{Bx}, \tilde{\mathbf{b}}_j \rangle| \leq \|\mathbf{Bx}\| \cdot \|\tilde{\mathbf{b}}_j\| \tag{3}$$

by the Cauchy-Schwarz inequality.

Putting together Equations 2 and 3, we get

$$\|\mathbf{Bx}\| \geq \frac{|\langle \mathbf{Bx}, \tilde{\mathbf{b}}_j \rangle|}{\|\tilde{\mathbf{b}}_j\|} = |x_j| \cdot \|\tilde{\mathbf{b}}_j\| \geq \|\tilde{\mathbf{b}}_j\| \geq \min_{i=1\ldots n} \|\tilde{\mathbf{b}}_i\|$$

where the third inequality follows from the fact that x_j is a non-zero integer. Since the length of any lattice vector is at least $\min_i \|\tilde{\mathbf{b}}_i\|$,

$$\lambda_1(\mathbf{B}) \geq \min_{i=1\ldots n} \|\tilde{\mathbf{b}}_i\|$$

Since $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are linearly independent, this quantity is strictly positive. □

A corollary of this theorem is that a lattice is a *discrete set*. In other words, lattice points cannot be arbitrarily close to one another. Formally:

Corollary 10. *For every lattice $\mathcal{L}$, there is an $\epsilon = \epsilon(\mathcal{L}) > 0$ such that $\|\mathbf{x} - \mathbf{y}\| \geq \epsilon$ for any two unequal lattice points $\mathbf{x}, \mathbf{y} \in \mathcal{L}$.*

Proof. For any two $\mathbf{x} \neq \mathbf{y} \in \mathcal{L}$, $\mathbf{x} - \mathbf{y} \in \mathcal{L}$. Then, $\|\mathbf{x} - \mathbf{y}\| \geq \lambda_1(\mathcal{L}) > 0$. In particular, set $\epsilon = \lambda_1(\mathcal{L})$ to obtain the statement of the corollary. □

In fact, this leads us to a *basis-independent* characterization of a lattice. Namely, every discrete subset of $\mathbb{R}^n$ that is closed under subtraction is a lattice.