CSE 206A: Lattice Algorithms and Applications Winter 2012

1: Introduction to Lattices

Instructor: *Daniele Micciancio* UCSD CSE

Lattices are regular arrangements of points in Euclidean space. The simplest example of lattice in n-dimensional space is $\mathbb{Z}^n$, the set of all n-dimensional vectors with integer entries. More generally, a lattice is the result of applying a nonsingular[1] linear transformation $\mathbf{B} \in \mathbb{R}^{d \times n}$ to the integer lattice $\mathbb{Z}^n$, to obtain the set $\mathbf{B}(\mathbb{Z}^n) = \{\mathbf{Bx} \colon \mathbf{x} \in \mathbb{Z}^n\}$.

Despite the simplicity of their definition, lattices are powerful objects that allow to apply geometric techniques to the solution of hard combinatorial problems. Lattices naturally occur in many settings, like crystallography, sphere packings (stacking oranges), communication theory, mathematics, etc. They have many applications in computer science and mathematics, including the solution of integer programming problems, diophantine approximation, cryptanalysis, the design of error correcting codes for multi antenna systems, and many more. Recently, lattices have also attracted much attention as a source of computational hardness for the design of secure cryptographic functions, and they are a powerful tool for the construction of the most advanced cryptographic primitives, including fully homomorphic encryption schemes.

This course offers an introduction to lattices. We will study the best currently known algorithms to solve the most important lattice problems, and how lattices are used in several representative applications, focusing on cryptography. We begin with the definition of lattices and their most important mathematical properties.

1. Lattices and Bases

Definition 1. Let $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_k] \in \mathbb{R}^{d \times n}$ be linearly independent vectors in $\mathbb{R}^d$. The lattice generated by $\mathbf{B}$ is the set

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} \colon \mathbf{x} \in \mathbb{Z}^n\} = \left\{ \sum_{i=1}^{n} x_i \cdot \mathbf{b}_i \colon x_i \in \mathbb{Z} \right\}$$

of all the *integer* linear combinations of the columns of $\mathbf{B}$. The matrix $\mathbf{B}$ is called a *basis* for the lattice $\mathcal{L}(\mathbf{B})$. The integer n is called the *dimension* or *rank* of the lattice. If $n = k$ then $\mathcal{L}(\mathbf{B})$ is called a *full rank* lattice.

Definition 1 also gives a simple way to represent a lattice (which is an infinite set of points) by a finite object: lattices can be represented by a basis matrix $\mathbf{B}$. In computer science applications, the basis matrix typically has integer or rational entries, and can be easily represented as an array of integers.

Notice the similarity between the definition of a lattice

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{B} \cdot \mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}.$$

[1] Here *nonsingular* means that the linear transformation $\mathbf{x} \mapsto \mathbf{Bx}$ from $\mathbb{R}^n$ to $\mathbb{R}^k$ defined by $\mathbf{B}$ is injective. We recall that this is true if and only if the columns of $\mathbf{B}$ are linearly independent, i.e., the only $\mathbf{x} \in \mathbb{R}^n$ such that $\mathbf{Bx} = \mathbf{0}$ is $\mathbf{x} = \mathbf{0}$.

and the definition of vector space generated by $\mathbf{B}$:

$$\text{span}(\mathbf{B}) = \{\mathbf{B} \cdot \mathbf{x} \colon \mathbf{x} \in \mathbb{R}^n\}.$$

The difference is that in a vector space you can combine the columns of $\mathbf{B}$ with arbitrary real coefficients, while in a lattice only integer coefficients are allowed, resulting in a discrete set of points. Notice that, since vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are linearly independent, any point $\mathbf{y} \in \text{span}(\mathbf{B})$ can be written as a linear combination $\mathbf{y} = x_1\mathbf{b}_1 + \cdots x_n\mathbf{b}_n$ with $\mathbf{x} \in \mathbb{R}^n$in a unique way. Therefore $\mathbf{y} \in \mathcal{L}(\mathbf{B})$ if and only if $\mathbf{x} \in \mathbb{Z}^n$.

If $\mathbf{B}$ is a basis for the lattice $\mathcal{L}(\mathbf{B})$, then it is also a basis for the vector space span($\mathbf{B}$). However, not every basis for the vector space span($\mathbf{B}$) is also a lattice basis for $\mathcal{L}(\mathbf{B})$. For example $2\mathbf{B}$ is a basis for span($\mathbf{B}$) as a vector space, but it is not a basis for $\mathcal{L}(\mathbf{B})$ as a lattice because vector $\mathbf{b}_i \in \mathcal{L}(\mathbf{B})$ (for any i) is not an *integer* linear combination of the vectors in $2\mathbf{B}$.

Definition 2. A matrix $\mathbf{U} \in \mathbb{Z}^{n\times n}$ is unimodular[2] if it has a multiplicative inverse in $\mathbb{Z}^{n\times n}$, i.e., there is a matrix $\mathbf{V} \in \mathbb{Z}^{n\times n}$ such that $\mathbf{VU} = \mathbf{UV} = \mathbf{I}$.

Proposition 3. *Unimodular matrices satisfy the following properties:*

(1) *If* $\mathbf{U}$ *is unimodular, then* $\mathbf{U}^{-1}$ *is also unimodular*
(2) *If* $\mathbf{U}$ *and* $\mathbf{V}$ *are unimodular, then* $\mathbf{UV}$ *is also unimodular*
(3) $\mathbf{U} \in \mathbb{Z}^{n\times n}$ *is unimodular if and only if* $\det(\mathbf{U}) = \pm 1$

Proof. See Exercises. □

The same lattice can be represented by several different bases. Unimodular matrices can be used to relate different bases of the same lattice.

Theorem 4. *Let* $\mathbf{B}$ *and* $\mathbf{C}$ *be two bases. Then* $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{C})$ *if and only if there exists a unimodular matrix* $\mathbf{U}$ *such that* $\mathbf{B} = \mathbf{CU}$.

Proof. First assume $\mathbf{B} = \mathbf{CU}$ for some unimodular matrix $\mathbf{U}$. Notice that Proposition 3 if $\mathbf{U}$ is unimodular, then $\mathbf{U}^{-1}$ is also unimodular. In particular, both $\mathbf{U}$ and $\mathbf{U}^{-1}$ are integer matrices, and $\mathbf{B} = \mathbf{CU}$ and $\mathbf{C} = \mathbf{BU}^{-1}$. It follows that $\mathcal{L}(\mathbf{B}) \subseteq \mathcal{L}(\mathbf{C})$ and $\mathcal{L}(\mathbf{C}) \subseteq \mathcal{L}(\mathbf{B})$, i.e., the two matrices $\mathbf{B}$ and $\mathbf{C}$ generate the same lattice.

Now assume $\mathbf{B}$ and $\mathbf{C}$ are two bases for the same lattice $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{C})$. Then, by definition of lattice, there exist integer square matrices $\mathbf{V}$ and $\mathbf{U}$ such that $\mathbf{B} = \mathbf{CU}$ and $\mathbf{C} = \mathbf{BV}$. Combining these two equations we get $\mathbf{B} = \mathbf{BVU}$, or equivalently, $\mathbf{B}(\mathbf{I} - \mathbf{VU}) = \mathbf{O}$. Since $\mathbf{B}$ is nonsingular, it must be $\mathbf{I} - \mathbf{VU} = \mathbf{O}$, i.e., $\mathbf{VU} = \mathbf{I}$ and $\mathbf{U}$ is unimodular. □

A simple way to obtain a basis of a lattice from another is to apply (a sequence of) elementary column operations, as defined below.

Definition 5. Elementary (integer) column operations on a matrix $\mathbf{B} \in \mathbb{R}^{d\times k}$ are:

(1) swap(i,j):$(\mathbf{b}_i, \mathbf{b}_j) \leftarrow (\mathbf{b}_j, \mathbf{b}_i)$. (Exchange two basis bectors)
(2) invert(i): $\mathbf{b}_i \leftarrow -\mathbf{b}_i$. (Change the sign of a basis vector)
(3) add(i,c,j):$\mathbf{b}_i \leftarrow (\mathbf{b}_i + c \cdot \mathbf{b}_j)$ where $i \neq j$ and $c \in \mathbb{Z}$. (Add an integer multiple of a basis vector to another)

[2]Unimodular matrices are usually defined as integer square matrices with determinant ± 1. The next proposition shows that the two definitions are equivalent.

It is easy to see that elementary column operations do not change the lattice generated by the basis because they can be expressed as right multiplication by a unimodular matrix.

Exercise 6. Give unimodular matrices corresponding to the elementary column operations swap(i,j), invert(i) and add(c,i,j) for $c \in \mathbb{Z}$ and $i, j \in \{1, ..., n\}$,$i \neq j$. For each operation, prove that your matrix is indeed unimodular by giving the inverse matrix and showing that it has integer entries. Give also an English description of the operation specified by the inverse matrix.

As we will prove later, any unimodular transformation can be expressed as a sequence of elementary integer column operations. So, two bases of the same lattice can always be related by a sequence of elementary column operations.

2. Gram-Schmidt orthogonalization

Any basis $\mathbf{B}$ can be transformed into an orthogonal basis for the same vector space using the well-known Gram-Schmidt orthogonalization method. Suppose we have vectors $\mathbf{B} = [\mathbf{b}_1|\dots|\mathbf{b}_n] \in \mathbb{R}^{d\times n}$ generating a vector space $V = \text{span}(\mathbf{B})$. These vectors are not necessarily orthogonal (or even linearly independent), but we can always find an orthogonal basis $\mathbf{B}^* = [\mathbf{b}_1^*|\dots|\mathbf{b}_n^*]$ for V where $\mathbf{b}_i^*$ is the component of $\mathbf{b}_i$ orthogonal to $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})$.

Definition 7. For any sequence of vectors $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$, define the orthogonalized vectors $\mathbf{B}^* = [\mathbf{b}_1^*|\dots|\mathbf{b}_n^*]$ iteratively according to the formula

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j}\mathbf{b}_j^* \text{ where } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}.$$

Exercise 8. Verify that the Gram-Schmidt vectors $\mathbf{B}^*$are indeed mutually orthogonal (i.e., $\langle \mathbf{b}_i^*, \mathbf{b}_j^* \rangle = 0$ for all $i \neq j$) and they span the same space as $\mathbf{B}$.

In matrix notation, $\mathbf{B} = \mathbf{B}^*\mathbf{T}$ where $\mathbf{T}$ is the upper triangular matrix with 1 along the diagonal and $t_{j,i} = \mu_{i,j}$ for all $j < i$. It also follows that $\mathbf{B}^* = \mathbf{B}\mathbf{T}^{-1}$ where $\mathbf{T}^{-1}$ is also upper triangular with 1 along the diagonal. Since the columns of $\mathbf{B}^*$ are mutually orthogonal, the (non-zero) columns of $\mathbf{B}^*$ are linearly independent and they form a basis for the vector space $\text{span}(\mathbf{B})$. However they are generally not a basis for the lattice $\mathcal{L}(\mathbf{B})$.

Example 9. The Gram-Schmidt orthogonalization of the basis $\mathbf{B} = [(2, 0)^\top, (1, 2)^\top]$ is $\mathbf{B}^* = [(2, 0)^\top, (0, 2)^\top]$. However this is not a lattice basis for $\mathcal{L}(\mathbf{B})$ because the vector $(0, 2)^T$ does not belong to the lattice. $\mathcal{L}(\mathbf{B})$ contains a sublattice generated by a pair of orthogonal vectors $(2, 0)^\top$ and $(0, 4)^\top$, but no pair of orthogonal vectors generate the entire lattice $\mathcal{L}(\mathbf{B})$.

So, while vector spaces always admit an orthogonal basis, this is not true for lattices.

3. The determinant

Definition 10. Given a basis $\mathbf{B} = [\mathbf{b_1}, ..., \mathbf{b_n}] \in \mathbb{R}^{k\times n}$, the *fundamental parallelepiped* associated to $\mathbf{B}$ is the set of points

$$\mathcal{P}(\mathbf{B}) = \mathbf{B}[0, 1)^n = \{\Sigma_{i=1}^n x_i \cdot \mathbf{b_i} \colon 0 \leq x_i < 1\}.$$

Remark 11. Note that $\mathcal{P}(\mathbf{B})$ is half-open, so that the translates $\mathcal{P}(\mathbf{B}) + \mathbf{v}$ (for $\mathbf{v} \in \mathcal{L}(\mathbf{B})$) form a partition of the whole space $\text{span}(\{)\mathbf{B}\}$. More precisely, for any $\mathbf{x} \in \text{span}(\{)\mathbf{B}\}$, there exists a unique lattice point $\mathbf{v} \in \mathcal{L}(\mathbf{B})$, such that $\mathbf{x} \in (\mathbf{v} + \mathcal{P}(\mathbf{B}))$.

We now define a fundamental quantity associated to any lattice, the determinant.

Definition 12. Let $\mathbf{B} \in \mathbb{R}^{d \times n}$ be a basis. The determinant of a lattice $\det(\mathcal{L}(\mathbf{B}))$ is defined as the n-dimensional volume of the fundamental parallelepiped associated to $\mathbf{B}$:

$$\det(\mathcal{L}(B)) = \mathrm{vol}(\mathcal{P}(\mathbf{B})) = \prod_i \|\mathbf{b}_i^*\|$$

where $\mathbf{B}^*$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$.

The above formula for the determinant of a lattice is a generalization of the well known formula for the area of a parallelepiped. Geometrically, the determinant represents the inverse of the density of lattice points in space (e.g., the number of lattice points in a large and sufficiently regular region of space A should be approximately equal to the volume of A divided by the determinant.) In particular, the determinant of a lattice does not depent on the choice of the basis. We will prove this formally later in this lecture.

The next simple upper bound on the determinant *(Hadamard inequality)* immediately follows from the fact that $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\|$.

Theorem 13. *For any lattice* $\mathcal{L}(\mathbf{B})$, $\det(\mathcal{L}(\mathbf{B})) \leq \prod \|\mathbf{b}_i\|$.

In the next lecture we will prove that the Gram-Schmidt orthogonalization of a basis can be computed in polynomial time. So, the determinant of a lattice can be computed in polynomial time by first computing the orthogonalized vectors $\mathbf{B}^*$, and then taking the product of their lengths. But there are simpler ways to express the determinant of a lattice that do not involve the Gram-Schmidt orthogonalized basis. The following proposition shows that the determinant of a lattice can be obtained from a simple matrix determinant computation. [3]

Proposition 14. *For any lattice basis* $\mathbf{B} \in \mathbb{R}^{d \times n}$

$$\det(\mathcal{L}(\mathbf{B})) = \sqrt{\det(\mathbf{B}^\top \mathbf{B})}.$$

In particular, if $\mathbf{B} \in \mathbb{R}^{n \times n}$ *is a (non-singular) square matrix then* $\det(\mathcal{L}(\mathbf{B})) = |\det(\mathbf{B})|$.

Proof. Remember the Gram-Schmidt orthogonalization procedure. In matrix notation, it shows that the orhogonalized vectors $\mathbf{B}^*$ satisfy $\mathbf{B} = \mathbf{B}^*\mathbf{T}$, where $\mathbf{T}$ is an upper triangular matrix with 1's on the diagonal, and the $\mu_{i,j}$ coefficients at position (j, i) for all $j < i$. So, our formula for the determinant of a lattice can be written as

$$\sqrt{\det(\mathbf{B}^\top \mathbf{B})} = \sqrt{\det(\mathbf{T}^\top \mathbf{B}^{*\top} \mathbf{B}^* \mathbf{T})} = \sqrt{\det(\mathbf{T}^\top)\det(\mathbf{B}^{*\top}\mathbf{B}^*)\det(\mathbf{T})}.$$

The matrices $\mathbf{T}^\top, \mathbf{T}$ are triangular, and their determinant can be easily computed as the product of the diagonal elements, which is 1. Now consider $\mathbf{B}^{*\top}\mathbf{B}^*$. This matrix is diagonal because the columns of $\mathbf{B}^*$ are orthogonal. So, its determinant can also be computed as the product of the diagonal elements which is

$$\det(\mathbf{B}^{*\top}\mathbf{B}^*) = \prod_i \langle \mathbf{b}_i^*, \mathbf{b}_i^* \rangle = (\prod_i \|\mathbf{b}_i^*\|)^2 = \det(\mathcal{L}(\mathbf{B}))^2.$$

Taking the square root we get $\sqrt{\det(\mathbf{T}^\top)\det(\mathbf{B}^{*\top}\mathbf{B}^*)\det(\mathbf{T})} = \det(\mathcal{L}(\mathbf{B}))$. □

[3] Recall that the determinant of a matrix can be computed in polynomial time by computing $\det(\mathbf{B})$ modulo many small primes, and combining the results using the Chinese reminder theorem.

Now it is easy to show that the determinant does not depend on the particular choice of the basis, i.e., if two bases generate the same lattice then their lattice determinants have the same value.

Theorem 15. *Suppose* $\mathbf{B}$, $\mathbf{C}$ *are bases of the same lattice* $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{C})$. *Then,* $\det(\mathbf{B}) = \pm \det(\mathbf{C})$.

Proof. Suppose $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{C})$. Then $\mathbf{B} = \mathbf{C} \cdot \mathbf{U}$ where $\mathbf{U} \in \mathbb{Z}^{n \times n}$ is a unimodular matrix. Then $det(\mathbf{B}^\top \mathbf{B}) = \det((\mathbf{CU})^\top (\mathbf{CU})) = \det(\mathbf{U}^\top) \det(\mathbf{C}^\top \mathbf{B}) \det(\mathbf{U}) = \det((\mathbf{C}^\top \mathbf{B})$ because $\det(\mathbf{U}) = 1$. □

We conclude this section showing that although not every lattice has an orthogonal basis, every integer lattice contains an orthogonal sublattice.

Theorem 16. *For any nonsingular* $\mathbf{B} \in \mathbb{Z}^{n \times n}$, *let* $d = |\det(\mathbf{B})|$. *Then* $d \cdot \mathbb{Z}^n \subseteq \mathcal{L}(\mathbf{B})$.

Proof. Let $\mathbf{v}$ be any vector in $d \cdot \mathbb{Z}^n$. We know $\mathbf{v} = d \cdot \mathbf{y}$ for some integer vector $\mathbf{y} \in \mathbb{Z}^n$. We want to prove that $\mathbf{v} \in \mathcal{L}(\mathbf{B})$, i.e., $d \cdot \mathbf{y} = \mathbf{B} \cdot \mathbf{x}$ for some integer vector $\mathbf{x}$. Since $\mathbf{B}$ is non-singular, we can always find a solution $\mathbf{x}$ to the system $\mathbf{B} \cdot \mathbf{x} = d \cdot \mathbf{y}$ over the reals. We would like to show that $\mathbf{x}$ is in fact an integer vector, so that $d\mathbf{y} \in \mathcal{L}(\mathbf{B})$. We consider the elements x_i and use Cramer's rule:

$$\begin{aligned} x_i &= \frac{\det([\mathbf{b_1}, ..., \mathbf{b_{i-1}}, d\mathbf{y}, \mathbf{b_{i+1}}, ..., \mathbf{b_n}])}{\det(\mathbf{B})} \\ &= \frac{d \cdot \det([\mathbf{b_1}, ..., \mathbf{b_{i-1}}, \mathbf{y}, \mathbf{b_{i+1}}, ..., \mathbf{b_n}])}{\det(\mathbf{B})} \\ &= \det([\mathbf{b_1}, ..., \mathbf{b_{i-1}}, \mathbf{y}, \mathbf{b_{i+1}}, ..., \mathbf{b_n}]) \in \mathbb{Z} \end{aligned}$$

So, $\mathbf{x}$ is an integer vector. □

We may say that any integer lattice $\mathcal{L}(\mathbf{B})$ is periodic modulo the determinant of the lattice, in the sense that for any two vectors $\mathbf{x}, \mathbf{y}$, if $\mathbf{x} \equiv \mathbf{y} \pmod{\det(\mathcal{L}(\mathbf{B}))}$, then $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ if and only if $\mathbf{y} \in \mathcal{L}(\mathbf{B})$.

4. Minimum Distance

Definition 17. For any lattice $\Lambda = \mathcal{L}(\mathbf{B})$, the minimum distance of Λ is the smallest distance between any two lattice points:

$$\lambda(\Lambda) = \inf\{\|\mathbf{x} - \mathbf{y}\| : \mathbf{x}, \mathbf{y} \in \Lambda, \mathbf{x} \neq \mathbf{y}\}.$$

We observe that the minimum distance can be equivalently defined as the length of the shortest nonzero lattice vector:

$$\lambda(\Lambda) = \inf\{\|\mathbf{v}\| : \mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}\}.$$

This follows from the fact that lattices are additive subgroups of $\mathbb{R}^n$, i.e., they are closed under addition and subtraction. So, if $\mathbf{x}$ and $\mathbf{y}$ are distinct lattice points, then $\mathbf{x} - \mathbf{y}$ is a nonzero lattice point. The first thing we want to prove about the minimum distance is that it is always achieved by some lattice vector, i.e., there is a lattice vector $\mathbf{x} \in \Lambda$ of length exactly $\|\mathbf{x}\| = \lambda(\Lambda)$. To prove this, we need first to establish a lower bound on $\lambda(\Lambda)$.

Theorem 18. *For every lattice basis* $\mathbf{B}$ *and its Gram-Schmidt orthogonalization* $\mathbf{B}^*$, $\lambda(\mathcal{L}(\mathbf{B})) \geq min\|\mathbf{b}_i^*\|$.

Proof. Note that $\mathbf{b}_i^*$ are not lattice vectors. Let us consider a generic lattice vector

$$\mathbf{Bx} \in \mathcal{L}(\mathbf{B}) \setminus \{\mathbf{0}\},$$

where $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ and let k be the biggest index such that $x_k \neq 0$. We prove that

$$\|\mathbf{Bx}\| \geq \|\mathbf{b}_k^*\| \geq \min_i \|\mathbf{b}_i^*\|. \tag{4.1}$$

In order to prove (4.1), we take the scalar product of our lattice vector and $\mathbf{b}_k^*$. Using the orthogonality of $\mathbf{b}_k^*$ and $\mathbf{b}_i$ (for $i < k$) we get

$$\langle \mathbf{Bx}, \mathbf{b}_k^* \rangle = \sum_{i \leq k} \langle \mathbf{b}_i x_i, \mathbf{b}_k^* \rangle = x_k \langle \mathbf{b}_k, \mathbf{b}_k^* \rangle = x_k \|\mathbf{b}_k^*\|^2.$$

By Cauchy-Shwartz,

$$\|\mathbf{Bx}\| \cdot \|\mathbf{b}_k^*\| \geq |\langle \mathbf{Bx}, \mathbf{b}_k^* \rangle| \geq |x_k| \cdot \|\mathbf{b}_k^*\|^2.$$

Using $|x_k| \geq 1$ and dividing by $\|\mathbf{b}_k\|^*$, we get $\|\mathbf{Bx}\| \geq \|\mathbf{b}_k^*\|$. □

An immediate consequence of Theorem 18 is that the minimum distance of a lattice $\lambda(\Lambda) > 0$ is strictly positive, and the lattice Λ is a *discrete* subgroup of $\mathbb{R}^n$. In fact, lattices can be alternatively defined as discrete subgroups of $\mathbb{R}^d$, because, as we will prove later, any discrete subgroup of $\mathbb{R}^n$ is a lattice.

Notice that the lower bound $\min_i \|\mathbf{b}_i^*\|$ depends on the choice of the basis. We will see later in the course that some bases give better lower bounds than others, but at this point any nonzero lower bound will suffice. We want to show that there is a lattice vector of length λ. Consider a sphere of radius $2\lambda > \lambda$. Clearly, in the definition of $\lambda = \inf\{\|\mathbf{x}\| \colon \mathbf{x} \in \Lambda \setminus \{0\}\}$, we can restrict $\mathbf{x}$ to range over all lattice vectors inside the sphere of radius 2λ. We observe that (by a volume argument) the sphere contains only finitely many lattice points. (Details below.) It follows that we can replace the inf operation with a min, and there is a point in the set achieving the smallest possible norm.

How can we use a volume argument, when points have volume 0? Put an open sphere of radius $\lambda/2$ around each lattice point. Since lattice points are at distance at least λ, the spheres are disjoint. The spheres with centers in S are also contained in a sphere S' of radius 2.5λ. So, since the volume of the small spheres (which is proportional to $1/2^n$) cannot exceed the volume of the big sphere S' (which has volume proportional to 2.5^n), there are at most 5^n lattice points.

5. Minkowski's theorem

We now turn to estimating the value of λ from above. Clearly, for any basis $\mathbf{B}$, we have $\lambda(\mathbf{B}) \leq \min_i \|\mathbf{b}_i\|$, because each column of $\mathbf{B}$ is a nonzero lattice vector. We would like to get a better bound, and, specifically, a bound that does not depend on the choice of the basis. Clearly, lattices with arbitrarily large minimum distance can be easily obtained simply by scaling an arbitrary lattice by a constant $c > 0$ to obtain $\lambda(c \cdot \Lambda) = c \cdot \lambda(\Lambda)$. What if we normalize the lattice so that $\det(\Lambda) = 1$? By definition of determinant, these are lattices with density 1, i.e., with about one lattice point per each unit volume of space. Can the lattice still have arbitrarily large minimum distance? Equivalently, we are asking if it is possible to bound the ratio $\lambda(\Lambda)/\det(\Lambda)^{1/n}$ for any n-dimensional lattice Λ. (Notice that the

quantity $\lambda(\Lambda)/\det(\Lambda)^{1/n}$ is invariant under linear scaling because $\det(c \cdot \Lambda) = c^n \cdot \det(\Lambda)$.) For historical reasons[4], mathematicians have defined and studied the square of this quantity, which is called Hermite's constant.

Definition 19. The Hermite constant of an n-dimensional lattice Λ is the quantity $\gamma(\Lambda) = (\lambda(\Lambda)/\det(\Lambda)^{1/n})^2$. The Hermite constant in dimension n is the supremum $\gamma_n = \sup_\Lambda \gamma(\Lambda)$, where Λ ranges over all n-dimensional lattices.

The upper bound on γ_n we are going to prove was originally proved by Minkowski. Here we follow a different approach, by first proving a theorem of Blichfeldt from which Minkowski's theorem can be easily derived as a corollary.

Theorem 20. *Given a lattice Λ and a set $S \subseteq span(\Lambda)$ if $vol(S) > \det(\Lambda)$ then S contains two points $z_1, z_2 \in S$ such that $\mathbf{z}_1 - \mathbf{z}_2 \in \Lambda$.*

Proof. Let $\Lambda = \mathcal{L}(\mathbf{B})$. Consider the sets $S_\mathbf{x} = S \cap (\mathbf{x} + \mathcal{P}(\mathbf{B}))$, where $\mathbf{x} \in \Lambda$. Notice that these sets form a partition of S, i.e., they are pairwise disjoint and

$$S = \bigcup_{x \in \Lambda} S_x.$$

In particular we have

$$\mathrm{vol}(S) = \sum_{\mathbf{x} \in \Lambda} \mathrm{vol}(S_\mathbf{x}).$$

Notice that the shifted sets $S_\mathbf{x} - \mathbf{x} = (S - \mathbf{x}) \cap \mathcal{P}(\mathbf{B})$ are all contained in $\mathcal{P}(\mathbf{B})$. We want to prove that the $S_\mathbf{x}$ cannot be all mutually disjoint. Since $\mathrm{vol}(S_x) = \mathrm{vol}(S_\mathbf{x} - \mathbf{x})$, we have

$$\mathrm{vol}(\mathcal{P}(\mathbf{B})) < \mathrm{vol}(S) = \sum_{x \in \Lambda} \mathrm{vol}(S_x) = \sum_{x \in \Lambda} \mathrm{vol}(S_\mathbf{x} - \mathbf{x}).$$

The facts that $S_\mathbf{x} - \mathbf{x} \subseteq \mathcal{P}(\mathbf{B})$ and $\sum_{\mathbf{x} \in \Lambda} \mathrm{vol}(S_\mathbf{x} - \mathbf{x}) > \mathrm{vol}(\mathcal{P}(\mathbf{B}))$ imply that these sets cannot be disjoint, i.e. there exist two distinct vectors $\mathbf{x} \neq \mathbf{y} \in \Lambda$ such that $(S_\mathbf{x} - \mathbf{x}) \cap (S_\mathbf{y} - \mathbf{y}) \neq 0$.

Let $\mathbf{z}$ be any vector in the (non-empty) intersection $(S_\mathbf{x} - \mathbf{x}) \cap (S_\mathbf{y} - \mathbf{y})$ and define

$$\mathbf{z}_1 = \mathbf{z} + \mathbf{x} \in S_\mathbf{x} \subseteq S$$

$$\mathbf{z}_2 = \mathbf{z} + \mathbf{y} \in S_\mathbf{y} \subseteq S.$$

These two vectors satisfy

$$\mathbf{z}_1 - \mathbf{z}_2 = \mathbf{x} - \mathbf{y} \in \Lambda.$$

□

As a corollary to Blichfeldt theorem we immediately get a result originally due to Minkowski that gives a bound on the length of the shortest vector in a lattice.

Corollary 21. *[Minkowski's convex body theorem] Let $\mathcal{L}(\mathbf{B})$ be a full dimensional lattice. If $S \subset span(\mathcal{L}(\mathbf{B})) = \mathbb{R}^n$ is a convex symmetric body of volume $vol(S) > 2^n \det(\mathbf{B})$, then S contains a nonzero lattice point.*

[4]These problems were originally formulated and studied in the equivalent language of positive definite quadratic forms.

Proof. Consider the set $S/2 = \{\mathbf{x} : 2\mathbf{x} \in S\}$. The volume of $S/2$ satisfies

$$\mathrm{vol}(S/2) = 2^{-n}\mathrm{vol}(S) > \det(B)$$

By Blichfeldt theorem there exist $z_1, z_2 \in S/2$ such that $\mathbf{z}_1 - \mathbf{z}_2 \in \mathcal{L}(B) \setminus \{\mathbf{0}\}$. By definition of S/2, $2\mathbf{z}_1, 2\mathbf{z}_2 \in S$. Since S is symmetric, also $-2\mathbf{z}_2 \in S$ and by convexity,

$$\mathbf{z}_1 - \mathbf{z}_2 = \frac{2\mathbf{z}_1 - 2\mathbf{z}_2}{2} \in S$$

is a non-zero lattice vector contained in the set S. □

The relation between Minkowski theorem and bounding the length of the shortest vector in a lattice is easily explained. Consider first the ℓ_∞ norm: $\|\mathbf{x}\| = \max_i |x_i|$. We show that every (full rank, n-dimensional) lattice Λ always contains a nonzero vector $\|\mathbf{x}\| \leq \det(\Lambda)^{1/n}$. Let $l = \min\{\|\mathbf{x}\|_\infty : \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}\}$ and assume for contradition $l > \det(\Lambda)^{1/n}$. Take the hypercube $C = \{\mathbf{x} : \|\mathbf{x}\| < l\}$. Notice that C is convex, symmetric, and has volume $\mathrm{vol}(C) = (2l)^n > 2^n \det(\Lambda)$. So, by Minkowski's theorem, C contains a nonzero lattice vector $\mathbf{x}$. By definition of C, we have $\|\mathbf{x}\|_\infty < l$, a contradiction to the minimality of l. This gives the following corollary.

Corollary 22. *For any full dimensionsional $\mathcal{L}(\mathbf{B})$ there exists a lattice point $x \in \mathcal{L}(\mathbf{B}) / \{0\}$ such that*

$$\|\mathbf{x}\|_\infty \leq \det(\mathbf{B})^{1/n}.$$

Using the inequality $\|\mathbf{x}\| \leq \sqrt{n}\|\mathbf{x}\|_\infty$ (valid for any n-dimensional vector $\mathbf{x}$), we get a corresponding bound in the ℓ_2 norm. It is easy to see that for Euclidean norm the full dimensionality condition is not necessary because one can embed any lattice $\Lambda \subset \mathbb{R}^d$ of rank n into $\mathbb{R}^n$ by a simple orthogonal projection operation.

Corollary 23. *Hermite constant is at most $\gamma_n \leq n$, i.e., for any lattice $\mathcal{L}(\mathbf{B})$ there exists a lattice point $\mathbf{x} \in \mathcal{L}(\mathbf{B}) \setminus \{0\}$ such that*

$$\|\mathbf{x}\|_2 \leq \sqrt{n}\det(\mathbf{B})^{1/n}.$$

We could have proved the bound for the Euclidean norm directly, using a sphere instead of a cube, and then plugging in the formula for the volume of an n-dimensional sphere. This can be useful to get slighly better bounds, but only by a constant (independent of n) factor. For example, in two dimensions, for any lattice Λ, the disk $S = \{\mathbf{x} : \|\mathbf{x}\| < \lambda(\Lambda)\}$ contains no nonzero lattice point. So, by Minkowki's theorem, the area of S can be at most $2^n \det(\Lambda) = 4\det(\Lambda)$. But we know that the area of S is $\pi\lambda^2$. So, $\lambda(\Lambda) \leq 2\sqrt{\det(\Lambda)/\pi}$, which is strictly smaller than $\sqrt{2}\det(\Lambda)^{1/n}$. This yields the bound $\gamma_2 \leq 4/\pi \approx 1.27 < 2$. In fact, $\gamma_2 = 2/\sqrt{3} \approx 1.15$ is even smaller, but we will not prove this.

We remark that a lattice Λ can contain vectors arbitrarily shorter than Minkowski's bound $\sqrt{n}\det(\Lambda)^{1/n}$. Consider for example the two dimensional lattice generated by the vectors $(1,0)^T$ and $(0,N)^T$, where N is a large integer. The lattice contains a short vector of length $\lambda = 1$. However, the determinant of the lattice is N, and Minkowski's bound $\sqrt{2}N^{1/2}$ is much larger than 1.

It can also be shown that Minkowski's bound cannot be asymptotically improved, in the sense that there is a constant c such that for any dimension n there is a n-dimensional lattice Λ_n such that $\gamma_n > c \cdot n$. (See Exercises.) So, up to constant factors, $O(\sqrt{n})\det(\Lambda)^{1/n}$

is the best upper bound one can possibly prove on the length of the shortest vector of any n-dimensional lattice as a function of the determinant.

6. A simple application

As an application of Minkowski's theorem we show that any prime number p congruent to 1 mod 4 can be written as the sum of two squares.

Theorem 24. *For every prime $p \equiv 1 \bmod 4$ there exist integers $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$*

Proof. Let $p \in \mathbb{Z}$ be a prime such that $p \equiv 1 \pmod 4$. Then $\mathbb{Z}_p^*$ is a group such that $4 \mid o(\mathbb{Z}_p^*) = p - 1$. Therefore, there exists an element of multiplicative order 4, and -1 is a quadratic residue modulo p, i.e. there exists an integer i such that $i^2 \equiv -1 \pmod p$. It immediately follows that

$$p \mid i^2 + 1. \tag{6.1}$$

Now define the lattice basis

$$\mathbf{B} = \begin{bmatrix} 1 & 0 \\ i & p \end{bmatrix}.$$

By Minkowski's theorem there exists an integer vector $\mathbf{x}$ such that $0 < \|\mathbf{Bx}\|_2 < \sqrt{2} \cdot \sqrt{\det(\mathbf{B})}$. Squaring this equation yields

$$0 < \|\mathbf{Bx}\|_2^2 < 2 \cdot \det(\mathbf{B}) = 2p. \tag{6.2}$$

The middle term expands to

$$\left\| \begin{bmatrix} x_1 \\ ix_1 + px_2 \end{bmatrix} \right\|^2 = x_1^2 + (ix_1 + px_2)^2 \tag{6.3}$$

If we let $a = x_1$ and $b = ix_1 + px_2$, (2) becomes

$$0 < a^2 + b^2 < 2p \tag{6.4}$$

Hence if we can show that $a^2 + b^2 \equiv 0 \bmod p$, by necessity $a^2 + b^2 = p$. Expanding the right side of (3) produces $x_1^2 + i^2 x_1^2 + p^2 x_2^2 + 2ix_1 px_2$, which can be factored into

$$p(px_2^2 + 2ix_1x_2) + x_1^2(i^2 + 1)$$

Obviously p divides the first term, and by (1) p divides the second term. Thus $a^2 + b^2 \equiv 0 \bmod p$, and therefore by (4) $a^2 + b^2 = p$. □

This application shows how lattices can be used to prove non-trivial facts in number theory. A similar theorem that can be proved with the same lattice techniques is the following.

Theorem 25. $\forall n \in \mathbb{Z}^+ \ \exists a, b, c, d \in \mathcal{Z} : n = a^2 + b^2 + c^2 + d^2$.

The proof is left to the reader as an excercise. As you can easily guess, the proofs involves a 4-dimensional lattice.

7. Successive Minima

Definition 26. For any n-dimensional lattice Λ and integer $k < n$, let $\lambda_k(\Lambda)$ be the smallest $r > 0$ such that Λ contains at least k linearly independent vectors of length at most r.

The successive minima of a lattice generalize the minimum distance $\lambda = \lambda_1$. By the same volume argument used to show that there exists vectors of length λ, one can show that there exist (linearly independent) lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ of lengths $\lambda_1, \ldots, \lambda_k$. Minkowski's theorem can also be generalized to provide a bound not just on λ_1, but on the geometric mean of all successive minima.

Theorem 27. *For any lattice Λ, $\prod_{i=1}^{n} \lambda_i \leq \frac{2^n \det(\Lambda)}{vol(S_n)}$, where S_n is the n-dimensional unit ball.*

Proof. Assume for contradiction this is not the case, i.e., $\prod_i \lambda_i > 2^n \det(\Lambda)/\mathrm{vol}(S_n)$ and let $\mathbf{x_1}, \ldots, \mathbf{x_n}$ be linearly independent vectors such that $\|\mathbf{x_i}\| = \lambda_i$. Consider the orthogonalized vectors $\mathbf{x_i}^*$ and define the transformation

$$T(\sum c_i \mathbf{x_i}^*) = \sum \lambda_i c_i \mathbf{x_i}^*$$

that expands coordinate $\mathbf{x_i}^*$ by the factor λ_i. If we apply T to the open unit ball S_n we get a symmetric convex body $T(S_n)$ of volume $(\prod_i \lambda_i)\mathrm{vol}(S_n) > 2^n \det(\Lambda)$. By Minkowski's first theorem $T(S_n)$ contains a lattice point $\mathbf{y} = T(\mathbf{x})$ (with $\|\mathbf{x}\| < 1$) different from the origin. Let $\mathbf{x} = \sum c_i \mathbf{x_i}^*$ and $\mathbf{y} = \sum \lambda_i c_i \mathbf{x_i}^*$. Since $\mathbf{y}$ is not zero, some c_i is not zero. Let k the largest index such that $c_i \neq 0$. Notice that $\mathbf{y}$ is linearly independent from $\mathbf{x_1}, \ldots, \mathbf{x_{k-1}}$ because $\langle \mathbf{x_k}^*, \mathbf{y} \rangle = \lambda_k c_k \|\mathbf{x_k}^*\|^2 > 0$. We now show that $\|\mathbf{y}\| < \lambda_k$, contradicting the definition of λ_i for some $i \leq k$.

$$\|\mathbf{y}\|^2 = \sum_{i \leq k} \lambda_i^2 c_i^2 \|\mathbf{x_i}^*\|^2 \leq \sum_{i \leq k} \lambda_k^2 c_i^2 \|\mathbf{x_i}^*\|^2 = \lambda_k^2 \|\mathbf{x}\|^2 < \lambda_k^2$$

□

8. Notes and Exercises

Lattices can be alternatively defined as discrete subgroups of $\mathbb{R}^n$, i.e., subsets $\Lambda \subset \mathbb{R}^n$ satisfying the following properties:

(subgroup) Λ is closed under addition and subtraction,[5]

(discrete) there is an $\epsilon > 0$ such that any two distinct lattice points $\mathbf{x} \neq \mathbf{y} \in \Lambda$ are at distance at least $\|\mathbf{x} - \mathbf{y}\| \geq \epsilon$.

Exercise 28. Prove that lattices (as defined in Definition 1) are discrete subgroups of $\mathbb{R}^n$.

You will prove the other direction (i.e., any discrete subgroup of $\mathbb{R}^n$ is a lattice according to Definition 1) in a later exercise. For now, we observe that not every subgroup of $\mathbb{R}^n$ is a lattice.

Example 29. $\mathbb{Q}^n$ is a subgroup of $\mathbb{R}^n$, but not a lattice, because it is not discrete.

The definition $\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} \colon \mathbf{x} \in \mathbb{Z}^m\}$ can be extended to matrices $\mathbf{B}$ whose columns are not linearly independent. However, in this case, the resulting set of points is not always a lattice because it may not be discrete. Still, we will see that if $\mathbf{B}$ is a matrix with integer or rational entries, then $\mathcal{L}(\mathbf{B})$ is always a lattice.

[5]Technically, closure under subtraction is enough because addition can be expressed as $a + b = a - (-b)$.

Exercise 30. Find a matrix $\mathbf{B} \in \mathbb{R}^{d \times n}$ such that $\mathcal{L}(\mathbf{B})$ is not a lattice. *[Hint:*$\mathbf{B}$ *can be as small as a 1-by-2 matrix.]*

Exercise 31. Prove parts (1) and (2), and the "only if" direction of part (3) of Proposition 3

Exercise 32. Prove that any lattice achieving Hermite's constant $\gamma_n = (\lambda(\Lambda)/\det(\Lambda)^{1/n})^2$ must necessarily have n linearly independent vectors of length $\lambda(\Lambda)$. (Equivalently, all its successive minima are the same $\lambda_1 = \lambda_2 = \ldots = \lambda_n$.) *[Hint: Use Minkowski's second theorem and Hadamard bound]*