CSE 206A: Lattice Algorithms and Applications Spring 2007

Lecture 2: Lattices and Bases

Lecturer: Daniele Micciancio *Scribe: Daniele Micciancio*

Motivated by the many applications described in the first lecture, today we start a systematic study of point lattices and related algorithm.

1 Lattices and Vector spaces

Geometrically, a lattice can be defined as the set of intersection point of an infinite, regular, but not necessarily orthogonal n-dimensional grid. For example, the set of integer vectors $\mathbb{Z}^n$ is a lattice. In computer science, lattices are usually represented by a generating basis.

Definition 1 *Let* $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *be linearly independent vectors in* $\mathbb{R}^m$. *The lattice generated by* $\mathbf{B}$ *is the set*

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

of all the integer *linear combinations of the vectors in* $\mathbf{B}$*, and the set* $\mathbf{B}$ *is called a* basis *for* $\mathcal{L}(\mathbf{B})$.

Notice the similarity between the definition of a lattice and the definition of vector space generated by $\mathbf{B}$:

$$\text{span}(\mathbf{B}) = \{\sum_{i=1}^{n} x_i \cdot \mathbf{b}_i : x_i \in \mathbb{R}\} = \{\mathbf{B} \cdot \mathbf{x} : \mathbf{x} \in \mathbb{R}^n\}.$$

The difference is that in a vector space you can combine the columns of 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 $\mathbf{y} = x_1\mathbf{b}_1 + \cdots x_n\mathbf{b}_n$ in a unique way. Therefore $\mathbf{y} \in \mathcal{L}(\mathbf{B})$ if and only if $x_1, \ldots, x_n \in \mathbb{Z}$.

Any basis $\mathbf{B}$ (i.e., any set of linearly independent vectors) can be compactly represented as an $m \times n$ matrix whose columns are the basis vectors. Notice that $m \geq n$ because the columns of $\mathbf{B}$ are linearly independent, but in general m can be bigger than n. If $n = m$ the lattice $\mathcal{L}(\mathbf{B})$ is said full-dimensional and $\text{span}(\mathbf{B}) = \mathbb{R}^n$.

Notice that if $\mathbf{B}$ is a basis for the lattice $\mathcal{L}(\mathbf{B})$, then it is also a basis for the vector space $\text{span}(\mathbf{B})$. However, not every basis for the vector space $\text{span}(\mathbf{B})$ is also a lattice basis for $\mathcal{L}(\mathbf{B})$. For example $2\mathbf{B}$ is a basis for $\text{span}(\mathbf{B})$ 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 $2\mathbf{B}$.

Another difference between lattices and vector spaces is that vector spaces always admit an orthogonal basis. This is not true for lattices. Consider for example the 2-dimensional lattice generated by the vectors $(2, 0)$ and $(1, 2)$. This lattice contains pairs of orthogonal vectors (e.g., $(0, 4)$ is a lattice point and it is orthogonal to $(2, 0)$) but no such a pair is a basis for the lattice.

2 Gram-Schmidt

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 $\mathbf{B} = [\mathbf{b}_1| \dots |\mathbf{b}_n] \in \mathbb{R}^{m\times n}$ 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 as follows:

$$\begin{array}{rcll} \mathbf{b}_1^* &=& \mathbf{b}_1 & \\ \mathbf{b}_2^* &=& \mathbf{b}_2 - \mu_{2,1}\mathbf{b}_1^* & \text{where } \mu_{2,1} = \frac{\langle \mathbf{b}_2, \mathbf{b}_1^* \rangle}{\langle \mathbf{b}_1^*, \mathbf{b}_1^* \rangle}. \\ \mathbf{b}_i^* &=& \mathbf{b}_i - \sum_{j<i} \mu_{i,j}\mathbf{b}_j^* & \text{where } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}. \end{array}$$

Note that the columns of $\mathbf{B}^*$ are orthogonal ($\langle \mathbf{b}_i^*, \mathbf{b}_j^* \rangle$ for all $i \neq j$). Therefore the (non-zero) columns of $\mathbf{B}^*$ are linearly independent and form a basis for the vector space span($\mathbf{B}$). However they are generally not a basis for the lattice $\mathcal{L}(\mathbf{B})$.

For example, the Gram-Schmidt orthogonalization of the basis $\mathbf{B} = [(2, 0)^T, (1, 2)^T]]$ is $(2, 0)^T, (0, 2)^T$. However this is not a lattice basis because the vector $(0, 2)^T$ does not belong to the lattice.

We see that the set of bases of a lattice has a much more complex structure of the set of bases of a vector space. Can we characterise the set of bases of a given lattice? The following theorem shows that different bases of the same lattices are related by unimodular transformations.

Theorem 2 *Let* $\mathbf{B}$ *and* $\mathbf{B}'$ *be two bases. Then* $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$ *if and only if there exists a unimodular matrix* $\mathbf{U}$ *(i.e., a square matrix with integer entries and determinant* ± 1*) such that* $\mathbf{B} = \mathbf{B}'\mathbf{U}$.

Proof Notice that if $\mathbf{U}$ is unimodular, then $\mathbf{U}^{-1}$ is also unimodular. To see this, recall Cramer's rule to solve a system of linear equations: for any nonsingular $\mathbf{A} = [\mathbf{a_1}, ...\mathbf{a_n}] \in \mathbb{R}^{n\times n}$, and $\mathbf{b} \in \mathbb{R}^n$, the (unique) solution to the system of linear equations $\mathbf{Ax} = \mathbf{b}$ is given by

$$x_i = \frac{\det([\mathbf{a_1}, ..., \mathbf{a_{i-1}}, \mathbf{b}, \mathbf{a_{i+1}}, ..., \mathbf{a_n}])}{\det(A)}.$$

In particular, if $\mathbf{A}$ and $\mathbf{b}$ are integer, then the unique solution to the system $\mathbf{Ax} = \mathbf{b}$ has the property that $\det(\mathbf{A}) \cdot \mathbf{x}$ is an integer vector. Now, let $\mathbf{U}'$ be the inverse of $\mathbf{U}$, i.e., $\mathbf{UU}' = \mathbf{I}$. Each column of $\mathbf{U}'$ is the solution to a system of linear equations $\mathbf{Ux} = \mathbf{e}_i$. By Cramer rule's the solution is integer because $\det(U) = \pm 1$. This proves that $\mathbf{U}'$ is an integer matrix. Matrix $\mathbf{U}'$ is unimodular because

$$\det(\mathbf{U}) \det(\mathbf{U}') = \det(\mathbf{UU}') = \det(\mathbf{I}) = 1.$$

So, we also have $\det(\mathbf{U}') = 1/\det(\mathbf{U}) = \det(\mathbf{U}') = \pm 1$.

Now, let us get to the proof. First assume $\mathbf{B} = \mathbf{B}'\mathbf{U}$ for some unimodular matrix $\mathbf{U}$. In particular, both $\mathbf{U}$ and $\mathbf{U}^{-1}$ are integer matrices, and $\mathbf{B} = \mathbf{B}'\mathbf{U}$ and $\mathbf{B}' = \mathbf{B}\mathbf{U}^{-1}$. It follows that $\mathcal{L}(\mathbf{B}) \subseteq \mathcal{L}(\mathbf{B}')$ and $\mathcal{L}(\mathbf{B}') \subseteq \mathcal{L}(\mathbf{B})$, i.e., the two matrices $\mathbf{B}$ and $\mathbf{B}'$ generate the same lattice.

Next, assume $\mathbf{B}$ and $\mathbf{B}'$ are two bases for the same lattice $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$. Then, by definition of lattice, there exist integer square matrices $\mathbf{M}$ and $\mathbf{M}'$ such that $\mathbf{B} = \mathbf{B}'\mathbf{M}'$ and $\mathbf{B}' = \mathbf{B}\mathbf{M}$. Combining these two equations we get $\mathbf{B} = \mathbf{B}\mathbf{M}\mathbf{M}'$, or equivalently, $\mathbf{B}(\mathbf{I} - \mathbf{M}\mathbf{M}') = \mathbf{0}$. Since vectors $\mathbf{B}$ are linearly independent, it must be $\mathbf{I} - \mathbf{M}\mathbf{M}' = \mathbf{0}$, i.e., $\mathbf{M}\mathbf{M}' = \mathbf{I}$. In particular, $\det(\mathbf{M}) \cdot \det(\mathbf{M}') = \det(\mathbf{M} \cdot \mathbf{M}') = \det(\mathbf{I}) = 1$. Since matrices $\mathbf{M}$ and $\mathbf{M}'$ have integer entries, $\det(\mathbf{M}), \det(\mathbf{M}') \in \mathbb{Z}$, and it must be $\det(\mathbf{M}) = \det(\mathbf{M}') = \pm 1$
■

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

1. Swap the order of two columns in $\mathbf{B}$.
2. Multiply a column by -1.
3. Add an integer multiple of a column to another column: $\mathbf{b}_i \leftarrow \mathbf{b}_i + a \cdot \mathbf{b}_j$ where $i \neq j$ and $a \in \mathbb{Z}$.

It is also possible to show that any unimodular matrix can be obtained from the identity as a sequence of elementary integer column operations. (Hint: show that any unimodular matrix can be transformed into the identity, and then reverse the sequence of operations.) It follows, that any two equivalent lattice bases can be obtained one from the other applying a sequence of elementary integer column operations.

3 The determinant

Definition 3 *Given a basis* $\mathbf{B} = [\mathbf{b_1}, ..., \mathbf{b_n}] \in \mathbb{R}^{m \times n}$*, the* fundamental parallelepiped *associated to* $\mathbf{B}$ *is the set of points*

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

Note that $\mathcal{P}(\mathbf{B})$ is half-open, so that the translates $\mathcal{P}(\mathbf{B}) + \mathbf{v}$ ($\mathbf{v} \in \mathcal{L}(\mathbf{B})$) form a partition of the whole space $\mathbb{R}^m$. This statement is formalized in the following observation.

Observation 4 *For all* $\mathbf{x} \in \mathbb{R}^m$*, 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 the determinant of a lattice.

Definition 5 *Let $\mathbf{B} \in \mathbb{R}^{m \times n}$ 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* $\mathbf{B}$*:*

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

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

Geometrically, the determinant represent 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.

A simple upper bound to the determinant is given by *Hadamard inequality*:

$$\det(\mathcal{L}(\mathbf{B})) \leq \prod \|\mathbf{b}_i\|.$$

The bound immediately follows from the fact that $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\|$.

We prove in the next section 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 are there simpler ways to compute the determinant without having to run Gram-Schmidt? Notice that when $\mathbf{B} \in \mathbb{R}^{n \times n}$ is a non-singular square matrix then $\det(\mathcal{L}(\mathbf{B})) = |\det(\mathbf{B})|$ can be computed simply as a matrix determinant. (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.)

The following formula gives a way to compute the lattice determinant to matrix determinant computation even when $\mathbf{B}$ is not a square matrix.

Theorem 6 *For any lattice basis $\mathbf{B} \in \mathbb{R}^{n \times m}$*

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

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

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

The matrices $\mathbf{T}, \mathbf{T}^T$ are triangular, and their determinant can be easily computed as the product of the diagonal elements, which is 1. Now consider $\mathbf{B}^{*T}\mathbf{B}^*$. 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

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

Taking the square root we get

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

■

We can now prove 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 7 *Suppose* $\mathbf{B}, \mathbf{B}'$ *are bases of the same lattice* $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$*. Then,* $\det(\mathcal{L}(\mathbf{B})) = \det(\mathcal{L}(\mathbf{B}'))$*.*

Proof Suppose $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$. Then $\mathbf{B} = \mathbf{B}' \cdot \mathbf{U}$ where $\mathbf{U} \in \mathbb{Z}^{n\times n}$ is a unimodular matrix. Then $det(\mathbf{B}^T\mathbf{B}) = \det((\mathbf{B}'\mathbf{U})^T(\mathbf{B}'\mathbf{U})) = \det(\mathbf{U}^T)\det((\mathbf{B}')^T\mathbf{B})\det(\mathbf{U}) = \det((\mathbf{B}')^T\mathbf{B})$ 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.

Claim 8 *For any nonsingular* $B \in \mathbb{Z}^{n\times n}$*, 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:

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

■

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 Running time of Gram-Schmidt

Is this section we analyze the running time of the Gram-Schmidt algorithm. The number of arithmetic operations performed by the Gram-Schmidt procedure is $O(n^3)$. Can we conclude that it runs in polynomial time? Not yet. In order to prove polynomial time termination, we also need to show that all the numbers involved do not grow too big. This will also be useful later on to prove the polynomial time termination of other algorithms that use Gram-Schmidt orthogonalized bases. Notice that even if the input matrix $\mathbf{B}$ is integer, the orthogonalized matrix $\mathbf{B}^*$ and the coefficients $\mu_{i,j}$ will in general not be integers. However, if $\mathbf{B}$ is integer (as we will assume for the rest of this section), then the $\mu_{i,j}$ and $\mathbf{B}^*$ are rational.

The Gram-Schmidt algorithm uses rational numbers, so we need to bound both the precision required by these numbers and their magnitude. From the Gram-Schmidts orthogonalization formulas we know that

$$\mathbf{b}_i^* = \mathbf{b}_i + \sum_{j<i} \nu_{i,j} \mathbf{b}_j$$

for some reals $\nu_{i,j}$. Since $\mathbf{b}_i^*$ is orthogonal to $\mathbf{b}_t$ for all $t < i$ we have

$$\langle \mathbf{b}_t, \mathbf{b}_i \rangle + \sum_{j<i} \nu_{i,j} \langle \mathbf{b}_t, \mathbf{b}_j \rangle = 0.$$

In matrix notation, if we let $\mathbf{B}_{i-1} = [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]$ and $(\nu_i)_j = \nu_{i,j}$ this can be written as:

$$(\mathbf{B}_{i-1}^T \cdot \mathbf{B}_{i-1}) \cdot \nu_i = -\mathbf{B}_{i-1}^T \cdot \mathbf{b}_i$$

which is an integer vector. Solving the above system of linear equations in variables ν_i using Cramer's rule we get

$$\nu_{i,j} \in \frac{\mathbb{Z}}{\det(\mathbf{B}_{i-1}^T \cdot \mathbf{B}_{i-1})} = \frac{\mathbb{Z}}{\det(\mathcal{L}(\mathbf{B}_{i-1}))^2}.$$

We use this property to bound the denominators that can occur in the coefficients $\mu_{i,j}$ and orthogonalized vectors $\mathbf{b}_i^*$. Let $D_i = \det(\mathbf{B}_{i-1})^2$ and notice that

$$D_{i-1} \cdot \mathbf{b}_i^* = D_{i-1} \cdot \mathbf{b}_i + \sum_{j<i} (D_{i-1} \nu_{i,j}) \mathbf{b}_j$$

is an integer combination of integer vectors. So, all denominators that occur in vector $\mathbf{b}_i^*$ are factors of D_{i-1}. Let's now compute the coefficients:

$$\begin{aligned} \mu_{i,j} &= \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} \\ &= \frac{D_{j-1} \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{D_{j-1} \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} \\ &= \frac{\langle \mathbf{b}_i, D_{j-1} \mathbf{b}_j^* \rangle}{D_j} \in \frac{\mathbb{Z}}{D_j} \end{aligned}$$

and the denominators in the $\mu_{i,j}$ must divide D_j.

This proves that all numbers involved in $\mu_{i,j}$ and $\mathbf{b}_i^*$ have denominators at most $\max_k D_k \leq \prod_k \|\mathbf{b}_k\|^2$. Finally, the magnitude of the numbers is also polynomial because $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\|$, so all entries in $\|\mathbf{b}_i^*\|$ are at most $\|\mathbf{b}_i\|$. This proves that the Gram-Schmidt orthogonalization procedure runs in polynomial time.

Theorem 9 *There exists a polynomial time algorithm that on input a matrix* $\mathbf{B}$*, computes the Gram-Schmidt orthogonalization* $\mathbf{B}^*$