CSE 206A: Lattice Algorithms and Applications Winter 2016

The dual lattice

Instructor: *Daniele Micciancio* UCSD CSE

1 Dual Lattice and Dual Basis

Definition 1 *The dual of a lattice Λ is the set $\hat{\Lambda}$ of all vectors $\mathbf{x} \in span(\Lambda)$ such that $\langle \mathbf{x}, \mathbf{y} \rangle$ is an integer for all $\mathbf{y} \in \Lambda$.*

Exercise 1 *Use Definition 1 to prove that the dual of $\mathbb{Z}^n$ is $\mathbb{Z}^n$.*

The dual lattice $\hat{\Lambda}$ lives in the same vector space as Λ, but its geometric relation to Λ is not immediately obvious, and it can often be source of confusion to the beginner. For example, as it will become clear soon, even if Λ and $\hat{\Lambda}$ live in the same vector space, it makes little sense, geometrically, to add up vectors from Λ with vectors from $\hat{\Lambda}$. The definition of the dual lattice is very natural if we compare it with the abstract definition of dual for vector spaces.[1] Recall that the dual of an abstract vector space V is defined as the set of linear functions $\phi: V \to \mathbb{R}$. When $V \subseteq \mathbb{R}^n$, any linear function $\phi: V \to \mathbb{R}$ can be represented as a vector $\mathbf{w} \in V$ such that $\phi(\mathbf{x}) = \langle \mathbf{w}, \mathbf{x} \rangle$. (Namely, the vector $\mathbf{w}$ with coordinates $w_i = \phi(\mathbf{e}_i)$.) The definition of dual lattice is analogous to that for vector spaces, but with $\mathbb{R}$ replaced by $\mathbb{Z}$: the dual of a lattice Λ is the set of linear functions $\phi: V \to \mathbb{Z}$, represented as vectors in span(Λ). In fact, this is how dual vectors are typically used: by taking scalar products with primal lattice vectors. Each vector in the dual lattice $\mathbf{w} \in \hat{\Lambda}$ defines a linear function $\phi_{\mathbf{w}}(\mathbf{x}) = \langle \mathbf{w}, \mathbf{x} \rangle$ with the property that $\phi_{\mathbf{w}}(\Lambda) \subseteq \mathbb{Z}$. This allows to use $\mathbf{w}$ to partition Λ into layers

$$\Lambda = \bigcup_{i \in \mathbb{Z}} \{\mathbf{v} \in \Lambda : \phi_{\mathbf{w}}(\mathbf{v}) = i\}$$

where, as we will see, each layer is a shifted copy of the lower dimensional sublattice

$$\Lambda \cap \mathbf{w}^{\perp} = \{\mathbf{v} \in \Lambda : \langle \mathbf{w}, \mathbf{v} \rangle = 0\}.$$

orthogonal to $\mathbf{w}$. (See Figure 1.) The distance between the layers is precisely $1/\|\mathbf{w}\|$, so that the shorter the dual vector $\mathbf{w}$, the bigger is the distance between the layers. In order to get a good understanding of the dual of a lattice, it is useful to regard dual elements not just as functions, but as vectors themselves, and study how the geometry of the primal lattice relates to the geometry of the dual.

The following properties of the dual lattice easily follow from the definition, and suggest that the dual is, in some sense, the "inverse" of the original lattice.

[1] In fact, they are both special cases of the definition of dual of a module over an arbitrary ring.

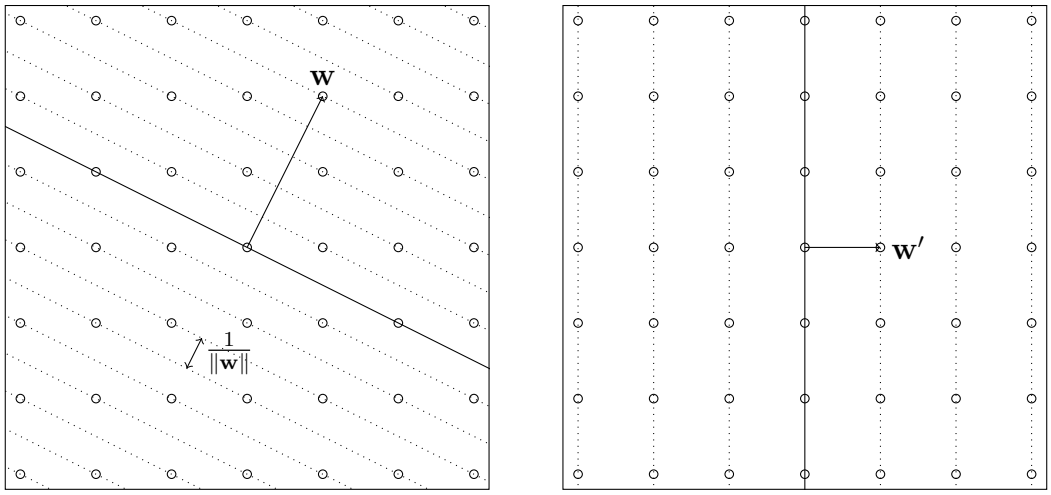

Figure 1: The integer lattice $\Lambda = \mathbb{Z}^2$, and some dual vectors $\mathbf{w}, \mathbf{w}' \in \hat{\Lambda} = \mathbb{Z}^2$. Each dual vector partitions Λ into layers Λ_i, corresponding to different values of the scalar product $\langle \mathbf{x}, \mathbf{w} \rangle = i \in \mathbb{Z}$. Each layer Λ_i is a shifter copy of the lower dimensional sublattice $\Lambda_0 \subset \Lambda$ orthogonal to $\mathbf{w}$. The distance between the layers is $1/\|\mathbf{w}\|$. In general, dual vectors do not belong to Λ.

Exercise 2 *Show that for any $c > 0$, the dual of $c\Lambda$ is $\frac{1}{c} \cdot \hat{\Lambda}$.*

Exercise 3 *Show that any two lattices with the same linear span span(Λ_1) = span(Λ_2) satisfy $\Lambda_1 \subseteq \Lambda_2$ if and only if $\hat{\Lambda}_1 \supseteq \hat{\Lambda}_2$.*

In order to prove additional properties of the dual lattice, it is useful to first show that the dual lattice is indeed a lattice, and give an explicit procedure to compute a lattice basis for it.

Theorem 2 *The dual of a lattice with basis $\mathbf{B}$ is a lattice with basis $\mathbf{D} = \mathbf{B}\mathbf{G}^{-1}$ where $\mathbf{G} = \mathbf{B}^\top\mathbf{B}$ is the Gram matrix[2] of $\mathbf{B}$.*

Before proving Theorem 2 in its full generality, we look at the special case when $\mathbf{B} \in \mathbb{R}^{n \times n}$ is a nonsingular square matrix. In this case, $\mathbf{v} \in \mathbb{R}^n$ is a dual vector if an only if it has integer scalar product with all lattice (basis) vectors, i.e., $\mathbf{B}^\top\mathbf{v} \in \mathbb{Z}^n$. Equivalently, this last condition can be written as $\mathbf{v} \in \mathbf{B}^{-\top}\mathbb{Z}^n = \mathcal{L}(\mathbf{B}^{-\top})$. So, $\mathbf{B}^{-\top}$ is a basis for the dual lattice. Notice that when $\mathbf{B} \in \mathbb{R}^{n \times n}$, the expression for the dual basis given in Theorem 2 simplifies to $\mathbf{D} = \mathbf{B}^{-\top}$. We now prove the Theorem 2 for arbitrary bases.

Proof. First of all, notice that for any vector $\mathbf{D}\mathbf{y} \in \mathcal{L}(\mathbf{D})$ we have

- $\mathbf{D}\mathbf{y} = \mathbf{B}((\mathbf{B}^\top\mathbf{B})^{-1}\mathbf{y}) \in \text{span}(\mathbf{B})$, and

[2]Notice that since $\mathbf{B}$ is a lattice basis, its columns are linearly independent, and the Gram matrix $\mathbf{G} = \mathbf{B}^\top\mathbf{B}$ is nonsingular, and it can be inverted in $\mathbb{R}^{n \times n}$.

- for all $\mathbf{Bx} \in \mathcal{L}(\mathbf{B})$, we have $(\mathbf{Dy})^\top(\mathbf{Bx}) = \mathbf{y}^\top\mathbf{x} \in \mathbb{Z}$.

So, $\mathbf{Dy} \in \hat{\mathcal{L}}(\mathbf{B})$ and $\mathcal{L}(\mathbf{D}) \subseteq \hat{\mathcal{L}}(\mathbf{B})$. Now consider an arbitrary vector $\mathbf{v}$ in the dual of $\mathcal{L}(\mathbf{B})$. By definition of dual, $\mathbf{B}^\top\mathbf{v} \in \mathbb{Z}^k$ and $\mathbf{v} \in \text{span}(\mathbf{B})$. It follows that

- $\mathbf{v} = \mathbf{Bw}$ for some $\mathbf{w} \in \mathbb{R}^n$ and
- $\mathbf{v} = \mathbf{Bw} = \mathbf{B}(\mathbf{B}^\top\mathbf{B})^{-1}\mathbf{B}^\top\mathbf{Bw} = \mathbf{D}(\mathbf{B}^\top\mathbf{v}) \in \mathcal{L}(\mathbf{D})$.

This proves that $\mathcal{L}(\mathbf{D}) \subseteq \mathcal{L}(\mathbf{B})$. □

Exercise 4 *Prove that the dual of the dual lattice equals the original lattice* $\hat{\hat{\Lambda}} = \Lambda$. [Hint: Use Theorem 2.]

Exercise 4 shows that duality is a symmetric relation, and we can talk about pairs of dual lattices without specifying which one is the primal and which is one is the dual. Notice that not only Theorem 2 shows that the dual of a lattice has some basis (and therefore, it is a lattice), but also gives a specific way to build a basis for the dual. This basis $\mathbf{D}$ for the dual lattice is called the *dual basis* of $\mathbf{B}$. It is easy to verify that also the relation between primal and dual basis is symmetric, i.e., if $\mathbf{D}$ is the dual basis of $\mathbf{B}$, then $\mathbf{B}$ is the dual basis for $\mathbf{D}$. The following exercise gives an alternative characterization of the dual basis that captures this symmetry already in the definition.

Exercise 5 *Prove that for any* $\mathbf{B}, \mathbf{D} \in \mathbb{R}^{m\times n}$, $\mathbf{D}$ *is the dual basis of* $\mathbf{B}$ *if and only if the following conditions are satisfied*

- *span*$(\mathbf{B})$ = *span*$(\mathbf{D})$, *and*
- $\mathbf{B}^\top\mathbf{D} = \mathbf{D}^\top\mathbf{B} = \mathbf{I}$.

In other words, $\mathbf{B}$ and $\mathbf{D}$ are dual bases if they have the same linear span, and any primal and dual basis vector have scalar product $\langle \mathbf{b}_i, \mathbf{d}_j \rangle = \delta_{i,j}$, where $\delta_{i,i} = 1$ and $\delta_{i,j} = 0$ for $i \neq j$.

Since the dual basis $\mathbf{D}$ uniquely determines $\mathbf{B}$, we can also regard $\mathbf{D}$ as an alternative method to represent a lattice $\mathcal{L}(\mathbf{B})$. In fact, the lattice $\mathcal{L}(\mathbf{B})$ can be defined as the set of all vectors $\mathbf{x} \in \text{span}(\mathbf{D})$ such that $\mathbf{D}^\top\mathbf{x}$ is an integer vector, or, equivalently, the set of solutions to a system of linear equations modulo 1:

$$\Lambda = \{\mathbf{x} \in \text{span}(\mathbf{D}) \colon \mathbf{D}^\top\mathbf{x} \equiv \mathbf{0} \pmod 1\}$$

where $\mathbf{D}$ is a basis for $\hat{\Lambda}$.

2 Relations between Primal and Dual

Using the dual basis, it is easy to prove many other properties of the dual lattice.

Exercise 6 *Show that for any pair of dual bases* $\mathbf{B}^\top\mathbf{D} = \mathbf{I}$*, the Gram matrix of the dual* $\mathbf{D}^\top\mathbf{D}$ *is the inverse of the Gram matrix of the primal* $\mathbf{B}^\top\mathbf{B}$*.*

Another simple geometric property of duality is that as a lattice gets denser, its dual gets sparser, and vice versa.

Exercise 7 *For every lattice* Λ*,* $\det\left(\hat{\Lambda}\right) = \frac{1}{\det(\Lambda)}$*.* [Hint: This is a direct consequence of the previous exercise.]

While the dual of an integer lattice is not in general an integer lattice, dual vectors have rational coordinates with bounded denominators.

Lemma 3 *The dual of an integer lattice* $\Lambda \subseteq \mathbb{Z}^d$ *satisfies* $\hat{\Lambda} \subseteq \mathbb{Z}^d/\det(\Lambda)^2$*. Moreover, if* Λ *has full rank, then* $\hat{\Lambda} \subseteq \mathbb{Z}^d/\det(\Lambda)$*.*

Proof. For the second part, let $\mathbf{B} \in \mathbb{Z}^{d\times d}$ be the basis of a full rank integer lattice, and assume, without loss of generality, that $\mathbf{B}$ is in Hermite Normal Form. The dual basis $\mathbf{D} = (\mathbf{B}^\top)^{-1}$ is the solution to the system of linear equations $\mathbf{B}^\top\mathbf{D} = \mathbf{I}$. It is easy to see (using the triangular structure of $\mathbf{B}$, and solving the system $\mathbf{B}^\top\mathbf{x}_i = \mathbf{e}_i$ by back substitution) that $\mathbf{D}$ has entries in $\mathbb{Z}/\det(\mathbf{B})$.

Now consider the first statement, and let $\mathbf{B} \in \mathbb{Z}^{d\times n}$ be a basis for Λ. Let $\mathbf{D} = \mathbf{B}\mathbf{G}^{-1}$ be the dual basis where $\mathbf{G} = \mathbf{B}^\top\mathbf{B}$ is the Gram matrix of $\mathbf{B}$. We need to show that $\mathcal{L}(\mathbf{B}\mathbf{G}^{-1}) \subseteq \mathbb{Z}^d/\det(\Lambda)^2$. Since $\mathbf{B}$ is an integer matrix, it is enough to show that $\mathcal{L}(\mathbf{G}^{-1}) \subseteq \mathbb{Z}^n/\det(\Lambda)^2$. But $\mathbf{G}$ is symmetric, and therefore $\mathbf{G}^\top\mathbf{G}^{-1} = \mathbf{I}$. Since $\mathbf{G}$ and $\mathbf{G}^{-1}$ are also full rank, they are dual bases, and $\mathcal{L}(\mathbf{G}^{-1}) = \widehat{\mathcal{L}(\mathbf{G})}$. Finally, using the fact that $\mathbf{G}$ has integer entries, we get $\widehat{\mathcal{L}(\mathbf{G})} \subseteq \mathbb{Z}^n/|\det(\mathbf{G})| = \mathbb{Z}^n/\det(\Lambda)^2$. □

As a simple application of the above proposition and lattice duality, we see that any integer lattice always contains a scaled copy of $\mathbb{Z}^n$ as a sublattice.

Exercise 8 *Show that for any nonsingular matrix* $\mathbf{B} \in \mathbb{Z}^{n\times n}$ *with absolute determinant* $d = |\det(\mathbf{B})|$*, we have* $d \cdot \mathbb{Z}^n \subseteq \mathcal{L}(\mathbf{B})$*.*

We may say that any full dimensional integer lattice $\Lambda \subseteq \mathbb{Z}^n$ is periodic modulo the determinant of the lattice, in the sense that for any two vectors $\mathbf{x}, \mathbf{y}$, if $\mathbf{x} \equiv \mathbf{y} \pmod{\det(\Lambda)}$, then $\mathbf{x} \in \Lambda$ if and only if $\mathbf{y} \in \Lambda$. A similar property holds for integer lattices that are not full dimensional, but modulo the squared determinant.

Exercise 9 *Show that for any (not necessarily full rank) integer lattice* $\Lambda \subseteq \mathbb{Z}^n$ *of determinant* $d = \det(\Lambda)$*, the lattice* $\Lambda = (d^2 \cdot \mathbb{Z}^n) \cap \mathit{span}(\Lambda)$ *is contained in* Λ*.*

Exercise 10 *Give a basis of an integer lattice* $\Lambda \subseteq \mathbb{Z}^d$ *such that* $(\det(\Lambda)\mathbb{Z}^d) \cap \mathit{span}(\Lambda)$ *is not contained in* Λ*.* [Hint: Remember that if Λ is not full rank, then $\det(\Lambda)$ is not necessarily an integer.]

3 Orthogonal projections and Dual Lattice

We now study how the dual lattice behaves with respect to basis changes, elementary column operations and the Gram-Schmidt orthogonalization procedure. This will be useful later on in the course. Let $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a basis and $\mathbf{D} = [\mathbf{d}_1, \ldots, \mathbf{d}_n]$ be the dual basis.

First of all, consider an arbitrary basis change $\mathbf{B} \mapsto \mathbf{BU}$ where $\mathbf{U}$ is a unimodular matrix. Then, the dual of the new basis changes as $\mathbf{D} \mapsto \mathbf{DU}^{-\top}$, because $(\mathbf{DU}^{-\top})^\top(\mathbf{BU}) = \mathbf{U}^{-1}(\mathbf{D}^\top\mathbf{B})\mathbf{U} = \mathbf{I}$. As a special case, when $\mathbf{U}$ corresponds to an elementary column operation, we get that the dual basis is updated as follows:

1. If SWAP(i,j) is applied to the primal basis, then SWAP(i,j) is also applied to the dual basis.

2. If INVERT(i) is applied to the primal basis, then INVERT(i) is also applied to the dual basis.

3. If ADD(i,c,j) is applied to the primal basis, then ADD(j,-c,i) is applied to the dual basis.

Note: in the last case, not only the sign of c is changed, but also i and j are swapped. These operations are all special cases of taking the inverse transpose of the transformation matrix $\mathbf{U}$ applied to the primal basis.

Now consider the Gram-Schmidt orthogonalization process. Let $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a basis, and $\mathbf{B}^* = [\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*]$ be its Gram-Schmidt orthogonalization. Let also $\pi_i(\mathbf{x}) = \mathbf{x}\perp[\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]$, for $i = 1, \ldots, n$, be the projection operations associated to $\mathbf{B}^*$. Consider the projected lattice

$$\pi_i(\mathcal{L}(\mathbf{B})) = \mathcal{L}([\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)]).$$

What is the dual of $\pi_i(\mathcal{L}(\mathbf{B}))$? We now show that the dual of $\pi_i(\mathcal{L}(\mathbf{B}))$ is the sublattice of $\mathcal{L}(\mathbf{D})$ generated by $\mathbf{d}_i, \ldots, \mathbf{d}_n$. (Notice that no orthogonal projection is applied to the dual (sub)lattice.)

Lemma 4 *Let $\mathbf{B}, \mathbf{D} \in \mathbb{R}^{d\times n}$ be a pair of dual basis. For all $i = 1, \ldots, n$, $[\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)]$ and $[\mathbf{d}_i, \ldots, \mathbf{d}_n]$ are also dual bases.*

Proof. We only need to prove the statement for $i = 2$. The general statement easily follows by induction on i. So, let $\mathbf{B}' = [\pi_2(\mathbf{b}_2), \ldots, \pi_2(\mathbf{b}_n)]$ and $\mathbf{D}' = [\mathbf{d}_2, \ldots, \mathbf{d}_n]$. We want to prove that $\mathbf{B}'$ and $\mathbf{D}'$ span the same vector space, and $(\mathbf{B}')^\top(\mathbf{D}') = \mathbf{I}$.

We know that $\mathbf{B}$ and $\mathbf{D}$ span the same vector space V. The linear span of $\mathbf{B}'$ is by definition the orhogonal complement of $\mathbf{b}_1$ in V. Since the vectors $\mathbf{d}_2, \ldots, \mathbf{d}_n$ are all orthogonal to $\mathbf{b}_1$ (by definition of dual basis) and they are linearly independent, they also span the orthogonal complement of $\mathbf{b}_1$ in V. So, $\mathbf{B}'$ and $\mathbf{D}'$ have the same linear span.

Let us prove that for all $i, j > 1$ we have $\langle \pi_2(\mathbf{b}_i), \mathbf{d}_j \rangle = \delta_{i,j}$, where $\delta_{i,i} = 1$ and $\delta_{i,j} = 0$ for $i \neq j$. Using the definition of $\pi_2(\mathbf{x}) = \mathbf{x} - (\langle \mathbf{x}, \mathbf{b}_1 \rangle / \|\mathbf{b}_1\|^2)\mathbf{b}_1$ we get

$$\begin{aligned} \langle \pi_2(\mathbf{b}_i), \mathbf{d}_j \rangle &= \langle \mathbf{b}_i - \mu_{i,1}\mathbf{b}_1, \mathbf{d}_j \rangle \\ &= \langle \mathbf{b}_i, \mathbf{d}_j \rangle - \mu_{i,1}\langle \mathbf{b}_1, \mathbf{d}_j \rangle \\ &= \delta_{i,j} - \mu_{i,j}\delta_{1,j} = \delta_{i,j} \end{aligned}$$

because $j > 1$ and $\delta_{1,j} = 0$. This proves that $(\mathbf{B}')^\top(\mathbf{D}') = \mathbf{I}$. □

Now define the orthogonalization of the dual basis in the usual way, but going through the basis vectors in reverse order from $\mathbf{d}_n$ to $\mathbf{d}_1$:

$$\mathbf{d}_i^\dagger = \tau_i(\mathbf{d}_i) \qquad \text{where} \qquad \tau_i(\mathbf{x}) = \mathbf{x} \perp [\mathbf{d}_{i+1}, \ldots, \mathbf{d}_n].$$

It follows by duality that for all i, the dual of $[\mathbf{b}_1, \ldots, \mathbf{b}_i]$ is the projected basis $[\tau_i(\mathbf{d}_1), \ldots, \tau_i(\mathbf{d}_i)]$. In general we have the following.

Theorem 5 *Let* $\mathbf{D}$ *be the dual of* $\mathbf{B}$*. Then for all* $i \leq j$ *the dual of* $[\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_j)]$ *is* $[\tau_j(\mathbf{d}_i), \ldots, \tau_j(\mathbf{d}_j)]$.

In particular, when $i = j$ we get the following corollary.

Corollary 6 *Let* $\mathbf{D}$ *be the dual of* $\mathbf{B}$ *and let* $\mathbf{B}^*$ *and* $\mathbf{D}^\dagger$ *the corresponding orthogonalized bases. Then for all* i *the two vectors* $\mathbf{b}_i^*$ *and* $\mathbf{d}_i^\dagger$ *satisfy*

- $\frac{\mathbf{b}_i^*}{\|\mathbf{b}_i^*\|} = \frac{\mathbf{d}_i^\dagger}{\|\mathbf{d}_i^\dagger\|}$
- $\|\mathbf{b}_i^*\| \cdot \|\mathbf{d}_i^\dagger\| = 1$.

In particular, $\mathbf{b}_n^*/\|\mathbf{b}_n^*\|^2 = \mathbf{d}_n$ *is a dual lattice vector.*

From the relation $\mathbf{b}_n^*/\|\mathbf{b}_n^*\|^2 = \mathbf{d}_n$ we see that the lattice partition into layes defined by taking scalar products with the dual vector $\mathbf{d}_n$ is precisely the same $c\mathbf{b}_n + \mathcal{L}([\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}])$ ($c \in \mathbb{Z}$) we first encountered when studying the Gram-Schmidt orthogonalization of a basis.

4 Application to Gram-Schmidt computation

A recurring problem, whenever a lattice algorithm makes use of orthogonal projection operations, is that of evaluating the precision required to carry out all necessary computation, and bounding the size of all numbers. For example, it is easy to see that the number of arithmetic operations performed by the Gram-Schmidt orthogonalization procedure is $O(n^3)$. However, this is not enough to conclude that the resulting computation is even polynomial time. That's because each time two n-bit numbers are multiplied together, the result may have up to $2n$ bits. So, a sequence of $O(n^3)$ arithmetic operations may lead to numbers as big as $2^{O(n^3)}$ bits! Also, 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. Bounding the size of the numbers (numerators and denominators) that occur in the Gram-Schmidt orthogonalization turns out to be useful in many other algorithms that employ orthogonal projections.

We start by bounding the denominators that occur in the entries of $\mathbf{B}^*$. This can be easily done using the simple facts about lattice duality proved so far.

Lemma 7 *Let $\mathbf{B} \in \mathbb{Z}^{d\times n}$ be an integer basis, and $\mathbf{B}^*$ its Gram-Schmidt orthogonalization. Then, for every $i = 1, \ldots, n$, the orthogonalized vector $\mathbf{b}_i^*$ satisfies $\mathbf{b}_i^* \in \mathbb{Z}^d / D_{i-1}^2$ where $D_{i-1} = \det(\mathcal{L}([\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]))$ is the determinant of the sublattice generated by the first $i-1$ basis vectors.*

Proof. It is enough to prove the statement for $i = n$. Let $\mathbf{B} \in \mathbb{Z}^{d\times n}$ be an integer basis, and let $\mathbf{b}_n^*$ be the component of $\mathbf{b}_n$ orthogonal to the other basis vectors. By Corollay 6 and Lemma 3, we have $\mathbf{b}_n^*/\|\mathbf{b}_n^*\|^2 = \mathbf{d}_n \in \mathbb{Z}^n/\det(\mathcal{L}(\mathbf{B}))^2$. Therefore $\mathbf{b}_n^* \in \|\mathbf{b}_n^*\|^2 \cdot \mathbb{Z}^n/\det(\mathcal{L}(\mathbf{B}))^2 = \mathbb{Z}^n/\det(\mathcal{L}([\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}]))^2$. □

It immediately follows also that the Gram-Schmidt coefficients satisfy

$$\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \in \frac{\mathbb{Z}}{\|\mathbf{b}_j^*\|^2 \cdot D_{j-1}^2} = \frac{\mathbb{Z}}{D_j^2}.$$

This proves that the denominators of all numbers involved in the Gram-Schmidt orthogonalization divide $\det(\mathbf{B})^2$, and all computations can be performed using $\det(\mathbf{B})^2$ as a common denominator. If M is an upper bound on the length $\|\mathbf{b}_i\|$ of all input basis vectors., by Hadamard inequality, this common denominator is at most $\det(\mathbf{B})^2 \leq M^{2n}$. Since $|\mu_{i,j}| \leq \frac{1}{2}$, the numerators of the Gram-Schmidt coefficients are also at most M^{2n}. It remains to bound the numerators of the coordinates of the orthogonalized vectors $\mathbf{b}_i^*$. All entries in $\|\mathbf{b}_i^*\|$ are at most $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\| \leq M$ in absolute value. It follows that their numerators are at most M^{2n+1}. This proves that the Gram-Schmidt orthogonalization procedure runs in polynomial time.

Theorem 8 *On input a basis $\mathbf{B} \in \mathbb{Z}^{d\times n}$ with vectors of length at most $\|\mathbf{b}_i\| \leq M$, the Gram-Schmidt orthogonalization procedure computes $\mathbf{B}^*$ and the Gram-Schmidt coefficients $\mu_{i,j}$ performing $O(d \cdot n^2)$ arithmetic operations on integers of bit size at most $(2n+1)\log M$.*

5 The closest vector problem

The Closest Vector Problem (CVP) is the inhomogeneous version of the Shortest Vector Problem (SVP), and it is, next to SVP, one of the most important and well studied computational problems on point lattices.

Definition 9 *The Closest Vector Problem (CVP) asks, given a lattice basis $\mathbf{B}$ and target vector $\mathbf{t}$, to find the lattice vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that the distance to the target $\|\mathbf{v} - \mathbf{t}\|$ is minimized. In the γ-approximate CVP, for $\gamma \geq 1$, the goal is to find a lattice vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \gamma \cdot dist(\mathbf{t}, \mathcal{L}(\mathbf{B}))$ where $dist(\mathbf{t}, \Lambda) = \inf\{\|\mathbf{v} - \mathbf{t}\| : \mathbf{v} \in \Lambda\}$ is the distance of $\mathbf{t}$ to Λ.*

The problem can be defined with respect to any norm, but the Euclidean norm is the most common. Usually the target $\mathbf{t}$ belongs to the linear span of the lattice, but this is not

always the case. When working in the Euclidean norm, one may assume without loss of generality that the target $\mathbf{t}$ belongs to the linear span of the lattice, as one can efficiently project any target $\mathbf{t}$ orthogonally onto $\text{span}(\mathbf{B})$ without modifying the solution. Of course, the target is certainly in the linear span of the lattice if the lattice is full dimensional.

The goal of CVP can be equivalently restated as that of finding a shortest vector in the lattice coset $\mathbf{t} + \Lambda$. If $\mathbf{e} = \mathbf{t} + \mathbf{v} \in \mathbf{t} + \Lambda$ is such a point, then $-\mathbf{v} = \mathbf{t} - \mathbf{e} \in \Lambda$ is a lattice point closest to the target, i.e., a CVP solution. The same holds for approximate solutions. Lattice cosests can be described using the dual lattice. Let $\mathbf{D} \in \mathbb{R}^{n \times k}$ be an arbitrary generating set for the dual lattice $\mathcal{L}(\mathbf{D}) = \hat{\Lambda} \subset \mathbb{R}^n$. For any vector $\mathbf{t} \in \mathbb{R}^n$, the vector $(\mathbf{D}^\top \mathbf{t}) \bmod 1 \in [0,1)^k$ is called the *syndrome* of $\mathbf{t}$ with respect to $\mathbf{D}$. Notice that the syndrome depends not just on $\hat{\Lambda} = \mathcal{L}(\mathbf{D})$, but also on the specific matrix $\mathbf{D}$. Also, the syndrome only depends on the component of $\mathbf{t}$ in $\text{span}(\mathbf{D}) = \text{span}(\Lambda)$, so it is often assumed that $\mathbf{t} \in \text{span}(\Lambda)$.

Exercise 11 *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\mathbf{D}$ an arbitrary generating set for the dual lattice $\mathcal{L}(\mathbf{D}) = \hat{\Lambda}$. Show that for any two vectors $\mathbf{t}, \mathbf{e} \in \mathbb{R}^n$, $\mathbf{e}$ belongs to the lattice coset of $\mathbf{t}$ (i.e., $\mathbf{e} \in \mathbf{t} + \Lambda$) if and only if they have the same syndrome $\mathbf{D}^\top \mathbf{e} = \mathbf{D}^\top \mathbf{t} \pmod 1$ and belong to the same affine span $\mathbf{e} \in \mathbf{t} + \text{span}(\Lambda)$.*

When the lattice has full rank, the condition $\mathbf{e} \in \mathbf{t} + \text{span}(\Lambda) = \mathbb{R}^n$ holds trivially, and we get the following *syndrome decoding* formulation of the closest vector problem.

Definition 10 *The syndrome decoding problem for lattices, on input a non-singular matrix $\mathbf{H} \in \mathbb{R}^{n \times n}$ and a syndrome vector $\mathbf{s} \in [0,1)^n$ asks to find a solution to the equation $\mathbf{Hx} = \mathbf{s} \pmod 1$ of smallest norm. In the γ-approximate version of the problem, the goal is to find a solution $\mathbf{x}$ of length within a factor γ from the optimal.*

6 Transference Theorems

Throughout this section, let Λ be an n-dimensional lattice with successive minima $\lambda_1, \ldots, \lambda_n$ and covering radius μ. We have seen that

$$\lambda_1 \leq \ldots \leq \lambda_n \leq 2\mu \leq \sqrt{n}\lambda_n.$$

But how do the successive minima and covering radius of Λ relate to the successive minima and covering radius of the dual lattice? As the dual of $c\Lambda$ is $\frac{1}{c}\hat{\Lambda}$, we may expect the successive minima of Λ to be inversely proportional to the successive minima of the dual. We want to turn this intuition into a quantitative statement that allows to "transfer" knowledge about the parameters of a lattice Λ, to knowledge about the parameters of its dual. We begin by looking at the minimum distance.

Exercise 12 *Prove that for any n-dimensional lattice Λ, $\lambda_1(\Lambda) \cdot \lambda_1(\hat{\Lambda}) \leq n$.* [Hint: Use Minkowski's theorem on both the primal and dual lattice.]

It immediately follows from the exercise that if $\lambda_1(\Lambda)$ is large (say, much bigger than n), then $\lambda_1(\hat{\Lambda}) \leq n/\lambda_1(\Lambda)$ must be small. However, the converse is not necessarily true, i.e., both $\lambda_1(\Lambda)$ and $\lambda_1(\hat{\Lambda})$ can be very small.

Exercise 13 *Show that for any $\epsilon > 0$ and dimension $n \geq 2$, there is an n-dimensional lattice Λ such that $\lambda_1(\Lambda) = \lambda_1(\hat{\Lambda}) \leq \epsilon$.*

Similarly, one can show that $\lambda_n(\Lambda)$ and $\lambda_n(\hat{\Lambda})$ cannot be simultaneously small, but they can both be very large.

Exercise 14 *Show that for any c and dimension $n \geq 2$, there is an n-dimensional lattice Λ such that $\lambda_n(\Lambda) = \lambda_n(\hat{\Lambda}) \geq c$.*

A better connection between the parameter of a lattice and those of its dual can be established by comparing the minimum distance $\lambda_1(\Lambda)$ with the last minimum (or covering radius) of the dual $\lambda_n(\hat{\Lambda})$.

Exercise 15 *Prove that for any n-dimensional lattice Λ, $\lambda_1(\Lambda) \cdot \lambda_n(\hat{\Lambda}) \geq 1$. More generally, prove that for any k, $\lambda_k(\Lambda) \cdot \lambda_{n-k+1}(\hat{\Lambda}) \geq 1$.* [Hint: For the first part, consider the scalar products between a shortest lattice vector and n short linearly independent vectors from the dual lattice.]

So, if $\lambda_n(\Lambda)$ (or the covering radius $\mu(\Lambda) \geq \lambda_n(\Lambda)/2$) is small, then the dual minimum distance $\lambda_1(\hat{\Lambda}) \geq 1/\lambda_n(\Lambda)$ must necessarily be large. Again, we may ask if the converse is also true: if $\lambda_n(\Lambda)$ is large, must the minimum distance of the dual lattice be necessarily small? The answer is yes, and it follows from the following bound.

Theorem 11 *For any n-dimensional lattice Λ*

$$1 \leq \lambda_k(\Lambda) \cdot \lambda_{n-k+1}(\hat{\Lambda}) \leq n,$$

$$1 \leq \lambda_1(\Lambda) \cdot 2\mu(\hat{\Lambda}) \leq n.$$

The lower bound was already proved in the last exercise (or follows from the relation $\lambda_n \leq 2\mu$). The upper bound is a result of Banaszczyk, which we will prove later in the course using harmonic analysis. These results are usually referred to as "transference theorems", because they allows to transfer information between the primal and dual lattice.