CSE 206A: Lattice Algorithms and Applications Winter 2012

2: The dual lattice

Instructor: *Daniele Micciancio* UCSD CSE

1. Dual lattice and Dual bases

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

Exercise 2. 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 usually it is not a sublattice of Λ. E.g., even if $\Lambda \subset \mathbb{Z}^n$ is an integer lattice, the dual will contain noninteger vectors. The definition of dual lattice is very natural if we compare it with the definition of dual for vector spaces. Recall that the dual of an abstract vector space V is defined as the set of linear functions $\phi\colon V \to \mathbb{R}$. When $V \subseteq \mathbb{R}^n$, it is customary to represent function ϕ as a vector $\mathbf{v} \in V$ such that $\phi(\mathbf{x}) = \langle \mathbf{v}, \mathbf{x} \rangle$.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 $\phi\colon V \to \mathbb{Z}$, represented as vectors in $\text{span}(\Lambda)$.

Theorem 3. *The dual of a lattice with basis* $\mathbf{B}$ *is a lattice with basis* $\mathbf{D} = \mathbf{B}(\mathbf{B}^\top\mathbf{B})^{-1}$.

Before proving Theorem 3 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 $\mathbf{B}^\top\mathbf{v} \in \mathbb{Z}^n$, or equivalently $\mathbf{v} \in \mathbf{B}^{-\top}\mathbb{Z}^n = \mathcal{L}(\mathbf{B}^{-\top})$. 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 3 reduces to $\mathbf{D} = \mathbf{B}^{-\top}$. We now prove the Theorem 3 for arbitrary bases.

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

- $\mathbf{Dy} = \mathbf{B}((\mathbf{B}^\top\mathbf{B})^{-1}\mathbf{y}) \in \text{span}(()\mathbf{B})$, and
- 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 if $\mathbf{D} = \mathbf{B}(\mathbf{B}^\top\mathbf{B})^{-1}$ then $\mathbf{B} = \mathbf{D}(\mathbf{D}^\top\mathbf{D})^{-1}$. In particular, the dual of the dual lattice equals the original lattice.

Exercise 4 shows that basis duality is a symmetric relation, and we can talk about pairs of dual bases without specifying which basis is for the primal and which is for the dual. 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

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

2. Relations between Primal and Dual

A simple geometric property of duality is that as a lattice gets denser, its dual gets sparser, and vice versa. Intuitively, a lattice and its dual are one the inverse of the other.

Proposition 6. *For every lattice* Λ, $\det\left(\hat{\Lambda}\right) = \frac{1}{\det(\Lambda)}$.

Proof. Let $\Lambda = \mathcal{L}(\mathbf{B})$ and $\mathbf{D} = \mathbf{B}(\mathbf{B}^\top\mathbf{B})^{-1}$. We know that $\det(\Lambda) = \sqrt{\det(\mathbf{B}^\top\mathbf{B})}$. Therefore

$$\det\left(\hat{\Lambda}\right) = \sqrt{\det(\mathbf{D}^\top\mathbf{D})} = \sqrt{\det((\mathbf{B}^\top\mathbf{B})^{-\top}\mathbf{B}^\top\mathbf{B}(\mathbf{B}^\top\mathbf{B})^{-1})} = \sqrt{\det(\mathbf{B}^\top\mathbf{B})^{-1}} = 1/\det(\Lambda).$$

□

There are many other properties that can be informally interpreted as saying that the dual is in some sense the "inverse" of a lattice.

Exercise 7. 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 $\mathbf{B}^\top\mathbf{B}$.

Exercise 8. Show that for any $c > 0$, the dual of $c\Lambda$ is $c^{-1} \cdot \hat{\Lambda}$.

The following property directly follows from the definition of dual lattice.

Exercise 9. Show that for any two lattices with the same linear span $\text{span}(\Lambda) = \text{span}(\Lambda')$, if $\Lambda \subseteq \Lambda'$, then $\hat{\Lambda} \supseteq \hat{\Lambda}$.

The following exercise shows that while the dual of an integer lattice is not in general an integer lattice, dual vectors have rational coordinates with bounded denominators.

Exercise 10. Show that if $\Lambda \subseteq \mathbb{Z}^d$ is a full rank integer lattice, then $\hat{\Lambda} \subseteq \mathbb{Z}^d/\det(\Lambda)$.

In fact, one can prove a similar result also for integer lattices that are not full rank.

Proposition 11. *The dual of an integer lattice* $\Lambda \subseteq \mathbb{Z}^d$ *satisfies* $\hat{\Lambda} \subseteq \mathbb{Z}^d/\det(\Lambda)^2$.

Proof. Let $\mathbf{B} \in \mathbb{Z}^{d\times n}$ be a basis for Λ, and let $\mathbf{D} = \mathbf{B}\mathbf{G}^{-1}$ be the dual basis where $\mathbf{G} = \mathbf{B}^\top\mathbf{B}$. 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 $\mathcal{L}(\mathbf{G}^{-1}) = \hat{\mathcal{L}}(\mathbf{G})$. Finally, using the fact that $\mathbf{G}$ has integer entries, we get $\hat{\mathcal{L}}(\mathbf{G}) \subseteq \mathbb{Z}^n/|\det(\mathbf{G})| = \mathbb{Z}^n/\det(\Lambda)^2$. □

3. Gram-Schmidt and Dual Lattice

We now study how the dual lattice behaves with respect to basis changes, basic 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 $\mathbf{B}' = \mathbf{B}\mathbf{U}$ where $\mathbf{U}$ is a unimodular matrix. Then, the dual of the new basis is $\mathbf{D}' = \mathbf{D}\mathbf{U}^{-\top}$ because $(\mathbf{D}')^\top\mathbf{B}' = \mathbf{U}^{-1}(\mathbf{D}^\top\mathbf{B})\mathbf{U} = \mathbf{I}$. For the special case when $\mathbf{U}$ corresponds to an elementary column operation, we see that in order maintain the relationship $\mathbf{D}^\top\mathbf{B} = \mathbf{I}$, the dual basis should be updated as follows:

(1) If $\mathbf{B}'$ is obtained from $\mathbf{B}$ by swapping columns i and j, then the dual basis of $\mathbf{B}'$ is also obtained from $\mathbf{D}$ by swapping columns i and j, i.e., the dual of the elementary column operation swap(i,j) is swap(i,j).
(2) If $\mathbf{B}'$ is obtained from $\mathbf{B}$ by multiplying columns i by -1, then the dual basis of $\mathbf{B}'$ is also obtained from $\mathbf{D}$ by multiplying column i by -1, i.e., the dual of invert(i) is invert(i).
(3) If $\mathbf{B}'$ is obtained from $\mathbf{B}$ by adding $c \cdot \mathbf{b}_i$ to $\mathbf{b}_j$, then the dual basis of $\mathbf{B}'$ is obtained from $\mathbf{D}$ by subtracting $c \cdot \mathbf{d}_j$ from $\mathbf{d}_i$, i.e., the dual of add(j,c,i) is add(i,-c,j).

This gives a simple way to update a basis and its dual at the same time.

Now consider the Gram-Schmidt orthogonalization process:

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

and the projection operations π_i from $\mathbb{R}^m$ onto $\sum_{j \geq i} \mathbb{R}\mathbf{b}_j^*$:

$$\pi_i(\mathbf{x}) = \sum_{j=i}^{n} \frac{\langle \mathbf{x}, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} \mathbf{b}_j^*.$$

Consider the projected lattice

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

What is the dual of $\pi_i(\Lambda)$? We now show that the dual of $\pi_i(\Lambda)$ is the sublattice generated by $\mathbf{d}_i, \ldots, \mathbf{d}_n$.

Proposition 12. *Let $\mathbf{B}, \mathbf{D}$ a pair of dual basis. For all i, $[\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)]$ and $[\mathbf{d}_i, \ldots, \mathbf{d}_n]$ are also dual basis.*

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 $(\mathbf{B}')^\top(\mathbf{D}') = \mathbf{I}$. Let's prove this second property first. We want to show that for all $i \neq j > 1$ we have $\langle \pi_2(\mathbf{b}_i), \mathbf{d}_j \rangle = \delta_{i,j}$. Using the definition of π_2 we get

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

because $j > 1$. This proves that $(\mathbf{B}')^\top(\mathbf{D}') = \mathbf{I}$. We now show that $\mathbf{B}'$ and $\mathbf{D}'$ span the same vector space. 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. This complete the proof. □

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

$$\mathbf{d}_i^\dagger = \mathbf{d}_i - \sum_{j>i} \eta_{i,j}\mathbf{d}_j^\dagger \quad \text{where } \eta_{i,j} = \frac{\langle \mathbf{d}_i, \mathbf{d}_j^\dagger \rangle}{\langle \mathbf{d}_j^\dagger, \mathbf{d}_j^\dagger \rangle}$$

and the corresponding projection operations τ_i from $\mathbb{R}^m$ onto $\sum_{j\le i}\mathbb{R}\mathbf{d}_j^\dagger$:

$$\tau_i(\mathbf{x}) = \sum_{j=1}^{i} \frac{\langle \mathbf{x}, \mathbf{d}_j^\dagger\rangle}{\langle \mathbf{d}_j^\dagger, \mathbf{d}_j^\dagger\rangle}\mathbf{d}_j^\dagger.$$

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 13. *Let* $\mathbf{D}$ *be the dual of* $\mathbf{B}$*. Then for all* $i \le j$ *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 14. *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.*

As a simple application of the results we proved, we use the dual basis to bound the size of the denominators that occur when applying the Gram-Schmidt orthogonalization process to an integer basis.

Proposition 15. *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 Proposition 12 (with $i = n$), $\mathbf{d}_n = \mathbf{b}_n^*/\|\mathbf{b}_n^*\|^2 \in \mathbb{Z}^n/\det(\mathcal{L}(\mathbf{B}))^2$. Therefore $\mathbf{b}_n^* \in \|\mathbf{b}_n^*\|^2 \cdot \mathbb{Z}^n/\det(\mathcal{L}(\mathbf{B}))^2 = \mathbb{Z}^n/\det(\mathcal{L}([\mathbf{b}_1,\ldots,\mathbf{b}_{n-1}]))^2$. □

4. The closest vector problem

Duality can be used to given an alternative and often very useful definition for the closest vector problem. In CVP, the input is a lattice Λ and a target vector $\mathbf{t}$ and the goal is to find a lattice vector $\mathbf{v} \in \Lambda$ for which the distance to the target $\|\mathbf{t}-\mathbf{e}\|$ is minimized. Equivalently, the goal is to find a point in the lattice coset $\mathbf{t} - \Lambda = \mathbf{t} + \Lambda$ of minimal norm. If $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is such a point, then $\mathbf{v} = \mathbf{t} - \mathbf{e}$ is a CVP solution.

Exercise 16. Let $\Lambda \subset \mathbb{R}^n$ be a lattice an $\mathbf{D}$ an arbitrary basis for the dual lattice $\mathcal{L}(\mathbf{D}) = \Lambda^*$. Then, for any two vectors $\mathbf{t}, \mathbf{e} \in \mathbb{R}^n$, $\mathbf{e} \in \mathbf{t} + \Lambda$ if and only if the following conditions are satisfied

(1) $\mathbf{e} \in \mathbf{t} + \mathrm{span}(()\Lambda)$, and
(2) $\mathbf{D}^\top\mathbf{e} = \mathbf{D}^\top\mathbf{t} \pmod 1$.

In particular, the CVP for lattice Λ with target $\mathbf{t}$ (i.e., minimizing $\|\mathbf{t}-\mathbf{v}\|$ over the lattice $\mathbf{v} \in \Lambda$) is equivalent to the problem of finding the shortest vector $\mathbf{e} \in \mathbf{t} + \mathrm{span}(()\Lambda)$ such that $\mathbf{D}^\top\mathbf{e} = \mathbf{D}^\top\mathbf{t} \pmod 1$.

In coding theory, $\mathbf{e}$ is a small error vector by which a lattice codeword $\mathbf{v} \in \Lambda$ has been perturbed to yield $\mathbf{t} = \mathbf{v} + \mathbf{e}$. The vector $\mathbf{D}^\top \mathbf{t} \pmod 1 = \mathbf{D}^\top \mathbf{e} \pmod 1$ is called the *syndrome* of the error because it can be computed from the target, but it only depends on the error vector $\mathbf{e}$ and not on the lattice codeword $\mathbf{v}$. When the lattice has full rank, the condition $\mathbf{e} \in \mathbf{t} + \mathrm{span}(()\Lambda) = \mathbb{R}^n$ holds trivially, and we get the following *syndrome decoding* formulation of the closest vector problem.

Definition 17. The syndrome decoding problem for lattices, on input a non-singular matrix $\mathbf{H} \in \mathbb{R}^{n \times n}$ and a vector $\mathbf{b} \in [0, 1)^n$ asks to find a solution to the equation $\mathbf{Hx} = \mathbf{b} \pmod 1$ of smallest norm.

Exercise 18. Prove that CVP for full rank lattices is equivalent to the syndrome decoding problem. More specifically, give efficient reductions between (approximation versions of) the two problems in both directions. The reductions should hold for any norm, and be approximation preserving.