In this lecture we define the notion of the *dual* of a lattice and see some if its applications.

DEFINITION 1 *For a full-rank lattice Λ we define its* dual lattice *(sometimes known as the* reciprocal lattice*)*

$$\Lambda^* = \{y \in \mathbb{R}^n \mid \forall x \in \Lambda,\ \langle x, y\rangle \in \mathbb{Z}\}.$$

In general, we define

$$\Lambda^* = \{y \in \mathrm{span}(\Lambda) \mid \forall x \in \Lambda,\ \langle x, y\rangle \in \mathbb{Z}\}.$$

In words, the dual of Λ is the set of all points (in the span of Λ) whose inner product with any of the points in Λ is integer. As we will show later, Λ^* is indeed a lattice, as the name suggests.

EXAMPLE 1 The lattice of integer points satisfies $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ (and hence can be called self-dual). Similarly, $(2\mathbb{Z}^n)^* = \frac{1}{2}\mathbb{Z}^n$, and this gives some justification to the name reciprocal lattice.

From the above definition, we have the following geometrical interpretation of the dual lattice. For any vector x, the set of all points whose inner product with x is integer forms a set of hyperplanes perpendicular to x and separated by distance $1/\|x\|$. Hence, any vector x in a lattice Λ imposes the constraint that all points in Λ^* lie in one of the hyperplanes defined by x. See the next figure for an illustration.

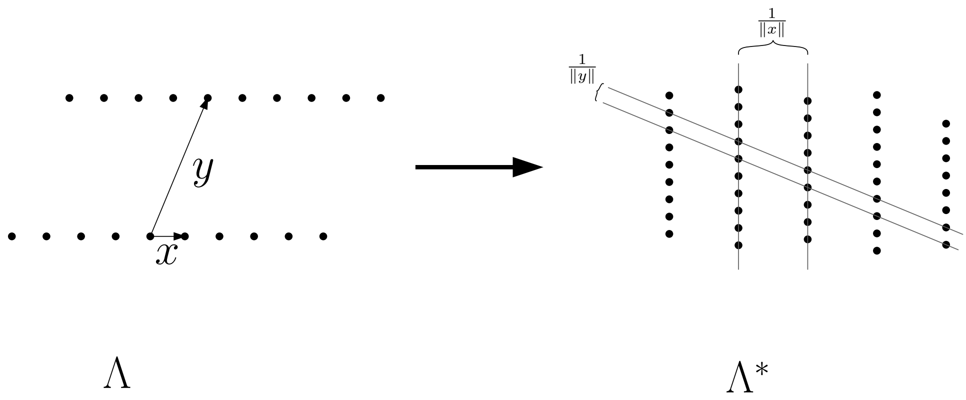

Figure 1: A lattice and its dual

DEFINITION 2 *For a basis $B = (b_1, \ldots, b_n) \in \mathbb{R}^{m\times n}$, define the* dual basis $D = (d_1, \ldots, d_n) \in \mathbb{R}^{m\times n}$ *as the unique basis that satisfies*

- $\mathrm{span}(D) = \mathrm{span}(B)$
- $B^T D = I$

The second condition can be interpreted as saying that $\langle b_i, d_j\rangle = \delta_{ij}$ where $\delta_{ij} = 1$ if $i = j$ and 0 otherwise. It is not hard to check that D is indeed unique. In fact, for the case of a full-rank lattice, D is given by $(B^T)^{-1}$; in general, we get $D = B(B^TB)^{-1}$ (and we could use this as our definition of a dual basis).

In the next claim, we show that if B is a basis of a lattice Λ, then the dual basis of B is a basis of Λ^*. In particular, this shows that Λ^* is indeed a lattice.

CLAIM 1 *If D is the dual basis of B then $(\mathcal{L}(B))^* = \mathcal{L}(D)$.*

PROOF: We first show that $\mathcal{L}(D)$ is contained in $(\mathcal{L}(B))^*$. Any $x \in \mathcal{L}(B)$ can be written as $\sum a_i b_i$ for some $a_i \in \mathbb{Z}$. Therefore, for any j we have

$$\langle x, d_j \rangle = \sum_i a_i \langle b_i, d_j \rangle = a_i \in \mathbb{Z}$$

and we get $D \subseteq (\mathcal{L}(B))^*$. It is easy to check that $(\mathcal{L}(B))^*$ is closed under addition, hence, $\mathcal{L}(D) \subseteq (\mathcal{L}(B))^*$. To complete the proof, we show that $(\mathcal{L}(B))^*$ is contained in $\mathcal{L}(D)$. Take any $y \in (\mathcal{L}(B))^*$. Since $y \in \mathrm{span}(B) = \mathrm{span}(D)$, we can write $y = \sum a_i d_i$ for some $a_i \in \mathbb{R}$. Now for all j, $\mathbb{Z} \ni \langle y, b_j \rangle = \sum a_i \langle d_i, b_j \rangle = a_j$. Hence, $y \in \mathcal{L}(D)$ and the proof is complete. $\Box$

CLAIM 2 *For any lattice* Λ, $(\Lambda^*)^* = \Lambda$.

PROOF: Let B be a basis of Λ. Then $B(B^T B)^{-1}$ is a basis of Λ^* and

$$\left(B(B^T B)^{-1}\right) \cdot \left((B(B^T B)^{-1})^T \cdot B(B^T B)^{-1}\right)^{-1} = B$$

is a basis of $(\Lambda^*)^*$. $\Box$

The next claim says that the volume of the basic parallelepiped of Λ^* is the reciprocal of that of Λ. For example, it implies that the volume of the basic parallelepiped of a self-dual lattice must be 1 (as is the case with $\mathbb{Z}^n$).

CLAIM 3 *For any lattice* Λ, $\det(\Lambda^*) = 1/\det(\Lambda)$.

PROOF: For full-rank lattices,

$$\det(\Lambda^*) = \left|\det((B^T)^{-1})\right| = \left|\frac{1}{\det(B^T)}\right| = \left|\frac{1}{\det(B)}\right| = \frac{1}{\det(\Lambda)}.$$

In general,

$$\begin{aligned}
\det(\Lambda^*) &= \sqrt{\det(D^T D)} \\
&= \sqrt{\det(((B^T B)^{-1})^T B^T \cdot B(B^T B)^{-1})} \\
&= \sqrt{(\det(B^T B)^{-1})} \\
&= \frac{1}{\sqrt{\det(B^T B)}} = \frac{1}{\det(\Lambda)}.
\end{aligned}$$

$\Box$

The following two claims give some relations between properties of a lattice and that of its dual. Such properties are known as transference theorem. In a few lectures, we will see a considertable strengthening of Claim 4 by Banaszczyk (showing that $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \le n$).

CLAIM 4 *For any rank* n *lattice* Λ, $\lambda_1(\Lambda) \cdot \lambda_1(\Lambda^*) \le n$.

PROOF: By Minkowski's bound,

$$\lambda_1(\Lambda) \le \sqrt{n} \cdot (\det(\Lambda))^{\frac{1}{n}}$$

and

$$\lambda_1(\Lambda^*) \le \sqrt{n} \cdot (\det(\Lambda^*))^{\frac{1}{n}} = \frac{\sqrt{n}}{(\det(\Lambda))^{\frac{1}{n}}}.$$

$\Box$

CLAIM 5 *For any rank n lattice Λ, $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geq 1$.*

PROOF: Let $v \in \Lambda$ be such that $\|v\| = \lambda_1(\Lambda)$. Take any set $x_1, \ldots, x_n$ of n linearly independent vectors in Λ^*. Not all of them are orthogonal to v. Hence, there exists an i such that $\langle x_i, v\rangle \neq 0$. By the definition of the dual lattice, we have $\langle x_i, v\rangle \in \mathbb{Z}$ and hence $\|x_i\| \geq \frac{1}{\|v\|}$. $\Box$

For a basis $b_1, \ldots, b_n$, let π_i denote the projection on the space $\mathrm{span}(b_1, \ldots, b_{i-1})^\perp$. In particular, $\pi_1(b_1), \ldots, \pi_n(b_n)$ is the Gram-Schmidt orthogonalization of $b_1, \ldots, b_n$.

CLAIM 6 *Let B, D be dual bases. Then, for all i, $B' = (\pi_i(b_i), \ldots, \pi_i(b_n))$ and $D' = (d_i, \ldots, d_n)$ are also dual bases.*

PROOF: First, notice that $\mathrm{span}(B') = \mathrm{span}(b_1, \ldots, b_{i-1})^\perp$. Moreover, since $d_i, \ldots, d_n$ are orthogonal to $b_1, \ldots, b_{i-1}$ and linearly independent, $\mathrm{span}(D') = \mathrm{span}(b_1, \ldots, b_{i-1})^\perp$. Hence, $\mathrm{span}(B') = \mathrm{span}(D')$. Finally, we have that for any $j, k \geq i$,

$$\langle d_j, \pi_i(b_k)\rangle = \langle d_j, b_k\rangle = \delta_{jk}$$

where the first equality holds since $d_j \in \mathrm{span}(b_1, \ldots, b_{i-1})^\perp$. $\Box$

CLAIM 7 *Let $b_1, \ldots, b_n$ be some basis and let $\tilde{b_1}, \ldots, \tilde{b_n}$ be its Gram-Schmidt orthogonalization. Let $d_n, \ldots, d_1$ be the dual basis of $b_1, \ldots, b_n$ in reverse order and let $\tilde{d_n}, \ldots, \tilde{d_1}$ be its Gram-Schmidt orthogonalization (using this order). Then for all i,*

$$\tilde{d_i} = \frac{\tilde{b_i}}{\|\tilde{b_i}\|^2}.$$

PROOF: The proof is by induction on n. Assume the claim holds for lattices of rank $n-1$ and let us prove it for lattices of rank n. First, notice that $\tilde{b_1} = b_1$ and $\tilde{d_1}$ is the projection of d_1 on $\mathrm{span}(d_2, \ldots, d_n)^\perp = \mathrm{span}(b_1)$. Hence, $\tilde{d_1} \in \mathrm{span}(b_1)$ and $\langle \tilde{d_1}, b_1\rangle = \langle d_1, b_1\rangle = 1$. This implies that

$$\tilde{d_1} = \frac{b_1}{\|b_1\|^2} = \frac{\tilde{b_1}}{\|\tilde{b_1}\|^2}.$$

We can now complete the proof by applying the inductive hypothesis to the bases $(\pi_2(b_2), \ldots, \pi_2(b_n))$ and $d_2, \ldots, d_n$. Indeed, Claim 6 says that these are dual bases, and moreover, the Gram-Schmidt orthogonalization of the former is $\tilde{b_2}, \ldots, \tilde{b_n}$. $\Box$

1 Korkine-Zolotarev bases

In this section we define the notion of a Korkine-Zolotarev (KZ) basis. This gives one way to formalize the idea of a 'shortest possible' basis.

DEFINITION 3 *For a rank n lattice Λ, we define its Korkine-Zolotarev (KZ) basis $b_1, \ldots, b_n$ recursively as follows. We let b_1 be the shortest vector in Λ. We then let Λ' be the lattice given by the projection of Λ on the subspace of $\mathrm{span}(\Lambda)$ orthogonal to b_1. Let $c_2, \ldots, c_n$ be the KZ basis of Λ'. Define $b_i = c_i + \alpha_i b_1$ where $\alpha_i \in (-\frac{1}{2}, \frac{1}{2}]$ is the unique number such that $b_i \in \Lambda$.*

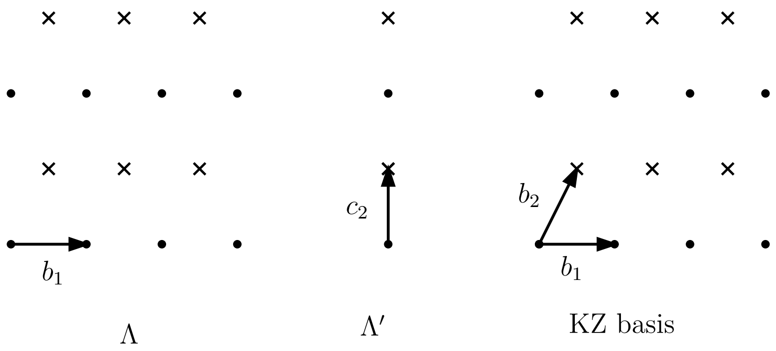

Figure 2: A lattice and its KZ basis

It is not too difficult to verify that Λ' is indeed a lattice. Moreover, b_1 is a primitive vector[1] in Λ (since it is a shortest vector) and hence the vectors $b_1, \ldots, b_n$ defined above indeed form a basis of Λ. The definition is illustrated in Figure 2.

As a first application of Korkine-Zolotarev bases, we prove the following lemma by Lagarias, Lenstra, and Schnorr. Recall that for any basis $b_1, \ldots, b_n$, we have that $\min(\|\tilde{b_1}\|, \ldots, \|\tilde{b_n}\|) \leq \lambda_1(\Lambda)$. The lemma says that any lattice has a basis where this lower bound is not far from being tight.

LEMMA 8 ([2]) *For any lattice Λ, there exists a basis $b_1, \ldots, b_n$ such that*

$$\min(\|\tilde{b_1}\|, \ldots, \|\tilde{b_n}\|) \geq \frac{1}{n} \cdot \lambda_1(\Lambda)$$

PROOF: Let $d_1, \ldots, d_n$ be a KZ basis of Λ^* and let $b_n, \ldots, b_1$ be its dual basis in reverse order. We claim that $b_n, \ldots, b_1$ satisfies the lemma. By Claim 7, we know that $\tilde{b_i} = \frac{\tilde{d_i}}{\|\tilde{d_i}\|^2}$. Hence, its enough to show that $\max(\|\tilde{d_1}\|, \ldots, \|\tilde{d_n}\|) \leq \frac{n}{\lambda_1(\Lambda)}$. First, $\tilde{d_1}$ is the shortest vector in Λ^*. By Claim 4, we have $\|\tilde{d_1}\| \leq \frac{n}{\lambda_1(\Lambda)}$. Next, $\tilde{d_2} = \pi_2(d_2)$ is the shortest vector in $\mathcal{L}(\pi_2(d_2), \ldots, \pi_2(d_n))$. By Claim 6, the dual of this lattice is $\mathcal{L}(b_2, \ldots, b_n)$. But $\lambda_1(\mathcal{L}(b_2, \ldots, b_n)) \geq \lambda_1(\Lambda)$ (since $\mathcal{L}(b_2, \ldots, b_n)$ is a sublattice of Λ) and hence

$$\|\tilde{d_2}\| \leq \frac{n-1}{\lambda_1(\mathcal{L}(b_1, \ldots, b_n))} \leq \frac{n}{\lambda_1(\Lambda)}.$$

We continue similarly for all i. $\square$

COROLLARY 9 $\mathsf{GapSVP}_n \in$ **coNP**

PROOF: Recall that an instance of GapSVP_n is given by (B, d); it is a YES instance if $\lambda_1(\mathcal{L}(B)) \leq d$ and a NO instance if $\lambda_1(\mathcal{L}(B)) > n \cdot d$. The verifier expects a witness of the form $v_1, \ldots, v_n$. It accepts if and only if $v_1, \ldots, v_n$ form a basis of $\mathcal{L}(B)$ (recall that this can be verified efficiently) and $\min(\|\tilde{v_1}\|, \ldots, \|\tilde{v_n}\|) > d$. If $\lambda_1(\mathcal{L}(B)) > n \cdot d$ then such a basis exists by Lemma 8. If $\lambda_1(\mathcal{L}(B)) \leq d$ then no such basis exists since $\min(\|\tilde{v_1}\|, \ldots, \|\tilde{v_n}\|) \leq \lambda_1(\mathcal{L}(B)) \leq d$ for any basis. $\square$

Using similar techniques, it can be shown that $\mathsf{GapCVP}_{n^{1.5}} \in$ **coNP**. We mention that it is by now known that in fact $\mathsf{GapCVP}_{\sqrt{n}}$ and $\mathsf{GapSVP}_{\sqrt{n}}$ are both in **coNP** [1].

We complete this lecture with the following somewhat surprising result by Lenstra and Schnorr. Recall that Minkowski's bound says that for any lattice Λ, $\lambda_1(\Lambda) \leq \sqrt{n}(\det(\Lambda))^{\frac{1}{n}}$. However, it is easy to see that in many cases Minkowski's bound is far from being tight. Nevertheless, the following lemma implies that being able to find vectors of length at most $\sqrt{n}(\det(\Lambda))^{\frac{1}{n}}$ is enough to imply an n-approximation to SVP.

[1] Recall that a primitive vector is a vector $v \in \Lambda$ such that there is no $k \geq 2$ for which $v/k \in \Lambda$

LEMMA 10 *Assume there exists an algorithm A that given a basis B, finds a non-zero vector $v \in \mathcal{L}(B)$ such that*

$$\|v\| \le f(n) \cdot (\det(\mathcal{L}(B)))^{\frac{1}{n}}$$

for some non-decreasing function $f(n)$. Then, we can approximate SVP *to within $(f(n))^2$.*

PROOF: By applying A to $\mathcal{L}(B)$ and $\mathcal{L}(B)^*$ we obtain $u \in \mathcal{L}(B)$, $v \in \mathcal{L}(B)^*$ such that $\|u\| \le f(n) \cdot (\det(\mathcal{L}(B)))^{\frac{1}{n}}$, $\|v\| \le f(n) \cdot (\det(\mathcal{L}(B)))^{-\frac{1}{n}}$. In particular, $\|u\| \cdot \|v\| \le (f(n))^2$. So the result follows from the following lemma. □

LEMMA 11 *Assume there exists an algorithm A that given a basis B, finds non-zero vectors $u \in \mathcal{L}(B)$, $v \in \mathcal{L}(B)^*$ such that $\|u\| \cdot \|v\| \le g(n)$ for some non-decreasing function $g(n)$. Then, we can approximate* SVP *to within $g(n)$.*

PROOF: First, we describe a recursive procedure that given a lattice, outputs a set of vectors $u_1, \ldots, u_n$ in Λ and a basis $v_1, \ldots, v_n$ of Λ^*. The procedure is recursive. First, apply A to obtain a pair u_1, v_1. Without loss of generality, we can assume that v_1 is primitive (indeed, write $v_1 = \sum a_i b_i$ and replace it by $v_1 / \gcd(a_1, \ldots, a_n)$). Let Λ' be the projection of Λ^* on the subspace of $\operatorname{span}(\Lambda^*)$ orthogonal to v_1. Then, apply the procedure recursively to Λ' and let $u_2, \ldots, u_n$, $v'_2, \ldots, v'_n$ be the result. Define $v_i = v'_i + \alpha_i v_1$ for the unique $\alpha_i \in (-\frac{1}{2}, \frac{1}{2}]$ for which $v_i \in \Lambda^*$. This completes the description of the procedure.

It can be checked that the output of the procedure satisfies that $v_1, \ldots, v_n$ is a basis of Λ^* and that for all i, $\|u_i\| \cdot \|\tilde{v_i}\| \le g(n-i+1) \le g(n)$. Let $b_n, \ldots, b_1$ be the reversed dual basis of $v_1, \ldots, v_n$. Then,

$$\min \|\tilde{b_i}\| = \min \frac{1}{\|\tilde{v_i}\|} \ge \frac{1}{g(n)} \min \|u_i\|.$$

Hence,

$$\min \|u_i\| \le g(n) \cdot \min \|\tilde{b_i}\| \le g(n) \cdot \lambda_1(\Lambda)$$

where we used that $b_n, \ldots, b_1$ is a basis of Λ. Therefore, by outputting the shortest vector among $u_1, \ldots, u_n$ we obtain a $g(n)$ approximation to SVP. □

References

[1] D. Aharonov and O. Regev. Lattice problems in NP intersect coNP. In *Proc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 362–371, 2004.

[2] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.