In the last two lectures we have seen the concept of a dual lattice and Fourier analysis on lattices. In this lecture we will prove an interesting theorem about the connection between a lattice and its dual. In the process, we will develop tools that will prove valuable in the next lecture.

In 1993, Banaszczyk proved the following theorem:

THEOREM 1 (BANASZCZYK '93 [2]) *For any rank-n lattice Λ it holds that*

$$1 \leq \lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \leq n.$$

The lower bound $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geq 1$ follows from the definition of a dual lattice and was already proven in a previous lecture. Hence, in this lecture we concentrate on the upper bound.

REMARK 1

- Recall that from Minkowski's bound we can obtain that $\lambda_1(\Lambda) \cdot \lambda_1(\Lambda^*) \leq n$. Theorem 1 is a considerable strengthening of this bound.
- Considerably weaker bounds were known prior to the work of Banaszczyk. This includes an upper bound of $(n!)^2$ given by Mahler in 1939 [5], an upper bound of $n!$ given by Cassels in 1959 [3], and an upper bound of n^2 given by Lagarias, Lenstra and Schnorr in 1990 [4].
- The upper bound given in Theorem 1 is tight up to a constant. This follows immediately from the fact that there exist self-dual lattices (i.e., lattices that are equal to their own dual) that satisfy $\lambda_1(\Lambda) = \Theta(\sqrt{n})$. Indeed, for such a lattice

  $$\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geq \lambda_1(\Lambda) \cdot \lambda_1(\Lambda^*) = \Omega(n).$$

  The fact that such lattices exist is not trivial and was shown by Conway and Thompson.
- In [2], Banaszczyk proves some other transference theorems, such as the bound $1 \leq \lambda_i(\Lambda) \cdot \lambda_{n-i+1}(\Lambda^*) \leq n$ that holds for any $1 \leq i \leq n$. He also notes that by following the same proofs, one can improve the upper bound to roughly $n/(2\pi)$.

One application of Theorem 1 is the following.

COROLLARY 1 $\mathsf{GapSVP}_n \in$ **coNP**

PROOF: Recall that the input to GapSVP_n consists of a lattice Λ and a number d. It is a YES instance if $\lambda_1(\Lambda) \leq d$ and a NO instance if $\lambda_1(\Lambda) > nd$. In order to show containment in **coNP**, we need to show a verifier such that when $\lambda_1(\Lambda) > nd$ there exists a witness that makes the verifier accept, and when $\lambda_1(\Lambda) \leq d$ no witness makes the verifier accept.

Our verifier expects as a witness a set of n vectors. It checks that the given vectors are contained in Λ^*, that they are linearly independent, and that they are all of length less than $1/d$. If all three conditions hold then it accepts, otherwise it rejects. It is easy to see that this can be done in polynomial time.

It remains to prove that such a witness exists in the case of a NO instance, and does not exist in the case of a YES instance. So first consider the case $\lambda_1(\Lambda) > nd$. By Theorem 1, $\lambda_n(\Lambda^*) < 1/d$, so there are indeed n such vectors. Now assume that $\lambda_1(\Lambda) \leq d$. By Theorem 1, $\lambda_n(\Lambda^*) \geq 1/d$, so there are no n such vectors. $\square$

Using a different transference theorem [2], one can also prove $\mathsf{GapCVP}_n \in$ **coNP**. Let us mention that both these results have since been improved, and it is now known that $\mathsf{GapSVP}_{\sqrt{n}}$ and $\mathsf{GapCVP}_{\sqrt{n}}$ are in **coNP** [1]. Interestingly, the proof of these containments, while not directly based on transference theorems, uses techniques similar to those applied in the proof of Theorem 1.

1 The Covering Radius

DEFINITION 2 *For a full-rank lattice Λ, define the covering radius of Λ as*

$$\mu(\Lambda) = \max_{x \in \mathbb{R}^n} \operatorname{dist}(x, \Lambda).$$

In other words, the covering radius of a lattice is the minimal r such that any point in space is within distance at most r from the lattice.

EXAMPLE 1 $\mu(\mathbb{Z}^n) = \frac{\sqrt{n}}{2}$, and this is realized by the point $(\frac{1}{2}, \ldots, \frac{1}{2})$.

CLAIM 3 $\mu(\Lambda) \geq \frac{1}{2}\lambda_n(\Lambda)$

PROOF: By the definition of λ_n, all lattice points inside the open ball $\mathcal{B}(0, \lambda_n)$ are contained in some $(n-1)$-dimensional hyperplane. Now take a point x of distance $\frac{\lambda_n}{2}$ from the origin perpendicular to this hyperplane. Then, as illustrated in Fig. 1, x must be at distance at least $\frac{\lambda_n}{2}$ from any lattice point inside the ball, as well as from any lattice point outside the ball. We thus obtain $\mu \geq \frac{\lambda_n}{2}$, as required.

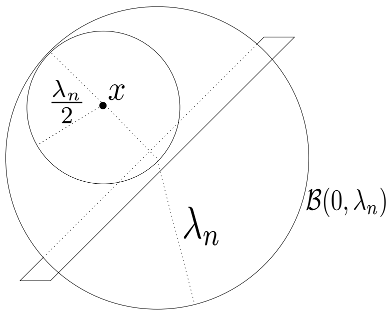

Figure 1: $\mu(\Lambda) \geq \frac{1}{2}\lambda_n(\Lambda)$

$\square$

Hence, to prove Theorem 1 it suffices to show $\lambda_1(\Lambda) \cdot \mu(\Lambda^*) \leq \frac{n}{2}$. In this lecture we prove something slightly weaker:

THEOREM 4 $\lambda_1(\Lambda) \cdot \mu(\Lambda^*) \leq n$.

2 Proof of Theorem 4

First, let us recall some of the things we saw in the previous lecture. For any $s > 0$ we define $\rho_s(x) = e^{-\pi\|x/s\|^2}$ and for the special case $s = 1$ we denote $\rho \equiv \rho_1$. As we saw in the previous class, the Fourier transform of ρ_s is given by $\widehat{\rho_s}(x) = s^n \rho_{1/s}(x)$. Moreover, by a property of the Fourier transform, the Fourier transform of the function mapping x to $\rho_s(x+u)$ is $s^n \rho_{1/s}(x) \cdot e^{2\pi i \langle u, x\rangle}$. Hence, from the Poisson summation formula we get

$$\rho_s(\Lambda) = \det(\Lambda^*) \cdot s^n \cdot \rho_{1/s}(\Lambda^*) \tag{1}$$

$$\rho_s(\Lambda + u) = \det(\Lambda^*) \cdot s^n \cdot \sum_{y \in \Lambda^*} \rho_{1/s}(y) \cdot e^{2\pi i \langle y, u\rangle}. \tag{2}$$

We next prove several useful lemmas. Our first lemma shows that ρ_s of a shifted lattice is upper bounded by ρ_s of the lattice itself.

LEMMA 5 *For any $s > 0$ and any $u \in \mathbb{R}^n$ it holds that*

$$\rho_s(\Lambda + u) \leq \rho_s(\Lambda).$$

As an example, consider the one-dimensional lattice $\Lambda = k\mathbb{Z}$ for some $k > 0$ and define

$$f_k(u) = \sum_{x \in k\mathbb{Z}} e^{-\pi(x+u)^2}.$$

Using the lemma with $s = 1$ we obtain that f_k is maximized when $u = 0$. See Figure 2 for some illustrations.

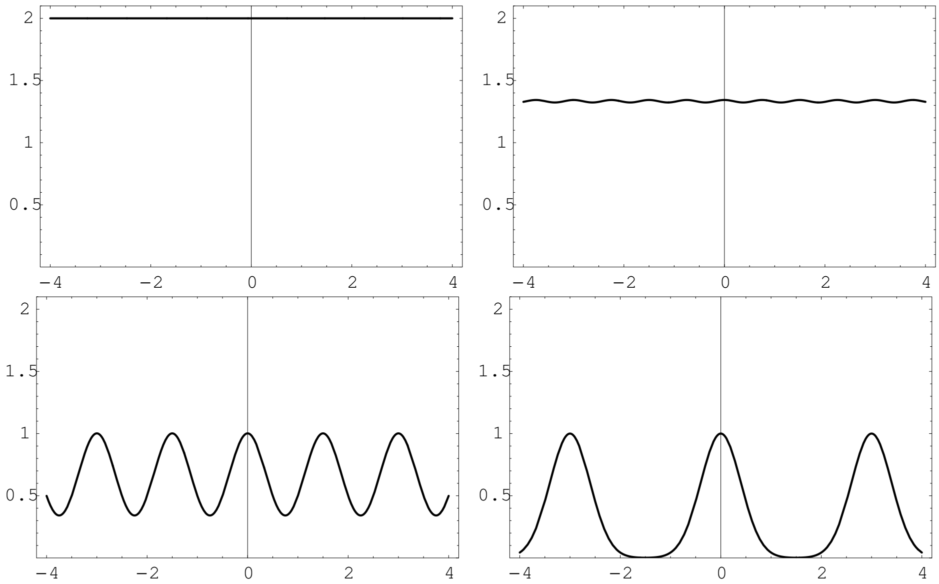

Figure 2: $f_k(u)$ for $k = 0.5$ (top left), 0.75 (top right), 1.5 (bottom left), and 3 (bottom right)

PROOF: Using Eq. (2) and Eq. (1),

$$\begin{aligned}
\rho_s(\Lambda + u) &= \det(\Lambda^*) \cdot s^n \cdot \sum_{y \in \Lambda^*} \rho_{1/s}(y) \cdot e^{2\pi i \langle y, u \rangle} \\
&\leq \det(\Lambda^*) \cdot s^n \cdot \sum_{y \in \Lambda^*} \rho_{1/s}(y) \\
&= \det(\Lambda^*) \cdot s^n \cdot \rho_{1/s}(\Lambda^*) \\
&= \rho_s(\Lambda)
\end{aligned}$$

where the inequality follows from the triangle inequality together with the fact that $\rho_{1/s}$ is a positive function. $\square$

Our second lemma upper bounds ρ_s (for $s \geq 1$) by ρ_1 times a multiplicative factor.

LEMMA 6 *For any $s \geq 1$ and any $u \in \mathbb{R}^n$ it holds that*

$$\rho_s(\Lambda + u) \leq s^n \rho(\Lambda)$$

Before we present the proof, let us see two examples. Consider the lemma for the case $u = 0$ and take Λ to be a very sparse lattice, say, $M \cdot \mathbb{Z}^n$ for some large M. Then it can be seen that $\rho(\Lambda) \approx 1$ and also

$\rho_s(\Lambda) \approx 1$, since both sums are dominated by $0 \in \Lambda$. In this case the inequality holds, but is far from being tight. Next, let us take Λ to be a very dense lattice, say $\varepsilon \cdot \mathbb{Z}^n$ for some small $\varepsilon > 0$. Then

$$\rho(\Lambda) \approx \frac{1}{\varepsilon^n} \int_{\mathbb{R}^n} \rho(x)dx = \frac{1}{\varepsilon^n}$$

while

$$\rho_s(\Lambda) \approx \frac{1}{\varepsilon^n} \int_{\mathbb{R}^n} \rho_s(x)dx = \frac{s^n}{\varepsilon^n}.$$

Hence, in this case the lemma is close to being tight.
PROOF: By Lemma 5 we know that $\rho_s(\Lambda + u) \leq \rho_s(\Lambda)$, so it is enough to prove that $\rho_s(\Lambda) \leq s^n \rho(\Lambda)$. Using Eq. (1) we can write

$$\rho_s(\Lambda) = \det(\Lambda^*) \cdot s^n \cdot \rho_{1/s}(\Lambda^*) = \det(\Lambda^*) \cdot s^n \cdot \sum_{y \in \Lambda^*} \rho_{1/s}(y).$$

It is easy to see that for any $s \geq 1$ and any y it holds that $\rho_{1/s}(y) \leq \rho(y)$ and so we get

$$\rho_s(\Lambda) \leq \det(\Lambda^*) \cdot s^n \cdot \sum_{y \in \Lambda^*} \rho(y) = s^n \rho(\Lambda)$$

where we have used (1) again. $\Box$

Our third lemma states that for any lattice Λ, almost all the contribution to $\rho(\Lambda)$ comes from a ball of radius $\sqrt{n}$ around the origin.

LEMMA 7 *For any $u \in \mathbb{R}^n$ it holds that*

$$\rho\big((\Lambda + u) \setminus \mathcal{B}(0, \sqrt{n})\big) \leq 2^{-n} \rho(\Lambda).$$

As before, let us consider two examples. First, consider the case that $u = 0$ and $\Lambda = M\mathbb{Z}^n$ for some very large M. In this case, the left hand side is essentially 0 while $\rho(\Lambda)$ is essentially 1 so the lemma holds. A more interesting example is when Λ is a dense lattice, say, $\varepsilon\mathbb{Z}^n$ for some small $\varepsilon > 0$. Then,

$$\rho(\Lambda) \approx \varepsilon^{-n} \int_{\mathbb{R}^n} e^{-\pi\|x\|^2} dx = \varepsilon^{-n}$$

while

$$\rho(\Lambda \setminus \mathcal{B}(0, \sqrt{n})) \approx \varepsilon^{-n} \int_{\mathbb{R}^n \setminus \mathcal{B}(0,\sqrt{n})} e^{-\pi\|x\|^2} dx.$$

In this case, the lemma tells us that the latter integral is at most 2^{-n}. Let us verify this by computing the integral. Instead of computing it directly (which is not too difficult), we compute it by using a nice trick, which will later be used in the proof of Lemma 7. The idea is to consider the integral $\int_{\mathbb{R}^n} e^{-\pi\|x/2\|^2} dx$. On one hand, by a change of variable, we see that

$$\int_{\mathbb{R}^n} e^{-\pi\|x/2\|^2} dx = 2^n.$$

On the other hand,

$$\begin{aligned}\int_{\mathbb{R}^n} e^{-\pi\|x/2\|^2} dx &\geq \int_{\mathbb{R}^n \setminus \mathcal{B}(0,\sqrt{n})} e^{-\pi\|x/2\|^2} dx \\ &= \int_{\mathbb{R}^n \setminus \mathcal{B}(0,\sqrt{n})} e^{\frac{3}{4}\pi\|x\|^2} \cdot e^{-\pi\|x\|^2} dx \\ &\geq e^{\frac{3}{4}\pi n} \cdot \int_{\mathbb{R}^n \setminus \mathcal{B}(0,\sqrt{n})} e^{-\pi\|x\|^2} dx.\end{aligned}$$

We obtain the required bound by combining the two inequalities and using $e^{\frac{3}{4}\pi} > 4$.
PROOF: The proof idea is similar to that used in bounding the integral above. Namely, we notice that lattice points that are far from the origin contribute to $\rho_2(\Lambda)$ much more than they contribute to $\rho_1(\Lambda)$. But by Lemma 6, $\rho_2(\Lambda)$ can only be larger than $\rho_1(\Lambda)$ by 2^n and so we obtain a bound on the number of such points. More specifically, we consider the expression $\rho_2(\Lambda + u)$. On one hand, using Lemma 6, we see that

$$\rho_2(\Lambda + u) \leq 2^n \rho(\Lambda).$$

On the other hand,

$$\begin{aligned}\rho_2(\Lambda + u) \geq \rho_2\big((\Lambda + u) \setminus \mathcal{B}(0, \sqrt{n})\big) &= \sum_{y \in \Lambda + u \text{ s.t. } \|y\| \geq \sqrt{n}} e^{-\pi\|y/2\|^2} \\ &= \sum_{y \in \Lambda + u \text{ s.t. } \|y\| \geq \sqrt{n}} e^{\frac{3}{4}\pi\|y\|^2} \cdot e^{-\pi\|y\|^2} \\ &\geq e^{\frac{3}{4}\pi n} \cdot \sum_{y \in \Lambda + u \text{ s.t. } \|y\| \geq \sqrt{n}} e^{-\pi\|y\|^2} \\ &= e^{\frac{3}{4}\pi n} \cdot \rho\big((\Lambda + u) \setminus \mathcal{B}(0, \sqrt{n})\big).\end{aligned}$$

We complete the proof by noting that $e^{\frac{3}{4}\pi} > 4$. □

One useful corollary of Lemma 7 is the following.

COROLLARY 8 *Let Λ be a lattice satisfying $\lambda_1(\Lambda) > \sqrt{n}$. Then,*

$$\rho(\Lambda \setminus \{0\}) \leq 2^{-n}/(1 - 2^{-n}) \leq 2 \cdot 2^{-n}.$$

PROOF: By applying Lemma 7 with $u = 0$ we obtain

$$\rho\big(\Lambda \setminus \mathcal{B}(0, \sqrt{n})\big) \leq 2^{-n} \rho(\Lambda).$$

By our assumption, $\Lambda \setminus \mathcal{B}(0, \sqrt{n}) = \Lambda \setminus \{0\}$ so we obtain

$$\rho(\Lambda \setminus \{0\}) \leq 2^{-n} \rho(\Lambda) = 2^{-n}\big(1 + \rho(\Lambda \setminus \{0\})\big).$$

The corollary follows by rearranging terms. □

Our last lemma says that if $\lambda_1(\Lambda) > \sqrt{n}$, then $\rho(\Lambda^* + u)$ is nearly constant as a function of u. Intuitively, this happens because Λ^* is dense and so $\rho(\Lambda^* + u)$ is not affected much by the shift u. A similar behavior can be seen in Figure 2 where $f_{0.5}$ is essentially constant.

LEMMA 9 *Let Λ be a lattice satisfying $\lambda_1(\Lambda) > \sqrt{n}$. Then, for any $u \in \mathbb{R}^n$,*

$$\rho(\Lambda^* + u) \in (1 \pm 2^{-\Omega(n)}) \det(\Lambda).$$

PROOF: Using the Poisson summation formula (Eq. (2)) we can write

$$\rho(\Lambda^* + u) = \det(\Lambda) \cdot \sum_{y \in \Lambda} \rho(y) \cdot e^{2\pi i \langle y,u \rangle}.$$

In the sum here, the point $y = 0$ contributes 1, and the contribution of all other points is at most $\rho(\Lambda \setminus \{0\})$ in absolute value. So we obtain that

$$\rho(\Lambda^* + u) \in \big(1 \pm \rho(\Lambda \setminus \{0\})\big) \det(\Lambda).$$

But by Corollary 8, $\rho(\Lambda \setminus \{0\}) \leq 2^{-\Omega(n)}$ so we are done. □

We finally present the proof of Theorem 4.

PROOF:(of Theorem 4) Assume by contradiction that there exists a lattice Λ for which $\lambda_1(\Lambda) \cdot \mu(\Lambda^*) > n$. By scaling Λ, we can assume without loss of generality that both $\lambda_1(\Lambda) > \sqrt{n}$ and $\mu(\Lambda^*) > \sqrt{n}$.

On one hand, Lemma 9, together with the bound on $\lambda_1(\Lambda)$, implies that $\rho(\Lambda^* + u)$ is essentially constant as a function of u. On the other hand, $\mu(\Lambda^*) > \sqrt{n}$ implies that there exists a point $v \in \mathbb{R}^n$ for which $\mathrm{dist}(v, \Lambda^*) > \sqrt{n}$. This is the same as saying that all points in $\Lambda^* - v$ are at distance more than $\sqrt{n}$ from the origin. Using Lemma 7,

$$\rho(\Lambda^* - v) = \rho\big((\Lambda^* - v) \setminus \mathcal{B}(0, \sqrt{n})\big) < 2^{-n} \rho(\Lambda^*).$$

But this contradicts the fact that $\rho(\Lambda^* + u)$ is almost constant as a function of u. □

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] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993.

[3] J. Cassels. *An Introduction to the Geometry of Numbers*. Springer, Berlin, Gttingen Heidelberg, 1959.

[4] 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.

[5] K. Mahler. Ein Übertragungsprinzip für konvexe Körper. *Časopis Pěst. Mat. Fys.*, 68:93–102, 1939.