End of Transference, Complexity of Lattice Problems

In this lecture, we conclude the section on transference with a final transference theorem and a one-dimensional tail bound for the discrete Gaussian. After that, we discuss the complexity of lattice problems.

LEMMA 1 *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\lambda_{n-i+1}(\mathcal{L}^*) = \sqrt{n}$ and $i \in [n]$, if linear independent vectors $\mathbf{v}_1^*, \ldots, \mathbf{v}_{n-i}^* \in \mathcal{L}^*$ achieve the successive minima ($\|\mathbf{v}_j^*\| = \lambda_j(\mathcal{L}^*)$ for all $j \in [n-i]$) and $W = \mathrm{span}(\mathbf{v}_1^*, \ldots, \mathbf{v}_{n-i}^*)^\perp$, then for all $\mathbf{t} \in W$, $d(\mathcal{L}, \mathbf{t}) \leq \sqrt{n}$.*

PROOF: We will use Corollary 13 from Lecture 7, which states that, for a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\mathbf{t} \in \mathbb{R}^n$, we have $\Pr_{\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t}}}[\|\mathbf{X}\| \geq \sqrt{n}] \leq \frac{\rho(\mathcal{L})}{\rho(\mathcal{L}+\mathbf{t})} 4^{-n}$ and $\rho((\mathcal{L}+\mathbf{t}) \setminus \sqrt{n}\mathcal{B}_2^{n,\circ}) \leq 4^{-n}\rho(\mathcal{L})$.

The tail bound implies that, if we can show $\rho(\mathcal{L}) \leq 2\rho(\mathcal{L}+\mathbf{t})$, then $\Pr_{\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t}}}[\|\mathbf{X}\| \geq \sqrt{n}] < 1$. If so, then by the probabilistic method, there must exist some $\mathbf{x} \in \mathcal{L}+\mathbf{t}$ such that $\|\mathbf{x}\| \leq \sqrt{n}$, so $\mathbf{x} - \mathbf{t}$ is a lattice vector at distance at most $\sqrt{n}$ from the target $\mathbf{t} \in W$.

By the Poisson summation formula, we have

$$\begin{aligned}\rho(\mathcal{L}+\mathbf{t}) &= \frac{1}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} \\ &= \frac{1}{\det(\mathcal{L})} \left(\sum_{\mathbf{y} \in \mathcal{L}^* \cap W^\perp} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} + \sum_{\mathbf{y} \in \mathcal{L}^* \setminus W^\perp} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} \right).\end{aligned}$$

As $\mathbf{t} \in W$, we know for $\mathbf{y} \in W^\perp$ that $e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} = 1$, hence $\sum_{\mathbf{y} \in \mathcal{L}^* \cap W^\perp} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} = \rho(\mathcal{L}^* \cap W^\perp)$. For $\mathbf{y} \in \mathcal{L}^* \setminus W^\perp$ we use the pessimistic bound $e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} \geq -1$ and get $\sum_{\mathbf{y} \in \mathcal{L}^* \setminus W^\perp} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} \geq -\rho(\mathcal{L}^* \setminus W^\perp)$. Hence we get

$$\begin{aligned}\rho(\mathcal{L}+\mathbf{t}) &= \frac{1}{\det(\mathcal{L})} \left(\sum_{\mathbf{y} \in \mathcal{L}^* \cap W^\perp} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} + \sum_{\mathbf{y} \in \mathcal{L}^* \setminus W^\perp} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} e^{-\pi \|\mathbf{y}\|^2} \right) \\ &\geq \frac{1}{\det(\mathcal{L})} (\rho(\mathcal{L}^* \cap W^\perp) - \rho(\mathcal{L}^* \setminus W^\perp)) \\ &= \frac{1}{\det(\mathcal{L})} (\rho(\mathcal{L}^*) - 2\rho(\mathcal{L}^* \setminus W^\perp))\end{aligned}$$

We assumed that $\lambda_{n-i+1}(\mathcal{L}^*) = \sqrt{n}$, so we have the inclusion $\mathcal{L}^* \setminus W^\perp \subset \mathcal{L}^* \setminus \sqrt{n}\mathcal{B}_2^{n,\circ}$. This inclusion tells us that $\rho(\mathcal{L}^* \setminus W^\perp) \leq \rho(\mathcal{L}^* \setminus \sqrt{n}\mathcal{B}_2^{n,\circ})$. Combining with $\rho(\mathcal{L} \setminus \sqrt{n}\mathcal{B}_2^{n,\circ}) \leq 4^{-n}\rho(\mathcal{L})$ gets us

$$\begin{aligned}\rho(\mathcal{L}+\mathbf{t}) &\geq \frac{1}{\det(\mathcal{L})} (\rho(\mathcal{L}^*) - 2\rho(\mathcal{L}^* \setminus \sqrt{n}\mathcal{B}_2^{n,\circ})) \\ &\geq \frac{1}{\det(\mathcal{L})} (\rho(\mathcal{L}^*) - 2 \cdot 4^{-n}\rho(\mathcal{L}^*)) \\ &= (1 - 2 \cdot 4^{-n}) \frac{\rho(\mathcal{L}^*)}{\det(\mathcal{L})} \\ &= (1 - 2 \cdot 4^{-n})\rho(\mathcal{L})\end{aligned}$$

as needed. □

COROLLARY 2 *For $i \in [n]$ and $\mathcal{L} \subset \mathbb{R}^n$ a full-rank lattice with $\lambda_{n-i+1}(\mathcal{L}^*) = \sqrt{n}$, there exist linearly independent $\mathbf{v}_1, \ldots, \mathbf{v}_i \in \mathcal{L}$ such that $\|\mathbf{v}_j\| \leq 2\sqrt{n}$ for all $j \in [i]$.*

PROOF: The proof is similar to Claim 3 and Theorem 4 from Lecture 6. Let linearly independent vectors $\mathbf{v}_1^*, \ldots, \mathbf{v}_{n-i}^*$ achieve the successive minima of the dual lattice $\|\mathbf{v}_j^*\| = \lambda_j(\mathcal{L}^*), j \in [n-i]$. We write $W = \text{span}(\mathbf{v}_1^*, \ldots, \mathbf{v}_{n-i}^*)^\perp$ and we will construct the vectors one by one. Let $V_0 = \{\mathbf{0}\}$. For $j = 1, \ldots, i$, pick $\mathbf{z}_j \in W$ orthogonal to the subspace V_{j-1} with norm $\|\mathbf{z}_j\| = \sqrt{n}$. As long as $j - 1 = \dim(V_{j-1}) < \dim(W) = i$, such a $\mathbf{z}_j$ is guaranteed to exist. The set $\mathbf{z}_j + \sqrt{n}\mathcal{B}_2^n$ must contain a lattice vector from $\mathcal{L} \setminus V_{j-1}$, for otherwise there would exist some $\varepsilon > 0$ such that $\mathrm{d}((1+\varepsilon)\mathbf{z}_j, \mathcal{L}) > \sqrt{n}$, which contradicts Lemma 1 above. Letting $\mathbf{v}_j \in \mathcal{L}$ be such a vector, we set $V_j = \text{span}(\mathbf{v}_1, \ldots, \mathbf{v}_j)$ and continue inductively.

The produced set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_i \in \mathcal{L}$ is linearly independent, since $\mathbf{v}_j \notin V_{j-1} = \text{span}(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1})$, $\forall j \in [i]$, by construction. Lastly, for each $j \in [i]$, by the triangle inequality $\|\mathbf{v}_j\| \leq \|\mathbf{z}_j\| + \sqrt{n} = 2\sqrt{n}$, as needed. □

THEOREM 3 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and $i \in [n]$, $\lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^*) \leq 2n$.*

PROOF: Since for $s > 0$, $\lambda_i(s\mathcal{L}) = s\lambda_i(\mathcal{L})$ and $\lambda_{n-i+1}((s\mathcal{L})^*) = \lambda_{n-i+1}(\mathcal{L}^*)/s$, the equality is independent of scaling. Without loss of generality, we can scale such that $\lambda_{n-i+1}(\mathcal{L}^*) = \sqrt{n}$. The result follows from the corollary above: $\lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^*) = \sqrt{n}\lambda_i(\mathcal{L}) \leq 2n$. □

The next lemma will set us up to prove a tail bound on $\langle \mathbf{X}, \mathbf{v} \rangle$ for fixed $\mathbf{v}$ and $\mathbf{X}$ discrete Gaussian.

LEMMA 4 *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\mathbf{v} \in \mathbb{R}^n$ with $\|\mathbf{v}\| = 1$, $\mathbb{E}_{\mathbf{X} \sim D_\mathcal{L}}[e^{\lambda\pi\langle \mathbf{v}, \mathbf{x} \rangle}] \leq e^{\pi\lambda^2/4}$.*

PROOF: The definition of $D_\mathcal{L}$ is such that

$$\mathop{\mathbb{E}}_{\mathbf{X} \sim D_\mathcal{L}}[e^{\lambda\pi\langle \mathbf{v}, \mathbf{x} \rangle}] = \frac{1}{\rho(\mathcal{L})} \sum_{\mathbf{x} \in \mathcal{L}} e^{\pi\lambda\langle \mathbf{v}, \mathbf{x} \rangle} e^{-\pi\|\mathbf{x}\|^2}.$$

If we multiply by $1 = e^{\pi\lambda^2/4} e^{-\pi\|\frac{\lambda}{2}\mathbf{v}\|^2}$, we can complete the square and find

$$\begin{aligned}
\mathop{\mathbb{E}}_{\mathbf{X} \sim D_\mathcal{L}}[e^{\lambda\pi\langle \mathbf{v}, \mathbf{x} \rangle}] &= e^{\pi\lambda^2/4} \frac{\sum_{\mathbf{x} \in \mathcal{L}} e^{-\pi\|\mathbf{x}\|^2 - \pi\|\frac{\lambda}{2}\mathbf{v}\|^2 - 2\pi\langle \mathbf{x}, \frac{\lambda}{2}\mathbf{v} \rangle}}{\rho(\mathcal{L})} \\
&= e^{\pi\lambda^2/4} \frac{\sum_{\mathbf{x} \in \mathcal{L}} e^{-\pi\|\mathbf{x} - \frac{\lambda}{2}\mathbf{v}\|^2}}{\rho(\mathcal{L})} \\
&= e^{\pi\lambda^2/4} \frac{\rho(\mathcal{L} - \frac{\lambda\mathbf{v}}{2})}{\rho(\mathcal{L})} \\
&\leq e^{\pi\lambda^2/4},
\end{aligned}$$

as needed. □

We use the above lemma to prove the following tail bound similarly to the proof of Theorem 12 from Lecture 7.

THEOREM 5 *For $\mathcal{L} \subset \mathbb{R}^n$ a full-rank lattice and any unit vector $\mathbf{v} \in \mathbb{R}^n, \|\mathbf{v}\| = 1, t > 0$, we have $\Pr_{\mathbf{X} \sim D_\mathcal{L}}[\langle \mathbf{X}, \mathbf{v} \rangle \geq t] \leq e^{-\pi t^2}$.*

PROOF: By monotonicity, Markov's inequality, and Lemma 4, we have, for any $\lambda > 0$,

$$\Pr_{\mathbf{x}\sim D_{\mathcal{L},s}}[\langle \mathbf{X}, \mathbf{v}\rangle \geq t] = \Pr_{\mathbf{x}\sim D_{\mathcal{L}}}[e^{\lambda\pi\langle \mathbf{X},\mathbf{v}\rangle} \geq e^{\lambda\pi t}] \leq \frac{\mathbb{E}[e^{\lambda\pi\langle \mathbf{X},\mathbf{v}\rangle}]}{e^{\lambda\pi t}} \leq e^{\pi\lambda^2/4-\lambda\pi t}.$$

The result follows by setting $\lambda = 2t$. □

Complexity of lattice problems

Many lattice problems are hard to calculate, or even to approximate. We prove NP-hardness of CVP and the fact that CVP is at least as hard as SVP, after which we discuss hardness of approximation.

THEOREM 6 *CVP is NP-hard.*

PROOF: We reduce solving $\mathbf{Ax} = \mathbf{b}, \mathbf{x} \in \{0,1\}^n$, where $\mathbf{A} \in \mathbb{Z}^{m\times n}, \mathbf{b} \in \mathbb{Z}^m$, to solving CVP: if you can solve CVP, you can solve systems $\mathbf{Ax} = \mathbf{b}, \mathbf{x} \in \{0,1\}^n$, which is at as hard as the NP-hard Subset Sum problem (given a finite set $S \subset \mathbb{Z}$ of integers, find a non-empty $T \subseteq S$ such that $\sum_{x\in T} x = 0$ or declare no such subset exists).

Given $\mathbf{A} \in \mathbb{Z}^{m\times n}, \mathbf{b} \in \mathbb{Z}^m, 0 \leq k \leq n$, we claim we can solve $\mathbf{Ax} = \mathbf{b}, \mathbb{1}^\mathsf{T}\mathbf{x} = k, \mathbf{x} \in \{0,1\}^n$ using a CVP oracle. Because for any solution to $\mathbf{Ax} = \mathbf{b}, \mathbf{x} \in \{0,1\}^n$ we have $0 \leq \mathbb{1}^\mathsf{T}\mathbf{x} \leq n$, we can solve $\mathbf{Ax} = \mathbf{b}, \mathbf{x} \in \{0,1\}^n$ by trying every possible integer value $0 \leq k \leq n$.

Fix some $k \in \mathbb{Z}, 0 \leq k \leq n$. We construct the following basis and target:

$$\mathbf{B}_k = \begin{pmatrix} 2n\mathbf{A} \\ 2n\mathbb{1}_n^\mathsf{T} \\ I_n \end{pmatrix} \qquad \mathbf{t}_k = \begin{pmatrix} 2n\mathbf{b} \\ 2kn \\ 0 \end{pmatrix}.$$

We claim that, for every $\mathbf{x} \in \mathbb{Z}^n$, $\|\mathbf{B}_k\mathbf{x} - \mathbf{t}_k\| \leq \sqrt{k}$ if and only if $\mathbf{Ax} = \mathbf{b}, \mathbb{1}^\mathsf{T}\mathbf{x} = k, \mathbf{x} \in \{0,1\}^n$. Hence solving CVP on the lattice $\mathcal{L}(\mathbf{B}_k)$ with target $\mathbf{t}_k$ gives us a solution (if it exists) to $\mathbf{Ax} = \mathbf{b}, \mathbb{1}^\mathsf{T}\mathbf{x} = k, \mathbf{x} \in \{0,1\}^n$, and hence trying every $k \in \{0,1,\ldots,n\}$ solves $\mathbf{Ax} = \mathbf{b}, \mathbf{x} \in \{0,1\}^n$.

Since the if direction is trivial, we restrict to proving the only if direction. Fix k and set $\mathbf{B} = \mathbf{B}_k, \mathbf{t} = \mathbf{t}_k$. Suppose $\mathbf{x} \in \mathbb{Z}^n$ gives a closest vector $\mathbf{Bx} \in \mathcal{L}(\mathbf{B})$ to $\mathbf{t}$ satisfying

$$\|\mathbf{Bx} - \mathbf{t}\| = \left\| \begin{pmatrix} 2n(\mathbf{Ax} - \mathbf{b}) \\ 2n(\sum_{i=1}^n x_i - k) \\ \mathbf{x} \end{pmatrix} \right\| \leq \sqrt{k}.$$

If $\mathbf{Ax} - \mathbf{b} \neq \mathbf{0}$, then there must be some row $\mathbf{a}_i$ of $\mathbf{A}$ such that $\mathbf{a}_i^\mathsf{T}\mathbf{x} - b_i \neq 0$. As $\mathbf{a}_i, \mathbf{x} \in \mathbb{Z}^n$, $b_i \in \mathbb{Z}$, this would imply that $\|\mathbf{Bx} - \mathbf{t}\| \geq \sqrt{2n} > \sqrt{k}$, contradicting our assumption that $\|\mathbf{Bx} - \mathbf{t}\| \leq \sqrt{k}$. Hence $\mathbf{Ax} = \mathbf{b}$.

If $\sum_{i=1}^n x_i - k \neq 0$, then $\|\mathbf{Bx} - \mathbf{t}\| \geq \sqrt{2n}$, since $\sum_{i=1}^n x_i - k$ takes integer values. Again this contradicts our assumption, so $\mathbf{x}$ must satisfy $\sum_{i=1}^n x_i = k$.

Now, we show that $\mathbf{x} \in \{0,1\}^n$. By the above we know that $\|\mathbf{Bx} - \mathbf{t}\| = \|\mathbf{x}\|$, so $\sum_{i=1}^n x_i^2 \leq k$. Because $\mathbf{x} \in \mathbb{Z}^n$, this means we have $k \geq \sum_{i=1}^n x_i^2 \geq \sum_{i=1}^n x_i = k$. The inequalities must be tight. As $x_i^2 \geq x_i$ and all $x_i^2 \geq 0$, the inequalities must be tight component-wise, and $x_i^2 = x_i$ forces $x_i \in \{0,1\}$.

□

THEOREM 7 *α-CVP is at least as hard as α-SVP for all $\alpha \geq 1$.*

PROOF: Given $\mathcal{L} = \mathcal{L}(\mathbf{B}), \mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$, we will solve α-SVP using an α-CVP oracle. For each $i \in [n]$, write $\mathbf{B}^i = (\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, 2\mathbf{b}_i, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n)$, and use the α-CVP oracle to find a vector $\mathbf{y}_i \in \mathcal{L}(\mathbf{B}^i)$ such that $\|\mathbf{y}_i - \mathbf{b}_i\| \leq \alpha \mathrm{d}(\mathcal{L}(\mathbf{B}_i), \mathbf{b}_i)$. We return the shortest of $\mathbf{y}_1 - \mathbf{b}_1, \ldots, \mathbf{y}_n - \mathbf{b}_n$, and claim that that vector has norm at most $\alpha\lambda_1(\mathcal{L})$.

Let $\mathbf{y}_i - \mathbf{b}_i = \sum_{i=1}^n z_i \mathbf{b}_i, \mathbf{z} \in \mathbb{Z}^n$ be the returned vector. By the guarantee of the oracle, we know that $\|\mathbf{y}_i - \mathbf{b}_i\| \leq \alpha \mathrm{d}(\mathcal{L}(\mathbf{B}_i), \mathbf{b}_i)$.

Let $\mathbf{v} = \sum_{i=1}^n z_i \mathbf{b}_i, \mathbf{z} \in \mathbb{Z}^n$ be the shortest vector in $\mathcal{L}$. There exists $i \in [n]$ such that z_i is odd, for otherwise $\mathbf{v}/2 \in \mathcal{L}$ would be a shorter vector. This implies that $\mathbf{v} + \mathbf{b}_i \in \mathcal{L}(\mathbf{B}^i)$. If there were another vector $\mathbf{p} \in \mathcal{L}(\mathbf{B}^i) \subset \mathcal{L}(\mathbf{B})$ with $\|\mathbf{p} - \mathbf{b}_i\| < \|(\mathbf{v} + \mathbf{b}_i) - \mathbf{b}_i\|$, that would contradict our assumption that $\mathbf{v}$ is the shortest vector in $\mathcal{L}$, because $\mathbf{p} - \mathbf{b}_i \in \mathcal{L}$ would be shorter. From this it follows that $\mathbf{v} + \mathbf{b}_i$ is the closest vector in $\mathcal{L}(\mathbf{B}^i)$ to $\mathbf{b}_i$, hence $\mathrm{d}(\mathcal{L}(\mathbf{B}^i), \mathbf{b}_i) = \lambda_1(\mathcal{L})$.

The result follows: if $\mathrm{d}(\mathbf{y}_i, \mathbf{b}_i) \leq \alpha \mathrm{d}(\mathcal{L}(\mathbf{B}^i), \mathbf{b}_i)$ then $\|\mathbf{y}_i - \mathbf{b}_i\| \leq \alpha\lambda_1(\mathcal{L})$. □

We showed that solving CVP exactly is NP-hard. Solving SVP exactly is NP-hard as well, though we do not prove that in these notes. We might ask, how hard is it to approximately solve these problems? Let us first define the decision problems we look at, which are the decision variants of α-SVP and α-CVP that were defined in Lecture 4.

DEFINITION 8 *γ-GapSVP has input $\mathbf{B} \in \mathbb{R}^{m \times n}, r \geq 0$ and output*

- *YES when $\lambda_1(\mathcal{L}(\mathbf{B})) \leq r$,*
- *NO when $\lambda_1(\mathcal{L}(\mathbf{B})) > \gamma r$.*

DEFINITION 9 *γ-GapCVP has input $\mathbf{B} \in \mathbb{R}^{m \times n}, \mathbf{t} \in \mathbb{R}^n, r \geq 0$ and output*

- *YES when $\mathrm{d}(\mathcal{L}(\mathbf{B}), \mathbf{t}) \leq r$,*
- *NO when $\mathrm{d}(\mathcal{L}(\mathbf{B}), \mathbf{t}) > \gamma r$.*

THEOREM 10 *$2n$-GapSVP is in $\mathsf{NP} \cap \mathsf{coNP}$.*

PROOF: The problem is in NP precisely if, when the answer must be YES, we can produce a certificate (of polynomial size) that can be used to verify (in polynomial time) that YES is an allowed answer. This is easy: we can certify $\lambda_1(\mathcal{L}) \leq r$ by showing a vector $\mathbf{x} \in \mathcal{L}$ satisfying $\|\mathbf{x}\| \leq r$.

For membership of coNP, we need to be able to certify that NO is an allowed answer, whenever we are required to answer NO. We use Theorem 3: $1 \leq \lambda_1(\mathcal{L})\lambda_n(\mathcal{L}^*) \leq 2n$. If $\lambda_1(\mathcal{L}) > nr$, then $\lambda_n(\mathcal{L}^*) < 1/r$. By showing linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}^*$ with $\|\mathbf{v}_i\| < 1/r$ for all $i \in [n]$, we certify that $\lambda_n(\mathcal{L}^*) < 1/r$. Such a certificate proves that $\lambda_1(\mathcal{L}) > r$, and can be produced whenever $\lambda_1(\mathcal{L}) \geq nr$, i.e., when the correct output is NO, we can certify that we are allowed to output NO. □

In 1998, Banaszczyk proved that $O(n)$-GapCVP is in $\mathsf{NP} \cap \mathsf{coNP}$, which later got improved by Aharonov and Regev to $O(\sqrt{n})$-GapCVP being in $\mathsf{NP} \cap \mathsf{coNP}$. We give Banaszczyk's result, from which $80n$-GapCVP $\in \mathsf{NP} \cap \mathsf{coNP}$ follows the same way as in the proof of Theorem 10.

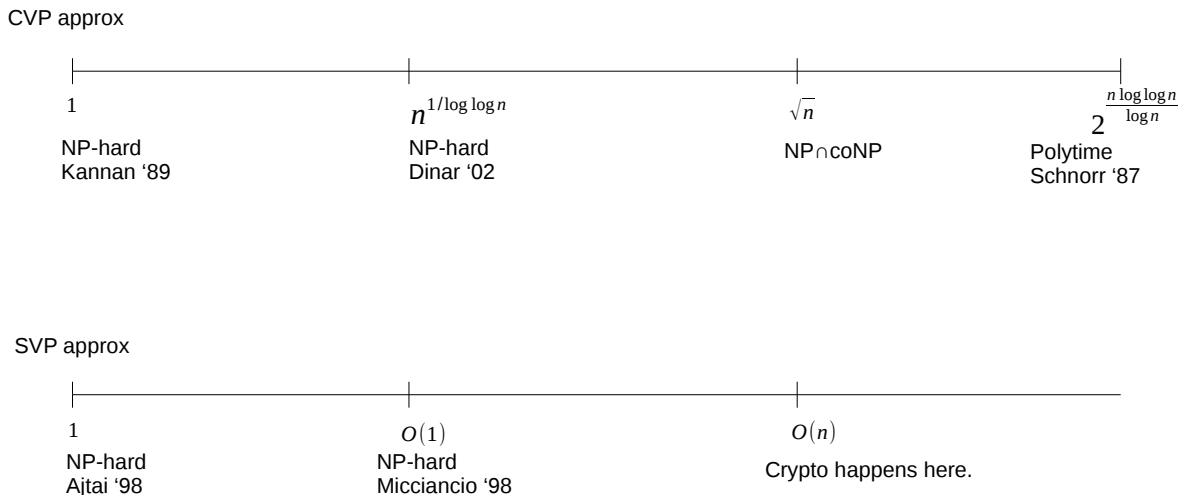

Figure 1: Hardness of approximating CVP and SVP

THEOREM 11 (MIDDLE OF BAND THEOREM, BANASZCZYK 1993) *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\mathbf{t} \in \mathbb{R}^n$, there exists $\mathbf{y} \in \mathcal{L}^* \backslash \{\mathbf{0}\}$ such that*

$$\mathrm{d}(\mathcal{L}, \mathbf{t}) \geq \frac{|\lfloor \langle \mathbf{y}, \mathbf{t} \rangle \rceil - \langle \mathbf{y}, \mathbf{t} \rangle|}{\|\mathbf{y}\|} \geq \frac{\mathrm{d}(\mathcal{L}, \mathbf{t})}{80n}.$$

PROOF: The first inequality holds for every $\mathbf{y} \in \mathcal{L}^* \backslash \{\mathbf{0}\}$: for every $\mathbf{x} \in \mathcal{L}$ we have $\langle \mathbf{y}, \mathbf{x} \rangle \in \mathbb{Z}$ and $\mathrm{d}(\mathbf{x}, \mathbf{t}) \geq \mathrm{d}(\pi_{\mathrm{span}(\mathbf{y})}(\mathbf{x}), \pi_{\mathrm{span}(\mathbf{y})}(\mathbf{t})) = \frac{|\langle \mathbf{y}, \mathbf{x}-\mathbf{t} \rangle|}{\|\mathbf{y}\|}$. This implies

$$\mathrm{d}(\mathcal{L}, \mathbf{t}) \geq \min_{\mathbf{y} \in \mathcal{L}^*} \frac{|\langle \mathbf{y}, \mathbf{x} \rangle - \langle \mathbf{y}, \mathbf{t} \rangle|}{\|\mathbf{y}\|} = \min_{z \in \mathbb{Z}} \frac{|z - \langle \mathbf{y}, \mathbf{t} \rangle|}{\|\mathbf{y}\|} = \frac{|\lfloor \langle \mathbf{y}, \mathbf{t} \rangle \rceil - \langle \mathbf{y}, \mathbf{t} \rangle|}{\|\mathbf{y}\|}.$$

We now prove the second inequality for suitable $\mathbf{y} \in \mathcal{L}^* \backslash \{\mathbf{0}\}$. For $\mathbf{t} \in \mathcal{L}$, all values in the theorem statement are 0 and the inequality holds, so we can assume that $\mathbf{t} \notin \mathcal{L}$. Without loss of generality, rescale such that $\mathrm{d}(\mathcal{L}, \mathbf{t}) = \sqrt{n}$. As in Lemma 1, we will use Corollary 13 from Lecture 7: for $\mathcal{L} \subset \mathbb{R}^n$ a full-rank lattice and $\mathbf{t} \in \mathbb{R}^n$, $\Pr_{\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t}}}[\|\mathbf{X}\| \geq \sqrt{n}] \leq \frac{\rho(\mathcal{L})}{\rho(\mathcal{L}+\mathbf{t})} 4^{-n}$ and $\rho((\mathcal{L}+\mathbf{t}) \backslash \sqrt{n}\mathcal{B}_2^{n,\circ}) \leq 4^{-n}\rho(\mathcal{L})$.

By our current assumption that $\mathrm{d}(\mathcal{L}, \mathbf{t}) = \sqrt{n}$, we have $(\mathcal{L}+\mathbf{t}) \cap \sqrt{n}\mathcal{B}_2^{n,\circ} = \emptyset$. This implies

$$\frac{\rho(\mathcal{L}+\mathbf{t})}{\rho(\mathcal{L})} \leq 4^{-n}. \tag{1}$$

We rewrite the fraction as an expectation using the Poisson summation formula and $\mathcal{L} = -\mathcal{L}$:

$$\begin{aligned} \frac{\rho(\mathcal{L}+\mathbf{t})}{\rho(\mathcal{L})} &= \frac{\frac{1}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} e^{-\pi\|\mathbf{y}\|^2} e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle}}{\frac{1}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} e^{-\pi\|\mathbf{y}\|^2}} \\ &= \frac{\sum_{\mathbf{y} \in \mathcal{L}^*} e^{-\pi\|\mathbf{y}\|^2} \frac{1}{2}(e^{2\pi i \langle \mathbf{y}, \mathbf{t} \rangle} + e^{-2\pi i \langle \mathbf{y}, \mathbf{t} \rangle})}{\sum_{\mathbf{y} \in \mathcal{L}^*} e^{-\pi\|\mathbf{y}\|^2}} \\ &= \mathop{\mathbb{E}}_{\mathbf{Y} \sim D_{\mathcal{L}^*}} [\cos(2\pi \langle \mathbf{Y}, \mathbf{t} \rangle)]. \end{aligned} \tag{2}$$

Now that we have introduced the random variable $\mathbf{Y} \sim D_{\mathcal{L}^*}$, we can split the expectation into two conditional expectations,

$$\begin{aligned}\mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle)] &= \mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) \mid \|\mathbf{Y}\| < \sqrt{n}] \Pr[\|\mathbf{Y}\| < \sqrt{n}] \\ &\quad + \mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) \mid \|\mathbf{Y}\| \geq \sqrt{n}] \Pr[\|\mathbf{Y}\| \geq \sqrt{n}] \\ &\geq \mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) | \|\mathbf{Y}\| < \sqrt{n}] \Pr[\|\mathbf{Y}\| < \sqrt{n}] - \Pr[\|\mathbf{Y}\| \geq \sqrt{n}],\end{aligned} \tag{3}$$

where we used that $\cos(\theta) \geq -1$. We recall the tail bound $\Pr[\|\mathbf{Y}\| \geq \sqrt{n}] \leq 4^{-n}$ and combine (1), (2) and (3):

$$\begin{aligned}4^{-n} &\geq \mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) | \|\mathbf{Y}\| < \sqrt{n}] \Pr[\|\mathbf{Y}\| < \sqrt{n}] - \Pr[\|\mathbf{Y}\| \geq \sqrt{n}] \\ &\geq \mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) | \|\mathbf{Y}\| < \sqrt{n}] \Pr[\|\mathbf{Y}\| < \sqrt{n}] - 4^{-n} \\ &\geq \mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) | \|\mathbf{Y}\| < \sqrt{n}](1 - 4^{-n}) - 4^{-n}\end{aligned} \tag{4}$$

We rearrange and deduce

$$\mathbb{E}[\cos(2\pi\langle \mathbf{Y}, \mathbf{t}\rangle) | \|\mathbf{Y}\| < \sqrt{n}] \leq \frac{2 \cdot 4^{-n}}{1 - 4^{-n}} \leq \frac{2}{3}.$$

Hence there exists some $\mathbf{y} \in \mathcal{L}^*$ such that $\|\mathbf{y}\| < \sqrt{n}$ and $\cos(2\pi\langle \mathbf{y}, \mathbf{t}\rangle) \leq 2/3$. Now recall the shape of the cosine function: if $\cos(2\pi\langle \mathbf{y}, \mathbf{t}\rangle) \leq 2/3$, then the argument $2\pi\langle \mathbf{y}, \mathbf{t}\rangle$ must be far from any integer multiple of 2π: $|\lfloor \langle \mathbf{y}, \mathbf{t}\rangle \rceil - \langle \mathbf{y}, \mathbf{t}\rangle| \geq 1/80$. We have hence proven that

$$\frac{|\lfloor \langle \mathbf{y}, \mathbf{t}\rangle \rceil - \langle \mathbf{y}, \mathbf{t}\rangle|}{\|\mathbf{y}\|} > \frac{1}{80\sqrt{n}} = \frac{\mathrm{d}(\mathcal{L}, \mathbf{t})}{80n},$$

by assumption on $\mathrm{d}(\mathcal{L}, \mathbf{t})$. □