MATH6302

AUSTIN WU

Date: May 28, 2025.

Problem 1:

a:

Given a $\mathcal{L}$, run the $\gamma-$svp on it. Thus we have obtained a non-zero vector v such that

$$||v|| \leq \gamma\lambda_1(\mathcal{L})$$

And since we know from minkowskis theorem that

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}\det(\mathcal{L})^{\frac{1}{n}}$$

Implies that

$$||v|| \leq \gamma\sqrt{n}\det(\mathcal{L})^{\frac{1}{n}}$$

Which implies that running γ-SVP returns a non-zero vector that satisfies $\gamma\sqrt{n}$-MSVP. Thus since γ-SVP runs in polynomial time there is trivially a reduction to polynomial time.

b:

Recall from cauchy schwartz that given

$$||v|| < \frac{1}{\delta}\det(\mathcal{L})^{\frac{1}{n}}$$

and

$$||w|| < \delta\det(\mathcal{L}^*)^{\frac{1}{n}}$$

That by cauchy schwartz, since

$$|\langle w, v\rangle| \leq ||w||||v||$$

Implies that

$$|\langle w, v\rangle| \leq ||v||||w|| < \frac{1}{\delta}\det(\mathcal{L})^{\frac{1}{n}}\delta\det(\mathcal{L}^*)^{\frac{1}{n}} = (\det(\mathcal{L})\det(\mathcal{L}^*))^{\frac{1}{n}} \tag{1}$$

Thus since $\det(\mathcal{L})\det(\mathcal{L}^*) = 1$ even for non full rank lattices, we know that

$$= 1^{\frac{1}{n}} \tag{2}$$

$$= 1 \tag{3}$$

But since by definition of a dual lattice we know that $\langle w, v\rangle \in \mathbb{Z}$ and $|\langle w, v\rangle| < 1$ there is only one possible solution which is tha t $|\langle w, v\rangle| = 0$

c:

Let $\det(\mathcal{L}_i)$ be the determinat of the i-th lattice. Let r_i be the rank of the i-th lattice. Since we start with a lattice at rank n this implies that $r_i = n - i + 1$. Thus since $\mathcal{A}$ solves γ-MSVP we know by theorem 1.1 that

$$||y_i|| \leq \delta \det(\mathcal{L}_i)^{\frac{1}{r_i}}$$

$$||w_i|| \leq \delta \det(\mathcal{L}_i^*)^{\frac{1}{r_i}}$$

We also know for any given lattice intersecting with $w_i^\perp$ reduces the determinant $\det(\mathcal{L}_{i+1}) = \frac{\det(\mathcal{L}_i)}{||w_i||}$. Now let $v = \lambda_1(\mathcal{L}) \in \mathcal{L}$. Recall also that $\det(\mathcal{L}_i)\det(\mathcal{L}_i^*) = 1$ for every i

Let $v \in \mathcal{L}$ be a non-zero vector with $\|v\| = \lambda_1(\mathcal{L})$. Now let t be the smallest index such that

$$t := \min\Big\{ i : ||v|| \leq \tfrac{1}{\delta} \det(\mathcal{L}_i)^{1/r_i} \Big\}.$$

Because $\delta \geq \sqrt{n}$, by Minkowski such an index exists. Thus for all $j < t$ we have $\|v\| > \det(\mathcal{L}_j)^{1/r_j}/\delta$. Combining this with the bound on $\|w_j\|$ and Problem 1.2 gives $\langle w_j, v\rangle \neq 0$ so $v \notin \mathcal{L}_{j+1}$. But since by construction $v \in \mathcal{L}_t$, and at $i = t$ the problem does apply, so since α guarentees a solution to δ-MSVP,

$$\langle w_t, v\rangle = 0, \qquad \text{i.e. } v \in \mathcal{L}_{t+1}.$$

$$\|y_{t+1}\| \leq \delta \det(\mathcal{L}_{t+1})^{1/r_{t+1}} = \delta \left(\det(\mathcal{L}_t)/\|w_t\|\right)^{1/(r_t-1)}.$$

Now since $\|w_t\| \leq \delta \det(\mathcal{L}_t^*)^{1/r_t}$ and $\det(\mathcal{L}_t)\det(\mathcal{L}_t^*) = 1$,

$$\det(\mathcal{L}_{t+1})^{1/r_{t+1}} \leq \left(\det(\mathcal{L}_t)\right)^{1/(r_t-1)} = \Big(\delta \|v\|\Big)^{\frac{r_t}{r_t-1}},$$

where the equality uses the definition of t. Thus,

$$\|y_{t+1}\| \leq \delta \Big(\delta \|v\|\Big) = \delta^2 \lambda_1(\mathcal{L}).$$

Thus the algorithm outputs the shortest vector among $y_1, \ldots, y_n$, so the final answer y satisfies

$$\|y\| \leq \|y_{t+1}\| \leq \delta^2 \lambda_1(\mathcal{L}),$$

i.e. it is a valid solution to δ^2-SVP.

Problem 2:

a:

Let $y_1, \ldots, y_l \in \mathcal{L}'$ be a basis of $\mathcal{L}'$ and extend it to $y_{l+1}, \ldots, y_n \in \mathcal{L}$ so that $y_1, \ldots, y_n$ is a basis of $\mathbb{R}^n$. Set $U := \text{span}(\mathcal{L}')$ and $V := \text{span}(y_{l+1}, \ldots, y_n)$. Because $U \oplus V = \mathbb{R}^n$, we have $(\mathcal{L}')^\perp = V^\perp$ and $\dim V^\perp = n - l$. Note that $V \cap U = \{0\}$.
For $i > l$ put $z_i := \Pi_{(\mathcal{L}')^\perp}(y_i)$. Since the vectors $z_{l+1}, \ldots, z_n$ are linearly independent (projection is injective on V since $\cap U = \{0\}$) and lie in $(\mathcal{L}')^\perp$, so they form a basis of $(\mathcal{L}')^\perp$.
Now for each z_i since we know it belongs to $S = \Pi_{(\mathcal{L}')^\perp}(\mathcal{L})$ we know that $(\mathcal{L}')^\perp \subseteq \text{span}(S)$. The opposite inclusion is also obvious, which implies equality.

b:

Let $y_1, \ldots, y_l \in \mathcal{L}'$ be a basis of $\mathcal{L}'$ and extend it to linearly independent $y_{l+1}, \ldots, y_n \in \mathcal{L}$. This is guarenteed to exist since $\mathcal{L}'$ is a sublattice. Now write $B := \{y_1 \ \ldots \ y_n\}$, so $L = B\mathbb{Z}^n$ and its dual lattice has basis $B^{-*} := B^{-T}$. Denote the dual basis vectors by $y_1^*, \ldots, y_n^*$, so $B^{-*} := \{y_1^* \ \ldots \ y_n^*\}$.
Now since by construction $y_j^* \in \mathcal{L}^*$. This implies that for $1 \le i \le l < j \le n$ we have $\langle y_i, y_j^* \rangle = \delta_{ij} = 0$, hence $y_j^* \perp \mathcal{L}'$, so $y_j^* \in (\mathcal{L}')^\perp$. Not since independence is inherited from the dual basis. Thus $y_{l+1}^*, \ldots, y_n^* \in \mathcal{L}^* \cap (L')^\perp = T$ and the vectors are linearly independent.
There are $n - l$ such vectors, matching $\dim(\mathcal{L}')^\perp$, so this implies that $\text{span}(T) \supseteq \text{span}\{y_{l+1}^*, \ldots, y_n^*\} = (\mathcal{L}')^\perp$.
Thus since we also know that by definition $T \subseteq (\mathcal{L}')^\perp$, hence

$$\text{span}(T) = (\mathcal{L}')^\perp.$$

c:

Let $w \in \mathcal{L}^* \cap (\mathcal{L}')^\perp$. For any $y \in \mathcal{L}$ let $s := \Pi_{(\mathcal{L}')^\perp}(y) \in S$. Thus since w is in $(\mathcal{L}')^\perp$ and $s(y)$ is in the proejction space which is self adjoint implies that for any $y \in \mathcal{L}$,

$$\langle s(y), w \rangle = \langle \Pi_{(\mathcal{L}')^\perp}(y), w \rangle = \langle y, \Pi_{(\mathcal{L}')^\perp}(w) \rangle = \langle y, w \rangle \in \mathbb{Z}$$

Since $w \in \mathcal{L}^*$. Thus since w $\text{span}(S) = (\mathcal{L}')^\perp$ implies that $w \in S^*$.
Now let $w \in S^*$. By definition of S^* we already have $w \in \text{span}(S) = (\mathcal{L}')^\perp$. To prove $w \in \mathcal{L}^*$, pick an arbitrary $y \in \mathcal{L}$ and set $y = y_\parallel + y_\perp$ with $y_\parallel \in \text{span}(\mathcal{L}')$ and

$y_\perp := \Pi_{(\mathcal{L}')^\perp}(y) \in S$. Then

$$\langle y, w \rangle = \langle y_\parallel, w \rangle + \langle y_\perp, w \rangle.$$

Because $w \in (\mathcal{L}')^\perp$, the first term vanishes ($w \perp \mathcal{L}'$) and the second term is an integer since $y_\perp \in S$ and $w \in S^*$. Hence $\langle y, w \rangle \in \mathbb{Z}$ for all $y \in \mathcal{L}$, which implies that $w \in \mathcal{L}^*$. Thus the two inclusions give $S^* = lat^* \cap (\mathcal{L}')^\perp$, establishing that

$$\left(\Pi_{(\mathcal{L}')^\perp}(\mathcal{L})\right)^* \;=\; \mathcal{L}^* \cap (\mathcal{L}')^\perp.$$

Problem 3:

Not as much as others