# CS 258: Quantum Cryptography (Fall 2025)
# Homework 3 (100 points)

## 1 Problem 1 (30 points)

In class, for a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $m > n$, we defined the lattices

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} \bmod q = 0\}$$
$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{r} \in \mathbb{Z}^n : \mathbf{x} = \mathbf{A}^T \cdot \mathbf{r} \bmod q\}$$

We said that $\Lambda_q^{\perp}(\mathbf{A})$ is spanned by the integer vectors in the kernel of $\mathbf{A}$ as well as $q\mathbf{I}$. However, this is not a basis. Likewise, $\Lambda_q(\mathbf{A})$ is spanned by the rows of $\mathbf{A}$ and $q\mathbf{I}$, but this is not a basis. Here, you will find explicit bases for these lattices.

Assume for simplicity that the first $n$ columns of $\mathbf{A}$ are linearly independent mod $q$. In general, we will always work in a regime where the some set of $n$ columns are linearly independent with overwhelming probability. If they are not the first $n$ columns, we can adjust the derivation below, but you are not required to do so.

**Part (a). 10 points.** Write $\mathbf{A} = (\mathbf{A}_0|\mathbf{A}_1)$ where $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times n}$ is full rank mod $q$. Define $\mathbf{A}' = \mathbf{A}_0^{-1}\mathbf{A} \bmod q = (\mathbf{I}, \mathbf{A}_1')$ where $\mathbf{A}_1' = \mathbf{A}_0^{-1}\mathbf{A}_1 \bmod q$. Here, the inverse is taking mod $q$, so that $\mathbf{A}_0^{-1} \in \mathbb{Z}_q^{n\times n}$; this inverse exists by assumption that $\mathbf{A}_0$ is full rank mod $q$. Show that $\Lambda_q(\mathbf{A}') = \Lambda_q(\mathbf{A})$ and $\Lambda_q^{\perp}(\mathbf{A}') = \Lambda_q^{\perp}(\mathbf{A})$.

**Part (b). 10 points.** Show that the columns of

$$\begin{pmatrix} q\mathbf{I}_n & -\mathbf{A}_1' \\ 0 & \mathbf{I}_{m-n} \end{pmatrix}$$

form a basis for $\Lambda_q^{\perp}(\mathbf{A})$, where $\mathbf{I}_k$ is the $k \times k$ identity matrix. To do so, show that the columns of this matrix are each in $\Lambda_q^{\perp}(\mathbf{A})$, and that any vector $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A})$ can be written as an integer linear combination of the columns.

**Part (c). 10 points.** Show that the columns of

$$\begin{pmatrix} \mathbf{I}_n & 0 \\ (\mathbf{A}_1')^T & q\mathbf{I}_{m-n} \end{pmatrix}$$

form a basis for $\Lambda_q(\mathbf{A})$.

## 2 Problem 2 (30 points)

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice, which we will assume to be full rank. The dual lattice, denoted $\mathcal{L}^*$, is defined as:

$$\mathcal{L}^* = \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{y} \in \mathcal{L}, \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z}\}$$

That is, the inner product of any vector $\mathbf{x} \in \mathcal{L}^*$ with any vector $\mathbf{y} \in \mathcal{L}$ is an integer.

**Part (a). 10 points** Suppose $\mathcal{L} = \mathcal{L}(\mathbf{B})$ for some basis $\mathbf{B} \in \mathbb{R}^{n\times n}$ ($\mathbf{B}$ is square since $\mathcal{L}$ is assumed to be full rank). Show that $\mathcal{L}^* = \mathcal{L}(\mathbf{B}^{-T})$, where $\mathbf{B}^{-T} = (\mathbf{B}^{-1})^T = (\mathbf{B}^T)^{-1}$. *[Hint: write any vector* $\mathbf{x} \in \mathbb{R}^n$ *as* $\mathbf{x} = \mathbf{B}^{-T} \cdot \mathbf{r}$ *for a unique* $\mathbf{r}$*, which is possible since* $\mathbf{B}$ *and hence* $\mathbf{B}^{-T}$ *is full rank. If* $\mathbf{r} \in \mathbb{Z}^n$ *(meaning that* $\mathbf{x} \in \mathcal{L}(\mathbf{B}^{-1})$*), what is the inner product of* $\mathbf{x}$ *with the elements of* $\mathcal{L}$*? If* $\mathbf{r} \notin \mathbb{Z}^n$*, what is the inner product of* $\mathbf{x}$ *with the elements of* $\mathcal{L}$*?]*

**Part (b). 10 points** Show that $(\mathcal{L}^*)^* = \mathcal{L}$.

**Part (c). 10 points** Suppose you have a basis $\mathbf{B}$ for $\mathcal{L}$ that is "short", in the sense that each column of $\mathbf{B}$ has norm at most $\sigma$. Here, you will see how to solve (approximate) CVP in $\mathcal{L}^*$.

Let $\mathbf{y}$ be a vector that is "close" to $\mathcal{L}^*$, in the sense that there exist a short vector $\mathbf{e}$ such that $\mathbf{u} = \mathbf{y} - \mathbf{e} \in \mathcal{L}^*$. In particular, assume that $|\mathbf{e}| < 1/2n\sigma$. Your goal is to compute $\mathbf{u}$, or equivalently $\mathbf{e}$.

To do so, compute $\mathbf{B}^T\mathbf{y}$, and use that $\mathbf{y} = \mathbf{u} + \mathbf{e}$. What happens if you round to the nearest integer? What happens if instead you remove the integer part (this is the same as reducing mod 1)? *[Hint: recall that* $|\mathbf{a} \cdot \mathbf{b}| \leq |\mathbf{a}| \times |\mathbf{b}|$*]*

# 3 Problem 3 (40 points)

The $S|LWE\rangle$ problem ($S$ for "state") problem asks to compute $\mathbf{s}$ from the state

$$|\tau_{\mathbf{s}}\rangle := \sum_{\mathbf{e}} \sqrt{\Pr[\mathbf{e} \leftarrow D_\sigma^m]}|\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q\rangle$$

**Part (a). 10 points.** Assume that $\mathbf{e}$ in the support of $D_\sigma^m$ has support constrained to $\sigma m$. Also, assume that there are no vectors of norm at most $2\sigma m$ in $\Lambda_q(\mathbf{A})$. Then show that the states $|\tau_{\mathbf{s}}\rangle$ for different $\mathbf{s} \in \mathbb{Z}_q^n$ are orthogonal. Thus, the task of finding $\mathbf{s}$ from $|\tau_{\mathbf{s}}\rangle$ is at least information-theoretically possible.

**Part (b). 10 points** Show how to construct $|\tau_{\mathbf{s}}\rangle$ from $\mathbf{s}$ efficiently. You may assume the ability to create Gaussian-weighted superpositions $\sum_e \sqrt{\Pr[e \leftarrow D_\sigma]}|e\rangle$, that $D_\sigma$ has support only on integers of absolute value at most $\sigma\sqrt{m}$, and that $\sigma\sqrt{m} < q/2$.

**Part (c). 10 points.** Explain that if search LWE is easy, then $S|LWE\rangle$ is easy, for the same parameters $q, n, m, \sigma$.

**Part (d). 10 points.** Show that if it is possible to solve $S|LWE\rangle$ perfectly with parameter $\sigma = q/2\gamma$, then it is possible to solve SIS with parameter $\beta = \gamma m$ (these are the same parameters we saw in class for Regev's reduction). Concretely, you may assume that the the $S|LWE\rangle$ solver is a unitary mapping $|\tau_{\mathbf{s}}\rangle|\mathbf{y}\rangle$ to $|\tau_{\mathbf{s}}\rangle|\mathbf{y} + \mathbf{s} \bmod q\rangle$.

For this problem, you may assume the ability to construct Gaussian-weighted superpositions of arbitrary parameter $\gamma$ such that $1 \ll \gamma \ll q$, that the support of such distributions constrained to "small" vectors as described above, and also the ability to construct the uniform superpositions over linear subspaces.

**Remark 1.** *The above shows that* $S|LWE\rangle$ *is at least as hard as SIS, and that LWE is at least has hard as* $S|LWE\rangle$*. But it could be that* $S|LWE\rangle$ *is actually an easier problem than ordinary LWE. We know, under some loss in the parameters* $n, m, q, \sigma$ *that* $S|LWE\rangle$ *and LWE are equivalent, but we do* not *know if they are equivalent for the exact same parameters.*