

## Q5

(1)

Denote the columns of  $A$  by  $A = [\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n]$ . Without loss of generality, let  $\mathbf{a}_n$  be a non-zero linear combination of the other  $n-1$  columns:  $\mathbf{a}_n = A'\mathbf{z}'$  for some  $\mathbf{z} \in \mathbb{Z}^{n-1}$ .

It is easy to see that because  $A'$  contains only a subset of columns of  $A$ , so  $A'\mathbb{Z}^{n-1} \subseteq A\mathbb{Z}^n$ . It naturally follows that

$$A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m \subseteq A\mathbb{Z}^n + q\mathbb{Z}^m$$

On the other hand, let  $\mathbf{v} \in A\mathbb{Z}^n + q\mathbb{Z}^m$ , then there exist  $\mathbf{x}_1 \in \mathbb{Z}^n, \mathbf{x}_2 \in \mathbb{Z}^m$  such that

$$\begin{aligned} \mathbf{v} &= A\mathbf{x}_1 + q\mathbf{x}_2 \\ &= \sum_{i=1}^n (\mathbf{a}_i x_{(1,i)}) + q\mathbf{x}_2 \\ &= \left( \sum_{i=1}^{n-1} \mathbf{a}_i x_{(1,i)} \right) + \mathbf{a}_n x_{(1,n)} + q\mathbf{x}_2 \\ &= A' \cdot (x_{(1,1)}, x_{(1,2)}, \dots, x_{(1,n-1)}) + A'\mathbf{z}'x_{(1,n)} + q\mathbf{x}_2 \\ &= A'((x_{(1,1)}, x_{(1,2)}, \dots, x_{(1,n-1)}) + \mathbf{z}'x_{(1,n)}) + q\mathbf{x}_2 \in A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m \end{aligned}$$

Therefore we have  $A\mathbb{Z}^n + q\mathbb{Z}^m \subseteq A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m$ , and the two lattices are indeed equal.

(2)

Let  $(A, \mathbf{b})$  be a sample from generic (aka potentially not full-rank)  $\text{LWE}(m, n, q, U_s, \chi_e)$ . Without loss of generality, assume that  $A = [A_1 \mid A_2] \in \mathbb{Z}_q^{m \times (n_1 + n_2)}$  where  $A_1$  is full-rank, and  $A_2 = A_1 B$  for some non-zero  $B \in \mathbb{Z}_q^{n_1 \times n_2}$ . Denote the secret by  $\mathbf{s} = [\mathbf{s}_1 \mid \mathbf{s}_2]$  where  $\mathbf{s}_1 \leftarrow \chi_s^{n_1}, \mathbf{s}_2 \leftarrow \chi_s^{n_2}$ , then:

$$\begin{aligned} \mathbf{b} &= A\mathbf{s} + \mathbf{e} \\ &= (A_1\mathbf{s}_1 + A_2\mathbf{s}_2) + \mathbf{e} \\ &= A_1\mathbf{s}_1 + A_1B\mathbf{s}_2 + \mathbf{e} \\ &= A_1(\mathbf{s}_1 + B\mathbf{s}_2) + \mathbf{e} \end{aligned}$$

Because secrets are sampled from a uniform distribution,  $\mathbf{s}_1 + B\mathbf{s}_2$  is uniformly random. Therefore  $(A_1, \mathbf{b})$  is a valid sample from full-rank  $\text{LWE}(m, n, q, U_s, \chi_e)$ . We can thus feed  $(A_1, \mathbf{b})$  to a full-rank LWE oracle, who will output some  $\mathbf{s}'$ . Assuming that the full-rank LWE problem has unique solution, we know  $\mathbf{s}' = \mathbf{s}_1 + B\mathbf{s}_2$