1 Dual Basis

Let $A = [I, A'] \in \mathbb{Z}^{k \times n}$, where $I$ is the identity matrix, and $A' \in \mathbb{Z}^{k \times (m-k)}$. Give a basis for the following lattices, and prove that your solution is correct:

1. $\Lambda_q(A) = \{ \vec{x} \in \mathbb{Z}^n : A\vec{x} = \vec{0} \pmod{q} \}$
2. $\Lambda_q^\perp(A) = \{ \vec{x} \in \mathbb{Z}^n : \vec{x} = A^T\vec{s} \pmod{q} \text{ for some } \vec{s} \in \mathbb{Z}^k \}$
3. The lattice dual of $\Lambda_q(A)$
4. The lattice dual of $\Lambda_q^\perp(A)$.

2 Minkowski’s bound for Random lattices

Let $A = [I, A'] \in \mathbb{Z}_q^{k \times n}$ be as in the first problem, with $A'$ chosen uniformly at random. Prove upper and lower bounds on the length of the shortest nonzero vector of the corresponding lattices:

1. Given an upper bound on the minimum distance $\lambda_1(\Lambda_q^\perp(A)) \leq M$ using Minkowki’s theorem
2. Prove that there is a constant $c > 0$ (independent of the parameters $n, k, q$) such that $\lambda_1(\Lambda_q^\perp(A)) \geq cM$ with high probability, when $A'$ is chosen at random. (“High probability” means very close to 1 when the parameters $n, m$ are sufficiently large.) (Hint: use a counting argument over all candidate short vectors.)
3. Given an upper bound on the minimum distance $\lambda_1(\Lambda_q(A)) \leq M'$ using Minkowki’s theorem
4. Prove that there is a constant $c' > 0$ (independent of the parameters $n, k, q$) such that $\lambda_1(\Lambda_q(A)) \geq c'M'$ with high probability, when $A'$ is chosen at random. (Hint: Use duality and the previous problems.)