Lecture 12
SIS Lattices & Applications

Instructor: Chris Peikert
Scribe: Jacob Alperin-Sheriff

1 SIS Lattices

In this lecture we give properties and applications of SIS (short integer solution) lattices. We first recall the SIS problem.

Definition 1.1 (Shortest Integer Solution Problem). For a positive integer modulus q, dimensions n, m and a norm bound $\beta > 0$, the $\mathsf{SIS}_{n,q,\beta,m}$ problem is defined as follows: given uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find a nonzero "short" solution $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{z} = \mathbf{0} \in \mathbb{Z}_q^n$ and $\|\mathbf{z}\| \leq \beta$.

Equivalently, the goal is to find a non-zero vector of norm at most β in the following integer "SIS lattice" (it is easy to verify that this set is a discrete additive subgroup):

$$\mathcal{L}^{\perp}(\mathbf{A}) := \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0}\}.$$

Borrowing a term from coding theory, matrix $\mathbf{A}$ is often called a *parity-check matrix* for the lattice $\mathcal{L}^{\perp}(\mathbf{A})$.