

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 $\text{SIS}_{n,q,\beta,m}$ 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 $\mathcal{L}^\perp(\mathbf{A})$.

We begin with some mathematical properties of SIS lattices. First, these lattices are called “ q -ary” because they contain every integer vector whose entries are all multiples of q :

$$q\mathbb{Z}^m \subseteq \mathcal{L}^\perp(\mathbf{A}) \subseteq \mathbb{Z}^m.$$

So, a vector’s membership in $\mathcal{L}^\perp(\mathbf{A})$ is determined solely by its entries modulo q .

Cosets. Borrowing another term from coding theory let $\mathbf{y} \in \mathbb{Z}_q^n$ be a “syndrome” in the image of \mathbf{A} , i.e., there exists some $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{y}$. Then we can define the corresponding lattice coset

$$\mathcal{L}_\mathbf{y}^\perp(\mathbf{A}) := \{\mathbf{x}' \in \mathbb{Z}^m : \mathbf{A}\mathbf{x}' = \mathbf{y}\} = \mathbf{x} + \mathcal{L}^\perp(\mathbf{A}),$$

where the equality holds because every $\mathbf{x}' \in \mathbf{x} + \mathcal{L}^\perp(\mathbf{A})$ satisfies $\mathbf{A}\mathbf{x}' = \mathbf{A}\mathbf{x} = \mathbf{y}$, and for any $\mathbf{x}' \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{x}' = \mathbf{y}$, we have $\mathbf{x}' = \mathbf{x} + (\mathbf{x}' - \mathbf{x}) \in \mathbf{x} + \mathcal{L}^\perp(\mathbf{A})$ because $\mathbf{A}(\mathbf{x}' - \mathbf{x}) = \mathbf{0}$.

Determinant. By the bijective correspondence between integer cosets and syndromes in the image of \mathbf{A} , we have that

$$\det(\mathcal{L}^\perp(\mathbf{A})) = |\mathbb{Z}^m / \mathcal{L}^\perp(\mathbf{A})| = |\text{Image}(\mathbf{A})| \leq q^n,$$

with equality if the image of \mathbf{A} is all of \mathbb{Z}_q^n (i.e., the columns of \mathbf{A} generate \mathbb{Z}_q^n), which will be the setting we are almost always interested in.

If q is prime, then $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ generates all of \mathbb{Z}_q^n if and only if it contains an $n \times n$ submatrix that is invertible modulo q . (It is not too hard to show that when, say, $m \geq (1 + \delta)n$ for a constant $\delta > 0$, this holds with high probability over the uniformly random choice of \mathbf{A} .) However, if q is composite, this condition is sufficient but not necessary. For example, $\mathbf{A} = (2, 3) \in \mathbb{Z}_6^{1 \times 2}$ generates all of \mathbb{Z}_6 , even though neither 2 nor 3 are invertible modulo 6.