Kaliningrad Summer School — 15-19 July 2019

Exercises, Day 1

Exercise 1: Counter-examples

1. Show that $a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$ is a lattice, for every $a, b \in \mathbb{Q}$.
   Show that $1 \cdot \mathbb{Z} + \sqrt{2} \cdot \mathbb{Z}$ is not a lattice.

2. Give a 2-dimensional lattice L such that L contains 6 vectors whose norms are $\lambda_1(L)$.

3. Show that the lattice spanned by the columns of the following basis has no basis $(\mathbf{b}_1, \ldots, \mathbf{b}_5)$ such that $\|\mathbf{b}_i\| = \lambda_i(L)$ for all $i \leq 5$.

$$\begin{bmatrix} 2 & & & & 1 \\ & 2 & & & 1 \\ & & 2 & & 1 \\ & & & 2 & 1 \\ & & & & 1 \end{bmatrix}$$

Exercise 2: From codes to lattices

Let $q \geq 2$ be a prime integer. Let $C \subseteq \mathbb{Z}_q^m$ be a linear code of rank n, i.e., $C = G \cdot \mathbb{Z}_q^n$ for some $G \in \mathbb{Z}_q^{m \times n}$ of rank n. We define the construction-A lattice obtained from C as

$$L(C) = C + q \cdot \mathbb{Z}^m = \{\mathbf{b} \in \mathbb{Z}^m : (\mathbf{b} \bmod q) \in C\}\,.$$

4. Show that $L(C)$ is a lattice, by exhibiting a basis of $L(C)$.
   Hint: Assume first that the first n rows of G form the identity matrix.

5. What are the dimension and determinant of $L(C)$?
   Apply Minkowski's theorem to obtain bounds on $\lambda_1(L(C))$ and $\lambda_1^\infty(L(C))$.
   Show that these bounds can be incorrect if we do not assume that q is prime.

6. Now, assume that we sample G uniformly in $\mathbb{Z}_q^{m \times n}$. We want to show that with overwhelming probability (over the choice of G), there is no very short vector in $L(G \cdot \mathbb{Z}_q^n)$. Let $B > 0$. Show that

$$\Pr_G\Big[\exists \mathbf{b} \in L(G \cdot \mathbb{Z}_q^n) \text{ with } 0 < \|\mathbf{b}\|_\infty < B\Big] \;\leq\; \sum_{\mathbf{s} \in \mathbb{Z}_q^n \setminus \mathbf{0}} \; \sum_{\substack{\mathbf{b} \in \mathbb{Z}^m \\ 0 < \|\mathbf{b}\|_\infty < B}} \Pr_G\Big[G \cdot \mathbf{s} = \mathbf{b} \bmod q\Big].$$

   Conclude.

7. Show that the probability of a uniform $G \in \mathbb{Z}_q^{m \times n}$ is of rank n is bounded from below by $1 - 4/q^{m-n+1}$. This implies that the probabilistic lower bound obtained at the previous question also holds for a uniformly chosen C rather than a uniformly chosen G, when $m \gg n$.