**Kaliningrad Summer School — 15-19 July 2019**

Exercises, Day 2

## Exercise 1: 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

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

1. 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.*

2. 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.[1]

3. 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.

4. 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 $m \gg n$.

## Exercise 2: A lower bound on the first minimum

5. Let $B$ be a basis of a lattice $L$, with QR-factorization $B = Q \cdot R$. Show that $\lambda_1(L) \geq \min_i r_{ii}$.
*Hint: Write $\mathbf{b} \in L \setminus 0$ as $\mathbf{b} = B \cdot \mathbf{x}$ and consider the last $x_i$ that is non-zero.*

[1] This is where we stopped yesterday

## Exercise 3: Sandpile modelling of LLL

Let $(x_1, \ldots, x_n)$ be a tuple of $n$ reals. We can perform the following operation $\mathbf{x}' \leftarrow \mathbf{x}$ on the tuple, if $x_i > x_{i+1} + 1$ (for some $i < n$):

$$\begin{aligned} x'_j &\leftarrow x_j \quad \text{if } j \notin \{i, i+1\}, \\ x'_i &\leftarrow x_i - 1/4, \\ x'_{i+1} &\leftarrow x_{i+1} + 1/4. \end{aligned}$$

This models the evolution of the $\log r_{ii}$'s during the execution of the LLL algorithm.

**6.** Give a bound on the number of times such an operation can be applied.

**7.** Show that when no such operation can be applied, then $x_1 \leq \frac{n-1}{2} + \frac{1}{n} \sum_{i \leq n} x_i$.

The Gauss-LLL algorithm would correspond to the following allowed operation $\mathbf{x}' \leftarrow \mathbf{x}$, when $x_i > x_{i+1} + 1$ (for some $i < n$):

$$\begin{aligned} x'_j &\leftarrow x_j \quad \text{if } j \notin \{i, i+1\}, \\ x'_i &\leftarrow \frac{x_i + x_{i+1}}{2} + 1/4, \\ x'_{i+1} &\leftarrow \frac{x_i + x_{i+1}}{2} - 1/4. \end{aligned}$$

**8.** Assume that the initial tuple satisfies $x_1 > \ldots > x_n > 1$. Show that there is a strategy (for choosing the index $i$ at every update) that allows to obtain a number of iterations bounded as $O(n^3 \log x_1)$. Show that there is an input sequence $x_1 > \ldots > x_n > 1$ such that all strategies require $\Omega(n^3 \log x_1)$ updates.