Kaliningrad Summer School — 15-19 July 2019

Exercises, Day 3

Exercise 1: 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.

1. Give a bound on the number of times such an operation can be applied.
2. 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 $i < n$):

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

3. 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.

Exercise 2: Insecure versions of Lyubashevsky's scheme

Recall the verification algorithm. It takes $vk \in \mathbb{Z}_q^{\ell \times n}$, $(Z, C) \in \mathbb{Z}^{\ell \times m} \times \mathbb{Z}^{\ell \times \ell}$ and $M \in \{0,1\}^*$ and outputs 1 if and only if the following two conditions are satisfied:

- Every entry in Z has magnitude below B_Z;
- $C = H(vk, Z \cdot A - C \cdot vk, M)$.

We assume that $q \geq 2$ is polynomially bounded in n, and that $\ell, n \leq m$.

4. Assume verification is modified so that the smallness of the entries in Z is not checked. Give a signature forgery attack.
5. Assume that $\ell = 1$. Give a signature forgery attack.
6. Assume that the rejection step in the signature algorithm is omitted. Give a key forgery attack.