CSE 206A: Lattices Algorithms and Applications (Fall 2021)

Problem Set 1

Lecturer: Daniele Micciancio **Due:** *Wed Oct 27, 2021*

1 HNF

Compute the (upper triangular) Hermite Normal Form of $\begin{bmatrix} 11 & 40 \\ 5 & 18 \end{bmatrix}$ via a sequence of elementary column operations. Give the final result, and the unimodular matrix corresponding to the sequence of operations.

2 Gram-Schmidt

Compute the Gram-Schmidt orthogonalization, Gram matrix and determinant of the lattice generated by the basis $\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$.

3 Sublattices

Let Λ be a full rank sublattice of Λ'. Prove that

- $\det(\Lambda')$ divides $\det(\Lambda)$
- $\Lambda = \Lambda'$ if and only if $\det(\Lambda) = \det(\Lambda')$.

4 Extremal Lattices

Let $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice achieving Hermite constant $\gamma_n = \left(\lambda(\Lambda)/\det(\Lambda)^{1/n}\right)^2$. Prove that Λ has n linearly independent vectors of length $\lambda(\Lambda)$, i.e., $\lambda_1(\Lambda) = \lambda_2(\Lambda) = \ldots = \lambda_n(\Lambda)$. *[Hint: Use Minkowski's second theorem and Hadamard inequality.]*

5 Bad HNF

The HNF can be very useful to check algebraic properties of lattices, e.g., two bases generate the same lattice if they have the same HNF. However, HNF typically gives a basis with very bad geometric properties. In this problem you are asked to explore how bad it can be.

Show that for any positive integer n, there is an $n \times n$ integer basis matrix $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$ with short vectors $\vec{b}_i \in \{0, 1, -1\}^n$ (in particular, $\|\vec{b}_i\| \leq \sqrt{n}$), while *all* vectors in the HNF basis $\mathbf{H} = HNF(\mathbf{B})$ have length $\|\vec{h}_i\| \geq 2^{\Omega(n)}$ that is exponentially bigger.

Partial credit: The problem has a relatively simple solution, but in case you cannot find it, you can settle for some of the following simpler tasks. Find a matrix $\mathbf{B}$ as above, such that at least *one* of the $\vec{h}_i$ has length $2^{\Omega(n)}$. If still too hard, just make $\vec{b}_i$ as short as you can, and $\vec{h}_i$ as long as you can.

Extra credit: Can you make the $\vec{h}_i$ even longer than $2^{\Omega(n)}$? How long? Can you solve the problem with $\mathbf{B} \in \{0, 1\}^{n \times n}$, rather than $\{0, 1, -1\}$?