CSE206A: Lattice Algorithms and Applications
Spring 2007, Homework 2: Representing lattices

Daniele Micciancio

May 1, 2007

Lattices are usually represented by a basis, i.e., a set of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k$ that generate the lattice. In this assignment we consider alternative representations, and algorithms to convert between them.

1 Working with a triangular basis

In the problem 2 you will show (among other things) that every full rank integer lattice has a lower triangular basis. Triangular bases are very convenient to work with, as shown in this first problem.

Give a polynomial time algorithm that on input a full rank lower triangular basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$ and a vector $\mathbf{t} \in \mathbb{Z}^n$ (not necessarily in the lattice generated by $\mathbf{B}$), returns a lower triangular basis $\mathbf{B}'$ for the lattice generated by all integer linear combinations of $\mathbf{B}$ and $\mathbf{t}$.

(Hint: first give an algorithm that on input $(\mathbf{B}, \mathbf{t})$, returns a new pair $(\mathbf{B}', \mathbf{t}')$ such that the first coordinate of $\mathbf{t}$ is zero. Use the determinant of the lattice to make sure all numbers involved do not get too big.)

2 Linear dependencies

Consider a set of (linearly dependent) integer vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{Z}^n$ (for $k > n$), and assume for simplicity that they span the entire space $\mathbb{R}^n$. Show that the set of their integer linear combinations

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) = \{\sum_i \mathbf{b}_i x_i : \forall i. x_i \in \mathbb{Z}\}$$

is a lattice, by giving a polynomial time algorithm that on input $\mathbf{b}_1, \ldots, \mathbf{b}_k$, returns a basis for the lattice they generate. *(Hint: Find a sublattice of the form $d \cdot \mathbb{Z}^n$, and then add the $\mathbf{b}_i$ vectors to it, one at a time, using the result proved in problem 1.)*

3 Systems of equations

Consider a system of k equations in n variables

$$(i = 1, \ldots, k) \quad \sum_{j=1}^{n} a_{i,j} x_j = 0 \pmod{m_i}$$

where all $a_{i,j}$ and m_i are integers. Show that the set of integer solutions to the system is a lattice, by giving a polynomial time algorithm that on input the coefficients $a_{i,j}$ and moduli m_i, returns a lattice basis. *(Hint: consider the dual of the lattice generated by the (linearly dependent) vectors $\frac{1}{m_i}(a_{i,1}, \ldots, a_{i,n})^T$ and $(0 \ldots, 0, 1, 0, \ldots, 0)^T$.)*