The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Sunday, 06 June 2010, 23:59h.

Exercise 7.1 (The travelling salesman problem). (20 points)

In the Travelling Salesman Problem (TSP) you are given some cities and (integer) distances between them, and have to find the shortest route covering all cities or decide whether there exits a tour that is no longer than a given value. The latter decision problem is NP-complete. In the *Euclidean Travelling Salesman Problem*, the cities are given by integer coordinates in the plane, and the distance is the Euclidean distance. This problem is NP-hard but not known to be in NP. The difficulty is in deciding whether one tour is shorter than another one. This amounts to telling whether one sum of square roots (of integers) is smaller than another such sum. It is conveivable that two such sums might differ only by an exponenitally small amount, and a conjecture states that this is not possible. More precisely we let $\delta(n, C)$ be the smallest distance between two such sums with at most n terms $\sqrt{a}$, with $1 \leq a \leq C$.

(i) Give a basis for a lattice L so that two close sums as above yield a short vector in L. Hint: Construct a lattice similar to the one used for the subsetsum cryptosystem by using square-free integers only. [10]

(ii) For several values of n and C compute short vectors in L and see whether they yield two sums with small difference. Use $n = 5, 10, 15, 20$ and $C = 100, 200, 500$. [10]

Exercise 7.2 (Filling a gap). (8+3 points)

In the lecture we have claimed that for a reduced basis B of a lattice L we have for all $i \in \{1, \ldots, n\}$ that $\|b_i\| \leq 2^{\frac{n-1}{2}} \lambda_i(L)$, where n is the dimension of the lattice and λ_i is the length of the i-th successive minimum of L. In this exercise we will prove this. As usual denote by B^* the Gram-Schmidt orthogonalization of B. We start by proving that for all $i \in \{1, \ldots, n\}$ we have $\lambda_i(L) \geq \min_{i \leq j \leq n} \|b_j^*\|$. By the definition of the successive minima we know that there are n linearly independent lattice vectors $a_1, \ldots, a_n$ with $\|a_i\| = \lambda_i(L)$. Write each using our reduced basis B, i.e. $a_i := \sum_{j=1}^{n} a_{i,j} b_j$ with $a_{i,j} \in \mathbb{Z}$.

(i) Let $c_i := \max\{j \mid a_{i,j} \neq 0\}$. Show that there is a $k \leq i$ with $c_k \geq i$. [2]

(ii) Argue that then $\lambda_i(L) \geq \lambda_k(L)$. [1]

(iii) Prove that we can now express $a_k = \sum_{j=1}^{c_k} a_{k,j}^* b_j^*$ with $a_{k,j}^* \in \mathbb{R}$. Hint: Recall the properties of the Gram-Schmidt orthogonalization. [2]

(iv) Show that we have $a_{k,c_k}^* = a_{k,c_k} \in \mathbb{Z} \setminus \{0\}$. [+3]

(v) Argue that $\|a_k\| \geq |a_{k,j}^*| \cdot \|b_j^*\|$ and conclude that $\lambda_i \geq \min_{i \leq j \leq n} \|b_j^*\|$. [1]

(vi) By the definition of a reduced basis we know that for $j \geq i$ we have $\|b_i\|^2 \leq 2^{j-1} \|b_j^*\|^2$. Conclude that $\|b_i\| \leq 2^{\frac{n-1}{2}} \lambda_i(L)$. [2]