The art of cryptography: Lattices and cryptography, summer 2013

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

5. Exercise sheet
Hand in solutions until Sunday, 26 May 2013, 23:59h.

Exercise 5.1 (Filling a gap). (5 points)

Prove that in the replacement step in the lattice basis reduction algorithm the Gram-Schmidt orthogonal vectors do not change. 5

Exercise 5.2 (The basis reduction algorithm). (24+3 points)

In this exercise we will do several experiments with the lattice basis reduction algorithm. For this particular task, we need a running implementation in which we can look in.

(i) Implement the basis reduction algorithm in a programming language of your choice. Hand in the source code. 15

(ii) For several bases (the choice is up to you) compare the result of your algorithm with the result of some running library function, such as the `LLL` function in NTL. What do you observe? +2

Now consider the lattice $L = \mathcal{L}(B)$ spanned by the basis $B = \begin{bmatrix} 2 & 1 & 5 & 8 \\ 7 & 2 & 5 & 5 \\ 2 & 3 & 1 & 1 \\ 5 & 8 & 9 & 9 \end{bmatrix}$.

(iii) Minkowski's theorem states that for any lattice we have $\lambda(L) \leq \sqrt{n}\det(L)^{1/n}$. What is the value of this bound in our example? 2

(iv) What is the length of the shortest vector in the output of the basis reduction algorithm? 1

(v) What is the value of the integer $\mathcal{D} = \prod_{i=1}^{4} \det(\mathcal{L}(b_1, \ldots, b_i))^2$ for the input basis? 2

(vi) What is the number of iterations predicted by the running time analysis from the lecture? 1

(vii) What is the value of $\mathcal{D}$ upon finding a reduced basis? 1

(viii) Give an upper bound on the number of iterations based on the initial and final value of $\mathcal{D}$. 2

(ix) What is the number of iterations actually executed? +1

Exercise 5.3 (Find a correct proof). (0+7 points)

+7

Prove the following

Lemma. *Let $L \subseteq \mathbb{R}^n$ be a lattice with basis $(b_1, \ldots, b_\ell)$ and Gram-Schmidt orthogonal basis $(b_1^*, \ldots, b_\ell^*)$. Then for any nonzero $x \in L$ we have*

$$\min\{\|b_1^*\|, \ldots, \|b_\ell^*\|\} \leq \|x\|. \qquad \square$$