The art of cryptography: Lattices and cryptography, summer 2013

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

4. Exercise sheet
Hand in solutions until Sunday, 12 May 2013, 23:59h.

Exercise 4.1 (Gram-Schmidt orthogonalization). (15 points)

Consider the Gram-Schmidt orthogonalization from the lecture. Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be linearly independent, and $b_i^*, \ldots, b_\ell^*$ their Gram-Schmidt orthogonalization. For $0 \leq k \leq \ell$ let $U_k = \sum_{1 \leq i \leq k} \mathbb{R} b_i \subseteq \mathbb{R}^n$ be the $\mathbb{R}$-subspace spanned by $b_1, \ldots, b_k$.

(i) Consider the vector space $V = \operatorname{span}(B)$, spanned by the basis $\boxed{2}$

$$B := \begin{bmatrix} 2 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}.$$

Compute an orthogonal basis of V.

(ii) Show that $\sum_{1 \leq i \leq k} \mathbb{R} b_i^* = U_k$. $\boxed{3}$

(iii) Show that $b_1^*, \ldots, b_\ell^*$ are pairwise orthogonal, that is, $b_i^* \star b_j^* = 0$ if $i \neq j$. $\boxed{3}$

(iv) Show that b_k^* is the projection of b_k onto the orthogonal complement $\boxed{4}$

$$U_{k-1}^\perp = \{b \in \mathbb{R}^n : b \star u = 0 \text{ for all } u \in U_{k-1}\}$$

of U_{k-1}, and hence in particular $\|b_k^*\| \leq \|b_k\|$.

(v) Show that $\det \begin{pmatrix} b_1 \\ \vdots \\ b_\ell \end{pmatrix} = \det \begin{pmatrix} b_1^* \\ \vdots \\ b_\ell^* \end{pmatrix}$. $\boxed{1}$

(vi) Construct out of the Gram-Schmidt orthogonalization procedure a method which returns an ortho*normal* basis, i.e. an orthogonal basis B^*, where we have for all b_i^* that $\|b_i^*\| = 1$. $\boxed{2}$

Exercise 4.2 (Close vectors). (5+12 points)

In the lecture we have seen an algorithm for computing an approximation to the closest vector problem.

(i) Consider the reduced basis $B := \begin{bmatrix} 3 & 2 & 1 \\ -2 & 1 & 4 \\ -2 & 2 & -2 \end{bmatrix}$ and the vector $u = (8, 9, 10)$. $\boxed{5}$ $\boxed{+2}$

Trace the values of the algorithm by hand and give the approximate solution to the CVP.

(ii) Implement the algorithm in a programming language of your choice. Hand in the source code. $\boxed{+10}$

Exercise 4.3 (The gcd lattice revisited). (9 points)

We are now going to prove that for $\gamma > 2C$, the basis reductions will always compute the correct solution for the gcd lattice L from exercise 2.2.

1 (i) Show that every vector $v \in L$ is of the form $(v_1, v_2, \gamma(v_1 a + v_2 b))$.

1 (ii) Take any such vector with $v_1 a + v_2 b \neq 0$. Show that then $\|v\|^2 \geq \gamma^2$.

2 (iii) Now consider a reduced basis $\bar{B}$. We know from the lecture that we have $\|\bar{b}_1\| \leq \sqrt{2}\lambda_1(L)$, where $\lambda_1(L)$ is the length of a nonzero shortest vector in L. In particular it follows that $\|\bar{b}_1\| \leq \sqrt{2}\|v\|$ for any nonzero vector $v \in L$. Show that from that it follows that $\|\bar{b}_1\| \leq 2C$. Hint: Consider the vector $(-b, a, 0)$.

1 (iv) Conclude that for $\gamma > 2C$ the vector $\bar{b}_1$ is of the form $(x_1, x_2, 0)$.

We now know that we have a reduced basis $\bar{B} = \begin{bmatrix} x_1 & x_2 & 0 \\ s & t & \pm\gamma g \end{bmatrix}$. Further we know from the lecture that there is a unimodular transformation U with $\bar{B} = UB$ with $U = \begin{bmatrix} x_1 & x_2 \\ s & t \end{bmatrix}$ such that $x_1 t - x_2 s = \pm 1$. The inverse is given as $U^{-1} = \begin{bmatrix} t & x_2 \\ s & x_1 \end{bmatrix}$.

2 (v) Argue that we have $U[\gamma a, \gamma b]^T = [0, \gamma g]^T$ and conclude from it that $g = \pm\gcd(a, b)$.

2 (vi) Compare your result to the experiments you were doing in exercise 2.2 .