The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

2. Exercise sheet
Hand in solutions until Sunday, 25 April 2010, 23:59h.

Exercise 2.1 (Gram-Schmidt orthogonalization). (17+10 points)

Consider the Gram-Schmidt orthogonalization from the lecture. There we constructed, given a basis $B \in \mathbb{R}^{n \times m}$ of the vectorspace $V := \text{span}(B)$, an orthogonal basis B^* by defining $b_1^* := b_1$, $b_i^* := b_i - \sum_{j<i} \mu_{i,j} b_j^*$ with $\mu_{i,j} := \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$.

(i) Show that for $i_1 \neq i_2$ the vectors $b_{i_1}^*$ and $b_{i_2}^*$ are orthogonal. $\boxed{3}$

(ii) Show that for $i < j$ the vectors b_i and b_j^* are orthogonal. $\boxed{3}$

(iii) Consider the vector space $V = \text{span}(B)$, 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.

(iv) Is your orthogonal basis of V also a basis of $\mathcal{L}(B)$? Justify your answer. $\boxed{2}$

(v) Define the orthogonal projection operator of $\mathbb{R}^n$ to $\text{span}(b_i^*, \ldots, b_n^*)$ as $\boxed{4}$

$$\pi_i(x) := \sum_{i \leq j \leq n} \frac{\langle x, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*.$$

Show that $b_i^* = \pi_i(b_i)$.

(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 $\|b_i^*\| = 1$. $\boxed{3}$

(vii) Implement Gram-Schmidt in a programming language of your choice! Hand in the source code. $\boxed{+10}$

Exercise 2.2 (A note on the volume). (5 points)

Let $B \in \mathbb{R}^{n \times m}$ a basis of the lattice $L = \mathcal{L}(B)$ and let B^* be the Gram-Schmidt matrix of B. We have defined the determinant of the lattice as $\det(L) = \text{vol}(P(B)) = \sqrt{\det(B^T B)}$. Prove that $\det(L) = \prod_i \|b_i^*\|$. Hint: Use the fact that $B^* = BT$ for some upper triangular matrix T with $T_{i,i} = 1$ for all $i = 1 \ldots m$. $\boxed{5}$

Exercise 2.3 (The orthogonalized centered parallelepiped). (3 points)

Let B be a basis of the lattice $L = \mathcal{L}(B)$ and let B^* be the Gram-Schmidt matrix of B. 3

(i) Show that the parallelepiped

$$P(B) := \{Bx \,|\, x_1, \ldots, x_m \in [0, 1)\}$$

is a fundamental region of the lattice.

(ii) Show that the orthogonalized centered parallelepiped

$$C(B^*) = \{B^*x \,|\, x_1, \ldots, x_m \in [-1/2, 1/2)\}$$

is a fundamental region of the lattice. Hint: You may use again the fact that $B^* = BT$ for some upper triangular matrix T.

Exercise 2.4 (Orthogonal sublattices). (4 points)

4 We will show here that – although not every lattice has an orthogonal basis – every integer lattice has an orthogonal sublattice. More specifically we will show that for any nonsingular $B \in \mathbb{Z}^{m \times m}$ with $d := |\det(B)|$ we have $d\mathbb{Z}^n \subseteq \mathcal{L}(B)$. Consider a vector $v = dy \in d\mathbb{Z}^n$. Show, using Cramer's rule, that $v \in \mathcal{L}(B)$.

Exercise 2.5 (A glimpse on the applications of basis reduction). (0+7 points)

In this exercise we will explore the power of the basis reduction algorithm. We will show that we can write every prime p for which $p \equiv 1 \pmod 4$ as the sum of two squares, i.e. that there are integers $a, b \in \mathbb{Z}$ with $p = a^2 + b^2$. This seems to be a difficult problem, but it is so easy to solve using lattices!!!

+2 (i) Show that if $p \equiv 1 \pmod 4$ there is an element $i \in \mathbb{F}_p$ with $i^2 = -1$. Hint: Little Fermat, for all $a \in \mathbb{F}_p^\times$ we have $a^{p-1} = 1$.

We consider now the two dimensional lattice $L = \mathcal{L}(B)$ spanned by the basis

$$B = \begin{bmatrix} 1 & 0 \\ i & p \end{bmatrix}$$

+2 (ii) Show that every element $[a, b]^T \in L$ has the property that $a^2 + b^2$ is a multiple of p.

Now the magic of lattice basis reduction applies: If we find a reduced basis of L, we know from the lecture that $\|b_1\| \leq \alpha^{1/4} \det(B)^{1/2}$ where $\alpha = \frac{1}{\delta - 1/4}$ and δ is the paramteter of the lattice reduction algorithm.

+3 (iii) Use this fact to observe that for $\delta > 3/4$ the short vector b_1 found by the algorithm gives you an algorithmic solution to the problem of writing the prime p as the sum of two squares.