The art of cryptography: Lattices and cryptography, summer 2013

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

9. Exercise sheet
Hand in solutions until Sunday, 23 June 2013, 23:59h.

Exercise 9.1 (The α-GapSVP). (6 points)

Consider the following definition of the α-GapSVP problem:

Definition. *For a function $\alpha\colon \mathbb{N} \longrightarrow \mathbb{R}$ with $\alpha(n) \geq 1$ for all n, we define the α-gap shortest vector problem α-GapSVP as follows. Input is a basis A of an n-dimensional lattice L and a positive real number d. The answer is*

$$\begin{cases} \textit{yes} & \textit{if } \lambda_1(L) \leq d, \\ \textit{no} & \textit{if } \lambda_1(L) \geq \alpha(n) \cdot d. \end{cases}$$

When $d < \lambda_1(L) < \alpha(n) \cdot d$, any answer is permitted.

(i) Give an algorithm that approximates $\lambda_1(L)$ by binary search on d using a subroutine for α-GapSVP. $\boxed{4}$

(ii) How good did your algorithm approximate $\lambda_1(L)$? $\boxed{2}$

Exercise 9.2 (Integer factorization revisited). (12 points)

In the course we have seen that $\sqrt{n}$-SVP lies in the complexity class $\mathrm{NP} \cap \mathrm{coNP}$.

(i) Consider the following problem $\mathcal{A}$: Given $(N, m) \in \mathbb{N}^2_{>1}$ decide whether N has a prime factor smaller than m. Prove that this problem is in $\mathrm{NP} \cap \mathrm{coNP}$. Hint: Use the fact that deciding primality is in P. $\boxed{8}$

(ii) Construct an algorithm that produces, given an integer N, a prime factorization of N using an oracle for problem $\mathcal{A}$. $\boxed{4}$

Exercise 9.3 (Gaussian distributions). (8 points)

In the lecture we discussed the Gaussian distributions

$$\varrho_r^{(n)}\colon \begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R}, \\ x & \longmapsto & \frac{1}{r^n} \exp\left(-\pi \left(\frac{\|x\|}{r}\right)^2\right) \end{array}.$$

(i) Draw a meaningful plot of the functions $\varrho_r^{(1)}$ and $\varrho_r^{(2)}$ for $r = 0.5, 1, 2, 10$. $\boxed{2}$

(ii) Plot for the same values of r the cumulative distribution $\int_{-\infty}^{x} \varrho_r^{(1)}(t)\,\mathrm{d}\,t$. $\boxed{2}$

We now consider the distribution τ_r on the torus $\mathbb{T} := \mathbb{R}/\mathbb{Z}$ induced by the distribution $\varrho_r^{(1)}$ via the canonical projection of $\mathbb{R}$ into $\mathbb{T}$.

(iii) Express formally τ_r in terms of $\varrho_r^{(1)}$. $\boxed{2}$

(iv) Plot the induced Gaussian distribution on $\mathbb{T}$ for the above values of r. $\boxed{2}$