The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Sunday, 11 July 2010, 23:59h.

Exercise 12.1 (Gaussian distributions). (8 points)

In the lecture we discussed the Gaussian distributions

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

(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. $\boxed{2}$

Exercise 12.2 (Δ of two balls). (8+5 points)

Let $B_n = \{x \in \mathbb{R}^n : \|x\| \leq 1\}$ be the n-dimensional unit ball. Consider two 2-dimensional balls of radius $\sqrt{2}$ whose distance of the centers is exactly 1. For example consider the two balls $\sqrt{2}B_2$ and $(0,1) + \sqrt{2}B_2$. In the lecture we defined for two probability distributions X and Y over a set S their *statistical distance* $\Delta(X, Y)$ as

$$\Delta(X, Y) = \max\{|X(A) - Y(A)| : A \subset S\}.$$

Consider here the distributions $X = \mathcal{U}(\sqrt{2}B_2)$ and $Y = \mathcal{U}((0,1) + \sqrt{2}B_2)$.

(i) Draw a picture of the two balls. Where in the picture do you find the statistical difference $\Delta(X, Y)$? $\boxed{3}$

(ii) Compute $\Delta(X, Y)$. Hint: You need a bit basic calculus here. Parametrize the balls by appropriate functions in one variable and compute some areas. $\boxed{5}$

(iii) What do you observe when you vary the radius and the distance? Perform experiments! $\boxed{+5}$

Exercise 12.3 (The α-GapSVP). (6 points)

In the lecture we encountered 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 positiv 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.

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

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