The art of cryptography: Lattices and cryptography, summer 2013

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

10. Exercise sheet
Hand in solutions until Sunday, 30 June 2013, 23:59h.

Exercise 10.1 (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 $\Delta(X, Y)$? $\boxed{2}$

(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. $\boxed{6}$

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

Exercise 10.2 (Amplification — or: A little bit better than guessing is enough). (12 points)

Think of a boolean variable T and an algorithm $\mathcal{A}$ with output A and a probability slightly better than guessing to determine the value of T, i.e.

$$p = \text{prob}(A = T) > \frac{1}{2}.$$

Imagine a new algorithm $\mathcal{B}$ which calls $\mathcal{A}$ m-times and outputs B as the majority of the As – returning failure in the event of a draw.

(i) Prove that $\boxed{4}$

$$\text{prob}(B == T) > \sum_{m/2 < i \leq m} \binom{m}{i} p^i (1-p)^{m-i}$$

and give a simple – but still useful – lower bound for the sum. (Hint: Use the Chernoff bound)

(ii) How many repetitions m do you need for $p = 0.6, 0.7, 0.8$ in order to guarantee $\text{prob}(B = T) > 0.9$. $\boxed{4}$

(iii) Let $p = \frac{1}{2} + \frac{1}{n}$. Determine a number of repetitions such that $\boxed{4}$

$$\text{prob}(B = T) > 1 - e^{-cn}$$

for some constant $c > 0$.