Test/Homework 1 - Prerequisites

Cryptography and Security 2020

- Homework submission deadline: **25.09.2020**

Exercise 1 Probabilities

A disease is infecting a population. The government decides it needs to know the extent of the disease and starts testing the population. They develop a test that is 99% accurate. More specifically, if you have the disease it will be positive 99% of the times, and show a false negative 1% of the times. If you do not have the disease, it will give a negative result 99% of the time but show a false positive 1% of the times. Overall, the disease infects 1% of the population.

Question 1.1 Reliability of the test

You (a random member of the population) have now taken the test, and it comes back positive! What is the probability of you having the disease?

Question 1.2 A new test

The Ecole Polytechnique Fédérale d'Ecublens decides to improve the test. This new test applies n times (you can assume n even) the old test and outputs *positive* iff **at least** $\frac{n}{2}$ of the old tests output *positive*. Using Markov's inequality, give an upper bound on the probability that this new test outputs a false positive. What do you think of the resulting bound when n grows, is it tight?
Hint: Assume that the outputs of the old tests are mutually independent, conditioned on the fact that the patient has (not) the disease.

Exercise 2 Euclidean Domains

Let $\mathcal{R}$ be a commutative ring which has a multiplicative neutral element, i.e $1 \in \mathcal{R}$. $\mathcal{R}$ is called a Euclidean domain if $\exists d : \mathcal{R}\backslash\{0\} \to \mathbb{Z}^+$ such that the following properties hold.

1. $\forall a, b \in \mathcal{R}\backslash\{0\}$ there exist $m, r \in \mathcal{R}$ such that $a = bm + r$ and either $r = 0$ or $d(r) < d(b)$
2. $\forall a, b \in \mathcal{R}\backslash\{0\}$, $d(a), d(b) \leq d(ab)$
3. $\exists a \in \mathcal{R}\backslash\{0\}$ s.t. $d(a) \neq 0$

Answer the following questions regarding Euclidean domains.

Question 2.1 Polynomial Rings

Let $\mathcal{R} = K[x]$ where K is a field.

1. Prove that $\mathcal{R}$ is a Euclidean domain.
2. Is the multivariate polynomial ring $K[x_1, x_2]$ also a Euclidean domain?

Justify your answers.

Question 2.2 PI property

Let $\mathcal{R}$ be a Euclidean domain. Prove that every ideal $I \leq \mathcal{R}$ is generated by a single element, i.e $I = x\mathcal{R}$ for some x.

hint: Take $x \in I$ such that $d(x)$ is the minimum in I.

Question 2.3 GCD

Let $\mathcal{R}$ be a Euclidean domain. $c \in \mathcal{R}$ is called the GCD of $a, b \in \mathcal{R}$ if for all ideals $I \leq \mathcal{R}$ such that $a, b \in I$, $c\mathcal{R} \subseteq I$, i.e $a\mathcal{R} + b\mathcal{R} = c\mathcal{R}$.

1. Is this notion compatible with the notion of GCD in $\mathbb{Z}$?
2. Modify the extended Euclidean algorithm such that it will output GCD of two elements $a, b \in \mathcal{R}$.

hint: How can you replace the comparison steps in the extended Euclidean algorithm using the d function?

Exercise 3 Mastering recursivity

Let $b, c > 0$ and $d \geq 0$ be real numbers and let $S, T \colon \mathbb{N} \longrightarrow \mathbb{N}$ be functions such that:

1. $S(2n) \geq cS(n)$ for all $n \in \mathbb{N}$,
2. $T(1) = d$ and $T(n) \leq bT(n/2) + S(n)$ for all $k \in \mathbb{N}$ and $n = 2^k$.

Question 3.1 Finite regime analysis

Show that the following assertion holds for all $k \in \mathbb{N}$ and $n = 2^k$:

$$T(n) \leq \begin{cases} dn^{\log b} + S(n) \log n & \text{if } b = c, \\ dn^{\log b} + \frac{c}{b-c} S(n) \left(n^{\log(b/c)} - 1 \right) & \text{if } b \neq c. \end{cases} \tag{1}$$

Question 3.2 Asymptotic behaviour

Assume that S and T are non-decreasing functions satisfying $S(1) > 0$ and such that there exists $\varepsilon > 0$ such that $S(2n) \leq \varepsilon S(n)$ for all $n \in \mathbb{Z}_+$. Show that the following assertion holds:

$$T(n) \in \begin{cases} O\left(S(n) \log n\right) & \text{if } b = c, \\ O\left(S(n) n^{\log(b/c)}\right) & \text{if } b \neq c. \end{cases} \tag{2}$$

Question 3.3 Application

Let R be an arbitrary commutative ring with unit and consider the following algorithm for multiplying two polynomials f and g in $R[x]$ of degrees **strictly less than** $n = 2^k$ (by convention, the zero polynomial has degree $-\infty$).

Algorithm 1 karatsuba(f, g)

```
if $n = 1$ then
    Compute the product $h = fg$ of $f$ and $g$ as elements in $R$.
    return $h$
end if
$f \to F_1 x^{n/2} + F_0$
$g \to G_1 x^{n/2} + G_0$
$h_0 \leftarrow$ karatsuba$(F_0, G_0)$
$h_1 \leftarrow$ karatsuba$(F_1, G_1)$
$h_2 \leftarrow$ karatsuba$(F_0 + F_1, G_0 + G_1)$
$h \leftarrow h_1 x^n + (h_2 - h_1 - h_0) x^{n/2} + h_0$
return $h$
```

1. Show that Karatsuba's algorithm is correct.

2. Assuming that the decomposition $f \to F_1 x^{n/2} + F_0$ has a negligible cost, use (1) to show that Karatsuba's algorithm requires at most $9n^{\log 3} - 8n$ ring operations in R. *For this question only, you may assume that (2) holds even if you failed to prove the result.*

3. Deduce that Karatsuba's algorithm requires $O(n^{1.59})$ ring operations.