

F. Autreau

P. Lafourcade

JL. Roch

P. Lafourcade.

SET 2

Date: 27.09.2007

Exercise 1

Let f and g be two negligible functions, then

1. $f.g$ is negligible.
2. For any $k > 0$, f^k is negligible.
3. For any λ, μ in \mathbb{R} , $\lambda.f + \mu.g$ is negligible.

Exercise 2

Prove that X and Y are independent if and only if for all values x taken by X with non-zero probability, the conditional distribution of Y given the event $X = x$ is the same as the distribution of Y .

Exercise 3

Consider the algorithm $D2$ that outputs 1 iff the input string contains more zeros than ones. If $D2$ can be implemented in polynomial time, then prove that X and Y are polynomial-time-indistinguishable.

Exercise 4

Let $X := \{X_n\}_{n \in \mathbb{N}}$, $Y := \{Y_n\}_{n \in \mathbb{N}}$ and $Z := \{Z_n\}_{n \in \mathbb{N}}$ three ensembles. If X and Y are indistinguishable in polynomial time, Y and Z are indistinguishable in polynomial time then X and Z are indistinguishable in polynomial time.

Exercise 5

Recall that the distributions D_0, D_1 are said to be indistinguishable ($0 \leq \epsilon \leq 1$) if

$$|Pr[A(x_0) = 1] - Pr[A(x_1) = 1]| \leq \epsilon$$

holds for all adversaries A running in time at most t , where the random variable x_0 is distributed according to D_0 and x_1 is distributed like D_1 .

Now, let's call the distributions D_0, D_1 inseparable just if

$$\frac{1}{2} - \frac{\epsilon}{2} \leq Pr[A(x) = b] \leq \frac{1}{2} + \frac{\epsilon}{2}$$

holds for all adversaries A running in time at most t , where the random variable b is a uniformly random bit and where the random variable x is distributed according to D_b . This is a very natural notion, because it talks about our chances of guessing correctly which distribution x came from, and whether we can do much better than simply flipping a coin.

Prove: D_0, D_1 are indistinguishable if and only if they are inseparable. (Hence the notion of inseparability is redundant.)