

UNIVERSITÉ DE GENÈVE

MULTIMEDIA SECURITY AND PRIVACY

14x016

---

## TP 3 : Elements of Detection Theory

---

*Author:* Deniz Sungurtekin

*E-mail:* [Deniz.Sungurtekin@etu.unige.ch](mailto:Deniz.Sungurtekin@etu.unige.ch)

April 2020



**UNIVERSITÉ  
DE GENÈVE**

---

**FACULTÉ DES SCIENCES**  
Département d'informatique

# 1 Exercises

## 1.1

Let  $X \sim \mathcal{N}(0, 1)$  and  $Y \sim \mathcal{N}(0, 3)$  :

$$P[-2 < Y \leq 1] : \quad (1)$$

$$\Rightarrow \{(-2 - (0))/3 < N \leq (1 - 0)/3\} : \quad (2)$$

$$\Rightarrow P[-2/3 < N \leq 1/3] = \phi(1/3) - \phi(-2/3) = \phi(1/3) - (1 - \phi(2/3)) = 0.63 - (1 - 0.74) = 0.37 \quad (3)$$

$$P[Y > 5.5] = 1 - P[Y \leq 5.5] : \quad (4)$$

$$P[Y \leq 5.5] = \phi(5.5/3) = 0.96 \quad (5)$$

$$\Rightarrow 1 - 0.96 = 0.04 \quad (6)$$

$$P[-2 < X \leq 2] : \quad (7)$$

$$\Rightarrow P[-2 < N \leq 2] = \phi(2) - (1 - \phi(2)) = 0.97 - 0.03 = 0.94 \quad (8)$$

$$P[X > 1.5] = 1 - P[X \leq 1.5] : \quad (9)$$

$$\Rightarrow P[X \leq 1.5] = \phi(1.5) = 0.93 \quad (10)$$

$$\Rightarrow 1 - 0.93 = 0.07 \quad (11)$$

## 1.2

Let  $X$  denote the peak temperature in Geneva, in June, as measured in Celsius, for which holds:  $X \sim N(27, 9)$ . What is:

$$P[X > 35] = 1 - P[X \leq 35] : \quad (12)$$

$$P[X \leq 35] = \phi((35 - 27)/9) = 0.81 \quad (13)$$

$$\Rightarrow 1 - 0.81 = 0.19 \quad (14)$$

$$P[X \leq 5] = \phi((5 - 27)/9) = \phi(-2.4) = 1 - \phi(2.4) = 0.01 \quad (15)$$

$$P[20 < X \leq 40] = P[((20 - 27)/9) < N \leq ((40 - 27)/9)] = P[-7/9 < N \leq 13/9] \quad (16)$$

$$= \phi(13/9) - \phi(-7/9) = \phi(13/9) - (1 - \phi(7/9)) = 0.91 - (1 - 0.77) = 0.68 \quad (17)$$

### 1.3

Let  $X$  be a Gaussian random variable, for which  $E[X] = 0$  and  $P[|X| \leq 10] = 0.3$ . What is  $\sigma_X$ ?

$$P[|X| \leq 10] = P[-10 \leq X \leq 10] = P[-10/\sigma \leq N \leq 10/\sigma] \quad (18)$$

$$= \phi(10/\sigma) - (1 - \phi(10/\sigma)) = 0.3 \quad (19)$$

$$\Rightarrow \phi(10/\sigma) = 0.65 \quad (20)$$

$$\Rightarrow 10/\sigma \cong 0.4 \quad (21)$$

$$\Rightarrow \sigma = 25 \quad (22)$$

### 1.4

Prove that:

$$Q(n) = \frac{1}{2} \operatorname{erfc}\left(\frac{n}{\sqrt{2}}\right) :$$

$$\Rightarrow Q(n) = \frac{1}{\sqrt{2\pi}} \int_n^\infty e^{-\frac{x^2}{2}} dx = \frac{1}{2} \left( \frac{2}{\sqrt{\pi}} \int_{n/\sqrt{2}}^\infty \exp(-x^2) dx \right) \quad (23)$$

$$= \frac{1}{2} - \frac{1}{2} \operatorname{erf}\left(\frac{n}{\sqrt{2}}\right) = \frac{1}{2} \operatorname{erfc}\left(\frac{n}{\sqrt{2}}\right) \quad (24)$$

### 1.5

Let there be two hypotheses,  $H_0$  and  $H_1$ :

$$H_0 : X = Z$$

$$H_1 : X = \mu 1 + Z$$

where  $Z \sim N(0, 1)$  and  $\mu 1 = 1$ .

Determine the separation threshold  $\tau$  following the MAP hypothesis, or likelihood ratio test:

We have that  $X \sim \mathcal{N}(0, 1)$  with hypothesis 0 and  $X \sim \mathcal{N}(1, 1)$  with hypothesis 1:

$$x \in A_0, \text{ if } x \leq \frac{e^{-\frac{x^2}{2\sigma^2}}}{e^{-\frac{(x-1)^2}{2\sigma^2}}} \geq \frac{P[H_1]}{P[H_0]}$$

$$x \in A_0, \text{ if } x \leq \ln\left(\frac{P[H_1]}{P[H_0]}\right) \frac{2\sigma^2 + 1}{-2}$$

$$x \in A_0, \text{ if } x \leq \tau$$

Determine the probability of correct detection  $p_d = 1 - p_m$ :

$$p_d = 1 - P(A_0|H_1) = 1 - \int_{x < \tau} f_{x|H_1}(x) dx = 1 - \phi(\tau - 1)$$

## 1.6

Derive the general formula's for the Probability of Miss,  $p_m$ , the Probability of correct detection,  $p_d$ , and the Probability of False Alarm,  $p_f$  :

$$p_d = 1 - P(A_0|H_1) = 1 - \int_{x < \tau} f_{x|H_1}(x)dx = 1 - \phi(\tau - \mu_1)$$

$$p_m = P(A_0|H_1) = \phi(\tau - \mu_1)$$

$$p_f = P(A_1|H_0) = 1 - \phi(\tau)$$

Receiver Operating Characteristic (ROC) curve for each different value of  $\mu_1 = 0, 1, 2$ :

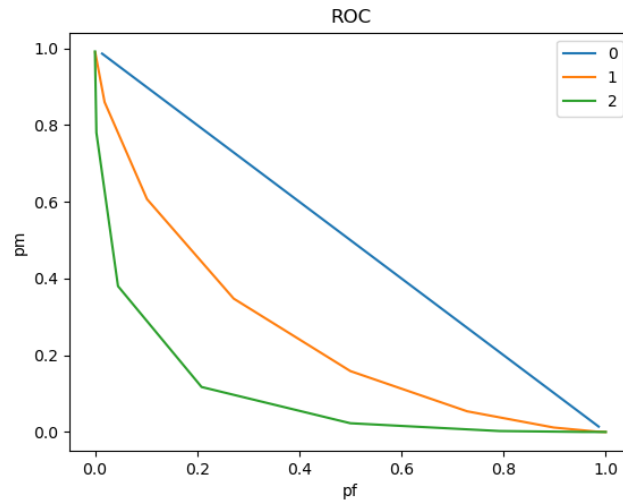


Figure 1: ROC

We clearly observe that for  $\mu_1 = 0$ ,  $pf = 1 - pm$ . The more  $\mu_1$  is big the more the  $pm$  decrease quickly over the  $pf$ . It can be explained by the fact that we centralize  $\tau$  by  $\mu_1$  so the obtained  $pm$  by using  $\phi$  is much smaller. Furthermore, the bigger is  $\mu_1$  the bigger is the  $p_d$ .

## 1.7

Formulate hypotheses  $H_0$  and  $H_1$ :

$$H_0: Y = W$$

$$H_1: Y = V + W$$

Use the binary hypothesis likelihood ratio test to determine the rule that minimises  $p_{err}$ , the probability of a decoding error:

$$x \in A_0, \text{ if } y \leq \frac{f_{Y|H_0}}{f_{Y|H_1}} \quad (25)$$

$$x \in A_0, \text{ if } y \leq \frac{e^{-y}}{ye^{-y}} \quad (26)$$

$$\Rightarrow y \leq \frac{1}{y} \quad (27)$$

$$\Rightarrow \tau = 1 \quad (28)$$

Determine  $p_{err}$  for the optimum decision rule:

$$p_{err} = p_m p(H_1) + p_f p(H_0) = p_m 0.5 + p_f 0.5 \quad (29)$$

$$\Leftrightarrow p_f = \int_{y>\tau} f_{Y|H_0} = 0.36 \Leftrightarrow p_m = \int_{y<\tau} f_{Y|H_1} = 0.26 \Rightarrow p_{err} = 0.5 * 0.26 + 0.5 * 0.36 = 0.31 \quad (30)$$