QIF 2021/1 Solution to First Exam

Question 1 (6 marks)

a) Set of actions is $W = \{ES, MG, RJ, SP\}$

Gain function is $g: W \times X \to [0,1]$ s.t.

$$g(s, X) = \begin{cases} 1, & \text{if there's } x \in X \text{ s.t. } x[\text{name}] = \text{Mário and } x[\text{state}] = s; \text{ or} \\ 0, & \text{otherwise} \end{cases}$$

b) Set of actions is $W = \{n \mid n \text{ is a name}\}$

Gain function is $g: W \times X \to [0,1]$ s.t.

$$g(n, X) = \begin{cases} 1, & \text{if } \exists x \in X \text{ s.t. } x[\text{name}] = n, \\ & x[\text{generation}] = \text{millenial and} \\ & x[\text{jeans}] = \text{baggy}. \\ 1/2, & \text{if } \exists x \in X \text{ s.t. } x[\text{name}] = n \\ & x[\text{generation}] = \text{gen-z and} \\ & x[\text{jeans}] = \text{skinny} \\ 0, & \text{otherwise}. \end{cases}$$

Question 2 (6 marks)

Let's find the reduced matrices for C and D.

In C we notice that column C_{-y_3} is four times column C_{-y_2}, so they can be merged. Hence the reduced channel C^r is:

C^r

x_1	2/3	1/3
x_2	1/3	2/3

As for D, columns D_{-z_2} and D_{-z_3} are similar, and can be merged to obtain the reduced channel:

D^r

x_1	2/3	1/3
x_2	1/3	2/3

Now, since $C^r = D^r$ we know that C and D represent the same abstract channel and, hence, present identical behavior with respect to additive and multiplicative leakage.

Question 3 (10 marks)

a) In the absence of any extra information it's reasonable to assume a uniform prior $\pi = (1/2, 1/2)$ on the secret set $X = \{0.3, 0.7\}$.

In this case the prior Bayes vulnerability is

$V_1(\pi) = 1/2$.

b) The output set for the channel is

$$Y = \{HH, HT, TH, TT\},$$

in which each entry represents the result of the first flip followed by the result of the second flip. Here H stands for heads, and T stands for tails. Now channel C is:

C	H H	H T	T H	T T
0.3	0.09	0.21	0.21	0.49
0.7	0.49	0.21	0.21	0.09

c) Finding the joint:

$J = \pi \triangleright C =$

π
1/2
1/2

$\triangleright$

C	H H	H T	T H	T T
0.3	0.09	0.21	0.21	0.49
0.7	0.49	0.21	0.21	0.09

$=$

J	H H	H T	T H	T T
0.3	9/200	21/200	21/200	49/200
0.7	49/200	21/200	21/200	9/200

$=$

J	H H	H T	T H	T T
0.3	0.045	0.105	0.105	0.245
0.7	0.245	0.105	0.105	0.045

Now the hyper $[\pi \triangleright C]$ is:

$[\pi \triangleright C]$	29/100	42/100	29/100
0.3	9/58	1/2	49/58
0.7	49/58	1/2	9/58

$=$

$[\pi \triangleright C]$	0.29	0.42	0.29
0.3	0.155	0.5	0.845
0.7	0.845	0.5	0.155

d) $V_1[\pi \triangleright C] = \sum_y \max_x J_{x,y}$

$= 49/200 + 21/200 + 21/200 + 49/200$

$= 7/10 = 0.70$

Hence additive Bayes leakage is

$\mathcal{L}_1^+(\pi, C) = V_1[\pi \triangleright C] - V_1(\pi)$

$= 0.70 - 0.50 = 0.20$,

and it means that by observing the results of 2 coin flips the adversary's probability of correctly guessing the type of the coin in one try increases in absolute value by 0.20

As for multiplicative leakage,

$\mathcal{L}_1^\times(\pi, C) = V_1[\pi \triangleright C] / V_1(\pi) = 0.70 / 0.50 = 1.40$,

meaning that the relative increase is of 1.4.

Question 4 (3 marks)

Assume π is a point distribution on some value $x' \in \mathcal{X}$, i.e., $\pi = [x']$ s.t. $\pi_x = \begin{cases} 1, & \text{if } x = x' \\ 0, & \text{if } x \neq x'. \end{cases}$

Then, for any gain function $g : \mathcal{W} \times \mathcal{X} \to \mathbb{R}$ we have:

$$\begin{aligned} V_g(\pi) &= \max_w \sum_x \pi_x \, g(w,x) && \text{(Def. of } V_g\text{)} \\ &= \max_w g(w,x') && \text{(π_x is a point on x')} \end{aligned}$$

Moreover, for any gain function g and channel $C : \mathcal{X} \to \mathbb{D}\mathcal{Y}$:

$$\begin{aligned} V_g[\pi \triangleright C] &= \sum_y \max_w \sum_x \pi_x C_{xy} \, g(w,x) && \text{(Def. of } V_g\text{)} \\ &= \sum_y \max_w C_{x'y} \, g(w,x') && \text{(π is a point on x')} \\ &= \sum_y C_{x'y} \max_w g(w,x') && \text{(C_{xy} is independent of } \max_w\text{)} \\ &= \max_w g(w,x') \cdot \sum_y C_{x'y} && \left(\max_w g(w,x') \text{ is independent of } \sum_y\right) \\ &= \max_w g(w,x') && \left(\sum_y C_{x'y} = 1\right) \\ &= V_g(\pi) && \text{(derivation above).} \end{aligned}$$

Now, since $V_g(\pi) = V_g[\pi \triangleright C]$ for all π, C, we have that multiplicative leakage will be always 1, and additive leakage will be always 0. ∎