Information Theory **DCC/ICEx/UFMG**
Prof. Mário S. Alvim **2017/02**

SOLUTION OF HOMEWORK

Advanced Information Measures
(Based on slide-set)

Necessary reading for this assignment:

- *Slide-set of the lecture on Advanced Information Measures*

Note: The exercises are labeled according to their level of difficulty: `[Easy]`, `[Medium]` or `[Hard]`. This labeling, however, is subjective: different people may disagree on the perceived level of difficulty of any given exercise. Don't be discouraged when facing a hard exercise, you may find a solution that is simpler than the one the instructor had in mind!

Review questions.

1. Answer formally the following questions.

   (a) Explain how probability distributions can be used to represent an agent's state of knowledge about the world.

   Instructor's solution: Given a set $\mathcal{X}$ of possible secret values, let us denote by $\mathbb{D}\mathcal{X}$ the set of all possible probability distributions over $\mathcal{X}$. An agent's state of knowledge about secrets can be represented by a probability distribution $\pi \in \mathbb{D}\mathcal{X}$.

   (b) What is a (prior) information measure? Explain what type of function it is (its domain and co-domain, and what it is supposed to mean).

   Instructor's solution: An information measure is a function that maps a state of knowledge to a real number.
   If the state of knowledge is a probability distribution on secrets, then an information measure has type $\mathbb{D}\mathcal{X} \to \mathbb{R}$, and the measure corresponds to the adversary's prior information about the secret.

   (c) Explain the essential components of a complete definition of an information measure: its mathematical definition, and operational significance.

   Instructor's solution: The mathematical definition of an information measure is a formula that allows us to compute the value of the measure for every possible input.
   The operational significance of the information measure is an interpretation of what the real number returned by the measure represents in the real world.

   (d) Give the formal definition and operational significance of the following information measures.

      i. Shannon entropy.

Instructor's solution: Shannon entropy is a function of type $\mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as

$$H(\pi) = -\sum_{x \in \mathcal{X}} \pi_x \log_2 \pi_x.$$

Its operational significance is the expected number of questions needed for an adversary to find out the value of the secret in an optimal binary search on the space of secrets.

ii. Bayes vulnerability.

Instructor's solution: Bayes vulnerability is a function of type $\mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as

$$V(\pi) = -\max_{x \in \mathcal{X}} \pi_x.$$

Its operational significance is the probability that an adversary can guess the value of the secret correctly in one try.

iii. Guessing entropy.

Instructor's solution: Guessing entropy is a function of type $\mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as

$$G(\pi) = \sum_{k} \pi_k \cdot k,$$

where k is an non-increasing ordering of π_i. Its operational significance is the expected number of guesses needed in an optimal linear search for the correct secret value.

(e) Give the formal definition of a g-vulnerability, and explain how it can be used to model different operational scenarios.

Instructor's solution: Let $\mathcal{X}$ be the set of secrets the adversary can exploit, and $\mathcal{W}$ be the set of possible actions that the adversary could make. Let $g : \mathcal{W} \times \mathcal{X} \to \mathbb{R}$ be a gain-function such that $g(w, x)$ represents the gain or benefit for the adversary when they take action $w \in \mathcal{W}$ and the secret takes value $x \in \mathcal{X}$.
The g-vulnerability of a distribution $\pi \in \mathbb{D}\mathcal{X}$ is an information measure defined as

$$V_g(\pi) = \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x g(w, x),$$

and its operational significance is the expected gain of a rational adversary taking a best action.

(f) What is the effect of a channel on the adversary's state of knowledge about a secret value? More precisely, how the posterior knowledge of an adversary can be represented, after they have observed the output of a channel?

Instructor's solution: The effect of a channel is to map the prior knowledge of the adversary about the secret value—represented as a probability distribution on secrets—to a new state of knowledge consisting in a collection of conditional probability distributions on secret values, one for every possible observation the channel permits. Each observation has its own probability of happening.
More formally, if $\mathcal{X}$ is the set of channel inputs and $\mathcal{Y}$ is the set of channel outputs, the posterior knowledge is a collection of conditional probability distributions $p_X(\text{cot} \mid Y = y)$ for every $y \in \mathcal{Y}$, each of them having probability $p(y)$ of happening.
One way of representing posterior knowledge is as a hyper-distribution, which is a distribution on distributions on secret values.

(g) How can the g-vulnerability framework be used to measure the amount of information contained in the adversary's posterior state of knowledge? More precisely, define the concept of posterior g-vulnerability.

Instructor's solution: Given prior π, gain function g, and channel matrix C from $\mathcal{X}$ to $\mathcal{Y}$, we have that the posterior g-vulnerability is an information measure of type $\mathbb{D}^2\mathcal{X} \to \mathbb{R}$ defined as

$$V_g\left[\pi\rangle C\right] = \sum_{\substack{y \in \mathcal{Y} \\ p(y) \neq 0}} p(y) V_g(p_{X|y}).$$

Its operational significance is a rational adversary's expected optimal gain over all possible channel outputs.

(h) How is the leakage of information of a channel, given a prior distribution on secrets, defined? What does it represent?

Instructor's solution: Given prior distribution π, gain function g, and channel C, multiplicative g-leakage is given by

$$\mathcal{L}_g^{\times}(\pi, C) = \frac{V_g\left[\pi\rangle C\right]}{V_g(\pi)},$$

and additive g-leakage is given by

$$\mathcal{L}_g^{+}(\pi, C) = V_g\left[\pi\rangle C\right] - V_g(\pi).$$

Leakage represents the amount by which the observation of the channel's output increases the adversary's information about the secret input.

Multiplicative leakage represents the ratio of increase in information, whereas additive leakage represents the absolute increase in information.

Exercises.

2. Consider the following piece of code in a pseudo-language.

```
if X mod 2 = 0
      Y := X
   else
      Y := 0
```

Assume that the variable X can take values in the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

(a) Give an information-theoretical channel that represents the behavior of this piece of code. You must provide the channel input and output sets, and the channel matrix.

Instructor's solution: The input set is $\mathcal{X} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, the output set is $\mathcal{Y} = \{0, 2, 4, 6\}$, and the channel matrix is

C	$Y=0$	$Y=2$	$Y=4$	$Y=6$
$X=0$	1	0	0	0
$X=1$	1	0	0	0
$X=2$	0	1	0	0
$X=3$	1	0	0	0
$X=4$	0	0	1	0
$X=5$	1	0	0	0
$X=4$	0	0	0	1
$X=5$	1	0	0	0

(b) Assume the adversary's prior knowledge about the secret value is represented by the uniform prior probability distribution π over all secret values.
Give the adversary's corresponding posterior state of knowledge after the secret is run through channel C.

Instructor's solution: Given the uniform prior

$$\pi = (1/8, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8),$$

and the channel matrix C above, we can compute the joint matrix J below

J	$Y=0$	$Y=2$	$Y=4$	$Y=6$
$X=0$	$1/8$	0	0	0
$X=1$	$1/8$	0	0	0
$X=2$	0	$1/8$	0	0
$X=3$	$1/8$	0	0	0
$X=4$	0	0	$1/8$	0
$X=5$	$1/8$	0	0	0
$X=4$	0	0	0	$1/8$
$X=5$	$1/8$	0	0	0

,

which is then converted into the following state of posterior knowledge

posterior distributions	$p(X \mid Y=0)$	$p(X \mid Y=2)$	$p(X \mid Y=4)$	$p(X \mid Y=6)$
$X=0$	$1/5$	0	0	0
$X=1$	$1/5$	0	0	0
$X=2$	0	1	0	0
$X=3$	$1/5$	0	0	0
$X=4$	0	0	1	0
$X=5$	$1/5$	0	0	0
$X=4$	0	0	0	1
$X=5$	$1/5$	0	0	0

,

where $p(Y=0) = 5/8$, $p(Y=2) = 1/8$, $p(Y=4) = 1/8$, and $p(Y=6) = 1/8$.

(c) Compute the prior Bayes vulnerability, the posterior Bayes vulnerability, and the multiplicative and additive Bayes leakage for this piece of code when the input distribution on secrets is uniform.

Instructor's solution: The prior Bayes vulnerability can be computed as

$$V(\pi) = \max_{x \in \mathcal{X}} \pi_x = 1/8.$$

The posterior Bayes vulnerability can be computed as follows. First we compute the Bayes vulnerability for each possible output of the channel:

$$\begin{aligned}
V(p(X \mid Y = 0)) &= \max_{x \in \mathcal{X}} p(X \mid Y = 0) = \frac{1}{5}, \\
V(p(X \mid Y = 2)) &= \max_{x \in \mathcal{X}} p(X \mid Y = 2) = 1, \\
V(p(X \mid Y = 4)) &= \max_{x \in \mathcal{X}} p(X \mid Y = 4) = 1, \qquad \text{and} \\
V(p(X \mid Y = 6)) &= \max_{x \in \mathcal{X}} p(X \mid Y = 6) = 1.
\end{aligned}$$

Then we compute posterior Bayes vulnerability by weighting the above values with the corresponding probability of the output.

$$\begin{aligned}
V\left[\pi\rangle C\right] &= \sum_{y \in \mathcal{Y}} p(Y = y) \cdot V(p(X \mid Y = y)) \\
&= p(Y = 0) \cdot V(p(X \mid Y = 0)) + p(Y = 2) \cdot V(p(X \mid Y = 2)) + \\
&\quad p(Y = 4) \cdot V(p(X \mid Y = 4)) + p(Y = 6) \cdot V(p(X \mid Y = 6)) \\
&= \frac{5}{8} \cdot \frac{1}{5} + \frac{1}{8} \cdot 1 + \frac{1}{8} \cdot 1 + \frac{1}{8} \cdot 1 \\
&= \frac{1}{2}.
\end{aligned}$$

Hence, the multiplicative Bayes leakage of this piece of code under the uniform prior is

$$\mathcal{L}^{\times}(\pi, C) = \frac{V_g\left[\pi\rangle C\right]}{V_g(\pi)} = \frac{1/2}{1/8} = 4,$$

and the corresponding additive Bayes leakage is

$$\mathcal{L}^{+}(\pi, C) = V\left[\pi\rangle C\right] - V(\pi) = \frac{1}{2} - \frac{1}{8} = \frac{3}{8}.$$