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

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.

   (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).

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

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

      i. Shannon entropy.
      ii. Bayes vulnerability.
      iii. Guessing entropy.

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

   (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?

   (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.

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

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.

(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.

(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.