Quantitative Information Flow (QIF) **DCC/ICEx/UFMG**
Prof. Mário S. Alvim **2021/1**

PROBLEM SET

Introduction

(Chapter 01)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 1: *Introduction*
    - Chapter 1.1: *A first discussion of information leakage*
    - Chapter 1.2: *Looking ahead*

Review questions.

1. Explain what are the main goals of the study of quantitative information flow (QIF).
2. Give an example of a system that could potentially leak sensitive information through observable outputs.

Exercises.

3. (Exercise 1.1) Recall dice channel C from §1.1, defined by $\mathsf{C}(r, w) = r+w$. Now consider a channel E that instead outputs the *maximum* of the two dice, so that $\mathsf{E}(r, w) = \max\{r, w\}$. Assuming a uniform prior distribution $\boldsymbol{\vartheta}$, find the additive and multiplicative Bayes leakage of E. What partition of $\mathcal{X}$ does E give?
4. (Exercise 1.2) Consider an election in which k voters choose between candidates A and B. Ballots are supposed to be secret, of course, so we can take the sequence of votes cast to be the secret input X. (For example, if $k = 3$ then the set $\mathcal{X}$ of possible values for X is $\{AAA, AAB, ABA, ABB, BAA, BAB, BBA, BBB\}$.) Assuming a uniform prior $\boldsymbol{\vartheta}$, the prior Bayes vulnerability $V_1(\boldsymbol{\vartheta}) = 2^{-k}$, since there are 2^k possible sequences of votes, each occurring with probability 2^{-k}.

   When the election is tallied, the number of votes for each candidate is made public. (For example, when $k = 8$ we might get the vote sequence $AABABAAB$, whose tally is 5 votes for A and 3 votes for B.) Note that election tabulation can be seen as a *deterministic channel* T from X to Y, where Y is the tally of votes.

   (a) Given k, what is the multiplicative Bayes leakage $\mathcal{L}_1^{\times}(\boldsymbol{\vartheta}, \mathsf{T})$ of the election tabulation channel?

   (b) Suppose we want the *posterior Bayes vulnerability* $V_1[\boldsymbol{\vartheta} \triangleright \mathsf{T}]$ to be at most $1/8$. Determine the minimum value of k that achieves that bound.