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

PROBLEM SET

Modeling secrets / On g-vulnerability
(Chapters 02 / 03)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 2: *Modeling secrets*
    - Chapter 2.1: *Secrets and probability distributions*
    - Chapter 2.2: *Shannon entropy*
    - Chapter 2.3: *Bayes vulnerability*
    - Chapter 2.4: *A more general view*
  - Chapter 3: *On g-vulnerability*
    - Chapter 3.1: *Basic definitions*
    - Chapter 3.2: *A catalog of gain functions*
    - Chapter 3.3: *Classes of gain functions*
    - Chapter 3.4: *Mathematical properties*
    - Chapter 3.5: *On "absolute" versus "relative" security*

Review questions.

1. Provide a brief description of the g-vulnerability framework, including a clear definition of secrets, actions, gain-functions, and g-vulnerability itself.

2. Describe what is meant by the "operational interpretation/significance" of a vulnerability measure. How does the g-vulnerability framework allows for the expression of different operational interpretations?

Exercises.

3. (Exercise 2.1) Recall that 3 flips of a fair coin results in a uniform prior π^{coin} on the 8 values HHH, HHT, HTH, HTT, THH, THT, TTH, and TTT. What is the prior π^{bent} that results from 3 flips of a *bent* coin that gives heads with probability $2/3$ and tails with probability $1/3$? Compare the Shannon entropies $H(\pi^{coin})$ and $H(\pi^{bent})$ and the Bayes vulnerabilities $V_1(\pi^{coin})$ and $V_1(\pi^{bent})$.

4. (Exercise 3.1) Let us explore g-vulnerability in the context of a hypothetical lottery. Suppose that the lottery sells tickets for \$2 each, in which the purchaser marks 6 choices out of the numbers from 1 to 40. (For example, the purchaser might mark 3, 23, 24, 31, 33, and 40.)

   Then a drawing is held in which 6 such numbers are selected randomly. Suppose that the rules are that a ticket wins only if it exactly matches the 6 selected numbers, in which case the player gets \$5 million; otherwise, the player gets nothing. (Real lotteries have more complicated rules!)

   (a) Design a gain function g suitable for modeling this lottery. The set $\mathcal{X}$ of possible secret values x is the set of all sets of 6 numbers from 1 to 40. Let the set $\mathcal{W}$ of possible actions include "buy t" for each set t of 6 numbers from 1 to 40, along with the action "don't play".

(b) Calculate the g-vulnerability $V_g(\boldsymbol{\vartheta})$, assuming that $\boldsymbol{\vartheta}$ is uniform. Which action is optimal?

5. (Exercise 3.2) Let g be a gain function with the following matrix representation:

G	x_1	x_2
w_1	3	-1
w_2	-8	2

Give a prior π such that $V_g(\pi) < 0$, which implies that $g \notin \mathbb{G}\mathcal{X}$.