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

SOLUTION OF PROBLEM SET

Axiomatics / The geometry of hypers, gains and losses / The Crowds protocol
(Chapters 11 / 12 / 18)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 11: *Axiomatics*
    - Chapter 11.1: *An axiomatic view of vulnerability*
    - Chapter 11.2: *Axiomatization of prior vulnerabilities*
    - Chapter 11.3: *Axiomatization of posterior vulnerabilities*
    - Chapter 11.4: *Applications of axiomatization to understanding leakage measures*
  - Chapter 12: *The geometry of hypers, gains and losses*
    - Chapter 12.1: *Barycentric representation of gain/loss functions*
    - Chapter 12.2: *Barycentric representation of hypers and their refinement*
  - Chapter 18: *The Crowds protocol*
    - Chapter 18.1: *Introduction to Crowds, and its purpose*
    - Chapter 18.2: *Modeling the Crowds protocol*
    - Chapter 18.3: *Bayes vulnerability and Bayes leakage*
    - Chapter 18.4: *Explanation of the paradox*
    - Chapter 18.5: *Why φ matters, even for uniform priors*
    - Chapter 18.6: *Refinement: increasing φ is always safe*
    - Chapter 18.7: *Multiple paths*

Review questions.

1. Explain in your own words what the following axioms for prior vulnerabilities mean.
   (a) Continuity (`CNTY`).
   (b) Convexity (`CVX`).

   Instructor's solution:

   (a) The axiom of continuity (`CNTY`) states that a prior vulnerability is continuous wrt. the prior distribution. Intuitively, this means that an adversary should not be infinitely risk-averse: "small" changes in her knowledge should cause "small" changes in the corresponding prior vulnerability.

   (b) The axiom of convexity (`CVX`) states that a prior vulnerability is a convex function of its input, i.e., prior distribution. Intuitively, this means that the expected value of the function should always be greater than the function of expected value. An explanation of this intuition as a game is given in the textbook.

2. Explain in your own words what the following axioms for posterior vulnerabilities mean.

   (a) Noninterference (`NI`).

   (b) Data-processing inequality (`DPI`).

   (c) Monotonicity (`MONO`).

   Instructor's solution:

   (a) The axiom of noninterference (`NI`) intuitively means that a channel that doesn't reveal any information should cause no leakage.

   (b) The axiom of data-processing inequality (`DPI`) intuitively means that post-processing the output of a channel can never increase information.

   (c) The axiom of monotonicity (`MONO`) intuitively means that a channel cannot cause "negative" leakage, in the sense that its output cannot decrease the adversary's information about the secret.

3. Explain in your own words what the following axioms relating prior and posterior vulnerabilities mean.

   (a) Averaging (`AVG`).

   (b) Maximum (`MAX`).

   Instructor's solution:

   (a) The axiom of averaging (`AVG`) states that posterior vulnerability is the expected value of prior vulnerability taken on the hyper coming out of a channel. This intuitively means the leakage measure is "rational", and takes into account expected value.

   (b) The axiom of maximum (`MAX`) intuitively states that posterior vulnerability is the maximum vulnerability value of the inners in the support of the outer of the hyper coming out of a channel. This intuitively means the leakage measure is "pessimistic" (from the point of view of who's protecting the secret value), and takes into account the worst possible scenario.

4. Explain in your own words the significance of the relationship among axioms depicted in Figure 11.1.

   Instructor's solution: The figure represents the fact that noninterference (`NI`) is an immediate consequence of averaging (`AVG`). Moreover, under averaging (`AVG`), the axioms of convexity (`CVX`), data-processing inequality (`DPI`), and monotonicity (`MONO`) are all equivalent, in the sense that if a pair of prior/posterior vulnerability definitions satisfies any of them, then it satisfies all of them.

Exercises.

5. (Exercise 12.1) Explain why the first action of a channel on a prior seems to reveal more (non-negative leakage), but subsequent multiplications (by refinement/post-processing matrices) loses information (the data-processing inequality *DPI* of §4.6.2).

Instructor's solution: The first and subsequent operations are not the same. Write the "pushing in" as matrix multiplication of the "diagonal prior" by the channel, so that everything is now matrix multiplication. Then the starting point is actually the joint distribution that reveals everything, and the matrix multiplication decreases that (makes it more secure), just as the subsequent multiplications do. In fact the diagonal prior, as a hyper, is concentrated (with different weights) at the vertices (only) of the barycentric diagram.

6. (Exercise 18.2) In §18.6 is was shown rigorously that increasing the forwarding probability φ results in a refinement of the protocol, i.e. that for any prior and gain function the effect of increasing φ cannot be to increase the adversary's gain — increasing φ can never do any harm.

   But from that it is elementary that *decreasing* φ cannot *decrease* the adversary's gain (because then increasing φ back to its original value would contradict the above). Thus decreasing φ can never do any good.

   If that reasoning is so elementary, why do we bother to prove the "only if" for Thm. 18.3?

   Instructor's solution: It is indeed elementary that *decreasing* φ cannot do any good. What the "only if" shows is more: that if you strictly decrease φ then there is *guaranteed* to exist a prior and a gain function such that the gain strictly decreases also. It's the difference between "not doing any good" and "definitely harmful".

   Results like that illustrate the astonishing significance of refinement.