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

PROBLEM SET

Channels

(Chapter 04)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 4: *Channels*
    - Chapter 4.1: *Channel matrices*
    - Chapter 4.2: *The effect of a channel on the adversary's knowledge*
    - Chapter 4.3: *From joint distributions to hyper-distributions*
    - Chapter 4.4: *Abstract channels*
    - Chapter 4.5: *More on abstract channels*
    - Chapter 4.6: *A first look at channel compositions*

Review questions.

1. Define an information-theoretic channel, and describe the effect of a channel on the adversary's knowledge about the channel's input.

2. Specify what a hyper-distribution is, explaining the concept of inner-distributions and outer distributions. Explain why a hyper-distribution is an appropriate model for the adversary's posterior knowledge.

3. What are abstract channels, and why are they relevant in QIF?

Exercises.

4. (Exercise 4.1) Compute the hyper $[\vartheta \triangleright \mathsf{C}]$ when $\vartheta = (1/4, 1/4, 1/4, 1/4)$ and C is

C	y_1	y_2	y_3	y_4
x_1	$1/2$	$1/2$	0	0
x_2	0	0	1	0
x_3	$1/2$	$1/4$	0	$1/4$
x_4	$1/8$	$1/8$	$1/4$	$1/2$

.

5. (Exercise 4.2) A password checker tests whether a guessed password is correct or not, outputting "accept" or "reject". This can be modeled as a *family* of channel matrices C^{g}, parameterized by the guess g, and whose secret input X is the correct password. [1] For instance, with 3-bit passwords and

[1] To clarify, the *correct password* X is the secret input to the checker; it is input when that password is created. The *guess* g is *not* a secret input to the checker, but instead a *parameter* that selects which channel matrix in the family is to be used.

guess 110, we get the following channel matrix:

C^{110}	reject	accept
000	1	0
001	1	0
010	1	0
011	1	0
100	1	0
101	1	0
110	0	1
111	1	0

.

Channel matrix C^{g} models the unavoidable information leakage inherent in password checking. (Recall the remarks about `Access Denied`, in the Preface.) But an *implementation* of the checker might work by comparing the guess and the correct password bit by bit, and rejecting as soon as a mismatch is found. In that case, the running time of the implementation is proportional to the length of the maximum correct prefix of the guess, resulting in a *timing side-channel*. Assuming that the adversary can observe that time precisely, the implementation is then more accurately modeled as a family of channels D^{g} whose set of possible outputs (still assuming 3-bit passwords) is $\{(\text{reject}, 1), (\text{reject}, 2), (\text{reject}, 3), \text{accept}\}$, reflecting the fact that the first mismatch can occur at the first, second, or third bit of g.

(a) Show the channel matrix D^{110}.

(b) Compute the two hyper-distributions $[\boldsymbol{\vartheta} \triangleright \mathsf{C}^{110}]$ and $[\boldsymbol{\vartheta} \triangleright \mathsf{D}^{110}]$ for the uniform prior $\boldsymbol{\vartheta} = (1/8, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8)$.

6. (Exercise 4.3) Prove Theorem 4.3 rigorously, with careful calculational steps and using the $p()$ notation.

7. (Exercise 4.4) Suppose that C is a channel matrix whose rows are all the same. What does its reduced matrix C^r look like? What abstract channel does it denote?