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

SOLUTION OF 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.

   Instructor's solution: A channel is a probabilistic mapping from an input set $\mathcal{X}$ to an output set $\mathcal{Y}$. More precisely, a channel $\mathsf{C} : \mathcal{X} \to \mathbb{D}\mathcal{Y}$ maps each $x \in \mathcal{X}$ to a distribution on $\mathcal{Y}$.

   By observing an output $y \in \mathcal{Y}$ of the channel, the adversary can update her knowledge about the secret from a prior distribution π to a conditional probability distribution $p_{X|y}$. This is done via Bayesian updating, and assuming that the adversary knows how the channel C works.

   For a given output y, the conditional probabilities $p(x|y)$ for each x in $\mathcal{X}$ form the posterior distribution $p_{X|y}$. This represents the posterior knowledge that the adversary has about input X after observing output y. Each posterior distribution $p_{X|y}$, for y in $\mathcal{Y}$, represents a different state of knowledge, or "world", hat an adversary seeing the output of C can end up in; and the posterior occurs when the output is y, and that output y itself occurs with probability $p(y)$.

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.

   Instructor's solution: If $\mathcal{X}$ is a finite set (of possible secret values), a *hyper-distribution* (or just a *hyper*) Δ is a distribution on distributions on $\mathcal{X}$, so that Δ has type $\mathbb{D}(\mathbb{D}\mathcal{X})$, which we abbreviate to $\mathbb{D}^2\mathcal{X}$. We recall that the support $\lceil\Delta\rceil$ of Δ is the set of distributions to which Δ gives positive probability (i.e. $\lceil\Delta\rceil = \{\delta : \mathbb{D}\mathcal{X} \mid \Delta_\delta > 0\}$) and we assume that set to be finite; they are the set of possible "worlds" under Δ and we call them the *inner distributions*, or just the *inners*, of Δ. We call the distribution on the inners themselves as the *outer distribution* of Δ.

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

Instructor's solution: The *abstract channel* C denoted by channel matrix C is the mapping of type $\mathbb{D}\mathcal{X} \to \mathbb{D}^2\mathcal{X}$ that C gives, namely $\pi \mapsto [\pi \triangleright \mathsf{C}]$. We use semantic brackets for that denotation, writing $C = [\![\mathsf{C}]\!]$.

A fundamental principle of QIF is that the information-theoretic essence of a channel matrix C is a mapping from priors π to hyper-distributions $[\pi \triangleright \mathsf{C}]$. More precisely, the effect of a channel C is to update an adversary's prior knowledge on the channel's input, modeled as a distribution $\pi : \mathbb{D}\mathcal{X}$, to some posterior knowledge $[\pi \triangleright \mathsf{C}] : \mathbb{D}^2\mathcal{X}$ consisting in a distribution on distributions, known as a hyper-distribution.

Channel matrices contain detail that is extraneous to their fundamental meaning (labels in $\mathcal{Y}$, order of rows, etc.) Abstract channels keep only relevant information wrt. information leakage. Abstract channel facilitate the mathematical approach to other results we'll see in this course (including on composition and on refinement of channels).

Exercises.

4. (Exercise 4.1) Compute the hyper $[\boldsymbol{\vartheta} \triangleright \mathsf{C}]$ when $\boldsymbol{\vartheta} = (1/4, 1/4, 1/4, 1/4)$ 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	$1/8$	$1/8$	$1/4$	$1/2$

.

Instructor's solution:

$[\boldsymbol{\vartheta} \triangleright \mathsf{C}]$	$9/32$	$7/32$	$5/16$	$3/16$
x_1	$4/9$	$4/7$	0	0
x_2	0	0	$4/5$	0
x_3	$4/9$	$2/7$	0	$1/3$
x_4	$1/9$	$1/7$	$1/5$	$2/3$

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 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

[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.

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 $\boldsymbol{\vartheta} = (1/8, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8)$.

Instructor's solution:

(a)

D^{110}	(reject, 1)	(reject, 2)	(reject, 3)	accept
000	1	0	0	0
001	1	0	0	0
010	1	0	0	0
011	1	0	0	0
100	0	1	0	0
101	0	1	0	0
110	0	0	0	1
111	0	0	1	0

(b)

$[\boldsymbol{\vartheta} \triangleright \mathsf{C}^{110}]$	7/8	1/8
000	1/7	0
001	1/7	0
010	1/7	0
011	1/7	0
100	1/7	0
101	1/7	0
110	0	1
111	1/7	0

$[\boldsymbol{\vartheta} \triangleright \mathsf{D}^{110}]$	1/2	1/4	1/8	1/8
000	1/4	0	0	0
001	1/4	0	0	0
010	1/4	0	0	0
011	1/4	0	0	0
100	0	1/2	0	0
101	0	1/2	0	0
110	0	0	0	1
111	0	0	1	0

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

Instructor's solution: Here is the calculational proof — still elementary, but given to illustrate the use of the $p()$ notations. Based on the above and the assumption that the "implicit J" is $\pi \triangleright \mathsf{C}$ for π and some C, we calculate

$$
\begin{array}{lll}
 & (\sum_y p(y)\, p_{X|y})(x) & \\
= & \sum_y p(y)\, p_{X|y}(x) & \text{“pointwise arithmetic”} \\
= & \sum_y p(y)\, {}^{p(x,y)}\!/_{p(y)} & \text{“definition } p_{X|y}\text{”} \\
= & \sum_y p(x,y) & \text{“assume no } p(y)\text{'s are zero”} \\
= & p_X(x) & \text{“definition } p_X\text{”} \\
= & \pi_x & \text{“}J = \pi \triangleright \mathsf{C}\text{”}
\end{array}
$$

whence, since x was arbitrary, we have $\sum_y p(y)\, p_{X|y} = \pi$.

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?

Instructor's solution: All of C's nonzero columns are similar, so C^r consists of a single column of 1's. The corresponding abstract channel is $\mathbb{1}$.