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

SOLUTION OF PROBLEM SET

Robustness / Capacity
(Chapters 06 / 07)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 6: *Robustness*
    * Chapter 6.1: *The need for robustness*
    * Chapter 6.2: *Approaches to robustness*
  - Chapter 7: *Capacity*
    * Chapter 7.1: *Multiplicative Bayes capacity*
    * Chapter 7.2: *Additive Bayes capacity*
    * Chapter 7.3: *General capacities*
    * Chapter 7.4: *Multiplicative capacities*
    * Chapter 7.5: *Additive capacities*
    * Chapter 7.6: *Obtaining bounds on leakage*

Review questions.

1. Briefly explain in your own words why *robustness* is a concern in QIF.

   Instructor's solution: When measuring the leakage of a channel C we need to specify a prior π on secrets and a gain function g, and make assumptions about the environment in which the channel we run. If our choice of π and/or g is incorrect, or our assumptions about the environment fail, the computed value of the leakage of of C under π and g may be misleading.

   The concern about *robustness*, then, regards how confident we can be that our leakage assessment is meaningful in practice, given such uncertainties.

2. Explain what is the concept of *capacity*.

   Instructor's solution: Capacity is the maximum leakage of a channel C, taken over a set of gain functions and/or a set of priors in $\mathcal{D} \subseteq \mathbb{D}\mathcal{X}$.

   Formally, for classes $\mathcal{G} \subseteq \mathbb{G}\mathcal{X}$, $\mathcal{D} \subseteq \mathbb{D}\mathcal{X}$ and channel C, the multiplicative and additive $(\mathcal{G}, \mathcal{D})$-*capacities* of C are given by

$$
\begin{aligned}
\mathcal{ML}^{\times}_{\mathcal{G}}(\mathcal{D}, C) \;&:=\; \sup_{g\colon \mathcal{G}, \pi\colon \mathcal{D}} \mathcal{L}^{\times}_{g}(\pi, C) \qquad \text{and} \\
\mathcal{ML}^{+}_{\mathcal{G}}(\mathcal{D}, C) \;&:=\; \sup_{g\colon \mathcal{G}, \pi\colon \mathcal{D}} \mathcal{L}^{+}_{g}(\pi, C) \quad .
\end{aligned}
$$

Exercises.

3. Consider the channel C realized by the matrix C below, the gain function g realized by the matrix G also below, and the prior $\pi = (0.2, 0.3, 0.0, 0.5)$.

C	y_1	y_2	y_3	y_4
x_1	0.8	0.0	0.0	0.2
x_2	0.2	0.4	0.1	0.3
x_3	0.1	0.5	0.3	0.1
x_4	0.2	0.0	0.1	0.7

G	x_1	x_2	x_3	x_4
w_1	0.3	1.0	0.0	0.2
w_2	0.7	0.0	0.5	0.5

Use the results we have seen to either compute efficiently the following capacities or to explain why you couldn't.

(a) $\mathcal{ML}_g^{\times}(\mathbb{D}, C)$

(b) $\mathcal{ML}_{\mathbb{G}^+}^{\times}(\pi, C)$

(c) $\mathcal{ML}_{\mathbb{G}^+}^{\times}(\mathbb{D}, C)$

(d) $\mathcal{ML}_g^{+}(\mathbb{D}, C)$

(e) $\mathcal{ML}_{\mathbb{G}\updownarrow}^{+}(\pi, C)$

(f) $\mathcal{ML}_{\mathbb{G}\updownarrow}^{+}(\mathbb{D}, C)$

Instructor's solution:

(a) It's unknown whether there is an efficient algorithm to find the capacity $\mathcal{ML}_g^{\times}(\mathbb{D}, C)$.

(b) Since $g \in \mathbb{G}^+$ (all its values are non-negative), and noting that $\lceil\pi\rceil = \{x_1, x_2, x_4\}$, we can we can reason

$$\begin{array}{lll} & \mathcal{ML}_{\mathbb{G}^+}^{\times}(\pi, C) & \\ = & \sum_{y:\mathcal{Y}} \max_{x:\lceil\pi\rceil} \mathsf{C}_{x,y} & \text{“Thm. 7.14”} \\ = & 0.8 + 0.4 + 0.1 + 0.7 & \\ = & 2.0 & \end{array}$$

(c) Since $g \in \mathbb{G}^+$ (all its values are non-negative), we can we can reason

$$\begin{array}{lll} & \mathcal{ML}_{\mathbb{G}^+}^{\times}(\mathbb{D}, C) & \\ = & \sum_{y:\mathcal{Y}} \max_{x:\mathcal{X}} \mathsf{C}_{x,y} & \text{“Thm. 7.5 (Miracle)”} \\ = & 0.8 + 0.5 + 0.3 + 0.7 & \\ = & 2.3 & \end{array}$$

(d) By Thm. 7.12 we know that probably there isn't an efficient algorithm to compute $\mathcal{ML}_g^{+}(\mathbb{D}, C)$, since its corresponding decision problem is NP-Complete.

(e) Since $g \in \mathbb{G}\updownarrow$ (all its values are at most 1), and noting that $\lceil\pi\rceil = \{x_1, x_2, x_4\}$, we can reason

$$\begin{array}{lll} & \mathcal{ML}_{\mathbb{G}\updownarrow}^{+}(\pi, C) & \\ = & 1 - \sum_{y:\mathcal{Y}} \min_{x:\lceil\pi\rceil} \mathsf{C}_{x,y} & \text{“Thm. 7.21”} \\ = & 1 - (0.2 + 0.0 + 0.0 + 0.2) & \\ = & 0.6 & \end{array}$$

(f) Since $g \in \mathbb{G}\updownarrow$ (all its values are at most 1), we can reason

$$\begin{array}{lll} & \mathcal{ML}_{\mathbb{G}\updownarrow}^{+}(\mathbb{D}, C) & \\ = & 1 - \sum_{y:\mathcal{Y}} \min_{x:\mathcal{X}} \mathsf{C}_{x,y} & \text{“Thm. 7.21”} \\ = & 1 - (0.1 + 0.0 + 0.0 + 0.1) & \\ = & 0.8 & \end{array}$$

4. (Exercise 6.1) Recall the dice channels C and D from Section 1.1., whose input is the value (r, w) resulting from throwing a red die and a white die and defined by $\mathsf{C}(r, w){:=}\ r + w$ and $\mathsf{D}(r, w){:=}\ r \cdot w$. Recall that with *fair* dice, C's multiplicative Bayes leakage is 11, while D's is 18. Show that with *biased* dice, it is possible to make C's multiplicative Bayes leakage *exceed* D's.

Instructor's solution: Bias the red die always to produce 1 or 2, each with probability $1/2$. Bias the white die to produce 3 or 6, each with probability $1/2$. Then the prior is uniform on $\{(1,3),(1,6),(2,3),(2,6)\}$. And then we can compute that C's multiplicative Bayes leakage is 4, while D's is 3.

5. (Exercise 7.1) Let C be a channel matrix from $\mathcal{X}$ to $\mathcal{Y}$. Show that for any $g{:}\,\mathbb{G}^{+}\mathcal{X}$ and any prior, its multiplicative g-leakage is bounded by both $|\mathcal{X}|$ and $|\mathcal{Y}|$. Does the result necessarily hold if g is not in $\mathbb{G}^{+}\mathcal{X}$?

Instructor's solution: For any channel C, prior π, and non-negative gain function $g{:}\,\mathbb{G}^{+}\mathcal{X}$, we have

$$
\begin{array}{lll}
 & \mathcal{L}^{\times}_{g}(\pi, C) & \\
\leq & \sum_{y:\mathcal{Y}} \max_{x:\mathcal{X}} \mathsf{C}_{x,y} & \text{“Thm. 7.5 (Miracle)”} \\
\leq & \sum_{y:\mathcal{Y}} \sum_{x:\mathcal{X}} \mathsf{C}_{x,y} & \text{“}\max_{x:\mathcal{X}} \mathsf{C}_{x,y} \leq \sum_{x:\mathcal{X}} \mathsf{C}_{x,y}\text{”} \\
\leq & \sum_{x:\mathcal{X}} \sum_{y:\mathcal{Y}} \mathsf{C}_{x,y} & \text{“rearranging sums”} \\
\leq & \sum_{x:\mathcal{X}} 1 & \text{“}\sum_{y:\mathcal{Y}} \mathsf{C}_{x,y} = 1\text{”} \\
= & |\mathcal{X}| &
\end{array}
$$

For any channel C, prior π, and non-negative gain function $g{:}\,\mathbb{G}^{+}\mathcal{X}$, we have

$$
\begin{array}{lll}
 & \mathcal{L}^{\times}_{g}(\pi, C) & \\
\leq & \sum_{y:\mathcal{Y}} \max_{x:\mathcal{X}} \mathsf{C}_{x,y} & \text{“Thm. 7.5 (Miracle)”} \\
\leq & \sum_{y:\mathcal{Y}} 1 & \text{“}\max_{x:\mathcal{X}} \mathsf{C}_{x,y} \leq 1\text{”} \\
= & |\mathcal{Y}| &
\end{array}
$$

6. (Exercise 7.4) Suppose that C is a deterministic channel matrix, meaning that all its entries are either 0 or 1. Show that $\mathcal{ML}^{+}_{\mathbb{G}\updownarrow}(\mathbb{D}, \mathsf{C})$, that is C's additive capacity over 1-bounded gain functions and all priors, has only *two* possible values.

Instructor's solution: By Thm. 7.21 we know that $\mathcal{ML}^{+}_{\mathbb{G}\updownarrow}(\mathbb{D}, \mathsf{C})$ is 1 minus the sum of the column minimums of C. Now, if C is deterministic then each row contains a single 1 entry, and all other entries 0. Hence there are just two possibilities: either all rows of C have their 1 entry in the same column, or else each column of C contains at least one 0 entry. In the former case $\mathcal{ML}^{+}_{\mathbb{G}\updownarrow}(\mathbb{D}, \mathsf{C})$ is 0 (and indeed C is the non-interfering channel $\mathbb{1}$), and in the latter case it is 1, which is as big as possible. (That result is reminiscent of the fact that an interfering deterministic mechanism can never be ϵ-differentially private, for any ϵ.)