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.

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

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) $\mathcal{ML}^{\times}_{g}(\mathbb{D}, C)$

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

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

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

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

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

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.

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 $\mathbb{G}^{+}\mathcal{X}$?

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.