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

PROBLEM SET

Composition of channels
(Chapter 08)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 8: *Composition of channels*
    - Chapter 8.1: *Compositions of (concrete) channel matrices*
    - Chapter 8.2: *Compositions of abstract channels*

Review questions.

1. Explain in your own words what the definition of *compositionality* (Def. 8.6) means.

2. Explain in your own words why the operation of cascading isn't compositional.

Exercises.

3. Recall Definition 8.1 of parallel composition of channel matrices. Prove that for any two compatible channel $\mathsf{C}^1\colon \mathcal{X} \rightarrowtriangle \mathcal{Y}^1$ and $\mathsf{C}^2\colon \mathcal{X} \rightarrowtriangle \mathcal{Y}^2$, their parallel composition $\mathsf{C}^1 \| \mathsf{C}^2$ is a proper channel (i.e., all of its entries are non-negative, and all of its rows add up to 1.)

4. (Exercise 8.1) Recall Def. 8.8 of abstract-channel parallel composition. Use the matrices $\mathsf{C}^{1,2}$ from §8.1.1 on concrete-channel parallel composition, and the uniform prior distribution $\boldsymbol{\vartheta}$ over $\mathcal{X} = \{x_1, x_2\}$, to illustrate the correspondence between the abstract and the concrete definitions.

   In particular, show that $[\boldsymbol{\vartheta} \triangleright \mathsf{C}^1]$ is the hyper-distribution

	$3/5$	$2/5$
x_1	$1/3$	$3/4$
x_2	$2/3$	$1/4$

   ,

   so that the inners δ, δ', over which the summation on the right-hand side of Def. 8.8 is taken, are the two shown above: that is, $(1/3, 2/3)$ and $(3/4, 1/4)$. The corresponding values of $\mathsf{C}^1(\boldsymbol{\vartheta})_\delta$ and $\mathsf{C}^1(\boldsymbol{\vartheta})_{\delta'}$ are then the two outers $3/5$ for δ and $2/5$ for δ'.

   Then calculate the hypers $[\delta \triangleright \mathsf{C}^2]$ and $[\delta' \triangleright \mathsf{C}^2]$ to complete the summation in Def. 8.8, and verify that the result is indeed $[\boldsymbol{\vartheta} \triangleright (C^1 \| C^2)]$ where $C^1 \| C^2$ is as calculated in the example following Def. 8.1.

   Will $\mathsf{C}^2 \| \mathsf{C}^1$ give the same result?

5. (Exercise 8.5) Our motivating example for internal choice was in fact the composition $\mathbb{0}\ {}_{1/2}\!\oplus \mathbb{1}$, where we interpreted $\mathbb{0}, \mathbb{1}$ in their *concrete* form, i.e. both as matrices of type $\{x_1, x_2\} \rightarrowtriangle \{y_1, y_2\}$. What is the channel matrix for that composition?

6. (Exercise 8.6) Recall §8.1.6. Give a definition of internal conditional choice analogous to Def. 8.3. Work out the behavior of this new composition on the same channels used in §8.1.3 to illustrate the behavior of external conditional choice.

7. (Exercise 8.7) Recall §8.1.7. Give a definition of internal (general) probabilistic choice analogous to Def. 8.4. Work out the behavior of this new composition on the same channels used in §8.1.4 to illustrate the behavior of external (general) probabilistic choice.

8. (Exercise 8.11) Prove that $\mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}_1 \parallel \mathsf{C}_2) \ \leq\ \mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}_1) \times \mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}_2)\,.$