SOLUTION OF 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.

   Instructor's solution: Intuitively the *compositionality* of Def. 8.6 is the property that a concrete operator corresponds an abstract operator st. the two following are equivalent:

   (i) First applying the concrete operator to concrete objects, followed by taking the semantics of the result.

   (ii) First taking the semantics of the concrete objects, then applying the abstract operator to the result.

   This is relevant

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

   Instructor's solution: Intuitively the operation of cascading depends on the exact labeling of the channels involved (more precisely, that of the first channel). Since abstract channels don't keep information about labels, there can't be a way to represent cascading at an abstract level.

Exercises.

3. Recall Definition 8.1 of parallel composition of channel matrices. Prove that for any two compatible channel $\mathsf{C}^1 : \mathcal{X} \to \mathcal{Y}^1$ and $\mathsf{C}^2 : \mathcal{X} \to \mathcal{Y}^2$, 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.)

Instructor's solution: By Definition 8.1, for every $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}^1$, and $y_2 \in \mathcal{Y}^2$, the corresponding entry in the parallel composition is given by $(\mathsf{C}^1 \| \mathsf{C}^2)_{x,(y_1,y_2)} = \mathsf{C}^1_{x,y_1} \times \mathsf{C}^2_{x,y_2}$, which is always non-negative because both both C^1_{x,y_1} and C^2_{x,y_2} are non-negative (since C^1 and C^2 are proper channels).

Now, notice that in every row x of $\mathsf{C}^1 \| \mathsf{C}^2$ we have:

$$
\begin{array}{lll}
& \sum_{y_1 \in \mathcal{Y}^1, y_2 \in \mathcal{Y}^2} \left[(\mathsf{C}^1 \| \mathsf{C}^2)_{x,(y_1,y_2)} \right] & \\
= & \sum_{y_1 \in \mathcal{Y}^1, y_2 \in \mathcal{Y}^2} \left[\mathsf{C}^1_{x,y_1} \times \mathsf{C}^2_{x,y_2} \right] & \text{“Def. 8.1”} \\
= & \sum_{y_1 \in \mathcal{Y}^1} \mathsf{C}^1_{x,y_1} \sum_{y_2 \in \mathcal{Y}^2} \mathsf{C}^2_{x,y_2} & \text{“Reorganizing summations”} \\
= & \sum_{y_1 \in \mathcal{Y}^1} \mathsf{C}^1_{x,y_1} \cdot 1 & \text{“}\textstyle\sum_{y_2 \in \mathcal{Y}^2} \mathsf{C}^2_{x,y_2} = 1\text{”} \\
= & 1 & \text{“}\textstyle\sum_{y_1 \in \mathcal{Y}^1} \mathsf{C}^1_{x,y_1} = 1\text{”}
\end{array}
$$

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?

Instructor's solution: First, from 8.1.1, by pushing uniform prior $\boldsymbol{\vartheta}$ through C^1, we get

$$[\boldsymbol{\vartheta} \triangleright \mathsf{C}^1] = \begin{array}{|c|c|c|}\hline & 3/5 & 2/5 \\ \hline x_1 & 1/3 & 3/4 \\ x_2 & 2/3 & 1/4 \\ \hline \end{array} \quad .$$

Now, by pushing $(1/3, 2/3)$ into C^2, we get

$$[(1/3, 2/3) \triangleright \mathsf{C}^2] = \begin{array}{|c|c|c|}\hline & 8/15 & 7/15 \\ \hline x_1 & 5/8 & 0 \\ x_2 & 3/8 & 1 \\ \hline \end{array} \quad ,$$

and by pushing $(3/4, 1/4)$ into C^2, we get

$$[(1/3, 2/3) \triangleright \mathsf{C}^2] = \begin{array}{|c|c|c|}\hline & 33/40 & 7/40 \\ \hline x_1 & 10/11 & 0 \\ x_2 & 1/11 & 1 \\ \hline \end{array} \quad .$$

Now, by pushing the uniform prior $\boldsymbol{\vartheta}$ through $\mathsf{C}^1 \parallel \mathsf{C}^2$, we get

$$[\boldsymbol{\vartheta} \triangleright \mathsf{C}^1 \parallel \mathsf{C}^2] = \begin{array}{|c|c|c|c|}\hline & 32/100 & 35/100 & 33/100 \\ \hline x_1 & 5/8 & 0 & 10/11 \\ x_2 & 3/8 & 1 & 1/11 \\ \hline \end{array} \quad .$$

Second, by 8.2.2, taking the uniform prior $\boldsymbol{\vartheta}$, the summation is over the two inners $(1/3, 2/3)$ and $(3/4, 1/4)$, whose weights are $3/5$ and $2/5$, respectively.

So we take

$$\frac{3}{5}\cdot\begin{array}{|c|c|c|}\hline & 8/15 & 7/15 \\ \hline x_1 & 5/8 & 10/11 \\ x_2 & 3/8 & 1/11 \\ \hline\end{array} + \frac{2}{5}\cdot\begin{array}{|c|c|c|}\hline & 33/40 & 7/40 \\ \hline x_1 & 10/11 & 0 \\ x_2 & 1/11 & 1 \\ \hline\end{array} = \begin{array}{|c|c|c|c|c|}\hline & 24/75 & 21/75 & 66/100 & 14/200 \\ \hline x_1 & 5/8 & 0 & 10/11 & 0 \\ x_2 & 3/8 & 1 & 1/11 & 1 \\ \hline\end{array}$$

$$= \begin{array}{|c|c|c|c|}\hline & 32/100 & 35/100 & 33/100 \\ \hline x_1 & 5/8 & 0 & 10/11 \\ x_2 & 3/8 & 1 & 1/11 \\ \hline\end{array} \quad .$$

Yes, you will get the same result, as Exercise 8.2 shows.

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 $\{x_1, x_2\} \to\!\!\!\!\triangleright \{y_1, y_2\}$. What is the channel matrix for that composition?

   Instructor's solution: It is

$$\begin{array}{|c|c|c|}\hline \mathbb{0} & y_1 & y_2 \\ \hline x_1 & 1 & 0 \\ x_2 & 0 & 1 \\ \hline\end{array}\ {}_{1/2}\!\oplus\ \begin{array}{|c|c|c|}\hline \mathbb{1} & y_1 & y_2 \\ \hline x_1 & 1/2 & 1/2 \\ x_2 & 1/2 & 1/2 \\ \hline\end{array} \quad = \quad \begin{array}{|c|c|c|}\hline \mathbb{0}\,{}_{1/2}\!\oplus\mathbb{1} & y_1 & y_2 \\ \hline x_1 & 3/4 & 1/4 \\ x_2 & 1/4 & 3/4 \\ \hline\end{array} \quad .$$

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.

   Instructor's solution: Here is the definition.

   Definition (Internal conditional choice between channel matrices)**.** *Let* $\mathsf{C}^1\colon \mathcal{X} \to\!\!\!\!\triangleright \mathcal{Y}^1$ *and* $\mathsf{C}^2\colon \mathcal{X} \to\!\!\!\!\triangleright \mathcal{Y}^2$ *be compatible channels. Their* internal conditional choice wrt. $\mathcal{A} \subseteq \mathcal{X}$ *is (again) of type* $\mathcal{X} \to\!\!\!\!\triangleright (\mathcal{Y}^1 \cup \mathcal{Y}^2)$ *and is defined*

$$(\mathsf{C}^1 \ll\!\mathcal{A}\!\gg \mathsf{C}^2)_{x,y} \;:=\; \begin{cases} \mathsf{C}^1_{x,y} & \text{if } x{\in}\mathcal{A} \text{ and } y{\in}\mathcal{Y}^1 \\ \mathsf{C}^2_{x,y} & \text{if } x{\notin}\mathcal{A} \text{ and } y{\in}\mathcal{Y}^2 \\ 0 & \text{otherwise.} \end{cases}$$

   As an example, consider the secret input set $\mathcal{X}{=}\{x_1, x_2, x_3, x_4\}$, and the condition $\mathcal{A}$ on them defined by the subset $\{x_1, x_2\}$. The internal conditional choice $\mathsf{C}^1 \ll\!\mathcal{A}\!\gg \mathsf{C}^2$, between channels C^1 and C^2

below, is

C^1	y_1	y_2
x_1	0.5	0.5
x_2	0.3	0.7
x_3	0	1
x_4	0.6	0.4

$\ll\{x_1, x_2\}\gg$

C^2	y_1	y_3
x_1	0.1	0.9
x_2	0.7	0.3
x_3	0.4	0.6
x_4	0.8	0.2

$=$

$\mathsf{C}^1 \ll\{x_1, x_2\}\gg \mathsf{C}^2$	y_1	y_2	y_3
x_1	0.5	0.5	0
x_2	0.3	0.7	0
x_3	0.4	0	0.6
x_4	0.8	0	0.2

.

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.

Instructor's solution: In the following, for each secret value x in $\mathcal{X}$ there is a probability $P(x)$ that the left-hand channel will be used; and with probability $1-P(x)$ the right-hand channel will be used instead.

Definition (Internal probabilistic choice between channel matrices)**.** *Let* $\mathsf{C}^1{:}\,\mathcal{X}\!\to\!\triangleright\mathcal{Y}^1$ *and* $\mathsf{C}^2{:}\,\mathcal{X}\!\to\!\triangleright\mathcal{Y}^2$ *be compatible channels. Their* internal probabilistic choice *wrt. P is of type* $\mathcal{X}\!\to\!\triangleright(\mathcal{Y}^1 \cup \mathcal{Y}^2)$ *and is defined*

$$(\mathsf{C}^1 \,{}_P\!\oplus \mathsf{C}^2)_{x,y} = \begin{cases} P(x)\mathsf{C}^1_{x,y} + (1-P(x))\mathsf{C}^2_{x,y} & \text{if } y \in \mathcal{Y}^1 \cap \mathcal{Y}^2 \\ P(x)\mathsf{C}^1_{x,y} & \text{if } y \in \mathcal{Y}^1 - \mathcal{Y}^2 \\ (1-P(x))\mathsf{C}^2_{x,y} & \text{if } y \in \mathcal{Y}^2 - \mathcal{Y}^1 \end{cases} .$$

As an example, consider the secret input set $\mathcal{X}=\{x_1, x_2, x_3\}$, and let P be the family of distributions below

x	$P(x)$	$1-P(x)$
x_1	0.25	0.75
x_2	1	0
x_3	0.5	0.5

.

The internal probabilistic choice $\mathsf{C}^1 \,{}_P\!\oplus \mathsf{C}^2$, between channels C^1 and C^2 below, is

C^1	y_1	y_2
x_1	0.5	0.5
x_2	0.3	0.7
x_3	0	1

$({}_P\!\oplus)$

C^2	y_1	y_3
x_1	0.1	0.9
x_2	0.7	0.3
x_3	0.4	0.6

$=$

$\mathsf{C}^1({}_P\!\oplus)\mathsf{C}^2$	y_1	y_2	y_3
x_1	0.2	0.125	0.675
x_2	0.3	0.7	0
x_3	0.2	0.5	0.3

.

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

Instructor's solution: For all channels $\mathsf{C}^1 \colon \mathcal{X} \to\!\!\!\triangleright \mathcal{Y}^1$ and $\mathsf{C}^2 \colon \mathcal{X} \to\!\!\!\triangleright \mathcal{Y}^2$, we can reason

$$
\begin{array}{lll}
 & \mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}_1 \parallel \mathsf{C}_2) & \\
= & \sum_{(y^1,y^2) \in \mathcal{Y}^1 \times \mathcal{Y}^2} \max_{x \in \mathcal{X}} (\mathsf{C}^1 \parallel \mathsf{C}^2)_{x,(y^1,y^2)} & \text{“Thm. 7.2”} \\
= & \sum_{y^1 \in \mathcal{Y}^1} \sum_{y^2 \in \mathcal{Y}^2} \max_{x \in \mathcal{X}} \mathsf{C}^1_{x,y^1} \mathsf{C}^2_{x,y^2} & \text{“def. of ‘$\parallel$’”} \\
\leq & \sum_{y^1 \in \mathcal{Y}^1} \sum_{y^2 \in \mathcal{Y}^2} \max_{x \in \mathcal{X}} \mathsf{C}^1_{x,y^1} \max_{x' \in \mathcal{X}} \mathsf{C}^2_{x',y^2} & \text{“directly”} \\
\leq & \sum_{y^1 \in \mathcal{Y}^1} \max_{x \in \mathcal{X}} \mathsf{C}^1_{x,y^1} \sum_{y^2 \in \mathcal{Y}^2} \max_{x' \in \mathcal{X}} \mathsf{C}^2_{x',y^2} & \text{“rearranging the sum”} \\
\leq & \mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}_1) \times \mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}_2) \quad . & \text{“Thm. 7.2”}
\end{array}
$$